جمهوری اسلامی ایران

وزارت علوم تحقیقات و فناوری

آموزش شبکه

از تئوری

تا عمل

Computer Networks Workshop

نصب و راه‌اندازی شبکه (آزمایشگاه شبکه)



ویرایش سوم

رضا رمضانی

دانشجوی دکترای نرم‌افزار

دانشگاه فردوسی مشهد

ramezani.cs@gmail.com

http://ramezani-cs.blogfa.com

نوروز ۱۳۹۲

آنچه در این مجموعه آموزشی می‌خوانید :

- ✓ مفاهیم شبکه‌های کامپیوتری
- ✓ توپولوژی، معماری و تجهیزات شبکه
- ✓ شبکه‌های بی‌سیم و حسگر
- ✓ محاسبات ابرین و کلاستری
- ✓ نرم‌افزارهای ارتباطی
- ✓ راه اندازی شبکه Work Group و Domain
- ✓ ویندوز سرور ۲۰۰۳
- ✓ سیاست‌های گروهی
- ✓ نرم‌افزارهای ISA Server و Packet Tracer
- ✓ و ...



مرجع کامل دروس:

سیستم‌عامل شبکه

نصب و راه‌اندازی شبکه

آزمایشگاه شبکه‌های کامپیوتری

مؤلف: رضا رمضانی

دانشجوی دکتری نرم افزار - دانشگاه فردوسی مشهد

هدیه به ساحت مقدس

حضرت فاطمه زهرا (س) و یوسف گمشده اش

و پیشکش آنان که دل هایشان به وسعت دریاست

و اندیشه هایشان از آن هم وسیع تر...

آنان که به رسم ادب این اوراق را تورق می کنند

گرچه از آن مستغنی اند.



تقدیم به

مامانم ، بابام

و خانواده عزیزم

که با محبت های خالصانه خود

یاد دادند به من

انسان بودن را

حق مؤلف

این جزوه به صورت رایگان در اینترنت توزیع شده است.

تنها عزیزانی حق استفاده از مطالب جزوه را دارند که با استفاده از نرم‌افزار زیر،

اطلاعات خود را در سامانه ثبت کرده باشند.

http://ramezani-cs.ugig.ir/users.exe

http://ramezani-cs.blogfa.com

هر گونه استفاده از مطالب جزوه با ذکر منبع بلامانع است.

عنوان ارجاع: رضا رمضانی؛ "نصب و راه‌اندازی شبکه (آزمایشگاه شبکه)"؛ ویرایش سوم

پیشگفتار

خداوند منان را شاکرم که مجددا توفیق خدمت در زمینه علم و دانش را به بنده عطا فرمود و توانستم با انتشار **نسخه سوم** از جزوه **نصب و راه‌اندازی شبکه (آزمایشگاه شبکه‌های کامپیوتری)**، گام کوچکی در این زمینه بردارم. همانطوری که می‌دانید یکی از مهمترین دروس دانشجویان رشته کامپیوتر، درس *آزمایشگاه شبکه‌های کامپیوتری*، *نصب و راه‌اندازی شبکه* و *سیستم‌عامل شبکه* است. زیرا امروزه اکثر شرکت‌ها و سازمان‌ها، نیاز زیادی به شبکه‌سازی رایانه‌ها و دفاتر تجاری خود دارند و وجود یک متخصص شبکه در هر بخشی ضروری به نظر می‌رسد. اما متاسفانه در دانشگاه‌ها و مراکز آموزش عالی، به این درس توجه زیادی نمی شود. یکی دیگر از مشکلات این دروس، کمبود منابع درسی *جامع و کامل است*، به طوری که بتواند مباحث عملی شبکه را به خوبی پوشش دهد.

لذا بنده بر خود لازم دانستم که مطالب مرتبط با این دروس را جمع‌آوری نموده و در قالب یک جزوه آموزشی در اینترنت قرار دهم تا هم کمبودهای آموزشی دانشجویان مرتفع گردد و هم اگر دانشجویی قصد داشت در آینده مباحث شبکه را ادامه دهد، منبعی برای آغاز کار خود داشته باشد. لذا در تهیه این جزوه هم مباحث ابتدایی و هم مباحث متوسط و هم مباحث پیشرفته مرتبط با شبکه قرار گرفته است. برخی از فصول این جزوه، فقط به مباحث تئوری شبکه‌های کامپیوتری می‌پردازد؛ فصل هایی هم که مباحث عملی را توضیح می‌دهند در دو قسمت سازماندهی شده‌اند، بخش اول آن‌ها، آموزش تئوری و مفاهیم پایه‌ای در مورد مباحث آن فصل است و بخش دوم نیز به آموزش عملی آن مبحث می‌پردازد که در تمام فصول عملی، سعی بر آن شده است که به همراه آموزش عملی، تصاویری را نیز قرار دهم تا درک مطالب راحت تر شود.

لازم به ذکر است که برخی مطالب این جزوه از اینترنت یا تحقیقات دانشجویان جمع‌آوری شده است.

به دانشجویان و مدرسین عزیز توصیه می‌کنم که مطالب این جزوه را حتما با کمک نرم افزار شبیه سازی Oracle VM Virtual Box به صورت عملی کار کنند. آموزش این نرم افزار در همین جزوه قرار داده شده است.

چرا ویندوز سرور ۲۰۰۳؟

دوستان زیادی به بنده پیشنهاد نمودند که این جزوه را از ویندوز سرور ۲۰۰۳ به ویندوز سرور ۲۰۰۸ و ۲۰۱۲ ارتقاء دهم. درست است که به روز بودن و همگام بودن با جدیدترین تکنولوژی‌ها، به خصوص در زمینه‌های کامپیوتری امری ضروری است، اما هدف من از تهیه این جزوه، ارائه منبعی برای درس آزمایشگاه شبکه‌های کامپیوتری در دانشگاه‌ها بوده است. امروزه اکثر دانشگاه‌های کشور، ویندوز سرور ۲۰۰۳ را بر روی کامپیوترهای خود نصب می‌کنند. به علاوه ویندوز سرور ۲۰۰۸ و ۲۰۱۲ از لحاظ میزان مصرف منابع، بسیار سنگین تر از ویندوز سرور ۲۰۰۳ هستند و با توجه به پر قدرت بودن و مجهز بودن کامپیوترهای دانشگاه‌های کشور به قطعات جدید!!!!، بر ما مسلم بود که قابلیت استفاده از ویندوز سرور ۲۰۰۸ و ۲۰۱۲ در بسیاری از دانشگاه‌ها وجود نخواهد داشت. همچنین با توجه به شبیه سازی این سیستم عامل بر روی Virtual Box و محدودیت‌های موجود، سختی استفاده از ویندوز سرور ۲۰۰۸ و ۲۰۱۲ دوچندان می‌شد. لذا تصمیم گرفتم بجای ارتقاء از نسخه ۲۰۰۳ به ۲۰۰۸ و ۲۰۱۲، سایر خدمات و قابلیت‌های ویندوز سرور ۲۰۰۳ یا دیگر سیستم‌عامل‌ها را معرفی کنم.

چرا این جزوه تبدیل به کتاب نشد؟

در ابتدای کار، قصد داشتم که مطالب جمع شده را به یک کتاب تبدیل کنم. همانطور که حتی از ظاهر جزوه هم پیداست، این جزوه چیزی از یک کتاب آموزشی کم ندارد. در پایان دیدم که هزینه کتاب چاپ شده بسیار بالا خواهد شد و با این قیمت بالا، تعداد بسیار کمی از دانشجویان توانایی تهیه کتاب را خواهند داشت. حتی از سوی یک سازمان دولتی نیز پیشنهادی مبنی بر

چاپ کتاب به نام آن سازمان، در ازاء کسر خدمت سربازی را داشتم؛ اما در نهایت به این نتیجه رسیدم که اگر جزوه را به صورت رایگان در اینترنت پخش کنم و دانشجویان زیادی بتوانند به صورت رایگان از کتاب استفاده کنند، مزیت این کار برای من بسیار بیشتر خواهد بود.

نسخه اول

استارت تهیه نسخه اول این جزوه آموزشی، در آذر ماه سال ۱۳۸۹ کلید خورد و پس از حدود دو ماه، نسخه اول این جزوه آماده شد و در دانشگاه علمی کاربردی علویجه مورد استفاده قرار گرفت.

نسخه دوم

نسخه اول جزوه، مطالب زائد زیادی داشت و کمبود برخی مطالب نیز در آن احساس می‌شد. همچنین به علت زمان کوتاهی که صرف تولید آن شده بود، غلط‌های املایی زیادی نیز در آن وجود داشت. در نسخه دوم جزوه، بسیاری از مطالب زائد و خسته کننده نسخه اول حذف گردید و مطالب متنوع دیگری نیز به آن اضافه شد. همچنین سعی شد که بسیاری از این غلط‌های املایی حذف شود. نسخه دوم، در مهرماه ۱۳۹۰ تهیه شد. به محض تهیه نسخه دوم، اقدام به انتشار آن در اینترنت نمودم که خوشبختانه با استقبال خوبی روبرو شد.

نسخه سوم

جزوه‌ای که در حال حاضر مشاهده می‌نمایید، نسخه سوم جزوه است. از جمله تغییرات این نسخه، نسبت به نسخه قبل، اصلاح برخی فصل‌ها همچون فصل DNS، فصل Group Policy، فصل نصب ویندوز سرور، فصل راه‌اندازی شبکه، بخش Subnet Mask و افزودن برخی مطالب همچون شبکه‌های بی‌سیم، شبکه‌های حسگر، محاسبات Cluster، نرم‌افزارهای ارتباطی، Streaming Media Server، MDaemon Mail Server، نرم‌افزارهای ISA Server و Packet Tracer و همچنین اصلاح برخی اشکالات تکنیکی و غلط‌های املایی می‌باشد. همچنین به همراه این نسخه، فیلم‌های گرفته شده از کلاس **نصب و راه‌اندازی شبکه، دانشگاه آزاد اسلامی واحد خوراسگان** در اینترنت قرار داده شده است که برای دانلود می‌توانید به وبلاگ مراجعه نمایید.

این جزوه آموزشی نیز مانند بسیاری از منابع آموزشی، عاری از خطا و اشتباه نیست و مسلما خطاها و اشتباهات زیادی چه از نظر فنی و چه از نظر محتوایی در بین مطالب وجود دارد؛ لذا از تمامی دانشجویان خواهشمندم که مشکلات این جزوه را به من اطلاع دهند تا آنها را تصحیح کنم تا بتوانیم جزوه‌ای کم نقص را با کمک یکدیگر آماده سازیم. امید است که این مجموعه آموزشی مورد قبول و رضایت خداوند متعال و شما دانشجویان گرامی قرار گیرد.

رضا رمضانی – نوروز ۱۳۹۲

Email : ramezani.cs@gmail.com
Weblog : http://ramezani-cs.blogfa.com
Webpage : https://www.facebook.com/ramezani.reza

ای خدا! من باید از نظر علم نیز از همه برتر باشم تا مبادا که دشمنان، مرا از این راه طعنه زنند. باید به آن سنگ‌دلانی که علم را بهانه کرده و به دیگران فخر می‌فروشند، ثابت کنم که خاک پای من هم نخواهند شد. باید همه آن تیره دلان مغرور و متکبر را به زانو در آورم؛ آنگاه خود خاضع ترین و افتاده ترین فرد روی زمین باشم.

از نیایش‌های دکتر چمران – سپتامبر ۱۹۶۱ – دانشگاه برکلی آمریکا

لینک‌های دانلود

دانلود مستقیم کتاب و فیلم های آموزشی از وب سایت دانشجوی ایرانی

http://www.irstu.com/?p=1971

نسخه سوم جزوه و فیلم‌های آموزشی مرتبط با جزوه را می‌توانید از آدرس‌های زیر با لینک مستقیم دانلود نمایید.

آدرس وبلاگ: http://ramezani-cs.blogfa.com

نسخه اصلی جزوه: http://ramezani-cs.ugig.ir/files/NW3/NW3.0.rar

محتویات	سرور اول
فایل جزوه	http://ramezani-cs.persiangig.com/NW3/NW3.0.rar
فایل ثبت‌نام	http://ramezani-cs.persiangig.com/NW3/users.exe
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 01.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 02.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 03.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 04.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 05.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 06.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 07.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 08.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 09.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 10.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 11.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 12.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 13.rar
فیلم آموزشی	http://ramezani-cs.persiangig.com/NW3/Session 14.rar

محتویات	سرور دوم
فایل جزوه	http://ramezani-cs2.persiangig.com/NW3/NW3.0.rar
فایل ثبت‌نام	http://ramezani-cs2.persiangig.com/NW3/users.exe
فیلم آموزشی	http://ramezani-cs2.persiangig.com/NW3/Session 01.rar
فیلم آموزشی	http://ramezani-cs2.persiangig.com/NW3/Session 02.rar
فیلم آموزشی	http://ramezani-cs2.persiangig.com/NW3/Session 03.rar
فیلم آموزشی	http://ramezani-css.persiangig.com/NW3/Session 04.rar

http://ramezani-cs2.persiangig.com/NW3/Session 05.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 06.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 07.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 08.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 09.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 10.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 11.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 12.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 13.rar	فیلم آموزشی
http://ramezani-cs2.persiangig.com/NW3/Session 14.rar	فیلم آموزشی

سرور سوم	**محتویات**
http://ramezani-cs.ugig.ir/files/NW3/NW3.0.rar	فایل جزوه
http://ramezani-cs.ugig.ir/files/NW3/users.exe	فایل ثبت‌نام
http://ramezani-cs.ugig.ir/files/NW3/Session 01.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 02.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 03.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 04.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 05.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 06.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 07.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 08.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 09.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 10.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 11.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 12.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 13.rar	فیلم آموزشی
http://ramezani-cs.ugig.ir/files/NW3/Session 14.rar	فیلم آموزشی

فهرست مطالب (۱)

فصل ۱ آشنایی با شبکه ۱

۱-۱- معرفی ۱

۱-۲- تاریخچه شبکه ۱

۱-۳- تعریف شبکه ۳

۱-۴- هدف از ایجاد شبکه ۳

۱-۵- مزایای شبکه ۴

۱-۶- دسته بندی شبکه‌های رایانه ای ۴

۱-۶-۱- بر اساس نوع اتصال ۴

۱-۶-۲- بر اساس تکنولوژی سیم کشی ۴

۱-۶-۳- بر اساس تکنولوژی بی‌سیم ۵

۱-۶-۴- بر اساس اندازه ۶

۱-۶-۵- بر اساس لایه شبکه ۹

۱-۶-۶- بر اساس معماری کاربری ۹

۱-۶-۷- بر اساس همبندی (توپولوژی) ۱۰

۱-۶-۸- بر اساس مسیر دهی بسته ها ۱۰

۱-۷- اجزای اصلی سخت‌افزاری ۱۲

۱-۷-۱- کارت شبکه (NIC) ۱۲

۱-۷-۲- تکرارگر (Repeater) ۱۲

۱-۷-۳- هاب (جعبه تقسیم) ۱۳

۱-۷-۴- راهگزین (Switch) ۱۳

۱-۷-۵- پل (Bridge) ۱۴

۱-۷-۶- مسیریاب (Router) ۱۴

۱-۸- سیستم‌های شبیه به شبکه ۱۵

۱-۸-۱- کامپیوترهای Mainframe ۱۵

۱-۸-۲- سیستم‌های توزیع شده ۱۶

۱-۸-۳- کامپیوتر هایی که به یکدیگر Link می‌شوند ۱۶

۱-۹- مراحل راه اندازی یک شبکه ۱۶

۱-۹-۱- طراحی شبکه (Design) ۱۶

۱-۹-۲- تنظیمات شبکه (Roll Out) ۱۶

۱-۹-۳- پیکربندی شبکه (Configuration) ۱۷

۱-۹-۴- مدیریت و اداره شبکه (Management) ۱۷

۱-۱۰- آشنایی با VoIP ۱۷

۱-۱۰-۱- مقدمه ۱۷

۱-۱۰-۲- VoIP چیست؟ ۱۸

۱-۱۰-۳- VoIP چگونه کار می‌کند؟ ۱۹

۱-۱۰-۴- مزایای استفاده از VoIP نسبت به PSTN ۱۹

۱-۱۰-۵- نحوه ایجاد یک اتصال VoIP ۲۰

۱-۱۰-۶- چالش‌های امنیتی VoIP ۲۰

فهرست مطالب (۲)

۱-۱۰-۷- نحوه حفاظت ۲۱

فصل ۲ آدرس IP ۲۲

۲-۱- آدرس IP چیست؟ ۲۲

۲-۲- انواع IP ۲۳

۲-۳- آدرس IP نسخه ۴ ..... ۲۳

۲-۳-۱- کلاس‌های مختلف IP نسخه ۴ ..... ۲۳

۲-۳-۲- IP خصوصی ۲۶

۲-۳-۳- NAT چیست؟ (Network Address Translation) ۲۶

۲-۳-۴- IP ایستا و پویا ۲۷

۲-۴- IP نسخه ۶ ..... ۲۷

۲-۴-۱- مقدمه ۲۷

۲-۴-۲- معرفی IPv6.0 ..... ۲۸

۲-۴-۳- NAT: ترجمه آدرس‌های شبکه ۳۸

۲-۵- تنظیم آدرس IP در ویندوز XP ۴۳

۲-۶- طریقه‌ی یافتن آدرس IP کامپیوتر ۴۶

۲-۷- Subnet Mask ۴۶

۲-۷-۱- مقدمه ۴۶

۲-۷-۲- Subnet Mask چه کاربردی دارد و چگونه ساخته می‌شود؟ ۴۸

۲-۷-۳- تنظیم Subnet ۴۹

۲-۸- Default Gateway ۵۷

۲-۹- Mac Address ۵۷

۲-۹-۱- دلیل استفاده از MAC Address ۵۷

۲-۹-۲- ساختار MAC Address ۵۸

۲-۹-۳- مشاهده MAC Address ۵۸

۲-۹-۴- قوانین تولید Mac Address ۵۸

فصل ۳ توپولوژی‌های شبکه ۶۰

۳-۱- توپولوژی شبکه ۶۰

۳-۲- انواع توپولوژی (همبندی) شبکه ۶۱

۳-۲-۱- آرایش خطی یا گذرگاهی (Bus) ۶۱

۳-۲-۲- آرایش حلقوی (Ring) ۶۲

۳-۲-۳- آرایش ستاره‌ای (Star) ۶۳

۳-۲-۴- ستاره گسترش یافته ۶۴

۳-۲-۵- آرایش مشبک (Mesh) ۶۵

۳-۲-۶- آرایش اتصال کامل (Fully Connected) ۶۵

۳-۲-۷- آرایش درختی (Tree) یا آرایش سلسله مراتبی ۶۵

۳-۲-۸- آرایش ترکیبی (Hybrid) ۶۶

فصل ۴ ساختارهای شبکه ۶۸

۴-۱- دسته بندی شبکه ۶۸

۴-۲- گروه کاری (Work Group یا Peer-To-Peer) ۶۸

فهرست مطالب (۳)

۴-۲-۱- معرفی مدل Peer-To-Peer (نظیر به نظیر) ۶۹
۴-۲-۲- شبکه سازی به روش نظیر به نظیر ۶۹
۴-۲-۳- ویژگی ها ۷۰
۴-۲-۴- معایب ۷۰
۴-۳- مبتنی بر دامنه (Client – Server یا Server Based) ۷۱
۴-۳-۱- معرفی شبکه‌های Server Based یا Client-Server ۷۱
۴-۴- تعاریف دیگری برای Client و Server ۷۲
فصل ۵ سیستم عامل شبکه ۷۴
۵-۱- سیستم‌های عامل شبکه ای ۷۴
۵-۲- ویژگی‌های یک سیستم عامل شبکه‌ای ۷۴
۵-۳- معرفی انواع سرور ۷۵
۵-۳-۱- File Server ۷۵
۵-۳-۲- Print Server ۷۵
۵-۳-۳- Application Server ۷۶
۵-۳-۴- Terminal Server ۷۶
۵-۳-۵- VPN Server / Remote Server ۷۶
۵-۳-۶- DNS Server ۷۶
۵-۳-۷- DHCP Server ۷۶
۵-۴- ویندوز سرور ۲۰۰۳ ..... ۷۶
۵-۵- انواع نسخه‌های ویندوز سرور ۲۰۰۳ ..... ۷۸
۵-۵-۱- Server 2003 Web Edition ۷۸
۵-۵-۲- Server 2003 Standard Edition ۷۸
۵-۵-۳- Server 2003 Enterprise Edition ۷۸
۵-۵-۴- Server 2003 Datacenter Edition ۷۸
۵-۵-۵- Server 2008 HPC ۷۹
۵-۶- مقایسه نسخه‌های ویندوز سرور ۲۰۰۳ در یک نگاه ۷۹
۵-۷- ویژگی‌های جدید ویندوز سرور ۲۰۰۸ ..... ۸۰
۵-۷-۱- قابلیت ایجاد محیط مجازی ۸۰
۵-۷-۲- ساخته شده برای وب ۸۱
۵-۷-۳- امنیت بالا ۸۱
۵-۷-۴- انجام محاسبات با کارایی بالا (HPC) ۸۱
۵-۸- لینوکس ۸۲
۵-۸-۱- نرم‌افزارهای Server تحت لینوکس ۸۲
۵-۸-۲- ویژگی‌های اصلی لینوکس ۸۲
۵-۸-۳- مزایای لینوکس ۸۳
۵-۸-۴- اجزای سیستم عامل لینوکس ۸۳
۵-۸-۵- نسخه‌های مختلف سیستم عامل لینوکس ۸۴
فصل ۶ تجهیزات شبکه ۸۵
۶-۱- کابل شبکه ۸۶

فهرست مطالب (۴)

۶-۱-۱- انواع رسانه ها ۸۶
۶-۱-۲- کابل کواکسیال ۸۷
۶-۱-۳- کابل UTP (Unshielded Twisted Pair) ۸۸
۶-۱-۴- آموزش سوکت زنی ۹۴
۶-۱-۵- فیبر نوری ۹۸
۶-۲- کارت واسط شبکه (NIC) ۱۰۰
۶-۲-۱- وظایف کارت شبکه ۱۰۱
۶-۲-۲- انواع کارت شبکه ۱۰۳
۶-۲-۳- انتخاب کارت شبکه ۱۰۴
۶-۲-۴- ساختار کارت واسط شبکه (NIC) ۱۰۴
۶-۳- تکرار کننده (Repeater) ۱۰۵
۶-۴- هاب (HUB) ۱۰۶
۶-۴-۱- انواع هاب ۱۰۷
۶-۴-۲- آشنائی با نحوه عملکرد هاب ۱۰۸
۶-۵- سوئیچ (Switch) ۱۰۹
۶-۵-۱- استفاده از سوئیچ ۱۱۱
۶-۵-۲- تکنولوژی سوئیچ‌ها ۱۱۲
۶-۵-۳- انواع سوئیچ LAN ۱۱۴
۶-۵-۴- روترها و سوئیچینگ لایه سوم ۱۱۵
۶-۵-۵- سوئیچ‌های مدیریتی ۱۱۶
۶-۵-۶- ماژول سوئیچ ۱۱۶
۶-۵-۷- مزایای سوئیچ ۱۱۷
۶-۵-۸- از چه نوع سوئیچ هایی استفاده کنیم؟ ۱۱۷
۶-۵-۹- تفاوت HUB با Switch ۱۱۷
۶-۵-۱۰- هاب چیست؟ ۱۱۸
۶-۵-۱۱- سوئیچ چیست؟ ۱۱۸
۶-۵-۱۲- آیا باید ما از هاب به سوئیچ ارتقاء پیدا کنیم؟ ۱۱۹
۶-۶- پل (Bridge) ۱۲۰
۶-۷- دروازه (Gateway) ۱۲۱
۶-۸- مسیریاب (Router) ۱۲۱
۶-۸-۱- آشنائی با روتر ۱۲۲
۶-۸-۲- انواع روتر ۱۲۲
۶-۸-۳- مهمترین ویژگی‌های یک روتر ۱۲۴
۶-۸-۴- آشنائی با اینترفیس‌های (رابط) روتر ۱۲۴
۶-۸-۵- پیکربندی روتر با استفاده از پورت‌های مدیریت ۱۲۵
۶-۸-۶- آشنایی با مسیریاب‌های سیسکو ۱۲۷
۶-۸-۷- BRouter ۱۳۰
۶-۹- مودم ADSL ۱۳۰
۶-۹-۱- مودم ADSL ۱۳۰

فهرست مطالب (۵)

۶-۹-۲- نحوه کار مودم‌های DSL ۱۳۱
۶-۹-۳- تجهیزات DSL ۱۳۳
۶-۱۰- اس‌اف‌پی (SFP) ۱۳۴
۶-۱۱-NAS ۱۳۴
۶-۱۱-۱-Filer چیست؟ ۱۳۵
۶-۱۱-۲-NAS در مقابل SAN ۱۳۵
۶-۱۱-۳-NAS برای کاربران شبکه ۱۳۶
۶-۱۱-۴-SAN برای اتاق سرورها ۱۳۶
۶-۱۱-۵- راه حل‌های NAS برای نیازهای امروز شرکت‌ها ۱۳۷
۶-۱۱-۶- نصب NAS روی شبکه خانگی ۱۳۸
۶-۱۲-POE ۱۴۰
۶-۱۳-DAS ۱۴۲
۶-۱۴-Modular Smart Array ۱۴۳
۶-۱۴-۱-MSA 50 ..... ۱۴۳
۶-۱۴-۲-MSA 60 ..... ۱۴۳
۶-۱۴-۳-MSA 70 ..... ۱۴۴
۶-۱۵-Splitter ۱۴۴
فصل ۷ معماری شبکه ۱۴۵
۷-۱- انواع معماری شبکه ۱۴۵
۷-۱-۱-اترنت ۱۴۵
۷-۱-۲-TOKEN RING ۱۵۰
۷-۱-۳-FDDI ۱۵۰
۷-۱-۴- شبکه بدون سیم ۱۵۰
فصل ۸ مدل‌های OSI و TCP/IP ۱۵۲
۸-۱- نحوه مبادله داده بین دو کامپیوتر ۱۵۲
۸-۲- ساختار لایه‌ها در مدل مرجع OSI ۱۵۳
۸-۳- عملکرد هر یک از لایه‌های مدل مرجع OSI ۱۵۵
۸-۳-۱-لایه Physical (لایه اول) ۱۵۵
۸-۳-۲-لایه Datalink (لایه دوم) ۱۵۶
۸-۳-۳-لایه Network (لایه سوم) ۱۵۷
۸-۳-۴-لایه Transport (لایه چهارم) ۱۵۷
۸-۳-۵-لایه Session (لایه پنجم) ۱۵۸
۸-۳-۶-لایه Presentation (لایه ششم) ۱۵۹
۸-۳-۷-لایه Application (لایه هفتم) ۱۶۰
۸-۴- نگاهی انتقادی به مدل OSI و پروتکل‌های آن ۱۶۰
۸-۴-۱- زمان نامناسب ۱۶۱
۸-۴-۲- تکنولوژی نامناسب ۱۶۱
۸-۴-۳- پیاده سازی نامناسب ۱۶۲
۸-۴-۴- سیاست‌های نامناسب ۱۶۲

فهرست مطالب (۶)

۸-۵- ساختار لایه‌ها در مدل TCP/IP ۱۶۲
۸-۵-۱- مفاهیم اولیه پروتکل TCP/IP ۱۶۲
۸-۵-۲- معرفی پروتکل TCP/IP ۱۶۳
۸-۶- عملکرد هر یک از لایه‌های مدل TCP/IP ۱۶۳
۸-۶-۱- لایه کاربردی ۱۶۳
۸-۶-۲- لایه انتقال ۱۶۵
۸-۶-۳- لایه شبکه ۱۶۵
۸-۶-۴- لایه Network Interface (Physical) ۱۶۵
۸-۷- نگاهی انتقادی به مدل TCP/IP ۱۶۶
فصل ۹ شبکه‌های بی‌سیم ۱۶۷
۹-۱- مبانی شبکه‌های بی‌سیم ۱۶۷
۹-۱-۱- مقدمه ۱۶۷
۹-۱-۲- تاریخچه شبکه‌های بی‌سیم ۱۶۷
۹-۱-۳- تشریح مقدماتی شبکه‌های بی‌سیم و کابلی ۱۶۹
۹-۱-۴- تقسیم‌بندی شبکه‌های بی‌سیم ۱۷۱
۹-۱-۵- کاربردها، مزایا و ابعاد ۱۷۳
۹-۱-۶- روش‌های ارتباطی بی‌سیم ۱۷۴
۹-۱-۷- عناصر فعال شبکه‌های محلی بی‌سیم ۱۷۵
۹-۱-۸- برد و سطح پوشش ۱۷۶
۹-۱-۹- معماری شبکه‌های محلی بی‌سیم ۱۷۷
۹-۱-۱۰- لایه‌های ۸۰۲.۱۱ ..... ۱۸۷
۹-۲- امنیت شبکه‌های بی‌سیم ۱۹۰
۹-۲-۱- مقدمه ۱۹۰
۹-۲-۲- امنیت شبکه بی‌سیم ۱۹۰
۹-۲-۳- چهار مشکل امنیتی مهم شبکه‌های بی‌سیم ۸۰۲.۱۱ ..... ۱۹۴
۹-۲-۴- سه روش امنیتی در شبکه‌های بی‌سیم ۲۰۰
۹-۲-۵- امن سازی شبکه‌های بی‌سیم ۲۰۰
۹-۲-۶- قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱ ..... ۲۰۴
۹-۳- WiFi ۲۰۵
۹-۳-۱- مقدمه ۲۰۵
۹-۳-۲- WiFi چیست؟ ۲۰۵
۹-۳-۳- چرا WiFi را بکار گیریم؟ ۲۰۶
۹-۳-۴- WiFi چگونه کار می‌کند؟ ۲۰۶
۹-۳-۵- IEEE 802.11 ..... ۲۰۸
۹-۳-۶- کاربردهای WiFi ۲۱۷
۹-۳-۷- دلایل رشد WiFi ۲۱۸
۹-۳-۸- نقاط ضعف WiFi ۲۱۸
۹-۴- تکنولوژی WiFi ۲۱۹
۹-۴-۱- مقدمه ۲۱۹

فهرست مطالب (۷)

۹-۴-۲- تکنولوژی رادیویی WiFi ۲۱۹
۹-۴-۳- شبکه واکی تاکی (Walkie Talkie) ۲۲۰
۹-۴-۴- به‌کارگیری WiFi در صنعت تلفن همراه ۲۲۱
۹-۴-۵- آنچه برای ساختن یک شبکه بی‌سیم نیاز دارید ۲۲۳
۹-۴-۶- WiFi را به دستگاه خود اضافه کنید ۲۲۴
۹-۵- WiFi و WiMax ۲۲۷
۹-۵-۱- مقدمه ۲۲۷
۹-۵-۲- مروری بر پیاده‌سازی شبکه‌های WiMax ۲۲۸
۹-۵-۳- WiMax در مقابل WiFi ۲۳۰
۹-۶- قطعات سخت‌افزاری WiMax ۲۳۳
۹-۶-۱- آنتن های WiMax ۲۳۳
۹-۶-۲- CPE ۲۳۶
۹-۶-۳- کارت شبکه WiMax ۲۳۶
۹-۶-۴- روترهای WiMax ۲۳۶
۹-۶-۵- رک های WiMax ۲۳۷
۹-۶-۶- تجهیزات مربوط به ایستگاه های WiMax ۲۳۷
۹-۷- بلوتوث ۲۳۷
۹-۷-۱- معماری بلوتوث ۲۳۹
۹-۷-۲- مزایای استاندارد Bluetooth ۲۴۰
۹-۷-۳- کاربردهای بلوتوث ۲۴۰
۹-۷-۴- پشته پروتکلی بلوتوث ۲۴۲
۹-۷-۵- لایه رادیوئی در بلوتوث ۲۴۳
۹-۷-۶- لایه باند پایه در بلوتوث ۲۴۴
۹-۷-۷- لایه CAP2L در بلوتوث ۲۴۵
۹-۷-۸- ساختار فرم در بلوتوث ۲۴۵
۹-۸- واژه نامه شبکه‌های بی‌سیم ۲۴۷
فصل ۱۰ شبکه‌های حسگر ۲۵۴
۱۰-۱- خلاصه ۲۵۴
۱۰-۲- مقدمه ۲۵۴
۱۰-۲-۱- توصیف شبکه‌های حسگر ۲۵۴
۱۰-۲-۲- تفاوت های شبکه های بی‌سیم و کابلی ۲۵۶
۱۰-۲-۳- تاریخچه شبکه‌های حسگر بی‌سیم ۲۵۷
۱۰-۲-۴- ویژگی های عمومی شبکه حسگر ۲۵۸
۱۰-۳- ویژگی‌های طراحی ۲۵۹
۱۰-۳-۱- تحمل خطا ۲۶۰
۱۰-۳-۲- مقیاس پذیری ۲۶۰
۱۰-۳-۳- هزینه تولید ۲۶۱
۱۰-۳-۴- محدودیت‌های سخت‌افزاری ۲۶۱
۱۰-۳-۵- توپولوژی شبکه‌های حسگر ۲۶۲

فهرست مطالب (۸)

۱۰-۳-۶- محیط عمل ۲۶۲
۱۰-۳-۷- رسانه انتقال ۲۶۲
۱۰-۳-۸- مصرف انرژی ۲۶۳
۱۰-۳-۹- داده محوری ۲۶۴
۱۰-۴- معماری ۲۶۴
۱۰-۴-۱- پشته پروتکل در شبکه‌های حسگر ۲۶۴
۱۰-۵- کاربرد ها ۲۷۲
۱۰-۶- پروتکل‌های مسیریابی ۲۸۴
۱۰-۶-۱- پروتکل‌های مسیریابی داده محور ۲۸۴
۱۰-۶-۲- پروتکل‌های مسیر یابی سلسله مراتبی ۲۸۷
۱۰-۶-۳- پروتکل‌های مسیریابی مبتنی بر مکان ۲۸۸
۱۰-۶-۴- پروتکل‌های مسیریابی آگاه به کیفیت سرویس ۲۸۹
۱۰-۷- شبکه‌های حسگر و بازیگر بی‌سیم ۲۹۰
۱۰-۸- خلاصه ۲۹۱
فصل ۱۱ محاسبات ابری (Cloud Computing) ۲۹۲
۱۱-۱- محاسبات ابری ۲۹۲
۱۱-۱-۱- چکیده ۲۹۲
۱۱-۱-۲- مقدمه ۲۹۳
۱۱-۱-۳- تعریف مسأله ۲۹۳
۱۱-۱-۴- ساختار فصل ۲۹۳
۱۱-۲- مفاهیم و پروتکل‌ها ۲۹۴
۱۱-۲-۱- مقدمه ۲۹۴
۱۱-۲-۲- محاسبات تورین (شبکه ای - Grid) ۲۹۴
۱۱-۲-۳- معماری سرویس گرا ۲۹۵
۱۱-۲-۴- سرویس وب ۲۹۶
۱۱-۲-۵- ترکیب سرویس ۲۹۸
۱۱-۲-۶- پروتکل SOAP ۲۹۸
۱۱-۲-۷- زبان توصیف وب سرویس WSDL ۲۹۹
۱۱-۲-۸- زبان اجرای فرآیند BPEL ۳۰۰
۱۱-۲-۹- جمع بندی مطالب فصل ۳۰۰
۱۱-۳- محاسبات ابرین ۳۰۱
۱۱-۳-۱- مقدمه ۳۰۱
۱۱-۳-۲- محاسبات ابرین چیست؟ ۳۰۱
۱۱-۳-۳- سیر تکامل سبک های محاسباتی ۳۰۲
۱۱-۳-۴- فواید استفاده از معماری ابرین ۳۰۴
۱۱-۳-۵- اهداف محاسبات ابرین ۳۰۴
۱۱-۳-۶- خصوصیات کلیدی ابر ۳۰۶
۱۱-۳-۷- مدل های تحویل سرویس (آناتومی ابر) ۳۰۶
۱۱-۳-۸- معماری ابر ۳۰۹

فهرست مطالب (۹)

۱۱-۳-۹- مدل های استقرار ۳۱۳
۱۱-۴- نمونه‌ها و کاربردهای محاسبات ابرین ۳۱۴
۱۱-۴-۱- سرویس دهنده گان اصلی ۳۱۴
۱۱-۴-۲-IaaS ۳۱۴
۱۱-۴-۳-PaaS ۳۱۶
۱۱-۴-۴-SaaS ۳۱۶
۱۱-۴-۵-DaaS ۳۱۷
۱۱-۴-۶-HaaS ۳۱۸
۱۱-۴-۷- کاربرد محاسبات ابرین ۳۱۸
۱۱-۴-۸- نتیجه گیری ۳۲۳
۱۱-۵- ترکیب سرویس و یکپارچه سازی سیستم در فضای ابر ۳۲۴
۱۱-۵-۱- مقدمه ۳۲۴
۱۱-۵-۲- ترکیب سرویس ابرین ۳۲۴
۱۱-۵-۳- ترکیب سرویس های داخل یک ابر ۳۲۴
۱۱-۵-۴- ترکیب سرویس هایی از چندین ابر ۳۲۵
۱۱-۵-۵- نتیجه گیری ۳۲۵
۱۱-۶- چالش های مطرح در حوزه محاسبات ابرین ۳۲۶
۱۱-۶-۱- چالش های عمومی ۳۲۶
۱۱-۶-۲- چالش های پیش رو ۳۲۷
۱۱-۶-۳- مشکلات ابرهای موجود ۳۲۸
۱۱-۶-۴- نتیجه گیری ۳۳۰
فصل ۱۲ خوشه‌بندی (Clustering) ۳۳۱
۱۲-۱- مقدمه ۳۳۱
۱۲-۱-۱- توصیف ۳۳۲
۱۲-۲- دوره‌های محاسبات ۳۳۳
۱۲-۳- معماری‌های مقیاس‌پذیر کامپیوتر موازی ۳۳۴
۱۲-۴- به سوی محاسبات موازی کم‌هزینه و انگیزه‌ها ۳۳۶
۱۲-۵- دریچه‌ای به سوی فرصت‌ها ۳۳۷
۱۲-۶- کامپیوتر کلاستر و معماری آن ۳۳۸
۱۲-۷- طبقه‌بندی کلاسترها ۳۴۰
۱۲-۸- اجزا مناسب جهت کلاسترها ۳۴۲
۱۲-۸-۱- پردازنده‌ها ۳۴۲
۱۲-۸-۲- حافظه و کاشه (Cache) ۳۴۳
۱۲-۸-۳- دیسک و ورودی / خروجی ۳۴۴
۱۲-۸-۴- گذرگاه سیستم ۳۴۴
۱۲-۸-۵- اتصالات درونی در یک کلاستر ۳۴۵
۱۲-۸-۶- سیستم‌عامل‌ها ۳۴۷
۱۲-۹- سرویس‌های شبکه / نرم‌افزارهای ارتباطی ۳۵۱
۱۲-۱۰- میان‌افزار کلاستر و تصویر سیستم واحد ۳۵۲

فهرست مطالب (۱۰)

۱۲-۱۰-۱- لایه‌ها / سطوح تصویر سیستم واحد ۳۵۳
۱۲-۱۰-۲- حدود SSI ۳۵۵
۱۲-۱۰-۳- اهداف طراحی میان‌افزار ۳۵۵
۱۲-۱۰-۴- خدمات کلیدی SSI و زیرساختار قابلیت دسترسی ۳۵۶
۱۲-۱۱- مدیریت منابع و زمان‌بندی (RMS) ۳۵۷
۱۲-۱۲- ابزارها و محیط‌های برنامه‌نویسی ۳۵۹
۱۲-۱۲-۱- رشته‌ها (Threads) ۳۵۹
۱۲-۱۲-۲- سیستم‌های انتقال پیام (MPI و PVM) ۳۶۰
۱۲-۱۲-۳- سیستم‌های حافظه اشتراکی توزیعی (DSM) ۳۶۱
۱۲-۱۲-۴- برنامه‌های رفع اشکال و پیش‌نمای (Profiler) موازی ۳۶۱
۱۲-۱۲-۵- ابزارهای بررسی کارآیی ۳۶۲
۱۲-۱۲-۶- ابزارهای اداره کردن کلاستر ۳۶۳
۱۲-۱۳- موارد کاربردی کلاستر ۳۶۴
۱۲-۱۴- سیستم‌های کلاستری نمونه ۳۶۴
۱۲-۱۴-۱- پروژه شبکه ایستگاه‌های کاری بِرکلی (Berkeley NOW) ۳۶۵
۱۲-۱۴-۲- پروژه ماشین مجازی با کارآیی بالا (HPVM) ۳۶۶
۱۲-۱۴-۳- پروژه Beowulf ۳۶۷
۱۲-۱۴-۴- Solaris MC: یک سیستم عامل با توانایی اجرایی سطح بالا برای کلاستر ۳۶۸
۱۲-۱۴-۵- مقایسه چهار محیط کلاستری ۳۶۹
۱۲-۱۵- کلاستری از SMPها (CLUMPS) ۳۷۰
۱۲-۱۶- خلاصه و نتایج ۳۷۱
۱۲-۱۶-۱- روندهای رشد نرم‌افزار و سخت‌افزار ۳۷۱
۱۲-۱۶-۲- روندهای رشد تکنولوژی کلاستر ۳۷۳
۱۲-۱۶-۳- تکنولوژی‌های آینده کلاستر ۳۷۳
۱۲-۱۶-۴- استدلال نهایی ۳۷۴
۱۲-۱۷- ضمیمه: تصاویر مختلف از کلاسترهای کامپیوتری ۳۷۵

فصل ۱۳ آشنایی با مدارک شبکه ۳۷۹

۱۳-۱- مقدمه ۳۷۹
۱۳-۲- سیسکو (Cisco) ۳۷۹
۱۳-۲-۱- سطوح مدارک سیسکو ۳۸۲
۱۳-۲-۲- سطح Entry ۳۸۲
۱۳-۲-۳- سطح Architect ۳۸۲
۱۳-۲-۴- سطح Associate ۳۸۳
۱۳-۲-۵- سطح Professional و Expert ۳۸۳
۱۳-۲-۶- CCNET (سطح Entry) ۳۸۳
۱۳-۲-۷- مدرک CCNA (سطح Associate) ۳۸۴
۱۳-۲-۸- CCDA (سطح Associate) ۳۸۵
۱۳-۲-۹- مدرک CCNP (سطح Professional) ۳۸۵
۱۳-۲-۱۰- CCDP (سطح Professional) ۳۸۸

فهرست مطالب (۱۱)

۱۳-۲-۱۱- CCIP (سطح Professional) ۳۸۸
۱۳-۲-۱۲- CCSP (سطح Professional) ۳۸۹
۱۳-۲-۱۳- CCVP (سطح Professional) ۳۸۹
۱۳-۲-۱۴- CCIE (سطح Expert) ۳۹۰
۱۳-۲-۱۵- پرطرفدارترین گرایش ها ۳۹۱
۱۳-۲-۱۶- مزایای دستیابی به مدارک سیسکو ۳۹۲
۱۳-۲-۱۷- وضعیت درآمد ۳۹۲
۱۳-۲-۱۸- خلاصه سطوح و مدارک سیسکو ۳۹۳
۱۳-۳- مایکروسافت (Microsoft) ۳۹۶
۱۳-۳-۱- مدارک شبکه‌ای مایکروسافت ۳۹۶
۱۳-۳-۲- MCP ۳۹۷
۱۳-۳-۳- MCSA ۳۹۷
۱۳-۳-۴- MCSE ۳۹۸
۱۳-۳-۵- مفاد آزمون MCSA و MCSE ۳۹۸
۱۳-۳-۶- MCITP ۴۰۰
۱۳-۳-۷- وضعیت درآمد ۴۰۲
۱۳-۳-۸- مزایای دستیابی به مدارک مایکروسافت ۴۰۳
۱۳-۳-۹- دیگر مدارک مایکروسافت ۴۰۳
۱۳-۳-۱۰- خلاصه مدارک مایکروسافت ۴۰۵
۱۳-۴- کامپتیا (CompTIA) ۴۰۶
۱۳-۴-۱- Network+ ۴۰۶
۱۳-۴-۲- A+ ۴۰۷
۱۳-۴-۳- Server+ ۴۰۹
۱۳-۴-۴- Security+ ۴۱۱
۱۳-۴-۵- Project+ ۴۱۲
۱۳-۴-۶- مزایای دستیابی به مدارک کامپتیا ۴۱۴
۱۳-۵- مدارک لینوکس ۴۱۵
۱۳-۵-۱- مدارک لینوکس‌کاران ۴۱۵
۱۳-۵-۲- مدرک Linux+ ۴۱۵
۱۳-۵-۳- مدرک Novell CLP ۴۱۷
۱۳-۵-۴- مدرک RHCE (RedHat Certified Engineer) ۴۱۸

فصل ۱۴ ساخت شبکه‌های مجازی با نرم‌افزار Virtual Box ۴۲۰

۱۴-۱- مقدمه ۴۲۰
۱۴-۲- Oracle VM VirtualBox ۴۲۱

فصل ۱۵ راه اندازی شبکه Workgroup و نحوه Share کردن داده ها ۴۳۱

۱۵-۱- اشتراک گذاری ۴۳۱
۱۵-۲- چگونه عملا چند کامپیوتر را به یکدیگر شبکه کنیم؟ ۴۳۲
۱۵-۳- مراحل انجام کار ۴۳۲
۱۵-۴- نام گذاری کامپیوتر ۴۳۳

فهرست مطالب (۱۲)

۱۵-۵- تنظیم آدرس IP ۴۳۵
۱۵-۶- به اشتراک گذاشتن فایل‌ها (File Sharing) و استفاده از آن‌ها ۴۳۷
۱۵-۶-۱- اشتراک گذاری ساده ۴۳۸
۱۵-۶-۲- اشتراک گذاری پیشرفته ۴۴۰
۱۵-۶-۳- استفاده از پوشه Share شده ۴۴۴
۱۵-۶-۴- تنظیمات امنیتی ۴۴۶
۱۵-۷- به اشتراک گذاشتن چاپگر ۴۴۸
۱۵-۸- به اشتراک گذاشتن اتصال اینترنت ۴۵۱
۱۵-۹- اتصال یک درایو به پوشه Share شده (Map Network Drive) ۴۵۱
۱۵-۱۰-Caching در File Sharing ۴۵۴
۱۵-۱۰-۱- فعال سازی امکانات Caching ۴۵۴
۱۵-۱۱- ساختار شبکه ۴۵۹
۱۵-۱۲- تجهیزات مورد نیاز ۴۶۰
۱۵-۱۳- راه اندازی شبکه Workgroup جدید در ویندوز XP ۴۶۱
فصل ۱۶ به اشتراک گذاشتن اتصال اینترنت ۴۷۰
۱۶-۱- مقدمه ۴۷۰
۱۶-۲- روش‌های به اشتراک گذاری اینترنت ۴۷۱
۱۶-۳- وب پروکسی (Web Proxy) ۴۷۱
۱۶-۳-۱- مزایای روش وب پروکسی ۴۷۲
۱۶-۳-۲- معایب وب پروکسی ۴۷۲
۱۶-۴- مترجم آدرس شبکه یا NAT ۴۷۳
۱۶-۴-۱- مزایا و معایب روش NAT ۴۷۳
۱۶-۵- آموزش عملی وب پروکسی یا Proxy Server ۴۷۳
۱۶-۵-۱- تنظیمات سرور ۴۷۴
۱۶-۵-۲- تنظیمات کلاینت ها ۴۸۹
۱۶-۵-۳- نرم‌افزار مدیریت Client در استفاده از Proxy Server ۴۹۰
۱۶-۶- آموزش عملی روش NAT یا ICS ۴۹۴
۱۶-۶-۱- شروع به کار ۴۹۴
۱۶-۶-۲- مراحل راه اندازی ۴۹۵
فصل ۱۷ امنیت فایل‌ها و پوشه ها ۴۹۸
۱۷-۱- انواع امنیت ۴۹۸
۱۷-۲- تنظیمات امنیتی ۴۹۹
فصل ۱۸ راه‌اندازی شبکه در ویندوز ۸ ..... ۵۰۶
۱۸-۱- مقدمه ۵۰۶
۱۸-۲- آیکن My Computer ۵۰۶
۱۸-۳- اتصال به شبکه ۵۰۷
۱۸-۴- مشاهده اتصالات شبکه ۵۰۸
۱۸-۵- تغییر آدرس IP ۵۱۰
۱۸-۶- تنظیمات اشتراک گذاری پیشرفته ۵۱۱
۱۸-۶-۱-Private ۵۱۱

فهرست مطالب (۱۳)

۱۸-۶-۲- Guest or Public ۵۱۱
۱۸-۶-۳- All Networks ۵۱۲
۱۸-۷- اتصال به HomeGroup ۵۱۳
۱۸-۸- تنظیمات فایروال ۵۱۴
۱۸-۹- راه اندازی اتصالات شبکه جدید ۵۱۶
۱۸-۱۰- اشتراک گذاری پوشه‌ها ۵۱۷
۱۸-۱۱- نگاشت درایو شبکه ۵۲۰
۱۸-۱۲- اشتراک گذاری چاپگر ۵۲۰
۱۸-۱۳- تغییر نام کامپیوتر، اتصال به دامنه ۵۲۲
فصل ۱۹ راه اندازی شبکه در لینوکس ۵۲۴
۱۹-۱- مقدمه ۵۲۴
۱۹-۲- اوبونتو ۵۲۵
۱۹-۳- شبکه کردن لینوکس ۵۲۵
۱۹-۳-۱- تخصیص IP از طریق رابط گرافیکی ۵۲۶
۱۹-۳-۲- تخصیص IP از طریق خط فرمان ۵۲۹
۱۹-۴- به اشتراک گذاری پوشه در اوبونتو ۵۳۰
۱۹-۵- استفاده از ویندوز XP به عنوان سرور ۵۳۳
۱۹-۶- چگونه به سرور Samba متصل شویم؟ ۵۳۴
۱۹-۶-۱- کلاینت اوبونتو ۵۳۴
۱۹-۶-۲- کلاینت ویندوز ۵۳۴
۱۹-۷- مدیریت سطح دسترسی در اوبونتو ۵۳۴
۱۹-۷-۱- سطوح دسترسی در لینوکس ۵۳۵
۱۹-۷-۲- تغییر سطح دسترسی ۵۳۶
فصل ۲۰ معرفی برخی از نرم‌افزارهای ارتباطی ۵۳۸
۲۰-۱- نرم‌افزار NetMeeting ۵۳۸
۲۰-۱-۱- مشاهده آدرس IP در سرور ۵۳۹
۲۰-۱-۲- اجرا و پیکربندی نرم‌افزار ۵۴۰
۲۰-۱-۳- نحوه کار با برنامه ۵۴۳
۲۰-۲- نرم‌افزار RaidCall ۵۴۶
۲۰-۲-۱- قابلیت‌های کلیدی نرم‌افزار Raidcall ۵۴۷
۲۰-۲-۲- نصب نرم‌افزار ۵۴۷
۲۰-۲-۳- ایجاد حساب کاربری ۵۴۹
۲۰-۲-۴- اجرای نرم‌افزار ۵۵۰
۲۰-۳- نرم‌افزار Skype ۵۵۳
۲۰-۳-۱- نصب نرم‌افزار ۵۵۴
۲۰-۳-۲- ایجاد حساب کاربری ۵۵۵
۲۰-۳-۳- اجرای نرم‌افزار ۵۵۷
۲۰-۴- نرم‌افزار oovoo ۵۶۰
۲۰-۴-۱- نصب نرم‌افزار ۵۶۱

فهرست مطالب (۱۴)

۲۰-۴-۲- ایجاد حساب کاربری ۵۶۱
۲۰-۴-۳- اجرای نرم‌افزار ۵۶۳
۲۰-۵- نرم‌افزار Net Support School ۵۶۸
۲۰-۵-۱- معرفی نرم‌افزار ۵۶۸
۲۰-۵-۲- نصب نرم‌افزار ۵۶۸
۲۰-۵-۳- اجرای نرم‌افزار ۵۶۹
۲۰-۵-۴- معرفی محیط اصلی Net Support ۵۷۲
فصل ۲۱ دستورات پر کاربرد شبکه ۵۹۰
۲۱-۱- محل اجرای دستورات ۵۹۰
۲۱-۲- دستور IPConfig ۵۹۰
۲۱-۳- دستور Ping ۵۹۴
۲۱-۴- دستور Tracert/Traceroute ۵۹۵
۲۱-۵- دستور NetStat ۵۹۷
۲۱-۶- دستور Net ۵۹۸
۲۱-۷- دستور nslookup ۶۰۳
۲۱-۸- دستور Whoami ۶۰۵
۲۱-۹- دستور Getmac ۶۰۶
۲۱-۱۰- دستور SFC ۶۰۶
۲۱-۱۱- دستور SystemInfo ۶۰۶
فصل ۲۲ آموزش نصب ویندوز سرور ۲۰۰۳ ..... ۶۰۷
۲۲-۱- ابتدا باید طرحی برای نصب داشته باشیم. ۶۰۷
۲۲-۲- شروع عملیات نصب در مرحله متنی ۶۰۷
۲۲-۳- مرحله نصب گرافیکی GUI ۶۱۲
فصل ۲۳ کاربران، گروه‌ها، واحدهای سازمانی ۶۲۵
۲۳-۱- کاربر (User) ۶۲۵
۲۳-۲- نحوه ساخت کاربر ۶۲۶
۲۳-۳- گروه (Group) ۶۲۹
۲۳-۳-۱- Built-In Local Group ۶۳۰
۲۳-۳-۲- Built-In System Group ۶۳۱
۲۳-۴- نحوه ساخت گروه ۶۳۲
۲۳-۴-۱- روش‌های اعطای مجوز به کاربران ۶۳۷
۲۳-۴-۲- پیاده سازی روش‌های مختلف اعطای مجوز به کاربران ۶۳۹
۲۳-۵- واحدهای سازمانی یا Organizational Unit (OU) ۶۴۲
۲۳-۶- نحوه ساخت واحد سازمانی ۶۴۳
۲۳-۷- واگذاری مدیریت OU ۶۴۴
فصل ۲۴ DNS Server ۶۴۷
۲۴-۱- معرفی DNS (Domain Name Server) ۶۴۷
۲۴-۲- تاریخچه DNS ۶۴۷
۲۴-۳- پروتکل DNS ۶۴۸
۲۴-۴- DNS Namespace ۶۴۸

فهرست مطالب (۱۵)

۲۴-۴-۱- معرفی FQDN (Fully Qualified Domain Names) ۶۵۰
۲۴-۴-۲- استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت ۶۵۱
۲۴-۴-۳- پیاده سازی نام یکسان برای منابع داخلی و خارجی ۶۵۱
۲۴-۴-۴- استفاده از اسامی متفاوت برای دامنه‌های اینترنت و اینترانت ۶۵۲
۲۴-۵- اجزاء DNS ۶۵۲
۲۴-۶- ناحیه‌ها یا Zoneها (Zones of Authority) ۶۵۳
۲۴-۶-۱- Forward Lookup Zone ۶۵۳
۲۴-۶-۲- Reverse Lookup Zones ۶۵۴
۲۴-۶-۳- تفاوت بین Domain و Zone ۶۵۴
۲۴-۶-۴- انواع Zone ۶۵۴
۲۴-۶-۵- ویژگی‌های یک Zone ۶۵۴
۲۴-۷- انواع روش تبدیل Hostname به IP Address ۶۵۶
۲۴-۷-۱- Non-Recursive Query (تکراری) ۶۵۶
۲۴-۷-۲- Recursive Query (بازگشتی) ۶۵۷
۲۴-۸- Cash Server ۶۵۸
۲۴-۹- پروتکل DNS و مدل مرجع OSI ۶۵۸
۲۴-۱۰- ساختار سرویس دهندگان نام دامنه‌ها در اینترنت ۶۵۹
۲۴-۱۱- DNS و WINS (Windows Internet Naming Service) ۶۶۰
۲۴-۱۱-۱- DNS ۶۶۰
۲۴-۱۱-۲- تفاوت بین DNS و WINS ۶۶۰
۲۴-۱۲- نصب DNS در ویندوز سرور ۲۰۰۳ ..... ۶۶۱
۲۴-۱۲-۱- تنظیم آدرس IP ۶۶۱
۲۴-۱۲-۲- نصب DNS از طریق آدرس‌دهی ۶۶۳
۲۴-۱۲-۳- نصب DNS از طریق شکل ۶۶۳
۲۴-۱۳- پیکربندی DNS Server ۶۶۵
۲۴-۱۴- تنظیمات DNS Server ۶۶۹
۲۴-۱۵- ایجاد Host جدید ۶۷۵
۲۴-۱۶- تست کردن DNS Server ۶۷۶
فصل ۲۵ مفاهیم اولیه در Active Directory ۶۷۷
۲۵-۱- آشنایی با زیرساخت‌های Active Directory ۶۷۷
۲۵-۲- آشنایی با سرویس دایرکتوری (Active Directory) ۶۷۷
۲۵-۲-۱- ویژگی‌های Active Directory ۶۷۷
۲۵-۲-۲- مزایای Active Directory ۶۷۸
۲۵-۳- اشیای موجود در Active Directory ۶۷۸
۲۵-۳-۱- اجزای منطقی ۶۷۹
۲۵-۳-۲- اجزای فیزیکی ۶۷۹
۲۵-۴- ساختار منطقی ۶۷۹
۲۵-۴-۱- دامنه - Domain ۶۸۰
۲۵-۴-۲- واحدهای سازمانی - OUs (Organization Units) ۶۸۲
۲۵-۴-۳- درخت‌ها - Trees ۶۸۳

فهرست مطالب (۱۶)

۲۵-۴-۴- جنگل‌ها – Forests ۶۸۳
۲۵-۵- ساختار فیزیکی ۶۸۴
۲۵-۵-۱- سایت‌ها (Sites) ۶۸۴
۲۵-۵-۲- کنترل‌کننده دامنه – DC (Domain Controller) ۶۸۵
۲۵-۶- برخی ویژگی‌های Active Directory ۶۸۵
۲۵-۶-۱- تکرار یا Replication ۶۸۶
۲۵-۶-۲- ارتباطات مطمئن (Trust Relationships) ۶۸۹
۲۵-۶-۳- سیاست‌های گروهی (Group Policies) ۶۹۰
فصل ۲۶ نصب و راه اندازی Active Directory ۶۹۲
۲۶-۱- نصب Active Directory ۶۹۲
۲۶-۲- حذف Active Directory ۷۰۲
۲۶-۳- مفاهیم Active Directory Backup ۷۰۵
۲۶-۴- پشتیبان گیری از Active Directory ۷۰۷
۲۶-۴-۱- پشتیبان گیری توسط رابط گرافیکی ۷۰۷
۲۶-۴-۲- پشتیبان گیری توسط خط فرمان ۷۱۰
۲۶-۵- بازگرداندن اطلاعات Restore Active Directory ۷۱۱
۲۶-۵-۱- شیوه‌های بازگرداندن پشتیبان ۷۱۱
۲۶-۵-۲- نحوه بازگرداندن به صورت Primary ۷۱۲
۲۶-۵-۳- نحوه بازگرداندن به صورت Normal ۷۱۵
۲۶-۵-۴- نحوه بازگرداندن به صورت Authoritative ۷۱۵
فصل ۲۷ DHCP Server ۷۱۸
۲۷-۱- آشنایی با DHCP Server ۷۱۸
۲۷-۱-۱- ویژگی‌های DHCP ۷۱۸
۲۷-۱-۲- جایگاه سرویس دهنده DHCP در یک شبکه مبتنی بر ویندوز ۲۰۰۳ ..... ۷۱۹
۲۷-۱-۳- پیکربندی سرویس دهنده DHCP ۷۱۹
۲۷-۱-۴- پیکربندی سرویس گیرندگان DHCP ۷۱۹
۲۷-۲- نصب DHCP Server ۷۲۱
۲۷-۲-۱- تنظیم IP Address برای سرور (به صورت دستی) ۷۲۱
۲۷-۲-۲- نصب DHCP Server ۷۲۳
۲۷-۲-۳- پیکربندی Firewall ۷۲۵
۲۷-۳- پیکربندی DHCP Server ۷۲۷
۲۷-۳-۱- قسمت‌های مختلف DHCP Server ۷۳۴
۲۷-۳-۲- تنظیم Client جهت استفاده از DHCP Server ۷۳۷
۲۷-۴- DHCP Backup & Restore ۷۴۰
فصل ۲۸ اتصال Client به Domain ۷۴۴
۲۸-۱- تنظیمات Server ۷۴۴
۲۸-۲- تنظیمات Client ۷۴۷
فصل ۲۹ Active Directory Users And Computers ۷۵۴
۲۹-۱- آشنایی با انواع Accountها و ابزارهای مدیریتی ۷۵۴

فهرست مطالب (۱۷)

۲۹-۲- مدیریت در Active Directory user and computer ۷۵۴
۲۹-۲-۱- آشنایی با گروه‌های Builtin ۷۵۵
۲۹-۲-۲- پوشه Computers ۷۵۵
۲۹-۲-۳- Domain Controllers ۷۵۶
۲۹-۲-۴- ForeignSecurityPrincipals ۷۵۶
۲۹-۳- مدیریت کاربران و گروه ها ۷۵۷
۲۹-۳-۱- تعریف کاربر، گروه و واحد سازمانی جدید ۷۵۷
۲۹-۴- مدیریت و تنظیمات کاربری ۷۵۷
۲۹-۴-۱- General ۷۵۸
۲۹-۴-۲- Account ۷۵۸
۲۹-۴-۳- Logon Hours ۷۵۹
۲۹-۴-۴- Log On To ۷۶۰
۲۹-۴-۵- Profile ۷۶۱
۲۹-۴-۶- Home Folder ۷۶۲
۲۹-۴-۷- Member of ۷۶۳
۲۹-۴-۸- Dial-in ۷۶۴
۲۹-۴-۹- Environment ۷۶۵
۲۹-۴-۱۰- Organization ۷۶۵
۲۹-۴-۱۱- تکثیر کاربران ۷۶۶
۲۹-۵- آشنایی با انواع گروه‌های Biult-in ۷۶۶
۲۹-۶- آموزش کار با Disk Quota ۷۶۷
فصل ۳۰ سیاست گروهی (Group Policy) ۷۷۴
۳۰-۱- تعریف Group Policy ۷۷۴
۳۰-۲- نحوه فعال شدن Group Policy ۷۷۷
۳۰-۳- ایجاد Organization Unit ۷۷۹
۳۰-۴- مثال‌های عملی از Group Policy ۷۸۱
۳۰-۴-۱- تنظیم Proxy برای کاربران به صورت گروهی ۷۸۱
۳۰-۴-۲- تغییر Title Bar اینترنت اکسپلورر ۷۸۴
۳۰-۴-۳- تنظیمات نوار وظیفه و منوی شروع (Start Menu and Taskbar) ۷۸۶
۳۰-۴-۴- تنظیمات و حذف و اضافه گزینه‌های مربوط به Control Panel ۷۸۷
۳۰-۴-۵- نصب برنامه‌های کاربردی ۷۸۹
۳۰-۴-۶- غیر فعال نمودن Ctrl + Alt + Delete ۷۹۱
۳۰-۴-۷- امنیت رمز عبور کاربران ۷۹۲
فصل ۳۱ کنترل از راه دور ۷۹۶
۳۱-۱- مقدمه ۷۹۶
۳۱-۲- Remote Desktop Connection ۷۹۷
۳۱-۲-۱- آماده سازی کامپیوتر راه دور ۷۹۷
۳۱-۲-۲- اتصال به کامپیوتر راه دور ۸۰۲
۳۱-۲-۳- Remote Desktop Connection در ویندوز سرور ۲۰۰۳ ..... ۸۰۸

فهرست مطالب (۱۸)

۳۱-۳- Terminal Server ۸۱۱
۳۱-۳-۱- راه اندازی Terminal Server در ویندوز سرور ۸۱۱
۳۱-۳-۲- Terminal Service Manager ۸۲۶
۳۱-۴- Remote Assistance ۸۲۹
۳۱-۴-۱- طریقه فعال سازی Remote Assistance ۸۲۹
۳۱-۴-۲- نکات مهم حین استفاده از Remote Assistance ۸۳۰
۳۱-۴-۳- روش ایجاد یک Invitation (دعوتنامه) توسط درخواست کننده ۸۳۱
۳۱-۴-۴- انواع روش ساخت دعوتنامه ۸۳۱
۳۱-۴-۵- روش استفاده از فایل Invitation توسط مددکار ۸۳۵
۳۱-۴-۶- تفاوت‌های Remote Desktop و Remote Assistance ۸۳۶
۳۱-۵- Team Viewer ۸۳۷
۳۱-۵-۱- معرفی نرم‌افزار Team Viewer ۸۳۷
۳۱-۵-۲- راه اندازی نرم‌افزار Team Viewer و کار با آن ۸۳۷
فصل ۳۲ اتصال از راه دور (VPN , Dial UP) ۸۴۵
۳۲-۱- چگونه از راه دور به شبکه خانگی خود متصل شویم؟ ۸۴۵
۳۲-۲- مفاهیم اولیه ۸۴۶
۳۲-۳- VPN ۸۴۷
۳۲-۳-۱- شبکه VPN چیست؟ ۸۴۷
۳۲-۳-۲- عناصر تشکیل دهنده یک VPN ۸۴۷
۳۲-۳-۳- شبکه های LAN جزایر اطلاعاتی ۸۴۸
۳۲-۳-۴- امنیت VPN ۸۴۹
۳۲-۳-۵- تکنولوژی های VPN ۸۵۰
۳۲-۳-۶- تونل سازی (Tunneling) ۸۵۱
۳۲-۳-۷- پروتکل های درون تونل ۸۵۲
۳۲-۳-۸- ویژگی های امنیتی در IPsec ۸۵۳
۳۲-۳-۹- Ipsec بدون تونل ۸۵۴
۳۲-۳-۱۰- پیش‌نیازها ۸۵۵
۳۲-۳-۱۱- نصب سرویس دهنده VPN ۸۵۵
۳۲-۳-۱۲- پیکربندی سرویسدهنده RAS ۸۵۵
۳۲-۳-۱۳- Transport در مقایسه با Tunnel ۸۵۶
۳۲-۳-۱۴- Authentication Header ۸۵۶
۳۲-۳-۱۵- Encapsulated Security Payload ۸۵۷
۳۲-۳-۱۶- Association Security ۸۵۷
۳۲-۳-۱۷- Internet Key Exchang ۸۵۷
۳۲-۳-۱۸- گواهینامه x.506 ..... ۸۵۸
۳۲-۴- راه‌های اتصال یک کاربر به یک شبکه راه دور ۸۵۸
۳۲-۵- آماده سازی ویندوز XP جهت دریافت و پذیرش درخواستها ۸۵۸
۳۲-۶- اتصال به کامپیوتر راه دور توسط Dial-UP یا VPDN ۸۶۴
۳۲-۷- اتصال به کامپیوتر راه دور توسط VPN ۸۶۸

فهرست مطالب (۱۹)

۳۲-۸- نصب VPN Server روی ویندوز سرور ۸۷۶
۳۲-۸-۱- غیر فعال کردن سرویس Firewall و ICS ۸۷۶
۳۲-۸-۲- نصب VPN Server ۸۷۷
۳۲-۸-۳- تنظیمات Routing and Remote Access (ویزارد RRAS) ۸۷۹
۳۲-۹- تنظیمات کاربران جهت اتصال راه دور به VPN ۸۸۸
۳۲-۱۰- معرفی DHCP Relay Agent و نحوه نصب آن ۸۸۹
۳۲-۱۱- نصب VPN Server با داشتن یک کارت شبکه ۸۹۵
۳۲-۱۲- ده نکته درباره رفع ایرادهای اتصالات VPN ۹۰۲
فصل ۳۳ Mail Server ۹۰۷
۳۳-۱- نصب Mail Server ۹۰۷
۳۳-۲- اجرای Mail Server ۹۱۰
۳۳-۳- ارسال و دریافت ایمیل با استفاده از Outlook Express ۹۱۲
۳۳-۴- نرم‌افزار مدیریت ایمیل MDaemon Mail Server ۹۲۰
۳۳-۴-۱- MDaemon Mail Server چیست؟ ۹۲۰
۳۳-۴-۲- نصب MDaemon Mail Server ۹۲۱
۳۳-۴-۳- پیکربندی نرم‌افزار MDaemon Mail Server ۹۲۷
۳۳-۴-۴- مدیریت حساب‌ها در MDaemon Mail Server ۹۳۲
۳۳-۴-۵- استفاده از MDaemon Mail Server تحت وب ۹۳۴
فصل ۳۴ FTP Server ۹۳۸
۳۴-۱- راه اندازی FTP Server ۹۳۹
۳۴-۲- قراردادن فایل‌ها بر روی FTP Server ۹۴۱
۳۴-۳- اتصال به FTP Server ۹۴۱
۳۴-۴- تنظیم Firewall ۹۴۳
فصل ۳۵ Microsoft Management Console یا MMC ۹۴۵
۳۵-۱- مفهوم Microsoft Management Console ۹۴۵
۳۵-۲- کار با MMC ۹۴۸
فصل ۳۶ Distributed File System یا DFS ۹۵۶
۳۶-۱- متمرکز کردن اطلاعات Share شده ۹۵۶
۳۶-۲- Distributed File System چیست؟ ۹۵۶
۳۶-۲-۱- مراحل انجام کار DFS ۹۵۷
۳۶-۲-۲- انواع DFS ۹۵۷
۳۶-۳- Distributed File System در ویندوز سرور ۹۵۸
۳۶-۴- ایجاد Link به یک پوشه Share شده ۹۶۲
۳۶-۵- دسترسی به پوشه‌های Share شده ۹۶۵
۳۶-۶- Replication در DFS ۹۶۶
فصل ۳۷ Streaming Media Server ۹۶۹
۳۷-۱- Streaming Media Server چیست؟ ۹۶۹
۳۷-۲- نصب Streaming Media Server ۹۷۰
۳۷-۳- اجرای Streaming Media Server ۹۷۲
۳۷-۴- روش Broadcast ۹۷۴

فهرست مطالب (۲۰)

۳۷-۴-۱- راه اندازی سرور ۹۷۴
۳۷-۴-۲- پخش قطعات صوتی/تصویری در Server ۹۷۷
۳۷-۴-۳- افزودن قطعه صوتی/تصویری جدید ۹۷۹
۳۷-۴-۴- پخش قطعات صوتی/تصویری در Client ۹۸۱
۳۷-۴-۵- پخش قطعات صوتی/تصویری از طریق مرورگر ۹۸۲
۳۷-۵- روش On-Demand ۹۸۸
۳۷-۶- ایجاد Publishing Point جدید ۹۹۰
فصل ۳۸ نصب و راه اندازی سرور سایت (IIS) ۹۹۹
۳۸-۱- معرفی IIS ۹۹۹
۳۸-۲- نصب IIS ۱۰۰۰
۳۸-۳- اجرا و پیکربندی IIS ۱۰۰۳
۳۸-۳-۱- تعریف Web Site جدید ۱۰۰۴
۳۸-۳-۲- تنظیم وب سایت ۱۰۰۷
۳۸-۳-۳- اجرای وب سایت ۱۰۱۰
۳۸-۴- اجرای وب سایت‌های ASP.Net ۱۰۱۳
فصل ۳۹ مجازی‌سازی با VMware vSphere 5 ..... ۱۰۱۸
۳۹-۱- مقدمه ۱۰۱۹
۳۹-۲- مجازی سازی ۱۰۲۰
۳۹-۲-۱- مدل مجازی‌سازی ۱۰۲۰
۳۹-۲-۲- لایه‌های مجازی‌سازی ۱۰۲۱
۳۹-۲-۳- چند اصطلاح – چند اشتباه ۱۰۳۶
۳۹-۳- معرفی مجموعه VMware vSphere 5 ..... ۱۰۴۰
۳۹-۳-۱- VMware ESXi ۱۰۴۱
۳۹-۳-۲- VMware vCenter Server ۱۰۴۲
۳۹-۳-۳- vSphere Update Manager ۱۰۴۲
۳۹-۳-۴- vSphere Client and vSphere web Client ۱۰۴۳
۳۹-۳-۵- VMware vShield Zones ۱۰۴۳
۳۹-۳-۶- VMware vCenter Orchestrator ۱۰۴۳
۳۹-۳-۷- چند پردازشی متقارن مجازی ۱۰۴۳
۳۹-۳-۸- vSphere vMotion and vSphere Storage vMotion ۱۰۴۴
۳۹-۳-۹- سیستم زمانبند منابع توزیع شده ۱۰۴۴
۳۹-۳-۱۰- vSphere Storage DRS ۱۰۴۵
۳۹-۳-۱۱- سیستم کنترل ورودی خروجی شبکه و کنترل ورودی خروجی سیستم‌های ذخیره سازی ۱۰۴۵
۳۹-۳-۱۲- قابلیت دسترسی مستمر (HA) ۱۰۴۶
۳۹-۳-۱۳- سیستم تحمل‌پذیر خطا (FT) ۱۰۴۶
۳۹-۳-۱۴- vSphere Storage API for data protection and VMware data recovery ۱۰۴۷
۳۹-۳-۱۵- مقایسه Xenserver , Hyper-V , VMware ۱۰۴۸
۳۹-۴- نصب و راه اندازی مجموعه WMware vSphere 5 ..... ۱۰۴۸
۳۹-۴-۱- نصب راه اندازی و پیکر بندی ESXi ۱۰۴۹

فهرست مطالب (۲۱)

۳۹-۴-۲- راه اندازی vCenter Server ۱۰۵۳
۳۹-۴-۳- نصب vSphere Client برای ورود به vCenter Server ۱۰۶۰
۳۹-۴-۴- نصب vSphere Web Client ۱۰۶۱
۳۹-۵- دستگاه‌های ذخیره‌سازی داده ۱۰۶۳
۳۹-۵-۱- انواع سیستم‌های ذخیره‌سازی ۱۰۶۳
۳۹-۵-۲- راه اندازی یک ISCSI SAN ۱۰۶۵
۳۹-۶- راه اندازی و مدیریت سیستم مجازی سازی ۱۰۷۵
۳۹-۶-۱- ایجاد دیتاسنتر و اضافه کردن میزبان‌های ESXi به vCenter ۱۰۷۵
۳۹-۶-۲- ساخت ماشین مجازی ۱۰۷۶
۳۹-۶-۳- تخصیص منابع به ماشین‌های مجازی ۱۰۷۷
۳۹-۶-۴- ساخت کلاستر و اضافه کردن میزبان‌های ESXi به آن ۱۰۷۸
۳۹-۶-۵- فعال‌سازی ویژگی DRS در کلاستر ۱۰۸۰
۳۹-۶-۶- مدیریت و تقسیم بندی منابع با Resource Pools ۱۰۸۴
۳۹-۶-۷- تکثیر ماشین‌های مجازی ۱۰۸۵
فصل ۴۰ نرم‌افزار ISA Server ۱۰۸۶
۴۰-۱- مقدمه ۱۰۸۶
۴۰-۱-۱- Cache ۱۰۸۶
۴۰-۱-۲- Firewall ۱۰۸۷
۴۰-۱-۳- دیگر قابلیت‌ها ۱۰۸۷
۴۰-۱-۴- حالات نصب ۱۰۸۸
۴۰-۲- ISA Server ۱۰۸۹
۴۰-۲-۱- Internet Security & Acceleration Server ۱۰۸۹
۴۰-۳- نصب نرم‌افزار ISA Server ۱۰۸۹
۴۰-۳-۱- مراحل نصب ISA Server ۱۰۹۰
۴۰-۴- تنظیمات ISA Server ۱۰۹۳
۴۰-۴-۱- تنظیمات امنیت شبکه خارجی در نقل وانتقال داده ۱۰۹۴
۴۰-۴-۲- تنظیمات ISA Server به عنوان یک Firewall ۱۰۹۶
۴۰-۴-۳- نحوه تنظیم یک شبکه جدید بر روی ISA Server ۱۰۹۷
۴۰-۴-۴- تنظیمات Network Rule on ISA Server (جهت ارتباط یک شبکه Local وخارجی) ۱۱۰۲
۴۰-۴-۵- تنظیمات Network Ruleon ISA Server (جهت ارتباط یک شبکه Local وخارجی) ۱۱۰۹
۴۰-۵- مشاهده روش‌های دستیابی به شبکه در ISA Server ۱۱۱۶
۴۰-۶- تشخیص نفوذ ۱۱۱۷
۴۰-۷- نحوه ایجاد سرویس‌های VPN با ISA Server ۱۱۱۹
۴۰-۷-۱- تنظیمات VPN در ISA Server ۱۱۲۰
فصل ۴۱ نرم‌افزار Packet Tracer ۱۱۳۲
۴۱-۱- آشنایی با نرم‌افزار Packet Tracer ۱۱۳۱
۴۱-۲- فضاهای کار فیزیکی و منطقی ۱۱۴۶
۴۱-۳- فضای کار منطقی ۱۱۴۶
۴۱-۴- فضای کار فیزیکی ۱۱۵۳

فهرست مطالب (۲۲)

۴۱-۵- حالت‌های عملکرد..... ۱۱۵۹
۴۱-۶- حالت RealTime..... ۱۱۵۹
۴۱-۷- حالت شبیه‌سازی (Simulation)..... ۱۱۶۱
۴۱-۸- اطلاعات بسته در حالت شبیه‌سازی..... ۱۱۶۴
۴۱-۹- حالت Challenge..... ۱۱۶۵
۴۱-۱۰- مدیریت سناریوها در حالت شبیه‌سازی..... ۱۱۶۷
۴۱-۱۱- Complex PDU در حالت شبیه‌سازی..... ۱۱۶۹
۴۱-۱۲- انواع اتصالات..... ۱۱۷۰
۴۱-۱۳- دستگاه‌ها و ماژول‌ها..... ۱۱۷۲
۴۱-۱۴- پیکربندی دستگاه‌ها..... ۱۱۷۳
۴۱-۱۵- مثال عملی) قسمت اول - ایجاد یک شبکه..... ۱۲۰۰
۴۱-۱۶- مثال عملی) قسمت دوم - توسعه توپولوژی شبکه..... ۱۲۱۰
۴۱-۱۷- مثال عملی) قسمت سوم - شبیه‌سازی یک ISP و شبکه خانگی..... ۱۲۱۸
۴۱-۱۸- Activity Wizard..... ۱۲۴۸

فصل ۱

آشنایی با شبکه

۱-۱- معرفی

دنیای امروز عصر ارتباطات نام گذاری شده است و جوامع امروزی جوامع اطلاعاتی نامیده می‌شوند. اصولا ارتباطات اساس اجتماع بشر را تشکیل می‌دهد و از نیازهای اصلی جوامع اطلاعاتی، انتقال سریع اطلاعات در مجمع‌های عمده است. اطلاعات مهم است چون عامل خلاقیت و اصولا انگیزه ارتباط است. شبکه‌ها از عظیم ترین تکنولوژی هایی هستند که بشر جهت ساده‌تر کرده پخش انبوه اطلاعات ایجاد کرده است. شبکه امکان ارتباط متقابل بین افراد در هر زمانی بدون توجه به بعد مسافت را می‌دهد و مهمترین ابزار تبادل اطلاعات بشمار می‌رود. استفاده از شبکه‌های کامپیوتری در چندین سال اخیر رشد فراوانی کرده و سازمان‌ها و موسسات اقدام به برپایی شبکه نموده‌اند. هر شبکه کامپیوتری باید با توجه به شرایط و سیاست‌های هر سازمان، طراحی و پیاده سازی گردد. در واقع شبکه‌های کامپیوتری زیر ساخت‌های لازم را برای به اشتراک گذاشتن منابع در سازمان فراهم می‌آورند؛ در صورتیکه این زیر ساخت‌ها به درستی طراحی نشوند، در زمان استفاده از شبکه مشکلات متفاوتی پیش آمده و باید هزینه‌های زیادی به منظور نگهداری شبکه و تطبیق آن با خواسته‌های مورد نظر صرف شود.

یک شبکه رایانه‌ای، اجازه به اشتراک گذاری منابع و اطلاعات در میان دستگاه‌ها و سیستم‌های متصل شده به هم را می‌دهد. در دهه ۶۰ میلادی، آژانس پروژه‌های تحقیقاتی پیشرفته (ARPA)، بودجه‌ای را به منظور طراحی شبکه آژانس پروژه‌های تحقیقاتی پیشرفته (ARPANET) برای وزارت دفاع ایالات متحده آمریکا اختصاص داد. این اولین شبکه رایانه‌ای در جهان بود. توسعه شبکه از سال ۱۹۶۹ و براساس طرح‌های توسعه یافته دهه ۶۰ آغاز شد.

۱-۲- تاریخچه شبکه

در سال ۱۹۵۷ نخستین ماهواره، یعنی اسپوتنیک توسط اتحاد جماهیر شوروی سابق به فضا پرتاب شد. در همین دوران دنیا در دوران رقابت سختی از نظر تسلیحاتی بین دو ابر قدرت آن زمان جریان داشت و دنیا در دوران جنگ سرد به سر می‌برد. وزارت دفاع امریکا در واکنش به این اقدام رقیب نظامی خود، آژانس پروژه‌های تحقیقاتی پیشرفته یا آرپا (ARPA) را تاسیس کرد. یکی از پروژه‌های مهم این آژانس تامین ارتباطات در زمان جنگ جهانی احتمالی تعریف شده بود. در همین

سال‌ها در مراکز تحقیقاتی غیر نظامی که بر امتداد دانشگاه‌ها بودند، تلاش برای اتصال کامپیوترها به یکدیگر در جریان بود. در آن زمان کامپیوترهای Mainframe از طریق ترمینال‌ها به کاربران سرویس می‌دادند. در اثر اهمیت یافتن این موضوع آژانس آرپا (ARPA) منابع مالی پروژه اتصال دو کامپیوتر از راه دور به یکدیگر را در دانشگاه MIT بر عهده گرفت. در اواخر سال ۱۹۶۰ اولین شبکه کامپیوتری بین چهار کامپیوتر که دو تای آن‌ها در MIT، یکی در دانشگاه کالیفرنیا و دیگری در مرکز تحقیقاتی استنفورد قرار داشتند، راه اندازی شد. این شبکه آرپانت نامگذاری شد. در سال ۱۹۶۵ نخستین ارتباط راه دور بین دانشگاه MIT و یک مرکز دیگر نیز برقرار گردید. در سال ۱۹۷۰ شرکت معتبر زیراکس یک مرکز تحقیقاتی در پالوآلتو تاسیس کرد. این مرکز در طول سال‌ها مهمترین فناوری‌های مرتبط با کامپیوتر را معرفی کرده است و از این نظریه به یک مرکز تحقیقاتی افسآن‌های بدل گشته است. این مرکز تحقیقاتی که پارک (PARC) نیز نامیده می‌شود، به تحقیقات در زمینه شبکه‌های کامپیوتری پیوست. تا این سال‌ها شبکه آرپانت به امور نظامی اختصاص داشت، اما در سال ۱۹۷۲ به عموم معرفی شد. در این سال شبکه آرپانت مراکز کامپیوتری بسیاری از دانشگاه‌ها و مراکز تحقیقاتی را به هم متصل کرده بود. در سال ۱۹۷۲ نخستین نامه الکترونیکی از طریق شبکه منتقل گردید. در این سال‌ها حرکتی غیر انتفاعی به نام MERIT که چندین دانشگاه بنیان گذار آن بوده‌اند، مشغول توسعه روش‌های اتصال کاربران ترمینال‌ها به کامپیوتر مرکزی یا میزبان بود. مهندسان پروژه MERIT در تلاش برای ایجاد ارتباط بین کامپیوترها، مجبور شدند تجهیزات لازم را خود طراحی کنند. آنان با طراحی تجهیزات واسطه برای مینی کامپیوتر DECPDP-11 نخستین بستر اصلی یا Backbone شبکه کامپیوتری را ساختند. تا سال‌ها نمونه‌های اصلاح شده این کامپیوتر با نام PCP یا Processor Communications Primary نقش میزبان را در شبکه‌ها ایفا می‌کرد. نخستین شبکه از این نوع که چندین ایالت را به هم متصل می‌کرد Michnet نام داشت. روش اتصال کاربران به کامپیوتر میزبان در آن زمان به این صورت بود که یک نرم‌افزار خاص بر روی کامپیوتر مرکزی اجرا می‌شد. و ارتباط کاربران را برقرار می‌کرد. اما در سال ۱۹۷۶ نرم‌افزار جدیدی به نام Hermes عرضه شد که برای نخستین بار به کاربران اجازه می‌داد تا از طریق یک ترمینال به صورت تعاملی مستقیماً به سیستم MERIT متصل شوند. این، نخستین باری بود که کاربران می‌توانستند در هنگام برقراری ارتباط از خود بپرسند: کدام میزبان؟ از وقایع مهم تاریخچه شبکه‌های کامپیوتری، ابداع روش سوئیچینگ بسته‌ای یا Packet Switching است. قبل از معرفی شدن این روش از سوئیچینگ مداری یا Circuit Switching برای تعیین مسیر ارتباطی استفاده می‌شد. اما در سال ۱۹۷۴ با پیدایش پروتکل ارتباطی TCP/IP از مفهوم Packet Switching استفاده گسترده تری شد. این پروتکل در سال ۱۹۸۲ جایگزین پروتکل NCP شد و به پروتکل استاندارد برای آرپانت تبدیل گشت. در همین زمان یک شاخه فرعی بنام MILnet در آرپانت همچنان از پروتکل قبلی پشتیبانی می‌کرد و به ارائه خدمات نظامی می‌پرداخت. با این تغییر و تحول، شبکه‌های زیادی به بخش تحقیقاتی این شبکه متصل شدند و آرپانت به اینترنت تبدیل گشت. در این سال‌ها حجم ارتباطات شبکه‌ای افزایش یافت و مفهوم ترافیک شبکه مطرح شد. مسیر یابی در این شبکه به کمک آدرس‌های IP به صورت ۳۲ بیتی انجام می‌گرفته است. هشت بیت اول آدرس IP به شبکه‌های محلی تخصیص داده شده بود که به سرعت مشخص گشت تناسبی با نرخ رشد شبکه‌ها ندارد و باید در آن تجدید نظر شود. مفهوم شبکه‌های LAN و شبکه‌های WAN در سال دهه ۷۰ میلادی از یکدیگر تفکیک شدند. در آدرس‌دهی ۳۲ بیتی اولیه، بقیه ۲۴ بیت آدرس به میزبان در شبکه اشاره می‌کرد. در سال ۱۹۸۳ سیستم نامگذاری دامنه‌ها

(Domain Name System) به وجود آمد و اولین سرویس دهنده نامگذاری(Name Server) راه اندازی شد و استفاده از نام به جای آدرس‌های عددی معرفی شد. در این سال تعداد میزبآن‌های اینترنت از مرز ده هزار عدد فراتر رفته بود.

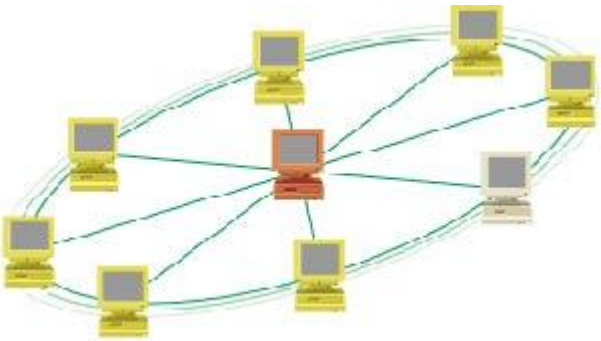
۱-۳- تعریف شبکه

شبکه‌های کامپیوتری، مجموعه‌ای از کامپیوترهای **مستقل و متصل** به یکدیگرند که با یکدیگر ارتباط داشته و تبادل اطلاعات می‌کنند. مستقل بودن کامپیوترها بدین معناست که هر کدام دارای واحدهای کنترلی و پردازشی مجزا بوده و بود و نبود یکی بر دیگری تاثیرگذار نیست.

متصل بودن کامپیوترها یعنی کامپیوترها از طریق یک رسانه مانند کابل، فیبر نوری، ماهواره‌ها و... به هم متصل می‌باشند. دو شرط فوق، شروط لازم برای ایجاد یک شبکه کامپیوتری می‌باشد؛ اما شرط کافی برای تشکیل یک شبکه کامپیوتری داشتن ارتباط و تبادل داده بین کامپیوترها است.

برای شبکه‌سازی، حداقل به دو کامپیوتر نیاز است. در مورد تعداد بیشتری رایانه که به هم متصل هستند، عموماً توابع پایه‌ای مشترکی دیده می‌شود. از این بابت برای آنکه شبکه‌ای به وظیفه اش عمل کند، سه نیاز اولیه بایستی فراهم گردد، اتصالات، ارتباطات و خدمات. **اتصالات** به بستر سخت‌افزاری اشاره دارد، **ارتباطات** به روشی اشاره می‌کند که بواسطه آن وسایل با یکدیگر صحبت کنند و **خدمات** آن‌هایی هستند که برای بقیه اعضای شبکه به اشتراک گذاشته شده‌اند.

اما در یک تعریف کلی می‌توان گفت که شبکه مجموعه‌ای از کامپیوترها، نرم‌افزار و سخت‌افزارهای متصل به هم است که باعث می‌شود کاربران بتوانند با یکدیگر کار کنند.



۱-۴- هدف از ایجاد شبکه

به طور کلی اهدافی مثل زیر در ایجاد یک شبکه کامپیوتری دنبال می‌شود:

۱. استفاده مشترک از منابع

۲. استفاده از منابع راه دور

۳. افزایش امنیت و انعطاف پذیری

۴. مکانیزه کردن یا اتوماسیون کردن مجموعه ها

۵. استفاده بهینه از وقت و امکانات و صرفه جویی در هزینه ها

به نظر می‌رسد که همین موارد دلایل خوبی برای به راه انداختن یک شبکه می‌باشد. ضمن اینکه موارد متعدد دیگری نیز موجود می‌باشد.

۱-۵- مزایای شبکه

۱. استفاده از منابع مشترک (اطلاعات، نرم‌افزارها و سخت‌افزارها)

۲. حذف محدودیتهای جغرافیایی

۳. تبادل سریع‌تر و دقیق‌تر اطلاعات

۴. صرفه جویی در هزینه ها

۵. افزایش امنیت

اما در مطالب فوق یک کلمه به نام منابع را بکار بردیم آیا می‌دانید منابع چه هستند؟

منظور از منابع در کامپیوترها امکانات آن‌ها مثل پردازنده مرکزی، هارد دیسک، چاپگر که جزء منابع سخت‌افزاری هستند و بانکهای اطلاعاتی، فایلهای صوتی و تصویری به عنوان منابع نرم‌افزاری می‌باشد.

۱-۶- دسته بندی شبکه‌های رایانه ای

در بحث شبکه‌های کامپیوتری دسته بندی‌های مختلفی وجود دارد که به مرور آن‌ها را بررسی خواهیم نمود.

۱-۶-۱- بر اساس نوع اتصال

شبکه‌های رایانه‌ای را می‌توان با توجه به تکنولوژی سخت‌افزاری و یا نرم‌افزاری که برای اتصال دستگاه‌های شبکه استفاده می‌شود، دسته بندی کرد؛ مانند **فیبر نوری، اترنت، شبکه بی‌سیم، ارتباط خط نیرو یا G.hn**.

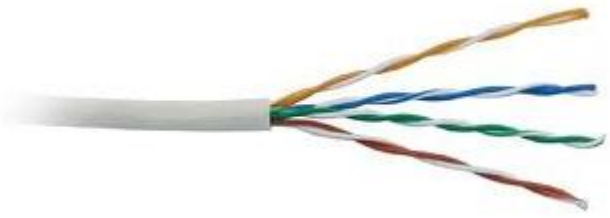
اترنت با استفاده از سیم کشی فیزیکی دستگاه‌ها را به هم متصل می‌کند. دستگاه‌های مستقر معمول شامل هاب‌ها، سوئیچ‌ها، پل‌ها و یا مسیریاب‌ها هستند.

تکنولوژی **شبکه بی‌سیم** برای اتصال دستگاه‌ها، بدون استفاده از سیم کشی طراحی شده است. این دستگاه‌ها از امواج رادیویی یا سیگنالهای مادون قرمز به عنوان رسانه انتقال استفاده می‌کنند.

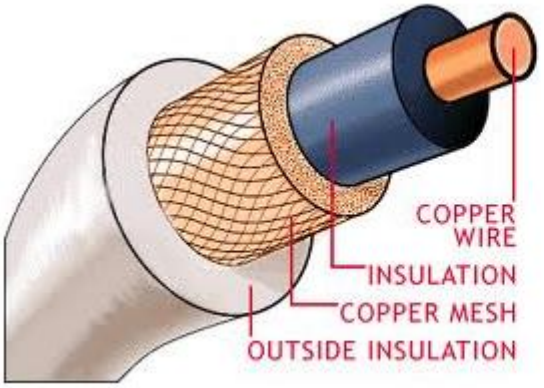
فناوری ITU-T G.hn از سیم کشی موجود در منازل (کابل هم محور، خطوط تلفن و خطوط برق) برای ایجاد یک شبکه محلی پر سرعت (تا۱ گیگابیت در ثانیه) استفاده می‌کند.

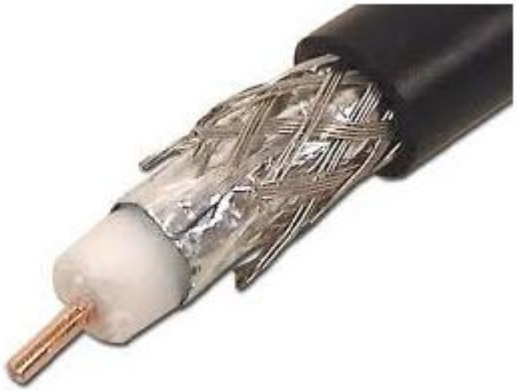
۱-۶-۲- بر اساس تکنولوژی سیم کشی

۱- زوج به هم تابیده (Twisted Pair): زوج به هم تابیده یکی از بهترین رسانه‌های مورد استفاده برای ارتباطات راه دور می‌باشد. سیم‌های زوج به هم تابیده، سیم تلفن معمولی هستند که از دو سیم مسی عایق که دو به دو به هم پیچ خورده‌اند درست شده‌اند. از زوج به هم تابیده برای انتقال صدا و داده‌ها استفاده می‌شود. استفاده از دو سیم به هم تابیده به کاهش تداخل و القای الکترومغناطیسی کمک می‌کند. سرعت انتقال داده، دامنه‌ای از ۲ مگابیت در هر ثانیه تا ۱۰۰ مگابیت در هر ثانیه دارد.

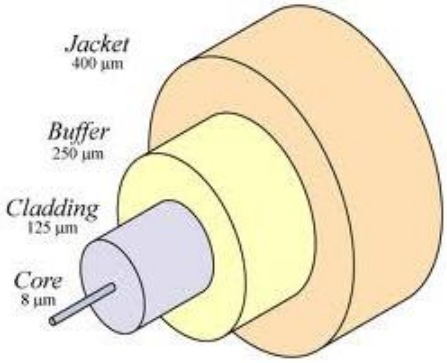


۲- کابل هم محور (Coaxial): کابل هم محور به طور گسترده‌ای در سیستم‌های تلویزیون کابلی، ساختمآن‌های اداری، و دیگر سایت‌های کاری برای شبکه‌های محلی، استفاده می‌شود. کابل‌ها یک رسانای داخلی دارند که توسط یک عایق منعطف محصور شده‌اند، که روی این لایه منعطف نیز توسط یک رسانای نازک برای انعطاف کابل، به هم بافته شده است. همه این اجزا، در داخل عایق دیگری جاسازی شده‌اند. لایه عایق به حداقل رساندن تداخل و اعوجاج کمک می‌کند. سرعت انتقال داده، دامنه‌ای از ۲۰۰ میلیون تا بیش از ۵۰۰ میلیون بیت در هر ثانیه دارد.





۳- فیبر نوری: کابل فیبر نوری شامل یک یا چند رشته از الیاف شیشه‌ای پیچیده شده در لایه‌های محافظ می‌باشد. این کابل می‌تواند نور را تا مسافت‌های طولانی انتقال دهد. کابل‌های فیبر نوری تحت تاثیر تابش‌های الکترومغناطیسی قرار نمی‌گیرند. سرعت انتقال ممکن است به چند تریلیون بیت در ثانیه برسد.







۱-۶-۳- بر اساس تکنولوژی بی‌سیم

۱- ریز موج (مایکروویو) زمینی: ریز موج‌های زمینی از گیرندهها و فرستنده‌های زمینی استفاده می‌کنند. تجهیزات این تکنولوژی شبیه به دیش‌های ماهواره است. مایکروویو زمینی از دامنه‌های کوتاه گیگاهرتز استفاده می‌کند، که این سبب می‌شود تمام ارتباطات به صورت دید خطی محدود باشد. فاصله بین ایستگاه‌های رله (تقویت سیگنال) حدود ۳۰ مایل است. آنتن‌های ریز موج معمولاً در بالای ساختمآن‌ها، برج‌ها، تپه‌ها و قله کوه نصب می‌شوند.

۲- ماهواره‌های ارتباطی: ماهواره‌ها از ریز موج‌های رادیویی که توسط جو زمین منحرف نمی‌شوند، به عنوان رسانه مخابراتی خود استفاده می‌کنند. ماهواره‌ها در فضا مستقر هستند؛ به طور معمول ۲۲۰۰۰ مایل (برای ماهواره‌های Geosynchronous) بالاتر از خط استوا. این سیستم‌های در حال چرخش به دور زمین، قادر به دریافت و رله صدا، داده‌ها و سیگنال‌های تلویزیونی هستند.

۳- تلفن همراه: سیستم‌های تلفن همراه از چندین فناوری ارتباطات رادیویی استفاده می‌کنند. این سیستم‌ها به مناطق مختلف جغرافیایی تقسیم شده‌اند. هر منطقه دارای فرستنده‌های کم قدرت و یا دستگاه‌های رله رادیویی آنتن برای تقویت تماس‌ها از یک منطقه به منطقه بعدی است.

۴- شبکه‌های محلی بی‌سیم: شبکه محلی بی‌سیم از یک تکنولوژی رادیویی فرکانس بالا (مشابه سلول دیجیتالی) و یک تکنولوژی رادیویی فرکانس پایین استفاده می‌کند. شبکه‌های محلی بی‌سیم از تکنولوژِی طیف گسترده، برای برقراری ارتباط میان دستگاه‌های متعدد در یک منطقه محدود، استفاده می‌کنند. نمونه‌ای از استاندارد تکنولوژی بی‌سیم، موج رادیویی IEEE است.

۵- ارتباطات مادون قرمز: ارتباط فروسرخ، سیگنال‌های بین دستگاه‌ها را در فواصل کوچک (کمتر از ۱۰ متر) به صورت همتا به همتا (رو در رو) انتقال می‌دهد؛ در خط انتقال نباید هیچ گونه شی‌ای قرار داشته باشد.

۱-۶-۴- بر اساس اندازه

ممکن است شبکه‌های رایانه‌ای بر اساس اندازه یا گستردگی ناحیه‌ای که شبکه پوشش می‌دهد طبقه بندی شوند. برای نمونه شبکه شخصی (PAN)، شبکه محلی (LAN)، شبکه دانشگاهی (CAN)، شبکه کلان شهری (MAN)، شبکه گسترده (WAN) و شبکه‌های متصل.

۱- شبکه شخصی (Personal Area Network): یک شبکه رایانه‌ای است که برای ارتباطات میان وسایل رایانه‌ای که اطراف یک فرد می‌باشند (مانند تلفن‌ها و رایانه‌های جیبی (PDA) که به آن دستیار دیجیتالی شخصی نیز می‌گویند) بکار می‌رود. این که این وسایل ممکن است متعلق به آن فرد باشند یا خیر جای بحث خود را دارد. برد یک شبکه شخصی عموماً چند متر بیشتر نیست. موارد مصرف شبکه‌های خصوصی می‌تواند جهت ارتباطات وسایل شخصی چند نفر به یکدیگر و یا برقراری اتصال این وسایل به شبکه‌ای در سطح بالاتر و شبکه اینترنت باشد.

ارتباطات شبکه‌های شخصی ممکن است به صورت سیمی به گذرگاه‌های رایانه مانند USB و FireWire برقرار شود. همچنین با بهره گیری از فناوری هایی مانند IrDA، بلوتوث و UWB می‌توان شبکه‌های شخصی را به صورت بی‌سیم ساخت.



۲- شبکه محلی (Local Area Network): یک شبکه رایانه‌ای است که محدوده جغرافیایی کوچکی مانند یک خانه، یک دفتر کار یا گروهی از ساختمآن‌ها را پوشش می‌دهد. در مقایسه با شبکه‌های گسترده (WAN) از مشخصات تعریف شده شبکه‌های محلی می‌توان به موارد زیر اشاره کرد:

۱. سرعت (نرخ انتقال) بسیار بالاتر از Wan

۲. محدوده جغرافیایی کوچکتر و عدم نیاز به خطوط استیجاری مخابراتی

۳. امنیت بالاتر

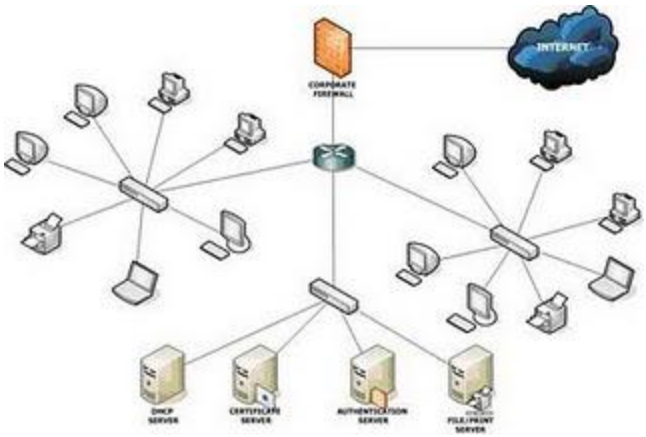
۴. تعداد کامپیوتر کمتر

۵. مدیریت راحت تر

دو فناوری اترنت (Ethernet) روی کابل جفت به هم تابیده بدون محافظ (UTP) و WiFi (WiFi) رایج ترین فناوری هایی هستند که امروزه استفاده می‌شوند، با این حال فناوری‌های آرکِنت (ARCNET) و توکن رینگ (Token Ring) و بسیاری روشهای دیگر در گذشته مورد استفاده بوده‌اند.

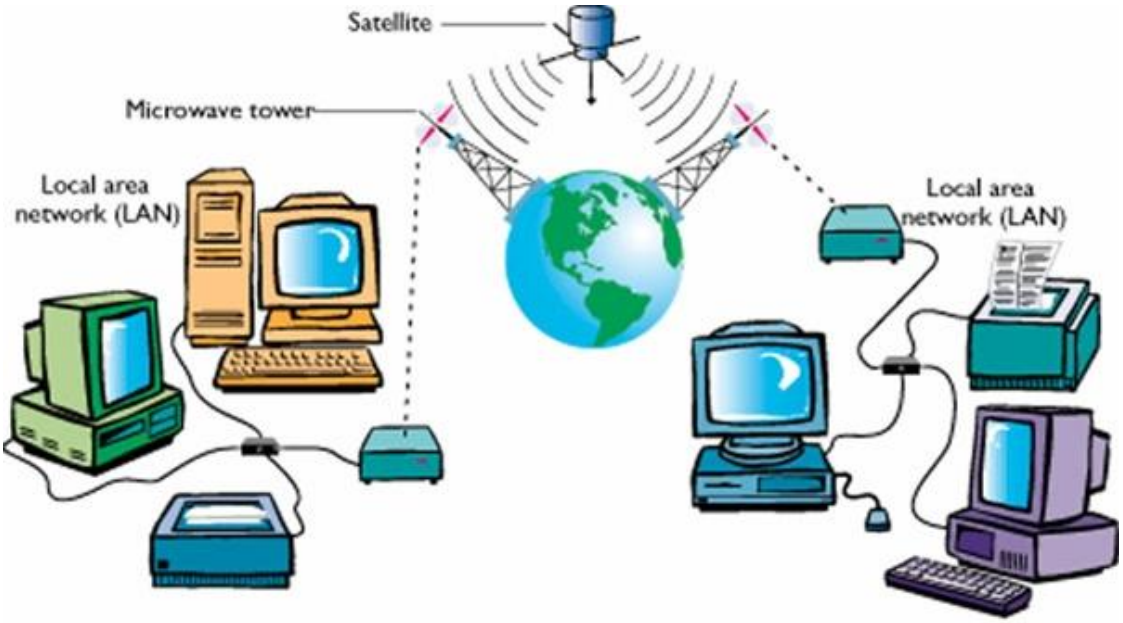


۳- شبکه دانشگاهی (Campus Area Network): که در بعضی ترجمه‌ها، به آن شبکه پردیس نیز گفته‌اند که یک شبکه رایانه‌ای است که از اتصال چند شبکه محلی (LAN) که همه آن‌ها محدود به یک ناحیه جغرافیایی هستند ساخته می‌شود، مانند محوطه یک دانشگاه، یک مجموعه صنعتی یا یک پایگاه نظامی. می‌توان آن را به عنوان یکی از انواع شبکه‌های کلان شهری (MAN) به حساب آورد که عموماً محدود به ناحیه‌ای کوچک‌تر از اندازه معمول یک شبکه کلان شهری است. در حالتی که در فضای یک دانشگاه شبکه‌ای از نوع شبکه دانشگاهی داشته باشیم، شبکه مورد نظر محتملا ساختمآن‌های دانشکدههای مختلف شامل بخش‌های آکادمیک، کتابخانه دانشگاه و ساختمان محل اقامت دانشجویان را به یکدیگر متصل می‌کند. شبکه دانشگاهی بزرگ‌تر از یک شبکه محلی ولی کوچکتر از یک شبکه گسترده (WAN) است.



۴- شبکه کلان شهری (Metropolitan Area Network): یک شبکه رایانه‌ای بزرگ است که معمولاً در سطح یک شهر گسترده می‌شود. در این شبکه‌ها معمولاً از زیرساخت بی‌سیم و یا اتصالات فیبر نوری جهت ارتباط محل‌های مختلف استفاده می‌شود. به عبارت دیگر شبکه Man، به شبکه هایی ما بین شبکه‌های LAN و WAN گفته می‌شود و یک راه تشخیص آن، این است که از تجهیزات مخابراتی آنچنانی استفاده نمی‌شود. مثلاً اگر شرکتی در یک شهر دارای چند شعبه باشد و بخواهید آن شعبه‌ها را به یکدیگر متصل کند، یک چنین شبکه‌ای ایجاد می‌کند

۵- شبکه گسترده (Wide Area Network): یک شبکه رایانه‌ای است که نسبتاً ناحیه جغرافیایی وسیعی را پوشش می‌دهد (برای نمونه از یک کشور به کشوری دیگر یا از یک قاره به قاره‌ای دیگر). این شبکه‌ها معمولاً از امکانات انتقال خدمات دهندگان عمومی مانند شرکت‌های مخابرات استفاده می‌کند. به عبارت کمتر رسمی این شبکه‌ها از مسیریاب‌ها و لینک‌های ارتباطی عمومی استفاده می‌کنند.



۶- شبکه متصل (Internetwork): دو یا چند شبکه یا زیرشبکه (Subnet) که با استفاده از تجهیزاتی که در لایه ۳ یعنی لایه شبکه مدل مرجع OSI (این لایه را در فصل‌های بعدی معرفی خواهیم نمود) عمل می‌کنند؛ مانند یک مسیریاب، به یکدیگر متصل می‌شوند تشکیل یک شبکه از شبکه‌ها یا شبکه متصل را می‌دهند. همچنین می‌توان شبکه‌ای که از اتصال داخلی میان شبکه‌های عمومی، خصوصی، تجاری، صنعتی یا دولتی به وجود می‌آید را شبکه متصل نامید.

در کاربردهای جدید، شبکه‌های به هم متصل شده از قرارداد IP استفاده می‌کنند. بسته به اینکه چه کسانی یک شبکه را مدیریت می‌کنند و اینکه چه کسانی در این شبکه عضو هستند، می‌توان سه نوع شبکه متصل دسته بندی نمود:

- **شبکه داخلی یا اینترانت (Intranet)**
- **شبکه خارجی یا اکسترانت (Extranet)**
- **شبکه اینترنت (Internet)**

شبکه‌های داخلی یا خارجی ممکن است که اتصالاتی به شبکه اینترنت داشته و یا نداشته باشند. در صورتی که این شبکه‌ها به اینترنت متصل باشند در مقابل دسترسی‌های غیرمجاز از سوی اینترنت محافظت می‌شوند. خود شبکه اینترنت به عنوان بخشی

از شبکه داخلی یا شبکه خارجی به حساب نمیاید، اگرچه که ممکن است شبکه اینترنت به عنوان بستری برای برقراری دسترسی بین قسمت هایی از یک شبکه خارجی خدماتی را ارائه دهد.

۱- شبکه داخلی (Intranet)

یک شبکه داخلی مجموعه‌ای از شبکه‌های متصل به هم می‌باشد که از قرارداد IP و ابزارهای مبتنی بر IP مانند مرورگرهای وب استفاده می‌کند و معمولاً زیر نظر یک نهاد مدیریتی کنترل می‌شود. این نهاد مدیریتی شبکه داخلی را نسبت به باقی قسمت‌های دنیا محصور می‌کند و به کاربران خاصی اجازه ورود به این شبکه را می‌دهد. به طور معمول‌تر شبکه درونی یک شرکت یا دیگر شرکت‌ها شبکه داخلی می‌باشد.

۲- شبکه خارجی (Extranet)

یک شبکه خارجی یک شبکه یا یک شبکه متصل است که به لحاظ قلمرو محدود به یک سازمان یا نهاد است ولی همچنین شامل اتصالات محدود به شبکه‌های متعلق به یک یا چند سازمان یا نهاد دیگر است که معمولاً، ولی نه همیشه، قابل اعتماد هستند. برای نمونه مشتریان یک شرکت ممکن است که دسترسی به بخش هایی از شبکه داخلی آن شرکت داشته باشند که بدین ترتیب یک شبکه خارجی درست می‌شود، چراکه از نقطه نظر امنیتی این مشتریان برای شبکه قابل اعتماد به نظر نمی‌رسند. همچنین از نظر فنی می‌توان یک شبکه خارجی را در گروه شبکه‌های دانشگاهی، کلان شهری، گسترده یا دیگر انواع شبکه (هر چیزی غیر از شبکه محلی) به حساب آورد، چراکه از نظر تعریف یک شبکه خارجی نمی‌تواند فقط از یک شبکه محلی تشکیل شده باشد، چون بایستی دست کم یک اتصال به خارج از شبکه داشته باشد.

۳- شبکه اینترنت (Internet)

شبکه ویژه‌ای از شبکه‌ها که حاصل اتصالات داخلی شبکه‌های دولتی، دانشگاهی، عمومی و خصوصی در سرتاسر دنیا است. این شبکه بر اساس شبکه اولیه‌ای کار می‌کند که آرپانت (ARPANET) نام داشت و به وسیله موسسه آرپا (ARPA) که وابسته به وزارت دفاع ایالات متحده آمریکا است ایجاد شد. همچنین منزلگاهی برای وب جهان گستر (WWW) است. در لاتین واژه Internet برای نامیدن آن بکار می‌رود که برای اشتباه نشدن با معنی عام واژه شبکه متصل حرف اول را بزرگ می‌نویسند.

۱-۶-۵- بر اساس لایه شبکه

ممکن است شبکه‌های رایانه‌ای مطابق مدلهای مرجع پایه‌ای که در صنعت به عنوان استاندارد شناخته می‌شوند مانند مدل مرجع ۷ لایه OSI و مدل ۴ لایه TCP/IP، بر اساس نوع لایه شبکه‌ای که در آن عمل می‌کنند طبقه بندی شوند. این دو مورد در فصلی جداگانه بررسی می‌شوند.

۱-۶-۶- بر اساس معماری کاربری

ممکن است شبکه‌های رایانه‌ای بر اساس معماری کاربری که بین اعضای شبکه وجود دارد طبقه بندی شود، برای نمونه معماری‌های Active Networking، مشتری-خدمت گذار (Client-Server) و همتا به همتا Peer-to-Peer (گروه کاری).

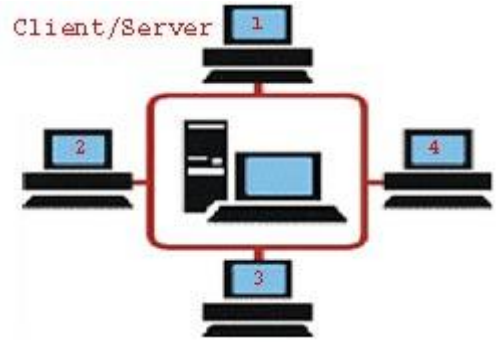
۱. **شبکه‌های نقطه به نقطه (Peer to Peer)** که نام دیگر آن‌ها WORK GROUP می‌باشد.

در مدل Peer-to-Peer هر کاربری می‌تواند فایلها را با دیگر کاربران بدون نیاز به یک سرور مرکزی و خاص، به اشتراک بگذارد.



۲. **شبکه‌های مبتنی بر سرور (Server Based)** که به آن‌ها Client / Server نیز می‌گویند.

در شبکه Client/Server یک یا چند کامپیوتر به عنوان سرویس دهنده (سرور) برای اشتراک فایلها، منابع و برنامه‌ها وجود دارد.



۱-۶-۷- بر اساس همبندی (توپولوژی)

ممکن است شبکه‌های رایانه‌ای بر اساس نوع همبندی شبکه طبقه بندی شوند مانند: شبکه خطی (Bus)، شبکه ستاره (Star)، شبکه حلقه‌ای (Ring)، شبکه توری (Mesh)، شبکه ستاره-باس (Star-Bus)، شبکه درختی (Tree) یا شبکه سلسله مراتبی (Hierarchical) و غیره.

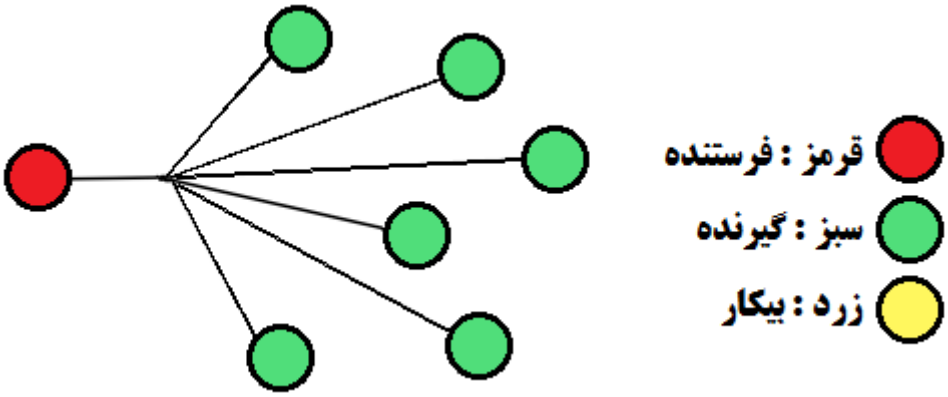
همبندی شبکه را می‌توان بر اساس نظم هندسی ترتیب داد. همبندی‌های شبکه طرح‌های منطقی شبکه هستند. واژه منطقی در اینجا بسیار پرمعنی است. این واژه به این معنی است که همبندی شبکه به طرح فیزیکی شبکه بستگی ندارد. مهم نیست که رایانه‌ها در یک شبکه به صورت خطی پشت سر هم قرار گرفته باشند، ولی زمانیکه از طریق یک هاب به یکدیگر متصل شده باشند تشکیل همبندی ستاره می‌کنند نه باس. و این عامل مهمی است که شبکه‌ها در آن فرق می‌کنند، جنبه ظاهری و جنبه عملکردی. توپولوژی‌ها در فصلی جداگانه بررسی می‌شوند.

۱-۶-۸- بر اساس مسیر دهی بسته ها

۱. Broadcast Network

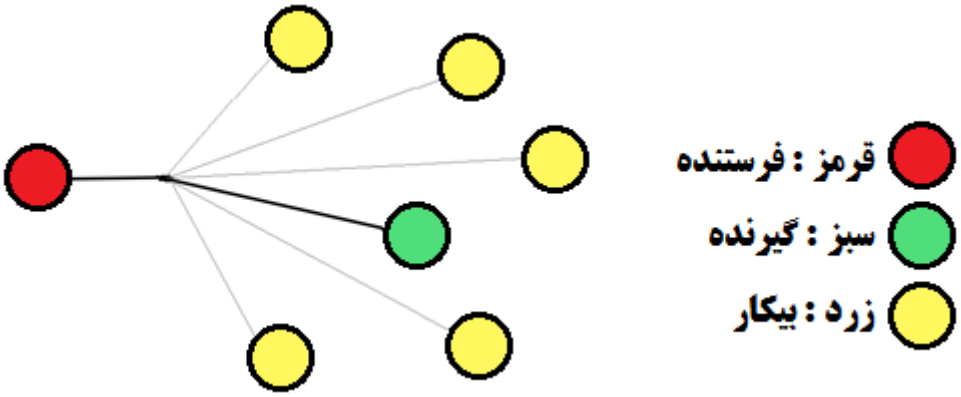
در اتصال Broadcast Network هر کامپیوتر توسط Node کابل شبکه خود همواره باید یا بطور مستقیم به کامپیوتر دیگر متصل بوده و یا توسط یک رسانه Media همانندHub به کامپیوتر دیگر متصل شود. در این روش کامپیوتر پیغام دهنده Packet اطلاعات خود را در کل رسانه رها می‌نماید با این توضیح که نام و آدرس کامپیوتر پیغام گیرنده را هم به همراه آن

ارسال می‌کند. این Packet به همه کامپیوترها رسیده و تنها توسط کامپیوتری دریافت و خوانده می‌شود که آدرس و نام کامپیوتری که همراه با Packet ارسال شده است – با آن همخوانی داشته باشد. در این ساختار علاوه بر اینکه ترافیک شبکه زیاد بوده و باعث کم شدن سرعت کارکرد شبکه می‌شود امنیت آن نیز از سطح مطلوبی برخوردار نیست. زیرا Packet اطلاعات که ممکن است محرمانه هم باشد در سطح شبکه پخش شده و به همه کامپیوترها می‌رسد. این ساختار از پیچیدگی کمتری برخوردار بوده و هزینه تهیه سخت‌افزارهای لازم برای راه اندازی آن کم است.



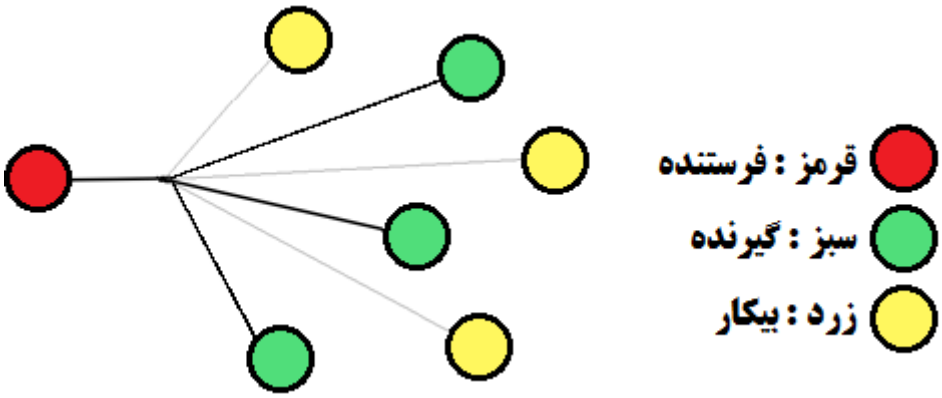
۲. Point to Point Network (Unicast)

در اتصال Point to Point Network دریافت و ارسال Packetها در شبکه توسط ابزاری هوشمند کنترل می‌شود بگونه‌ای که Packet اطلاعاتی که برای یک کامپیوتر مشخص ارسال می‌گردد تنها به سمت همان کامپیوتر ارسال شده و دیگر کامپیوترها امکان دسترسی به آن را ندارند از طرف دیگر به دلیل اینکه این بسته اطلاعاتی در کل شبکه منتشر نمی‌شود. ترافیک شبکه بطور قابل ملاحظه‌ای پایین آمده و امنیت درسطح شبکه بالا می‌رود. اینگونه شبکه‌ها به دلیل داشتن ابزاری چون سوئیچ‌های هوشمند گران‌تر از نوع قبل می‌باشد.



۳. Multicast Network

در این روش، کامپیوتر ارسال کننده، بسته‌ها را نه به تمامی کامپیوترهای موجود ارسال می‌کند و نه به یک تک کامپیوتر خاص؛ بلکه در این روش، کامپیوتر ارسال کننده، از بین کامپیوترهای موجود، تعدادی را انتخاب کرده و بسته‌ها را به سمت آن‌ها ارسال می‌کند. مثلاً بسته‌ها را به سمت کامپیوترهای با شماره زوج یا کامپیوترهای با حافظه RAM بیشتر از 2 GB می‌فرستد. در این روش، فرآیند ارسال به کمک الگویی خاص (Pattern) انجام می‌گیرد.



۱-۷- اجزای اصلی سخت‌افزاری

همه شبکه‌ها از اجزای سخت‌افزاری پایه‌ای تشکیل شده‌اند تا گره‌های شبکه را به یکدیگر متصل کنند، مانند کارت‌های شبکه، تکرارگرها، هاب‌ها، پلها، راهگزین‌ها (Switch) و مسیریاب‌ها. علاوه بر این، روشهایی برای اتصال این اجزای سخت‌افزاری لازم است که معمولاً از کابل‌های الکتریکی استفاده می‌شود. (از همه رایجتر کابل رده ۵ (کابل Cat5) است)، و کمتر از آن‌ها، ارتباطات مایکروویو (مانند IEEE 802.11) و (کابل فیبر نوری Optical Fiber Cable) بکار می‌روند.

۱-۷-۱- کارت شبکه (NIC)

کارت شبکه، آداپتور شبکه یا کارت واسط شبکه (Network Interface Card) قطعه‌ای از سخت‌افزار رایانه است و طراحی شده تا این امکان را به رایانه‌ها بدهد که بتوانند بر روی یک شبکه رایانه‌ای با یکدیگر ارتباط برقرار کنند. این قطعه دسترسی فیزیکی به یک رسانه شبکه را تامین می‌کند و با استفاده از آدرس‌های MAC، سیستمی سطح پایین جهت آدرس‌دهی فراهم می‌کند. این شرایط به کاربران اجازه می‌دهد تا به وسیله کابل یا به صورت بی‌سیم به یکدیگر متصل شوند.



۱-۷-۲- تکرارگر (Repeater)

تکرارگر تجهیزی الکترونیکی است که سیگنالی را دریافت کرده و آن را با سطح دامنه بالاتر، انرژی بیشتر و یا به سمت دیگر یک مانع ارسال می‌کند. بدین ترتیب می‌توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. از آنجا که تکرارگرها با سیگنال‌های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده‌ای که انتقال می‌دهند تلاشی نمی‌کنند، این تجهیزات در **لایه فیزیکی** یعنی اولین لایه از مدل مرجع OSI عمل می‌کنند.

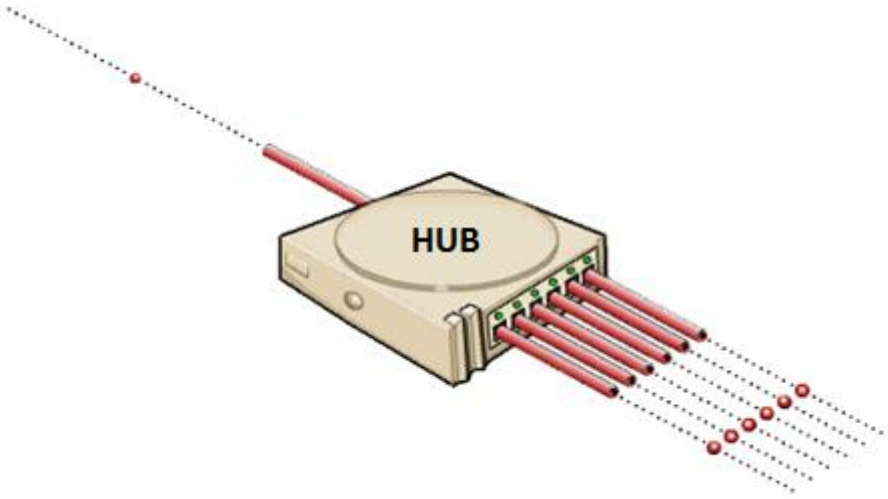




۱-۷-۳- هاب (جعبه تقسیم)

هاب قطعه‌ای سخت‌افزاری است که امکان اتصال قسمت‌های یک شبکه را با هدایت ترافیک در سراسر شبکه فراهم می‌کند. هاب‌ها در **لایه فیزیکی** از مدل مرجع OSI عمل می‌کنند. عملکرد هاب بسیار ابتدایی است، به این ترتیب که داده رسیده از یک گره را برای تمامی گره‌های شبکه کپی می‌کند. هاب‌ها مانند تکرارگرها، عملیات تقویت سیگنال را نیز انجام می‌دهند. هاب‌ها عموماً برای متصل کردن بخش‌های یک شبکه محلی بکار می‌روند. هر هاب چندین درگاه (پورت) دارد. زمانی که بسته‌ای از یک درگاه می‌رسد، به دیگر درگاه‌ها کپی می‌شود، بنابراین همه قسمت‌های شبکه محلی می‌توانند بسته‌ها را ببینند.

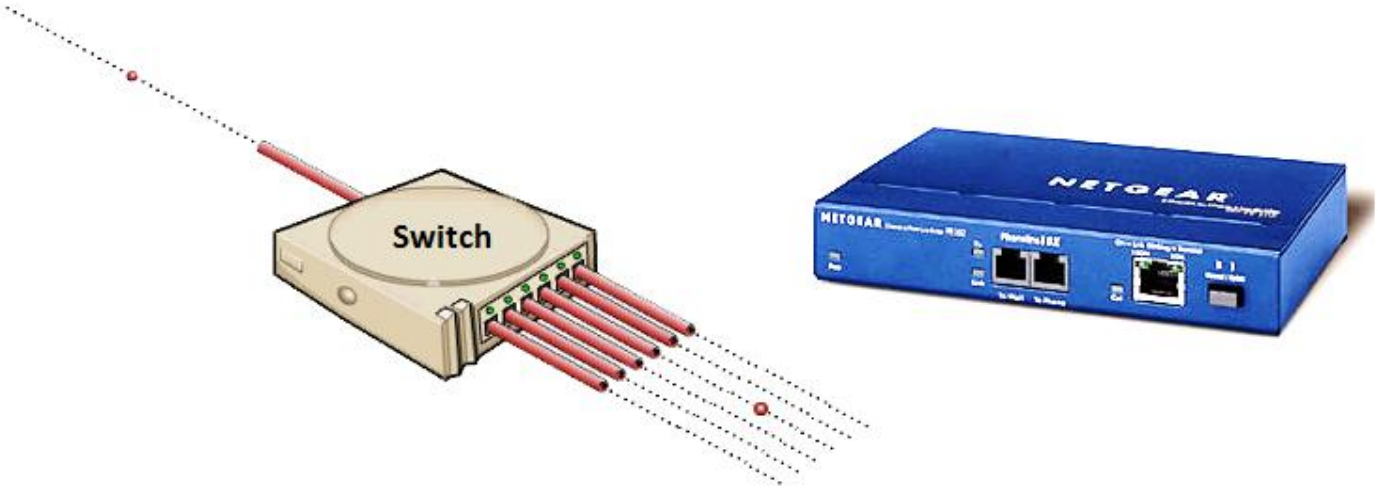




۱-۷-۴- راهگزین (Switch)

راهگزین که در پارسی بیشتر واژه سوئیچ برای آن بکار برده می‌شود، وسیله‌ای است که قسمت‌های شبکه را به یکدیگر متصل می‌کند. راهگزین‌های معمولی شبکه تقریباً ظاهری شبیه به هاب دارند، ولی یک راهگزین در مقایسه با هاب از هوشمندی بیشتری (و همچنین قیمت بیشتری) برخوردار است. راهگزین‌های شبکه این توانمندی را دارند که محتویات بسته‌های داده‌ای که دریافت می‌کنند را بررسی کرده، دستگاه فرستنده و گیرنده بسته را شناسایی کنند، و سپس آن بسته را به شکلی مناسب ارسال نمایند. با ارسال هر پیام فقط به دستگاه متصلی که پیام به هدف آن ارسال شده، راهگزین پهنای باند شبکه را به شکل بهینه تری استفاده می‌کند و عموماً عملکرد بهتری نسبت به یک هاب دارد.

از نظر فنی می‌توان گفت که راهگزین در لایه پیوند داده از مدل مرجع OSI عمل کنند. ولی بعضی انواع راهگزین قادرند تا در لایه‌های بالاتر نیز به بررسی محتویات بسته بپردازند و از اطلاعات بدست آمده برای تعیین مسیر مناسب ارسال بسته استفاده کنند. به این راه گزین‌ها به اصطلاح راهگزین‌های چندلایه (Multilayer Switch) می‌گویند.



۱-۷-۵- پل (Bridge)

یک پل دو زیر شبکه (سگمنت) را در لایه پیوند داده از مدل مرجع OSI به هم متصل می‌کند. پل‌ها شبیه به تکرارگرها و هاب‌های شبکه‌اند که برای اتصال قسمت‌های شبکه در لایه فیزیکی عمل می‌کنند، با این حال پل با استفاده از مفهوم پل زدن کار می‌کند، یعنی به جای آنکه ترافیک هر شبکه بدون نظارت به دیگر درگاه‌ها کپی شود، آنرا مدیریت می‌کند. بسته هایی که از یک طرف پل وارد می‌شوند تنها در صورتی به طرف دیگر انتشار می‌یابند که آدرس مقصد آن‌ها مربوط به سیستم هایی باشد که در طرف دیگر پل قرار دارند. پل مانع انتشار پیغام‌های همگانی در قطعه‌های کابل وصل شده به آن نمی‌شود. **در اصل می‌توان گفت که وظیفه پل، اتصال سگمنت‌های مختلف شبکه می‌باشد. منظور از سگمنت می‌تواند شبکه‌های با معماری مختلف یا شبکه‌های با آدرس مختلف باشد.**

البته گاهی از پل به عنوان دروازه (Gateway) یاد می‌کنند.Gateway، کامپیوتری است که بسته‌های خارج شده از هر کامپیوتر ابتدا به سمت آن می‌رود. البته پل برای اتصال شبکه‌های نا همگون نیز به کار می‌رود.

پل‌ها به سه دسته تقسیم می‌شوند:

پل‌های محلی: مستقیماً به شبکه‌های محلی متصل می‌شود.

پل‌های دوردست: از آن می‌توان برای ساختن شبکه‌های گسترده جهت ایجاد ارتباط بین شبکه‌های محلی استفاده کرد. پل‌های دور دست در شرایطی که سرعت اتصال از شبکه‌های انتهایی کمتر است با مسیریابها جایگزین می‌شوند.

پل‌های بی‌سیم: برای اتصال شبکه‌های محلی به شبکه‌های محلی بی‌سیم یا شبکه‌های محلی بی‌سیم به هم یا ایستگاه‌های دوردست به شبکه‌های محلی استفاده می‌شوند.

۱-۷-۶- مسیریاب (Router)

مسیریاب‌ها تجهیزات شبکه‌ای هستند که بسته‌های داده را با استفاده از سرآیندها (Header) و جدول ارسال تعیین مسیر کرده، و ارسال می‌کنند. مسیریاب‌ها در لایه شبکه از مدل مرجع OSI عمل می‌کنند. همچنین مسیریاب‌ها اتصال بین بسترهای

فیزیکی متفاوت را امکان پذیر می‌کنند. این کار با چک کردن سرآیند یک بسته داده انجام می‌شود. مسیر یاب‌ها قادر به انتقال داده‌ها به صورت Broadcast نیستند.

مسیریاب‌ها از قراردادهای مسیر یابی مانند OSPF استفاده می‌کنند تا با یکدیگر گفتگو کرده و بهترین مسیر بین هر دو ایستگاه را پیکربندی کنند. هر مسیریاب دسته کم به دو شبکه، معمولاً شبکه‌های محلی، شبکه‌های گسترده و یا یک شبکه محلی و یک سرویس دهنده اینترنت متصل است. بعضی انواع مودم‌های DSL و کابلی جهت مصارف خانگی درون خود از وجود یک مسیریاب نیز بهره می‌برند.



۱-۸- سیستم‌های شبیه به شبکه

گاهی اوقات می‌توان کامپیوترها را به شکلی بکار برد که دقیقا با یک شبکه سر و کار نداریم اما می‌توان آن‌ها را شبکه نیز به حساب آورد. به همین دلیل نام آن‌ها را سیستم‌های شبیه شبکه می‌نامیم و در زیر آن‌ها را توضیح می‌دهیم. اما قبل از آن باید با مفهوم کامپیوتر Standalone آشنا شوید. به طور کلی به کامپیوترهای که قادر باشیم پشت آن‌ها قرار گیریم و با آن‌ها کار انجام دهیم خواه به شبکه متصل نباشد یا امکان آن را نداشته باشد یک کامپیوتر Standalone گوییم.

سیستم‌های شبیه شبکه، بطور کلی سه مورد می‌باشند:

۱-۸-۱- *کامپیوترهای Mainframe*

این کامپیوترها دارای چندین پردازنده و حافظه‌های بزرگ می‌باشند و ترمینال‌ها که فقط دارای مانیتور و صفحه کلید می‌باشند به آن متصل می‌شوند و از آن استفاده می‌کنند. پس به نوعی می‌توان آن‌ها را نوعی شبکه نامید اما نه بطور کامل.





۱-۸-۲- سیستم‌های توزیع شده

این سیستم‌های شامل چندین کامپیوتر جداگانه می‌باشند که بر روی همه آن‌ها یک سیستم عامل مخصوص مانند ماخ (Mach) نصب می‌شود و این سیستم عامل است که کلیه پردازش‌ها را مدیریت می‌کنند و تصمیم می‌گیرد که مثلاً این برنامه روی کدام سیستم‌ها انجام شود و یا مثلاً این داده روی کدام سیستم‌ها ذخیره شود و در این موارد کاربر نمی‌تواند هیچ کاری انجام دهد. این کامپیوترها بیشتر برای انجام پردازش‌های بسیار سنگین و به صورت موازی بکار می‌روند.

۱-۸-۳- کامپیوتر هایی که به یکدیگر Link می‌شوند

یکی از راه‌هایی که می‌توان کامپیوترها را به یکدیگر متصل کرد از طریق پورت‌های پشت آن‌ها می‌باشد. اگر دو کامپیوتر را بتوان از طریق پورت‌های پشت آن‌ها به یکدیگر متصل کرد در اصطلاح آن‌ها را لینک کرده‌ایم. در سیستم عامل ویندوز نیز می‌توانید دو کامپیوتر را بدین روش به یکدیگر متصل کنید. برای اینکار در موقع نصب ویندوز باید نرم‌افزار آن را نصب کنید تا بتوانید دو کامپیوتر را در قالب Host و Guest استفاده نمایید

۱-۹- مراحل راه اندازی یک شبکه

برای راه اندازی هر نوع شبکه‌ای مراحل زیر را باید طی کرد.

۱. طراحی (Design)
۲. تنظیمات (Roll Out)
۳. پیکربندی (Configuration)
۴. مدیریت (Management)

۱-۹-۱- طراحی شبکه (Design)

فاز طراحی معمولاً یک الی سه روز طول میکشد که بستگی به بزرگی شبکه و کار آن دارد.

نکاتی که در فاز طراحی باید به آن‌ها توجه کرد:

۱. شبکه Peer-to-Peer است یا Client/Server
۲. انتخاب نرم‌افزار شبکه
۳. انتخاب زبان شبکه
۴. تهیه لیست سخت‌افزارهای موردنیاز
۵. تعیین میزان سطح امنیت اطلاعات
۶. یادگیری راه حل‌های نرم‌افزاری و سخت‌افزاری برای رفع مشکلات مدیریتی روزمره

۱-۹-۲- تنظیمات شبکه (Roll Out)

برای تنظیم کردن شبکه مراحل زیر را باید انجام داد:

۱. آزمایش کابل ها

۲. نصب یک یا چند سِرور، اگر شبکه از نوع مدل Client/Server باشد.
۳. نصب سخت‌افزار کامپیوترهای دیگر (گروه کاری)
۴. اتصال کارت‌های شبکه به کابل‌ها (NIC-کارت شبکه باعث اتصال کامپیوترها به شبکه می‌شود.)
۵. نصب یک یا چند Hub (اگر از کابل Twisted Pair استفاده می‌شود. در این نوع شبکه‌ها از توپولوژی Star استفاده می‌شود.)
۶. نصب چاپگر ها
۷. نصب برنامه سرویس دهنده (سیستم عامل شبکه یا NOS) اگر مدل شبکه Client/Server است
۸. نصب برنامه روی کامپیوترهای دیگر
۹. نصب برنامه‌های کاربردی

۱-۹-۳- پیکربندی شبکه (Configuration)

پیکربندی شبکه به معنای سفارشی کردن آن برای کاربر است.

۱. ایجاد حساب‌های دسترسی به شبکه برای کاربران (نام کاربری- کلمه عبور- گروه کاری)
۲. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن فایلها و داده‌های کاربران
۳. تخصیص فضایی از هارد دیسک برای به اشتراک گذاشتن برنامه‌ها توسط کاربران
۴. تنظیم نوبت چاپ (نرم‌افزاری که اجازه میدهد کاربران از چاپگرهای شبکه استفاده کنند)
۵. نصب سیستم پشتیبانی شبکه برروی ایستگاه‌های کاری کاربران

۱-۹-۴- مدیریت و اداره شبکه (Management)

۱. نقشه برداری از شبکه به منظور مدیریت و اشکال زدایی آسانتر
۲. نصب سطوح امنیتی مناسب به منظور جلوگیری از خسارات عمدی و سهوی
۳. بالا بردن سرعت شبکه از طریق تنظیم LAN
۴. ایجاد استانداردهای شرکت برای اضافه کردن سخت‌افزار و نرم‌افزار. با این کار می‌توان از بروز مشکلات در آینده جلوگیری کرد.

۱-۱۰- آشنایی با VoIP

۱-۱۰-۱- مقدمه

ارتباطات یکی از نیازهای حیاتی بشریت است و انسان همواره به دنبال ابداع فن آورهائی بوده است که بتواند با استفاده از آنان با سایر همنوعان خود ارتباط برقرار نماید. در گذشته‌ای نه چندان دور که انسان استفاده از اینترنت را تجربه نکرده بود، ارتباطات محاوره‌ای صرفاً از طریق تلفن و به کمک خطوط PSTN (برگرفته از Public Switched Telephone Network)، انجام می‌گردید. در سیستم فوق، سیگنال‌های صوتی آنالوگ با استفاده از کابل‌های مسی حمل و مبادله داده

خصوصا" در مسافت‌های طولانی گرانقیمت و ارتباطات دوسویه ویدیوئی رویائی بیش نبود (در آن زمان صرفا" از تلویزیون استفاده می‌گردید که به عنوان یک رسانه دوسویه محسوب نمی‌گردد).در سالیان اخیر ما شاهد اتفاقات جالبی بوده ایم که هر یک به سهم خود تاثیری غیرقابل انکار در حیات بشریت داشته‌اند. ابداع کامپیوترهای شخصی، فن آوری‌های جدید ارتباطی نظیر تلفن‌های سلولی و نهایتا" اینترنت نمونه هائی در این زمینه می‌باشند که باعث شده است انسان بتواند با استفاده از سرویس‌های جدیدی نظیر نامه الکترونیکی، چت و مواردی دیگر با سایر افراد ارتباط برقرار نماید.

در حال حاضر می‌توانیم نظاره گر یک انقلاب واقعی در عرصه ارتباطات باشیم. هر شخص با استفاده از کامپیوتر و اینترنت می‌تواند با سایر افراد مورد علاقه خود ارتباط برقرار نموده، داده ئی را مبادله و یا از طریق امکانات نرم‌افزاری موجود با یکدیگر گفتگو نمایند. ما نمی‌دانیم دقیقا" در آینده چه اتفاقی خواهد افتاد ولی این را می‌دانیم که کامپیوتر دارای نقشی محوری و اساسی در این رابطه خواهد بود. اینترنت با سرعت بالا در همه جا استفاده خواهد شد و مردم با یکدیگر به صورت صوتی و تصویری ارتباط برقرار خواهند نمود.به هرحال، رشد بی سابقه اینترنت در سالیان اخیر این نوید را می‌دهد که بتوان از زیرساخت موجود به عنوان یک گزینه مطلوب به منظور ارتباطات استفاده نمود.



۱-۱۰-۲- VoIP چیست؟

VoIP (برگرفته از Voice over Internet Protocol) که با نام IP تلفنی نیز از آن یاد می‌شود، امکان استفاده از اینترنت برای مکالمات تلفنی را فراهم می‌نماید. در مقابل استفاده از خطوط تلفن سنتی، VoIP از فن آوری دیجیتال استفاده می‌نماید و نیازمند یک اتصال broadband نظیر DSL است. هم اینک شرکت‌های متعددی سرویس فوق را در اختیار علاقه مندان قرار می‌دهند.

متداولترین کاربرد VoIP برای موارد شخصی و استفاده در منازل، سرویس‌های تلفنی مبتنی بر اینترنت است که با محوریت یک سوئیچ تلفن انجام می‌شود. با استفاده از فن آوری فوق، استفاده کنندگان می‌توانند همچنان دارای یک شماره

تلفن باشند. در چنین مواردی ممکن است از یک آداپتور نیز استفاده گردد. آداپتور فوق این امکان را دراختیار استفاده کننده قرارخواهد داد تا بتوانند از یک تلفن معمولی نیز استفاده نمایند. در زمان استفاده از سرویس فوق، مخاطب شما متوجه این موضوع نخواهد شد که شما از فن آوری VoIP استفاده می‌نمائید و قادر به تشخیص دقیق تفاوت سرویس فوق نسبت به یک تلفن سنتی نمی‌باشد.

۱-۱۰-۳- VoIP چگونه کار می کند؟

در گذشته‌ای نه چندان دور، پیشگامان عرصه‌های علمی به این نتیجه رسیدند که می‌توان یک سیگنال را به صورت دیجیتال و در یک مسافت طولانی ارسال نمود. بدین منظور می‌بایست قبل از ارسال سیگنال، آن را با استفاده از یک مبدل آنالوگ به دیجیتال(ADC)، دیجیتال و سپس ارسال و در نقطه پایانی انتقال،با استفاده از یک مبدل دیجیتال به آنالوگ (DAC)مجدداً آن را به آنالوگ تبدیل نمود.فن آوری VoIP نظیر آنچه اشاره گردید کار می‌کند. در ابتدا، صدای دیجیتال شده در بسته‌های اطلاعاتی قرار می‌گیرد و پس از ارسال در مقصد مجدداً به صوت تبدیل می‌گردد. با ذخیره اطلاعات به فرمت دیجیتال می‌توان بر روی آنان کنترل بهتری را اعمال نمود. مثلاً می‌توان آنان را فشرده، مسیر آنان را تعیین و یا آنان را به یک فرمت جدید دیگر تبدیل نمود.

شبکه‌های مبتنی بر پروتکل TCP/IP از بسته‌های اطلاعاتی IP تشکیل می‌گردند که شامل یک هدر (برای کنترل ارتباطات) و یک paylaod به منظور مبادله داده می‌باشند. فن آوری VoIP از بسته‌های اطلاعاتی IP به منظور حرکت در شبکه و رسیدن به مقصد نهائی استفاده می‌نماید. Voice (source) - > ADC - - - Internet - - - DAC - > Voice (dest)

۱-۱۰-٤- مزایای استفاده از VoIP نسبت به PSTN

در زمان استفاده از خطوط PSTN، کاربران عملاً هزینه زمان استفاده شده توسط شرکتی که مدیریت خط PSTN را برعهده دارد، پرداخت می‌نمایند و هر اندازه که بیشتر با تلفن صحبت نمایند هزینه بیشتری را نیز می‌بایست پرداخت نمایند. علاوه بر این، نمی‌توان بطور همزمان با بیش از یک شخص گفتگو نمود.در فن آوری VoIP می‌توان هر زمان و با هر شخص گفتگو نمود. کافی است که در آن مقطع زمانی سایر افرادی که شما می‌خواهید با آنان گفتگو نمائید نیز به اینترنت متصل شده باشند. مکالمه برقرار شده تا زمان دلخواه (مستقل از هزینه‌های مربوطه) می‌تواند ادامه یابد. علاوه بر این، می‌توان در یک زمان با چندین نفر گفتگو نمود. در زمان گفتگو با سایر افراد و بطور همزمان می‌توان با آنان داده ئی (نظیر تصاویر، نمودارها و تصاویر ویدیوئی) را نیز مبادله نمود.

چرا تاکنون از این فن آوری در ابعاد گسترده‌ای استفاده نشده است؟

در این بخش لازم است به برخی مسائل حاصل از ائتلاف بین معماری VoIP و اینترنت اشاره گردد. مبادله داده صوتی می‌بایست به صورت بلادرنگ و بدون توقف انجام گردد و این موضوع با معماری نامتجانس اینترنت که ممکن است از تعدادی روتر (ماشین هائی که مسیریابی بسته‌های اطلاعاتی را انجام می‌دهند) به منظور مسیریابی بسته‌های اطلاعاتی استفاده نماید، همخوانی نداشته و می‌تواند باعث بروز مسائل خاصی نظیر افزایش زمان RTT (برگرفته Round Trip Time) گردد.

بنابراین، می‌بایست با اعمال تغییرات لازم و بکارگیری فن آوری‌های دیگر، زمینه استفاده موثر از فن آوری VoIP را فراهم نمود.

۱-۱۰-۵- نحوه ایجاد یک اتصال VoIP

برای ایجاد یک ارتباط مبتنی بر VoIP، می‌بایست مراحل زیر را دنبال نمود (تمامی مراحل می‌بایست به صورت بلادرنگ انجام گردد).

• تبدیل سیگنال آنالوگ به دیجیتال: تبدیل سیگنال صوتی آنالوگ به سیگنال دیجیتال (مجموعه‌ای از صفر و یک) توسط یک مبدل آنالوگ به دیجیتال (ADC)

• فشرده سازی سیگنال دیجیتال: پس از تبدیل سیگنال صوتی به دیجیتال، بیت‌های موجود می‌بایست بر اساس یک فرمت مناسب فشرده تا آماده ارسال گردند. در این رابطه از پروتکل‌های متعددی استفاده می‌گردد. PCM و استاندارد ITU-T G.711 نمونه هائی در این زمینه می‌باشند. • استفاده از یک پروتکل بلادرنگ: در این مرحله، بسته‌های صوتی در بسته‌های اطلاعاتی و با استفاده از یک پروتکل بلادرنگ (عموماً RTP بر روی UDP) قرار می‌گیرند.

• استفاده از یک پروتکل سیگنالینگ: در این مرحله لازم است از یک پروتکل سیگنالینگ به منظور فراخوانی کاربر استفاده گردد. پروتکل ITU-T H323 نمونه‌ای دراین زمینه می‌باشد. • تبدیل سیگنال دیجیتال به آنالوگ: در سمت گیرنده، می‌بایست بسته‌های اطلاعاتی از یکدیگر مجزاء، داده‌ها استخراج و به سیگنال‌های صوتی آنالوگ تبدیل و در نهایت برای کارت صدا و یا تلفن ارسال گردند.

۱-۱۰-۶- چالش‌های امنیتی VoIP

با توجه به این که فن آوری VoIP در ارتباط با اتصال اینترنت است و از آن استفاده می‌نماید، مشکلات و مسائل امنیتی در ارتباط با کامپیوتر متصل شده به اینترنت می‌تواند سرویس فوق را نیز تحت تاثیر قرار دهد. فن آوری VoIP هنوز جوان است و بحث‌های مختلفی در خصوص ظرفیت ریسیک پذیری آن وجود دارد. مهاجمان ممکن است قادر به انجام فعالیت هائی نظیر قطع مکالمه تلفنی، استراق سمع، برنامه ریزی و هدایت حملات مبتنی بر مهندسی اجتماعی با بررسی Caller ID و در نهایت از کار انداختن سرویس فوق باشند. فعالیت هائی که مستلزم استفاده از حجم بالائی از منابع شبکه است، نظیر دریافت فایل‌های حجیم، بازی‌های online، استفاده از محتویات چندرسآن‌های (صوت و تصویر)، می‌تواند سرویس VoIP را تحت تاثیر قرار دهد.

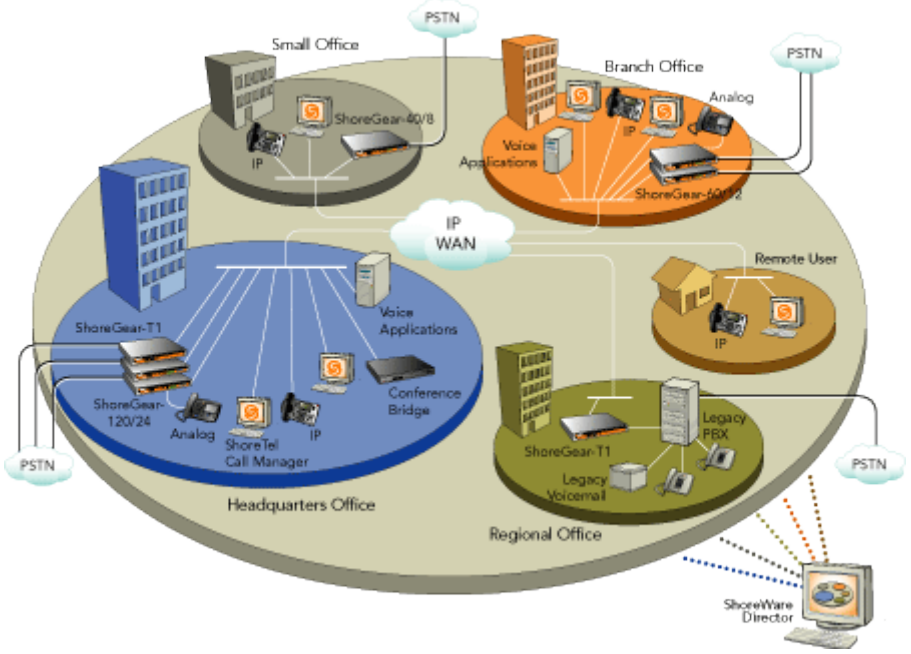
در زمان استفاده از فن آوری VoIP ممکن با مسائل دیگری که در ارتباط با روتینگ تلفن بر روی اتصال broadband اینترنت است نیز برخورد نمائیم. برخلاف خطوط تلفن سنتی، که امکان استفاده از آنان حتی در صوت قطع برق وجود دارد، سرویس VoIP در چنین مواردی غیرقابل استفاده می‌گردد و ممکن است مسائل خاصی را برای سیستم‌های امنیتی منازل و یا دستیابی به شماره تلفن‌های اضطراری به دنبال داشته باشد.

۱-۱۰-۷- نحوه حفاظت

در زمان استفاده از سرویس فوق لازم است به موارد زیر توجه گردد: • بهنگام نگه داشتن نرم‌افزارها: در صورتی که تولید کنندگان نرم‌افزار برای سیستم عامل دستگاه مورد نظر نسخه‌های بهنگام شده‌ای را ارائه داده‌اند، می‌بایست در اولین فرصت نسبت به نصب آنان اقدام گردد. نسخه‌های بهنگام شده ممکن است فرآیند بهنگام سازی را در سطح Firmware انجام دهند. با بهنگام سازی نرم‌افزارهای موجود، پیشگیری لازم در خصوص برخی حملات برنامه ریزی شده با هدف بهره گیری از نقاط آسیب پذیر انجام خواهد شد.

• استفاده و بهنگام سازی نرم‌افزارهای آنتی ویروس: برنامه‌های ضد ویروس قادر به تشخیص و حفاظت کامپیوتر شما در مقابل ویروس‌های شناخته شده می‌باشند. با توجه به این واقعیت که مهاجمان به صورت مستمر اقدام به نوشتن ویروس‌های جدید می‌نمایند، لازم است که این نوع نرم‌افزارها همواره بهنگام باشند. • استفاده از گزینه‌ها و تنظیمات امنیتی: برخی از ارائه دهندگان سرویس VoIP، امکان رمزنگاری اطلاعات را نیز به عنوان یک سرویس دیگر در اختیار مشتریان خود قرار می‌دهند. در صورت وجود نگرانی در خصوص تعرض به حریم خصوصی خود، می‌توان از این ویژگی و سایر گزینه‌های موجود در این رابطه استفاده نمود.

• نصب و یا فعال نمودن یک فایروال: فایروال‌ها با بررسی بسته‌های اطلاعاتی می‌توانند یک سطح حفاظتی مناسب در خصوص فیلتر نمودن برخی کدهای مخرب جهت ورود به سیستم شما را انجام دهند. برخی از سیستم‌های عامل به همراه یک فایروال ارائه می‌گردند. در چنین مواردی لازم است از فعال بودن آنان اطمینان حاصل نمود. • بررسی تنظیمات امنیتی: هم کامپیوتر شما و هم تجهیزات و نرم‌افزارهای ارائه شده جهت استفاده از سرویس VoIP، امکانات و گزینه‌های متفاوتی را در اختیار شما قرار می‌دهند. فعال نمودن برخی گزینه‌ها ممکن است ضریب آسیب پذیری شما را در مقابل حملات افزایش دهد. بنابراین لازم است گزینه‌های غیرضروری را غیرفعال نمود. پیشنهاد می‌گردد تنظیمات امنیتی به دقت بررسی گردد و صرفا" گزینه هائی انتخاب شود که ضمن تامین اهداف عملیاتی، باعث افزایش ضریب آسیب پذیری شما نگردد.



فصل ۲

آدرس IP

۲-۱- آدرس IP چیست؟

یکی از سوالاتی که معمولاً پیش می‌آید این است که "آدرس IP چیست؟" آدرس IP، شماره شناسایی هر کامپیوتر متصل به شبکه است. بنابر این می‌توان گفت که IP، شماره شناسایی هر کاربر شبکه است.

نشانی پروتکل اینترنت (Internet Protocol Address) یا به اختصار آدرس IP (IP Address) نشانی عددی است که به هریک از دستگاه‌ها و رایانه‌های متصل به شبکه‌ی رایانه‌ای که بر مبنای مدل مرجع TCP/IP (از جمله اینترنت) کار می‌کند، اختصاص داده می‌شوند. پیام هایی که دیگر رایانه‌ها برای این رایانه می‌فرستند با این نشانه‌ی عددی همراه است و مسیر یاب‌های شبکه آن را مانند نشانی گیرنده در نامه‌های پستی تعبیر می‌کنند، تا بالاخره پیام به شبکه رایانه مورد نظر برسد.

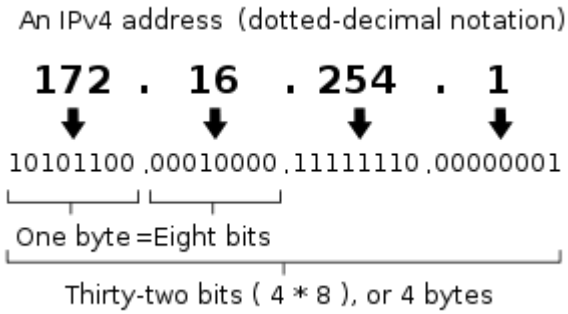
آدرس IP را می‌توان با شماره تلفن‌های افراد در شبکه تلفن مقایسه کرد. البته تفاوت‌های زیادی بین آدرس IP و شماره تلفن‌ها وجود دارد. ولی همانند آن، پیش شماره دارد و وقتی کامپیوتری متصل به شبکه اینترنت است، این آدرس انحصاری بوده و فقط در اختیار آن کامپیوتر قرار دارد. تفاوت مهم آن با شماره تلفن‌ها در این است که چنانکه به هر دلیلی (ارادی و یا غیر ارادی) کامپیوتری که این شماره (IP) به آن تخصیص داده شده، از شبکه اینترنت جدا شود (ارتباطش قطع گردد) این IP آزاد شده و ممکن است به کامپیوتر دیگری تخصیص داده شود.

البته در اینجا باز نکته مهمی وجود دارد: شماره IP برای کامپیوترهای سرور شبکه (کامپیوتر هایی که به شبکه سرویس می‌دهند و شبکه را تحت نظارت مستمر خود دارند) و نیز کامپیوتر هایی که به روشی غیر از روش شماره گیری تلفنی (Dial Up) به اینترنت وصل هستند (کامپیوترهای کلاینت) معمولاً عددی ثابت بوده و تغییر نمی‌کند. ولی همانطوری که اشاره شد برای دیگر کامپیوترها، عددی متغیر است و در هر بار اتصال به اینترنت ممکن است این شماره عوض شود. یعنی هر بار که شما با شرکت ISP خود تماس می‌گیرید و از طریق آن به شبکه اینترنت وصل می‌شوید، عددی جدید (از مجموعه شماره‌های IP آزاد در آن موقع) به کامپیوتر شما تخصیص داده می‌شود.

۲-۲- انواع IP

در حال حاضر، دو نسخه IP درحال استفاده می‌باشد: IP نسخه ۴ و IP نسخه ۶ که هر یک نشانی IP را به روش متفاوتی ارائه می‌نمایند.

۲-۳- آدرس IP نسخه ۴



آدرس IP نسخه ۴، یک عدد ۳۲ بیتی است که برای سادگی آن را به شکل چهار بخش عددی در مبنای ده می‌نویسند که با نقطه از هم جدا می‌شوند (مانند ۱۹۹.۲۱۱.۴۵.۵). این روش نشانی دهی را ده دهی نقطه دار می‌نامند. هر یک از چهار بخش را یک هشتایی (Octet) می‌گویند، زیرا طول آن ۸ بیت (یا ۱ بایت) است و می‌تواند عددی از ۰ تا ۲۵۵ باشد. پس ۲ به توان ۳۲ آدرس مختلف یا به عبارتی ۴.۲۹۴.۹۶۷.۲۹۶ آدرس متمایز داریم.

اصولاً هر نشانی IP که ۳۲ بیتی است، به دو بخش تقسیم می‌شود: **یک پیشوند** و **یک پسوند**. این دو سطح به منظور ایجاد یک روش مسیر یابی کارآمد طراحی شده است. پیشوند، آدرس شبکه‌ای که رایانه به آن متصل است را مشخص می‌کند (Network). در حالیکه پسوند، یک رایانه یکتا را روی شبکه مشخص می‌کند (Host)؛ یعنی به هر شبکه در اینترنت، یک مقدار یگانه که تحت عنوان شماره شبکه شناخته شده است، اختصاص دارد. شماره شبکه به عنوان یک پیشوند در نشانی هر رایانه‌ای که به شبکه وصل است ظاهر می‌شود. بعلاوه به هر رایانه روی یک شبکه، یک پسوند نشانی یکتا تخصیص یافته است.

هر نشانی کامل، شامل یک پیشوند و یک پسوند است و طوری تخصیص داده می‌شوند که یکتا باشند، بنابراین ویژگی اول تضمین می‌گردد. اگر دو رایانه به دو شبکه مختلف وصل شده باشند، نشانی هایشان پیشوندهای متفاوت خواهند داشت. اما اگر دو رایانه به یک شبکه وصل باشند، نشانی هایشان دارای پسوندهای متفاوت خواهد بود.

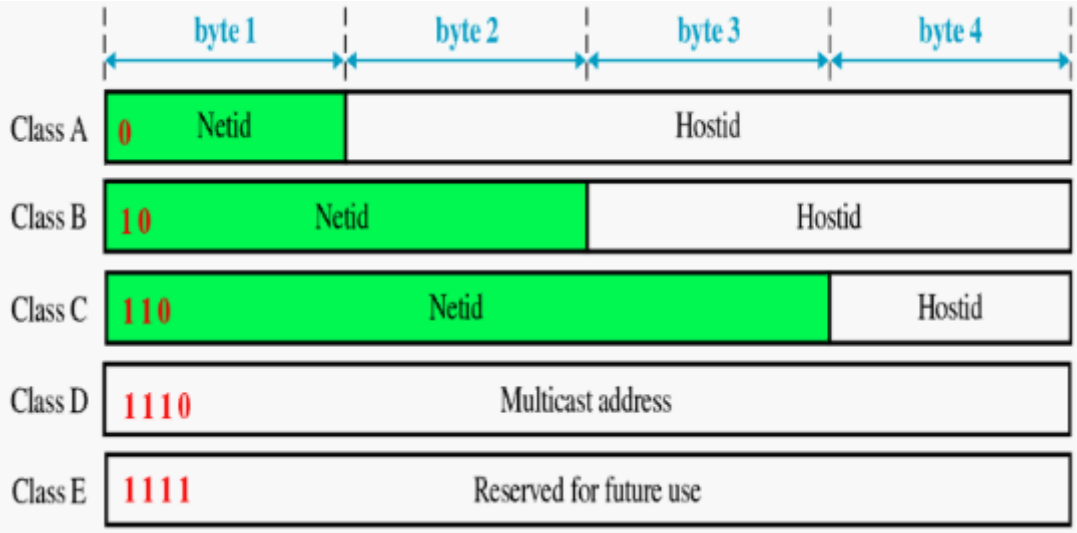
۲-۳-۱- کلاس‌های مختلف IP نسخه ۴

سه کلاسِ پایه‌ای مختلفِ نشانی دهی IP، برای شبکه‌های بزرگ، متوسط و کوچک (از نظر تعداد کامپیوتر در یک شبکه)، وجود دارد. کلاس A برای شبکه‌های بزرگ، کلاس B برای شبکه‌های متوسط و کلاس C برای شبکه‌های کوچک است. علاوه بر این سه کلاس، کلاس D برای پخش چندگانه ارسال اطلاعات به گروهی از رایانه‌ها، و کلاس E برای کارهای جستجو و تحقیقاتی وجود دارد. برای شرکت در پخش چندگانه IP، مجموعه‌ای از رایانه‌های میزبان باید بر سر استفاده از آدرس پخش چندگانه، به طور مشترک توافق داشته باشند. پس از تشکیل گروه پخش چندگانه یک کپی از هر بسته اطلاعاتی فرستاده شده به نشانی پخش چندگانه به هر رایانه میزبان در مجموعه تحویل می‌گیرد. نخستین ۴ بیت (از سمت چپ) آدرس

IP کلاس آن را مشخص می‌کند. همچنین اگر نمایش نقطه دار را در نظر بگیریم از روی مقدار ده دهی بایت اول کلاس آن تشخیص داده می‌شود:

کلاس	بیت آغازین	شروع	پایان	CIDR	Subnet Mask
Class A	۰	۰.۰.۰.۰	۱۲۷.۲۵۵.۲۵۵.۲۵۵	۸	۲۵۵.۰.۰.۰
Class B	۱۰	۱۲۸.۰.۰.۰	۱۹۱.۲۵۵.۲۵۵.۲۵۵	۱۶	۲۵۵.۲۵۵.۰.۰
Class C	۱۱۰	۱۹۲.۰.۰.۰	۲۲۳.۲۵۵.۲۵۵.۲۵۵	۲۴	۲۵۵.۲۵۵.۲۵۵.۰
Class D [multicast]	۱۱۱۰	۲۲۴.۰.۰.۰	۲۳۹.۲۵۵.۲۵۵.۲۵۵	۴	Not Defined
Class E [reserved]	۱۱۱۱	۲۴۰.۰.۰.۰	۲۵۵.۲۵۵.۲۵۵.۲۵۵	۴	Not Defined

شکل زیر تصویر بهتری از کلاس‌های آدرس IP به شما می‌دهد:

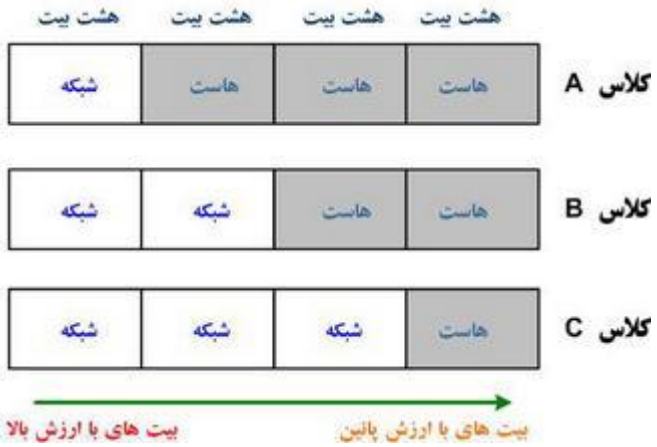


تصویر زیر نیز محدوده هر کلاس IP را نشان می‌دهد:



اصولا در سامانه IP دهی به مشترکان، IPها به صورت تعدادی که توانی از عدد ۲ باشد (۲، ۴، ۸، ۱۶، ۳۲، ۶۴ و ۱۲۸) دسته بندی می‌شوند. لازم به ذکر است که در هر دسته IP اختصاص داده شده به مشترک، IPهای اول و آخر بر اساس

استاندارد معمولاً غیر قابل استفاده است و از باقیمانده IPها می‌توان در شبکه محصور شده استفاده کرد. به عنوان مثال در یک کلاس هشت تایی، حداکثر شش نشانی IP قابل استفاده است. این بدین دلیل است که آدرس کامپیوتر در شبکه (پسوند) نمی‌تواند تماما ۱ یا تماما ۰ باشد. بنابراین تعداد ۲ تا از IPهای قابل تخصیص در هر شبکه کم می‌شود.



۰.۰.۰.۰: پیش فرض شبکه

کلاس A: این نوع کلاس بیشتر برای تخصیص IP در شبکه های بزرگ مورد استفاده قرار می گیرد. اکتت اول این کلاس‌ها از ۱ تا ۱۲۶ متفاوت می باشد. از باقی اکتت‌ها برای Host استفاده می شود. به این ترتیب ۱۲۶ شبکه، ۱۶۷۷۷۲۱۴ هاست و ۲۱۴۷۴۸۳.۶۴۸ آدرس در کلاس A تعریف می شود. حدود نیمی از ترکیب های موجود برای تمام آدرس های IP در این کلاس قرار می گیرند.

Loopback: آدرس ۱۲۷.۰.۰.۱ برای عملیاتی به نام Loopback استفاده می شود. Loopback زمانی انجام می شود که یکی از کامپیوترهای میزبان بسته ای را برای خودش می فرستد. کاربرد این متد در رفع مشکل و تست اتصالات شبکه در خود سیستم است.

کلاس B: معمولاً شبکه های متوسط از این نوع کلا س بهره می برند. آدرس هایی که اولین اکتت آ نها از ۱۲۸ تا ۱۹۱ تغییر می کند عضو این کلاس هستند. اکتت دوم این آدرس‌ها نیز برای تعیین Net و دو اکتت دیگر برای مشخص کردن آدرس، Host مورد استفاده قرار می گیرد. به این ترتیب ۱۶۳۴۸ شبکه با ۶۵۵۳۴ هاست و ۱۰۷۳۷۴۱۸۲۴ آدرس IP مختلف در این کلاس قابل تخصیص است.

کلاس C: شبکه های کوچک می توانند از این کلاس استفاده کنند. آدرس های که اکتت اول آن‌ها از ۱۹۲ تا ۲۲۳ است در این کلاس قرار می گیرند. اکتت های اول تا سوم برای معین کردن آدرس Net و باقی برای تخصیص آدرس به Host مورد استفاده قرار می گیرد. می توان ۲۰۹۷۱۵۲ شبکه با ۲۵۴ Host و ۵۳۶۸۷۰۹۱۲ آدرس IP در کلاس C ایجاد کرد.

کلاس D: از این کلاس برای Mulsticast (جهت ارسال اطلاعات برای گروهی از Nod های موجود در یک شبکه مورد استفاده قرار می گیرد) استفاده می شود و کمی با کلاس‌ها و آدرس‌ها قبلی تفاوت دارد. آدرس های که اکتت اول آن‌ها از ۲۲۴ تا ۲۳۹ است.

کلاس E: این کلاس شباهتی زیادی به کلاس D دارد و بیشتر در موارد آزمایشی مورد استفاده قرار می گیرد. آدرس های که اکتت اول آن‌ها از ۲۴۰ تا ۲۵۴ است.

Broadcast: آدرس ۲۵۵.۲۵۵.۲۵۵.۲۵۵ که برای ارسال به همه Nod های شبکه می باشد.

نکته: آدرس های بالا برای استفاده در اینترنت می باشد و یک سری از آدرس خصوصی از داخل کلاس های IP برای شبکه های خصوصی خارج می شود که در اینترنت قابل استفاده نیست. این آدرس‌های خصوصی در بخش بعدی توضیح داده می‌شوند. **منبع: آزمایشگاه شبکه؛ مهندس ریاضی**

۲-۳-۲- IP خصوصی

برای جلوگیری از هدر دهی IP در هر کلاس، یک محدوده IP برای شبکه‌های خصوصی (مانند شبکه داخلی ادارات و شرکت ها) در نظر گرفته شده است. این آدرس‌ها قابل استفاده در شبکه اینترنت نمی‌باشد و معمولاً در شبکه‌های خصوصی و محلی استفاده می‌شود. این آدرس‌ها عبارتند از:

کلاس	تعداد آدرس ها	محدوده IP
Class A	۱۶،۷۷۷،۲۱۶	۱۰.۰.۰.۰ تا ۱۰.۲۵۵.۲۵۵.۲۵۵
Class B	۱،۰۴۸،۵۷۶	۱۷۲.۱۶.۰.۰ تا ۱۷۲.۳۱.۲۵۵.۲۵۵
Class C	۶۵،۵۳۶	۱۹۲.۱۶۸.۰.۰ تا ۱۹۲.۱۶۸.۲۵۵.۲۵۵

برای اتصال یک شبکه خصوصی به اینترنت از پروتکل NAT (Network Address Translation) استفاده می‌شود به این ترتیب که **نشانی خصوصی** به یک یا چند نشانی **منحصر به فرد عمومی** ترجمه می‌شود.

نام دیگر IP خصوصی، IP Invalid است. یعنی نمی‌توان در شبکه اینترنت از آن‌ها برای آدرس Serverها استفاده کرد. نقطه مقابل IP خصوصی، IP عمومی (Public) یا Valid IP قرار دارد که برای آدرس‌دهی Hostهای اینترنت از آن‌ها استفاده می‌شود.

۲-۳-۳- NAT چیست؟ (Network Address Translation)

می دانیم که هر کامپیوتری که قصد استفاده از اینترنت را دارد، بایستی یک آدرس Valid داشته باشد تا بتواند از خدمات اینترنت استفاده کند. بدین معنا که مثلاً اگر کامپیوتری درخواست مشاهده سایت http://www.google.com را نمود، صفحه باز شده (نتیجه کار نه درخواست انجام کار)، بایستی به کدام یک از کامپیوترهای متصل به اینترنت ارسال شود؟ یعنی کامپیوتر شما چگونه بایستی شناسایی شود؟ بنابراین بایستی کامپیوتر شما به صورت یکتا در اینترنت شناخته گردد. اما متاسفانه به تعداد کافی آدرس IP برای تخصیص به تمامی کامپیوترها و تجهیزات متصل به اینترنت و یکتا نمودن آن‌ها در اینترنت وجود ندارد. راه حل چیست؟

راه حل این است که دستگاهی خاص یا کامپیوتری خاص که یک آدرس IP به صورت Valid دارد و در سطح دنیا نیز شناخته می‌شود، نقش NAT Server را بازی نموده و کار ترجمه آدرس را انجام دهد. روال کار بدین صورت خواهد بود که به جای اینکه شما، آدرس IP به صورت Valid داشته باشید و به صورت مستقیم به اینترنت وصل شوید، شما به NAT Server متصل می‌شوید و درخواست‌های اینترنت خود را به آن می‌دهید. این سرور که یک آدرس Valid دارد نیز درخواست‌های شما را به سمت اینترنت می‌دهد و پاسخ دریافت شده را به شما باز می‌گرداند. بدین ترتیب شما نیازی به داشتن

آدرس Valid نخواهید داشت. در واقع با این کار، NAT Server، یک آدرس Valid را با چند کامپیوتر متصل به آن، به اشتراک می‌گذارد.

مثلاً زمانی که به صورت Dial-UP به اینترنت متصل می‌شوید، درخواست‌های اینترنت خود را به کامپیوتری در ISP ارائه دهنده خدمات اینترنت خود می‌دهید. این کامپیوتر نیز درخواست‌های شما را به سمت اینترنت فرستاده و پاسخ دریافت شده را به سمت شما باز می‌گرداند.

NAT Server هم به صورت سخت‌افزاری (تجهیزی جداگانه) و هم به صورت نرم‌افزاری (ویندوز سرور) قابل پیاده سازی است که نوع نرم‌افزاری آن را در فصول انتهایی همین جزوه و در قسمت VPN Server آموزش خواهیم داد.

۲-۳-۴- IP ایستا و پویا

IP پویا با هر بار وصل شدن به شبکه داخلی و یا اینترنت تغییر می‌کند. اما IP ایستا (Static) اینطور نیست. IP پویا (Dynamic) در هر شبکه توسط سرور پروتکل پیکربندی پویای میزبان (DHCP Server) به رایانه‌ها در شبکه اختصاص داده می‌شود. یعنی وقتی شما به اینترنت و یا شبکه داخلی وصل می‌شوید، سرور پروتکل پیکربندی پویای میزبان به شما یک نشانی IP اختصاص می‌دهد.

DHCP Server می‌تواند یک سرویس در سیستم عامل‌های سرور باشد یا یک قطعه سخت‌افزاری مانند مسیریاب (Router) و یا نقطه دسترسی (Access Point) در شبکه باشد.

برای دیدن نشانی IP رایانه خود می‌توان از برنامه winipcfg.exe (در ویندوز ۹۵ و ۹۸ و ME) یا ipconfig.exe (در ویندوز ۲۰۰۰ و XP و Vista و ۷) استفاده کرد (با تایپ دستور در Command Prompt). در لینوکس یا یونیکس (یا سیستم‌های مبتنی بر آن ها) نیز می‌توان از دستور ifconfig استفاده کرد.

۲-۴- IP نسخه ۶

۲-۴-۱- مقدمه

گسترش روز افزون اینترنت و نیاز به آدرس‌های بسیار بیشتر تیم Internet Engineering Task Force را برآن داشت تا به فکر تکنولوژی‌های جدیدی باشند تا امکان تعریف آدرس‌های IP بیشتری فراهم گردد. بهترین راه ساخت مجدد نشانی پروتکل اینترنت بود. در سال ۱۹۹۵ میلادی نسخه جدید نشانی پروتکل اینترنت با نام IP نسخه ۶ معرفی گردید. اندازه آدرس از ۳۲ بیت به ۱۲۸ بیت افزایش یافت و امکان آدرس‌دهی تا ۲ به توان ۱۲۸ آدرس (یعنی خیلی آدرس: به عبارتی می‌گویند در هر متر مربع، ۷×۱۰^{۲۳} آدرس IP موجود خواهد بود) افزایش یافت. این کار تنها تعداد آدرس‌های اینترنتی را گسترش نداد، بلکه باعث خواهد شد جدول مسیریاب‌های اینترنتی (روتر ها) کوچکتر شود. کلیه سیستم عامل‌های جدید سرور و خانگی از جمله ویندوز ویستا به طور کامل پشتیبانی می‌شود ولی متاسفانه هنوز توسط بسیاری از مسیریاب‌های شبکه‌های خانگی و تجهیزات شبکه عادی پشتیبانی نشده است.

احتمالا در خیلی از مقاله‌ها و در سایت‌های مختلفِ تکنولوژی و فناوری، درباره آینده عجیبی که در آن همه وسایل اعم از PC، PDA گرفته تا تلفن سلولی (موبایل)، اتومبیل، یخچال و به طور کل لوازم خانگی که به اینترنت وصل می‌شوند،

مطالبی را خواندهاید. برای مثال شما تصور کنید که از خانه خود برای انجام یک سفر به کشوری خارجی اعزام شدهاید و شخصی در نبود شما بستهای را برای شما می‌آورد و زنگ خانه شما را می‌زند در حالی که شما کیلومترها از خانه خود دور هستید و ناگهان تلفن همراه شما زنگ می‌خورد و دوربینی که در جلوی درب منزل خود نصب کردهاید تصویر شخص مورد نظر را بر روی تلفن همراه شما نمایان می‌سازد و مشاهده می‌کنید که بستهای را برای شما آورده‌اند، از همان جا درب منزل خود را باز می‌کنید و با سیستم‌های صوتی به او می‌گویید که بسته را داخل منزل بگذارد و درب را بسته و قفل می‌نمایید و همه این کارها را به صورت از راه دور و به صورت Remote انجام می‌دهید.

خوب برای چند دقیقه رویای جالبی بود اما یک ایراد در این بین وجود دارد: هر دستگاهی که بخواهد به اینترنت متصل شود و معرفی شود بایستی آدرس IP خاص خود را داشته باشد. ولی برای این همه دستگاه الکترونیکی به اندازه کافی IP وجود ندارد. هیچ کس تصور نمی‌کرد که بیش از چهار میلیارد آدرس IP (که در IPv4.0 برای شناسایی تمامی کامپیوترها در نظر گرفته شده بود) یک روز تمام شود. اما امروزه خیلی‌ها پیش بینی می‌کنند که این آدرس‌ها حداکثر تا سال آینده بیشتر دوام نخواهد آورد.

اینترنت در دنیای غرب تقریباً همه جا را گرفته و با سرعتی که در آسیا و کشورهای توسعه یافته پیش می‌رود، همه آدرس‌های خالی در آینده پر خواهند شد. این که درصد بالایی از آدرس‌های IP به خاطر لجبازی و چشم و هم چشمی‌های دانشگاه‌ها و سازمان‌های آمریکایی حیف و میل شدند و IPهای متعددی از پیش به آن‌ها اختصاص داده شد فرقی در اصل قضیه نمی‌کند. مثلاً دانشگاه استنفورد بیش از ۱۷ میلیون آدرس IP را برای خود گرفته است و این در حالی است که کشوری همانند هند که بیش از یک میلیارد جمعیت دارد فقط ۲ میلیون آدرس IP را به خود اختصاص داده است.

امروزه بسیاری از شبکه‌های کامپیوتری با استفاده از NAT یا Network Address Translation آدرس‌های اینترنتی خود را افزایش داده و بدین روش کمبود خود را در داشتن آدرس‌های IP اختصاصی حل می‌کنند. NAT به روتر، فایروال و دیگر دستگاه‌ها این امکان را می‌دهد که یک آدرس IP جهانی را با سایر تجهیزات داخلی طوری به اشتراک بگذارد که هر کدام از دستگاه‌ها آدرس خصوصی مربوط به خود را داشته باشند. مسائل دیگری وجود دارند که نشان می‌دهد که عمر IPV4.0 (نسخه فعلی IP) رو به پایان است. برای مثال امروزه این توقع که ارتباط شما با اینترنت ضمن حرکت از ساختمانی به ساختمان دیگر، یا شهری به شهر دیگر و حتی کشوری به کشور دیگر پابرجا بماند خواسته‌ای بی جا به حساب نمیاید. در واقع تکنولوژی نسبتا جدیدی موسوم به IP Mobile برای تحقق بخشیدن به چنین خواسته هایی به وجود آمده است ولی این تکنولوژی با IPv4.0 به خوبی کار نمی‌کند و شامل نقص هایی است و همچنین قابل توجه است که این تکنولوژی بایستی توسط سیستمی پیاده سازی شود که دارای امنیت بالایی باشد ولی IPV4.0 از این مسئله تا حدودی فاصله دارد.

۲-۴-۲- معرفی *IPv6.0*

منبع: http://hking.blogfa.com

IPV6 اگرچه ممکن است مکانیزم‌های NAT و CIDR چند سالی دیگر به دوام نسخه چهارم IP کمک کنند ولی تقریبا بر همه آشکار شده که نفس‌های پروتکل IP در شکل کنونی آن،به شماره افتاده است. مضاف بر مشکلات فنی IP،برخی از موارد پشت صحنه و زمینه‌ای دیگر نیز مطرح است.در سال‌های اولیه، از اینترنت عموما در دانشگاه‌ها،صنایع

پیشرفته و دولت ایالات متحده (خصوصا وزارت دفاع) استفاده می‌شد. با گرایش بسیار زیاد مردم به اینترنت که از اواسط دهه نود شروع شد، گروه‌های مختلفی از افراد به آن رو آوردند، افرادی که نیازها و انتظارات متفاوتی داشتند، یکی از موارد آنست که افراد با کامپیوترهای بی سیم قابل حمل برای در ارتباط بودن با محل استقرار دائمی خود (ایستگاه‌های خانگی) می‌خواهند از اینترنت بهره بگیرند. مورد دیگر آن که با هم گرایی قریب الوقوع صنایع کامپیوتر و مخابرات و صنایع تولید بازی و ابزار تفریح، دیری نخواهد پایید که حتی دستگاه‌های تلفن و تلویزیون در دنیا، به عنوان گرهی از اینترنت، به آن خواهد پیوست و در آن زمان میلیاردها ماشین، از صدا و تصویر بهره خواهند گرفت. با در نظر داشتن چنین اندازی،IP بوضوح نیازمند تغییرات اساسی است و باید انعطاف بیشتری داشته باشد.

IETF که چنین افقی را پیش روی خود می‌دید در اوان ۱۹۹۰ کار را بر روی نسخه جدیدی از پروتکل IP شروع کرد که در آن فضای آدرس هرگز با کمبود مواجه نشود و مشکلات عدیده‌ای را حل کند؛ قابلیت انعطاف بیشتری داشته باشد و در ضمن کارآمدتر باشد اهداف عمده IPV6 عبارت بودند از:

۱- پشتیبانی از میلیاردها ماشین میزبان حتی در صورتی که تخصیص فضای آدرس ناکارآمد و با اسراف انجام شود.

۲-کاهش اندازه جداول مسیر یابی

۳- ساده سازی پروتکل به منظور افزایش سرعت پردازش مسیریاب‌ها

۴- ارائه امنیت بهتر در مقایسه با نسخه فعلی IP (شامل احراز هویت و سری ماندن داده‌ها).

۵- توجه بیشتر به نوع خدمات و QoS، به ویژه برای داده‌های بی درنگ

۶- کمک به فرآیند ارسال چند بخشی از طریق توصیف حوزه‌ها

۷- فراهم آوردن امکان جابجایی ماشین‌های میزبان بدون تغییر در آدرس (Scopes)

۸- امکان ایجاد تغییر و پیشرفت در آینده

۹- امکان همزیستی پروتکل‌های جدید و قدیم در طی سال‌ها

برای توسعه پروتکلی که تمام نیازهای فوق الذکر را برآورده نماید، IETF با انتشار ۱۵۵۰ RFC و در طی یک فراخوان، خواستار پیشنهادات دیگران در این خصوص شد. ۲۱ پیشنهاد دریافت گردید که اغلب آن‌ها جامع نبودند. تا دسامبر ۱۹۹۲ فقط هفت طرح پیشنهادی قابل توجه در دستور کار قرار داشت. این طرح‌های پیشنهادی از اصلاحات جزیی در نسخه فعلی IP تا پیشنهاد دور انداختن آن و جایگزینی با یک پروتکل کاملا متفاوت را شامل می‌شد.

یک پیشنهاد آن بود که TCP برروی CLNP اجرا شود، پروتکلی که با آدرس‌های ۱۶۰ بیتی فضای آدرس‌دهی نامحدود و جاویدان را فراهم کرده بود و دو پروتکل عمده و مهم لایه شبکه را متحد و یکنواخت می‌کرد. ولیکن بسیاری افراد احساس کردند که پذیرش آن مهر تاییدی است بر این ادعا که هر کاری که OSI انجام داده صحیح تلقی می‌شود، داعیه‌ای که لااقل در حوزه اینترنت به دلایل خاص نادرست است. الگوی CLNR بسیار شبیه به IP بود و این دو، تفاوت چندانی با هم ندارند، در آخر نیز طراحی شد که تفاوت بسیار زیادی با IP و از آن بیشتر با CLNP دارد. ضربه دیگری که CLNP خورد از آنجا بود که پشتیبانی ضعیفی از «نوع خدمات» (Type of Service) می‌کرد، خصوصیتی که برای انتقال کارآمد داده‌های چند رسآن‌های به شدت نیاز بود.

سه تا از بهترین طرح‌های پیشنهادی در ژورنال IEEE Network منتشر شد. پس از مباحثات فراوان بازبینی ارزیابی موقعیت و سنجش استقبال عمومی، نسخه‌ای ترکیبی از طرح‌های پیشنهادی Deering و Francis که SIPP نامیده می‌شد به عنوان طرح برگزیده معرفی و با عنوان IPV6 معرفی گردید.

IPV6 بخوبی اهداف مورد نظر را برآورده می‌کند: ویژگی‌های خوب IP را نگه داشته، ویژگی‌های بد را کنار گذاشته یا کمرنگ کرده و ویژگی‌های جدیدی به آن افزوده است. بطور کلی IPV6 با IPV4 سازگار نیست ولی با تمام پروتکل‌های جانبی اینترنت مثل TCP، UDP، ICMP، IGMP، OSPF،BGP،DNS سازگار است. (البته ممکن است به دلیل آنکه آدرس‌ها طولانی‌تر شده‌اند نیاز به اندکی تغییر داشته باشند). ویژگی‌های اساسی IPV6 در زیر تشریح شده است. برای آگاهی بیشتر در خصوص آن به RFCهای ۲۴۶۰ تا ۲۴۶۶ مراجعه نمایید.

اولین مهمترین ویژگی که IPV6 آدرس‌ها بسیار طولانی تری نسبت به IPV4 دارد. این آدرس‌ها ۱۶ بایت طول دارند و دقیقا مشکلی را حل کرده که به همان دلیل طراحی شد: یعنی تقریبا فضای نامحدودی از آدرس‌های IP را فراهم آورده است. در این خصوص بیشتر صحبت خواهیم کرد.

دومین پیشرفت عمده IPV6 ساده سازی سرآیند آنست. این سرآیند جمعا هفت فیلد دارد(در مقابل سیزده فیلد در IPV4). این تغییر، امکان آنرا فراهم آورده که مسیریاب بسته‌ها را سریعتر پردازش نماید و ظرفیت مفید مسیریاب را افزایش و تاخیر را کاهش دهد. در ادامه مختصرا به سرآیند خواهیم پرداخت.

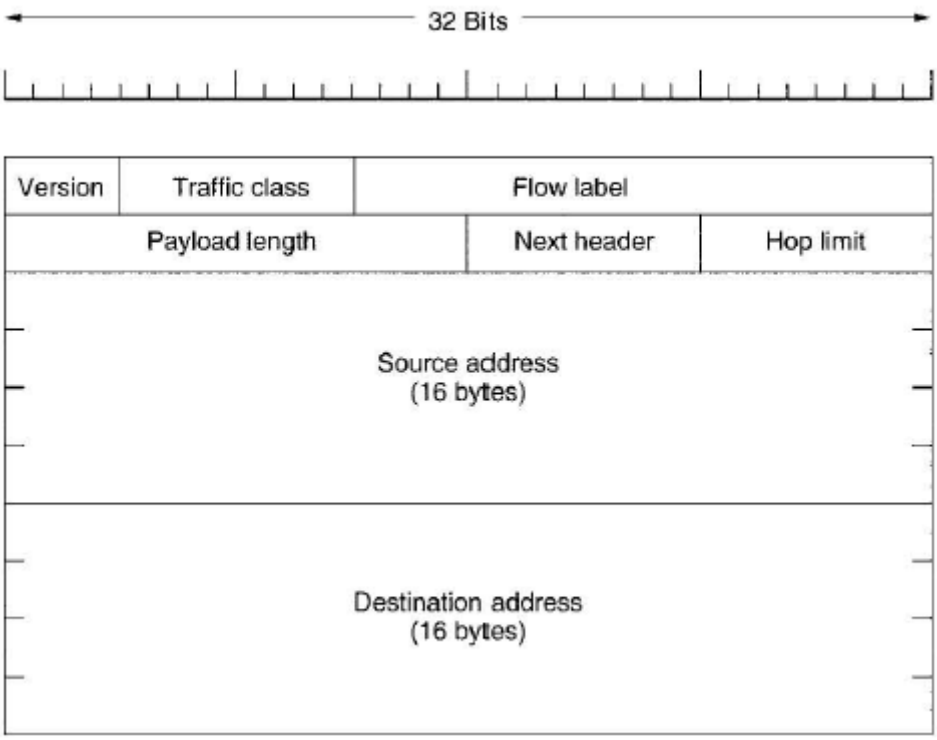
سومین بهبود عمده آن پشتیبانی از گزینه‌های اختیاری (Options) است. این تغییر برای سرآیند جدید حیاتی بود چرا که برخی از فیلدهایی که در نسخه قبلی وجودشان الزامی است در نسخه فعلی اختیارند. مضاف بر این، روش درج گزینه‌ها در این فیلد متفاوت از قبل است و اجازه می‌دهد مسیریاب‌ها بتوانند به سادگی از گزینه‌هایی که برایشان مهم نیست رد شوند. (یعنی در نسخه جدید، دسترسی تصادفی و مستقیم به گزینه‌ها ممکن شده است). این ویژگی سرعت پردازش بسته را افزایش می‌دهد.

چهارمین موضوعی که IPV6 در آن پیشرفت عمده‌ای داشته است.« امنیت »است.IETF با انبوهی از گزارش‌های مطبوعاتی در خصوص نابغه‌های دوازده ساله‌ای مواجه بود که با کامپیوترهای شخصی خود، به شبکه‌های بانکی یا پایگاه‌های نظامی در سراسر اینترنت، نفوذ کرده بودند و جود شدیدی براه افتاده بود که باید برای بهبود امنیت شبکه‌ها کاری کرد. در نسخه جدید IP « احراز هویت» (Authentication) و «حفظ امنیت اطلاعات » (Privacy) جزو ویژگی‌های کلیدی به شمار می‌رود. البته این ویژگی‌ها بعدا به IPV4 نیز افزوده شد (با عنوان IPSec) و لذا در حال حاضر این دو در زمینه امنیت تفاوت چندانی با یکدیگر ندارند.

موضوع آخر آنکه در نسخه جدید به کیفیت خدمات (QoS) دقت بیشتری شده است. قبل از آن نیز تلاش‌های جسته و گریخته‌ای در این رابطه انجام شده بود، ولیکن با رشد کاربردهای چند رسآن‌های در اینترنت، این موضوع جدی‌تر و حساس‌تر به نظر می‌رسد.

سرآیند اصلی IPV6

سرآیند اصلی IPV6 در شکل زیر نشان داده شده است. فیلد Version (شماره نسخه پروتکل) برای IPv6 همیشه ۶ است؛ کما اینکه برای IPv4 همیشه ۴ است. در دوران گذر از IPv4 به نسخه جدید که ممکن است یک دهه طول بکشد. مسیریاب‌ها قادرند با بررسی این فیلد تشخیص بدهند که با چه نوع بسته‌ای روبرو هستند. البته از آنجایی که بررسی این فیلد به چندین دستورالعمل اجرایی CPU نیاز دارد و این کار زمان مفید پردازش هر بسته را هدر می‌دهد لذا در بسیاری از پیاده سازی‌های عملی، برای اجتناب از این زمان تلفاتی، تشخیص آنکه یک بسته از نوع IPV4 است یا IPV6، با استفاده از فیلد خاصی در سرآیند لایه پیوند داده‌ها برعهده سخت‌افزار گذاشته شده است. بدین ترتیب بسته بر اساس نوعشان مستقیما به نرم‌افزار مناسب در لایه شبکه هدایت می‌شوند. البته این الزامی که لایه پیوند داده از جزییات نوع بسته‌های لایه شبکه آگاه باشد با این اصل اساسی که هر لایه نباید از معنای بیت‌هایی که از لایه بالاتر تحویل او می‌شود، آگاه باشد در تناقض است. بدون شک بحث و مناقشه بین طرفداران ایدههای« انجام اصولگرایانه وصحیح کار» و «تسریع کار» به شدت ادامه خواهد داشت.



فیلد Traffic Class (کلاس ترافیک)برای تشخیص تفاوت بسته‌ها ازلحاظ نیازمندی‌های تحویل بی درنگ و QoS درخواستی، بکار می‌آید. فیلدی با همین منظور از ابتدا در IP وجود داشت ولیکن استفاده از آن به صورت پراکنده و سلیقه‌ای بر روی مسیریاب‌ها پیاده سازی شد و اغلب مسیریاب‌ها آن را نادیده می‌گرفتند. اکنون تجربیات گذشته چراغ راهی شده تا بتوان بهترین راه و روش تحویل بسته‌های اطلاعات چند رسآن‌های را تعیین کرد.

فیلد Flow Label (برچسب جریان) همچنان آزمایشی است ولی کاربرد مورد نظرآن، این بوده که بتوان یک « شبه اتصال» (Pseudoconnection) بین مبداء و مقصد، با ویژگی‌ها و نیازمندی‌های خاص ایجاد کرد. به عنوان مثال، جریانی از بسته‌ها که از یک پروسه در مبداء باند لازم را رزرو کرد. در چنین مواردی می‌توان پیشاپیش یک «جریان» (Flow) با مشخصات درخواستی تنظیم کرد و به آن یک شناسه اختصاص داد.هرگاه مسیریاب بسته‌ای دریافت کند و فیلد Flow Label

آن غیر صفر باشد، با مراجعه به جداول درونی خود مشخص می‌دهد که به این بسته چگونه رفتارکند. در حقیقت استفاده از مفهوم «جریان» در IPV6، تلاشی است برای رسیدن به قابلیت انعطاف در زیر شبکه‌های دیتاگرام و تضمین کیفیت خدمات در زیر شبکه‌های مدار مجازی.

هویت هر «جریان » برحسب آدرس مبداء، آدرس مقصد و شماره جریان (برچسب جریان) مشخص می‌شود فلذا بین دو مبداء و مقصد در شبکه می‌توان بطور همزمان چندین «جریان» فعال تنظیم کرد. همچنین در این روش حتی اگر دو جریان متفاوت با شماره جریان یکسان از دو ماشین میزبان مختلف تولید و از مسیریاب‌ها مشابهی عبور کنند، مسیریاب‌ها به کمک آدرس مبداء و مقصد قادر به تشخیص آن‌ها خواهند بود. انتظار آنست که «برچسب‌های جریان» به جای آنکه به صورت ترتیبی و از ۱ شروع به صورت کاملا تصادفی انتخاب گردند تا مسیریاب بتواند آن‌ها را در Hash Table خوددرج کند.

فیلد Payload Lengh (طول قسمت حمل داده) مشخص می‌کند که پس از سرآیند ۴۰ بایتی در شکل ۱ چند بایت داده قرار گرفته است. همین فیلد در IPV4 به نام Total Length وجود داشت. تغییرنام به آن دلیل بوده که در نسخه جدید، سرآیند جزو طول بسته به حساب نمی‌آید بلکه فقط اندازه بخش حمل داده تعیین می‌شود.

فیلد Next Header ساختار بسته را سبک بار کرده است دلیل آنکه سرآیند بسته ساده شده آنست که می‌توان در صورت لزوم سرآیند اضافی و انتخابی داشت. این فیلد مشخص می‌کند که پس از سرآیند ۴۰ بایتی کدامیک از سرآیندهای ششگانه اضافی قرار گرفته است (در صورت وجود). اگر سرآیند اخیر، آخرین سرآیند بسته IP باشد، این فیلد مشخص می‌کند که کدام پروسه در لایه انتقال محتوای بسته را تحویل خواهد گرفت (مثلا TCP، UDP و نظائر آن).

کاربرد فیلد Hop Limit آنست که بسته‌ها عمر محدودی داشته باشند. این فیلد در عمل مشابه با فیلد Time to Live (زمان حیات بسته) در IPV4 است یعنی به ازای عبور بسته از یک مسیریاب، یک واحد از مقدار آن کاسته می‌شود. در تئوری، مبنایی که IPV4 برای این فیلد در نظر داشت،«زمان بر مبنای ثانیه» بود در حالی که هیچ مسیریابی از چنین مبنایی استفاده نمی‌کند(بلکه به ازای هرگام یک واحد از آن می‌کاهد) لذا نام این فیلد را به گونه‌ای عوض کردند که عملکرد واقعی آن را نشان بدهد. هرگاه مقدار این فیلد در یک بسته به صفر برسد آن بسته حذف خواهد شد.

در ادامه فیلدهای Destination Address و Source Address (آدرس مبداء و مقصد) قرار گرفته‌اند. در طرح پیشنهادی آقای Deering آدرس‌ها ۸ بایتی انتخاب شده بودند در حالی که در مراحل بازبینی دیگران احساس کردند که شاید این فضای آدرس نیز در خلال چند دهه، IPV6 را نیز با کمبود فضای آدرس مواجه کند، در حالی که با آدرس‌های ۱۶ بایتی هرگز چنین کمبودی رخ نخواهد داد. برخی از افراد معتقد بودند که آدرس‌های ۱۶ بایتی بیش از حد بزرگ هستند در حالی برخی دیگر اعتقاد داشتند باید از آدرس‌های ۲۰ بایتی استفاده شود تا با پروتکل دیتاگرام پیشنهادی OSI سازگار باشد. گروه دیگری نیز به آدرس‌های با طول متغییر گرایش داشتند. پس از بحث و جدل فراوان، به این نتیجه رسیدند که آدرس‌های با طول ثابت ۱۶ بایتی بهترین انتخاب است.

با توجه به طول زیاد آدرس‌های IP زیاد آدرس‌های IP، نماد جدیدی برای نوشتن آن‌ها پیشنهاد شد. این آدرس‌ها به صورت هشت گروه که با علامت: از هم جدا شده، نوشته می‌شوند. هر گروه نیز به صورت چهار رقم هگزادیسمال نمایش داده می‌شود:

8000:0000:0000:0000:0123:4567:89AB:CDEF

از آنجایی که در آدرس‌ها تعداد ارقام صفر زیاد است، سه نوع بهینه سازی مجاز شمرده شده: صفرهای سمت چپ در هر گروه نوشته نمی‌شوند. یعنی ۰۱۲۳ به صورت ۱۲۳ نشان داده می‌شود؛ دوم آنکه اگر یک یا چند گروه شانزده بیتی تماما صفر باشد، با یک زوج علامت:: نشان داده می‌شود. بنابراین آدرس مثال بالا به صورت زیر نوشته خواهد شد:

8000::123:4567:89AB:CDEF

نهایتا آنکه آدرس‌های IPV4 را می‌توان با یک جفت: و سپس آدرس نقطه دار قدیمی، نشان داد:

::192.31.20.46

شاید لازم به گفتن نباشد که آدرس‌های شانزده بایتی، فضایی معادل $۲^{۱۲۸}$ آدرس هستنn که چنین فضایی تقریبا معادل ۳×۱۰^{۳۸} آدرس است. اگر کل کره زمین شامل خشکی‌ها و دریاها پراز کامپیوتر شوند باز هم Piv6 می‌تواند برای هر متر مربع ۷×۱۰^{۲۳} آدرس IP فراهم کند. دانشجویان رشته شیمی می‌دانند که این عدد حتی از عدد آووگادرو نیز بزرگ است. (عدد آووگادرو $۶/۰۲\times۱۰^{۲۳}$).چون در نظر نبوده که حتی به مولکول‌های سطح زمین آدرس بدهیم آدرس‌های IP شانزده بایتی، به هیچ وجه کم نخواهد آمد!!

در عمل از فضای آدرس IP، بخوبی استفاده نخواهد شد(دقیقا همانند فضای شماره‌های تلفن که مثلا فضای شماره‌های تلفن منهتن با پیش شماره ۲۱۲ پر شده ولی فضای شماره‌های ویومینگ (wyoming) با پیش شماره ۳۰۷ تقریبا خالی مانده است). دو نفر به نام‌های Durand، Huitema در سند RFC ۳۱۹۴ محاسبه کرده‌اند که با ایده گرفتن از تخصیص شماره‌های تلفن و حتی در بدبینانه ترین حالت ممکن، باز هم می‌توان برای هر متر مربع از کره زمین ۱۰۰۰ آدرس IP کنار گذاشت. در حالت کلی نیز می‌توان تریلیون‌ها آدرس IP برای هر مترمربع از زمین در نظر گرفت. کوتاه سخن آنکه، در آینده هیچ گاه به مشکل فضای آدرس برنخواهیم خورد.

مقایسه سرآیند IPV4 با سرآیند IPV6 از این دیدگاه که چه فیلدی و چرا حذف شده است، آموزنده خواهد بود:فیلد LHL حذف شده زیرا سرآیند بسته‌های IPV6 طول ثابتی دارد. فیلد«پروتکل» وجود ندارد و چرا که فیلد Next Header مشخص می‌کند که پس از آخرین سرآیند چه بسته دیگری آمده است (بسته UDP.TCP یا نظائر آن).

تمام فیلدهایی که در ارتباط با « قطعه قطعه سازی» بسته‌ها در IPV4 تعریف شده بود در IPV6 حذف گردیده است زیرا پروتکل اخیر راهکار دیگری برای مکانیزم قطعه قطعه سازی برگزیده است. انتظار آنست که تمام ماشین‌های سازگار با IPV6 بتوانند به صورت خودکار و پویا اندازه دیتاگرام‌ها را تعیین کنند و بدین نحو نیاز به قطعه قطعه شدن بسته‌ها کمتر اتفاق می‌افتد. همچنین حداقل طول بسته‌ای که هر ماشین موظف به پذیرش آنست که ۵۷۶ بایت به ۱۲۸۰ بایت افزایش یافته تا بتوان یک قطعه داده ۱۰۲۴ بایتی را به همراه تعداد زیادی سرآیند(۲۵۶ بایت)، بدون نیاز به قطعه قطعه شدن ارسال و دریافت کرد. مضاف بر این، وقتی ماشینی که بسته بیش از حد بزرگ IPV6 را ارسال می‌دارد مسیریاب ناتوان از هدایت آن، به جای قطعه قطعه کردن بسته آن را حذف کرده و پیام خطایی را باز می‌گرداند. این پیام به ماشین میزبان تفهیم می‌کند که باید بسته‌هایش را بشکند. البته اگر ماشین میزبان خودش بسته‌ها را با اندازه مناسب ارسال کند کارآمدتر از آنست که بسته‌ها در طول مسیر شکسته شود.

فیلد Checksum نیزحذف شد؛ زیرا محاسبه آن کارآیی و سرعت پردازش بسته‌ها را به نحو چشمگیری کاهش خواهد داد. با توجه به قابلیت اعتماد شبکه‌های کنونی و با در نظر داشتن این حقیقت که در لایه پیوند داده و لایه انتقال نیز (بطور

مجزا) صحت داده‌ها بررسی می‌شود، محاسبه یک کد کشف خطای دیگر مثل Checksum در مقایسه با کاهش کارآیی ارزشی ندارد. حذف این ویژگی‌های زائده، IPV6 را به پروتکل متعادل و جمع و جور تبدیل کرده است. بدین ترتیب IPV6 با اهداف مورد نظر خود که همانا انعطاف، سرعت و فضای بزرگ آدرس بوده، نائل شده است.

سرآیندهای اضافی (سرآیندهای توسیع یا Extension Header)

گاهی به برخی از فیلدهای حذف شده IPV4 نیاز می‌شود و به همین منظوره در IPV6 مفهوم جدیدی به نام «سرآیندهای توسیع» معرفی شده است. این سرآیندهای اختیاری برای افزودن اطلاعات به هر بسته بکار می‌آیند ولیکن روش کدینگ(و جاسازی) آن‌ها کارآمد و سریع است. شش نوع مختلف سرآیند توسیع که تاکنون معرفی شده در جدول زیر فهرست گردیده است. هر کدام از این سرآیندها اختیارند ولیکن اگر به بیش از یک سرآیند نیاز باشد باید بطور پیاپی، پس از سرآیند ثابت و ترجیحا به ترتیب فهرست قرار بگیرند.

نام سرآیند توسیع(سرآیند اضافی)	توصیف عملکرد
Hop-by-hop options	حاوی اطلاعات گوناگون برای مسیریاب‌ها
Destination options	اطلاعات اضافی برای مقصد
Routing	فهرست ناکاملی از مسیریاب‌ها که بسته باید از آن‌ها بگذرد
Fragmentation	مدیریت قطعات دیتاگرام
Authentication	بررسی هویت فرستنده
Encrypted security payload	اطلاعاتی در خصوص محتوای رمزنگاری شده بسته

برخی از سرآیندها دارای قالب ثابتی هستند در حالی که برخی دیگر تعداد متغیری فیلد با طول متفاوت دارند. به همین دلیل هر آیتم در قالب سه تایی (نوع، طول، مقدار) سازماندهی و کد می‌شود. فیلد Type مشخص می‌کند که نوع گزینه چیست. مقدار فیلد نوع Type به نحوی انتخاب شده است که دو بیت ابتدایی آن به مسیریاب‌هایی که نمی‌دانند آن گزینه را چگونه پردازش کنند، راه و چگونگی کار را نشان می‌دهند. این راهکارها عبارتند از: (۱) گزینه مربوط را نادیده بگیر(۲) بسته را حذف کن (۳) بسته را حذف و یک بسته ICMP برگردان (۴) بسته را حذف کن و یک بسته ICMP برگردان لیکن بسته ICMP را برای آدرس‌های «چند پخشی»(Multicast) نفرست.(تا یک بسته چندپخشی اشتباه، منجر به تولید میلیون‌ها گزارش ICMP نشود).

فیلد یک بایتی طول (Length) مشخص می‌کند که فیلد مقدار (Value)نفرست. (تا یک بسته چند پخشی اشتباه، منجر به تولید میلیون‌ها گزارش ICMPنشود.) فیلد یک بایتی طول (Length) مشخص می‌کند که فیلدمقدار(Value) چند بایتی است.(صفر تا ۲۵۵ بایت). فیلد مقدار (Value) در برگیرنده اطلاعات مورد نیاز است و حداکثر می‌تواند ۲۵۵ بایت باشد.

«سرآیند توسیع Hop-by-Hop» (گام به گام) برای حمل اطلاعاتی کاربرد دارد که مسیریاب‌های واقع بر مسیر باید آن‌ها را بررسی نمایند. قبلا یکی از گزینه‌ها را معرفی کردیم: پشتیبانی از دیتاگرام‌هایی با طول بیش از ۶۴ کیلو بایت. قالب این سرآیند در شکل زیر نشان داده شده است. وقتی از این سرآیند استفاده نمی‌شود باید فیلد Payload Length (درآیند اصلی) به صفر مقداردهی شود.

Next header	0	194	4
Jumbo payload length			

همانند تمام سرآیندهای اختیاری دیگر، این سرآیند نیز با فیلدی یک بایتی به نام Next header شروع می‌شود و مشخص می‌کند که سرآیند بعدی از چه نوع است. پس از بایت، بایت دیگری قرار گرفته که طول سرآیند Hop-by-Hop را بر مبنای بایت تعیین می‌کند ولیکن در مقدار آن، ۸ بایت ابتدایی (که وجود آن الزامی است) لحاظ نمی‌شود. تمام سرآیندهای توسیع دیگر نیز به همین نحو شروع می‌شوند. در ادامه فیلدی دو بایتی آمده که بایت اول مشخص می‌کند که این گزینه Option قرار است اندازه دیتاگرام را تعریف کند (کد ۱۹۴) و بایت بعدی مشخص می‌کند که اندازه دیتاگرام یک شماره چهار بایتی است.چهار بایت آخر این سرآیند، طول دیتاگرام را مشخص می‌کند. اندازه زیر ۶۵۵۳۶ مجاز نیست و منجر به حذف بسته در اولین مسیریاب بازگشت پیام خطای ICMP خواهد شد. دیتاگرام‌هایی که از این سرآیند اختیاری(یعنی Hop-by-Hop Header) استفاده کرده‌اند اصطلاحا Jumbogram (دیتاگرام عظیم) نامیده می‌شوند، (بدین ترتیب در IPV6 می‌توان قطعات داده بسیار بزرگ را به کمک سرآیند فوق به صورت یکجا ارسال کرد). کاربدر جامبوگرام‌ها در سوپر کامپیوترها که باید چندین گیگابایت اطلاعات را از طریق اینترنت منتقل کنند، بسیار حیاتی است.

«سرآیند توسیع Destination options» برای درج فیلدهایی در نظر گرفته شده که صرفا توسط ماشین مقصد پردازش و تفسیر می‌شوند. در نسخه اولیه IPV6 مقدار این گکزینه پوچ در نظر گرفته شده و کاربردی نداشته است. وجود چنین فیلدی برای آن بوده که نرم‌افزار ماشین‌های میزبان و مسیریاب‌ها چنین سرآیندی را به رسمیت بشناسند تا اگر روزگاری به آن نیاز شد، شرایط مهیا باشد وگرنه باید پروتکل عوض شد.

«سرآیند توسیع Routing» فهرست مسیریاب‌هایی را مشخص می‌نماید که بسته باید در راه رسیدن به مقصد از آن‌ها عبور کند. این گزینه شباهت زیادی به گزینه Loose Source Routing در IPV4 دارد. فهرست آدرس‌هایی که در این سرآیند مشخص شده باید در طول مسیر و به ترتیب ملاقات شوند ولی این امکان وجود دارد که مسیریاب‌هایی هم که آدرس آن‌ها در فهرست نیست ما بین مسیر باشند. قالب سرآیند Routing در شکل زیر مشخص شده است.

Next header	Header extension length	Routing type	Segments left
Type-specific data			

چهار بایت اول از این سرآیند، شامل چهار فیلد یک بایتی است:دو فیلد Next Header و Header Extension length را قبلا تعریف کردیم. فیلد Routing Type، ساختار مابقی سرآیند را مشخص می‌نماید: مقدار صفر مشخص کننده می‌گیرد. به غیر از این ساختار، فعلا ساختار دیگری تعریف نشده مگر آنکه در آینده چیز جدیدی ابداع شود. فیلد آخر یعنی Segment Left تعداد آدرس‌هایی را مشخص می‌کند که هنوز ملاقات نشده‌اند. مقدار اولیه این فیلد معادل با تعداد مسیریاب‌هایی است که آدرس آن‌ها در فهرست مورد نظر درج شده است و به ازای ملاقات در هر مسیریاب که آدرس آن در فهرست آمده که یک واحد از این فیلد کاسته می‌شود. وقتی مقدار این فیلد دربسته به صفر برسد بسته روال طبیعی مسیرخود را

از سر می‌گیرد بدون آنکه اجبار به عبور از مسیر خاصی داشته باشد. معمولا در چنین لحظه‌ای بسته به مقصد خود نزدیک شده است.

سرآیند Framentation مشابه با IPV4، با مسئله قطعه قطعه سازی بسته‌ها سروکار دارد. در این سرآیند نیز فیلدهای «شماره شناسایی دیتاگرام» «شماره قطعه» و یک بیت MF تعریف شده‌اند که بیت MF مشخص می‌کند که آیا قطعه جاری آخرین قطعه دیتاگرام است یا آنکه قطعات دیگری در ادامه وجود دارند. البته در IPV6، فقط ماشین مبدا می‌تواند بسته‌ای را قطعه قطعه کند و مسیریاب‌ها را ساده‌تر کرده و فرآیند مسیریابی سریعتر خواهد شد. همانگونه که قبلا اشاره کردیم هرگاه یک مسیر یاب با بسته‌ای بیش از حد بزرگ مواجه گردد آن را حذف کرده و بسته ICMP (حامل پیغام خطا و اطلاعات مفید دیگر) به مبداء آن بر می‌گرداند. اطلاعات ارسالی به مبداء بسته، امکان آنرا می‌دهد که به کمک این سرآیند، بسته را به قطعات کوچکتر تقسیم و آن‌ها را از نو ارسال کند.

سرآیند Authentication (سرآیند احراز هویت) مکانیزمی را فراهم آورده تا گیرنده بتواند از هویت فرستنده بسته مطمئن شود. سرآیند Encrypted Security payload اجازه می‌دهد تا محتوای بسته رمزنگاری شود و بدین ترتیب فقط گیرنده مورد نظر قادر به خواندن آنست. این گونه سرآیندها برای انجام ماموریت خود از تکنیک‌های رمزنگاری بهره می‌گیرند.

اختلاف نظرها و مناقشات

نظر به آنکه فرآیند طراحی IPV6 «باز» بوده و افراد درگیر در طراحی، بر عقاید خود تاکید داشته‌اند فلذا شگفت آور نیست که بسیاری از گزینه‌های انتخابی در IPV6 متناقض باشند. در زیرا اجمالا برخی از آن‌ها را بررسی خواهیم کرد. برای آگاهی از جزییات ماجرا به RFCهای مربوطه مراجعه نمایید.

قبلا اشاره کردیم که بحث و جدل گسترده‌ای پیرامون طول آدرس‌ها وجود داشت و توافق نهایی آن بود که آدرس‌ها با طول ثابت و ۱۶ بایتی باشند.

جدل دیگری بر سرحداکثر تعداد گام (Hop limit) درگرفت. یک گروه احساس می‌کرد که محدود کردن حداکثر تعداد گام (Hop) به ۲۵۵ یک اشتباه محض است چرا که اگرچه در آن زمان حداکثر طول مسیرها عموما از ۳۲ تجاوز نمی‌کرد ولی مدعی بودند که ممکن است ده سال بعد مسیرها طولانی‌تر از ۲۵۵ باشند. استدلال آن‌ها این بود که فضای آدرس ۱۶ بایتی آینده نگری بیش از اندازه و درعوض مقدار کم Count، کوته نظری است. از دیدگاه آن‌ها بزرگترین اشتباه یک دانشمند کامپیوتر، آنست که برای هر فیلدی، تعداد بیت کمی در نظر بگیرد.

پاسخ گروه مقابل آن بود که افزایش بی مورد فضای هر فیلد منجر به تشکیل یک سرآیند حجیم خواهد شد. همچنین استدلال دیگرشان آن بود که وظیفه فیلد Hop Count جلوگیری از سرگردانی بسته‌ها به مدت طولانی است و ۶۵۵۳۵ گام بیش از حد زیاد است. استدلال آخر آنکه با رشد اینترنت، لینک‌های بسیار طولانی ساخته می‌شوند و این امکان فراهم می‌شود که برای رسیدن از یک کشور به کشور دیگر به کمتر از ده گام نیاز باد. اگر یک بسته برای رسیدن از مبداء به مقصد مجبور شود از ۱۲۵ مسیریاب بین المللی بگذرد، ستون فقرات این شبکه بین المللی در جایی اشکال دارد بدین ترتیب طرفداران فیلد ۸ بیتی در عقیده خود پیروز شدند.

یکی دیگر از بحث‌های داغ بر سر حداکثر طول بسته‌ها بود. سوپر کامپیوترها به بسته‌هایی با طول بیش از ۶۴ کیلوبایت احتیاج داشتند. وقتی یک سوپر کامپیوتر شروع به ارسال می‌کند و به کار خود مشغول می‌شود نباید به ازای هر ۶۴ کیلو بایت یکبار متوقف شود. استدلال گروه مخالف آن بود که اگر یک بسته یک مگابایتی در طول مسیر به یک خط TI برسد آن خط به مدت حداقل ۵ ثانیه اشغال شده و کاربران دیگری که در این خط سهیم هستند با تاخیر قابل توجهی روبرو خواهند شد. توافق نهایی بدینجا ختم شد که بسته‌های معمولی حداکثر ۶۴ کیلوبایتی باشند ولی به کمک سرآیند اختیاری Hop-by-Hop بتوان جامبوگرام‌هایی با هر طول دلخواه ارسال کرد.

موضوع سوم مناقشه، حذف فیلد IPV4 checksum (کد نشخیص خطاهای احتمالی در سرآیند)بودوبرخی از افراد حذف این فیلد را مشابه با برداشتن ترمزهای یک خودرو می‌دانستند که اگرچه ماشین را سبکبار و سریعتر می‌کند ولی اگر اتفاق غیرمترقبه‌ای رخ بدهد مشکل جدی بوجود می‌آید.استدلال گروه مقابل آن بود هر برنامه کاربردی که نگران صحت داده‌های خود است باید از پروتکلی در لایه انتقال بهره بگیرد که داده‌ها را از لحاظ سلامت بررسی می‌کند. لذا اضافه کردن کد کنترلی دیگر به لایه IP برای کشف خطا(در حالی که هر بسته یکبار هم در لایه پیوند داده بررسی می‌شود. بیهوده و زائد است. مضاف برآن، تجربه نشان داده بود که محاسبه جمع کنترلی (Checksum)در IPv4 هزینه بالایی دارد. در این مناقشه نیز طرفداران حذف کد کشف خطا پیروز شدند. موضوع دیگر، بحث ماشین‌های همراه بود. وقتی یک کامپیوتر قابل حمل، در نیمی از کل دنیا حرکت می‌کند(مثلا درون هواپیما)، آیا می‌تواند با همان آدرس PIv6 قبلی، کار خود را ادامه بدهد، یا آنکه مجبور به استفاده از ساختار «عامل فرنگی» و «عامل خارجی»؟ ماشین‌های همراه مشکل «عدم تقارن» را به سیستم مسیریابی تحمیل می‌کنند:یک کامپیوترتر همراه و کوچک براحتی قادر به شنیدن سیگنال قوی منتشره از مسیریاب ثابت خود هست ولی مسیریاب ثابت براحتی قادر به احساس سیگنال ضعیف ارسال شده توسط کامپیوتر همراه نیست. در نتیجه برخی از افراد گرایش داشتند که در IPV6 از ماشین‌های همراه حمایت شود ولی تمام این تلاش‌ها به دلیل آنکه بر روی هیچیک از طرح‌های پیشنهادی توافقی بدست نیامد، با شکست مواجه گردید.

شاید بزرگترین مناقشه بر سر موضوع «امنیت» بود: همه بر این اصل که « امنیت لازم است» اشتراک نظر داشتند. دعوا بر سر چگونگی رسیدن به امنیت و محل پرداختن به آن بود. اولین محل پرداختن به امنیت لایه شبکه است. استدلال موافقین مبنی بر آن بود که پیاده سازی امنیت در لایه شبکه، سرویسی استاندارد فراهم می‌کند که تمام برنامه‌های کاربردی بدون هیچگونه برنامه ریزی قبلی می‌توانند از آن‌ها بهره بگیرند. استدلال مخالفین نیز آن بود که برنامه‌های کاربردی امن، عموما به هیچ مکانیزمی کمتر از رمزنگاری انت‌ها به انت‌ها (End-to-End Encryption) احتیاج ندارند، به نحوی که پروسه مبدا خودش داده‌های ارسالی خود را رمز کرده و پروسه مقصد آن‌ها را از رمز خارج کند. هر چیزی کمتر از این، می‌تواند کاربر را با خطراتی مواجه کند که از اشکالات امنیتی لایه شبکه ناشی می‌شود و هیچ تقصیری از او نیست. پاسخ به استدلال آن بود که کاربر می‌تواند امنیت لایه IP را نادیده بگیرد و کار خودش را انجام بدهد. پاسخ نهایی مخالفین نیز آن بود که افرادی که به عملکرد صحیح شبکه (در خصوص امنیت) اعتماد ندارند چرا باید هزینه پیاده سازی سنگین و کندی IP را بپردازند.

یکی دیگر از جنبه‌های مربوط به امنیت این حقیقت بود که بسیاری از کشورها قوانین سخت گیرآن‌های در مورد صادرات محصولات مرتبط با رمزنگاری وضع کرده‌اند. از مثال‌های بارز می‌توان به فرانسه و عراق اشاره کرد که حتی استفاده از

رمزنگاری در داخل را نیز محدود کرده‌اند و عموم افراد نمی‌توانند چیزی را از پلیس مخفی نگه دارند. در نتیجه هرگونه پیاده سازی از IP که از روش‌های رمزنگاری قوی استفاده می‌کند مجوز صدور از ایالات متحده (و بسیاری از کشورهای دیگر) را نخواهد گرفت. پیاده سازی دو نرم‌افزار یکی برای کاربرد داخلی و یکی برای صادرات، موضوعی است که عرضه کنندگان صنعت کامپیوتر با آن مخالفند.

موضوعی که پیرامون آن هیچ اختلاف نظر پیش نیامد آن بود که نمی‌توان انتظار داشت صبح روز یکشنبه IPV4 را در اینترنت از کار انداخت و صبح دوشنبه IPV6 را روشن نمود. در عوض مسیریاب‌ها و ماشین‌هایی که به IPV6 مجهز می‌شوند به مثابه جزایر مستقل با استفاده از تونل با یکدیگر مبادله داده می‌کنند و با افزایش این جزایر، در یکدیگر ادغام شده و جزیره بزرگتری پدید می‌آید. در نهایت تمام این جزایر به هم می‌پیوندند و اینترنت کاملا متحول می‌شود.

سرمایه گذاری حجیمی که از قبل بر روی مسیریاب‌های مبتنی بر IPV4 صورت گرفته، فرایند تغییر و تحول اینترنت را سال‌ها به تاخیر می‌اندازد. به همین دلیل تلاش زیادی صورت می‌گیرد تا این اطمینان حاصل شود که گذار از IPV4به IPV6 حتی الامکان بدون زحمت و گرفتاری انجام گیرد. برای کسب آگاهی بیشتر در خصوص IPV6 به مرجع (Loshin ,1999) مراجعه نمایید.

۲-۴-۳- NAT: ترجمه آدرس‌های شبکه

آدرس‌های IP کمیاب و ارزشمند هستند: یک ISP ممکن است یک بلوک آدرس با الگوی ۱۶(همان کلاس B سابق) و توانایی آدرس‌دهی ۶۵۵۳۴ ماشین میزبان، داشته باشد. اگر تعداد مشتریان این ISP از این تعداد بیشتر شود مشکل بهم می‌زند. برای مشتریان خانگی که از طریق خطوط تلفن متصل می‌شوند، راه حل این مشکل آن است که وقتی مشتری شماره گیری کرد و ارد شد به او موقتا یک آدرس IP پویا اختصاص داده شود و پس از پایان نشست و قطع ارتباط، این آدرس پس گرفته شود. در این روش شبکه‌ای با آدرس ۱۶ (کلاس B) می‌تواند حداکثر ۶۵۵۳۴ کاربر فعال داشته باشد که این تعداد حتی برای ISP با چند صد هزار مشتری نیز کفایت می‌کند. به محض آنکه یک نشست خاتمه یافت آدرس IP منتسب شده قبلی، به تماس گیرنده بعدی داده می‌شود. این استراتژی اگرچه برای یک ISP با تعداد متوسطی از کاربران خانگی به خوبی کار می‌کند ولی برای ISPهایی که به مشتریان اداری خدمات می‌دهند مفید نیست.

مشکل از اینجا ناشی می‌شود که مشتریان اداری انتظار دارند که حداقل در ساعات کاری روز خطی دائم و فعال on-line داشته باشند. امروزه، چه دفاتر کوچک دارای مثل یک آژانس مسافرتی با سه کارمند و چه شرکت‌های بزرگ که دارای تعداد زیادی کامپیوتر و شبکه محلی هستند، نیاز به خط دائم و فعال دارند. برخی از این کامپیوترها، PC کارمندان و برخی دیگر مثلا سرویس دهندههای وب هستند. عموما در هر LAN یک مسیریاب وجود دارد که از طریق یک خط اجاره‌ای (Leased) به ISP متصل شده است. چنین ساختاری متضمن آن است هر کامپیوتر آدرس PI خود را داشته باشد و به طور روزانه تغییرنکند. در نتیجه، تعداد کل کامپیوترهایی که در اختیار مشتریان اداری است نباید از تعداد آدرس‌های IP متعلق به ISP بیشتر شود. برای آدرس ۱۶/، حداکثر تعداد کامپیوترها ۶۵۵۳۴ است. برای یک ISP با دهها هزار مشتری اداری، این فضا سریعا اشباع می‌شود. آنچه که مشکل را حادتر می‌کند آن است که روز به روز بر تعداد مشترکین اینترنت از طریق مودم‌های کابلی ADSL افزوده می‌شود. ویژگی چنین سرویسی عبارت است از:(۱) کاربر یک آدرس IP دائم و ثابت می‌گیرد. (۲)

هزینه شماره گیری و اتصال ندارد (مگر یک هزینه ثابت ماهانه) بدین ترتیب اینگونه کاربران همیشه در شبکه حضور دارند. این موضوع، مشکل کمبود آدرس‌های IP را افزایش می‌دهد. در اینجا تخصیص موقت آدرس‌های IP (شبیه به مکانیزمی که برای کاربران تلفنی داشتیم) عملی نیست.

حتی از این هم پیچیده‌تر آنکه ممکن است کاربران ADSL و اینترنت کابلی دارای دو یا چند کامپیوتر در خانه باشند و تمام اعضای خانواده از طریق همین خط فعال و مشترک به ISP متصل شوند. یک راه حل آن است که تمام PCها از طریق یک LAN به هم متصل شده و با یک مسیریاب به ISP وصل شوند. از دیدگاه ISP شبکه این خانواده فرقی با یک دفتر اداری کوچک ندارد.

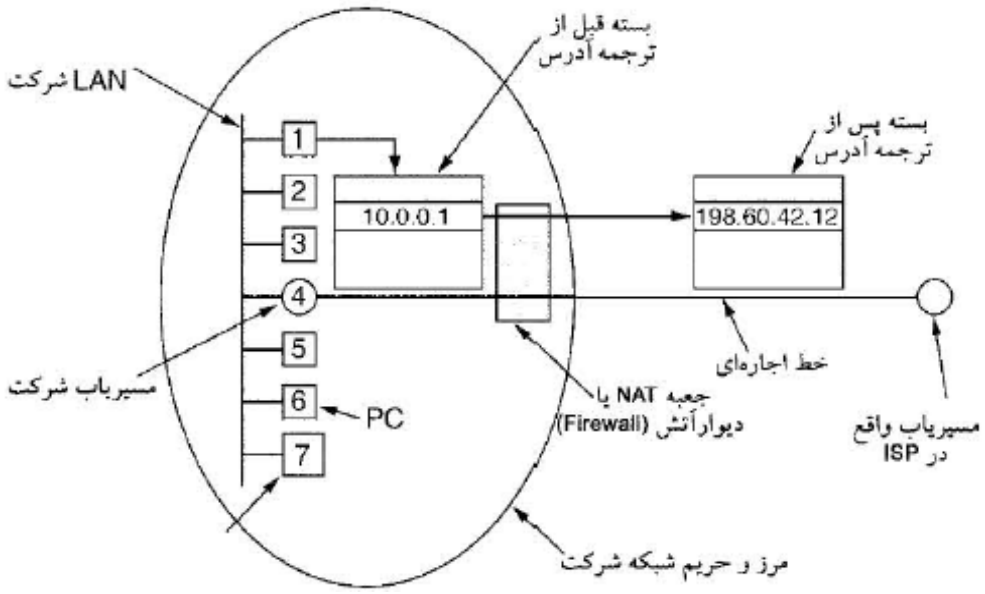
مشکل کمبود آدرس‌های IP یک مسئله تئوریک نیست که در آینده‌ای دور رخ بدهد. همین الان با این مشکل مواجه هستیم. راه حل طولانی مدت و همیشگی این منشکل آنست که به سوی IPV6 (که آدرس‌های آن ۱۲۸ بیتی است) حرکت نماییم ولیکن گذار از نسخه ۴ به نسخه ۶ به آهستگی صورت می‌گیرد و سال‌ها طول می‌کشد تا این تغییر به طور کامل انجام شود. در نتیجه بسیاری افراد احساس کردند که به یک راه حل سریع و کوتاه مدت نیاز است. این راه حل سریع، NAT (ترجمه آدرس شبکه) است که در RFC ۳۰۲۲ تشریح شده و در ادامه آنرا مختصرا بررسی می‌نماییم. برای کسب آگاهی بیشتر به مرجع (Dutcher ،۲۰۰۱) مراجعه نمایید.

ایده اصلی در NAT آن است که به هر شرکت یک یا تعداد کمی آدرس IP معتبر و جهانی اختصاص بدهیم. درون این شرکت، هر کامپیوتر دارای یک آدرس IP یکتا است که برای مسیریابی ترافیک داخلی بکار می‌آید. با این حال وقتی بسته‌ای بخواهد شرکت را ترک کرده و به ISP برود باید قبل از خروج ترجمه آدرس صورت بگیرد، برای آنکه این روش ممکن باشد سه محدوده از فضای آدرس IP جهت بکارگیری در شبکه‌های داخلی به صورت «خصوصی » (Private) تعریف شده است و شرکت‌ها می‌توانند به صورت دلخواه از آن‌ها استفاده کنند. نیازی به ثبت جهانی آن‌ها نیست، تنا قانون آن است که هیچ بسته‌ای نباید با چنین آدرسی بر روی انیترنت ظاهر شود. این سه محدوده رزرو شده عبارتند از:

10.0.0.0 – 10.255.255.255/8 (16,777,216 Hosts)
172.16.0.0 – 172.31.255.255/12 (1,048,576 Hosts)
192.168.0.0 – 192.168.255.255/16 (65535 Hosts)

در محدوده اول ۱۶۷۷۲۱۶ آدرس (به استثنای ۰ و ۱-) در دسترس است و عموما اکثر شرکت‌ها از آن استفاده می‌کنند هرچند نیازی به چنین تعداد آدرسی نداشته باشند.

عملکرد NAT در شکل زیر نشان داده شده است ماشین‌ها در درون شبکه دارای یک آدرس یکتا به فرم x.y.z.۱۰ هستند. ولیکن وقتی بسته‌ای بخواهد مرز شرکت را ترک کند. ابتدا باید از درون یک جعبه NAT (NAT BOX) عبور کرده و آدرس مبداء آن با آدرس IP حقیقی شرکت جانشین شود. مثلا در شکل زیر آدرس 10.0.0.1 با آدرس 198.60.42.1عوض شده است. اغلب « جعبه NAT » در یک « دیوار آتش»(Firewall) ادغام می‌شود تا این ابزار ضمن ترجمه آدرس، امنیت شبکه را نیز با نظارت دقیق بر ورود و خروج اطلاعات تضمین نماید. در فصل ۸ مفهوم «دیوار آتش» را بررسی خواهیم کرد. همچنین می‌توان « جعبه NAT » را در مسیریاب شرکت قرار داد. اکثر مسیریاب‌ها امروزی از فرآیند NAT پشتیبانی می‌کنند.



تا اینجا جزییات کمی از فرآیند NAT مطرح کرده‌ایم: وقتی پاسخ یک بسته برمی گردد(مثلا از سرویس دهنده وب) طبعا آدرس ماشین گیرنده پاسخ ۱۹۲.۶۰.۴۲.۱ است. سوال این است که جعبه NAT از کجا بداند که آدرس کدام ماشین داخلی را به جای آن قرار بدهد؟ مسئله اصلی در NAT همین نکته است. اگر فیلدی اضافی در سرآیند بسته IP وجود داشت می‌شد از آن برای درج آدرس واقعی گیرنده بسته بهره گرفت ولیکن در سرآیند بسته تن‌ها یک بیت بلااستفاده مانده است. همچنین می‌توان یک گزینه جدید (در فضای فیلد اختیاری Option) تعریف کرد تا آدرس حقیقی ماشین مبداء بسته را نگاه دارد ولی انجام این کار مستلزم آن است که کد نرم‌افزار IP در تمام ماشی‌ها و درکل اینترنت تغییر کند تا گزینه جدید به رسمیت شناخته شده و به درستی تعبیر شود. این راه حل نیز فرایند زمان بری است و مشکل را در کوتاه مدت حل نخواهد کرد.

آنچه که بطور واقعی اتفاق می‌افتد به نحو ذیل است: طراحان NAT بدین نتیجه رسیده بودند که اغلب بسته‌های IP در درون فیلد داده خود یک بسته TCP یا UDP حمل می‌کنند. اگر با پروتکل‌های UDP,TCP آشنا باشید، می‌دانید که هر دوی این پروتکل‌ها دارای سرآیندی برای بسته‌های خود هستند که دو فیلد «شماره پورت مبداء» و «شماره پورت مقصد» جزو آن‌هاست. در زیر اگرچه تمرکز ما بر پورت‌های TCp است ولی همین قضیه برای پورت‌های TCP است ولی همین قضیه برای پورت‌های UDP نیز صادق است. این پورت‌ها که اعداد صحیح ۱۶ بیتی است. مشخص می‌کنند که اتصال TCP از چه پروسه‌ای شروع و به چه پروسه‌ای ختم می‌شود. این شماره پورت‌ها فیلدهای لازم برای عملکرد NAT را فراهم آورده‌اند. هرگاه یک پروسه بخواهد یک اتصال TCP با یک پروسه راه دور برقرار کند یک شماره پورت بلا استفاده برای خود برمی گزیند. این پورت، اصطلاحا« پورت مبدا» نام دارد و به کد برنامه TCp تفیهم می‌کند که باید بسته‌های ورودی با این شماره پورت را برای او بفرستد. همچنین هر پروسه یک شماره پورت مقصد تعیین می‌کند تا مشخص شود که بسته‌ها باید به کدام پروسه در ماشین مقصد تحویل شود. شماره پورت‌های صفر تا ۱۰۲۳ برای سرویس دهندههای مشهور رزرو شده است. به عنوان مثال پورت شماره ۸۰ توسط سرویس دهندههای وب بکار گرفته شده است، لذا برنامه‌های مشتری Client براحتی با آن‌ها ایجاد ارتباط می‌کنند. کوتاه سخن آنکه، هر پیام خروجی از TCP دارای شماره پورت مبداء و شماره پورت مقصد است و این دو شماره پورت هویت پروسه‌های طرفین ارتباط را مشخص می‌نمایند.

تمثیلی از یک نمونه می‌تواند به فهم شماره‌های پورت کمک کند: یک شرکت را در نظر بگیرید که دارای یک شماره تلفن اصلی و واحد است. وقتی افراد با این شماره تماس می‌گیرند. بلافاصله اپراتور مربوطه از آن‌ها سوال می‌کند که کدام شماره داخلی مد نظر آن‌هاست، سپس خط داخلی را وصل می‌کند. شماره اصلی به مثابه آدرس IP است و شماره‌های داخلی، مشابه با شماره پورت هستند، پورت‌ها، ۱۶ بیت آدرس اضافی دیگر هستند که هویت پروسه گیرنده بسته‌ها را مشخص می‌نمایند.

با استفاده از فیلد «شماره پورت مبداء» می‌توان مشکل نگاشت آدرس‌ها در NAT را حل کرد. هرگاه بسته‌ای برای خروج از شبکه به NAT وارد شود، آدرس مبداء آن که به شکل 10.x.y.z است با آدرس IP حقیقی و معتبر شرکت عوض می‌شود. مضاف بر این فیلد شماره پورت مبدا TCPSource port با عددی عوض می‌شود که در حقیقت این عدد جدول ترجمه آدرس در جعبه NAT است. هر یک از زاویه‌های این جدول، آدرس IP اصلی و همچنین شماره پورت واقعی آن بسته را نگه می‌دارند. در آخر کد کشف خطای بسته TCP و بسته IP از نو محاسبه و در بسته قرار داده می‌شود.(چرا که هم فیلد شماره پورت و هم فیلد آدرس IP مبدا در جعبه NAT عوض می‌شود.) عوض کردن مقدار فیلد پورت مبدا (Source port الزامی است چرا که ممکن است بطور همزمان از دو ماشین به آدرس‌های 10.0.0.1 و 10.0.0.2 یک اتصال TCP اتفاقا با شماره پورت مبدا یکسان (مثلا ۵۰۰۰) ایجاد شود، لذا شماره پورت مبداء نمی‌تواند هویت واقعی پروسه ارسال کننده بسته‌ها را مشخص کند. وقتی بسته‌ای از طریق ISP به جعبه NAT وارد می‌شود ابتدا مقدار فیلد پورت مبداء استخراج شده و از آن به عنوان اندیس جدول نگاشت در جعبه NAT استفاده می‌شود. پس از پیدا شدن درایه متناظر آدرس IP داخلی و شماره اصلی پورت مبدا بسته استخراج شده و درون بسته قرار می‌گیرد. سپس این بسته از طریق مسیریاب داخلی شرکت، برای تحویل به آدرس 10.x.y.z مسیر طبیعی خود را طی می‌کند.

همچنین از NAT می‌توان برای تخفیف مشکل کمبود آدرس IP برای کاربران ADSL و کاربران کابلی بهره گرفت. هرگاه ISP بخواهد به هر یک از این کاربران آدرسی انتساب بدهد، از آدرسی در فضای 10.x.y.z بهره می‌گیرد. قبل از آنکه بسته‌های ماشین کاربران، ISP را ترک کنند و به اینترنت وارد شوند باید ابتدا وارد جعبه NAT شده و آدرس غیرحقیقی و محلی آن‌ها به آدرس واقعی متعلق به ISP نگاشته شود. در مسیر برگشت، عکس فرآیند نگاشت انجام می‌شود. بدین نحو ازدیدگاه اینترنت این ISP (و کاربران ADSL یا کابلی آن) دقیقا مثل یک شرکت بزرگ به نظر می‌رسند، هر چند تعداد آدرس‌هایی واقعی و معتبر ISP ناچیز است.

اگرچه این روش مشکل کمبود آدرس‌های IP را حل می‌کند ولیکن بسیاری از افراد در جامعه اینترنت از آن به عنوان کاری بی ارزش و مردود یاد می‌کنند. برخی از مخالفت‌های آنان را به اختصار ارائه می‌نماییم. اول آنکه Nat مدل معماری IP را نقض می‌کند چرا که در این مدل بیان شده که آدرس IP به صورت یکتا ماشینی واحد را درکل جهان مشخص می‌نماید. ساختار تمام نرم‌افزارهای اینترنت با تکیه بر این واقعیت بنیان گذاشته شده است. با NAT ممکن است هزاران ماشین از آدرس 10.0.0.1 استفاده کنند و می‌کنند.

دوم آنکه NAT اینترنت را از حالت «بدون اتصال» به شبکه‌ای «اتصال گرا» تبدیل می‌نماید. مسئله اینجاست که جعبه NAT باید اطلاعاتی را در خصوص نگاشت اتصال‌هایی که از آن می‌گذرند در خود نگاه دارد. نگهداری وضعیت هر اتصال

ویژگی شبکه‌های اتصال گراست و سنخیتی با شبکه‌های بدون اتصال ندارد. اگر جعبه NAT به ناگاه از کار بیفتد و جدول نگاشت آن از دست برود تمام اتصالات TCP برقرار شده از دست می‌رود. بدین ترتیب با وجود NAT، اینترنت به یک شبکه آسیب پذیر مدار مجازی تبدیل می‌شود.

سوم آنکه، NAT اصول بنیانی لایه بندی پروتکل‌ها را نقض می‌کند. لایه K نباید هیچ تصوری از آنچه که لایه K+1 در فیلد حمل داده از بسته او قرار می‌دهد، داشته باشد یا در آن دخالتی کند. اصل اساسی در معماری لایه به لایه آنست که تمام لایه‌ها مستقل از دیگری باشند. اگر مثلا زمانی TCP به نسخه TCP-2 ارتقاء یابد و سرآیند بسته‌ها تغییر کنند.(مثلا شماره پورت‌ها ۳۲ بیتی شوند)، NAT از کار خواهد افتاد ایده اصلی در پروتکل‌های لایه آن بوده که تغییر در یک لایه نیازی، به تغییر در لایه‌های دیگر نداشته باشد در حالیکه NAT این عدم وابستگی را از بین می‌برد.

چهارم آنکه پروسه‌ای اینترنت مجبور به استفاده از TCP یا UDP نیستند. اگر فرضا کاربری بر روی ماشین A تصمیم بگیرد برای محاوره و مبادله داده با کاربری بر روی ماشین B از یک پروتکل جدید در لایه انتقال استفاده کند(مثلا برای کاربردهای چند رسآن‌های)، وجود NAT منجر به عدم کارکرد آن برنامه کاربردی خواهد شد چرا که NAT نخواهد توانست فیلد پورت مبدا را به درستی پیدا کرده و از آن استفاده نماید.

پنج آنکه برخی از برنامه‌های کاربردی آدرس IP ماشین خود را در متن اطلاعات ارسالی قرار می‌دهند. گیرنده نیز این آدرس را استخراج کرده و از آن در جایی استفاده می‌کند. از آنجایی که NAT چیزی در مورد این آدرس‌های مخفی نمی‌داند فلذا قادر به تغییر آن‌ها نبوده و هرگونه تلاش برای استفاده از این آدرس‌های ناصحیح (در ماشین راه دور) با شکست مواجه می‌شود. FTP، یعنی استاندارد انتقال فایل در اینترنت به همین ترتیب عمل می‌کند و با وجود NAT از کار می‌افتد مگر آنکه اقدامات احتیاطی خاصی به عمل آید. به دلیل مشابه، پروتکل H,323 که برای تلفن اینترنتی کاربرد دارد(و در فصل هفتم به معرفی آن خواهیم پرداخت) با وجود NAT کار نخواهد کرد. البته می‌توان با تغییرات اصلاحی در NAT آن را بکار گرفت ولی این که با معرفی هر برنامه کاربردی جدید مجبور به اصلاح NAT شویم، اصلا ایده جالبی نیست.

ششم آنکه چون فیلد آدرس پورت مبداء، ۱۶ بیتی است. حداکثر ۶۵۵۳۶ ماشین را می‌توان به یک آدرس IP واحد نگاشت. این تعداد حقیقتا مقدار کمی است (گذشته از آن، ۴۰۹۶ شماره پورت نیز برای کاربردهای خاص کنار گذاشته شده اند)، ولیکن اگر تعداد آدرس‌های IP معتبر و جهانی که در اختیار ISP قرار دارد، بیش از یک باشد به ازای هر یک می‌توان ۶۱۴۲۰ ماشین را با آدرس‌های غیرحقیقی مدیریت کرد.

این مشکلات بهمراه مسائل دیگر NAT، در RFC ۲۹۹۳ تشریح شده است. عموما مخالفین NAT می‌گویند که با حل نازیبا و موقتی مسئله کمبود آدرس‌های IP، اصرار بر روی راه حل واقعی و نهایی که همانا رفتن به طرف IPV6 است، کم می‌شود و تعویق انداختن در این تغییر و تحول اصلا خوب نیست.

به طور خلاصه می‌توان گفت که قابلیت‌های این پروتکل جدید (IPv6) عبارتند از:

۱. فرمت سرآیند (Header) ساده‌تر شده است.

۲. اولویت دهی به بسته‌ها بر اساس محتوا

۳. پیکربندی خودکار (Auto Configuration)

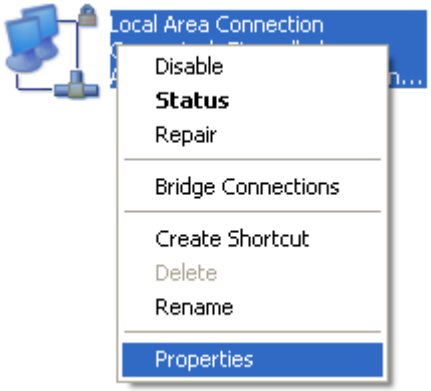
۴. IP سیار (Mobile IP)

۵. امنیت (Security)

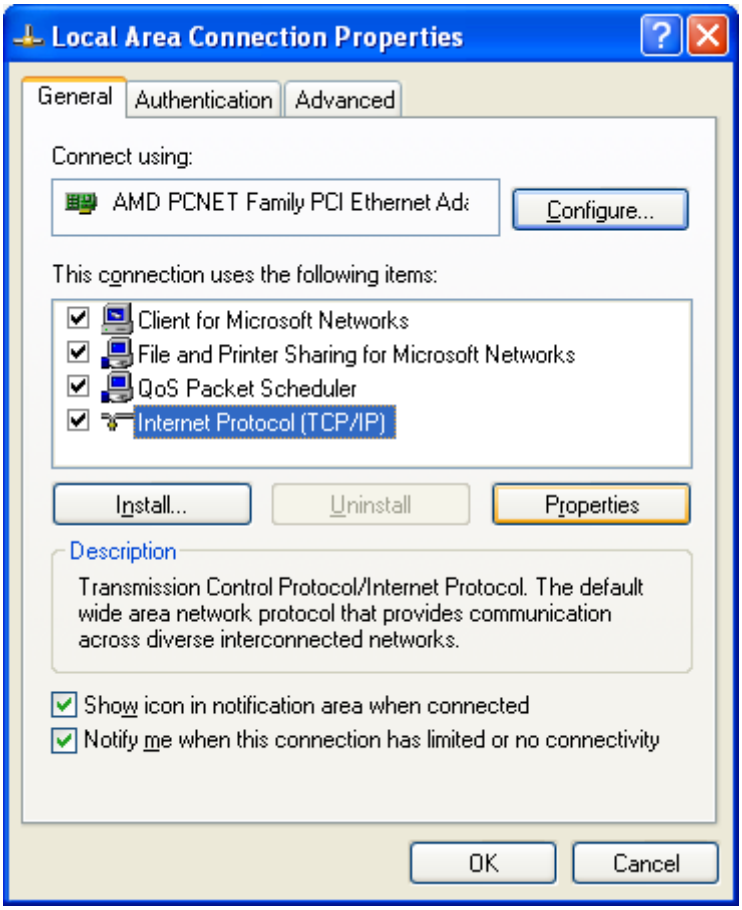
۶. کیفیت خدمات (Quality of Service)

۲-۵- تنظیم آدرس IP در ویندوز XP

در این بخش به آموزش نحوه تغییر آدرس IP در ویندوز XP می‌پردازیم. بدین منظور پس از اتصال به شبکه، وارد مسیر Control Panel ➔ Network Connections می‌شویم. سپس روی Connection ساخته شده راست کلیک کرده و سپس گزینه Properties را انتخاب می‌کنیم.

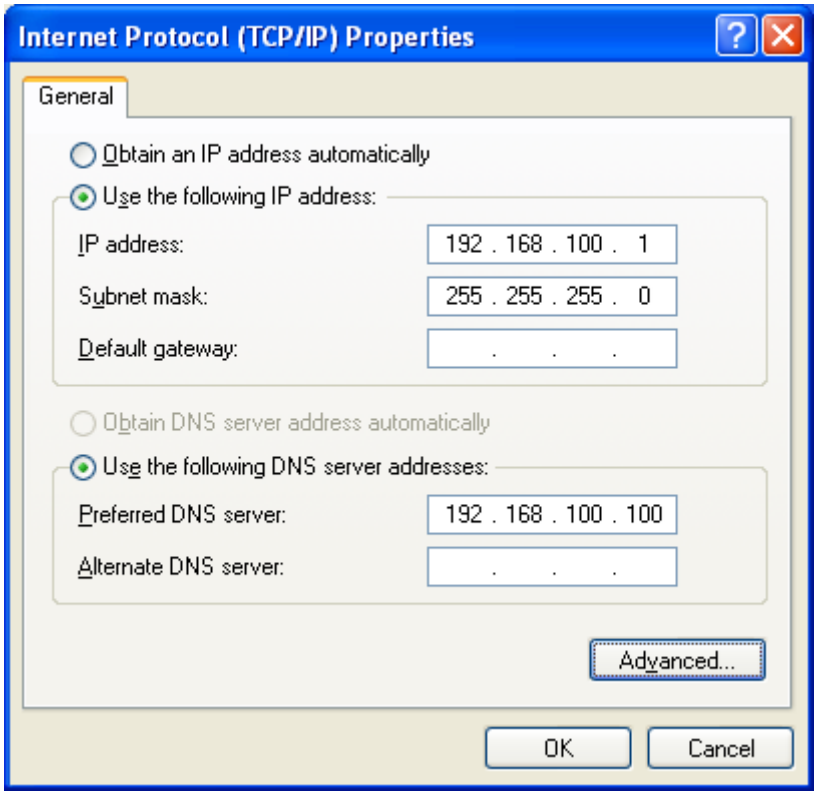


در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب نموده و سپس روی Properties کلیک نمایید.

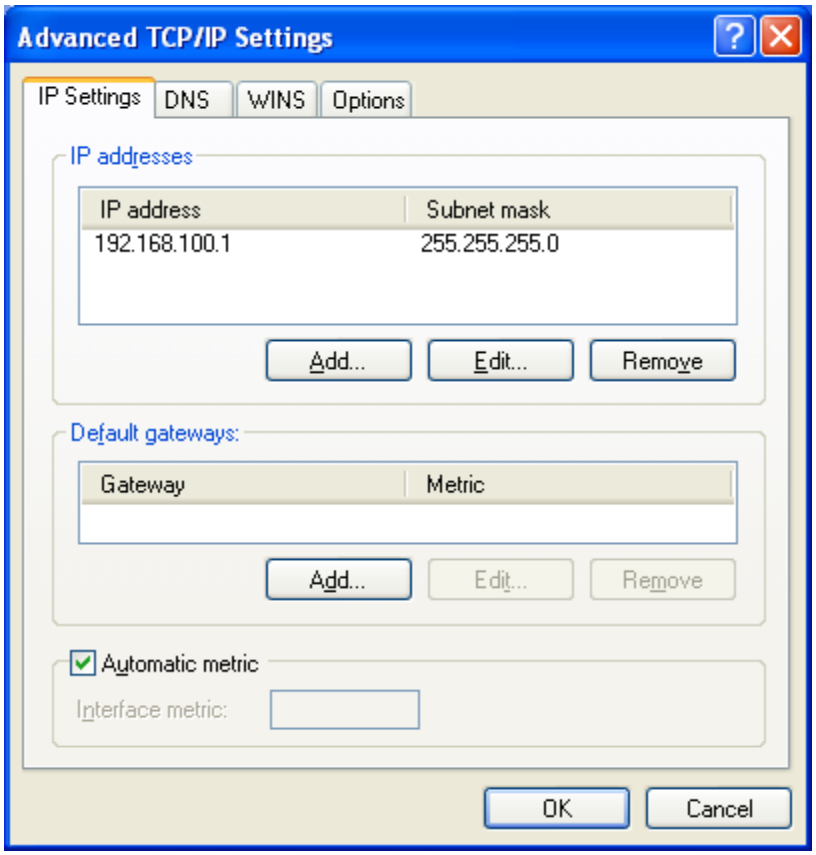


در صفحه باز شده، اگر می‌خواهید آدرس IP به صورت خودکار تعیین شده و کامپیوتر آدرس خود را از DHCP سرور بگیرد، گزینه **Obtain an IP address automatically** را انتخاب نمایید. اما اگر قصد دارید آدرس IP را دستی تعیین نمایید، گزینه **Use the following IP address** را انتخاب نمایید. سپس در قسمت **IP Address** آدرس IP را با توجه به نوع کلاس (A، B یا C) وارد نمایید. قسمت **Subnet Mask** با توجه به نوع آدرس IP تعیین می‌شود. ولی امکان تغییر آن نیز وجود دارد. در قسمت **Default Gateway** نیز دروازه پیش فرض که بسته‌های اطلاعاتی هنگام خروج از کامپیوتر به سمت آن می‌روند را تعیین نمایید. در قسمت **Preferred DNS server** نیز آدرس DNS Server که وظیفه تبدیل Host Name به IP Address عهده دارد را وارد نمایید. در قسمت **Alternate DNS server** نیز می‌توانید تعیین نمایید که اگر DNS Server اولیه جواب نداد، از یک DNS Server جایگزین استفاده نماید.

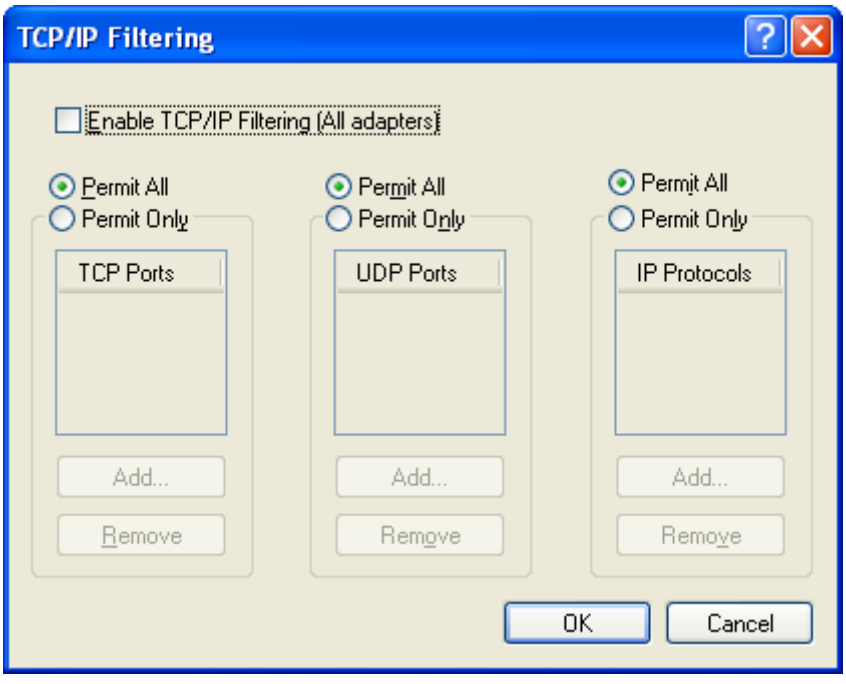
برای انجام تنظیمات پیشرفته تر، روی دکمه Advanced کلیک نمایید.



در صفحه باز شده امکان افزودن تنظیمات زیادتری وجود دارد. مثلاً در سربرگ IP Settings، می‌توان آدرس‌های IP یا دروازه‌های پیش فرض زیاد تری افزود. کامپیوتری که بیش از یک آدرس IP داشته باشد، به آن **Multi Home** می‌گویند. از طریق سربرگ‌های DNS و WINS نیز می‌توان تنظیماتی را در مورد سرویس‌های DNS یا WINS انجام داد که این مفاهیم را در فصول بعدی توضیح خواهیم داد.

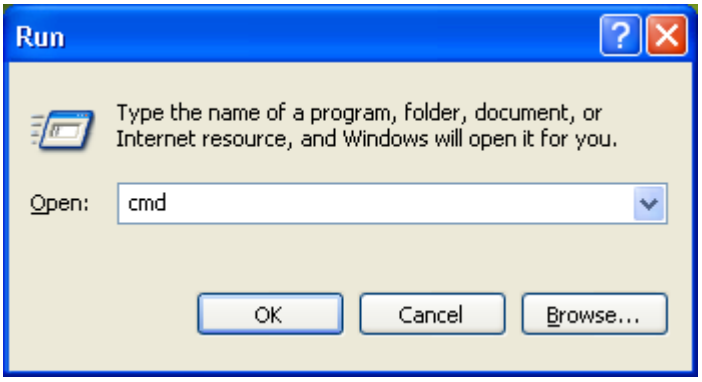


از طریق سربرگ Options نیز امکان مسدود کردن یا قابل اجرا کردن پورت‌های TCP یا UDP خاص یا پروتکل‌های IP وجود دارد. گزینه Permit All به معنای اجازه فعالیت به تمامی پورت‌ها وجود دارد. اما اگر گزینه Permit Only را انتخاب نمایید، می‌توانید فعالیت پورت هایی خاص را توسط کلیک روی دکمه Add تعیین نمایید و بدین ترتیب دیگر پورت هایی که Add نشده‌اند، مسدود خواهند شد.



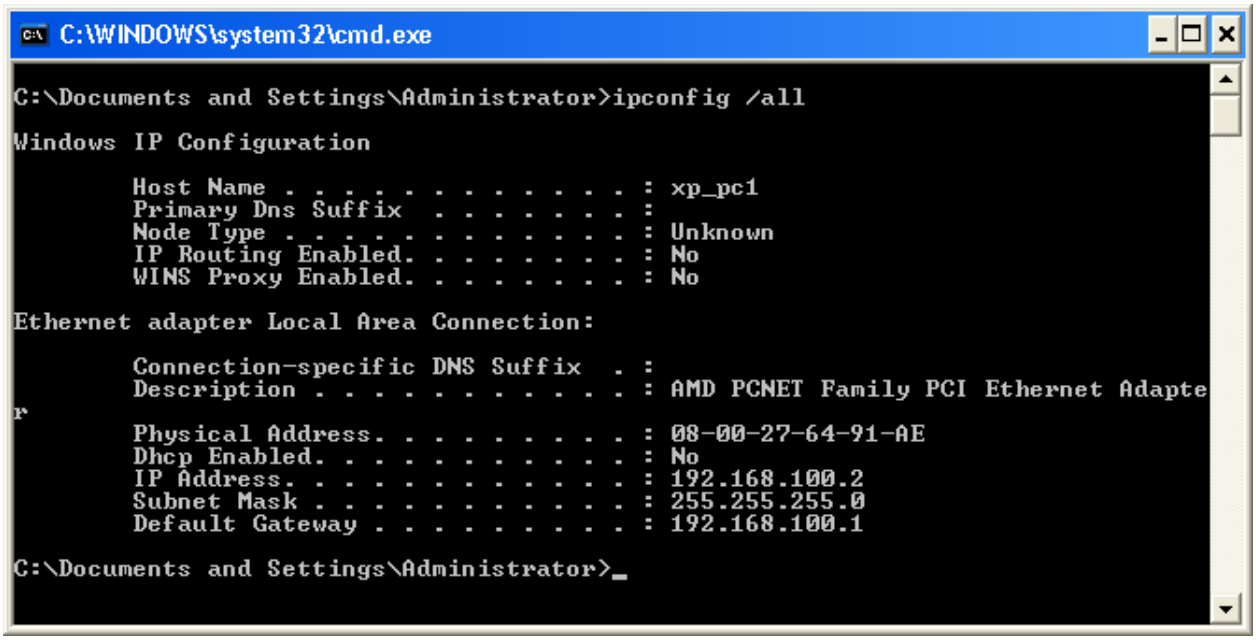
۲-۶- طریقه‌ی یافتن آدرس IP کامپیوتر

از منوی Start به گزینه Run می‌رویم و در آن تایپ می‌کنیم: cmd



سپس پنجره‌ای باز می‌شود. در آن پنجره تایپ می‌کنیم: ipconfig /all. بدین ترتیب می‌توانید بسیاری از تنظیمات کارت خود را مشاهده نمایید.

مشخصاتی ظاهر می‌شود که بیان گر کل مشخصات کارت‌های شبکه‌ی شما است. از میان اطلاعات ظاهر شده، ابتدا پیدا کنید که کدام کارت شما را به اینترنت متصل نموده، سپس در مقابل عبارت IP Address عددی را مشاهده خواهید کرد که بیان گر IPی شماست.



Subnet Mask -۲-۷

۲-۷-۱- مقدمه

اگر بخواهم خیلی ساده بگویم، Subnet Mask برای استخراج آدرس شبکه از داخل یک آدرس IP مورد استفاده قرار می‌گیرد. Subnet Mask، همانند آدرس IP، یک عدد چهار قسمتی ۳۲ بیتی است که همیشه همراه با آدرس IP به کار می‌رود و هر کدام از قسمت‌های آن، به قسمت متناظر از آدرس IP نگاشت می‌شود.

Subnet Mask مشخص میکند که محدوده شبکه ای که کامپیوترشما در آن قرار دارد کجاست. به عنوان مثال Subnet Mask با مقدار ۲۵۵.۲۵۵.۲۵۵.۰ شبکه ای مشتمل از ۲۵۴ کامپیوتر است، حال اگر Subnet با یک IP همراه باشد می توان فهمید IP کامپیوترهای آن شبکه در چه محدوده ای هست.مثلا ۱۹۲.۱۶۸.۰.۲۴ با subnet با مقدار ۲۵۵.۲۵۵.۲۵۵.۰ نشان می دهد کامپیوترهای آن شبکه میتوانند، IP هایی از محدوده ۱۹۲.۱۶۸.۰.۱ الی ۱۹۲.۱۶۸.۰.۲۵۴ داشته باشند. اولین آدرس یعنی ۱۹۲.۱۶۸.۰.۰ به عنوان IP آن شبکه مشخص می شود و آخرین آدرس یعنی ۱۹۲.۱۶۸.۰.۲۵۵ به عنوان IP، Broadcast در آن شبکه می باشد. برای وارد کردن Subnet Mask یک Device باید آن را در سطر بعد از IP وارد کنیم.

برای توضیح ساده‌تر که هر کامپیوتری در شبکه، یک آدرس دارد و آن آدرس، IP Address نامیده می‌شود. آدرس IP، خود شامل دو آدرس است. یکی **آدرس شبکه**‌ای که کامپیوتر در آن قرار دارد (Net ID) و دیگری **آدرس کامپیوتر** در آن شبکه (Host ID). مثلا اصفهان به عنوان آدرس شبکه و خیابان امام خمینی، کوچه نرگس، پلاک ۲۰۰ به عنوان آدرس کامپیوتر در آن شبکه. بر همین اساس دو کامپیوتر می‌توانند Host ID، یکسان داشته باشند ولی Net ID آن‌ها با یکدیگر متفاوت باشد. بر عکس آن نیز امکان پذیر است. یکسان بودن قسمت Net ID دو آدرس IP، بدین معناست که آن دو کامپیوتر در یک شبکه قرار دارند. به کمک Subnet Mask، می‌توان آدرس شبکه (Net ID) را از آدرس IP بیرون کشید.

هر کدام از کلاس‌های آدرس IP، Subnet Mask مربوط به خود را دارند.

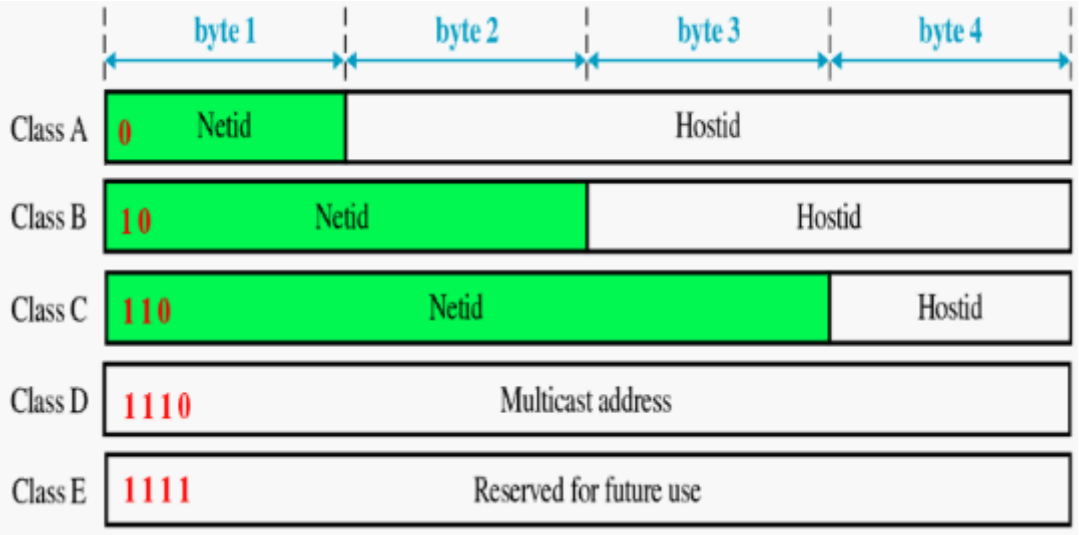
Subnet Mask در حالت Full Class، یکی از سه حالت زیر است:

کلاس	مبنای ۱۰	مبنای ۲
Class A	۲۵۵.۰.۰.۰	۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰
Class B	۲۵۵.۲۵۵.۰.۰	۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰
Class C	۲۵۵.۲۵۵.۲۵۵.۰	۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰

Subnet Mask در کلاس A به صورت ۲۵۵.۰.۰.۰ است. یعنی همان طور در بحث گذشته گفته شد، Net ID دارای هشت بیت است (هشت بیت اول) و بقیه بیت‌ها مربوط به Host ID می‌شوند.

Subnet Mask در کلاس B به صورت ۲۵۵.۲۵۵.۰.۰ است (زیرا دو بایت اول این کلاس، بیانگر آدرس شبکه است) و در کلاس C نیز به صورت ۲۵۵.۲۵۵.۲۵۵.۰ می‌باشد (زیرا سه بایت اول این کلاس، بیانگر آدرس شبکه است).

مجددا به شکل زیر دقت نمایید:



نحوه ساخت Subnet Mask، بدین صورت می‌باشد که در آدرس IP، به ازاء هر بیت Net ID، عدد ۱ و به ازاء هر بیت Host ID، عدد ۰ می‌گذاریم. سپس عدد به دست آمده را به مبنای ده می‌بریم. برای بردن به مبنای ده، عدد معادل هر کدام از چهار قسمت آدرس IP را جداگانه حساب می‌کنیم. برای مثال، کلاس A، ۸ بیت برای Net ID و ۲۴ بیت (۳ تا ۸ بیت) برای Host ID دارد. لذا داریم: ۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ که معادل آن در مبنای ده برابر با عدد ۲۵۵.۰.۰.۰ می‌شود.

۲-۷-۲- Subnet Mask چه کاربردی دارد و چگونه ساخته می‌شود؟

کاربرد Subnet Mask در ساخت کلاس‌های جدید شبکه است. فرض کنید که می‌خواهیم شبکه‌ای بسازیم که دارای 2^{12} شبکه و در هر شبکه دارای 2^{20} کامپیوتر باشد (۳۲=۱۲+۲۰ که آدرس IP ۳۲ بیتی است). لذا بایستی Subnet Mask را عوض کنیم. بدین منظور به تعداد بیت Net ID، عدد ۱ (در اینجا ۱۲ عدد) و به تعداد بیت Host ID، عدد ۰ (در اینجا ۲۰ عدد) می‌گذاریم. عدد به دست آمده در مبنای دو برابر ۱۱۱۱۱۱۱۱.۱۱۱۱۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ می‌باشد که معادل آن در مبنای ده می‌شود: ۲۵۵.۲۴۰.۰.۰. یعنی اگر Subnet Mask را به ۲۵۵.۲۴۰.۰.۰ تغییر دهیم، یعنی کلاس جدیدی در شبکه ساخته‌ایم که در این کلاس می‌توان $2^{12} - 2$ شبکه و در هر شبکه می‌توان $2^{20} - 2$ کامپیوتر داشت. لطفا به حالت خاص تمام بیت‌ها ۱ و تمام بیت‌ها ۰ نیز توجه نمایید که باعث می‌شود از تعداد کل، دو عدد کمتر شود.

اما اگر Subnet Mask را دادند و تعداد شبکه و تعداد کامپیوتر در هر شبکه را خواستند، بایستی ابتدا، هر کدام از چهار قسمت Subnet Mask را جداگانه به مبنای ۲ برد (Subnet Mask نیز مانند IP Address، چهار قسمت دارد و در مجموع ۳۲ بیتی است). سپس تعداد شبکه برابر با $2^{\text{تعداد یک}} - 2$ و تعداد کامپیوتر در هر شبکه برابر با $2^{\text{تعداد صفر}} - 2$ می‌باشد. دلیل تفریق عدد ۲، این است که حالت خاصی در Net ID و Host ID وجود دارد که نمی‌توان تمام بیت‌ها را ۰ یا ۱ گذاشت.

اگر این مطلب را متوجه شده باشید به راحتی می‌توانید Subnet Mask را در بقیه کلاس‌ها و دیگر حالت‌ها به راحتی برای خود تحلیل کنید.

سوال: اگر Subnet Mask برابر با ۲۵۵.۲۵۵.۲۵۲.۰ باشد، چند شبکه و در هر شبکه چند کامپیوتر داریم؟

پاسخ: معادل ۲۵۵.۲۵۵.۲۵۲.۰ در مبنای ۲، برابر با ۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۰۰.۰۰۰۰۰۰۰۰ است. لذا از آنجا که ۲۲ تا ۱ و ۱۰ تا ۰ داریم، لذا $2^{22} - 2$ تا شبکه و $2^{10} - 2$ تا کامپیوتر در هر شبکه داریم.

سوال: برای شبکه‌ای با ساختار زیر، یک Subnet Mask طراحی کنید؟

الف) داشتن ۱۰۰ شبکه

پاسخ: به دلیل، دو حالت خاصِ تمام بیت‌ها ۰ و تمام بیت‌ها ۱، به عدد ۱۰۰، دو واحد اضافه می‌کنیم که می‌شود ۱۰۲. از آنجا که $2^6 < 102 \leq 2^7$، لذا حداقل به ۷ بیت جهت آدرس‌دهی هر شبکه نیاز داریم. لذا Subnet Mask، دارای ۷ عدد ۱ و ۲۵ عدد ۰ است (۲۵ = ۷ – ۳۲). لذا

۱۱۱۱۱۱۱۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰.۰۰۰۰۰۰۰۰ = ۲۵۴.۰.۰.۰

ب) داشتن ۴۰۰ کامپیوتر در هر شبکه

پاسخ: به دلیل، دو حالت خاصِ تمام بیت‌ها ۰ و تمام بیت‌ها ۱، به عدد ۴۰۰، دو واحد اضافه می‌کنیم که می‌شود ۴۰۲. از آنجا که $2^8 < 402 \leq 2^9$، لذا حداقل به ۹ بیت جهت آدرس‌دهی هر کامپیوتر در شبکه نیاز داریم. لذا Subnet Mask، دارای ۹ عدد ۰ و ۲۳ عدد ۱ است (۲۳ = ۹ – ۳۲). لذا

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۰.۰۰۰۰۰۰۰۰ = ۲۵۵.۲۵۵.۲۵۴.۰

ج) داشتن ۱۶ کامپیوتر در هر شبکه

پاسخ: به دلیل، دو حالت خاصِ تمام بیت‌ها ۰ و تمام بیت‌ها ۱، به عدد ۱۶، دو واحد اضافه می‌کنیم که می‌شود ۱۸. از آنجا که $2^4 < 18 \leq 2^5$، لذا حداقل به ۵ بیت جهت آدرس‌دهی هر کامپیوتر در شبکه نیاز داریم. لذا Subnet Mask، دارای ۵ عدد ۰ و ۲۷ عدد ۱ است (۲۷ = ۵ – ۳۲). لذا

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۰۰۰۰۰ = ۲۵۵.۲۵۵.۲۵۵.۲۲۴

نکته‌ای که در مثال آخر درخور توجه است، اینکه اگر عدد ۲ را به تعداد ۱۶ کامپیوتر اضافه نمی‌کردیم، ۴ بیت برای Host ID کافی بود، یعنی Subnet Mask بصورت زیر می‌شد که اشتباه است:

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۰۰۰۰ = ۲۵۵.۲۵۵.۲۵۵.۲۴۰

۲-۷-۳- *تنظیم Subnet*

منبع: آزمایشگاه شبکه؛ مهندس ریاضی

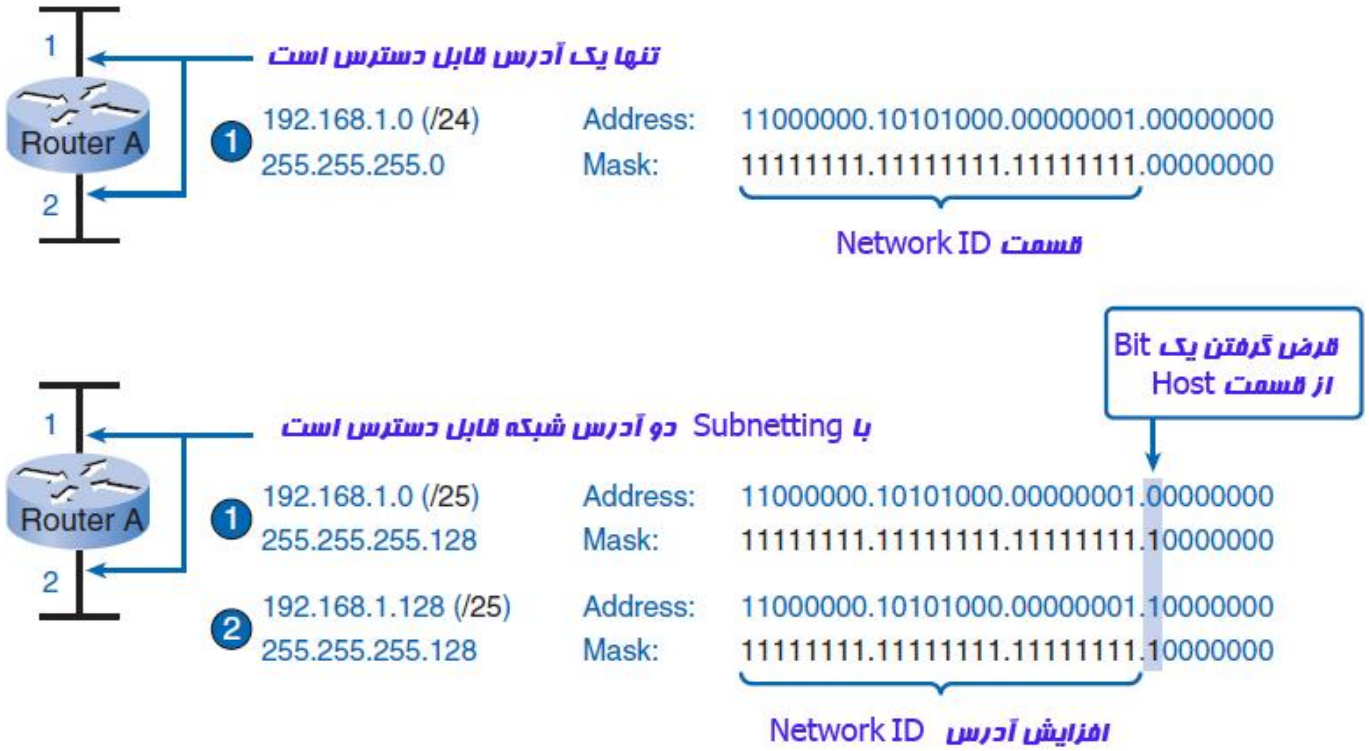
در یک سازمان جدا کردن بخشی از شبکه مثل بخش مالی یک شبکه برای حفظ امنیت از یک سو و از سوی دیگر نیاز به استفاده بهینه از IP برای اختصاص دادن به نودهای (Node) شبکه نیاز به استفاده از Subnetting را پی ریزی کرد. IP Address دارای دو بخش Network ID و Host ID می باشد. به عمل قرض دادن بیتهای Net ID به Host ID در اصطلاح Subnetting می گویند. در واقع عمل Subnetting بر روی Host Address صورت می گیرد. بیتهای Network ID همه یک می باشد و بیتهای host ID، می تواند صفر یا یک باشند. در حقیقت با تغییر در این بیتها IP Address های مختلف ساخته می شود. برای مثال، در آدرس (۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰) ۲۴ بیت اول جزء Network ID هستند و ۸ بیت آخر جزء Host ID می باشد. به عبارتی این محدوده می تواند یک سگمنت (Subnet) با حداکثر تعداد

۲-۲^۸ باشد. (هشت بیت که هر کدام ۲ حالت دارد و ۲ عدد از IP Addressها را نمی توان به Node اختصاص داد که یکی Network Address و دیگری Broadcast Address می باشد). توجه داشته باشید که در هر بار عمل Subnetting دو عدد از IPها غیرقابل استفاده می شوند و این به آن دلیل است که هر کدام از زیرشبکه‌ها دارای یک Network Address و یک Broadcast Address جدا می شوند و همانطور که گفته شد این دو عدد IP غیر قابل اختصاص هستند. و همچنین توجه داشته باشید برای اتصال زیرشبکه‌ها به یکدیگر از یک روتر بهره ببرید.

CIDR (Classless Inter-Domain Routing)

در این روش از نشانه slash (/) برای Subnetting Mask استفاده می شود و به معنای این است که چه مقدار از بیت‌ها یک است. بدیهی است که بیشترین مقدار ممکن ۳۲/ است، زیرا بیشترین بیت، ۳۲ است (آدرس IP، ۴ بایت یا ۳۲ بیت است). اما بخاطر داشته باشید که بیشترین subnet mask می‌تواند ۳۰/ باشد، است زیرا حداقل دو bits برای host bits نیاز است. بطور مثال در کلاس A، subnet mask برابر با ۲۵۵.۰.۰.۰ است. این بدین معنی است که اولین byte از subnet mask همگی یک است (۱۱۱۱۱۱۱۱). وقتی استناد به علامت slash (/) کنیم، بطور مسلم ۲۵۵.۰.۰.۰ برابر با ۸/ است زیرا هشت تا بیت با مقدار ۱ دارد. همچنین در کلاس B، defulf subnet mask برابر با ۲۵۵.۲۵۵.۰.۰ (11111111.11111111.00000000.00000000) است و همجنین میتوانیم تعریف کنیم ۱۶/، زیرا ۱۶ بیت یک است.

ساختن دو Subnet:



ما در این جا در دو طرف Router دو interface (رابط نقطه تعامل بین دو سیستم و یا گروه های کاری) داریم که به دو شبکه متصل است. ما یک آدرس 192.168.1.0 /24 داریم و می خواهیم دو subnet از آن درست کنیم. همانطور که ذکر شد فرمت یک IP در کلاس C به شکل ۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۰۰۰۰۰۰۰۰ می باشد. Subnet Mask نشان دهنده ارزش تعداد بیتهای جزء Network ID یک کلاس می باشد. در کلاس بالا Subnet mask برابر با ۲۵۵.۲۵۵.۲۵۵.۰ می باشد. حالا برای تغییر این کلاس به ۲ زیرشبکه یکی از بیتهای Host ID را یک می کنید تا IP به شکل

۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۱۱۱۱۱۱۱.۱۰۰۰۰۰۰۰ تبدیل شود. حالا ۲۵ بیت اول را جزء Network ID می گیریم و ۷ بیت آخر را جزء host ID که با این تعریف Subnetting در IP جدید برابر با ۲۵۵.۲۵۵.۲۵۵.۱۲۸ می باشد که می تواند ۲ الی ۲۷ گره را آدرس دهی کند. شما در شکل زیر می توانید این دو Subnetting را مشاهده کنید. که یکی عبارت است از 192.168.1.0 /25 و دیگری 192.168.1.128 /25 می باشد. حال با اختصاص یکی از محدوده‌ها به Subnet اول و اختصاص محدوده دیگر به Subnet دوم شبکه مذکور در هر Subnet ۲ الی ۲۷ آدرس خواهیم داشت.

ubnet	Network Address	Host Range	Broadcast Address
	192.168.1.0/25	192.168.1.1–192.168.1.126	192.168.1.127
	192.168.1.128/25	192.168.1.129–192.168.1.254	192.168.1.255

ساختن سه Subnet:



ما در این جا. یک آدرس 192.168.1.0 /24 داریم و می خواهیم سه subnet از آن درست کنیم. این مثال شبیه مثال قبل می باشد که با این تفاوت دو تا Bit از Host قرض گرفته می شود و به صورت زیر می شود. اگر دقت کنید خواهید فهمید که چهار subnet تولید شده است و یکی از آن‌ها در این مثال استفاده نمی شود. علت یک subnet $۲^{۲}$ اضافی که چهار می شود و باز به این نکته باید توجه داشته باشد که در هر subnet دوآدر س از Host Range کم می شود یکی برای Network Address و دیگری برای Broadcast Address می باشد.

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0/26	192.168.1.1–192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65–192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129–192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193–192.168.1.254	192.168.1.255

تمرین

زمانی که به شما IP address و Network Mask و Subnetwork Mask را بدهند. شما این توانایی را دارید که اطلاعاتی IP address را را تعیین کنید. این اطلاعات عبارت است از:

- Network address
- Network broadcast address
- Total number of host bits
- Number of hosts
- The subnet address of this subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet
- The maximum number of subnets for this subnet mask
- The number of hosts for each subnet
- The number of subnet bits
- The number of this subnet

فعالیت ۱: برای IP address داده شده، اطلاعات خواسته شده شبکه آن را تعیین کنید.

با توجه به:

Host IP Address	172.25.114.250
Network Mask	255.255.0.0 (/16)

اطلاعات زیر را پیدا کنید:

Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

مرحله ۱- Host IP address و network mask را به Binary تبدیل کنید.

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Network Mask	11111111	11111111	00000000	00000000
	255	255	0	0

مرحله ۲- تعیین Network Address.

۱. زیر Mask یک خط بکشید.

۲. IP Address و Network Mask را باهم ضرب منطقی کنید. در ضرب منطقی، ۱ و ۱، یک می شود و صفر با هر چیزی صفر می شود.

1 AND 1 = 1 , 0 AND 0 (or) 1 = 0

۳. نتیجه Network Address برای این Host، می‌شود: 172.25.0.0

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Subnet Mask	11111111	11111111	00000000	00000000
Network Address	10101100	11001000	00000000	00000000
	172	25	0	0

مرحله ۳- Broadcast Address برای Network Address تعیین کنید.

Mask جدا کننده قسمت Network از Host می باشد. Broadcast Address شبیه Network Address فقط با این تفاوت که در قسمت Host هر کجا Network Add، صفر است Broadcast یک می باشد.

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Subnet Mask	11111111	11111111	00000000	00000000
Network Address	10101100	11001000	00000000	00000000
	172	25	0	0

با شمارش تعداد بیت های host ما می توانیم تعداد کل، Hostها را برای این شبکه مشخص کنیم.

Host bits: 16 , Total number of hosts: 216 = 65,536

65,536 – 2 = 65534 (آدرس های Network و Broadcast کم می شود)

سوال ۵-۱: بااطلاعات فوق جدول زیر را پر کنید:

Host IP Address	172.25.114.250
Network Mask	255.255.0.0 (/16)
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

فعالیت ۲: با داشتن IP Address و Subnet Mask اطلاعات، Subnet را تعیین کنید.

با توجه به:

Host IP Address	172.25.114.250

Network Mask	255.255.0.0 (/16)
Subnet Mask	255.255.255.192 (/26)

سوال ۵-۲: اطلاعات زیر را پیدا کنید:

Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

مرحله ۱- Host IP address و network mask به Binary تبدیل کنید.

مرحله ۲- آدرس شبکه یا Subnet که به این host address تعلق دارد را تعین کنید.

۱. زیر Mask یک خط بکشید.

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
	11111111	11111111	11111111	11000000
Subnet Mask	255	255	255	192

۲. IP Address و Subnet Mask را با هم ضرب منطقی کنید. در ضرب منطقی ۱ و ۱، یک می شود و صفر با هر چیزی صفر می شود.

1 AND 1 = 1 , 0 AND 0 (or) 1 = 0

۳. نتیجه Subnet Address برای این Subnet می شود 172.25.114.192.

	172	25	114	250
IP Address	10101100	11001000	01110010	11111010
Subnet Mask	11111111	11111111	11111111	11000000
Subnet Address	10101100	11001000	01110010	11000000
	172	25	114	192

این اطلاعات را به جدول اضافه کنید:

Subnet Address for this IP Address	172.25.114.192

مرحله ۳: مشخص است که کدام بیت دراین آدرس مربوط به Network ID و کدام مربوط به Host ID می باشد.

۱. با یک خط موج دار (Major Divide (MD)) که جدا کننده اصلی یک های Network Mask که در مثال ما ۲۵۵.۲۵۵.۰.۰ می باشد، جدا کنید.

۲. با یک خط صاف (Subnet Divide (SD)) که جدا کننده Subnet یک های Subnet Mask جدا کنید.

			M.D.	S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← 10 bits →		

۳. نتیجه بیت های Subnet را مشخص می کند که از شمارش بیت های بین .M.D و .S.D بدست می آید. در این جا ۱۰ بیت می باشد.

مرحله ۴- تعیین محدوده های بیت برای subnetها و Host

۱. محدوده subnet عبارت است از بیت های بین .M.D. و .S.D که برای ایجاد آدرس Subnet این محدوده شامل ۱۰ بیت است که در حال افزایش می یابد.

۲. محدوده Host.ها عبارت است از بیت های بین .S.D و آخرین بیت که برای ایجاد آدرس Hostها، این محدوده شامل ۵ بیت است که در حال افزایش میابد.

			M.D.	S.D.	
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← subnet counting range →		←host→ counting range

مرحله ۵- تعیین محدوده از آدرس Hostها قابل دسترس در این subnet و آدرس broadcast دراین subnet

۱. برای بدست آوردن اولین Host در هر subnet باید همه بیت های IP Address تا خط .S.D را نوشته و از آنجا به بعد اولین شماره را که در اینجا ۰۰۰۰۰۱ می باشد به آن اضافه کرد که در این صورت اولین Host می شود: ۱۷۲.۲۵.۱۱۴.۱۹۳

۲. برای بدست آوردن آخرین Host در هر subnet باید همه بیت های IP Address تا خط S.D. را نوشته و از آنجا به بعد آخرین شماره منهای یک را که در اینجا ۱۱۱۱۱۰ می باشد به آن اضافه کرد که در این صورت آخرین Host می شود: ۱۷۲.۲۵.۱۱۴.۲۵۴

۳. برای بدست آوردن Broadcast Address در هر subnet باید همه بیت های IP Address تا خط S.D. را نوشته و از آنجا به بعد همه بیت‌ها را یک کرد که در اینجا ۱۱۱۱۱۱ می باشد به آن اضافه کرد که در این صورت Broadcast Address می شود: ۱۷۲.۲۵.۱۱۴.۲۵۵

		M.D.	S.D.		
IP Address	10101100	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10101100	11001000	01110010	11	000000
			← subnet → counting range		← host → counting range
First Host	10101100	11001000	01110010	11	000001
	172	25	114		193
Last Host	10101100	11001000	01110010	11	111110
	172	25	114		254
Broadcast	10101100	11001000	01110010	11	111111
	172	25	114		255

اطلاعات فوق را به جدول اضافه می کنیم:

Host IP Address 1	72.25.114.250
Major Network Mask	255.255.0.0 (/16)
Major (Base) Network Address	172.25.0.0
Major Network Broadcast Address	172.25.255.255
Total Number of Host Bits Number of Hosts	16 bits or 2^{16} or 65,536 total hosts 65,536 – 2 = 65,534 usable hosts
Subnet Mask	255.255.255.192 (/26)
Number of Subnet Bits Number of Subnets	
Number of Host Bits per Subnet Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

مرحله ۶- تعیین تعداد subnetها تعداد subnet ها

با استفاده تعداد بیت های محدوده subnet مشخص می شود که در اینجا ۱۰ بیت می باشد که شما می توانید آن را در فرمول زیر بگذارید: 2^n $۲^{۱۰} = ۱۰۲۴$

Number of Subnet Bits	10 bits
Number of Subnets (all 0s used, all 1s not used)	$2^{10} = 1024$ subnets

مرحله ۷- تعیین تعداد Host قابل استفاده در subnet

تعداد Hostها با استفاده تعداد بیت های محدوده Host مشخص می شود که در اینجا ۶ بیت می باشد که شما می توانید آن را در فرمول زیر بگذارید: 2^m-2 $2^6 – 2 = 64 – 2 = 62$ hosts per subnet

Number of Host Bits per Subnet	6 bits
Number of Usable Hosts per Subnet	26 – 2 = 64 – 2 = 62 hosts per subnet

۲-۸- Default Gateway

Default Gateway آدرسی (IP) است که نشان می‌دهد ما به کدام کامپیوتر متصل هستیم و از آن سرویس می‌گیریم. بنابراین در یک شبکه، تمام بسته‌های خارج شده از کامپیوتر، به سمت Default Gateway می‌رود و سپس Default Gateway در مورد آن بسته تصمیم گیری می‌کند. در مورد Default Gateway بعدا بیشتر صحبت خواهیم کرد.

۲-۹- Mac Address

مورد آخری که باقی می‌ماند این موضوع است، که با وجود اینکه مسیر یابی در شبکه بر اساس آدرس IP انجام می‌گیرد، اما سیستم‌ها قادر به تغییر آدرس IP خود هستند. با این وجود، شبکه از کجا تشخیص می‌دهد که هر آدرس IP مربوط به کدام کامپیوتر است؟ راه حل این است که هر کارت شبکه آدرسی سخت‌افزاری به نام Mac (Media Access Control) دارد که در تمام دنیا Unique (یکتا) است. آدرس سخت‌افزاری یا آدرس MAC، آدرس عددی است که به صورت سخت‌افزاری روی کارت واسط شبکه در کارخانه حک شده است. این نوع آدرس‌دهی موجب شناسایی منحصر به فرد کارت واسط شبکه در بین کارت‌ها می‌شود. طول این آدرس ۶ بایت است. استاندارد این آدرس‌دهی توسط انجمن مهندسان برق و الکترونیک (IEEE) تعیین شده است.

۲-۹-۱- دلیل استفاده از *MAC Address*

هر کامپیوتر موجود در شبکه، می‌بایست با استفاده از روش هایی خاص شناسائی گردد. برای شناسائی یک کامپیوتر موجود در شبکه، صرف داشتن یک آدرس IP به تنهایی کفایت نخواهد کرد. حتما علاقمند هستید که علت این موضوع را بدانید. بدین منظور، لازم است نگاهی به مدل معروف OSI (Open Systems Interconnect) و لایه‌های آن داشته باشیم:

- **مدل OSI**

الف) Network Layer (لایه سوم): آدرس IP در این لایه قرار دارد.

ب) Data Link Layer (لایه دوم): آدرس MAC در این لایه قرار دارد.

ج) Physical Layer (لایه اول): شبکه فیزیکی

همانگونه که مشاهده می‌نمائید، MAC Address در لایه Data Link (لایه دوم مدل OSI) قرار دارد و این لایه مسئول بررسی این موضوع خواهد بود که داده متعلق به کدامیک از کامپیوترهای موجود در شبکه است. زمانی که یک بسته اطلاعاتی (Packet) به لایه Data Link می‌رسد (از طریق لایه اول)، وی آن را در اختیار لایه بالائی خود (لایه سوم) قرار خواهد داد. بنابراین ما نیازمند استفاده از روش خاصی به منظور شناسائی یک کامپیوتر قبل از لایه سوم هستیم. MAC Address در پاسخ به نیاز فوق در نظر گرفته شده و با استقرار در لایه دوم، وظیفه شناسائی کامپیوتر قبل از لایه سوم را بر عهده دارد. تمامی ماشین‌های موجود بر روی یک شبکه، اقدام به بررسی بسته‌های اطلاعاتی نموده تا مشخص گردد که آیا MAC Address موجود در بخش "آدرس مقصد" بسته اطلاعاتی ارسالی با آدرس آنان مطابقت می‌نماید؟ لایه فیزیکی (لایه اول) قادر به شناخت سیگنال‌های الکتریکی موجود بر روی شبکه بوده و فریم هایی را تولید می‌نماید که در اختیار لایه Data Link، گذاشته می‌شود. در صورت مطابقت MAC Address موجود در بخش "آدرس مقصد" بسته اطلاعاتی ارسالی با MAC Address یکی از کامپیوترهای موجود در شبکه، کامپیوتر مورد نظر آن را دریافت و با ارسال آن به لایه سوم، آدرس شبکه‌ای بسته اطلاعاتی (IP) بررسی تا این اطمینان حاصل گردد که آدرس فوق با آدرس شبکه‌ای که کامپیوتر مورد نظر با آن پیکربندی شده است به درستی مطابقت می‌نماید.

۲-۹-۲- ساختار *MAC Address*

یک MAC Address بر روی هر کارت شبکه همواره دارای طولی مشابه و یکسان می‌باشند. (شش بایت و یا ۴۸ بیت). در صورت بررسی MAC Address یک کامپیوتر که بر روی آن کارت شبکه نصب شده است، آن را با فرمت مبنای شانزده (Hex)، مشاهده خواهید دید. مثلاً MAC Address کارت شبکه موجود بر روی یک کامپیوتر می‌تواند به صورت زیر باشد:

مشاهده MAC Address					
استفاده از دستور IPconfig /all و مشاهده بخش Physical address:					
A6	DB	79	BA	50	00
تعریف شده توسط تولید کننده			تعریف شده توسط IEEE با توجه به RFC 1700		

۳-۹-۲- مشاهده *MAC Address*

استفاده از دستور IPconfig /all در محیط Command Prompt و مشاهده بخش Physical address.

۴-۹-۲- قوانین تولید *Mac Address*

بر اساس قوانین تعریف شده توسط IEEE، زمانی که یک تولید کننده نظیر اینتل، کارت‌های شبکه خود را تولید می‌نماید، آنان هر آدرس دلخواهی را نمی‌توانند برای MAC Address در نظر بگیرند. در صورتی که تمامی تولید کنندگان کارت‌های شبکه بخواهند بدون وجود یک ضابطه خاص، اقدام به تعریف آدرس‌های فوق نمایند، قطعا امکان تعارض بین آدرس‌های فوق به وجود خواهد آمد. (عدم تشخیص تولید کننده کارت و وجود دو کارت شبکه از دو تولید کننده متفاوت

با آدرس‌های یکسان). حتما این سوال برای شما مطرح می‌گردد که MAC Address توسط چه افراد و یا سازمان هایی و به چه صورت به کارت‌های شبکه نسبت داده می‌شود؟ به منظور برخورد با مشکلات فوق، گروه IEEE، هر MAC Address را به دو بخش مساوی تقسیم که از اولین بخش آن به منظور شناسائی تولید کننده کارت و دومین بخش به تولید کنندگان اختصاص داده شده تا آنان یک شماره سریال را در آن درج نمایند. با این که MAC Address در حافظه کارت شبکه ثبت می‌گردد، برخی از تولید کنندگان به شما این اجازه را خواهند داد که با دریافت و استفاده از یک برنامه خاص، بتوانید بخش دوم MAC Address کارت شبکه خود را تغییر دهید.

فصل ۳

توپولوژی‌های شبکه

۳-۱- توپولوژی شبکه

توپولوژی شبکه تشریح کننده نحوه اتصال کامپیوترها در یک شبکه به یکدیگر است. به عبارت دیگر، الگوی هندسی استفاده شده جهت اتصال کامپیوترها، توپولوژی نامیده می‌شود. پارامترهای اصلی در طراحی یک شبکه، **قابل اعتماد بودن** و **مقرون به صرفه بودن** است. توپولوژی انتخاب شده برای پیاده سازی شبکه‌ها، عاملی مهم در جهت **کشف و برطرف نمودن خطا** در شبکه خواهد بود. انتخاب یک توپولوژی خاص نمی‌تواند بدون ارتباط با محیط انتقال و روش‌های استفاده از خط مطرح گردد. نوع توپولوژی انتخابی جهت اتصال کامپیوترها به یکدیگر، مستقیماً بر نوع محیط انتقال و روش‌های استفاده از خط تاثیر می‌گذارد. با توجه به تاثیر مستقیم توپولوژی انتخابی در نوع کابل کشی و هزینه‌های مربوط به آن، می‌بایست با دقت و تامل به انتخاب توپولوژی یک شبکه همت گماشت. عوامل مختلفی جهت انتخاب یک توپولوژی بهینه مطرح می‌شود. مهمترین این عوامل بشرح ذیل است:

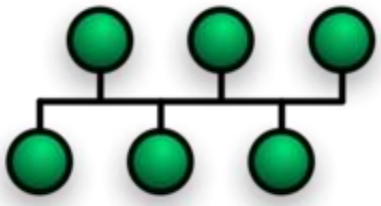
- **هزینه:** هر نوع محیط انتقال که برای شبکه LAN انتخاب گردد، در نهایت می‌بایست عملیات نصب شبکه در یک ساختمان پیاده سازی گردد. عملیات فوق فرآیندی طولانی جهت نصب کانال‌های مربوطه به کابل‌ها و محل عبور کابل‌ها در ساختمان است. در حالت ایده آل، کابل کشی و ایجاد کانال‌های مربوطه می‌بایست قبل از تصرف و بکارگیری ساختمان انجام گرفته باشد. به هرحال می‌بایست هزینه نصب شبکه بهینه گردد.

- **انعطاف پذیری:** یکی از مزایای شبکه‌های LAN، توانائی پردازش داده‌ها و گستردگی و توزیع گره‌ها در یک محیط است. بدین ترتیب، توان محاسباتی سیستم و منابع موجود در اختیار تمام استفاده کنندگان قرار خواهد گرفت. در ادارات همه

چیز تغییر خواهد کرد. (لوازم اداری، اتاق‌ها و...). توپولوژی انتخابی می‌بایست به سادگی امکان تغییر پیکربندی در شبکه را فراهم نماید. مثلاً سیستم را از نقطه‌ای به نقطه دیگر انتقال و یا قادر به ایجاد یک سیستم جدید در شبکه باشیم.

۳-۲- انواع توپولوژی (همبندی) شبکه

۳-۲-۱- آرایش خطی یا گذرگاهی (Bus)



شبکه‌ای که از همبندی گذرگاهی استفاده می‌کند معمولاً دارای یک کابل واحد (**معمولاً کابل Coaxial**) و بلند بوده که دستگاه‌های مختلف شبکه به آن متصل هستند (توسط T-Connector) و در هر واحد زمانی تنها یک رایانه امکان ارسال اطلاعات را دارد. در این روش کلیه رایانه‌های متصل به خط، اطلاعات ارسال شده را دریافت می‌کنند (**روش Broadcast**)؛ ولی تنها رایانه‌ای که آدرس مقصد بسته داده متعلق به او است این اطلاعات را ذخیره می‌نماید و بقیه رایانه‌ها از بسته صرف نظر می‌کنند. راه اندازی آن آسان است و به این منظور از یک رشته کابل کواکسیال استفاده می‌شود و هر سیستم به کمک یک **کانکتور** به شبکه متصل می‌شود. ابتدا و انتهای شبکه با **ترمیناتور** بسته می‌شود. اما نگهداری از آن با مشکلاتی همچون خطا یابی مشکل همراه است به همین دلیل تقریباً منسوخ شده است.

مزایای توپولوژی BUS

کم بودن طول کابل. به دلیل استفاده از یک خط انتقال جهت اتصال تمام کامپیوترها، در توپولوژی فوق از کابل کمی استفاده می‌شود. موضوع فوق باعث پایین آمدن هزینه نصب و ایجاد تسهیلات لازم در جهت پشتیبانی شبکه خواهد بود.

ساختار ساده. توپولوژی BUS دارای یک ساختار ساده است. در مدل فوق صرفاً از یک کابل برای انتقال اطلاعات استفاده می‌شود.

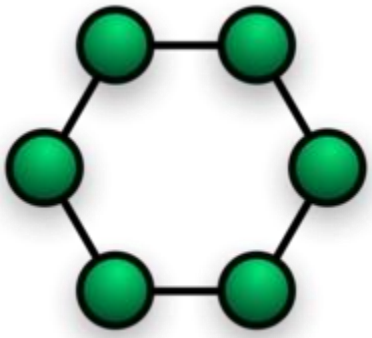
توسعه آسان. یک کامپیوتر جدید را می‌توان براحتی در نقطه‌ای از شبکه اضافه کرد. در صورت اضافه شدن ایستگاه‌های بیشتر در یک سگمنت، می‌توان از تقویت کننده هایی به نام Repeater استفاده کرد.

معایب توپولوژی BUS

مشکل بودن عیب یابی. با اینکه سادگی موجود در توپولوژی BUS امکان بروز اشتباه را کاهش می‌دهند، ولی در صورت بروز خطا، کشف آن ساده نخواهد بود. در شبکه هایی که از توپولوژی فوق استفاده می‌نمایند، کنترل شبکه در هر گره دارای مرکزیت نبوده و در صورت بروز خطا می‌بایست نقاط زیادی به منظور تشخیص خطا بازدید و بررسی گردند.

ایزوله کردن خطا مشکل است. در صورتی که یک کامپیوتر در توپولوژی فوق دچار مشکل گردد، می‌بایست کامپیوتر را در محلی که به شبکه متصل است رفع عیب نمود. در موارد خاص می‌توان یک گره را از شبکه جدا کرد. در حالتی که اگر **اشکال در محیط انتقال** باشد، تمام یک سگمنت می‌بایست از شبکه خارج گردد.

۳-۲-۲- آرایش حلقوی (Ring)



این همبندی توسط شرکت IBM اختراع شد و کلیه رایانه‌ها به گونه‌ای به یکدیگر متصل هستند که مجموعه آن‌ها یک حلقه را تشکیل می‌دهد. همیشه یک بسته کوچک با نام نشانه (Token) در داخل شبکه از یک رایانه به دیگری می‌رود، زمانی که یک رایانه اطلاعاتی جهت ارسال دارد، نشانه را در اختیار گرفته و از چرخش آن داخل شبکه جلوگیری می‌کند، تا زمانیکه نشانه توسط یک رایانه نگه داشته شده باشد، تمام رایانه‌های شبکه پذیرای اطلاعاتی خواهند بود که رایانه مالک نشانه ارسال می‌کند. که معایب این نوع توپولوژی این است که اگر قسمتی از کابل اصلی به علتی آسیب ببیند کل شبکه از کار می‌افتد و عیب یابی آن بسیار وقت گیر می‌باشد و از مزایای آن، می‌توان به **کم هزینه بودن و سادگی شبکه** اشاره کرد.

این توپولوژی بر روی نوع دستیابی تاثیر می‌گذارد. هر گره در شبکه دارای مسئولیت عبور دادن داده‌ای است که از گره مجاور دریافت داشته است. قبل از اینکه یک گره بتواند داده خود را ارسال نماید، می‌بایست به این اطمینان برسد که محیط انتقال برای استفاده قابل دستیابی است.

مزایای توپولوژی RING

کم بودن طول کابل. طول کابلی که در این مدل بکار گرفته می‌شود، قابل مقایسه با توپولوژی BUS نبوده و طول کمی را در بردارد. ویژگی فوق باعث کاهش تعداد اتصالات (کانکتور) در شبکه شده و ضریب اعتماد به شبکه را افزایش خواهد داد.

نیاز به فضائی خاص جهت انشعابات در کابل کشی نخواهد بود. به دلیل استفاده از یک کابل جهت اتصال هر گره به گره همسایه اش، اختصاص محل هایی خاص به منظور کابل کشی ضرورتی نخواهد داشت.

مناسب جهت فیبر نوری. استفاده از فیبر نوری باعث بالا رفتن نرخ سرعت انتقال اطلاعات در شبکه است. چون در توپولوژی فوق ترافیک داده‌ها در یک جهت است، می‌توان از فیبر نوری به منظور محیط انتقال استفاده کرد. در صورت تمایل می‌توان در هر بخش از شبکه از یک نوع کابل به عنوان محیط انتقال استفاده کرد. مثلاً در محیط‌های اداری از مدل‌های مسی و در محیط کارخانه از مدل فیبر نوری استفاده کرد.

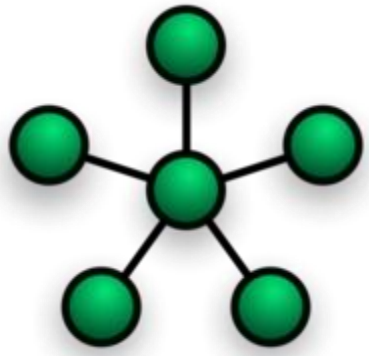
معایب توپولوژی RING

اشکال در یک گره باعث اشکال در تمام شبکه می‌گردد. در صورت بروز اشکال در یک گره، تمام شبکه با اشکال مواجه خواهد شد. و تا زمانیکه گره معیوب از شبکه خارج نگردد، هیچگونه ترافیک اطلاعاتی را روی شبکه نمی‌توان داشت.

اشکال زدایی مشکل است. بروز اشکال در یک گره می‌تواند روی تمام گره‌های دیگر تاثیر گذار باشد. به منظور عیب یابی می‌بایست چندین گره بررسی تا گره مورد نظر پیدا گردد.

تغییر در ساختار شبکه مشکل است. در زمان گسترش و یا اصلاح حوزه جغرافیائی تحت پوشش شبکه، به دلیل ماهیت حلقوی شبکه مسائلی به وجود خواهد آمد.

۳-۲-۳- آرایش ستاره‌ای (Star)



در این نوع همبندی کلیه رایانه‌ها به یک کنترل‌کننده مرکزی به نام میانگاه (Hub) و یا سوئیچ (Switch) متصل می‌شوند و هرگاه رایانه‌ای بخواهد با رایانه دیگری تبادل اطلاعات کند رایانه مبدا اطلاعات را به میانگاه/سوییچ ارسال نموده و اطلاعات از طریق آن به رایانه مقصد انتقال می‌یابد.

نکته ها:

۱) یک پیوند **نقطه به نقطه** را می‌توان به عنوان حالت خاصی از یک شبکه با آرایش ستاره در نظر گرفت. در نتیجه ساده ترین شبکه که براساس آرایش ستاره ساخته می‌شود را می‌توان یک گره که به یک گره دیگر از طریق یک پیوند نقطه به نقطه متصل است در نظر گرفت انتخاب یک گره به عنوان میانگیر به دلخواه ممکن است.

۲) ساده ترین نوع شبکه براساس آرایش ستاره علاوه بر شبکه توضیح داده شده در فوق، یک میانگیر (Hub) متصل به دو گره می‌باشد.

۳) با وجود این که می‌توان آرایش ستاره را با استفاده از یک هاب (Hub) یا سوئیچ (Switch) براحتی پیاده سازی نمود، اما به کار بردن یک کامپیوتر یا یک اشتراک مشترک نیز برای میانگیر کافی است. به هر حال چون در بیشتر نمایش‌های آرایش ستاره یکی از این ابزار ویژه نشان داده شده است، در نتیجه ممکن است این ابهام به وجوداید که حتماً باید از یکی از این ابزار استفاده نمود در حالی که مثلاً سه کامپیوتر متصل به یکدیگر بدون استفاده از هیچ ابراز ویژه‌ای نیز خود یک شبکه با آرایش ستاره است.

۴) شبکه‌های ستاره را می‌توان به صورت پخشی (Broadcast) با دسترسی چندگانه (Multicast) یا غیر پخشی با دسترسی چندگانه (NBMA) توصیف نمود که وابسته به توانایی میانگیر در ارسال سیگنال‌های موجود به تمام گره‌های تابع یا ارسال سیگنال به صورت جداگانه برای هر ارتباط است.

مزایای توپولوژی STAR

سادگی سرویس شبکه. توپولوژی STAR شامل تعدادی از نقاط اتصالی در یک نقطه مرکزی است. ویژگی فوق تغییر در ساختار و سرویس شبکه را آسان می‌نماید.

در هر اتصال یک دستگاه. نقاط اتصالی در شبکه ذاتاً مستعد اشکال هستند. در توپولوژی STAR اشکال در یک اتصال، باعث خروج آن خط از شبکه و سرویس و اشکال زدایی خط مزبور است. عملیات فوق تاثیری در عملکرد سایر کامپیوترهای موجود در شبکه نخواهد گذاشت.

کنترل مرکزی و عیب یابی. با توجه به این مسئله که نقطه مرکزی مستقیماً به هر ایستگاه موجود در شبکه متصل است، اشکالات و ایرادات در شبکه به سادگی تشخیص و مهار خواهند گردید.

روش‌های ساده دستیابی. هر اتصال در شبکه شامل یک نقطه مرکزی و یک گره جانبی است. در چنین حالتی دستیابی به محیط انتقال جهت ارسال و دریافت اطلاعات دارای الگوریتمی ساده خواهد بود.

معایب توپولوژی STAR

زیاد بودن طول کابل. به دلیل اتصال مستقیم هر گره به نقطه مرکزی، مقدار زیادی کابل مصرف می‌شود. هزینه کابل نسبت به تمام شبکه، کم است، ام تراکم در کانال کشی جهت کابل‌ها و مسائل مربوط به نصب و پشتیبانی آن‌ها، به طور قابل توجهی هزینه‌ها را افزایش خواهد داد.

مشکل بودن توسعه. اضافه نمودن یک گره جدید به شبکه مستلزم یک اتصال از نقطه مرکزی به گره جدید است. با اینکه در زمان کابل کشی پیش بینی‌های لازم جهت توسعه در نظر گرفته می‌شود، ولی در برخی حالات نظیر زمانی که طول زیادی از کابل مورد نیاز بوده و یا اتصال مجموعه‌ای از گره‌های غیر قابل پیش بینی اولیه، توسعه شبکه را با مشکل مواجه خواهد کرد.

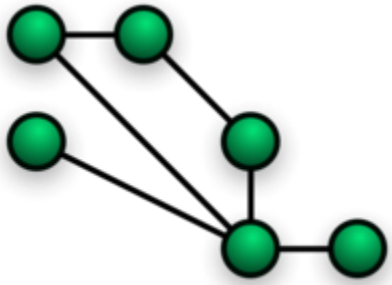
وابستگی به نقطه مرکزی. در صورتی که نقطه مرکزی (هاب یا سوئیچ) در شبکه با مشکل مواجه شود، تمام شبکه غیرقابل استفاده خواهد بود.

۳-۲-۴- *ستاره گسترش یافته*

اگر بین میانگیر (هاب یا سوئیچ) و گره‌ها (کامپیوتر ها)، تکرارکننده قرار دهیم تا مسافت قابل پوشش توسط میانگیر افزایش یابد، به آن آرایش **ستاره گسترش یافته** گفته می‌شود و اگر به جای تکرارکنندهها، میانگیر قرار داده شود، یک آرایش ترکیبی از ستاره سلسله مراتبی به وجود می‌آید که در بعضی از کتاب‌ها بین این آرایش و آرایش ستاره تفاوتی قائل نمی‌شوند.

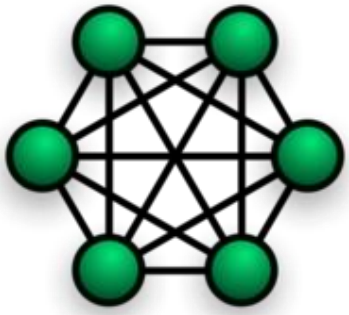
ماهیت تکرارکننده ها: در مواردیکه برای توسعه شبکه از تکرارکنندهها استفاده می‌گردد، ممکن است در ساختار شبکه تغییراتی نیز داده شود. موضوع فوق مستلزم بکارگیری کابل بیشتر و اضافه نمودن اتصالات مخصوص شبکه است.

۳-۲-۵- آرایش مشبک (Mesh)



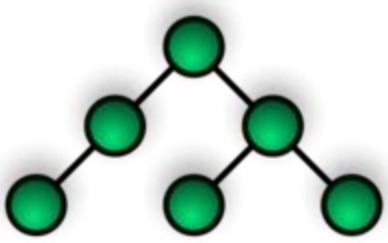
در این آرایش شبکه نظم مشخصی نداشته و هر یک از رایانه‌ها به یک یا چند رایانه دیگر متصل شده‌اند. این آرایش در واقع نسخه ناقص آرایش اتصال کامل است، لذا هزینه و پیچیدگی کمتری نسبت به روش مذکور دارد. از معایب این توپولوژی می‌توان به پیچیدگی و هزینه‌ی بالای آن اشاره کرد و چون شبکه گسترده است عیب یابی ان هم نسبت سخت می‌باشد. از مزایای این توپولوزی این است که اگر قسمتی از کابل قطع شود، کل شبکه از کار نمی‌افتد و انتقال اطلاعات به صورت دوبه دو می‌باشد؛ یعنی تمامی کامپیوترها بدون اینکه شبکه مشغول شود می‌توانند به یک دیگر اطلاعات ارسال و دریافت کنند که برای اینکه از توپولوژی Mesh بتوان از حداکثر استفاده را برد، از دستگاهی به نام روتر یا مسیر یاب استفاده می‌شود که کار این دستگاه این است که باعث می‌شود از خط‌ها یا مسیر هایی که خالی هستند ارسال اطلاعات انجام داد و در نتیجه این دستگاه باعث سرعت بخشیدن به ارسال اطلاعات می‌شود.

۳-۲-۶- آرایش اتصال کامل (Fully Connected)



در این آرایش تمام رایانه‌های شبکه مستقیماً به همدیگر متصل هستند. عمده ترین اشکال این روش پیچیدگی و هزینه بالای این اتصالات است. مزیت این روش ارسال سریع و بی واسطه اطلاعات از هر رایانه به رایانه دیگر می‌باشد. در این حالت اگر n کامپیوتر داشته باشیم، به $\frac{n\,(n-1)}{2}$ کابل نیاز خواهد بود.

۳-۲-۷- آرایش درختی (Tree) یا آرایش سلسله مراتبی



در آرایش درختی یک گره مرکزی (بالاترین سطح در سلسله مراتب) که ریشه نام دارد، به دو یا چند گره در سطحی پایین‌تر با استفاده از یک پیوند نقطه به نقطه متصل است (به عنوان مثال در سطح دو) و گره‌های سطح دو نیز به چندین گره در سطحی پایین‌تر متصل هستند (برای مثال در سطح سوم). گره مرکزی تنها گره‌ای است که هیچ گره‌ای در سطحی بالاتر از خود ندارد. سلسله مراتب درخت متقارن است یعنی تعداد گره‌های متصل به هر گره در سطح پایین‌تر عدد ثابت F است. عدد F به عنوان عامل شاخه بندی در درخت سلسله مراتب شناخته می‌شود.

نکته ها:

۱) یک شبکه مبتنی بر آرایش درختی فیزیکی حتماً باید حداقل سه سطح داشته باشد در غیر این صورت اگر دو سطح داشته باشد نشان دهنده آرایش ستاره است.

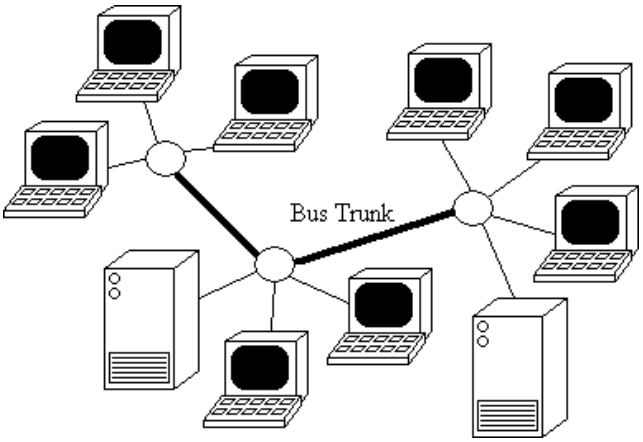
۲) اگر یک آرایش درختی عامل شاخه بندی برابر با یک داشته باشد این آرایش نشان دهنده آرایش خطی است.

۳) عامل شاخه بندی مستقل از تعداد کل گره‌ها است. اگر یک گره نیاز به درگاه هایی برای اتصال به گره‌های دیگر داشته باشد، می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد. در نتیجه تعداد درگاه‌های مورد نیاز وابسته به عامل شاخه بندی است و در نتیجه می‌توان تعداد درگاه‌ها را بدون توجه به تعداد کل گره‌ها کاهش داد.

۴) تعداد کل پیوندهای نقطه به نقطه در شبکه بر اساس آرایش درختی یکی کمتر از تعداد گره‌های شبکه می‌باشد.

۵) اگر نیاز به پردازش اطلاعات توسط گره‌ها در یک آرایش درختی فیزیکی باشد گره‌های سطح بالاتر باید پردازش بیشتری نسبت به گره‌های سطح پایین‌تر انجام دهند.

۳-۲-۸- آرایش ترکیبی (Hybrid)



آرایش ترکیبی نوعی از آرایش‌های شبکه است که از همبندی یک یا چند شبکه با آرایش‌های فیزیکی متفاوت و یا همبندی چندین شبکه که دارای آرایش فیزیکی یکسان است به وجود می‌آید و آرایش فیزیکی شبکه حاصل مشابه آرایش فیزیکی شبکه‌های اولیه نمی‌باشد (مثلاً آرایش فیزیکی شبکه‌ای که از همبندی چندین شبکه براساس آرایش فیزیکی ستاره بدست می‌آید ممکن است با توجه به نحوه اتصال شبکه‌ها به صورت ترکیبی از آرایش‌های ستاره و خطی یا ستاره و درختی باشد در حالی که اگر چندین شبکه با آرایش خطی توزیع شده به یکدیگر متصل گردند شبکه حاصل آرایش خطی توزیع شده را به خود خواهد گرفت)

این توپولوژی ترکیبی است از چند شبکه با توپولوژی متفاوت که توسط یک کابل اصلی بنام Backbone به یکدیگر مرتبط شده‌اند. توسط یک پل ارتباطی به نام Bridge به کابل Backbone متصل می‌شود.

فصل ۴

ساختارهای شبکه

۴-۱- دسته بندی شبکه

شبکه‌های کامپیوتری از لحاظ منطقی به دو دسته تقسیم می‌شوند:

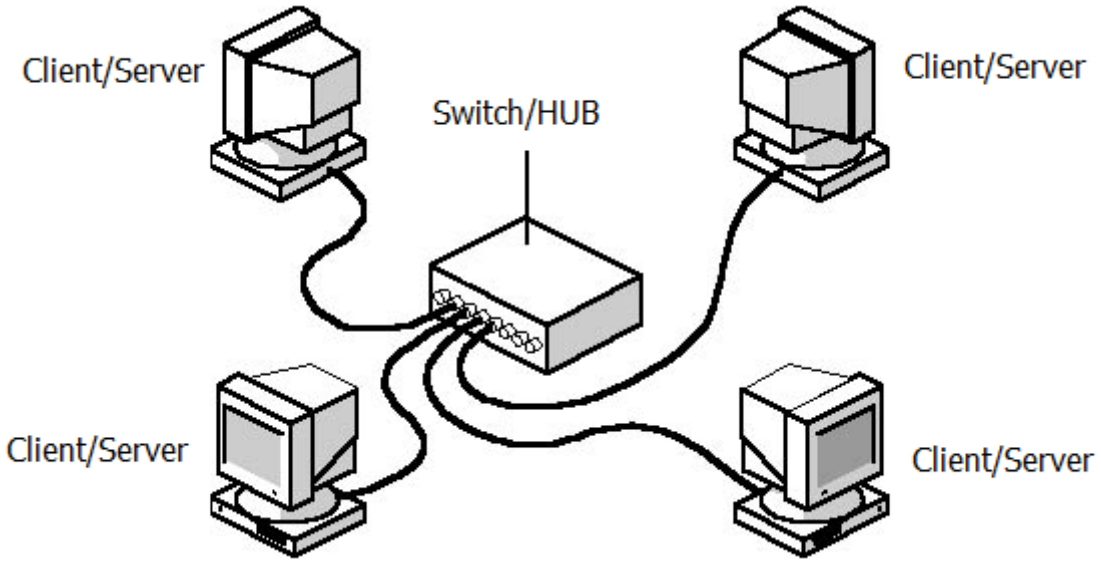
۱. **Work Group (Peer-To-Peer)**

۲. **Domain (Server Based یا Client - Server)**

در ادامه به معرفی هر کدام از روش‌های فوق خواهیم پرداخت:

۴-۲- گروه کاری (Work Group یا Peer-To-Peer)

شبکه‌های Peer-to-Peer: اگر در یک شبکه‌ای، سیستم‌ها همزمان علاوه بر ارایه‌ی سرویس، از سرویس‌های بقیه هم استفاده کنند یا به عبارتی به طور همزمان هم سرویس دهنده باشند و هم سرویس گیرنده، در این صورت می‌گوییم مدل سرویس دهی در شبکه به صورت Peer-to-Peer یا نظیر به نظیر است. (به اختصار PtP).



۴-۲-۱- معرفی مدل Peer-To-Peer (نظیر به نظیر)

در شبکه‌های نظیر به نظیر، سرویس دهنده اختصاصی وجود نداشته و سلسله مراتبی در رابطه با کامپیوترها رعایت نمی‌گردد. تمام کامپیوترها معادل و همتراز می‌باشند. هر کامپیوتر در شبکه هم به عنوان سرویس گیرنده وهم به عنوان سرویس دهنده ایفای وظیفه نموده و امنیت به صورت محلی و بر روی هر کامپیوتر ارائه می‌گردد.(هر کامپیوتری مسئول تعیین امنیت و سیاست‌های کاری خود می‌باشد). کاربر هر یک از کامپیوترها مشخص می‌نماید که چه داده‌ای بر روی کامپیوتر خود را به اشتراک قرار دهد. شبکه‌های نظیر به نظیر، Workgroup نیز نامیده می‌شوند. واژه Workgroup، نشان دهنده یک گروه کوچک (معمولاً ۱۰ و یا کمتر) از کامپیوترهای مرتبط با یکدیگر است. شبکه‌های نظیر به نظیر، گزینه‌ای مناسب برای محیط هایی با شرایط زیر می‌باشند:

۱. حداکثر تعداد کاربران ۱۰ و یا کمتر.
۲. کاربران منابع و چاپگرها را به اشتراک گذاشته و در این راستا، سرویس دهندگان خاصی وجود ندارد.
۳. امنیت متمرکز مورد نظر نباشد.
۴. رشد سازمان و شبکه بر اساس آنالیز شده، محدود باشد.
۵. این نوع شبکه ساده ترین و سریعترین روش شبکه سازی به ویژه در محیط‌های ویندوز می‌باشد که ابزار خاصی لازم نداشته و دارای مزایای زیر می‌باشد:
۶. هزینه راه اندازی و نگهداری پایین تر
۷. سرعت بیشتر در راه اندازی
۸. عدم نیاز به یک کامپیوتر مجزا به عنوان سرور

۴-۲-۲- شبکه سازی به روش نظیر به نظیر

برای ایجاد چنین شبکه‌ای تجهیزات زیر لازم است:

۱. کارت شبکه.
۲. کابل شبکه.
۳. سوکت از نوع استاندارد RJ45 که به سر کابل‌ها وصل می‌شود.
۴. میانگاه (Hub) یا سوئیچ (Switch) در صورتی که بیش از دو رایانه را بخواهید شبکه کنید.
۵. نرم‌افزار مناسب: به عنوان مثال سیستم عامل ویندوز به تنهایی می‌تواند کافی باشد.
۶. برخلاف حالت Client/Server در این روش کامپیوترهای شخصی می‌توانند بدون Server به هم متصل شده و تبادل اطلاعات نمایند. پس از نصب مراحل سخت‌افزاری فقط کافی است که سرویسهای شبکه را در ویندوز و یا سیستم عامل‌های دیگر همچون لینوکس نصب کرده و دیسک گردان ها (درایو ها) را به اشتراک گذارید.
۷. ادعا می‌شود که امنیت آن از روش Client/Server بالاتر است. (اما نقیض این صحبت را جلوتر اعلام خواهیم کرد)
۸. نیاز به Administrator (مدیر شبکه) ندارد.

یکی از کاربردهای شبکه نظیر به نظیر دسترسی یافتن از طریق رایانه شخصی خود به پرونده هایی است که در سخت دیسک رایانه دیگری قرار دارد.

به طور پیش فرض شبکه‌ها در ویندوز به صورت Workgroup هستند. برای مشاهده این قسمت ابتدا بر روی My Computer راست کلیک کرده و گزینه‌ی Properties را انتخاب کنید. سپس Tab دوم یعنی Computer Name را انتخاب کنید. در این قسمت می‌توانید با کلیک بر روی گزینه یChange تنظیمات را مشاهده کنید. در فیلد آخر که Workgroup است، می‌توانید یک نام دیگر برای گروهتان در نظر بگیرید و بدین صورت کامپیوترهای موجود در شبکه را دسته بندی کنید. مثلاً ۵ کامپیوتر در گروه IT و ۵ کامپیوتر در گروه Computer. این نکته بسیار مهم است که قرار گرفتن کامپیوترها در دسته‌های گوناگون، باعث مسدود شدن دسترسی به منابع آن‌ها نمی‌شود. در واقع ۲ کامپیوتر می‌توانند عضو دو گروه کاری متفاوت باشند اما در عین حال منابع یکدیگر را ببینند و در صورت لزوم ویرایش کنند. تنها فایده‌ی این دسته بندی‌ها، راحتی کار در هنگام در هنگام جست و جو است. به همین دلیل این نوع شبکه‌ها، جز شبکه هایی با امنیت پایین (Low Security) هستند. (نقیض ادعایی که در بالا مطرح شد.)

حال سوالی که مطرح می‌شود این است که آیا هر کامپیوتری با وصل کردن کابل شبکه می‌تواند وارد این چرخه شود و از منابع بقیه کامپیوترها استفاده کند؟

جواب منفی است. درست است گفتیم این شبکه‌ها **Low Security** هستند اما نه آنقدر. هر کامپیوتر بخشی به نام **LSD** (**L**ocal **S**ecurity **D**atabase) دارد که اطلاعات مربوط به کاربران را در خود ثبت می‌کند. LSD هر کامپیوتر نیز متعلق به خود آن کامپیوتر است. این قسمت از طریق راست کلیک کردن بر روی My Computer و انتخاب Manage و سپس Local Users and Groups قابل دسترسی است. در شبکه‌های Workgroup برای اتصال به کامپیوتر دیگر، باید یک User و Pass وارد کرد که این دو، همان نام کاربری و رمز عبور شما در ویندوز هستند. بعد از وارد کردن این اطلاعات، کامپیوتر میزبان در LSD خود به دنبال این اطلاعات می‌گردد و اگر User Name و Password شما در LSD آن موجود بود، به شما اجازه‌ی دسترسی می‌دهد.

نکته‌ای که اینجا وجود دارد این است که اگر شما در کامپیوتر خود دارای حساب Admin هستید اما در کامپیوتر دیگر به عنوان یک کاربر معمولی تعریف شده‌اید، در هنگام اتصال به آن کامپیوتر شما تنها اجازه‌ی دسترسی در حد یک کاربر معمولی را دارید. بنابراین در شبکه‌های Workgroup چیزی که اهمیت دارد کامپیوتر میزبان است و نه کامپیوتر میهمان.

۴-۲-۳- ویژگی ها

به نظر میرسد تنها ویژگی این نوع شبکه‌ها نصب و راه اندازی فوق آسان و همچنین هزینه‌ی کم باشد.

۴-۲-۴- معایب

۱. **Low Security:** در قسمت قبل چرایی پایین بودن امنیت این شبکه‌ها را باهم بررسی کردیم.
۲. **No Centralize Manage:** در این نوع شبکه‌ها، هیچ گونه مدیریت مرکزی وجود ندارد. به عنوان مثال در صورت اضافه شدن یک کاربر جدید، باید User و Pass آن را، در **LSD** همه‌ی کامپیوترها به صورت دستی وارد کرد و این یعنی فاجعه!

۳. **Limit 10:** تعداد کاربران در این نوع شبکه‌ها محدود است و بهترین حالت آن تا ۱۰ کاربر است. برای توضیح علت این موضوع باید کمی از بحث خارج شویم:

ما در شبکه‌ها ۳ نوع ارسال Packet داریم:

- **Uni Cast:** اگر آدرس مقصد Packet (داده ارسالی)، یکی باشد، نوع ارسال **Uni Cast** است.
- **Multi Cast:** اگر آدرس مقصد Packet، چند تا باشد، نوع ارسال **Multi Cast** است. در این روش فقط کامپیوتر هایی Packet را دریافت می‌کنند که Packet به سمت آن‌ها ارسال شده باشد.
- **Broad Cast:** اگر آدرس مقصد Packet، یک دسته باشد، نوع ارسال **Broad Cast** است. در این روش تمام کامپیوترها Packet را دریافت می‌کنند، اما فقط کامپیوتر هایی از Packet استفاده می‌کنند که آدرس آن‌ها در Packet قید شده باشد.

این نکته را هم داشته باشید که در شبکه‌ها، هیچ گاه در حالت عادی نمی‌توان از طریق نام یک کامپیوتر به آن کامپیوترها دسترسی پیدا کرد (نیاز به تبدیل نام کامپیوتر به آدرس IP وجود دارد).

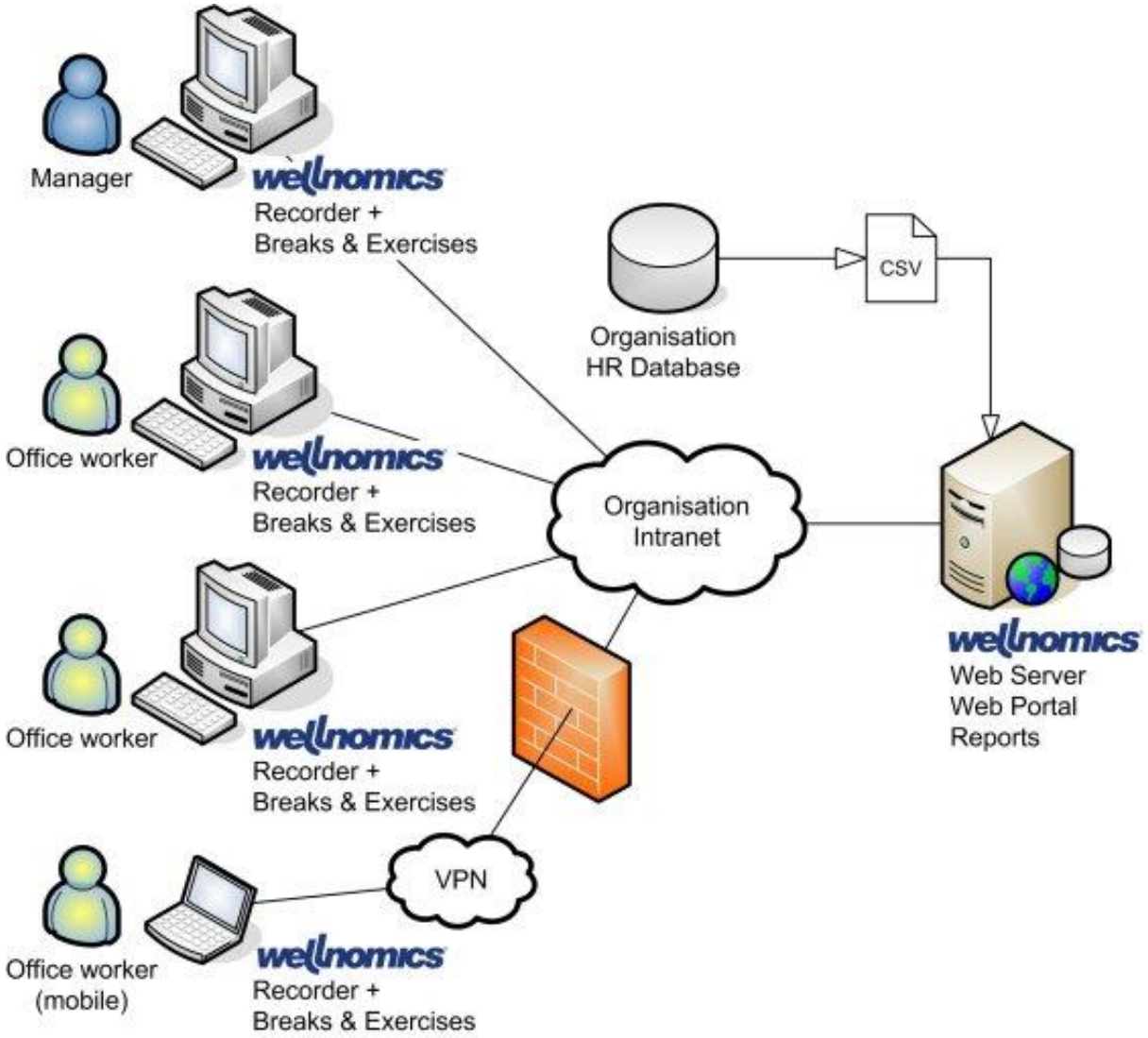
قضیه خیلی ساده شد. چون در شبکه‌های Work Group هیچ سرویسی برای تبدیل IP به اسم و بر عکس وجود ندارد، بنابراین برای اتصال به یک کامپیوتر، یک Packet به صورت Broad Cast به همه‌ی کامپیوترها ارسال می‌شود تا کامپیوتر مورد نظر شناسایی شود. به همین دلیل است که با افزایش تعداد کاربران، سرعت این نوع شبکه به شدت افت پیدا می‌کند.

۴-۳- مبتنی بر دامنه (Server Based یا Client – Server)

اگر در یک شبکه تعدادی از سیستم‌ها فقط در نقش سرویس دهنده و تعدادی فقط در نقش سرویس گیرنده ظاهر شوند در این صورت می‌گوییم که مدل سرویس دهی آن شبکه به صورت Server –Based (به اختصار SB) است.

۴-۳-۱- معرفی شبکه‌های Server Based یا Client-Server

به موازات رشد شبکه و افزایش کاربران و منابع موجود، یک شبکه نظیر به نظیر قادر به پاسخگوئی به حجم بالای تقاضا برای منابع اشتراکی نخواهد بود. به منظور هماهنگی با افزایش تقاضا و ارائه سرویس‌های مورد نیاز، شبکه‌ها می‌بایست از سرویس دهندگان اختصاصی استفاده نمایند. یک سرویس دهنده اختصاصی، صرفاً به عنوان یک سرویس دهنده در شبکه ایفای وظیفه می‌نماید (نه به عنوان یک سرویس گیرنده). شبکه‌های سرویس گیرنده – سرویس دهنده، به عنوان مدلی استاندارد برای برپاسازی شبکه مطرح شده‌اند. به موازات رشد یک شبکه (تعداد کامپیوترها متصل شده، فاصله فیزیکی، ترافیک موجود) می‌توان تعداد سرویس دهندگان در شبکه را افزایش داد. با توزیع مناسب فعالیت‌های شبکه بین چندین سرویس دهنده، کارآیی شبکه به طرز محسوسی افزایش خواهد یافت.



سرویس دهی در این شبکه توسط سیستم هایی صورت می‌گیرد که اصطلاحا سرویس دهنده یا Sever نامیده می‌شوند. سیستم هایی که از این سرویس استفاده می‌کنند اصطلاحا سرویس گیرنده یا Client نامیده می‌شوند. برای سرویس گیرندهها اصطلاح Workstation نیز به کار می‌رود.

۴-۴- تعاریف دیگری برای Client و Server

Server یا سِرور به برنامه‌ای رایانه‌ای گفته می‌شود که خدمات خود را به دیگر برنامه‌های رایانه‌ای (و کاربران آن ها) در همان رایانه یا در رایانه‌های دیگر ارائه می‌کند. به رایانه‌ای که چنین برنامه‌ای روی آن اجرا شود نیز Server گفته می‌شود.

Serverها انواع گوناگونی دارند، نظیر: Application Server, Web Server, Backup Server

Client، یک نرم‌افزار کاربردی یا سامآن‌های است که به خدمات یک سامانه رایانه‌ای دیگر به نام Server از طریق یک شبکه دسترسی دارد.

این عبارت نخستین بار برای نرم‌افزارهایی که قابلیت اجرای برنامه‌های مستقل خودشان را نداشتند اما می‌توانستند با رایانه‌های دور از طریق شبکه برهم کنش داشته باشند، به کار رفت. مدل Client-Server امروزه نیز در اینترنت به کار

می‌رود. مرورگرهای وب، Client هایی هستند که به Serverهای وب وصل می‌شوند و صفحات وب را برای نمایش بازیابی می‌کنند.

یک مدل Client-Server، یک ساختار توزیع شده است که وظایف یا حجم کار را بین سرویس دهندهها و سرویس گیرندهها تقسیم می‌کند.

یک معماری Client-Server یک معماری شبکه‌ای است که در آن هر رایانه یا پردازش روی شبکه یا یک Server است، یا یک Client. Serverها معمولاً رایانه‌های پرقدرت، یا پردازش هایی هستند که مختص انجام کار خاصی مانند مدیریت دیسک گردآن‌ها، چاپگرها، مدیریت ترافیک شبکه می‌باشند.

Clientها، ایستگاه‌های کاری یا رایانه‌های شخصی هستند که کاربران بر روی آن‌ها برنامه‌های کاربردی را اجرا می‌نمایند.Clientها به منابعی که Server به آن‌ها اختصاص می‌دهد مانند، پرونده، دستگاه‌ها، و قدرت پردازش اعتماد دارند. این معماری از سایر معماری‌ها در این نکته متمایز است که می‌تواند با استفاده از لایه‌ها ساختار دهی مطمئنی از سیستم به وجود آورد.

در سال‌های اخیر استفاده از یک Client کوچک (Thin Client) که حاوی منطق کاری نیست، و تنها عناصر رابط کاربری جهت اتصال به یک Server کاربردی که منطق کاری روی آن پیاده سازی شده باب شده است.

تنها نکته‌ای که در مورد Server Based بسیار حائز اهمیت می‌باشد، این است که Serverها مدیریت کل شبکه را بر عهده دارند و Clientها فقط کارهایی را می‌توانند انجام دهند که Server اجازه انجام آن کارها را به Clientها داده باشد. (و این یعنی مدیریت متمرکز). مثلاً کاربری مانند Ali، فقط اجازه دارد که از کامپیوترهای خاصی استفاده کند یا مثلاً حق دارد ماهیانه فقط ۱۰۰ عدد چاپ و آن هم با چاپگری خاص بگیرد.

فصل ۵

سیستم عامل شبکه

۵-۱- سیستم‌های عامل شبکه ای

هسته یک شبکه، سیستم عامل شبکه (Network Operating System) است. همانگونه که یک کامپیوتر بدون استفاده از سیستم عامل، قادر به انجام عملیات خود نخواهد بود، یک شبکه (چه شبکه Workgroup و چه شبکه Server Based) نیز بدون وجود یک سیستم عامل شبکه‌ای، قادر به انجام عملیات و ارائه سرویس‌های مربوطه نخواهد بود.

به عبارت دیگر، سیستم عامل شبکه، سیستم عاملی است که ویژه پشتیبانی از شبکه طراحی می‌شود. همین طور می‌توان گفت سیستم عامل شبکه، نرم‌افزاری است که یک شبکه و **ترافیک و صف پیام‌های روی آن** را کنترل می‌کند. همچنین **کنترل دسترسی چندین کاربر به یک منبع** بر روی شبکه نظیر یک فایل را بر عهده دارد و عملیات مدیریتی مهمی نظیر **کنترل امنیت** را میسر می‌سازد. سیستم عامل‌های مبتنی بر سرویس دهنده (Server) علاوه بر کارهای **نظارتی، امنیتی و مدیریتی**، پشتیبانی از کار در شبکه را نیز هم زمان برای چندین کاربر فراهم می‌کنند. سیستم عاملی که از وجود شبکه آگاه باشد (Network-Aware) می‌تواند امکان دستیابی به منابع شبکه را برای کاربران فراهم سازد. بر خلاف سیستم عامل‌های تک کاربره، این سیستم عامل‌ها باید درخواست‌های دریافتی از ایستگاه‌های کاری مختلف را پاسخ گویند و جزئیاتی چون دستیابی و ارتباطات شبکه، تخصیص و به اشتراک گذاشتن منابع، محافظت داده‌ها و کنترل خطاها را نیز مدیریت کنند. سر نام سیستم عامل‌های شبکه، NOS است که Network OS نیز نامیده می‌شود.

سیستم‌های عامل شبکه‌ای، سرویس‌ها و خدمات خاصی را در اختیار کامپیوترهای موجود در شبکه قرار خواهند داد:

۱. هماهنگی لازم در خصوص عملکرد دستگاه‌های متفاوت در شبکه به منظور حصول اطمینان از برقراری ارتباط در مواقع ضروری
۲. امکان دستیابی سرویس گیرندگان به منابع شبکه نظیر فایل‌ها و دستگاه‌های جانبی نظیر چاپگرها و دستگاه‌های فاکس
۳. اطمینان از ایمن بودن داده‌ها و دستگاه‌های موجود در شبکه از طریق تمرکز ابزارهای مدیریتی

۵-۲- ویژگی‌های یک سیستم عامل شبکه‌ای

یک سیستم عامل شبکه‌ای می‌بایست امکانات و خدمات اولیه زیر را ارائه نماید:

۱. ارائه مکانیزم‌های لازم به منظور برقراری ارتباط بین چندین دستگاه کامپیوتر برای انجام یک فعالیت خاص
۲. حمایت از چندین پردازنده
۳. حمایت از مجموعه‌ای (کلاستر) دیسک درایو – پردازنده – حافظه
۴. ارائه امکانات و سرویس‌های امنیتی در رابطه با حفاظت از داده‌ها و سایر منابع موجود در شبکه
۵. قابلیت اطمینان بالا
۶. تشخیص و برطرف نمودن خطا با سرعت مناسب

بر اساس نوع سیستم عامل، یک نرم‌افزار شبکه‌ای می‌تواند به سیستم عامل، اضافه و یا به صورت یکپارچه با سیستم عامل همراه باشد. نرم‌افزار سیستم عامل شبکه‌ای با مجموعه‌ای از سیستم‌های عامل رایج نظیر: ویندوز سرور (۲۰۰۰، ۲۰۰۳ و ۲۰۰۸)، ویندوز NT، ویندوز ۹۸، ویندوز ۹۵، و اپل مکینتاش، به صورت یکپارچه همراه می‌گردد.

البته نکته‌ای دیگر وجود دارد و آن اینکه برای راه اندازی یک شبکه، همیشه نیاز به داشتن سیستم عامل شبکه وجود ندارد. بلکه می‌توان از سیستم عامل‌های همه منظوره (مثل Windows XP) استفاده کرد. به خصوص در شبکه‌های Workgroup این موضوع بسیار مطرح می‌شود. اما اگر بخواهیم شبکه‌ای به مفهوم واقعی راه اندازی کنیم (Server Based)، عقل سلیم می‌گوید که برای Server از یک سیستم عامل شبکه استفاده کنیم.

برخی از سیستم عامل‌های معروف شبکه به قرار زیر است:

- Windows NT
- IBM AIX
- Sun Solaris
- Plan 9 from Bell Labs
- Inferno
- Windows 2000, 2003, 2008 Server
- Novell NetWare
- Linux (Red Hat, Ubuntu, SUSE, …)
- Unix… ،

۵-۳- معرفی انواع سرور

۵-۳-۱- *File Server*

یک سروری می‌باشد که از طریق آن می‌توان امکانی جهت مدیریت فایل‌ها و دسترسی کاربران مختلف شبکه در درایوهای مختلف به صورت متمرکز بر روی یک سرور در شبکه خود برقرار کنیم؛ که جهت راه اندازی این نوع سرور در Windows Server از طریق Manage Your Server option در منوی Administrative Tools اقدام می‌کنیم.

۵-۳-۲- *Print Server*

اگر بر روی کامپیوتری ویندوز سرور نصب شود و این کامپیوتر مجهز به یک دستگاه چاپگر باشد و این چاپگر جهت دسترسی کاربران مختلف شبکه به اشتراک گذاشته شود (Share)، این کامپیوتر می‌تواند به عنوان Print Server مورد استفاده قرار گیرد.

۵-۳-۳- Application Server

سروری می‌باشد که بر روی آن برنامه‌های تحت وب قرار می‌گیرد و از طریق سرویس IIS (Internet Information Services) این برنامه در اختیار کامپیوترهای دیگر شبکه قرار می‌گیرد.

تعریف دیگری نیز وجود دارد و آن اینکه رایانه‌ای است که نرم‌افزارهای کاربردی را به درخواست کاربران برای آن‌ها اجرا کرده و نتایج حاصل از اجرا را روی رایانه خودشان نمایش می‌دهد. هسته‌ی مرکزی روی سرویس دهنده است و نه سرویس گیرنده. در اینجا سرویس گیرنده تنها یک درخواست کننده برای اجرای عمل است.

دلایل استفاده از Application Server:

- امکانات سخت‌افزاری سرویس گیرنده ممکن است برای اجرای مستقیم برنامه کافی نباشد، مانند دستگاه‌های ATM
- نیاز به مدیریت بیشتر و کنترل نرم‌افزار ها

۵-۳-۴- Terminal Server

توسط این سرویس می‌توان به صورت Remote یا از راه دور به سرور متصل شده و به مدیریت مربوطه را انجام دهیم و یا برنامه‌ای تحت شبکه را بدین طریق و با استفاده از این سرویس اجرا نمود.

۵-۳-۵- VPN Server / Remote Server

توسط این سرورها می‌توانیم به کاربران مختلف جهت متصل شدن به صورت راه دور (Remote) به شبکه داخلی مجوز هایی را بدهیم و یا با استفاده از VPN (Virtual Private Network) ارتباطی امن بین دو نقطه ایجاد کنیم. (با کمک پروتکل‌های PPTP، L2TP، SSTP و...)

۵-۳-۶- DNS Server

سروری می‌باشد که کار Name Resolution را برای ما انجام می‌دهد و وظیفه آن تبدیل IP به اسم و بالعکس می‌باشد.

۵-۳-۷- DHCP Server

DHCP مخفف Dynamic Host Configuration Protocol می‌باشد. این سرور از طریق محدوده IP که بر روی آن تعریف می‌شود به صورت اتوماتیک به کلاینت‌ها IP می‌دهد و بسیاری کارهای دیگر که به جای خود به آن اشاره خواهیم کرد. در ضمن این سرویس حتما باید بر روی کامپیوتری که نسخه سرور دارد نصب شود.

۵-۴- ویندوز سرور ۲۰۰۳

سیستم عامل ویندوز سرور ۲۰۰۳، امکانات گسترده و پیشرفته‌ای را در اختیار کاربران قرار می‌دهد:

- **Multitasking:** با استفاده از ویژگی فوق، کاربران قادر به اجرای چندین برنامه به صورت همزمان بر روی یک سیستم می‌شوند. تعداد برنامه هایی که یک کاربر قادر به اجرای همزمان آنان خواهد بود به میزان حافظه موجود بر روی سیستم بستگی خواهد داشت.
- **Memory Support:** به منظور انجام عملیات مربوط به برنامه هایی که در محیط ویندوز ۲۰۰۳ اجراء می‌گردند، به میزان مطلوبی از حافظه، نیاز خواهد بود. برای اجرای چندین برنامه به صورت همزمان و یا اجرای برنامه هایی که میزان بالائی از حافظه را نیاز دارند، ویندوز ۲۰۰۳ امکان حمایت تا ۶۴ و ۱۲۸ گیگابایت را فراهم می‌نماید.

- **Symmetric Multiprocessing:** سیستم‌های عامل از ویژگی فوق، به منظور استفاده همزمان از چندین پردازنده استفاده می‌نمایند. بدین ترتیب کارآیی سیستم بهبود و یک برنامه در محدوده زمانی کمتری اجراء خواهد شد. ویندوز ۲۰۰۳، امکان حمایت (با توجه به نوع نسخه) از حداکثر ۳۲ پردازنده را فراهم می‌نماید.
- **Plug & Play:** با استفاده از ویندوز ۲۰۰۳، دستگاه‌هایی از نوع PNP به سادگی نصب می‌گردند. دستگاه‌های PNP، دستگاه‌هایی هستند که پس از اتصال به سیستم، بدون نیاز به انجام فرآیندهای پیچیده، نصب خواهند شد. پس از اتصال چنین دستگاه‌هایی، ویندوز ۲۰۰۳ به صورت اتوماتیک آنان را تشخیص و عناصر مورد نیاز را نصب و پیکربندی مربوطه را انجام خواهد داد.
- **Clustering:** ویندوز ۲۰۰۳، امکان گروه بندی مستقل کامپیوترها را با یکدیگر و به منظور اجرای یک مجموعه از برنامه‌ها فراهم می‌نماید. این گروه به عنوان یک سیستم برای سرویس گیرندگان و برنامه‌ها در نظر گرفته خواهد شد. **چنین گروه بندی، Clustering نامیده شده و گروه هایی از کامپیوترها را کلاستر می‌گویند.** این نوع سازماندهی کامپیوترها، باعث برخورد مناسب در صورت بروز اشکال در یک نقطه می‌گردد. در صورتیکه یک کامپیوتر دچار مشکل گردد، کامپیوتر دیگر در کلاستر، سرویس مربوطه را ارائه خواهد داد.
- **File System:** ویندوز ۲۰۰۳، از ۳ نوع مختلف سیستم فایل (قدیمی و جدید) حمایت می‌کند: FAT (File Allocation Table)، FAT32 و NTFS (New Technology File System). در صورتی که نیازی به استفاده از قابلیت‌های بوت دوگانه (راه اندازی سیستم از طریق دو نوع متفاوت سیستم عامل با توجه به خواسته کاربر) وجود نداشته باشد، ضرورتی به استفاده از سیستم فایل FAT و یا FAT32 وجود نخواهد داشت. NTFS، سیستم فایل پیشنهادی برای ویندوز ۲۰۰۳ بوده و امکانات امنیتی مناسبی را ارائه می‌نماید. ویندوز ۲۰۰۳، با استفاده از سیستم NTFS امکانات متعددی نظیر: بازیافت سیستم فایل، اندازه پارتیش‌های بالا، امنیت، فشرده سازی و Disk Quotas (سهمیه بندی دیسک) را ارائه می‌نماید.
- **Quality of Service (QoS):** امکان QoS، مجموعه‌ای از سرویس‌های مورد نظر به منظور حصول اطمینان از انتقال داده‌ها با یک سطح قابل قبول کیفیت در یک شبکه است. با استفاده از QoS، می‌توان نحوه پهنای باند اختصاصی به یک برنامه را کنترل نمود. QoS، یک سیستم مناسب، سریع و تضمین شده برای اطلاعات در شبکه را فراهم می‌نماید.
- **Terminal Service:** با استفاده از ویژگی فوق، امکان دستیابی از راه دور به یک سرویس دهنده از طریق یک ترمینال شبیه سازی شده، فراهم می‌گردد. یک ترمینال شبیه سازی شده، برنامه‌ای است که امکان دستیابی به یک کامپیوتر از راه دور را به گونه‌ای فراهم می‌نماید که تصور می‌شود شما در کنار سیستم به صورت فیزیکی قرار گرفتهاید (نوعی پیشرفته از Remote Desktop). با استفاده از سرویس ترمینال، می‌توان برنامه‌های سرویس گیرنده را بر روی سرویس دهنده اجراء و بدین ترتیب کامپیوتر سرویس گیرنده به عنوان یک ترمینال ایفای وظیفه خواهد کرد (نه به عنوان یک سیستم مستقل). بدین ترتیب هزینه مربوط به عملیات و نگهداری شبکه کاهش و می‌توان مدیریت سرویس دهنده را از هر مکانی بر روی شبکه انجام داد.

- **Remote Installation Services (RIS):** سرویس فوق، امکان بکارگیری سیستم عامل در یک سازمان توسط مدیران سیستم را تسریع و بهبود خواهد بخشید. بدین ترتیب نیاز به ملاقات فیزیکی هر یک از کامپیوترهای سرویس گیرنده وجود نداشته و می‌توان از راه دور، اقدام به نصب نمود. سرویس فوق، یک عنصر انتخابی بوده و به عنوان بخشی از نسخه Windows 2003 Server است.

۵-۵- انواع نسخه‌های ویندوز سرور ۲۰۰۳

1. Web Edition
2. Standard Edition
3. Enterprise Edition
4. Data Center Edition

۵-۵-۱- *Server 2003 Web Edition*

این نسخه از ویندوز سرور ۲۰۰۳ تا 2 GB حافظه RAM و در صورتی که سخت‌افزار شما پشتیبانی کند تا ۲ عدد CPU را به صورت **متقارن** (Symmetric) پشتیبانی می‌کند. این نسخه بیشتر در شبکه برای Web Server یا Application Server استفاده می‌شود و نمی‌توان به عنوان Domain Controller یا DHCP و یا FAX Server در نظر گرفته شود.

نکته: در اینجا مفهوم Symmetric و Asymmetric را می‌گوییم تا در ادامه کار اگر جایی استفاده کردیم دچار ابهام نشویم. در صورتی که در کامپیوتر خود ۲ یا تعداد بیشتری CPU داشته باشیم چه به صورت Dual Core و یا به طور کل دو CPU مجزا از هم، زمانی که دو CPU همزمان با یکدیگر کار می‌کنند و هر نوع دستورالعمل یا برنامه‌ای توسط هر یک اجرا می‌شود و محدودیتی در نوع دستورالعمل‌ها نمی‌باشد به این نوع CPUها متقارن یا Symmetric می‌گویند و در صورتی که برای هر کدام از CPUها یک سری دستورالعمل خاص تعریف شده باشد، به طور مثال یک CPU فقط دستورالعمل‌های سیستمی و CPU دیگر درخواستها و برنامه‌های کاربر را اجرا کند به این نوع پردازنده‌ها، نا متقارن یا Asymmetric می‌گویند.

۵-۵-۲- *Server 2003 Standard Edition*

این نسخه از ویندوز سرور ۲۰۰۳ تا 4 GB حافظه RAM و تا ۴ عدد CPU را به صورت **متقارن** پشتیبانی می‌کند. این نسخه معمولاً در شبکه‌های محلی استفاده می‌شود و می‌تواند به عنوان Web Server و یا Application Server و یا Mail Server مورد استفاده قرار گیرد. البته این مسئله را در نظر بگیرید که مطمئنا نسخه Web Edition برای راه انداختن Web Server دارای کارایی و Performance بهتری می‌باشد چرا که بسیاری از سرویس هایی که در Web Edition استفاده نمی‌شوند Stop شده‌اند و این مسئله سرعت سیستم را تا حد قابل توجهی بالا برده است.

۵-۵-۳- *Server 2003 Enterprise Edition*

نسخه ۳۲ بیتی Enterprise تا 32 GB حافظه RAM و تا ۸ عدد CPU و نسخه ۶۴ بیتی آن تا 64GB حافظه RAM و تا ۸ عدد CPU را پشتیبانی می‌کنند. قدرت پردازش این Platform در حالت کلی بیشتر از نسخه Standard می‌باشد.

۵-۵-۴- *Server 2003 Datacenter Edition*

این نسخه از ویندوز سرور ۲۰۰۳ نیز در دو نسخه ۳۲ و ۶۴ بیتی عرضه می‌شود. نسخه ۳۲ بیتی در حالت کلی تا 64 GB حافظه RAM و تا ۳۲ عدد CPU را به صورت متقارن پشتیبانی می‌کند. اما نسخه ۶۴ بیتی این ویندوز تا 512 GB حافظه

RAM و تا ۱۲۸ عدد CPU را به صورت **متقارن** پشتیبانی می‌کند. در جاهایی که بخواهیم حجم بسیار سنگینی را جا به جا کنیم از این نسخه استفاده می‌کنیم. (که باید بگویم که نسخه ۶۴ بیتی این ویندوز بر روی CPUهای Itanuim اجرا می‌شود).

۵-۵-۵- *Server 2008 HPC*

به همراه ویندوز سرور ۲۰۰۸، ویرایش جدیدی به نام HPC که مخفف High Performance Computing بوده و به معنای "انجام محاسبات با کارآیی بالا" می‌باشد، معرفی شد. در واقع HPC، نسخه بهبود یافته Windows Compute Cluster Server 2003 می‌باشد. این نسخه بیشتر در محافل علمی کاربرد دارد؛ به خصوص در سرور هایی که می‌خواهیم محاسبات علمی سنگینی را انجام دهد. یکی از ویژگی‌های این ویرایش، پشتیبانی و استفاده بهینه از سخت‌افزارهای موازی به منظور انجام سریع‌تر محاسبات می‌باشد. در این ویرایش، Clustering به خوبی انجام می‌گیرد. HPC قابلیت پشتیبانی از هزاران هسته پردازشی و همچنین برخی نرم‌افزارهای پردازش موازی مانند LPI و MPICH2 را دارد.

۵-۶- مقایسه نسخه‌های ویندوز سرور ۲۰۰۳ در یک نگاه

ویژگی	Web Server	Server	Enterprise Server	Datacenter Server
کلاسترینگ	خیر	خیر	2 - way	4 - way
حمایت از VPN	محدود	بلی	بلی	بلی
سرویس Internet Authentication	خیر	بلی	بلی	بلی
Network Bridging	خیر	بلی	بلی	بلی
حمایت از Active Directory	فقط Domain Member	Domain Member or Domain Controller	Domain Member or Domain Controller	Domain Member or Domain Controller
حمایت از MetaDirectory Service	خیر	خیر	بلی	خیر
حمایت از SharePoint Team Service	خیر	بلی	بلی	بلی
Removable & Remote Storage	خیر	بلی	بلی	بلی
Fax Services	خیر	بلی	بلی	بلی
Remote Installation Service	خیر	بلی	بلی	بلی
نسخه ۶۴ بیتی برای	خیر	خیر	بلی	بلی

کامپیوترهای Itanium				
Hot -Add Memory Capacity	خیر	خیر	بلی	بلی
Internet Connection Firewall	خیر	خیر	بلی	بلی
حمایت از Public Key Infrastructure (PKI)	محدود	بلی	بلی	بلی
Terminal Service Application) (Server mode	خیر، فقط Remote admin	بلی	بلی	بلی
حداکثر حافظه اصلی	۲ گیگا بایت	۴ گیگا بایت	۳۲ گیگا بایت ------ کامپیوترهای Itanium حداکثر ۶۴ گیگا بایت	۶۴ گیگا بایت ------ کامپیوترهای Itanium حداکثر ۱۲۸ گیگا بایت
تعداد پردازنده	حداقل: ۱ حداکثر: ۲	حداقل: ۱ حداکثر: ۲	حداقل: ۱ حداکثر: ۸	حداقل: ۸ حداکثر: ۳۲

۵-۷- ویژگی‌های جدید ویندوز سرور ۲۰۰۸

۵-۷-۱- قابلیت ایجاد محیط مجازی

قابلیت Hyper-V ویندوز سرور (نسل جدید تکنولوژی محیط مجازی Hypervisor-Based سرور) به شما امکان می‌دهد تا چند سرور با وظایف متفاوت در شبکه را توسط راه اندازی ماشین‌های مجازی مجزا روی یک ماشین فیزیکی واحد ادغام کرده و از این طریق از دارایی‌های سخت‌افزاری سرور خود بهترین استفاده را ببرید. همچنین شما می‌توانید سیستم عامل‌های مختلف مانند ویندوز، لینوکس و... را به صورت همزمان روی یک سرور واحد اجرا نمایید. برنامه‌های کاربردی هم می‌توانند با استفاده از تکنولوژی‌های دسترسی متمرکز شده به برنامه‌های کاربردی در ویندوز سرور ۲۰۰۸ به صورت موثری از

مجازی سازی استفاده نمایند. با اجرای Terminal Services Gateway و Terminal Services RemoteApp روی Terminal Server، شما به راحتی اجازه خواهید یافت بدون نیاز به اتصال VPN، از هر کجا به برنامه‌های استاندارد بر مبنای ویندوز دسترسی داشته باشید.

۵-۷-۲- ساخته شده برای وب

ویندوز سرور ۲۰۰۸ به همراه IIS 7.0 به بازار عرضه می‌گردد که وب سروری با پلتفرمی ساده و امن برای توسعه و میزبانی مطمئن سرویس‌ها و برنامه‌های کاربردی وب می‌باشد. تغییر مهمی که در پلتفرم وب ویندوز (IIS 7.0) داده شده آن است که **به منظور کنترل و انعطاف بیشتر، از معماری طبقه بندی شده استفاده می‌کند**. همچنین IIS 7.0 از امکان مدیریت آسان و مکانیزم تشخیص و رفع عیب بسیار قدرتمندی بهره می‌برد که موجب کاهش اتلاف زمان و افزایش توسعه پذیری همه جانبه می‌گردد. IIS7.0 به همراه.NET Framework 3.0 پلتفرم جامعی برای ساخت برنامه‌های کاربردی که ارتباط بین کاربران و داده‌ها را برقرار می‌کنند، فراهم می‌آورد و آن‌ها را قادر می‌سازد اطلاعات مورد نیاز را ببینند، به اشتراک بگذارند و بر روی آن‌ها عملیات انجام دهند. به علاوه IIS 7.0 در یکپارچه سازی دیگر پلتفرم‌های وب شرکت مایکروسافت نظیر ASP.NET, Windows Communication Foundation Web Services, Windows SharePoint یک نقش اساسی را ایفا می‌کند.

۵-۷-۳- امنیت بالا

ویندوز سرور ۲۰۰۸ امن ترین ویندوز ارائه شده تا کنون می‌باشد. این سیستم عامل به منظور محافظت در **برابر خرابی‌ها** بسیار مقاوم شده است و از تکنولوژی‌های جدید متفاوتی برای **ممانعت از برقراری ارتباطات غیر مجاز** به شبکه، سرورها، داده‌ها و حسابرسی کاربران شما استفاده کرده است. سرویس Network Access Protection به شما کمک می‌کند مطمئن شوید کامپیوتر هایی که جهت اتصال به شبکه شما تلاش می‌کنند با سیاست‌های امنیتی سازمان متبوع شما مطابقت دارند. ادغام تکنولوژی‌های مختلف و چندین مورد بهبود در Active Directory، آن را به ابزاری یکپارچه و قدرتمند برای راهکارهای شناسایی هویت و کنترل مبدل کرده است. در پایان سرویس‌های Read-Only Domain Controller و BitLocker Drive Encryption به شما اجازه می‌دهند تا Active Directory را به صورت کاملاً امن در محل شعبات خود راه اندازی نمایید.

۵-۷-۴- انجام محاسبات با کارایی بالا (HPC)

مزایا و امکان کاهش هزینه‌ها در ویندوز سرور ۲۰۰۸ با توسعه آن توسط Windows HPC Server 2008 که برای محیط‌های با نیاز محاسباتی بالا طراحی شده است نمود بیشتری می‌یابد. ویندوز HPC سرور ۲۰۰۸ روی ویندوزهای سرور ۲۰۰۸ با تکنولوژی x64-bit ساخته شده است و می‌تواند بطور موثری با استفاده از عملکرد Out-Of-The-Box به هزاران هسته پردازشی گسترش یافته و در نتیجه کارایی محیط HPC شما را افزایش داده و پیچیدگی آن را کاهش دهد. ویندوز HPC سرور ۲۰۰۸ با تجمیع توانایی کاربران یکپارچه و توانا و تبدیل کامپیوترهای رومیزی به کلاسترهای بزرگ، شما را قادر

به گسترش همه جانبه می‌نماید و مجموعه جامعی از ابزارهای گسترش، مدیریت و نظارت را شامل می‌شود که گسترش، مدیریت و تجمیع با زیرساخت‌های موجود شما را ساده‌تر می‌کند.

۵-۸- لینوکس

سیستم عامل لینوکس بر عکس سیستم عامل ویندوز سرور، به صورت پیش فرض خدمات و نرم‌افزارهای شبکه‌ای را با خود به همراه ندارد (البته ویندوز سرور نیز به صورت پیش فرض تمام امکانات شبکه‌ای را نصب نمی‌کند ولی در خود دارا می‌باشد)، و لذا در لینوکس، شما بایستی خودتان نرم‌افزارها و سرویس‌های مورد نیاز را نصب نمایید. سیستم عامل‌های شکل گرفته بر پایه لینوکس، به دلیل پایداری و انعطاف، گزینه‌های خوبی برای نصب بر روی سیستم‌های سرور هستند.

۵-۸-۱- نرم‌افزارهای Server تحت لینوکس

نمونه نرم‌افزارهای مشهوری که معمولاً تحت لینوکس به عنوان نرم‌افزار Server استفاده می‌شوند:

- سرور پروکسی-کش (Proxy-Cache)
- بایند (BIND)
- سرور سامانه نام دامنه (DNS)
- آپاچی (APACHE)
- سرور وب
- پست فیکس(Postfix)
- سرور پست الکترونیکی
- مای اس کیوال (MySQL)
- سرور پایگاه داده
- اسکوئید (SQUID)

۵-۸-۲- ویژگی‌های اصلی لینوکس

۱. چند کاربره بودن (Multi user)
۲. چند وظیفه‌ای بودن (Multi-Tasking)
۳. واسط کاربر گرافیکی (X windows system)
۴. سرویس دهندههای شبکه (Network Server)
۵. پشتیبانی برنامه‌های کاربردی (Application Support)
۶. پشتیبانی (Support)
۷. اتصالات شبکه‌ای (Network Connectivity)

- **چند کاربره بودن**

سیستم عامل لینوکس می‌تواند به چندین کاربر، اجازه کار کردن با سیستم را بدهد و لذا برای هر کاربر حساب کاربری جداگانه‌ای را تعریف می‌کند. ضمنا چندین کاربر می‌توانند به صورت همزمان به سیستم وارد شوند و در آن مشغول به کار شوند.

- **چند وظیفه‌ای بودن**

در لینوکس این امکان وجود دارد که چندین برنامه در یک لحظه اجرا شوند؛ یعنی یک کاربر می‌تواند از چندین برنامه به صورت همزمان استفاده نماید.

- **واسط کاربر گرافیکی**

کاربران مبتدی، ترجیح می‌دهند از طریق رابط گرافیکی از لینوکس استفاده نمایند. دو رابط گرافیکی GNOME و KDE متداول ترین رابط‌های گرافیکی برروی این سیستم عامل می‌باشند.

- **سرویس دهندههای شبکه**

سیستم عامل لینوکس برای کاربردهای شبکه توسعه یافته به طوری که می‌تواند به عنوان سیستم عامل سرور برای مدیریت منابع مختلف موجود روی شبکه پیکربندی شود.

- **پشتیبانی برنامه‌های کاربردی**

به خاطر سازگاری لینوکس با استانداردهای صنعتی سیستم عامل، محدوده وسیعی از نرم‌افزارها برای لینوکس در دسترس می‌باشند. معمولاً در سی دی نسخه‌های مختلف لینوکس، برنامه‌های کاربردی فراوانی وجود دارند که بسیاری از نیازهای عمومی کاربران را برآورده می‌سازند.

- **پشتیبانی**

جامعه Open Source و برخی از شرکت‌های تولید کننده نسخه‌های لینوکس، از این سیستم عامل پشتیبانی دارند و اگر در کار با لینوکس دچار مشکل شدید، عملیات پشتیبانی را انجام خواهند داد.

- **اتصالات شبکه**: پشتیبانی از انواع مختلف واسط شبکه (سیمی و بی‌سیم)

۵-۸-۳- مزایای لینوکس

۱. رایگان بودن

۲. قابلیت اعتماد

۳. منابع اطلاعاتی لینوکس در اینترنت

۵-۸-۴- اجزای سیستم عامل لینوکس

سیستم عامل لینوکس دارای سه قسمت اصلی: هسته، محیط و ساختار فایل است.

- **هسته**

هسته بخش اصلی لینوکس است و ارتباط میان سیستم عامل لینوکس و نرم‌افزارهای نصب شده بر روی آن با سخت‌افزار را برقرار می‌کند. به عبارت دیگر، اجرای برنامه‌ها و مدیریت سخت‌افزارها را برعهده دارد.

- **محیط**

محیط نیز واسطی را برای کاربران ایجاد و دستورات کاربران را دریافت نموده و آن‌ها را برای اجرا به هسته ارسال می‌کند. هر برنامه‌ای که با هسته ارتباط برقرار می‌کند، برنامه‌ای است که در حالت کاربر (User Mode) اجرا می‌شود.

- **ساختار فایل**

ساختار فایل، نحوه ذخیره شدن فایل‌ها بر روی دیسک سخت را تعیین می‌کند. در لینوکس نیز همانند ویندوز، فایل‌ها در داخل دایرکتوری‌ها قرار می‌گیرند و کاربران می‌توانند دایرکتوری‌ها و فایلهای مورد نظر خود را ایجاد کنند و سپس برای هر یک از آن‌ها مجوزهای دسترسی تعیین نمایند.

۵-۸-۵- نسخه‌های مختلف سیستم عامل لینوکس

1. BlueCat
2. Caldera OpenLinux
3. Debian
4. Ubuntu
5. Dragon Linux
6. Mandrak
7. Red Hat
8. Slackware
9. SUSE
10. Fedora Core

فصل ۶

تجهیزات شبکه

تجهیزات شبکه:

تجهیزات شبکه به مجموعه‌ای از ابزار و وسایلی گفته می‌شود که برای راه اندازی یک شبکه رایانه‌ای نیاز است.

تجهیزات شبکه به دو دسته تقسیم می‌شوند:

- تجهیزات فعال (Active Products)
- تجهیزات غیر فعال (Passive Products)

تجهیزات فعال: (Active Products) تجهیزاتی هستند که فعالیت الکترونیکی در درون آن‌ها صورت می‌گیرد و اطلاعات وارد شده به آن‌ها بسته به شرایط برنامه ریزی شده برای دستگاه، پردازش و رد و بدل می‌گردد

انواع تجهیزات فعال عبارتند از:

- مسیر یاب ACCESS POINTS
- مودم
- دیواره‌های آتش سخت‌افزاری FIRE WALL ACCESORIES
- کارت شبکه
- سوئیچ
- روتر
- مینی جیبیک
- و...

نام چند تولید کننده مطرح این محصولات در دنیا عبارت است از:

سیسکو – رد لاین – ساندوین

تجهیزات غیر فعال: (Passive Products) تجهیزاتی هستند که قابل برنامه ریزی نبوده و نمی‌توانند تغییراتی روی اطلاعات و یا محتوای تبادل شده در شبکه داشته باشند. بخشی از تجهیزاتی هم که بمنظور نصب و پیکر بندی سخت‌افزاری شبکه (از قبیل کابل کشی و نصب دستگاه‌ها) استفاده می‌شود در این دسته جای می گیرند.

انواع تجهیزات غیر فعال عبارتند از:

- کابل
- پچ پنل
- پچ کورد
- فیبر نوری
- کیستون پریز
- سر سوکت
- رک
- نگهدارنده کابل
- و...

نام چند تولید کننده مطرح این محصولات در دنیا عبارت است از:

امپ - بلدن - لتیس

در این فصل، به معرفی تجهیزات سخت‌افزاری شبکه خواهیم پرداخت.

کابل شبکه – Cable
کارت واسط شبکه – NIC
تکرار کننده – Repeater
هاب – HUB
سوئیچ - Switch
پل – Bridge
دروازه - Gateway
مسیر یاب - Router

۶-۱- کابل شبکه

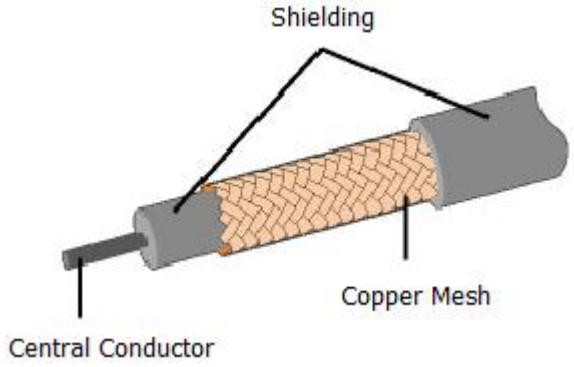
۶-۱-۱- انواع رسانه ها

در شبکه‌های محلی از کابل به عنوان محیط انتقال و به منظور ارسال اطلاعات استفاده می‌گردد. از چندین نوع کابل در شبکه‌های محلی استفاده می‌گردد. در برخی موارد ممکن است در یک شبکه صرفاً از یک نوع کابل استفاده و یا با توجه به شرایط موجود از چندین نوع کابل استفاده گردد. نوع کابل انتخاب شده برای یک شبکه به عوامل متفاوتی نظیر: **توپولوژی**

شبکه، پروتکل و **اندازه شبکه** بستگی خواهد داشت. آگاهی از خصایص و ویژگی‌های متفاوت هر یک از کابل‌ها و تاثیر هر یک از آن‌ها بر سایر ویژگی‌های شبکه، به منظور طراحی و پیاده سازی یک شبکه موفق بسیار لازم است.

۶-۱-۲- کابل کواکسیال

یکی از مهمترین محیط‌های انتقال در مخابرات کابل کواکسیال و یا هم محور می‌باشد. این نوع کابل‌ها از سال ۱۹۳۶ برای انتقال اخبار و اطلاعات در دنیا به کار گرفته شده‌اند. در این نوع کابل‌ها، دو سیم تشکیل دهنده یک زوج، از حالت متقارن خارج شده و هر زوج از یک سیم در مغز و یک لایه مسی بافته شده در اطراف آن تشکیل می‌گردد. ماده‌ای پلاستیکی این دو هادی را از یکدیگر جدا می‌کند و مانع از تماس دو هادی در تمام طول کابل با یکدیگر می‌شود.



مزایای کابل‌های کواکسیال:

- قابلیت اعتماد بالا
- ظرفیت بالای انتقال، ***حداکثر*** پهنای باند ۳۰۰ مگاهرتز
- دوام و پایداری خوب
- پایین بودن مخارج نگهداری
- قابل استفاده در سیستم‌های آنالوگ و دیجیتال
- هزینه پائین در زمان توسعه

پهنای باند نسبتا" وسیع که مورد استفاده اکثر سرویس‌های مخابراتی از جمله تله کنفرانس صوتی و تصویری است.

معایب کابل‌های کواکسیال:

- مخارج بالای نصب
- نصب مشکل‌تر نسبت به کابل‌های بهم تابیده
- محدودیت فاصله
- نیاز به استفاده از عناصر خاص برای انشعابات

از کانکتورهای BNC (Bayone-Neill-Concelman) به همراه کابل‌های کواکسیال استفاده می‌گردد. اغلب کارت‌های شبکه دارای کانکتورهای لازم در این خصوص می‌باشند.



۶-۱-۳- کابل UTP (Unshielded Twisted Pair)

متداولترین نوع کابلی که در انتقال اطلاعات استفاده می‌گردد، کابل‌های به هم تابیده می‌باشند. این نوع کابل‌ها دارای دو رشته سیم به هم پیچیده بوده که هر دو نسبت به زمین دارای یک امپدانس یکسان می‌باشند. بدین ترتیب امکان تاثیر پذیری این نوع کابل‌ها از کابل‌های مجاور و یا سایر منابع خارجی کاهش خواهد یافت.

کابل‌های بهم تابیده دارای دو مدل متفاوت: STP (Shielded Twisted Pair) و UTP (Unshielded Twisted Pair) می‌باشند. کابل UTP نسبت به کابل STP به مراتب متداول‌تر بوده و در اکثر شبکه‌های محلی استفاده می‌گردد.



کیفیت کابل‌های UTP متغیر بوده و با توجه به مشخصه‌ها و سطوح کارایی به گروه‌های خاصی، طبقه بندی می‌شوند (Category). هرچه درجه بندی طبقه یک کابل بالاتر باشد به این معنی است که آن کابل بهتر است و می‌تواند داده‌ها را با سرعت بالاتری ارسال کند.

جدول دسته بندی کابل‌های UTP

موارد استفاده	سرعت انتقال اطلاعات	گروه
سیستم‌های قدیمی تلفن، ISDN و مودم	حداکثر تا یک مگابیت در ثانیه	CAT1
شبکه‌های Token Ring	حداکثر تا چهار مگابیت در ثانیه	CAT2
شبکه‌های Token Ring و 10BASE-T	حداکثر تا ده مگابیت در ثانیه	CAT3
شبکه‌های Token Ring	حداکثر تا شانزده مگابیت در ثانیه	CAT4
اترنت (ده مگابیت در ثانیه)، اترنت سریع (یکصد مگابیت در ثانیه) و شبکه‌های Token Ring (شانزده مگابیت در ثانیه)	حداکثر تا یکصد مگابیت در ثانیه	CAT5
شبکه‌های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT5e
شبکه‌های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT6

مزایای کابل‌های بهم تابیده:

- سادگی و نصب آسان
- انعطاف پذیری مناسب
- دارای وزن کم بوده و براحتی بهم تابیده می‌گردند.

معایب کابل‌های بهم تابیده:

- تضعیف فرکانس
- بدون استفاده از تکرار کننده‌ها، قادر به حمل سیگنال در مسافت‌های طولانی نمی‌باشند.

- پایین بودن پهنای باند
- به دلیل پذیرش پارازیت، در محیط‌های الکتریکی سنگین به خدمت گرفته نمی‌شوند.

کانکتور استاندارد برای کابل‌های UTP، از نوع **RJ-45** می‌باشد. کانکتور فوق شباهت زیادی به کانکتورهای تلفن (RJ-11) دارد. هر یک از پین‌های کانکتور فوق می‌بایست به درستی پیکربندی گردند.

(RJمخفف Registered Jack می‌باشد)



جدول زیر، اطلاعات کاملی در خصوص کابل‌های بهم تابیده یا UTP ارائه می‌دهد:

جدول انواع مدل‌های کابل UTP

نوع	نرخ انتقال	فرکانس	بیشترین طول	تعداد جفت	کاربرد
Cat1	1 Mbps	1 MHz	90 meters	1 pair	Telephone and ISDN
Cat2	4 Mbps	1 MHz	90 meters	2 pairs	Token ring
Cat3	10 Mbps	16 MHz	100 meters	3 or 4 pairs	10BaseT (Can reach 100 Mbps with 100VGAnyLAN)
Cat4	16 Mbps	16 MHz	100 meters	4 pairs	Token ring
Cat5	10 Mbps 1 Gbps if using all 4 pairs	100 MHz	100 meters	4 pairs	10BaseT and 100BaseT 155 Mbps ATM Gigabit Ethernet
Cat5e	1000 Mbps	100 MHz	100 meters	4 pairs	Gigabit Ethernet
Cat6	4-10 Gbps	250 MHz	100 meters	4 pairs	Gigabit Ethernet, uses all 4 pairs

به یاد داشته باشید که یکی دیگر از تفاوت‌های موجود بین طبقه‌های مختلف UTP، تعداد زوج سیم‌های موجود در کابل می‌باشد. در ضمن هر جفت سیم رنگ بندی خاصی دارد که مطابق استانداردهای خاصی تعریف شده‌اند.

به عنوان مثال، کابل Cat5 که امروزه متداولترین نوع کابل UTP می‌باشد دارای ۴ جفت زوج سیم می‌باشد که رنگ بندی آن‌ها عبارتند از:

جفت۱: آبی و سفید آبی
جفت۲: نارنجی و سفید نارنجی
جفت ۳: سبز و سفید سبز
جفت۴: قهوه‌ای و سفید قهوه ای

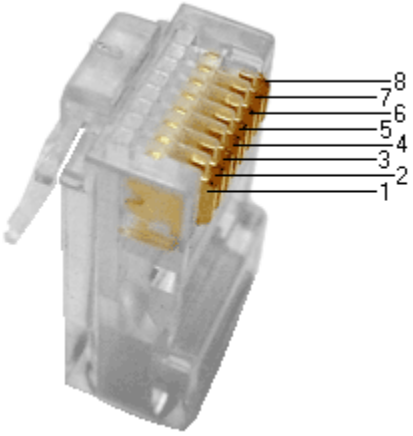
اصول کابل کشی:

کابل کشی شبکه یکی از مراحل مهم در زمان پیاده سازی یک شبکه کامپیوتری است که می‌بایست با دقت، ظرافت خاص و پایبندی به اصول کابل کشی ساخت یافته، انجام شود. با رعایت اصول کابل کشی ساخت یافته، در صورت بروز اشکال در شبکه، تشخیص و اشکال زدائی آن با سرعتی مناسبی انجام خواهد شد.

اترنت عموما با استفاده از هشت کابل هادی به همراه هشت پین ماژولار Plugs/Jacks، داده را حمل می‌کند. کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می‌گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هایی خاص است. (یک رشته رنگی و یک رشته سفید و رنگ رشته زوج مربوط). زوج‌های در نظر گرفته شده برای Ethernet10 و Ethernet100 به رنگ نارنجی و سبز می‌باشند. از دو زوج دیگر (رنگ قهوه‌ای و آبی) نیز می‌توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود.

به منظور کابل کشی کابل‌های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا AT&T، 258A)، استفاده می‌گردد. تنها تفاوت موجود بین آنان ترتیب اتصالات است.

نحوه شماره گذاری سوکت RJ-45



شماره پین‌های استاندارد T568B (کلاس B):

همانگونه که در جدول زیر مشاهده می‌گردد، شماره پین‌های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می‌شوند.

کد رنگ‌ها در استاندارد T568B		
کاربرد	رنگ	شماره پین
TxData +	سفید/ نارنجی	یک
TxData –	نارنجی	دو
RecvData +	سفید / سبز	سه
	آبی	چهار

	سفید /آبی	پنج
RecvData –	سبز	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

شماره پین‌های استاندارد T568A (کلاس A):

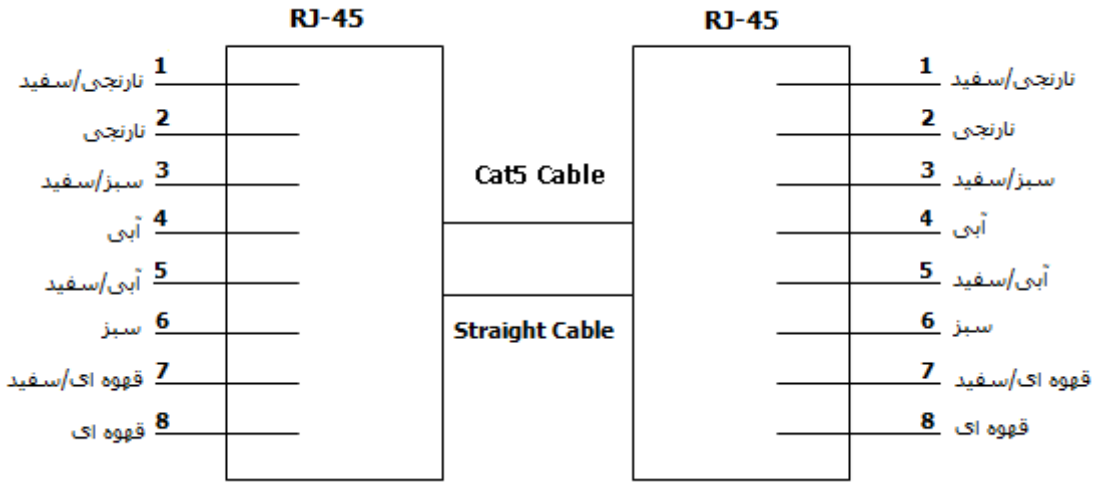
در استاندارد T568A، اتصالات سبز و نارنجی برعکس شده است، بنابراین زوج‌های یک و دو بر روی چهار پین وسط قرار می‌گیرند.

کد رنگ‌ها در استاندارد T568A		
کاربرد	**رنگ**	**شماره پین**
+RecvData	سفید/ سبز	یک
–RecvData	سبز	دو
+TxData	سفید / نارنجی	سه
	آبی	چهار
	سفید /آبی	پنج
–TxData	نارنجی	شش
	سفید/قهوه ای	هفت
	قهوه ای	هشت

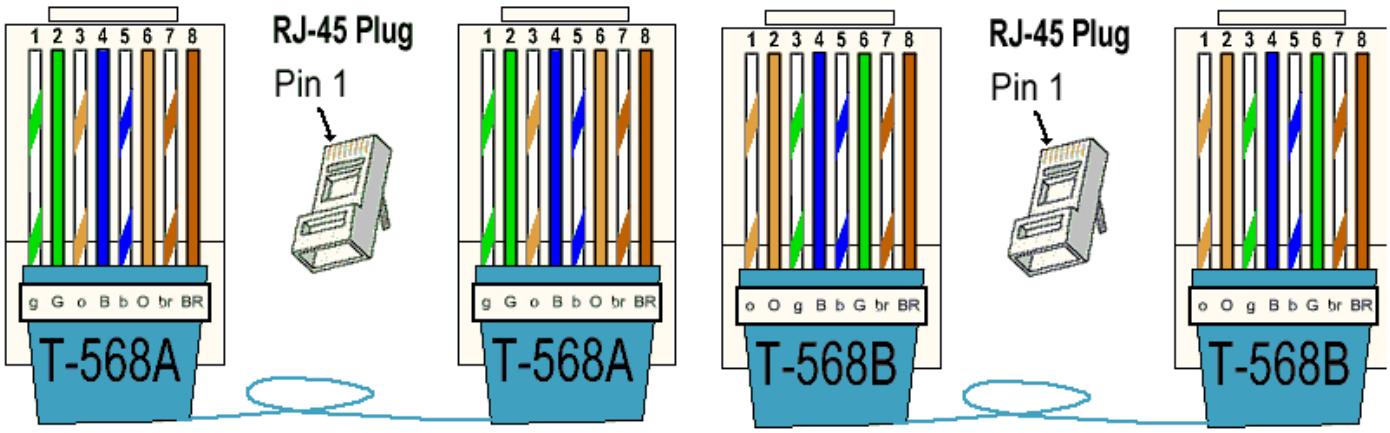
ایجاد یک کابل Straight

متداولترین کاربرد یک کابل Straight، اتصال بین یک **کامپیوتر و هاب/سوئیچ** است.

شکل زیر یک اتصال استاندارد Straight در کابل‌های CAT5 را نشان می‌دهد که از آن به منظور اتصال یک PC به هاب و یا سوئیچ استفاده می‌گردد. البته همانطور که در شکل زیر نیز مشاهده می‌کنید رنگ بندی و آرایش هر دو سر کابل CAT5 متناظر و مطابق استاندارد T568B صورت گرفته است.



البته کابل‌های Straight را به صورت T568A نیز می‌توان ایجاد نمود.



ایجاد کابل Cross-Over

کابل‌های کراس CAT5 UTP که از آنان با نام Cross-Over نیز نام برده می‌شود، یکی از متداولترین کابل‌های استفاده شده پس از کابل‌های Straight می‌باشند. با استفاده از کابل‌های فوق، می‌توان دو کامپیوتر را بدون نیاز به یک هاب و یا سوئیچ به یکدیگر متصل نمود. به عبارت دیگر، هاب عملیات Cross-Over را به صورت داخلی انجام می‌دهد، در زمانی که یک کامپیوتر را به یک هاب متصل می‌نماییم، صرفاً به یک کابل Straight نیاز می‌باشد. در صورتی که قصد اتصال دو کامپیوتر به یکدیگر را بدون استفاده از یک هاب داشته باشیم، می‌بایست عملیات Cross-Over را به صورت دستی انجام داد و کابل مختص آن را ایجاد نمود.

چرا به کابل‌های Cross-Over نیاز داریم؟

در زمان مبادله داده بین دو دستگاه (مثلاً کامپیوتر)، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می‌نماید. تمامی عملیات ارسال داده از طریق کابل‌های شبکه انجام می‌شود. یک کابل شبکه از چندین رشته سیم دیگر تشکیل می‌گردد. از برخی رشته سیم‌ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می‌شود. برای ایجاد یک کابل Cross-Over از رویکرد فوق استفاده شده و TX (ارسال) یک سمت به RX (دریافت) سمت دیگر، متصل می‌گردد. شکل زیر نحوه انجام این عملیات را نشان می‌دهد:



کابل CAT5 Cross-Over

به منظور ایجاد کابل‌های کراس CAT5 صرفاً از یک روش استفاده می‌گردد. همانگونه که قبلاً اشاره گردید، یک کابل Cross-Over پین TX یک سمت را به پین RX سمت دیگر متصل می‌نماید (و برعکس). شکل زیر شماره پین‌های یک کابل CAT5 معمولی Cross-Over را نشان می‌دهد.



همانگونه که در شکل فوق مشاهده می‌گردد در کابل‌های Cross-Over صرفاً از **پین‌های شماره یک، دو، سه و شش** استفاده می‌گردد. پین‌های یک و دو به منزله یک زوج بوده و پین‌های سه و شش زوج دیگر را تشکیل می‌دهند. از پین‌های چهار، پنج، هفت و هشت استفاده نمی‌گردد. (صرفاً از چهار پین برای ایجاد یک کابل Cross-Over، استفاده می‌گردد.)

موارد استفاده از کابل‌های Cross-Over

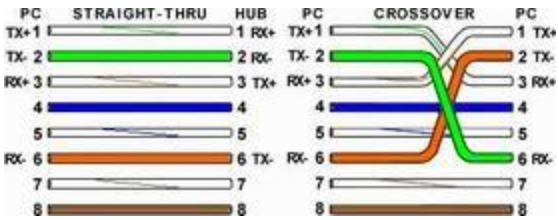
از کابل‌های Cross-Over **صرفاً** به منظور اتصال دو کامپیوتر استفاده نمی‌شود و می‌توان از آنان در دستگاه‌های متفاوتی نظیر سوئیچ و یا هاب نیز استفاده نمود. در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نماییم، معمولاً از پورت **Uplink** استفاده می‌گردد. **یعنی پورت‌های Uplink دو هاب را توسط یک کابل Straight به هم وصل می‌کنیم.** شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق پورت Uplink را نشان می‌دهد:



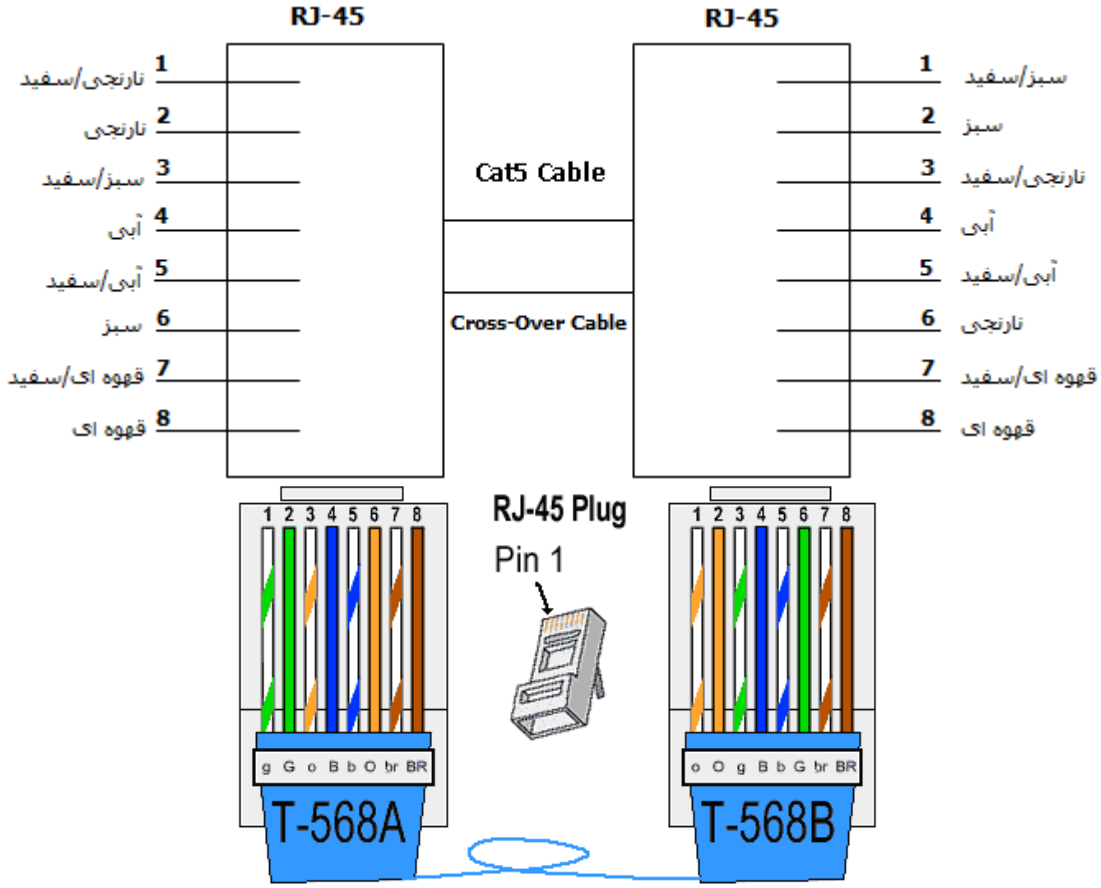
با توجه به وجود پورت Uplink، نیازی به استفاده از یک کابل Cross-Over نخواهد بود. به عبارت دیگر پورت‌های Uplink از داخل و به طور سخت‌افزاری، عمل Cross را انجام می‌دهند. در صورتی که امکان استفاده از پورت Uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از پورت‌های معمولی به یکدیگر متصل نماییم، می‌توان از یک کابل Cross-Over استفاده نمود. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Cross-Over را و بدون استفاده از پورت Uplink نشان می‌دهد:



شکل زیر تفاوت موجود بین شماره پین‌های یک کابل Straight و Cross-Over را نشان می‌دهد:



به عبارت دیگر، برای ایجاد یک کابل Cross کافیست رنگ بندی یک سر کابل را مطابق استاندارد کلاس A و رنگ بندی سر دیگر کابل را مطابق استاندارد کلاس B، در نظر گرفته و سوکت بزنید. به این ترتیب سیم‌های ارسال در هر طرف به سیم‌های دریافت در طرف دیگر منتهی می‌شوند و برعکس.



۶-۱-۴- آموزش سوکت زنی

برای سوکت زنی کابل شبکه به تجهیزات زیر نیاز داریم:

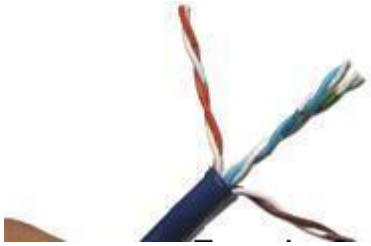
۱. کابل شبکه Cat-5

۲. سوکت کابل شبکه

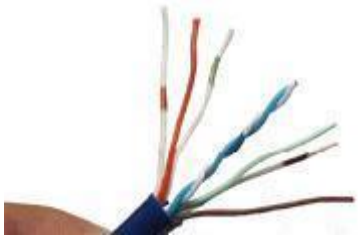
۳. آچار شبکه (دستگاه سوکت زن)

ابتدا مانند شکل زیر، کابل را لخت می کنیم:





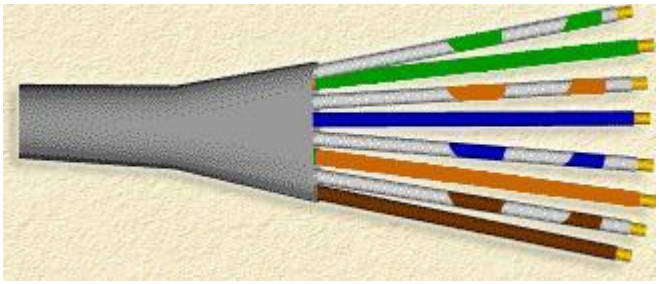
هشت تا سیم داریم که اول دو به دو به هم پیچیده شده است و سپس شده چهار جفت. مجددا این چهار جفت هم دوباره دور هم پیچیده‌اند. اول جفت‌ها را از هم جدا کنید:



حالا هر کدام از جفت‌ها را هم باز کنید و خوب صافشان کنید:

حالا باید سیم‌ها رو طبق استاندارد کنار هم بچینید.۲ تا استاندارد برای ترتیب رنگی کابل داریم. یکی 568-A که عکسش را در پایین می‌بینید و به ترتیب از چپ به راست:

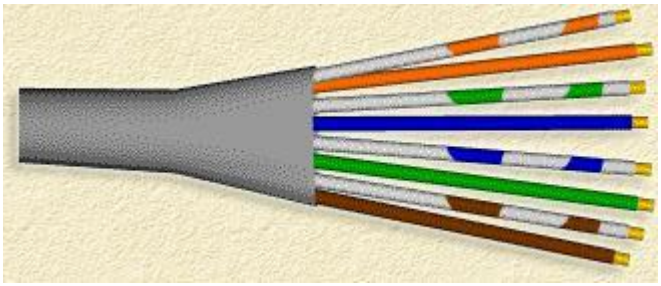
سفید/سبز – سبز – سفید/نارنجی – آبی – سفید/آبی – نارنجی – سفید/قهوه‌ای – قهوه ای



استاندارد بعدی 568-B است که رنگ هایش به این ترتیب از چپ به راست است (تصویر پایین):

سفید/نارنجی – نارنجی – سفید/سبز – آبی – سفید/آبی – سبز – سفید/قهوه‌ای – قهوه ای

نکته: در حالی که این دو استاندارد با هم فرقی ندارند، ولی استاندارد دوم (568-B) را بیشتر استفاده می‌کنند.



حالا که استانداردها را یاد گرفتیم، سیم‌ها را به ترتیب استاندارد کنار هم می‌چینیم و با انگشت شصت و سبابه پایین سیم‌ها را نگه میداریم تا بهم نریزد.



حالا سر سیم‌ها را به اندازه ۳ سانتی متر و به طور ۹۰ درجه قطع می‌کنیم تا صاف و یکدست بشود.





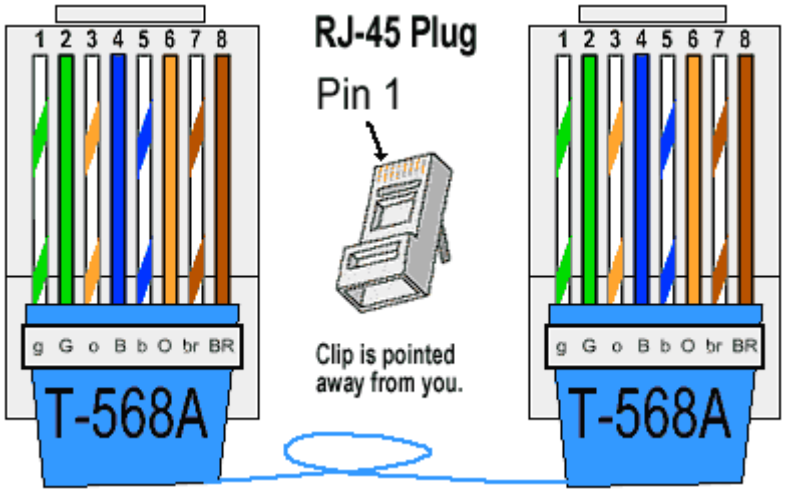
حالا سوکت را طوری در دست می‌گیریم که ضامنش پایین باشد و با دقت در حالی که زیر سیم را محکم نگه داشته‌ایم، درون سوکت جا می‌زنیم به طوری که هر سیم درون شیار خودش قرار بگیرد.



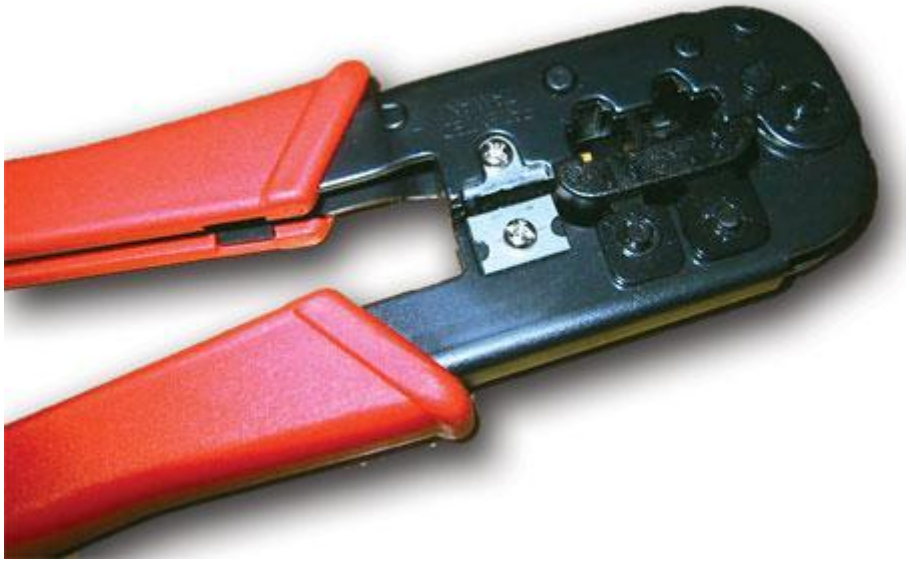
به دقت سوکت را بررسی کرده و مطمئن شوید که سیم‌ها مرتب و یکسان تا ته سوکت رفته باشند. ضمنا رنگ‌ها را هم چک کنید که احیانا جابجا نرفته باشد.

انتهای سوکت، فلزهای تیغ مانندی هست که بعد از پرس شدن، درون سیم‌ها فرو رفته و اتصال الکتریکی را برقرار می‌کند.

در ترتیب رنگ‌ها بایستی توجه داشته باشید که می‌خواهید کابل خود را به صورت Cross تولید کنید یا Straight که در بالا توضیح داده‌ایم. شکل زیر نوعی کابل Cross است.







حالا وقت آن رسیده است که سوکت را با آچار شبکه پرس کنید. بدین منظور سوکت را در محل تعبیه شده داخل آچار قرار داده و سپس آچار را محکم فشار دهید.



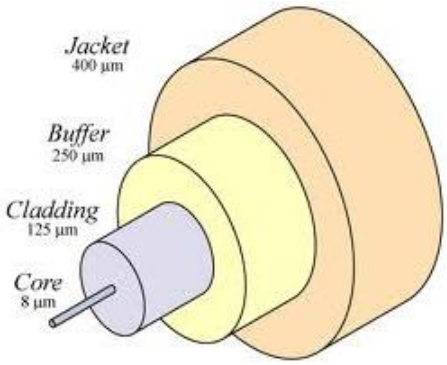
نکته ۱: اگه هر دو سر کابل را با یکی از استانداردهای A یا B ببندید، از این کابل می‌توانید برای اتصال کامپیوتر به سوییچ یا مودم/روتر استفاده کنید (نوع Straight).

نکته ۲: اگه یکی از سرها را A و دیگری را B ببندید، اصطلاحا یک کابل کراس آور یا کراس یا همون ضربدری دارید و با آن می‌توانید ۲ تا کامپیوتر رو بدون نیاز به سوییچ به هم شبکه کنید (نوع Cross).

۶-۱-۵- فیبر نوری

یکی از جدیدترین محیط‌های انتقال در شبکه‌های کامپیوتری، فیبر نوری است. کابل فیبر نوری برخلاف همه کابل هایی که تاکنون بحث کردیم، بر اساس سیگنال‌های الکتریکی که در هادی مسی جریان می‌یابند، نمی‌باشد؛ بلکه در کابل فیبر نوری از پالس‌های نور (فوتون ها) برای ارسال سیگنال‌های باینری تولید شده توسط منبع نورانی (دیود لیزری و یا دیودهای ساطع کننده نور) استفاده می‌شود. از آنجا که کابل فیبر نوری از نور به جای الکتریسیته استفاده می‌کند، تقریباً هیچ یک از مشکلات ذاتی کابل مسی همچون تداخل الکترومغناطیسی و نیاز به زمین کردن را ندارد.

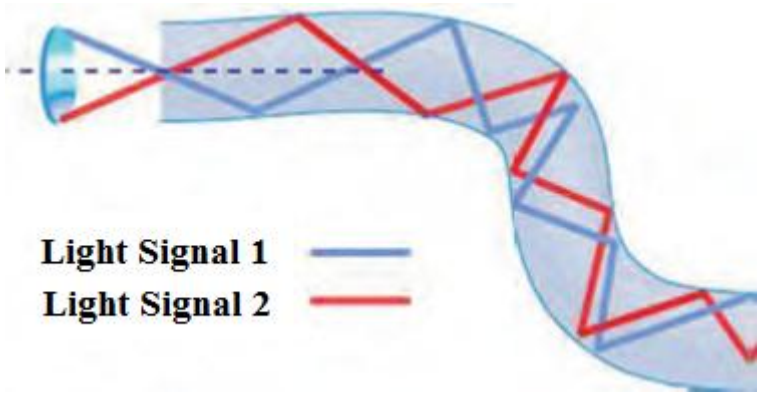
کابل فیبر نوری از یک میله استوآن‌های که **هسته** نامیده می‌شود و جنس آن از **سیلیکات** است تشکیل می‌گردد. شعاع استوانه بین دو تا سه میکرون است. روی هسته، استوانه دیگری (از همان جنس هسته) که **غلاف** نامیده می‌شود، استقرار می‌یابد. ضریب شکست هسته را با M1 و ضریب شکست غلاف را با M2 نشان داده و همواره M1>M2 است. در این نوع فیبرها، نور در اثر انعکاسات کلی در فصل مشترک هسته و غلاف، انتشار پیدا خواهد کرد.







در شکل زیر نحوه شکست نور را مشاهده می‌نمایید:



انواع فیبر نوری

فیبرهای نوری دو نوعند:

۱. **فیبرهای نوری تک وجهی:** این نوع از فیبرها، هسته‌های کوچکی دارند (قطری در حدود 10x 5/3 (-4) inch یا ۹ میکرون) و می‌توانند نور لیزر مادون قرمز (با طول موج ۱۳۰۰ تا ۱۵۵۰ نانومتر) را درون خود هدایت کنند.

۲. فیبرهای نوری چند وجهی: این نوع از فیبرها هسته‌های بزرگتری دارند (قطری در حدود 10x 5/2 (-3) inch یا ۶۲/۵ میکرون) و نور مادون قرمز گسیل شده از دیودهای نوری موسوم به LEDها را (با طول موج ۸۵۰ تا ۱۳۰۰ نانومتر) درون خود هدایت می‌کنند.

برخی از فیبرهای نوری از پلاستیک ساخته می‌شوند. این فیبرها هسته بزرگی (با قطر ۴ صدم inch یا یک میلیمتر) دارند و نور مرئی قرمزی را که از LEDها گسیل می‌شود (و طول موجی برابر با ۶۵۰ نانومتر دارد) را هدایت می‌کنند.

مزایای فیبر نوری:

- حجم و وزن کم
- پهنای باند بالا
- تلفات سیگنال کم و در نتیجه فاصله تقویت کنندهها زیاد می‌گردد.
- مصون بودن از اثرات القاهای الکترومغناطیسی مدارات دیگر
- آتش زا نبودن آن‌ها به دلیل عدم وجود پالس الکتریکی در آن‌ها
- مصون بودن در مقابل عوامل جوی و رطوبت
- سهولت در امر کابل کشی و نصب
- استفاده در شبکه‌های مخابراتی آنالوگ و دیجیتال
- مصونیت در مقابل پارازیت

معایب فیبر نوری:

- به راحتی شکسته شده و می‌بایست دارای یک پوشش مناسب باشند. مسئله فوق با ظهور فیبرهای تمام پلاستیکی و پلاستیکی/شیشه‌ای کاهش پیدا کرده است.
- اتصال دو بخش از فیبر یا اتصال یک منبع نور به فیبر، فرآیند دشواری است. در چنین حالتی می‌توان از فیبرهای ضخیم‌تر استفاده کرد اما این مسئله باعث تلفات زیاد و کم شدن پهنای باند می‌گردد.
- از اتصالات T شکل در فیبر نوری نمی‌توان جهت گرفتن انشعاب استفاده نمود. در چنین حالتی فیبر می‌بایست بریده شده و یک Detector اضافه گردد. دستگاه فوق می‌بایست قادر به دریافت و تکرار سیگنال را داشته باشد.

تقویت سیگنال نوری یکی از مشکلات اساسی در زمینه فیبر نوری است. برای تقویت سیگنال میبایست سیگنال‌های نوری به سیگنال‌های الکتریکی تبدیل، تقویت و مجددا" به علائم نوری تبدیل شوند.

یک فیبر نوری چگونه نور را هدایت می‌کند؟

فرض کنید می‌خواهید یک باریکه نور را بطور مستقیم و در امتداد یک کریدور بتابانید. نور براحتی در خطوط راست سیر می‌کند و مشکلی ازین جهت نیست. حال اگر کریدور مستقیم نباشد و در طول خود خمیدگی داشته باشد چگونه نور را به انتهای آن می‌رسانید؟

برای این منظور می‌توانید از یک آینه استفاده کنید که در محل خمیدگی راهرو قرار می‌گیرد و نور را در جهت مناسب منحرف می‌کند. اگر راهرو خیلی پیچ در پیچ باشد و خمهای زیادی داشته باشد چه؟ می‌توانید دیوارها را با آینه بپوشانید و نور

را به دام بیندازید بطوریکه در طول راهرو از یک گوشه به گوشه دیگر بپرد. این دقیقا همان چیزی است که در یک فیبرنوری اتفاق می‌افتد.

نور در یک کابل فیبرنوری، بر اساس قاعده‌ای موسوم به بازتابش داخلی، مرتبا بوسیله دیواره آینه پوش لایه‌ای که هسته را فراگرفته، به این سو و آن سو پرش می‌کند و در طول هسته پیش می‌رود.

از آنجا که لایه آینه پوش اطراف هسته هیچ نوری را جذب نمی‌کند، موج نور می‌تواند فواصل طولانی را طی کند. به هر حال، برخی از سیگنال‌های نوری در حین حرکت در طول فیبر، ضعیف می‌شوند که علت عمده آن وجود برخی ناخالصی‌ها داخل شیشه است. میزان ضعیف شدن سیگنال به درجه خلوص شیشه بکار رفته در داخل فیبر و نیز طول موج نوری که درون فیبر سیر می‌کند بستگی دارد.

سیستم ارتباط بوسیله فیبرنوری

برای پی بردن به اینکه فیبرهای نوری چگونه در سیستم‌های ارتباطی مورد استفاده قرار می‌گیرند، اجازه دهید نگاهی بیاندازیم به فیلم یا سندی که مربوط به جنگ جهانی دوم است. دو کشتی نیروی دریایی را درنظر بگیرید که از کنار یکدیگر عبور می‌کنند و لازم است باهم ارتباط برقرار کنند درحالی که امکان استفاده از رادیو وجود ندارد و یا دریا طوفانی است. کاپیتان یکی از کشتی‌ها پیامی را برای یک ملوان که روی عرشه است می‌فرستد. ملوان آن پیام را به کد مورس ترجمه می‌کند و از نورافکنی ویژه که یک پنجره کرکره جلو آن است برای ارسال پیام به کشتی مقابل استفاده می‌نماید. ملوانی که در کشتی مقابل است این پیام مورس را می‌گیرد، ترجمه می‌کند و به کاپیتان می‌دهد. (ملوان کشتی دوم عکس عملی را انجام می‌دهد که ملوان کشتی اول انجام داد.)

حالا فرض کنید این دو کشتی هر یک در گوشه‌ای از اقیانوسند و هزاران مایل فاصله دارند و در فاصله بین آن‌ها یک سیستم ارتباطی فیبرنوری وجود دارد.

سیستم‌های ارتباط بوسیله فیبرنوری، شامل این قسمت هاست:

- فرستنده: سیگنال‌های نور را تولید می‌کند و به رمز در می‌آورد.
- فیبرنوری: سیگنال‌های نور را تا فواصل دور هدایت می‌کند.
- تقویت کننده نوری: ممکن است برای تقویت سیگنال‌های نوری لازم باشد. (برای ارسال سیگنال به فواصل خیلی دور)
- گیرنده نوری: سیگنال‌های نور را دریافت و رمزگشائی می‌نماید.

۶-۲- کارت واسط شبکه (NIC)

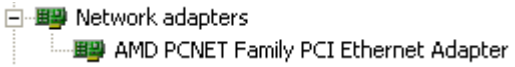
کارت شبکه، یکی از مهمترین عناصر سخت‌افزاری در زمان پیاده سازی یک شبکه کامپیوتری است. هر کامپیوتر موجود در شبکه (سرویس گیرندگان و سرویس دهندگان)، نیازمند استفاده از یک کارت شبکه است. کارت شبکه، ارتباط بین کامپیوتر و محیط انتقال (نظیر کابل‌های مسی و یا فیبر نوری) را فراهم می‌نماید.

اکثر مادربوردهای امروزی که از آنان در کامپیوترهای شخصی استفاده می‌گردد، دارای یک کارت شبکه OnBoard می‌باشند. کامپیوترهای قدیمی و یا کامپیوترهای جدیدی که دارای اینترفیس شبکه‌ای OnBoard نمی‌باشند، در زمان اتصال به شبکه، می‌بایست بر روی آنان یک کارت شبکه نصب گردد.

شکل زیر یک نمونه کارت شبکه را که دارای یک پورت RJ-45 است را نشان می‌دهد.



کامپیوترها جهت اتصال به هم و استفاده از برنامه‌های هم و اشتراک برنامه‌ها از نظر سخت‌افزاری احتیاج به کارت شبکه یا LAN Card دارند. که بطور معمول در بازار دو نوع کارت معمول می‌باشد. یک قسم آن‌ها کارت‌های ۱۰ در ۱۰ بوده و قسم دیگر کارتهای ۱۰ در ۱۰۰ می‌باشند. جهت کنترل اتصال درست کارت شبکه به کامپیوتر می‌توانید روی آیکون My Computer کلیک راست نموده و از قسمت Properties پوشه Device Manager را انتخاب نمایید. در بین ابزارهای نصب شده طبق شکل باید در قسمت Network Adapters، نام و مشخصات کارت شبکه شما وجود داشته باشد.



اگر در این بخش علامت سوال یا تعجب به شکل زرد رنگ وجود داشته باشد، نشان می‌دهد که راه انداز (Driver) کارت شبکه شما ناقص بوده و درست نصب نشده است و بایستی طبق روش‌های Hardware Settings آنرا برداشته (Remove) و مجددا نصب نمایید و یا از قسمت Add New Hardware در بخش Control Panel، درایور یا راه انداز مناسب و صحیح آن را نصب نمایید. توجه نمایید که بعد از نصب کارت شبکه، آیکون Network Neighborhood در روی میز کار (Desktop) مشاهده خواهد شد. از آنجایی که ما معمولاً دو نوع شبکه **BNC و HUB** را مورد استفاده قرار می‌دهیم بر روی اکثر کارت‌ها جهت اتصال هر دو نوع رابط وجود دارد. کارت‌های OnBoard، معمولا فقط جای HUB را دارند.

۶-۲-۱- وظایف کارت شبکه

۱. **برقراری ارتباط لازم بین کامپیوتر و محیط انتقال**

۲. **تبدیل داده:** داده‌ها بر روی گذرگاه (Bus) کامپیوتر به صورت موازی حرکت می‌نمایند. نحوه حرکت داده‌ها بر روی محیط انتقال شبکه به صورت سریال است. ترانسیور کارت شبکه (یک ارسال کننده و یا دریافت کننده)، داده‌ها را از حالت موازی به سریال و بالعکس تبدیل می‌نماید.

۳. **ارائه یک آدرس منحصر به فرد سخت‌افزاری:** آدرس سخت‌افزاری (MAC) درون تراشه ROM موجود بر روی کارت شبکه نوشته می‌گردد. آدرس MAC در واقع یک زیر لایه از لایه Data Link مدل مرجع OSI می‌باشد. آدرس سخت‌افزاری موجود بر روی کارت شبکه، یک آدرس منحصر به فرد را برای هر یک از کامپیوترهای موجود

در شبکه، مشخص می‌نماید. پروتکل هایی نظیر TCP/IP از یک سیستم آدرس‌دهی منطقی (آدرس IP)، استفاده می‌نمایند. در چنین مواردی قبل از دریافت داده توسط کامپیوتر، می‌بایست آدرس منطقی به آدرس سخت‌افزاری ترجمه گردد.

۴. **کپسوله کردن داده ها:** کارت شبکه و درایور آن مجموعاً قبل از انتقال اطلاعات باید داده هایی را که توسط پروتکل لایه شبکه تولید شده است، در یک فریم کپسوله کنند. عمل دیگری که کارت شبکه در این زمینه انجام می‌دهد خواندن محتوای فریم‌های دریافت شده از شبکه و انتقال داده‌های آن‌ها به پروتکل مناسب در لایه شبکه می‌باشد.

۵. **کد گذاری و کد گشایی سیگنال ها:** کارت شبکه مسئول پیاده سازی روش کد گذاری لایه شبکه می‌باشد که در آن اطلاعات باینری تولید شده در لایه شبکه که حالا در فریم، کپسوله شده است را به بارهای الکتریکی یعنی ولتاژهای الکتریکی، پالس‌های نور یا هر نوع سیگنالی که رسانه شبکه استفاده می‌کند تبدیل می‌کند. از طرف دیگر کارت شبکه سیگنال‌های دریافتی از شبکه را برای پروتکل‌های لایه بالاتر به اطلاعات باینری تبدیل می‌کند.

۶. **دریافت و انتقال اطلاعات:** مهمترین وظیفه کارت شبکه تولید و ارسال سیگنال‌های مناسب روی شبکه و دریافت سیگنال‌های موجود در شبکه می‌باشد. ماهیت سیگنال‌ها به رسانه شبکه و پروتکل لایه پیوند-داده بستگی دارد. در LANهای متداول امروزی، هریک از کامپیوترهای موجود در شبکه همه بسته‌های فرستاده شده روی شبکه را دریافت می‌کنند و سپس کارت شبکه آدرس مقصد لایه پیوند-داده هر یک از آن‌ها را بررسی می‌کند تا بسته هایی که به مقصد آن کامپیوتر تولید شده‌اند را برای پردازش به لایه بعدی از پشته پروتکل منتقل کند، در غیر اینصورت بسته دور انداخته می‌شود.

۷. **بافر کردن داده ها:** کارت‌های شبکه هر زمان فقط یک فریم داده را روی شبکه می‌فرستند یا از آن دریافت می‌کنند، بنابراین در خود بافری دارند که تا زمان کامل و آماده شدن یک فریم برای پردازش، داده هایی که از طرف کامپیوتر یا شبکه در یافت می‌کنند را ذخیره کنند.

۸. **تبدیل سریال به موازی و برعکس:** ارتباطات بین کامپیوتر و کارت شبکه به صورت موازی انجام می‌شود، مگر در کارتهای شبکه USB که ارتباط با کامپیوتر در آن‌ها به صورت سریال است. اما ارتباطات شبکه‌ای به صورت سریال انجام می‌شوند، بنابراین کارت شبکه مسئول تبدیل این دو نوع روش انتقال اطلاعات به همدیگر می‌باشد.

روند نصب یک کارت شبکه، شامل قراردادن کارت داخل کامپیوتر، پیکربندی کارت برای استفاده از منابع سخت‌افزاری مناسب، و نهایتا نصب درایور کارت می‌باشد که بسته به توانایی‌ها و نوع کامپیوتر از نظر قدیمی یا جدید بودن این پروسه می‌تواند بسیار ساده و یا بسیار پر دردسر باشد.

توجه: قبل از لمس کردن قطعات داخلی کامپیوتر یا درآوردن کارت شبکه از بسته محافظ مخصوص آن، دست خود را با ورقه فلزی دور منبع تغذیه کامپیوتر تماس دهید یا اینکه از دستکش‌های مخصوص استفاده کنید تا به دلیل تخلیه الکترواستاتیکی به قطعات آسیبی وارد نشود.

۶-۲-۲- انواع کارت شبکه

واسط شبکه کابل‌های UTP به شکل سوکت RJ-45 و برای کابل‌های کواکسیال، کانکتور BNC یا AUI می‌باشد، البته در بعضی موارد می‌توان از فرستنده‌های بی‌سیم هم استفاده کرد.

کارت شبکه به کمک درایور خود موظف به انجام اغلب **وظایف پروتکل‌های لایه پیوند-داده و فیزیکی** می‌باشد و زمان خرید باید کارت متناسب با پروتکلی که برای لایه پیوند-داده انتخاب کرده‌اید (مثل اترنت یا Token Ring) را خریداری کنید و توجه داشته باشید که این دو نوع کارت را نمی‌توان به جای یکدیگر استفاده کرد. نکته دیگری که زمان خرید باید مورد توجه قرار گیرد انتخاب کارتی است که علاوه بر تناسب با پروتکل لایه پیوند-داده، از گونه مورد نظر آن پروتکل هم پشتیبانی کند.

فراموش نکنید که کارت شبکه منتخب شما باید با اسلات باس کامپیوتری که قرار است در آن نصب شود، متناسب باشد و دارای کانکتور مخصوص رسانه شبکه باشد.

غیر از کارت‌های شبکه‌ای که مختص اتصال کامپیوترها به شبکه‌های محلی سرویس گیرنده /دهنده استاندارد هستند، انواع دیگری وجود دارند که کامپیوترها و دستگاه‌های دیگر را به شبکه‌های بخصوصی بنام شبکه ذخیره ناحیه‌ای یا **SAN** (Storage Area Network) متصل می‌کنند. یک SAN شبکه‌ای مجزا است که مختص ارتباطات بین سرورها و دستگاه‌های ذخیره سازی خارجی، از قبیل RAID می‌باشد. اغلب کارت‌های شبکه SAN بجای اترنت و Token Ring از پروتکل دیگری بنام Fiber Channel استفاده می‌کنند.

برای اتصال کارت شبکه به Motherboard نیز دو نوع اسلات PCI و ISA داریم. اسلات‌های PCI به مراتب از اسلات‌های ISA سریع‌تر هستند و دارای قابلیت خود پیکربندی می‌باشند، بنابراین کارت هایی که از این استاندارد استفاده می‌کنند متداول ترند.

اما در صورتیکه کامپیوتر تان فقط دارای اسلات ISA باشد به ناچار می‌توانید از کارت‌های شبکه ISA استفاده کنید. در سیستم‌های قابل حمل تنها انتخاب، کارت‌های PC Card می‌باشد. این نوع کارت‌ها مختص اسلات‌های PCMCIA می‌باشند و در این نوع اسلات‌ها قرار می‌گیرند. اما در صورتیکه سیستم شما از استاندارد CardBus پشتیبانی می‌کند، زمان خرید باید کارتی را انتخاب کنید که آن هم از این استاندارد پشتیبانی کند. CardBus استانداردی است که برای لوازم جانبی PC Card، بازدهی معادل بازدهی استاندارد PCI مهیا می‌کند.

در بازار کارت‌های شبکه‌ای که از پورت USB برای اتصال به کامپیوتر استفاده می‌کنند هم وجود دارد، اما رابط USB قدیمی، حداکثر می‌تواند در سرعت ۱.۲ مگابیت در ثانیه کار کند که حتی در مقایسه با استاندارد ISA کند است. همیشه سرعت انتقال داده در کارت شبکه شما باید با تجهیزات دیگر شبکه متناسب باشد.

کارت‌های شبکه متناسب با نوع کابلی که پشتیبانی می‌کنند دارای انواع مختلف کانکتور می‌باشند. بعضی از NICها (کارت‌های شبکه) بیش از یک کانکتور کابل دارند که شما را قادر به انتخاب رسانه شبکه مطلوب می‌کنند. به عنوان مثال، کارت هایی وجود دارند که دارای سه کانکتور AUI، BNC و RJ45 می‌باشند و **کارت مرکب** نامیده می‌شوند. این نوع

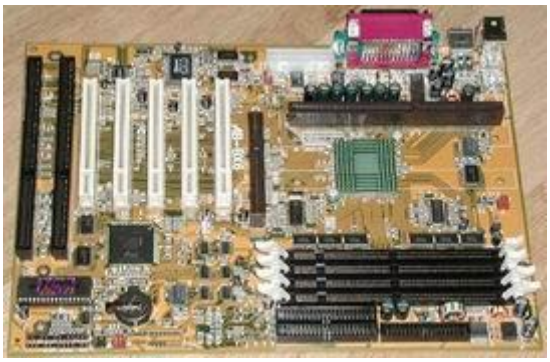
کارت‌ها از کارت هایی که فقط یک کانکتور دارند به مراتب گران ترند. توجه داشته باشید که همزمان فقط از یکی کانکتورها می‌توانید استفاده نمایید.

۶-۲-۳- انتخاب کارت شبکه

برای انتخاب یک کارت شبکه، می‌بایست پارامترهای متعددی را بررسی نمود:

- **سازگاری با معماری استفاده شده در شبکه**: کارت‌های شبکه دارای مدل‌های متفاوتی با توجه به معماری استفاده شده در شبکه (اترنت، Token ring) می‌باشند. اترنت، متداولترین معماری شبکه در حال حاضر است که در شبکه هایی با ابعاد بزرگ و کوچک، استفاده می‌گردد.
- **سازگاری با Throughput شبکه**: در صورتی که یک شبکه اترنت سریع (سرعت 100 Mbps) پیاده سازی شده است، انتخاب یک کارت اترنت با سرعت 10 Mbps تصمیم مناسبی در این رابطه نخواهد بود. اکثر کارت‌های شبکه جدید قادر به سوئیچینگ اتوماتیک بین سرعت‌های 10 و 100 Mbps می‌باشند (اترنت معمولی و اترنت سریع)
- **سازگاری با نوع اسلات‌های خالی مادربورد**: کارت‌های شبکه دارای مدل‌های متفاوتی با توجه به نوع اسلات مادربورد می‌باشند. کارت‌های شبکه PCI درون یک اسلات خالی PCI و کارت هایی از نوع ISA در اسلات‌های ISA نصب می‌گردند. کارت شبکه می‌بایست متناسب با یکی از اسلات‌های خالی موجود بر روی مادربورد، انتخاب گردد. اسلات آزاد به نوع مادربورد بستگی داشته و در این رابطه گزینه‌های متعددی نظیر ISA، PCI و EISA می‌تواند وجود داشته باشد.

شکل زیر یک نمونه مادربورد را که دارای اسلات‌های ISA و PCI است، نشان می‌دهد:



۶-۲-۴- ساختار کارت واسط شبکه (NIC)

کارت‌های شبکه از نظر ساختاری به چند دسته تقسیم بندی می‌شوند. از لحاظ استاندارد مورد استفاده سه نوع کارت شبکه وجود دارند این دسته بندی بر اساس نحوه ارتباط با مادربورد به شرح زیر است:

1. ISA/EISA: Architecture Standard Industry / Extended ISA
2. PCI: Peripheral Components Industry
3. USB: Universal Synchronous Bus

- **ISA:** تجهیزات ISA تا سالهای ۱۹۹۹ و ۲۰۰۰ تولید می‌شدند. اما این تجهیزات به دلیل نواقصی زیادی که داشت با شکست مواجه شد. دو دلیل عمده این شکست به شرح زیر است:

۱. اسلات‌های ISAی نصب شده روی مادربورد با نصف سرعت Bus مادربورد کار می‌کردند؛ که نتیجه آن کاهش خواندن و فرستادن اطلاعات به RAM بود.
۲. در هر لحظه تنها یک اسلات اجازه استفاده از باس مادربورد را داشت و در صورتیکه دو اسلات همزمان به انتقال داده روی مادربورد می‌پرداختند، هر دو از عمل خارج میشدند.

– **PCI:** از مزایای این فناوری از بین رفتن دو مشکل عمده تکنولوژی ISA بود. در این فناوری هر اسلات با سرعت باس مادربورد و همزمان با اسلات‌های دیگر نیز می‌توانست کار کند.

– **USB:** کارتهای واسط را می‌توان به نوعی سه دسته دانست که دسته سوم استفاده از ورودی‌های USB می‌باشد. تکنولوژی استفاده شده در این تجهیزات عینا شبیه به PCI می‌باشد. (گذرگاه فراگیر(گسترده) همزمان)

دسته بندی شبکه از نظر نوع مبادله اطلاعات:

شبکه سنکرون:

در این روش، هر دو طرف، قابلیت تبادل اطلاعات را دارند.

دو نوع شبکه سنکرون (Synchronous) داریم:

۱- دوطرفه غیر همزمان:

دوطرفه غیر همزمان: کارت شبکه A اطلاعات برای کارت B میفرستد و B تنها زمانی که کارت A فرستادن را تمام کرده است، جواب می‌دهد مثل برخی LANها. (شبکه تلفن بین المللی بی‌سیم)

۲- دوطرفه همزمان:

همزمان می‌توانند اطلاعات را بفرستند و بگیرند (تلفن شهری)

شبکه آسنکرون:

در این شبکه داده‌های ارسالی تنها می‌توانند از یک مسیر از مبدا به مقصد منتقل شوند و گذرگاه همیشه یکطرفه باقی میماند. اگر A فرستنده و B دریافت کننده باشد، همیشه از A به B انتقال داده صورت میپذیرد. یعنی فقط یک طرفه هستند (مانند رادیو – تلویزیون)

۶-۳- تکرار کننده (Repeater)

وسیله‌ای در تجهیزات شبکه است که در مدارات ارتباطی (معمولاً شبکه Bus) مورد استفاده قرار می‌گیرد و تضعیف سیگنال‌ها را از طریق تقویت یا تولید مجدد آن‌ها کاهش می‌دهد تا سیگنال‌ها با همان شکل اول به راه خود ادامه دهند. بدین ترتیب می‌توان سیگنال را بدون کاستی به فواصل دورتری فرستاد. این وسیله حداکثر فاصله‌ای را که یک کابل شبکه محلی می‌تواند گسترده شود افزایش دهد. استفاده از یک تکرارگر یک شبکه محلی را به دو قسمت تقسیم نمی‌کند و شبکه تقابلی نمی‌سازد. از آنجا که تکرارگرها با سیگنال‌های فیزیکی واقعی سروکار دارند و در جهت تفسیر داده‌ای که انتقال می‌دهند تلاشی نمی‌کنند، این تجهیز در **لایه فیزیکی** یعنی اولین لایه از مدل مرجع OSI عمل می‌کند.

این وسیله در واقع نوع خاصی از HUB است که فقط دارای ۲ پورت است.

۱. کار تکرارگر تقویت سیگنال‌های بین دو شبکه یا سگمنت‌های یک شبکه که فاصله‌ی زیادی از هم دارند می‌باشد.

۲. این قطعه در دو نوع Passive و Active قابل دسترس بوده است:

۱.۲. Passive Repeater: این نوع Repeater دو تا پورت دارد که هر یک به یک کابل شبکه متصل هستند و سیگنالی که از یک کابل دریافت کرده است از خود عبور می‌دهد و بر روی کابل دیگر می‌فرستد. به این ترتیب هیچگونه تغییری در سیگنال به وجود نیامده و تقویتی صورت نگرفته است بلکه Repeater مانند یک کانکتور (اتصال دهنده) عمل می‌کند و نیاز به منبع تغذیه و برق ندارد.

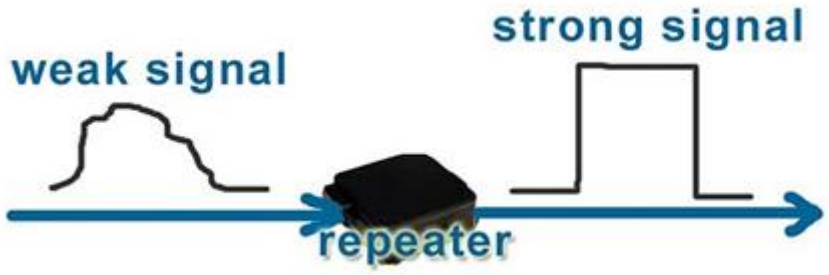
۲.۲. Active Repeater: در این نوع Repeater سیگنال دریافت شده را مجددا تقویت و بازسازی می‌کند، به طوری که به نظر می‌رسد که سیگنال جدید است. البته برای انجام چنین عملیاتی نیاز به منبع تغذیه و برق دارد.

به یاد داشته باشید که عملکرد Repeaterها صرفاً الکتریکی است و در لایه فیزیکی شبکه (لایه اول) عمل می‌کنند. به عبارت دیگر Repeaterها فقط سیگنال‌های الکتریکی ورودی را تقویت می‌کنند و بیرون می‌دهند و هیچ درکی از داده‌ها ندارند و قادر به هیچ نوع فیلتر کردن داده‌ها نیز نیستند.

اما تفاوت‌های دیگری نیز بین دو مدل Passive و Active وجود دارد:

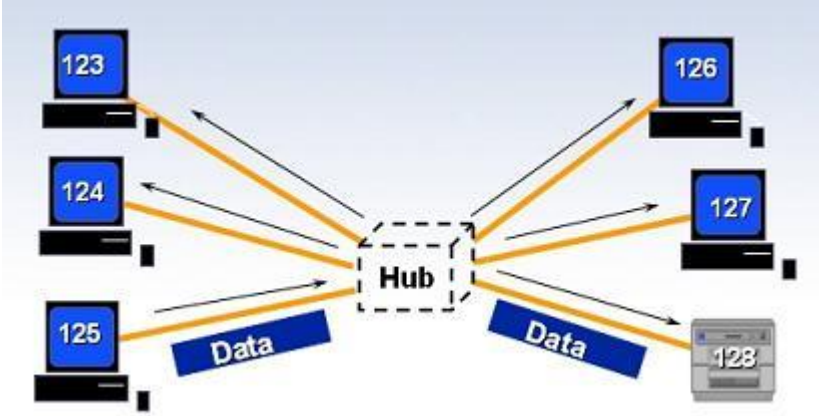
۱. نوع اول علاوه بر سیگنال هر چیز دیگری حتی نویز امواج نا خواسته که به همراه سیگنال اصلی که دارای اطلاعات است می‌باشند (Passive). مثلاً در امواج صوتی نویزی که باعث افت کیفیت صدا و شنیدن اصوات اضافه می‌شود را هم تقویت می‌کند.

۲. اما تکرار کننده‌ی نوع Active، سیگنال را قبل از ارسال بازدید کرده و چیزهای اضافه را خارج می‌کند و مثلاً دیگر نویز ر ا تقویت نمی‌کند.

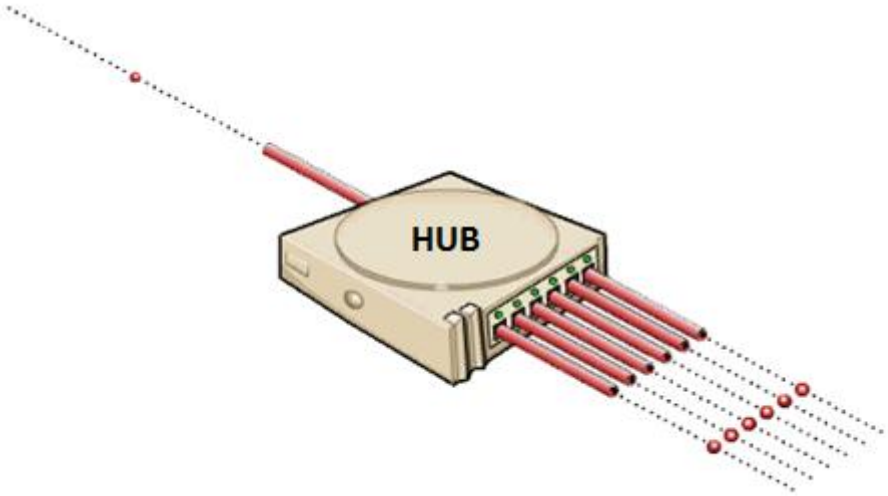


۶-۴- هاب (HUB)

هاب به وسیله‌ای گفته می‌شود که خطوط ارتباطی را در یک نقطه مرکزی به یکدیگر متصل می‌کند و اتصالات مشترکی برای تمامی وسایل فراهم می‌آورد.



هاب در مرکز شبکه‌های Star قرار می‌گیرد و تمام کامپیوترهای موجود در شبکه توسط یک کابل مستقل به آن متصل می‌شوند. هاب در حقیقت از ترکیب چندین Repeater ساخته شده است به این ترتیب که هریک از پورت‌های هاب، حکم یک Repeater را دارند. به عبارت دیگر یک پالس ورودی به یکی از پورت‌ها، به همه پورت‌های خروجی ارسال می‌شود.





به عبارت دیگر هاب‌ها، جهت اتصال گروهی از کاربران به یک شبکه محلی به کار می‌روند. هاب‌ها، کلیه بسته داده‌های دریافتی برروی یک درگاه از ایستگاه کاری را (همچون E-mail، اسناد Word، صفحه‌های گسترده گرافیک‌ها و درخواست‌های چاپ) به کلیه پورت‌های دیگر انتقال می‌دهند. کلیه کاربران متصل به یک هاب منفرد و یا گروهی از هاب‌های متصل، در یک ‘‘قطعه’’ قرار دارند، یعنی پهنای باند هاب یا ظرفیت انتقال داده‌ها را به اشتراک می‌گذارند. با افزایش تعداد کاربران به ‘‘قطعه’’، مسئله رقابت برای به دست گرفتن مقدار محدودی از پهنای باند اختصاص یافته به آن قطعه افزایش می‌یابد.

۶-۴-۱- انواع هاب

سه نوع هاب رایج وجود دارد:

الف – هاب فعال (Active):

که مانند آمپلی فایر عمل می‌کند و باعث تقویت مسیر عبور سیگنال‌ها می‌شود و از تصادم و برخورد سیگنال‌ها در مسیر جلوگیری به عمل می‌آورد. این هاب نسبتا قیمت بالایی دارد.

ب – غیر فعال (Passive):

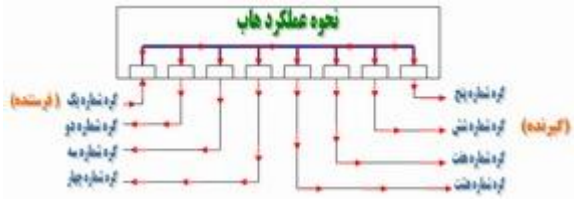
که بر خلاف نوع اول که در مورد تقویت انتقال سیگنال‌ها فعال است، این هاب منفعل بوده و هیچ برنامه و رفتاری جهت جلوگیری از تصادم ندارد.

ج – آمیخته (Mixed):

که قادر به ترکیب انواع رسانه‌ها " کابل کواکسیال نازک، ضخیم و.... " و باعث تعامل درون خطی میان سایر هاب‌ها می‌شود.

۶-۴-۲- آشنائی با نحوه عملکرد هاب

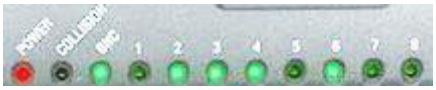
نحوه کار هاب بسیار ساده است. زمانی که یکی از کامپیوترهای متصل شده به هاب اقدام به ارسال داده‌ای می‌نماید، سایر پورت‌های هاب نیز آن را دریافت خواهند کرد (داده ارسالی تکرار و برای سایر پورت‌های هاب نیز فرستاده می‌شود). شکل زیر نحوه عملکرد هاب را نشان می‌دهد.



همانگونه که در شکل فوق مشاهده می‌نمائید، گره ۱ داده‌ای را برای گره ۶ ارسال می‌نماید، ولی تمامی گره‌های دیگر نیز داده را دریافت خواهند کرد. در ادامه، بررسی لازم در خصوص داده ارسالی توسط هر یک از گره‌ها انجام و در صورتی که تشخیص داده شود که داده ارسالی متعلق به آنان نیست، آن را نادیده خواهند گرفت. عملیات فوق از طریق کارت شبکه موجود بر روی کامپیوتر که آدرس MAC مقصد فریم ارسالی را بررسی می‌نماید، انجام می‌شود. کارت شبکه بررسی لازم را انجام و در صورت عدم مطابقت آدرس MAC موجود در فریم، با آدرس MAC کارت شبکه، فریم ارسالی دور انداخته می‌گردد.

اکثر هاب‌ها دارای یک پورت خاص می‌باشند که می‌تواند به صورت یک پورت معمولی و یا یک پورت Uplink رفتار نماید. با استفاده از یک پورت Uplink می‌توان یک هاب دیگر را به هاب موجود و به کمک کابل Straight، متصل نمود. بدین ترتیب تعداد پورت‌ها افزایش یافته و امکان اتصال تعداد بیشتری کامپیوتر به شبکه فراهم می‌گردد. روش فوق گزینه‌ای ارزان قیمت به منظور افزایش تعداد گره‌ها در یک شبکه است ولی با انجام این کار شبکه شلوغ‌تر شده و همواره بر روی آن حجم بالائی داده غیر ضروری در حال جابجائی است.

در اکثر هاب‌ها از یک LED به منظور نشان دادن فعال بودن ارتباط برقرار شده بین هاب و گره و از LED دیگر به منظور نشان دادن بروز یک Collision (تصادم – تصادف)، استفاده می‌گردد. (دو LED مجزا). در برخی از هاب‌ها دو LED مربوط به فعال بودن لینک ارتباطی بین هاب و گره و فعالیت پورت با یکدیگر ترکیب و زمانی که پورت در حال فعالیت است، LED مربوطه چشمک زن شده و زمانی که فعالیتی انجام نمی‌شود، LED فوق به صورت پیوسته روشن خواهد بود.



LED مربوط به Collision موجود بر روی هاب‌ها زمانی روشن می‌گردد که یک Collision به وجوداید. Collision زمانی به وجود می‌آید که دو کامپیوتر و یا گره سعی نمایند در یک لحظه بر روی شبکه صحبت نمایند. پس از بروز یک

Collision، فریم‌های مربوط به هر یک از گره‌ها با یکدیگر برخورد نموده و خراب می‌گردند. هاب به منظور تشخیص این نوع تصادم‌ها به اندازه کافی هوشمند بوده و برای مدت زمان کوتاهی چراغ مربوط به Collision روشن می‌گردد. (یک دهم ثانیه به ازای هر تصادم).

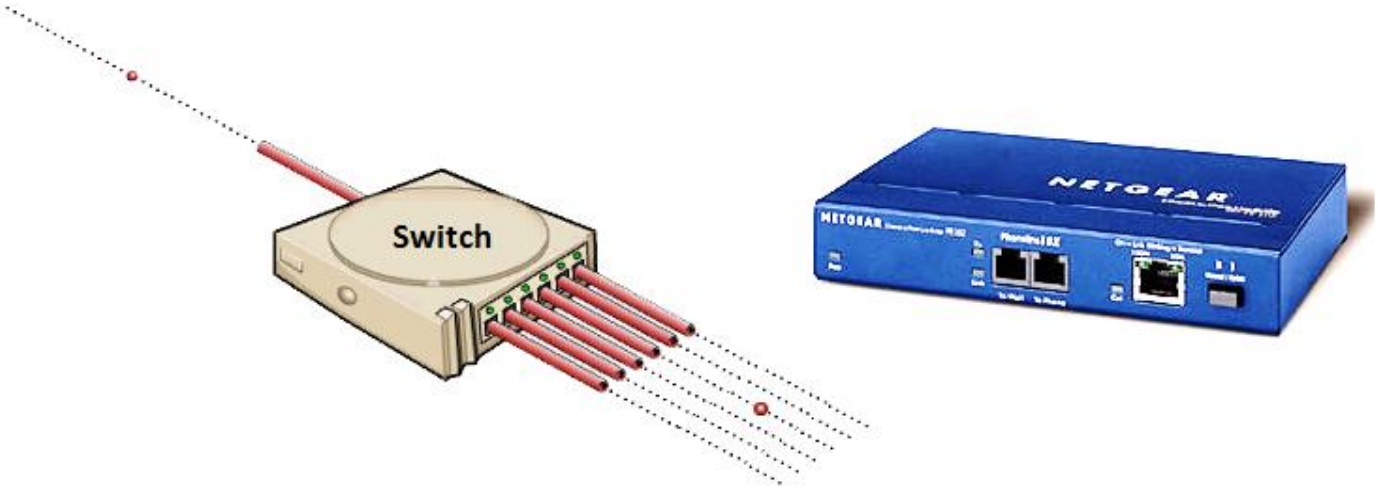
تعداد اندکی از هاب‌ها دارای یک اتصال خاص از نوع BNC بوده که می‌توان از آن به منظور اتصال یک کابل کواکسیال، استفاده نمود. پس از اتصال فوق، LED مربوط به اتصال BNC روی هاب روشن می‌گردد. لازم به ذکر است که این وسیله (HUB) امروزه دیگر تولید نمی‌شود و به جای آن در شبکه‌های امروزی از Switch استفاده می‌گردد.

به یاد داشته باشید که هاب نیز در لایه فیزیکی شبکه کار می‌کند و ضمن توزیع کردن سیگنال ورودی بین سایر پورت‌ها، سیگنال ورودی را تقویت نیز می‌کند. به این ترتیب در شبکه‌های Star در فواصل دور، برای اتصال کامپیوترها به یکدیگر نیز می‌توان از آن استفاده کرد.

۶-۵- سوئیچ (Switch)

سوئیچ یکی از عناصر اصلی و مهم در شبکه‌های کامپیوتری است. با استفاده از سوئیچ، چندین کاربر قادر به ارسال اطلاعات از طریق شبکه در یک لحظه خواهند بود. سرعت ارسال اطلاعات هر یک از کاربران بر سرعت دستیابی سایر کاربران شبکه تاثیر نخواهد گذاشت.

سوئیچ همانند روتر که امکان ارتباط بین چندین شبکه را فراهم می‌نماید، امکان ارتباط گره‌های متفاوت (معمولاً کامپیوتر) یک شبکه را مستقیماً با یکدیگر فراهم می‌نماید. شبکه‌ها و سوئیچ‌ها دارای انواع متفاوتی می‌باشند.



سوئیچ‌ها، هوشمندتر از هاب‌ها می‌باشند و به هر کاربر یا هر گروه از کاربران پهنای باند مشخصی را اختصاص می‌دهند. سوئیچ، بر اساس اطلاعات موجود در Header هر بسته، بسته داده‌ها را تنها به پورت گیرنده مورد نظر و متصل به شبکه LAN ارسال می‌کند. سوئیچ در هر انتقال ویژه باعث ایجاد تماس‌های فردی و موقت بین منابع و مقاصد شده و پس از اتمام مکالمه، به این تماس خاتمه می‌دهد.

به عبارت دیگر، سوئیچ وسیله‌ای است که بسته‌ها را مستقیماً به پورت‌های مرتبط با نشانی‌های خاص شبکه هدایت می‌کند. سوئیچ‌ها فهم بیشتری به مدیریت انتقال داده اضافه می‌کنند.

سوئیچ‌ها معمولاً در لایه ۲ مدل OSI هستند (سوئیچ لایه ۳ را بعدا توضیح می‌دهیم) و با تعداد پورت ۵، ۸، ۱۶، ۲۴ و گاهی ۳۶ و ۴۸ پورت نیز تولید می‌شوند. سرعت آن‌ها معمولاً ۱۰۰/۱۰ و یا ۱۰۰۰ مگابیت بر ثانیه است. سوئیچ‌ها دارای پورت های RJ-45 و یا فیبر نوری و یا ترکیبی از هر دو هستند. در دو نوع رومیزی و رکمونت (نصب در رک‌های ۱۹ اینچ استاندارد) وجود دارند.



سوئیچ هایی که برای هر یک از اتصالات موجود در یک شبکه داخلی استفاده می‌گردند، سوئیچ‌های LAN نامیده می‌شوند. این نوع سوئیچ‌ها مجموعه‌ای از ارتباطات شبکه را صرفاً بین دو دستگاه که قصد ارتباط با یکدیگر را دارند، در زمان مورد نظر ایجاد می‌نماید.

قبل از ادامه مباحث، به معرفی برخی اصطلاحات استفاده شده می‌پردازیم:

۱- **گره.** گره، شامل هر چیزی که به شبکه متصل می‌گردد، خواهد بود. (کامپیوتر، چاپگر و...)

۲- **سگمنت.** سگمنت یک بخش خاص از شبکه بوده که توسط یک سوئیچ، روتر و یا Bridge از سایر بخش‌ها جدا شده است.

۳- **ستون فقرات.** کابل اصلی که تمام سگمنت‌ها به آن متصل می‌گردند. معمولاً ستون فقرات یک شبکه دارای سرعت بمراتب بیشتری نسبت به هر یک از سگمنت‌های شبکه است. مثلاً ممکن است نرخ انتقال اطلاعات ستون فقرات شبکه ۱۰۰ مگابیت در ثانیه بوده در صورتیکه نرخ انتقال اطلاعات هر سگمنت ۱۰ مگابیت در ثانیه باشد.

۴- **توپولوژی.** روشی که هر یک از گره‌ها به یکدیگر متصل می‌گردند را گویند.

۵- **آدرس MAC.** آدرس فیزیکی هر دستگاه (کارت شبکه) در شبکه است. آدرس فوق یک عدد شش بایتی بوده که سه بایت اول آن مشخص کننده سازنده کارت شبکه و سه بایت دوم، شماره سریال کارت شبکه است.

۶- **Unicast.** ارسال اطلاعات توسط یک گره با آدرس خاص و دریافت اطلاعات توسط گره دیگر است.

۷- **Multicast.** یک گره، اطلاعاتی را برای یک گروه خاص (با آدرس مشخص یا الگویی خاص) ارسال می‌دارد. فقط دستگاه‌های موجود در گروه، اطلاعات ارسالی را دریافت خواهند کرد.

۸- **Broadcast.** یک گره اطلاعاتی را برای تمام گره‌های موجود در شبکه ارسال می‌نماید.

۶-۵-۱- استفاده از سوئیچ

در اکثر شبکه‌های متداول، به منظور اتصال گره‌ها از هاب استفاده می‌شود. همزمان با رشد شبکه (تعداد کاربران، تنوع نیازها، کاربردهای جدید شبکه و...) مشکلاتی در شبکه‌های **هاب** به وجود می‌آید:

۱. **Scalability:** در یک شبکه مبتنی بر هاب، پهنای باند به صورت مشترک توسط کاربران استفاده می‌گردد. با توجه به محدود بودن پهنای باند، همزمان با توسعه، کارآیی شبکه به شدت تحت تاثیر قرار خواهد گرفت. برنامه‌های کامپیوتر که امروزه به منظور اجراء بر روی محیط شبکه، طراحی می‌گردند به پهنای باند مناسبی نیاز خواهند داشت. عدم تامین پهنای باند مورد نیاز برنامه‌ها، تاثیر منفی در عملکرد آن‌ها را بدنبال خواهد داشت.

۲. **Latency:** به مدت زمانی که طول خواهد کشید تا بسته اطلاعاتی به مقصد مورد نظر خود برسد، اطلاق می‌گردد. با توجه به اینکه هر گره در شبکه‌های مبتنی بر هاب می‌بایست مدت زمانی را در انتظار سپری کرده (ممانعت از تصادم اطلاعات)، به موازات افزایش تعداد گره‌ها در شبکه، مدت زمان فوق افزایش خواهد یافت. در این نوع شبکه‌ها در صورتیکه یکی از کاربران فایل با ظرفیت بالائی را برای کاربر دیگر ارسال نماید، تمام کاربران دیگر می‌بایست در انتظار آزاد شدن محیط انتقال به منظور ارسال اطلاعات باشند. به هرحال افزایش مدت زمانی که یک بسته اطلاعاتی به مقصد خود برسد، هرگز مورد نظر کاربران یک شبکه نخواهد بود.

۳. **Network Failure:** در شبکه‌های مبتنی بر هاب، یکی از دستگاه‌های متصل شده به هاب قادر به ایجاد مسائل و مشکلاتی برای سایر دستگاه‌های موجود در شبکه خواهد بود. عامل بروز اشکال می‌تواند عدم تنظیم مناسب سرعت (مثلاً تنظیم سرعت یک هاب با قابلیت ۱۰ مگابیت در ثانیه به ۱۰۰ مگابیت در ثانیه) و یا ارسال بیش از حد بسته‌های اطلاعاتی از نوع Broadcast، باشد.

۴. **Collisions:** در شبکه‌های مبتنی بر تکنولوژی اترنت (Ethernet) از فرآیند خاصی با نام CSMA/CD به منظور ارتباط در شبکه استفاده می‌گردد. فرآیند فوق نحوه استفاده از محیط انتقال به منظور ارسال اطلاعات را قانونمند می‌نماید. در چنین شبکه هایی تا زمانی که بر روی محیط انتقال ترافیک اطلاعاتی باشد، گره‌ای دیگر قادر به ارسال اطلاعات نخواهد بود. در صورتیکه دو گره در یک لحظه اقدام به ارسال اطلاعات نمایند، یک تصادم اطلاعاتی ایجاد و عملاً بسته‌های اطلاعاتی ارسالی توسط هر یک از گره‌ها نیز از بین خواهند رفت. هر یک از گره‌های مربوطه (تصادم کننده) می‌بایست بمدت زمان کاملاً تصادفی در انتظار باقی مانده و پس از فراهم شدن شرایط ارسال، اقدام به ارسال اطلاعات مورد نظر خود نمایند.

هاب مسیر ارسال اطلاعات از یک گره به گره دیگر را به حداقل مقدار خود می‌رساند ولی عملاً شبکه را به سگمنت‌های گسسته تقسیم نمی‌نماید. سوئیچ به منظور تحقق خواسته فوق عرضه شده است. یکی از مهمترین تفاوت‌های موجود بین هاب و سوئیچ، تفسیر هر یک از پهنای باند است. تمام دستگاه‌های متصل شده به هاب، پهنای باند موجود را بین خود به اشتراک می‌گذارند. در صورتیکه یک دستگاه متصل شده به سوئیچ، دارای تمام پهنای باند مختص خود است. مثلاً در صورتیکه ۱۰ گره به هاب متصل شده باشند، (در یک شبکه ۱۰ مگابیت در ثانیه) هر گره موجود در شبکه بخشی از تمام پهنای باند موجود (۱۰ مگابیت در ثانیه) را اشغال خواهد کرد (یعنی هر یک ۱ مگابیت در ثانیه، البته در صورتیکه سایر گره‌ها نیز قصد ارتباط را داشته باشند). در سوئیچ، هر یک از گره‌ها قادر به برقراری ارتباط با سایر گره‌ها با سرعت ۱۰ مگابیت در ثانیه خواهد بود.

در یک شبکه مبتنی بر سوئیچ، برای هر گره، یک سگمنت اختصاصی ایجاد خواهد شد. سگمنت‌های فوق به یک سوئیچ متصل خواهند شد. در حقیقت سوئیچ امکان حمایت از چندین (در برخی حالات صدها) سگمنت اختصاصی را دارا است. با توجه به اینکه تنها دستگاه‌های موجود در هر سگمنت سوئیچ و گره می‌باشند، سوئیچ قادر به انتخاب اطلاعات، قبل از رسیدن به سایر گره‌ها خواهد بود. در ادامه، سوئیچ فریم‌های اطلاعاتی را به سگمنت مورد نظر هدایت خواهد کرد. با توجه به اینکه هر سگمنت دارای صرفاً یک گره می‌باشد، اطلاعات مورد نظر به مقصد مورد نظر ارسال خواهند شد. بدین ترتیب در شبکه‌های مبتنی بر سوئیچ امکان چندین مبادله اطلاعاتی به صورت همزمان وجود خواهد داشت.

با استفاده از سوئیچ، شبکه‌های اترنت به صورت Full-Duplex خواهند بود. قبل از مطرح شدن سوئیچ، اترنت به صورت Half-Duplex بود. در چنین حالتی داده‌ها در هر لحظه امکان ارسال در یک جهت را دارا می‌باشند. در یک شبکه مبتنی بر سوئیچ، هر گره صرفاً با سوئیچ ارتباط برقرار می‌نماید (گره‌ها مستقیماً با یکدیگر ارتباط برقرار نمی‌نمایند). در چنین حالتی اطلاعات از گره به سوئیچ و از سوئیچ به گره مقصد به صورت همزمان منتقل می‌گردند.

در شبکه‌های مبتنی بر سوئیچ امکان استفاده از کابل‌های بهم تابیده و یا فیبر نوری وجود خواهد داشت. هر یک از کابل‌های فوق دارای کانکتورهای مربوط به خود برای ارسال و دریافت اطلاعات می‌باشند. با استفاده از سوئیچ، شبکه‌ای عاری از تصادم اطلاعاتی به وجود خواهد آمد. انتقال دو سویه اطلاعات در شبکه‌های مبتنی بر سوئیچ، سرعت ارسال و دریافت اطلاعات افزایش می‌یابد.

اکثر شبکه‌های مبتنی بر سوئیچ به دلیل قیمت بالای سوئیچ، صرفاً از سوئیچ به تنهایی استفاده نمی‌نمایند. در این نوع شبکه‌ها از ترکیب هاب و سوئیچ استفاده می‌گردد. مثلاً یک سازمان می‌تواند از چندین هاب به منظور اتصال کامپیوترهای موجود در هر یک از دپارتمآن‌های خود استفاده و در ادامه با استفاده از یک سوئیچ تمام هاب‌ها (مربوط به هر یک از دپارتمان ها) به یکدیگر متصل می‌گردد.

۶-۵-۲- تکنولوژی سوئیچ‌ها

سوئیچ‌ها دارای پتانسیل‌های لازم به منظور تغییر روش ارتباط هر یک از گره‌ها با یکدیگر می‌باشند. تفاوت سوئیچ با روتر چیست؟ سوئیچ‌ها معمولاً در لایه دوم (Data layer) مدل OSI فعالیت می‌نمایند. در لایه فوق امکان استفاده از آدرس‌های MAC (آدرس‌های فیزیکی) وجود دارد. روتر در لایه سوم (Network) مدل OSI فعالیت می‌نمایند. در لایه فوق از آدرس‌های IP ر IPX و یا Apple Talk استفاده می‌شود. (آدرس‌های منطقی). الگوریتم استفاده شده توسط سوئیچ به منظور اتخاذ تصمیم در رابطه با مقصد یک بسته اطلاعاتی با الگوریتم استفاده شده توسط روتر، متفاوت است.

یکی از موارد اختلاف الگوریتم‌های سوئیچ و هاب، نحوه برخورد آنان با Broadcast است. مفهوم بسته‌های اطلاعاتی از نوع Broadcast در تمام شبکه‌ها مشابه می‌باشد. در چنین مواردی، دستگاهی نیاز به ارسال اطلاعات داشته ولی نمی‌داند که اطلاعات را برای چه کسی می‌بایست ارسال نماید. به دلیل عدم آگاهی و دانش نسبت به هویت دریافت کننده اطلاعات، دستگاه مورد نظر اقدام به ارسال اطلاعات به صورت Broadcast می‌نماید. مثلاً هر زمان که کامپیوتر جدید و یا یک دستگاه به شبکه وارد می‌شود، یک بسته اطلاعاتی از نوع Broadcast برای معرفی و حضور خود در شبکه ارسال می‌دارد. سایر گره‌ها قادر به افزودن کامپیوتر مورد نظر در لیست خود و برقراری ارتباط با آن خواهند بود. بنابراین بسته‌های اطلاعاتی از نوع

Broadcast در مواردی که یک دستگاه نیاز به معرفی خود به سایر بخش‌های شبکه را داشته و یا نسبت به هویت دریافت کننده اطلاعات شناخت لازم وجود نداشته باشند، استفاده می‌گردند.

هاب و یا سوئیچ‌ها قادر به ارسال بسته‌ای اطلاعاتی از نوع Broadcast برای سایر سگمنت‌های موجود در حوزه Broadcast می‌باشند. روتر عملیات فوق را انجام نمی‌دهد. در صورتیکه آدرس یک دستگاه مشخص نگردد، روتر قادر به مسیر یابی بسته اطلاعاتی مورد نظر نخواهد بود. ویژگی فوق در مواردی که قصد جداسازی شبکه‌ها از یکدیگر مد نظر باشد، بسیار ایده آل خواهد بود. ولی زمانیکه هدف مبادله اطلاعاتی بین بخش‌های متفاوت یک شبکه باشد، مطلوب به نظر نمیاید. سوئیچ‌ها با هدف برخورد با مشکل فوق عرضه شده‌اند.

سوئیچ‌های LAN بر اساس تکنولوژی Packet-Switching فعالیت می‌نمایند. سوئیچ یک ارتباط بین دو سگمنت ایجاد می‌نماید. بسته‌های اطلاعاتی اولیه در یک محل موقت (بافر) ذخیره می‌گردند، آدرس فیزیکی (MAC) موجود در هدر خوانده شده و در ادامه با لیستی از آدرس‌های موجود در جدول Lookup (جستجو) مقایسه می‌گردد. در شبکه‌های LAN مبتنی بر اترنت، هر فریم اترنت شامل یک بسته اطلاعاتی خاص است. بسته اطلاعاتی فوق شامل یک عنوان (هدر) خاص و شامل اطلاعات مربوط به آدرس فرستنده و گیرنده بسته اطلاعاتی است.

سوئیچ‌های مبتنی بر بسته‌های اطلاعاتی، به منظور مسیر یابی ترافیک موجود در شبکه از سه روش زیر استفاده می‌نمایند.

1. **Cut-Through**
2. **Store-and-forward**
3. **Fragment-free**

Cut-Through

سوئیچ‌های Cut-through، بلافاصله پس از تشخیص بسته اطلاعاتی توسط سوئیچ، آدرس MAC خوانده می‌شود. پس از ذخیره سازی شش بایت اطلاعات که شامل آدرس می‌باشند، بلافاصله عملیات ارسال بسته‌های اطلاعاتی به گره مقصد آغاز می‌گردد. (همزمان با دریافت سایر بسته‌های اطلاعاتی توسط سوئیچ). با توجه به عدم وجود کنترل‌های لازم در صورت بروز خطا در روش فوق، سوئیچ‌های زیادی از روش فوق استفاده نمی‌نمایند.

Store-and-forward

سوئیچ‌های Store-And-Forward، تمام بسته اطلاعاتی را در بافر مربوطه ذخیره و عملیات مربوط به بررسی خطا (CRC) و سایر مسائل مربوطه را قبل از ارسال اطلاعات انجام خواهند داد. در صورتی که بسته اطلاعاتی دارای خطا باشد، بسته اطلاعاتی دور انداخته خواهد شد.. در غیر اینصورت، سوئیچ با استفاده از آدرس MAC، بسته اطلاعاتی را برای گره مقصد ارسال می‌نماید. اغلب سوئیچ‌ها از ترکیب دو روش گفته شده استفاده می‌نمایند. در این نوع سوئیچ‌ها از روش Cut-Through استفاده شده و به محض بروز خطا از روش Store-And-Forward استفاده می‌نمایند.

Fragment-free

یکی دیگر از روش‌های مسیر یابی ترافیک در سوئیچ‌ها که کمتر استفاده می‌گردد، Fragment-Free است. روش فوق مشابه Cut-Through بوده با این تفاوت که قبل از ارسال بسته اطلاعاتی ۶۴ بایت آن ذخیره می‌گردد.

۶-۵-۳- انواع سوئیچ LAN

سوئیچ‌های LAN دارای مدل‌های متفاوت از نقطه نظر طراحی فیزیکی می‌باشند. سه مدل رایج در حال حاضر بشرح زیر می‌باشند:

۱- **Shared Memory:** این نوع از سوئیچ‌ها تمام بسته‌های اطلاعاتی اولیه در بافر مربوط به خود را ذخیره می‌نمایند. بافر فوق به صورت مشترک توسط تمام پورت‌های سوئیچ (اتصالات ورودی و خروجی) استفاده می‌گردد. در ادامه اطلاعات مورد نظر به کمک پورت مربوطه برای گره مقصد ارسال خواهند شد.

۲- **Matrix:** این نوع از سوئیچ‌ها دارای یک شبکه (تور) داخلی ماتریس مانند بوده که پورت‌های ورودی و خروجی همدیگر را قطع می‌نمایند. زمانیکه یک بسته اطلاعاتی بر روی پورت ورودی تشخیص داده شد، آدرس MAC آن با جدول Lookup مقایسه تا پورت مورد نظر خروجی آن مشخص گردد. در ادامه سوئیچ یک ارتباط را از طریق شبکه و در محلی که پورت‌ها همدیگر را قطع می‌کنند، برقرار می‌گردد.

۳- **Bus Architecture:** در این نوع از سوئیچ‌ها به جای استفاده از یک شبکه (تور)، از یک مسیر انتقال داخلی (Bus) استفاده و مسیر فوق با استفاده از TDMA توسط تمام پورت‌ها به اشتراک گذاشته می‌شود. سوئیچ‌های فوق برای هر یک از پورت‌ها دارای یک حافظه اختصاصی می‌باشند.

۴- **Transparent Bridging:** اکثر سوئیچ‌های LAN مبتنی بر اترنت از سیستمی با نام Transparent Bridging برای ایجاد جداول آدرس Lookup استفاده می‌نمایند. تکنولوژی فوق امکان یادگیری هر چیزی در رابطه با محل گره‌های موجود در شبکه، بدون حمایت مدیریت شبکه را فراهم می‌نماید. تکنولوژی فوق داری پنج بخش متفاوت است:

1. **Learning**
2. **Flooding**
3. **Filtering**
4. **Forwarding**
5. **Aging**

نحوه عملکرد تکنولوژی فوق بشرح زیر است:

- سوئیچ به شبکه اضافه شده و تمام سگمنت‌ها به پورت‌های سوئیچ متصل خواهند شد.
- گره A بر روی اولین سگمنت (سگمنت A)، اطلاعاتی را برای کامپیوتر دیگر (گره B) در سگمنت دیگر (سگمنت C) ارسال می‌دارد.
- سوئیچ اولین بسته اطلاعاتی را از گره A دریافت می‌نماید. آدرس MAC آن خوانده شده و آن را در جدول Lookup سگمنت A ذخیره می‌نماید. بدین ترتیب سوئیچ از نحوه یافتن گره A آگاهی پیدا کرده و اگر در آینده گره‌ای قصد ارسال اطلاعات برای گره A را داشته باشد، سوئیچ در رابطه با آدرس آن مشکلی نخواهد داشت. فرآیند فوق را Learning می‌گویند.

– با توجه به اینکه سوئیچ دانشی نسبت به محل گره B ندارد، یک بسته اطلاعاتی را برای تمام سگمنت‌های موجود در شبکه (بجز سگمنت A که اخیراً یکی از گره‌های موجود در آن اقدام به ارسال اطلاعات نموده است.) فرآیند ارسال یک بسته اطلاعاتی توسط سوئیچ، به منظور یافتن یک گره خاص برای تمام سگمنت‌ها، Flooding نامیده می‌شود.

– گره B بسته اطلاعاتی را دریافت و یک بسته اطلاعاتی را به عنوان Acknowledgement برای گره A ارسال خواهد کرد.

– بسته اطلاعاتی ارسالی توسط گره B به سوئیچ می‌رسد. در این زمان، سوئیچ قادر به ذخیره کردن آدرس MAC گره B در جدول Lookup سگمنت C می‌باشد. با توجه به اینکه سوئیچ از آدرس گره A آگاهی دارد، بسته اطلاعاتی را مستقیماً برای آن ارسال خواهد کرد. گره A در سگمنتی متفاوت نسبت به گره B قرار دارد، بنابراین سوئیچ می‌بایست به منظور ارسال بسته اطلاعاتی دو سگمنت را به یکدیگر متصل نمائید. فرآیند فوق Forwarding نامیده می‌شود.

– در ادامه بسته اطلاعاتی بعدی از گره A به منظور ارسال برای گره B به سوئیچ می‌رسد، با توجه به اینکه سوئیچ از آدرس گره B آگاهی دارد، بسته اطلاعاتی فوق مستقیماً برای گره B ارسال خواهد شد.

– گره C اطلاعاتی را از طریق سوئیچ برای گره A ارسال می‌دارد. سوئیچ آدرس MAC گره C را در جدول Lookup سگمنت A ذخیره می‌نماید، سوئیچ آدرس گره A را دانسته و مشخص می‌گردد که دو گره A و C در یک سگمنت قرار دارند. بنابراین نیازی به ارتباط سگمنت A با سگمنت دیگر به منظور ارسال اطلاعات گره C نخواهد بود. بدین ترتیب سوئیچ از حرکت بسته‌های اطلاعاتی بین گره‌های موجود در یک سگمنت ممانعت می‌نماید. فرآیند فوق را Filtering می‌گویند.

– Learning و Flooding ادامه یافته و به موازات آن سوئیچ، آدرس‌های MAC مربوط به گره‌ها را در جداول Lookup ذخیره می‌نماید. اکثر سوئیچ‌ها دارای حافظه کافی به منظور ذخیره سازی جداول Lookup می‌باشند. به منظور بهینه سازی حافظه فوق، اطلاعات قدیمی‌تر از جداول فوق حذف تا فرآیند جستجو و یافتن آدرس‌ها در یک زمان معقول و سریعتر انجام پذیرد. بدین منظور سوئیچ‌ها از روشی با نام Aging استفاده می‌نمایند. زمانیکه یک Entry برای یک گره در جدول Lookup اضافه می‌گردد، به آن یک زمان خاص نسبت داده می‌شود. هر زمان که بسته‌ای اطلاعاتی از طریق یک گره دریافت می‌گردد، زمان مورد نظر بهنگام می‌گردد. سوئیچ دارای یک زمان سنج قابل پیکربندی بوده که باعث می‌شود، Entryهای موجود در جدول Lookup که مدت زمان خاصی از آن‌ها استفاده نشده و یا به آن‌ها مراجعه‌ای نشده است، حذف گردند. با حذف Entryهای غیر ضروری، حافظه قابل استفاده برای سایر Entryها بیشتر می‌گردد.

در مثال فوق، دو گره سگمنت A را به اشتراک گذاشته و سگمنت‌های A و D به صورت مستقل می‌باشند. در شبکه‌های ایده آل مبتنی بر سوئیچ، هر گره دارای سگمنت اختصاصی مربوط بخود است. بدین ترتیب امکان تصادم حذف و نیازی به عملیات Filtering نخواهد بود.

۶-۵-۴- روترها و سوئیچینگ لایه سوم

همانگونه که قبلاً اشاره گردید، اکثر سوئیچ‌ها در لایه دوم مدل OSI فعالیت می‌نمایند (Data Layer). اخیراً برخی از تولیدکنندگان سوئیچ، مدلی را عرضه نموده‌اند که قادر به فعالیت در لایه سوم مدل OSI است (Network Layer). این نوع سوئیچ‌ها دارای شباهت زیادی با روتر می‌باشند.

زمانی که روتر یک بسته اطلاعاتی را دریافت می‌نماید، در لایه سوم به دنبال آدرس‌های مبداء و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ‌های استاندارد از آدرس‌های MAC به منظور مشخص کردن آدرس مبداء و مقصد استفاده می‌نمایند (از طریق لایه دوم). مهمترین تفاوت بین یک روتر و یک سوئیچ لایه سوم، استفاده سوئیچ‌های لایه سوم از سخت‌افزارهای بهینه به منظور ارسال داده با سرعت مطلوب نظیر سوئیچ‌های لایه دوم است. نحوه تصمیم گیری آن‌ها در رابطه با مسیر یابی بسته‌های اطلاعاتی مشابه روتر است. در یک محیط شبکه‌ای LAN، سوئیچ‌های لایه سوم معمولاً دارای سرعتی بیشتر از روتر می‌باشند. علت این امر استفاده از سخت‌افزارهای سوئیچینگ در این نوع سوئیچ‌ها است. اغلب سوئیچ‌های لایه سوم شرکت سیسکو، به منزله روتر هایی می‌باشند که به مراتب از روترها سریعتر بوده (با توجه به استفاده از سخت‌افزارهای اختصاصی سوئیچینگ) و دارای قیمت ارزان تری نسبت به روتر می‌باشند. نحوه Pattern Matching و Caching در سوئیچ‌های لایه سوم مشابه یک روتر است. در هر دو دستگاه از یک پروتکل روتینگ و جدول روتینگ، به منظور مشخص نمودن بهترین مسیر استفاده می‌گردد. سوئیچ‌های لایه سوم قادر به برنامه ریزی مجدد سخت‌افزار به صورت پویا و با استفاده از اطلاعات روتینگ لایه سوم می‌باشند و همین امر باعث سرعت بالای پردازش بسته‌های اطلاعاتی می‌گردد. سوئیچ‌های لایه سوم، از اطلاعات دریافت شده توسط پروتکل روتینگ به منظور بهنگام سازی جداول مربوط به Caching استفاده می‌نمایند.

همانگونه که ملاحظه گردید، در طراحی سوئیچ‌های LAN از تکنولوژی‌های متفاوتی استفاده می‌گردد. نوع سوئیچ استفاده شده، تاثیر مستقیم بر سرعت و کیفیت یک شبکه را بدنبال خواهد داشت.

۶-۵-۵- سوئیچ‌های مدیریتی

برای کنترل و نگهداری شبکه‌های بزرگ و یا شبکه هایی که نیاز به پهنای باند زیاد و کنترل شده دارند نیاز به استفاده از سوئیچ‌های مدیریتی است. با اینگونه سوئیچ‌ها می‌توان تنظیمات متنوعی از قبیل پهنای باند، شبکه‌های مجازی، کنترل و گزارشات ترافیکی شبکه و... را انجام داد. از مشخصاتی که تقریباً در تمام آن‌ها مشترک است می‌توان به رکمونت بودن، تعداد ۲۴ پورت به بالا، امکان افزودن چندین نوع ماژول برای کاربردهای مختلف، وجود پورت سریال برای مدیریت مستقیم، امکان مدیریت از طریق وب، دارا بودن نرم‌افزار مدیریتی، پاورهای اضافی و قیمت بسیار بالا نسبت به سوئیچ‌های رایج اشاره کرد. سرعت سوئیچ کردن داخلی و همچنین حجم داده انتقالی در زمان واحد از جمله مشخصات مهم سوئیچ‌ها و تعیین کننده قیمت آن‌ها می‌باشد. برخی از این سوئیچ‌ها امکان مدیریت در لایه ۲ شبکه و بالاتر را نیز دارند.

۶-۵-۶- ماژول سوئیچ

ماژول‌ها قطعاتی سخت‌افزاری هستند که به سخت‌افزار اصلی متصل شده و امکاناتی را بسته به نیاز شبکه به آن اضافه می‌نمایند. به سوئیچ هایی که دارای ورودی برای نصب ماژول هستند سوئیچ‌های ماژولار گفته می‌شود. جدیدترین ماژول‌ها، ماژول‌های SFP یا Mini GIBIC هستند که انواع پورت‌های گیگابیت بر روی فیبر نوری و کابل مسی ارائه می‌کنند. سوئیچ ماژولار این امکان را به طراح شبکه میدهد تا بتواند چندین نوع مدیا را در کنار هم داشته باشند.



۶-۵-۷- مزایای سوئیچ

۱. یک سوئیچ اترنت مزایای زیادی دارد، از قبیل اجازه به تعدادی کاربر برای برقراری ارتباط موازی از طریق استفاده از مدارهای مجازی و قسمتهای اختصاصی شبکه در یک محیط عاری از برخورد، یعنی از طریق پهنای باند بیشتر آزاد و هر کاربر پهنای باند مخصوص به خود دارد.

۲. مزیت دیگر آن این است که جایگزینی آن با هاب به سادگی انجام پذیر است و نیازی به تعویض سخت‌افزار و کابل‌های موجود نمی‌باشد و بالاخره مدیر شبکه به سادگی می‌تواند آنرا مدیریت کند.

۳. سوئیچ‌ها در لایه پیوند داده‌ای (از لایه‌های شبکه) کار می‌کنند و همانند پل‌ها اجازه اتصال Segmentهای LAN به یکدیگر برای تشکیل یک شبکه بزرگتر را می‌دهند.

۴. سوئیچ‌ها ترافیک را کاهش می‌دهد و در نتیجه نسبت به دیگر تجهیزات فعال شبکه از سرعت بالاتری برخوردار هستند و می‌توانند از کاربرهای جدیدی همانند VLAN (LAN مجازی) پشتیبانی کنند.

۶-۵-۸- از چه نوع سوئیچ هایی استفاده کنیم؟

با توجه به طرح توسعه شبکه دولت، مطرح شده از طرف نهاد ریاست جمهوری در راستای اجرای پروژه دولت الکترونیکی که بر اساس فن آوری جدید 1000 Mbps (GIGABIT ETHERNET) طراحی شده، بهتر است در شبکه هایی که هنوز راه اندازی نشده‌اند و مراحل طراحی را طی می‌نمایند از سوئیچ هایی با امکانات وجود یک یا دو یا چند پورت فعال 1000 Mbps استفاده نماییم. همچنین در این طرح (شبکه دولت) مسئله امنیت شبکه حائز اهمیت می‌باشد، به همین دلیل بهتر است یکباره از سوئیچ هایی استفاده نماییم که در آن‌ها یک تکنولوژی جدید بنام IP SECURITY جهت بالا بردن امنیت شبکه بکار گرفته شده است، بدین صورت که امکان تخصیص یک پورت خاص به یک ترمینال خاص را دارد، چنانکه یک تغییر فیزیکی در محل پورت سوئیچ و جابجایی کامپیوترها بدون هماهنگی با مدیر شبکه رخ دهد، امکان استفاده از شبکه از بین خواهد رفت.

محل نصب سوئیچ در شبکه در Backbone (کانال اصلی انتقال داده ها) و یا در Gateways (ورودی ها) که دو شبکه را به هم مرتبط می‌سازند می‌باشد.

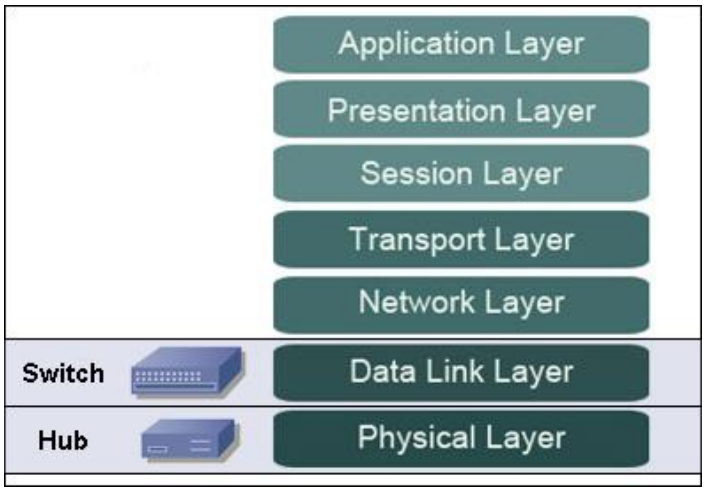
۶-۵-۹- تفاوت HUB با Switch

هاب و سوئیچ در اصل عملکرد یکسانی را انجام می‌دهند، اگرچه روش‌های انجام کار آن‌ها متفاوت می‌باشد. از هر دو آن‌ها در جهت احیای سیگنال‌های ضعیف شده استفاده می‌شود، همچنین هر دو آن‌ها توانایی تقسیم و جداسازی یک سیگنال

به چند سیگنال را نیز دارا می‌باشند. اما شما باید مراقب عملکرد انجام کار آن‌ها باشید. اگر هر دو آن‌ها اعمال یکسانی را انجام می‌دهند پس در چه مواردی متفاوت هستند؟

۶-۵-۱۰- هاب چیست؟

هاب در مدل OSI در لایه فیزیکی عمل می‌کند. از طرف دیگر، سوئیچ قدری هوشمندتر بوده و در مدل OSI در لایه انتقال داده (Data Link) عمل می‌کند.



زمانی که هاب از یک پورت اطلاعاتی را دریافت می‌کند، آن اطلاعات را به همه پورت‌ها پخش می‌کند. این عملکرد در هاب باعث هدر رفتن پهنای باند و ایجاد تداخل می‌شود.

تصور کنید که دو کامپیوتر به صورت همزمان اقدام به ارسال اطلاعات کنند، بسته‌های اطلاعات با یکدیگر برخورد کرده و در اثر این تداخل، اطلاعات دچار مشکل می‌شوند. در این شرایط ما مجبور به دوباره تکرار کردن اطلاعات از طریق فرآیند CSMA/CD که مخفف Carrier Sense Multiple Access / Collision Detection می‌باشد هستیم. به عبارت ساده تر، این فرآیند یک پروتکل می‌باشد که ما با استفاده از آن داده را دوباره ارسال می‌کنیم، قبل از اینکه تداخل رخ دهد.

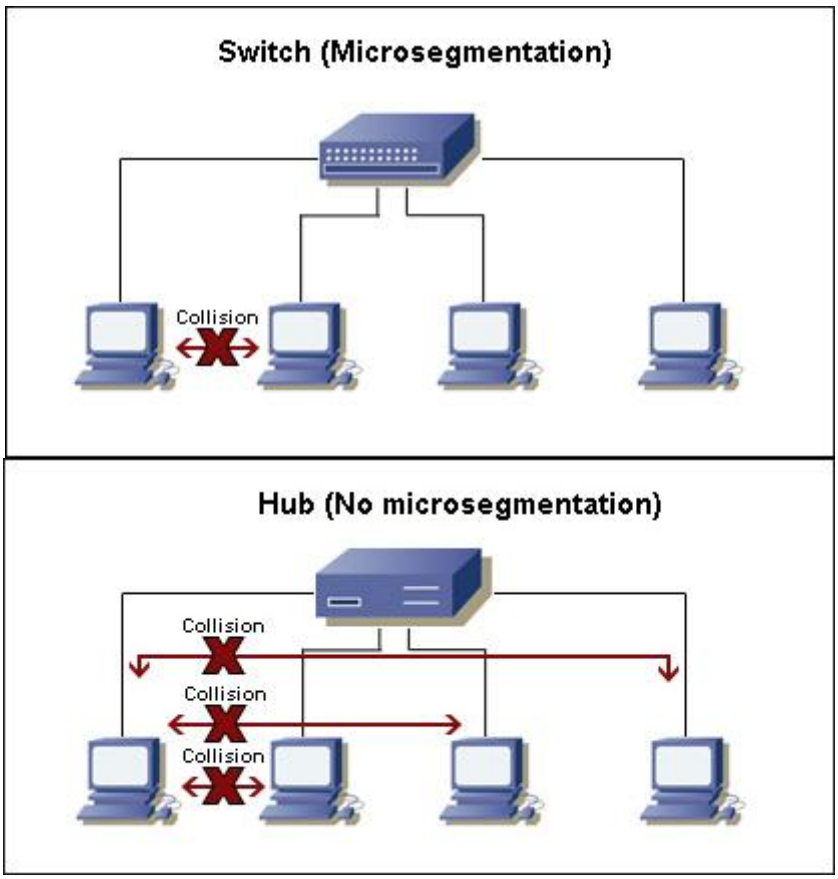
تداخل‌ها معمولاً مسئله‌ای در هاب‌ها می‌باشند. اما مسئله مهمتر این است که هاب‌ها پهنای باند را نیز هدر می‌دهند. هاب‌ها به صورت یکطرفه عمل می‌کنند، بدین معنی که در یک زمان اطلاعات فقط می‌توانند در یک مسیر حرکت کنند. از آنجایی که ما به صورت یکطرفه عمل می‌کنیم، پهنای باند باید بین هر پورت در هاب تقسیم بندی شود. تصور کنید که شما یک هاب ۲۰ پورت و یک سرعت ۲۰ کیلوبیت در ثانیه داریم. جالب است، اما شما فقط می‌توانید به هر کامپیوتر در شبکه ۱ کیلوبیت در ثانیه اختصاص دهید.

۶-۵-۱۱- سوئیچ چیست؟

در مدل OSI، سوئیچ در لایه انتقال داده (Data Link) عمل می‌کند. این بدان معنی است که سوئیچ هوشمندتر از هاب می‌باشد، بطوریکه سوئیچ در یک سطح پویا داده‌ها را مسیر دهی نماید. اگر اطلاعات بطور مثال مقصد معینی برای کامپیوتر A دارند سوئیچ فقط اطلاعات را به سمت کامپیوتر A مسیر دهی می‌کند.

برای جلوگیری از برخورد و تداخل آدرس‌دهی، سوئیچ‌ها از Micro Segmentation استفاده می‌کنند. Micro Segmentation اجازه‌ی تقسیم بندی دامنه‌های تداخل می‌دهد.

اجازه بدهید مثالی بزنیم، در شکل زیر، دامنه‌های تداخل بسیاری برای سوئیچ وجود دارند. برای نمونه اگر کامپیوترهای A و B در یک زمان با هم اقدام به ارسال اطلاعات نمایند، ممکن است تداخل به وجوداید. کامپیوتر A با کامپیوتر C یا کامپیوتر D، به هرحال هیچکدام فرآیند تداخل را تجربه نمی‌کنند. در یک شبکه مجهز به هاب، فقط یک دامنه تداخل وجود دارد. بدین معنی که اگر کامپیوتر اول بخواهد داده انتقال دهد، آن می‌تواند به صورت فاصله دار این کار را نسبت به کامپیوترهای دیگر شبکه انجام دهد.



سوئیچ می‌تواند آدرس یک کامپیوتر مورد پردازش قرار دهد که آیا یک پورت معین می‌باشد. اگر مقصد اطلاعات به سمت کامپیوتر A می‌باشد، اطلاعات فقط از طریق پورت کامپیوتر A انتقال داده می‌شود. بخاطر دارید که هاب چگونه پهنای باند را بین هر پورت تقسیم می‌کرد؟ تکنولوژی Micro Segmentation به ما این اجازه را می‌دهد که پهنای باند را برای هر کامپیوتر در بالاترین حد ممکن قرار دهیم. اگر 20 kb/s سرعت داریم هر کامپیوتر می‌تواند تمام 20 Kb/s را به خود اختصاص می‌دهد. (توجه داشته باشید که سوئیچ جادوگری نمی‌کند، اگر دو یا چند کامپیوتر در یک زمان در خط هستند، باید پهنای باند بین آن‌ها تقسیم شود. در حال حاضر این تکنولوژی بهتر از هاب می‌باشد، به این دلیل که زمانیکه کامپیوتر در خط نیست پهنای باند به صورت اتوماتیک در خط تقسیم می‌شود.)

۶-۵-۱۲- آیا باید ما از هاب به سوئیچ ارتقاء پیدا کنیم؟

جواب این سوال قطعی است. بله. هاب‌ها ارزان‌تر و نصب آن‌ها نیز ساده‌تر می‌باشد. اما عملکرد مناسبی ندارند و پهنای باند را نیز هدر می‌دهند. سوئیچ‌ها مقداری گرانتر هستند، و پیکربندی آن‌ها گزینه‌های زیادی دارد، اما عملکرد آن‌ها در شبکه بسیار بهتر و کارآمدتر می‌باشد.

۶-۶- پل (Bridge)

پل وسیله‌ای است که دو شبکه محلی را بدون توجه به اینکه از پروتکل یا ساختار یکسان استفاده می‌کنند یا خیر به یکدیگر متصل می‌کند و امکان جریان یافتن اطلاعات در بین آن‌ها را فراهم می‌آورد.



به عبارت دیگر Bridge، سخت‌افزاری است که پل ارتباطی دو LAN مختلف می‌باشد. تفاوت بین یک پل یا Bridge و Router در تکنیک برقراری ارتباط بین دو LAN در این است که Router در هر شبکه‌ای عمل مسیر یابی را انجام می‌دهد و بر اساس IP مبدا و مقصد اطلاعات را در شبکه انتقال می‌دهد. اما یک Bridge که معمولاً در شبکه‌های مخابراتی و بی‌سیم بکار می‌رود، سخت‌افزار یا نرم‌افزاری است که اطلاعات از جنس لایه دوم یک شبکه (Frame) را در شبکه دیگر کپی می‌کند؛ به عنوان مثال دو LAN می‌توانند به وسیله خط تلفن به یک دیگر متصل شوند. استفاده از Bridge کارایی شبکه را تا حد زیادی کاهش می‌دهد و باعث کندی شبکه می‌شود. پل‌ها اصولا در شبکه هایی استفاده می‌شوند که از پروتکل‌های غیر قابل مسیر دهی استفاده می‌کنند. یعنی آدرس مبدا و مقصد ندارند. این پروتکل‌ها به راحتی از Bridge عبور می‌کنند. نمونه‌ای از این پروتکل‌ها NetBIOS و NetBeui می‌باشند.

توجه داشته باشید که با تقسیم یک شبکه‌ی بزرگ به چندین سگمنت و استفاده از یک پل برای اتصال آن‌ها به یکدیگر، توان عملیاتی شبکه افزایش خواهد یافت. اگر یک سگمنت شبکه از کار بیفتد، سایر سگمنت‌های متصل به پل می‌توانند شبکه را فعال نگه دارند. پل‌ها موجب افزایش وسعت شبکه محلی می‌شوند.

همانطور که می‌دانید، Repeater و هاب چنان طراحی شده‌اند که همه بار شبکه را که دریافت کرده‌اند به همه پورت‌های متصل به آن‌ها، توزیع می‌نمایند. به عبارت دیگر ترافیک ایجاد شده در قسمتی از شبکه را به بخشهای دیگر شبکه عمومیت می‌دهند. به منظور رفع این مشکل از پل (Bridge) استفاده می‌کنند.

فرض کنید ۸ کامپیوتر را توسط ۲ تا هاب ۵ پورت به یکدیگر متصل کرده‌ایم. در این مثال، اگر اتصال هاب‌ها را به طور مستقیم به یکدیگر وصل کنیم، این امر باعث می‌شود که ترافیک هر بخش از شبکه، از هاب مربوطه رد شده و به هاب دیگر رسیده و از طریق آن، بخش دیگر شبکه را نیز تحت تاثیر خود قرار دهد. به این ترتیب ترافیک شبکه سیر صعودی خواهد داشت. برای رفع این مشکل از Bridge (پل) در نقطه میانی دو هاب استفاده می‌شود تا ترافیک در هر بخش، محلی باقی بماند و به بخش دیگر منتقل نشود و به این ترتیب ترافیک شبکه کاهش می‌یابد.

پل، این عملیات را توسط فیلتر کردن داده‌ها انجام می‌دهد. نحوه کار به این ترتیب است که پل آدرس فیزیکی تمام کامپیوترهای موجود در یک بخش را می‌داند و موقعیت آن‌ها را در یک جدول داخل خود ذخیره می‌کند. وقتی که یک فریم از یک بخش وارد آن می‌شود، در جدول داخلی خود به دنبال آدرس فیزیکی آن می‌گردد تا آدرس مقصد فریم را مشخص کند.

اگر آدرس مقصد فریم در همان سگمنت آدرس مبدا باشد، پل از عبور فریم به بخشهای دیگر ممانعت به عمل آورده و فریم مربوطه در همان بخش به دنبال مقصد خود می‌گردد. ولیکن اگر فریم به سگمنت دیگری تعلق داشته باشد، پل فریم مربوطه را به آن بخش پاس می‌دهد. به عبارت دیگر پل، فریم هایی را که آدرس مبدا و مقصدشان در یک بخش از شبکه است، در همان بخش نگه می‌دارد و با این کار باعث می‌شود ترافیک یک قسمت از شبکه به قسمت دیگر منتقل نشود.

به یاد داشته باشید که Bridge در لایه ۲ کار می‌کند و مفهوم MAC Address را از روی بسته‌ها می‌تواند بخواند و طبق جدول MAC Addressها، عمل فیلتر فریم‌ها را انجام می‌دهد.

همچنین Bridge می‌تواند شبکه‌های با رسانه‌های مختلف را به هم متصل کند. به عنوان مثال یک Bridge می‌تواند یک شبکه مبتنی بر فیبر نوری (100BaseFX) را به یک شبکه مبتنی بر کابل UTP (10BaseTX) متصل کند و کامپیوترهای موجود در بخشهای با رسانه‌ها و توپولوژی‌های متفاوت با یکدیگر به نقل و انتقالات داده بپردازند.

۶-۷- دروازه (Gateway)

Gateway یا مترجم پروتکل: وسیله‌ای است که معمولاً مانند یک دروازه ورودی/خروجی در شبکه عمل می‌کند. لفظ Gateway برای هر سخت‌افزاری به کار می‌رود که معمولاً دو شبکه غیر همجنس را به هم متصل کند. یک Gateway می‌تواند یک کامپیوتر، یک مسیریاب، یک Firewall، یک Proxy Server و یا هر چیز دیگری باشد. اما تجهیزاتی که خاص Gateway هستند معمولاً در شبکه هایی بکار می‌روند که براساس پروتکل TCP/IP کار نمی‌کنند. این تجهیزات وظیفه ترجمه پروتکل بین دو شبکه غیر همجنس را انجام می‌دهند. به عنوان مثال در شبکه هایی که TCP/IP Base نیستند، با استفاده از یک Gateway می‌توان پروتکل شبکه را به پروتکل TCP/IP و برعکس تبدیل نمود. یک کاربرد دیگر Gateway این است که می‌توان تنظیم نمود که تمامی Packetهای خروجی یک کامپیوتر به سمت کامپیوتری خاص برود. مثلاً کامپیوتر سرویس دهنده اینترنت.

۶-۸- مسیریاب (Router)

مسیریاب و یا همان روتر، یک وسیله میانجی در شبکه‌های ارتباطی است که مسئولیت تحویل پیام‌ها را بر عهده دارد. در شبکه‌ای که کامپیوترهای زیادی را از طریق حلقه‌ای از اتصالات با یکدیگر مرتبط می‌کند، مسیریاب پیام‌های مورد نظر را هدایت می‌کند.

مسیریاب‌ها در مقایسه با هاب‌ها و سوئیچ‌ها، از هوشمندی بیشتری برخوردارند. مسیریاب‌ها از بسته، اطلاعات کاملتری جهت تشخیص این مسئله که کدام مسیریاب یا ایستگاه کاری، می‌بایست بسته بعدی را دریافت کند، دارا می‌باشد. مسیریاب‌ها از طریق نقشه مسیر شبکه، تحت عنوان "جدول مسیر یابی"، ارسال بسته‌ها از طریق بهترین مسیر به مقصد را تضمین می‌کنند. در صورت قطع ارتباط بین دو مسیریاب، مسیریاب ارسال کننده، مسیر دیگری را جهت ادامه سیر و حرکت در نظر می‌گیرد. در ضمن مسیریاب می‌تواند بین شبکه هایی که به زبان‌های مختلفی صحبت می‌کنند، یعنی دارای "پروتکل های" مختلفی می‌باشند، ارتباط برقرار کند. برخی از این پروتکلها عبارتند از: پروتکل اینترنت (IP)، تبادل بسته‌های اینترنتی (IPX) و Apple Talk.

مسیریاب‌ها به سبب برخورداری از هوش بیشتر، قادرند با اجتناب از ایجاد ترافیک در برخی بخشهای دستیابی شبکه، باعث تامین امنیتی بیشتر بشوند.

مسیریاب‌ها می‌توانند شبکه‌ها را به یک مکان منفرد یا مجموعه‌ای از ساختارها متصل کرده و سبب تامین رابط هایی برای اتصال LANها به WAN بشوند، درست مثل ارتباط شعبه‌های اداری به یکدیگر یا به اینترنت.

مسیریاب‌ها در لایه ۳ مدل مرجع OSI کار می‌کنند؛ یعنی هر مسیریاب بسته را شناخته و می‌تواند از روی Header بسته‌ها، مبدا و مقصد را تشخیص دهد. وقتی کامپیوتری در یک شبکه بسته‌ای را ارسال می‌کند که مقصد آن در شبکه محلی متصل به آن کامپیوتر موجود نیست، کامپیوتر آن بسته را تحویل Gateway می‌دهد تا از شبکه خارج شود. Gatewayها در شبکه معمولاً تجهیزاتی هستند که عمل مسیر یابی را نیز انجام می‌دهند. پس Router شبکه یا همان Gateway آدرس مقصد بسته‌ها را با مسیرهای خود مقایسه می‌کند تا کوتاه ترین و بهترین مسیر را بین مبدا و مقصد انتخاب کنند و در صورت وجود مسیر، بسته به خروجی مورد نظر ارسال می‌شود و در صورت عدم وجود مسیر، برای مسیر یابی Router یا با مسیریاب‌های مجاور مشورت می‌نماید و یا بسته را تحویل مسیریاب بعدی که در واقع Gateway مربوط به این مسیریاب می‌باشد هدایت می‌کند. هر Router دارای یک Routing Table می‌باشد که این جدول به صورت پویا نسبت به مسیریاب‌های همسایه به روز رسانده می‌شود. (پروتکل هایی مانند RIP و OSPF). به عبارت بهتر مسیریاب‌ها همیشه در مورد مسیرهای موجود برروی اینترنت با یکدیگر تبادل نظر می‌نمایند. مسیریاب‌ها همواره به دنبال بهترین مسیر با کمترین هزینه برروی اینترنت می‌گردند.

۶-۸-۱- آشنائی با روتر

استفاده از روترها در شبکه به امری متداول تبدیل شده است. یکی از دلایل مهم گسترش استفاده از روتر، ضرورت اتصال یک شبکه به چندین شبکه دیگر (اینترنت و یا سایر سایت‌های از راه دور) در عصر حاضر است. نام در نظر گرفته شده برای روترها، متناسب با کاری است که آنان انجام می‌دهند: "ارسال و مسیر دهی داده از یک شبکه به شبکه‌ای دیگر". مثلاً در صورتی که یک شرکت دارای شعبه‌ای در اصفهان و یک دفتر دیگر در شیراز باشد، به منظور اتصال آنان به یکدیگر می‌توان از یک خط Leased (اختصاصی) که به هر یک از روترهای موجود در دفاتر متصل می‌گردد، استفاده نمود. بدین ترتیب، هر گونه ترافیکی که لازم است از یک سایت به سایت دیگر انجام شود از طریق روتر محقق شده و تمامی ترافیک‌های غیر ضروری دیگر فیلتر و در پهنای باند و هزینه‌های مربوطه، صرفه جویی می‌گردد.

۶-۸-۲- انواع روتر

روترها را می‌توان به دو گروه عمده سخت‌افزاری و نرم‌افزاری تقسیم نمود:

روترهای سخت‌افزاری: روترهای فوق، سخت‌افزارهایی می‌باشند که نرم‌افزارهای خاص تولید شده توسط تولیدکنندگان را اجراء می‌نمایند (در حال حاضر صرفاً به صورت Black Box (جعبه سیاه) به آنان نگاه می‌کنیم). نرم‌افزار فوق، قابلیت مسیر دهی را برای روترها فراهم نموده تا آنان مهمترین و شاید ساده ترین وظیفه خود که ارسال داده از یک شبکه به شبکه دیگر است را به خوبی انجام دهند. اکثر شرکت‌ها ترجیح می‌دهند که از روترهای سخت‌افزاری استفاده نمایند، چراکه آنان در مقایسه با روترهای نرم‌افزاری، دارای سرعت و اعتماد پذیری بیشتری می‌باشند. شکل زیر یک نمونه روتر را نشان می‌دهد.



روترهای نرم‌افزاری: روترهای نرم‌افزاری دارای عملکردی مشابه با روترهای سخت‌افزاری بوده و مسئولیت اصلی آنان نیز ارسال داده از یک شبکه به شبکه دیگر است. یک روتر نرم‌افزاری می‌تواند یک سرویس دهنده NT، یک سرویس دهنده ویندوز سرور، یک سرویس دهنده Novell Netware و یا یک سرویس دهنده لینوکس باشد. تمامی سیستم‌های عامل شبکه‌ای مطرح، دارای قابلیت‌های مسیر دهی از قبل تعبیه شده می‌باشند.

در اکثر موارد از روترها به عنوان فایروال و یا Gateway اینترنت، استفاده می‌گردد. در این رابطه لازم است به یکی از مهمترین تفاوت‌های موجود بین روترهای نرم‌افزاری و سخت‌افزاری، اشاره گردد: در اکثر موارد نمی‌توان یک روتر نرم‌افزاری را جایگزین یک روتر سخت‌افزاری نمود، چراکه روترهای سخت‌افزاری دارای سخت‌افزار لازم و از قبل تعبیه شده‌ای می‌باشند که به آنان امکان اتصال به یک لینک خاص WAN (از نوع Frame Relay، ISDN و یا ATM) را خواهد داد. یک روتر نرم‌افزاری (نظیر سرویس دهنده ویندوز) دارای تعدادی کارت شبکه است که هر یک از آنان به یک شبکه LAN متصل شده و سایر اتصالات به شبکه‌های WAN از طریق روترهای سخت‌افزاری، انجام خواهد شد.

مثال ۱: استفاده از روتر به منظور اتصال دو شبکه به یکدیگر و ارتباط به اینترنت

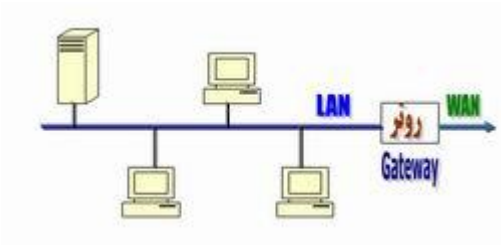
فرض کنید از یک روتر مطابق شکل زیر به منظور اتصال دو شبکه LAN به یکدیگر و اینترنت، استفاده شده است. زمانی که روتر داده‌ای را از طریق یک شبکه LAN و یا اینترنت دریافت می‌نماید، پس از بررسی آدرس مبداء و مقصد، داده دریافتی را برای هر یک از شبکه‌ها و یا اینترنت ارسال می‌نماید. روتر استفاده شده در شکل زیر، شبکه را به دو بخش متفاوت تقسیم نموده است (دو شبکه مجزا). هر شبکه دارای یک هاب است که تمامی کامپیوترهای موجود در شبکه به آن متصل شده‌اند. علاوه بر موارد فوق، روتر استفاده شده دارای اینترفیس‌های لازم به منظور اتصال هر شبکه به آن بوده و از یک اینترفیس دیگر به منظور اتصال به اینترنت، استفاده می‌نماید. بدین ترتیب، روتر قادر است داده مورد نظر را به مقصد درست، ارسال نماید.



مثال ۲: استفاده از روتر در یک شبکه LAN

فرض کنید از یک روتر مطابق شکل زیر در یک شبکه LAN، استفاده شده است. در مدل فوق، هر یک از دستگاه‌های موجود در شبکه با روتر موجود نظیر یک Gateway برخورد می‌نمایند. بدین ترتیب، هر یک از ماشین‌های موجود بر روی شبکه LAN که قصد ارسال یک بسته اطلاعاتی (اینترنت و یا هر محل خارج از شبکه LAN) را داشته باشند، بسته اطلاعاتی

موردنظر را برای Gateway ارسال می‌نمایند. روتر (Gateway) نسبت به محل ارسال داده دارای آگاهی لازم می‌باشد (در زمان تنظیم خصلت‌های پروتکل TCP/IP برای هر یک از ماشین‌های موجود در شبکه یک آدرس IP برای Gateway در نظر گرفته می‌شود). شکل زیر نحوه استفاده از یک روتر به منظور دستیابی کاربران به اینترنت در شبکه LAN را نشان می‌دهد:



مثال ۳: استفاده از روتر به منظور اتصال دو دفتر کار

فرض کنید، بخواهیم از روتر به منظور اتصال دو دفتر کار یک سازمان به یکدیگر، استفاده نماییم. بدین منظور هر یک از روترهای موجود در شبکه با استفاده از یک پروتکل WAN نظیر ISDN به یکدیگر متصل می‌گردند. عملاً، با استفاده از یک کابل که توسط ISP مربوطه ارائه می‌گردد، امکان اتصال به اینترفیس WAN روتر فراهم شده و از آنجا سیگنال مستقیماً به شبکه ISP مربوطه رفته و سر دیگر آن به اینترفیس WAN روتر دیگر متصل می‌گردد. روترها، قادر به حمایت از پروتکل‌های WAN متعددی نظیر Frame Relay , ATM , HDLC و یا PPP، می‌باشند.



۶-۸-۳- مهمترین ویژگی‌های یک روتر

روترها دستگاه‌های لایه سوم (مدل مرجع OSI) می‌باشند.

روترها مادامی که برنامه ریزی نگردند، امکان توزیع داده را نخواهند داشت.

اکثر روترهای مهم دارای سیستم عامل اختصاصی خاص خود می‌باشند.

روترها از پروتکل‌های خاصی برای مبادله اطلاعات ضروری خود (منظور داده نیست)، استفاده می‌کنند.

نحوه عملکرد یک روتر در اینترنت: مسیر ایجاد شده برای انجام مبادله اطلاعاتی بین سرویس گیرنده و سرویس دهنده در تمامی مدت زمان انجام تراکنش ثابت و یکسان نبوده و متناسب با وضعیت ترافیک موجود و در دسترس بودن مسیر، تغییر می‌نماید.

۶-۸-۴- آشنائی با اینترفیس‌های (رابط) روتر

اینترفیس‌ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می‌توان آنان را به سه گروه عمده اینترفیس‌های مختص شبکه محلی، اینترفیس‌های مختص شبکه WAN و اینترفیس‌های کنسول و کمکی تقسیم نمود. در ادامه با اینترفیس‌های فوق آشنا خواهیم شد.

انواع اینترفیس‌های روتر

اینترفیس‌ها مسئولیت اتصالات روتر به دنیای خارج را برعهده داشته و می‌توان آنان را به سه گروه عمده تقسیم نمود:

۱- **اینترفیس‌های مختص شبکه محلی:** با استفاده از اینترفیس‌های فوق یک روتر می‌تواند به محیط انتقال شبکه محلی متصل گردد. اینگونه اینترفیس‌ها معمولاً نوع خاصی از اترنت می‌باشند. در برخی موارد ممکن است از سایر تکنولوژی‌های LAN نظیر Token Ring و یا ATM (برگرفته از Asynchronous Transfer Mode) نیز استفاده گردد.

۲- **اینترفیس‌های مختص شبکهWAN:** این نوع اینترفیس‌ها اتصالات مورد نیاز از طریق یک ارائه دهنده سرویس به یک سایت خاص و یا اینترنت را فراهم می‌نمایند. اتصالات فوق ممکن است از نوع سریال و یا هر تعداد دیگر از اینترفیس‌های WAN باشند. در زمان استفاده از برخی اینترفیس هایWAN، به یک دستگاه خارجی نظیرCSU به منظور اتصال روتر به اتصال محلی ارائه دهنده سرویس نیاز می‌باشد. در برخی دیگر از اتصالاتWAN، ممکن است روتر مستقیماً به ارائه دهنده سرویس متصل گردد.

۳- **اینترفیس‌های کنسول و کمکی:** عملکرد پورت‌های مدیریتی متفاوت از سایر اتصالات است. اتصالات LAN وWAN، مسئولیت ایجاد اتصالات شبکه‌ای به منظور ارسال فریم‌ها را برعهده دارند ولی پورت‌های مدیریتی یک اتصال مبتنی بر متن به منظور پیکربندی و اشکال زدایی روتر را ارائه می‌نمایند. پورت‌های کمکی (Auxiliary) و کنسول (Console) دو نمونه متداول از پورت‌های مدیریت روتر می‌باشند. این نوع پورت‌ها، از نوع پورت‌های سریال غیر همزمان EIA-232 می‌باشند که به یک پورت ارتباطی کامپیوتر متصل می‌گردند. در چنین مواردی از یک برنامه شبیه ساز ترمینال بر روی کامپیوتر به منظور ایجاد یک ارتباط مبتنی بر متن با روتر استفاده می‌گردد. مدیران شبکه می‌توانند با استفاده از ارتباط ایجاد شده مدیریت و پیکربندی دستگاه مورد نظر را انجام دهند.

شکل زیر انواع اتصالات یک روتر را نشان می‌دهد.



۶-۸-۵- پیکربندی روتر با استفاده از پورت‌های مدیریت

پورت‌های کنسول و کمکی به منزله پورت‌های مدیریتی می‌باشند که از آنان به منظور مدیریت و پیکربندی روتر استفاده می‌گردد. این نوع پورت‌های سریال غیر همزمان به عنوان پورت‌های شبکه‌ای طراحی نشده‌اند. برای پیکربندی اولیه روتر از یکی از پورت‌های فوق استفاده می‌گردد. معمولاً برای پیکربندی اولیه، استفاده از پورت کنسول توصیه می‌گردد چراکه تمامی روترها ممکن است دارای یک پورت کمکی نباشند.

زمانی که روتر برای اولین مرتبه وارد مدار و یا سرویس می‌گردد، با توجه به عدم وجود پارامترهای پیکربندی شده، امکان برقراری ارتباط با هیچ شبکه‌ای وجود نخواهد داشت. برای پیکربندی و راه اندازی اولیه روتر، می‌توان از یک ترمینال و یا کامپیوتر که به پورت کنسول روتر متصل می‌گردد، استفاده نمود. پس از اتصال کامپیوتر به روتر، می‌توان با استفاده از دستورات پیکربندی، تنظیمات مربوطه را انجام داد. پس از پیکربندی روتر با استفاده از پورت کنسول و یا کمکی، زمینه اتصال روتر به شبکه به منظور اشکال زدایی و یا مانیتورینگ فراهم می‌گردد.

نحوه اتصال به پورت کنسول روتر

برای اتصال کامپیوتر به پورت کنسول روتر به یک کابل Rollover و یک آداپتور RJ-45 to DB-9 نیاز می‌باشد. روترهای سیسکو به همراه آداپتورهای مورد نیاز برای اتصال به پورت کنسول ارائه می‌گردند. کامپیوتر و یا ترمینال می‌بایست قادر به حمایت از شبیه سازی ترمینال VT100 باشند. در این رابطه از نرم‌افزارهای شبیه‌ساز ترمینال نظیر HyperTerminal استفاده می‌گردد.

برای اتصال کامپیوتر به روتر می‌بایست مراحل زیر را دنبال نمود:

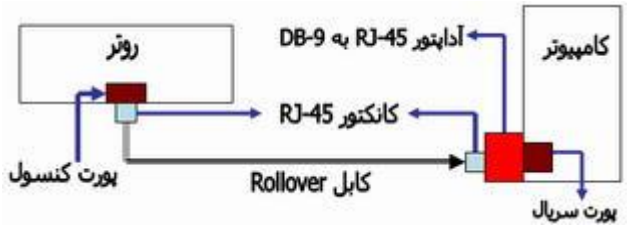
پیکربندی نرم‌افزار شبیه سازی ترمینال بر روی کامپیوتر انتخاب شماره پورت مناسب و...

اتصال کانکتور RJ-45 کابل rollover به پورت کنسول روتر

اتصال سر دیگر کابل rollover به آداپتور RJ-45 to DB-9

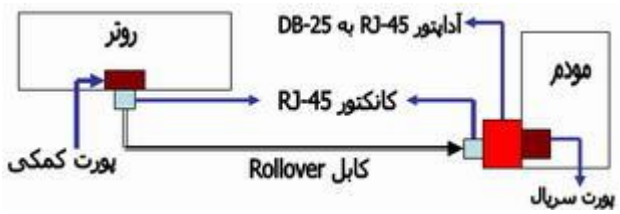
اتصال آداپتور DB-9 به کامپیوتر

شکل زیر نحوه اتصال کامپیوتر به روتر را با استفاده از یک کابل Rollover نشان می‌دهد:



اتصال کامپیوتر به روتر

برای مدیریت و پیکربندی از راه دور روتر، می‌توان یک مودم را به پورت کنسول و یا کمکی روتر متصل نمود. شکل زیر نحوه اتصال روتر به یک مودم را نشان می‌دهد:



ارتباط با روتر از طریق مودم

به منظور اشکال زدایی روتر، استفاده از پورت کنسول نسبت به پورت کمکی ترجیح داده می‌شود. در زمان استفاده از پورت کنسول به صورت پیش فرض پیام‌های خطا، اشکال زدایی و راه اندازی نمایش داده می‌شوند. از پورت کنسول در مواردی که سرویس‌های شبکه فعال نشده و یا با مشکل مواجه شده‌اند نیز می‌توان استفاده نمود. بنابراین پورت کنسول گزینه‌ای مناسب برای بازیابی رمز عبور و سایر مشکلات غیرقابل پیش بینی می‌باشد.

اتصال اینترفیس‌های LAN

در اکثر محیط های LAN، روتر با استفاده از یک اینترفیس Ethernet و یا Fast Ethernet به شبکه متصل می‌گردد. در چنین مواردی روتر همانند یک میزبان است که با شبکه LAN از طریق یک هاب و یا سوئیچ ارتباط برقرار می‌نماید.

به منظور ایجاد اتصال از یک کابل Straight-Through استفاده می‌گردد. در برخی موارد، اتصال اترنت روتر مستقیماً به کامپیوتر و یا روتر دیگری متصل می‌گردد. در چنین مواردی از یک کابل Cross-over استفاده می‌گردد. در صورت عدم استفاده صحیح از اینترفیس‌ها، ممکن است روتر و یا سایر تجهیزات شبکه‌ای با مشکل مواجه گردند.

اتصال اینترفیس‌های WAN

اتصالات WAN دارای انواع مختلفی بوده و از تکنولوژی‌های متفاوتی استفاده می‌نمایند. سرویس‌های WAN معمولاً از ارائه دهندگان سرویس اجاره می‌گردد. خطوط Leased و یا Packet-Switched نمونه هایی از انواع متفاوت اتصالات WAN می‌باشند.

برای هر یک از انواع سرویس هایWAN، دستگاه مشتری (اغلب یک روتر است) به منزله یک DTE (Data Terminal Equipment) رفتار می‌نماید. پایانه فوق با استفاده از یک دستگاه DCE (Data Circuit-Terminating Equipment) که معمولاً یک مودم و یا CSU/DSU (Channel Service Unit/Data Service Unit) می‌باشد به ارائه دهنده سرویس متصل می‌گردد.

از دستگاه فوق برای تبدیل داده از DTE به یک شکل قابل قبول برای ارائه دهنده سرویسWAN، استفاده می‌گردد.



۶-۸-۶- آشنایی با مسیریاب‌های سیسکو

تاریخچه مسیریاب‌های سخت‌افزاری

نام کلی که برای مسیریاب‌ها در نظر گرفته شده به خاطر اولین و اصلی ترین وظیفه هر روتر یعنی عمل مسیر یابی است و انتخاب این نام هم به سال ۱۹۸۴ بر می‌گردد. یعنی زمانی که رفته رفته با ظهور کامپیوترهای شخصی مشکل تعدد استانداردها تبدیل به یک مشکل حاد برای شبکه‌های موجود شد. گویا در این هنگام دو دانشمند به نام‌های Leonard Bosack و Sandy Lerner از دانشگاه استنفورد برای اتصال شبکه‌ها و مسیر یابی داده‌ها بین این شبکه‌ها و حل مشکل عدم سازگاری پروتکل‌های مختلف در سطح مسیریاب‌ها، ایده مسیر یابی (Routing) را مطرح نمودند و موفق شدند اولین مسیریاب را با هزینه شخصی تولید کرده و آن را در دانشگاه استنفورد نصب نمایند. با توجه به استقبالی که از این محصول جدید شد این دو نفر تصمیم گرفتند که محصول خود را تجاری کنند. در این سال بود که غول تجهیزات شبکه‌های کامپیوتری یعنی شرکت سیسکو در زمینه طراحی و تولید مسیریاب‌های سخت‌افزاری حرف اول را زد و در این زمینه به جز چند شرکت ازجمله Foundry Networks و Nortel Networks رقیب جدی دیگری نداشت و طی سال‌ها با ارائه راه حل‌های جدیدی نظیر ایجاد تنوع در کلیه محصولات و ارائه گواهینامه‌های مهندسی تجهیزات سیسکو نظیر CCNA، CCDA، CCNP و CCIE و... موقعیت خود را بیش از پیش تثبیت نموده است. به همین دلیل از مجموعه شرکت‌های تولیدکننده روترهای سخت‌افزاری تنها برروی مسیریاب‌های شرکت سیسکو تمرکز می‌کنیم و به دلیل تنوع زیاد مسیریاب‌های این شرکت و همچنین تعدد

ماژول‌های مورد استفاده که به منظور افزایش انعطاف پذیری مسیریاب‌ها استفاده می‌شوند، تنها به تشریح مدل‌های معروف‌تر خواهیم پرداخت. یک مسیریاب صرف نظر از نوع، سری و قیمت آن، همانند یک کامپیوتر دارای اجزای سخت‌افزاری نظیر جعبه (Case) برد اصلی (Mother Board)، پردازنده، حافظه موقت (RAM)، حافظه دائمی (Flash) و رابط‌ها و ماژول‌های مختلف است که بسته به کاربرد هر مسیریاب توان و ظرفیت متفاوتی دارند و همچنین هر مسیریاب دارای یک سیستم عامل است که IOS نامیده می‌شود و سرنام کلمات Internetworking Operating System می‌باشد. ولی از آنجائی که مسیریاب‌ها فاقد صفحه کلید و مانیتور هستند، معمولاً به سه طریق می‌توان فرامین سیستم عامل را برای پیکربندی مسیریاب وارد نمود، این سه روش عبارتند از:

۱) کنسول

به همراه هر مسیریاب یک کابل ۸ رشته مخصوص به نام کابل Rollover ارائه می‌شود که با استفاده از آن و یک کامپیوتر شخصی و از طریق برنامه هایی نظیر Term90 یا HyperTerminal ویندوز که قابلیت تبادل داده با پورت‌های سریال کامپیوتر را دارند، می‌توان پیکربندی روتر را در بالاترین سطح دسترسی انجام داد.



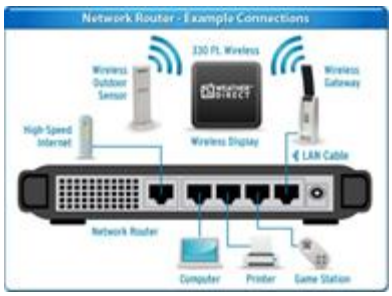
کابل کنسول روتر

نکته:

- با امکان دسترسی فقط در این سطح، می‌توان تحت شرایطی حتی رمزهای عبور دستگاه را نیز تعویض نمود. به همین دلیل است که حفاظت فیزیکی دستگاه روتر بسیار حائز اهمیت است.
- اولین باری که بخواهید پیکربندی یک روتر را انجام دهید، حتماً می‌بایست از این طریق اقدام کنید.

۲) Telnet

از آنجایی که اصولا مسیریاب‌ها در لایه شبکه مدل TCP/IP کار می‌کنند، می‌توانیم به آن‌ها آدرس IP اختصاص دهیم و طبعاً با استفاده از پروتکل Telnet و پورت اترنت روتر می‌توانیم از راه دور به آن متصل شده و روتر را پیکربندی کنیم. البته باید بدانید که اجازه این نوع دسترسی قبلاً می‌بایست از طریق کنسول صادر شده باشد و همچنین این که کاربری که به این صورت به مسیریاب متصل شده، نسبت به روش اول از سطح دسترسی کمتری برخوردار است.



۳) Aux

این امکان برای مدیرانی است که می‌خواهند از طریق شماره گیری به مودم مسیریاب متصل شوند و آن را متناسب شرایط مد نظرشان پیکربندی کنند. برای این کار نیز لازم است از طریق کنسول دستگاه امکان استفاده از Aux را فعال نماییم.

در ادامه ابتدا در خصوص سری‌ها و مدل‌های مختلف مسیریاب‌های سیسکو و سپس درباره مشخصه‌های سخت‌افزاری مسیریاب‌ها و انواع آن‌ها نکاتی را عنوان می‌نماییم.

مشخصه‌های سخت‌افزاری مسیریاب‌های سیسکو

- **Case**

روترهای سیسکو با توجه به نوع و مدل دارای بدنه‌های متفاوتی هستند. مثلاً بدنه‌های Desktop که مربوط به سری‌های ۷۰ یا ۹۰ می‌باشند. این بدنه‌ها قابلیت افزودن ماژول یا سایر ملحقات را ندارند. در مقابل بدنه‌های Rackmount هستند که قابلیت نصب در رک را دارند. از همین نوع بدنه، بعضی که بزرگتر بوده و قابلیت نصب ماژول‌ها و کارت‌های زیادی به نام شاسی (Chasis) دارند شناخته می‌شوند.

- **CPU**

اگر بخواهید سرعت پردازنده‌های کامپیوترهای شخصی را با مسیریاب‌ها مقایسه کنید حتماً تعجب خواهید کرد، چرا که حتی سریع ترین روترها که می‌توانند در ستون فقرات شبکه‌های اینترنتی استفاده شوند و طبعاً می‌بایست حجم بسیار وسیعی از ترافیک اینترنت را در زمان بسیار کوتاهی پردازش نمایند، سرعتی در حدود ۲۰۰ مگاهرتز دارند. ولیکن از آنجایی که مسیریاب‌ها واسط گرافیکی کاربر ندارند و در محیط متنی کار می‌کنند و همچنین به دلیل تک منظوره بودن این پردازنده‌ها این سرعت برای این منظور کفایت خواهد کرد. ضمناً جالب است که بدانید مسیریاب‌های سیسکو عمدتاً از پردازنده‌های سری ۶۸۰۰۰ شرکت موتورولا استفاده می‌کنند.

- **مادربورد**

مادربوردهای مورد استفاده شرکت سیسکو عمدتا توسط شرکت‌های Asus و Iwill و Supermicro ساخته می‌شوند و طبیعتاً برای سری‌های مختلف توان و مشخصه‌های متفاوتی ارائه می‌شود.

- **حافظه**

در سخت‌افزار مسیریاب‌های سیسکو بسته به نوع و کاربرد، از انواع مختلفی از حافظه‌ها پشتیبانی می‌شود که عبارتند از:

۱. **RAM** که گاهی DRAM نیز نامیده می‌شود و برای ذخیره اطلاعات حین کار به کار می‌رود و یا به اصلاح سیسکو برای نگهداری Running Config مورد استفاده قرار می‌گیرد.

در بعضی مدل‌ها، این حافظه قابل ارتقاء و در برخی دیگر ثابت می‌باشد و عموماً در ظرفیت‌های ۴ و ۸ و ۱۶ و ۳۲ و ۶۴ مگابایت موجود می‌باشد.

۲. **ROM**: که در این نوع حافظه یک تصویر قابل بوت از سیستم عامل روتر (IOS Image) قرار می‌گیرد و در مراحل اولیه روند بوت مسیریاب مورد استفاده قرار می‌گیرد.

۳. **Flash Memory**: همانند هارد دیسک در PCها می‌باشد و برای ذخیره کل IOS مورد استفاده قرار می‌گیرد. ضمناً برای ذخیره فایل‌های پیکربندی نیز از این حافظه استفاده می‌شود که در ظرفیت‌های مختلفی عرضه می‌شود. البته نسبت به مدل و سری مسیریاب معمولاً قابل ارتقا است.

۴. **NVRAM**: روترها از فایلی به نام Startup Config برای نگهداری تنظیمات ابتدایی پیکربندی مسیریاب استفاده می‌کنند و این فایل در این حافظه نگهداری می‌شود و پس از این که در روند بوت به داخل RAM دستگاه روتر بارگذاری شد، Running Config نامیده می‌شود.

- **Interface**

لینک‌های هر مسیریاب برای ارتباط با دنیای خارج در قالب پورت‌ها و ماژول‌ها که برای انعطاف پذیری روترها در جهت انجام وظایف گوناگون قابل استفاده و تغییر است و داخل اسلات‌های توسعه قرار می‌گیرند. به عنوان مثال می‌توان یک ISP را در نظر گرفت که پس افزایش خطوط تلفن خود قادر خواهد بود ماژولی به نام AM (که شامل تعدادی مودم است) را به اسلات روتر خود (روتری که در نقش یک Access Server عمل می‌کند) متصل کند و کارآیی روتر را افزایش دهد. البته به شرط این که آن روتر خاص امکان این گسترش را داشته باشد. برای آگاهی از امکانات هر مسیریاب و بررسی قابل گسترش بودن آن و نوع ماژول هایی که می‌توانید به آن متصل کنید، می‌بایست به راهنمای فنی هر مسیریاب یا سایت وب شرکت سیسکو (www.Cisco.Com) مراجعه کنید، مطمئنا در این سایت اطلاعات بسیار مفیدی خواهید یافت.

۶-۸-۷- *BRouter*

این وسیله ترکیبی از پل و مسیر یاب می‌باشد (Bridge+Router). بسته‌های محلی می‌توانند از یک طرف شبکه به طرف دیگر با توجه به آدرس مقصد هدایت شوند؛ حتی اگر از هیچ پروتکل ارسالی هم پیروی نکنند. بسته هایی که دارای پروتکل مناسب هستند می‌تواند طبق مسیر خود به دنیای خارج از شبکه محلی فرستاده شوند. این دستگاه جزء قطعات گران قیمت شبکه محسوب می‌شوند که می‌توانند با توجه به پروتکلی که در شبکه پیاده سازی شده است. عمل پل و یا عمل روتر را انجام دهند.

BRouter می‌تواند دو دسته از ترافیک شبکه را مدیریت کند. (Bridged Traffic) و (Router Traffic)

۱. **در Bridge Traffic**، BRouter ترافیک شبکه را به همان روش Bridge مدیریت می‌کند یعنی در لایه ۲ عمل کرده و داده‌ها را بر اساس آدرس فیزیکی آن‌ها فیلتر می‌کند و یا از خود عبور میدهد.
۲. **در Router Traffic**، BRouter می‌تواند بخش‌های مختلف شبکه با توپولوژی‌های متفاوت به هم وصل کند و عمل فیلتر داده‌ها را با توجه به آدرس منطقی آن‌ها انجام دهد.

به عنوان مثال. یک BRouter می‌تواند به گونه‌ای پیکربندی شود که بخشی از شبکه با پروتکل NetBEUI را پل کند و بخش دیگر شبکه با توپولوژی TCP/IP را مسیر یابی کند.

۶-۹- مودم ADSL

۶-۹-۱- *مودم ADSL*

ابزاری است که جهت اتصال به شبکه اینترنت بر روی خطوط دیجیتالی Digital Subscriber Line به کار می‌رود.

به بیان ساده داده‌های اینترنتی در مرکز مخابراتی بر روی سیم تلفن یک مشترک خاص قرار گرفته و در مقصد یعنی در منزل مشترک توسط یک دستگاه به نام اسپلیتر (جداساز)از خط تلفن استخراج شده و وارد رایانه مشترک خواهندشد. از آنجا که سیگنال بر روی کابل‌های تلفن معمولی مسافت زیادی را نمی‌تواند طی کند ADSL در فواصل اندک قابل استفاده‌است که معمولاً کمتر از ۵ کیلومتر است. البته بسته به کیفیت مودم و مشخصات فیزیکی آن این مقدار می‌تواند متفاوت باشد. وقتی سیگنال به دفتر تلفن منطقه برسد ADSL از آن جدا شده و به سمت شبکه اینترنت هدایت می‌شود و در عین حال – فرکانس‌های صوتی سیگنال نیز وارد شبکه تلفن می‌شوند. به این صورت از یک انشعاب تلفن هم برای برقراری ارتباط تلفنی و هم برای ADSL استفاده خواهد شد. برخی از پارامترهای مهمی که جزو ویژگی‌های اساسی در شبکه‌های‌ای دی اس ال حساب می‌شوند و بعضی از آن‌ها معیار برتری کیفیت مودم‌ها هم شمرده می‌شوند عبارتند از:

نسبت سیگنال به نویز (SNR): عبارتست از نسبت بین سیگنال ارسال شده رو خط تلفن و نویز (هر چه میزان SNR تولیدی توسط مودم بالاتر باشد نشانگر این است که توانایی و کیفیت مودم برای ارسال یک سیگنال با کیفیت بالا و با نویز کمتر روی خط بیشتر است.

میرایی خط (Line Attenuation): عبارتست از نسبت میرایی سیگنال در طول خط که بعلت مشخصات فیزیکی خط از جمله مقاومت الکتریکی آن متغیر است.

قدرت خروجی سیگنال(Output Power): عبارتست از میزان توان خروجی سیگنال فرستاده شده روی خط. قدرت خروجی سیگنال با میزان SNR نسبت مستقیم دارد. بعبارت دیگر با بالاتر رفتن قدرت سیگنال خروجی، میزان SNR نیز افزایش خواهد یافت. البته بالا بودن قدرت سیگنال خروجی و بدست آوردن SNR بالا به این روش مفید فایده نیست زیرا بالا رفتن توان سیگنال خروجی باعث ایجاد همشنوایی (Cross Talk) روی خطوط تلفن بقیه مشترکان مرکز تلفن خواهد شد.

برخی از معروفترین تولید کنندگان مودم‌های‌ای دی اس ال در دنیا عبارتند از:

Linksys – D-LinkAsus - - Buffalo – Lattice Communications

۶-۹-۲- نحوه کار مودم‌های DSL

برای آنکه بدانیم یک مودم ADSL چگونه کار می‌کند اول در مورد ارتباط مودمهای DSL که ADSL نیز از خانواده آن‌هامی باشد صحبت می‌کنیم

کاربران از طریق یک مودم معمولی، یا با استفاده از شبکه محلی در دفتر کار خود، یا از طریق یک مودم کابلی و یا با استفاده از یک اتصال DSL به اینترنت متصل می‌شوند. اتصال DSL یک اتصال پر سرعت است که از سیم‌های عادی به کار رفته در خطوط تلفن استفاده می‌کند.

مزایای اتصال DSL عبارت هستند از:

- کاربران می‌توانند در هنگام اتصال به اینترنت از خط تلفن برای برقراری مکالمات تلفنی نیز استفاده کنند
- سرعت مودم‌های DSL از مودم‌های معمولی بسیار بالاتر است(۱/۵مگابیت در ثانیه) در مقایسه با۵۶کیلوبیت درثانیه
- برای استفاده از مودم‌های DSL لزومی به سیم‌کشی جدید نیاز نیست. این مودم‌ها می‌توانند از خط تلفن موجود کاربران استفاده کنند

ـ شرکتی که اتصال DSL را ارائه می‌کند، معمولاً مودم را نیز به همراه خدمات نصب ارائه می‌کند

مودم‌های DSL نقاط ضعفی نیز دارند که عبارت هستند از:

ـ هر چه فاصله کاربران از مرکز ارائه کننده خدمات کمتر باشد، این مودم‌ها بهتر کار می‌کنند

ـ سرعت اتصال از طریق این مودم‌ها به هنگام دریافت داده‌ها از اینترنت، بیشتر از زمان ارسال داده است

ـ خدمات DSL یا به عبارت دیگر روشی که برای گنجانیدن اطلاعات بیشتر در یک خط تلفن معمولی به کار می‌رود تا امکان برقراری ارتباط تلفنی را در حین اتصال به اینترنت به کاربران دهد، شرح داده شده است

ـ تقسیم سیگنال‌ها

دو استاندارد رقیب و ناسازگار برای مودم‌های ADSL وجود دارد:

۱) استاندارد رسمی ANSl که سیستمی به نام Discrete Multitone یاDMT است و طبق گزارش تولید کنندگان، امروز، اکثر تجهیزات ADSL از آن استفاده می‌کنند؛

۲) استانداری که در گذشته مورد استفاده قرار می‌گرفت و کاربرد ساده‌تری داشت، سیستم CAP بود که در بسیاری از اتصالات اولیه ADSL به کار می‌رفت.

سیستم CAP، سیگنال‌های خط تلفن را به سه باند مختلف تقسیم می‌کند: مکالمات تلفنی در باند صفر تا چهار کیلوهرتزی حمل می‌شوند، مانند وضعیت موجود در تمام مدارهای POTS کانال انتقال دهنده داده‌ها از کاربر به سرور که در باند بین۲۵و۱۶۰کیلوهرتز، منتقل می‌شود. کانال انتقال داده از سرور به کاربر که از فرکانس۲۴۰کیلوهرتز آغاز شده و طبق شرایط (طول خط، میزان پارازیت و تعداد کاربران در یک مرکز سوئیچ مخابرات) تا حداکثر۱/۵مگاهرتز افزایش می‌یابد

این سیستم، با سه کانال که با فاصله زیاد از یکدیگر قرار دارند، احتمال تداخل بین کانال‌های یک خط یا تداخل بین سیگنال‌های خطوط مختلف را به حداقل می‌رساند. سیستم DMT نیز سیگنال‌ها را به کانال‌های مجزا تجزیه می‌کنداما برای تبادل داده‌ها بین کلاینت و سرور از دو کانال عریض استفاده نمی‌کند، بلکه داده‌ها را در

۲۴۷ کانال جداگانه با پهنای باند ۴ کیلوهرتز جای می‌دهددر مقام مقایسه، مجسم کنید که شرکت مخابرات خط مسی تلفن شما را به۲۴۷خط چهار کیلوهرتزی تقسیم کرده و سپس به هر یک از آن‌ها یک مودم وصل کند ؛ در نتیجه معادل۲۴۷مودم در یک زمان به کامپیوتر شما متصل خواهد شد. هر کانال کنترل می‌شود و اگر کیفیت آن بیش از حد پایین باشد، سیگنال به کانال دیگری انتقال داده می‌شوداین سیستم به‌طور دائم سیگنال‌ها را به کانال‌های مختلف منتقل می‌کند تا بهترین کانال‌ها را برای انتقال و دریافت بیابد. به علاوه، بعضی از کانال‌های سطح پایین‌تر (کانال‌هائی که با فرکانس۸کیلوهرتز آغاز می‌شوند)، به عنوان کانال‌های دو جهته مورد استفاده قرار می‌گیرند. کنترل و مرتب سازی اطلاعات در کانال‌های دو جهته و حفظ کیفیت در تمامی۲۴۷کانال، موجب پیچیده شدن پیاده‌سازی DMT در مقایسه با سیستم CAP شده است، اما در عوض DMT انعطاف پذیری خطوطی را که کیفیت‌های مختلف دارند، افزایش می‌دهد. البته از نظر کاربرانDSL سیستم‌هایCAP وDMT با یکدیگرمشابه هستند. با نصب ADSL معمولا چند فیلتر کوچک در اختیار کاربر قرار می‌گیرد تا آن‌ها را به پریزهای مورد استفاده تلفن متصل کند. این فیلترها، فیلترهای ساده‌ای به نام فیلتر پایین گذرLP هستند که تمام سیگنال‌هائی را که فرکانس آن‌ها از حد خاصی بالاتر است، حذف می‌کنندازآنجائیکه تمام مکالمات تلفنی در فرکانس‌های

پایین‌تر از چهار کیلوهرتز صورت می‌گیرند، فیلترهایLP برای متوقف کردن تمام ارتباطات بالاتر از این فرکانس ساخته می‌شوند تا سیگنال‌های داده با مکالمات استاندارد تلفنی تداخل نکنند

۶-۹-۳- تجهیزات DSL

تجهیزات اتصالاتADSL شامل دو قطعه است؛ یک قطعه که مورد استفاده کاربران قرار می‌گیرد و قطعه دیگر که ارائه دهندگان خدمات اینترنتی، شرکت تلفن یا سایر تامین کنندگان خدماتDSL به آن نیاز دارندقطعه مورداستفاده کاربران، یک گیرنده/فرستنده DSL است که می‌تواند خدمات دیگری نیز ارائه کند. تامین کنندگان خدمات DSL برای دریافت اتصالات مشتریان خود، به یکDSLAM نیاز دارند.

گیرنده/فرستنده DSL:

اغلب کاربران خانگی به دستگاه گیرنده/فرستنده DSL خود(مودمDSL)گویند اما مهندسان شرکت مخابرات یا ارائه دهندگان خدمات اینترنتی، آن را ATU_R می‌نامند. صرف نظر از نام این دستگاه، این وسیله، نقطه ارتباطی داده‌های موجود در کامپیوتر یا شبکه کاربر با خط DSL است. اگر چه اکثر مودم‌های نصب شده در مناطق مسکونی از اتصالات USB یا اترنت 10Base_T استفاده می‌کنند اما می‌توان دستگاه گیرنده / فرستنده را به روش‌های مختلفی به تجهیزات کاربر متصل کرد. با وجود این که اکثر گیرنده/فرستنده‌هایADSL عرضه شده توسط ارائه دهندگان خدمات اینترنتی و شرکت مخابرات صرفاً گیرنده/فرستنده هستند، دستگاه‌هائی که شرکت‌های مورد استفاده قرار می‌دهند ممکن است از ترکیب روترهای شبکه، سوئیچ‌ها یا سایر تجهیزات شبکه سازی در یک پلت فرم تشکیل شده باشند

:DSLAM

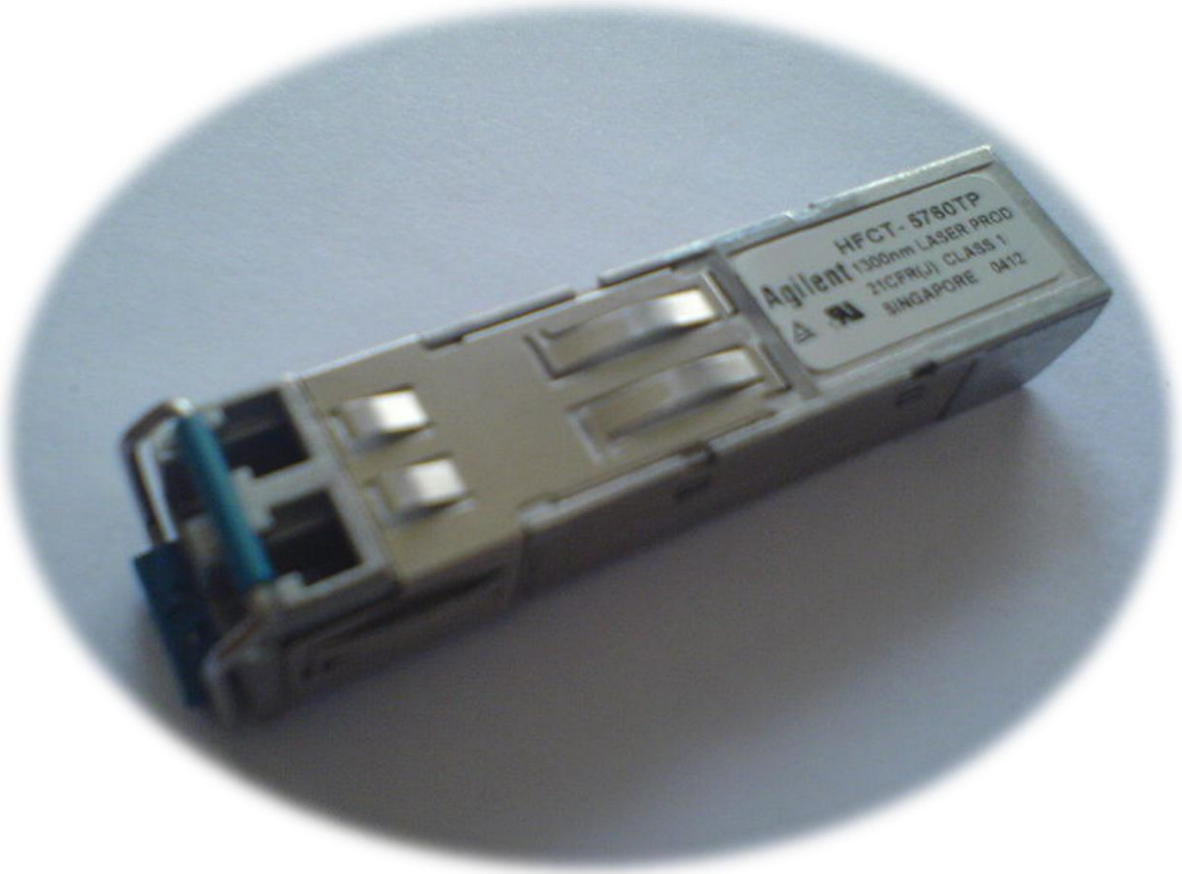
دستگاه DSLAM مورد استفاده ارائه کنندگان خدمات دسترسی، دستگاهی است که در واقع امکان کارکرد DSL را به وجود می‌آورد. DSL_AM اتصالات تعداد زیادی از مشتریان را جمع آوری کرده و آن‌ها را در یک اتصال پرظرفیت به اینترنت قرار می‌دهد. دستگاه‌های DSLAM معمولا انعطاف‌پذیر هستند و می‌توانند از انواع DSL و انواع مختلف پروتکل‌ها و استانداردها (برای مثال CAP و DMT) پشتیبانی کنند. به علاوه، دستگاه SLAM ممکن است قابلیت‌های دیگری از جمله مسیریابی یا اختصاص آدرس‌هایLP پویا به مشتریان را نیز داشته باشد. DSLAM تفاوت‌هائی اساسی میان اتصالات ADSL و مودم‌های کابلی ایجاد می‌کند. از آنجائیکه کاربران مودم‌هایکابلی معمولاً یک شبکه را که یک محله مسکونی را تحت پوشش قرار می‌دهد بین خود تقسیم می‌کنند، در بسیاری از موارد افزایش تعداد کاربران به کاهش کیفیت منجر می‌شود.مودم‌های ADSL یک اتصال اختصاصی را از هر کاربر به DSLAM باز می‌گردانند و به این ترتیب کاربران به هنگام اضافه شدن کاربران جدید به شبکه، کاهشی در عملکرد احساس نمی‌کنند، البته تا زمانی که تعداد کل کاربران موجب ازدحام در یک اتصال مجزا و پرسرعت به اینترنت نشود. در آن مقطع، تامین کنندگان خدمات می‌توانند با ارتقاء این فناوری، امکانات بیشتری را برای تمام کاربران متصل بهDSLAM فراهم کنند.

۶-۱۰- اس‌اف‌پی (SFP)

ترانسیور اس‌اف‌پی (small form-factor pluggable) عبارت است از واحد فرستنده-گیرنده) ترانسیور) قابل نصب داغ که معمولاً به عنوان رابط ورودی درسیستم‌های مخابراتی نسل جدید (NGN) و نوری امروزی استفاده می‌شوند.

مطابق استاندارد، ماژول‌های ۱۳۰۰ و ۱۵۰۰ نانومتری نوری (لیزری) در سامانه‌هایی نظیر اس‌دی‌اچ مورد استفاده قرار می‌گیرند.

اس‌اف‌پی‌ها معمولاً دارای سوکت خاصی روی بُرد میزبان هستند که شامل نگهدارنده فیزیکی و اتصال‌های سیگنالی است. برخی اس‌اف‌پی‌ها کنترل سیگنال و برخی آلارم هم دارند.



۶-۱۱- NAS

انباره (Storage) ذخیره سازی متصل به شبکه (Nas) دستگاهی است که به صورت اشتراکی در شبکه مورد استفاده قرار می‌گیرد. این دستگاه، با استفاده از NFS سیستم فایلی شبکه‌ای مختص یونیکسی CIFS سیستم فایلی شبکه‌ای مختص محیط‌های ویندوزی FTP و HTTP و سایر پروتکل‌ها با اجزای شبکه ارتباط برقرار می‌کند. وجود NAS در یک شبکه برای کاربران آن شبکه افزایش کارایی و استقلال از سکو را به ارمغان می‌آورد، گویی که این انباره مستقیما به کامپیوتر خودشان متصل است.

خود دستگاه NAS یک وسیله پر سرعت، کارآمد، تک منظوره و اختصاصی است که در قالب یک ماشین یا جعبه عرضه می‌شود. این دستگاه طوری طراحی شده که به تنهایی کار کند و نیازهای خاص ذخیره سازی سازمان را با استفاده از سیستم

عامل و سخت‌افزار و نرم‌افزار خود در بهترین حالت برآورده سازد. NAS را می‌توان مثل یک دستگاه Plug-and-play در نظر گرفت که وظیفه آن تامین نیازمندی‌های ذخیره سازی است. این سیستم‌ها با هدف پاسخگویی به نیازهای خاص در کوتاه ترین زمان ممکن (به صورت بلا درنگ) طراحی شده‌اند. ماشین NAS برای به کار گیری در شبکه هایی مناسب‌تر است که انواع مختلف سرور و کلاینت در آن‌ها وجود دارند و وظایفی چون پراکسی، فایروال، رسانه جریانی و از این قبیل را انجام می‌دهند.

در این بخش به معرفی دسته‌ای از دستگاه‌های NAS می‌پردازیم به نام "فایلر" که امکان به اشتراک گذاشتن فایل‌ها و داده‌ها را میان انواع متفاوت کلاینت‌ها فراهم می‌سازند. در عین حال، مزایای NAS در مقایسه با SAN شبکه‌های موسوم به Storage Area Network مورد بررسی قرار خواهد گرفت.

۶-۱۱-۱- Filer چیست؟

دستگاه‌های NAS موسوم به فایلر تمام توان پردازشی خود را صرفا روی خدمات فایلی و ذخیره سازی فایل متمرکز می‌کنند. در واقع فایلر به عنوان یک وسیله ذخیره سازی، نقش یک فایل سرور اختصاصی را ایفا می‌کند. فایلر مستقیما به شبکه LAN متصل می‌شود تا دسترسی به داده‌ها را در سطح فایل فراهم سازد. نصب، راه اندازی و مدیریت آسان فایلر، و همچنین مستقل از سکو بودن آن، باعث شده تا هزینه‌های مدیریتی کاهش چشمگیری پیدا کنند.

فایلرهای NAS می‌توانند در هر جایی از شبکه مستقر شوند، بنابراین مدیر شبکه آزادی کامل دارد که آن‌ها را در نزدیکی محلی قرار دهد که نیاز به خدمات ذخیره سازی دارد. یکی از فوایداصلی استفاده از فایلر آزاد شدن سرورهای همه منظوره و گران قیمت سازمان از انجام عملیات مدیریت فایل است. سرورهای همه منظوره غالبا درگیر عملیاتی می‌شوند که CPU را زیاد به کار می‌کشند و بنابراین نمی‌توانند به خوبی فایلر از عهده عملیات مدیریت فایل بر آیند.

برای هر سازمانی که در حال استفاده از فایل سرورهای همه منظوره هستند (یا قصد استفاده از آن‌ها را دارند) بهترین راه حل این است که سیستم‌های NAS را جایگزین سرورهای خود بکنند.

۶-۱۱-۲- NAS در مقابل SAN

NAS سرنام عبارت Network Attached Storage است در حالی که SAN مخفف Storage Area Network می‌باشد. این دو تکنولوژی شباهت‌های بسیاری به یکدیگر دارند، مثلا این که هر دو بهترین حالت یکپارچگی (Consolidation) را تامین می‌کنند، هر دو به محل ذخیره سازی داده‌ها مرکزیت می‌بخشند، و هر دو دسترسی به فایل را در کار آمدترین حالت فراهم می‌سازند. قابلیت به اشتراک گذاشتن انباره ذخیره سازی میان چند میزبان، حمایت از سیستم عامل‌های مختلف، و تفکیک محل ذخیره سازی از محل اجرای برنامه‌ها از دیگر مشترکات این دو تکنولوژی است. علاوه بر این، هر دو آن‌ها می‌توانند با استفاده از RAID و اجزای یدکی، آمادگی و یکپارچگی داده‌ها را تضمین کنند.

اما تفاوت این دو تکنولوژی اصولا در نحوه اتصال آن‌ها به شبکه است. NAS محصولی مشخص و شناخته شده است که بین Application Server و File System می‌نشیند، در حالی که SAN معماری است که بر روی سیستم فایلی و ابزارهای فیزیکی ذخیره سازی اعمال می‌شود. SAN در واقع خودش یک شبکه است، شبکه‌ای که تمام مخازن ذخیره سازی

و سرورها را به هم متصل می‌کند. بنابراین، هر یک از این دو فناوری، برای تامین نیازهای ذخیره سازی بخش‌های متفاوت از یک سازمان مورد استفاده قرار می‌گیرد.

۶-۱۱-۳- NAS برای کاربران شبکه

NAS یک وسیله شبکه محور است و عموما به خاطر یکسان سازی محل ذخیره سازی داده‌های کاربران در شبکه LAN مورد استفاده قرار می‌گیرد. NAS یک راه حل مناسب ذخیره سازی است که دسترسی سریع و مستقیم کاربران به سیستم فایلی را فراهم می‌سازد. استفاده از NAS مشکل معطلی هایی را بر طرف می‌سازد که غالبا کاربران برای دسترسی به فایل‌های موجود در سرورهای همه منظوره با آن مواجه هستند.

NAS ضمن تامین امنیت لازم، تمام خدمات فایلی و ذخیره سازی را از طریق پروتکل‌های استاندارد شبکه‌ای فراهم می‌سازد: TCP/IP برای انتقال داده‌ها، Ethernet و Giga Ethernet برای دسترسی میانی، و CIFS، HTTP، و NFS برای دسترسی به فایل از راه دور. علاوه بر این، با NAS می‌توان به طور همزمان به کاربران یونیکس و ویندوز سرویس داد و اطلاعات را بین معماری‌های متفاوت به اشتراک گذاشت. از نظر کاربران شبکه، NAS وسیله‌ای است که دسترسی به فایل را بدون مزاحمت. ایجاد اختلال برای آن‌ها مهیا می‌سازد.

اگرچه NAS تا حدودی کارایی را فدای مدیریت پذیری و سادگی می‌کند، اما به هیچ وجه نمی‌توان آن را یک فناوری که در ذات خود تاخیر دارد، پنداشت. NAS به کمک گیگا بایت اترنت به کارایی بالا و تاخیر کوتاه دست یافته و هزاران کاربران را از طریق فقط یک اینتر فیس سرویس می‌دهد. بسیاری از سیستم‌های NAS دارای چند اینترفیس هستند و می‌توانند همزمان به چند شبکه متصل شوند. با رشد شبکه و نیاز بیشتر به سرعت بالا، NAS بهترین انتخاب برای پاسخگویی به برنامه هایی خواهد شد که به کارایی بالایی احتیاج دارند.

۶-۱۱-۴- SAN برای اتاق سرورها

SAN دیتا محور است. شبکه‌ای است که برای ذخیره سازی داده‌ها اختصاص داده شده است. SAN برخلاف NAS، جدای از LAN مرسوم است. بنابراین SAN می‌تواند از ایجاد ترافیک‌های استاندارد شبکه، به عنوان یک عامل بازدارنده سرعت، جلوگیری کند. SANهای مبتنی بر Filber Channel، با بهره گیری از مزایای کانال‌های I/O در یک شبکه اختصاصی جداگانه، سرعت را بهتر و تاخیر را کمتر می‌کنند.

SAN با استفاده از روتر، سوییچ و Gateway، انتقال داده‌ها بین محیط‌های ناهمگن ذخیره سازی و سروری را سهولت می‌بخشد. از همین رو، ایجاد یک شبکه ذخیره سازی نسبتا دور (در حد ۱۰ کیلومتر) با SAN امکان پذیر است. معماری SAN برای انتقال داده‌های بلوکی در بهترین حالت است. در اتاق کامپیوترها، SAN غالبا بهترین انتخاب برای بررسی مسائل پهنای باند، دسترسی به داده‌ها، و یکپارچه سازی است.

با توجه به تفاوت‌های بنیادینی که بین تکنولوژی و اهداف SAN و NAS وجود دارد، برای انتخاب هر یک باید تصمیم اساسی گرفته شود. هر یک از این دو را می‌توان برای رفع نیازهای ذخیره سازی مورد استفاده قرار دارد. البته در آینده ممکن است مرز بین دو تکنولوژی آن چنان روشن نباشد و در یک مجموعه از هر دو روش استفاده شود.

۶-۱۱-۵- راه حل‌های NAS برای نیازهای امروز شرکت‌ها

نیازهای شرکت‌های ISP، ASP و دات کام به سیستم‌های قابل اطمینان، کم هزینه، و قابل نصب در رک به گسترش راه حل‌های NAS کمک خواهد کرد. کاهش هزینه‌های کادر IT شرکت‌ها نیز از دیگر دلایل مقبولیت این راه حل‌ها خواهد بود. از دید کاربر، این که دسترسی به انبوه اطلاعات به صورت بلا درنگ امکان پذیر است، چیز خوشایندی است، و در سمت مدیریت، عدم نیاز به نیروی متخصص. IT مدیریت NAS از طریق یک رابط گرافیکی در مرورگر وب امکان پذیر است. از آنجا که فایلر NAS از قبل برای تامین نیازهای ذخیره سازی تنظیم شده است، اداره آن کار ساده‌ای است، و همین امر موجب کاهش خطاهایی می‌شود که هنگام دستکاری و تنظیم سیستم‌ها پیش می‌آیند. به علاوه، از آنجا که با NAS ظرفیت بیشتری را (نسبت به سرورهای همه منظوره) به ازاء هر مدیر می‌توان اداره کرد، هزینه کل مالکیت (TCO) نیز کاهش می‌یابد.

توسعه سریع، بدون توقف سرویس

شرکت‌های دات کام و سایر شرکت‌های رو به رشد، همواره در تلاشند تا زیر ساخت‌های IT خود را با فعالیت‌های پویای کسب و کار خود همگام نگه دارند. اتکا به سرور یا سرورهای عمومی در بعضی فعالیت‌های شرکت، شاید ضروری باشد، اما نباید این سرورها را با نیازهای رو به افزون ذخیره سازی تحت فشار گذاشت. با اضافه کردن ظرفیت ذخیره سازی در سرورهای عمومی، قطعا با توقف سرویس (Downtime) مواجه خواهید شد. وقتی سیستمی را خاموش می‌کنید تا ظرفیت ذخیره سازی آن را افزایش دهید، برنامه‌های کاربردی شما از کار می‌افتند و تین یعنی کاهش بهره وری.

از سوی دیگر، افزایش ظرفیت ذخیره سازی با NAS نه تنها ساده است، بلکه بدون ایجاد اختلال در شبکه انجام می‌شود. طی ۱۵ دقیقه می‌توانیدیک فایلر جدید به مجموعه اضافه کنید بدون اینکه مزاحم کار دیگران بشوید. بیشتر سیستم‌های پیشرفته NAS می‌توانند "درجا" ظرفیت ذخیره سازی را افزایش دهند و نیازی به اضافه کردن node جدید به شبکه ندارند. این بدان معنی است که کاربران به محض نیاز به ظرفیت ذخیره سازی بیشتر، به آن دست خواهند یافت.

رها شدن سرور

با استفاده از فایلر NAS، سرورهای شما از انجام عملیات پرمصرف و زمان بر فایلینگ خلاص شده و بدین ترتیب، می‌توانند با توان بیشتر به پردازش داده‌ها بپردازند. اگر سرور عمومی خود را برای انجام عملیات فایلینگ (علاوه بر اعمال دیگر) اختصاص داده باشید، خواهید دید که فشار زیادی روی آن وارد می‌آید، به طوری که عملا از انجام سایر وظایف خود (مثل ارسال و دریافت email یا اداره برنامه ها) باز می‌ماند.

اشتراک داده‌ها و اتصال Multi-OS

شرکت‌های رو به توسعه یا شرکت هایی که در پی ادغام با شرکت‌های دیگر هستند، بدون شک با وضعیت ناهمگن بودن محیط‌ها و سیستم عامل‌ها مواجه خواهند شد. در چنین شرایطی، سیستم NAS می‌تواند پاسخگوی این چالش باشد، چرا که توانایی کار با دو سیستم اصلی NFS و CIFS را دارد. یکی از توانایی‌های غیر قابل انکار NAS حمایت آن از این پروتکل‌ها و قابلیت به اشتراک گذاری داده‌ها بین سکوهای مختلف است. با توجه به این که روز به روز استفاده شرکت‌ها از فایل‌های حجیم در برنامه‌ها (نظیر فایل‌های صوتی-تصویری) بیشتر می‌شود، این ویژگی NAS اهمیت فوق العاده‌ای دارد.

بهبود زیر ساخت‌های موجود

با افزادن NAS به شبکه، دانش و مهارت مدیریتی خود را بالاتر برده و به ارتقا شبکه کمک می‌کنید. به کار بستن NAS در هر کجا از شبکه که نیاز آن احساس می‌شود امکان پذیر است. NAS را می‌توان با ابزارهای مدیریتی بزرگ تری چون Microsoft Management Consol، Tivoli و HP OpenView نیز تلفیق کرد. و دیگر این که NAS نیازی به مجوزهای پرهزینه سیستم عامل شبکه (NOS) ندارد.

۶-۱۱-۶- نصب NAS روی شبکه خانگی

Network Attached Storage (NAS) می‌تواند بسیار مفید باشد، خصوصاً اگر بخواهید توانائی دسترسی به فایلهای خود را از تمام کامپیوترهای موجود بر روی شبکه تان بصورت مستقل از هر PC در اختیار داشته باشید. ابزارهای NAS در عین حال می‌توانند برای کارهای Backup بزرگ مورد استفاده قرار گیرند و بسیاری از آن‌ها دارای قابلیتهای - Print Server یا Midia-Streaming توکار هستند که به شما اجازه می‌دهند اسناد چاپی را از تمام کامپیوترهای خود ایجاد نموده و یا کتابخانه‌های فیلم و موسیقی خود را ذخیره سازی کرده و به اشتراک بگذارید.

نصب چنین ابزاری باید به سادگی اتصال آن به روترتان باشد. اما متاسفانه فرآیند راه اندازی آن‌ها می‌تواند پیچیده‌تر باشد. ما در این مقاله به شما نشان خواهیم داد که چگونه یک ابزار NAS را نصب کنید و در عین حال نکات و توصیه‌های مختلفی را در زمینه پیکربندی چیدمان مربوطه در اختیارتان قرار می‌دهیم. ما برای مقاصد این مقاله از یک درایو دیسک سخت Home Network (گیگابایتی ۳۲۰) شرکت Iomega بهره گیری خواهیم کرد. اما دستورالعملهای ارائه شده برای بسیاری از مدل‌های دیگر اینگونه ابزارها نیز قابل استفاده خواهند بود.

قدم ۱

برای استفاده از ابزار NAS، بایستی یک شبکه خانگی را از قبل راه اندازی کرده باشید. شبکه شما باید در قلب خود دارای یک روتر (و یا حداقل یک سوئیچ شبکه) باشد. بعضی از ابزارهای NAS به قابلیتهای اتصال بی‌سیم توکار مجهز هستند اما معمولاً بهتر است از یک اتصال کابلی یا روتر استفاده نمایند، زیرا به این ترتیب سرعت انتقال داده بالاتری را فراهم کرده و عملکرد پایدارتری خواهند داشت. اکثر ابزارهای NAS با یک کابل اترنت در بسته بندی خود ارائه می‌شوند. کافی است یک انتهای این کابل را به یک درگاه آزاد روتر خود متصل نموده و انتهای دیگر آن را به درگاه شبکه متناظر بر روی واحد NAS متصل کنید. سپس، منبع تغذیه را به ابزار متصل کرده و آن را روشن نمائید.

قدم ۲

پیش از آنکه بتوانید از درایو شبکه جدید استفاده کنید، بایستی یک یوتیلیتی خاص را بر روی PCهای خود نصب نمائید تا بتوانند ابزار NAS را تشخیص دهند. یکی از PCهای خود را بر روی شبکه بوت کنید. ابزار NAS شما بایستی به همراه یک دیسک نرم‌افزاری ارائه شده باشد. دیسک را در درایو سیستم خود بگذارید. اگر نرم‌افزار نصب CD بطور خودکار انجام نشد، در پنجره My Computer (یا Computer در ویندوز ویستا) بر روی درایو مربوطه دوبار کلیک کنید. در مورد درایو دیسک سخت Iomega، ما باید گزینه Automatic Install را انتخاب کرده و از اعلآن‌های On-Screen برای نصب نرم‌افزار Discovery Tool استفاده نمائیم. نامها و عبارات دقیق در سایر مدلها و مارکها متفاوت خواهد بود، اما قاعده کلی معمولاً یکسان است.

قدم ۳

پس از اتمام نصب نرم‌افزار، شما باید بوتیلیتی جدید را اجرا کنید. ممکن است فرآیند نصب گزینه اجرای خودکار نرم‌افزار جدید را پس از اتمام کار خود در اختیار شما قرار دهد و یا اینکه مجبور شوید خودتان بر روی آیکن آن دوبار کلیک نمائید. در هر صورت، هنگامیکه شما یوتیلیتی را اجرا می‌کنید، ممکن است با یک هشدار وسواسی از طرف فایروال خود مواجه شوید. ما در این مرحله پیامی از فایروال ویندوز را دریافت کردیم که می‌پرسید آیا مایل به مسدود کردن نرم‌افزار کاربردی Iomega Discovery Home هستیم یا خیر. برای آنکه یوتیلیتی بطور صحیح به کار خود ادامه دهد، بر روی Unblock کلیک نمائید. اگر از فایروالی غیر از نسخه توکار ویندوز استفاده می‌کنید، ممکن است هشدارهای متفاوتی را دریافت کنید و یا اینکه مجبور شوید آن را طوری پیکربندی نمائید که به یوتیلیتی جدید ابزار NAS شما اجازه اجرا بدهد. برای فهمیدن اینکه چگونه می‌توانید امکان اجرای نرم‌افزار کاربردی مورد نظر را فراهم کنید، به مستندات و یا فایلهای Help فایروال خود مراجعه نمائید.

قدم ۴

وظیفه اصلی یوتیلیتی که نصب کرده اید، مکانیابی دیسک شبکه شما و Mount نمودن آن بعنوان یک حرف درایو بر روی کامپیوترتان است. پیش از آنکه استفاده از این درایو جدید را آغاز کنید، ممکن است ابزار شما به پیکربندی نیاز داشته باشد. در مورد درایو دیسک سخت Iomega، ابزارهای پیکربندی از طریق ابزار Discovery Home که در مرحله قبل نصب کردیم قابل دسترسی هستند. گزینه Management را فعال کرده و سپس بر روی کلید Search for Remote Devices کلیک نمائید. این ابزار برای یافتن ابزارهای NAS به جستجوی شبکه شما پرداخته و آن‌ها را به همراه نام، آدرسهای IP مربوطه و نام گروه کاری در پنجره اصلی فهرست می‌نماید. وقتی ابزار مورد نظر در فهرست ظاهر شد، بر روی آن کلیک کنید تا یوتیلیتی پیکربندی باز شود. ممکن است از شما خواسته شود تا یک کلمه عبور را وارد کنید. جزئیات پیش فرض Login در دفترچه راهنمای ابزار NAS شما ذکر شده است.

قدم ۵

مهمترین نکته‌ای که باید در این بخش بررسی نمائید، تنظیمات گروه کاری است. ابزار NAS شما باید به همان گروه کاری تعلق داشته باشد که سایر کامپیوترهای شبکه تان بر روی آن قرار دارند برای آگاهی از نام گروه کاری شبکه خود (البته اگر هنوز از آن اطلاع ندارید)، بر روی آیکن My Computer (یا Computer در ویندوز ویستا) کلیک راست کرده و سپس گزینه Properties را انتخاب نمائید. در ویندوز XP باید به برگه Computer Name مراجعه کنید اما در ویندوز ویستا این نام گروه در قسمت پائین پنجره System Properties ذکر شده است. در صورت لزوم، باید تنظیمات نام گروه کاری ابزار NAS خود را برای انطباق با این نام تغییر دهید. در یوتیلیتی Iomega، اینکار تنها مستلزم کلیک بر روی کلید Change در کنار تنظیمات Group name، وارد کردن نام جدید گروه کاری و سپس کلیک بر روی OK است.

قدم ۶

هنگانیکه ابزار NAS خود را به عنوان درایوی که برای کامپیوترهایتان قابل دسترسی است Mount می‌کنید، فرآیند مورد نیاز بر حسب مارک و مدل درایو شما تا حدودی متفاوت خواهد بود. در مورد ابزار Iomega ما یوتیلیتی Discovery را اجرا

کرده، گزینه Mount را فعال نموده و سپس بر روی کلید Search for Remote Devices کلیک کردیم. این ابزار به جستجوی درایوهای NAS پرداخته و آن‌ها را در پنجره اصلی فهرست می‌کند. وقتی درایو NAS شما در این فهرست ظاهر شد، بر روی آن کلیک نمائید تا Mount شود. در این مرحله ممکن است از شما خواسته شود، تا یک نام کاربری و کلمه عبور را وارد نمائید. جزئیات Login پیش فرض که در دفترچه راهنمای درایو شما ذکر شده است را وارد کرده و از منوی Dropdown یک فولدر را برای Mount انتخاب نمائید. بر روی OK کلیک نمائید تا فرآیند به پایان برسد. شما باید یوتیلیتی ابزار ذخیره سازی خود را بر روی تمام PCهای دیگری که بر روی شبکه تان حضور دارند نیز نصب کرده و فرآیند راه اندازی را تکرار نمائید.

POE -۱۲-۶

انتقال توان از طریق اترنت POE (Power Over Ethernet)، قابلیت دادن توان یا برق موردنیاز به تجهیزات شبکه از طریق کابل‌های موجود شبکه بدون نیاز به منبع انرژی الکتریکی خارجی (هر دستگاه) اشاره دارد. با وجود POE دستگاه‌هایی مانند تلفن‌های IP، نقاط دسترسی بی‌سیم (AP)، دوربین‌های امنیتی و سایر دستگاه‌های موجود در شبکه، انرژی خود را از کابل‌های موجود در شبکه LAN، به راحتی دریافت می‌کنند.

- حل مشکل تلفن‌های IP

اولین تقاضا برای ایجاد POE، هنگام توسعه پروتکل انتقال صدا روی اینترنت (VOIP) به وجود آمد. در ابتدا سیسکو و سایر تولیدکنندگان تلفن‌های IP، محصولات خود را همراه با اینترفیس‌های اختصاصی خود عرضه‌می‌کردند. اما هنگامی که مؤسسه مهندسان برق و الکترونیک (IEEE) استاندارد af۸۰۲.۳ را در ژوئن ۲۰۰۳ به تصویب رساند، تولیدکنندگان بزرگ تلفن‌های IP به طرفداری از این استاندارد اقدام کردند.

POE مشکل بزرگ تلفن‌های IP را حل کرد و استفاده از آن‌ها را مانند تلفن‌های معمولی، آسان و مفید نمود. از آن‌جایی که فناوری POE امکان انتقال نیرو برای تلفن‌های IP را روی کابل‌های زوج به هم‌تابیده (۶e,۵, ۳cat) امکانپذیر نموده است، آزادی عملی برای قراردادن این تلفن‌ها در هر مکان، بدون‌نیاز به منبع نیروی خارجی و وجود پریز برق، به وجود آورده است.

اکنون دیگر تلفن‌های IP به صورت گسترده استفاده می‌شوند. اکنون IEEE در حال توسعه استاندارد af۸۰۲۸.۳ برای هماهنگ کردن تعداد بی‌شماری دستگاه دیگر و ایجاد قابلیت استفاده از نیروی الکتریکی روی کابل است. فناوری POE به‌دلیل عدم نیاز دستگاه‌ها به نیروی خارجی مانند دوربین‌های امنیتی IP که در راهروها و پارکینگ‌ها نصب شده‌اند، کارت‌خوان‌های مغناطیسی، Access Pointهای بی‌سیم در سقف‌ها، سیستم‌های هشدار و سیستم‌های تشخیص امواج رادیویی آزادی نصب آن‌ها را در هر مکانی آسان نموده‌است. POE امکان استفاده از باتری پشتیبان را برای دستگاه‌هایی که نقش مهمی در امنیت و کنترل دسترسی در ساختمان دارند، فراهم می‌کند. زیرا با POE، تمام این دستگاه‌ها UPS متصل می‌شوند و هنگام قطع برق همچنان به کار خود ادامه می‌دهند.

- استاندارد AF802.3

تحت استاندارد کنونی POE،AF802.3 جریان متعادلی را به دو جفت از چهار جفت کابل انتقال داده وارد می‌کند. یعنی سوییچ POE جریان را به جفت‌هایی که داده‌ها را انتقال می‌دهند، وارد می‌نماید. (پین‌های ۲-۱ و ۶-۳)بالاترین کلاس توانی

که تحت استاندارد کنونی در دسترس است (Powerclass ۳ وات و Powerclass ۱۵.۴ وات را فراهم می‌کند، که از کمینه ولتاژ (۴۴ ولت) ضرب‌در کمینه جریان (۳۵۰ میلی‌آمپر) به دست می‌آید. به دلیل آن‌که طول هر قطعه کابل به حدود صد متر می‌رسد، توان تا حدود ۱۲/۹۵وات کاهش می‌یابد. تاکنون البته این مقدار توان مشکل خاصی را به وجود نیاورده است. اغلب تلفن‌های VoIP که به عنوان اولین مصرف‌کننده POE شناخته می‌شوند، فقط نیروی هشت وات یا کمتر را در حالت انتظار به خود اختصاص می‌دهند. اما به هرحال دستگاه‌های جدید نیاز به انرژی بیشتری دارند و این مسئله از اساسی‌ترین موضوعات بحث در مورد فناوری POE است.

- فناوری بعدی

به‌تازگی IEEE گروهی را برای مطالعه روی فناوری POE plus تشکیل داده است. این مطالعه در مورد قدم‌های بعدی درتوسعه استاندارد AF802.3 صورت می‌گیرد. این گروه چهارده مورد را تعیین کرده‌اند که چند مورد آن عبارتند از:

- بهبود استاندارد AF802.3 در قالب کنونی آن و فراهم کردن سازگاری با دستگاه‌های قدیمی و جدیدتر.
- بی‌نیاز از معرفی امکانات امنیتی جدید برای سیستم‌های قدیمی براساس ISO/IEC۶۰۹۵۰ این بدان معنی است که POE plus موجب اختلال در کارکرد دستگاه‌های موجود نمی‌شود و با آن‌ها کار می‌کند.
- ممکن است POE plus مدل‌های عملکرد خاصی را برای سازگاری باتجهیزات موجود و همچنین ابزارهای جدید داشته باشد. هنگامی که استاندارد اصلی در حال توسعه بود، شامل کلاس توان چهار می‌شد که مخصوصاً برای ورود یک استاندارد بهبود یافته‌تر و جدیدتر ذخیره شده بود.
- POE Plus امکان فراهم کردن "بیشینه توان الکتریکی ممکن" روی کابل‌های LAN موجود را دارد.

- بیشینه توان الکتریکی ممکن چیست؟

تاکنون گروه مطالعه POE plus در مورد مفهوم <بیشینه توان الکتریکی ممکن> به هیچ نتیجه دقیقی نرسیده‌اند. به وضوح محدودیت دمای سطح برای کابل‌های (cat 5, 5e, 6) وجود دارد. ولی نکته قابل توجه در این بحث آن است که محدودیت دمایی که برای پشتیبانی از POE plus باید وجود داشته باشد، چیست؟ این دما باید شصت یا هفتاد درجه سانتیگراد باشد یا حتی فراتر از آن، که تاکنون هیچ تصمیمی در این مورد گرفته نشده است.

موضوع دیگر بحث بیشینه دمای واقعی برای محیطی است که POE Plus در آن فعالیت می‌کند. به دلیل آن‌که دما در سطح کابل پراکنده می‌شود، اگر دما با بیشینه دمای روی کابل یکسان شوند، ممکن است جریان به صفر برسد. به همین دلایل برای این استاندارد نیاز به اتاق‌هایی با سقف‌های بلند است.

سوال بعدی این است که: بدترین شرایط افزایش دما برای کابل‌های میانی چیست؟ چه نوع استانداردی برای توانایی عبور جریان کابل‌ها در زیر ساختار شبکه‌های فعلی به کار بسته می‌شود؟

این نوع سوال‌ها سخت هستند. هنگامی که رابط‌های سیستم (کانکتورهای هشت پین و RJ 45) برای قابلیت عبور جریان و دما مورد مطالعه قرار می‌گیرند، مفاهیم جدیدی در مورد بیشینه جریان قابل عبور از کابل می‌رسیم. البته هنوز گروه مطالعه POE Plus به هیچ نتیجه دقیقی در مورد سطح دما در محفظه عبور کابل نرسیده‌اند.

- پشتیبانی از دستگاه‌های قدیمی و جدید

به دلیل این‌که گروه مطالعه POE Plus، گیگابیت اترنت و فراتر از آن را مدنظر دارند، نیاز به استاندارد جدیدی برای سازگاری پیش‌رو است. ولی گروه، نیاز به سازگاری دستگاه‌های قدیمی با تجهیزات جدید و امکان توان دادن به تجهیزات موجود را هم می‌خواهد.

سازگاری با تجهیزات قدیمی نیازمند آن است که بالاترین ولتاژ روی ۵۶ یا ۵۷ ولت محدود شود تا به تجهیزات آسیبی نرسد. از آن جایی که تجهیزات برای پشتیبانی از ۱۰/۱۰۰/۱۰۰۰ مگابیت‌برثانیه طراحی شده‌اند، باید از هر چهار زوج موجود برای انتقال داده‌ها استفاده نمایند یا خیر. در اینجا مسئله‌ای پیش می‌آید که آیا باید از هر چهار زوج برای عبور جریان استفاده نمود. اغلب افراد گروه مطالعه از این نظر حمایت می‌کنند. با این حال اگر مسئله این باشد، تمام سیم‌های یک لینک اترنت به تولید گرما می‌پردازند. در اینجا باز هم به موضوع محدودیت دما می‌رسیم. مسئله این است که این قبیل محدودیت‌ها تا چه حد قابل تشخیص هستند.

گیگابیت اترنت نیاز به تعادل دقیقی برای ارسال / دریافت سیگنال اترنت دارد. این بدان معناست که مشکل جدیدی پیش می‌آید و آن برقراری تعادل جریان در هر زوج است که باید دقیق‌تر از استانداردهای پیشین باشد.

- از گیگابایت به ده گیگابایت

هدف دیگر گروه مطالعه آن است که استاندارد POE plus AF802.3 هیچ‌گونه مانع و تناقضی با اترنتGig 10 نداشته باشد. پیامد این مطالعه منجر به بحث "بیشینه توان ممکن" می‌گردد. هدف گروه مطالعه‌کننده آن است که حدود توان را در حدود سی‌وات برای هر پورت تنظیم کنند. اعضا حتی روی بالا بردن توان تا صد وات نیز به بحث پرداخته‌اند. غیرقابل اجرابودن بحث آخر برای همه اعضا ثابت شده‌است. تصمیم کلی در محدوده سی تا پنجاه وات برای هر پورت گرفته شده‌است که منجر به تولید دستگاه‌های جدید در زمینه POE plus می‌گردد. برای مثال حتی یک لپ‌تاپ متوسط نیز می‌تواند در این محدوده توان، عملکرد خوبی داشته باشد.

معمای اصلی در بحث "حداکثر دمای ممکن" این است که کابل‌ها چه‌مقدار جریان و دمایی را می‌توانند تحمل کنند و چه استانداردی برای اندازه‌گیری و مدل‌بندی این پارامتر باید ایجاد شود؟ بدیهی است که انتقال توان از طریق اترنت در نسل بعدی شبکه‌ها امکانپذیر خواهدشد. هدف در ارائه استاندارد IEEE POE Plus AF802.3، اطمینان از ساختار ایمن و قابل اعتماد شبکه‌سازی در ساختمآن‌هایی است که از این قابلیت استفاده خواهند کرد.

دستگاه‌های 10,100,1000 BaseT برای کار با کابل‌های زوج به‌هم تابیده طراحی‌شده‌اند که از کابل، سخت‌افزار متصل‌کننده و یک توپولوژی پیشنهادی شبیه ANSI/TIA/EIA/568B.1 تشکیل شده است.

تامین‌کننده توان واسطه (PSE) اجازه تامین نیرو از خارج به داخل شبکه اترنت را می‌دهد. بنابراین داده و توان را به صورت همزمان روی کابل زوج به هم تابیده برای کارایی هر پورت فراهم می‌کند.

DAS -۱۳-۶

DAS یا Direct-Attached Storage وسیله ذخیره‌سازی از نوع external یا بیرونی است و می‌توان آن را به‌طور مستقیم به سرور متصل کرد.

DAS از سوی کارشناسانی که به ابزارهای ذخیره‌سازی تحت شبکه به‌عنوان جهت‌گیری اصلی این وسایل در آینده اعتقاد دارند، مورد انتقاد قرار گرفته است. اگر چه کاربرد این وسیله با محدودیت‌هایی همراه است، یعنی می‌توان آن را فقط به یک سرور متصل کرد و گسترش آن نیز معمولاً دشوار است، اما بیشتر کسب و کارهای کوچک به این دلیل که نیازی به ذخیره‌سازهایی در حد NAS و SAN ندارند، مایلند از آن استفاده کنند.

در گذشته، محدود کردن کاربران برای ذخیره کردن فایل روی سرور قابل توجیه بود، اما امروزه درایوهای ذخیره‌سازی روی سرور نسبت به گذشته خیلی ارزان‌ترند و در عین حال حفاظت از داده‌ها و فایل‌های کاربران روی سرور خیلی آسان‌تر از هنگامی است که روی Laptop و PC خودشان ذخیره شده باشند. به‌علاوه، آن دسته از کسب و کارها که فایل‌های خود را روی چندین سرور ذخیره می‌کنند بهتر است به متمرکز کردن داده‌های خود روی تعداد کمتری از سرورها بیندیشند.

سرورهایی که قدرتمندترند، ظرفیت ذخیره‌سازی آن‌ها بیشتر است و فرآیند مدیریت و تهیه نسخه پشتیبان (Backup) روی آن‌ها آسان‌تر است. با استفاده از نرم‌افزارهایی مانند Microsoft Volume Shadow Copy که در ویندوز ۲۰۰۳ می‌توان یافت (ابزارهای NAS توانایی مشابهی دارند)، کاربران می‌توانند در صورتی که تصادفاً فایل‌های خود را حذف و یا overwrite کردند، به آسانی آن‌ها را بازیابی کنند. به این ترتیب مدیران شبکه (administrators) نیز می‌توانند عملیات تهیه نسخه پشتیبان را به صورت متمرکز انجام دهند. قیمت انواع DAS بستگی زیادی به نوع فناوری که انتخاب می‌کنید (IDE، SATA یا SCSI) دارد.

Modular Smart Array -۱۴-۶

MSA 50 -۱-۱۴-۶

دستگاهی به ارتفاع U۱ است که از رابط Serial Attach SCSI (SAS) استفاده کرده و برای ذخیره اطلاعات از دیسک درایوهای SAS یا SATA پشتیبانی میکند.

این دستگاه از قابلیت اتصال مستقیم به سرور و مجتمع شدن با آن پشتیبانی میکند و همچنین دو دستگاه MSA 50 به ارتفاع U۲ که حداکثر دارای ۲۰ هارد درایو می‌باشند را می‌توان به پورت کنترلر متصل کرد که این پورت جهت حداکثر کارایی و رسیدن به سرعت انتقال Gb۱۲ برثانیه، چهار اتصال(مسیر) را برای SAS با هم ترکیب میکند.

خصوصیات و مزایا:

قابل انعطاف برای استفاده از هردو دیسک درایوهای SAS/SATA

- به دو دستگاه اجازه میدهد که از طریق یک پورت کنترلر به هم متصل شوند

پشتیبانی از هارد دیسکهای Hot-plug که باعث افزایش قابلیت اطمینان می‌شود

MSA 60 -۲-۱۴-۶

MSA 60 یک Platform انعطاف پذیر در اندازه U۲ با پشتیبانی از هارد درایوهای ۳.۵" SAS/SATA می‌باشد. این دستگاه با ترکیبی از چگالی بالا و در دسترس بودن، یک محیط ذخیره سازی خارجی و قابل اطمینان به همراه قابل دسترس

بودن، افزونگی، کارایی بالا، هزینه پایین و ظرفیت بالای ذخیره سازی تا TB۳.۶ بوسیله هارد درایوهای SAS و TB۹ بوسیله هارد درایوهای SATA فراهم می‌کند.

خصوصیات:

- پشتیبانی از هارد درایوهای SAS/SATA "۳.۵
- قابلیت اتصال ۴ enclosure به این دستگاه جهت افزایش فضای ذخیره سازی
- دارای فن و منبع تغذیه Redundant
- پشتیبانی از RAID 0,1,1+0,5,6

۶-۱۴-۳- *MSA 70*

MSA 70 مجموعه‌ای شامل ۲۵ هارددیسک SAS SFF و SATA SFF، با قابلیت ارتباط با پورت SAS، پشتیبانی از سطوح مختلف Raid بسته به کنترلر SCSI مورد استفاده برای ارتباط با سرور، قابل استفاده به صورت Cascade1+1 (دو برابر کردن تعداد دیسکها)، حداکثر ظرفیت ذخیره سازی اطلاعات، ۳/۶ ترابایت.

۶-۱۵- Splitter

Splitter یا میکروفیلتر



Splitter ابزاری‌ست برای جدا کردن Voice و Data از یکدیگر. از نظر فیزیکی قطعه‌ای‌ست کوچک با یک ورودی برای خط تلفن و دو خروجی برای گوشی تلفن ومودم ADSL.

همان‌طور که می‌دانید یکی از مزایای سرویس ADSL استفاده هم‌زمان از اینترنت و تلفن است. برای جلوگیری از اختلال در دو سرویس (اینترنت و تلفن) نباید دستگاه‌های جانبی (تلفن، فکس و...) به صورت مستقیم بر روی خط تلفن قرار گیرند. (این بدان معناست که برای استفاده از هر دستگاهی که قرار است به صورت مستقیم بر روی خط وصل باشد، یک Splitter نیاز است.) Splitter می‌تواند از اختلالات جانبی مانند نویز و قطع و وصلی تلفن و اینترنت جلوگیری کند.

توجه: برای اتصال بعضی از مودم‌ها افزون بر اتصال Splitter به دیگر خط‌ها، به مودم نیز باید Splitter وصل شود.

فصل ۷

معماری شبکه

در فصل‌های گذشته با انواع توپولوژی‌ها، رسانه‌ها و ادوات اتصال به شبکه آشنا شدید. در این فصل قصد داریم به معرفی معماری‌های مختلف شبکه بپردازیم:

معماری یک شبکه بیانگر استانداردهای تعریف شده در خصوص نحوه اتصال کامپیوترها با یکدیگر و نحوه ارسال اطلاعات می‌باشد. به عبارت دیگر، **معماری شبکه مجموعه‌ای از استاندارد هایی است که نوع کابل کشی، اتصالات، توپولوژی، نحوه دسترسی به خطوط انتقال و سرعت انتقال را مشخص می‌کند.** بنابراین هنگام راه اندازی یک شبکه، باید ابتدا معماری شبکه مشخص شود و سپس با توجه به استاندارد هایی که معماری شبکه مشخص می‌کند، قطعات و اتصالات شبکه خریداری و پیکربندی گردد.

۷-۱- انواع معماری شبکه

- اترنت (Ethernet)
- Token Ring
- FDDI
- Wireless

۷-۱-۱- اترنت

اترنت متداولترین معماری شبکه است که با استفاده از مجموعه‌ای از قوانین و استانداردها، پیکربندی بستر شبکه و بالطبع نقل و انتقال داده‌ها در شبکه را قانونمند می‌کند. به عبارت دیگر با ارائه یکسری از استانداردها و یکسری محدودیت‌ها در بکارگیری تجهیزات، اتصالات، پهنای باند و.... تمام اجزای شبکه را با هم همزمان می‌کند.

قوانین نامگذاری اترنت توسط مؤسسه IEEE:

مؤسسه IEEE که یکی از مؤسسات بزرگ در خصوص استاندارد سازی تجهیزات و تکنولوژی‌ها است، استانداردهای شبکه را با روش 802.X نامگذاری می‌کند. به عنوان مثال این مؤسسه برای معماری شبکه اترنت، استاندارد 802.3 را مشخص کرده است که تمام جزئیات مربوط به این معماری شبکه در متن این استاندارد آورده شده است.

اترنت اولین بار در سال ۱۹۷۰ و بر روی شبکه‌های محلی با تکنولوژی خطی تعریف شد و در سال ۱۹۹۵ مؤسسه IEEE این معماری را با استاندارد 802.3 معرفی کرد. و لیکن از آن زمان تا کنون این معماری توسعه یافته و شامل خانواده‌ای از تکنولوژی‌های دیگر شده است و قابلیت‌های زیادی به این معماری افزوده شده است. به همین ترتیب مؤسسه IEEE نیز ضمیمه‌های جدیدی را برای 802.3 ارائه کرده است که این ضمیمه‌ها به صورت یک یا دو حرف تکمیلی است که در انتهای این استاندارد قید می‌شود. (802.3U)

به عنوان مثال پهنای باند ارائه شده توسط اترنت در ابتدا ۱۰ مگابیت در ثانیه بود و برای کامپیوترهای شخصی دهه ۸۰ که دارای سرعت پائین بودند، کافی بنظر می‌آمد؛ ولی در اوایل سال ۱۹۹۰ که سرعت کامپیوترهای شخصی و اندازه فایل‌ها افزایش یافت، مشکل پائین بودن سرعت انتقال داده بهتر نمایان شد. اکثر مشکلات فوق به کم بودن پهنای باند موجود مربوط می‌گردید. در سال ۱۹۹۵ موسسه IEEE، استانداردی را برای اترنت با سرعت ۱۰۰ مگابیت در ثانیه معرفی نمود. این روال ادامه یافت و در سال‌های ۱۹۹۸ و ۱۹۹۹ استاندارد هایی برای گیگابیت نیز ارائه گردید.

تمامی استانداردهای ارائه شده با استاندارد اولیه اترنت سازگار می‌باشند. به عنوان مثال یک فریم اترنت می‌تواند از طریق یک کارت شبکه با کابل کواکسیال ۱۰ مگابیت در ثانیه از یک کامپیوتر شخصی خارج و بر روی یک لینک فیبر نوری اترنت ۱۰ گیگابیت در ثانیه ارسال و در انتها به یک کارت شبکه با سرعت ۱۰۰ مگابیت در ثانیه برسد. تا زمانی که بسته اطلاعاتی بر روی شبکه‌های اترنت باقی است در آن تغییری داده نخواهد شد. موضوع فوق وجود استعداد لازم برای رشد و گسترش اترنت را به خوبی نشان می‌دهد. بدین ترتیب امکان تغییر پهنای باند بدون ضرورت تغییر در تکنولوژی‌های اساسی اترنت همواره وجود خواهد داشت.

مفهوم پهنای باند (Band Width):

در سیستم‌های انتقال آنالوگ، پهنای باند به حد فاصل بین پایین ترین و بالاترین فرکانسی که یک رسانه می‌تواند از خود عبور دهد گفته می‌شود. (پهنای باند بر حسب فرکانس و با واحد هرتز بیان می‌شود) (300HZ - 3000HZ)

در سیستم‌های انتقال دیجیتال، پهنای باند به ظرفیت انتقال اطلاعات گفته می‌شود وبا واحد bps (بیت در ثانیه) سنجیده می‌شود. از عوامل موثر در پهنای باند: طول، قطر و جنس کابل است. پهنای باند با طول کابل نسبت معکوس و با قطر کابل نسبت مستقیم دارد. یعنی هرچه طول کابل بیشتر شود پهنای باند کمتر شود و هر چه قطر کابل بیشتر شود پهنای باند نیز بیشتر است.

برای انتقال اطلاعات می‌توان به دو روش از پهنای باند استفاده کرد:

۱. **تک باند (Base Band)**
۲. **باند پهن (Band Broad)**

۱. در روش Base Band (تک باند) از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می‌شود. به این معنی که در روش تک باند رسانه در هر لحظه فقط می‌تواند یک سیگنال را از خود عبور دهد در نتیجه ارسال نوبتی می‌شود و اطلاعات پشت سر هم و به صورت سریال ارسال می‌شوند. این روش انتقال دلیل به وجود آمدن مفهوم بسته (Packet) است. در شبکه‌های محلی از این روش برای انتقال اطلاعات استفاده می‌شوند. بدین ترتیب که از دو رشته کابل استفاده می‌شود که یکی برای ارسال و دیگری دریافت اطلاعات را انجام میدهد. اطلاعات به صورت بسته‌های مشخص پشت سر هم قرار میگیرند

و ارسال شده و دریافت می‌گردد. (تمام سیستم‌های انتقال دیجیتال از روش Base Band استفاده می‌کنند) (کابل هم محورUTP).

۲. در روش Band Broad (باند پهن)، یک رسانه (کابل) می‌تواند در آن واحد یک یا چند سیگنال را به طور همزمان عبور دهد. هر سیگنال به صورت جداگانه ارسال می‌شود و تداخل بین سیگنال هایی متفاوت به وجود نمیاید. از این روش در سیستم‌های انتقال آنالوگ استفاده می‌شود و رسانه می‌تواند در آن واحد سیگنالهای متفاوتی را با فرکانس‌های مختلف از خود عبور دهد. از این روش در شبکه تلویزیون‌های کابلی و شبکه‌های WAN استفاده می‌گردد. (کابل هم محور – فیبر نوری).

مفهوم سرعت انتقال اطلاعات:

مقدار اطلاعاتی که در واحد زمان توسط تجهیزات شبکه ارسال می‌شود گفته می‌شود (مثلاً کارت شبکه 100 Mbps). سرعت انتقال اطلاعات با پهنای باند رابطه مستقیم دارد. هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می‌شود و بر عکس.

نکته: پهنای باند، ظرفیت انتقال یک رسانه یا یک کابل است. در صورتی که سرعت انتقال، سرعت ارسال اطلاعات در واحد زمان است.

تکنولوژی‌های مختلف اترنت:

همانطور که پیشتر نیز گفته شد. معماری شبکه اترنت برای اولین بار در سال ۱۹۷۰ مطرح شد و طی سالیان بعد این معماری و استانداردهای آن توسعه یافته و با نام‌های دیگری نامگذاری شدند. امروزه برای معماری اترنت، تکنولوژی مختلفی مطرح شده است:

- **10 BASE 2**
- **10 BASE 5**
- **10 BASE T**
- **10 BASE FL**
- **100 BASE X**
- **1000 BASE X**
- **1000 BASE T**

نکته: در استاندارد هایی که نام برده شد، عدد اول نمایانگر سرعت انتقال، عبارت BASE به معنای BASE BAND بودن توپولوژی مذکور و عبارت پس از ان نوع کابل را مشخص می‌کند.

(T: Twisted Pair ،F: Fiber Optic)

10 BASE 2

10 BASE 2 برای انتقال داده‌ها از کابل‌های کواکسیال THINNET استفاده می‌کند که مشخصات این کابل توضیح داده شد. کانکتورهای این شبکه از نوع BNC بوده و دو سر کابل باید توسط TERMINATOR مسدود شود تا شبکه فعال شود. از مزایای 10 BASE 2، می‌توان نصب ساده و هزینه راه اندازی بسیار کم آن را نام برد. توپولوژی 10 BASE 2 همان توپولوژی خطی است.

قوانینی که در 10 BASE 2 باید رعایت شود. عبارتند از:

- حداقل طول کابلی که کامپیوتر را به هم متصل می‌کند نباید کمتر از ۰/۵ متر باشد.
- برای اتصال T_CONNECTOR به کامپیوتر نباید از کابل استفاده کرد و باید آن را مستقیماً به کامپیوتر متصل نمود.
- فاصله اولین و آخرین کامپیوتر در شبکه نباید بیش از ۱۸۵ متر باشد. این فاصله از روی اندازه کابل اندازه گیری می‌شود.
- با استفاده از هاب (REPEATER) می‌توان حداکثر فاصله بین اولین و آخرین کامپیوتر را تا ۹۲۵ متر افزایش داد و کامپیوترها نباید خارج از این محدوده باشند.
- در فواصل بین هر دو REPEATER نمی‌توان بیش از ۳۰ دستگاه کامپیوتر به شبکه متصل کرد.
- ابتدا و انتهای کابل باید با TERMINATOR مسدود شود. TERMINATOR شبکه 10BASE2 یک مقاومت ۵۰ اهمی است که سیگنالهای الکتریکی به وجود آمده در کابل شبکه را مصرف کرده و از باقی ماندن آن در شبکه جلوگیری می‌کند.

10 BASE 5

در 10 BASE 5 از کابل کواکسیال THICKNET برای اتصال کامپیوترها به یکدیگر استفاده می‌شود. هر کامپیوتر توسط یک کابل AUI یا DIX به یک عدد TRANSCEIVER که به کابل شبکه متصل شده است، وصل می‌شود و هر دو انتهای کابل با TERMINATOR مسدود می‌شود. اولین مزیت 10BASE5 مسافت نسبتا زیادی است که تحت پوشش خود قرار میدهد. قوانینی که در مورد 10BASE 5 وجود دارد. عبارتند از:

- حداقل طول کابلی که برای اتصال دو کامپیوتر استفاده می‌شود ۲/۵ متر است.
- حداکثر طول کابل یا حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه ۵۰۰ متر است.
- یکی از TERMINATOR.ها باید به زمین متصل شود.
- اندازه کابلی که کامپیوتر را با TRANSCEIVER متصل می‌کند. نباید بیشتر از ۵۰ متر باشد.

10 BASE T

برای راه اندازی شبکه 10 BASE T از کابل‌های Twisted Pair (زوج به هم تابیده) استفاده می‌شود که حداکثر سرعت آن 10 Mbps است. در این استاندارد هر کامپیوتری که می‌خواهد به شبکه متصل شود مستقیماً توسط یک کابل به هاب وصل شده و هاب، ارتباط کامپیوترها را برقرار می‌کند. اتصالات این توپولوژی از نوع RJ-45 می‌باشد. SEGMENTEهای مختلف می‌توانند توسط کابل‌های کواکسیال یا فیبر نوری به یکدیگر متصل شوند. برخی از انواع دستگاه‌هایی که می‌توانند جایگزین هاب شوند. هوشمند بوده و می‌توانند ترافیک شبکه را کنترل کرده و آن را کاهش دهند. از مشخصه‌های بارز این شبکه گران قیمت بودن هزینه راه اندازی و نصب آن است.

قوانین 10 BASE T عبارتند از:

- حداکثر تعداد کامپیوتری که این شبکه به هم متصل می‌کند. ۱۰۲۴ دستگاه کامپیوتر است.

- کابل‌ها باید از نوع زوج به هم تابیده CAT 3 و CAT4 و CAT 5 باشند (نوع کابل از نظر داشتن محافظ تفاوتی نمی‌کند. می‌توان از هر دو کابل UTP یا STP استفاده کرد).
- حداکثر فاصله هر کامپیوتر تا هاب ۱۰۰ متر است.
- حداقل طول کابل (فاصله بین کامپیوتر تا هاب.) ۲/۵ متر است.

10 BASE FL

10 BASE FL یکی از خصوصیات شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده می‌کند. سرعت انتقال در این شبکه 10 MBPS است. مهمترین مزیت 10 BASE FL، مسافت زیادی است که تحت پوشش قرار میدهد. این مسافت ۲ کیلومتر است. از مزایای دیگر این شبکه این است که عوامل خارجی، تاثیری روی اطلاعات داخل فیبر ندارد. به عبارت دیگر. در فیبر نوری هم شنوایی وجود ندارد و اطلاعات سالم به مقصد میرسد.

دو استاندارد دیگر به نام‌های 10 Base FB و 10 Base FP نیز مورد استفاده قرار می‌گیرد. 10 Base FB یک شبکه اترنت همزمان است و برای اتصال دو تقویت کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قرار دارد، استفاده می‌شود. استاندارد دیگر 10 Base FP است که یک شبکه ستاره‌ای با استفاده از فیبر نوری می‌باشد که برای Backbone شبکه‌ها مورد استفاده قرار می‌گیرد. در 10Base FP، نور به جای سیگنالهای الکترونیکی مسئولیت انتقال اطلاعات را برعهده دارد.

100Base X

ساختار شبکه 100 BASE X همانند شبکه 10 BASE T است. (سرعت این شبکه 100 MBPS است) با این تفاوت که 100 BAE X با سه مدل کابل کشی متفاوت مورد استفاده قرار می‌گیرد. این سه مدل عبارتند از:

- 100BASE TX: در این مدل از دو کابل CAT-5 از نوع UTP یا STP به صورت همزمان استفاده می‌شود.
- 100 BASE FX: در این مدل از دو رشته فیبر نوری در کنار هم استفاده می‌شود.
- 100 BASE T4: در این مدل ۴ رشته کابل Cat-5 یا Cat-3 در کنار هم استفاده می‌شود.

توجه: 100 BASE X با نام Fast Ethernet نیز شناخته می‌شود.

1000 BASE X

این استاندارد شبکه‌ای را توضیح میدهد که درآن سرعت انتقال اطلاعات یک گیگابایت در ثانیه است و برای انتقال اطلاعات از فیبر نوری استفاده می‌شود. این استاندارد خود از چند قسمت تشکیل شده است که عبارتند از:

۱. 1000 BASE SX
۲. 1000 BASE LX/LH
۳. 1000 BASE ZX

تفاوت استانداردهای ذکر شده در طول کابل و نوع فیبر نوری است که در آن‌ها استفاده می‌شود.

1000 BASE T

در این استاندارد، از کابل‌های زوج به هم تابیده برای راه اندازی شبکه‌ای با سرعت یک گیگابیت در ثانیه استفاده می‌شود. این کابل‌ها از نوع CAT5 و کانکتورهای آن نیز از نوع RJ-45 است. نحوه ارسال اطلاعات در این استاندارد به گونه‌ای است که سیستم، توانایی انتقال اطلاعات با سرعت یک گیگابیت در ثانیه را پیدا می‌کند.

۷-۱-۲- TOKEN RING

شبکه Token Ring از نظر ظاهری یک شبکه ستاره‌ای است ولی به صورت Token Passing کار می‌کند. در این شبکه یک حلقه منطقی به وجود می‌آید و Token در امتداد حلقه حرکت کرده و به کامپیوترها میرسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد. Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می‌کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی می‌کند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به کامپیوتر مبداء ارسال می‌کند. کامپیوتر مبداء نیز Token اصلی را از بین برده و یک Token جدید تولید می‌نماید و آن را در امتداد مسیر Token قبلی به حرکت در می‌آورد. این پروسه به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوترها به جای هاب از دستگاهی بنام MAU استفاده می‌شود. سرعت انتقال اطلاعات در این شبکه 16 Mbps یا 4 Mbps است. کارت‌های 16 Mbps می‌توانند با سرعت 4 Mbps نیز فعالیت کنند.

در شبکه Token Ring از کابل‌های زوج به هم تابیده استفاده می‌شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل می‌تواند ۴۵ متر باشد و این شبکه فقط با سرعت ۴ مگابیت در ثانیه کار می‌کند و اگر از کابل STP استفاده شود. حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می‌شود.

۷-۱-۳- FDDI

FDDI، تکنولوژی یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده می‌کند. در این تکنولوژی به جای فیبر نوری از کابل مسی نیز می‌توان استفاده کرد ولی در صورت استفاده از کابل مسی طول کابل کمتر می‌شود. FDDI به عنوان Backbone در محل هایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می‌شود. از جمله این محیط‌ها می‌توان به دانشگاه‌ها اشاره کرد. در FDDI می‌توان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر ساخته می‌شود و در هر ۲ کیلومتر یک تقویت کننده قرار میگیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می‌آید، از دو حلقه فیبر نوری در کنار هم استفاده می‌شود تا در صورتی که یکی از رشته‌ها قطع شود، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

۷-۱-۴- شبکه بدون سیم

شبکه بدون سیم. شبکه‌ای است که از امواج رادیویی Broad Band برای مرتبط کردن کامپیوترها به یکدیگر استفاده می‌کند. از سیستم بی‌سیم معمولاً در شبکه‌های WAN استفاده می‌شود. کاربرد آن می‌تواند مرتبط کردن دو یا چند شبکه محلی، ارائه سرویس اینترنت و سرویس‌های دیگر باشد. شبکه بی‌سیم برای برقراری بین کامپیوتر هایی که نزدیک یکدیگر قرار دارند نیز استفاده می‌شود که در اینصورت نوعی شبکه به نام PAN بکار می‌رود.

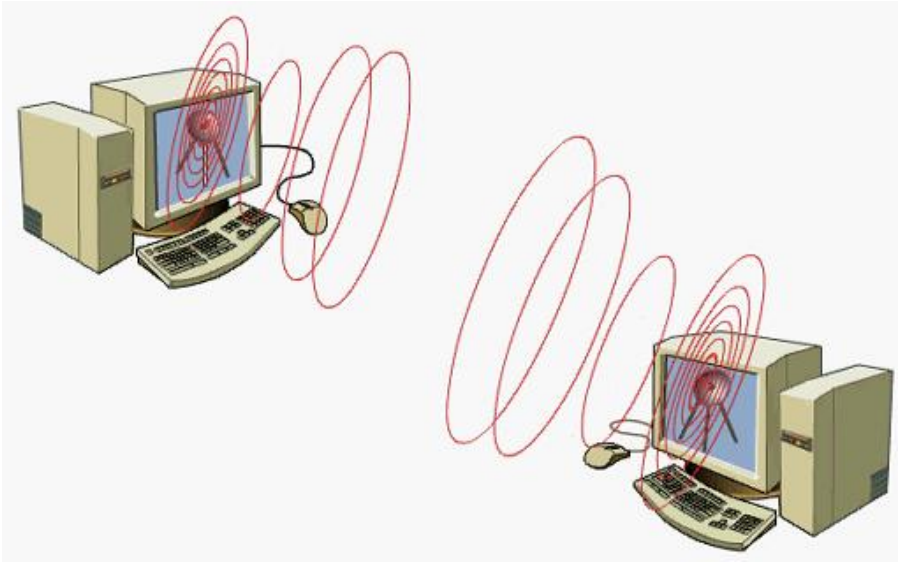
در شبکه‌های PAN نیازی به استفاده از تجهیزات خاص شبکه نیست و فقط با نصب دو کارت شبکه PAN روی دو کامپیوتر که در فاصله مناسب از یکدیگر قرار گرفته‌اند، می‌توان یک شبکه را راه اندازی کرد. از مزایای شبکه‌های بی‌سیم این

است که نیازی به نصب کابل شبکه و تجهیزات آن نیست و سرعت انتقال اطلاعات نیز می‌تواند تا سرعت ۵۲ مگابیت در ثانیه افزایش پیدا کند.

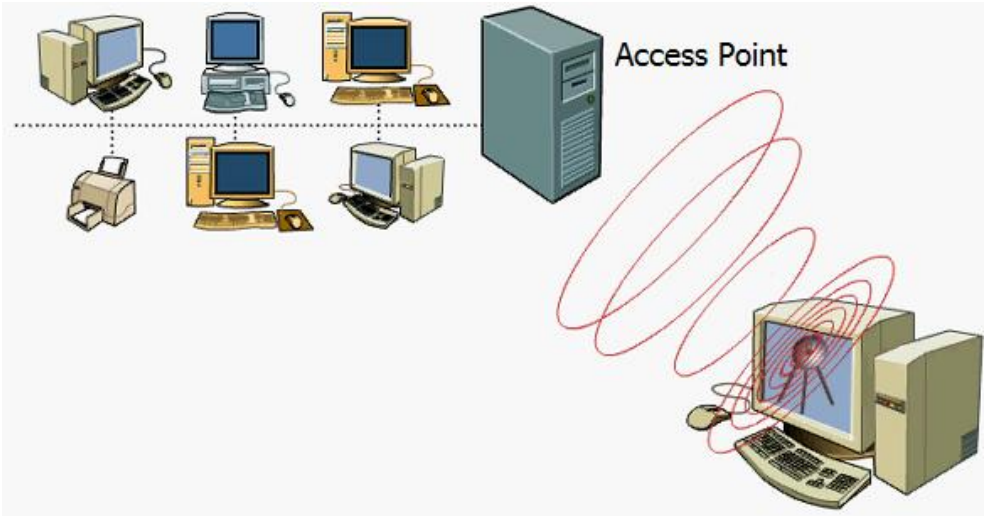
شبکه‌های بی‌سیم به ۲ طریق می‌توانند با یکدیگر ارتباط برقرار کنند.

۱- Ad hoc: در این روش، دو یا چند کامپیوتر توسط کارت شبکه بی‌سیم و به صورت مستقیم (Peer to Peer) به یکدیگر متصل می‌شوند. در این روش به هیچ عنصر سخت‌افزاری دیگری نیاز نمی‌باشد و همچنین الگوریتم مسیر یابی به صورت توزیع شده و توسط تمامی کامپیوترها انجام می‌گیرد. لذا می‌توان در حرکت از این نوع شبکه استفاده نمود و مثلاً هر کامپیوتر در یک اتومبیل جدا بوده و اتومبیل‌ها نیز در حال حرکت باشند.

به عبارت دیگر AD HOC استانداردی است که ارتباط بی‌سیم بین رایانه و تجهیزات جانبی مانند رایانه جیبی PDAs، تلفن همراه یا رایانه کیفی را برقرار می‌سازد.



۲- Infra-Structure: در این روش می‌توان کامپیوتری که کارت شبکه بی‌سیم دارد را به یک شبکه سیمی متصل نمود. بدین منظور کافی است که به یکی از سیستم‌های شبکه سیمی یک سخت‌افزار به نام Access Point یا به اختصار AP نصب کرد و از طریق آن با کامپیوتری که کارت شبکه بی‌سیم دارد ارتباط برقرار نمود. در این روش، بر عکس روش Ad hoc، یک نقطه مرکزی وجود دارد که به عنوان محور بوده و به عنوان محل اتصال کامپیوترها شناخته می‌شود.



فصل ۸ مدل‌های OSI و TCP/IP

۸-۱- نحوه مبادله داده بین دو کامپیوتر

آیا تاکنون برای شما این سوال مطرح شده است که نحوه مبادله اطلاعات بین دو کامپیوتر موجود در یک شبکه به چه صورت است؟

در سالهای آغازین طراحی شبکه، مشکل عمده‌ای که وجود داشت نا سازگاری بین محصولات تولید شده توسط شرکت‌های بزرگ تولید کننده تجهیزات شبکه بود. این مشکل زمانی آغاز گردید که شرکت HP تصمیم به تولید یک محصول شبکه‌ای نمود و این محصول با محصولات مشابه سایر شرکت‌ها (مثلاً IBM) سازگار نبود. برای حل این مشکل نیاز به یک مدل مرجع برای تبادل اطلاعات در شبکه احساس می‌شد تا اینکه کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات، پیشگام تعریف یک استاندارد برای محصولات شبکه شد و در سال ۱۹۸۴ مدل مرجع OSI را معرفی کرد. مدل فوق، همانند یک دستورالعمل اجرائی بوده و عملیات لازم در زمان ارسال و یا دریافت داده را برای یک کامپیوتر مشخص می‌نماید. به منظور آشنائی و آنالیز فرآیند مبادله داده بین دو کامپیوتر موجود در یک شبکه به بررسی یک نمونه مثال کاربردی خواهیم پرداخت

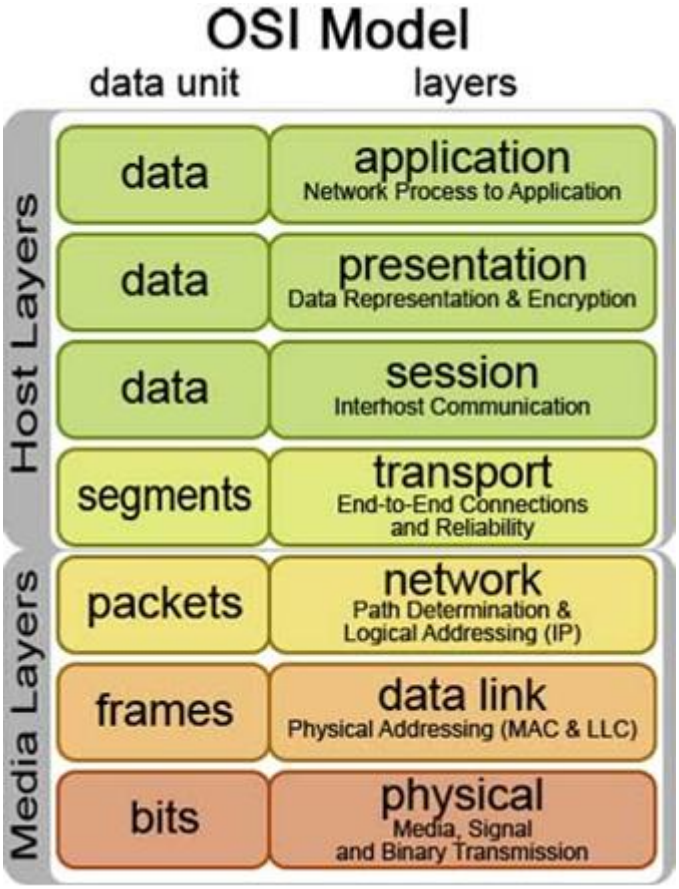
زمانی که یک اتومبیل در کارخآن‌های تولید می‌گردد، یک نفر تمامی کارها را انجام نخواهد داد. تولید یک اتومبیل بر اساس یک خط تولید انجام شده و همزمان با حرکت اتومبیل در خط تولید هر شخص بخش‌های متفاوتی را به آن اضافه نموده و زمانی که به انتهای خط تولید می‌رسیم، اتومبیل مورد نظر تولید و آماده استفاده خواهد بود.

وضعیت فوق در رابطه با داده ارسالی از یک کامپیوتر به کامپیوتر دیگر نیز صدق می‌کند. مدل OSI، قوانین لازم به منظور مبادله اطلاعات بین کامپیوترها را فراهم می‌نماید و داده‌ها در حین حرکت در هر لایه با توجه به مجموعه رهنمود هایی که OSI مشخص کرده است، تغییر شکل پیدا کرده و در نهایت از حالتی که در کامپیوتر قابل استفاده است به حالتی که از طریق کابل شبکه قابل ارسال باشد تبدیل می‌گردند و به این ترتیب داده‌ها از کامپیوتر مبدا قادر به ارسال به سایر کامپیوترها خواهد بود.

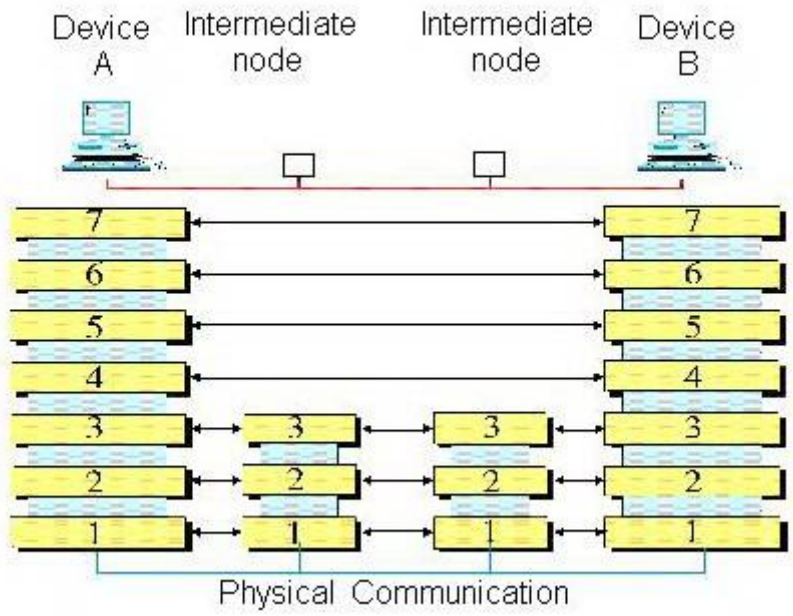
۸-۲- ساختار لایه‌ها در مدل مرجع OSI

کمیته IEEE به منظور جلوگیری از عدم هماهنگی بین محصولات و در نتیجه ناتوانی در برقراری ارتباط بین شبکه‌ای مدل مرجع OSI را معرفی کرد. این استاندارد تمامی فعالیتهایی را که باعث می‌شد اطلاعات از طریق شبکه و از کامپیوتری به کامپیوتر دیگر منتقل شود را در یک ساختار ۷ لایه‌ای در بر می‌گرفت. هر کدام از این لایه‌ها مسئولیت انجام عملیات خاصی را برعهده دارند و در حقیقت ارسال و دریافت اطلاعات از طریق این لایه‌ها در کامپیوترهای فرستنده و گیرنده انجام خواهد شد.

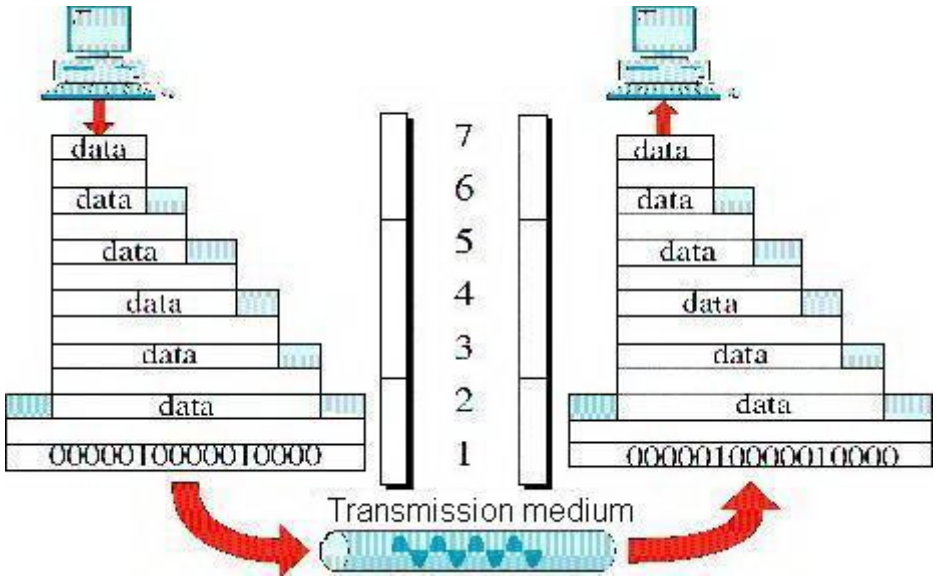
هنگام بررسی فرآیند انتقال اطلاعات بین دو کامپیوتر، مدل هفت لایه‌ای OSI روی هر یک از کامپیوترها پیاده سازی می‌گردد. در تحلیل این فرآیندها می‌توان عملیات انتقال اطلاعات را بین لایه‌های متناظر مدل OSI واقع در کامپیوترهای مبدا و مقصد در نظر گرفت. این تجسم از انتقال اطلاعات را انتقال مجازی (Virtual) می‌نامند. اما انتقال واقعی اطلاعات بین لایه‌های مجاور مدل OSI واقع در یک کامپیوتر انجام می‌شود. در کامپیوتر مبدا اطلاعات از لایه فوقانی به طرف لایه تحتانی مدل OSI حرکت کرده و از آنجا به لایه زیرین مدل OSI واقع در کامپیوتر مقصد ارسال می‌شوند. در کامپیوتر مقصد اطلاعات از لایه‌های زیرین به طرف بالاترین لایه مدل OSI حرکت می‌کنند. عمل انتقال اطلاعات از یک لایه به لایه دیگر در مدل OSI از طریق واسطه‌ها یا Interfaceها انجام می‌شود. این واسطه‌ها تعیین کننده سرویس هایی هستند که هر لایه مدل OSI می‌تواند برای لایه مجاور فراهم آورد. مزیت این لایه‌ای بودن این است که پیچیدگی را کاهش می‌دهد بنابراین اگر سخت‌افزار یا نرم‌افزاری را تغییر دهیم دیگر تاثیری بر روی دیگر لایه‌ها نخواهد داشت. **شکل زیر هفت لایه مدل OSI را نشان می‌دهد.**



در شکل زیر لایه‌های متناظر ماشین A و ماشین B می‌توانند با هم ارتباط برقرار کنند، بنابراین هر لایه با لایه بالاتر یک پروتکل یکسان دارد. هیچ لایه‌ای نمی‌تواند مستقیماً اطلاعات را روی محیط ارتباطی قرار دهد، بلکه برای انتقال اطلاعات ابتدا لایه ۷ به لایه ۶ و لایه ۶ به لایه ۵ و به همین ترتیب انتقال می‌دهند تا اطلاعات روی محیط ارتباطی انتقال یابد.

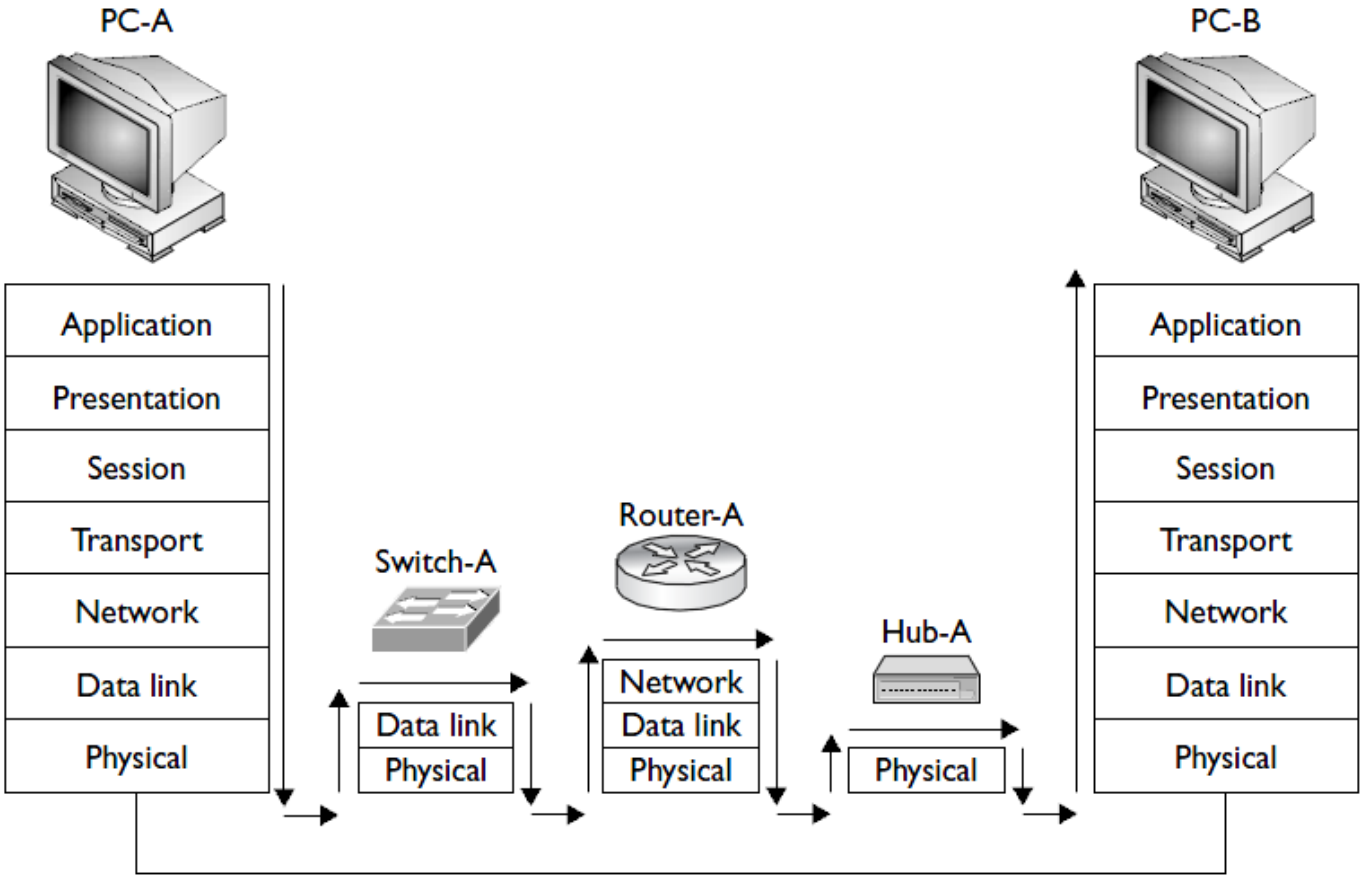


هر لایه برای انجام دادن کار باید یک سری اطلاعات کنترلی داشته باشد تا گیرنده بتواند بر حسب آن اطلاعات کار انجام دهد. که هر لایه یک سری اطلاعات کنترلی به داده‌ها اضافه می‌کند و به لایه بعدی می‌فرستد.



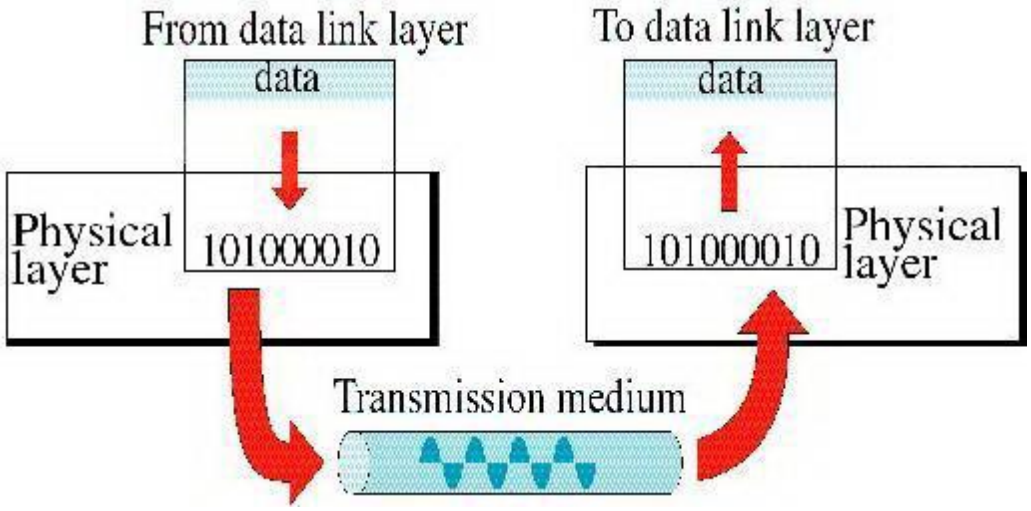
داده‌ها توسط یک برنامه و توسط کاربر تولید خواهند شد (نظیر یک پیام الکترونیکی). شروع ارسال داده‌ها از لایه Application است. در ادامه و با حرکت به سمت پایین، در هر لایه عملیات مربوطه انجام و داده هایی به بسته‌های اطلاعاتی اضافه خواهد شد. در آخرین لایه (لایه فیزیکی) با توجه به محیط انتقال استفاده شده، داده‌ها به سیگنالهای الکتریکی، پالس هایی از نور و یا سیگنالهای رادیوئی تبدیل و از طریق کابل و یا هوا برای کامپیوتر مقصد ارسال خواهند شد. پس از دریافت داده در کامپیوتر مقصد، عملیات مورد نظر (معکوس عملیات ارسال) توسط هر یک از لایه‌ها انجام و در نهایت با رسیدن داده

به لایه Application و به کمک یک برنامه، امکان استفاده از اطلاعات ارسالی فراهم خواهد شد. شکل زیر نحوه انجام فرآیند فوق را نشان می‌دهد.



۸-۳- عملکرد هر یک از لایه‌های مدل مرجع OSI

۸-۳-۱- لایه Physical (لایه اول)

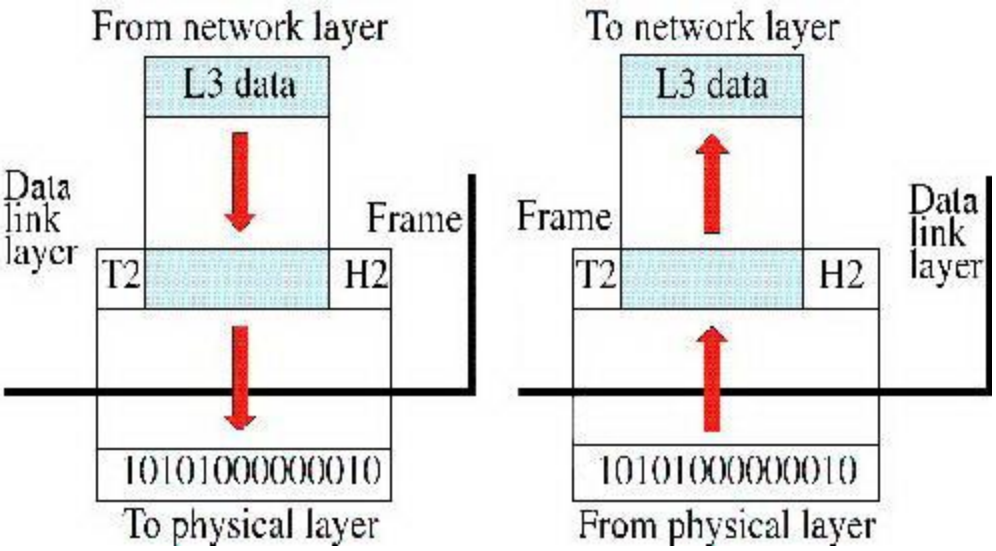


مسئولیت انتقال مجموعه‌ای از بیت‌ها از طریق رسانه‌ی فیزیکی بر عهده‌ی این لایه می‌باشد. در این لایه ابتدا توپولوژی فیزیکی، روش سیگنال دهی داخل رسانه انتقال و وسیله انتقال شبکه مورد بررسی قرار گرفته سپس اقدام به انتقال بیت‌ها می‌شود. از پروتکل هایی که در این لایه استفاده می‌شود، می‌توان از Ethernet ,ATM Gigabit و یا RS-233 نام برد.

خصوصیات به طور خلاصه

- کابل‌ها، کانکتورها، ولتاژها، نرخ انتقال داده.
- ارسال اطلاعات به صورت مجموعه‌ای از بیت‌ها، سیگنال‌های الکتریکی و اینترفیس‌های سخت‌افزاری.

۸-۳-۲- لایه Datalink (لایه دوم)



این لایه تهیه کننده آدرس‌های سخت‌افزاری (MAC) و مشخص کننده خطاها و کنترل‌کننده جریان می‌باشد. این لایه وظیفه دارد تا اطلاعات دریافت شده از لایه شبکه را به قالبی منطقی به نام فریم (Frame) تبدیل کند. در کامپیوتر مقصد این لایه همچنین مسئول دریافت بدون خطای این فریم‌ها است. ما در لایه پیوند داده‌ها با توپولوژی منطقی شبکه سروکار داریم. از جمله توپولوژی BUS و توپولوژی RING.

در توپولوژی BUS ما اطلاعات را طوری فریم بندی می‌کنیم که هر کس در شبکه وجود دارد بتواند اطلاعات را دریافت کند حالا اگر آدرس فیزیکی موجود در فریم مربوط به خود او باشد اطلاعات را قبول کند، و گرنه به اطلاعات کار نداشته باشد که این نوع توپولوژی در شبکه‌های BUS وStar رواج دارد.

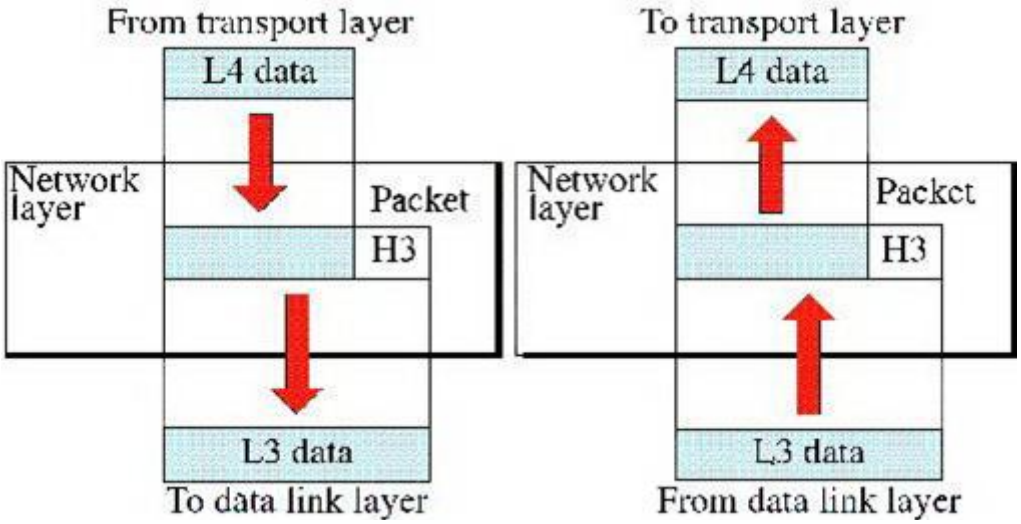
برای انتقال از یک دستگاه به دستگاه مشخص دیگر از توپولوژی منطقی RING استفاده می‌شود در اینجا هم توپولوژی فیزیکی شبکه می‌تواند RING یا STAR باشد.

آدرس سخت‌افزاری یا همان MAC Address، آدرس منحصر به فردی است که برای هر دستگاه وجود دارد.

خصوصیات به طور خلاصه

- انتقال مطمئن داده از طریق محیط انتقال
- آدرس‌دهی فیزیکی و یا سخت‌افزاری (MAC)، توپولوژی شبکه
- فریم‌ها در این لایه قرار دارند.

۸-۳-۳- لایه Network (لایه سوم)



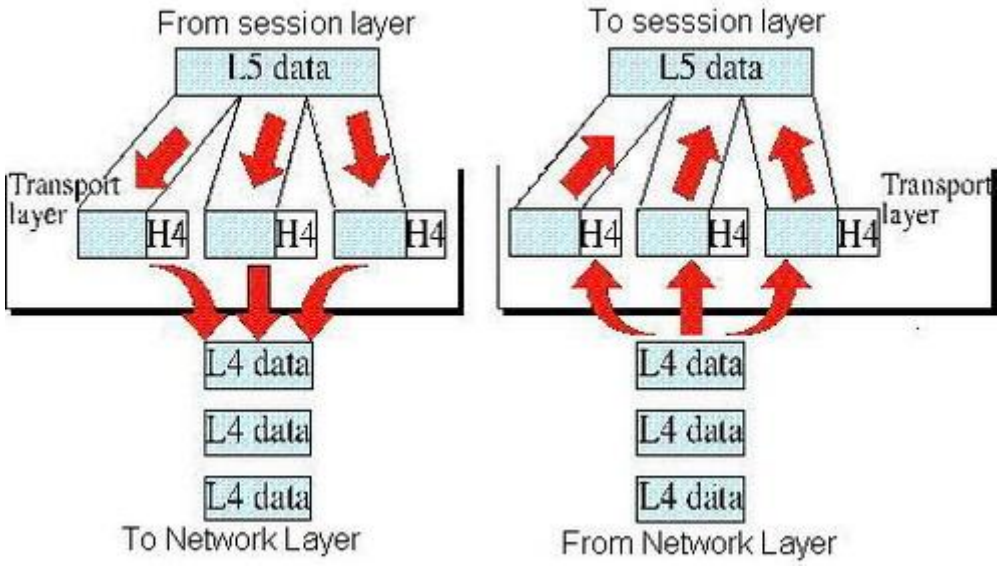
در این لایه با توجه به آدرس منطقی که به دستگاه‌ها در شبکه داده می‌شود مسیر یابی صورت میگیرد، در نتیجه ترافیک شبکه مدیریت می‌شود. می‌توان کارهایی که در این لایه انجام می‌شود را به صورت زیر دسته بندی کرد:

۱. تهیه آدرس منطقی منحصر به فرد که برای هر بخش از شبکه در نظر گرفته می‌شود و با آدرس MAC متفاوت است.
۲. مسیر یابی داده و پیداکردن بهترین مسیر از بین چند مسیر.
۳. کنترل خطا، کنترل ارتباط و ترتیب بندی بسته‌ها.

خصوصیات به طور خلاصه

- ارائه ارتباط و مسیر انتخابی برای دو سیستم
- حوزه روتینگ (مسیر یابی)
- پاسخ به سوالات متعددی نظیر نحوه ارتباط سیستم‌های موجود در سگمنت‌های متفاوت شبکه
- آدرس‌های مبداء، مقصد، Subnet و تشخیص مسیر لازم
- پروتکل‌های IP و IPX در این لایه استفاده می‌گردند.

۸-۳-۴- لایه Transport (لایه چهارم)



مسئول ارسال و دریافت اطلاعات و کمک به رفع خطاهای ایجاد شده در طول ارتباط است. هنگامی که حین یک ارتباط خطایی بروز دهد، این لایه مسئول تکرار عملیات ارسال داده است.

دو نوع انتقال در لایه انتقال برقرار است:

۱- بدون اتصال (Connection Less):

در این انتقال ما به رسیدن پیام به مقصد کاری نداریم و منتظر رسیدن پیغام تصدیق نمی‌مانیم که این باعث کاهش قابلیت اطمینان و افزایش سرعت می‌شود.

۲- اتصال گرا (Connection Oriented):

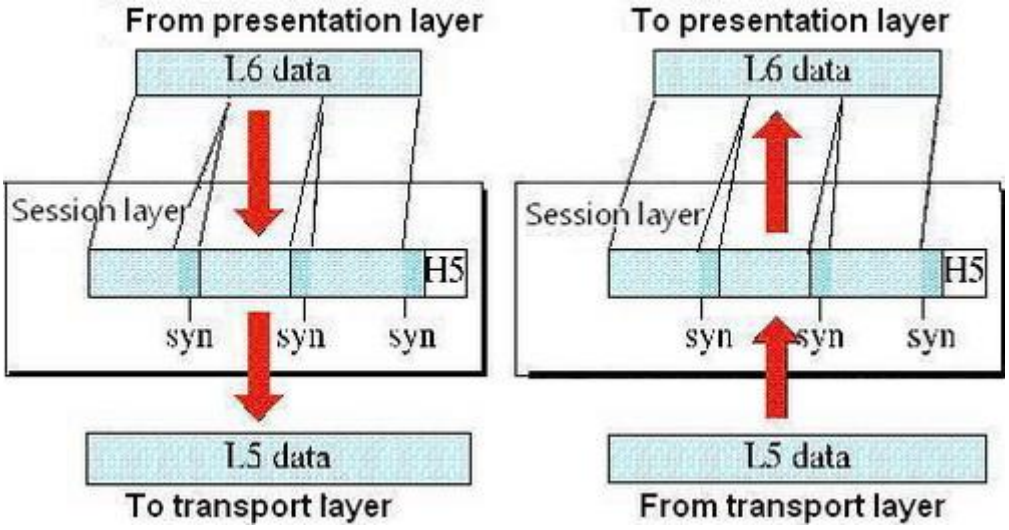
در این انتقال در پی هر ارسال، منتظر رسیدن پیغام تصدیق می‌شویم که این باعث افزایش قابلیت اطمینان ولی کاهش سرعت می‌شود. در لایه انتقال مدیریتی بر روی کنترل جریان صورت میگیرد و در گیرنده امکان تصحیح خطا و مرتب کردن بسته‌ها وجود دارد.

از پروتکلهای رایج در این لایه می‌توان از TCP و یا UDP نام برد.

خصوصیات به طور خلاصه

- در ارتباط با رویکردهای متفاوت حمل داده بین کامپیوترهای میزبان
- حمل مطمئن داده
- ایجاد، مدیریت و خاتمه مدارات مجازی
- تشخیص و برطرف نمودن خطا
- تقسیم داده به فریم و نسبت دهی یک دنباله عددی مناسب به هر یک از آنان
- پروتکل‌های TCP، UDP و SPX در این لایه قرار دارند.

۸-۳-۵- لایه Session (لایه پنجم)



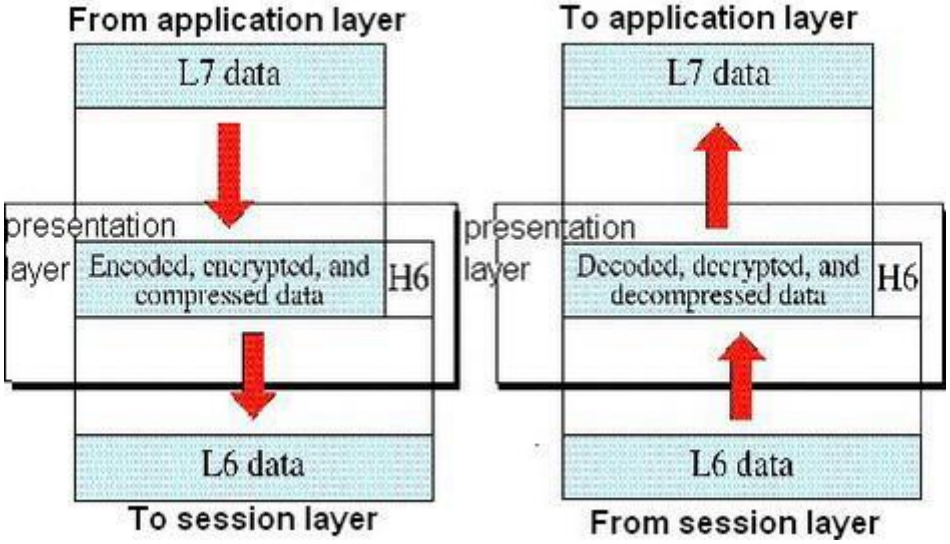
لایه‌ای است برای مدیریت ارتباط بین دو کاربر و در واقع ارائه کننده جلسه بین دو کاربر می‌باشد.

لایه جلسه یکسری قرارداد هایی را به اجرا می‌گذارد. مانند بررسی Username و Password کاربر در طول استفاده. در واقع این لایه بر برقراری اتصال بین دو برنامه کاربردی روی دو کامپیوتر مختلف واقع در شبکه نظارت دارد. همچنین تامین کننده همزمانی فعالیت‌های کاربر نیز هست.

خصوصیات به طور خلاصه

- ایجاد، مدیریت و خاتمه ارتباط برقرار شده بین برنامه ها

۸-۳-۶- لایه Presentation (لایه ششم)

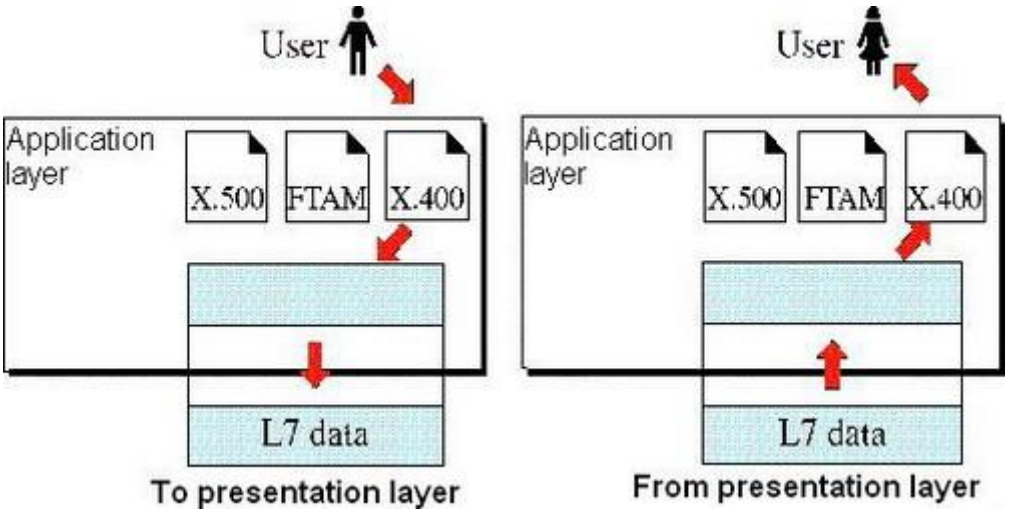


لایه‌ی Presentation راه هایی را فراهم می‌کند تا داده برای کاربر ارائه شود. پروتکل مربوط به این لایه فرمت داده را فراهم می‌کند و وقتی که می‌خواهیم داده را به لایه پایین‌تر بدهیم، لایه‌ی ارائه این داده را به گونه‌های Bit order Byte order, , Character order , File syntax به جمله انتقالیTransfer Syntax ترجمه می‌کند. در واقع این لایه تعیین کننده فرمت یا قالب انتقال داده‌ها بین کامپیوترهای واقع در شبکه است. این لایه در کامپیوتر مبدا داده هایی که باید انتقال داده شوند را به یک قالب میانی تبدیل می‌کند. این لایه در کامپیوتر مقصد اطلاعات را از قالب میانی به قالب اولیه تبدیل می‌کند.

خصوصیات به طور خلاصه

- ایجاد اطمینان لازم در رابطه با قابل استفاده بودن داده برای سیستم دریافت کننده
- فرمت داده
- ساختمآن‌های داده
- توافق در رابطه با گرامر انتقال داده برای لایه Application
- رمزنگاری داده

۸-۳-۷- لایه Application (لایه هفتم)



این آخرین لایه در اصل لایه‌ای است که کاربر تمام موارد قابل مشاهده را در آن مشاهده می‌کند. در این لایه دستگاه‌های فرستنده و گیرنده تعریف می‌شوند، کیفیت سرویس دهی و امنیت مشخص می‌شود. این لایه تامین کننده سرویس‌های پشتیبانی برنامه‌های کاربردی نظیر انتقال فایل، دسترسی به بانک اطلاعاتی و پست الکترونیکی است.

به عنوان مثال می‌توان به کارهای زیر اشاره کرد:

۱. انتقال فایل
۲. پیغام Email، وب و چت
۳. چاپ تحت شبکه
۴. بقیه عملیات هایی که دستگاه را با بقیه فرمآن‌های شبکه مرتبط می‌کنند.

نکته: معروفترین پروتکل این لایه FTP می‌باشد.

خصوصیات به طور خلاصه

- ارائه سرویس‌های شبکه به برنامه‌ها (نظیر پست الکترونیکی، ارسال فایل‌ها و...)
- تشخیص زمان لازم به منظور دستیابی به شبکه

۸-۴- نگاهی انتقادی به مدل OSI و پروتکل‌های آن

مدل OSI و پروتکل هایش هیچکدام کامل نیستند، و جا دارد برخی از نقاط ضعف آن‌ها را بر شماریم. در این قسمت، برخی از نقاط ضعف مدل OSI را برسی خواهیم کرد. در سال ۱۹۸۹، بسیاری متخصصان برجسته شبکه بر این باور بودند که آینده در بست متعلق به مدل OSI و پروتکل‌های آن است، و هیچ چیز نمی‌تواند در مقابل پیشرفت آن مقاومت کند. اما این اتفاق نیفتاد. چرا؟ نگاهی به گذشته درس‌های بسیاری را برای چشمان عبرت بین دارد، که می‌توان آن‌ها را چنین خلاصه کرد:

۱. زمان نامناسب
۲. تکنولوژی نامناسب
۳. پیاده سازی نامناسب
۴. سیاست‌های نامناسب

۸-۴-۱- زمان نامناسب

اولین عامل شکست مدل OSI زمان نامناسب بود. زمانی که یک استاندارد وضع می‌شود، زمان ارائه، اهمیت حیاتی در موفقیت و عدم موفقیت آن دارد. دیوید کلارک از دانشگاه MIT (برترین دانشگاه صنعتی جهان) فرضیه‌ای در زمینه استانداردها دارد که به **ملاقات فیل‌ها** معروف است. این فرضیه میزان فعالیت‌ها حول یک موضوع جدید را نشان می‌دهد. وقتی موضوعی برای اولین بار کشف می‌شود، گرداگرد آن سیلی از فعالیت‌های تحقیقی (به شکل بحث، مقاله و سخنرانی) فرا می‌گیرد. بعد از مدتی این فروکش می‌کند و بعد از اینکه صنعت به این موضوع علاقمند شد، موج سرمایه گذاری‌ها، به صورت پی در پی می‌آید.

بسیار مهم است که در محل تلاقی این دو فیل (موج تحقیق و موج سرمایه گذری) استانداردها به طور کامل وضع شوند. اگر استاندارد زودتر از موعد (قبل از پایان تحقیقات) نوشته شود، خطر آن است که موضوع به درستی درک نشده باشد و استاندارد ضعیف از آب دراید. اگر استاندارد دیرتر از موعد (بعد از شروع موج سرمایه گذاری) نوشته شود، شرکتهای بسیاری قبلاً (از مسیرهای مختلف) در آن سرمایه گذاری کرده‌اند، و این خطر وجود دارد که استانداردهای آن‌ها را نادیده بگیرد. اگر فاصله این دو فیل خیلی کم باشد (همه عجله داشته باشند که کار را زودتر شروع کنند)، خطر آن است که نویسندگان استاندارد بین آن‌ها له شوند.

اکنون معلوم شده است که پروتکل‌های استاندارد OSI بین فیل‌ها له شده‌اند. وقتی که پروتکل‌های OSI پا به عرصه وجود گذاشتند، پروتکل‌های رقیب (TCP/IP) مدت‌ها بود که در مراکز تحقیقاتی و دانشگاه‌ها پذیرفته شده بودند. با اینکه هنوز موج سرمایه گذاری صنعتی در TCP/IP شروع نشده بود. اما بازار آکادمیک آنقدر بزرگ بود که شرکتهای بسیاری را تشویق به تولید محصولات TCP/IP کند. و وقتی OSI بالاخره از راه رسید، کسی نبود که داوطلبانه از آن پشتیبانی کند. همه منتظر بودند دیگری قدم اول را بر دارد.، قدمی که هرگز برداشته نشد و OSI در نطفه خفه شد.

۸-۴-۲- تکنولوژی نامناسب

دلیل دیگری که OSI هرگز پا نگرفت، آن بود که این مدل و پروتکل‌های آن هر دو ناقص و معیوب بودند. انتخاب هفت لایه برای این مدل بیشتر یک انتخاب سیاسی بود تا فنی، و در حالی که دو لایه آن (نشست و نمایش) تقریباً خالی بودند، در لایه‌های دیگر (لینک داده و شبکه) جای نفس کشیدن نبود.

مدل OSI (و سرویس‌ها و پروتکل‌های آن) به طور باور نکردی پیچیده است. اگر کاغذهای چاپی این استاندارد را روی هم بچینید. ارتفاع آن از نیم متر هم بیشتر خواهد شد. پیاده سازی پروتکل‌های OSI بسیار دشوار، و عملکرد آن‌ها ناقص است. در این رابطه، نقل جمله جالبی از پاول موکاپتریس (۱۹۹۳، Rose) خالی از لطف نیست:

سوال: از ترکیب یک گانگستر با یک استاندارد بین المللی چه چیزی بدست می‌آید؟

جواب: کسی پیشنهادی به شما می‌کند که از آن سر در نمی‌آورید.

مشکل دیگر مدل OSI، علاوه بر غیر قابل فهم بودن آن، این است که برخی از عملکردهای آن (مانند آدرس‌دهی، کنترل جریان داده‌ها و کنترل خطا)در تمام لایه‌ها تکرار می‌شود. برای مثال، سالتزر و همکارانش (۱۹۸۴) نشان دادند که کنترل خطا

باید در بالاترین لایه انجام شود تا بیشترین تاثیر را داشته باشد، بنابراین تکرار آن در لایه‌های پائین‌تر نه تنها غیر ضروری است، بلکه باعث افت کارایی هم خواهد شد

۸-۴-۳- پیاده سازی نامناسب

با توجه به پیچیدگی بیش از حد مدل OSI و پروتکل‌های آن، جای تعجب نبود که اولین پیاده سازی‌های آن حجیم، سنگین و کند است. آن‌هایی که با این مدل کار کرده بودند، به زودی پشیمان شدند، و طولی نکشید که کلمه OSI مترادف شد با "کیفیت بد". بعدها محصولات بهتری به بازار آمد، اما آوازه منفی OSI فراموش نشد.

از طرف دیگر، اولین پیاده سازی TCP/IP (که بخشی از سیستم عامل یونیکس دانشگاه برکلی بود) بسیار خوب از کار در آمد (و لازم به گفتن نیست که مجانی هم بود). افراد بسیاری با سرعت شروع به استفاده از آن کردند، طرفدار آن شدند، آن را توسعه دادند، و این باعث شد که باز هم به خیل طرفداران آن اضافه شود. در اینجا، بر خلاف OSI، مارپیچ رو به بالا می‌رفت، نه پایین.

۸-۴-۴- سیاست‌های نامناسب

دلیل استفاده از TCP/IP این بود که بسیاری از افراد (به ویژه در محیط‌های دانشگاهی) تصور می‌کردند که TCP/IP جزئی از یونیکس است، و یونیکس هم در آن دوران محبوبیتی فوق العاده داشت.

از سوی دیگر، این عقیده رواج داشت که OSI یک مخلوق دولتی (مخصوصا دولت‌های اروپایی و آمریکایی) است. البته این عقیده تا حدی درست بود، اما همین تصور هم که عده‌ای دیوان سالار دولتی بخواهد یک استاندارد دولتی را به زور به جا بیندازد، باعث شد تا برنامه نویسان و طراحان شبکه تمایلی از خود برای همکاری نشان ندهند. زبان‌های برنامه نویسی PL/1 (که در دهه ۱۹۶۰ از سوی IBM به عنوان زبان آینده توسعه داده شد) و Ada (که وزارت دفاع آمریکا حامی آن بود) به همین دلیل دچار سرنوشتی مشابه شدند.

۸-۵- ساختار لایه‌ها در مدل TCP/IP

در قسمت قبل، معایب مدل OSI را مشاهده نمودید.، در ادامه مدل دیگری به نام TCP/IP معرفی می‌کنیم. از آنجا که پروتکل TCP/IP در اینترنت بسیار مناسب است از این پروتکل در اغلب شبکه‌های داخلی نیز استفاده می‌شود این پروتکل برای کاربران حرفه‌ای شبکه بسیار کاربردی است. زیرا اتصال شبکه را تضمین می‌کند و به کاربر اجازه ارسال و دریافت فایل‌ها را به راحتی می‌دهد. حال به لایه‌های TCP/IP که برگرفته از مدل OSI است اشاره می‌کنیم.

۸-۵-۱- مفاهیم اولیه پروتکل TCP/IP

TCP/IP، یکی از مهمترین پروتکل‌های استفاده شده در شبکه‌های کامپیوتری است. اینترنت به عنوان بزرگترین شبکه موجود، از پروتکل فوق به منظور ارتباط دستگاه‌های متفاوت استفاده می‌نماید.

مقدمه

امروزه اکثر شبکه‌های کامپیوتری بزرگ و اغلب سیستم‌های عامل موجود از پروتکل TCP/IP، استفاده و حمایت می‌نمایند. TCP/IP، امکانات لازم به منظور ارتباط سیستم‌های غیر مشابه را فراهم می‌آورد. از ویژگی‌های مهم پروتکل فوق، می‌توان به مواردی همچون: قابلیت اجراء بر روی محیط‌های متفاوت، ضریب اطمینان بالا، قابلیت گسترش و توسعه آن، اشاره

کرد. از پروتکل فوق، به منظور دستیابی به اینترنت و استفاده از سرویس‌های متنوع آن نظیر وب و یا پست الکترونیکی استفاده می‌گردد. تنوع پروتکل‌های موجود در پشته TCP/IP و ارتباط منطقی و سیستماتیک آن‌ها با یکدیگر، امکان تحقق ارتباط در شبکه‌های کامپیوتری را با اهداف متفاوت، فراهم می‌نماید. فرآیند برقراری یک ارتباط، شامل فعالیت‌های متعددی نظیر: تبدیل نام کامپیوتر به آدرس IP معادل، مشخص نمودن موقعیت کامپیوتر مقصد، بسته بندی اطلاعات، آدرس‌دهی و مسیر دهی داده‌ها به منظور ارسال موفقیت آمیز به مقصد مورد نظر، بوده که توسط مجموعه پروتکل‌های موجود در پشته TCP/IP انجام می‌گیرد.

۸-۵-۲- معرفی پروتکل TCP/IP

از پروتکل TCP/IP، به منظور ارتباط در شبکه‌های بزرگ استفاده می‌گردد. برقراری ارتباط از طریق پروتکل‌های متعددی که در ۴ لایه مجزا سازماندهی شده‌اند، میسر می‌گردد. هر یک از پروتکل‌های موجود در پشته TCP/IP، دارای وظیفه‌ای خاص در این زمینه (برقراری ارتباط) می‌باشند. در زمان ایجاد یک ارتباط، ممکن است در یک لحظه تعداد زیادی از برنامه‌ها، با یکدیگر ارتباط برقرار نمایند. TCP/IP، دارای قابلیت تفکیک و تمایز یک برنامه موجود بر روی یک کامپیوتر با سایر برنامه‌ها بوده و پس از دریافت داده‌ها از یک برنامه، آن‌ها را برای برنامه متناظر موجود بر روی کامپیوتر دیگر ارسال می‌نماید. نحوه ارسال داده توسط پروتکل TCP/IP از محلی به محل دیگر، با فرآیند ارسال یک نامه از شهری به شهر، قابل مقایسه است.

برقراری ارتباط مبتنی بر TCP/IP، با فعال شدن یک برنامه بر روی کامپیوتر مبدا آغاز می‌گردد. برنامه فوق، داده‌های مورد نظر جهت ارسال را به گونه‌ای آماده و فرمت می‌نماید که برای کامپیوتر مقصد قابل خواندن و استفاده باشند. (مشابه نوشتن نامه با زبانی که دریافت کننده، قادر به مطالعه آن باشد). در ادامه آدرس کامپیوتر مقصد، به داده‌های مربوطه اضافه می‌گردد (مشابه آدرس گیرنده که بر روی یک نامه مشخص می‌گردد). پس از انجام عملیات فوق، داده به همراه اطلاعات اضافی (درخواستی برای تائید دریافت در مقصد)، در طول شبکه بحرکت درآمده تا به مقصد مورد نظر برسد. عملیات فوق، ارتباطی به محیط انتقال شبکه به منظور انتقال اطلاعات نداشته، و تحقق عملیات فوق با رویکردی مستقل نسبت به محیط انتقال، انجام خواهد شد.

۸-۶- عملکرد هر یک از لایه‌های مدل TCP/IP

۸-۶-۱- لایه کاربردی

این لایه مجموع لایه‌های کاربردی، ارائه و جلسه در مدل OSI می‌باشد. این لایه داده اولیه را برای کاربر فراهم می‌کند و برای کاربران این دلیل خوبی است که به راحتی از آن استفاده کنند. در زیر به پروتکلهای این لایه اشاره می‌کنیم:

:Telnet

پروتکل کاربردی برای ارتباط از راه دور به کامپیوتر میزبان است که البته مدل ابتدایی است و مدلهای بالایی برای این کار وجود دارد از جمله RDP، ICA و یا Windows. البته Telnet ارتباط دقیق به پنجره جاری کامپیوتر میزبان است که از طریق پروتکل TCP/IP این عمل را انجام میدهد. البته از Telnet برای ارتباط با مسیریاب و همچنین تست اینکه ارتباط شبکه برقرار است یا نه استفاده می‌شود.

:FTP

پروتکلی است برای اتصال به کامپیوتر میزبان، فرستادن یا دریافت فایل بین کامپیوتر میزبان (راه دور) است که اتصال گرا بوده و انتقال داده را ضمانت می‌کند.

:TFTP

شبیه FTP است ولی برای مسافتهای طولانی استفاده شده و از پروتکل UDP استفاده می‌کند.

:HTTP

مشهورترین پروتکل در این گروه بوده و از آن برای رایج ترین سرویس اینترنت یعنی وب استفاده می گردد. با استفاده از پروتکل فوق کامپیوترها قادر به مبادله فایل‌ها با فرمت های متفاوت متن، تصاویر،گرافیکی، صدا، ویدئو و... خواهند بود. برای مبادله اطلاعات با استناد به پروتکل فوق می بایست، کاربران با استفاده از یک مرورگر وب قادر به استفاده از سرویس فوق خواهند بود.

:HTTPS

HTTPS یا HTTP Over SSL همان پروتکل HTTP است با افزودن امنیت برای مرور صفحات با امنیت بالاتر

:IMAP4/POP3

دوپروتکل برای انتقال پیام الکترونیکی از طریق اینترنت هستند.

پروتکل POP3 برای دریافت پیغام در کلاینت و همچنین برای ارسال و دریافت در سرور استفاده می‌شود.

فرق بین POP3 و IMAP4 در اینست کهIMAP4 همانند یک فایل سرور از راه دور عمل می‌کند در حالی که POP3 در جایگاه اصلی کار می‌کند.

:SMTP

پروتکلی است برای ارسال پیغام الکترونیکی ولی قابلیت دریافت هم دارد و حجم آن کم است.

در واقع POP3 در حکم دریافت کننده پیغام و SMTP در حکم ارسال کننده پیغام کار می‌کند.

:NTP

پروتکلی است برای تنظیم زمان در اینترنت و مدیریت زمانی دریافت و ارسال اطلاعات در سرور.

:SNMP

پروتکلی است برای مشاهده و مدیریت وسایل شبکه که به مدیر شبکه در صورت بروز خطا، اخطارهای لازم را میدهد.

:DHCP

پروتکل DHCP (Dynamic Host Configuration Protocol) به شما اجازه می دهد آدرسهای IP را بصورت اتوماتیک به کامپیوترها و وسایل جانبی روی شبکه اختصاص دهید. آدرس های IP از مخزنی از آدرس های تهیه شده و به کامپیوترها اختصاص داده می شوند و نیاز به وارد کردن دستی آدرسهای IP نباشد.

:DNS

پروتکل DNS (Domain Name System) هر کامپیوتر در شبکه یک Host نامیده می شود و علاوه بر آدرس IP دارای یک عنوان مشخص کننده دیگر به نام Host Name می باشد. از پروتکل فوق به منظور ترجمه Host Name به آدرس های IP استفاده می گردد. یک کامپیوتر برای بدست آوردن IP Address متناظر با Host Name از کامپیوتری در

شبکه با نام، DNS Server کمک می گیرد. DNS Server حاوی نام و IP Address کامپیوتر مورد نظر می باشد که پس از مقایسه درخواست با اطلاعات موجود در Database (پایگاه داده) خود، IP Address مورد نظر را بر میگرداند.

۸-۶-۲- لایه انتقال

همانند لایه انتقال در پروتکل مدل OSI می‌باشد با پروتکلهای زیر:

:TCP

این پروتکل اتصال گرا، رسیدن داده‌ها به مقصد و درست به هم پیوستن بسته‌ها را تضمین می‌نماید.

کارکرد پروتکل TCP به نوع شبکه، توپولوژی و سرعت شبکه ربطی ندارد بلکه در این پروتکل با شماره گذاری هر بسته، بسته‌ها از مبدا به مقصد فرستاده می‌شود و در آنجا دوباره بسته‌ها به ترتیب شده و پیغام دریافت درست بسته‌ها، به مبدا ارسال می‌شود.

:UDP

اگر شبکه‌ای از TCP استفاده نکند از UDP استفاده می‌کند در پروتکل UDP که برای ارسال داده‌های کم و برای سرعت بالا استفاده می‌شود هیچگونه پیغام تصدیقی مبنی بر رسیدن درست داده به مقصد ارسال نمی‌شود.

۸-۶-۳- لایه شبکه

برگرفته از همان لایه شبکه در مدل OSI است با این تفاوت که فقط از پروتکل IP استفاده می‌کند. زیر پروتکلهای این لایه عبارتند از:

:ARP

پروتکلی برای مشخص کردن آدرس می‌باشد، یعنی آدرس فیزیکی و آدرس IP را با یکدیگر Map (نگاشت) می‌کند. این پروتکل در حقیقت برای زمانی که قرار است از یک کامپیوتر در یک ساختمان به کامپیوتر دیگر در ساختمان دیگر اطلاعاتی فرستاده شود و مابین یک مسیریاب بر اساس آدرس فیزیکی کار می‌کند، استفاده می‌شود. در اینجا از این پروتکل برای تبدیل آدرس IP به فیزیکی و بر عکس استفاده می‌شود.

:ICMP

پروتکلی است برای کنترل پیغام و گزارش خطا به این معنی که وقتی از دستور Ping برای اینکه ببینیم که می‌توانیم با کامپیوتر میزبان ارتباط برقرار کنیم یا نه استفاده می‌کنیم، در حقیقت در حال استفاده از ICMP هستیم.

:IP

یک پروتکل بدون اتصال است و تمام کارها در مدل TCP/IP مبتنی بر این پروتکل IP می‌باشد این پروتکل آدرس وسیله میزبان و وسایل شبکه را برای بر قراری ارتباط فراهم می‌کند.

۸-۶-۴- لایه Network Interface (Physical)

لایه "اینترفیس شبکه"، مسئول استقرار داده بر روی محیط انتقال شبکه و دریافت داده از محیط انتقال شبکه است. لایه فوق، شامل دستگاه‌های فیزیکی نظیر کابل شبکه و آداپتورهای شبکه است. کارت شبکه (آداپتور) دارای یک عدد دوازده رقمی مبنای شانزده (نظیر: B5-50-04-22-D4-66) بوده که آدرس MAC، نامیده می‌شود. لایه "اینترفیس شبکه"، شامل پروتکل‌های مبتنی بر نرم‌افزار مشابه لایه‌های قبل، نمی‌باشد. پروتکل‌های Ethernet و Asynchronous Transfer(ATM

Mode)، نمونه هایی از پروتکل‌های موجود در این لایه می‌باشند. پروتکل‌های فوق، نحوه ارسال داده در شبکه را مشخص می‌نمایند.

۸-۷- نگاهی انتقادی به مدل TCP/IP

مدل TCP/IP و پروتکل‌های آن نیز مشکل خاص خود را دارند.

اول اینکه، در این مدل مفاهیم سرویس، واسط و پروتکل به روشنی از یکدیگر تفکیک نشده‌اند. کاری که در مدل OSI به خوبی انجام شده است. به همین دلیل نمی‌توان از TCP/IP به عنوان ابزاری برای طراحی و توسعه شبکه‌های جدید استفاده کرد.

دوم اینکه، مدل TCP/IP به هیچ عنوان یک مدل کلی نیست، و نمی‌توان از آن برای توصیف شبکه‌های غیر TCP/IP استفاده کرد. برای مثال، توصیف بلوتوث با مدل TCP/IP به کلی غیر ممکن است.

سوم این که، با در نظر گرفتن مفاهیم شبکه‌های چند لایه، لایه –میزبان– به شبکه اساسا یک لایه واقعی نیست، بلکه فقط یک واسط (بین لایه‌های شبکه و لینک داده) است. در واقع، این یکی از مهمترین جاهایی است که مدل TCP/IP مفاهیم واسط و لایه‌ها را با هم ترکیب کرده است.

چهارم اینکه، در مدل TCP/IP هیچ تمایزی بین لایه‌های فیزیکی و لینک داده نیست (و حتی حرفی از آن‌ها به میان نیامده است). اینها دو لایه کاملاً متفاوت هستند. لایه فیزیکی با مشخصات کابل و فیبر نوری و کانال‌های مخابراتی سر و کار دارد، در حالی که وظیفه لایه پیوند داده شکستن لایه‌ها به قطعات کوچکتر و اطمینان از تحویل صحیح آن‌ها به مقصد است. در یک مدل کامل این دو لایه باید از هم جدا باشند؛ کاری که در مدل TCP/IP انجام نشده است.

در تصویر زیر تشابه لایه‌ها در دو مدل مرجع OSI و TCP/IP را مشاهده می‌کنید:

<table>
<tr><td>Application</td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td></tr>
<tr><td>Transport</td><td>Transport</td></tr>
<tr><td>Network</td><td>Internet</td></tr>
<tr><td>Data Link</td><td rowspan="2">Network Address</td></tr>
<tr><td>Physical</td></tr>
</table>

فصل ۹

شبکه‌های بی‌سیم

۹-۱- مبانی شبکه‌های بی‌سیم

۹-۱-۱- مقدمه

نیاز روز افزون به پویایی کارها، استفاده از تجهیزاتی مانند تلفن همراه، پیجرها و... بواسطه وجود شبکه‌های بی‌سیم امکان پذیر شده است. اگر کاربر یا شرکت یا برنامه کاربردی خواهان آن باشد که داده و اطلاعات مورد نیاز خود را به صورت متحرک در هر لحظه در اختیار داشته باشند شبکه‌های بی‌سیم جواب مناسبی برای آن‌ها ست.

۹-۱-۲- تاریخچه شبکه‌های بی‌سیم

یکی ازمواردی که در عصر ارتباطات همواره مورد توجه بوده و هست، سرعت دسترسی به اطلاعات است. کابران در انواع و اقسام شبکه های مختلف، همواره در پی دستیابی به سرعت های بالاتر در انتقال اطلاعات هستند و به نظر می‌رسد که اشتهای سیری ناپذیری در این زمینه وجود دارد. پیشرفت‌ها و فعالیت های صورت گرفته در این زمینه، شاهد و گواه این مسأله است.

از طرفی دیگر با وجود آمدن شبکه های بی‌سیم، روز به روز بر تعداد کاربران این نوع شبکه‌ها افزوده می‌شود. دسترسی آسان و فراگیر که کاربران را قادر می‌سازد تا فارغ از مسائلی مانند کابل شبکه، به شبکه دلخواه خود متصل شوند. بنابراین سرعت دسترسی به اطلاعات و همچنین دسترسی به صورت بی‌سیم، دو مسئله ای هستند که در کنار یکدیگر در قالب شبکه بی‌سیم پر سرعت و با برد مناسب مطرح می‌شوند. کاربران خواهان شبکه ای هستند که سرعت مناسب و بالایی برای انتقال اطلاعات داشته باشد و علاوه بر آن برد مؤثر این شبکه در حدی باشد که آن‌ها را محدود به موقعیت و وسعت جغرافیایی خاصی نکند.

همانطور که در بخش قبلی اشاره شد، شبکه های مادون قرمز اولین دسته از شبکه های بی‌سیم بودند که از آن‌ها برای انتقال اطلاعات در محیط های کامپیوتری استفاده شد. این نوع شبکه‌ها سرعت چندان بالایی نداشتند و از طرفی دیگر برد

مناسب و کاربر پسندی برای آن‌ها وجود نداشت. به همین دلیل و دلایل مشابه، استقبال و پیشرفت چندانی نداشتند و رفته رفته فراموش شدند.

در اوائل دهه ۹۰ میلادی، نسل جدید از شبکه های بی‌سیم با عنوان شبکه های بی‌سیم Wi-Fi وارد بازار شدند. این دسته از شبکه‌ها در مقایسه با شبکه های مادون قرمز، سرعت و برد مناسبی داشتند ولی همچنان از دید بسیاری از کاربران مورد تمسخر قرار می‌گرفتند. عده ای از آن‌ها سرعت پایین در مقایسه با شبکه های کابلی و عده ای دیگر نبود امنیت و یا برد پایین را بهانه و دلیلی برای استفاده نکردن از این شبکه‌ها مطرح می‌کردند.

اما شبکه های Wi-Fi به رشد صعودی خود ادامه دادند و با وجود آمدن استانداردها و نسل های جدید از این نوع شبکه، تعداد کابران آن‌ها روز به روز بیشتر و بیشتر شد. انواع جدید شبکه های Wi-Fi، سرعت مناسب، برد خوب و همچنین امنیت بیشتر را به همراه داشتند.

نسل اول شبکه های Wi-Fi سرعتی در حدود 11Mbps داشتند و می‌توانستند کاربران را تا محدوده ای چند ده متری مورد پوشش قرار دهند. همچنین نسل های بعدی این نوع شبکه‌ها، سرعت هایی برابر با 22Mbps و حتی 54Mbps دارند و می‌توانند کاربران را تا محدوده ای چند صد متری مورد پوشش قرار دهند.

اما باز هم شبکه های Wi-Fi نتوانسته‌اند به نیازهای رو به رشد کاربران پاسخ بدهند. زیرا برای دسترسی های بالا مانند 54Mbps کاربران مجبور به پرداخت هزینه های سنگینی هستند در حالی که با همین مقدار هزینه می‌توان یک شبکه کابلی بسیار مناسب را طراحی و تجهیز کرد. از طرفی دیگر برد شبکه های Wi-Fi در حد چند صد متری است و این برد برای شبکه های کوچک و خانگی مناسب است و نمی‌توان از آن برای ایجاد و یا توسعه یک شبکه تجاری و بزرگ (مانند شبکه ای که در سطح یک شهر گسترده است) استفاده کرد.

نکته: البته در شبکه های Wi-Fi می‌توان از انواع آنتن های شبکه برای گسترش برد و توسعه آن‌ها استفاده کرد اما این کار هزینه در خور توجهی دارد و حتی با مصرف این هزینه نمی‌توان به شبکه با برد دلخواه دسترسی پیدا کرد. در حالی که با همین هزینه می‌توان یک شبکه کابلی با سرعت و امکانات مناسب را طراحی و پیاده سازی کرد.

مطالب بیان شده در مورد شبکه های Wi-Fi بدان معنا نیست که این نوع شبکه‌ها مناسب و یا مفید نیستند. بلکه می‌توان نتیجه گرفت که شبکه های Wi-Fi برای محیط های کوچک و یا حداکثر متوسط مفید و مناسب هستند و نمی‌توانند به نیازهای کاربران در شبکه های بزرگ و گسترده پاسخ بدهند.

بنابراین هنوز پاسخ مشخص و روشنی به کاربرانی که نیازمند شبکه های بی‌سیم با برد و سرعت مناسب هستند، داده نشده بود. در اوایل هزاره جدید، گروهی از متخصصان، طراحان و صاحب نظران در زمینه شبکه های کامپیوتری به خصوص شبکه های بی‌سیم، ایده و ساختاری را پیشنهاد کردند که بر اساس آن نسل جدیدی از شبکه های بی‌سیم یا قابلیت هایی که بتواند به دو نیاز اصلی برد و سرعت مناسب کاربران پاسخ بدهد، معرفی شدند.

این نوع از شبکه با عنوان تبادل و استفاده از اطلاعات در سطح جهانی از طریق امواج بی‌سیم مایکرو ویو، مطرح شد که به آن به طور اختصار WIMAX گفته می‌شود. هسته اصلی وایمکس بر اساس برد و سرعت بالا طراحی شده است تا بتواند به نیاز کاربران پاسخ بدهد و مشکلات و معایب شبکه های قبلی مانند Wi-Fi را برطرف کند.

نکته: یکی از گروه های اصلی و بنیان گذار شبکه های وایمکس، گروه WiMAX Forum است. در حال حاضر این گروه علاوه بر توسعه و ارتقاء شبکه های وایمکس، برنامه های متعددی را برای همگانی و فراگیر کردن این نوع شبکه بی‌سیم، در دستور کار خود قرار داده است.

۹-۱-۳- تشریح مقدماتی شبکه‌های بی‌سیم و کابلی

شبکه‌های محلی (LAN) برای خانه و محیط کار می‌توانند به دو صورت کابلی (Wired) یا بی‌سیم (Wireless) طراحی گردند. درابتدا این شبکه‌ها به روش کابلی با استفاده از تکنولوژی Ethernet طراحی می‌شدند اما اکنون با روند رو به افزایش استفاده از شبکه‌های بی‌سیم با تکنولوژی WiFi مواجه هستیم.

در شبکه‌های کابلی (که در حال حاضر بیشتر با توپولوژی ستاره‌ای بکار می‌روند) بایستی از محل هر ایستگاه کاری تا دستگاه توزیع کننده (هاب یا سوئیچ) به صورت مستقل کابل کشی صورت پذیرد (طول کابل ازنوع CAT5 نبایستی ۱۰۰ متر بیشتر باشد در غیر اینصورت از فیبر نوری استفاده می گردد) که تجهیزات بکار رفته از دونوع غیر فعال (Passive) مانند کابل، پریز، داکت، پچ پنل و... و فعال (Active) مانند هاب، سوئیچ، روتر، کارت شبکه و... هستند.

موسسه مهندسی IEEE استانداردهای 802.3u را برای Fast Ethernet و 802.3ab و802.3z را برای Gigabit Ethernet (مربوط به کابلهای الکتریکی و نوری) در نظر گرفته است.

شبکه‌های بی‌سیم نیز شامل دستگاه مرکزی (Access Point) می‌باشد که هر ایستگاه کاری می‌تواند حداکثر تا فاصله ۳۰ متری آن (بدون مانع) قرار گیرد. شبکه‌های بی‌سیم (Wlan) یکی از سه استاندارد ارتباطی WiFi زیر را بکار می‌برند:

- 802.11b که اولین استانداردی است که به صورت گسترده بکار رفته است.
- 802.11a سریعتر اما گرانتر از 802.11b می‌باشد.
- 802.11g جدیدترین استاندارد که شامل هر دو استاندارد قبلی بوده و از همه گرانتر می‌باشد.

هر دونوع شبکه‌های کابلی و بی‌سیم ادعای برتری بر دیگری را دارند، اما انتخاب صحیح با در نظر گرفتن قابلیتهای آن‌ها میسر می‌باشد.

عوامل مقایسه

در مقایسه شبکه‌های بی‌سیم و کابلی می‌تواند قابلیتهای زیر مورد بررسی قرار گیرد:

- نصب و راه اندازی
- هزینه
- قابلیت اطمینان
- کارائی
- امنیت

نصب و راه اندازی

در شبکه‌های کابلی بدلیل آنکه به هر یک از ایستگاه‌های کاری بایستی از محل سویئچ مربوطه کابل کشیده شود با مسائلی همچون سوارخکاری، داکت کشی، نصب پریز و... مواجه هستیم در ضمن اگر محل فیزیکی ایستگاه مورد نظر تغییر یابد بایستی که کابل کشی مجدد و... صورت پذیرد

شبکه‌های بی‌سیم از امواج استفاده نموده و قابلیت تحرک بالائی را دارا هستند بنابراین تغییرات در محل فیزیکی ایستگاه‌های کاری به راحتی امکان پذیر می‌باشد برای راه اندازی آن کافیست که از روش‌های زیر بهره برد:

- Ad hoc که ارتباط مستقیم یا همتا به همتا (Peer to Peer) تجهیزات را با یکدیگر میسر می‌سازد.
- Infrastructure که باعث ارتباط تمامی تجهیزات با دستگاه مرکزی می‌شود.

بنابراین می‌توان دریافت که نصب و را ه اندازی شبکه‌های کابلی یا تغییرات در آن بسیار مشکلتر نسبت به مورد مشابه یعنی شبکه‌های بی‌سیم است.

هزینه

تجهیزاتی همچون هاب، سوئیچ یا کابل شبکه نسبت به موردهای مشابه در شبکه‌های بی‌سیم ارزان‌تر می‌باشد اما درنظر گرفتن هزینه‌های نصب و تغییرات احتمالی محیطی نیز قابل توجه است.

قابل به ذکر است که با رشد روز افزون شبکه‌های بی‌سیم، قیمت آن نیز در حال کاهش است.

قابلیت اطمینان

تجهیزات کابلی بسیار قابل اعتماد می‌باشند که دلیل سرمایه گذاری سازندگان از حدود بیست سال گذشته نیز همین می‌باشد فقط بایستی در موقع نصب و یا جابجائی، اتصالات با دقت کنترل شوند.

تجهیزات بی‌سیم همچون Broadband Routerها مشکلاتی مانند قطع شدن‌های پیاپی، تداخل امواج الکترومغناطیس، تداخل با شبکه‌های بی‌سیم مجاور و... را داشته‌اند که روند رو به تکامل آن نسبت به گذشته (مانند 802.11g) باعث بهبود در قابلیت اطمینان نیز داشته است.

کارائی

شبکه‌های کابلی دارای بالاترین کارائی هستند در ابتدا پهنای باند 10 Mbps سپس به پهنای باندهای بالاتر (100 Mbps و 1000Mbps) افزایش یافتند حتی در حال حاضر سوئیچهائی با پهنای باند 1Gbps نیز ارائه شده است.

شبکه‌های بی‌سیم با استاندارد 802.11b حداکثر پهنای باند 11Mbps و با 802.11a و 802.11g پهنای باند 54 Mbps را پشتیبانی می‌کنند حتی در تکنولوژیهای جدید این روند با قیمتی نسبتا بالاتر به 108Mbps نیز افزایش داده شده است علاوه بر این کارائی WiFi نسبت به فاصله حساس می‌باشد یعنی حداکثر کارائی با افزایش فاصله نسبت به Access Point پایین خواهد آمد. این پهنای باند برای به اشتراک گذاشتن اینترنت یا فایلها کافی بوده اما برای برنامه‌هائی که نیاز به رد و بدل اطلاعات زیاد بین سرور و ایستگاهای کاری (Client to Server) دارند کافی نیست.

امنیت

بدلیل اینکه در شبکه‌های کابلی که به اینترنت هم متصل هستند، وجود دیواره آتش از الزامات است و تجهیزاتی مانندهاب یا سوئیچ به تنهایی قادر به انجام وظایف دیواره آتش نمی‌باشند، بایستی در چنین شبکه‌هایی دیواره آتش مجزایی نصب شود.

تجهیزات شبکه‌های بی‌سیم مانند Broadband Routerها دیواره آتش بصورت نرم‌افزاری وجود داشته و تنها بایستی تنظیمات لازم صورت پذیرد. از سوی دیگر به دلیل اینکه در شبکه‌های بی‌سیم از هوا بعنوان رسانه انتقال استفاده می‌شود، بدون پیاده سازی تکنیک‌های خاصی مانند رمزنگاری، امنیت اطلاعات بطور کامل تامین نمی‌گردد استفاده از رمزنگاری WEP (Wired Equivalent Privacy) باعث بالا رفتن امنیت در این تجهیزات گردیده است.

جدول مقایسه ای

نوع سرویس	شبکه‌های کابلی	شبکه‌های بی‌سیم
نصب و راه اندازی	نسبتا مشکل	آسان
هزینه	کمتر	بیشتر
قابلیت اطمینان	بالا	متوسط
کارائی	خیلی خوب	خوب
امنیت	خوب	نسبتا خوب
پویایی حرکت	محدود	پویاتر

۹-۱-٤- تقسیم‌بندی شبکه‌های بی‌سیم



شبکه‌های بی‌سیم (Wireless) یکی از تکنولوژی‌های جذابی هستند که توانسته‌اند توجه بسیاری را بسوی خود جلب نمایند و عده‌ای را نیز مسحور خود نموده‌اند.

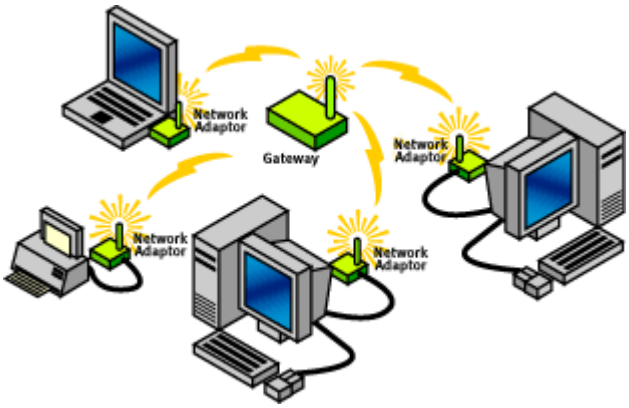
ارائه سرویس بدون سیم اینترنت یا WiFi، که امروزه در بسیاری نقاط دنیا به منظور جذب مشتری و به عنوان خدمتی نوین در جهت ارتقای سازمان در بازار رقابت، انجام می‌گیرد. خدمات اینترنت بی‌سیم علاوه بر مکآن‌های متعدد مانند هتل‌ها، نمایشگاه‌ها، بنادر، سالن‌های همایش و فرودگاه‌ها در منازل و محل‌های کار نیز عرضه می‌گردد و موجبات رضایت خاطر مشتریان و مسافران، به‌خصوص مشتریان و مسافران خارجی را فراهم آورده است.

بر اساس آمار تعداد کاربران این سرویس از ۱۲ میلیون نفر در سال ۲۰۰۲ به حدود ۷۰۰ میلیون نفر در سال ۲۰۰۸ برآورد می‌گردد. از طرفی META Group و In-Stat/MDR تخمین می‌زنند که در ۹۹٪از تولیدات شرکت‌های تولید کنندهٔ کامپیوترهای Laptop که در سال ۲۰۰۷ به فروش خواهند رسید، قابلیت استفادهٔ بی‌سیم (WiFi) بطور پیش‌فرض لحاظ خواهد گردید. اینترنت بی‌سیم که تحت نام WiFi نیز شناخته می‌شود، یک تکنولوژی شبکه پرسرعت است که بطور وسیعی در خانه‌ها، مدارس، کافه‌ها، هتل‌ها و سایر مکآن‌های عمومی مانند کنگره‌ها و فرودگاه‌ها مورد استفاده قرار می‌گیرد. WiFi امکان دسترسی به اینترنت، بدون نیاز به کابل یا سیم را برای وسایلی مانند کامپیوترهای کیفی (Laptop)، کامپیوترهای جیبی (PDA) و کامپیوترهای شخصی (PC) دارای کارت Wireless فراهم می‌کند. بدین ترتیب مسافر بدون آنکه مجبور به اتصال کامپیوتر خود به خط تلفن یا شبکهٔ اتاق خود باشد، می‌تواند در محل هتل با آسودگی از اینترنت استفاده نماید.

امروزه، حدود ۹۸٪ از لپ‌تاب‌های جدید با توانایی کارکردن بصورت بی‌سیم به بازار ارائه می‌شوند. تمام محصولات جدید لپ‌تاب‌های اپل (Apple) هم با امکانات بی‌سیم و هم بلوتوث ساخته شده در درونشان به بازار عرضه می‌شوند. بسیاری از لپ‌تاب‌های با سیستم عامل ویندوز مایکروسافت بطور مشابه با توانایی کار کردن بصورت بی‌سیم می‌باشند.

انواع شبکه‌های بی‌سیم

WLANS (Wireless Local Area Networks)



این نوع شبکه برای کاربران محلی از جمله محیطهای (Campus) دانشگاهی یا آزمایشگاه‌ها که نیاز به استفاده از اینترنت دارند مفید می‌باشد. در این حالت اگر تعداد کاربران محدود باشند می‌توان بدون استفاده از Access Point این ارتباط را برقرار نمود.در غیر اینصورت استفاده از Access Point ضروری است.می توان با استفاده از آنتن‌های مناسب مسافت ارتباطی کاربران را به شرط عدم وجود مانع تاحدی طولانی‌تر نمود.

WPANS (Wireless Personal Area Networks)

دو تکنولوژی مورد استفاده برای این شبکه‌ها عبارت از: IR (Infra Red) و Bluetooth (IEEE 802.15) می‌باشد که مجوز ارتباط در محیطی حدود ۹۰ متر را می‌دهد؛ البته در IR نیاز به ارتباط مستقیم بوده و محدودیت مسافت وجود دارد.

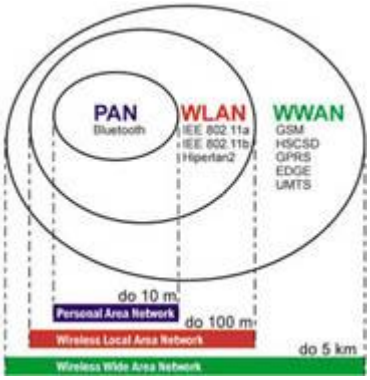
WMANS (Wireless Metropolitan Area Networks)

توسط این تکنولوژی ارتباط بین چندین شبکه یا ساختمان در یک شهر برقرار می‌شود برای Backup آن می‌توان از خطوط اجاره‌ای، فیبر نوری یا کابلهای مسی استفاده نمود.

WWANS (Wireless Wide Area Networks)

برای شبکه‌هائی با فواصل زیاد همچون بین شهرها یا کشورها بکار می‌رود این ارتباط از طریق آنتن‌ها ی بی‌سیم یا ماهواره صورت می‌پذیرد.

جدول و شکل زیر کاربرد انواع شبکه‌های بی‌سیم در فواصل متفاوت را نشان می‌دهد:



Network	Meters
Personal Area Network	0-10
Local Area Network	0-100
Wide Area Network	0-10000

۹-۱-۵- کاربردها، مزایا و ابعاد

تکنولوژی شبکه‌های بی‌سیم، با استفاده از انتقال داده‌ها توسط امواج رادیویی، در ساده‌ترین صورت، به تجهیزات سخت‌افزاری امکان می‌دهد تا بدون‌استفاده از بسترهای فیزیکی همچون سیم و کابل، با یکدیگر ارتباط برقرار کنند. شبکه‌های بی‌سیم بازه‌ی وسیعی از کاربردها، از ساختارهای پیچیده‌یی چون شبکه‌های بی‌سیم سلولی -که اغلب برای تلفن‌های همراه استفاده می‌شود- و شبکه‌های محلی بی‌سیم (WLAN – Wireless LAN) گرفته تا انوع ساده‌یی چون هدفون‌های بی‌سیم، را شامل می‌شوند. از سوی دیگر با احتساب امواجی همچون مادون قرمز، تمامی تجهیزاتی که از امواج مادون قرمز نیز استفاده می‌کنند، مانند صفحه کلیدها، ماوس‌ها و برخی از گوشی‌های همراه، در این دسته‌بندی جای می‌گیرند. طبیعی‌ترین مزیت استفاده از این شبکه‌ها عدم نیاز به ساختار فیزیکی و امکان نقل و انتقال تجهیزات متصل به این‌گونه شبکه‌ها و هم‌چنین امکان ایجاد تغییر در ساختار مجازی آن‌هاست. از نظر ابعاد ساختاری، شبکه‌های بی‌سیم به سه دسته تقسیم می‌گردند: WWAN، WLAN و WPAN.

مقصود از WWAN، که مخفف Wireless WAN است، شبکه‌هایی با پوشش بی‌سیم بالاست. نمونه‌یی از این شبکه‌ها، ساختار بی‌سیم سلولی مورد استفاده در شبکه‌های تلفن همراه است. WLAN پوششی محدودتر، در حد یک ساختمان یا سازمان، و در ابعاد کوچک یک سالن یا تعدادی اتاق، را فراهم می‌کند. کاربرد شبکه‌های WPAN یا Wireless Personal Area Network برای موارد خانه‌گی است. ارتباطاتی چون Bluetooth و مادون قرمز در این دسته قرار می‌گیرند.

شبکه‌های WPAN از سوی دیگر در دسته‌ی شبکه‌های Ad hoc نیز قرار می‌گیرند. در شبکه‌های Ad hoc، یک سخت‌افزار، به‌محض ورود به فضای تحت پوشش آن، به‌صورت پویا به شبکه اضافه می‌شود. مثالی از این نوع شبکه‌ها، Bluetooth است. در این نوع، تجهیزات مختلفی از جمله صفحه کلید، ماوس، چاپگر، کامپیوتر کیفی یا جیبی و حتی گوشی تلفن همراه، در صورت قرارگرفتن در محیط تحت پوشش، وارد شبکه شده و امکان رد و بدل داده‌ها با دیگر تجهیزات متصل به شبکه را می‌یابند. تفاوت میان شبکه‌های Ad hoc با شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌هاست. به‌عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستاست درحالی‌که شبکه‌های Ad hoc از هر نظر پویا هستند. طبیعی‌ست که در کنار مزایایی که این پویایی برای استفاده کننده‌گان فراهم می‌کند، حفظ امنیت چنین شبکه‌هایی

نیز با مشکلات بسیاری همراه است. با این وجود، عملاً یکی از راه حل‌های موجود برای افزایش امنیت در این شبکه‌ها، خصوصاً در انواعی همچون Bluetooth، کاستن از شعاع پوشش سیگنال‌های شبکه است. در واقع مستقل از این حقیقت که عملکرد Bluetooth بر اساس فرستنده و گیرندههای کم‌توان استوار است و این مزیت در کامپیوترهای جیبی برتری قابل‌توجه‌یی محسوب می‌گردد، همین کمی توان سخت‌افزار مربوطه، موجب وجود منطقه‌ی محدود تحت پوشش است که در بررسی امنیتی نیز مزیت محسوب می‌گردد. به‌عبارت دیگر این مزیت به‌همراه استفاده از کدهای رمز نه‌چندان پیچیده، تنها حربه‌های امنیتی این دسته از شبکه‌ها به‌حساب می‌آیند.

۹-۱-۶- روش‌های ارتباطی بی‌سیم

تجهیزات و شبکه‌های کامپیوتری بی‌سیم بر دو قسم Indoor یا درون سازمانی و Outdoor یا برون سازمانی تولید شده و مورد استفاده قرار می‌گیرند.

۱- شبکه‌های بی‌سیم Indoor

نیاز سازمان‌ها و شرکت‌ها برای داشتن شبکه‌ای مطمئن و وجود محدودیت در کابل کشی، متخصصین را تشویق به پیدا کردن جایگزین برای شبکه کامپیوتری کرده است. شبکه‌های Indoor به شبکه‌هایی اتلاق می‌شود که در داخل ساختمان ایجاد شده باشد. این شبکه‌ها بر دو گونه طراحی می‌شوند. شبکه‌های Ad hoc و شبکه‌های Infra Structure . در شبکه‌های Ad hoc دستگاه متمرکز کننده مرکزی وجود ندارد و کامپیوترهای دارای کارت شبکه بی‌سیم هستند. استراتژی Ad hoc برای شبکه‌های کوچک با تعداد ایستگاه کاری محدود قابل استفاده است. روش و استراتژی دوم جهت پیاده سازی استاندارد شبکه بی‌سیم، شبکه Infra Structure می‌باشد. در این روش یک یا چند دستگاه متمرکز کننده به نام Access Point مسؤولیت برقراری ارتباط را برعهده دارد.

۲- شبکه‌های بی‌سیم Outdoor

برقراری ارتباط بی‌سیم در خارج ساختمان به شبکه بی‌سیم Outdoor شهرت دارد. در این روش داشتن دید مستقیم یا Line Of Sight، ارتفاء دو نقطه و فاصله، معیارهایی برای انتخاب نوع Access Point و آنتن هستند.

انواع ارتباط

شبکه بی‌سیم Outdoor با سه توپولوژی Point To Point، Point To Multipoint و Mesh قابل پیاده سازی می‌باشد.

۲-۱- Point To point

در این روش ارتباط دو نقطه مدنظر می‌باشد. در هر یک از قسمت‌ها آنتن و AccessPoint نصب شده و ارتباط این دو قسمت برقرار می‌شود.

۲-۲- Point To Multi Point

در این روش یک نقطه به عنوان مرکز شبکه درنظر گرفته می‌شود و سایر نقاط به این نقطه در ارتباط هستند.

۲-۳- Mesh

ارتباط بی‌سیم چندین نقطه بصورت‌های مختلف را توپولوژی Mesh می‌گویند. در این روش ممکن است چندین نقطه مرکزی وجود داشته باشد که با یکدیگر در ارتباط هستند.

ارتباط بی‌سیم بین دو نقطه به عوامل زیر بستگی دارد

۱- توان خروجی Access Point (ارسال اطلاعات)

۲- میزان حساسیت Access Point (دریافت اطلاعات)

۳- توان آنتن

۱- توان خروجی Access Point

یکی از مشخصه‌های طراحی سیستم‌های ارتباطی بی‌سیم توان خروجی Access Point می‌باشد. هرچقدر این توان بیشتر باشد قدرت سیگنال‌های توایدی و برد آن افزایش می‌یابد.

۲- میزان حساسیت Access Point

از مشخصه‌های تعیین کننده در کیفیت دریافت امواج تولید شده توسط Access Point نقطه مقابل میزان حساسیت Access Point می‌باشد. هرچقدر این حساسیت افزایش یابد احتمال عدم دریافت سیگنال کمتر می‌باشد و آن تضمین کننده ارتباط مطمئن و مؤثر خواهد بود.

۳- توان آنتن

در مورد هر آنتن توان خروجی آنتن و زاویه پوشش یا انتشار مشخصه‌های حائز اهمیت می‌باشند در این راستا آنتن‌های مختلفی با مشخصه‌های مختلف توان و زاویه انتشار بوجود آمده است که آنتن‌های Omni، Sectoral ، Parabolic ، Panel، Solied و.... مثال‌هایی از آن هستند

۹-۱-۷- عناصر فعال شبکه‌های محلی بی‌سیم

در شبکه‌های محلی بی‌سیم معمولاً دو نوع عنصر فعال وجود دارد:

۱- ایستگاه بی‌سیم

ایستگاه یا مخدوم بی‌سیم به طور معمول یک کامپیوتر کیفی یا یک ایستگاه کاری ثابت است که توسط یک کارت شبکه‌ی بی‌سیم به شبکه‌ی محلی متصل می‌شود. این ایستگاه می‌تواند از سوی دیگر یک کامپیوتر جیبی یا حتی یک پویش گر بارکد نیز باشد. در برخی از کاربردها برای این‌که استفاده از سیم در پایانه‌های رایانه‌یی برای طراح و مجری دردسرساز است، برای این پایانه‌ها که معمولاً در داخل کیوسک‌هایی به‌همین منظور تعبیه می‌شود، از امکان اتصال بی‌سیم به شبکه‌ی محلی استفاده می‌کنند. در حال حاضر اکثر کامپیوترهای کیفی موجود در بازار به این امکان به‌صورت سرخود مجهز هستند و نیازی به اضافه‌کردن یک کارت شبکه‌ی بی‌سیم نیست.

کارت‌های شبکه‌ی بی‌سیم عموماً برای استفاده در چاک‌های PCMCIA است. در صورت نیاز به استفاده از این کارت‌ها برای کامپیوترهای رومیزی و شخصی، با استفاده از رابطی این کارت‌ها را بر روی چاک‌های گسترش PCI نصب می‌کنند.

۲- نقطه ی دسترسی (Access Point)

نقاط دسترسی در شبکه‌های بی‌سیم، همان‌گونه که در قسمت‌های پیش نیز در مورد آن صحبت شد، سخت‌افزارهای فعالی هستند که عملاً نقش سوییچ در شبکه‌های بی‌سیم را بازی‌کرده، امکان اتصال به شبکه‌های سیمی را نیز دارند. در عمل ساختار بستر اصلی شبکه عموماً سیمی است و توسط این نقاط دسترسی، مخدوم‌ها و ایستگاه‌های بی‌سیم به شبکه‌ی سیمی اصلی متصل می‌گردد.

۹-۱-۸- برد و سطح پوشش

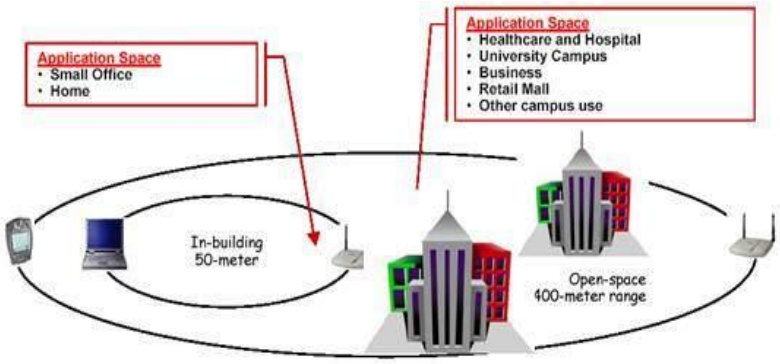
شعاع پوشش شبکه‌ی بی‌سیم بر اساس استاندارد 802.11 به فاکتورهای بسیاری بستگی دارد که برخی از آن‌ها به شرح زیر هستند:

- پهنای باند مورد استفاده
- منابع امواج ارسالی و محل قرارگیری فرستنده‌ها و گیرنده‌ها
- مشخصات فضای قرارگیری و نصب تجهیزات شبکه‌ی بی‌سیم
- قدرت امواج
- نوع و مدل آنتن

شعاع پوشش از نظر تئوری بین ۲۹ متر (برای فضاهای بسته‌ی داخلی) و ۴۸۵ متر (برای فضاهای باز) در استاندارد 802.11b متغیر است. با این‌وجود این مقادیر، مقادیری متوسط هستند و در حال حاضر با توجه به گیرنده‌ها و فرستنده‌های نسبتاً قدرت‌مندی که مورد استفاده قرار می‌گیرند، امکان استفاده از این پروتکل و گیرنده‌ها و فرستنده‌های آن، تا چند کیلومتر هم وجود دارد که نمونه‌های عملی آن فراوان‌اند.

با این وجود شعاع کلی‌یی که برای استفاده از این پروتکل (802.11b) ذکر می‌شود چیزی میان ۵۰ تا ۱۰۰متر است. این شعاع عمل‌کرد مقداری‌ست که برای محل‌های بسته و ساختمان‌های چند طبقه نیز معتبر بوده و می‌تواند مورد استناد قرار گیرد.

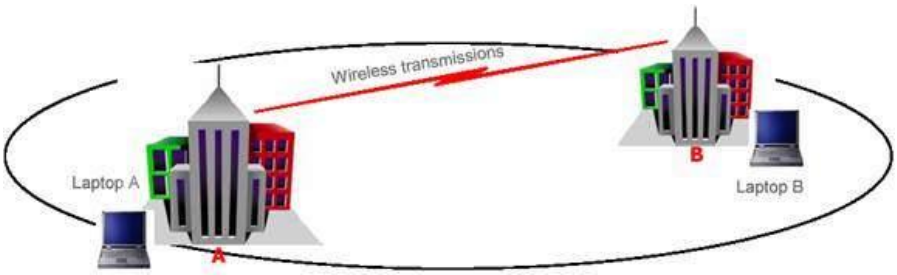
شکل زیر مقایسه‌یی میان بردهای نمونه در کاربردهای مختلف شبکه‌های بی‌سیم مبتنی بر پروتکل 802.11b را نشان می‌دهد:



یکی از عمل‌کردهای نقاط دسترسی به عنوان سوییچ‌های بی‌سیم، عمل اتصال میان حوزه‌های بی‌سیم است. به‌عبارت دیگر با استفاده از چند سوییچ بی‌سیم می‌توان عمل‌کردی مشابه Bridge برای شبکه‌های بی‌سیم را به‌دست آورد.

اتصال میان نقاط دست‌رسی می‌تواند به صورت نقطه‌به‌نقطه، برای ایجاد اتصال میان دو زیرشبکه به یکدیگر، یا به صورت نقطه‌یی به چند نقطه یا بالعکس برای ایجاد اتصال میان زیرشبکه‌های مختلف به یکدیگر به‌صورت همزمان صورت گیرد.

نقاط دسترسی‌یی که به عنوان پل ارتباطی میان شبکه‌های محلی با یکدیگر استفاده می‌شوند از قدرت بالاتری برای ارسال داده استفاده می‌کنند و این به‌معنای شعاع پوشش بالاتر است. این سخت‌افزارها معمولاً برای ایجاد اتصال میان نقاط و ساختمآن‌هایی به‌کار می‌روند که فاصله‌ی آن‌ها از یکدیگر بین ۱ تا ۵ کیلومتر است. البته باید توجه داشت که این فاصله، فاصله‌یی متوسط بر اساس پروتکل 802.11b است. برای پروتکل‌های دیگری چون 802.11a می‌توان فواصل بیشتری را نیز به‌دست آورد. شکل زیر نمونه‌یی از ارتباط نقطه به نقطه با استفاده از نقاط دست‌رسی مناسب را نشان می‌دهد:



از دیگر استفادههای نقاط دسترسی با برد بالا می‌توان به امکان توسعه‌ی شعاع پوشش شبکه‌های بی‌سیم اشاره کرد. به عبارت دیگر برای بالابردن سطح تحت پوشش یک شبکه‌ی بی‌سیم، می‌توان از چند نقطه‌ی دست‌رسی بی‌سیم به‌صورت همزمان و پشت به پشت یکدیگر استفاده کرد. به عنوان نمونه در مثال بالا می‌توان با استفاده از یک فرستنده‌ی دیگر در بالای هریک از ساختمآن‌ها، سطح پوشش شبکه را تا ساختمآن‌های دیگر گسترش داد.

۹-۱-۹- معماری شبکه‌های محلی بی‌سیم

معماری ۸۰۲.۱۱ از عناصر ساختمانی متعددی تشکیل شده است که در کنار هم، سـّیار بودن ایستگاه‌های کاری را پنهان از دید لایه‌های فوقانی برآورده می‌سازد. ایستگاه بی‌سیم یا به اختصار ایستگاه (STA)، بنیادی‌ترین عنصر ساختمانی در یک شبکه محلی بی‌سیم است. یک ایستگاه، دستگاهی است که بر اساس تعاریف و پروتکل‌های ۸۰۲.۱۱ (لایه‌های MAC و PHY) عمل کرده و به رسانه بی‌سیم متصل است. توجه داشته باشید که براساس تعریف کلاسیکِ شبکه‌های کامپیوتری، یک شبکه کامپیوتری مجموعه‌ای از کامپیوترهای **مستقل** و **متصل** است که منظور از اتصال در این تعریف، توانایی جابجایی و مبادله پیام‌ها است. ایستگاه‌های کاری بی‌سیم امروزی عمدتاً به صورت مجموعه سخت‌افزاری/نرم‌افزاری کارت‌های شبکه بی‌سیم پیاده‌سازی می‌شوند. همچنین یک ایستگاه می‌تواند یک کامپیوتر قابل حمل، کامپیوتر کفدستی و یا یک نقطه دسترسی باشد. نقطه دسترسی در واقع در حکم پلی است که ارتباط ایستگاه‌های بی‌سیم را با سیستم توزیع یا شبکه سیمی برقرار می‌سازد. کوچکترین عنصر ساختمانی شبکه‌های محلی بی‌سیم در استاندارد ۸۰۲.۱۱ *مجموعه سرویس پایه* یا BSS نامیده می‌شود. در واقع BSS مجموعه‌ای از ایستگاه‌های بی‌سیم است.

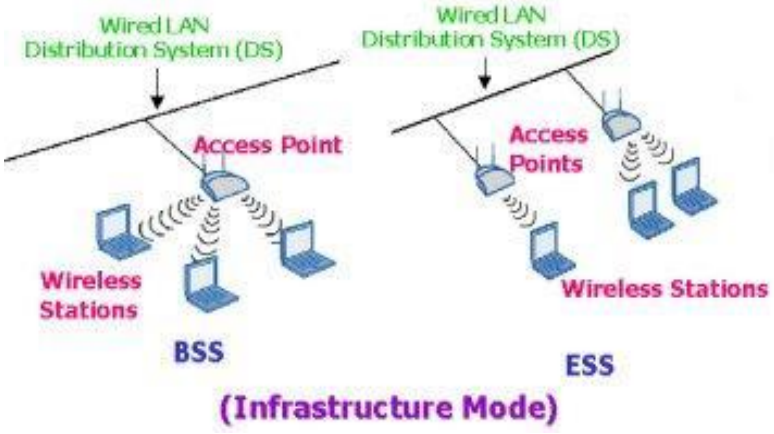
همبندی‌های ۸۰۲.۱۱

در یک تقسیم بندی کلی می‌توان دو همبندی را برای شبکه‌های محلی بی‌سیم در نظر گرفت. ساده‌ترین همبندی، **فی‌البداهه** (Ad hoc) و براساس فرهنگ واژگان استاندارد ۸۰۲.۱۱، IBSS است. در این همبندی ایستگاه‌ها از طریق رسانه بی‌سیم به صورت نظیر به نظیر با یکدیگر در ارتباط هستند و برای تبادل داده (تبادل پیام) از تجهیزات یا ایستگاه واسطی استفاده

نمی‌کنند. واضح است که در این همبندی به سبب محدودیت‌های فاصله هر ایستگاهی ضرورتاً نمی‌تواند با تمام ایستگاه‌های دیگر در تماس باشد. به این ترتیب شرط اتصال مستقیم در همبندی IBSS آن است که ایستگاه‌ها در محدوده عملیاتی بی‌سیم یا همان بُرد شبکه بی‌سیم قرار داشته باشند. شکل زیر همبندی IBSS را نشان می‌دهد.



همبندی دیگر زیرساختار (Infrastructure) است. در این همبندی عنصر خاصی موسوم به نقطه دسترسی وجود دارد. نقطه دسترسی ایستگاه‌های موجود در یک مجموعه سرویس را به سیستم توزیع متصل می‌کند. در این همبندی تمام ایستگاه‌ها با نقطه دسترسی تماس می‌گیرند و اتصال مستقیم بین ایستگاه‌ها وجود ندارد در واقع نقطه‌دسترسی وظیفه دارد فریم‌ها (قاب‌های داده) را بین ایستگاه‌ها توزیع و پخش کند. شکل زیر همبندی زیرساختار را نشان می‌دهد.



در این همبندی سیستم توزیع، رسآن‌های است که از طریق آن نقطه دسترسی (AP) با سایر نقاط دسترسی در تماس است و از طریق آن می‌تواند فریم‌ها را به سایر ایستگاه‌ها ارسال نماید. از سوی دیگر می‌تواند بسته‌ها را در اختیار ایستگاه‌های متصل به شبکه سیمی نیز قراردهد. در استاندارد ۸۰۲.۱۱ توصیف ویژه‌ای برای سیستم توزیع ارائه نشده است، لذا محدودیتی برای پیاده سازی سیستم توزیع وجود ندارد، در واقع این استاندارد تنها خدماتی را معین می‌کند که سیستم توزیع می‌بایست ارائه نماید. بنابراین سیستم توزیع می‌تواند یک شبکه ۸۰۲.۳ معمولی و یا دستگاه خاصی باشد که سرویس توزیع مورد نظر را فراهم می‌کند.

استاندارد ۸۰۲.۱۱ با استفاده از همبندی خاصی محدوده عملیاتی شبکه را گسترش می‌دهد. این همبندی به شکل *مجموعه سرویس گسترش یافته* (ESS) بر پا می‌شود. در این روش یک مجموعه گسترده و متشکل از چندین BSS یا *مجموعه سرویس پایه* از طریق نقاط دسترسی با یکدیگر در تماس هستند و به این ترتیب ترافیک داده بین مجموعه‌های سرویس پایه

مبادله شده و انتقال پیام‌ها شکل می‌گیرد. در این همبندی ایستگاه‌ها می‌توانند در محدوده عملیاتی بزرگ‌تری گردش نمایند. ارتباط بین نقاط دسترسی از طریق سیستم توزیع فراهم می‌شود. در واقع سیستم توزیع ستون فقرات شبکه‌های محلی بی‌سیم است و می‌تواند با استفاده از فنّاوری بی‌سیم یا شبکه‌های سیمی شکل گیرد. سیستم توزیع در هر نقطه دسترسی به عنوان یک لایه عملیاتی ساده است که وظیفه آن تعیین گیرنده پیام و انتقال فریم به مقصدش می‌باشد. نکته قابل توجه در این همبندی آن است که تجهیزات شبکه خارج از حوزه ESS تمام ایستگاه‌های سیّار داخل ESS را صرفنظر از پویایی و تحرکشان به صورت یک شبکه منفرد در سطح لایه MAC تلقی می‌کنند. به این ترتیب پروتکل‌های رایج شبکه‌های کامپیوتری کوچکترین تأثیری از سیّار بودن ایستگاه‌ها و رسانه بی‌سیم نمی‌پذیرند. جدول زیر همبندی‌های رایج در شبکه‌های بی‌سیم مبتنی بر ۸۰۲.۱۱ را به اختصار جمع بندی می‌کند.

802.11 Topologies		
Independent Basic Service Set (IBSS) ("Ad hoc" or "Peer to Peer")	**Infrastructure**	
	Basic Service Set (BSS)	Extended Service Set (ESS)

خدمات ایستگاهی

بر اساس این استاندارد خدمات خاصی در ایستگاه‌های کاری پیاده‌سازی می‌شوند. در حقیقت تمام ایستگاه‌های کاری موجود در یک شبکه محلی مبتنی بر ۸۰۲.۱۱ و نیز نقاط دسترسی موظف هستند که خدمات ایستگاهی را فراهم نمایند. با توجه به اینکه امنیت فیزیکی به منظور جلوگیری از دسترسی غیر مجاز بر خلاف شبکه‌های سیمی، در شبکه‌های بی‌سیم قابل اعمال نیست استاندارد ۸۰۲.۱۱ خدمات هویت سنجی را به منظور کنترل دسترسی به شبکه تعریف می‌نماید. سرویس هویت سنجی به ایستگاه کاری امکان می‌دهد که ایستگاه دیگری را شناسایی نماید. قبل از اثبات هویت ایستگاه کاری، آن ایستگاه مجاز نیست که از شبکه بی‌سیم برای تبادل داده استفاده نماید. در یک تقسیم بندی کلی ۸۰۲.۱۱ دو گونه خدمت هویت سنجی را تعریف می‌کند:

- Open System Authentication
- Shared Key Authentication

روش اول، متد پیش فرض است و یک فرآیند دو مرحله‌ای است. در ابتدا ایستگاهی که می‌خواهد توسط ایستگاه دیگر شناسایی و هویت سنجی شود یک فریم مدیریتی هویت سنجی شامل شناسه ایستگاه فرستنده، ارسال می‌کند. ایستگاه گیرنده نیز فریمی در پاسخ می‌فرستد که آیا فرستنده را می‌شناسد یا خیر. روش دوم کمی پیچیده‌تر است و فرض می‌کند که هر ایستگاه از طریق یک کانال مستقل و امن، یک کلید مشترک سّری دریافت کرده است. ایستگاه‌های کاری با استفاده از این کلید مشترک و با بهره‌گیری از پروتکلی موسوم به WEP اقدام به هویت سنجی یکدیگر می‌نمایند. یکی دیگر از خدمات ایستگاهی خاتمه ارتباط یا خاتمه هویت سنجی است. با استفاده از این خدمت، دسترسی ایستگاهی که سابقاً مجاز به استفاده از شبکه بوده است، قطع می‌گردد.

در یک شبکه بی‌سیم، تمام ایستگاه‌های کاری و سایر تجهیزات قادر هستند ترافیک داده‌ای را "بشنوند" – در واقع ترافیک در بستر امواج مبادله می‌شود که توسط تمام ایستگاه‌های کاری قابل دریافت است. این ویژگی سطح امنیتی یک ارتباط بی‌سیم

را تحت تأثیر قرار می‌دهد. به همین دلیل در استاندارد ۸۰۲.۱۱ پروتکلی موسوم به WEP تعبیه شده است که برروی تمام فریم‌های داده و برخی فریم‌های مدیریتی و هویت سنجی اعمال می‌شود. این استاندارد در پی آن است تا با استفاده از این الگوریتم سطح اختفاء وپوشش را معادل با شبکه‌های سیمی نماید.

خدمات توزیع

خدمات توزیع عملکرد لازم در همبندی‌های مبتنی بر سیستم توزیع را مهیا می‌سازد. معمولاً خدمات توزیع توسط نقطه دسترسی فراهم می‌شوند. خدمات توزیع در این استاندارد عبارتند از:

پیوستن به شبکه، خروج از شبکه بی‌سیم، پیوستن مجدد، توزیع، مجتمع سازی

سرویس اول یک ارتباط منطقی میان ایستگاه سیار و نقطه دسترسی فراهم می‌کند. هر ایستگاه کاری قبل از ارسال داده می‌بایست با یک نقطه دسترسی برروی سیستم میزبان مرتبط گردد. این عضویت، به سیستم توزیع امکان می‌دهد که فریم‌های ارسال شده به سمت ایستگاه سیار را به درستی در اختیارش قرار دهد. خروج از شبکه بی‌سیم هنگامی بکار می‌رود که بخواهیم اجباراً ارتباط ایستگاه سیار را از نقطه دسترسی قطع کنیم و یا هنگامی که ایستگاه سیار بخواهد خاتمه نیازش به نقطه دسترسی را اعلام کند. سرویس پیوستن مجدد هنگامی مورد نیاز است که ایستگاه سیار بخواهد با نقطه دسترسی دیگری تماس بگیرد. این سرویس مشابه "پیوستن به شبکه بی‌سیم" است با این تفاوت که در این سرویس ایستگاه سیار نقطه دسترسی قبلی خود را به نقطه دسترسی جدیدی اعلام می‌کند که قصد دارد به آن متصل شود. پیوستن مجدد با توجه به تحرک و سیار بودن ایستگاه کاری امری ضروری و اجتناب ناپذیر است. این اطلاع، (اعلام نقطه دسترسی قبلی) به نقطه دسترسی جدید کمک می‌کند که با نقطه دسترسی قبلی تماس گرفته و فریم‌های بافر شده احتمالی را دریافت کند که به مقصد این ایستگاه سیار فرستاده شده‌اند. با استفاده از سرویس توزیع فریم‌های لایه MAC به مقصد مورد نظرشان می‌رسند. مجتمع سازی سرویسی است که شبکه محلی بی‌سیم را به سایر شبکه‌های محلی و یا یک یا چند شبکه محلی بی‌سیم دیگر متصل می‌کند. سرویس مجتمع سازی فریم‌های ۸۰۲.۱۱ را به فریم‌هایی ترجمه می‌کند که بتوانند در سایر شبکه‌ها (به عنوان مثال ۸۰۲.۳) جاری شوند. این عمل ترجمه دو طرفه است بدان معنی که فریم‌های سایر شبکه‌ها نیز به فریم‌های ۸۰۲.۱۱ ترجمه شده و از طریق امواج در اختیار ایستگاه‌های کاری سیار قرار می‌گیرند.

دسترسی به رسانه

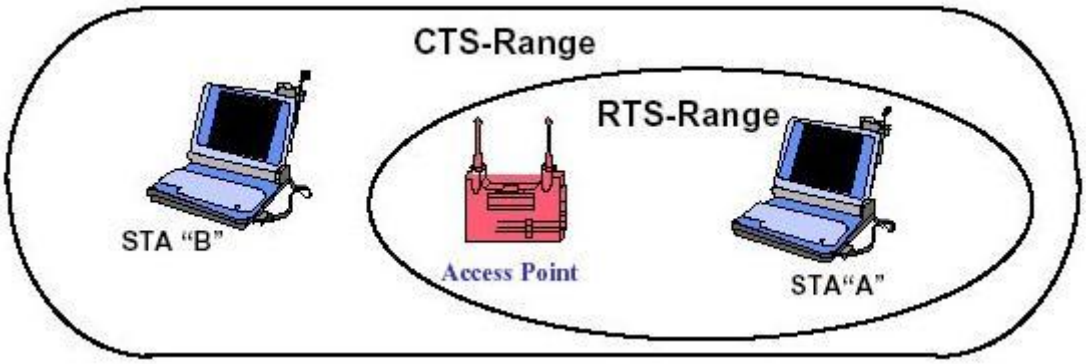
روش دسترسی به رسانه در این استاندارد CSMA/CA است که تاحدودی به روش دسترسی CSMA/CD شباهت دارد. در این روش ایستگاه‌های کاری قبل از ارسال داده کانال رادیویی را کنترل می‌کنند و در صورتی که کانال آزاد باشد اقدام به ارسال می‌کنند. در صورتی که کانال رادیویی اشغال باشد با استفاده از الگوریتم خاصی به اندازه یک زمان تصادفی صبر کرده و مجدداً اقدام به کنترل کانال رادیویی می‌کنند. در روش CSMA/CA ایستگاه فرستنده ابتدا کانال فرکانسی را کنترل کرده و در صورتی که رسانه به مدت خاصی موسوم به DIFS آزاد باشد اقدام به ارسال می‌کند. گیرنده فیلد کنترلی فریم یا همان CRC را چک می‌کند و سپس یک فریم تصدیق می‌فرستد. دریافت تصدیق به این معنی است که تصادمی بروز نکرده است. در صورتی که فرستنده این تصدیق را دریافت نکند، مجدداً فریم را ارسال می‌کند. این عمل تا زمانی ادامه می‌یابد که فریم

تصدیق ارسالی از گیرنده توسط فرستنده دریافت شود یا تکرار ارسال فریم‌ها به تعداد آستآن‌های مشخصی برسد که پس از آن فرستنده فریم را دور می‌اندازد.

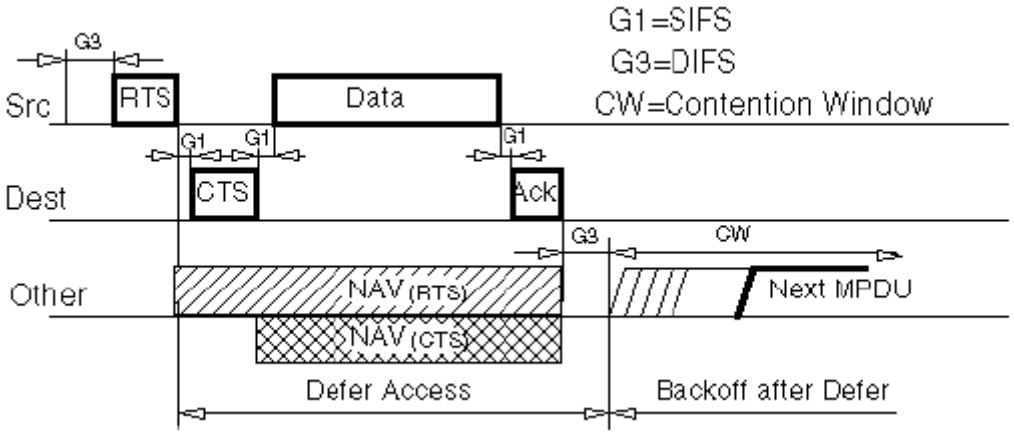
در شبکه‌های بی‌سیم بر خلاف اترنت امکان شناسایی و آشکار سازی تصادم به دو علت وجود ندارد:

۱. پیاده سازی مکانیزم آشکار سازی تصادم به روش ارسال رادیویی دوطرفه نیاز دارد که با استفاده از آن ایستگاه سیار بتواند در حین ارسال، سیگنال را دریافت کند که این امر باعث افزایش قابل توجه هزینه می‌شود.

۲. در یک شبکه بی‌سیم، بر خلاف شبکه‌های سیمی، نمی‌توان فرض کرد که تمام ایستگاه‌های سیار امواج یکدیگر را دریافت می‌کنند. در واقع در محیط بی‌سیم حالاتی قابل تصور است که به آن‌ها *نقاط پنهان* می‌گوییم. در شکل زیر ایستگاه‌های کاری "A" و "B" هر دو در محدوده تحت پوشش نقطه دسترسی هستند ولی در محدوده یکدیگر قرار ندارند.



برای غلبه بر این مشکل، استاندارد ۸۰۲.۱۱ از تکنیکی موسوم به *اجتناب از تصادم* و مکانیزم تصدیق استفاده می‌کند. همچنین با توجه به احتمال بروز روزنه‌های پنهان و نیز به منظور کاهش احتمال تصادم در این استاندارد از روشی موسوم به *شنود مجازی رسانه* یا VCS استفاده می‌شود. در این روش ایستگاه فرستنده ابتدا یک بسته کنترلی موسوم به تقاضای ارسال حاوی نشانی فرستنده، نشانی گیرنده، و زمان مورد نیاز برای اشغال کانال رادیویی را می‌فرستد. هنگامی که گیرنده این فریم را دریافت می‌کند، رسانه را کنترل می‌کند و در صورتی که رسانه آزاد باشد فریم کنترلی CTS را به نشانی فرستنده ارسال می‌کند. تمام ایستگاه‌هایی که فریم‌های کنترلی RTS/CTS را دریافت می‌کنند وضعیت کنترل رسانه خود موسوم به شاخص NAV را تنظیم می‌کنند. در صورتی که سایر ایستگاه‌ها بخواهند فریمی را ارسال کنند علاوه بر کنترل فیزیکی رسانه (کانال رادیویی) به پارامتر NAV خود مراجعه می‌کنند که مرتباً به صورت پویا تغییر می‌کند. به این ترتیب مشکل روزنه‌های پنهان حل شده و تصادم‌ها نیز به حداقل مقدار می‌رسند. شکل زیر زمان‌بندی RTS/CTS و وضعیت سایر ایستگاه‌ها را نشان می‌دهد.



لایه فیزیکی

در این استاندارد لایه فیزیکی سه عملکرد مشخص را انجام می‌دهد. اول آنکه رابطی برای تبادل فریم‌های لایه MAC جهت ارسال و دریافت داده‌ها فراهم می‌کند. دوم اینکه با استفاده از روش‌های تسهیم فریم‌های داده را ارسال می‌کند و در نهایت وضعیت رسانه (کانال رادیویی) را در اختیار لایه بالاتر (MAC) قرار می‌دهد.

سه تکنیک رادیویی مورد استفاده در لایه فیزیکی این استاندارد به شرح زیر می‌باشند:

- استفاده از تکنیک رادیویی DSSS
- استفاده از تکنیک رادیویی FHSS
- استفاده از امواج رادیویی مادون قرمز

در این استاندار لایه فیزیکی می‌تواند از امواج مادون قرمز نیز استفاده کند. در روش ارسال با استفاده از امواج مادون قرمز، اطلاعات باینری با نرخ ۱ یا ۲ مگابیت در ثانیه و به ترتیب با استفاده از مدولاسیون PPM-۱۶ و PPM-٤مبادله می‌شوند.

ویژگی‌های سیگنال‌های طیف گسترده

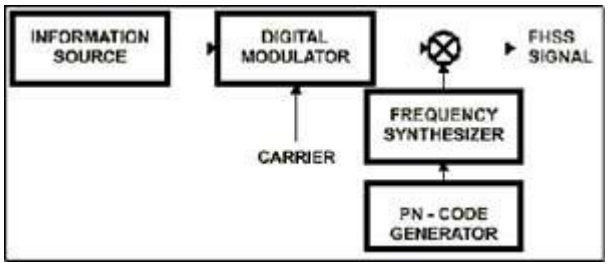
عبارت طیف گسترده به هر تکنیکی اطلاق می‌شود که با استفاده از آن پهنای باند سیگنال ارسالی بسیار بزرگ‌تر از پهنای باند سیگنال اطلاعات باشد. یکی از سوالات مهمی که با در نظر گرفتن این تکنیک مطرح می‌شود آن است که با توجه به نیاز روز افزون به پهنای باند و اهمیت آن به عنوان یک منبع با ارزش، چه دلیلی برای گسترش طیف سیگنال و مصرف پهنای باند بیشتر وجود دارد. پاسخ به این سوال در ویژگی‌های جالب توجه سیگنال‌های طیف گسترده نهفته است. این ویژگی‌های عبارتند از:

- پایین بودن توان چگالی طیف به طوری که سیگنال اطلاعات برای شنود غیر مجاز و نیز در مقایسه با سایر امواج به شکل اعوجاج و پارازیت به نظر می‌رسد.
- مصونیت بالا در مقابل پارازیت و تداخل
- رسایی با تفکیک پذیری و دقت بالا
- امکان استفاده در CDMA

مزایای فوق کمیسیون FCC را بر آن داشت که در سال ۱۹۸۵ مجوز استفاده از این سیگنال‌ها را با محدودیت حداکثر توان یک وات در محدوده ISM صادر نماید.

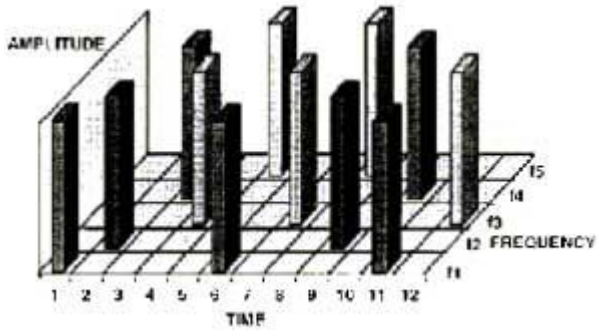
سیگنال‌های طیف گسترده با جهش فرکانسی

در یک سیستم مبتنی بر جهش فرکانسی، فرکانس سیگنال حامل به شکلی شبه تصادفی و تحت کنترل یک ترکیب کننده تغییر می‌کند. شکل زیر این تکنیک را در قالب یک نمودار نشان می‌دهد.



PN-CODE= Pseudonoise code

در این شکل سیگنال اطلاعات با استفاده از یک تسهیم کننده دیجیتال و با استفاده از روش تسهیم FSK تلفیق می‌شود. فرکانس سیگنال حامل نیز به شکل شبه تصادفی از محدوده فرکانسی بزرگ‌تری در مقایسه با سیگنال اطلاعات انتخاب می‌شود. با توجه به اینکه فرکانس‌های pn-code با استفاده از یک ثبات انتقالی همراه با پس خور ساخته می‌شوند، لذا دنباله فرکانسی تولید شده توسط آن کاملا تصادفی نیست و به همین خاطر به این دنباله، شبه تصادفی می‌گوییم.



بر اساسی مقررات FCC و سازمان‌های قانون گذاری، حداکثر زمان توقف در هر کانال فرکانسی ٤٠٠ میلی ثانیه است که برابر با حداقل ۲.۵ جهش فرکانسی در هر ثانیه خواهد بود. در استاندارد ۸۰۲.۱۱ حداقل فرکانس جهش در آمریکای شمالی و اروپا ٦ مگاهرتز و در ژاپن ۵ مگاهرتز می‌باشد.

سیگنال‌های طیف گسترده با توالی مستقیم

اصل حاکم بر توالی مستقیم، پخش یک سیگنال برروی یک باند فرکانسی بزرگتر از طریق تسهیم آن با یک امضاء یا کُد به گونه‌ای است که نویز و تداخل را به حداقل برساند. برای پخش کردن سیگنال هر بیت واحد با یک کُد تسهیم می‌شود. در گیرنده نیز سیگنال اولیه با استفاده از همان کد بازسازی می‌گردد. در استاندارد ۸۰۲.۱۱ روش مدولاسیون مورد استفاده در سیستم‌های DSSS روش تسهیم DPSK است. در این روش سیگنال اطلاعات به شکل تفاضلی تهسیم می‌شود. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد.

از آنجا که در استاندارد ۸۰۲.۱۱ و سیستم DSSS از روش تسهیم DPSK استفاده می‌شود، داده‌های خام به صورت تفاضلی تسهیم شده و ارسال می‌شوند و در گیرنده نیز یک آشکار ساز تفاضلی سیگنال‌های داده را دریافت می‌کند. در نتیجه نیازی به فاز مرجع برای بازسازی سیگنال وجود ندارد. در روش تسهیم PSK فاز سیگنال حامل با توجه به الگوی بیتی

سیگنال‌های داده تغییر می‌کند. به عنوان مثال در تکنیک QPSK دامنه سیگنال حامل ثابت است ولی فاز آن با توجه به بیت‌های داده تغییر می‌کند. جدول زیر ایده مدولاسیون فاز را نشان می‌دهد.

Symbols	Bits	Phase Modulation
1	00	$A\sin(\omega t+\theta_1)$
2	01	$A\sin(\omega t+\theta_2)$
3	10	$A\sin(\omega t+\theta_3)$
4	11	$A\sin(\omega t+\theta_4)$

در الگوی مدولاسیون QPSK چهار فاز مختلف مورد استفاده قرار می‌گیرند و چهار نماد را پدید می‌آورند. واضح است که در این روش تسهیم، دامنه سیگنال ثابت است. در روش تسهیم تفاضلی سیگنال اطلاعات با توجه به میزان اختلاف فاز و نه مقدار مطلق فاز تسهیم و مخابره می‌شوند. به عنوان مثال در روش pi/4-DQPSK، چهار مقدار تغییر فاز 3pi/4-، 3pi/4، pi/4، و pi/4- است. با توجه به اینکه در روش فوق چهار تغییر فاز به کار رفته است لذا هر نماد می‌تواند دو بیت را کُدگذاری نماید.

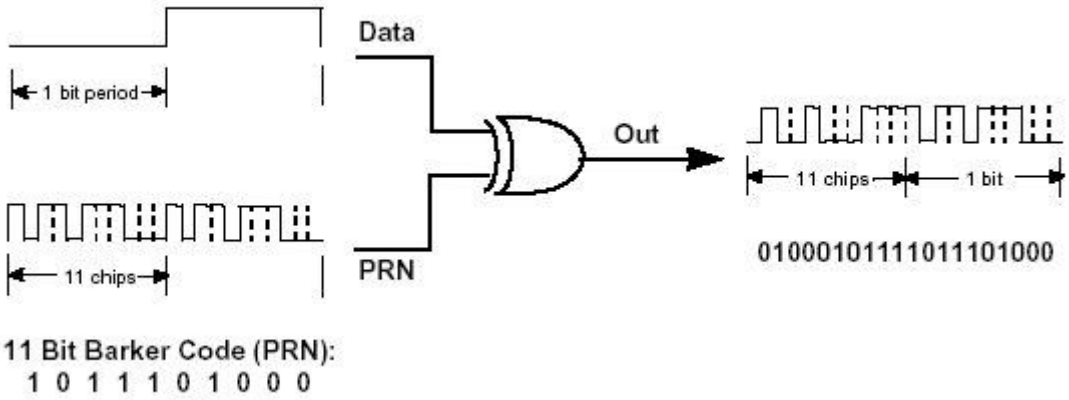
اختلاف فاز	بیتهای زوج	بیتهای فرد
-3pi/4	1	1
3 pi/4	1	0
Pi/4	0	0
-pi/4	0	1

در روش تسهیم طیف گسترده با توالی مستقیم مشابه تکنیک FH از یک کد شبه تصادفی برای پخش و گسترش سیگنال استفاده می‌شود. عبارت توالی مستقیم از آنجا به این روش اطلاق شده است که در آن سیگنال اطلاعات مستقیماً توسط یک دنباله از کدهای شبه تصادفی تسهیم می‌شود. در این تکنیک نرخ بیتی شبه کُد تصادفی، نرخ تراشه نامیده می‌شود. در استاندارد ۸۰۲.۱۱ از کُدی موسوم به کُد *بارکر* برای تولید کدها تراشه سیستم DSSS استفاده می‌شود. مهم‌ترین ویژگی کدهای بارکر خاصیت غیر تناوبی و غیر تکراری آن است که به واسطه آن یک فیلتر تطبیقی دیجیتال قادر است به راحتی محل کد بارکر را در یک دنباله بیتی شناسایی کند.

جدول زیر فهرست کامل کدهای بارکر را نشان می‌دهد. همانگونه که در این جدول مشاهده می‌شود کدهای بارکر از ۸ دنباله تشکیل شده است. در تکنیک DSSS که در استاندارد ۸۰۲.۱۱ مورد استفاده قرار می‌گیرد، از کد بارکر با طول ۱۱ (N=11) استفاده می‌شود. این کد به ازاء یک نماد، شش مرتبه تغییر فاز می‌دهد و این بدان معنی است که سیگنال حامل نیز به ازاء هر نماد ٦ مرتبه تغییر فاز خواهد داد. جدول زیر کدهای بارکر را نشان می‌دهد.

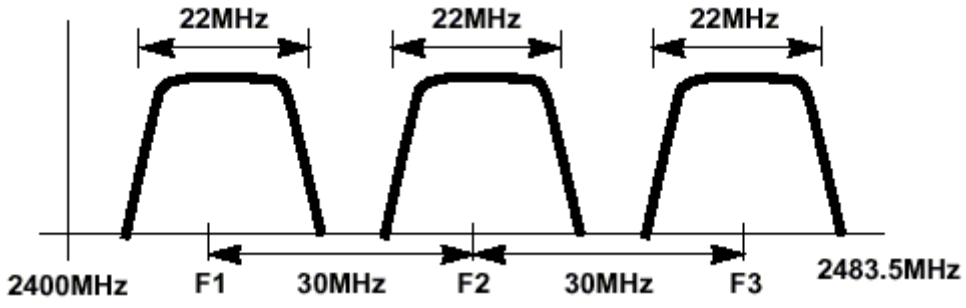
CODE LENGTH (N)	BARKER SEQUENCE
1	+
2	+ + or + -
3	+ + -
4	+ + + - or + + - +
5	+ + + - +
7	+ + + - - + -
11	+ + + - - - + - - + -
13	+ + + + + - - + + - + - +

لازم به یادآوری است که کاهش پیچیدگی سیستم ناشی از تکنیک تسهیم تفاضلی DPSK به قیمت افزایش نرخ خطای بیتی به ازاء یک نرخ سیگنال به نویز ثابت و مشخص است. شکل زیر مدل منطقی مدولاسیون و پخش سیگنال اطلاعات با استفاده از کدهای بارکر را نشان می‌دهد.

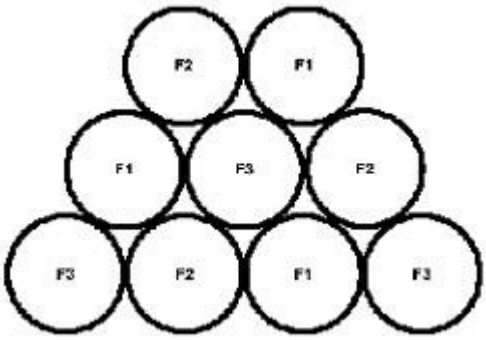


استفاده مجدد از فرکانس

یکی از نکات مهم در طراحی شبکه‌های بی‌سیم، طراحی شبکه سلولی به گونه‌ای است که تداخل فرکانسی را تا جای ممکن کاهش دهد. شکل زیر سه کانال DSSS در محدوده فرکانسی ISM را نشان می‌دهد.



شکل زیر نیز مفهوم استفاده مجدد از فرکانس با استفاده از شبکه‌های مجاور فرکانسی را نشان می‌دهد. در این شکل مشاهده می‌شود که با استفاده از یک طراحی شبکه سلولی خاص، تنها با استفاده از سه فرکانس متمایز F3,F2,F1 امکان استفاده مجدد از فرکانس فراهم شده است.



در این طراحی به هریک از سلول‌های همسایه یک کانال متفاوت اختصاص داده شده است و به این ترتیب تداخل فرکانسی بین سلول‌های همسایه به حداقل رسیده است. این تکنیک همان مفهومی است که در شبکه تلفنی سلولی یا شبکه تلفن همراه به کار می‌رود. نکتهجالب دیگر آن است که این شبکه سلولی به راحتی قابل گسترش است. خوانندگان علاقمند می‌توانند دایره‌های جدید را در چهار جهت شبکه سلولی شکل فوق با فرکانس‌های متمایز F1,F2,F3 ترسیم و گسترش دهند.

آنتن‌ها

در یکی تقسیم بندی کلی آنتن‌های مورد استفاده در استاندارد IEEE 802.11 به دو دسته: تمام جهت و نقطه به نقطه تقسیم می‌شوند. واضح است که آنتن‌های تمام جهته با توجه به آنکه نیازی به تنظیم ندارند، راحت‌تر مورد استفاده قرار می‌گیرند. این آنتن‌ها در اغلب کارت‌های شبکه (کارت‌های دسترسی) و نیز نقاط دسترسی یا ایستگاه‌های پایه بکار می‌روند.

این آنتن‌ها در فواصل کوتاه قابل استفاده هستند و برای بهره گیری در فواصل طولانی‌تر به تقویت کنندههای خارجی نیاز دارند که البته در بسیاری موارد استفاده از این تقویت کنندههای خارجی میسر و یا قانونی نیست. از سوی دیگر آنتن‌های نقطه به نقطه یا خطی در کاربردهای خارجی استفاده می‌شوند و به تنظیم دقیق نیاز دارند. محدوده عملیاتی رایج در آنتن‌های تمام جهته ٤٥ متر و محدوده عملیاتی آنتنهای نقطه به نقطه و توان بالا در حدود ٤٠ کیلومتر است. در کاربردهایی که استفاده از تقویت کننده بلا مانع است، این محدوده عملیاتی به شکل قابل توجهی افزایش یافته و تنها توسط خط دید (مسیر دید) محدود می‌شود. از جمله عوامل مهمی که محدوده عملیاتی تجهیزات مبتنی بر IEEE 802.11 را تحت تأثیر قرار می‌دهد محل نصب نقاط دسترسی یا ایستگاه پایه و نیز تداخل رادیویی است. همانگونه که پیشتر گفته شد، تجهیزات مبتنی بر این استاندارد سعی می‌کنند که با بالاترین نرخ ارسال داده کار کنند و در صورت نیاز به سرعت‌های پایین‌تر برگردند.

نتیجه

استاندارد 802.11b به تجهیزات اجازه می‌دهد که به دو روش ارتباط در شبکه برقرار شود. این دو روش عبارت‌اند از برقراری ارتباط به صورت نقطه به نقطه –همان‌گونه در شبکه‌های Ad hoc به‌کار می‌رود– و اتصال به شبکه از طریق نقاط تماس یا دسترسی (AP=Access Point).

معماری معمول در شبکه‌های محلی بی‌سیم بر مبنای استفاده از AP است. با نصب یک AP، عملاً مرزهای یک سلول مشخص می‌شود و با روش‌هایی می‌توان یک سخت‌افزار مجهز به امکان ارتباط بر اساس استاندارد 802.11b را میان سلول‌های مختلف حرکت داد. گستره‌یی که یک AP پوشش می‌دهد را BSS (Basic Service Set) می‌نامند. مجموعه‌ی

تمامی سلول‌های یک ساختار کلی شبکه، که ترکیبی از BSSهای شبکه است، را ESS (Extended Service Set) می‌نامند. با استفاده از ESS می‌توان گستره‌ی وسیع‌تری را تحت پوشش شبکه‌ی محلی بی‌سیم درآورد.

در سمت هریک از سخت‌افزارها که معمولاً مخدوم هستند، کارت شبکه‌یی مجهز به یک مودم بی‌سیم قرار دارد که با AP ارتباط را برقرار می‌کند. AP علاوه بر ارتباط با چند کارت شبکه‌ی بی‌سیم، به بستر پرسرعت‌تر شبکه‌ی سیمی مجموعه نیز متصل است و از این طریق ارتباط میان مخدوم‌های مجهز به کارت شبکه‌ی بی‌سیم و شبکه‌ی اصلی برقرار می‌شود.

همان‌گونه که گفته شد، اغلب شبکه‌های محلی بی‌سیم بر اساس ساختار فوق، که به نوع Infrastructure نیز موسوم است، پیاده‌سازی می‌شوند. با این وجود نوع دیگری از شبکه‌های محلی بی‌سیم نیز وجود دارند که از همان منطق نقطه‌به‌نقطه استفاده می‌کنند. در این شبکه‌ها که عموماً Ad hoc نامیده می‌شوند یک نقطه‌ی مرکزی برای دسترسی وجود ندارد و سخت‌افزارهای همراه – مانند کامپیوترهای کیفی و جیبی یا گوشی‌های موبایل – با ورود به محدوده‌ی تحت پوشش این شبکه، به دیگر تجهیزات مشابه متصل می‌گردند. این شبکه‌ها به بستر شبکه‌ی سیمی متصل نیستند و به همین منظور IBSS (Independent Basic Service Set) نیز خواند می‌شوند. شکل زیر شمایی ساده از یک شبکه‌ی Ad hoc را نشان می‌دهد:



شبکه‌های Ad hoc از سویی مشابه شبکه‌های محلی درون دفتر کار هستند که در آن‌ها نیازی به تعریف و پیکربندی یک سیستم رایانه‌یی به عنوان خادم وجود ندارد. در این صورت تمامی تجهیزات متصل به این شبکه می‌توانند پروندههای مورد نظر خود را با دیگر گره‌ها به اشتراک بگذارند.

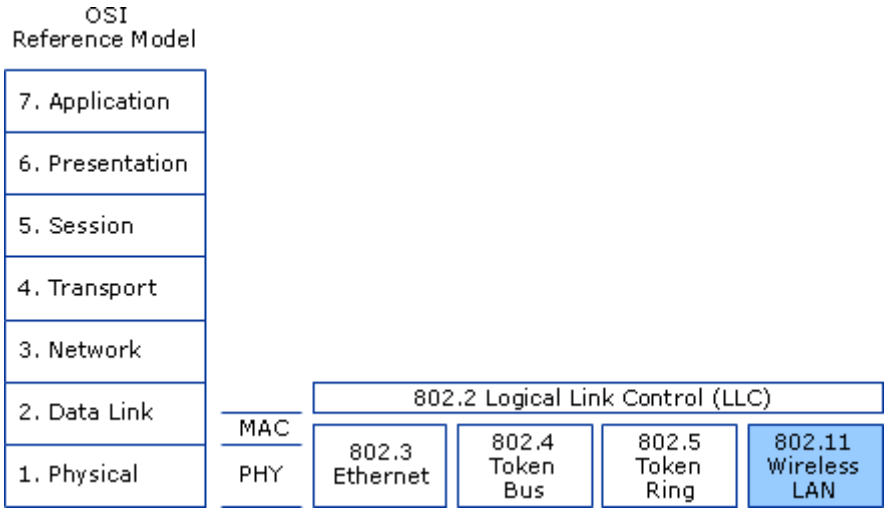
۹-۱-۱۰- لایه‌های ۸۰۲.۱۱

یک مدل مناسب برای تجزیه و تحلیل یک شبکه اطلاعاتی، مدل OSI (Open System Interconnection) تشکیل شده از ۷ لایه است که کنترل شبکه را به عهده دارند.

1) **Physical Layer**
2) **Data Link Layer**
3) **Network Layer**
4) **Transport Layer**
5) **Session Layer**
6) **Presentation Layer**
7) **Application Layer**

لایه‌های ۸۰۲.۱۱

استاندارد IEEE 802.11 در June 1997 برای WLANها منتشر شد. در این استاندارد فقط درباره ی دو لایه ی PHY و MAC صحبت شده است.



لایه اول: Physical Layer. این لایه مستقیما در رابطه با ارسال و دریافت سیگنال و تکنیک‌ها و سخت‌افزار لازم برای این کار است (مثلا فیبر نوری در شبکه‌های مخابراتی نوری یا کابل مسی در شبکه تلفن).

لایه دوم: Data Link Layer. مسئولیت اصلی این لایه مدیریت و کنترل بسته‌های اطلاعاتی (packets) است. مفاهیمی مانند کنترل خطا و پروتکل‌ها به این لایه مربوط است. این لایه خود از دو زیر لایه (sub (Logical Link Control، که وظیفه همزمان ارسال شدن اطلاعات و کنترل خطا (error checking)، و پنهان کردن تفاوتهای استانداردهای مختلف از لایه‌های بالاتر شبکه را به عهده دارد. Medium Access Control layer) (MAC) که کنترل اجازه دسترسی (Access) به اطلاعات و زیر لایه

محدوده فرکانسی ارسال داده در باند آزاد 2.4 GHz، ISM (Industrial Scientific and Medical) و نرخ ارسال بین ۱ تا ۲ Mbps است.

۸۰۲.۱۱ از دو مکانیزم متفاوت ارسال رادیویی در لایه PHY خود استفاده می‌کند. روش‌های DSSS (Direct Sequence Spread Spectrum) و FHSS (Frequency Hopped Spread Spectrum) و یک مکانیزم ارسال بوسیله مادون قرمز. اما چون در روش مادون قرمز پهنای باند کوچک است ازاین روش کمتر استفاده می‌شود.

در دو روش اول، سیگنال مورد نظر ارسالی به طوری تغییر شکل داده می‌شود که در حالیکه انرژی کل سیگنال ثابت است، محدوده فرکانسی بیشتری را اشغال می‌کند تا از اطمینان ارسال بیشتری برخوردار باشد.

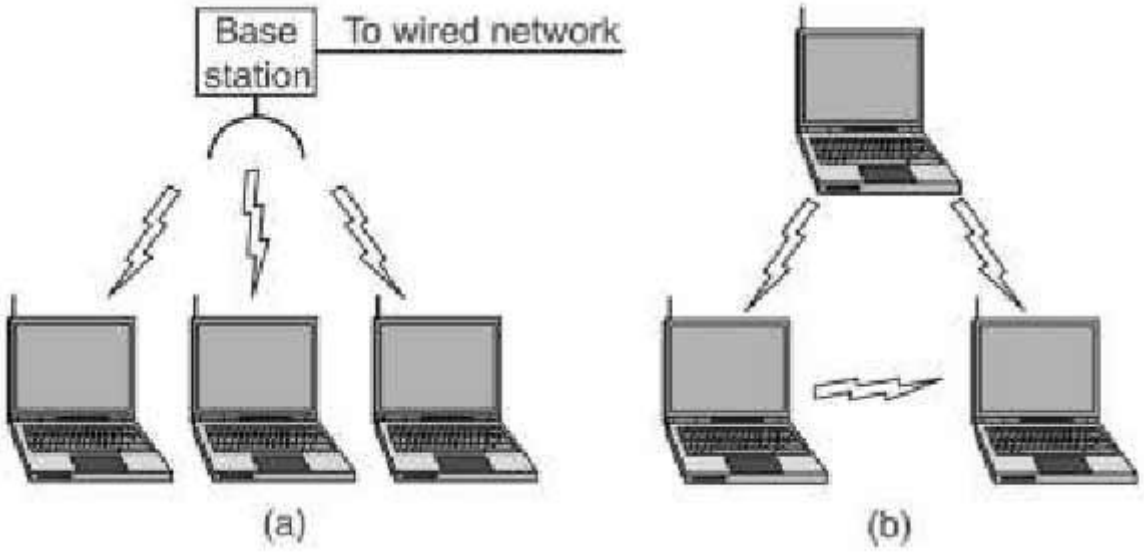
در لایه MAC ۸۰۲.۱۱ دو حالت برای ارتباطات درون شبکه تعریف می‌شود:

۱) DCF (Distributed Coordination Function)

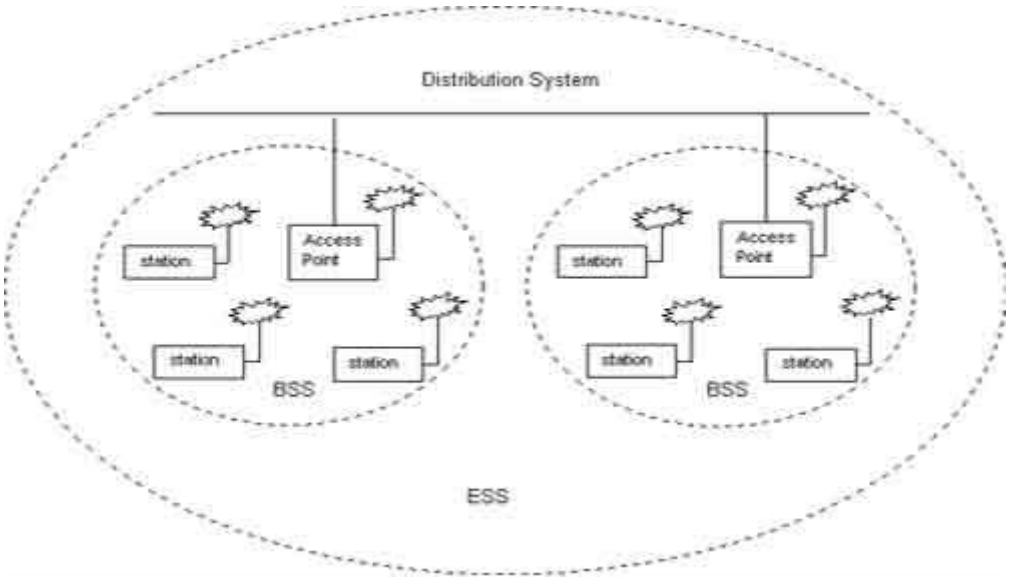
۲) PCF (Point Coordination Function)

DCF که استاندارد موظف است آن را پشتیبانی کند، تا قابلیتهای Ethernet را داشته باشد، وقتی است که Stationها بتوانند با یکدیگر به طور بی واسطه ارتباط داشته باشند. حالت دیگر یعنی PCF وقتی است که همه Stationها به واسطه یک

base Station با هم مرتبط هستند. در این مد، چون همه چیز با واسطه است، base Station می‌تواند به Stationها نوبت برای ارسال اطلاعات خود دهد و بدین صورت مشکلی پیش نمی‌آید. ولی در DCF چنین امکانی وجود ندارد و برای جلوگیری از برخورد اطلاعات فرستاده شده باید فکر دیگری کرد. طبیعی است که در شبکه سیار موانع و مسائلی که باید حل شود به مراتب پیچیده‌تر از Ethernet است که در آن یک محیط پایدار برای تبادل اطلاعات وجود دارد می‌باشند. برای مثال در Ethernet هر Station به سادگی می‌تواند هر Station را ببیند، ولی در شبکه‌های سیار مشکل Range محدود فرستنده‌های رادیویی وجود دارد و لزوما همه Stationها نمی‌توانند از فعالیتهای هم باخبر باشند.روشی که بدین منظور استفاده می‌شود CSMA/CA (Carrier Sense Multiple Access with Collision Avoidence) است. در شکل زیر قسمت (a) عملیات PCF و قسمت (b) عملیات DCF را نشان می‌دهد.



با دو روش Authentication و Encryption امنیت رد و بدل اطلاعات بالا می‌رود. Authentication یعنی دادن اجازه ارسال و دریافت اطلاعات به وسیله یک Station به Stationهای دیگر. این در صورتی است که Stationها دو به دو با هم مرتبط باشند. اصطلاحا به این روش ارتباط Stationها روش IBSS (Independent Basic Service Set) گفته می‌شود. اگر Stationها از طریق یک Access Point با هم در ارتباط با شند یک Infrastructure Basic Service Set تشکیل می‌شود. با ارتباط چند BSS Infrastructure به هم از طریق یک Distribution System (که معمولا یک شبکه wired مثل Ethernet LAN است.) یک شبکه گسترده‌تر به نام ESS (Extended Service Set) به وجود می‌آید. شکل زیر ESS را نشان می‌دهد.



۹-۲- امنیت شبکه‌های بی‌سیم

۹-۲-۱- مقدمه

در طی چند سال گذشته یک پیام واضح و روشن وجود داشت ایجاد امنیت برای تکنولوژی WiFi در عین سودمندی بسیار آن کار ساده‌ای نیست در اکثر نقاط دسترسی بی‌سیم سیتم امنیتی به طور پیش فرض غیر فعال است و حتی سیستم ایمنی موجود در آن‌ها نیز مناسب و کافی نیست. WEP (Wired Equivalent Privacy) اولین کوشش برای ایمن کردن WiFi مکرا نقاط ضعف زیادی را به نمایش گذاشته است.ابزار بسیلر زیادی برای حمله به WiFi وجود دارد که این ابزار فقط در عرض چند دقیقه می‌توانند کلید به کار رفته برای محافظت از شبکه را دور بزنند و از کار بیندازند.حتی نسل بعدی تکنیک‌های ایمنی هنوز هم مشکلات متعددی دارند جدیدترین مشخصات ایمنی بی‌سیم یعنی ۸۰۲.۱۱ امکان انجام انواع روش‌های تایید اعتبار شبکه شامل کلمه‌های عبور ساده و سایر مکانیزم‌های تائید اعتبار ضعیف را که پشت سر گذاشتن آن‌ها بسیار ساده است فراهم می‌کند. با رواج بیشتر استفاده از اینترنت بی‌سیم، کاهش قیمت آن و افزایش سهولت دسترسی به آن طبعاً مشکلات امنیتی آن نیز افزایش می‌یابد. از جمله مشکلات امنیتی در زمینهٔ WiFi می‌توان به موارد زیر اشاره کرد:

۹-۲-۲- امنیت شبکه بی‌سیم

Rouge Access Point Problem

این مشکل یکی از مهم‌ترین نگرانی‌های امنیتی در زمینهٔ استفاده از شبکه‌های WiFi به حساب می‌آید. Rouge Access Point به هر نقطهٔ دسترسی WiFi (Access Point) اطلاق می‌شود که بدون اجازهٔ شما به شبکه وصل شده است و از امکانات آن از جمله پهنای باند اینترنت استفاده می‌کند.این معزل علاوه بر اتصال غیر مجاز به شبکه و استفاده از پهنای باند آن سایر مشکلات امنیتی مانند hacking را نیز سبب شود.

- دستگاه‌های ناامن WiFi: از جمله Access Pointها و دستگاه‌های مورد استفادهٔ کاربران ممکن است موجب مشکلات جدی در این زمینه گردد. و این مورد معمولاً بیش از همه مورد توجه هکرهاست.
- تنظیمات ناصحیح دستگاه‌های بی‌سیم و عدم تغییر در تنظیمات پیش‌فرض آن‌ها امکانات متنوع نفوذگران

استاندارد 802.11 سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد.

با به کار گیری تائید اعتبار دو طرفه مبتنی بر مجوز با رمزگذاری مبتنی بر AES شبکه‌های WiFi مدرن می‌توانند حتی برای مهاجمان حرفه‌ای نیز یک مانع قابل توجه محسوب شوند.با بعضی از WAP کاربران می‌توانند عدم پخش SSIDرا انتخاب کنند.SSID سر واژه عبارت زیر است:SSID service set identifier ورود نفوذ گران به شبکه را دشوارتر می‌سازد.

شبکه‌های WiFi دارای امکانات امنیتی بسیار قدرتمند می‌باشند که از دسترسی غیر مجاز به این شبکه‌ها جلوگیری می‌کند. از جمله این استانداردها می‌توان به

۱. IEEE 802.1x
۲. WEP - Wired Equivalent Privacy
۳. WPA - WiFi Protected Access
۴. TKIP - Temporal Key Integrity Protocol

اشاره کرد. علاوه بر استانداردهای یاد شده در Access Pointهایی که دارای نرم‌افزارهای کارآمد می‌باشند، امکان فیلتر کردن MAC Address وجود دارد، در این صورت فقط MAC Addressهای تعریف شده در نرم‌افزار AP امکان بهره برداری از سرویس AP را دارا می‌باشند.

Hotspotهای WiFi می‌توانند آشکار و باز باشند یا محفوظ باشند.اگر آن‌ها آشکار باشند هر کسی با یک کارت WiFi می‌تواند به hotspot دسترسی داشته باشد اما اگر محفوظ باشد لازم است کاربر رمز wep را برای اتصال بداند. WEP یک سیستم رمزگذاری داده‌ها است که۸۰۲/۱۱ از طریق هوا ارسال می‌کند. WEP دو نوع دارد: رمز گذلری ۶۴ بیتی و رمز گذلری ۱۲۸ بیتی. رمزگذاری ۱۲۸ بیتی امن‌تر است و افراد بیشتر ازان استفاده می‌کنند غیر قابل دسترس است مگر اینکه کد WEP را بداند.

اگر شما یک hotspot در منزل خود نصب کنید با ایجاد و استفاده از یک کد wep می‌توانید از استراق سمع تصادفی شبکه تان توسط همسایگان خود جلوگیری کنید.چه در خانه و چه در بیرون شما باید کد wep را بدانید سپس ان را در نرم‌افزار کارت وای فتی وارد کنید تا بتوانید به شبکه دسترسی داشته باشید.

با به کارگیری نکات زیر می‌توان یک امنیت شبکه بی‌سیم را تا حد قابل قبولی بهبود بخشید.

لازم به ذکر است که این نکات لازم است ولی کافی نیست.

۱. کلمه عبور پیش‌فرض مدیر سیستم (Administrator) را روی نقاط دسترسی و مسیریاب‌های بی‌سیم تغییر دهید.

اغلب نقاط دسترسی (Access Point) و مسیریاب‌های بی‌سیم امکان مدیریت شبکه WiFi را از طریق یک حساب کاربری مدیریتی فراهم می‌کنند. این حساب کاربری امکان دسترسی ابزار و پیکربندی آن را با نام کاربری و کلمه عبور فراهم می‌کند. اغلب تولیدکنندگان نام کاربری و کلمه عبور را در کارخانه تنظیم می‌کنند. نام کاربری معمول Admin یا Administrator و کلمه عبور یا خالی است یا کلماتی مثل Admin، Public، Password و... می‌باشد.

اولین گام برای افزایش امنیت شبکه بی‌سیم تغییر کلمه عبور پیش‌فرض نقاط دسترسی و مسیریاب‌های بی‌سیم بلافاصله پس از نصب است. اغلب ابزارها اجازه تغییر نام کاربری را نمی‌دهند اما اگر ابزارهای شما این امکان را می‌دهند، اکیدا توصیه می‌شود که نام کاربری را هم تغییر دهید.

برای امن نگه‌داشتن شبکه در آینده، می‌بایست به‌طور منظم این کلمه عبور را تغییر دهید. اغلب کارشناسان توصیه می‌کنند کلمه عبور را بعد از ۳۰ تا ۹۰ روز تغییر دهید.

۲. فعال‌سازی قابلیت WPA/WEP

WPA (WiFi Protected Access) یک استاندارد امنیتی برای شبکه‌های بی‌سیم است (با Windows XP Product Activation اشتباه نشود). برای استفاده از WPA با Windows XP باید Clientهای دارای Windows XP را به صورت دستی Patch کنید و هم‌چنین مطمئن شوید کارت شبکه‌ها و نقاط دسترسی به درستی پیکربندی شده‌اند.

۳. تغییر SSID پیش فرض

نقاط دسترسی و مسیریاب‌های بی‌سیم دارای یک نام شبکه (SSID (Service Set Identifier هستند که توسط تولیدکنندگان به‌طور پیش‌فرض انتخاب می‌شود. SSID از ابزارهای پیکربندی بر مبنای وب یا ویندوز این سازندگان قابل دسترسی است. اغلب SSIDهای پیش فرض کلمات ساده‌ای مثل Wireless، Netgear، Linksys، Default و... هستند. هرچند نفوذگر صرفا با دانستن SSID قادر به نفوذ به شبکه شما نیست ولی این مساله به عنوان یک نقطه شروع خوب برای نفوذگر به حساب می‌آید. زمانی که کسی شبکه‌ای با SSID پیش فرض بیابد، با دانستن این نکته که به احتمال فراوان این شبکه به درستی پیکربندی نشده است، ترغیب به نفوذ به شبکه می‌شود.

SSID می‌تواند هر زمانی تغییر کند به شرطی که این تغییر در تمام Clientها نیز اعمال شود. برای افزایش امنیت شبکه‌های بی‌سیم، نام پیش فرض SSID را تغییر دهید. در انتخاب SSID توصیه‌های زیر را در نظر داشته باشید:

- از نام، آدرس، تاریخ تولد، شماره تلفن یا دیگر اطلاعات شخصی تان به عنوان بخشی از SSID استفاده نکنید.
- از کلمات عبور نام کاربری ویندوزتان یا emailتان یا... استفاد نکنید.
- با استفاده از عباراتی مثل "TOP_SECRET"، "FUNNY_BOX" و... نفوذگران را وسوسه نکنید.!!!
- از ترکیب حروف و اعداد استفاده کنید.
- عباراتی با طول حداکثر یا نزدیک به حداکثر انتخاب کنید.
- هرچند ماه یک بار SSIDتان را تغییر دهید.

۴. قابلیت پالایش آدرس MAC را روی نقاط دسترسی و مسیریاب‌های بی‌سیم فعال کنید.

اغلب نقاط دسترسی و مسیریاب‌های بی‌سیم دارای قابلیتی به نام پالایش آدرس MAC (MAC Address Filtering) هستند. این مشخصه اغلب به‌طور پیش فرض فعال نیست. برای افزایش امنیت شبکه بی‌سیم تان این قابلیت را فعال کنید. در

صورتی که این قابلیت فعال نباشد، هر clientای با دانستن SSID شبکه شما (در نظر داشته باشید که فهمیدن SSID کار بسیار ساده‌ای است) شاید چند پارامتر امنیتی دیگر مثل کلید رمزگذاری (در صورتی که قابلیت WEP فعال باشد) می‌تواند به شبکه شما وصل شود.

برای تنظیم قابلیت پالایش آدرس MAC شما به عنوان مدیر شبکه بی‌سیم باید لیست Clientهایی که مجازند به شبکه وصل شوند را پیکربندی کنید. ابتدا آدرس MAC هر client را از طریق سیستم عامل یا ابزارهای پیکربندی به دست آورید و سپس آن‌ها را در صفحه پیکربندی نقاط دسترسی و مسیریاب‌های بی‌سیم وارد کنید و نهایتا قابلیت پالایش را فعال کنید. از این پس هر درخواست اتصال به شبکه بی‌سیم که برسد آدرس MAC آن با لیست تنظیم شده بررسی شده و در صورتی که در لیست نباشد اجازه اتصال به شبکه را نمی‌یابد. البته باید نوجه داشت که نفوذگران با جعل آدرس MAC (MAC Spoofing) قادرند به شبکه بی‌سیم شما وصل شوند ولی این مساله نباید باعث شود که شما از خیر این قابلیت بگذرید.

۵. قابلیت همه‌پخشی SSID را روی نقاط دسترسی و مسیریاب‌های بی‌سیم غیرفعال کنید.

اغلب نقاط دسترسی و مسیریاب‌های بی‌سیم به‌طور خودکار SSID خوشان را در فواصل زمانی مشخص پخش می‌کنند. این مشخصه برای این است که Clientها بتوانند به‌طور پویا شبکه‌های بی‌سیم را تشخیص دهند و بین آن‌ها جابه‌جا شوند (از شبکه‌ای به شبکه دیگر نقل مکان کنند). لازم به ذکر است که این مشخصه برای Hotspotهای تجاری و سیار طراحی شده است که Clientهای زیادی می‌آیند و می‌روند ولی برای شبکه‌های خانگی لازم نیست. از آن جایی که Ssid به صورت واضح پخش می‌شود و هیچ رمزگذاری روی آن صورت نمی‌گیرد، به دست آوردن آن توسط نفوذگران کار راحتی است. همان‌طور که در گام ۳ اشاره شد نفوذگر با دانستن SSID یک مرحله به هدف نزدیک‌تر می‌شود.

در یک شبکه بی‌سیم بحث Roaming (جابه‌جایی بین دو شبکه بی‌سیم) مطرح نیست و پخش کردن SSID هیچ ضرورتی ندارد. برای افزایش امنیت شبکه بی‌سیم باید این قابلیت را غیرفعال کنید. یک بار که client شما با SSID درست پیکربندی شد دیگر نیازی به پیغام‌های همه‌پخشی نیست.

دقت داشته باشید که غیرفعال کردن قابلیت همه‌پخشی SSID فقط یکی از تکنیک‌های محکم‌سازی و افزایش امنیت شبکه‌های بی‌سیم است. این روش ۱۰۰ درصد موثر نیست و نفوذگرها هنوز می‌توانند با sniff کردن پیغام‌های مختلف پخش شده در پروتکل WiFi، SSID را تشخیص دهند. در واقع تکنیک‌هایی مثل غیرفعال کردن همه‌پخشی SSID باعث می‌شئد که شبکه بی‌سیم شما هدف راحتی برای نفوذگران نباشد.

اگر هم اکنون دارای یک شبکه بی‌سیم می‌باشید ممکن است این مسئله را در نظر بگیرید که آیا شبکه تان ایمن است یا خیر؟ چهار مورد وجود دارند که شما می‌توانید انجام دهید که اطمینان حاصل نمایید که شبکه تان امن می‌باشد .

۱- اطمینان حاصل نمایید که نقطه یا نقاط دسترسی SSID تان (شناسایی تنظیم کننده خدمات) را پخش نمی‌نماید (که بطور اساسی یک شناسایی کننده برای شبکه شما می‌باشد

۲- اطمینان حاصل نمایید که نقطه یا نقاط دسترسی تان ترافیک بی‌سیم را با بکارگیری WEP رمز سازی می‌نماید.

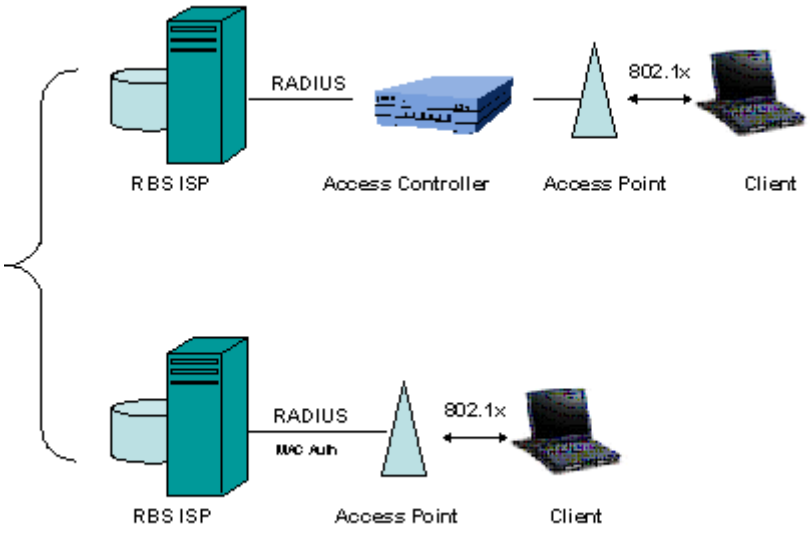
۳- یک سیستم "شناسایی بدون اجازه وارد شدن افراد غیر مجاز به شبکه بی‌سیم تان" را خریداری نمایید. تعداد زیادی از این محصولات که آماده و قابل دسترس می‌باشند، طراحی شده‌اند که بشما کمک نمایند که امنیت شبکهء WiFi تان و همینطور اینکه چه افرادی از آن استفاده می‌نمایند را دیده بانی نمایید.

۴- اگر نیاز به امنیت خیلی بالا دارید، می‌توانید یا اطمینان حاصل نمایید که افرادیکه با شبکه شما کار می‌نمایند بطور مناسب و کارآیی آموزش دیده و یا از یک مشاور بی‌سیم استفاده نمایید. شما نیاز خواهید داشت که نقاط دسترسی غیر استاندارد و اختصاصی از شرکتهایی مثل سیسکو (Cisco) خریداری نمایید (اگرچه حتی بعضی استانداردهای اختصاصی از شرکتهایی مثل (Cisco) مشکل خودشان را دارند). متاسفانه این بطور قابل ملاحظه‌ای هزینه شبکه بی‌سیم شما را افزایش خواهد داد.

۹-۲-۳- چهار مشکل امنیتی مهم شبکه‌های بی‌سیم ۸۰۲.۱۱

موفقیت حیرت انگیز 802.11 به علت توسعه «اترنت بی‌سیم» است. همچنانکه 802.11 به ترقی خود ادامه می‌دهد، تفاوت‌هایش با اترنت بیشتر مشخص می‌شود. بیشتر این تفاوت‌ها به دلیل نا آشنایی نسبی بسیاری از مدیران شبکه با لایه فیزیکی فرکانس رادیویی است. در حالیکه همه مدیران شبکه باید درک پایه‌ای از لینک رادیویی داشته باشند، تعدادی از ابزارها برای کمک به آن‌ها به خدمت گرفته می‌شوند. آنالایزرهای (تحلیل کننده) شبکه‌های بی‌سیم برای مدت‌ها ابزاری لازم برای مهندسان شبکه در اشکال زدایی و تحلیل پروتکل بوده‌اند. بسیاری از آنالایزرها بعضی کارکردهای امنیتی را نیز اضافه کرده‌اند که به آن‌ها اجازه کار با عملکردهای بازرسی امنیتی را نیز می‌دهد.

در این سلسله چهار مشکل از مهم ترین آسیب پذیری‌های امنیتی موجود در LANهای بی‌سیم، راه حل آن‌ها و در نهایت چگونگی ساخت یک شبکه بی‌سیم امن مورد بحث قرار می‌گیرد. بسیاری از پرسش‌ها در این زمینه در مورد ابزارهایی است که مدیران شبکه می‌توانند استفاده کنند. یک آنالایزر از اولین خریدهایی است که یک مدیر شبکه باید انجام دهد. آنالایزرها علاوه بر عملکردهای سنتی تحلیل پروتکل و ابزار تشخیص عیب، می‌توانند برای تشخیص بسیاری از نگرانی‌های امنیتی که استفاده از شبکه بی‌سیم را کند می‌کنند، استفاده شوند.



مسأله شماره ۱: دسترسی آسان

LANهای بی‌سیم به آسانی پیدا می‌شوند. برای فعال کردن کلاینت‌ها در هنگام یافتن آن‌ها، شبکه‌ها باید فریم‌های Beacon با پارامترهای شبکه را ارسال کنند. البته، اطلاعات مورد نیاز برای پیوستن به یک شبکه، اطلاعاتی است که برای

اقدام به یک حمله روی شبکه نیاز است. فریم‌های Beacon توسط هیچ فانکشن اختصاصی پردازش نمی‌شوند و این به این معنی است که شبکه 802.11 شما و پارامترهایش برای هر شخصی با یک کارت 802.11 قابل استفاده است. نفوذگران با آنتن‌های قوی می‌توانند شبکه‌ها را در مسیرها یا ساختمآن‌های نزدیک بیابند و ممکن است اقدام به انجام حملاتی کنند حتی بدون اینکه به امکانات شما دسترسی فیزیکی داشته باشند.



راه حل شماره ۱: تقویت کنترل دسترسی قوی

دسترسی آسان الزاماً با آسیب پذیری مترادف نیست. شبکه‌های بی‌سیم برای ایجاد امکان اتصال مناسب طراحی شده‌اند، اما می‌توانند با اتخاذ سیاستهای امنیتی مناسب تا حد زیادی مقاوم شوند. یک شبکه بی‌سیم می‌تواند تا حد زیادی در این اتاق محافظت شده از نظر الکترومغناطیس محدود شود که اجازه نشت سطوح بالایی از فرکانس رادیویی را نمی‌دهد. به هرحال، برای بیشتر موسسات چنین بردهایی لازم نیستند. تضمین اینکه شبکه‌های بی‌سیم تحت تأثیر کنترل دسترسی قوی هستند، می‌تواند از خطر سوءاستفاده از شبکه بی‌سیم بکاهد.

تضمین امنیت روی یک شبکه بی‌سیم تا حدی به عنوان بخشی از طراحی مطرح است. شبکه‌ها باید نقاط دسترسی را در بیرون ابزار پیرامونی امنیت مانند فایروال‌ها قرار دهند و مدیران شبکه باید به استفاده از VPNها برای میسر کردن دسترسی به شبکه توجه کنند. یک سیستم قوی تأیید هویت کاربر باید به کار گرفته شود و ترجیحاً با استفاده از محصولات جدید که برپایه استاندارد IEEE 802.1x هستند. 802.1x انواع فریم‌های جدید برای تأیید هویت کاربر را تعریف می‌کند و از دیتابیس‌های کاربری جامعی مانند RADIUS بهره می‌گیرد. آنالایزرهای باسیم سنتی می‌توانند با نگاه کردن به تقاضاهای RADIUS و پاسخ‌ها، امکان درک پروسه تأیید هویت را فراهم کنند. یک سیستم آنالیز خبره برای تأیید هویت 802.11 شامل یک روتین عیب یابی مشخص برای LANهاست که ترافیک تأیید هویت را نظاره می‌کند و امکان تشخیص عیب را برای مدیران شبکه فراهم می‌کند که به آنالیز بسیار دقیق و کدگشایی فریم احتیاج ندارد. سیستم‌های آنالیز خبره که پیام‌های تأیید هویت 802.1x را دنبال می‌کنند، ثابت کرده‌اند که برای استفاده در LANهای استفاده کننده از 802.1x فوق العاده باارزش هستند.

هرگونه طراحی، بدون در نظر گرفتن میزان قدرت آن، باید مرتباً بررسی شود تا سازگاری چینش فعلی را با اهداف امنیتی طراحی تضمین کند. بعضی موتورهای آنالیز تحلیل عمیقی روی فریم‌ها انجام می‌دهند و می‌توانند چندین مسأله معمول امنیت

802.1x را تشخیص دهند. تعدادی از حملات روی شبکه‌های باسیم در سال‌های گذشته شناخته شده‌اند و لذا وصله‌های فعلی به خوبی تمام ضعف‌های شناخته شده را در این گونه شبکه‌ها نشان می‌دهند. آنالایزرهای خبره پیاده سازی‌های ضعیف را برای مدیران شبکه مشخص می‌کنند و به این ترتیب مدیران شبکه می‌توانند با به کارگیری سخت‌افزار و نرم‌افزار ارتقاء یافته، امنیت شبکه را حفظ کنند.

پیکربندی‌های نامناسب ممکن است منبع عمده آسیب پذیری امنیتی باشد، مخصوصاً اگر LANهای بی‌سیم بدون نظارت مهندسان امنیتی به کارگرفته شده باشند. موتورهای آنالیز خبره می‌توانند زمانی را که پیکربندی‌های پیش فرض کارخانه مورد استفاده قرار می‌گیرند، شناسایی کنند و به این ترتیب می‌توانند به ناظران کمک کنند که نقاطی از دسترسی را که بمنظور استفاده از ویژگی‌های امنیتی پیکربندی نشده‌اند، تعیین موقعیت کنند. این آنالایزرها همچنین می‌توانند هنگامی که وسایلی از ابزار امنیتی قوی مانند VPNها یا 802.1x استفاده نمی‌کنند، علائم هشدار دهنده را ثبت کنند.

مسأله شماره ۲: نقاط دسترسی نامطلوب

دسترسی آسان به شبکه‌های LAN بی‌سیم امری منفک از راه اندازی آسان آن نیست. این دو خصوصیت در هنگام ترکیب شدن با یکدیگر می‌توانند برای مدیران شبکه و مسوولان امنیتی ایجاد دردسر کنند. هر کاربر می‌تواند به فروشگاه کامپیوتر نزدیک خود برود، یک نقطه دسترسی! بخرد و بدون کسب اجازه‌ای خاص به کل شبکه متصل شود. بسیاری از نقاط دسترسی با اختیارات مدیران میانی عرضه می‌شوند و لذا دپارتمآن‌ها ممکن است بتوانند LAN بی‌سیمشان را بدون صدور اجازه از یک سازمان IT مرکزی در معرض عموم قرار دهند. این دسترسی به اصطلاح «نامطلوب» بکارگرفته شده توسط کاربران، خطرات امنیتی بزرگی را مطرح می‌کند. کاربران در زمینه امنیتی خبره نیستند و ممکن است از خطرات ایجاد شده توسط LANهای بی‌سیم آگاه نباشند. ثبت بسیاری از ورودها به شبکه نشان از آن دارد که ویژگی‌های امنیتی فعال نیستند و بخش بزرگی از آن‌ها تغییراتی نسبت به پیکربندی پیش فرض نداشته‌اند و با همان پیکربندی راه اندازی شده‌اند.



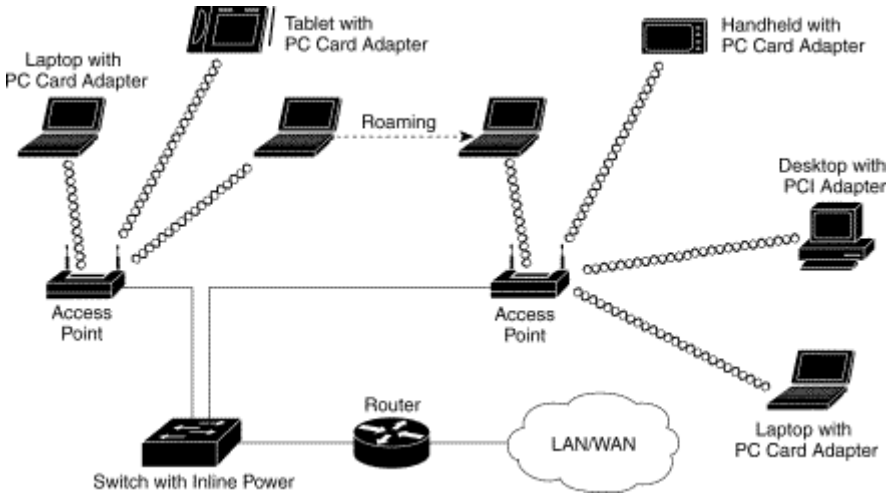
راه حل شماره۲: رسیدگی‌های منظم به سایت

مانند هر تکنولوژی دیگر شبکه، شبکه‌های بی‌سیم به مراقبت از سوی مدیران امنیتی نیاز دارند. بسیاری از این تکنولوژی‌ها به دلیل سهولت استفاده مورد بهره برداری نادرست قرار می‌گیرند، لذا آموختن نحوه یافتن شبکه‌های امن نشده از اهمیت بالایی برخوردار است.

روش بدیهی یافتن این شبکه‌ها انجام همان کاری است که نفوذگران انجام می‌دهند: استفاده از یک آنتن و جستجوی آن‌ها به این منظور که بتوانید قبل از نفوذگران این شبکه‌ها را پیدا کنید. نظارت‌های فیزیکی سایت باید به صورت مرتب و در حد امکان انجام گیرد. اگرچه هرچه نظارت‌ها سریع‌تر انجام گیرد، امکان کشف استفادههای غیرمجاز بیشتر است، اما زمان زیادی که کارمندان مسوول این امر باید صرف کنند، کشف تمامی استفادههای غیرمجاز را بجز برای محیط‌های بسیار

حساس، غیرقابل توجیه می‌کند. یک راهکار برای عدم امکان حضور دائم می‌تواند انتخاب ابزاری در اندازه دستی باشد. این عمل می‌تواند استفاده تکنسین‌ها از اسکنرهای دستی در هنگام انجام امور پشتیبانی کاربران، برای کشف شبکه‌های غیرمجاز باشد.

یکی از بزرگترین تغییرات در بازار 802.11 در سال‌های اخیر ظهور 802.11a به عنوان یک محصول تجاری قابل دوام بود. این موفقیت نیاز به ارائه ابزارهایی برای مدیران شبکه‌های 802.11a را بوجود آورد. خوشبختانه، 802.11a از همان MAC پیشینیان خود استفاده می‌کند، بنابراین بیشتر آنچه مدیران راجع به 802.11 و تحلیل کنندهها می‌دانند، بدرد می‌خورد. مدیران شبکه باید دنبال محصولی سازگار باشند که هر دو استاندارد 802.11a و 802.11b را بصورت یکجا و ترجیحاً به صورت همزمان پشتیبانی کند. چیپ ست‌های دوباندی 802.11a/b و کارت‌های ساخته شده با آن‌ها به آنالایزرها اجازه می‌دهد که روی هر دو باند بدون تغییرات سخت‌افزاری کار کنند، و این بدین معنی است که مدیران شبکه نیاز به خرید و آموزش فقط یک چارچوب پشتیبانی شده برای هر دو استاندارد دارند. این روال باید تا 802.11g ادامه یابد، تا جایی که سازندگان آنالایزرها کارت‌های 802.11a/b/g را مورد پذیرش قرار دهند.



بسیاری از ابزارها می‌توانند برای انجام امور رسیدگی به سایت و ردیابی نقاط دسترسی نامطلوب استفاده شوند، اما مدیران شبکه باید از نیاز به همگامی با آخرین تکنیک‌های استفاده شده در این بازی موش و گربه! آگاه باشند. نقاط دسترسی می‌توانند در هر باند فرکانسی تعریف شده در 802.11 بکارگرفته شوند، بنابراین مهم است که تمام ابزارهای مورد استفاده در بررسی‌های سایت بتوانند کل محدوده فرکانسی را پویش کنند. حتی اگر شما استفاده از 802.11b را انتخاب کرده اید، آنالایزر استفاده شده برای کار نظارت بر سایت، باید بتواند همزمان نقاط دسترسی 802.11a را نیز پویش کند تا در طول یک بررسی کامل نیازی به جایگزین‌های سخت‌افزاری و نرم‌افزاری نباشد.

بعضی نقاط دسترسی نامطلوب سعی دارند کانالهایی را به صورت غیرقانونی روی کانال‌های 802.11b به کار بگیرند که برای ارسال استفاده نمی‌شوند. برای مثال قوانین FCC تنها اجازه استفاده از کانال‌های ۱ تا ۱۱ از 802.11b را می‌دهد. کانال‌های ۱۲ تا ۱۴ جزء مشخصات آن تعریف شده‌اند اما فقط برای استفاده در اروپا و ژاپن کاربرد دارند. به هرحال، بعضی کاربران ممکن است از نقطه دسترسی کانال‌های اروپایی یا ژاپنی استفاده کنند، به این امید که رسیدگی یک سایت متمرکز روی کانال‌های مطابق با FCC از کانال‌های فرکانس بالاتر چشم پوشی کند. این قضیه مخصوصاً برای ردیابی ابزارهایی اهمیت دارد که بیرون باند فرکانسی مجاز بکارگرفته شده‌اند تا از اعمال اجرایی اتخاذ شده توسط نمایندگی‌های مجاز برحذر

باشند. آنالایزرهای غیرفعال (Passive Analyzers) ابزار ارزشمندی هستند زیرا استفادههای غیرمجاز را تشخیص می‌دهند، اما چون توانی ارسال نمی‌کنند استفاده از آن‌ها قانونی است.

مدیران شبکه همواره تحت فشار زمانی هستند، و به روش آسانی برای یافتن نقاط دسترسی نامطلوب و در عین حال چشم پوشی از نقاط دسترسی مجاز نیاز دارند. موتورهای جستجوی خبره به مدیران اجازه می‌دهند که لیستی از نقاط دسترسی مجاز را پیکربندی کنند. هر نقطه دسترسی غیرمجاز باعث تولید علامت هشدار دهنده‌ای می‌شود. در پاسخ به علامت هشدار دهنده، مدیران شبکه می‌توانند از ابزار دیگری برای پیدا کردن نقطه دسترسی براساس مقیاس‌های قدرت سیگنال استفاده کنند. اگرچه این ابزارها ممکن است خیلی دقیق نباشند، ولی برای محدود کردن محوطه جستجوی نقطه دسترسی نامطلوب به اندازه کافی مناسب هستند.

مسأله شماره ۳: استفاده غیرمجاز از سرویس

چندین شرکت مرتبط با شبکه‌های بی‌سیم نتایجی منتشر کرده‌اند که نشان می‌دهد اکثر نقاط دسترسی با تنها تغییرات مختصری نسبت به پیکربندی اولیه برای سرویس ارائه می‌گردند. تقریباً تمام نقاط دسترسی که با پیکربندی پیش فرض مشغول به ارائه سرویس هستند، WEP (Wired Equivalent Privacy) را فعال نکرده‌اند یا یک کلید پیش فرض دارند که توسط تمام تولیدکنند گان محصولات استفاده می‌شوند. بدون WEP دسترسی به شبکه به راحتی میسر است. دو مشکل به دلیل این دسترسی باز می‌تواند بروز کند: کاربران غیرمجاز لزوماً از مفاد ارائه سرویس تبعیت نمی‌کنند، و نیز ممکن است تنها توسط یک اسپم ساز اتصال شما به ISPتان لغو شود.

راه حل شماره۳: طراحی و نظارت برای تأیید هویت محکم

راه مقابله مشخص با استفاده غیرمجاز، جلوگیری از دسترسی کاربران غیرمجاز به شبکه است. تأیید هویت محکم و محافظت شده توسط رمزنگاری یک پیش شرط برای صدور اجازه است، زیرا امتیازات دسترسی برپایه هویت کاربر قرار دارند. روش‌های VPN که برای حفاظت از انتقال در لینک رادیویی به کارگرفته می‌شوند، تأیید هویت محکمی را ارائه می‌کنند. تخمین مخاطرات انجام شده توسط سازمان‌ها نشان می‌دهد که دسترسی به 802.1x باید توسط روش‌های تأیید هویت برپایه رمزنگاری تضمین شود. از جمله این روش‌ها می‌توان به TLS (Transport Layer Security)، TTLS (Tunneled TLS) یاPEAP (Protected Extensible Authentication Protocol) اشاره کرد.

هنگامی که یک شبکه با موفقیت راه اندازی می‌شود، تضمین تبعیت از سیاست‌های تایید هویت و اعطای امتیاز مبتنی بر آن حیاتی است. همانند مسأله نقاط دسترسی نامطلوب، در این راه حل نیز نظارت‌های منظمی بر تجهیزات شبکه بی‌سیم باید انجام شود تا استفاده از مکانیسم‌های تأیید هویت و پیکربندی مناسب ابزارهای شبکه تضمین شود. هر ابزار نظارت جامع باید نقاط دسترسی را در هر دو باند فرکانسی 802.11b (باند 2.4 GHz ISM) و 802.11a (5 GHz U-NII) تشخیص دهد و پارامترهای عملیاتی مرتبط با امنیت را نیز مشخص کند. اگر یک ایستگاه غیرمجاز متصل به شبکه کشف شود، یک رسیور دستی می‌تواند برای ردیابی موقعیت فیزیکی آن استفاده شود. آنالایزرها نیز می‌توانند برای تأیید پیکربندی بسیاری از پارامترهای نقاط دسترسی استفاده گردند و هنگامی که نقاط دسترسی آسیب پذیری‌های امنیتی را نمایان می‌کنند، علائم هشدار دهنده صوتی تولید کنند.

مسأله شماره ۴: محدودیت‌های سرویس و کارایی

LANهای بی‌سیم ظرفیت‌های ارسال محدودی دارند. شبکه‌های 802.11b سرعت انتقالی برابر با 11 Mbps و شبکه‌های برپایه تکنولوژی جدید 802.11a نرخ انتقال اطلاعاتی تا 54 Mbps دارند. البته ماحصل مؤثر واقعی، به دلیل بالاسری لایه MAC، تقریباً تا نیمی از ظرفیت اسمی می‌رسد. نقاط دسترسی کنونی این ظرفیت محدود را بین تمام کاربران مربوط به یک نقطه دسترسی قسمت می‌کنند. تصور اینکه چگونه برنامه‌های محلی احتمالاً چنین ظرفیت محدودی را اشغال می‌کنند یا چگونه یک نفوذگر ممکن است یک حمله انکار سرویس (DoS) روی این منابع محدود طرح ریزی کند، سخت نیست.

ظرفیت رادیویی می‌تواند به چندین روش اشغال شود. ممکن است توسط ترافیکی که از سمت شبکه باسیم با نرخی بزرگتر از توانایی کانال رادیویی می‌آید، مواجه شود. اگر یک حمله کننده یک ping flood را از یک بخش اترنت سریع بفرستد، می‌تواند به راحتی ظرفیت یک نقطه دسترسی را اشغال کند. با استفاده از آدرس‌های broadcast امکان اشغال چندین نقطه دسترسی متصل به هم وجود دارد. حمله کننده همچنین می‌تواند ترافیک را به شبکه رادیویی بدون اتصال به یک نقطه دسترسی بی‌سیم تزریق کند. 802.11 طوری طراحی شده است که به چندین شبکه اجازه به اشتراک گذاری یک فضا و کانال رادیویی را می‌دهد. حمله کنندگانی که می‌خواهند شبکه بی‌سیم را از کار بیاندازند، می‌توانند ترافیک خود را روی یک کانال رادیویی ارسال کنند و شبکه مقصد ترافیک جدید را با استفاده از مکانیسم CSMA/CA تا آنجا که می‌تواند می‌پذیرد. مهاجمان بداندیش که فریم‌های ناسالم می‌فرستند نیز ظرفیت محدود را پر می‌کنند. همچنین ممکن است مهاجمان تکنیک‌های تولید پارازیت رادیویی را انتخاب کنند و اقدام به ارسال اطلاعات با نویز بالا به شبکه‌های بی‌سیم مقصد کنند.

بارهای بزرگ ترافیک الزاماً با نیات بدخواهانه تولید نمی‌شوند. انتقال فایل‌های بزرگ یا سیستم client/server ترکیبی ممکن است مقادیر بالایی از دیتا روی شبکه ارسال کنند. اگر تعداد کافی کاربر شروع به گرفتن اندازه‌های بزرگی از دیتا از طریق یک نقطه دسترسی کنند، شبکه شبیه سازی دسترسی dial-up را آغاز می‌کند.

راه حل شماره۴: دیدبانی شبکه

نشان یابی مسائل کارایی با دیدبانی و کشف آن‌ها آغاز می‌شود. مدیران شبکه بسیاری از کانال‌ها را برای کسب اطلاعات در مورد کارایی در اختیار دارند: از ابزارهای تکنیکی خاص مانند SNMP (Simple Network Management Protocol) گرفته تا ابزارهای بالقوه قوی غیرفنی مانند گزارش‌های کارایی کاربران. یکی از مسائل عمده بسیاری از ابزارهای تکنیکی، فقدان جزئیات مورد نیاز برای درک بسیاری از شکایت‌های کاربران در مورد کارایی است. آنالایزرهای شبکه‌های بی‌سیم می‌توانند با گزارش دهی روی کیفیت سیگنال و سلامت شبکه در مکان کنونی خود، کمک باارزشی برای مدیر شبکه باشند. مقادیر بالای ارسال‌های سرعت پایین می‌تواند بیانگر تداخل خارجی یا دور بودن یک ایستگاه از نقطه دسترسی باشد. توانایی نشان دادن سرعت‌های لحظه‌ای روی هر کانال، یک تصویر بصری قوی از ظرفیت باقی مانده روی کانال می‌دهد که به سادگی اشغال کامل یک کانال را نشان می‌دهد. ترافیک مفرط روی نقطه دسترسی می‌تواند با تقسیم ناحیه پوشش نقطه دسترسی به نواحی پوشش کوچک‌تر یا با اعمال روش شکل دهی ترافیک در تلاقی شبکه بی‌سیم با شبکه اصلی تعیین شود.

در حالیکه هیچ راه حل فنی برای آسیب پذیری‌های ناشی از فقدان تأیید هویت فریم‌های کنترل و مدیریت وجود ندارد، مدیران می‌توانند برای مواجهه با آن‌ها گام‌هایی بردارند. آنالایزرها اغلب نزدیک محل‌های دردسرساز استفاده می‌شوند تا به تشخیص عیب کمک کنند و به صورت ایده آل برای مشاهده بسیاری از حملات DoS کار گذاشته می‌شوند. مهاجمان

می‌توانند با تغییر دادن فریم‌های 802.11 با استفاده از یکی از چندین روش معمول واسط‌های برنامه نویسی 802.11 موجود، از شبکه سوءاستفاده کنند. حتی یک محقق امنیتی ابزاری نوشته است که پیام‌های قطع اتصال فرستاده شده توسط نقاط دسترسی به کلاینت‌ها را جعل می‌کند. بدون تأیید هویت پیام‌های قطع اتصال بر اساس رمزنگاری، کلاینت‌ها به این پیام‌های جعلی عمل می‌کنند و اتصال خود را از شبکه قطع می‌کنند. تا زمانی که تأیید هویت به صورت یک فریم رمزشده استاندارد درنیاید، تنها مقابله علیه حملات جعل پیام، مکان یابی حمله کننده و اعمال عکس العمل مناسب است.

۹-۲-۴- سه روش امنیتی در شبکه‌های بی‌سیم

- WEP (Wired Equivalent Privacy)

در این روش از شنود کاربرهایی که در شبکه مجوز ندارند جلوگیری به عمل می‌آید که مناسب برای شبکه‌های کوچک بوده زیرا نیاز به تنظیمات دستی (KEY) مربوطه در هر Client می‌باشد.

اساس رمز نگاری WEP بر مبنای الگوریتم RC4 بوسیله RSA می‌باشد.

- SSID (Service Set Identifier)

شبکه‌های WLAN دارای چندین شبکه محلی می‌باشند که هر کدام آن‌ها دارای یک شناسه (Identifier) یکتا می‌باشند این شناسه‌ها در چندین Access Point قرار داده می‌شوند. هر کاربر برای دسترسی به شبکه مورد نظر بایستی تنظیمات شناسه SSID مربوطه را انجام دهد.

- MAC (Media Access Control)

لیستی از MAC آدرس‌های مورد استفاده در یک شبکه به AP (Access Point) مربوطه وارد شده بنابراین تنها کامپیوترهای دارای این MAC آدرسها اجازه دسترسی دارند به عبارتی وقتی یک کامپیوتر درخواستی را ارسال می‌کند MAC آدرس آن با لیست MAC آدرس مربوطه در AP مقایسه شده و اجازه دسترسی یا عدم دسترسی آن مورد بررسی قرار می‌گیرد.این روش امنیتی مناسب برای شبکه‌های کوچک بوده زیرا در شبکه‌های بزرگ امکان ورود این آدرسها به AP بسیار مشکل می‌باشد.

۹-۲-۵- امن سازی شبکه‌های بی‌سیم

با وجود امکاناتی که در شبکه‌های مبتنی بر 802.11 ارائه شده است ولی این واقعیت وجود دارد که، چون برای انتقال اطلاعات در این شبکه‌ها هیچ حد و مرز فیزیکی وجود ندارد و این ترافیک توسط هوا منتقل می‌شود به این دلیل این نوع شبکه ذاتاً نا امن هستند.

از تمام عناصری که برای ایجاد امنیت در شبکه سیم کشی شده استفاده شده می‌توان در شبکه‌های بی‌سیم نیز برای برقراری امنیت استفاده نمود. نکته مهمی که در شبکه‌های بی‌سیم از لحاظ امنتی دارای اهمیت می‌باشد طراحی این گونه از شبکه‌های می‌باشد. در ادامه به چگونگی طراحی امن شبکه‌های بی‌سیم می‌پردازیم.

طراحی شبکه

یکی از موارد مهم که در طراحی شبکه می‌بایست در نظر گرفته شود، چگونگی طراحی و نحوه ارتباط با شبکه سیم کشی شده است.

راه‌های زیادی جهت امن کردن شبکه و همین طور برای به خطر انداختن امنیت آن وجود دارد.

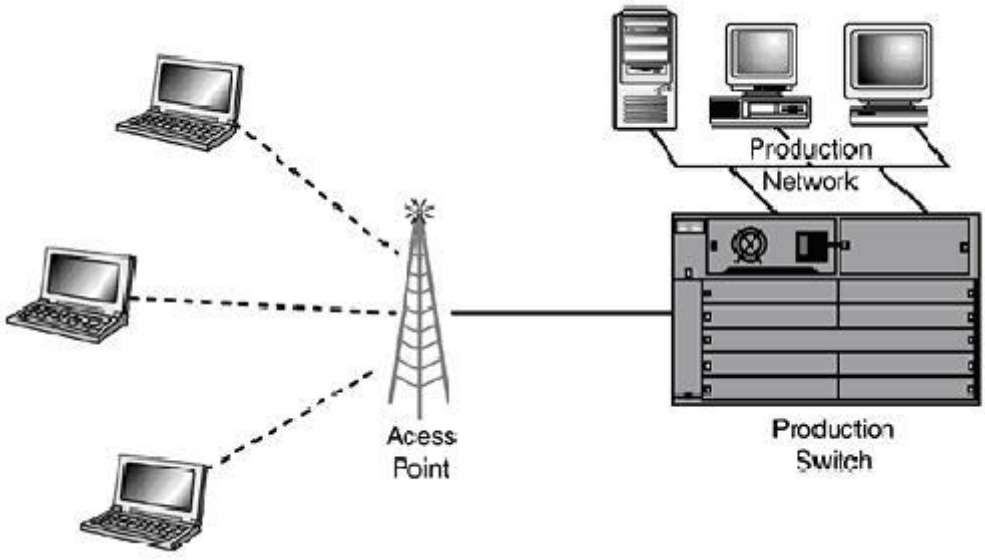
با طراحی و بکار گیری یک استراتژی محکم در شبکه‌های بی‌سیم می‌توان از دسترسی هکرها به شبکه جلوگیری بعمل آورد همچنین با اعمال کنترل‌های بیشتر روی بخش بی‌سیم شبکه، شبکه سیم کشی شده را نیز محافظت نمود تا هکرها از این طریق نیز نتوانند وارد شبکه شوند. استفاده از فایروال و روتر در شبکه بی‌سیم همانند شبکه‌های سیم کشی شده نیز توصیه می‌شود.

جداسازی توسط مکانیزم‌های جداسازی

به دلیل اینکه معمولاً APها رابط بین شبکه بی‌سیم و سیم کشی شده هستند، ایستگاه‌های کاری موجود در دو طرف این APها معمولاً در یک Broadcast Domain می‌باشند. با این توضیحات، هکر شبکه بی‌سیم می‌تواند با استفاده از روشهای موجود روی شبکه‌های سیم کشی شده مانندARP cache Poisoning نسبت به اجرای Exploit روی ترافیک Broadcast اقدام نماید. همچنین هکر می‌تواند ایستگاه‌های بی‌سیم دیگری را که به AP متصل هستند را مورد حمله قرار دهد. این اتفاق در مورد ایستگاه‌های کاری موجود روی شبکه سیم کشی شده که به شبکه بی‌سیم متصل هستند روی خواهد داد.

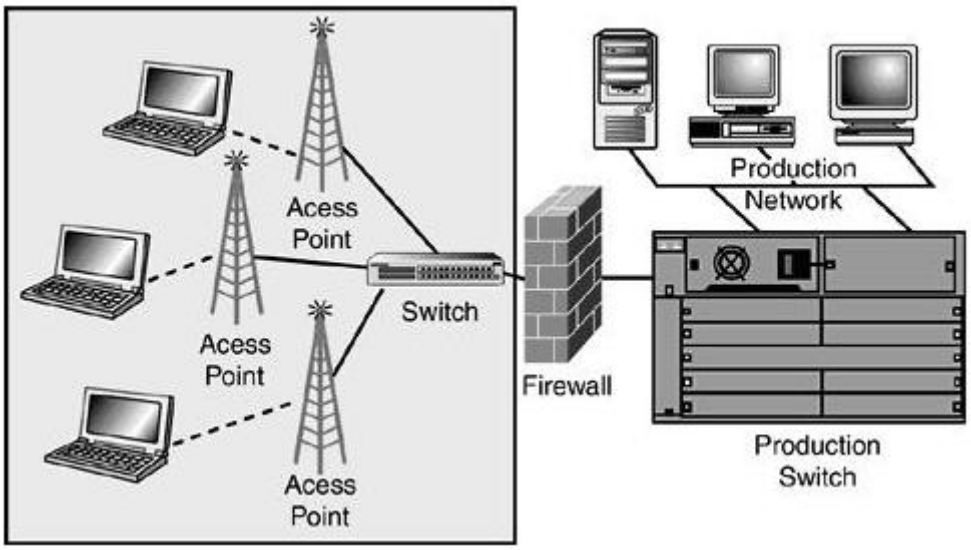
به دلیل آسیب پذیری‌های زیادی که در شبکه‌های بی‌سیم و با توجه به نحوه پیاده سازی این شبکه‌ها، این فکر در ذهن ایجاد می‌شود که شبکه‌های سیم کشی ایزوله شده از این شبکه‌ها امن‌تر می‌باشند.

همانطوری که در شکل زیر مشاهده می‌شود، طراحی ساده ولی با یک نکته اصلی و آن اینکه، در این طرح، دسترسی مستقیم لایه ۲ و اتصال به منابع شبکه برای تمامی ایستگاه‌های کاری بی‌سیم میسر می‌شود و این امر مشکلات امنیتی را در پی خواهد داشت. حداقل پیشنهادی که برای امنیت در این طرح مورد نظر می‌باشد، جدا سازی و ایزوله کردن شبکه بی‌سیم از شبکه داخلی در VLAN جداگانه و با قرار دادن مکانیزم‌های لایه ۳ در شبکه می‌باشد.

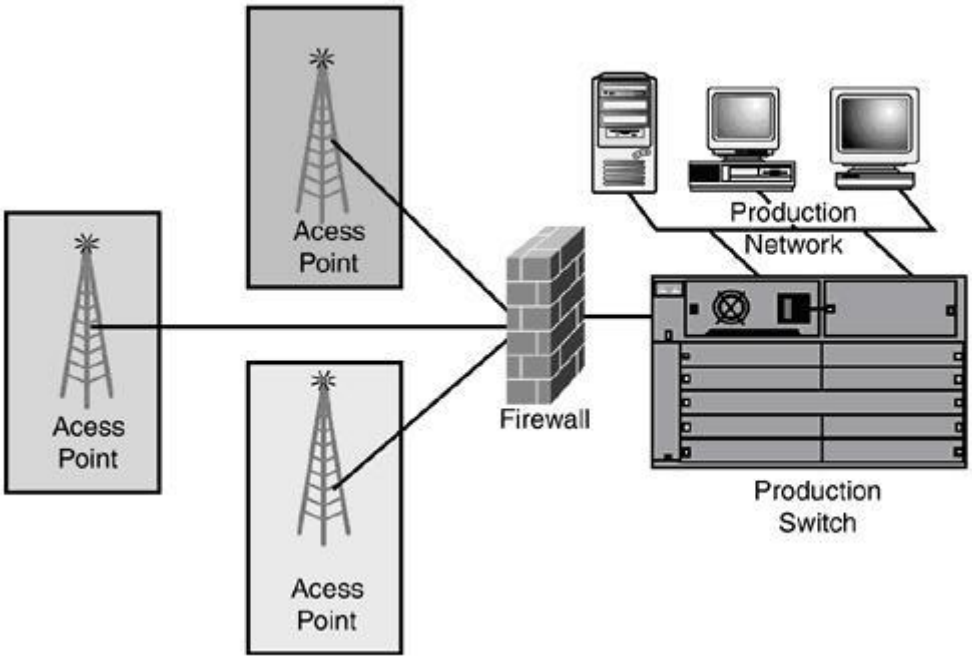


طراحی بهتر شبکه با درک مفهوم Wireless-DMZ که در شکل زیر نشان داده شده است انجام خواهد شد. با قرار دادن APها در ناحیه امنیت خاص، پیاده سازی کنترل‌های لایه۳ و کنترل‌های دسترسی مانند پیاده سازی فایروال می‌توان به امنیت بالاتری دست یافت.

به طور مثال اگر تمام APها به یک سوئیچ (یا دو سوئیچ برای افزونگی (Redundancy)) متصل و سپس سوئیچ به فایروال متصل شود، ما یک نقطه کنترلی یا Layer 3+ بین شبکه داخلی و شبکه AP خواهیم داشت.



با توجه به شبکه فوق، اگر هکری ایستگاه‌های بی‌سیم و یا حتی APها را تحت کنترل خود در آورد، محدود به شبکه خود (شبکه خارج از فایروال) و به سرویسهایی که در فایروال باز گذاشته شده می‌باشد. بعلاوه هرگونه ترافیک ورودی و خروجی در فایروال ثبت شده و بدین ترتیب ما رد ممیزی حتی و با بررسی این گزارشات شانس بیشتری برای جلوگیری از حملات خواهیم داشت. و اگر APها دارای رده امنیت مختلفی باشند می‌توان هرکدام را در ناحیه امنیتی خود قرار داده و به فایروال مربوطه با چند Interface مطابق شکل زیر متصل نمود. با این طرح منابع هرکدام از شبکه‌های بی‌سیم در مقابل شبکه‌های دیگر محافظت می‌شود.



محافظت در برابر ضعف‌های ساده

ساختار شبکه‌های بی‌سیم، اصولا نسبت به حملات ضعف دارد.بدین صورت که دسترسی به اطلاعات شبکه بی‌سیم را از طریق APها و حتی شبکه‌های مبتنی بر سیم متصل به آن را، به حمله کننده می‌دهد. از حملات متداول، دسترسی لایه ۲ حمله کننده به شبکه بدون نفوذ فیزیکی به شبکه می‌باشد. برای جلوگیری از این ضعف امواج 802.11، می‌بایست قرار گیری APها و جهت آنتن‌های آن‌ها را طوری طراحی کرد تا دامنه امواج آن محدود به شبکه داخلی داشته باشد. همچنین استفاده از پنجره‌ها و دیوارهای عایق بندی شده به ضعیف کردن امواج خروجی کمک می‌کند یا می‌توان محلی را که امواج درآن نقطه ارسال می‌شود را جزو محدوده کنترلی شبکه و به صورت فیزیکی کنترل نمود. واضح است که هرچه دسترسی از شبکه عمومی به شبکه محلی کمتر و محدودتر باشد، شبکه از امنیت بالاتری برخوردار می‌باشد.

کنترل در برابر حملات DoS

این حمله باعث کند شدن، از کار افتادن سرویس بی‌سیم (بسته به نوع طراحی شبکه) و یا تاثیر روی شبکه اصلی خواهد شد. بیشتر شرکت‌ها، دستگاه‌های ردیاب این نوع از حملات را ندارند اگر چه امروزه نرم‌افزارهایی برای این کار در دسترس می‌باشد مانند Airmagnet. جدا سازی DoS از شبکه داخلی با استفاده از فایروال یا دستگاه‌های دیگری که دارای این قابلیت هستند نیز می‌تواند در مقابله با حمله DoS موثر باشد. کنترل‌های QoS می‌تواند در لبه wireless DMZ پیاده سازی شود حس گرهای IDS می‌بایست در نقطه ارتباط بین شبکه بی‌سیم و شبکه مبتنی بر سیم قرارگیرد و در نهایت روشی کامل برای جلوگیری ازDoS وجود ندارد و طراحی درست با در نظر گرفتن موارد امنیتی می‌تواند خطر این نوع حمله را کاهش دهد.

رمزنگاری شبکه بی‌سیم

اگرچه در شبکه‌های سیم کشی شده از رمزنگاری در لایه ۱و۲ استفاده نمی‌شود ولی طراحان ۸۰۲.۱۱ نوعی مکانیزم رمزنگاری را جهت امکان تشخیص هویت و رمزنگاری را بین دو ایستگاه کاری روی لایه ۱و۲ فراهم ساخته‌اند.

رمزنگاری بی‌سیم به معنی محافظت و محدود کردن دسترسی به منابع و ساختار شبکه بی‌سیم می‌باشد این کار برای محافظت در برابر خاصیت بی‌سیم است که از دیوار و سایر موانع فیزیکی عبور می‌کند. حمله کننده براحتی می‌تواند به شبکه بی‌سیم که سیستم‌های کد گذاری و محدودیت‌های دسترسی پیاده سازی نشده راه پیدا کند. در شناسایی‌های به عمل آمده در سال ۲۰۰۱ در Boston از هر ۱۰۰ شبکه بی‌سیم ۴۴ شبکه با سیستم‌های رمزنگاری پیاده سازی شده‌اند.

به خاطر داشته باشید که پیاده سازی هرنوع رمزنگاری از نداشتن آن بهتر است.

واضح است که اگرحمله کننده‌ای با دو شبکه که یکی دارای رمزنگاری ضعیف و دیگری بدون رمزنگاری باشد مواجه باشد، به شبکه‌ای که بدون رمزنگاری است حمله خواهد کرد.

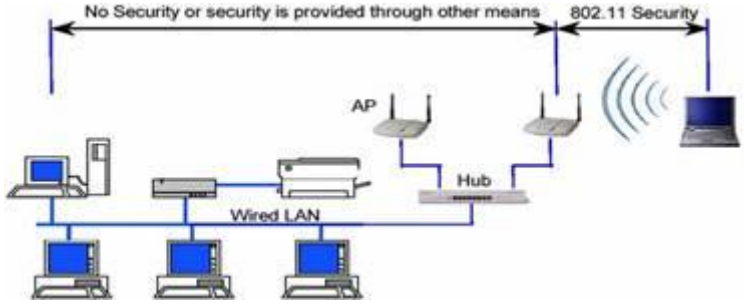
(Wired equivalent privacy) WEP

از بخشهای مهم امن کردن شبکه بی‌سیم، استفاده از الگوریتم مناسب رمزنگاری برای محافظت از اطلاعاتی است که در هوا منتشر می‌شود. WEP برای امن کردن ارتباط بین کارت شبکه‌های بی‌سیم و APها، بوجود آمد. ویرایش اصلی آن قابلیت پشتیبانی از کلیدهای ۴۰ بیتی یا ۶۴ بیتی را داشت که در ویرایش‌های بعدی (WEP2) پشتیبانی ۱۲۸ بیتی نیز به آن اضافه گردید. WEP ازالگوریتم RC4 برای رمزنگاری استفاده میکند که خود دارای ضعف‌هایی نیز می‌باشد و حمله کننده می‌تواند

با بکارگیری روش‌ها و نرم‌افزارهای خاص، نظیرWEP crack و Air Snort برای رمزگشایی آن‌ها استفاده نماید.اگر چه WEP دارای ضعف‌هایی می‌باشد، همچنان استفاده می‌شود. اگرWEP تنها انتخاب شما برای رمزنگاری می‌باشد بهتر است که از آن استفاده نمایید و شبکه بدون رمزنگاری را پیاده سازی نکنید. بعضی از سازندگان تجهیزات بی‌سیم، با اضافه کردن LEAP، که یک پروتکل تشخیص هویت می‌باشد، به WEP و استفاده در تجهیزات خود، ضعف WEP را پوشش داده‌اند.

۹-۲-۶- قابلیت‌ها و ابعاد امنیتی استاندارد ۸۰۲.۱۱

استاندارد 802.11 سرویس‌های مجزا و مشخصی را برای تأمین یک محیط امن بی‌سیم در اختیار قرار می‌دهد. این سرویس‌ها اغلب توسط پروتکل WEP (Wired Equivalent Privacy) تأمین می‌گردند و وظیفه‌ی آن‌ها امن‌سازی ارتباط میان مخدوم‌ها و نقاط دسترسی بی‌سیم است. درک لایه‌یی که این پروتکل به امن‌سازی آن می‌پردازد اهمیت ویژه‌یی دارد، به عبارت دیگر این پروتکل کل ارتباط را امن نکرده و به لایه‌های دیگر، غیر از لایه‌ی ارتباطی بی‌سیم که مبتنی بر استاندارد 802.11 است، کاری ندارد. این بدان معنی است که استفاده از WEP در یک شبکه‌ی بی‌سیم به‌معنی استفاده از قابلیت درونی استاندارد شبکه‌های محلی بی‌سیم است و ضامن امنیت کل ارتباط نیست زیرا امکان قصور از دیگر اصول امنیتی در سطوح بالاتر ارتباطی وجود دارد. شکل زیر محدوده‌ی عمل کرد استانداردهای امنیتی 802.11 (خصوصاً WEP) را نشان می‌دهد.



در حال حاضر عملاً تنها پروتکلی که امنیت اطلاعات و ارتباطات را در شبکه‌های بی‌سیم بر اساس استاندارد 802.11 فراهم می‌کند WEP است. این پروتکل با وجود قابلیت‌هایی که دارد، نوع استفاده از آن همواره امکان نفوذ به شبکه‌های بی‌سیم را به نحوی، ولو سخت و پیچیده، فراهم می‌کند. نکته‌یی که باید به‌خاطر داشت این‌ست که اغلب حملات موفق صورت گرفته در مورد شبکه‌های محلی بی‌سیم، ریشه در پیکربندی ناصحیح WEP در شبکه دارد. به عبارت دیگر این پروتکل در صورت پیکربندی صحیح درصد بالایی از حملات را ناکام می‌گذارد، هرچند که فی‌نفسه دچار نواقص و ایرادهایی نیز هست.

بسیاری از حملاتی که بر روی شبکه‌های بی‌سیم انجام می‌گیرد از سویی است که نقاط دسترسی با شبکه‌ی سیمی دارای اشتراک هستند. به عبارت دیگر نفوذگران بعضاً با استفاده از راه‌های ارتباطی دیگری که بر روی مخدوم‌ها و سخت‌افزارهای بی‌سیم، خصوصاً مخدوم‌های بی‌سیم، وجود دارد، به شبکه‌ی بی‌سیم نفوذ می‌کنند که این مقوله نشان دهنده‌ی اشتراکی هرچند جزءیی میان امنیت در شبکه‌های سیمی و بی‌سیم‌بی‌ست که از نظر ساختاری و فیزیکی با یکدیگر اشتراک دارند.

سه قابلیت و سرویس پایه توسط IEEE برای شبکه‌های محلی بی‌سیم تعریف می‌گردد:

Authentication

هدف اصلی WEP ایجاد امکانی برای احراز هویت مخدوم بی‌سیم است. این عمل که در واقع کنترل دسترسی به شبکه‌ی بی‌سیم است. این مکانیزم سعی دارد که امکان اتصال مخدوم‌هایی را که مجاز نیستند به شبکه متصل شوند از بین ببرد.

Confidentiality

محرمانه‌گی هدف دیگر WEP است. این بُعد از سرویس‌ها و خدمات WEP با هدف ایجاد امنیتی در حدود سطوح شبکه‌های سیمی طراحی شده است. سیاست این بخش از WEP جلوگیری از سرقت اطلاعات در حال انتقال بر روی شبکه‌ی محلی بی‌سیم است.

Integrity

هدف سوم از سرویس‌ها و قابلیت‌های WEP طراحی سیاستی است که تضمین کند پیام‌ها و اطلاعات در حال تبادل در شبکه، خصوصاً میان مخدوم‌های بی‌سیم و نقاط دسترسی، در حین انتقال دچار تغییر نمی‌گردند. این قابلیت در تمامی استانداردها، بسترها و شبکه‌های ارتباطاتی دیگر نیز کم و بیش وجود دارد.

WiFi -۳-۹

۹-۳-۱- مقدمه

شبکه‌های بی‌سیم از دیر باز از امواخ رادیویی برای انتقال سیگنال‌ها سود می‌بردند در این قبیل از شبکه‌ها یک قطعه سخت‌افزاری اطلاعات را به امواج رادیویی تبدیل میکند و سپس آن‌ها را از طریق انتن‌های موجود در شبکه ارسال می‌کند اما در طرف دیگر یک دریافت کنند ه بدون سیم مستقر است تا با دریافت سیگنال‌های ارسالی و تبدیل آن‌ها به اطلاعات و رمزگشایی اطلاعات آن‌ها را به داده‌های قابل فهم برای رایانه تبدیل کند.یکی از راه‌های ارسال داده‌ها در سیتم‌های بی‌سیم استفاده از تکنولوژی WiFi می‌باشد که به تازگی در شبکه‌ها به وجود آمده است و مراحل پیشرفت خود را به تازگی آغاز نموده است.

۹-۳-۲- WiFi چیست؟

WiFi که مخفف عبارت Wireless Fidelity است، یک تکنولوژی ارتباطات بی‌سیم یا همون wireless می‌باشد که مزایای بسیار و معایب کمی دارد. شبکه‌های محلی بی‌سیم WLAN که تحت پوشش مجوعه استانداردهای IEEE 802.11 فعال می‌باشند را WiFi می‌نامند.

اما در حقیقت طیف گسترده تری از استانداردهای WLAN محسوب می‌شود که شامل 802.11a و ظهور سریع استاندارد 802.11g می‌شود. این استاندارد توسط اتحادیه سازگاری اترنت بی‌سیم (WECA) به ثبت رسیده است. WiFi تا حدود ۱۰۰ فوت (۳۰/۵ متر) تمام جهت‌ها را تحت پوشش قرار می‌دهد هر چند دیوارها و منابع ممکن است این محدوده را کاهش دهد. برای مکآن‌های بزرگتر باید از تقویت کنندههای سیگنال برای افزایش این محدوده استفاده کرد. مهمترین مزیت WiFi سادگی آن است. در این مدل حداکثر سرعت انتقال اطلاعات 11Mbps است و از فرکانس رادیویی ۲/۴ گیگاهرتز استفاده می‌کند. برای سرعت بخشیدن به این استاندارد مدل دیگری نیز به نام 802.11b+ ایجاد شده که سرعت انتقال را تا 22mbps افزایش می‌دهد. در مدل 802.11a سرعت اطلاعات حدود 54Mbps است و از فرکانس 5GHz استفاده می‌شود.

به طور حتم این مدل در آینده‌ای نه چندان دور جای 802.11b را خواهد گرفت. به زبانی ساده، سیستم WiFi را می‌توان به یک جفت واکی - تاکی که شما از آن برای مکالمه با دوستان خود استفاده می‌کنید تشبیه نمود. این لوازم، رادیوهای کوچک و ساده‌ای هستند که قادرند تا سیگنال‌های رادیویی را ارسال و دریافت نمایند. هنگامی که شما بوسیله آن‌ها صحبت می‌کنید، میکروفون دستگاه، صدای شما را دریافت نموده و با تلفیق آن با امواج رادیویی، از طریق آنتن آن‌ها را ارسال می‌کند. در طرف دیگر، دستگاه مقصد، با دریافت سیگنال ارسال شده از طرف شما توسط آنتن، آن‌ها را آشکار سازی نموده و از طریق بلندگوی دستگاه، صدای شما را پخش خواهد کرد. توان خروجی و یا قدرت فرستنده این گونه لوازم اغلب در حدود یک چهارم وات است و با این وصف، برد آن‌ها چیزی در حدود ۵۰ تا ۱۰۰ متر می‌رسد.

در تکنولوژی WiFi این امکان فراهم شده که طیف رادیویی موجود را بتوان بین تعداد زیادی و متنوعی از گیرندهها و فرستنده‌ها توزیع کرد و همه آن‌ها نیز قابلیت در یافت سیگنال ارسالی را داشته باشند.

۹-۳-۳- چرا WiFi را بکار گیریم؟

نیروی کاری امروزه که با دستیارهای شخصی دیجیتالی (PDAها)، لپ‌تاب‌ها و دیگر وسایل متحرک (موبایل) تجهیز شده‌اند، تقاضای دسترسی به شبکهء شما را از هر کجا که باشند، بدون دردسر یک شبکه ثابت، می‌نمایند WiFi .به کار و تجارت شما اجازه میدهد که یک شبکه را سریعتر و با هزینه پایین‌تر و با انعطاف پذیری بیشتر نسبت به سیستم با سیم، بکار گیرید . سودمندی WiFi نیز افزایش می‌یابد، از آنجائیکه کارمندان می‌توانند مدت زیادتری به یک شبکه متصل بوده، و قادر خواهند بود که با همکارانشان در زمان و مکانی که نیاز باشد کار نمایند .

شبکه‌های WiFi نسبت به شبکه‌های باسیم روان‌تر می‌باشند. یک شبکه دیگر بیش از این یک چیز ثابت نمی‌باشد، شبکه‌ها می‌توانند در یک بعداظهر ایجاد یا از هم باز شوند بجای اینکه روزها یا هفته‌ها نیاز به ایجاد یک شبکهء کابلی ساختار یافته باشد . این شبکه‌ها می‌توانند دارای کابردهای خانگی، اداری یا صنعتی باشند که نمونه‌هایی از آن‌ها را می‌توان به شرح زیر نام برد:

۱.- شبکه‌های توزیع اینترنت در مکان‌های عمومی مانند فرودگاه‌ها، مراکز تجاری و... (Hot Spot)

۲- شبکه‌های محلی بی‌سیم در شرکت‌ها و ادارات با هدف انتقال اطلاعات (Data)

۳-. شبکه‌های محلی بی‌سیم با هدف انتقال مکالمات صدا (VOIP)

٤-شبکه‌های محلی بی‌سیم با هدف انتقال تصویر (CCTV , Video Conference)

۵.- شبکه‌های محلی بی‌سیم با هدف استفاده در سیستم‌های امنیتی (Security)

۹-۳-۴- WiFi چگونه کار می‌کند؟

فناوری WiFi یا ۸۰۲.۱۱ بسیار شبیه به گوشی تلفن دیجیتال بی‌سیم کار می‌کند.میکروفون موجود در گوشی صدای شما را می‌گیرد و پردازنده درونی این گوشی این صدا را به یک سیگنال دیجیتال تبدیل می‌کند که سپس به دستگاه پایه انتقال می‌یابد. دستگاه پایه به نوبه خود داده‌هایی که از خط تلفن می‌اید می‌گیرد و یک تبدیل مشابه انجام میدهد و سیگنا حاصل را به گوشی می‌فرستد.این ارتباط دو طرفه پیوسته تا حدودی به ملیات یک شبکه بی‌سیم شباهت دارد.یک دستگاه WAP (نقطه

دست بی‌سیم) یا دستگاه مسیر یابی بی‌سیم را می‌توانید همان دستگاه پایه گوشی تلفن و کارتهای شبکه بی‌سیم را خود گوشی در نظر بگیرید. WAP یا مسیر یاب رابط با سیم به یک شبکه باسیم موجود یا به یک مودم باند عریض است و با استفاده از سیگنالهای رادیویی با کارتهای شبکه بی‌سیم نصب شده در کامپیوترهای شما ارتباط بر قرار می‌کنند.

برای درک بهتر و ساده یک شبکه بی‌سیم یک جفت دستگاه رادیویی ترانزیستوری کوچک (walkie-talkie) پنج دلاری در نظر بگیرید. پیوند بی‌سیم بین کارتهای نصب شده در کامپیوترهای شما و مسیریاب WAP نیاز به کابلهای اترنت را بر طرف می‌کند. واکی تاکی دستگاه رادیویی کوچک است که می‌تواند سیگنا لهای رادیویی را ارسال و دریافت کند.زمانی که شما با این دستگاه صحبت می‌کنید صدای شما توسط میکروفن در یافت می‌شود و رد یک فرکانس رادیویی کد گذاری می‌شود و توسط آنتن ارسال می‌شود.

یک رادیوی مشابه دیگر می‌تواند این مخابره را به وسیله آنتن خود دریافت کند رمز صدای شما را از سیگنا رادیویی بردارد و صدا را توسط بلندگو بشنود.چنین دستگاه‌های مخابره ساده‌ای سیگنال‌هایی با قدرت ۰/۲۵ وات ارسال می‌کند و می‌توانند تا حدود ۵۰۰ تا ۱۰۰۰ فوت مخابره کنند. تصور کنید که می‌خواهید دو کامپیوتر را در شبکه با استفاده از این تکنولوژی به یکدیگر متصل کنید.این سیستم کار خواهد کرد اما سرعت انتقال اطلاعات بسیار کند است. یک دستگاه کوچک پنج دلاری برای صدای انسان طراحی شده است بنابراین شما نمی‌توانبد اطلاعات بسیار زیادی را با استفاده از این روش ارسال کنید.



برای استفاده از این سیستم ایستگاه‌هایی به نام Access Point در مناطق مختلف و به فواصل چند صد متری قرار می‌گیرد. این ایستگاه‌ها امواج رادیویی را در هوا منتشر می‌کنند و هر کامپیوتری که به WiFi مجهز باشد و در محدوده این ایستگاه‌ها قرار داشته باشد قادر به استفاده از اینترنت است و کاربران با قرار دادن یک کارت سخت‌افزاری IEEE802.11b و یا وصل کردن یک دستگاه WiFi اکسترنال از طریق USB به کامپیوتر خود قادر به استفاده از این سیستم هستند. قیمت اینترنت در این سیستم بسیار مناسب است. مثلاً در کشور آمریکا یک Account نامحدود یک ماهه با این سرویس به مبلغ ۲۰ تا ۳۰ دلار در اختیار کاربران قرار می‌گیرد. از نظر برد موثر هم حداکثر تا ۱۵۰ متر اطراف Access Point مورد پوشش قرار می‌گیرد. در این حالت سرعت انتقال ارتباط 1mbps است. البته هر چقدر فاصله کاربر با ایستگاه اصلی کمتر از ۱۵۰ متر باشد سرعت انتقال اطلاعات بیشتر خواهد شد. مثلاً سرعت انتقال اطلاعات در فاصله ۱۰۰ متری mbps5.5، در فاصله ۸۰ متری 8mbps و در فاصله ۵۰ متری و کمتر از آن 11mbps است.

اتصال به WiFi

یکی از مهمترین مزایای WiFi سادگی آن است. در بسیاری از لپ‌تاب‌های جدید یک کارت WiFi قرار دارد و در بیشتر موارد نیازی نیست تا شما برای شروع استفاده از WiFi کاری انجام دهید. همچنین اضافه کردن کارت به لپ تاب‌های قدیمی‌تر یا یک کامپیوتر رومیزی بسیار آسان است.

Hotspot یک نقطه ارتباطی برای شبکه WiFi است. Hotspot یک جعبه کوچک است که حاوی یک کارت ۸۰۲/۱۱ است و می‌تواند به طور همزمان با بیشتر از صد کارت ۸۰۲/۱۱ ارتباط بر قرار کند. در حال حاضر تعداد بسیار زیادی از این نقاط ارتباطی WiFi در مکآن‌های عمومی مانند رستورآن‌ها وهتل‌ها و کتابخانه‌ها و فرودگاه‌ها وجود دارد شما همچنین می‌توانید یک Hotspot در منزلتان ایجاد کنید.

در ماشین‌های جدید یک کارت۸۰۲/۱۱ به طور خودکار به یک hotspot 802/11 متصل می‌شود و ارتباط با شبکه برقرار می‌شود. به محض اینکه شما کامپیوترتان را روشن کنید به شبکه متصل می‌شوید و شما می‌توانیدای میل خودتان را چک کنید و با اینترنت کارکنید.در تجهیزات۸۰۲/۱۱ قدیمی خصوصیت جستجوی خوکار وجود ندارد. در این حالت شما باید یک لغت که SSID نامیده می‌شود (معمولا یک کلمه کوتاه حداکثر با ۱۰ کلمه) و شماره کانال که عدد صحیحی بین صفر و یازده است را یافته و این دو را تایپ کند.در مدل‌های جدیدتر که به طور خوکار عمل می‌کنند این دو بخش اطلاعات از سیگنالهای رادیویی تولید شده توسط hotsopt گرفته می‌شودو برای شما نمایش داده می‌شود.

۹-۳-۵- *IEEE 802.11*

امروزه با بهبود عملکرد، کارایی و عوامل امنیتی، شبکه‌های بی‌سیم به شکل قابل توجهی در حال رشد و گسترش هستند و استاندارد IEEE 802.11 استاندارد بنیادی است که شبکه‌های بی‌سیم بر مبنای آن طراحی و پیاده سازی می‌شوند.

802.11 از استانداردهای پیاده سازی شبکه‌های بی‌سیم می‌باشد که توسط IEEE ارائه شده است. این استاندارد شبیه استاندارد 802.3 روی Ethernet گره‌های شبکه بیسم نیز توسط آدرس MAC حک شده روی کارت‌های شبکه آدرس‌دهی می‌شوند. اگر چه 802.11 از سیم به عنوان رسانه در لایه ۱ استفاده نمی‌کند و گره‌ها در استاندارد فوق به صورت بی‌سیم و در دامنه‌ای که توسط دستگاهای بی‌سیم تعریف می‌شوند با یکدیگر تبادل اطلاعات می‌نمایند.

استاندارد ۱۹۹۷، پهنای باند 2Mbps را تعریف می‌کند با این ویژگی که در شرایط نامساعد و محیط‌های دارای اغتشاش (نویز) این پهنای باند می‌تواند به مقدار 1Mbps کاهش یابد. روش تلفیق یا مدولاسیون در این پهنای باند روش DSSS است. بر اساس این استاندارد پهنای باند 1Mbps با استفاده از روش مدولاسیون FHSS نیز قابل دستیابی است و در محیط‌های عاری از اغتشاش (نویز) پهنای باند 2Mbps نیز قابل استفاده است. هر دو روش مدولاسیون در محدوده باند رادیویی 2.4 GHz عمل می‌کنند. یکی از نکات جالب توجه در خصوص این استاندارد استفاده از رسانه مادون قرمز علاوه بر مدولاسیون‌های رادیویی DSSS و FHSS به عنوان رسآن‌هانتقال است. ولی کاربرد این رسانه با توجه به محدودیت حوزه عملیاتی آن نسبتاً محدود و نادر است. گروه کاری ۸۰۲.۱۱ به زیر گروه‌های متعددی تقسیم می‌شود. برخی از مهم‌ترین زیر گروه‌ها به قرار زیر است:

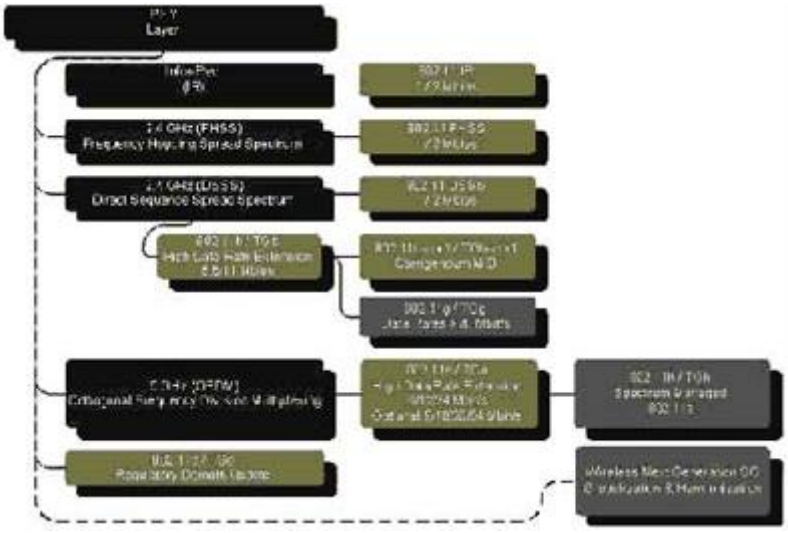
- 802.11D: Additional Regulatory Domains
- **802.11E: Quality of Service (QoS)**

- 802.11F: Inter-Access Point Protocol (IAPP)
- **802.11G: Higher Data Rates at 2.4 GHz**
- 802.11H: Dynamic Channel Selection and Transmission Power Control
- **802.11i: Authentication and Security**

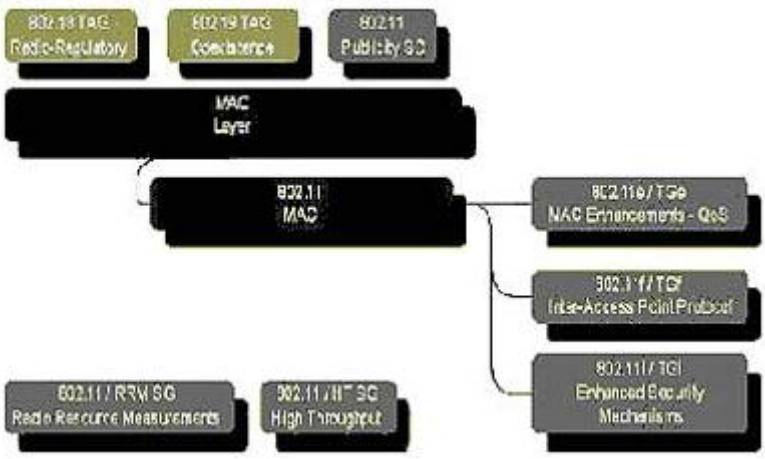
کمیته 802.11e کمیته‌ای است که سعی دارد قابلیت QoS اِترنت را در محیط شبکه‌های بی‌سیم ارائه کند. توجه داشته باشید که فعالیت‌های این گروه تمام گونه‌های ۸۰۲.۱۱ شامل a، b، و g را در بر دارد. این کمیته در نظر دارد که ارتباط کیفیت سرویس سیمی یا Ethernet QoS را به دنیای بی‌سیم بیاورد.

کمیته 802.11g کمیته‌ای است که با عنوان ۸۰۲.۱۱ توسعه یافته نیز شناخته می‌شود. این کمیته در نظر دارد نرخ ارسال داده‌ها در باند فرکانسی ISM را افزایش دهد. باند فرکانسی ISM یا باند فرکانسی صنعتی، پژوهشی، و پزشکی، یک باند فرکانسی بدون مجوز است. استفاده از این باند فرکانسی که در محدوده ۲٤۰۰ مگاهرتز تا ۲٤۸۳.۵ مگاهرتز قرار دارد، بر اساس مقررات FCC در کاربردهای تشعشع رادیویی نیازی به مجوز ندارد. استاندارد 802.11g تا کنون نهایی نشده است و مهم‌ترین علت آن رقابت شدید میان تکنیک‌های مدولاسیون است. اعضاء این کمیته و سازندگان تراشه توافق کرده‌اند که از تکنیک تسهیم OFDM استفاده نمایند ولی با این وجود روش PBCC نیز می‌تواند به عنوان یک روش جایگزین و رقیب مطرح باشد.

کمیته 802.11h مسئول تهیه استانداردهای یکنواخت و یکپارچه برای توان مصرفی و نیز توان امواج ارسالی توسط فرستنده‌های مبتنی بر ۸۰۲.۱۱ است. فعالیت دو کمیته 802.11i و 802.11x در ابتدا برروی سیستم‌های مبتنی بر 802.11b تمرکز داشت. این دو کمیته مسئول تهیه پروتکل‌های جدید امنیت هستند. استاندارد اولیه از الگوریتمی موسوم به WEP استفاده می‌کند که در آن دو ساختار کلید رمز نگاری به طول ٤۰ و ۱۲۸ بیت وجود دارد. WEP مشخصاً یک روش رمزنگاری است که از الگوریتم RC4 برای رمزنگاری فریم‌ها استفاده می‌کند. فعالیت این کمیته در راستای بهبود مسائل امنیتی شبکه‌های محلی بی‌سیم است.



شکل گروه‌های کاری لایه فیزیکی



گروه‌های کاری لایه دسترسی به رسانه

این استاندارد لایه‌های کنترل دسترسی به رسانه (MAC) و لایه فیزیکی (PHY) در یک شبکه محلی با اتصال بی‌سیم را دربردارد.

محیط‌های بی‌سیم دارای خصوصیات و ویژگی‌های منحصر به فردی می‌باشند که در مقایسه با شبکه‌های محلی سیمی جایگاه خاصی را به این گونه شبکه‌ها می‌بخشد. به طور مشخص ویژگی‌های فیزیکی یک شبکه محلی بی‌سیم محدودیت‌های فاصله، افزایش نرخ خطا و کاهش قابلیت اطمینان رسانه، همبندی‌های پویا و متغیر، تداخل امواج، و عدم وجود یک ارتباط قابل اطمینان و پایدار در مقایسه با اتصال سیمی است. این محدودیت‌ها، استاندارد شبکه‌های محلی بی‌سیم را وا می‌دارد که فرضیات خود را بر پایه یک ارتباط محلی و با بُرد کوتاه بنا نهد. پوشش‌های جغرافیایی وسیع‌تر از طریق اتصال شبکه‌های محلی بی‌سیم کوچک برپا می‌شود که در حکم عناصر ساختمانی شبکه گسترده هستند. سیّار بودن ایستگاه‌های کاری بی‌سیم نیز از دیگر ویژگی‌های مهم شبکه‌های محلی بی‌سیم است. در حقیقت اگر در یک شبکه محلی بی‌سیم ایستگاه‌های کاری قادر نباشند در یک محدودهعملیاتی قابل قبول و همچنین میان سایر شبکه‌های بی‌سیم تحرک داشته باشد، استفاده از شبکه‌های محلی بی‌سیم توجیه کاربردی مناسبی نخواهد داشت.

از سوی دیگر به منظور حفظ سازگاری و توانایی تطابق و همکاری با سایر استانداردها، لایه دسترسی به رسانه (MAC) در استاندارد ۸۰۲.۱۱ می‌بایست از دید لایه‌های بالاتر مشابه یک شبکه محلی مبتنی بر استاندارد ۸۰۲ عمل کند. بدین خاطر لایه MAC در این استاندارد مجبور است که سیّاربودن ایستگاه‌های کاری را به گونه‌ای شفاف پوشش دهد که از دید لایه‌های بالاتر استاندارد این سیّاربودن احساس نشود. این نکته سبب می‌شود که لایهMAC در این استاندارد وظایفی را بر عهده بگیرد که معمولاً توسط لایه‌های بالاتر شبکه انجام می‌شوند. در واقع این استاندارد لایه‌های فیزیکی و پیوند داده جدیدی به مدل مرجع OSI اضافه می‌کند و به طور مشخص لایه فیزیکی جدید از فرکانس‌های رادیویی به عنوان رسانه انتقال بهره می‌برد. وجود این دولایه از دید لایه‌های فوقانی شفاف است.

پذیرش استانداردهای WLAN از سوی کاربران

802.11b اولین نسخه‌ای بود که به بازار مصرف رسید و کندترین و ارزان قیمت ترین در بین این سه استاندارد محسوب می‌شود. .تا کنون استاندارد مورد استفاده در شبکه‌های بی‌سیم 802.11b بوده است. محصولات مبتنی بر 802.11b به عنوان اولین استاندارد رایج با مزایایی از قبیل سرعت قابل قبول، قیمت مناسب، سازگاری جهانی، استفاده از طیف فرکانسی 2.4

GHz (که نیازی به مجوز از ارگان‌های دولتی ندارد) و همچنین یکپارچگی محصولات تحت نظارت اتحادیه WiFi همه و همه موجب شده‌اند تا چیزی حدود ۹۵٪ از سهم بازار را به خود اختصاص دهند.

به طور سنتی این استانداردر از دو فنّاوری DSSS یا FHSS استفاده می‌کند. هر دو روش فوق برای ارسال داده با نرخ‌های ۱ و ۲ مگابیت در ثانیه مفید هستند.

جدول زیر سرعت مختلف قابل دسترسی در این استاندارد را نشان می‌دهد.

Bits/Symbol	Symbol Rate	Modulation	Code Length	Data Rate
1	1 MSps	BPSK	11 (Barker Sequence)	1 Mbps
2	1 MSps	QPSK	11 (Barker Seq.)	2 Mbps
4	1.375 MSps	QPSK	8 CCK	5.5 Mbps
8	1.375 MSps	QPSK	8 CCK	11 Mbps

در ایالات متحده آمریکا کمیسیون فدرال مخابرات یا FCC، مخابره و ارسال فرکانس‌های رادیویی را کنترل می‌کند. این کمیسیون باند فرکانس خاصی موسوم به ISM را در محدوده 2.4 GHz تا 2.4835 GHz برای فنّاوری‌های رادیویی استاندارد IEEE تعریف می‌کند.

اثرات فاصله

فاصله از فرستنده برروی کارایی و گذردهی شبکه‌های بی‌سیم تاثیر قابل توجهی دارد. فواصل رایج در استاندارد ۸۰۲.۱۱ با توجه به نرخ ارسال داده تغییر می‌کند و به طور مشخص در پهنای باند 11 Mbps این فاصله ۳۰ تا ٤٥ متر و در پهنای باند 5.5Mbps، 40 تا ٤٥ متر و در پهنای باند 2 Mbps، ۷۵ تا ۱۰۷ متر است. لازم به یادآوری است که این فواصل توسط عوامل دیگری نظیر کیفیت و توان سیگنال، محل استقرار فرستنده و گیرند و شرایط فیزیکی و محیطی تغییر می‌کنند.

در استاندارد 802.11b پروتکلی وجود دارد که گیرنده بسته را ملزم به ارسال بسته تصدیق می‌نماید (رجوع کنید به بخش دسترسی به رسانه). توجه داشته باشید که این مکانیزم تصدیق علاوه بر مکانیزم‌های تصدیق رایج در سطح لایه انتقال (نظیر آنچه در پروتکل TCP اتفاق می‌افتد) عمل می‌کند. در صورتی که بسته تصدیق ظرف مدت زمان مشخصی از طرف گیرنده به فرستنده نرسد، فرستنده فرض می‌کند که بسته از دست رفته است و مجدداً آن بسته را ارسال می‌کند. در صورتی که این وضعیت ادامه یابد نرخ ارسال داده نیز کاهش می‌یابد (Fall Back) تا در نهایت به مقدار 1 Mpbs برسد. در صورتی که در این نرخ حداقل نیز فرستنده بسته‌های تصدیق را در زمان مناسب دریافت نکند ارتباط گیرنده را قطع شده تلقی کرده و دیگر بسته‌ای را برای آن گیرنده ارسال نمی‌کند. به این ترتیب فاصله 802.11b اختصاص داده است. این گزینه نقش مهمی در کارایی (میزان بهره‌وری از شبکه) و گذردهی (تعداد بسته‌های غیرتکراری ارسال شده در واحد زمان) ایفا می‌کند.

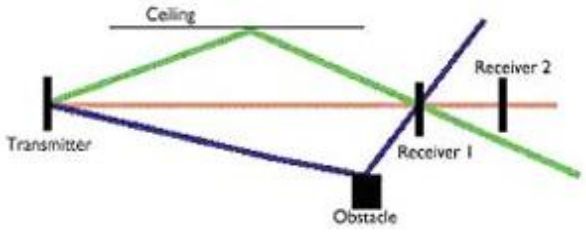
پل بین شبکه‌ای

بر خلاف انتظار بسیاری از کارشناسان شبکه‌های کامپیوتری، پل بین شبکه‌ای یا Bridging در استاندارد 802.11b پوشش داده نشده است. در پل بین شبکه‌ای امکان اتصال نقطه به نقطه (و یا یک نقطه به چند نقطه) به منظور برقراری ارتباط

یک شبکه محلی با یک یا چند شبکه محلی دیگر فراهم می‌شود. این کاربرد به خصوص در مواردی که بخواهیم بدون صرف هزینه کابل کشی (فیبر نوری یا سیم مسی) شبکه محلی دو ساختمان را به یکدیگر متصل کنیم بسیار جذاب و مورد نیاز می‌باشد. با وجود اینکه استاندارد 802.11b این کاربرد را پوشش نمی‌دهد ولی بسیاری از شرکت‌ها پیاده‌سازی‌های انحصاری از پل بی‌سیم را به صورت گسترش و توسعه استاندارد 802.11b ارائه کرده‌اند. پل‌های بی‌سیم نیز توسط مقررات FCC کنترل می‌شوند و گذردهی مؤثر یا به عبارت دیگر توان مؤثر ساطع شده همگرا (EIRP) در این تجهیزات نباید از ٤ وات بیشتر باشد. بر اساس مقررات FCC توان سیگنال‌های ساطع شده در شبکه‌های محلی نیز نباید از ۱ وات تجاوز نماید.

پدیده چند مسیری

شکل زیر پدیده چند مسیری را نشان می‌دهد. در این پدیده مسیر و زمان بندی سیگنال در اثر برخورد با موانع و انعکاس تغییر می‌کند. پیاده سازی‌های اولیه از استاندارد 802.11b از تکنیک FHSS در لایه فیزیکی استفاده می‌کردند. از ویژگی‌های قابل توجه این تکنیک مقاومت قابل توجه آن در برابر پدیده چند مسیری است. در این تکنیک از کانال‌های متعددی (۷۹ کانال) با پهنای باند نسبتاً کوچک استفاده شده و فرستنده و گیرنده به تناوب کانال فرکانسی خود را تغییر می‌دهند. این تغییر کانال هر ٤۰۰ میلی ثانیه بروز می‌کند لذا مشکل چند مسیری به شکل قابل ملاحظه‌ای منتفی می‌شود. زیرا گیرنده، سیگنال اصلی (که سریع‌تر از سایرین رسیده و عاری از تداخل است) را دریافت کرده و کانال فرکانسی خود را عوض می‌کند و سیگنال‌های انعکاسی زمانی به گیرنده می‌رسد که گیرنده کانال فرکانسی قبلی خود را عوض کرده و در نتیجه توسط گیرنده احساس و دریافت نمی‌شوند.



802.11a

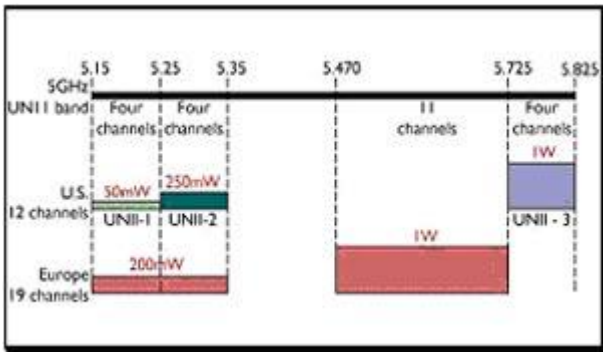
802.11a نسخه بعدی استاندارد 802.11b بود. اولین محصولات مبتنی بر استاندارد 802.11a اوایل سال ۲۰۰۱ به بازار راه یافتند. با وجود استفاده از فرکانس 5GHz و همچنین سرعتی در حدود 54Mbps استقبال چندانی از آ نها نشد. می‌توان دلایل اصلی این عدم استقبال را عدم سازگاری با 802.11b، برد پایین، هزینه بالا، و همچنین استفاده از با ند فرکانسی نیازمند به مجوز نام برد.

استاندارد 802.11a، از باند رادیویی جدیدی برای شبکه‌های محلی بی‌سیم استفاده می‌کند و پهنای باند شبکه‌های بی‌سیم را تا 54 Mbps افزایش می‌دهد. این افزایش قابل توجه در پهنای باند مدیون تکنیک مدولاسیونی موسوم به OFDM است. نرخ‌های ارسال داده در استاندارد IEEE 802.11a عبارتند از:٦، ۹، ۱۲، ۱۸، ۲٤، ۳٦، ٤۸، ٥٤ Mbps که بر اساس استاندارد، پشتیبانی از سرعت‌های ٦، ۱۲، ۲٤ مگابیت در ثانیه اجباری است. برخی از کارشناسان شبکه‌های محلی بی‌سیم، استاندارد IEEE 802.11a را نسل آینده IEEE 802.11 تلقی می‌کنند و حتی برخی از محصولات مانند تراشه‌های Atheros وکارت‌های شبکه PCMCIA/Cardbus محصول Access Inc Card. استاندارد IEEE 802.11a را پیاده‌سازی کرده‌اند. بدون شک این پهنای باند وسیع و نرخ داده سریع محدودیت‌هایی را نیز به همراه دارد. در واقع افزایش پهنای باند در استاندارد

IEEE 802.11a باعث شده است که محدوده عملیاتی آن در مقایسه با IEEE 802.11/b کاهش یابد. علاوه بر آن به سبب افزایش سربارهای پردازشی در پروتکل، تداخل، و تصحیح خطاها، پهنای باند واقعی به مراتب کمتر از پهنای باند اسمی این استاندارد است. همچنین در بسیاری از کاربردها امکان سنجی و حتی نصب تجهیزات اضافی نیز مورد نیاز است که به تبع آن موجب افزایش قیمتِ زیرساختارِ شبکه بی‌سیم می‌شود. زیرا محدوده عملیاتی در این استاندارد کمتر از محدوده عملیاتی در استاندارد IEEE 802.11b بوده و به همین خاطر به نقاط دسترسی یا ایستگاه پایه بیشتری نیاز خواهیم داشت که افزایش هزینه زیرساختار را به دنبال دارد. این استاندارد از باند فرکانسی خاصی موسوم به UNII استفاده می‌کند. این باند فرکانسی به سه قطعه پیوسته فرکانسی به شرح زیر تقسیم می‌شود:

UNII-1 @ 5.2 GHz
UNII-2 @ 5.7 GHz
UNII-3 @ 5.8 GHz

یکی از تصورات غلط در زمینهاستانداردهای ۸۰۲.۱۱ این باور است که 802.11a قبل از 802.11b مورد بهره برداری واقع شده است. در حقیقت 802.11b نسل دوم استانداردهای بی‌سیم (پس از ۸۰۲.۱۱) است و 802.11a نسل سوم از این مجموعه استاندارد به شمار می‌رود. استاندارد 802.11a برخلاف ادعای بسیاری از فروشندگان تجهیزات بی‌سیم نمی‌تواند جایگزین 802.11b شود زیرا لایه فیزیکی مورد استفاده در هریک تفاوت اساسی با دیگری دارد. از سوی دیگر گذردهی (نرخ ارسال داده) و فواصل در هریک متفاوت است.



در شکل فوق این سه ناحیه عملیاتی UNII و نیز توان مجاز تشعشع رادیویی از سوی FCC ملاحظه می‌شود. این سه ناحیه کاری ۱۲ کانال فرکانسی را فراهم می‌کنند. باند UNII-1 برای کاربردهای فضای بسته، باند UNII-2 برای کاربردهای فضای بسته و باز، و باند UNII-3 برای کاربردهای فضای باز و پل بین شبکه‌ای به کار برده می‌شوند. این نواحی فرکانسی در ژاپن نیز قابل استفاده هستند. این استاندارد در حال حاضر در قارهاروپا قابل استفاده نیست. در اروپا HyperLAN2 برای شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد که به طور مشابه از باند فرکانسی 802.11a استفاده می‌کند. یکی از نکات جالب توجه در استاندارد 802.11a تعریف کاربردهای پل سازی شبکه‌ای در کاربردهای داخلی و فضای باز است. در واقع این استاندارد مقررات لازم برای پل سازی و ارتباط بین شبکه‌ای از طریق پل را در کاربردهای داخلی و فضای باز فراهم می‌نماید. در یکی تقسیم بندی کلی می‌توان ویژگی‌ها و مزایای 802.11a را در سه محور زیر خلاصه نمود.

- افزایش در پهنای باند در مقایسه با استاندارد 802.11b (در استاندارد 802.11a حداکثر پهنای باند 54Mbps) می‌باشد.
- استفاده از طیف فرکانسی خلوت (باند فرکانسی 5 GHz)

- استفاده از ۱۲ کانال فرکانسی غیرپوشا (سه محدودهفرکانسی که در هریک ٤ کانال غیرپوشا وجود دارد)

افزایش پهنای باند

استاندارد 802.11a در مقایسه با 802.11b و پهنای باند 11 Mbps حداکثر پهنای باند 54 Mbps را فراهم می‌کند. مهم‌ترین عامل افزایش قابل توجه پهنای باند در این استاندارد استفاده از تکنیک پیشرفته مدولاسیون، موسوم به OFDM است. تکنیکOFDM یک تکنولوژی (فناوری) تکامل یافته و بالغ در کاربردهای بی‌سیم به شمار می‌رود. این تکنولوژی مقاومت قابل توجهی در برابر تداخل رادیویی داشته و تأثیر کمتری از پدیده چند مسیری می‌پذیرد. OFDM تحت عناوین مدولاسیون چند حاملی و یا مدولاسیون چندآهنگی گسسته نیز شناخته می‌شود. این تکنیک مدولاسیون علاوه بر شبکه‌های بی‌سیم در تلویزیون‌های دیجیتال (در اروپا، ژاپن، و استرالیا) و نیز به عنوان تکنولوژی پایه در خطوط مخابراتی ADSL مورد استفاده قرار می‌گیرد.

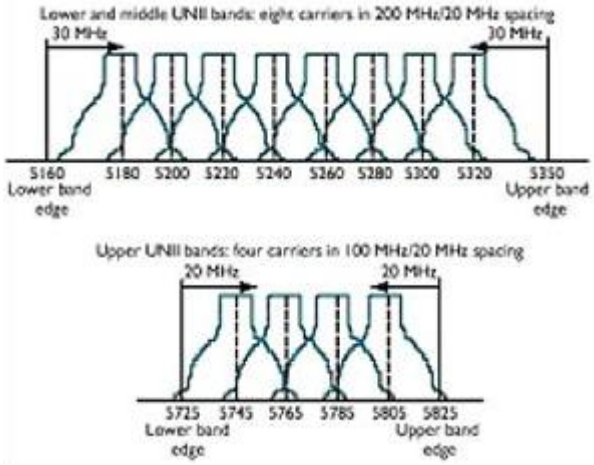
تکنیک OFDM از روش QAM و پردازش سیگنال‌های دیجیتال استفاده کرده و سیگنال داده را با فرکانس‌های دقیق و مشخصی تسهیم می‌کند. این فرکانس‌ها به گونه‌ای انتخاب می‌شوند که خاصیت تعامد را فراهم کنند و به این ترتیب علیرغم همپوشانی فرکانسی هر یک از فرکانس‌های حامل به تنهایی آشکار می‌شوند و نیازی به باند محافظت برای فاصله گذاری بین فرکانس‌ها نیست. برای کسب اطلاعات بیشتر در خصوص این تکنیک می‌توانید به نشانی زیر مراجعه نمایید:

http://wireless.per.nl/telelearn/ofdm

در کنار افزایش پهنای باند در این استاندارد فواصل مورد استفاده نیز کاهش می‌یابند. در واقع باند فرکانسی 5 GHz تقریباً دوبرابر باند فرکانسی 2.4 GHz است که در استاندارد 802.11a مورد استفاده قرار می‌گیرد. محدوده موثر در این استاندارد با توجه به سازندگان تراشه‌های بی‌سیم متفاوت و متغیر است.

طیف فرکانسی تمیزتر

طیف فرکانسی UNII در مقایسه با طیف ISM خلوت‌تر است و کاربرد دیگری برای طیف UNII به جز شبکه‌های بی‌سیم تعریف و تخصیص داده نشده است. در حالی که در طیف فرکانسی ISM تجهیزات بی‌سیم متعددی نظیر تجهیزات پزشکی، اجاق‌های مایکروویو، تلفن‌های بی‌سیم و نظایر آن وجود دارند. این تجهیزات بی‌سیم در باند ٢.٤ GHz یا طیف ISM هیچگونه تداخلی با تجهیزات باند UNII (تجهیزات بی‌سیم 802.11a) ندارند. شکل زیر فرکانس مرکزی و فاصله‌های فرکانسی در باند UNII را نشان می‌دهد.



کانال‌های غیرپوشا

باند فرکانسی UNII، دوازده کانال منفرد و غیر پوشای فرکانسی را برای شبکه سازی فراهم می‌کند. از این ۱۲ کانال ۸ کانال مشخص (UNII-1 , 2) در شبکه‌های محلی بی‌سیم مورد استفاده قرار می‌گیرند. این ویژگی غیرپوشایی گسترش و پیاده سازی شبکه‌های بی‌سیم را ساده‌تر از باند ISM می‌کند که در آن تنها ۳ کانال غیر پوشا از مجموع ۱۱ کانال وجود دارد.

802.11g

802.11g تلفیقی از هر دو مورد قبل است. استاندارد نوظهور شبکه‌های بی‌سیم که نیازهای پهنای باند، سرعت وهزینه کاربران را بر آورده کرده در عین حال با استاندارد WiFi نیز سازگاری دارد.

این استاندارد مشابه IEEE 802.11b از باند فرکانسی 2.4 GHz (یا طیف ISM) استفاده می‌کند و از تکنیک OFDM به عنوان روش مدولاسیون بهره می‌برد. البته PBCC نیز یکی از روش‌های جایگزین و تحت بررسی برای انتخاب تکنیک مدولاسیون در این استاندارد به شمار می‌رود. 802.11g از نظر فرکانسی، تعداد کانال‌های غیرپوشا، و توان مشابه 802.11b است. محدودههای عملیاتی نیز کم و بیش مشابه هستند با این تفاوت که حساسیت OFDM به نویز تاحدودی این محدوده عملیاتی را کاهش می‌دهد. پهنای باند 54 Mbps یکی از اهداف احتمالی این استاندارد جدید به شمار می‌رود. یکی دیگر از مزایای جالب توجه 802.11g سازگاری با 802.11b است. در نتیجه ارتقاء از تجهیزات 802.11b به استاندارد جدید 802.11g امری سرراست خواهد بود. جدول زیر استانداردهای بی‌سیم IEEE 802.11 را با یکدیگر مقایسه می‌کند.

کارایی و مشخصات استاندارد 802.11g

نرخ انتقال داده، برد ومسافت اتصال وسازگاری مشخصاتی هستند که در بین سه استاندارد تفاوت می‌کنند. این تفاوتها و تمایزات ناشی از مشخصاتی از قبیل فرکانس، مدولاسیون و تعداد نرخ داده می‌با شد.

نرخ انتقال داده در 802.11g

فن آوری 802.11g نرخ‌های انتقال داده متفاوتی را پشتیبانی می‌کند تا به کاربران امکان برقراری ارتباط در بهترین سرعت را بدهد.انتخاب بهترین نرخ انتقال داده موازنه–ای بین بدست آوردن بهترین نرخ انتقال و کمینه کردن تعداد خطاهای رخ داده است. هرگاه خطایی رخ دهد سیستم موظف به صرف زمان برای انتقال مجدد اطلاعات برای رفع خطای رخ داده است و این مسئله باعث می‌شود تا تعداد خطاهای رخ داده عاملی تعیین کننده باشد.

برد ومسافت در 802.11g

با افزایش فاصله از نقاط دسترسی (Access Point) تجهیزات مبتنی بر 802.11g نرخ انتقال را کاهش داده تا ارتباط با کاربران را حفظ کنند. 802.11g نیز مانند 802.11b دارای خصوصیات انتشار امواج رادیویی مشابه‌ای است زیرا مخابره سیگنالهای هر دو استاندارد در باند فرکانسی منحصر به فرد 2.4 GHz انجام می‌شود و به دلیل پیاده سازی یکسان این وضعیت در این دو استاندارد خواص یکسان نرخ انتقال وماکسیمم برد مشاهده می‌شود.در حالیکه استاندارد 802.11a از باند فرکانسی کاملا مجزای 5GHz استفاده می‌کند و قابلیت سازگاری با دو نوع دیگر را ندارد.

معمولا برد مسافتی دو نوع a و b (به دلیل استفاده از باند فرکانسی 2.4 Ghz) یکسان می‌باشد. استاندارد 802.11b از مدولاسیون CCK استفاده می‌کند در حالیکه 802.11g هم از مدولاسیون CCK (برای حفظ سازگاری به 802.11b) و هم

از مدولاسیون OFDM برای دستیابی به برد بیشتر بهره می‌جوید. 802.11a هم از OFDM استفاده می‌کند اما درصد اعوجاج و خرابی سیگنا لها به دلیل استفاده از فرکانس بالاتر (امواج با فرکانس بالا از اجسام عبور می‌کنند) بیشتر است.

. تمام استانداردهای این خانواده بر اساس استانداردهای ذیل در لایه فیزیکی طراحی و پیاده سازی شده است.

- Ethernet
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)

جدول زیرسه استاندارد شبکه‌های بی‌سیم را با یکدیگر مقایسه می‌کند.

	IEEE 802.11b	IEEE 802.11a	IEEE 802.11g
کاربردهای احتمالی	- جایگزین شبکه‌های سیمی - فراهم آوردن تحرک و سیار بودن کاربران - شبکه‌سازی در محل‌هایی که استفاده از سیم میسر نیست - پل‌سازی بین شبکه‌های محلی در فواصل دور (٤٠ کیلومتر)	- جایگزین شبکه‌های سیمی - فراهم کننده پهنای باند زیاد در کابردهای (صدا، تصویر، CAD و نظایر آن) - شبکه سازی در محل‌هایی که استفاده از سیم میسر نیست.	- ارتقاء شبکه‌های 802.11b و رقیبی برای 802.11a - کارایی مشابه با 802.11a در فواصل طولانی
مزایا	- استاندارد رایج و تکامل یافته - قیمت منطقی -گذردهی قابل قبول در فاصله زیاد (نرخ ارسال داده)	- گذردهی (نرخ ارسال داده) بالا در فواصل کم - افزایش تعداد کانال‌های فرکانسی غیرپوشا (٤ برابر بیشتر از 802.11b) - تداخل فرکانسی کمتر	- سازگاری با 802.11b - محدوده عملیاتی زیاد (نظیر802.11b) - گذردهی (نرخ ارسال داده) بیشتر
معایب	- دارابودن کمترین گذردهی (نرخ ارسال داده) در مقایسه با سایر فناوری‌های بی‌سیم (11Mbps) - استفاده از تنها ۳ کانال فرکانسی غیر پوشا	- فنّاوری نسبتاً گران - ناسازگاری با 802.11b - محدوده عملیاتی کوچک - محدودیت‌های FCC برروی آنتن‌ها (حداکثر توان مجاز) در هر باند فرکانسی	- عدم وجود محصول فراگیر (احتمالاً تا اواسط سال۲۰۰۳ میلادی) - محدودیت‌ها کانال فرکانسی نظیر 802.11b (۳ کانال غیرپوشا)

جدول زیر خلاصه سایر استانداردهای IEEE در شبکه‌های بی‌سیم را نمایش می‌دهد:

این مجموعه از استانداردها شامل سه استاندار می‌باشد که در شبکه‌های بی‌سیم مورد استفاده قرار می‌گیرد.

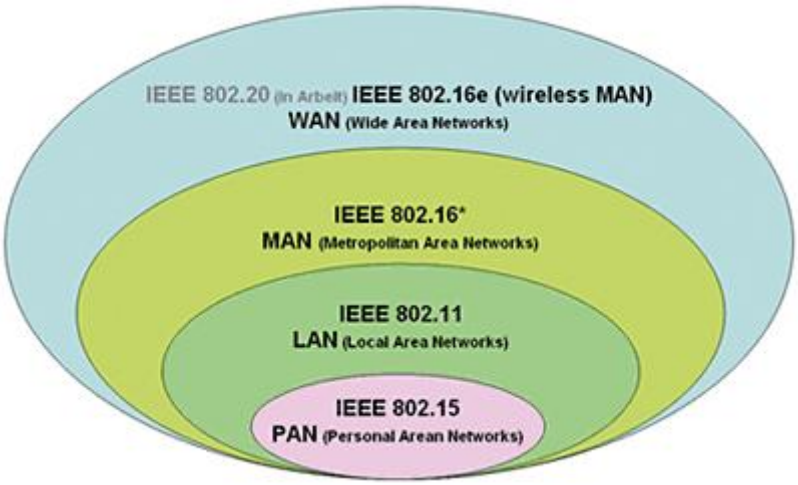
Best Usage	Modulation	Max. Data Transfer Rate	Frequency Range	IEEE
Outdoor	OFDM [1]	54 Mbps	5.x GHz	802.11a
Indoor	PSK [2] – CCK [3]	11 Mbps	2.4x GHz	802.11b
Indoor	OFDM	54 Mbps	2.4x GHz	802.11g

۱. PSK – Phase Shift Keying
۲. OFDM – Orthogonal Frequency Division Multiplexing
۳. CCK – Complementary Code Keying

قابل ذکر است که استاندارد g دارای تطابق با استاندارد قدیمی b می‌باشد. بدین مفهوم که دستگاه‌های دارای استاندارد 802.11g قادر به کار با استاندارد قدیمی‌تر 802.11b می‌باشند.

استاندارد 802.11e

این استاندارد برای تکمیل استانداردهای *a,b,g* با ویژگی امکان ایجاد اولویت در ارسال بسته‌های اطلاعات حساس به تاخیر زمانی مانند بسته‌های صوتی و تصویری (*Voice & Video Packet*) تعریف شده است. به این ترتیب با ایجاد اولویت در ارسال بسته‌های حاوی اطلاعات صوتی و تصویری کیفیت ارسال صوت و تصویر بالا رفته و تاخیر (*Latency*) در ارسال و دریافت بوجود نخواهد آمد.



۹-۳-۶- کاربردهای *WiFi*

تکنولوژی WiFi علاوه بر استفاده در ارتباط رایانه‌های شخصی در اتصال به اینترنت به صورت بی‌سیم امکان استفاده از هر شبکه دیگری رانیز دارد.به عنوان نمونه در تلفن همراه‌های نسل جدید امکان اتصال به اینترنت از طریق واب فای فراهم شده و نیز سرویس (roice) اتقال صدا از طریق تکنولوژی اینترنت که امکان بر قراری تماس تلفنی روی شبکه‌های رایانه‌ای را مقدور می‌سازد نیز از WiFi بهره می‌گیرد.با استفاده از Telephony Dualmode و دستگاه‌های تلفن همراه نیز قادر خواهند بود با استفاده لز تکنولوژی WiFi تماس‌هایی با کیفیت تکنولوژی سلولی را بر قرار سازند و بدین ترتیب شما امکان اتصال به اینترنت روی گوشی خود را خواهید داشت و هم امکان مکالمه تلفنی را.

۹-۳-۷- دلایل رشد WiFi

شبکه‌های مبتنی بر WiFi راه موفقیت و پیشرفت را در پیش گرفته است. تعداد کاربران WiFiکه در سال۲۰۰۰درحدود۲/۵ ملیون نفر بود اکنون به ۱۸ ملیون کاربر رسیده است و می‌رود تا مسیر رشد و پیشرفت خود را ادامه دهد از مهمترین دلایل رشد WiFi می‌توان به موارد زیر اشاره کرد:

۱) پشتیبان شرکت‌های مختلف:شرکت‌های بزرگ و معتبری همچون مایکروسافت، اینتل سیسکو وای بی ام به شدت مشغول کار بر روی تکنولوژی WiFi هستند و سرمایه گذاری‌های هنگفتی نیز در این زمینه انجام داده‌اند به عنوان نمونه شرکت اینتل سیصد ملیون دلار برای توسعه WiFi بر روی centrino سرمایه گذاری کرده است.

۲) توسعه ارتباط باند پهن:استفاده از فناوری WiFi سبب توسعه شبکه‌های باند پهن شده است به گونه‌ای که در سال جاری در حدود ۳۰ درصد رشددر زمینه باند پهن مشاهده شده است.

۳) شبکه‌های بزرگ ملی:هم اکنون در برخی از کشورهای دنیا شبکه بزرگ ملی WiFi در حال فعالیت است به عنوان نمونه در کشور آمریکا چهار شبکهToshiba، voice stream، comeate Network، Boingo مشغول سرویس دهی به کاربران هستند.

۴) تجهیزات آماده:شرکت‌های تولید کننده سخت‌افزار در سال‌های اخیر همراه با سخت‌افزارهای خود لوازم و متعلقات مورد نیاز سیستم‌های WiFi را به صورت آماده در اختیار مشتریان قرار می‌دهندو دیگر نیازی به تهیه این وسایل از بازارها رایانه به صورت جداگانه وجود ندارد.هم اکنون شرکت‌های Dell، Toshiba، ..... درراینه‌ها و قطعات تولیدی خود تکنولوژی WiFiرا گنجانده‌اند.بر طبق اعلام شرکت‌های سخت‌افزاری در دو سال آینده همه رایانه‌های همراه (laptop) به تجهیزات WiFi مجهز خواهند شد.

۵) گسترش شبکه:پیشگامان صنعت WiFi در همه نقاط دنیا به شدت در حال توسعه شبکه‌های WiFi هستند به عنوان نمونه در همه پارکها، رستورآن‌ها و اماکن تفریحی این تکنولوژی‌ها به چشم می‌خورد.

۶) نو آوری‌های بیشتر:تکنولوژی WiFi به دلیل تازه واردبودن به سرعت در حال پیشرفت است.شرکت‌های اینتل وMash در حال ساختن آنتن‌هایی هستندکه نسبت به آنتن‌های فعلی محدوده بیشتری راپوشش می‌دهدبه علاوه شرکت‌های سازنده گوشی تلفن همراه نیز در حال ساخت گوشی‌هایی با امکانات WiFi هستند.

۹-۳-۸- نقاط ضعف WiFi

۱) قیمت‌های گران:هزینه‌های اشتراک ماهانه در بسیاری از کشورها در حدود ۵۰ دلار در ماه است.

۲) هزینه‌های پنهان فراوان: جدا از هزینه‌های اولیه WiFi شما بایدهزینه‌های پنهان دیگری نیز مانند نصب و نگداری تجهیزات شبکه و نیز راه حل امنیتی را بپردازد.

۳) فواصل کوتاه: هم اکنون فاصله‌ای را که به جرات اعلام کرد در حدود یک صد متر است که با وجود موانع فیزیکی موجود در ساختمآن‌ها و ادارات این فاصله دریافت سیگنال کمتر نیز خواهد شد.

۴) عدم پوشش همه نقاط:در برخی کشورها که تکنولوژی WiFi فعال شدهپوشش کابل شبکه فراهم نشدهو شما مجبور به استفاده از سرویس دهندگان مختلف در نقاط جغرافیایی متفاوت خواهید بود.

۵) مشخص نبودن استانداردها:استانداردهای شربت‌های ارائه دهنده تجهیزات WiFi استفاده از طیف رادیویی بدون مجوز را ترجیح می‌دهند زیرا در این صورت هزینه‌های ان کاهش خواهد یافت و همین امر سبب شد که استاندارد واحدی برای این کار طراحی نشود اما در سال‌های اخیر سازندگان به سمت متحد شدن استانداردها حرکت رو به جلویی را آغاز کردند.

۶) عدم وجود امنیت:در شبکه‌های بی‌سیم قبلی اجازه ارتباط کاربران غیر مجاز شبکه نیز داده می‌شدکه امکان شنود از طریق این کاربران یکی از خطرات این قبیل از شبکه‌ها بود اما هم اکنون سازندگان به سوی توسعه شبکه‌های امن حرکت خود را آغاز کردند.

۹-۴- تکنولوژی WiFi

۹-٤-۱- مقدمه

سیستم رادیویی که در WiFi استفاده می‌شود با آنچه در دستگاه مخابره رادیویی استفاده می‌شود چندان متفاوت نیست.آن‌ها قادر هستند مخابره و دریافت کنند.می توانند صفرها ویک‌ها را به امواج رادیویی تبدیل کنند و سپس آن‌ها را دوباره به صفر و یک تبدیل کنند.

۹-۴-۲- تکنولوژی رادیویی WiFi

سه تفاوت عمده بین سیستم رادیویی WiFi و یک دستگاه مخابره کوچک وجود دارد:

سیستم WiFi که با استاندارد 802.11B و 802.11g کار میکند در فرکانس ۲/۴ گیگاهرتز عمل می‌کندو آن‌هایی که با ستاندارد 802.11aکار می‌کنند در فرکانس ۵ گیگاهرتز ارسال می‌کنند. در حالی که یک دستگاه مخابره کوچک د رفرکانس ۴۹ مگاهرتز عمل می‌کند.فرکانس بابلاتر موجب افزایش سرعت انتقال اطلاعات می‌شود.

برای استاندارد 802.11a و 802.11g از تکنیک OFDM استفاده می‌شودو برای استاندارد 802.11b از تکنیک CCK استفاده می‌شود.

سیستم رادیویی استفاده شده در WiFi توانایی تغییر فرکانس را دارد. 802.11b می‌توانند در هر سه باند مخابره کنند یا می‌توانند پهنای رادیویی در دسترس را به دوازده کانال تقسیم کنند و جهش فرکانسی به سرعت بین آن‌ها انجام شود. مزیت جهش فرکانسی این است که باعث تداخل کمتر می‌شود و اجازه می‌دهد که چندین کارت WiFi به طور همزمان بدون تداخل با یکدیگر مداخله کنند.بنابراین سیستم رادیویی WiFi می‌تواند میزان بسیار زیادی از اطلاعات را در هر ثانیه مخابره کند.

کارت‌های ۶۰۲.۱۱ bمی‌توانند مسیقیماً بر روی هر یک از این سه باند ارسال شوند، یا می‌توانند پهنای باند رادیویی در دسترس را به چندین کانال و hop frequency بین آن‌ها تبدیل کنند. مزیت frequency hopping در این است که در مقابل اختلال و پارازیت بسیار ایمن‌تر است و به چندین عدد از کارت‌های WiFi اجازه می‌دهد بطور همزمان و بدون ایجاد اختلال در کار هم با یکدیگر مکالمه کنند.

به دلایلی که ذکر شد، سیستم‌های رادیویی WiFi ظرفیت و سرعت انتقال داده با لاتری را نسیت به رادیوهای واکی – تاکی دارند، این سرعت‌ها برای استاندارد 802.11b تا ۱۱ مگابایت بر ثانیه و برای 802.11a و 802.11g در حدود ۳۰ مگابایت بر ثانیه است.



۹-٤-۳- شبکه واکی تاکی (Walkie Talkie)

اگر می‌خواهید با شبکه سازی بی‌سیم در ساده ترین سطح آن آشنا شوید، یک جفت Walkie_Talkie ارزان قیمت ۵ دلاری را در نظر بگیرید. اینها رادیوهای کوچکی هستند که قادر به ارسال و دریافت امواج رادیویی می‌باشند. وقتی در یک Walkie_Talkie صحبت می کنید، صدای شما توسط یک میکروفون دریافت می‌شود. سپس به شکل یک فرکانس رادیویی کد گذاری می‌شود و توسط آنتن آن ارسال می گردد. Walkie_Talkie دیگر می‌تواند امواج ارسال شده را توسط آنتن خود دریافت کند، صدای شما را که به شکل امواج رادیویی کد گذاری شده decode کند و آن را از یک بلند گو پخش نماید. یک Walkie_Talkie نمونه مثل این، با قدرت سیگنالی در حدود ۰.۲۵ وات امواج را ارسال می کند و برد آن‌ها می‌تواند و برد آن‌ها می‌تواند به حدود ۵۰۰ تا ۱۰۰۰ فوت برسد.

بیایید تصور کنیم که شما قصد دارید دو کامپیوتر را با استفاده از تکنولوژی Walkie_Talkie در یک شبکه به هم وصل کنید: شما هر دو کامپیوتر با یک Walkie_Talkie تجهیز می کنید. شما برای هر دو کامپیوتر روشی را برای مشخص نمودن اینکه آیا قصد ارسال یا دریافت امواج را دارد معین می‌نمایید.

شما روشی را بمنظور تبدیل کدهای باینری (دودویی) ۰ و ۱ها به دو beep متفاوت که Walkie_Talkie بتواند آن‌ها را ارسال و دریافت کند و بین beepها و ۰ و ۱ها عمل تبدیل به انجام برساند مشخص می کنید. این سناریو عملاً کار می کند. تنها مشکلی که در این زمینه وجود دارد این است که نرخ تبادل داده بسیار آهسته و کند است. یک Walkie_Talkie ۵ دلاری برای کار با صدای انسان طراحی شده است، بنابراین شما نمی‌توانید حجم زیادی از داده‌ها را به این روش ارسال کنید. شاید ۱۰۰۰ بیت در ثانیه.

۹-۴-۴- به‌کارگیری WiFi در صنعت تلفن همراه



مقدمه

سازندگان گوشی‌های تلفن همراه همواره مشتاق هستند تا شما و دوستانتان را هر ساله به تعویض گوشی قدیمیتان با نمونه‌های جدید و مجهز به انواع امکانات پیشرفته ترغیب کنند. تا یک سال پیش از این، امکانات موجود روی یک گوشی همراه پیشرفته شامل دوربین عکاسی و پخش موسیقی بود. نسل پس از آن شامل دستگاهی می‌شد که با ضخامت بسیار کم به راحتی در جیب جای می‌گرفت و بالاخره در چند ماه گذشته پخش ویدیو آخرین گزینه‌ای بود که بر صفحه نه چندان بزرگ گوشی‌های همراه ظاهر شد. با این وجود و به‌رغم معرفی انواع مدل‌های مختلف گوشی‌های همراه، مدل‌های باریک و ضخیم، گوشی‌های شکلاتی و تاشو، این وسیله همیشه همراه، به طور بسیار ناراحت‌کننده‌ای ناکارآمد و ناقص به نظر می‌آید؛ به ویژه با اینترفیس‌های گیج‌کننده، عدم آنتن‌دهی مناسب و پیام‌های ناخواسته. آیا وقت آن نرسیده است که نوکیا با همکاری شرکت Cingular Wireless به این وضعیت پایان داده و باعث شوند تا این شبکه پر از وصله و رفو بهتر کار کند؟

در این رابطه هیچ‌کس قولی نمی‌دهد، اما سازندگان گوشی می‌گویند نسل بعدی فناوری تلفن‌های همراه که امسال معرفی خواهد شد، علاوه بر راحتی در استفاده، مشکلات کمتری در مسائل ارتباطی داشته و به خاطر دارا بودن امکان تبادل اطلاعات چندرسآن‌های، ارزش امتحان کردن را دارد. همچنین صنعت موبایل امیدوار است به فناوری ساخت گوشی‌هایی دست یابد که بنا به گفته Rob N. Shaddock، مهندس ارشد بخش ابزارهای موبایل شرکت موتورولا، "کنترلی برای زندگی شما" محسوب گردند. این تصور جذابی است که بخواهیم یک گوشی هر کاری، از ضبط برنامه‌های تلویزیون گرفته تا بروزرسانی تقویم پی‌سی را انجام دهد؛ آن هم درحالی‌که شما سرگرم کارهای خود هستید.

این تصورات، جالب به نظر می‌رسند، اما بگذارید زیاده‌روی نکنیم. اگر تنها یک کار وجود داشته باشد که سازندگان این دستگاه‌ها مایل هستند صحیح انجام گیرد، این یک کار، بهتر انجام دادن همان وظیفه اصلی گوشی‌ها یعنی برقراری تماس خواهد بود. صنعت موبایل پاسخی برای این تمایل یافته است؛ پاسخی به نام WiFi. همان فناوری‌ای که شما را قادر می‌سازد توسط آن به صورت بی‌سیم پی‌سی‌های خود را به هم متصل کنید.

پهنای باند پشتیبان

در حال حاضر کیفیت ارتباط موبایل بستگی به موقعیت قرارگیری شما نسبت به آنتن BTS دارد و در مکآن‌های مسقف نیز در خیلی از موارد نخواهید توانست از گوشی خود استفاده کنید. هیچ‌کس بهتر از شش میلیون کاربر در ایالات متحده که

برای داشتن تحرک کامل دست از خطوط تلفن ثابت خود کشیدند، این مشکل را لمس نمی‌کند. پل آوبری ۳٤ ساله مدرس موسیقی و ساکن کانزاس‌سیتی می‌گوید: "در بیمارستان‌ها، در داخل آسانسورها و در مدرسه تا زمانی‌که کنار یک پنجره قرار نگیرم، نمی‌توانم تماس خوبی داشته باشم. برای حل این مشکل نوکیا و موتورولا تصمیم گرفتند تا نقاط تماس (Hotspots) دوگانه شبکه WiFi را معرفی کنند و آن‌ها را در خانه‌ها، دفاتر، نقاط اتصال جاوا و هرجای دیگری که لازم باشد، نصب نمایند. اطلاعات گوشی‌های موبایل در مجاورت این نقاط تماس بدون بروز اختلال و مشکل از یک سیستم به سیستم دیگر منتقل خواهند شد. البته میزان موفقیت این فناوری در آینده مشخص خواهد گردید. ترکیب شبکه‌های سلولی و WiFi یک ترکیب قدرتمند و کارا می‌باشد." این گفته فرانک‌هانزلیک، مدیر گروه تجاری WiFi Alliance، است.

از لحاظ تئوری، WiFi کاری بیش از پایدار ساختن تماس‌های تلفنی انجام خواهد داد. گوشی‌های دو حالته از دو طریق به اینترنت متصل می‌شوند و اتصال WiFi نیز سرعت پهن‌باند را ایجاد می‌نماید. شرکت T-Mobile دو مدل گوشی معرفی نموده که با آنتن‌های این شرکت کار می‌کنند. البته همانند تمام تجهیزات موبایل، مدل‌های نخستین ممکن است ایراداتی داشته باشند. ظرفیت و مدت دوام باتری عنصر مهمی تلقی می‌شود. برای مثال، WiFi جهت انتقال اطلاعات از یک کامپیوتر به کامپیوتر دیگر به وجود آمد. اما پرگویی و حرف زدن در تمام طول روز با تلفن، تمام نیروی باتری را مصرف می‌کند. سازندگان می‌گویند مدل‌های اولیه قادر خواهند بود چهار - پنج ساعت گفت‌وگو با استفاده از WiFi را پشتیبانی نمایند. آنان امیدوارند تا در انتها بتوانند به مرز هشت ساعت دست یابند. هانزلیک همچنین می‌گوید: "در ابتدا مشکلاتی وجود داشت، اما ما پیشرفت‌های خوبی در این زمینه داشته‌ایم. این موارد درباره سرویس‌های فعلی ویدیویی یعنی Live TV نیز صادق هستند".

مردم آن‌گونه که شرکت‌های بزرگ فعال در این حوزه یعنی Mobile ESPN، Verizon Wireless و Amp'd Mobile آرزویش را دارند، برای دریافت اشتراک مقابل این شرکت‌ها صف نمی‌کشند. با استفاده از خدمات Sprint Nextel Corp یا Cingular Wireless. بیشترین چیزی که عاید کاربر می‌شود، خبرهای کوتاه سی‌ان‌ان یا خلاصه اعلام نتایج لیگ بیسبال خواهد بود. با این‌حال، چنانچه عده‌ای درهمان زمان و در نزدیکی شما بخواهند همین کلیپ‌ها را مشاهده کنند، آن وقت چه اتفاقی می‌افتد؟ تصویر دریافتی یا محو می‌شود یا اصلاً دریافت نمی‌شود. پل کاتالانو شریک و متخصص شبکه‌های بی‌سیم از شرکت مشاور RelevantC Business Group، می‌گوید: "در حال حاضر شما نمی‌توانید برنامه‌های یک شرکت کابلی را برای استفاده صدها کاربر روی شبکه سلولی پخش کنید."

برای حل این مشکل، صنعت موبایل در حال سرمایه‌گذاری روی سیستم‌های جدید می‌باشد؛ مانند آنچه Qualcomm در دست ساخت دارد و همچنین شبکه رقیب دیگری که توسط نوکیا، اینتل، موتورولا و دیگران پشتیبانی می‌شود. این شرکت‌ها قول داده‌اند تا سیگنال‌های زنده تلویزیونی را همانند شبکه‌های کابلی و ماهواره‌ای در سطح وسیعی از کشور پخش نمایند. این سیستم‌ها در آن واحد توانایی پخش بیست تا سی کانال را دارند و طراحی آنان به شکلی است که قدرت کافی برای تماشای صحنه‌های پرتحرک مانند فوتبال و بسکتبال را فراهم میآورند. این ویژگی‌ای است که فناوری‌های فعلی قادر به انجام آن نیستند.Verizon Wireless انتظار دارد تا انتهای سال سرویس Qualcomm را در نیمی از بازار تحت کنترل خود گسترش دهد. اما عده کمی معتقدند که این سرویس همان‌گونه که پیش از این و در تبلیغات نشان داده شد کار کند و در انتها تبدیل به یک موفقیت چشمگیر گردد. علاوه برآن، وادار ساختن میلیون‌ها کاربر به این‌که گوشی تلفن خود را "نگاه" کنند، مستلزم این

است که این گوشی‌ها کمتر شبیه "گوشی" باشند. مسلماً کار آسانی نخواهد بود تا وسیله‌ای در اندازه یک شکلات ساخته شود و کار کردن با آن به سادگی روشن‌کردن مایکروویو باشد.

اما سازندگان و طراحان به سختی در حال کار روی امکان حذف کلیدها و افزودن فرامین صوتی بیشتر می‌باشند. به جای فشردن چندین دکمه و سرگردانی در بین منوها به منظور جست‌وجو در مورد مسئله‌ای مثل جام جهانی، در گوشی‌های آینده با فشار دادن تنها یک کلید و بر زبان آوردن فرمان صوتی "جست‌وجوی جام جهانی"، پس از چند لحظه چندین لینک درباره این مطلب روی صفحه نمایش داده می‌شوند. زمان پاسخ‌دهی نیز کوتاه‌تر شده و به گفته John C. Burris، جانشین مدیریت محصولات Sprint Nextel، حتی به اندازه یک کلیک هم منتظر نخواهید ماند. درخواست شما همانجا حاضر و آماده است. این‌هم قسمتی که منتظرش بودید؛ یعنی استفاده از گوشی موبایل به عنوان کنترل از راه دور جهانی. در آینده‌ای نه چندان دور محتویات شامل عکس‌های دیجیتالی، موسیقی، نمایش‌های تلویزیونی یا حتی فهرست‌های تماس پیش پا افتاده، به جای ذخیره روی یک پی‌سی ترجیحاً روی اینترنت ذخیره خواهند شد. در این‌حال یک گوشی موبایل شما را قادر خواهد ساخت تا از هر جا به این اطلاعات دسترسی داشته باشید.

شما می‌توانید به وسیله آن عکس‌ها را روی پی‌سی خود یا یک تلویزیون بفرستید. همچنین می‌توانید از گوشی خود بخواهید تا در زمانی‌که در راه هستید، کلیپ ویدیویی را برای شما ذخیره کند. به همین شکل می‌توانید از گوشی برای گوش دادن به موسیقی دیجیتالی مورد علاقه خود در منزل استفاده نموده و در حالی‌که به سمت پارکینگ می‌روید، آهنگ‌ها را به ماشین خود انتقال دهید. در آخر شما قادر خواهید بود گوشی خود را آن‌گونه که تاکنون ممکن نبوده است سسفارشی‌سازی کنید. ما در این‌جا از یک تغییر کوچک در محدوده مد صحبت نمی‌کنیم. با آغاز سال جدید، شرکت‌هایی همچون Sprint و Verizon Wireless یک قدم حساس دیگر برخواهند داشت و کاربران تلفن‌های همراه را قادر می‌سازند تا صفحه گوشی خود را به هر اطلاعاتی که مایل هستند، مزین نمایند. کافی است گوشی را روشن کنید تا نتایج تیم ورزشی مورد علاقه خود یا آخرین قیمت‌های بورس را مشاهده نمایید. Burris می‌گوید: "اطلاعات در طول شب یا در مدت جابه‌جایی کاربر، به گوشی او ارسال می‌شود." چه کسی می‌داند؟ شاید Sprint و دیگران بتوانند این‌کار را انجام دهند و اقتدار شبکه‌های ویدیویی زمینی بالاخره شکسته شود.

۹-۴-۵- آنچه برای ساختن یک شبکه بی‌سیم نیاز دارید

برای ساختن یک شبکه بی‌سیم نیاز به چند عضو پایه دارید.معمول ترین شبکه‌های بی‌سیم شامل یک مسیر یاب یا دستگاه نقطه دستیابی (Wireless Access Point یا WAP) و کارت شبکه بی‌سیم (به تعداد کامپوترهای متصل به شبکه) هستند.به عنوان مثال فرض کنیم در حال پیکربندی یک شبکه بی‌سیم در خآن‌های هستید که دو کامپیوتر رومیزی یک ارتباط اینترنت باند عریض و یک لپ تاپ دارد.گام اول بای ساخت شبکه آن است مسیر یاب بی‌سیم را به مودم باند عریض وصل کنید.وقتی مسیر یاب به درستی پیکربندی شود به دروتزهای به سوی اینترنت تبدیل می‌شود.به هر کامپیوتر وصل شده در پشت مسیر یاب یک نشانی IP ثبت شده داخلی اختصاص می‌یابد که معمولا در محدوده 192.168.x.x است.

مسیر یاب ترافیک ورودی از نشانی IP ثبت شده – که به وسیلهISP اختصاص می‌یابد را بر دوش می‌گیرد و آن داده‌ها را به نشانی I P مقتضی هدایت می‌کند.این خصوصیت که به NAT یا (network Address Translation) مشهور است یک لایه پایه حفاظتی بین کامپیوترهای شما و اینترنت به وجود می‌آورد.

پس از پیکربندی مسیریاب گام بعدی نصب کارتهای شبکه بی‌سیم در هر کامپیوتر شبکه است.کارتهای شبکه‌های بی‌سیم در انواع متنوعی عرضه شده‌اند.بعضی از آن کارتهای متداول PCI که شبیه به سایر کارتهای PCI مانند کارتهای صذا نصب می‌شوند.

بعضی دیگر بای لپ‌تاب‌هاساخته شده‌اند و از استاندارد PCMCIA تبعیت می‌کنند. اگر پی سی یا نوت بوک شما حاوی شکاف (slot) اضافی نباشد می‌توانید از آداپتورهای بی‌سیم USB بهره بگیرید.نصب آداپتور شبکه معمولا آسان است.آن را در یک شکاف خالی فرو کنیدیا اگر از نوع USBاست رابطه آن را به یک درگاه USBوصل کنید.سپس وقتی کامپیوتر خود را رئشن می‌کنید سیستم عامل باید این وسیله جدید را شناسایی کند و دستگاه رآن‌های (driver) جدید را نصب کند.دستگاه رآن‌ها معمولا بر روی یک سی دی یا دیسکت قرار دارندو ویندوز می‌تواند آن‌ها را شناساییو برای آداپتور نصب کند.وقتی دستکاه رآن‌ها نصب شدند کامپیوتر را باز راه اندازی کنید و برنامه خدماتی ارتباط بی‌سیم را که به همراه آداپتور عرضه شده است رابرای پیداکردن امواج هوایی مربوط به مسیر یاب به اجرا در آورید. (ویندوز اکس پی خود امکاناتی برای اداره ارتباطات شبکه بی‌سیم دارد.) اگر همه چیز درست کار کند و شما در برد موثر شبکه باشید مسیر یاب باید در یک فهرست به عنوان یک ارتباط موجود ظاهر شود روی دکمهconnection کلیک کنید و کار برپایی شبکه تمام است.

۹-٤-٦- WiFi را به دستگاه خود اضافه کنید



مجهز بودن یک PDA یا اسمارت‌فون به WiFi با گسترش روزافزون این فناوری یک امر ضروری به‌نظر می‌رسد. حال اگر شما هم مانند من دستگاهی داشته باشید که فاقد این فناوری باشد، چه کار می‌کنید؟ مسلماً اولین راه حل، خریدن یک PDA جدید است، اما راه‌های ارزان‌تری نیز برای این مشکل وجود دارد. یکی از این راه‌ها افزودن سیستم WiFi به صورت خارجی به دستگاه می‌باشد. در ادامه نگاهی به این روش می‌اندازیم و کارت WiFi شرکت Spectec را بررسی می‌کنیم.

اکثر دستگاه‌های PDA امروزی از درگاه‌های حافظه استفاده می‌کنند و بسیاری نیز دارای دو درگاه حافظه هستند. در اکثر دستگاه‌ها این دو درگاه از نوع SD (Secure Digital) و CF (Compact Flash) هستند. اگر دستگاهی نیز دارای یک

درگاه حافظه باشد، آن درگاه از نوع SD می‌باشد. البته استثنای این مسئله شرکت سونی می‌باشد که از کارت‌های حافظه خاص خود، یعنی stick memory استفاده می‌کند. در اکثر تجهیزات همراه، از جمله اسمارت فون‌ها امروزه از کارت‌های حافظه SD و نوع کوچک شده آن Mini SD استفاده می‌شود.کارت حافظه باعث افزایش توانایی ذخیره اطلاعات شده و بدون آن نمی‌توان به موسیقی گوش داد یا به فیلمی نگاه کرد؛ چرا که در اکثر دستگاه‌ها مقدار حافظه داخلی برای این کار کافی نیست. در حال حاضر حداکثر ظرفیت کارت حافظه SD چهارگیگابایت و کارت SD mini دوگیگابایت می‌باشد. این محدودیت ظرفیت در کارت CF کمتر بوده و حداکثر ظرفیت این نوع کارت ۳۲ گیگابایت می‌باشد.از این درگاه‌ها برای کاربردهای دیگری نیز استفاده می‌شود. به‌طور مثال، برای درگاه CF انواع مختلف دوربین، WiFi، بلوتوث و GPS ساخته شده است که قیمت‌های مناسبی نیز دارند.

حال اگر درگاه SD از فناوری SDIO (Secure Digital Input /Output) پشتیبانی کند، از این درگاه نیز می‌توان برای وسایل جانبی بهره برد. علاوه بر وسایل جانبی نامبرده، اسکنر بارکد و گیرنده امواج تلویزیونی نیز برای این درگاه طراحی شده است.البته استفاده از این وسایل به این راحتی نیست. این وسایل به نسبت وسایل جانبی درگاه CF گران‌تر بوده و در بازار به راحتی پیدا نمی‌شوند. در ضمن اگر یک Pocket PC داشته باشید که فقط یک درگاه SD دارد، چه می‌کنید؟ کارت‌های جدیدی به بازار آمده‌اند که دو کار را با هم انجام می‌دهند. مثلاً هم بلوتوث هستند و درضمن ۲۵٦ مگابایت حافظه فلاش نیز دارند. همان‌طور که می‌دانید کارت‌های mini SD نمونه کوچک شده کارت‌های SD هستند. این فناوری نیز از SDIO پشتیبانی می‌کند. البته محصولات این گروه به علت اندازه کوچک بسیار کم هستند. SDW-822 یک کارت mini SD می‌باشد که WiFi را به دستگاه شما می‌افزاید. تولیدکنندگان PocketPc، اسمارت‌فون و Communicator امروزه بیشتر به کارت mini SD علاقمند شده‌اند و علت این علاقه، استفاده بهینه از فضا در داخل دستگاه می‌باشد.این کارت برای دستگاهی مانند HP hw 6515 که فاقد WiFi می‌باشد، بسیار مناسب است. نصب کارت بسیار ساده است.

کافی است. آن را به جای کارت حافظه وارد کنید و راه‌انداز را نصب کنید. بعد از آن نرم‌افزار داخلی ویندوز موبایل کارت WiFi را می‌شناسد و با آن کار می‌کند. با این‌که آنتن این کارت در حد چند میلی‌متر است، کیفیت سیگنال بسیار خوب است. این کارت از استاندارد b۸۰۲.۱۱ استفاده می‌کند و در اکثر اوقات ارتباط مناسبی برقرار می‌کند. مهندسان سازنده این کارت تلاش زیادی کرده‌اند تا تمام اجزای یک سیستم WiFi را در فضای اندکی بزرگ‌تر از یک سیستم کارت موبایل جا بدهند. قیمت کارت در بازار جهانی در حدود صد و ده دلار می‌باشد و با توجه به این‌که WiFi گزینه مطلوبی برای بسیاری از کاربران است، قیمت این کارت مناسب به نظر می‌رسد.

به شبکه‌های WiFi باز وصل نشوید

مطمئن شوید که تنظیمات سیستم به گونه‌ای است که مانع اتصال خودکار به نقاط دسترسی ناامن شود.

اتصال به یک شبکه WiFi باز مثل یک hotspot یا مسیریاب بی‌سیم آزاد، کامپیوتر شما را در معرض خطرات فراوانی قرار می‌دهد. هرچند به طور معمول این امکان فعال نیست ولی اغلب کامپیوترها دارای تنظیماتی هستند که امکان اتصال خودکار بدون اطلاع کاربر را فراهم می‌کنند. این تنظیمات به‌جز در موارد ضروری و به‌طور موقت نباید فعال باشد.

برای بررسی این‌که آیا اتصال خودکار به شبکه‌های WiFi باز، مجاز است یا نه، تنظیمات بی‌سیم کامپیوتر را بررسی کنید. برای مثال در کامپیوترهایی که دارای Windows XP هستند، تنظیمات بی‌سیم Automatically Connect To Non-Preferred Networks نامیده می‌شود.

برای بررسی مراحل زیر را انجام دهید:

- از منوی start به گزینه Windows Control Panel بروید.
- به گزینه Network Connections بروید
- بر روی Wireless Network Connection کلیک راست کنید و گزینه Properties را انتخاب کنید.
- روی گزینه Wireless Networks کلیک کنید.
- بر روی دکمه Advanced کلیک کنید.
- گزینه Automatically connect to non-preferred networks را پیدا کنید، اگر انتخاب شده بود این تنظیمات فعال است در غیر این صورت غیرفعال است.



اگرچه در Windows XP به‌طور پیش فرض Automatically connect to non-preferred networks فعال نیست، برخی کاربران برای سهولت اتصال به شبکه خودشان آن را فعال می‌کنند. کاربران باید شبکه خودشان را به عنوان Windows XP Preferred networks تنظیم کنند که اجازه اتصال خودکار را می‌دهد و اتصال خودکار به بقیه شبکه‌ها را غیرفعال کنند.

به تجهیزات آدرس (IP) ایستا اختصاص دهید.

اختصاص آدرس ایستا جایگزینی برای پروتکل DHCP است. اختصاص آدرس پویا با استفاده از DHCP راحت‌تر است و هم چنین به کامپیوترهای سیار اجازه می‌دهد که بین شبکه‌های مختلف جابه جا شوند.

آدرس‌دهی ایستا نیز مزایایی دارد، از جمله:

- آدرس ثابت ترجمه آدرس را بهتر پشتیبانی می‌کند، بنابراین یک کامپیوتر روی شبکه با نام دامنه اش به طور مطمئن قابل دستیابی است. مخصوصا سرورهایی مثل سرور وب و سرور FTP بهتر است آدرس ایستا داشته باشند.
- استفاده از آدرس‌دهی ایستا در مقابل DHCP محافظت بیشتری در برابر حملات امنیتی فراهم می‌کند.
- برخی تجهیزات شبکه پروتکل DHCP را پشتیبانی نمی‌کنند.
- استفاده از آدرس‌دهی ایستا برای تمام اجزای شبکه تضمین می‌کند که ناسازگاری آدرس‌ها رخ نمی‌دهد.

آدرس‌های ایستا باید از محدوده آدرس‌های خصوصی استاندارد انتخاب شود از جمله:

- "10.0.0.0" تا "10.255.255.255"
- "172.16.0.0" تا "172.31.255.255"
- "192.168.0.0" تا "192.168.255.255"

این محدودهها تعداد زیادی آدرس را پشتیبانی می‌کنند. برخلاف تصور اکثر افراد، تمام آدرس‌های این محدودهها نمی‌توانند انتخاب شوند.

برای انتخاب آدرس درست نکات زیر را مدنظر داشته باشد:

۱. آدرس‌هایی که با "0" یا "255" تمام می‌شوند را انتخاب نکنید. این آدرس‌ها برا ی استفاده پروتکل‌های شبکه رزرو شده‌اند.

۲. آدرس‌های ابتدای یک محدود آدرس خصوصی را انتخاب نکنید. آدرس‌هایی مثل "10.0.0.1" یا "192.168.0.1" معمولا به مسیریاب‌ها ی شبکه اختصاص می‌یابند. این آدرس‌ها اولین آدرس‌هایی هستند که معمولا یک نفوذگر تلاش می‌کند به آن‌ها نفوذ کند، بنابراین بهتر است از آن‌ها استفاده نکنید.

۳. از آدرس‌هایی که خارج از محدوده mask شبکه شما می‌باشد استفاده نکنید. برای مثال، برای پشتیبانی تمام آدرس‌های محدوده "10.x.x.x"، mask شبکه برای تمام سیستم‌ها باید به "255.0.0.0" تنظیم شود، در غیراین صورت برخی آدرس‌های ایستای این محدوده کار نمی‌کنند.

۹-۵- WiFi و WiMax

۹-۵-۱- مقدمه



ایجاد امکان دسترسی به اینترنت پرسرعت به صورت بی‌سیم، سال‌هاست که مد نظر ارائه‌دهندگان سرویس در سراسر جهان می‌باشد. معمولاً در حوزه‌های تحت پوشش اپراتورها مناطقی وجود دارد که ارائه خدمات ارتباطی به‌صورت سنتی امکان پذیر نمی‌باشد و یا هزینه بالایی در بر دارد. این مناطق معمولاً در حومه شهرها قرار داشته و جمعیت کمی دارند. ایجاد زیرساخت‌های سیمی برای این نقاط مقرون‌به‌صرفه نمی‌باشد. استفاده از تکنولوژی WiMAX راه‌حل بهینه‌ای است که از جانب اپراتورها با استقبال زیادی روبه رو شده است.

۹-۵-۲- مروری بر پیاده‌سازی شبکه‌های WiMax

همان‌طور که در قبلا اشاره گردید، این استاندارد باندهای فرکانسی مختلفی را در محدوده‌های بامجوز و بدون مجوز متناسب با ساختار خود تحت پوشش قرار می‌دهد و استاندارد امکان ارائه خدمات بی‌سیم را به صورت ثابت و متحرک فراهم می‌نمایند.

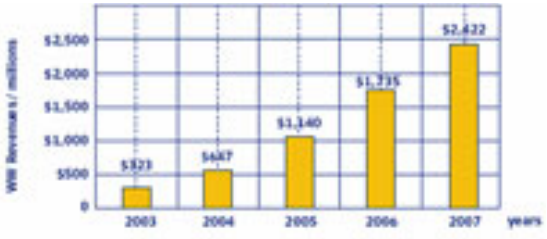
استاندارد	شرح		
	فرکانس	Bit Rate	Fixed / Mobile
802.16a	2-11 GHz	32-134 Mbps at 28MHz	Fixed (NLoS)
802.16b	5 , 6 GHz	32-134 Mbps at 128 MHz	Fixed (NLoS)
802.16c	66 -10 GHz	32-134 Mbps at 128 MHz	Fixed (LoS)
802.16d	2-11 GHz	Up to 75 Mbps at 20 MHz	Fixed (NLoS)
802.16e	< 6>	Up to 15 Mbps at 5 MHz	Mobile (NLoS)

بخش‌هایی از این استاندارد در سال ۲۰۰٤ به رسمیت شناخته شد و در حال حاضر محصولات متعددی بر پایه آن ساخته و وارد بازار شده‌اند، اما بخش‌هایی مانند IEEE 802.16e که در شبکه‌های موبایل کاربرد دارد، هنوز به عنوان یک استاندارد رسمی معرفی نشده است و درنتیجه هنوز هیچ تجهیزاتی مبتنی بر این استاندارد به تولید انبوه نرسیده است. در جدول فوق یک مقایسه‌ای بین استانداردهای مختلف و فرکانس کاری و نرخ بیتی آن‌ها دیده می‌شود. مطالعات اخیر در زمینه میزان رشد تقاضا برای استفاده از این تکنولوژی نشان می‌دهد که تنها در چند سال گذشته تعداد خطوط نصب‌شده، از ۵۷ میلیون در سال ۲۰۰۲ به ۸۰ میلیون در سال ۲۰۰۳ افزایش یافته است.



روش‌های دسترسی مبتنی بر WDSL (DSL بی‌سیم) در مقایسه با دسترسی از طریق خطوط DSL از هزینه کمتری برخوردارند، در نتیجه به سرعت در مکآن‌هایی که امکان ارائه خدمات ارتباطی وجود ندارد و یا تراکم جمعیت به اندازه‌ای است که ایجاد زیرساخت سیمی مقرون به صرفه نمی‌باشد جایگزین روش‌های موجود می‌شوند. بدنه رگولاتوری دولت‌ها نیز از این تکنولوژی به عنوان ابزاری برای از بین بردن فاصله دیجیتالی بهره می‌برند. به این منظور اقدام به بازنگری در فرکانس‌های موجود در باندهای با مجوز و بدون‌مجوز نموده‌اند تا به‌واسطه آن بتوانند از طیف‌های فرکانسی مطرح در این

تکنولوژی پشتیبانی نمایند. از نقطه‌نظر بازگشت سرمایه نیز این فناوری قابل تامل است. همان‌طور که در نمودار زیر مشاهده می‌شود، شروع ۲۳۲ میلیون دلاری و تخمین رشد تا ۱/۷۵ میلیارد دلار در سال ۲۰۰۶ برای بازگشت سرمایه در این فناوری، یک رشد قابل‌ملاحظه اقتصادی است که مشوق اصلی اپراتورها در ایجاد شبکه‌های مبتنی‌بر این تکنولوژی محسوب می‌شود.



هر یک از تجهیزات مورداستفاده در این تکنولوژی شامل تجهیزات سمت مشترک، تجهیزات Station Base و تجهیزات لایه هسته و توزیع هر کدام به تنهایی در ایجاد هزینه‌های پیاده‌سازی سهیم می‌باشند. جدول زیر نوع سرمایه گذاری برای هر یک از تجهیزات را نشان می‌دهد.

با استفاده از این تکنولوژی سرویس‌های متعددی را می‌توان در نواحی حاشیه‌ای شهرها و مناطق تجاری ارائه نمود.

هزینه‌های سرمایه گذاری تجهیزات	نوع سرمایه گذاری	نحوه تاثیر بر بازگشت سرمایه
تجهیزات لایه هسته و توزیع	سرمایه گذاری به صورت یکباره برای پوشش کلیه نقاط شبکه انجام می‌پذیرد.	APEX کلی بین مشترکین تقسیم می‌گردد. مثلاً در مناطق پرجمعیت به ازای هر کاربر کمتر از ۱۰ دلار در نظر گرفته می‌شود.
تجهیزات Base Station	این سرمایه گذاری به صورت فازبه‌فاز متناسب با پیشرفت پروژه انجام می‌شود.	APEX در این قسمت بین هر ۱۰۰۰ مشترک تقسیم می‌شود. به طور معمول CAPEX به ازای هر مشترک کمتر از ۱۰۰ دلار برای هر BS در ماکزیمم ظرفیت در نظر گرفته می‌شود.
تجهیزات CPE	این سرمایه گذاری نیز به‌صورت فازبه‌فاز انجام می‌شود. میزان سرمایه متناسب با نیازهای مشترکین متغیر می‌باشد.	بازگشت سرمایه در این قسمت متناسب با نحوه ارائه خدمات می‌باشد. به طور مثال بیشترین بازگشت سرمایه زمانی است که تجهیزات CPE به مشترکین اجاره داده می‌شوند و کمترین بازگشت سرمایه زمانی است که مشترکین تجهیزات سمت خود را خریداری می‌نمایند.

سرویس‌هایی که با استفاده از این تکنولوژی در مناطق تجاری قابل‌پیاده‌سازی می‌باشد، عبارتند از: سرویس‌های عمومی که شامل دسترسی به اینترنت، سرویس‌های صوتی، تصویری و از این قبیل می‌باشد و سرویس‌های تجاری که عموماً با تجارت‌الکترونیکی مرتبط است و دارای ویژگی‌های خاص خود از لحاظ امنیتی و کیفیت می‌باشد. این سرویس‌ها با توجه به ماهیتشان، غالباً از پهنای باند بالایی استفاده می‌کنند. در نتیجه درآمد ناشی از ارائه آن‌ها نیز برای اپراتورها قابل‌ملاحظه می‌باشد.

پیاده سازی WiMAX

فناوری WiMAX دارای مزایای زیادی است که آن‌را بر سایر تکنولوژی‌های موجود در زمینه شبکه‌های بی‌سیم ارجح می‌سازد.

این مزایا عبارتند از:

- ❖ کیفیت سرویس
- ❖ کارآیی بالا
- ❖ ساختار استاندارد
- ❖ پشتیبانی از آنتن‌های هوشمند

تجهیزاتی که برای پیاده‌سازی شبکه‌های شهری مورداستفاده قرار می‌گیرند در سه لایه تجهیزات سمت مشترک (CPE) تجهیزات مربوط به Base Stationها و تجهیزات لایه هسته شبکه می‌باشد. تجهیزات مربوط به سمت مشترک به‌طور کلی به‌گونه‌ای پیکربندی می‌شوند تا بتوانند کلیه اطلاعات مربوطه را با فرکانس‌های رادیویی به نزدیکترین Base Station انتقال دهند.

مرحله بعدی در ایجاد شبکه شهری بی‌سیم ایستگاه‌های ارائه‌دهنده سرویس است که به POP یا CO معروفند، این ایستگاه‌ها باید به‌گونه‌ای طراحی شوند که امکان تخصیص پهنای باند حداقل 1Mbps را برای هر مشترک تضمین نمایند. هرگونه ارتباطی با شبکه سایر ارائه‌دهندگان سرویس از طریق این نقاط صورت می‌پذیرد

ساختار این تکنولوژی به‌گونه‌ای است که می‌توان آن‌را در هر قسمت از شبکه مورداستفاده قرار داد، اما بهینه‌سازی نحوه استفاده از این تکنولوژی به هزینه آن نیز بستگی دارد. همان‌گونه که در بررسی‌های اقتصادی انجام‌شده دیده می‌شود، این فناوری در لایه دسترسی قابل‌جایگزینی برای سایر تکنولوژی‌های مطرح در زمینه بی‌سیم می‌باشد.

با استفاده از این تکنولوژی می‌توان در لایه توزیع (Backhaul) و دسترسی (Last Mile) با صرف هزینه پایین، کارآیی بالایی ایجاد نمود. از WiMAX برای مجتمع‌سازی WiFi نیز استفاده می‌شود. درحال حاضر برای بهینه‌سازی شبکه‌های بی‌سیم، توصیه می‌شود با بهره‌گیری از قابلیت‌های هریک از تکنولوژی‌های مطرح در زمینه ایجاد شبکه‌های بی‌سیم از هر دو تکنولوژی WiMAX و WiFi در کنار یکدیگر استفاده شود. به این ترتیب می‌توان از قابلیت‌های هر یک به صورت بهینه بهره برد.

همان‌گونه که مشاهده می‌شود در شبکه‌های محلی و Campus از همبندی Mesh تکنولوژی WiFi استفاده شده است و برای لایه توزیع (Backhaul) نیز WiMAX مورداستفاده قرار گرفته است.

انجمن WiMAX این استاندارد را برای پیاده‌سازی ارتباطات نقطه به نقطه (P2P) و یک نقطه به چند نقطه (P2MP) در مناطق روستایی و حومه شهرها که از تراکم جمعیت بالایی برخوردار نمی‌باشند.

۹-۵-۳- WiMax در مقابل WiFi

به روشنی واضح است که **WiMax** و **WiFi** تکنولوژی‌های مکمل یکدیگرند و برای آینده‌ای قابل پیش بینی به همین صورت خواهند ماند. تکنولوژی **WiFi** که به طور گسترده‌ای در دسترس می‌باشد و در نواحی متمرکزی چون هتل‌ها،

رستورآن‌ها، فرودگاه‌ها و حتی در مناطق گسترده تری در بعضی از شهرها مورد استفاده قرار می‌گیرد، برای سال‌های زیادی به رشد خود ادامه خواهد داد.

مقبولیت گسترده و پروتکل جامع و یکپارچه ۸۰۲.۱۱ b/g/a در امواج رادیویی کامپیوترهای laptop، رشد دائمی بر پایه مصرف کنندگان **WiFi** فراهم می‌سازد. گروه Forum حداقل سه موج از ابزار **WiMax** را در طول دو سال آینده پیش بینی می‌کند که برای کامپیوترهای laptop (سیار) مقرون به صرفه می‌باشد و بر پایه امواج رادیویی **WiMax** بنا نهاده شده است که سومین موجی است که در سال‌های ۲۰۰۶ تا ۲۰۰۷ عرضه خواهد شد.

هر چند حتی این واحدها تقریبا دوگانه می‌شوند (**WiMax / WiFi**)، یا اینکه چندگانه خواهد شد (**WiMax / WiFi / سلولی**) و برای چندین سال بعد از آن به کارشان ادامه خواهند داد. همانطوری که استاندارد **WiMax** رشد می‌کند و برای بدست آوردن پذیرش و کاهش هزینه‌های پیشرفت خود راه‌هایی می‌گشاید، تراشه‌های جدیدتری هستند که توانایی کارکرد در طول پایگاه‌های چند گانه را با هم ترکیب می‌کنند و با بخش شبکه‌های شهری مشترک می‌شوند که آن‌ها نیز به آرامی تبدیل به سیستم‌های **WiMax** قدرتمندی برای حالت‌های تجاری آن می‌شوند که از مزیت حوزه‌ها و نواحی متمرکز نیز بهره مند می‌شوند.

اساسا این بدان معناست که کاربران **WiMax** در چند سال آینده قادر خواهند بود نه تنها به نواحی متمرکز **WiFi** مثلا در یک کافی نت دسترسی داشته باشند بلکه همچنین می‌توانند دسترسی سیار **WiMax** را نیز در سراسر شهر به همان خوبی داشته باشند.

به هر حال سایر استانداردهای تکنولوژی LAN به عنوان مثال بلوتوث، Ultraband و خصوصیات دیدار شده در پروتکل ۸۰۲.۱۱n که مقدار کمتری را از لحاظ برد شبکه‌های نواحی متمرکز ارائه می‌دهند نیز تراشه‌ها و امواج رادیویی کامپیوترهای لپ تاپ خود را گسترش داده و ملزوم می‌سازد که در نهایت قادر باشند.

به طور دائمی و به خوبی از این بردهای کوتاهتر شبکه‌های داده **سلولی** و شبکه‌های **WiMax** شهری بگذرند. استاندارد **WiMax** بخش اصلی دیدگاه درخشان آینده ی بی‌سیم پهن باند می‌باشد که این انعطاف پذیری را وعده می‌دهد.

انواع مختلف اتصالها با یکدیگر در زیر مقایسه شده اند:

نوع	سرعت	محدوده (برد)	شرح
IrDA (مادون قرمز)	۹/۶ کیلو بیت تا ۱۱۵ کیلو بیت تا (۴ مگا بیت)	کمتر از ۶ فیت	۱- از طریق مادون قرمز تبادل اطلاعات می‌کنند، ۲- از قدرت وانرژی کمتری استفاده می‌کنند.
WiFi	۱مگا بیت تا ۵۴ مگا بیت	جدول زیر را ملاحظه نمایید	WiFi به هر سه نوع خدمات بی‌سیمی که مدل 802.11 که در جدول زیر نشان داده‌ایم، اشاره می‌کند همینطور به دسته بندیهای جدیدی که در آینده ارائه خواهد شد، این تکنولوژی همانند یک شبکه عادی از طریق سیم از جنبه‌های مختلف عمل

			می‌کند. این تکنولوژی یا در درون دستگاه نصب شده و یا به شکل کارتها یا رابطهای قابل اضافه شدن به کامپیوترهای رومیزی یا همان لپ‌تاب‌ها در دسترس می‌باشد.
802.11a	۱ تا ۵۴ مگا بیت	۵۰ تا ۱۵۰ فیت فاصله	از این تکنولوژی زیاد بصورت همگانی استفاده نمی‌شود، همچنین این روش نسبت به مدل 802.11b/g از فرکانس متفاوتی استفاده می‌کند.
802.11b	۱ تا ۱۱ مگا بیت	۱۰۰ تا ۳۰۰ فیت فاصله	روشی است، که در حال حاضر بیشترین استفاده را دارد.
802.11g	۱ تا ۵۴ مگا بیت	۱۲۰ تا ۳۵۰ فیت فاصله	آخرین روشی است که با مدل 802.11b سازگار می‌باشد.
بلوتوث	۱۲۰ کیلوتا ۷۲۳ کیلو بیت	۳۰ تا ۳۰۰ فیت	۱- از این سیستم برای وسایل و دستگاه‌هایی که ازنسل کامپیوتر هستند، استفاده می‌شود. ۲- دارای برد ۳۰ فوتی می‌باشد. ۳- طریقه نصب آن اینست که یا در خود دستگاه نصب می‌شود، و یا بصورت کارتهایی است که قابل اضافه شدن به دستگاه می‌باشند.
GPRS	کمتر از ۱۱۵ کیلو بیت	هر جایی که برای پوشش تلفن همرا مناسب باشد	۱- خدمات دیتایی است که توسط تلفنهای همراه، که تحت شبکه GSM هستند استفاده می‌شود ۲- سرعت آن حدود ۳۰ کیلو بیت در ثانیه است، این سرعت بستگی به تعداد کاربرهایی دارد، که از این خدمات بصورت مشترک در زمان تعیین شده استفاده می‌کنند. ۳- همچنین اینها یک سرویس و خدماتی از نسل ۲/۵ تلفنهای همراه به حساب می‌آیند.
نسل ۲/۵	سرعت آن مختلف بوده و تا حدود ۱۲۸ کیلو بیت	هر جایی که برای پوشش تلفن همراه مناسب باشد.	بنابر توافقهایی بعمل آمده این نسل هنوز آماده ارائه خدمات همیشه برقرار برای نسل سوم نمی‌باشد، تمامی شرکتهای تلفنهای همراه امیدوار هستند، که اگر تامین مالی شان و تکنولوژی اجازه دهد، آنرا

	می‌باشد.		معرفی کنند.
نسل سوم (3G)	۲ مگا بیت در حال سکون، ۳۸۴ کیلو بیت در حال حرکت با سیگنال خوب. ۱۴۴ کیلو بیت در حرکت سریع دارای سیگنال ضعیف	هر کجا که برای تلفن همراه مناسب باشد	انتقال دیتا را بطور بسیار سریع برای کاربرانش فراهم می‌آورد، به مدل پی سی اس اسپیرینت (PCS Sprint) وای تی‌اند تی اج (AT&T) (EDGE) (۱۰۰ تا ۱۳۰ کیلو بیت) که در حال حاضر در ایالات متحده موجود است، نزدیک می‌باشد.
مودم	کمتر از ۵۶ کیلو بیت.	هرجایی که بصورت بی‌سیم نمی‌باشد.	روش قدیمی است که باید از طریق کامپیوتر برای وارد شدن به اینترنت از روش شماره گیری (Dial-Up) استفاده نماید.
DSL / کابل	۱۰۰ کیلو بیت تا ۱/۵ مگا بیت	بصورت بی‌سیم نمی‌باشد.	۱–بی‌سیم نمی‌باشد. ۲– با یک باند پهن، وسایل را به اینترنت متصل می‌کند.
شبکه محلی (LAN)	۱۰مگا بیت تا ۱۰۰ مگا بیت	بصورت بی‌سیم نمی‌باشد.	۱– بی‌سیم نمی‌باشد. ۲– متداول‌ترین نوع شبکه‌ای است که با کابل کار می‌کند.

۹-۶- قطعات سخت‌افزاری WiMax

منبع: احمد فرهمند؛ "شبکه های بی‌سیم WiMax"

۹-۶-۱- آنتن های WiMax

به طور کلی یکی از اجزا اصلی هر شبکه بی‌سیم، آنتن شبکه است. از آنتن برای ارسال و دریافت اطلاعات استفاده می‌شود. در یک شبکه بی‌سیم، فرستنده و گیرنده از آنتن برای تبادل اطلاعات استفاده می‌کنند. هر آنتن مشخصات فیزیکی و فنی خاص خود را دارد که در ادامه با آن‌ها آشنا می‌شویم.

الف- مشخصات فنی آنتن: مشخصات فنی هر آنتن، نحوه عملکرد و کارایی آن را مشخص می‌کند. به طور کلی مهمترین مشخصات فنی هر آنتن عبارت است از:

مقدار دسی بل یا dB آنتن: این مقدار مشخص کننده توان سیگنال آنتن است. این مقدار به ورت (ده لگاریتم در مبنای ده) بیان می‌شود.

نکته: دسی بل یا dB یکی از واحدها و صورت های نمایش ریاضی اعداد است که از آن برای نمایش بهره افت و سطح توان سیگنال استفاده می‌شود. نمایش این مقادیر بر اساس دسی بل راحت‌تر است زیرا توان یک سیگنال به صورت لگاریتمی کاهش یا افزایش می‌یابد و به همین دلیل می‌توان به راحتی این مقادیر را جمع، تفریق و یا مقایسه کرد. به عبارت دیگر انجام عملیات ریاضی ساده‌تر است. دسی بل معیاری از نسبت بین دو سطح سیگنال است و به صورت

$$N_{dB} = 10log\frac{P_1}{P_2}$$

نمایش داده می‌شود. در این رابطه مقدار،NdB تعداد واحد دسی بل است، P1 سطح توان ورودی و P2 سطح توان خروجی است به عبارت ساده تر، اگر در یک سیستم انتقال (کابلی یا بی‌سیم)، مقدار توان سیگنال ورودی به اندازه P1 WiMax مقدار توان سیگنال خروجی به اندازه P2 باشد، مقدار افت یا تقویت توان سیستم برابر با NdB خواهد بود. اگر مقدار NdB به صورت منفی باشد، به معنای افت و کاهش توان است. یعنی این که در سیستم مورد نظر، توان خروجی کمتر از توان ورودی است و به نوعی افت توان اتفاق افتاده است. در نقطه مقابل، اگر مقدار NdB به صورت مثبت باشد، به معنای افزایش توان است، یعنی این که در سیستم مورد نظر توان خروجی بیشتر از توان ورودی است و به نوعی افزایش توان اتفاق افتاده است. مقدار dB برای هر آنتن، در هر نقطه متغیر است به عنوان مثال در یک نقطه خاص، یک آنتن می‌تواند مقدار dB مثبت و در یک نقطه دیگر مقدار dB منفی داشته باشد. به عبارت دیگر در نقطه اول، آنتن افت توان و

در نقطه دوم، آنتن افزایش توان داشته است.

نکته: به عنوان مثال وقتی گفته می‌شود که یک آنتن، در انتقال امواج بی‌سیم از یک نقطه به نقطه دیگر مقدار دسی بل اتلاف توان داشته است، به معنای آن است که انرژی سیگنال برای رسیدن از یک نقطه به نقطه دیگر، ۲۰ - به میزان صدبرابر کاهش یافته است. همچنین وقتی گفته می‌شود که یک آنتن، مقدار ۳۰ دسی بل افزایش توان داشته است، به معنای آن است که انرژی سیگنال برای رسیدن از یک نقطه به نقطه دیگر مقدار هزار برابر افزایش یافته است. محاسبات این مثال نمونه به صورت زیر است:

$$-20 = 10log\frac{P_1}{P_2} \rightarrow \frac{P_1}{P_2} = 10^{-2} = \frac{1}{100}$$
$$+30 = 10log\frac{P_1}{P_2} \rightarrow \frac{P_1}{P_2} = 10^{+3} = 1000$$

بنابراین هر آنتن یک مقدار دسی بل دارد که می‌تواند به صورت مثبت (به معنای افزایش توان) و یا به صورت منفی (به معنای کاهش توان) باشد.

مقدار dBi (دی – بی – آی)آنتن: به صورت معمول، مقدار توان هر آنتن را یک آنتن را با یک آنتن مرجع و پایه به نام آنتن آیزوتروپیک اندازه گیری می‌کنند. هر چقدر مقدار dBi یک آنتن بیشتر باشد، مقدار بهره آنتن بیشتر می‌شود. بدیهی است که برای انتقال امواج بی‌سیم به صورتی که توان بیشتری داشته باشد، از آنتن با dBi بیشتر استفاده می‌شود.

نکته: آنتن آیزوتروپیک یک آنتن تئوری و مرجع است که عملکرد سایر آنتن‌ها با آن سنجیده می‌شود. این آنتن، می‌تواند امواج بی‌سیم را به صورت ۳۶۰ درجه کامل و به شکل کروی منتقل کند. در عمل ساختن آنتن ایزوتروپیک، مشکل است به همین دلیل آنتن های ساخته شده را با این آنتن مقایسه می کنند.

خط دید: هر آنتن برای خود یک خط دید تعریف شده دارد و در صورتی که از این خط خارج شود، سایر آنتن‌ها و یا ایستگاه‌ها نمی‌توانند با آن رابطه داشته باشند. در انتقال امواج در فاصله های بسیار طولانی، از آنتن های جهت دار استفاده می‌کنند. آنتن های جهت دار برای خود خط دید دارند و در صورتی که از خط دید خود خارج شوند، نمی‌توانند ارتباط داشته باشند. به عبارت دیگر هر دو آنتن فرستنده و گیرنده بایستی به طور مستقیم در خط دید و زاویه دید همدیگر باشند. در استفاده از آنتن های جهت دار بایستی به ناحیه فرنل و ارتفاع آن نیز توجه کرد تا هر دو آنتن در خط دید یکدیگر قرار گیرند.

ب- مشخصات فیزیکی آنتن‌ها: مشخصات فیزیکی هر آنتن، بیان کننده شرایط نصب WiMax شکل ظاهری آنتن است و مهم ترین آن‌ها عبارتند از:

آنتن داخلی و خارجی: محیط های بی‌سیم را می‌توان به دو دسته کلی محیط های داخلی ۴ و خارجی ۵ تقسیم کرد. بدیهی است که برای هر محیط بایستی از سخت‌افزارها و تجهیزات خاص و مخصوص آن محیط استفاده کرد. این قضیه در مورد آنتن های شبکه نیز صادق است. آنتن های داخلی برای نصب در محیط داخل و شبکه های داخلی استفاده می‌شود. به طور معمول آنتن های داخلی از لحاظ ابعاد و اندازه کوچک و ظریف هستند. آنتن های خارجی برای نصب در محیط های خارجی و شبکه های خارج از ساختمآن‌ها، ساخته شده‌اند. این آنتن‌ها از لحاظ ابعاد بزرگتر هستند و مواد به کار رفته در تهیه آن‌ها به شکلی انتخاب شده‌اند تا بتوانند در انواع شرایط محیطی مقاوم باشند.

شکل ظاهری آنتن‌ها: هر آنتن کاربرد خاص خود را دارد و از این رو طراحی وشکل ظاهری آنتن‌ها نیز متفاوت است. براین اساس می‌توان آنتن‌ها را به انواع سقف کوب ۶ یا سقف آویز ۷ (مناسب برای نصب در محیط های داخلی)، آنتن های قابل نصب بر روی پایه یا دکل ۸ (مناسب برای محیط های خارجی)، دیوار کوب ۹ (مناسب برای محیط های خارجی یا داخلی) و آنتن های بشقابی (مناسب برای محیط های خارجی) تقسیم کرد.

در شبکه های WiMax از آنتن های داخلی برای سرویس دهی به کاربران داخل ساختمآن‌ها، مراکز تجاری و به طول کلی محیط های داخلی استفاده می‌شود.

از آنتن های خارجی برای سرویس دهی به کاربران در محیط های خارجی و یا ارتباط به صورت مستقیم استفاده می‌شود.

۱-۱۹) رادیوهای WiMax:

یکی از تجهیزاتی که در شبکه های WiMax از آن استفاده بسیار زیادی می‌شود، رادیوهای WiMax است. هر ایستگاه پایه (BS) از رادیو WiMax برای ارسال و یا دریافت اطلاعات استفاده می‌کند. در حقیقت در یک شبکه WiMax، رادیو WiMax اطلاعات ارسالی خود را در اختیار آنتن شبکه قرار می‌دهد و آنتن WiMax نیز آن را ارسال می‌کند. همچنین آنتن WiMax اطلاعات دریافتی خود را در اختیار رادیو WiMax قرار می‌دهد. هر رادیو WiMax ویژگی های خاص خود را

دارد که به عوامل مختلفی از جمله نوع سرویس شبکه LOS WiMax یا (NLOS)، نوع آنتن WiMax و رنج فرکانسی شبکه، بستگی دارد.

۹-۶-۲- CPE

یکی دیگر از تجهیزات مهم و کلیدی در شبکه های WiMax، تجهیزات پایه مشتری یا CPE است. هر ایستگاه کاری مشتری (SS) در شبکه های WiMax از یک یا چند CPE برای ارسال و یا دریافت اطلاعات استفاده می کند. به طور کلی دو نوع CPE در شبکه های WiMax وجود دارد که عبارتند از:

الف - نوع CPE داخلی: از این نوع CPE برای ایستگاه های مشتری استفاده می‌شود که در آن کاربران شبکه در محیط داخلی قرار گرفته‌اند.

ب-نوع CPE خارجی: از این نوع CPE برای ایستگاه های مشتری استفاده می‌شود که در آن کاربران شبکه در محیط خارجی قرار گرفته‌اند و محیط شبکه به صورت خارجی است.

همانند رادیوهای WiMax، هر CPE مشخصات خاص خود را دارد که به عوامل مختلفی از جمله نوع شبکه WiMax (LOS,NLOS)، رنج فرکانسی شبکه، نوع کاربران (ثابت یا سیار بودن) بستگی دارد.

۹-۶-۳- کارت شبکه WiMax

یکی از ارکان جدا نشدنی در هر شبکه، اعم از کابلی یا بی‌سیم کارت شبکه است که به طور اختصار به آن NIC ۱۳ گفته می‌شود. در شبکه های WiMax، کاربران برای اتصال به شبکه از کارت شبکه استفاده می کنند. هر کاربر می‌تواند از طریق کارت شبکه خود به نزدیکترین CPE متصل شود و از خدمات و سرویس های شبکه استفاده کند. به طور کلی دو نوع کارت شبکه WiMax وجود دارد که عبارتند از:

نوع ثابت: از این نوع کارت شبکه برای کاربرانی استفاده می‌شود که در شبکه به صورت ثابت هستند. این نوع کارت های شبکه به صورت داخلی در کامپیوترهای شخصی کاربران نصب می‌شود.

نوع متحرک: از این نوع کارت شبکه برای کاربرانی استفاده می‌شود که در شبکه به صورت متحرک هستند. این نوع کارت شبکه در کامپیوترهای همراه کاربران نصب می‌شوند و کاربران می‌توانند به صورت متحرک و سیار به نزدیکترین CPE متصل و در نهایت به شبکه WiMax متصل شوند.

۹-۶-۴- روترهای WiMax

یکی از تجهیزات مورد استفاده در شبکه های کابلی یا بی‌سیم، روتر یا مسیریاب است. وظیفه اصلی روتر برقراری ارتباط بین دو یا چند شبکه است که از لحاظ فیزیکی یا فنی با یکدیگر اختلاف دارند. به عنوان مثال برای ارتباط بین شبکه بی‌سیم و شبکه کابلی از روتر استفاده می‌شود. به طور کلی از روترهای WiMax به دو شکل استفاده می‌شود. یا این که این روترها دو وظیفه اصلی دارند که عبارتند از:

اتصال شبکه های کابلی به شبکه های WiMax: در این حالت از مسیر یاب برای اتصال شبکه بی سیم به یک شبکه کابلی مانند شبکه اینترنت استفاده می‌شود.

اتصال شبکه های بی‌سیم و شبکه WiMax: در این حالت از مسیر یاب برای اتصال یک شبکه بی سیم متفاوت با WiMax، مانند Wi-Fi به شبکه بی‌سیم WiMax استفاده می‌شود.

بنابراین می‌توان گفت که روترهای WiMax، برای اتصال شبکه های WiMax به شبکه های غیر از WiMax، اعم از کابلی یا بی‌سیم استفاده می‌شود.

۹-۶-۵- رک های WiMax

یکی دیگر از تجهیزات جانبی هر شبکه رک (Rack) است. رک یا قفسه به صورت یک چهارچوب فلزی است که شکل قفسه، محلی برای نگهداری تجهیزات شبکه است به عبارت دیگر با استفاده از رک می‌توان به شبکه انسجام بخشید و مانع از آشفتگی محیطی ناشی از تجهیزات شبکه شد.

۹-۶-۶- تجهیزات مربوط به ایستگاه های WiMax

هر شبکه WiMax از دو بخش اصلی ایستگاه های پایه (BS) و ایستگاه های مشتری (SS) تشکیل شده است. هر ایستگاه تجهیزات خاص خود را دارد که ترکیبی از سخت‌افزارهای مختلف است. بنابراین تجهیزات ایستگاه های WiMax را می‌توان به شکل زیر بیان کرد.

تجهیزات مربوط به ایستگاه های پایه: هر ایستگاه پایه از بخش های مختلفی تشکیل شده است که مهم ترین آن‌ها دکل، آنتن، رادیو WiMax و رک است. در هر ایستگاه از یک دکل برای نگه داری آنتن‌ها استفاده می‌شود و هر آنتن نیز به رادیو WiMax خود متصل است. به طور معمول رادیو WiMax را در رک‌ها نگه داری می‌کنند تا علاوه بر جلوگیری از دسترسی افراد ناشناس و نامربوط به شبکه، انسجام و یکپارچگی شبکه حفظ شود.

نکته: برای اتصال آنتن به رادیوهای WiMax، از کابل های خاصی به نام کابل Pigtail استفاده می‌شود. این کابل‌ها گران قیمت هستند و توسط رابط های مخصوص، به آنتن و رادیوهای WiMax متصل می‌شوند و بین آن‌ها ارتباط برقرار می‌کنند هر چقدر کابل Pigtail طول کمتری داشته باشد، به مراتب بهتر است و موجب می‌شود تا افت توان کمتری حاصل شود.

تجهیزات مربوط به ایستگاه های مشتری: هر ایستگاه مشتری از بخش های مختلفی تشکیل شده است که مهمترین آن‌ها CPE، کارت شبکه WiMax و رک است. هر ایستگاه می‌تواند از یک یا چندین CPE تشکیل شده است که هر CPE به تعدادی مشخص از کاربران سرویس دهی می‌کند. کاربران شبکه نیز می‌توانند از طریق کارت شبکه خود (ثابت یا سیار) به شبکه متصل شوند. در صورتی که در ایستگاه های کاری، از تجهیزات جانبی دیگری استفاده شود، این تجهیزات در رک های مربوطه قرار می‌گیرند.

۹-۷- بلوتوث

منبع: حسن کریمی، مجید محمدی و عیسی حاجی زاده؛ "شبکه‌های کامپیوتری (بی‌سیم)"؛ موسسه آموزش عالی آزاد مدیریت و فناوری امیرکبیر

در سال ۱۹۹۸ شرکت ال. ام. اریکسون علاقمند شد تا گوشی تلفن های همراه تولیدی او بتوانند بصورت بی سیم به ابزارهای دیگر (مثل PDA) وصل شوند. اریکسون و چهار شرکت دیگر (آی‌بی ام.اینتل. نوکیا و توشیبا) یک "گروه SIG"

تشکیل دادند تا استانداردی بی سیم برای اتصال ابزارهای مخابراتی / رایآن‌های و ابزارهای جانبی آن‌ها طراحی کنند که بردی کوتاه، مصرف توان و پائین و قیمتی ارزان داشته باشد. نام این پروپه، بلوتوث انتخاب شد که برگرفته از نام "هوالدبلاتاند دوم" (مشهور به Bluetooth)، یکی از پادشاهان وایکینگ است (۹۸۱ - ۹۴۰) که دانمارک و نروژ را با هم متحد کرد.

اگر چه تفکر اصلی، رهایی از شر کابلهای مابین دستگاه های دیجیتالی بود ولی به سرعت در حوزه های دیگر نیز گسترش یافت و به تدریج در حیطه شبکه های محلی بی سیم نیز وارد شد. اگر چه گسترش و رشد این استاندارد، روز بروز کاربرد آنرا بیشتر می کرد ولی در عوض چالشهائی بین این استاندارد و ۸۰۲،۱۱ پدید آورد. نقطه شدت این چالش آنجاست که این دو سیستم از لحاظ الکتریکی با یکدیگر تداخل فرکانسی دارند. اشاره به این نکته مهم است که شرکت هیولیت پاکارد چندین سال

قبل از آن شبکه ای مبتنی بر نور مادون قرمز برای وصل بی سیم دستگاه های جانبی کامپیوتر عرضه کرده بود، ولی استقبال چندانی از آن نشد.

فارغ از همه اینها، در ژولای ۱۹۹۹ گروه طراح بلوتوث، مشخصات هزار و پانصد صفحه ای از نسخه ۱ آن یعنی V 1.0 را منتشر نمود. به فاصله کوتاهی، گروه استاندارد سازی IEEE که در اندیشه تدوین استاندارد ۸۰۲،۱۵ برای شبکه های شخصب بی سیم بودند مستندات استاندارد بلوتوص را به عنوان مبنای کار خود برگزیدند و شروع به پلایش و تکمیل آن نمودند. اگر چه استاندارد سازی چیزی که مشخصات تفضیلی و مشروح آن در اختیاراست و پیاده سازی و هماهنگی داشته باشد) عجیب به

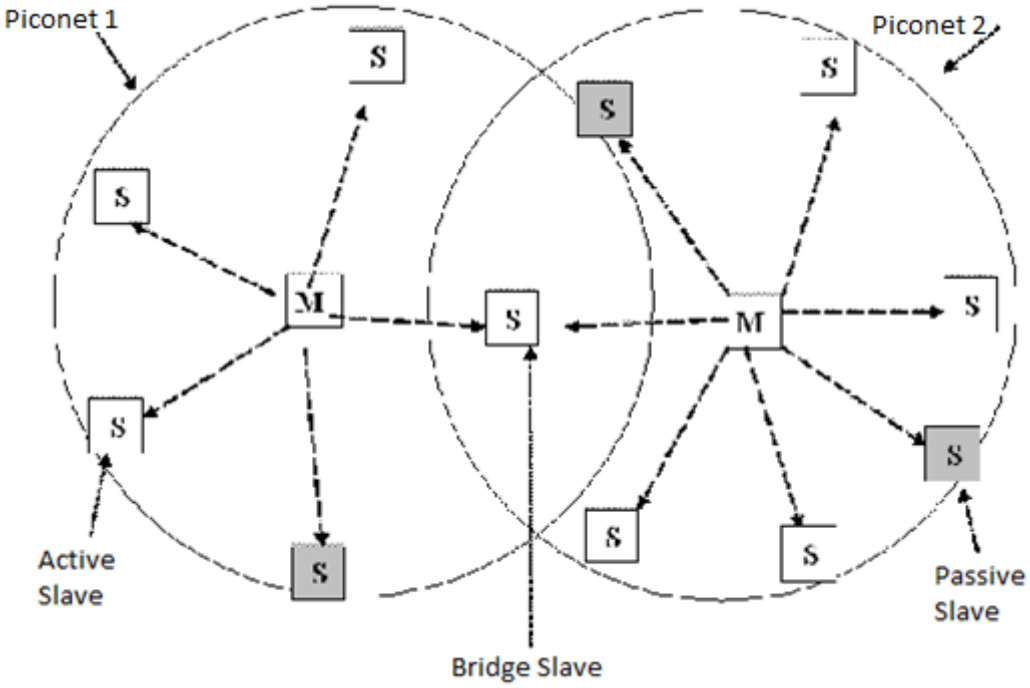
نظر میرسد ولی تاریخ نشان داده که وجود یک استاندار باز که توسط سازمانی بی طرف مصل IEEE تدوین و مدیریت می شود عموماً کاربری یک تکنولوژی را ترویج و ترغیب خواهد کرد. اگر بخواهیم اندکی دقیقتر سخن بگوئیم باید اشاره کنیم که توصیف استاندارد بلوتوث برای سیستمی کامل تدوین شده که از لایه فیزیکی تا لایه کاربرد را در بر می گیرد در حالیکه کمیته IEEE۸۰۲،۱۵ فقط لایه های فیزیکی و پیوند داده را استاندارد سازی کرده و باقیمانده پشته پروتکلی خارج از برنامه این استاندارد است.

هر چند IEEE اولین استاندارد PAN را در سال ۲۰۰۲ با عنوان ۸۰۲،۱۵،۱ به تصویب رساند ولی هنوز کنسرسیوم بلوتوث فعال و سر گرم بهبود و توسعه آنست. اگر چه نسخه استاندارد عرضه شده توسط کنسرسیوبلوتوث و IEEE ایمنی نیستند ولی انتظار می رود بزودی به یک استاندارد واحد همگرا شوند.



۹-۷-۱- معماری بلوتوث

اجازه بدهید بررسی سیستم بلوتوث را با مروری سریع بر دستاوردها و اهداف آن آغاز نمائیم. واحد پایه در سیستم بلوتوث یک پیکونت است که از یک گروه و حداکثر هفت گره پیرو فعال به فاصله حداکثر هفت گرو پیرو فعال (Active Slave Node) به فاصله حداکثر ده متر، تشکیل شده است. در یک فضای بزرگ و واحد می توان چندین پیکونت داشت و حتی می توان آن‌ها را از طریق یک گروه که نقش پل (Bride) ایفا می کند به هم متصل کرد (به شکل زیر نگاه کنید) به مجموعه ای از پیکونتهای متصل بهم اصطلاحا شبکه متفرق / پراکنده گفته می شود.



در یک پیکونت علاوه بر هفت گروه فعال پژو، می تواند تا ۲۵۵ گروه غیر فعال وجود داشته باشد. اینها دستگاه هائی هستند که گروه اصلی آن‌ها را در خالت استراحت و کم توان وارد کرده تا مصرف باطری آن کاهش باید.

یک ایستگاه در حالت غیر فعال هیچ کاری نمی توان انجام بدهد به جز آنکه به سیگنال فعال سازی خود یا سیگنال Beacon که از گروه اصلی می رسد، پاسخ بدهد. به غیر از این حالات، دو حالت میانی در مصرف توان به نامهای حالت Hold و Sniff نیز وجود دارد که در اینجا بدان نخواهدیم پرداخت.

دلیل طراحی اصلی/پیرو (Active/Passive) آن بود که طراحان آن در نظر داشتند قیمت کل سیستم بلوتوث پیاده سازی شده بر روی تراشه، زیر پنج دلار باشد. نتیجه این تصمیم گیری آنست که گروه های پیرو {مثل صفحه کلیدها، موس، چاپگر} تقریباً غیر همشمند و ساده هستند و اساسا آنچه را که گروه اصلی (Master) به آن‌ها دستور بدهد اجرا می کنند. یک پیکونت سیستمی مینی بر TDM متمرکز است که در آن هسته مرکزی (یعنی گروه اصلی یا Master) بر سیگنال ساعت نظارت دارد و تعیین می کند که چه دستگاه‌هی و در کدام برش زمانی (Slot) مخابره داشته باشد. تبادل اطلاعات صرفاً بین گره مرکزی و گروه های پیرو انجام می شود و ارتباط مستقیم دو گره پیرو { مثلاً دو صفحه کلید یا دو چاپگر} ممکن نیست.

۹-۷-۲- مزایای استاندارد Bluetooth

- قابلیت کار با تجهیزات ساخته شده توسط شرکت‌های متفاوت
- سرعت و فاصله انتقال مناسب
- ایمنی در انتقال اطلاعات
- ذخیره انرژی باطری به خاطر مصرف کم

۹-۷-۳- کاربردهای بلوتوث

بیشتر پروتکل های شبکه فقط کانالی را بین چند مولفه مخابراتی، ساماندهی و ایجاد می کنند و اجازه می دهند طراحان برنامه های کاربردی به پیاده سازی هر آنچه که مورد نیاز است بپردازند. به عنوان مثال ۸۰۲،۱۱ مشخص نکرده که کاربران باید صرفاً از کاربران باید صرفا از کامپیوتر کیفی خود برای خواندن ایمیل یا جستجو در وب یا هر چیز دیگری بهره بگیرند. برعکس، در تشریح بلوتوث نسخه V 1.1 از ۱۳ کاربرد مختلف که باید از آن‌ها پشتیبانی شود، نام برده شده و برای هر یک، پشته پروتکلی متفاوتی ارائه گردیده است. متاسفانه این راهکار به پیچیدگی بسیار زیتد منتهی می شود و ما از آن صرف نظر خواهیم کرد. این سیزده کاربرد که (پروفایل) نام گرفته‌اند در زیر فهرست شده‌اند با نگاهی اجمالی به پروفایلها ممکن است به آنچه که کنسرسیوم بلوتوث در پی انجام بیشتر پی ببریم.

نام پروفایل	عملکرد
Generic Access	روال هایی برای مدیریت لینک
Service Discovery	پروتکلی برای کشف سرویس‌های عرضه شده
Serial Port	جایگزینی برای کابل معمولی پورت سریال
Generic Object Exchenge	مدل ارتباطی بین سرویس دهنده و مشتری برای جابجایی اشیاء
LAN Access	پروتکل ارتباطی بین کامپیوتر همراه و شبکه محلی ثابت (با کابل مسی)
Dial-UP Networking	امکان برقراری تماس یک کامپیوتر کیفی زا طریق تلفن همراه را فراهم می‌آورد.

Fax	امکان ارتباط یک دستگاه دور نگار بی‌سیم و تلفن همراه را فراهم می‌آورد.
Cordless Teleohony	ارتباط بین یک دستگاه گوشی تلفن بی‌سیم و ایستگاه ثابت و محلی آن را برقرار می‌کند.
Intercom	امکانی برای واکی تاکی دیجیتال
Headset	امکان ارتباط از طریق هندزفری را فراهم می‌کند
Object Push	روشی برای مبادله اشیاء ساده
File Transfer	عرضه کننده امکانات عمومی بیشتر جهت انتقال فایل
Synchronization	امکان همزمان سازی داده‌های یک PDA با کامپیوتری دیگر

پروفایل عمومی دسترسی حقیقتاً یک برنامه کاربردی نیست بلکه بیشتر یک زیر بناست که بر اساس آن برنامه های کاربرهای حقیقس ساخته و پیاده می شوند. وظیفه اصلی آن ارائه تمهیداتی اسست که بتوان بین گروه اصلی (Master) و گروه پیرو (Slave) یک کانال مطمئن برقرار و آنرا حفظ کرد.

پروفایل تشخیص خدمات که آنهم تقریباً عمومی و کلی است توسط دستگاه‌هابرای آگاهی از خدماتی مه دیگر دستگاه‌ها ارائه می دهند، استفاده می شود. تمام دستگاه‌های مبتنی بر بلوتوث موظف به پیاده سازی این دو پروفایل هستند.بقیه پروفایلها اختیارینند.

پروفایل درگاه سریال یک پروتکل انتقال است که بقیه پروفایلها از آن بهره می گیرند. این پروفایل یک درگاه سریال را شبیه سازی می کند و ببطور خاص برای کاربردهای قدیمی که به خط سریال نیاز دارند، سودمند است.

پروفایل عمومی مبادله شی ء یک ارتباط مبتنی بر مدل مشتری/ سرویس دهنده، برای انتقال داده‌ها اعریف کرده است. اگر چه همیشه مشتری، آغاز کننده عملیات لست ولیکن یک گره پیرو می توان هم سرویس دهنده و هم مشتری باشد. همانند پروفایل درگاه سریال این پروفایل تیز زیر بنای دیگر پروفایلهاست.

گروه سه تائی پروفایلهای بعدی به منظور کاربردهای شبکه ای (Networking) تعریف شده‌اند. پروفایل دسترسی به LAN اجازه می دهد که یک دستگاه مبتنی بر بلوتوث به یک شبکه ثابت متصل شود.

این پروفایل رقیب مستقیم ۸۰۲.۱۱ است پروفایل شبکه مبنب بر شماره گیری (Dialup) انگیزه اصلی کل این پروژه بوده است. این پروفایل اجازه می دهد که یک کامپیوتر کیفی بتواند به یک تلفن همراه که دارای مودم داخلی بی سیم است متصل شود.پروفایل دورنگار (FAX) شبیه به پروفایل شماره گیری است با این تفاوت که اجازه می دهد ماشینهای دورنگار بی سیم از طریق یک دستگاه تلفن همراه و بدون نیاز به سیم، اقدام به ارسال یا دریافت دورنگار کنند.

سه پروفایل بعدی در خصوص تلفن کاربرد دارند. پروفایل تلفن بی سیم راهی را برای اتصال گوشی یک تلفن بی سیم به دستگاه ثابت است. در حال حاضر تلفنهای بی سیم خانگی را نمی توان به عنوان تلفن همراه به کارگرفت ولی در آینده شاید تلفن بی سیم و تلفن همراه در هم ادغام شوند.

پروفایل Intercom این امکان را فراهم می کند تا دو تلفن، شبیه به واکی تاکی بهم متصل گردند. نهایتا (پروفایل گوشی –Headset–) امکان ارتباط بی سیم بین گوشی و ایستگاه ثابت (مثل هندزفری Hands Free) را فراهم می کند که به عنوان مثال برای صحبت با تلفن در حین رانندگی مفید است.

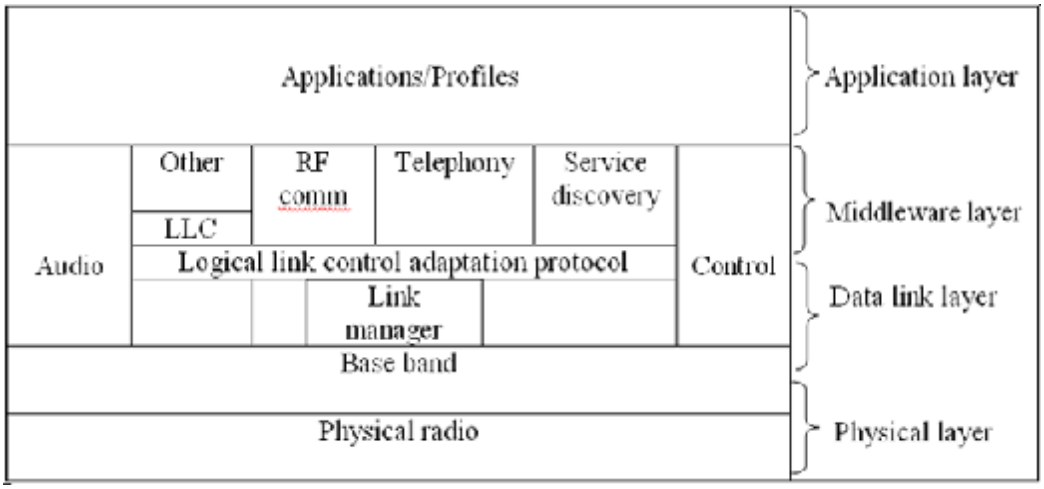
سه پروفایل باقیمانده برای مبادله اشیاء بین دو ابزار تعریف شده است. اشیاء می توانند فایلهای داده، تصویر یا کارتهای تجاری باشند پروفایل سنکرواسیون برای بار کردن داده در درون کامپیوتر کیفی یا PDA (کامپیوتر های دستی) در حین ترک منزل و جمع آوری اطلاعات پس از برگشت، مفید است.

آیا واقعاً نیاز بوده که تمام این کاربردها به تفصیل تحلیل شوند و برای هر کدام پشته پروتکلی متفاوتی تعریف گردد؟ شاید نه! اما بخشهای متفاوت این استاندارد را گروه‌ها بر روی نیازهای خاص خود متمرکز بودند، درنتیجه هر یک پروفایل مورد نظر خود را پدید آوردند.

برای توجیه این موضوع به قانون کانوی بیندیشید.(در یکی از شماره های مجله Datamation در آوریل ۱۹۶۸، ملوین کانوی مشاهدات خود را بدین نحو منتشر کرد که اگر n شخص را به نوشتن یک کامپایلر بگمارید، آنچه که بدست خواهید آورد یک کامپایر n-pass است (یعنی کامپایلری که در آن تعداد مراحل ترجمه یک برنامه، n گذر می باشد.) به عبارت عام ساهتار نهائی یک نرم‌افزار آیینه تمام نمای ترکیب گروهی است که آن را تولید کرده‌اند. شاید می شد که جای سیزده پشته پروتکلی به دو پشته کلی بسنده کرد: یکی برای انتقال فایل و دیگری برای انتقال بی درنگ جریان اطلاعات.

۹-۷-۴- پشته پروتکلی بلوتوث

استاندارد بلوتوث پروتکلهای متعددی دارد که بطور ناموزون در چند لایه گروه بندی شده‌اند. ساختار لایه‌ها از مدل OSI، مدل TCP/IP، مدل ۸۰۲ یا هر مدل شناخته شده دیگر تبعیت نمی کند. با این وجود IEEE در حال اصلاح بلوتوت است تا با مدل ۸۰۲ سازگارتر شود. معماری پروتکل بلوتوث که توسط کمیته ۸۰۲ اصلاح شده در شکل زیر مشاهده می شود.



لایه زیرین (لایه رادیو فیزیکی) است که تقریبا متناظر با لایه فیزیکی از مدل OSI یا مدل ۸۰۲ می باشد این لایه با انتقال رادیوئی و مدولاسیون سرکار دارد. بسیاری از ملاحظاتی که در طراحی این لایه باید مورد توجه قرار می گرفت آن بود که سیستم ارزان قیمت باشد و بطور انبوه در بازار عرضه شود.

(لایه باند پایه) از جهاتی شبیه به زیر لایه MAC است ولیکن مولفه هائی از لایه فیزیکی را نیز در بر می گیرد. این لایه با مسائلی مثل چگونگی نظارت گروه اصلی (Master) بر برشهای زمانی و چگونگی گروه بندی این برشهای زمانی در قالب فریمها، سرکار دارد.

سپس لایه ای شامل یک گروه از پروتکلهای مرتبط با هم، تعریف شده است. مدیر لینک (Link Manager)عملیات ایجاد کانالهای منطقی بین دستگاه‌ها، شامل (مدیریت توان مصرفی)، (احراز هویت) (Authentication) و کیفیت خدمات (QoS) را بر عهده دارد. پروتکل تطبیق کنترل لینک منطقی (که اغلب L2CAP گفته می شود) وظیفه دارد لایه هایی را از درگیری با جزئیات ارسال، راحت کند.این لایه مشابه با استاندارد زیر لایه LLC۸۰۲ است ولی از لحاظ مسائلی فنی با آن متفاوت است. دو پروتکل (کنترل) و (صدا) همانگونه که از نامشان بر می آید با مسائل انتقال صدا و عملیات کنترل سروکار دارند. برنامه های کاربردی می توانند.بدون نیاز به L2CAP، مستقیماً این دو پروتکل را به خدمت بگیرند.

لایه بعدی یک لایه میانی است و تلفیقی از پروتکلهای متفاوت را در می گیرد.

در این لایه از پروتکل IEEE 802 LLC، بمنظور سازگاری با دیگر شبکه های سری ۸۰۲ استفاده شده تست.

پروتکلهای RF comm. , Telephony و Service Discovery صرفا مرتبط با بلوتوث هستند RF comm. (Radio Frequency Communication)، پروتکلی جهت شبیه سازی استاندارد درگاه سریال (Serial port) است که تمام pcها از آن برای اتصال صفحه کلید، موس و امثال آن استفاده می شود. این پروتکل برای آن طراحی شده تا بتوان از دستگاه‌های قدیمی بسهولت استفاده کرد.

پروتکل تلفنی پروتکلی بی درنگ است که برای سه پروفایل مبتنی بر انتقال صدا بکار می آید. این پروتکل همچنین تنظیم و قطع ارتباط را برعهده دارد. نهایتاً پروتکل تشخیص خدمات (Service Discovery) برای کشف و تشخیص اناع خدماتی که درون شبکه عرضه می شود، کاربرد دارد.

بالاترین لایه، محل قرار گرفتن انواع برنامه های کاربردی و پروفایلها است. این لایه برای انجام کار از خدمات پروتکلهای موجود در لایه های زیر بهره می گیرد. هر برنامه کاربردی، و پروفایلها است. این لایه برای انجام کار از خدمات پروتکلهای موجود در لایه های زیر بهره می گیرد. هر برنامه کاربردی، زیر مجموعه ای از پروتکلهای مختص به خود را به خدمت می گیرد. ایزارهای ویژه ای مثل گوشی بی سیم بسته به نوع برنامه کاربردی آن‌ها فقط به برهی از پروتکل‌ها نیازمندند.

در بخشهای بعدی سه لایه پائینی از پشته پروتکلی بلوتوث را بررسی خواهیم کرد چرا که تقریباً متناظر زیر لایه های فیزیکی و MAC است.

۹-۷-۵- لایه رادیوئی در بلوتوث

لایه رادیوئی بیت‌ها را از گروه اصلی به گره پیرو و بالعکس، منتقل می کند. این لایه، سیستمی با توان کم و برد ده متر است که در باند فرکانسی ۲.۴ GHz ISM عمل مب کند. این باند به ۷۹ کانال یک مگاهرتزی تقسیم می شود. مدولاسیون به کاررفته FSK و هر هرتز (هر سیکل) معادل یک بیت است که جمعاً نرخ یک مگابیت بر ثانیه را در اختیار می گذارد ولی بیشتر این پهنای باند به دلیل سرباز تلف می شود.

برای تخصیص مناسب این کانالها از روش پرش فرکانس در طیف گسترده با نرخ پرس 1600 hops/sec, Dwell time معادل ۶۲۵ میکروثانیه بهره گرفته شده است.

چون بلوتوث و ۸۰۲.۱۱ هر دو باند 2.4GHz ISM و دقیقا در همان ۷۹ کانال کار می کنند لذا با یکدیگر تداخل فرکانس خواهد داشت. از آنجایی که پرش فرکانس در بلوتوث چون ۸۰۲.۱۱ و ۸۰۲.۱۵ هر دو استانداردهای IEEE هستند لذا IEEE به دنبال راه حلی برای این مشکل می گردد ولی حل این مشکل چندان ساده نیست چرا که هر دو سیستم، بدلیل مشابهب از این باند فرکانسی بهره گرفته‌اند: زیرا برای استفاده از این باند فرکانسی به اخذ هیچ مجوزی نیاز نیست. استاندارد 802.11a از باند دیگر ISM (باند GHz۵) استفاده می کند ولیکن برد کمتری نسبت به 802.11b دارد (دلیل ماهیت فیزیکی امواج رادیوئی این باند) لذا استفاده از 802.11a ره حل مناسبی نخواهد بود. برخی از شرکتها این مشکل را با ممنوعیت استفاده از بلوتوث حل کرده‌اند. راه حل بازاری این مشکل آنست که صبر کنیم مقابل بخواهد تا استاندارد خود را برای حل مشکل تداخل، اصلاح نماید. در این خصوص مطالبی در مرجع (Lansford et al. ,2001) ارائه شده است.

۹-۷-۶- لایه باند پایه در بلوتوث

لایه باند پایه شبیه ترین بخش بلوتوث با زیر لایه MAC است. این لایه، دنباله بیتهای خام را به فریمها تبدیل می کند و بدین منظور چندین قالب مهم فریم تعدیف نموده است. در ساده ترین حالت، گروه اصلی در هر پیکونت دنباله ای از برشهای زمانی ۶۲۵ میکروثانیه ای (Time Slot) Spread Spectrum تولید می کند، با این توصیف که ارسال داده های گره اصلی در برشهای زمانی با شماره زوج انجام می شود و گره های پیرو (Slaves) در برشهای زمانی فرد ارسال می نمایند. این روش مشابه با روش تسهیم زمانی (TDM) معمولی است که در آن گره اصلی نیمی از برشهای زمانی را در اختیار دارد و بقیه گره‌ها (حداکثر هفت گره) در نیم دیگر سهیم هستند. ارسال هر فریم می تواند ۱،۳ یا ۵ برش زمانی طول بکشد.

در هر پرش فرکانسی ۲۵۰ تا ۲۶۰ میکروثانیه طول خواهد کشید تا مدار رادیوئی بتواند پایداری سریعتر نیز از هر پرش فرکانسی، ۳۶۶ بیت از کل ۶۲۵ بیت باقی خواهد ماند. از این مقدار ۱۲۶ بیت به کد دسترسی (Access Code) و سر آیند اختصاص دارد و ۲۴۰ بیت برای داده‌ها باقی می ماند. وقتی پنج برش زمانی به هم ملحق می شوند {برای ارسال فریمها ئی به طول ۵ برش}تنها به یک زمان پایداری نیاز خواهد بود و طبعاً زمان کوتاهتری برای زمان پایداری، تلف می شود و ۳۱۲۵=۶۲۵×۵ بیت در پنج برش زمانی ارسال می گردد که از این مقدار ۲۷۸۱ بیت برای ارسال داده در اختیار لایه باند پایه خواهد بود. بنابر این در بلوتوث فریمهای طولانی کار آمدتر از فریمهای کوچک هستند.

هر فریم بر روی یک کانال منطقی که اصطلاحاً لینک بین گروه پیرو نام دارد ارسال خواهد شد. دو نوع لینک وجود دارد: لینک اول ACL است که برای ارسال داده‌ها در برشها زمانی نامنظم کاربرد دارد. این داده‌ها از لایه L2CAP می شوند. ترافیک داده های ACL مبتنی بر روش بیشترین تلاش (Best Effort) ارسال می شود ولی هیچ تضمینی در تحویل آن‌ها نیست. فریمها می توانند گم شده یا از بین بروند، بدون آنکه ارسال مجدد شوند. هر گره پیرو فقط می تواند یک لینک ACL با گره اصلی داشته باشد.

لینک دیگر، SCO نام دارد که برای ارسال داده های بی درنگ، مثل ارتباط تلفنی کاربرد دارد. این نوع کانال با تخصیص برشهای زمانی مشخص در هر دو جهت، ایجاد می شود. بدلیل آنکه لینکهای SCO نسبت به زمان حساس هستند

فلذا فریمهای ارسالی بر روی این لینک هرگز ارسال مجدد نخواهند شد، در عوض از روش تصحیح مستقیم خطا استفاده شده تا اطمینان بیشتری داشته باشد. ارسال مجدد فریمهای هراب بر عهده لایه بعدی است و در این لایه در صورت امکان به تصحیح خطا بسنده می شود–م هر گره پیرو می تواند حداکثر سه لینک SCO با گره اصلی داشته باشد. هر لینک SCO می تواند یک کانال صدا مبتنی بر PVM با نرخ ۶۴۰۰۰ بیت بر ثانیه را حمل کند.

۹-۷-۷- لایه CAP2L در بلوتوث

لایه L2CAP سه دسته عملیات مهم را بر عهده دارد: اول آنکه بسته هائی با طول حداکثر ۶۴ کیلوبایت را از لایه های بالائی پذیرفته و آن‌ها را جهت انتقال، به فریمهای کوچکتری می شکند. در سمت مقابل این فریمها مجدداً به بسته اصلی بازسازی خواهد شد.

دوم آنکه این لایه عمل جمع آور و توزیع بسته هائی که از چندین مبداء آمده (یا به چندین مقصد می روند) را بر عهده دارد. وقتی یک بسته بازسازی می شود لایه L2CAP تعیین خواهد کرد که باید به کدام پروتکل در لایه بالاترتحویل شود.

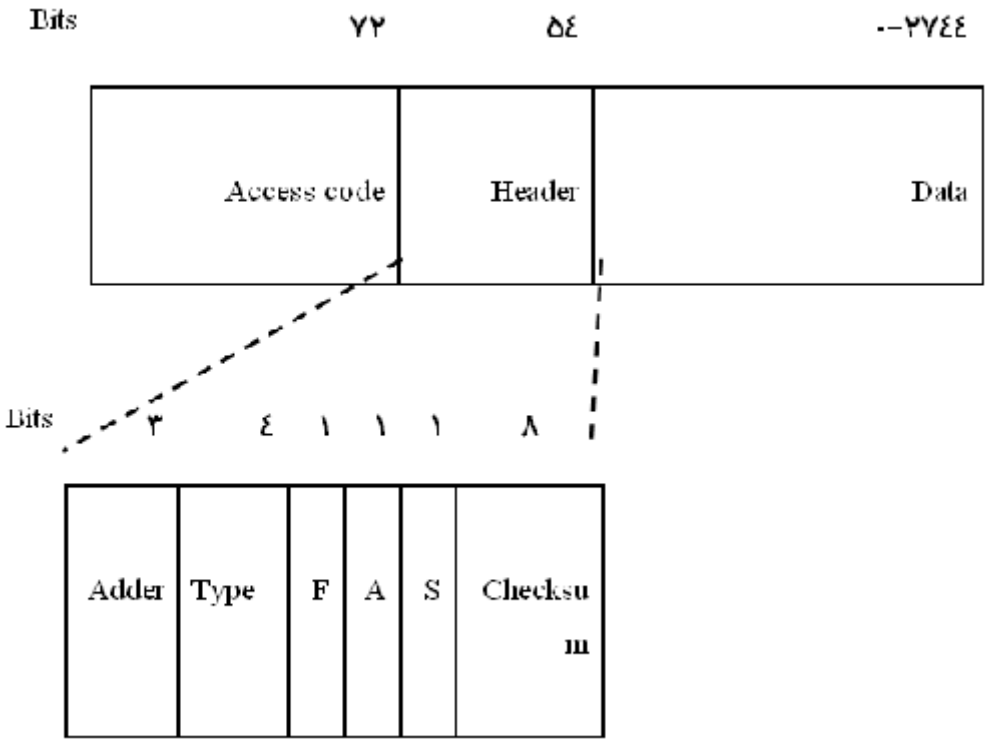
سوم اینکه این لایه، عملیات تامین کیفیت خدمات را بر عهده دارد چه در هنگام ایجاد لینک و چه در خلال عملکرد طبیعی. همچنین در زمان ایجاد لینک، بر سر اندازه حداکثر و مجاز طول داده، توافق صورت می گیرد تا ابرازهائی با طول بسته بزرگ از ارسال چنین بسته ای به ابزارهائی با طول بسته کوچک اجتناب کنند. از آنجایی که تمام ابزارهای مبتنی بر بلوتوث نمی توانند بسته هائی با طول ۶۴ کیلوبایت را بپذیرند فلذا به این ویژگی نیاز است.

۹-۷-۸- ساختار فرم در بلوتوث

چندین نوع قالب فریم در بلوتوث وجود دارد که مهمترین آن‌ها در شکل زیر نشان داده شده است. این فریم با فیلد کد دسترسی، ۱۴۱شروع می شود که عموما هویت یک گره اصلی Master را مشخص خواهد کرد تا بدینگونه یک گره پیرو که در برد رادیوئی دو گره اصلی قرار دارد، گیرنده حقیقی ترافیک داده‌ها را مشخص نماید.

سپس یک سرآیند ۵۴ بیتی آمده که شامل فیلدهای معمولی زیر لایه MAC است. سپس فیلد داده قرارگرفته که حداکثر ۲۷۴۴ بیت را برای انتقال در پنج برش زمانی در بر می گیرد. در فریمهائی که تنها در یک برش زمانی ارسال می شوند.قالب فریم همین است با این تفاوت که فیلد داده آن‌ها حداکثر ۲۴۰ بیت است.

حال اجازه بدهید به فیلدهای سرآیند، نگاهی سریع بیندازیم. فیلد آدرس هویت گیرنده فریم را از بین هشت دستگاه فعال در هر پیکونت مشخص می کند. فیلد Type اولا نوع فریم را از بین انواع ACL,SCO,POLL یا NULL ثانیاً روش تصحیح خطای داده‌ها را و ثانیا تعداد برشهای زمان که ارسال فریم جاری بدان نیاز دارد را مشخص می نماید.بیت Flow توسط گره های پیرو و زمانی تنظیم فعال می شود که بافر آن‌ها پرشده باشد و نتواند داده بیشتری دریافت کنند. این بیت شکل ابتدائی کنترل جریان داده‌ها، به حساب می آید.



بیت Acknowledgement بدین منظور است تا دریافت صحیح یک فریم از طرف مقابل، در فریم ارسالی جاسازی و اعلام شود (یعنی فرآیند Piggybacking). نظم بیتی برای شماره گذاری فریمهاست تا بسته های تکراری کشف شوند. در بلوتوث پروتکل ارسال مجدد روش توقف و انتظار است و طبعاً یک بیت برای شاره گذاری فریمها کفایت می کند. در ادامه فیلد هشت بیتی Checksum برای کشف خطای احتمالی در سرآیند تعریف شده است. کل این سرآیند ۱۸ بیتی سه بار تکرار می شود تا سرآیند ۵۴ بیتی نشان داده شده در شکل بالا بوجود آید.

در سمت گیرنده با یک مدار ساده سه نسخه تکراری هر بیت بررسی می شود. اگر هر سه بیت مثل هم بودند، آن بیت پذیرفته می شود در غیر اینصورت، بیتی که بیشترین تکرار را دارد قبول می شود. بدین ترتیب برای ارسال یک سرآیند ۱۰ بیتی ظرفیتی معادل ۵۴ بیت صرف می شود. دلیل آ« این بوده که برای ارسال مطمئن داده‌ها در محیطی سرشار از نویز و با ابزاری ارزان قیمت و توان ناچیز mW۲.۵ و قدرت پردازش پائین، یه افزونگی بسیار زیادی نیاز خواهد بود.

برای فیلد داده در فریمهای ACL قالبهای متفاوتی تعریف شده است. فریمهای SCO ساده‌تر هستند: فبلد داده همیشه ۲۴۰ بیتی است. سه گزینه دیگر نیز تعریف شده که در آن‌ها مقدار واقعی داده‌ها ۸۰، ۱۶۰ یا ۲۴۰ بیتی است و باقیمانده بیتها برای تصحیح خطا به کار می آیند. در مطمئن ترین نسخه (یعنی داده ۸۰ بیتی) بهش داده همانند سرآیند، سه بار متوالی تکرار می شود.

از آنجا یی که پیرو Slave تنها می تواند از برشهای زمانی با شماره فرد استفاده نماید فلذا در هر صانیه ۸۰۰ برش زمانی بدست خواهد آورد بدین ترتیب با فیلد داده ۸۰ بیتی، ظرفیت کانال از سمت گره پیرو به سمت گره اصلی معادل ۶۴۰۰۰ بیت بر ثانیه خواهد بود (ظرفیت کانال از گره اصلی به گره پیرو نیز ۶۴۰۰۰ بیت است) لذا این کانال دقیقاً برای یک کانال صوتی دو طرفه مبتنی بر pcm کافی است. (دلیل انتخاب نرخ ۱۶۰۰ Hops/sec برای تغییر فرکانس همین بوده است.)

این اعداد و ارقام بدین معنا هستند که یک کانال صوتی دو طرفه PCM با نرخ ۶۴۰۰۰ بیت بر ثانیه، در حالت مطمئن {یعنی وقتی داده های ۸۰ بیتی با سه بار تکرار ارسال می شوند کل پهنای باند موجود در پیکونت را (علیرغم پهنای باند 1Mbps آن) اشباع خواهد کرد.با گزینه نامطمئنتر (یعنی ۲۴۰ بیت در هر برش زمانی بدون هیچگونه افزونگی یا تکرار) می توان از حداکثر سه کانال صوتی همزمان حمایت کرد و به همین دلیل حداکثر سه لینک SCO برای هر گره پیرو مجاز شمرده شده است.

۹-۸- واژه نامه شبکه‌های بی‌سیم

در این بخش معانی برخی واژه‌های مورد استفاده در شبکه‌های بی‌سیم، به نمایش در خواهد آمد.

- 2G: امروزه رایج‌ترین نوع ارتباط تلفنی بی‌سیم است که ارتباطات اطلاعاتی کندی را فراهم می‌سازد و تمرکز اصلی آن روی کیفیت صدا است.
- 2.5G: یک استاندارد حد وسط و رابط بین G۲ و G۳ است. برقراری ارتباط به طریقه دیجیتال زمینه پست الکترونیکی و مرور وب آسان را فراهم می‌سازد.
- 3G: به عنوان سومین نسل از تکنولوژی ارتباطات بی‌سیم عمل می‌کند و حاکی از پیشرفت‌های سریع و قریب الوقوع در ارتباطات صوتی و اطلاع‌رسانی بی‌سیم با انواع استانداردهای موجود می‌باشد. مصرف اصلی این تکنولوژی، بالا بردن سرعت انتقال داده به ۲ مگابیت در ثانیه است.
- 802.11: گروهی از ویژگی‌های بی‌سیم می‌باشد که از سوی IEEE عرضه می‌شود و شامل رابط بی‌سیمی بین دستگاه‌ها برای کنترل ترافیک بسته‌های اطلاعاتی است (برای اجتناب از برخورد در انتقال داده و غیره). این ویژگی‌ها با علائم و نشانه‌های متفاوتشان شامل موارد زیر هستند.
- 802.11a: با دامنه فرکانس ۵ گیگاهرتز (۵.۱۲۵ تا ۵.۸۵ گیگاهرتز) و حداکثر سرعت سیگنال ٥٤ مگابیت در ثانیه عمل می‌کند. باند فرکانس ۵ گیگاهرتز به اندازه فرکانس ۲.٤ گیگاهرتز شلوغ نیست، چون کانال‌های بیشتری نسبت به 802.11b دارد و در واقع از 802.11b جدیدتر است، ولی با آن سازگاری ندارد.
- 802.11b: در باند ۲.٤ گیگاهرتزی، Industrial، 2.4 (ISM) Scientific and Measurement تا ۲.٤۸۳۵ گیگاهرتز عمل می‌کند و میزان سیگنال‌دهی آن تا ۱۱ مگابیت در ثانیه است که معمولا این میزان فرکانس کاربرد بیشتری دارد، مثل اجاق‌های مایکروویو، تلفن‌های بی‌سیم، تجهیزات علمی و پزشکی که همه همچون دستگاه‌های بلوتوث با باند ۲.٤ گیگاهرتز ISM کار می‌کنند.
- 802.11e:این استاندارد در اواخر ماه سپتامبر سال ۲۰۰۵ توسط IEEE تصویب شد. کیفیت سرویس دهی آن طوری است که می‌تواند کیفیت ترافیک صوتی و تصویری را تضمین نماید و برای شرکت‌هایی حائز اهمیت است که به استفاده از تلفن‌های WiFi تمایل دارند.
- 802.11g: شبیه 802.11b است، ولی این استاندارد از میزان سیگنال‌دهی تا ٥٤ مگابیت در ثانیه پشتیبانی می‌کند، همچنین در باند ISM، 2.4 گیگاهرتز کاربرد دارد، ولی از تکنولوژی رادیویی متفاوتی برای افزایش ظرفیت پذیرش کلی استفاده می‌کند؛ با 802.11b قدیمی نیز سازگار است.

- 802.11i: گاهی WPA 2 (WiFi Protected Access 2) نامیده می‌شود و در ژوئن سال ۲۰۰٤ به تصویب رسیده است. WPA 2 ازEncryption Standard Advanced (استاندارد رمزگذاری پیشرفته) در حد ۱۲۸ بیت و بالاتر از آن پشتیبانی می‌کند و با ویژگی‌های کنترل کلید و شناسایی کاربر 802.1x همراه است.
- 802.11k: در اواسط سال ۲۰۰٦ به تصویب می‌رسد و استانداردRadio Resource Management (کنترل منابع رادیویی) است که اطلاعات سنجش نقاط دستیابی و تغییرات لازم برای اجرای بهتر LAN (شبکه‌های) بی‌سیم را فراهم می‌سازد. مثلا می‌تواند با استفاده از نقاط دستیابی، بار ترافیک را مدیریت نماید یا به تنظیم مرتب و دائم نیروی انتقال داده، جهت کاهش تداخل (داده‌ها) کمک نماید.
- 802.11n: این استاندارد بهینه‌سازی برای توان عملیاتی بالاتر و برای بالا بردن ظرفیت پذیرش WLAN تا بیش از ۱۰۰ مگابیت در ثانیه طراحی شده است. این استاندارد در اواخر سال ۲۰۰٦ به تصویب نهایی می‌رسد.
- 802.11r: این استاندارد در سال جاری به تصویب می‌رسد و یک استاندارد گشت و گذار سریع است که برای حفظ ارتباط‌پذیری کاربر در هنگام جابه‌جایی و حرکت از یک نقطه دستیابی به نقطه دیگر به کار می‌رود، همچنین در برنامه‌های کاربردی که به استانداردهای کیفیت خدمات بالا با تاخیر کم، مثل کیفیت صدای روی WLAN نیاز دارند، مهم است.
- 802.11s: این استاندارد در شبکه‌بندی mesh به کار می‌رود و در اواسط سال ۲۰۰۸ به تصویب خواهد رسید. Access Point (نقطه دستیابی): یک فرستنده/گیرنده WLAN یا Base station است که می‌تواند یک شبکه را به شبکه دیگر یا چند دستگاه بی‌سیم وصل نماید. نقاط دستیابی (APها) به عنوان پل و رابطی برای یکدیگر هستند.
- حالت Ad hoc: یک چهارچوب شبکه بی‌سیم است که در آن دستگاه‌ها بدون اینکه لازم باشد از یکAP استفاده کنند یا به شبکه وصل شوند، قابلیت برقراری ارتباط مستقیم با یکدیگر را خواهند داشت و درست برعکس شبکه زیربنایی است که در آن همه دستگاه‌ها از طریق AP به یکدیگر وصل شده و ارتباط برقرار می‌نمایند.
- بلوتوث: یک لینک (اتصال) رادیویی کم هزینه با بورد کوتاه بین لپ‌تاپ‌ها، تلفن‌های همراه، نقاط دستیابی شبکه و دستگاه‌های دیگر است. بلوتوث می‌تواند جایگزین کابل‌ها شود و برای ایجاد شبکه‌هایAd hocمفید باشد، همچنین روش استانداردی را برای اتصال دستگاه‌ها در هر جای دنیا ارائه می‌دهد.
- Code Division Multiple Access یا CDMA: یک تکنولوژی سلولی دیجیتال است که از تکنیک‌های طیف گسترده استفاده می‌کند و به جای جداسازی کاربران از یکدیگر آن‌ها را با استفاده از کدهای فرکانس دیجیتال با دسترسی کامل به طیف، جدا می‌سازد. CDMA با GSM و TDMAرقابت می‌کند.
- تکنولوژی CDPD (Cellular Digital Packet Data) برای حاملان ارتباطات از راه دور کاربرد دارد که آن را برای انتقال داده به کاربران از طریق شبکه‌های سلولی آنالوگ استفاده نشده به کار می‌برند. اگر یک قسمت از شبکه مثل یک محدوده جغرافیایی خاص یا یک "سلول"، بیش از اندازه استفاده شود، CDPDمی‌تواند بطور خودکار منابع شبکه را برای کنترل ترافیک اضافه به کار برد.

- CTIA (Cellular Telecommunications & Internet Association): یک سازمان بین‌المللی است که به معرفی و عرضه همه عناصر مخصوص ارتباطات بی‌سیم، مثل سرویس‌های ارتباطات شخصی، سلولی، سرویس‌های پیشرفته مخصوص ماهواره و رادیوی سیار، کمک کرده و توجه سرویس دهندگان، سازندگان و غیره را به خود جلب می‌کند.
- EDGE: نرخ (سرعت) انتقال داده پیشرفته برای GSM Evolution است. این تکنولوژی 3G، انتقال داده به طریقه بی‌سیم را با سرعت ۳۸٤ کیلوبیت در ثانیه میسر می‌سازد و مبتنی‌بر تکنولوژی GSM بوده و امکان خدمات باندپهن بالایی، مثل مولتی مدیا (چند رسآن‌های) را فراهم می‌سازد. در آمریکای شمالی از آن بیشتر پشتیبانی می‌شود، چون تکنولوژی‌هایی مثل CDMA و UMTS مورد توجه بوده و کاربرد بیشتری دارد.
- Evolution Data Only یا Data Optimized Evolution: تکاملی از شبکه‌های CDMA است که بر مبنای استاندارد 1xRTT کار می‌کند و سرعت انتقال داده بی‌سیم بیشتری را یعنی از ٤۰۰ کیلوبیت در ثانیه به ۷۰۰ کیلوبیت در ثانیه، با رکورد تقریبی ۲.٤ مگابیت در ثانیه فراهم می‌سازد.
- FLASH-OFDM: یک تکنولوژی باندپهن سلولی اختصاصی است که اپراتورهای شبکه می‌توانند از آن برای کامپیوترهای نوت‌بوک کاربران در حال حرکت یا به عنوان یک سیستم دستیابی بی‌سیم ثابت استفاده کنند که برای اتصال کامپیوترهای خانگی و اداری کوچک تا آخرین مسافت، جواب می‌دهد. ویژگی‌های مهم آن، معماری IP کامل و سرعت بالای آن است. این تکنولوژی به کاربران امکان می‌دهد تا با سفر در حد ۲۵۰ کیلومتر در ساعت، داده را با سرعت ۱.۵ مگابایت در ثانیه دریافت کنند یا با سرعت ۵۰۰ کیلوبیت در ثانیه آن را ارسال نمایند. Division Multiplexing Orthogonal Frequency یا (OFDM) با تبدیل سیگنال‌های رادیویی به سیگنال‌های کوچکتر و با سرعت پایین‌تر که به صورت موازی منتقل می‌شوند، اختلال ایجاد شده هنگام انتقال را کاهش داده و از باندپهن کافی استفاده می‌کند، ولی بورد آن را کاهش می‌دهد.
- GPS یا Global Positioning System: "منظومه‌ای" از ۲٤ ماهواره است که زمین را در ارتفاع ۲۰،۲۰۰ کیلومتری دور می‌زند و استفاده از گیرندههای زمینی را برای افراد، جهت شناسایی موقعیت جغرافیایی آن‌ها بین ۱۰ تا ۱۰۰ متر امکان‌پذیر می‌سازد. این ماهواره‌ها از محاسبات ریاضی ساده‌ای برای پخش اطلاعات استفاده می‌کنند که به عنوان طول و عرض و ارتفاع جغرافیایی، توسط گیرندههای زمین ترجمه شده‌اند.
- GPRS: تکنولوژیGeneral Packet Radio Service با سرعت حداکثر ۱۱۵ کیلوبیت در ثانیه، در مقایسه با سرعت ٦/۹ کیلوبیت در ثانیه در سیستم‌های GSM قدیمی‌تر کار می‌کند؛ اینترنت و ارتباطات بی‌سیم دیگر با سرعت بالا، مثل پست الکترونیکی، بازی‌ها و برنامه‌های کاربردی را فعال و امکان‌پذیر می‌سازد، همچنین از حد وسیعی از باندپهن پشتیبانی کرده و در باندپهن محدود نیز کاربرد مناسبی دارد. برای ارسال و دریافت مقادیر کوچک داده، مثل نامه‌های الکترونیکی و مرور وب به همان اندازه مقادیر زیاد داده، مناسب است.
- Communications Global System for Mobile: یا GSM (سیستم جهانی مخصوص ارتباطات تلفنی) یک سیستم سلولی دیجیتال مبتنی‌بر تکنولوژی باند باریک TDMAاست که به کاربران امکان دسترسی به اسلات‌های

زمانی روی باندهای با همان فرکانس را می‌دهد، همچنین تا ۸ ارتباط همزمان با همان فرکانس را برقرار می‌سازد؛ این تکنولوژی رقیب DMAاست.

- HSDPA یا High-Speed Downlink Packet Access: یک تکنولوژی داده با سرعت بالای 3G است و در واقع همان استانداردWCDMA پیشرفته است که سرعت را بالا برده و میزان تاخیر را کاهش می‌دهد؛ با طیف ۵ مگاهرتز کار می‌کند و سرعت واقعی از ٤۰۰ کیلوبیت در ثانیه را به ٦۰۰ کیلوبیت در ثانیه می‌رساند؛ حداکثر سرعت تقریبی آن ٤/١٤ مگابیت در ثانیه می‌باشد.
- Hot spot: مکانی مثل، هتل، رستوران یا فرودگاه که دسترسی WiFi را به صورت رایگان یا با پرداخت هزینه امکان‌پذیر می‌سازد.
- I-Mode: یک سرویس اینترنت بی‌سیم عمومی است که در سال ۱۹۹۹ به وسیله شرکت NTT DoCoMoدر ژاپن دایر گردید و برمبنای شکل ساده شده‌ای از HTML کار می‌کند و اطلاعات بسته‌ای، مثل بازی‌ها، نامه‌های الکترونیکی و حتی برنامه‌های بازرگانی را برای دستگاه‌های کوچک دستی ارسال می‌کند.
- IEEE یا Institute of Electrical and Electronics Engineers: یک سازمان غیرانتفاعی فنی حرفه‌ای با بیش از ۳٦۰۰۰۰ کارمند اختصاصی در بیش از ۱۷۵ کشور است که در زمینه‌های فنی، مثل مهندسی کامپیوتر و ارتباطات از راه دور تخصص و صلاحیت دارد؛ این سازمان ویژگی‌های ۸۰۲.۱۱ را نیز توسعه داده است.
- MAC: هر دستگاه بی‌سیم۸۰۲.۱۱ دارای یک آدرس Media Access Control منحصر به خود است که درون آن بصورت کد و برنامه‌ای برای کنترل عملیات آن قرار گرفته است. این شناسه ویژه برای برقراری امنیت شبکه‌های بی‌سیم به کار می‌رود. وقتی یک شبکه از یک جدول MAC استفاده می‌کند، تنها رادیوهای ۸۰۲.۱۱ که دارای آدرس‌های MAC اضافه شده به جدولMAC شبکه بوده‌اند، می‌توانند به این شبکه دسترسی داشته باشند.
- Networking Mesh (شبکه‌بندی مش): نمایانگر گره‌های شبکه بی‌سیم و مجزا است که با یکدیگر در ارتباط بوده و شبکه‌هایی را می‌سازند که خود را پیکربندی نموده و تنها با گره‌ای این کار را انجام می‌دهند که برای قرار گرفتن درون یک LAN (شبکه) دارای سیم لازم است.
- MIMO یا Multiple Input Multiple Output: به استفاده از چند آنتن در یک دستگاه WiFi به ارتقاء عملکرد و ظرفیت پذیرش اشاره می‌کند. تکنولوژی MIMO از یک ویژگی به نام multipath (چند مسیری) بهره می‌گیرد و زمانی اتفاق می‌افتد که یک مخابره رادیویی در نقطهAآغاز شده و سپس قبل از دریافت از چند سطح یا شیء و از چند مسیر در نقطه Bعبور می‌کند. تکنولوژیMIMO از چند آنتن برای جمع‌آوری و سازماندهی سیگنال‌هایی استفاده می‌کند که از طریق این مسیرها دریافت می‌شوند؛ این تکنولوژی بیشتر در استاندارد 802.11n کاربرد دارد.
- RFID: شناسایی فرکانس رادیویی از فرستنده‌های رادیویی دارای برق ضعیف، برای خواندن اطلاعات ذخیره شده در یک tag فرستنده و گیرنده خودکار در فواصل بین ۲.۵ سانت تا ۳ متر استفاده می‌کند. Tagهای RFID برای کنترل دارایی‌ها، صورت موجودی و تایید و توصیه پرداخت‌ها به کار می‌روند و بیشتر به عنوان کلیدهای الکترونیکی در ابزارهای خودکار و تهدیدات امنیتی دیگر استفاده می‌شوند.

- Roaming: عبارت است از جابجایی یک دستگاه سیار از یک مکان و وضعیت شبکه بی‌سیم به دیگری بدون هیچ وقفه یا اختلال در سرویس یا قطع اتصال.
- Smart Phone (تلفن هوشمند): یک تلفن بی‌سیم با قابلیت‌های اینترنت و متن است که می‌تواند تماس‌های تلفنی بی‌سیم را کنترل نموده، آدرس‌ها را حفظ کند، پست صوتی را دریافت کرده، به اطلاعات روی اینترنت دست یافته و نامه‌های الکترونیکی و مخابره‌های فاکس را ارسال و دریافت نماید.
- Site Survey (بررسی سایت): در وضعیت یکWLANجدید برای اجتناب از اتلاف وقت و بروز مشکلات پرهزینه انجام می‌شود که شامل طراحی شبکه، کنترل روی ساخت و تجهیزات و آزمایش آن‌ها است.
- SMS یا Short Message Service (سرویس پیام کوتاه): امکان ارسال پیام‌های متنی کوتاه بین دستگاه‌های سیار، مثل موبایل، دستگاه‌های فکس وBerry Black را فراهم می‌سازد. این پیام‌ها با تعداد ۱۶۰ حرف الفبایی، فاقد تصویر یا گرافیک به عنوان متنی روی صفحه نمایش دستگاه گیرنده ظاهر می‌شوند و با شبکه‌های GSM نیز کار می‌کنند.
- SSI یا Service Set Identifier: یک سلسله کاراکتر منحصر به شبکه خاص یا بخشی از شبکه است که از شبکه و همه دستگاه‌های ضمیمه آن، برای شناسایی خود استفاده می‌کند و هنگامیکه بیش از یک شبکه مستقل در محلی نزدیک به هم وجود داشته باشند، به دستگاه‌ها امکان می‌دهند تا به شبکه درست متصل شوند.
- Symbian Ltd: یک سرمایه‌گذاری مشترک بین شرکت‌هایLM Ericsson Telephone، موتورولا، نوکیا وPsion PLC برای توسعه سیستم‌عامل‌های جدید مبتنی‌بر پلات‌فرمEPOC32شرکتPsionکه برای دستگاه‌های کوچک سیار و بی‌سیم، مثل تلفن‌ها و دستگاه‌های دستی مناسب می‌باشد.
- TDMA یا Time Division Multiple Access: یک فرکانس رادیویی در دسترس را به یک شبکه درون اسلات‌های زمانی تقسیم می‌کند و سپس این اسلات‌ها را به چند تماس اختصاص می‌دهد، بنابراین یک فرکانس از چند کانال داده همزمان پشتیبانی می‌کند و می‌تواند نسبت به تکنولوژی‌های قدیمی‌تر از باندپهن استفاده بهتری داشته باشد.TDMA در فرکانس‌های ۸۰۰ تا ۱۹۰۰ مگاهرتز در دسترس بوده و در سیستم سلولی دیجیتال GSM نیز به کار می‌رود.
- UMTS یا Universal Mobile Telecommunications System: یک تکنولوژی شبکه سلولی 3G است که از (Wideband Code WCDMA Division Multiple Access) استفاده می‌کند و از اواسط سال ۲۰۰۵ در ۲۵ کشور به اجر درآمده است. سرعت انتقال داده از ۳۸۴ کیلوبیت در ثانیه برای تلفن‌ها تا ۲ مگابیت در ثانیه برای دستگاه‌های ثابت می‌باشد.
- UWB یا Ultrawideband: که پالس دیجیتال نیز نامیده می‌شود، یک تکنولوژی بی‌سیم مخصوص انتقال اطلاعات دیجیتال به بخش وسیعی از طیف فرکانس رادیویی با قدرت بسیار پایین است و چون به برق ضعیفی نیاز دارد، می‌تواند سیگنال‌ها را از بین درها و دیگر موانعی که معمولا سیگنال‌ها را در باندهای پهن محدودتر با نیروی قویتر منعکس می‌کنند، عبور دهد، همچنین می‌تواند مقادیر زیادی از داده را حمل نماید و برای سیستم‌های مکآن‌های رادیویی و راداری که به زمین احاطه دارند، مناسب است.

- VoIP یا Internet Protocol Voice over: سیستمی برای ارائه ارتباطات صوتی رقمی شده (دیجیتالی شده) از طریق شبکه‌های IP است. این تکنولوژی به تلفن‌های دستی سازگار با یکدیگر یا کامپیوترهای دارای نرم‌افزار مناسب امکان می‌دهد تا تماس تلفنی برقرار نمایند.
- WAP یا The Wireless Application Protocol: مجموعه‌ای از ویژگی‌ها است که به وسیله WAP Forum توسعه یافته است و به توسعه‌دهندگان امکان می‌دهد تا با استفاده از Wireless، برنامه‌های کاربردی شبکه‌بندی شده مناسب برای دستگاه‌های بی‌سیم دستی را بسازند.WAP برای کار با این دستگاه‌ها و محدودیت‌هایشان طراحی شده است: یک حافظه و اندازه cpu محدود، صفحه نمایش‌های کوچک و سیاه‌وسفید، باندپهن کم و اتصالات نامنظم.WAPیک استاندارد واقعی است که بیش از ۲۰۰ فروشنده از آن پشتیبانی می‌کند.
- WCDMA یا Wideband Code Division Multiple Access: یک تکنولوژی بی‌سیم 3G است که از CDMA نشات می‌گیرد و اطلاعات دیجیتالی شده را روی دامنه وسیعی از فرکانس‌ها، جهت افزایش سرعت ارسال می‌کند و از کانال‌های وسیع ۵ مگاهرتزی استفاده می‌نماید و برای بالا بردن سرعت با جایگزین کردن تکنولوژی TDMA به جای CDMA به GSM و UMTS وابسته است. برای سرویس‌های تصویری، صوتی و اطلاع رسانی مفید بوده و می‌تواند با سرعت تا ۲ مگابیت در ثانیه داده را ارسال نماید.
- WEP یا Wired-Equivalent Privacy protocol: در استاندارد IEEE 802.11 برای ایجاد یک WLAN با حداقل سطح ایمنی و حفاظت، در مقایسه با یک LAN دارای سیم، با استفاده از رمزنگاری داده تعیین شده است. اکنون به خاطر طول نامناسب کلید و مشکلات دیگر آن ناقص شناخته شده و با وجود ابزارهای در دسترس می‌تواند به زودی مورد تهاجم قرار گیرد.
- WME یا Wireless Multimedia Extensions: مجموعه‌ای از ویژگی‌های مبتنی بر استاندارد مقدماتی IEEE 802.11e است که ویژگی‌های اولیه QoS (کیفیت خدمات) را در شبکه‌های IEEE 802.11 ارائه می‌دهد. WME ترافیک برنامه‌های کاربردی مختلف، مثل برنامه‌های صوتی و تصویری را در محیط‌ها و شرایط مختلف در اولویت قرار داده است.
- WPA یا WiFi Protected Access: یک ویژگی رمزنگاری داده برای شبکه‌های بی‌سیم ۸۰۲.۱۱ است که جایگزینWEPضعیف‌تر شده است. WPA به وسیله اتحادیه WiFi، قبل از تصویب استاندارد امنیتی802.11i توسط IEEE ایجاد شده و با استفاده از کلیدهای فعال وExtensible Authentication Protocol (پروتکل شناسایی کاربر قابل توسعه)، برای ایمن‌سازی دسترسی به شبکه و روشی برای کدگذاری به نام (TKIP) Temporal Key Integrity Protocol برای ایمن‌سازی ارسال اطلاعات، WFPرا بهینه می‌سازد.
- WPA2 یا WiFi Protected Access 2: یک نسخه ارتقاء یافته از WPA است. WPA استاندارد رسمی 802.11i بوده که به وسیله IEEE در ژوئن ۲۰۰٤ به تصویب رسیده و به جای TKIP (فوق‌الذکر) از استاندارد Advanced Encryption استفاده می‌کند. AESاز کلیدهای ۱۲۸، ۱۹۲ و ۲۵٦ بیت پشتیبانی می‌نماید.
- WiFi یا Wireless fidelity: یک اصطلاح عمومی برای تکنولوژی۸۰۲.۱۱ است.

- WLAN: شبکه‌های محلی بی‌سیم، از امواج رادیویی به جای کابل برای اتصال یک دستگاه کاربر استفاده می‌کنند، مثل اتصال لپ‌تاپ به یک LAN. آن‌ها اتصالات اترنت را برقرار ساخته و در گروه و خانواده۸۰۲.۱۱ که ویژگی‌های آن به وسیله IEEE توسعه یافته است، به کار می‌روند.
- War driving: به رانندگی با یک لپ‌تاپ با قابلیت بی‌سیم و آنتن برای یافتن مکآن‌هایی جهت دستیابی به شبکه‌های بی‌سیم بی‌حفاظ، اشاره می‌کند. آن‌ها معمولا شبکه‌های شرکتی بوده که در خارج از زیربنای واقعی شرکت توسعه یافته و به صورت بی‌حفاظ باقی مانده‌اند.
- WiMax: نام عمومی استاندارد شبکه بی‌سیم ۸۰۲.۱۶ مخصوص منطقه پایتخت است که باید تاکنون توسعه یافته باشد.WiMax که دارای برد ۵۰ کیلومتر می‌باشد و دستیابی به باند پهن شبکه با مشکل کمتر در دسترس‌پذیری و بدون پرداخت هزینه بابت به رشته درآوردن سیم‌ها (مثل دسترسی کامل در باندپهن) یا محدودیت‌های فاصله، Subscriber Digitalرا هدف قرار داده است. دو نوع WiMax وجود دارد: یکی 802.16-2004 یا 802.16d برای پیاده‌سازی‌های ثابت و 802.16e برای سرویس‌های متحرک.
- WML یا Wireless Markup Language: مثل زبان برنامه‌نویسی اینترنتHTML است که محتوای اینترنت را به دستگاه‌های کوچک بی‌سیم، مثل تلفن‌های موبایل مجهز به مرورگر و دستگاه‌های دستی که دارای صفحه نمایش‌های کوچک و سی‌پی‌یوهای کند، ظرفیت حافظه محدود و باندپهن کم با قابلیت‌های ورودی محدود کاربر هستند، ارسال می‌کند.
- WiFi Alliance: یک سازمان بین‌المللی غیرانتفاعی که در سال ۱۹۹۹ برای تصویب قابلیت عمل محصولات WLAN مبتنی‌بر ویژگی IEEE 802.11 در چند محیط تشکیل شد. در حال حاضر نیز اتحادیه WiFi دارای بیش از ۲۰۰ شرکت عضو از سراسر دنیا می‌باشد و بیش از ۱۰۰۰ محصول گواهینامه WiFi را دریافت کرده است، یعنی از زمان شروع ارائه گواهینامه آن در مارس۲۰۰۰. هدف اعضای این اتحادیه، بالا بردن میزان آگاهی و تجربه کاربران است.

فصل ۱۰

شبکه‌های حسگر

۱۰-۱- خلاصه

پیشرفت‌های اخیر در بخش‌های مختلف تکنولوژی بویژه در بخش سیستم‌های میکروالکترومکانیکی (MEMS) ظهور نوع تازه‌ای از شبکه‌های الکترونیکی با نام شبکه‌های حسگر (Sensor Network) را ممکن ساخته است. شبکه‌های حسگر معمولا متشکل از تعداد زیادی گره‌های خودمختار و محدود از نظر نیرو، قدرت پردازش و توانایی برقراری ارتباط می‌باشند که نزدیک یا داخل پدیده مورد بررسی قرار می‌گیرند. با ظهور این نوع شبکه‌ها و ارائه پروتکل‌ها و معماری‌های مختلف کاربردهای متنوعی برای آن پیش بینی شدند که برخی از آن‌ها به مرحله پیاده سازی رسیده‌اند و بسیاری نیز هنوز در دست پژوهش هستند. در این مقاله سعی شده است مروری بر مباحث اساسی در شبکه‌های حسگر از قبیل؛ وجه تمایز این نوع شبکه از سایر شبکه‌ها، معماری، پروتکل‌های مسیریابی و کاربردهای پیشنهاد شده برای آن داشته باشیم.

۱۰-۲- مقدمه

۱۰-۲-۱- توصیف شبکه‌های حسگر

پیشرفت‌های اخیر در صنعت الکترونیک و ارتباطات، تولید گره‌های حسگر چند منظوره، کم هزینه و با مصرف پائین انرژی را در ابعاد کوچک و با امکان ایجاد ارتباط در فواصل کوتاه را امکان پذیر ساخته است. این گره‌های حسگر که شامل اجزایی برای حس کردن محیط، پردازش داده و ارتباط می‌باشند، بستر لازم برای ظهور شبکه‌های حسگر را فراهم نموده‌اند. یک شبکه حسگر از تعداد زیادی گره حسگر تشکیل شده است که با تراکم بالا داخل پدیده‌ای که مورد نظر است یا بسیار نزدیک به آن استقرار داده می‌شود. مکان گره‌های حسگر نیازی به تعیین و تنظیم قبلی ندارند. این ویژگی امکان استقرار این نوع گره‌ها را بصورت کاملا تصادفی در مکآن‌های غیر قابل دسترسی یا خطرناک ایجاد می‌کند. از سوی دیگر، این ویژگی نیاز به در نظر گرفتن قابلیت خود پیکربندی را در پروتکل‌ها و الگوریتم‌های مختص این شبکه‌ها مطرح می‌کند. ویژگی دیگر شبکه‌های حسگر تلاش جمعی گره‌های حسگر است. گره‌های حسگر مجهز به یک پردازنده ساده هستند تا بجای ارسال داده

خام دریافت شده از محیط، پردازش مختصری بر روی داده‌ها انجام دهند و محاسبات محلی را تنها به کمک گره‌های نزدیک خود انجام دهند. این عمل یعنی ارسال داده‌های کم تعداد ضروری و پردازش شده بجای ارسال داده‌های خام و متعدد هم باعث کاهش ترافیک شبکه می‌شود و هم باعث می‌شود عملیات جمع آوری بهتر و ساده‌تر صورت گیرد.

ویژگی‌های تعریف شده در قسمت قبل امکان ایجاد طیف وسیعی از کاربردها را برای این نوع شبکه فراهم می‌کند. برخی از کاربردهای ممکن کاربردهای مرتبط با بهداشت، مسایل نظامی و خانه‌های هوشمند می‌باشند. بطور نمونه، در مسایل نظامی ویژگیهای قابلیت خود پیکربندی، استقرار سریع و تحمل خطا شبکه‌های حسگر را برای سیستم‌های نظامی اعمال دستور، کنترل، ارتباطات، محاسبات، هوشمندی، مراقبت، شناسایی و هدف گیری بسیار مناسب می‌نماید. در کاربردهای بهداشت، شبکه‌های حسگر می‌توانند برای مراقبت از بیماران و کمک به بیماران دارای ناتوانی جسمی به کار گرفته شوند. برخی کاربردهای تجاری دیگر شامل مدیریت انبار، نظارت بر کیفیت محصولات و نظارت بر مناطق حادثه خیز می‌باشند.

اگرچه طبق تعریف، شبکه‌های حسگر می‌توانند از ارتباطات باسیم نیز برای تبادل داده بهره ببرند، در سال‌های اخیر بجز موارد نادر کاربردها از رسانه بی‌سیم در این نوع شبکه استفاده کرده‌اند که دلیل آن وسعت حوزه کاربردها و سادگی استفاده آن بدون ایجاد زیر ساخت اختصاصی می‌باشد. از شبکه‌های حسگر بی‌سیم با نماد WSN یاد می‌شود. در سال‌های اخیر شبکه‌های WSN به دلیل پیچیدگی و وسعت زمینه پژوهش، غالب پژوهش‌ها در حوزه شبکه‌های حسگر را به خود اختصاص داده‌اند. لذا ما نیز در این فصل مبنای بررسی خود را شبکه‌های WSN قرار می‌دهیم.

درک کاربردهای شبکه‌های حسگر بی‌سیم نیاز به شناخت تکنیک‌های شبکه سازی دارد. اگرچه پروتکل‌ها و الگوریتم‌های متعددی برای شبکه‌های Ad hoc بی‌سیم ارائه شده‌اند، آن‌ها به طور کامل مناسب ویژگی‌ها و نیازمندی‌های کاربردهای شبکه‌های حسگر نیستند. تفاوت‌های اصلی بین شبکه‌های حسگر و Ad hoc عبارتند از:

- در شبکه‌های حسگر تعداد گره‌ها می‌تواند چندین برابر یک شبکه Ad hoc باشد.
- گره‌های حسگر به طور انبوه و با تراکم بالا استقرار داده می‌شوند.
- گره‌های حسگر بسیار مستعد خرابی هستند.
- توپولوژی شبکه‌های حسگر به سرعت تغییر می‌کند.
- گره‌های حسگر اغلب از مدل ارتباطی همه پخشی استفاده می‌کنند در حالی که ارتباطات در شبکه‌های Ad hoc معمولا مبتنی بر مدل ارتباطی نقطه به نقطه است.
- گره‌های حسگر معمولا در میزان حافظه، توان محاسباتی و انرژی محدود هستند.
- گره‌های حسگر معمولا به دلیل تعداد زیاد حسگرها و ایجاد سربار زیاد فاقد شناسه سراسری می‌باشند.

در سالهای اخیر اغلب پژوهشگران سعی در توسعه روش هایی برای برطرف کردن این نیازمندیها داشته‌اند. در این فصل سعی شده است تا جنبه‌های مختلف این تکنولوژی نوظهور مورد بررسی قرار گیرد.

ادامه فصل به صورت زیر تنظیم شده است: در قسمت سوم به بررسی ویژگی‌های اصلی شبکه‌های حسگر که می‌بایست در طراحی‌ها لحاظ شود، خواهیم پرداخت. در قسمت چهارم به بیان معماری شبکه‌های حسگر می‌پردازیم. در قسمت پنجم طبقه بندی‌های پیشنهادی برای کاربردهای احتمالی این نوع شبکه‌ها معرفی می‌شود و در قسمت ششم به بررسی پروتکل‌های

مسیریابی شناخته شده در آن‌ها پرداخته می‌شود. در قسمت هفتم به بررسی مختصر نوع خاصی از شبکه‌های حسگر با نام WSAN می‌پردازیم که پیش بینی می‌شود طیف وسیعی از کاربردها تحت آن ارائه شوند. در انتها نیز با ارائه یک جمع بندی کوتاه از عناوین مطرح شده، فصل را در قسمت هشتم به پایان خواهیم برد.

۱۰-۲-۲- تفاوت های شبکه های بی‌سیم و کابلی

منبع: سمانه ا... یاری؛ "شبکه‌های حسگر بی‌سیم"؛ پروژه کارشناسی؛ دانشگاه فردوسی مشهد

برطبق دسته بندی متداول شبکه‌ها به دو صورت کابلی و بی‌سیم طراحی می‌شوند. درابتدا به روش کابلی با استفاده از تکنولوژی Ethernet طراحی می‌شدند اما اکنون با روند رو به افزایش استفاده از شبکه های بی‌سیم مواجه هستیم. در هرصورت هر دو نوع شبکه های کابلی و بی‌سیم ادعای برتری بر دیگری را دارند اما انتخاب صحیح با در نظر گرفتن قابلیت های آن‌ها میسر می‌باشد.

در مقایسه شبکه های بی‌سیم و کابلی می‌توان به مورد زیر اشاره کرد:

۱) نصب و راه اندازی: در شبکه های کابلی به دلیل آن که به هر یک از ایستگاه های کاری بایستی از محل سوئیچ مربوطه کابل کشیده شود با مسائلی همچون سوراخکاری، نصب پریز و... مواجه هستیم، درضمن اگر محل فیزیکی ایستگاه موردنظر تغییر یابد بایستی که کابل‌کشی مجدد صورت پذیرد؛ درحالیکه شبکه های بی‌سیم از امواج استفاده نموده و قابلیت تحرک بالائی را در اختیار دارند. بنابراین تغییرات در محل فیزیکی ایستگاه های کاری به راحتی امکانپذیر می‌باشد، برای راهاندازی آن کافیست که ازروشهای زیر بهره برد:

- ✓ Adhoc:که ارتباط مستقیم یا همتا به همتا تجهیزات را با یکدیگر میسر میسازد.
- ✓ Infrastructure: که باعث ارتباط تمامی تجهیزات با دستگاه مرکزی می‌شود.

پس می‌توان دریافت که نصب و راهاندازی شبکه های کابلی یا تغییرات در آن بسیار مشکل‌تر نسبت به شبکه های بی‌سیم است.

۲) هزینه: تجهیزاتی همچون هاب، سوئیچ یا کابل شبکه نسبت به موارد مشابه در شبکه های بی‌سیم ارزانتر می‌باشد، اما درنظرگرفتن هزینه های نصب و تغییرات احتمالی محیطی نیز قابل توجه است. قابل به ذکر است که با رشد روز افزون شبکه های بی‌سیم، قیمت آن نیز در حال کاهش است.

۳) قابلیت اطمینان: تجهیزات کابلی بسیار قابلاعتماد می‌باشندکه این دلیل سرمایه گذاری سازندگان از حدود بیست سال گذشته می‌باشد؛ فقط بایستی در موقع نصب و یا جابجائی، اتصالات با دقت کنترل شوند. تجهیزات بی‌سیم با مشکلاتی مانند قطع شدن های پیاپی، تداخل امواج الکترومغناطیس، تداخل با شبکه های بی‌سیم مجاور و... مواجه است که روند رو به تکامل آن نسبت به گذشته باعث بهبود در قابلیت اطمینان آن‌ها شده است.

۴) امنیت: به دلیل اینکه در شبکه های کابلی که به اینترنت هم متصل هستند، وجود دیواره ی آتش از الزامات است و تجهیزاتی مانند هاب یا سوئیچ به تنهایی قادر به انجام وظایف دیواره آتش نمی‌باشند، بایستی در چنین شبکه هایی دیواره آتش مجزایی نصب شود. درتجهیزات شبکه‌های بی‌سیم دیوارهی آتش به صورت نرم‌افزاری وجود داشته و تنها بایستی تنظیمات لازم صورت پذیرد. از سوی دیگر به دلیل اینکه در شبکه های بی‌سیم از هوا به عنوان رسانه انتقال استفاده می‌شود، بدون پیاده

سازی تکنیک های خاصی مانندرمزنگاری، امنیت اطلاعات به طور کامل تأمین نمی‌گردد. استفاده از رمزنگاری باعث بالا رفتن امنیت در این تجهیزات گردیده است.

۱۰-۲-۳- تاریخچه شبکه‌های حسگر بی‌سیم

منبع: سمانه ا... یاری؛ "شبکه‌های حسگر بی‌سیم"؛ پروژه کارشناسی؛ دانشگاه فردوسی مشهد

همانند بسیاری دیگر از فناوری‌ها، کار بر روی شبکه‌های حسگر از کارهای نظامی و دفاعی آغاز شد.در طول جنگ سرد، دولت آمریکا، حمایت از پروژهای به نام سیستم نظارت صوتی را بر عهده گرفت. در این پروژه با قرار دادن تعدادی حسگر در نقاط استراتژیک زیر اقیانوس، سعی در تشخیص نفوذ و ردیابی زیر دریایی های شوروی داشتند.

کار بر روی شبکه‌های حسگر به طور جدی از سال ۱۹۸۰ و با پروژهی شبکه‌های حسگر توزیع شده در آژانس پروژه های تحقیقات دفاعی پیشرفته آمریکا آغاز شد. پروژه WINS در سال ۱۹۹۳ و با همکاری دانشگاه کالیفرنیا و مرکز علوم شرکت Rockwell شروع شد. این پروژه در سال ۱۹۹۸ به یک محصول تجاری تبدیل شد. درحدود سال ۱۹۹۹ دانشگاه برکلی دو پروژه تحقیقاتی بر روی شبکه‌های حسگر آغاز کرد. پروژه PicoRadio و Smart Dust پروژه های بلند پروازانه بود و هدف آن ساختن گره های حسگری با ابعاد یک میلیمتر مکعب بود که البته به موفقیت هایی هم رسید.

در سالهای اخیر پروژه‌های دیگری مانند µAMPS در دانشگاه MIT و پروژه SenseIT توسط آژانس پروژه های تحقیقات دفاع آمریکا انجام گرفته است و تحقیقات در این زمینه به شتاب روز افزونی در مجامع علمی و تحقیقاتی در حال گسترش است.

همانطور که در مقدمه بیان شد پیشرفتهای اخیر در فنا وری ساخت مدارات مجتمع در اندازه های کوچک از یک سو و توسع هی فناوری ارتباطات بی‌سیم از سوی دیگر زمینه ساز طراحی شبکه‌های حس/کار بی‌سیم شده است. تفاوت اساسی این شبکه‌ها ارتباط آن با محیط و پدیده های فیزیکی است. شبکه‌های سنتی ارتباط بین انسآن‌ها و پایگاه های اطلاعاتی را فراهم می‌کند در حالی که شبکه حس/کار مستقیماً با جهان فیزیکی در ارتباط است. با استفاده از حسگرها محیط فیزیکی را مشاهده کرده، بر اساس مشاهدات خود تصمیم‌گیری نموده و عملیات مناسب را انجام میدهند. نام شبکه حس/کار بی‌سیم یک نام عمومی است برای انواع مختلف که به منظورهای خاص طراحی می‌شود. برخلاف شبکه‌های دیگر که همهمنظورهاند شبکه های حس /کارنوعاً تک منظوره هستند. در صورتی که گره‌ها توانایی حرکت داشته باشند شبکه می‌تواند گروهی از ربات های کوچک درنظرگرفته شود که با هم به صورت تیمی کار می‌کنند و جهت مقصد خاصی مثلاً بازی فوتبال یا مبارزه با دشمن طراحی شده است. از دیدگاه دیگر اگر در شبکه تلفن همراه ایستگاه های پایه را حذف نماییم و هر گوشی را یک گره فرض کنیم ارتباط بین گره‌ها باید به طور مستقیم یا از طریق یک یا چند گره میانی برقرار شود. این خود نوعی شبکه حس/کار بی‌سیم می‌باشد. اگرچه تاریخچه شبکه های حس /کار به دوران جنگ سرد و ایده اولیه آن به طراحان نظامی صنایع دفاع آمریکا برمی‌گردد، ولی این ایده می‌توانسته در ذهن طراحان ربات های متحرک مستقل یا حتی طراحان شبکه‌های بی‌سیم موبایل نیز شکل گرفته باشد.

کاربرد فراوان این نوع شبکه و ارتباط آن با مباحث مختلف مطرح در کامپیوتر و الکترونیک ازجمله امنیت شبکه، ارتباط بلادرنگ، پردازش صوت و تصویر، دادهکاوی، رباتیک، طراحی خودکار سیستمهای جاسازی شده دیجیتال و... میدان وسیعی برای پژوهش محققان با علاقمندی های مختلف فراهم نموده است.

با این تفاسیر وجود برخی ویژگیها در شبکه حسگر/ کارانداز، آن را از سایر شبکه‌های سنتی بی‌سیم متمایز می‌کند. از آن جمله عبارتند از:

۱. تنگناهای سخت‌افزاری شامل محدودیت های اندازه فیزیکی، منبع انرژی، قدرت پردازش، ظرفیت حافظه

۲. تعداد بسیار زیاد گره ها

۳. چگالی بالا در توزیع گره‌ها در ناحیه عملیاتی

۴. وجود استعداد خرابی در گره ها

۵. تغییرات توپولوژی به صورت پویا و احیاناً متناوب

۶. استفاده از روش پخش همگانی در ارتباط بین گره‌ها در مقابل ارتباط نقطه به نقطه

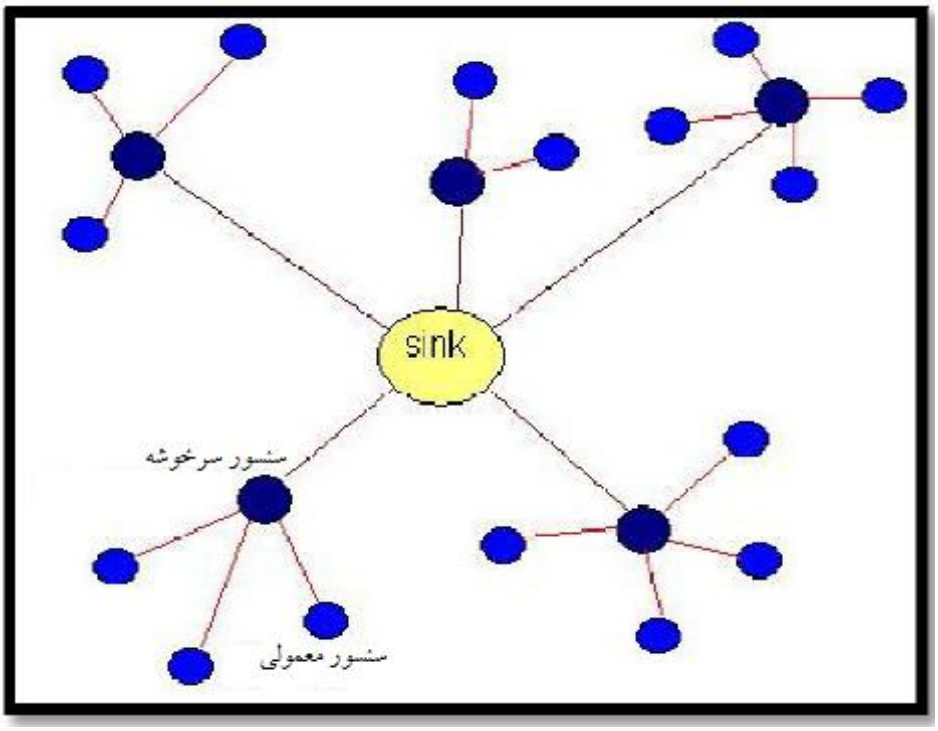
۷. داده محور بودن شبکه به این معنی که گره‌ها کد شناسایی ندارند.

۱۰-۲-۴- ویژگی های عمومی شبکه حسگر

منبع: سمانه ا... یاری؛ "شبکه‌های حسگر بی‌سیم"؛ پروژه کارشناسی؛ دانشگاه فردوسی مشهد

علاوه بر نکاتی که تاکنون درباره شبکه های حسگر بیان کردیم، این شبکه‌ها دارای یک سری ویژگی های عمومی نیز هستند. مهم ترین این ویژگی‌ها عبارتنداز:

۱. برخلاف شبکه های بی‌سیم سنتی، همه گره‌ها در شبکه های حسگر بی‌سیم نیازی به برقراری ارتباط مستقیم با ایستگاه پایه ندارند.در واقع برخی از پروتکل‌ها در این شبکه‌ها برای تأمین نیازمندی های شبکه‌های حسگر از خوشه بندی استفاده می‌کنند، بدین ترتیب که حسگرها به ناحیه هایی تقسیم می‌شوند که هر ناحیه دارای یک سرخوشه است و پس از وقوع یک رویداد هر ناحیه، اطلاعات خود را به سرخوشه ارسال می‌کنند وسرخوشه این اطلاعات رامستقیم به اطلاع چاهک میرساند. جمع آوری اطلاعات توسط سرخوشه‌ها به منظورکاهش اطلاعات ارسالی از گره‌ها به ایستگاه پایه و در نتیجه بهبود بازده انرژی شبکه انجام می‌شود. البته چگونگی انتخاب سرخوشه خود بحثی تخصصی است که معمولا در تئوری شبکه های بی‌سیم حسگر مورد بحث قرار می‌گیرد. شکل زیر را ملاحظه نمایید.

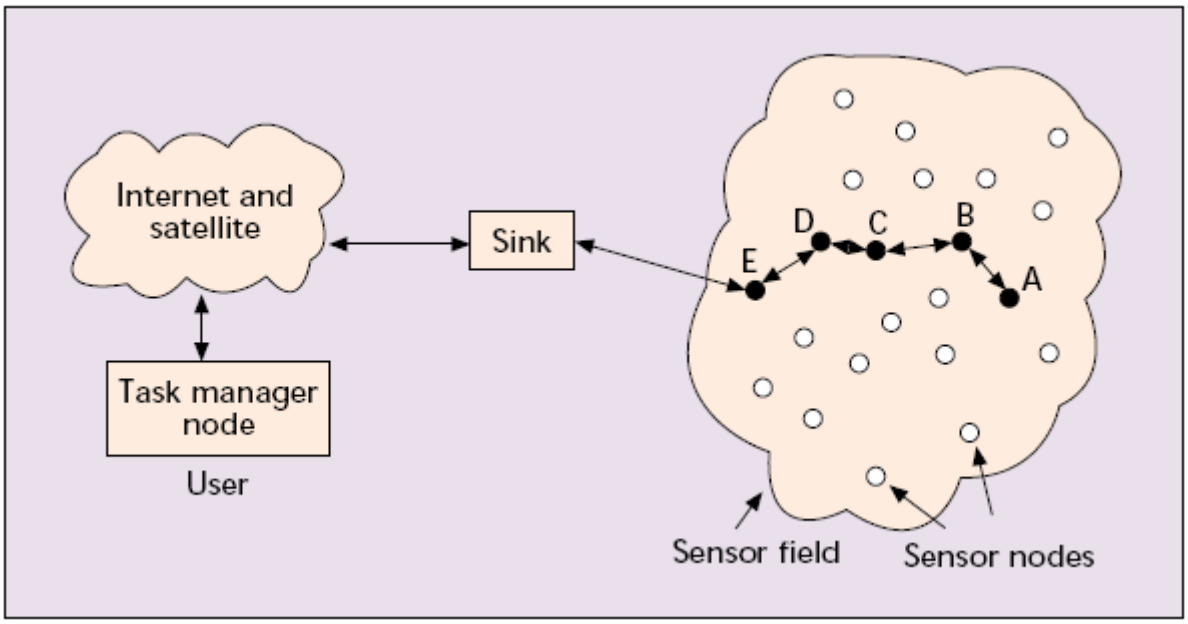


۲. پروتکل های شبکه ای نظیر به نظیر یک سری ارتباطات مش (Mesh) مانند را جهت انتقال اطلاعات بین هزاران دستگاه کوچک با استفاده از روش چندجهشی ایجاد می‌کنند. معماری انطباق پذیر مش، قابلیت تطبیق با گره های جدید جهت پوشش دادن یک ناحیه جغرافیایی بزرگ‌تر را دارا است. علاوه براین، سیستم می‌تواند به طورخودکار از دست دادن یک گره یاحتی چند گره را جبران کند.

۳. هر حسگر موجود درشبکه دارای یک گستره حسگری است که به نقاط موجود در آن احاطه کامل دارد. یکی از اهداف شبکه های حسگری این است که هر محل در فضای مورد نظر بایستی حداقل در گستره حسگری یک گره قرار گیرد تا شبکه قابلیت پوشش همه منطقه موردنظر را داشته باشد. یک حسگر با شعاع حسگری r رامی توان با یک دیسک با شعاع r مدل کرد. این دیسک نقاطی را که درون این شعاع قرار می‌گیرند، تحت پوشش قرار می‌دهد. بدیهی است که برای تحت پوشش قرار دادن کل منطقه این دیسک‌ها باید کل نقاط منطقه را بپوشانند. با این که توجه زیادی به پوشش کامل منطقه توسط حسگرها می‌شود، احتمال دارد نقاطی تحت پوشش هیچ حسگری قرار نگیرد. این نقاط تحت عنوان حفره های پوششی نامیده می‌شوند.

۱۰-۳- ویژگی‌های طراحی

گره‌های حسگر معمولا در یک حوزه حسگر آنچنانکه در شکل ۱ نشان داده شده است، پراکنده می‌شوند. همگی این گره‌ها قابلیت جمع آوری داده و ارجاع آن به گره چاهک (Sink) یا ایستگاه پایه (Base Station) را دارا می‌باشند. داده‌های جمع آوری شده با استفاده از یک معماری بدون زیر ساختار چند گامی (Multihop Infrastructureless Architecture) شبیه به شکل ۱ به سمت گره چاهک ارسال می‌شوند.



گره چاهک ممکن است با استفاده از اینترنت یا ماهواره به گره مدیر کار (Task Manager) متصل شده باشد. طراحی شبکه‌های حسگر همانطور که در شکل ۱ نمایش داده شده است، از چندین فاکتور اصلی شامل تحمل خرابی، مقیاس پذیری، هزینه تولید، محیط اجرا، توپولوژی شبکه‌های حسگر، محدودیت‌های سخت‌افزاری، رسانه انتقال و مصرف انرژی، تاثیر می‌پذیرد. در ادامه به بررسی این فاکتورها می‌پردازیم.

۱۰-۳-۱- تحمل خطا

برخی از گره‌های حسگر ممکن است به دلایل کمبود انرژی، آسیب فیزیکی و یا تداخلات محیطی از کار بیفتد. این خرابی‌های گره‌های حسگر نباید تاثیری در عملکرد کلی شبکه حسگر داشته باشد. این مبحث همان قابلیت اطمینان یا تحمل خطاست. تحمل خطا توانایی فعال نگه داشتن شبکه حسگر بدون هیچ وقفه‌ای به دلیل خرابی گره‌های حسگر می‌باشد.

تحمل پذیری اشکال یا قابلیت اطمینان با توزیع پواسون در بازه (0, t) مدل می‌شود:

$$R_k(t) = e^{-\lambda_k t}$$

که در آن λ_k نرخ خرابی برای گره k ام و دوره زمانی t است.

۱۰-۳-۲- مقیاس پذیری

تعداد گره‌های حسگر استقرار داده شده برای مطالعه یک پدیده ممکن است از مرتبه صدها یا هزارها باشد. بسته به نوع کاربرد این تعداد ممکن است به چندین میلیون هم ارتقا پیدا کند. یک روش کامل باید قابلیت کار با این تعداد گره را فراهم کند. روش ارائه شده همچنین می‌بایست تراکم بالای شبکه‌های حسگر را مورد بهره برداری قرار دهد. این تراکم یا چگالی می‌تواند شامل استقرار چند تا چند صد گره حسگر در یک ناحیه با شعاع حدود ۱۰ متر شود. تراکم (α) می‌تواند بصورت زیر محاسبه شود:

$$\alpha(R) = (N.\pi R^2)/A$$

که در آن N تعداد گره‌های پراکنده شده در ناحیه A و پارامتر R طیف رادیویی انتقال هر گره می‌باشد. در حقیقت $\alpha(R)$ متوسط تعداد گره‌های قرار گرفته شده در شعاع انتقال هر گره را در ناحیه A را بیان می‌کند.

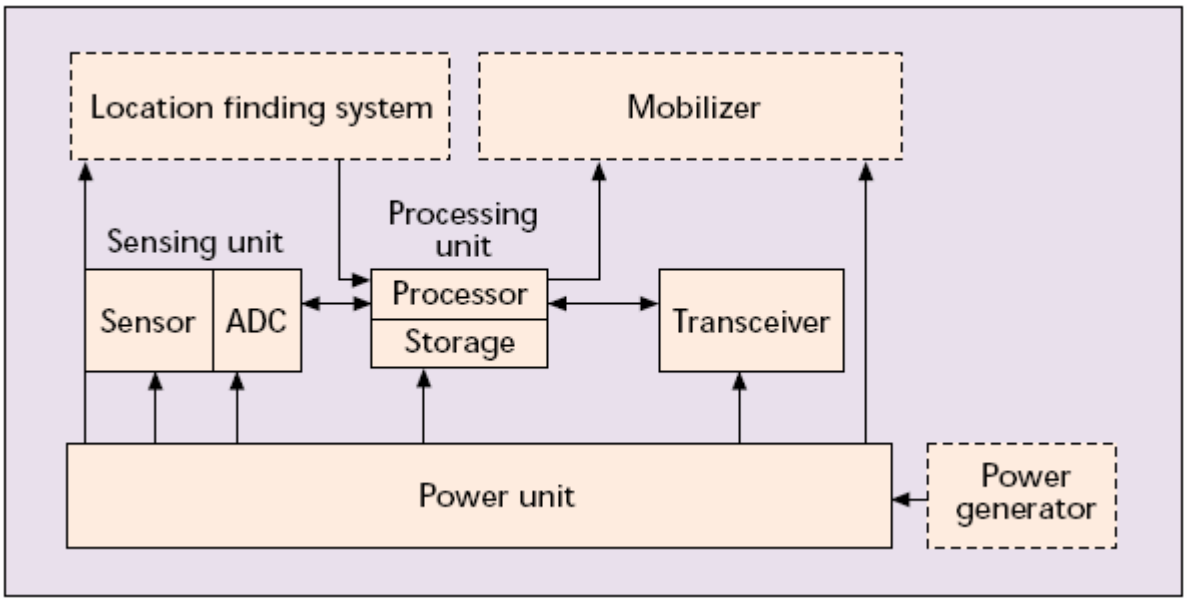
۱۰-۳-۳- هزینه تولید

به دلیل آنکه شبکه‌های حسگر شامل تعداد زیادی از گره‌های حسگر می‌باشند، هزینه یک گره منفرد برای توجیه اقتصادی هزینه کل شبکه بسیار مهم است. اگر هزینه شبکه حسگر بسیار گران‌تر از استقرار حسگرهای سنتی باشد آنگاه این شبکه توجیه اقتصادی نخواهد داشت.

در نتیجه، هزینه هر گره منفرد می‌بایست پائین نگه داشته شود. تکنولوژی بسیار پیشرفته امروزی اجازه تولید سیستم‌های رادیویی بلوتوث با هزینه کمتر از ۱۰ دلار آمریکا را فراهم کرده است. این هزینه بسیار شگفت انگیز است اما باز هم برای امکان پذیر بودن توسعه و استقرار شبکه‌های حسگر هزینه هر گره می‌بایست سعی شود هزینه هر گره منفرد به کمتر از یک دلار کاهش یابد.

۱۰-۳-۴- محدودیت‌های سخت‌افزاری

همانطور که در شکل زیر نمایش داده شده است، یک گره حسگر از چهار جزء اصلی تشکیل شده است: واحد احساس (Sensing)، واحد پردازش، واحد فرستنده – گیرنده و واحد نیرو. همچنین این گره‌ها ممکن است شامل اجزای اضافی دیگری مختص کاربردهای خاص مانند سیستم یافتن مکان، تولید کننده نیرو و جابجا کننده (Mobilizer) باشند.



واحد احساس معمولا شامل دو زیر قسمت می‌شود: حسگرها و مبدل آنالوگ به دیجیتال (ADC). سیگنال‌های آنالوگ تولید شده توسط حسگرها بعد از احساس و دریافت یک پدیده از محیط توسط ADC به سیگنال دیجیتال تبدیل و سپس به واحد پردازش ارائه می‌شود. واحد پردازش، که معمولا شامل حافظه کوچکی نیز می‌باشد، مدیریت و اجرای پروسه‌های ارتباطی که در نظر گرفته شده در هر گره جهت ارتباط با سایر گره‌ها و انجام وظایف تخصیص داده شده را به عهده دارد. واحد فرستنده – گیرنده نیز گره را به شبکه متصل می‌نماید.

یکی از اجزای بسیار مهم در گره حسگر واحد نیرو است. واحد نیرو ممکن است شامل یک واحد تولید یا بازیافت نیرو مثل سلول‌های خورشیدی باشد. اجزای دیگری نیز که وابسته به کاربرد هستند وجود دارند. بطور نمونه بسیاری از تکنیک‌های مسیریابی در شبکه‌های حسگر نیازمند اطلاع از مکان خویش و گره‌های مجاور با دقت بالا می‌باشند. بنابراین، قابل توجیه

خواهد بود که در صورت نیاز کاربرد، هر گره حسگر شامل یک سیستم یافتن مکان نیز باشد. در برخی از کاربردها نیز ممکن است یک جابجا کننده برای جابجا کردن گره‌های حسگر در جهت انجام وظیفه تخصیص داده شده، مورد استفاده قرار گیرد.

معمولا همه این اجزا می‌بایست داخل یک بسته به اندازه یک قوطی کبریت جا داده شود. در برخی موارد اندازه مورد نیاز ممکن است در حد یک مکعب مربع یک سانتیمتری باشد که حتی ممکن است آنقدر سبک باشد که امکان معلق ماندن در هوا را هم داشته باشد. جدا از اندازه، برخی محدودیت‌های دشوار سخت‌افزاری دیگر در شبکه‌های حسگر وجود دارند. این گره‌ها می‌بایست مصرف نیروی به شدت پائین داشته باشند، توانایی عمل در در حالتهای استقرار با تراکم بالا را دارا باشند، هزینه تولید آن‌ها بسیار کم باشد، خود مختار باشند، بدون نیاز به نظارت خارجی عمل کنند و سازگار با محیط خود باشند.

۱۰-۳-۵- توپولوژی شبکه‌های حسگر

در شبکه‌های حسگر معمولا چند صد تا چند هزار گره در یک حوزه حسگر پراکنده شده‌اند. آن‌ها در فاصله چند فوتی از یکدیگر قرار گرفته‌اند و تراکم گره‌ها می‌تواند تا ۲۰ گره در متر مکعب باشد. این تراکم بالا نیازمند اداره دقیق توپولوژی می‌باشد. سه مرحله در پشتیبانی توپولوژی و تغییر آن عبارتند از:

- مرحله پیش از استقرار و استقرار: گره‌های حسگر می‌توانند به صورت توده‌ای در محیط پراکنده شوند یا به صورت دانه به دانه چیده شوند. آن‌ها می‌توانند بوسیله یک هواپیما یا راکت بصورت توده‌ای و تصادفی و یا دانه به دانه توسط انسان یا ربات استقرار داده شوند.
- مرحله بعد از استقرار: بعد از استقرار، ممکن است به دلیل تغییر در مکان گره‌های حسگر، قابلیت دسترسی (به دلیل نویز، موانع متحرک و...) یا میزان انرژی، خراب کار کردن گره‌ها و توپولوژی تغییر یابد.
- مرحله استقرار مجدد گره‌های اضافی: گره‌های حسگر اضافی می‌توانند در هر زمانی برای جایگزینی گره‌های خراب و یا اعمال تغییرات پویا در نحوه اجرای کار استقرار داده شوند.

۱۰-۳-۶- محیط عمل

گره‌های حسگر با تراکم بالا درون پدیده مورد بررسی یا بسیار نزدیک به آن استقرار داده می‌شوند. بنابراین، می‌بایست توانایی عمل به صورت خود مختار و بدون نیاز به کنترل در نواحی جغرافیایی دور را دارا باشند. محیط عمل در شبکه‌های حسگر ممکن است داخل یک ماشین بزرگ در انتهای اقیانوس، یک ناحیه آلوده شده شیمیایی یا بیولوژیکی، پشت خطوط دشمن در میدان جنگ و یک خانه یا ساختمان بزرگ باشد.

۱۰-۳-۷- رسانه انتقال

در یک شبکه حسگر چند گامی، گره‌های ارتباطی بوسیله یک رسانه بی‌سیم به هم متصل می‌شوند. این اتصالات می‌توانند بوسیله رادیو، مادون قرمز و یا رسانه نوری صورت گیرد. برای ایجاد قابلیت بکارگیری این نوع شبکه‌ها در سراسر دنیا، رسانه انتقال انتخاب شده می‌بایست در تمام دنیا موجود و در دسترس باشد. اغلب مدارات موجود امروزی مبتنی بر امواج رادیویی هستند.

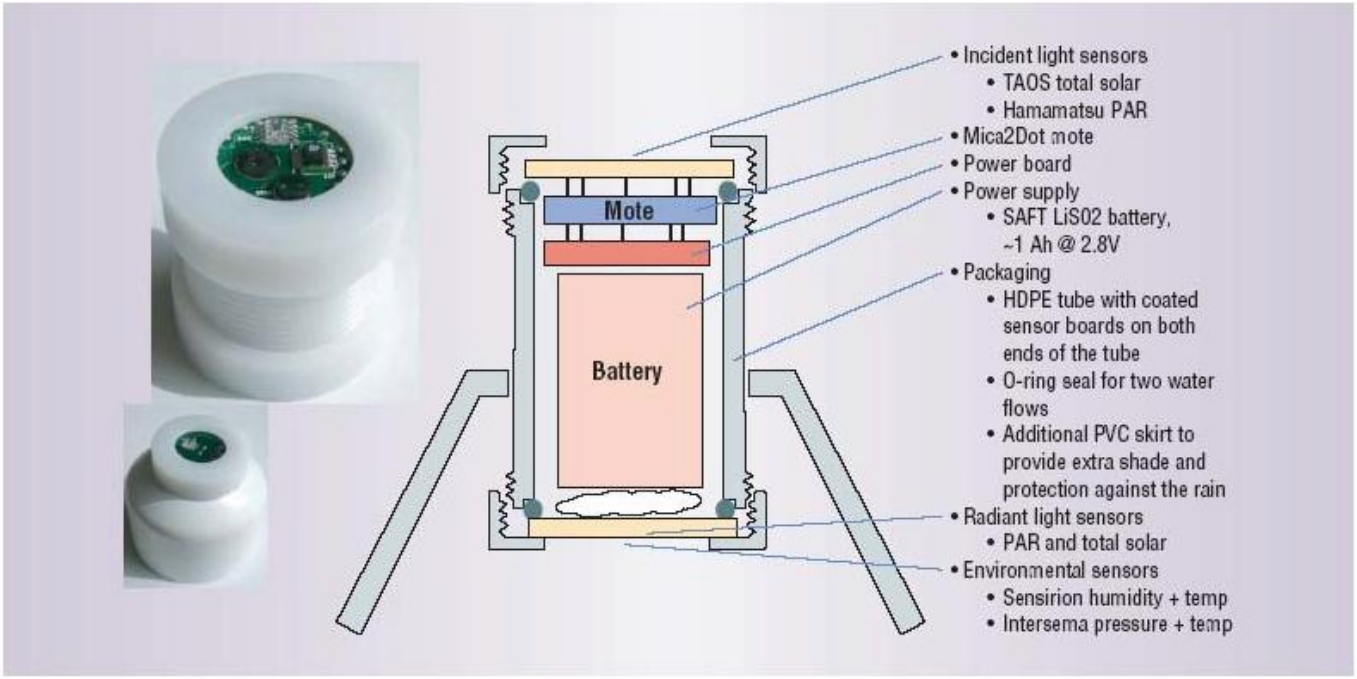
حالت دیگر برای ارتباطات میان گره‌ای در شبکه‌های حسگر مادون قرمز است. ارتباطات مادون قرمز نیازمند مجوز نیستند و در مقابل تداخل وسایل الکترونیکی مقاوم هستند. همچنین گیرنده و دریافت کننده‌های مادون قرمز برای تولید ساده‌تر و ارزان‌تر هستند. نوع دیگر ارتباطات یعنی رسانه نوری در پروژه ذره‌های غبار هوشمند استفاده شده است که یک سیستم احساس، محاسبه و ارتباط خود مختار می‌باشد. هم ارتباط مادون قرمز و هم رسانه نوری نیازمند خط دید (Line of Sight) می‌باشند.

۱۰-۳-۸- مصرف انرژی

گره‌های حسگر بی‌سیم که با استفاده از قطعات میکرو الکترونیک ساخته شده‌اند تنها با منبع نیروی محدودی می‌توانند تجهیز شوند (معمولا <0.5 Ah, 1.2 V). در برخی از کاربردها شارژ یا تعویض منابع نیرو غیر قابل انجام است بنابراین، طول عمر گره حسگر بستگی زیادی به عمر باطری آن دارد.

در یک شبکه حسگر، مشابه شبکه‌های Ad hoc هر گره بسته به زمان هم نقش تولید کننده داده و هم نقش مسیریاب را ایفا می‌کند. خرابی یا از کار افتادن تعداد اندکی از گره‌ها می‌تواند باعث ایجاد تغییرات قابل توجه در توپولوژی شبکه و نیاز به مسیریابی مجدد بسته‌ها یا سازماندهی مجدد شبکه شود. بنابراین، ذخیره نیرو و مدیریت نیرو اهمیت مضاعف پیدا می‌کند. از این رو، تاکنون پروتکل‌های آگاه نسبت به نیروی بسیاری توسط پژوهشگران پیشنهاد شده است.

وظیفه اصلی یک گره حسگر در یک حوزه حسگر احساس محیط و کشف وقایع آن، انجام عملیات سریع محلی و پردازش اولیه داده‌ها و ارسال داده نهایی است. در نتیجه، مصرف نیرو می‌تواند به سه قسمت تقسیم شود که عبارتند از احساس، پردازش داده و ارتباط که بیشترین مصرف را بخش ارتباطات دارا می‌باشد. لذا اغلب پژوهشگران به دنبال کاهش دفعات ارتباط و خاموش کردن قسمت فرستنده – گیرنده گره‌های حسگر در زمان‌های بی کاری به عنوان راهکاری برای کاهش مصرف انرژی در گره‌ها و در نتیجه افزایش طول عمر مفید شبکه حسگر بوده‌اند. در شکل ۳ عناصر یک گره حسگر واقعی که برای تشخیص میزان رطوبت در جنگلهای آمازون طراحی شده است، دیده می‌شود.



۱۰-۳-۹- داده محوری

در برخی از کاربردها به دلیل اهمیت و هزینه کم و طول عمر نسبتا کوتاه گره‌های حسگر، استقرار افزونه گره‌های حسگر صورت می‌گیرد. در نتیجه، اهمیت هر یک از گره‌ها به صورت خاص در مقایسه با شبکه‌های سنتی (که در آن‌ها کاربر قصد اتصال تنها و تنها به یک سرور خاص را برای برآورده کردن نیازش داشت) کاهش می‌یابد. در این حالت داده همه گره هایی که توانایی مشاهده پدیده‌ای را دارند ارزش یکسان دارند و بنا به دلایل تکنیکی مثل مصرف انرژی می‌توانیم به دسته‌ای از آن‌ها متصل شویم تا نیاز ما برآورده شود. لذا در حقیقت داده احساس شده دارای اهمیت است نه گره خاص. این تغییر در محتوای موارد مهم، هم امکان و هم نیاز به تغییر در روش شبکه سازی از معماری گره محور به معماری داده محور را ایجاد می‌کند.

۱۰-۴- معماری

در این قسمت به بررسی معماری و پشته پروتکل پیشنهادی برای شبکه‌های حسگر می‌پردازیم.

۱۰-۴-۱- پشته پروتکل در شبکه‌های حسگر

پشته پروتکل مورد استفاده در گره‌های حسگر و گره ویژه چاهک در شکل ۴ نمایش داده شده است. این پشته پروتکل آگاهی نیرو و مسیریابی را ترکیب می‌کند، داده را با پروتکل‌های شبکه سازی یکپارچه می‌کند، ارتباطات موثر و بهینه از نظر نیرو در رسانه بی‌سیم ایجاد می‌کند و تلاش جمعی گره‌های حسگر را بهبود می‌بخشد. این پشته شامل **لایه فیزیکی، لایه پیوند داده، لایه شبکه، لایه انتقال، لایه کاربرد** و سه لایه مدیریتی **طرح مدیریت نیرو، طرح مدیریت جابجایی** و **طرح مدیریت کار** می‌باشد.

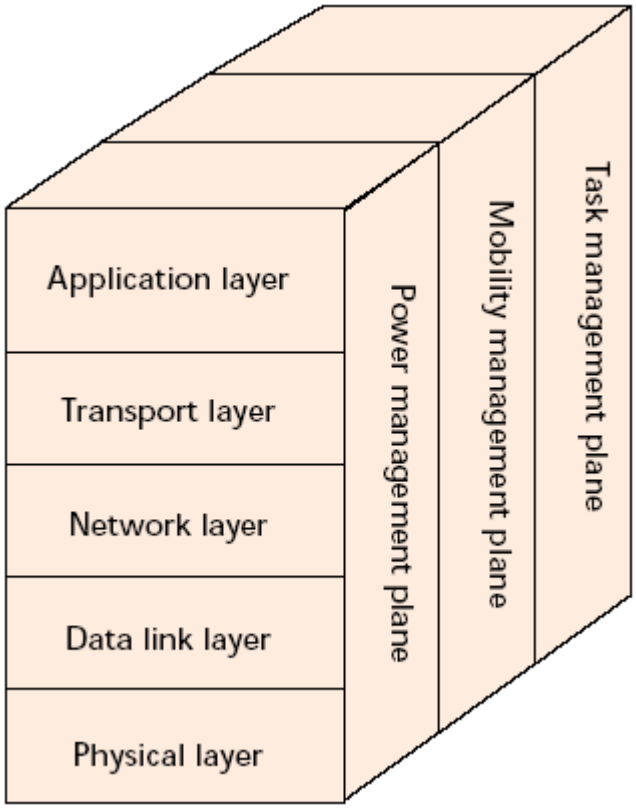
لایه فیزیکی وظیفه تعیین نوع مدولاسیون و انجام آن، و بکارگیری تکنیک‌های دریافت و ارسال ساده اما استوار (Robust) را بر عهده دارد. به دلیل وجود نویز در محیط و قابلیت جابجایی گره‌های حسگر، لایه **کنترل دسترسی به رسانه** (MAC) در شبکه‌های حسگر می‌بایست آگاه به نیرو و قادر به کمینه کردن برخورد با همه پخشی‌های گره‌های مجاور باشد. **لایه شبکه** وظیفه مسیریابی داده تهیه شده توسط **لایه انتقال** را به عهده دارد. **لایه انتقال** نیز به برقراری جریان داده مورد نیاز هر کاربرد کمک می‌کند. بسته به نوع گره‌ها و توانایی‌های آن‌ها در احساس محیط، انواع مختلفی از کاربردها نیز می‌توانند ساخته و در **لایه کاربرد** استفاده شوند.

بعلاوه، طرح‌های مدیریت نیرو، جابجایی و کار، حرکت و توزیع کار میان گره‌های حسگر را مورد نظارت قرار می‌دهند. این طرح‌ها باعث همکاری گره‌ها در کار و به صورت کلی باعث کاهش مصرف نیرو می‌شوند. طرح مدیریت نیرو چگونگی استفاده گره حسگر از نیرویش را مدیریت می‌کند. برای نمونه، گره حسگر می‌تواند بعد از دریافت پیامی از گره‌های مجاور خود قسمت دریافت خود را خاموش کند. این عمل باعث عدم دریافت پیغام‌های تکراری چند مسیری می‌شود. همچنین وقتی سطح نیروی موجود در یک گره پائین باشد، گره حسگر به همه گره‌های مجاور خود اعلام می‌کند که انرژی کمی دارد و نمی‌تواند در مسیریابی پیغام‌ها شرکت کند. انرژی باقیمانده گره حسگر نیز برای احساس محیط استفاده می‌شود.

طرح **مدیریت جابجایی** حرکت گره حسگر را تشخیص و ثبت می‌کند و به کاربر اعلام می‌کند و این کار باعث می‌شود که گره‌های حسگر بتواند در هر لحظه تشخیص دهند در مجاورت آن‌ها چه گره هایی وجود دارند. با اطلاع از اینکه چه گره‌های حسگری در همسایگی وجود دارند، گره‌ها می‌توانند بین نیرو و کار تخصیص داده شده به آن‌ها تعادلی برقرار کنند.

طرح **مدیریت کار** وظیفه احساس یک ناحیه خاص را زمان بندی و متعادل می‌کند. لزومی ندارد که همه گره‌های قرار گرفته در یک ناحیه وظیفه احساس محیط را به طور همزمان انجام دهند. در نتیجه، برخی حسگرها بسته به سطح نیرویشان بیشتر از سایرین در اجرای یک کار مشارکت می‌کنند. این طرح‌های مدیریتی پیشنهاد شده برای همکاری موثر از نظر انرژی میان گره‌ها، مسیریابی داده‌ها در یک شبکه حسگر متحرک و به اشتراک گذاری منابع میان گره‌های حسگر مورد نیاز است.

در ادامه این بخش به ارائه توضیحات بیشتر در مورد هر لایه از پشته پروتکل شبکه‌های حسگر که در شکل ۴ نمایش داده شده است، می‌پردازیم.



لایه فیزیکی

در شبکه‌های حسگر لایه فیزیکی مسئول انتخاب فرکانس، ایجاد فرکانس حامل، کشف سیگنال، مدولاسیون و رمزنگاری داده است. تا اکنون، باند فرکانسی ۹۱۵ مگاهرتز ISM به صورت گسترده برای شبکه‌های حسگر پیشنهاد و استفاده شده است. تولید فرکانس و کشف سیگنال بیشتر مختص طراحی‌های سطح پائین در سخت‌افزار و فرستنده – گیرنده می‌باشد. بنابراین در حوزه این مقاله قرار نمی‌گیرد. در ادامه تمرکز ما بر روی تاثیرات انتشار سیگنال، راندمان نیرو و تمهیدهای (Scheme) مدولاسیون در شبکه‌های حسگر خواهد بود.

بسیار بدیهی است که برقراری ارتباطات فواصل دور بی‌سیم هم به جهت انرژی و هم به جهت پیچیدگی بسیار پر هزینه است. در طراحی لایه فیزیکی در شبکه‌های حسگر در نظر گرفتن کمینه کردن مصرف انرژی، اهمیت قابل توجهی حتی بیشتر

از تاثیرات محو شدن و انتشار را به خود اختصاص می‌دهد. به طور کلی، میزان حداقل نیروی مورد نیاز برای ارسال یک سیگنال در فاصله مفروض d نسبتی از d^n می‌باشد که 2<= n <4. توان n در شبکه‌های با آنتن‌های نزدیک سطح زمین و کم ارتفاع نزدیک به ۴ است. این ویژگی می‌تواند به دلیل حذف جزئی سیگنال به وسیله اشعه بازتاب شده از زمین باشد.

ارتباط چند گامی در یک شبکه حسگر می‌تواند به طور موثری بر تاثیرات در سایه قرار گرفتن و گم کردن مسیر غلبه کند اگر تراکم استقرار گره‌ها به حد کافی بالا باشد. به طور مشابه، هنگامی که تلفات انتشار و ظرفیت کانال قابلیت اطمینان داده را محدود می‌کنند، این حقیقت می‌تواند برای استفاده مجدد از فرکانس فضایی بکار گرفته شود. تا کنون چند راه حل موثر از نظر نیرو برای لایه فیزیکی ارائه شده است اما به نظر می‌رسد هنوز تا رسیدن به روشهای اختصاصی و سازگار با شرایط شبکه‌های حسگر فاصله داریم. بطور نمونه مقایسه میان تمهیدهای مدولاسیون دودویی و m تایی نشان داده است که مدولاسیون m تایی با ارسال چندین بیت بر روی یک سیمبول، باعث کاهش تبادلات می‌شود در حالیکه نیازمند مصرف انرژی بالاتر و مدارات پیچیده‌تر است. این موازنه میان پارامترها نشان می‌دهد در محیط‌های با شرایط نیرویی دشوار، مدولاسیون دودویی از نظر انرژی بسیار موثرتر است. این معماری با انرژی پائین می‌تواند به یک تکنولوژی مدار مجتمع ویژه کاربرد (ASIC) برای دستیابی به راندمان بالاتر در آینده نگاشت داده شود.

اخیرا سیگنال‌های بسیار باند پهن (UWB) به دلیل مصرف انرژی پائین و مدار ساده برای قسمت فرستنده – گیرنده به عنوان کاندید بسیار مناسبی در شبکه‌های حسگر بویژه برای کاربردهای داخلی معرفی شده‌اند. UWB از انتقال باند پایه (Base Band) بهره می‌برد و بنابراین نیازمند هیچ فرکانس حامل رادیویی و واسط نمی‌باشد. از ویژگی‌های اصلی این تکنولوژی می‌توان به گریز از پدیده چند مسیری اشاره کرد.

لایه پیوند داده

لایه پیوند داده مسئول مالتی پلکس کردن جریان داده، تشخیص فریم‌های داده، کنترل رسانه و کنترل خطا می‌باشد. این لایه ایجاد اتصالات قابل اطمینان نقطه به نقطه و نقطه به چند نقطه را در یک شبکه ارتباطی تضمین کند. در ادامه به بررسی این لایه در شبکه‌های حسگر می‌پردازیم.

کنترل دسترسی به رسانه - پروتکل MAC در یک شبکه حسگر چند گامی و خود سازمان دهنده بی‌سیم می‌بایست دو هدف را برآورده کند. هدف اول ایجاد یک زیر ساختار برای شبکه می‌باشد. به دلیل آنکه هزاران گره حسگر با تراکم بالا در یک حوزه حسگر پراکنده شده‌اند، لایه MAC می‌بایست پیوندهای ارتباطی برای انتقال داده برقرار کند. با این روش زیرساختار اولیه مورد نیاز برای ارتباط گام به گام شکل می‌گیرد و قابلیت خود سازماندهی را به شبکه حسگر می‌دهد. هدف دوم به اشتراک گذاشتن عادلانه و موثر منابع میان گره‌های حسگر می‌باشد.

دلایل عدم کارآیی مناسب پروتکل‌های MAC موجود در شبکه‌های حسگر- همانطور که در قسمت‌های قبلی تاکید شد، پروتکل‌ها و الگوریتم‌های جدید که برای شبکه‌های نوظهور حسگر ارائه می‌شوند می‌بایست توانایی کلنجار رفتن با محدودیت‌های منابع و نیازمندی‌های کاربردهای شبکه‌های حسگر را دارا باشند. برای شرح این محدودیت‌ها، با مروری بر عملکرد MAC در شبکه‌های بی‌سیم دیگر، به تحلیل آنکه چرا آن‌ها نمی‌توانند برای شبکه‌های حسگر پذیرفته شوند، می‌پردازیم. در سیستم‌های سلولی، ایستگاه‌های پایه یک کمربند ارتباطی باسیم را شکل می‌دهند. این نوع از شبکه‌ها در

مقالات گاهی به عنوان شبکه‌های مبتنی بر زیر ساختار نیز خوانده می‌شوند. هدف اصلی پروتکل MAC در این گونه از سیستم‌ها مهیا کردن کیفیت سرویس (QoS) و راندمان بالای پهنای باند می‌باشد. صرفه جویی در مصرف نیرو در درجه دوم اهمیت قرار دارد چرا که ایستگاه‌های پایه از منبع تغذیه بدون محدودیت برخوردارند و کاربران متحرک نیز می‌توانند منبع تغذیه دستگاه‌های خود را شارژ کنند. بنابراین، پروتکل دسترسی به رسانه در این گونه سیستم‌ها متمایل به توسعه یک استراتژی ویژه برای تخصیص منابع می‌باشد. این روش دسترسی برای شبکه‌های حسگر غیر عملی است چرا که هیچ عنصر کنترلی مرکزی شبیه به ایستگاه‌های پایه وجود ندارد. این ویژگی باعث دشواری عمل همگام سازی در سراسر شبکه است. علاوه بر این، راندمان نیرو مستقیما عمر شبکه را در یک شبکه حسگر تحت تاثیر قرار می‌دهد. لذا این ویژگی مهمترین ویژگی در این گونه شبکه هاست.

شبکه‌های بلوتوث و (Ad hoc) متحرک (MANET) احتمالا شبیه ترین شبکه به شبکه‌های حسگر هستند. بلوتوث یک سیستم بی‌سیم بدون زیر ساختار و با برد کوتاه است که به منظور جایگزینی کابل در سیستم‌های الکترونیک طراحی شده است. توپولوژی مورد استفاده در بلوتوث ستاره است که در آن گره رئیس (Master)می تواند تا ۷ گره زیر دست (Slave) داشته باشد که به صورت بی‌سیم به آن متصل شده‌اند و ساختار یک Piconet را ایجاد می‌کنند. هر Piconet از یک روش زمان بندی و الگوی پرش فرکانسی TDMA مرکزی استفاده می‌کند. نیروی انتقال عموما حدود 20 dBm و برد انتقال در حد چند ده متر است.

پروتکل MAC در شبکه‌های MANET وظیفه شکل دهی یک زیر ساختار و پشتیبانی از آن در مقابل جابجایی را بر عهده دارد. بنابراین، هدف اصلی در آن مهیا ساختن کیفیت سرویس بالا تحت شرایط متحرک است. اگرچه گره‌ها وسایل آگاه به سطح نیروی قابل حمل هستند، منبع تغذیه در آن‌ها می‌تواند توسط کاربر تعویض شود و بنابراین صرفه جویی در مصرف نیرو در این شبکه‌ها نیز در درجه دوم اهمیت قرار خواهد داشت.

در مقابل این دو گونه سیستم، شبکه‌های حسگر ممکن است شامل تعداد بسیار بیشتر گره باشند. نیروی انتقال (ایده آل 0~ dBm) و برد رادیویی یک گره حسگر بسیار کمتر از آن در سیستم‌های بلوتوث و MANET است. تغییرات توپولوژی در شبکه‌های حسگر بسیار بیشتر رخ می‌دهد که می‌تواند به دلیل جابجایی گره و یا خرابی گره‌ها باشد. البته نرخ جابجایی در شبکه‌های حسگر، می‌تواند بسیار کمتر از MANET فرض شود. اهمیت ذاتی و کلیدی صرفه جویی در مصرف نیرو برای طولانی‌تر کردن عمر شبکه در شبکه‌های حسگر باعث می‌گردد که هیچکدام از پروتکل‌های MAC ارائه شده برای سیستم‌های بلوتوث و MANET مستقیما قابل استفاده در شبکه‌های حسگر نباشند.

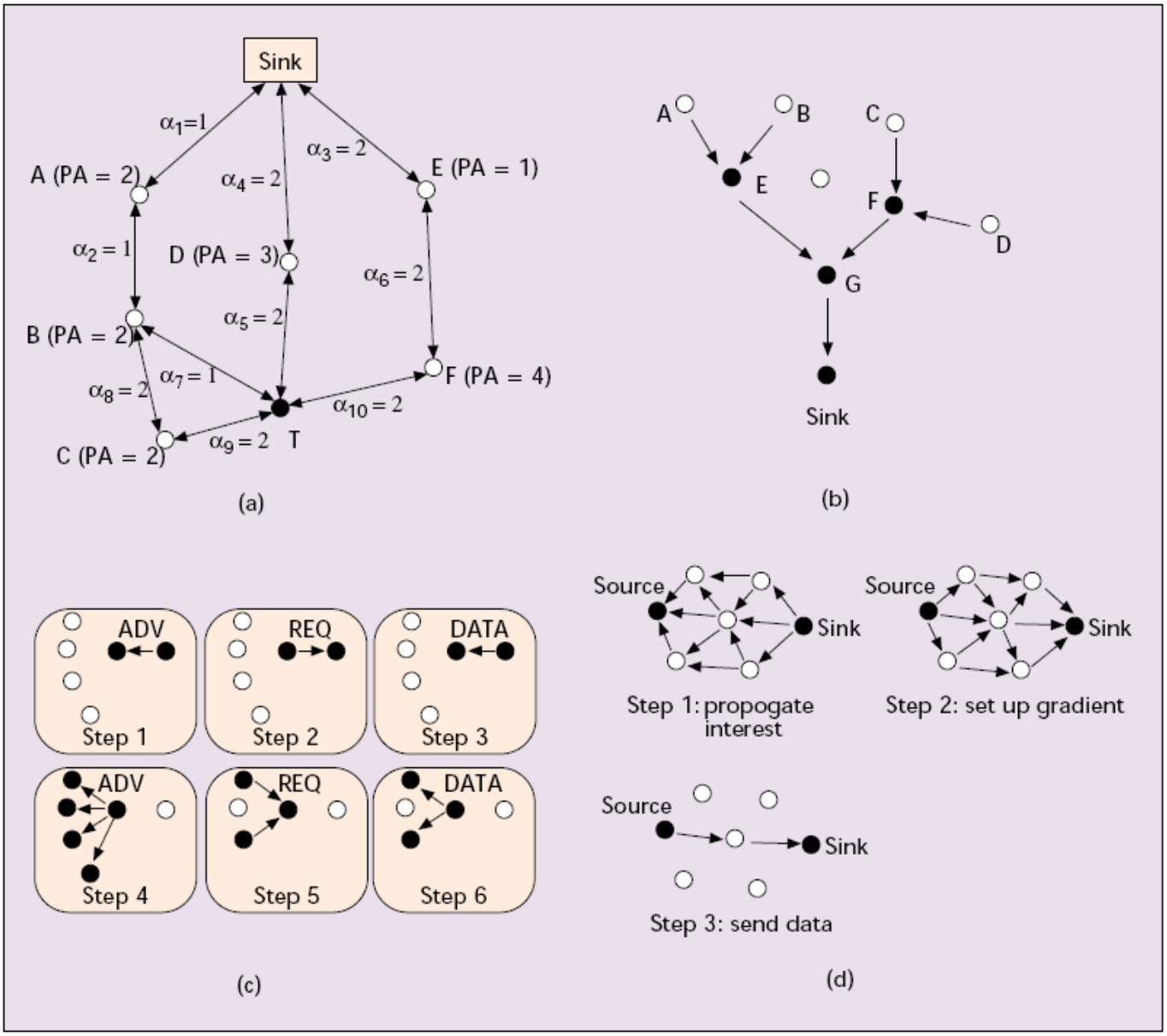
پروتکل MAC برای شبکه‌های حسگر- تاکنون نسخه‌های تخصیص ثابت و دسترسی تصادفی برای دسترسی به رسانه پیشنهاد شده‌اند. روشهای MAC مبتنی بر تقاضا به دلیل سربار ارسال پیغام و تاخیر برقراری پیوند احتمالا مناسب شبکه‌های حسگر نیستند. صرفه جویی در مصرف نیرو با استفاده از مدهای عملیاتی ذخیره نیرو و با ترجیح دادن بازه‌های زمانی به تائیدیه‌ها در موارد قابل ممکن بدست می‌آید.

لایه شبکه

همانطور که در شکل ۱ نمایش داده شد، گره‌های حسگر با تراکم بالا داخل یا بسیار نزدیک به پدیده‌ای که می‌بایست بررسی شود، استقرار داده می‌شوند. همانطور که در قسمت‌های قبل گفته شد، پروتکل‌های مسیریابی بی‌سیم چند گامی ویژه‌ای برای این دسته از شبکه‌ها مورد نیاز است. به دلایل ذکر شده در قسمت‌های قبل روشهای مسیریابی سنتی مورد استفاده در شبکه‌های Ad hoc نمی‌توانند بطور کامل نیازهای شبکه‌های حسگر را برآورده کنند. لایه شبکه در شبکه‌های حسگر معمولا با توجه به موارد زیر طراحی می‌شود:

- راندمان نیرو همیشه یک نکته بسیار مهم قلمداد می‌شود.
- شبکه‌های حسگر اغلب داده- محور هستند.
- جمع آوری داده تنها زمانی مفید است که مانع تلاش جمعی گره‌های حسگر نباشد.
- یک شبکه حسگر ایده آل می‌بایست آدرس‌دهی مبتنی بر صفات و آگاهی نسبت به مکان داشته باشد.

مسیرهای موثر از نظر انرژی می‌توانند بر مبنای نیروی در دسترس (PA) در گره‌ها یا انرژی مورد نیاز (α) برای انتقال از مسیر میان گره‌ها شناخته شوند. در شکل 5a گره T گره مبدا است که یک پدیده را احساس کرده است. گره T برای ارتباط با گره چاهک (Sink) انتخاب‌های زیر را دارد:



شکل ۵. a) راندمان نیرو در مسیرهای مختلف؛ b) مثالی از جمع‌آوری داده c) پروتکل SPIN-1 d) مثالی از Diffiusion مستقیم

- Route 1: Sink-A-B-T, Total PA = 4, Total <= 3
- Route 2: Sink-A-B-C-T, Total PA = 6, Total <= 6
- Route 3: Sink-D-T, Total PA = 3, Total <= 4
- Route 4: Sink-E-F-T, Total PA = 5, Total <= 6

مسیر مناسب از نظر راندمان انرژی بوسیله یکی از رویکردهای زیر می‌تواند انتخاب شود:

مسیر با بیشینه PA: مسیری که در مجموع بیشترین PA را دارا است انتخاب می‌شود. مجموع PAهای یک مسیر با جمع کردن همه PAهای گره‌های واقع در یک مسیر بدست می‌آید. بر مبنای این رویکرد مسیر ۲ در شکل 5a به عنوان مسیر بهینه انتخاب می‌شود. با وجود این، مسیر ۲ در حقیقت شامل گره‌های مسیر ۱ و یک گره اضافی می‌شود. بنابراین، اگرچه این مسیر دارای مجموع PA بالاتر است، اما بهینه نیست. در نتیجه، در این روش باید توجه شود مسیرهای طولانی تری که از مشتق شدن از مسیرهای دیگر بدست می‌آیند، فاقد ارزش هستند. با حذف مسیر ۲، ما می‌توانیم مسیر ۴ را به عنوان مسیر بهینه خود در این رویکرد انتخاب کنیم.

مسیر با کمینه انرژی (ME): در این رویکرد مسیری انتخاب می‌شود که کمینه انرژی مورد نیاز برای انتقال بسته‌های داده بین گره‌های حسگر و Sink را داراست. طبق شکل 5a، مسیر ۱ مسیر ME است.

مسیر دارای کمینه گام (MH): در این رویکرد مسیری که کمترین گام را تا رسیدن به گره چاهک می‌پیماید ترجیح داده می‌شود. مسیر ۳ در شکل 5a طبق این رویکرد مسیر بهینه است. واضح است که رویکرد ME نیز همان مسیر مشابه MH را انتخاب می‌کند در صورتی که همه یالهای یک مسیر، میزان انرژی مساوی برای ارسال نیاز داشته باشند. بنابراین، هنگامی که گره‌ها بدون هیچ کنترل نیرویی با سطح نیروی یکسان همه پخشی انجام می‌دهند، رویکرد MH برابر رویکرد ME خواهد بود.

مسیر بیشینه کمینه PA: مسیری که در آن کمینه PA بزرگتر از کمینه PA مسیرهای دیگر است، ترجیح داده می‌شود. طبق این رویکرد، در شکل 5 a مسیر ۳ مسیر بهینه است. این روش از ریسک استفاده از یک گره حسگر با سطح PA بسیار پائین را قبل از بقیه گره‌ها از بین می‌برد چراکه آن‌ها بر روی مسیرهایی قرار دارند که گره‌های آن‌ها دارای PA بالاتری است.

مبحث مهم دیگر آنست که مسیریابی ممکن است مبتنی بر رویکرد داده- محور باشد. در مسیریابی داد- محور، برای تخصیص وظیفه احساس پدیده‌ها به گره‌ها تقاضای انتشار انجام می‌شود. دو روش برای اعمال تقاضای انتشار وجود دارد: گره چاهک تقاضا را ارسال می‌کند، و یا اینکه گره‌ها اعلانی را برای داده در دسترسی خود همه پخشی می‌کنند و منتظر دریافت درخواست برای داده‌ها خود از سوی گره‌های علاقه مند به دریافت آن‌ها می‌مانند.

مسیر یابی‌های داده - محور نیاز به نامگذاری مبتنی بر صفات دارد. برای نامگذاری میتنی بر صفات، کاربران بیشتر علاقه‌مند به ارائه پرسش در مورد صفتی از یک پدیده می‌باشند تا ارائه پرسشی از یک گره مجزا. برای نمونه، *"ناحیه‌ای که دمای بالای ۱۰ درجه فارنهایت دارد؟"* پرسش معمول تری از *"دستور خواندن دما از گره معین"* است. نامگذاری مبتنی بر صفات امکان ارائه پرسش در مورد صفات خاصی از پدیده مورد ارزیابی را ممکن می‌سازند. نامگذاری مبتنی بر صفات همچنین همه پخشی، چند پخشی مبتنی بر صفات، پخش مبتنی بر ناحیه جغرافیایی و پخش برای همه را ممکن می‌سازد. جمع آوری داده یکی از تکنیک‌های استفاده شده برای حل مسایل همپوشانی و حجم بالای اطلاعات در مسیریابی داده- محور می‌باشد.

در این تکنیک، یک شبکه حسگر همانطور که در شکل 5a نمایش داده شده است، معمولا به صورت یک درخت چند پخشی برعکس فرض می‌شود که در آن گره چاهک از سایر گره‌های حسگر وضعیت پدیده را سوال می‌کند. داده دریافت شده از سوی چندین گره در صورتی که در مورد همان صفت درخواست شده باشد، در هر قسمت که به یک گره در طی مسیر می‌رسد، جمع آوری می‌شود و روی هم ریخته می‌شود. برای نمونه، گره حسگر E داده‌های دریافت شده از سوی گره‌های A و B و گره F اطلاعات دریافت شده از گره‌های C و D را روی هم می‌ریزد.

جمع آوری داده می‌تواند به عنوان مجموعه‌ای از روش‌های اتوماتیک ترکیب داده از داده‌های دریافت شده از چندین گره در قالب چند دسته از داده‌های با معنی و هدف دار باشد.

از این جنبه، جمع آوری داده را می‌تواند به معنی امتزاج داده نامید. همچنین، در حین این پروسه باید توجه شود که اطلاعات ویژه مثل محل گره‌های حسگر گزارش دهنده صفات، دور انداخته نشوند چرا که ممکن است برخی از کاربردها به آن نیاز داشته باشند. یکی دیگر از عملیات مهم و کلیدی در لایه شبکه تهیه یک رابط بین شبکه‌ای برای ارتباط با شبکه‌های

بیرونی مثل شبکه‌های حسگر دیگر، سیستم‌های کنترل و فرمان و اینترنت می‌باشد. به طور نمونه، گره چاهک می‌تواند به عنوان دروازه شبکه حسگر به یک شبکه بیرونی متصل باشد. در یک روش دیگر می‌توان گره‌های چاهک مختلف را به شکل یک کمربند ارتباطی به هم متصل کرد و این کمربند را با استفاده از یک دروازه به شبکه‌های بیرونی متصل کرد.

لایه انتقال

این لایه بطور ویژه هنگامی مورد نیاز خواهد بود که قصد داشته باشیم شبکه را به شبکه اینترنت یا سایر شبکه‌های بیرونی متصل کنیم. پروتکل TCP با مکانیزم پنجره انتقال فعلی خود، با بسیاری از ویژگیهای محیط شبکه حسگر سازگاری دارد. برای ارتباط با سایر شبکه‌ها، مکانیزمی مثل مکانیزم مورد استفاده در TCP برای قطعه قطعه کردن داده مورد نیاز است.

در این رویکرد، اتصالات TCP در گره‌های چاهک پایان می‌یابند و یک پروتکل لایه انتقال ویژه می‌تواند ارتباطات میان گره چاهک و گره‌های حسگر آنچنانکه در شکل نمایش داده شده است، مدیریت کند. در نتیجه، ارتباط میان کاربر و گره چاهک بوسیله UDP و یا TCP از طریق اینترنت یا ماهواره قابل انجام است. از سوی دیگر، ارتباط میان گره چاهک و گره‌های حسگر می‌تواند کاملا مبتنی بر UDP باشد چراکه هر گره حسگر حافظه محدود در اختیار دارد.

برخلاف پروتکل هایی مانند TCP ارتباطات انتها به انتها در شبکه‌های حسگر مبتنی بر آدرس‌دهی، سراسری نیست.در شبکه‌های حسگر نامگذاری مبتنی بر صفات می‌بایست برای تعیین مقصد بسته‌های داده استفاده شود. نامگذاری مبتنی بر صفات در قسمت‌های قبل معرفی شد. فاکتورهایی از قبیل مصرف نیرو و مقیاس پذیری و ویژگی هایی مثل مسیریابی داده- محوری نیاز به ارائه مدیریت متفاوتی در لایه انتقال را قوت می‌بخشند.

لایه کاربرد

اگرچه، تاکنون حوزه‌های کاربردی زیادی برای شبکه‌های حسگر تعریف و پیشنهاد شده است، پروتکل‌های لایه کاربرد بالقوه برای شبکه‌های حسگر هنوز به صورت وسیع کشف نشده باقی مانده‌اند. در این مقاله ما به بررسی اجمالی سه پروتکل ارائه شده در این لایه می‌پردازیم. یادآوری می‌شود که هر سه پروتکل هنوز در مرحله تحقیق و پژوهش هستند.

پروتکل مدیریت حسگر (SMP) طراحی یک پروتکل مدیریتی لایه کاربرد چندین مزیت دارد. شبکه‌های حسگر دارای چندین حوزه کاربردی متفاوت می‌باشد و دسترسی به آن‌ها از شبکه‌ای بیرونی مثل اینترنت می‌بایست با استفاده از پروتکلی شبیه به SMP صورت گیرد.

یک پروتکل مدیریت لایه کاربرد سخت‌افزار و نرم‌افزار لایه‌های پائین‌تر را برای کاربردهای مدیریتی شبکه حسگر به صورت شفاف مهیا می‌سازد. مدیران سیستم با استفاده از SMP با شبکه‌های حسگر تعامل می‌کنند. برخلاف بسیاری از شبکه‌های دیگر، شبکه‌های حسگر شامل گره هایی می‌شوند که شناسه سراسری، ندارند و و معمولا بدون زیر ساختار هستند. بنابراین SMP برای دسترسی به گره‌ها، با استفاده از آدرس‌دهی مبتنی بر مکان و نامگذاری مبتنی بر صفات که در قسمت‌های قبلی معرفی شد عملیات نرم‌افزاری مورد نیاز برای اجرای کارهای مدیریتی زیر را مهیا می‌سازد:

- اعلان قواعد مربوط به جمع آوری داده، نامگذاری مبتنی بر صفات و بخش بندی گره‌های حسگر
- تبادل اطلاعات مربوط به الگوریتم‌های یافتن مکان
- همگام سازی زمانی گره‌های حسگر

• جابجایی گره‌های حسگر • روشن و خاموش کردن گره حسگر

• پرسش در مورد نوع پیکربندی شبکه حسگر، وضعیت گره‌ها و پیکربندی مجدد شبکه حسگر

• تصدیق هویت، توزیع کلید و امنیت در ارتباطات داده ای

پروتکل تخصیص کار و اعلان داده (TADAP) یکی دیگر از اعمال مهم در شبکه‌های حسگر انتشار تقاضا است. کاربران تقاضای خود را به یکی از گره‌های حسگر، زیر مجموعه‌ای از گره‌ها یا همه آن‌ها ارسال می‌کنند. این تقاضا ممکن است در مورد صفت خاصی از پدیده مورد بررسی یا حادثه‌ای در حال انجام باشد. رویکرد دیگر اعلان داده در دسترس است که طی آن گره‌های حسگر داده‌های در دسترس خود را در مورد صفات مورد تقاضای کاربر در مورد پدیده مورد بررسی یا حادثه در حال اجرا به کاربران اعلان می‌کند و سپس کاربران می‌توانند داده‌های مورد نیاز خود را از میان آن‌ها مورد پرسش قرار دهند.

یک پروتکل لایه کاربرد که نرم‌افزار کاربری با واسط‌های موثر برای انتشار تقاضا را برای کاربران مهیا می‌سازد برای تعیین عملیات لایه‌های پائین‌تر مثل مسیریابی مفید خواهد بود.

پروتکل پرسش و انتشار داده (SQDDP) این پروتکل واسط هایی برای انتشار پرسش‌ها، ارائه پاسخ به پرسش‌ها و جمع آوری پاسخ‌های دریافت شده میان گره‌های حسگر و کاربردها را مهیا می‌سازد. یادآوری می‌شود که این پرسش‌ها عموما روی گره‌های خاصی اعمال نمی‌شوند. بلکه نامگذاری مبتنی بر صفات یا مکان ترجیح داده می‌شود. برای نمونه پرسش *"مکان گره هایی که دارای دمای بالای ۷۰ درجه فارنهایت هستند؟"* یک پرسش مبتنی بر صفات است. بطور مشابه پرسش *"دمای خوانده شده توسط حسگرهای قرار گرفته شده در ناحیه A؟"* نیز یک مثال از پرسش مبتنی بر مکان است.

زبان پرسش و ارائه کار (SQTL) به عنوان کاربردی که سرویس‌های زیادی ارائه می‌کند، پیشنهاد شده است. SQTL سه گونه از رویدادها را پشتیبانی می‌کند که با کلمات کلیدی receive، every و expire تعریف می‌شوند. فرمان receive رویدادهای احساس شده از محیط در زمان دریافت این پیغام، فرمان every رویدادهای احساس شده به صورت دوره‌ای طبق تنظیم تایمر و فرمان expire رویدادهای احساس شده در زمان منقضی شدن تایمر را تعریف می‌کنند. اگر یک گره حسگر یک پیغام دریافت کرد که برای آن گره ارسال شده، بود و حامل اسکریپتی بود، آنگاه آن اسکریپت را اجرا می‌کند. اگرچه SQTL پیشنهاد شده است، انواع مختلفی از SQDDP می‌تواند برای کاربردهای مختلف توسعه داده شود. استفاده از SQDDP می‌تواند برای هر کاربرد منحصر به فرد باشد.

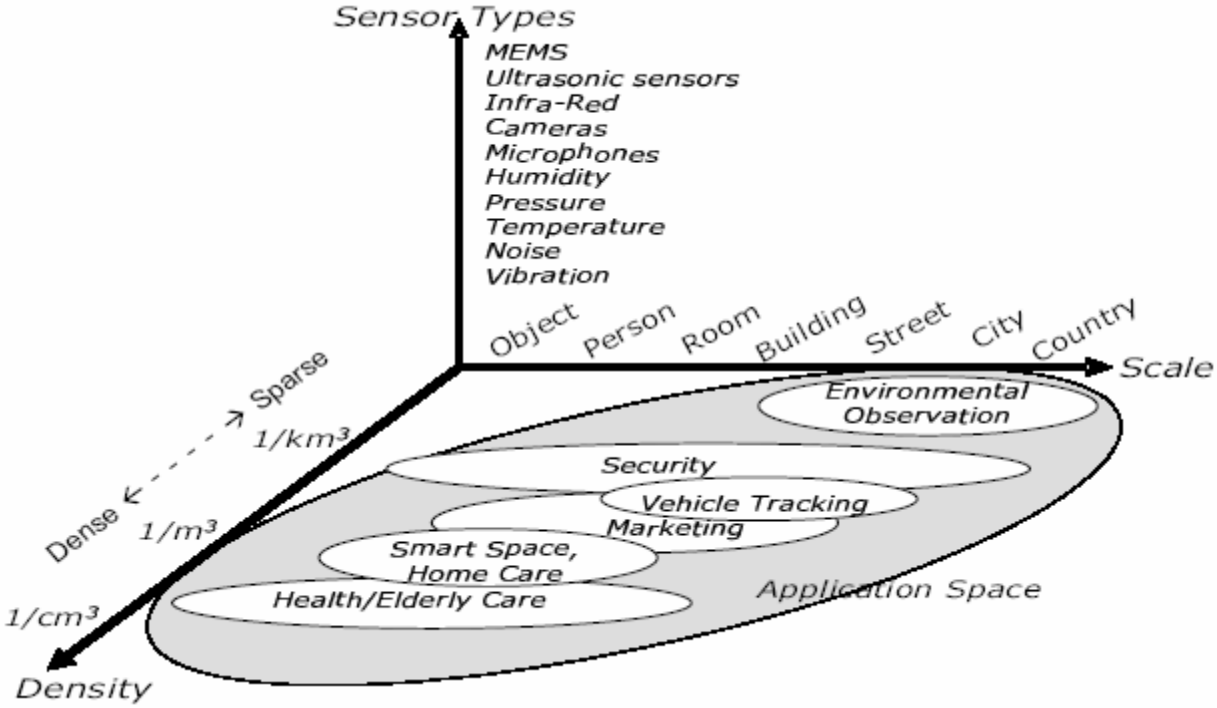
۱۰-۵- کاربرد ها

توسعه کاربرد، امکان استقرار حسگرها در نواحی مختلف از مناطق جنگی تا بدن انسان برای جمع آوری و سپس تحلیل داده، رویای محاسبات هرجایی را واقعیت بخشیده است. چندین کاربرد ویژه نظامی برای ابزارهای ردیابی هدف و کشف داده طبیعی ایجاد شده است. تکنولوژی‌های مرتبط دیگری ارائه شده‌اند که امکان استقرار حسگر بر روی بدن انسان فراهم می‌کنند.

سیستم نظارت صوتی اولین کاربرد توسعه داده شده برای شبکه‌های حسگر می‌باشد. این سیستم در طی جنگ سرد اوایل دهه ۱۹۵۰ برای کشف و ردیابی زیردریایی‌های شوروی سابق بوسیله حسگرها آکوستیک یا هایدروفون‌ها استفاده می‌شده

است. پروژه شبکه‌های حسگر توزیع شده (DSN) توسط آژانس پروژه‌های تحقیقاتی پیشرفته وزارت دفاع امریکا (DARPA) حدود سال ۱۹۸۰ آغاز شد. امکان توسعه شبکه آرپانت به شبکه‌های حسگر همراه با تحقیقاتی روی اجزای آن مثل سیستم عامل و تکنیک‌های پردازش سیگنال مبتنی بر دانش، در همان زمان مورد توجه قرار گرفت.

در حال حاضر، گره‌های حسگر کوچکتر، دارای ذخیره نیروی بیشتر و هزینه تولید کمتر شده‌اند. قابلیت قرار دادن حسگرها در محیط‌های خطرناک و دور از دسترس بدون هیچگونه خطوط ارتباطی نقش کلیدی در توسعه بیشتر اینگونه شبکه‌ها در مقایسه با شبکه‌های سنتی با سیم ایفا می‌کند. داده‌های محیطی مختلف می‌توانند برای پیش بینی پدیده‌های آینده جمع آوری و تحلیل شوند و سپس پیغام‌های هشدار ارسال شوند. حسگرها می‌توانند برای نمونه، داخل خاک جنگلهای باران خیز، یا حتی در سطوح یخی برای پیگیری تغییرات آب و هوایی و اعلان خطرهای سراسری قرار داده شوند. حسگرهای صنعتی نیز می‌توانند همچنین در سیستم‌های انبار و کنترل موجودی بسیار مفید باشند.



شکل ٦. فضای کاربردهای شبکه‌های حسگر

داده‌های دقیق جمع آوری شده از یک ناحیه در شبکه‌های حسگر می‌توانند برای فهم بهتر در موضوعات ویژه مثل نظارت برقلمرو برای مطالعه رفتار پرندگان، کلاس درس‌های هوشمند برای ارزیابی محیط‌های یادگیری کودکان و یا کشف سیاره مریخ بکار گرفته شوند. امروزه سنسورها در تجهیزات الکترونیک برای ساده‌تر کردن زندگی روزمره، در ساختمآن‌ها برای بررسی لرزش و هوشیاری نسبت به باد یا زلزله و یا در بدن انسان برای نظارت بر علائم یک بیماری یا امراض جسمی تعبیه می‌شوند.

شکل ۷ یک دید کلی از کاربردهای توسعه داده شده در شبکه‌های حسگر را ارائه می‌کند. این دسته بندی مبتنی بر تعامل انسان است نه بازه زمانی توسعه کاربرد. تلاش‌های زیادی برای دسته بندی کاربردهای شبکه‌های حسگر صورت گرفته است. تمرکز همه آن‌ها بر حوزه استفاده کاربرد بوده است مثل بهداشت یا نظارت محیطی. در این مقاله ما دوگونه تقسیم بندی برای آن‌ها ارائه می‌کنیم:

دسته بندی سنتی: هشت نوع کاربرد در جدول ارائه شده است. این دسته‌ها سودمندی شبکه‌های حسگر را برای هر هدف خاص نشان می‌دهند.

دسته بندی شیء گرا: در این تقسیم بندی، پنج دسته کاربرد: نظامی، سیستم‌های هشدار و امنیت عمومی، آموزش، بهبود تجارت‌های رقابتی (BC) و بهبود کیفیت زندگی (QoL) ارائه شده است. به دلیل امکان بروز همپوشانی میان این دسته‌ها ممکن است برخی از کاربردهای سنتی در دو یا چند دسته قرار بگیرند.

مبحث اصلی در این کاربردها در حقیقت پیگیری بی‌سیم و جمع آوری داده‌های مورد تقاضا از محیط برای تحلیل‌های آتی است.

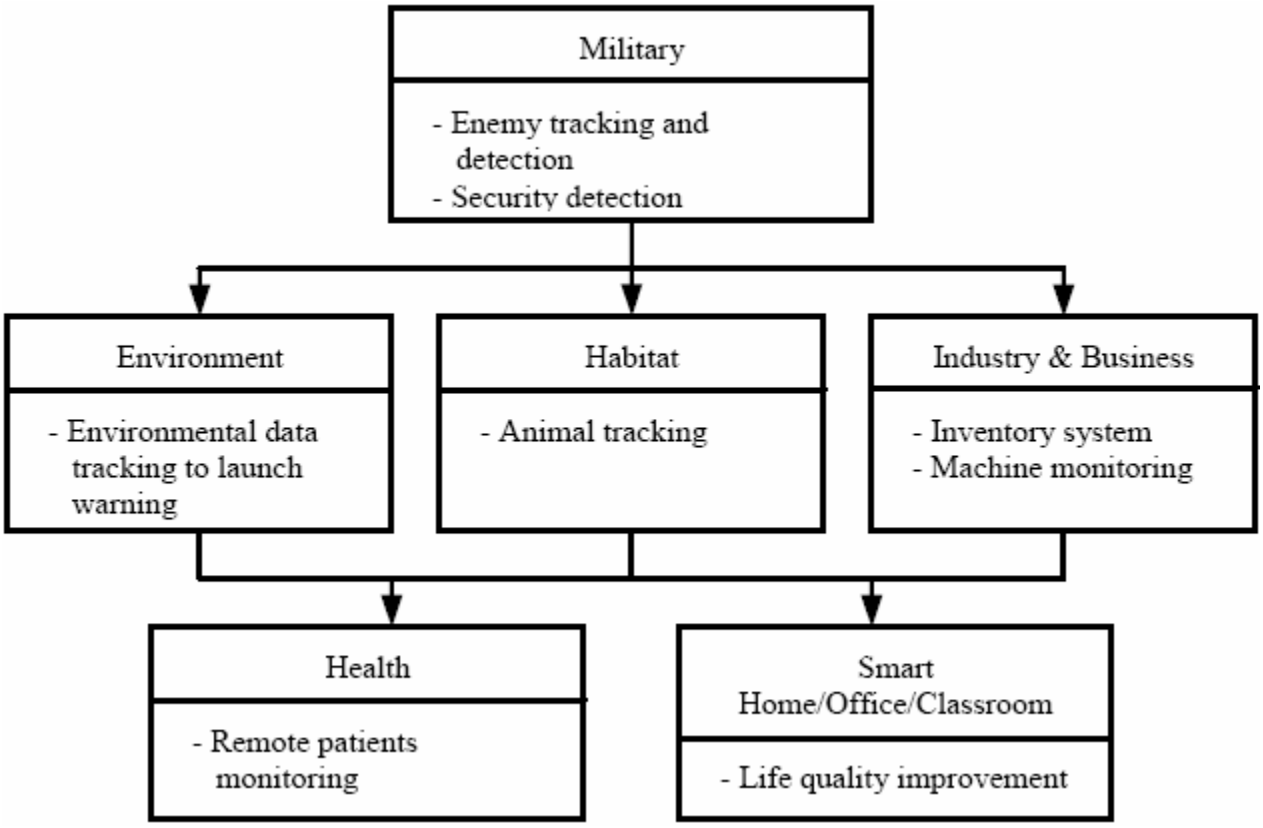
با وجود این، این نیازمندی‌ها و کاربردها به دلیل نیاز به کسب تجربیات اجرایی در شبکه‌های حسگر، هنوز مورد چالش هستند. با دسته بندی شیء گرا این اعتقاد وجود دارد که با در نظر گرفتن نیازهای. مشترک میان کاربردهای هر دسته بتوان گره‌های حسگر چند منظوره طراحی و تولید کرد.

جدول زیر کاربردهای شبکه‌های حسگر را دسته بندی می کند.

Sensor Network Applications

Objective-Oriented Categorisation	Traditional Categorisation
1. Military	- Military
2. Public Security/Warning	- Environmental Observation and Forecasting
	- Health Monitoring
	- Structural Monitoring
3. Education	- Environmental Observation and Forecasting
	- Health Monitoring
	- Structural Monitoring
	- Habitat Monitoring
	- Smart Classroom
4. Business Competitiveness Improvement	- Tracking (Inventory System)
	- Smart Office
5. Quality-of-Life Improvement	- Environmental Observation and Forecasting
	- Health Monitoring
	- Tracking (Traffic Monitoring)
	- Smart Home/Office

شکل زیر نیز کاربردهای توسعه داده شده در شبکه‌های حسگر را نشان می‌دهد.



کاربردهای توسعه داده شده در شبکه‌های حسگر

در ادامه به بیان جزئیات کاربردها می‌پردازیم:

منبع: سمانه ا... یاری؛ "شبکه‌های حسگر بی‌سیم"؛ پروژه کارشناسی؛ دانشگاه فردوسی مشهد

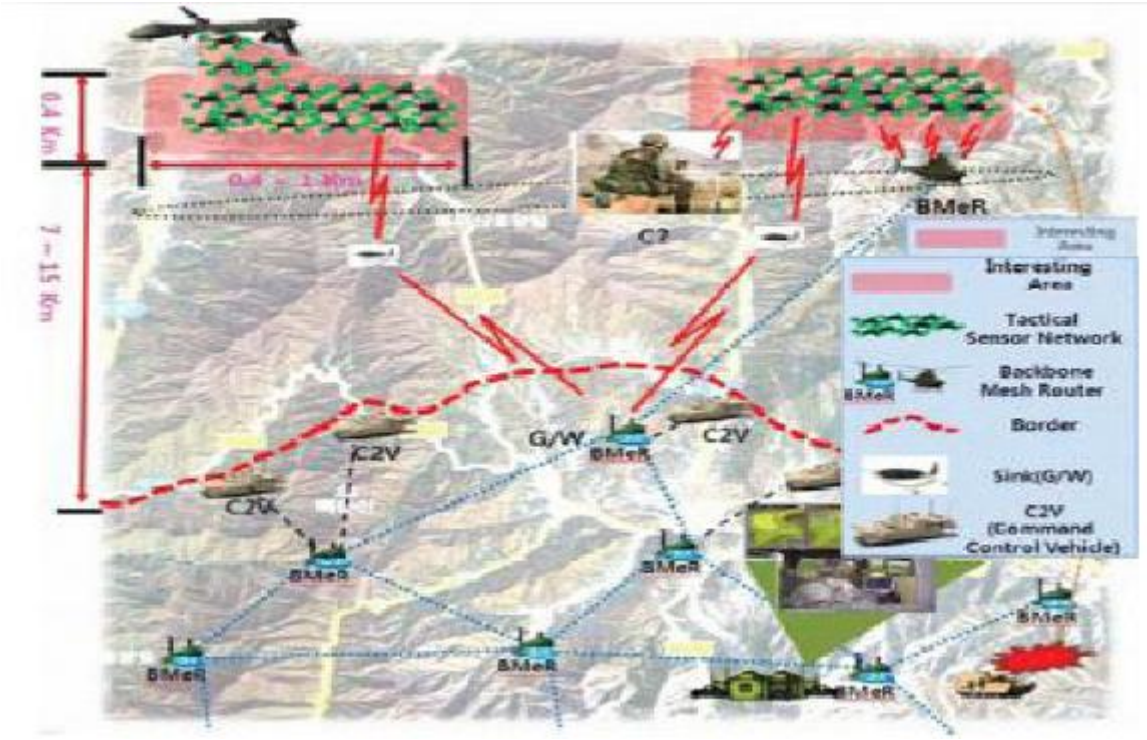
۱) کاربردهای رهایی از سانحه

از پراشاره ترین کاربردهای شبکه های حسگر بی‌سیم می‌باشد. یکی از سناریوها می‌تواند شناسایی مناطق مستعد آتش سوزی و یا اطلاع از وضعیت یک کوه آتشفشان باشد. حسگرهای حساس به گرما برای تعیین نقشه گرمایی یک منطقه مستعد آتش سوزی مثل جنگل بوسیله هواپیما، پخش می‌شوند. سپس آتش نشآن‌ها می‌توانند اطلاعات این شبکه از حسگرها را جمع آوری و تحلیل کنند.

از دیگر کاربردها از این شاخه کاربردهایی در زمینه نظامی است که عبارتند از:

- ✓ مانیتورینگ نیروهای خودی، تجهیزات و مهمات: فرمانده ی عملیات باید دا ئم اً از وضعیت مهمات و نیروهای خودی در منطقه اطلاع کافی داشته باشد. می‌توان به هر کدام از سربازان، خودروهای نظامی، تجهیزات و مهمات یک گره متصل کرد که وضعیت آن‌ها را گزارش دهد.
- ✓ سیستمهای حسگر پوششی سربازان: این سیستم گزارشی از همه ی حوادثی که در طول عملیات اتفاق می‌افتد تهیه می کند.
- ✓ تشخیص حملات میکروبی، هسته ای و شیمیایی: در جنگهای میکروبی، شیمیایی تشخیص نوع حمله سریعاً قبل از آلوده شدن محیط خیلی مهم می‌باشد. برای دستیابی به این هدف گره های حسگر در منطقه خودی مستقر شده و با استفاده از سیستم های هشدار دهنده هشدارهای لازم اطلاع رسانی می‌شوند.

- ✓ هدف‌گیری: استفاده از گره های حسگر برای سیستم هدایت مهمات استفاده برای کنترل از راه دور منطقه با مقیاس بزرگ: تعداد زیادی از گره های حسگر در منطقه مستقر شده و به وسیله خودشان سازماندهی می‌شوند. شکل زیر را مشاهده نمایید.



در نتیجه درمیدان های جنگی، می‌توان جهت شناسایی وبررسی آماری تجهیزات و نیروی دشمن و همینطورکلاس‌بندی وپیگردی نحوه آرایش نیروهای خودی، ازشبکه‌های حسگر استفاده کرد و در نهایت وضعیت نیروهای خودی را در قبال نیروهای دشمن بررسی نمود.

به عنوان مثال در جنگ عراق و آمریکا وقتی که چتر بازهای آمریکایی قصد پایین پریدن را داشتند، تک‌تیراندازهای عراقی آن‌ها را درهمان آسمان موردهدف قرار می‌دادند. آمریکایی‌ها برای پیدا کردن موقعیت تکتیراندازهای عراقی، تعداد زیادی از گره های حسگر بی‌سیم را با هلیکوپتر در منطقه پخش کردند. زمانی که تکتیراندازها شروع به شلیک می‌کردند، این حسگرها با تعاملی که با هم داشتند می‌توانستند موقعیت تکتیراندازها را تشخیص بدهند و برای پایگاه آمریکایی‌ها ارسال کنند و آمریکایی‌ها هم با خمپاره آن‌ها را مورد هدف قرار میدادند (خدا لعنتشون کنه!). تانک هایی هم که به صورت دسته ای حرکت می‌کنند و یکباره هدفی در مقابل آن‌ها ظاهر می‌شود، اگرهمه با هم شلیک کنند باعث اتلاف هزینه می‌شود. به همین دلیل به صورت اتوماتیک با هم ارتباط برقرار می‌کنند و آن تانکی که بهترین موقعیت را دارد را برای شلیک انتخاب می‌کنند.

۲) کنترل محیطی و نگاشت تنوع زیستی

در محیط های مختلف امکان وجود آلودگی های مختلف وجود دارد. لذا با استفاده از چنین شبکه‌هایی، می‌توان وجود آلودگی های مشخصی را در سطح محیط تحت نظر، بررسی کرد و حتی میزان غلظت آلودگی در قسمت های مختلف را مشاهده نمود و در نهایت با استفاده از اطلاعات آماری به دست آمده در خروجی سیستم می‌توان نمودار سه بعدی وضعیت

آلودگی در سطح محیط زیر نظر رابه دست آورد. نوع آلودگی نیز می‌تواند یکتا نباشد و با توجه به امکانات، هرگره در شبکه حسگر می‌تواند شناسایی چندین نمونه آلودگی راپشتیبانی کند.

اندازه گیری میزان فرسایش سطوح زیر آب و پی بردن به تعداد یک گونه خاص در یک بوم خاص را می‌توان در این شاخه جای داد. ویژگی مثبت شبکه های حسگر بی‌سیم کوچکی گره‌ها و نزدیکی آن‌ها به اشیا مورد مشاهده می‌باشد که در این زمینه بسیار موثر است.

۳) سازه های هوشمند

بسیاری از سازمان‌ها و مؤسسات تحقیقاتی در زمینه ی عمران و مسکن برای انجام مطالعات و تحقیقات خود از وضعیت بناهای مدنظر، در طول زمان یا در هنگام بروز حوادث طبیعی بخصوص زلزله، نیازمند استفاده از تجهیزات مانیتورینگ می‌باشند تا اطلاعاتی مانند میزان فشار و تحمل مصالح، وجود ترک، میزان آسیب وارده، وضعیت فرسودگی، امنیت و حفاظت ساختمان و یا سایر جزئیات مرتبط با هدف تحقیقات در مورد بناهایی مثل ساختمان های قدیمی، پل‌ها، سدها، موزه‌ها و... را جمع‌آوری کنند و با توجه به توانایی های شبکه‌های حسگر، می‌توان از این شبکه‌ها برای دست یافتن به اهداف مطرح شده در بالا استفاده نمود.

تخریب نشدن پل‌ها یکی از مثال هایی است که می‌توان ذکر کرد. برطبق یک ارزیابی انجام شده توسط انجمن مهندسان عمران آمریکا در سال ۲۰۰۹، بیش از یک چهارم پل های ساخته شده در این کشور دارای کمبود های ساختاری هستند و یا از لحاظ عملکرد منسوخ شدند. درحالی که برای اطمینان از بی عیب و نقص بودن پل های هوشمند امروزی شبکه ای سیم کشی شده از حسگرهای مختلف در آن‌ها تعبیه شده است، بودجه های شهری، ایالتی و فدرالی آمریکا واقعاً استطاعت کافی برای هزینه نصب چنین سیستم هایی را بر روی پل های موجود ندارند، هم اکنون حسگر بی‌سیم بسیار کوچکی طراحی شده است که اطلاعات مربوط به نقایص ساختاری پل را دقیقه به دقیقه نظارت و مخابره می‌کند و بنا بر ارزیابی‌ها قیمت این وسیله نیز نزدیک به یک صدم نمونه مشابه شبکه سیم کشی شده است.

این حسگرهای بی‌سیم که نام تجاری SenSpot را برای آن برگزیده‌اند، همانند سیستم های سیم کشی شده متعارف تمامی متغیرهای منعکس کننده مربوط به عیب و نقص های پل مانند فشار، ارتعاش، شیب، شتاب، تغییر شکل و ترک خوردگی را اندازه گیری می‌کند. ضخامت آن پنج میلی متر و از چهارلایه انعطاف پذیر نازک تشکیل شده است. اولین لایه پارامترهای ساختاری را ردیابی و اندازه‌گیری می‌کند؛ دومین لایه وظیفه ذخیره ی انرژی را برعهده دارد؛ لایه ی سوم اطلاعات را برای تجزیه و تحلیل به کامپیوتر مرکزی منتقل می‌کند و لایه خارجی یا همان لایه چهارم نیز انرژی مورد نیاز را از نور محیط و امواج رادیویی برداشت می‌کند. این حسگرها بسیار بادوام‌اند و از آن جایی که قابلیت چسبیدن بر روی بدنه پل را دارند، برای نصب آن‌ها هیچ گونه سوراخ کاری در ساختار پل لازم نیست. این دستگاه حداقل به مدت ده سال بدون نیاز به هیچگونه نگهداری دوام داشته و بدون نیاز به سیم‌کشی، باتری و یا هرگونه منبع نیروی اختصاصی دیگر، می‌تواند انرژی مورد نیاز خود را از حداقل نور و امواج رادیویی تأمین کند. شکل زیر را ببینید.



استفاده دیگر شبکه‌های حسگر بی‌سیم در این زمینه برای مقاصد تهویه هوا و تنظیم رطوبت در ساختمآن‌ها می‌باشد. با استفاده از شبکه های حسگر بی‌سیم می‌توان به مقدار تهویه مورد نیاز برای ساکنین ساختمان دست یافت که می‌تواند انرژی بسیاری صرفه جویی کند. نوع دیگری از حسگرها می‌توانند برای شناسایی افراد گیر افتاده در آسانسور یک ساختمان استفاده شوند و اطلاعات جمع‌آوری شده به سرپرست ساختمان ارسال شود.

۴) پزشکی و بهداشت

در زمینه بررسی و مطالعات پزشکی درموردگیاهان و یا انسآن‌ها، جهت آگاهی از وضعیت جسمانی آن‌ها، می‌توان از گره‌های حسگر استفاده نمود و در موارد مختلف، ازجمله قراردادن گره‌ها در لایه‌های زیر پوست برای انجام مطالعات مکرر در طی مدت زمان نسبتاً طولانی، دستگاه‌های پزشکی و به خصوص در زمینه فیزیک پزشکی، می‌توان از شبکه های حسگر استفاده نمود.

اغلب بیماران زمانی به پزشک مراجعه می‌کنند که علائمی غیرطبیعی در بدن خود حس کرده باشند. پس از مراجعه به پزشک یا بیمارستان در واقع مدتی از بیماری فرد گذشته و بیمار باید سریعا مورد مداوا قرار گیرد. در واقع زمان از پیشگیری بیماری گذشته و امکان دارد بیمار مجبور شود هزینه بسیار بالایی صرف درمان خود کند. اما با استفاده از شبکه حسگرها نه تنها می‌توان به وضعیت سلامت جسمانی خود پی برد که می‌توان حتی بیماری را پیش بینی کرد و از هزینه‌ها و ریسک بعدی در زمان درمان کاست. بنابر آخرین خبرها، تحقیقات جدید توسط مهندسان برق در دانشگاه ایالتی اورگان این مسئله را تأیید کرده است که یک فناوری الکترونیک به نام باند بسیار پهن که می‌توان از آن در شبکه حسگرهای نظارتی استفاده کرد، امکان دارد در آینده به عنوان بخشی از راه حل دستیابی به یک هدف بلند پروازانه در زمینه مانیتورینگ بهداشتی بدن یا نظارت بر سلامت جسمانی افراد مورد استفاده قرار گیرد.هم اکنون از نوعی از این حسگرهای ابتدایی‌تر در بعضی بیمارستان های پیشرفته برای نظارت بر داده های فیزیولوژی بیمار، پیگیری دوره های خوردن دارو و نظارت کردن بر پزشکان و بیماران داخل بیمارستان، استفاده می‌شود. در آینده و با پیشرفت فناوری و استفاده از تکنولوژی باند بسیار پهن چنین شبکه هایی به طور مداوم و منظم می‌توانند به تشخیص وضعیت واقعی سلامت بدن کمک کنند. زمان واقعی تشخیص سلامت این فناوری می‌تواند باعث جبران تأخیر در شناسایی بیماری های تحلیل برنده و نجات زندگی انسآن‌ها و در نتیجه کاهش هزینه های بهداشتی شود.

در حال حاضر می‌توان در برخی از موارد از راه دور بر سلامتی نظارت کرد اما برای تکمیل سیستم های نظارت از راه دور هنوز به زمان بیشتری نیاز است. اما دستگاه حسگر نظارتی اخیر که ذکر آن رفت و با فناوری باند بسیار پهن کار می‌کند به احتمال زیاد بسیار کوچک و قابل پوشیدن خواهد بود و شاید انرژی مورد نیاز خود را از گرمای بدن دریافت کند. این دستگاه با وجود حجم کم قادر به انتقال مقادیر زیادی از اطلاعات خواهد بود و تا حد زیادی باعث بهبود شرایط خدمات درمانی و مراقبت های پزشکی، پایین آمدن هزینه درمان و کمک به پیشگیری بیماری خواهد شد.

پاتریک چیانگ، متخصص در الکترونیک بی‌سیم و دستیار استاد پزشکی در دانشکده مهندسی برق و علوم کامپیوتر (OSU) می‌گوید: برای این نوع سنجش و نظارت بر سلامتی، دستگاهی در اندازه یک باند قابل پوشش طراحی خواهد شد. این حسگر امکان ارائه و انتقال داده‌ها درباره بعضی از چیزها و موارد مهم مانند سلامت قلب، حجم استخوان، فشار خون یا وضعیت میزان انسولین در بدن را فراهم می‌کند. در بهترین وضعیت، با استفاده از این دستگاه شما نه تنها بر سلامت خود نظارت دارید که می‌توانید از بیماری‌ها پیش از ابتلا پیشگیری کنید. به عنوان مثال شاید تشخیص آریتمی‌ها و پیش بینی حملات قلبی از جمله مواردی است که این دستگاه می‌تواند در پیشگیری بیماری‌ها مؤثر واقع شود. این دستگاه باید ارزان و در دسترس همگان بوده و همچنین باید قادر به ذخیره کردن و ارائه حجم بزرگی از داده‌ها باشد.

انواع کاربردهای نظارت بر سلامت:

۱) پرستاری در خانه

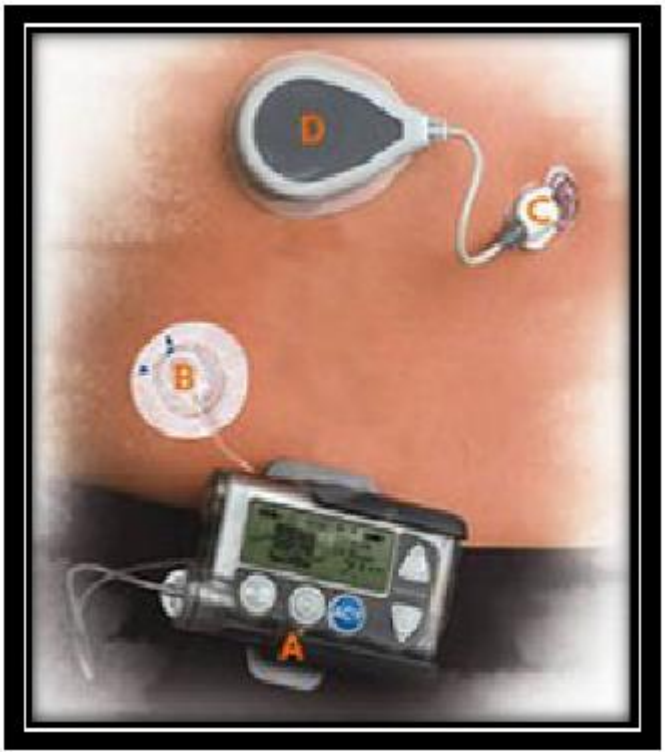
۲) آزمایشات پزشکی

۳) بالا بردن مراقبت های پزشکی

پرستاری در خانه: این کاربرد بر پرستاری افراد سالمند تأکید دارد. در دوربین هایی حسگرهای اندازه گیر فشار، جهت یاب و حسگر برای تشخیص فعالیت های ماهیچه کارگذاشته شده است که یک شبکه پیچیده ایجاد می‌کند. این شبکه افتادن فرد سالمند، عدم هوشیاری،علائم حیاتی، رژیم غذایی و ورزش او را نظارت می‌کند.

آزمایشات پزشکی:به عنوان مثال لوزالمعده مصنوعی به زودی بر روی گروهی از کودکان انگلیسی مبتلا به دیابت نوع ۱ مورد آزمایش قرار خواهد گرفت. این وسیله به کاربران امکان می‌دهد که بدون نیاز به آزمایش هایی مکرر قند خون و تزریق انسولین قند خونشان را کنترل کنند، در نتیجه شیوه زندگی انعطاف پذیرتری داشته باشند و با کنترل دقیق‌تر قند خون از عوارض دیابت در امان بمانند.

این لوزالمعده مصنوعی از یک حسگر، یک برنامه کامپیوتری که میزان انسولین مورد نیاز برای کنترل قند خون را محاسبه می‌کند و یک پمپ انسولین مطابق شکل زیر ساخته شده است.



هدف از این آزمون که بوسیله دکتر رومن هوورکا سرپرستی می‌شود و بنیاد پژوهش دیابت نوجوانان انگلیس از آن حمایت می‌کند، این است که این الگوریتم کامپیوتری طوری کامل شود که حسگر گلوگز بتواند با پمپ انسولین به طور مؤثری ارتباط برقرار کند و کار یک لوزالمعده طبیعی را تقلید کند.

بسیاری از دیابتی‌ها در حال حاضر از پمپ انسولین استفاده می‌کنند. وسیله کوچکی که در بیرون از بدن نصب می‌شود و انسولین را به تدریج از راه یک لوله باریک زیر پوست تزریق می‌کند تا نیاز به تزریقات روزانه انسولین به وسیله فرد برطرف شود؛ اما این افراد باید چند بار در روز میزان قند خونشان را اندازه گیری کنند. آزمایش قندخون با سوراخ کردن نوک انگشت که تنها خون مویرگی را مورد بررسی قرار می‌دهد، تنها تصویری آنی از قند خون به دست می‌دهد.

در مقابل حسگرهای مداوم قند خون، که به اندازه یک کارت اعتباری هستند و روی پوست نصب می‌شوند، میزان قند خون را دقیقه به دقیقه با استفاده از یک حسگر کوچک که زیر پوست قرار دارد اندازه گیری می‌کنند.

کنترل دقیق قند خون به میزان قابل توجهی خطر عوارض وخیمی مانند کوری، سکته مغزی و مرگ زودرس کاهش می‌دهد. بررسی‌ها نشان داده‌اند حتی بیمارانی که به شدت بیماریشان را کنترل می‌کنند؛ به طور میانگین ۹ بار در روز قند خون را اندازه گیری می‌کنند. درکمتر از ۳۰ درصد از روز قندشان در محدوده طبیعی قرار دارد و در بقیه زمآن‌ها قند خون آن‌ها یا خیلی بالا یا خیلی پایین است. اما آزمون های بالینی نشان می‌دهند که استفاده از حسگرهای مداوم قند خون ۲۶ درصد بیشتر از شیوه اول قند خون را در محدوده طبیعی قرار می‌دهد و معیار اندازه گیری کنترل درازمدت قند خون – هموگلوبین A1C – بهبودی قابل توجهی را نشان می‌دهد.

بالا بردن مراقبتهای پزشکی: با ارائه چند مثال موضوع را دنبال می‌کنیم.

کلی موریس، مادری است که هر روز صبح، یک برچسب پلاستیکی قرمز روی پیراهن دخترش می‌چسباند و عملاً از این قابلیت‌ها استفاده می‌کند. مایکلا –دختر او– که سیزده ساله است مبالا به نوعی صرع است که به درمان های معمول ضد صرع

پاسخ نمی‌دهد و این داروها به جای قطع کردن حمله تشنج منجر به مانیای او می‌شوند. پس تنها راه چاره برای اجتناب از این مسئله، استفاده از همین برچسب بود، در یک سوی این برچسب نوشته شده است که در مورد اورژانسی، در سوی دیگر از پزشکان خواسته شده است که اگر مایکلا دچار تشنج شد، پیامکی را به یک شماره مشخص ارسال کنند تا دستورالعمل درمان اختصاصی مایکلا برایشان ارسال شود. این کار او اصطلاحاً دست بند نامرئی نام دارد، در حال حاضر با داشتن گره‌های حسگر بی‌سیم که وقوع تشنج را به پزشکان هشدار می‌دهد و ارتباط این حسگر با مرکزی که دستور العمل درمان اختصاصی مایکلا را می‌دهد هم مشکلات ناشی از گم شدن برچسب و مشکلات احتمالی دیگر حل شده و هم وقوع تشنج به موقع گزارش می‌شود.

یوکو دی آمبروسیا، یکی از پزشکان زنان و زایمان اهل دنور برای اطلاع از مراحل پیشرفت زایمان بیمارانش، پرستاران و ماماها در اتاق زایمان از حسگرهایی برای پایش ضربان قلب جنین و الگوی انقباض رحم و میزان اکسیژن استفاده می‌کند. قبل از این، این متخصص باید هر ساعت یک تا دو بار با بیمارستان تماس می‌گرفت و برای مطلع شدن از وضعیت بیمارانش، به توصیف پرستاران اکتفا می‌کرد، اما حالا او می‌تواند اطلاعات حس گرها را ببیند. هر زمان که او علایم خطر را ببیند، می‌تواند دستور انجام یک عمل سزارین را بدهد. در حال حاضر صدها بیمارستان در ایالات متحده از این سیستم استفاده می‌کنند.

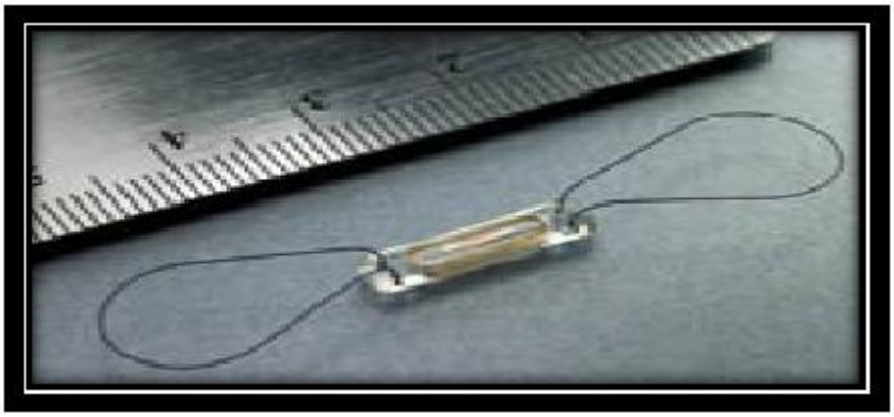
بیمارستان دیگری در لس آنجلس از سیستم پایش دیگری برای بیماران بدحال به نام EverOn استفاده می‌کند، هر زمان که علایم حیاتی بیمار مشکل پیدا کند، هشداری به ایستگاه پرستاری ارسال می‌شود. شکل زیر را ملاحظه نمایید.



شرکت دیگری در سن دیه گو، یک حسگر ساخته است که به مچ دست بسته می‌شود، هر زمان که بیمار احساس ناراحتی کرد، می‌تواند فشار خون، ریتم و حتی سطح فعالیت اش را به صورت بی‌سیم برای اطلاع به پزشک اش ارسال کند.

به عنوان مثالی دیگر می‌توان استفاده از حسگر بی‌سیم جهت کنترل فشار شاهرگ وریدی قلب را ذکر کرد. شرکت CardioMEMS مستقر در آتلانتا، اقدام به ساخت یک حسگر بی‌سیم کرده است که تعداد بیماران مبتلا به نارسایی قلبی بستری شده در بیمارستان را تا ۳۹ درصد کاهش می‌دهد. این ایمپلنت کوچک مانیتورینگ فشار مایع داخل شریان وریدی، می‌تواند میزان این فشار را به صورت بی‌سیم به پزشکان انتقال دهد و سپس دکتر می‌تواند داروهای بیمار بر این اساس تنظیم کند. محققان می‌گویند این حسگر می‌تواند هزینه خدمات درمانی برای افراد مبتلا به نارسایی congestive قلب را کاهش داده و به بهبود کیفیت زندگی آن‌ها کمک کند.

این سیستم توسط یک تغذیه بیرون حسگر که داخل بالش نصب می‌شود نیرو را به گیرنده حسگر می‌فرستد. وقتی بیمار روی بالش دراز میکشد، حسگر فعال شده و اقدام به اندازه گیری و ارسال اطلاعات به صورت بی‌سیم به یک کامپیوتر می کند، که با آن پزشک می‌تواند داده‌ها را بررسی کند. این دستگاه کوچک در شریان وریدی و منطقه ای که خطر کمتری برای لخته شدن خون داشته باشد،کار گذاشته می‌شود. این دستگاه از ایمپلنتهای دیگر کوچکتر است زیرا به باتری و سیم برای خواندن فشار خون نیاز ندارد. دو حلقه فلزی می‌توانند آن را در کنار عروق نگه داشته و یک فشارسنج، جریان عبوری از رگهای خونی را اندازهگیری می کند. شکل زیر را در نظر بگیرید.



۵) حمل و نقل

در بسیاری از کاربردهای حمل و نقل این امکان وجود دارد که بسته‌ها را به حسگرهایی مجهز کرد تا بتوان این بسته‌ها را در طول حمل و نقل، رهگیری کرد یا صورت اجناس یک انبار را کنترل کرد. این حسگرها می‌توانند ادوات بسیار ساده غیرفعال باشند و احتیاجی به ارتباط فعال از طرف حسگر نمی‌باشد.

۶) پردازش راه دور (درجادهها و بزرگراه‌های هوشمند)

تقریباً مرتبط به کاربردهای حمل و نقل، کاربردهای برای این شاخه وجود دارد. یکی از مشکلات جامعه وراهنمایی و رانندگی، کنترل وضعیت ترافیک در سطح شهر می‌باشد. با برپایی شبکه‌هایی از گره‌های حسگر در سطح شهر و قراردادن آن‌ها دربزرگراه‌ها و خیابان های شهر، می‌توان بزرگراه‌ها و خیابآن‌ها را هوشمند ساخت و از وضعیت تراکم عبور ومرور وسایل نقلیه و یا بروز حوادثی مانند برخورد چندین وسیله نقلیه، در نقاط زیرنظر گره‌های حسگر، اطلاع یافت و در نهایت در کل سطح شهر وضعیت ترافیک و تصادفات راشناسایی و پیگیری نمود.

۷) مانیتورکردن محیط زیست

مجموعه ای از تحقیقات در زمینه محیط زیست نیازمند انجام مطالعات مکرر و متمرکز و صرف زمان زیادی جهت جمع‌آوری اطلاعات می‌باشد که معمولاً از حوصله و توانایی چشمان انسان خارج است و در چنین مواردی از دستگاه‌های مانیتورینگ، تحلیلگر و ذخیره کننده نتایج استفاده می‌شود. از طرفی دیگر، به خاطر وجود برخی شرایط محیط زیست، اکثر کارهای تحقیقاتی بایستی در سکوت و آرامش صورت گیرد تا وجود انسان و تجهیزات در محیط اثر منفی در عملکرد غریزه ای و واقعی موجودات نداشته باشد و موجب کاهش کیفیت تحقیق گردد. از این رو معمولا تمام سیستم های مانیتورینگ، قابلیت کنترل از راه دور را دارند. در عین حال این سیستم‌ها طوری انتخاب می‌گردند که وجود آن‌ها در محیط محسوس نباشد. با در نظرگرفتن تمام موارد فوق، ملاحظه می‌شود که شبکه‌های حسگر، علاوه بر بحث هزینه پایین مصرفی، در زمینه

مانیتورکردن محیط زیست، از توانایی بالایی برخودار می‌باشند. در مواردی همچون بررسی وضعیت آب و هوای جوی محیط و بررسی وضعیت ظاهری آن، بخصوص محیط سرسبز وجنگلی، بررسی رشد و نمو گیاهان و موجودات و موقعیت‌یابی موجودات زنده در محیط زیست می‌توان از قدرت بالای شبکه‌های حسگر استفاده کرد.

۸) کشاورزی دقیق

هر گونه عملیات کشاورزی متناسب با شرایط حاکم بر محیط زراعی مورد نظر انجام می‌شود. بنابراین دقت در برآورد شرایط محیطی باعث افزایش بازده می‌شود. این شرایط زمانی و مکانی مختلف متفاوت هستند. در نتیجه بهتر است که عملیات کشاورزی متناسب با شرایط نواحی مختلف مزرعه در هر زمان انجام شود. با افزایش دقت در اندازه گیری نقطه به نقطه، بازده افزایش می‌یابد. جهت دستیابی به اهداف فوق، از حسگر استفاده می‌گردد که به وسیله آن‌ها پارامترهای مختلف محیطی اندازه گرفته می‌شوند. گره‌ها به طور گسترده می‌توانند در سطح مزرعه توزیع شوند و به دریافت اطلاعات لازم به کمک حسگرهای تعبیه شده بر روی آن‌ها می‌پردازند. گره‌ها شامل حسگرحرارتی، رطوبت و نوری می‌باشد که اطلاعات دریافتی را از طریق ارتباط بی‌سیم به گره دیگر ارسال می‌کنند.

حسگرها به طور کلی به منظورهای زیر در کشاورزی به کار می‌روند:

۱. حس کردن خواص خاک: بافت، ساختمان و حالت فیزیکی خاک، رطوبت خاک، مواد غذایی خاک.

۲. حس کردن گیاهان: جمعیت گیاهان، تنش و موقعیت غذایی گیاه.

۳. سامانه های نظارت بر محصول: محصول گیاه، رطوبت محصول، دروی عرض ردیف کاشت.

۴. نظارت بر پارامترهای آب و هوایی: دما، رطوبت هوا، سرعت باد، جهت باد، روشنایی.

استفاده از شبکه های حسگر بی‌سیم امکان آبیاری و کود دهی دقیق را از طریق نصب حسگرهای ترکیب رطوبت و خاک در زمین تحت کشت فراهم می‌کند. به طور مشابه، کنترل آفت نیز می‌تواند با استفاده از این شبکه‌ها انجام پذیرد.

همچنین این شبکه‌ها می‌توان در کنترل دام‌ها به کار برد. مثلاً با اتصال یک حسگر به هر گاو یا گوسفندی می‌توان دمای بدن، تعداد گام‌ها یا دیگر معیارها را اندازه گرفت و در صورت عبور ازآستآن‌های خاص اخطاری مشخص تولید شود.

۹) مدیریت تأسیسات

در مدیریت تأسیساتی در یک ساختمان شبکه های حسگر بی‌سیم می‌توانند مثلاً برای کنترل ورود افراد به بخش هایی خاص استفاده شوند. افراد می‌توانند با داشتن یک علامت خاص از طریق یک حسگر شناسایی شوند و این طریق ورودشان به بخشی خاص کنترل شود.

در مورد دیگر در این زمینه یک شبکه حسگر بی‌سیم می‌تواند در یک کارخانه مواد شیمیایی برای تشخیص نشتی استفاده شود.

۱۰) نظارت ماشین آلات و نگهداری پیشگیرانه

از حسگرها می‌توان برای استفاده در نواحی دشوار دسترسی ماشین آلات استفاده کرد تا با استفاده از الگوی ارتعاشات زمان مناسب سرویس و نگهداری آن ماشین تعیین شود. این ماشین آلات می‌توانند ربات‌ها یا محور قطارها باشند.

با توجه به ماهیت شبکه‌های حسگر، می‌توان مزایایی مانند برپایی سریع در مواقع اضطراری، استفاده در محیطهای که بایستی پارازیت و اختلال در آن‌ها وجود نداشته باشد، اجتناب از قرارگرفتن در محیط های خطرناک و غیرعاقلانه برای مطالعات مکرر، شیوه اقتصادی مقرون به صرفه برای جمع‌آوری اطلاعات در طولانی مدت و... نام برد.

۱۰-۶- پروتکل‌های مسیریابی

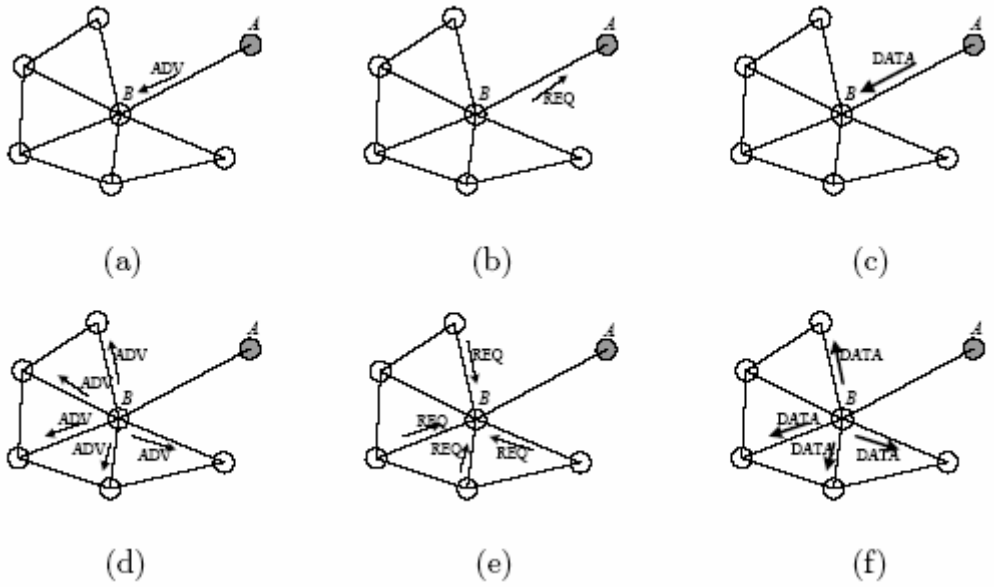
تکنیک‌های مسیریابی برای ارسال داده میان گره‌های حسگر و ایستگاه پایه مورد نیاز است. چندین پروتکل‌های مسیریابی برای شبکه‌های حسگر پیشنهاد شده‌اند. این پروتکل‌ها می‌توانند به صورت زیر دسته بندی شوند:

۱۰-۶-۱- پروتکل‌های مسیریابی داده محور

نمونه‌ای از پروتکل‌های مسیریابی در این دسته شامل SPIN، امتزاج مستقیم، همه پخشی زاویه‌ای (GRAB)، و نسخه چند مسیره آن، و مسیریابی شایعه‌ای است. پروتکل‌های مسیریابی داده- محور بر مبنای اینکه مبدا جریان داده را برقرار کند یا مقصد، می‌توانند به پروتکل‌های ناشی از رویداد، ناشی از پرسش و یا ترکیبی از این دو تقسیم شوند.

SPIN اولین پروتکل مسیریابی داده- محور است. این پروتکل شامل خانواده‌ای از پروتکل‌ها می‌شود که برای انتشار موثر اطلاعات در یک شبکه حسگر بی‌سیم استفاده می‌شوند. SPIN-1 یک پروتکل شروع شونده از سوی مبدا می‌باشد. این پروتکل از یک روش دست تکانی سه مرحله‌ای (ADV-REQ-DATA) برای انتشار داده استفاده می‌کند. گره‌های SPIN نام‌های سطح بالایی به داده‌های خود اختصاص می‌دهند که به این اسامی meta-data گفته می‌شود. این گره‌ها این اسامی را برای محاوره با یکدیگر بکار می‌برند. این حالت از ایجاد افزونگی داده در شبکه جلوگیری می‌کند.

در شکل ۸ نمونه‌ای از عملکرد پروتکل SPIN-1 نشان داده شده است. گره A یک پیغام ADV برای همسایگان خود ارسال می‌کند به این معنی که داده جدیدی برای انتشار دارد. وقتی گره B بسته حاوی پیغام ADV را دریافت کرد، با استفاده از meta-data بررسی می‌کند که آیا همه اطلاعات اعلان شده از سوی A را دارد؟ (8a) اگر نه، گره B یک پیغام REQ به گره A باز می‌گرداند (8b). هنگامی که گره A بسته REQ ارسال شده از سوی گره B را دریافت کرد، در جواب آن بسته‌ای با محتوای داده جدید خود آماده و ارسال می‌کند (8c). بعد از دریافت داده ارسال شده توسط گره A گره، B مشابه عملکرد گره A یک پیغام ADV برای همسایگان خود بجز گره A ارسال می‌کند و آن‌ها را از دراختیار داشتن داده جدید آگاه می‌کند (8d). در این حالت این گره‌ها درخواست خود را به گره B ارسال می‌کنند و بدین طریق پروتکل ادامه می‌یابد (8e, 8f).



شکل ۸. پر.تکل SPIN-1

پروتکل SPIN-2 آستانه انرژی پائین را به پروتکل SPIN-1 اضافه کرده است. گره‌های SPIN-2 به سطح انرژی جاری خود دسترسی دارند. هنگامی که یک گره متوجه می‌شود که در آستانه انرژی پائین قرار دارد، میزان همکاری خود در پروتکل را کاهش می‌دهد. برای مثال، هنگامی که یک گره داده جدید را دریافت می‌کند، اگر انرژی کافی برای انجام کامل پروتکل با همسایگان خود نداشت، اصلا پروتکل را به اجرا در نمی‌آورد.

امتزاج (Diffusion) مستقیم یک پروتکل شروع شونده از سوی مقصد است. خصوصیات آن شامل نامگذاری مبتنی بر صفات، مسیریابی داده- محور و جمع آوری داخل شبکه است. در این پروتکل هر گره داده خود را با یک یا چند صفت نامگذاری می‌کند. گره مقصد تقاضای خود را برای در اختیار داشتن داده‌ها بر مبنای صفاتشان ارسال می‌کند. تقاضاها بر روی شبکه پخش می‌شوند. هنگامی که یک گره تقاضایی را از سوی یکی از همسایگان خود دریافت کرد و متوجه شد داده مورد تقاضا را در اختیار دارد، آنگاه زاویه‌ای را برای ارسال داده به همسایه برقرار می‌کند. هر گره همسایگان خود را تنها بر مبنای داده‌های درخواست شده آن‌ها می‌شناسد. ممکن است یک داده از سوی چند همسایه بصورت همزمان مورد تقاضا قرار بگیرد. در این حالت چند مسیر برای ارسال داده به همسایگان برقرار می‌شود. در میان این مسیرها، یک مسیر یا تعداد اندکی مسیر با نرخ بالای نقل و انتقال داده تعریف می‌شوند و سایر مسیرها با نرخ پائین فرض می‌شوند. بسته به تعداد مسیرهایی که تقویت می‌شوند، روش امتزاج مستقیم می‌تواند مسیریابی یک مسیره یا چند مسیره باشد. اگر مسیر بهتر جدیدی به وجودآمد، پروتکل یک یا چند مسیر با نرخ بالا را به وسیله تقویت منفی به نرخ پائین تبدیل می‌کند. علاوه بر این، امتزاج مستقیم برای بهبود دست یابی به داده و راندمان انرژی جمع آوری و ذخیره داده را توسط گره‌های میانی ممکن می‌سازد.

هم SPIN و هم امتزاج مستقیم ویژگی‌های داده-محوری شبکه‌های حسگر را برآورده می‌کنند. SPIN یک روش شروع شونده از مبدا (یا ناشی از رویداد) می‌باشد. انتشار اطلاعات از سوی مبدا با ارسال اعلان دارا بودن اطلاعات جدید شروع می‌شود. این روش ترافیک و مصرف انرژی شبکه را نسبت به محاوره مبتنی بر meta-data کاهش می‌دهد. محدودیت یا عیب روش SPIN عدم تضمین تحویل داده در مقصد می‌باشد.گره‌های مبدا می‌بایست به طور مستقیم با گره‌های تقاضادار

محاوره کنند. همچنین این امکان وجود دارد که گره‌های تقاضادار و گره‌های مبدا بوسیله برخی گره‌های غیر علاقه مند از هم جدا شده باشند.

در مقابل، امتزاج مستقیم یک روش شروع شونده از سوی مقصد (یا ناشی از پرسش) است. گره‌های مقصد تقاضاهای خود را همه پخشی می‌کنند. گره‌های دریافت کننده این تقاضاها را ذخیره می‌کنند و آن‌ها را برای همسایگان خود منتشر می‌کنند. این پروسه تا زمانی که همه گره‌های شبکه تقاضا را در اختیار داشته باشند ادامه پیدا کنند. در این پروتکل یک یا چند مسیر از مبدا به مقصد برقرار می‌شود. گره‌های میانی در طول مسیر داده‌ها را ذخیره و پردازش (تحلیل و تجمیع) می‌کنند.

همه پخشی زاویه‌ای (GRAB) بر مبنای امتزاج مستقیم ایجاد شده است. با وجود این، گره‌های GRAB هزینه (بطور نمونه تعداد گام ها) را زمانی که یک تقاضا در طول شبکه تجمیع می‌شود ذخیره می‌کند. در این پروتکل هدف تحویل پیغام‌ها از طریق مسیر دارای هزینه کمینه در یک شبکه بزرگ است. هر گره دارای فیلد هزینه است که گویای حداقل هزینه میان آن گره و چاهک است و می‌تواند به عنوان ارتفاع گره تعریف شود. پیغام‌ها هزینه کمینه از گره مبدا تا گره جاری و هزینه کمینه از مبدا تا گره چاهک را به همراه خود منتقل می‌کنند. گره مبدا پیغام را همه پخشی می‌کند. یکی از همسایگان این پیغام را به سمت جلو حرکت می‌دهد؛ تنها اگر جمع هزینه مصرف شده و هزینه خود گره با هزینه مبدا برابر باشد. GRAB برای محاسبه هزینه کمینه از یک الگوریتم مبتنی بر تاخیر استفاده می‌کند. در این روش یک گره همه پخشی کردن تقاضای خود را برای مدت زمانی به تاخیر می‌اندازد و پیغام هایی را که منجر به هزینه کمینه می‌شوند را انتخاب می‌کند. بنابراین تاخیر استفاده شده توسط گره حیاتی است. اثبات شده است که میزان زمان به تاخیر انداخته شدن همه پخشی می‌بایست نسبتی از هزینه کمینه هر گره باشد.

GRAB بوسیله به جلو فرستادن داده تنها در مسیر با هزینه کمینه راندمان انرژی را بهبود می‌بخشد. بنابراین، این پروتکل یک پروتکل مسیریابی تک-مسیره می‌باشد. نسخه چند-مسیره آن یعنی MESH اجازه می‌دهد هر بسته یک فیلد اعتبار که ارزش بالاتری نسبت به فیلد هزینه کمینه دارد به همراه داشته باشد و بنابراین قابلیت عبور از همه مسیرهای دارای هزینه کمتر از مقدار فیلد اعتبار را به فرم MESH فراهم می‌کند. پهنای قسمت MESH که میزان افزونگی و استحکام پروسه به سمت جلو ارسال کردن را معین می‌کند، می‌تواند با تخصیص مقادیر مختلف به فیلد اعتبار تنظیم شود.

همه رویکردهای ذکر شده بالا یا مانند اعلان در اختیار داشتن داده در SPIN رویدادها و یا مانند امتزاج مستقیم تقاضاه ارا روی شبکه ارسال می‌کنند. ارسال رویداد هنگامی که تعداد اندکی رویداد و پرسش وجود دارند موثرتر است در حالیکه، ارسال پرسش زمانی ترجیح داده می‌شود که تعداد پرسش‌ها در مقابل تعداد رویداد اندک است.

مسیریابی شایعه‌ای برای پر کردن شکاف میان ارسال رویداد و ارسال پرسش پیشنهاد شده است. این پروتکل تنها زمانی موثر است نسبت میان تعداد پرسش‌ها و رویدادها در بازه معینی قرار داشته باشد و این پروتکل طوری تنظیم شده است که برای پشتیبانی نسبت پرسش‌ها به رویدادهای مختلف قابل تنظیم باشد.

هدف مسیریابی شایعه‌ای گریز از عملیات ارسال سنگین است. برخلاف امتزاج مستقیم و GRAB که با ارسال پرسش هایی سعی در یافتن مسیر بهینه و تنظیم زاویه ارسال داشتند، مسیریابی شایعه‌ای یک پرسش را بصورت تصادفی در مسیری ارسال می‌کند تا مسیر رویداد را بیابد. در مسیریابی شایعه‌ای، هر گره یک جدول رویداد و یک لیست از همسایگان خود را

نگه داری می‌کند. هنگامی که یک گره به رخداد رویدادی علم پیدا کرد، آنگاه آن رویداد را به جدول رویداد خود اضافه می‌کند. گره هایی که یک رویداد را به تازگی مشاهده کرده‌اند یک کارگزار با یک احتمال معین تولید می‌کنند. یک کارگزار یک بسته با طول عمر زیاد است که در طول شبکه پرسه می‌زند و اطلاعات را منتشر می‌کند. هر کارگزار لیست رویدادهایی که با آن‌ها روبرو شده است و تعداد گام‌ها تا آن رویداد را حمل می‌کند.

هنگامی که کارگزار به یک گره رسید، لیست خود را با لیست داخل گره همگام می‌کند. کارگزار به تعداد مشخصی گام در شبکه حرکت می‌کند و سپس از بین می‌رود. هر گره می‌تواند پرسشی را که مختص رویداد مشخصی است، تولید کند. اگر مسیری به رویداد وجود داشت، آنگاه آن گره پرسش را به سمت رویداد ارسال می‌کند. اگر وجود نداشت، آنگاه گره پرسش خود را بصورت تصادفی به یکی از همسایگان خود ارسال می‌کند. اگر پرسش تا منقضی شدن فیلد TTL پرسش به مقصد نرسید، آنگاه پرسش مجددا ارسال یا همه پخشی می‌شود.

۱۰-۶-۲- پروتکل‌های مسیر یابی سلسله مراتبی

پروتکل LEACH یکی از اولین پروتکل‌های سلسله مراتبی در شبکه‌های حسگر می‌باشد. ایده اساسی مورد استفاده در LEACH بخش بندی گره‌های حسگر با استفاده از قدرت سیگنال دریافتی به قسمت هایی با نام کلاستر و استفاده از گره ابتدایی هر کلاستر به عنوان مسیریاب به سمت ایستگاه پایه یا همان گره چاهک است. LEACH امتزاج و جمع آوری داده را در گره ابتدایی کلاستر انجام می‌دهد تا مصرف انرژی را کاهش دهد. گره‌های حسگر با یک احتمال مشخص مبتنی بر میزان انرژی باقیمانده در گره خود را به عنوان گره ابتدایی کلاستر انتخاب می‌کنند. همه گره‌های دیگر که گره ابتدای کلاستر واقع نشده‌اند با توجه به کلاستری که در آن کمترین نیرو را برای ارتباط با گره ابتدایی نیاز دارند، انتخاب می‌کنند که جزو کدام کلاستر قرار بگیرند. هنگامی که همه گره‌ها داخل کلاسترها سازماندهی شدند، هر کدام از گره‌های ابتدایی کلاسترها یک برنامه برای گره‌های واقع شده در کلاستر خود طرح ریزی می‌کنند. یک گره غیر گره ابتدایی کلاستر می‌تواند قسمت فرستنده- گیرنده خود در مواقعی که طبق زمان بندی زمان انتقال آن نیست، خاموش کند. مکان گره ابتدایی کلاسترها برای جلوگیری از اتمام کامل انرژی یک گره، بصورت تصادفی میان گره‌های هر کلاستر انتخاب می‌گردد.

پروتکل TEEN و TEEN دوره‌ای انطباقی یا APTEEN، همان کار پروتکل LEACH را دنبال می‌کنند. TEEN برای عکس العمل به تغییرات ناگهانی که در صفات احساس شده از محیط صورت می‌گیرد، طراحی شده است. TEEN برای کاهش انتقال پیغام‌ها از دو حد آستانه با نام‌های آستانه سخت و آستانه نرم بهره می‌برد. در هنگام بروز تغییرات در هر کلاستر، گره ابتدایی هر کلاستر آستانه‌های سخت و نرم را برای اعضای کلاستر خود همه پخشی می‌کند. گره‌های حسگر به طور مداوم محیط خود را احساس می‌کنند و تنها زمانی داده را به گره ابتدایی کلاستر گزارش می‌دهند که مقدار داده برابر یا بزرگ‌تر آستانه سخت باشد و یا تغییرات در آن مقدار آن صفت برابر یا بزرگتر از آستانه نرم باشد.

به دلیل آنکه این آستانه‌ها در هر بار پیکربندی جدید کلاسترها از نو تعیین می‌شوند، کاربر می‌تواند آنرا متناسب با نیاز خود تغییر دهد. نقطه ضعف اصلی TEEN آنست که اگر آستانه تعیین شده هیچگاه به دست. نیامد، گره‌ها هیچگاه ارتباطی با یکدیگر ارتباط برقرار نمی‌کنند APTEEN برای برطرف کردن این ضعف به کاربر اجازه می‌دهد که مقادیر آستانه‌ها را تعیین کند و تعداد فواصل زمانیرا تعیین کند. تعداد فواصل زمانی تعیین کننده پریود زمانی بیشینه بین دو گزارش موفق ارسال

شده توسط یک گره است که طی آن اگر یک گره در بازه زمانی تعیین شده هیچ ارسال داده‌ای نداشت، ملزم به احساس محیط در انتهای آن بازه و ارسال داده به سمت گره ابتدایی کلاستر است.

PEGASIS یک پروتکل مبتنی بر زنجیر است که بهبودی بر روی پروتکل LEACH صورت می‌دهد. در PEGASIS هر گره تنها با نزدیکترین همسایه خود ارتباط برقرار می‌کند. هنگامی که یک گره در، زنجیر داده‌ای از همسایه خود دریافت می‌کند، داده آن را با داده درونی خود تجمیع می‌کند و به همسایه بعدی خود در زنجیر ارسال می‌کند. به جای آنکه چندین گره ابتدایی کلاستر داده را به ایستگاه پایه ارسال کنند مثل LEACH تنها یک گره در زنجیر برای انتقال داده به ایستگاه پایه انتخاب می‌شود.

LEACH و اصلاحات بعدی آن (PEGASIS، APTEEN، TEEN) همگی فرض را بر آن می‌گذارند که گره ایستگاه پایه ثابت است و در فاصله‌ای دور از حسگرها قرار دارد. همچنین فرض می‌کنند که هر حسگر می‌تواند به صورت مستقیم به ایستگاه پایه دستیابی داشته باشد. این مفروضات در عمل قابلیت اجرای این پروتکل‌ها را محدود می‌کنند.

۱۰-۶-۳- پروتکل‌های مسیریابی مبتنی بر مکان

برخی از پروتکل‌های مسیریابی در شبکه‌های حسگر نیازمند اطلاعات مکان گره‌ها می‌باشند. اطلاعات مکان می‌تواند توسط سیگنال‌های GPS، قدرت سیگنال رادیویی دریافت شده و... بدست آید. با استفاده از اطلاعات مکان، می‌توان بدون ارسال توده‌ای (Flooding) مسیر بهینه نسبی را یافت. در این قسمت، به بررسی سه پروتکل مسیریابی مبتنی بر مکان در شبکه‌های حسگر می‌پردازیم.

پروتکل GPSR (Greedy Perimeter Stateless Routing)، بصورت حریصانه تصمیم گیری برای ارسال به جلوی بسته را بر مبنای مکان نزدیک ترین همسایگان خود انجام می‌دهد. هر گره برای ارسال بسته‌ها به سمت جلو از ارسال به جلوی حریصانه بسته به آنکه نزدیکترین همسایه خود به مقصد کدام است، انتخاب صورت می‌دهد. وقتی بسته به ناحیه،ای وارد شد که مسیر حریصآن‌های وجود ندارد GPSR بوسیله ارسال به پیرامون محیط ناحیه مقصد، عمل می‌کند. GPSR بسیار مقیاس پذیر است چراکه گره‌های حسگر تنها وضعیت توپولوژی محلی خود را ذخیره می‌کنند. همچنین این پروتکل می‌تواند مسیرهای جدید صحیح را در صورت تغییرات در توپولوژی پیدا کند.

GEAR (Geographical Energy Aware Routing)، بسته‌ها را طی دو مرحله به همه گره‌های داخل ناحیه هدف ارسال می‌کند: (۱) ارسال به جلوی بسته‌ها به سوی ناحیه هدف (۲) انتشار بسته‌ها درون ناحیه. در اولین مرحله، گره بسته را به همسایه‌ای که نزدیکترین فاصله را تا ناحیه هدف دارد ارسال می‌کند. هنگامی که بسته به ناحیه هدف رسید، می‌تواند در آن ناحیه بوسیله ارسال به جلوی جغرافیایی امتزاج یابد. ناحیه هدف به چهار زیر ناحیه تقسیم می‌شود و چهار کپی از بسته ایجاد می‌شود. این پروسه تقسیم و ارسال رو به جلوی بازگشتی تا هنگامی که تنها یک گره داخل زیر ناحیه قرار دارد ادامه می‌یابد. در برخی شرایط تراکم پائین، ارسال رو به جلوی جغرافیایی اتمام نمی‌یابد. در این مواقع بجای GEAR از ارسال انبوه محدود شده استفاده می‌شود.

TTDD (Two-Tier Data Dissemination)، یک مدل انتشار داده دو مرحله‌ای است که برای کار با مسئله متحرک بودن گره چاهک طراحی شده است. در کارهای گذشته، گره‌های چاهک متحرک می‌بایست بطور مداوم اطلاعات

مکان خود را همه پخشی کنند، لذا همه گره‌های حسگر می‌توانند اطلاعات مکان جدید آن‌ها را بروز رسانی کنند. این همه پخشی‌های پیوسته، باعث بروز برخوردهایی در انتقال بی‌سیم و همینطور مصرف انرژی اضافی می‌شوند. TTDD مشکل گره‌های چاهک چندگانه را بوسیله ایجاد یک ساختار توری شکل فعال حل می‌کند. نزدیکترین حسگرها به نقاط توری گره‌های انتشاری نامیده می‌شوند. بجای ارسال پیغام‌های پرسش انتشاری به همه حسگرها، تنها گره‌های انتشاری نیازمند بدست آوردن اطلاعات مورد نیاز برای به سمت جلو ارسال کردن داده هستند. یک پرسش دو سطح را برای رسیدن به یک مبدا می‌پیماید. سطح پائینی داخل مربع تور داخلی مکان فعلی گره چاهک است که به آن سلول گفته می‌شود، و سطح بالایی از گره‌های انتشاری در نقاط توری ایجاد می‌شود. گره چاهک پرسش خود را داخل یک سلول ارسال انبوه می‌کند. سپس پرسش به نزدیک ترین گره انتشاری می‌رسد که آن را به سوی گره‌های انتشاری به سوی مبدا می‌فرستد. این عمل آنقدر صورت می‌گیرد تا پرسش یا به مبدا برسد یا به آن گره انتشاری که داده را از مبدا دریافت می‌کند. در این روش، TTDD در عمل ارسال به جلوی خود جنبه متحرک بودن گره چاهک را مورد توجه قرار می‌دهد. تنها مجموعه کوچکی از گره‌های حسگر نیازمند نگهداری وضعیت ارسال به جلو هستند.

۱۰-۶-۴- پروتکل‌های مسیریابی آگاه به کیفیت سرویس

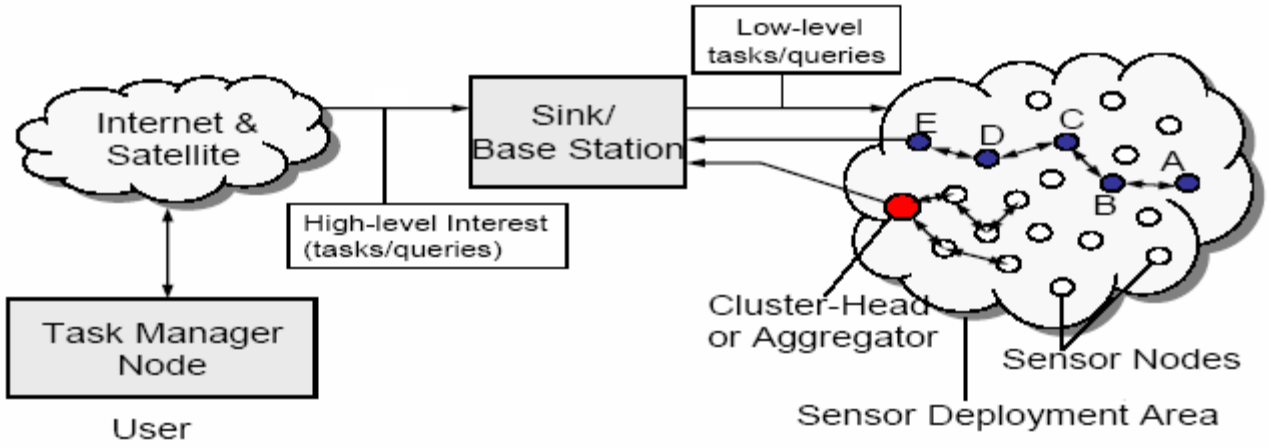
چندین پروتکل مسیریابی آگاه به کیفیت سرویس برای برآورده ساختن نیازمندی‌های مختلف از قبیل راندمان انرژی، قابلیت اطمینان و نیازمندی‌های بلادرنگ تاکنون توسعه داده شده‌اند. در مقاله‌ای تحت عنوان Energy aware routing for low energy Ad hoc sensor networks یک پروتکل مسیریابی آگاه به انرژی پیشنهاد شده است که کمک می‌کند تا حد امکان عمر شبکه و اتصالات میان گره‌ها طولانی‌تر شود. هر گره لیستی از مسیرهای خوب را نگهداری می‌کند و یکی را به صورت تصادفی انتخاب می‌کند. بنابراین، بجای یک مسیر، آن‌ها در زمآن‌های مختلف از مسیرهای مختلف استفاده می‌کنند. لذا، هیچکدام از مسیرها از انرژی تهی نمی‌شوند. این پروتکل از جنبه نگهداری چندین مسیر شبیه به امتزاج مستقیم است. با وجود این، امتزاج مستقیم داده‌ها را در طول همه مسیرها ارسال می‌کند در حالیکه پروتکل مسیریابی آگاه به انرژی تنها یکی از مسیرها را در هر لحظه انتخاب می‌کند. این پروتکل سه مرحله دارد: مرحله برپاسازی؛ ایجاد مسیرها با استفاده از ارسال توده‌ای محدود شده، مرحله ارتباط داده؛ انتخاب یک مسیر و ارسال داده، مرحله نگهداری مسیر؛ ارسال انبوه محدود شده برای زنده نگهداشتن مسیرها.

SPEED یک پروتکل مسیریابی است که تضمین تاخیر انتها به انتهای بلادرنگ نرم را ممکن می‌سازد. هرگره اطلاعات همسایگان خود را حفظ می‌کند و ارسال به جلوی جغرافیایی را برای یافتن مسیرها استفاده می‌کند. SPEED سعی در تضمین یک سرعت معین برای هر بسته در شبکه دارد. برای هر گره حسگر، دو گروه همسایه وجود دارد: همسایگان سریع و همسایگان آهسته. همسایگان سریع سرعت بالاتر از یک حد آستانه را مهیا می‌کنند بنابراین می‌توانند برای داده‌های مسیریابی انتخاب شوند. اگر همسایه سریعی وجود نداشت، گره حسگر می‌تواند بسته را از بین ببرد یا داده را به سمت جلو به سوی یکی از همسایه‌های آهسته خود ارسال کند.

۱۰-۷- شبکه‌های حسگر و بازیگر بی‌سیم

شبکه‌های حسگر و بازیگر (Actor) بی‌سیم (WSAN) شامل گروهی از حسگرها و بازیگران (راه اندازها) هستند که برای اجرای عمل احساس توسط گره‌ها و راه اندازی و بهره گیری توزیع شده از این داده‌های احساس شده توسط بازیگران متحرک میان گره‌ها با یک رسانه بی‌سیم به هم متصل شده‌اند. در این نوع شبکه‌ها حسگرها اطلاعات دنیای فیزیکی را جمع آوری می‌کنند، در حالیکه بازیگران تصمیمات را اخذ می‌کنند و سپس عملیات مناسب را بر روی محیط به اجرا در می‌آورند. این قابلیت اجازه می‌دهد که یک کاربر بطور موثر احساس صورت دهد و عملیاتی را در فاصله دور انجام دهد.

با تعریف بالا، به دلیل وجود بازیگران متحرک، WSANها تفاوت هایی با WSNها خواهند داشت که به مهمترین آن‌ها اشاره می‌شود. برخلاف گره‌های حسگر که عموما وسایلی کوچک و ارزان با قابلیت احساس، محاسبه و ارتباط بی‌سیم محدود هستند، بازیگران می‌بایست بسیار پیچیده‌تر باشند. عملیات آن‌ها بسیار از نظر انرژی پر مصرف‌تر از احساس توسط گره‌ها خواهد بود و بازیگران گره هایی مجهز به منبع نیرو با عمر بسیار طولانی تر، واحد حافظه و محاسبات و همینطور واحد ارتباطات قدرتمندتر هستند. تعداد گره‌های حسگر عموما از مرتبه چندین هزار است در حالی که در مورد بازیگران به دلیل نیازمندی‌های پوشش متفاوت و متدهای محاوره فیزیکی، دارای تراکم کمتر خواهند بود. بنابراین، نسبت تعداد بازیگران به حسگرها در WSANها بسیار کمتر است. برای تهیه احساس و راه اندازی موثر، یک مکانیزم همکاری محلی توزیع شده میان بازیگران و گره‌ها مورد نیاز است.



شکل ۹. عملکرد شبکه‌های WSAN

در WSANها، بسته به کاربرد، نیازی برای پاسخ سریع به ورودی‌های حسگر ممکن است وجود داشته باشد. علاوه بر این، برای مهیا ساختن عملیات مناسب و صحیح، داده‌های حسگر می‌بایست در لحظه استفاده توسط بازیگران هنوز معتبر باشند. بنابراین، به دلیل آنکه عملیات به جهت اطلاعات احساس شده روی محیط صورت می‌گیرند، مبحث ارتباطات بلادرنگ در WSANها نیاز است. WSANها به عنوان یک روش احساس جدید مبتنی بر تلاش جمعی تعداد زیادی از حسگرها که داخل یا نزدیک به یک پدیده استقرار یافته‌اند، زمینه نوظهوری می‌باشند و پتانسیل فراوانی را برای تهیه سرویس‌های متنوع در کاربردهای بی شمار ارائه می‌کنند.

۱۰-۸- خلاصه

در این فصل تلاش شد مروری بر معماری و ویژگی‌های اصلی شبکه‌های نوظهور حسگر صورت گیرد. این شبکه از جنبه‌های مختلفی با شبکه‌های متداول کنونی متفاوت هستند از قبیل؛ محدودیت در نیرو، قدرت پردازش و برقراری ارتباط، استقلال و تعداد زیاد گره‌های حسگر و.... با گذشت عمر کوتاهی از ظهور این شبکه‌ها و ارائه پیشنهادات مختلف در رابطه با پروتکل‌های مسیریابی ویژه این نوع شبکه، معماری و کاربردهای پیش بینی شده آن افق بسیار روشنی برای این دسته از شبکه‌ها پیش بینی می‌شود.

در حال حاضر بیشترین پژوهش‌ها در حوزه مسایل بنیادین این نوع شبکه‌ها از قبیل پروتکل‌های مسیریابی هوشمند با در نظر گرفتن سطح نیروی گره‌ها و برقراری ارتباطات به نحوی که بیشترین راندمان از شبکه حاصل شود، پروتکل‌های مسیریابی هوشمند و آگاه به مکان که در آن گره‌ها به یکی از روش‌های ارائه شده از مکان خود نسبت به سایر گره‌ها آگاهی می‌یابند و از این اطلاعات برای افزایش راندمان، کیفیت سرویس و قابلیت اطمینان بهره می‌برند، توپولوژی‌های مختلف برای آن، طراحی و ساخت گره‌های حسگری که متناسب با نیازهای کاربردهای مختلف باشند و توانایی ارضای نیازهای آن‌ها را داشته باشند و همینطور پیشنهادات در مورد کاربردهای مفید و منحصر به فرد این دسته از شبکه‌ها در زندگی روزمره و صنعت صورت می‌گیرد.

با توجه به نو بودن این حوزه از پژوهش‌ها و فراگیر بودن کنفرانس‌ها و ژونال‌های مرتبط با این حوزه، به نظر می‌رسد این تکنولوژی زمینه پژوهشی بسیار مناسبی برای علاقه مندان به پژوهش به صورت شخصی و آکادمیک می‌باشد.

منبع: محمد خنجری؛ مروری بر شبکه‌های حسگر

فصل ۱۱

محاسبات ابری

(Cloud Computing)

۱۱-۱- محاسبات ابری

منبع: امیررضا غفاری؛ "سیستم های محاسبات ابرین: نمونه‌ها، کاربردها، چالش ها"؛ دانشگاه شهید بهشتی؛ ۱۳۸۹

۱۱-۱-۱- چکیده

محاسبات ابرین اخیرا به عنوان یک الگو برای میزبانی و تحویل سرویس‌ها بر روی اینترنت پدیدار گشته است. این الگو به این دلیل برای صاحبان مشاغل جذابیت دارد که دیگر نیازی نیست تا کاربران از مدتها قبل نیازهای خود را مطرح نمایند تا برای پاسخگویی به آن‌ها برنامه ریزی شود، بنابراین یک سازمان می تواند کار خود را با اندازه کوچک آغاز نموده و منابع بیشتر را تنها زمانی اضافه کند که نیاز به سرویس‌ها افزایش یافته است. علاوه بر این محاسبات ابرین مزایای بسیاری را در اختیار سازمان‌ها و افراد قرار می دهد. به همین دلیل به سرعت به موضوعی داغ در محیط های دانشگاهی و تجاری بدل شده است و همانطور که انتظار می رود توانسته نظر بسیاری را به خود جلب نماید و امروزه با نمونه های متعددی از سرویس دهنده های ابر روبرو هستیم. در این تحقیق نمونه های مختلف را از جنبه های گوناگون شناسایی نموده و مورد ارزیابی قرار دادیم تا بتوانیم در این راه چالش های پیش رو را شناسایی نموده و تا حد امکان راه حل هایی را برای آن‌ها ارائه نماییم. نمونه های مورد بحث در این گزارش انواع مدل های تحویل سرویس از جمله نرم‌افزار به عنوان سرویس، زیرساخت به عنوان سرویس، داده به عنوان سرویس و غیره را در بر می گیرند. در این تحقیق علاوه بر نمونه های سیستم های محاسبات ابرین، تعدادی از معماری های ارائه شده نیز شناسایی گردیده‌اند و مزایایی که سیستم های مبتنی بر این معماری‌ها با خود به همراه می آورند از بعد فنی مورد

بحث قرار گرفته‌اند. تمرکز اصلی بر روی چالش های مطرح در بحث ترکیب سرویس‌ها و یکپارچه سازی سیستم‌ها قرار گرفته و سعی شده است جزئیات مورد نیاز بررسی گردد. در نهایت نتایج حاصل از همین بخش، نمایی از مسیر آینده تحقیق و کارهای بعدی را شکل داده و آن ارائه روشی نوین و مبتنی بر محاسبات ابرین برای مدیریت سرویس های مرکب می باشد. مدیریت صحیح و بهینه سرویس های مرکب از اصلی ترین چالش های مطرح در بحث ترکیب سرویس‌ها می باشد. در روش ذکر شده محاسبات ابرین به عنوان بستری مناسب جهت پاسخگویی به مشکلات این حوزه به کار گرفته خواهد شد.

۱۱-۱-۲- مقدمه

محاسبات ابرین – به عنوان یک سبک محاسباتی جدید – مفهوم جدیدی است که در اواخر سال ۲۰۰۷ پا به عرصه وجود نهاد. در واقع این مفهوم تعمیمی است بر روی بحث " تغییر بر طبق نیاز " که می‌گوید در حالیکه نیازهای کاربران تغییر می‌کند؛ تولیدکننده می‌بایست سخت‌افزار، نرم‌افزار و سرویس های مرتبط با آن نیاز را تامین نماید. امروزه با توسعه سریع اینترنت غالباً نیاز کاربران از طریق اینترنت به تحقق می‌رسد و همین امر پایه و اساس محاسبات ابرین را شکل داده است. محاسبات ابرین گسترش یافته ی مفاهیمی چون محاسبات تورین (Grid)، محاسبات توزیع شده (Distributed) و محاسبات موازی (Parallel) می‌باشد. هدف قابل لمس این سبک نوین فراهم آوردن منابع محاسباتی،ذخیره سازی و ارتباطی به شکلی امن، سریع و البته مبتنی بر سرویس از طریق اینترنت برشمرده شده است.

۱۱-۱-۳- تعریف مسأله

جهان محاسباتی که امروزه با آن روبرو هستیم روز به روز در حال بزرگتر و پیچیده‌تر شدن است. همانطور که گفته شد محاسبات ابرین نیز در ادامه سبک های دیگر مانند محاسبات تورین با هدفی مشترک معرفی گردید. این هدف مشترک چیزی نیست جز پردازش حجم عظیمی از داده با استفاده از خوشه هایی از کامپیوترها. طبق گزارش ارائه شده در، شرکت گوگل در حال حاضر به لطف محاسبات توزیع شده روزانه بیش از ۲۰تر ابایت داده خام اینترنتی را مورد پردازش قرار می‌دهد. تکامل و شکل گیری محاسبات ابرین خواهد توانست این چنین مسائل محاسباتی را به راحتی و به شکلی مناسبتر از طریق سرویس های بنابر تقاضا حل وفصل نماید. از زاویه ای دیگر جهان محاسباتی اطراف ما در حال حرکت به سمت الگوهای " پرداخت برای استفاده " حرکت می‌کند و همین الگو یکی دیگر از پایه های اصلی محاسبات ابرین را تشکیل می‌دهد.

با توجه به ظهور این سبک محاسباتی نوین، در راستای برداشتن قدم در راه تکامل آن لازم است تا این پدیده به طور کامل شناسایی شده و نمونه های موجود آن تا حد امکان بررسی شوند تا بتوان ضعف‌ها و کاستی های آن را شناسایی نموده و نسبت به ارائه راه حل برای آن‌ها اقدام نمود. در این فصل سعی شده است تا از زوایای مختلف، از معماری و مدل های استقرار گرفته تا نمونه‌ها و چالش های مطرح، محاسبات ابرین مورد بررسی قرار گیرد.

۱۱-۱-۴- ساختار فصل

ساختار این فصل به صورت زیر است:

در فصل دوم به شرح ادبیات تحقیق می‌پردازیم و در آن مفاهیم مرتبط و مورد نیاز برای ادامه بحث را مطرح می‌نماییم. در فصل سوم به معرفی محاسبات ابرین پرداخته می‌شود و سپس به طور جزئی مورد بررسی قرار می‌گیرد. در ادامه در فصل

چهارم به معرفی تعدادی از نمونه های سیستم های محاسبات ابرین و همچنین ارزیابی و مقایسه این نمونه‌ها پرداخته می‌شود و البته زمینه های کاربرد محاسبات ابرین مورد بحث قرار می‌گیرند. در فصل پنجم ترکیب سرویس و مفهوم یکپارچه سازی سیستم‌ها در فضای ابر مطرح می‌شود و جوانب آن مورد ارزیابی قرار گرفته و تعدادی از ابزارهای قابل استفاده در این حوزه معرفی می‌گردند. در ادامه و در فصل ششم چالش های مطرح در زمینه محاسبات ابرین مطرح گردیده و راه حل های ممکن نیز ارائه خواهند شد. در فصل های بعدی نیز آینده محتمل محاسبات ابرین و همچنین جمع‌بندی ارائه خواهد شد.

۱۱-۲- مفاهیم و پروتکل‌ها

۱۱-۲-۱- مقدمه

در فصل قبل به طرح مسئله مورد مطالعه در این تحقیق پرداختیم. از آن جا که برای اصطلاحات موجود در حیطه محاسبات ابرین ممکن است تعاریف متعددی از منابع مختلفی مطرح شده باشد، در این فصل به تعریف مفاهیم اصلی در این زمینه که استفاده از این مفاهیم در این تحقیق بر اساس این تعاریف شکل گرفته است، می‌پردازیم. برای درک بهتر و دسته بندی، مطالب این بخش به دو قسمت اصلی تقسیم می‌شوند، مفاهیم مورد استفاده در ترکیب سرویس وب و پروتکل‌ها و استانداردهای مطرح در این زمینه. در پایان فصل نیز جمع بندی و نتیجه گیری از مطالب مطرح شده بیان می‌گردد.

۱۱-۲-۲- محاسبات تورین (شبکه ای - Grid)

یک شبکه از کلیه قابلیتهای سخت‌افزاری و نرم‌افزاری موجود که به صورت یک سیستم جامع و کامل در خدمت مؤسسات تجاری و سازمان‌ها است تا بدین وسیله حداکثر استفاده را از این منابع ببرند. محاسبات تورین یک تکنولوژی جدید فناوری اطلاعات است که عکس العمل سریعتر با هزینه کمتری را در مورد سیستمهای اطلاعات مؤسسات تجاری و حرفه ای ارائه می‌کند. با وجود محاسبات تورین بنا به تقاضا و جهت برآورده ساختن تغییرات مورد نیاز مؤسسات تجاری و سازمان‌ها، گروهای مستقل از سخت‌افزارها و اجزاء نرم‌افزاری می‌توانند به این شبکه متصل شده و به ارائه سرویسهای مورد نظر کمک کنند.

مزایای محاسبات تورین

در مقایسه با دیگر مدلهای محاسباتی از قبیل Mainframe،Client/Server یا چند لایه ای (Multi-tier)، هدف سیستمهای طراحی شده و پیاده سازی شده در روش محاسبات تورین(در حوزه فناوری اطلاعات)، کیفیت بالای سرویس‌ها، هزینه کمتر و انعطاف پذیری بیشتر است.

کیفیت بالای سرویس‌ها نتیجه نداشتن نقاط خطای منفرد، زیرساخت امنیت مستحکم و متمرکز و مدیریت سیاستهای اعمال شده می‌باشد. هزینه پایین نیز ناشی از افزایش بهره وری از منابع و به طور قابل توجه کاهش هزینه های مدیریت و پشتیبانی است.

تخصیص منابع سخت‌افزاری و نرم‌افزاری به یک وظیفه خاص، منجر به از بین رفتن ظرفیتهای بهره وری و قابلیت‌ها می‌گردد. محاسبات تورین امکان استفاده از اجزاء سخت‌افزاری خاص کوچکتر را فراهم می‌سازد.بدین وسیله هزینه هر جزء خاص کاهش یافته و انعطاف پذیری بیشتری جهت تخصیص منابع بر مبنای تغییر نیازها را فراهم می‌کند.

شیوه و روش محاسبات تورین رفتار کردن با مجموعه ای از منابعفناوری اطلاعات یکسان در حالت کلی به عنوان یک مخزن و انبار واحد، و بهره برداری کردن از هر یک از این منابع به عنوان یک نوع مجزا و متمایز می‌باشد. برای رفع مسائل و مشکلات سیستمهای یکپارچه به همراه منابع پراکنده، محاسبات تورین یک تعادل بین مزایای مدیریت منابع در دید کلی از یک سو و کنترل هر یک از منابع بطور انعطاف پذیر از سوی دیگر، برقرار می‌کند. که این منابع مدیریت شده در محاسبات تورین عبارتند از:

- زیرساخت: مجموعه ای از سخت‌افزارها و نرم‌افزارها که محیطی را جهت ذخیره داده‌ها و اجرای برنامه‌ها فراهم می‌کنند.
- برنامه های کاربردی: که منطق و جریان فرآیندهای خاص مؤسسات را تعریف می‌کنند.
- اطلاعات: مفاهیم اصلی در مدیریت تجارت.

اصول هسته محاسبات تورین

دو اصل در هسته محاسبات تورین آنرا به طور منحصر به فردی از دیگر روشهای Computing از قبیل،Mainframe Client/Server یا چند لایه ای (Multi-tier) متمایز می‌سازد: مجازی سازی و تأمین.

- با مجازی سازی، منابع خاص (مانند رایانه‌ها، دیسک‌ها، اجراء نرم‌افزاری و منابع اطلاعاتی) به عنوان منابع درهم آمیخته و مشترک جهت دسترسی مصرف کنندگان (از قبیل افراد و برنامه های نرم‌افزاری) بطور انتزاعی در نظر گرفته می‌شود.مجازی سازی یعنی شکستن اتصالاتی که به سختی بین ارائه کننده و مصرف کننده (مشتری) منابع برقرار شده است و مهیا ساختن منابع برای سرویس دهی به نیازهای خاص، بدون اینکه مشتری نگران چگونگی انجام آن باشد.
- تأمین یعنی اینکه، وقتی مشتری از طریق لایه مجازی سازی نیاز به منبع خاصی دارد، در پشت پرده، آن منبع جهت انجام در خواست،شناسایی شده و به مشتری تخصیص داده شود.تأمین به عنوان بخشی از محاسبات تورین به این معنی است که سیستم تعیین می‌کند چگونه نیاز مشتری را برآورده سازد در حالیکه عملیات در کل، به صورت بهینه انجام شود. برای نمونه می‌توان از Oracle 10g به عنوان تنها DBMS پیشتاز در این زمینه یاد کرد.

۱۱-۲-۳- معماری سرویس گرا

معماری سرویس گرا (Service Oriented) مفهومی جدید نیست و از دهه ۹۰ وجود داشته است، آنچه جدید است توانائی اجرا و عینیت بخشیدن به آن است که به کمک ابزارها و پروتکل های مربوطه میسر شده است. معماری سرویس گرا از دیدگاه های مختلف قابل بررسی است، هر فرد یا ذینفع بر طبق جایگاه خود تصویری از معماری سرویس گرا دارد. برای معماری سرویس گرا تعاریف متنوع و بعضا مختلفی ارائه شده که هر کدام از نگاهی به تبیین خصوصیات آن پرداخته‌اند، برای

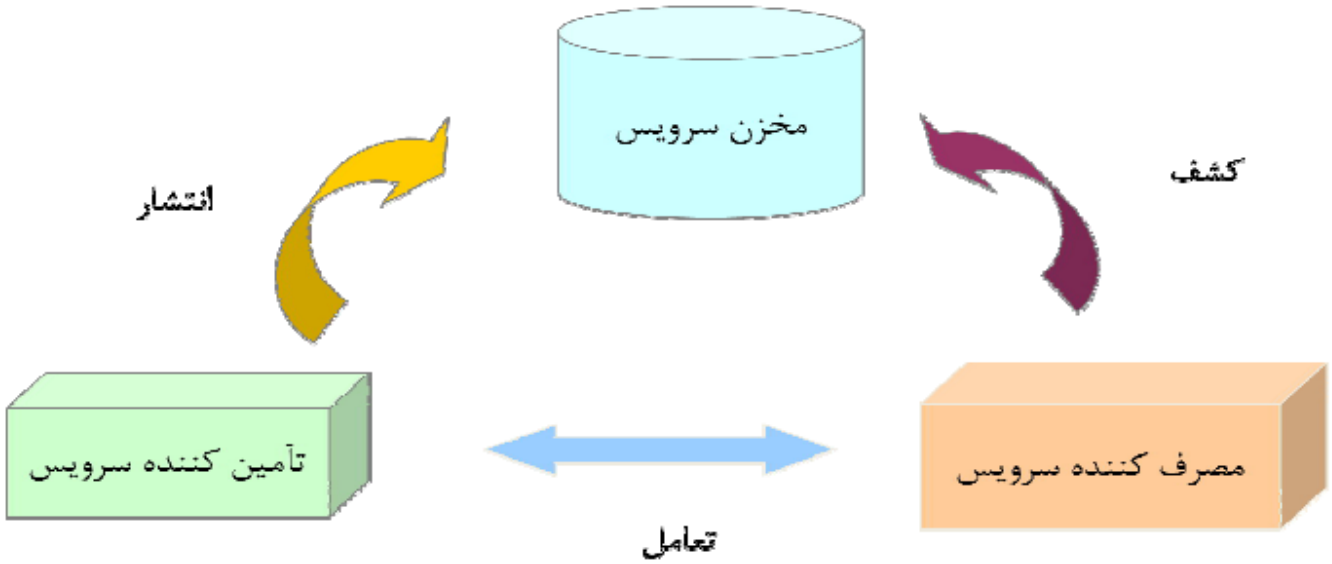
درک بهتر این مفهوم و آگاهی از کلیه برداشت‌ها و نگاه های موجود، در ادامه یکی از تعاریف اصلی و همین طور توصیف آن از دید کمپانی IBM آورده شده است:

- ❖ سبکی از معماری که از اتصال سست سرویسها جهت انعطاف پذیری و تعامل پذیری کسب و کار و بصورت مستقل از فناوری، پشتیبانی می‌کند و از ترکیب مجموعه سرویس های مبتنی برکسب و کار تشکیل شده که این سرویس‌ها انعطاف پذیری و پیکربندی پویا را برای فرآیندها محقق می‌کنند.
- ❖ معماری سرویس گرا از نگاه IBM: رهیافتی برای ساخت سیستم های توزیع شده که کارکردهای نرم‌افزاری را در قالب سرویس ارائه می‌کنند. این سرویس‌ها هم توسط دیگر نرم‌افزارها قابل فراخوانی هستند و هم برای ساخت سرویس های جدید مورد استفاده قرار می‌گیرند، این رهیافت برای یکپارچه سازی فناوری‌ها در محیطی که انواع مختلفی از سکو های نرم‌افزاری و سخت‌افزاری وجود دارند ایده آل است.خواص معماری سرویس گرا به این شرح است:

- استفاده از استانداردهای مستقل از فناوری و مورد توافق برای ارائه مولفه های نرم‌افزاری تحت قالب سرویس.
- معرفی کننده یک روش مشخص و مورد توافق برای تعریف و ارتباط بین مولفه های نرم‌افزاری.
- امکان استفاده ازمولفه های نرم‌افزاری منفرد در ساخت دیگر نرم‌افزارها.
- تقویت کننده رهیافت سرهم بندی اجزاء از قبل تعریف شده برای ساخت نرم‌افزارها به جای توسعه و پیاده سازی آن‌ها.
- توانایی اتصال به نرم‌افزار های خارج سازمانی مانند انواع داخلی آن.

۱۱-۲-۴- سرویس وب

یک سرویس وب یک سرویس نرم‌افزاری است که با یک URL شناخته شده و واسط های عمومی و انقیادهای (Bind) آن با استفاده از XML توصیف و شناسایی می‌شود. تعریف آن می‌تواند توسط سایر سیستم های نرم‌افزاری کشف شود. این سیستم‌ها ممکن است با سرویس وب از طریق روشی که در تعریف آن ارائه شده است، با آن تعامل داشته باشند، با استفاده از پیام های بر مبنای XML که از طریق پروتکل های اینترنت منتقل می‌شوند. یک مدل سرویس وب شامل سه موجودیت، تأمین کننده سرویس، مخزن سرویس و مصرف کننده سرویس می‌باشد. شکل زیر نشان دهنده مدل بیان شده است.



تأمین کننده سرویس، سرویس را ایجاد و یا پیشنهاد می‌دهد. نیاز است تأمین کننده سرویس، سرویس وب را در فرمت استانداردی توصیف کند که معمولا در فرمت XML می‌باشد. سپس آن را در یک مخزن مرکزی سرویس، انتشار دهد. مخزن سرویس، شامل اطلاعات بیشتری درمورد تأمین کننده سرویس، مانند آدرس و تماس با شرکت تأمین کننده و جزئیات فنی در مورد سرویس می‌باشد. مصرف کننده سرویس، اطلاعات را از مخزن بازیابی کرده و از توصیف سرویس بدست آمده برای اتقیاد (Binding) به آن و یا فراخوانی سرویس وب استفاده می‌کند. متدهای ’bind‘ ’publish‘، و ’find‘ در شکل بالا نشان داده شد. به منظور ارتباط برنامه های کاربردی در حال اجرا بر روی سکو های متفاوت و نوشته شده توسط زبان های برنامه نویسی متفاوت، نیاز به استفاده از استاندارد برای هر یک از عملیات های ذکر شده است. معماری سرویس های وب، اتصال سست و سرویس گرا می‌باشد.

با بیانی دیگر سرویس های وب، نرم‌افزارهای کاربردی می‌باشندکه تحت وب منتشر شده، شناسایی و مورد فراخوانی قرار می‌گیرند و دارای ویژگی های زیر می‌باشند:

- مستقل از سکو و زبان هستند.
- نوعی از پیاده سازی معماری سرویس گرا می‌باشند.
- با منطق حرفه در تماس هستند ولی هیچ شخصی مستقیماً با آن‌ها ارتباط ندارد.
- خود شمول هستند.
- خود توصیف هستند.
- یک رهیافت کلیدی برای عینیت بخشیدن به معماری سرویس گرا هستند.

تعریف سرویس وب از نظر W3C: یک سرویس وب، نوعی سیستم نرم‌افزاری است که جهت تعامل ماشین با ماشین در سطح شبکه طراحی شده است و دارای یک تعریف(توصیف) قابل پردازش توسط ماشین با نام WSDL است. دیگر سیستم‌ها بر طبق این توصیف از قبل مهیا شده، با سرویس دهنده تعامل خواهند داشت، پیامها توسط پروتکل SOAP (ترکیب HTTP با XML) و یا سایر پروتکل های مربوطه منتقل می‌شوند.

۱۱-۲-۵- ترکیب سرویس

به فرآیند توسعه یک سرویس مرکب، ترکیب سرویس گفته می‌شود. مراحل ترکیب سرویس در ادامه آورده شده‌اند.

۱. بررسی درخواست یک سرویس مرکب از طرف کاربر و تحلیل نیازمندی های کاربر

۲. کشف سرویس های قابل استفاده برای پاسخگویی به نیازهای عملکردی، این سرویس‌ها می‌توانند هم از منابع داخل سازمان که در مخزن سرویس موجود است و یا از منابع سایر سازمان‌ها از طریق اینترنت کشف شوند.

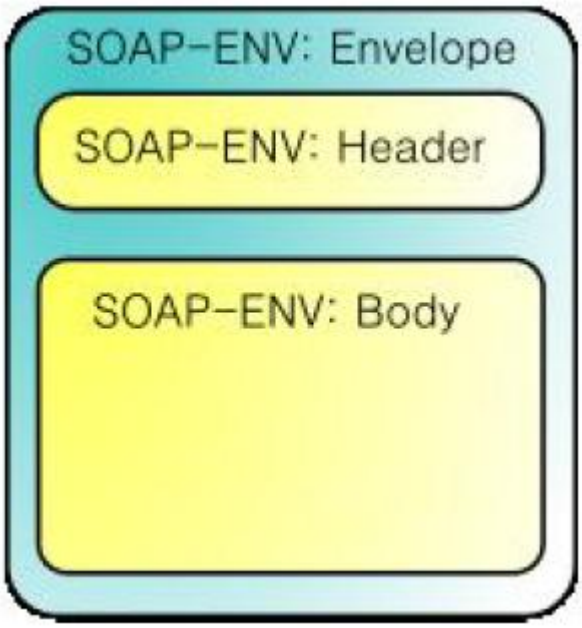
۳. انتخاب سرویس مورد نظر از بین سرویس های مرکب کاندید بر اساس نیازهای غیر عملکردی نظیر کارایی، دقت وکیفیت

۴. تولید توصیف سرویس مرکب

۵. اجرای سرویس مرکب

۱۱-۲-۶- پروتکل SOAP

SOAP پروتکلی برای تبادل پیام‌ها در قالب XML است که بین سرویس های وب استفاده شده و معمولا توسط پروتکلهای انتقالی نظیر HTTPS،HTTP و FTP استفاده می‌شود. همچنین SOAP یک استاندارد مهم در سرویسهای وب برای توصیف ساختار پیامهای منتقل شونده در زمان اجرا و برای فراخوانی است. پیام SOAP یک مستند XML برای توصیف عملیاتی که باید اجرا شوند و پارامترهایی که به برنامه های کاربردی فرستاده می‌شوند، است. به طور دلخواه پیام می‌تواند شامل اطلاعاتی در مورد نحوه پردازش پیام SOAP توسط گیرنده باشد.ساختار پیام SOAP در شکل زیر نشان داده شده است.



قدرت SOAP به عنوان بسته بندی کننده کد این است که پیام SOAP به صورت فایل متنی است که به صورت عمومی از طریق پروتکل های HTTP و HTTPS فرستاده می‌شود. به همین علت می‌تواند از دیوار آتش عبور کند. این مزیت در روش هایی مانند DCOM،CORBA و RPC وجود ندارد.

به سرویس وبی که از پروتکل SOAP پیروی کند، سرویس مبتنی بر SOAP گفته می‌شود.

۱۱-۲-۷- زبان توصیف وب سرویس WSDL

WSDL زبانی مبتنی بر XML می‌باشد که به منظور توصیف ویژگی های عملیاتی و متدهایی که در یک سرویس وب استفاده می‌شود، شامل پارامترهای ورودی و خروجی، نوع داده ای و پروتکل های انتقال مورد استفاده، که معمولا HTTP می‌باشد، است. WSDL یک واژه نامه XML برای توصیف سرویس های وب، مکانی که سرویس‌ها در آنجا قرار دارند و چگونگی فراخوانی آن‌هاست. فایل های WSDL توصیف کننده واسط سرویس های وب است. هر نرم‌افزاری در صورت وجود WSDL سرویس وب، می‌تواند به عنوان مشتری سرویس وب باشد.

هر سرویس وب که بر روی اینترنت قرار می‌گیرد دارای یک فایل WSDL است که مشخصات، مکان و نحوه استفاده از آن سرویس را توضیح می‌دهد. یک فایل WSDL توضیح دهنده ی نوع پیغام هایی است که یک سرویس وب می‌فرستد ویا می‌گیرد. در تئوری یک برنامه در وب برای یافتن سرویس وب مورد نظر خود از روی توضیحات WSDLها جستجو می‌کند. در WSDL اطلاعات مربوط به چگونگی ارتباط با سرویس وب بر روی HTTP یا هر پروتکل دیگر نیز وجود دارد.

همانطور که در شکل زیر نمایش داده شده است اجزاء تشکیل دهنده WSDL عبارتند از:

- type: مشخص کننده پارامترهای ارسالی و دریافتی.
- message: مشخص کننده پارامترهای ورودی و خروجی و نوع آن‌ها، پیام می‌تواند شامل چند بخش باشد.
- operation: متدهای سرویس های وب بوده و دارای پیامهای ورودی و خروجی‌اند.
- port type: مجموعه ای از عملیات است.
- service: مجموعه ای از نقاط انتهائی.

WSDL توصیف چیستی، چگونگی و مکان سرویس های وب را مستند سازی می‌کند.

ویژگی های نسخه های مختلف WSDL در ادامه بیان شده است:

- نسخه ۱.۱۱۹: این نسخه برای توصیف سرویس های وب مبتنی بر SOAP استفاده می‌شود و بر مبنای XML می‌باشد.
- نسخه ۲.۰۲۰: این نسخه برای توصیف سرویس های وب مبتنی بر SOAP و REST استفاده می‌شود. و بر مبنای XML می‌باشد.

WADL (Web Application Description Language): این نسخه برای توصیف سرویس های وب مبتنی بر REST استفاده می‌شود. WADL فرمت فایلی بر اساس XML است که توصیفی قابل فهم برای ماشین از برنامه هاب کاربردی تحت وب مبتنی بر HTTP فراهم می‌کند. این برنامه های کاربردی به طور معمول سرویس های وب RESTful می‌باشند. هدف از WADL اجازه دادن به سرویس های اینترنت یا شبکه های دیگر مبتنی بر IP است که به صورتی قابل پردازش برای ماشین توصیف شوند، برای ایجاد آسان برنامه هایی به سبک وب ۲.۰ و ساخت روشی پویا برای ایجاد و پیکربندی سرویس‌ها. قبل از این، لازم بود یک سرویس وب موجود را مطالعه کرده و سپس به صورت دستی برنامه کاربردی را بنویسیم. مشابه WSDL، این زبان نیز مستقل از سکو و زبان می‌باشد و هدفگیری آن ترفیع استفاده مجدد برنامه های

کاربردی فراتر از استفاده در جستجوگر های وب است. WADL منابعی که توسط سرویس‌ها تأمین می‌شوند و ارتباط بین آن‌ها را مدل می‌کند. سرویس با استفاده از مجموعه ای از عناصر منابع توصیف می‌شود، هر کدام شامل عناصر پارامتری برای توصیف ورودی‌ها و عناصر متدی برای توصیف درخواست و پاسخ به منابع است. عناصر درخواستی، چگونگی درخواست ورودی، نوع مورد نیاز، نوع هدر http مورد نیاز را مشخص می‌کند. پاسخ، پاسخ سرویس و یا هر اطلاعاتی در مورد خطا برای رسیدگی به خط اها را نمایش می‌دهد.

۱۱-۲-۸- زبان اجرای فرآیند BPEL

BPEL زبان اجرای فرآیند های حرفه است که بلوک های سازنده آن سرویس های وب می‌باشند، که دارای مشخصات زیر است:

- استفاده از WSDL برای توصیف واسط سرویس ها
- دارابودن ساختارهای کنترل جریان و شرط های انشعاب
- زبانی مستقل از سکو و مبتنی بر XML
- دارا بودن قابلیت پوشش مواردی نظیر فرآیند های تودر تو و الحاق و شکست زیر فرآیندها

با وجود مزایای زیاد BPEL، این زبان دارای محدودیت هایی نیز می‌باشد. از آنجا که BPEL نوع پورت WSDL را به عنوان اطلاعات سرویس مورد استفاده قرار م ی دهد بنابراین محدودی ت های WSDL را به ارث می‌برد.

از میان تمامی زبان های پردازش نظیر: BPSS، BPML،WS-CDL، XCDL و BPEL، تنها BPEL سازگاری وسیعی هم در حوزه صنعت و هم در حوزه آکادمیک داشته است و مزایایی نظیر سادگی، داشتن ساختاری جامع، پشتیبانی ابزاری، کنترل استثناءها و تصحیح و مانیتورینگ و اجرای زمان اجرا دارد. همچنین این زبان محدودیت هایی نظیر مستعد خطا بودن، توسعه و نگهداری تنها با استفاده از BPEL را بدلیل داشتن دیدگاه پیاده سازی با سطح انتزاع پائینی را دارد. علاوه براین دراین زبان مکانیزمی برای شناسایی ناسازگاری‌ها و ابهامات در مرحله ابتدایی فرآیند توسعه سرویس‌ها وجود ندارد. همچنین BPEL قادر به توصیف وراثت و ارتباطات بین و ب سرویس‌ها نیست.

۱۱-۲-۹- جمع بندی مطالب فصل

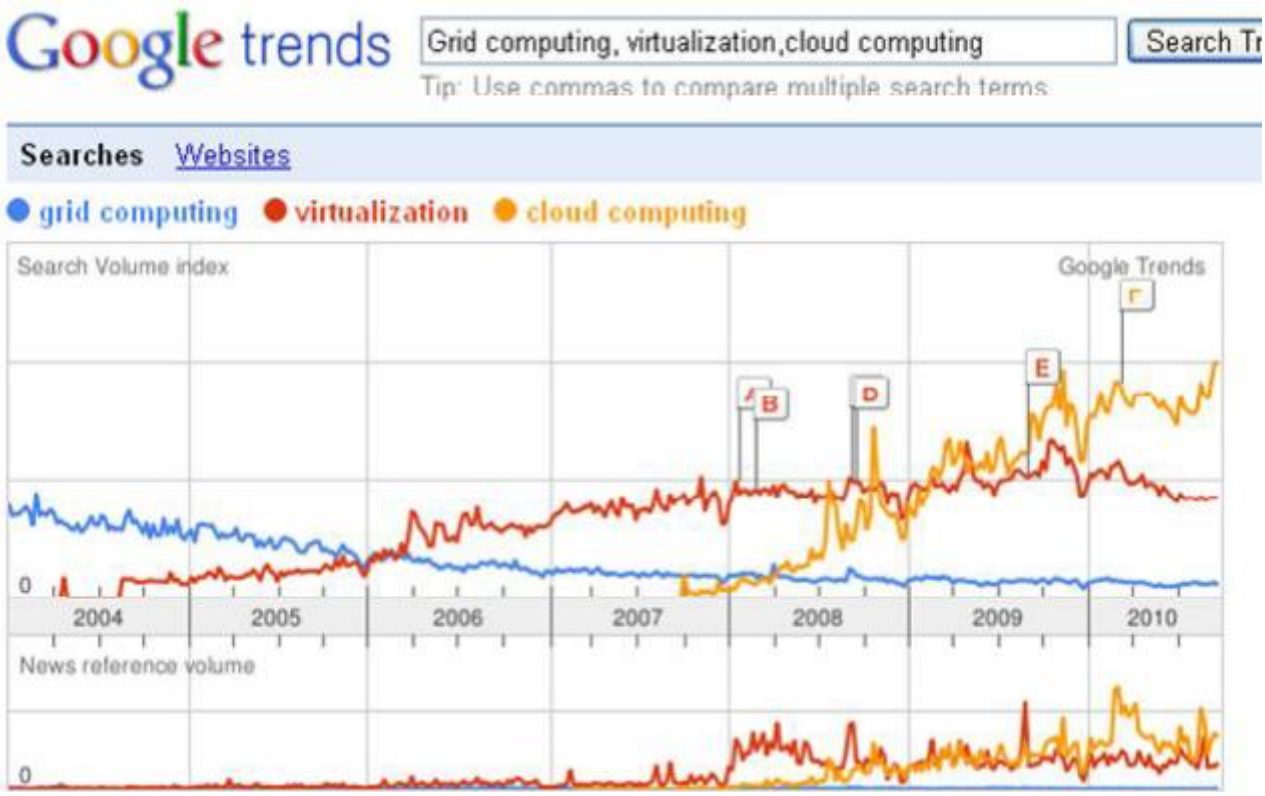
در این فصل به معرفی معماری سرویس گرا و محاسبات ابرین به عنوان مدلی نوین برای تحویل سرویس در معماری سرویس گرا اشاره کردیم. همچنین محاسبات تورین به عنوان سبک محاسباتی توزیع شده که از منظر فناوری پیش نیازی برای محاسبات ابرین به شمار می‌آید نیز معرفی گردید. در ادامه فصل از آنجا که زمینه پیشنهادی کار آینده، بر روی چالشهای ترکیب سرویس در محاسبات ابرین متمرکز خواهد شد لذا به توصیف مفاهیم و پزوتکل های مرتبط ب ا ترکیب سرویس‌ها در معماری سرویس گرا پرداختیم. به دلیل اینکه مفهوم محاسبات ابرین مفهوم نوینی است که در طی سال های اخیر مطرح گردیده، لذا نیاز به استانداردهایی در زمینه تعاملات سرویس های درون ابرها و یا تعاملات بین چندین ابر و غیره احساس می‌شود.

۱۱-۳- محاسبات ابرین

۱۱-۳-۱- مقدمه

محاسبات ابرین که در اواخر سال ۲۰۰۷ پا به عرصه ظهور گذاشت، هم اکنون به دلیل توانایی اش در ارائه زیرساخت فناوری پویا و بسیار منعطف، محیط های محاسباتی تضمین شده از نظر کیفیت و همچنین سرویس های نرم‌افزاری قابل پیکربندی به موضوع داغ بدل شده است. در گزارش گوگل Trends و همانطور که در شکل زیر مشاهده می‌نمایید، محاسبات ابرین که از تکنولوژی مجازی سازی بهره می‌برد، محاسبات تورین را پشت سر گذاشته است.

پروژه های متعددی در حوزه صنعت و دانشگاه بر روی محاسبات ابرین آغاز شده‌اند و شرکت های بسیار بزرگی با این موضوع درگیر شده‌اند و این نشان از توجه عمومی به سمت این پدیده نوین است.



۱۱-۳-۲- محاسبات ابرین چیست؟

در این مرحله توضیحات اولیه که پیش نیاز بحث هستند مطرح می‌شوند و پس از آن سعی می‌شود تا یک تعریف نسبتاً دقیق از محاسبات ابرین ارائه شود. در اینجا لازم است میان دو مفهوم که عموماً با هم اشتباه گرفته می‌شوند، تفاوت قائل شویم، یکی ابر و دیگری محاسبات ابرین. ابر عبارتست از منابع و سرویس های مورد تقاضا بر روی اینترنت که قابلیت توسعه و اطمینان بالایی دارند؛ اما محاسبات ابرین یک سبک محاسباتی است که در آن منابع با قابلیت گسترش پویا و عموماً به شکل مجازی توسط تامین کنندگان سرویس بر روی اینترنت فراهم و تحویل می‌شوند. این سبک محاسباتی مزایای بسیاری را برای کاربران نهایی خود به همراه می‌آورد از جمله، عدم نیاز کاربران به داشتن دانش فنی یا اعمال کنترل بر روی زیرساخت ابر. سایر مزیت های این مدل محاسباتی در ادامه فصل در کنار چالش های استفاده از این مدل بحث خواهند شد. در این مدل توان

پردازشی نیز خود به عنوان یک خدمت یا سرویس اولیه ارائه می‌شود. در واقع محاسبات ابرین(Cloud Computing) به معنی توسعه و به کارگیری فناوری کامپیوتر (Computing) بر مبنای اینترنت (Cloud) است. این عبارت شیوه ای از محاسبات کامپیوتری در فضایی است که قابلیت های مرتبط با فناوری اطلاعات به عنوان سرویس یا خدمات برای کاربر عرضه می‌شود و به او امکان می‌دهد به سرویس های مبتنی بر فناوری در اینترنت دسترسی داشته باشد؛ بدون آنکه اطلاعات تخصصی در مورد این فناوری‌ها داشته باشد و یا بخواهد کنترل زیرساخت های فناوری که از آن‌ها پشتیبانی می‌کند را در دست بگیرد. سرویس های ارائه شده در ابر، برنامه های کاربردی را به صورت برخط فراهم می‌کنند به شکلی که قابل دسترسی با مرورگر وب باشند در این زمان، نرم‌افزار و داده‌ها بر روی سرورها ذخیره شده‌اند.

تعریف محاسبات ابرین

برای اینکه یک تعریف جامع از محاسبات ابرین ارائه دهیم در اینجا از تعریف موسسه NIST استفاده می‌نماییم. البته تعاریف متعدد دیگری نیز ارائه شده‌اند اما این تعریف تقریباً تمامی مشخصات اصلی محاسبات ابرین را که مد نظر ما است را پوشش می‌دهد.

"محاسبات ابرین یک مدل برای دسترسی بنابر تقاضا و راحت تحت شبکه به یک مجموعه اشتراکی از منابع محاسباتی قابل پیکربندی (از جمله سرورها، شبکه‌ها، دستگاه های ذخیره سازی، برنامه های کاربردی و سرویس ها) است که این منابع به سرعت فراهم و استفاده می‌شوند و با کمترین تلاش و هزینه آزاد می‌شوند ".

۱۱-۳-۳- سیر تکامل سبک های محاسباتی

در مدل محاسباتی ابرین کاربران سعی می‌کنند بر اساس نیاز هایشان و بدون توجه به اینکه یک سرویس در کجا قرار دارد و یا چگونه تحویل داده می‌شود، به آن دسترسی یابند. قبلاً نمونه های متنوعی از سیستم های محاسباتی ارائه شده اندکه سعی داشته‌اند چنین خدماتی را به کاربران ارئه دهند. برخی از آن‌ها عبارتند از: محاسبات کلاستری (Cluster)، محاسبات شبکه ای (Grid)، محاسبات همگانی (Utility) و مورد آخر محاسبات ابرین که مورد بحث ما می‌باشد. در شکل زیر روند تکامل این سبک های را مشاهده می‌نمایید.



محاسبات ابرین ساختاری شبیه یک توده ابر دارد که بواسطه آن کاربران می‌توانند به برنامه های کاربردی از هر جایی از دنیا دسترسی داشته باشند. بنابراین، محاسبات ابرین می‌تواند با کمک ماشین های مجازی شبکه شده، بعنوان یک روش جدید

برای ایجاد پویای نسل جدید مراکز داده مورد توجه قرار گیرد. بدین ترتیب، دنیای محاسبات به سرعت به سمت توسعه نرم‌افزارهایی پیش می‌رود که به جای اجرا بر روی کامپیوترهای منفرد، بعنوان یک سرویس در دسترس میلیون‌ها مصرف کننده قرار میگیرند.

دلایل نیاز به یک مدل جدیدتر

برای پاسخ به این سوال که مگر سبک های محاسباتی قبلی چه عیب و نقصی داشتند که نیاز به یک سبک جدید محاسباتی حس شده است، می‌توان به مسائلی که امروزه (بدون بهره گرفتن از محاسبات ابرین) با آن‌ها درگیر هستیم نگاهی اجمالی بیاندازیم.

- امروزه از هر ۱۰۰۰ ریالی که برای یک سیستم هزینه می‌شود تقریباً ۷۰۰ ریال آن صرف تهیه و نگهداری از زیرساخت می‌شود. در واقع به جای اینکه سهم عمده ای از هزینه صرف افزودن قابلیت های جدید یا بهبود قابلیت های قبلی گردد، صرف خرید و به روز رسانی تجهیزات می‌شود.
- در دنیای کنونی با پدیده ای به نام انفجار داده و اطلاعات روبرو هستیم یعنی حجم داده های تولید شده هر ساله ۱.۵ برابر رشد می‌کند. این یعنی اینکه با حجم داده زیادی برای ذخیره سازی و پردازش آن‌ها روبرو هستیم و بنابراین توان پردازشی ما نیز می‌بایست سریعاً رشد نموده و عقب نماند.
- حقیقتی دیگر که با آن روبرو هستیم این است که گاهی تا ۸۵ درصد ظرفیت منابع محاسباتی ما در محیط های توزیع شده بی کار می‌مانند و این یعنی هدر دادن منابع.
- آمار و ارقام نشان داده‌اند که ۳۳ درصد مشتریان سیستم‌ها، به محض اطلاع از وجود یک نقص امنیتی در یک سیستم، ارتباط خود را با کمپانی مسئول برای همیشه قطع می‌کنند. بنابراین بحث امنیت از جمله مهمترین دغدغه های مشتریان بوده و هست و تامین آن یکی از بزرگترین چالش های پیش روی سیستم های نرم‌افزاری می‌باشد.

هدف از مطرح کردن این مسائل این بود که نشان دهیم سبک های محاسباتی فعلی نتوانسته‌اند پاسخ قانع کننده ای به مسائل بالا بدهند و بنابراین محاسبات ابرین با پاسخی مناسب برای هر یک از آن‌ها به عنوان سبکی نوین پا به عرصه ظهور گذاشت.

دلیل انتخاب محاسبات ابرین

با در نظر گرفتن مطالب عنوان شده در بحث قبل باز این سوال مطرح می‌شود که " چرا محاسبات ابرین؟ ". در واقع چرا سبک دیگری از محاسبات برای پاسخ گویی نیازهای مطرح شده استفاده نمی‌گردد. باید بگوییم که درست است که می‌توان به مسائل مطرح شده بالا از راه های دیگری نیز پاسخ داد اما با این حال در حال حاظر مشکلات دیگری نیز وجود دارند که راه حل استفاده شده به اجبار باید پاسخی برای اینها نیز داشته باشد.

این بار مشکلاتی که به پردازش داده‌ها در سطح مقیاس وسیع مربوط هستند را مورد بررسی قرار می‌دهیم.

- در اختیار گرفتن تعداد دلخواهی ماشین برای پردازش مشکل است.
- به فرض وجود ماشین‌ها، در زمان نیاز همگی آن‌ها در دسترس نیستند.

- توزیع و هدایت یک کار بزرگ بر روی ماشین های متفاوت کار سختی است و همچنین جایگزینی ماشین‌ها به هنگام از کار افتادن.
- بزرگ و کوچک شدن پویای سیستم با توجه به بار کاری دشوار است.
- آزادسازی ماشین‌ها به هنگام اتمام کاری ساده نیست.

و باز هم محاسبات ابرین آمده است تا علاوه بر حل مشکلات قبلی، انجام این کارها را نیز تسهیل نماید.

تصویری از کامپیوترها و سازمان‌ها در آینده

پس از همه گیر شدن محاسبات ابرین و در آینده ای نه چندان دور شاهد کوچک‌تر شدن کامپیوتر های شخصی و حذف سرورهای جداگانه خواهیم بود. در واقع چیزی که افراد برای انجام فعالیت های حتی پیچیده خود نیاز دارند تنها یک مرورگر اینترنت است و یک اتصال نسبتاً پر سرعت به شبکه اینترنت. در حال حاضر نسخه های آنلاین نرم‌افزار های کاربردی و معروفی چون آفیس شرکت مایکروسافت نیز به شکل آنلاین و طبق محاسبات ابرین ارائه می‌شود و سیستم عامل های ابرین نیز در حال پدیدار شدن هستند. بنابراین باید منتظر روزی باشیم که به جای استفاده از سخت‌افزار های مستقل و گران، همگی از بستری کاملاً اشتراکی به عنوان زیرساخت اصلی نرم‌افزارها استفاده نموده و تنها از نمونه های ارزان آن برای اتصال به ابر استفاده نماییم. همانطور که گفته شد با حذف سرور های فیزیکی اختصاصی، سازمان‌ها نیز مجبور نیستند هزینه های گزاف تامین زیرساخت را پرداخت نمایند و کافی است اتصال ارزان خود را به ابر مهیا نمایند.

۱۱-۳-۴- فواید استفاده از معماری ابرین

استفاده از محاسبات ابرین و سرویس های ارائه شده مبتنی بر این معماری مزایای بسیاری را به همراه خواهد داشت که تعدادی از آن‌ها در ادامه به طور خلاصه بیان گردیده‌اند.

- صرف سرمایه ناچیز برای زیرساخت
- زیرساخت، درست به اندازه و درست به موقع.
- بهره وری بهینه‌تر از منابع
- کاهش هزینه به دلیل وجود هزینه گذاری بر حسب با استفاده.
- وجود پتانسیل کاهش زمان پردازش
- کاهش مسئولیت مدیریت زیرساخت
- عرضه سریعتر برنامه های کاربردی
- امنیت
- قابلیت اطمینان بالا

۱۱-۳-۵- اهداف محاسبات ابرین

خدمت محوری: در این سیستم همه چیز در قالب سرویس ارائه می‌شود، از نرم‌افزار گرفته تا سخت‌افزار.

هزینه های راه اندازی کم: شما برای اجرای برنامه های کاربردی مبتنی بر وب، نیازی به استفاده از یک کامپیوتر قدرتمند و گران قیمت ندارید. از آن جائی که برنامه های کاربردی بر روی ابر اجرا می‌شوند، نه بر روی یک پی سی، پی سی دسکتاپ شما نیازی به توان پردازشی زیاد یا فضای دیسک سخت که نرم‌افزارهای دسکتاپ محتاج آن هستند ندارد. وقتی شما یک برنامه کاربردی تحت وب را اجرا می‌کنید، پی سی شما می‌تواند ارزان تر، با یک دیسک سخت کوچک تر، با حافظه کم‌تر و دارای پردازنده کارآمدتر باشد. در واقع، پی سی شما در این سناریو حتی نیازی به یک درایو CD یا DVD هم ندارد زیرا هیچ نوع برنامه نرم‌افزاری بار نمی‌شود و هیچ سندی نیاز به ذخیره شدن بر روی کامپیوتر ندارد.

کارآیی بالا و توسعه یافته: با وجود برنامه های کم تری که منابع کامپیوترشما، خصوصا حافظه آن را به خود اختصاص می‌دهند، شما شاهد کارآیی بهتر پی سی خود هستید. به عبارت دیگر کامپیوترهای یک سیستم محاسبات ابرین، سریع‌تر بوت و راه اندازی می‌شوند زیرا آن‌ها دارای فرآیندها و برنامه های کم تری هستند که به حافظه بار می‌شود.

هزینه های نرم‌افزاری کم: به جای خرید برنامه های نرم‌افزاری گران قیمت برای هر پی سی، شما می‌توانید تمام نیازهای خود را به صورت رایگان برطرف کنید. بله درست است، اغلب برنامه های کامپویتری محاسبات ابرین که امروزه عرضه می‌شوند، نظیر Google Docs، کاملاً رایگان هستند. این، بسیار بهتر از پرداخت ۲۰۰ دلار یا بیشتر برای خرید برنامه office مایکروسافت است که این موضوع به تنهایی می‌تواند یک دلیل قوی برای سوئیچ کردن به محاسبات ابرین محسوب شود.

ارتقای نرم‌افزاری سریع و دائم: یکی دیگر از مزایای مربوط به نرم‌افزار در محاسبات ابرین این است که شما دیگر نیازی به Update کردن نرم‌افزارها و یا اجبار به استفاده از نرم‌افزارهای قدیمی، به دلیل هزینه زیاد ارتقای آن‌ها ندارید. وقتی برنامه های کاربردی، مبتنی بر وب باشند، ارتقاها به صورت اتوماتیک رخ می‌دهد و دفعه بعد که شما به ابر، Login کنید به نرم‌افزار اعمال می‌شوند. وقتی شما به یک برنامه کاربردی مبتنی بر وب دسترسی پیدا می‌کنید، بدون نیاز به پرداخت پول برای دانلود یا ارتقای نرم‌افزار، از آخرین نسخه آن بهره مند می‌شوید.

همکاری گروهی ساده: به اشتراک گذاشتن اسناد، شما را مستقیما به همکاری بر روی اسناد رهنمون می‌شود. برای بسیاری از کاربران، این یکی از مهم ترین مزایای استفاده از محاسبات ابرین محسوب می‌شود زیرا چندین کاربر به طور همزمان می‌توانند برروی اسناد و پروژه‌ها کار کنند، به دلیل این که اسناد بر روی ابر میزبانی می‌شوند، نه بر روی کامپیوترهای منفرد، همه چیزی که شما نیاز دارید یک کامپیوتر با قابلیت دسترسی به اینترنت است.

استقلال از سخت‌افزار: در نهایت، در این جا به آخرین و بهترین مزیت محاسبات ابرین اشاره می‌کنیم. شما دیگر مجبور نیستید به یک شبکه یا یک کامپیوتر خاص محدود باشید. کافی است کامپیوتر خود را تغییر دهید تا ببینید برنامه های کاربردی و اسناد شما کماکان و به همان شکل قبلی، بر روی ابر در اختیار شما هستند. حتی اگر از ابزار پرتابل نیز استفاده کنید، باز هم اسناد به همان شکل در اختیار شما هستند. دیگر نیازی به خرید یک نسخه خاص از یک برنامه برای یک وسیله خاص، یا ذخیره کردن اسناد با یک فرمت مبتنی بر یک ابزار ویژه ندارید. فرقی نمی‌کند که شما از چه نوع سخت‌افزاری استفاده می‌کنید زیرا اسناد و برنامه های کاربردی شما در همه حال به یک شکل هستند.

۱۱-۳-۶- خصوصیات کلیدی ابر

محاسبات ابرین از خصوصیات منحصر به فردی بهره می‌برد که این سبک محاسباتی را از سایر سبک‌ها متمایز می‌کند. البته برخی از این خصوصیات کما بیش در سبک های پیشین نیز وجود داشته‌اند.

- ارائه سرویس مبتنی بر تقاضا: در اینجا لازم نیست تا برای آنچه استفاده نمی‌کنید هزینه ای پرداخت کنید کافی است تنها تقاضای یک منبع را صادر کرده و در صورتی که از آن استفاده کردید هزینه مربوطه را بپردازید. در این سیستم به راحتی می‌توان در صورت نیاز یک یا چند پردازنده اضافی و یا حافظه و پهنای باند تقاضا داد و از آن‌ها بهره مند شد.
- دسترسی شبکه گسترده (اینترنت): این سیستم برای تحویل و ارائه سرویس‌ها از بستر موجود برای اینترنت استفاده می‌نماید بنابراین مشتریان سرویس‌ها به هیچگونه نرم‌افزار یا سخت‌افزار خاصی نیاز ندارند و با همان مرورگری که هر روزه به گشت و گذار در وب می‌پردازند می‌توانند از سرویس های ابر بهره ببرند.
- استخر منبع: در این سیستم با حجم وسیعی از منابع روبرو هستیم. این منابع از طریق مجازی سازی از محل فیزیکی خود مستقل شده‌اند بنابراین به راحتی می‌توانند در بستر شبکه جابجا شوند.، در واقع نرم‌افزارها، پایگاه داده‌ها، وب سرورها، سیستم عامل‌ها و دستگاه های ذخیره سازی و شبکه ای همگی به عنوان سرورهای مجازی در سیستم حضور دارند.

خصوصیات دیگری نیز برای ابر ارائه شده‌اند که در ادامه به آن‌ها اشاره شده است.

- فوق مقیاس وسیع
- مجازی سازی
- قابلیت اطمینان بالا
- چند کاربردی
- قابلیت گسترش بالا
- سرویس مبتنی بر تقاضا

۱۱-۳-۷- مدل های تحویل سرویس (آناتومی ابر)

سرویس های ارائه شده در محاسبات ابرین را می‌توان به انواع مختلفی تقسیم بندی نمود. در واقع می‌توان برای تفکیک انواع سرویس از مدل XaaS یا "هر چیزی به عنوان سرویس" استفاده نمود. X می‌تواند با مفاهیم مختلفی از جمله نرم‌افزار، کو، زیرساخت، نیروی انسانی، امنیت و غیره جایگزین شود که در ادامه تعدادی از مهمترین آن‌ها که در محیط های دانشگاهی و حتی تجاری به رسمیت شناخته شده‌اند، معرفی می‌گردند.

در شکل زیر سه مدل اصلی تحویل سرویس در محاسبات ابرین را به همراه تعدادی از سیستم های نمونه در هر دسته را مشاهده می‌نمایید.

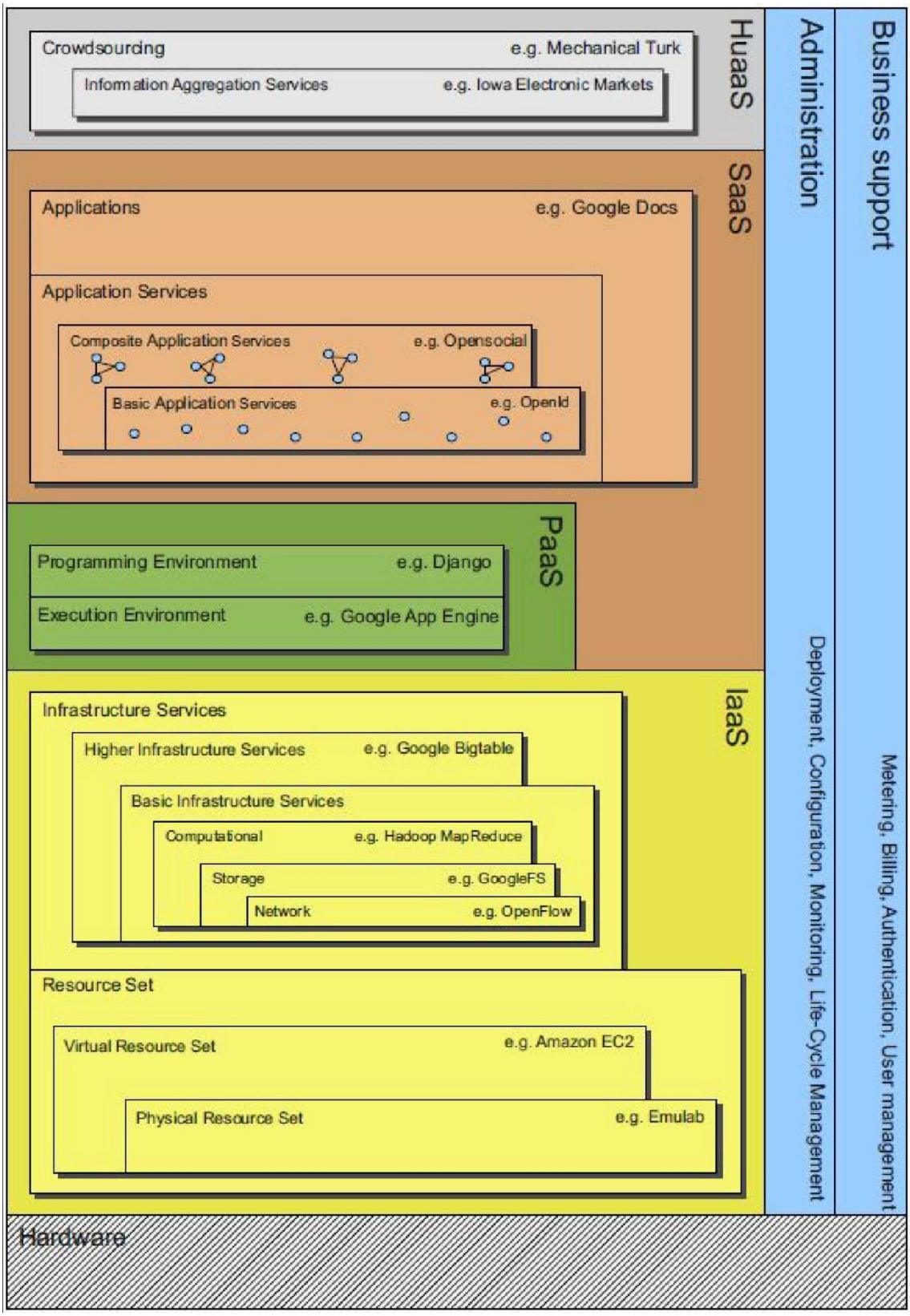


این سه مدل اصلی در واقع بنیان سرویس های محاسبات ابرین را تشکیل می‌دهند و به همین دلیل در معماری محاسبات ابرین به خصوص در مدل معماری لایه ای صریحاً مورد استفاده قرار می‌گیرند و از این رو از اهمیت ویژه ای برخوردار هستند و سایر سرویس های محاسبات ابرین عموماً در یکی از این سه مدل قرار می‌گیرند.

البته همانطور که ذکر شد سرویس های محاسبات ابرین به این سه نوع ختم می‌نوشند و انواع گوناگون زیادی در منابع مختلف برای آن ذکر شده است. از جمله عباراتی چون:

Data, Human, Integration, Enterprise, Security, Operation, Communication, Hardware…

مستقل از طرح عبارت برای برخی از آن‌ها نمونه های تجاری نیز به وجود آمده است و بنابراین تنها جنبه تئوریک نخواهند داشت. مقالات زیادی پشته مرجع ارائه شده توسط لنک را مبنای دسته بندی سرویس‌ها قرار داده‌اند. ما نیز در اینجا از همین پشته برای معرفی انواع اصلی سرویس‌ها استفاده خواهیم نمود. در شکل زیر نمایی کلی از این پشته را مشاهده می‌نمایید.



شرح بخش های اصلی این مدل به اضافه Data as a Service (که آن هم از اهمیت ویژه ای برخوردار میباشد)، به همراه نمونه هایی از سرویس های مرتبط با آن‌ها را در فصل ۴ خواهیم دید.

۱۱-۳-۸- معماری ابر

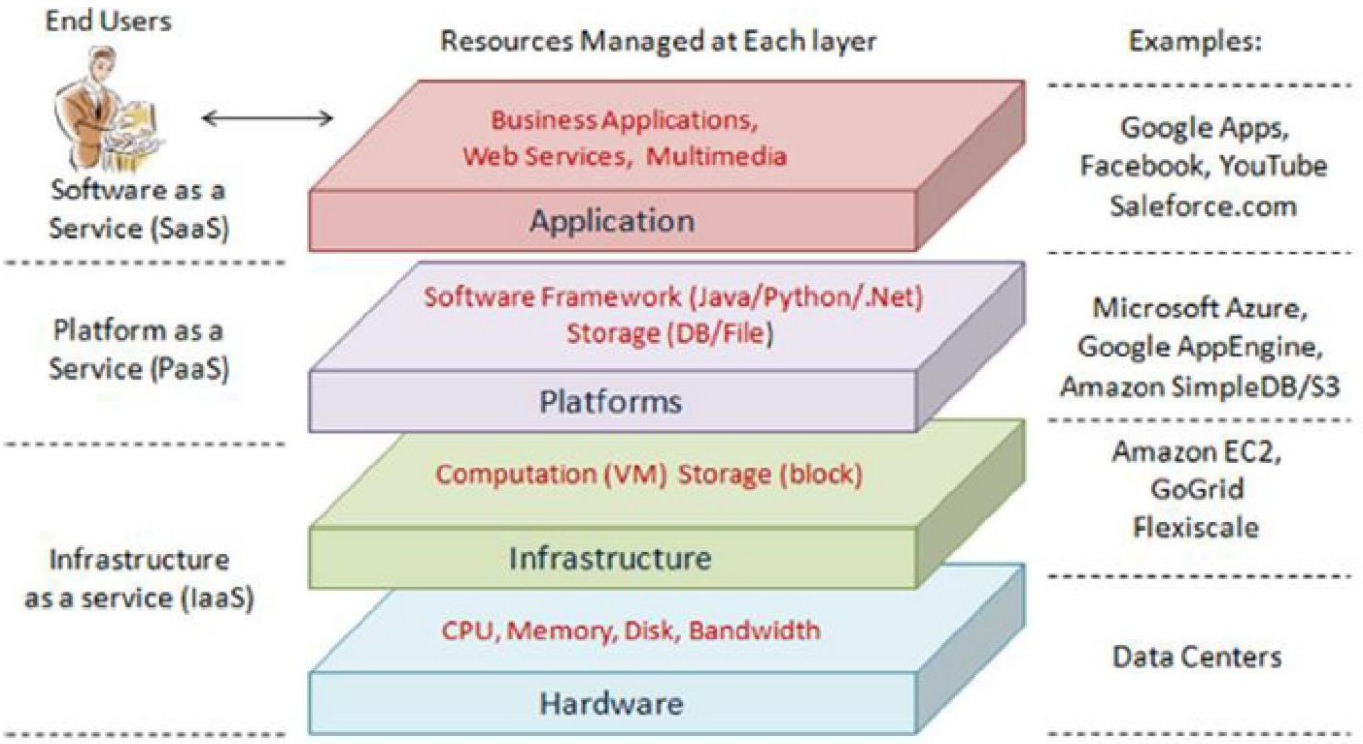
معماری محاسبات ابرین از دو بخش کلی تشکیل شده است؛ بخش جلویی (Front End) و بخش پشتی (Back End).

بخش جلویی مربوط به کاربر و رابط کاربری که او از طریق آن به سرویس های ابر دسترسی پیدا می‌کند، می‌باشد. این بخش شامل شبکه کاربر، سخت‌افزار و نرم‌افزارهایی که او برای بهره بردن از خدمات استفاده می‌کند می‌باشد. بخش پشتی مربوط به خود ابر می‌باشد که در واقع مجموعه از اطلاعات ذخیره شده در سرورها است و سرویس گیرندگان مایل هستند تا به آن‌ها دسترسی پیدا کنند. این دو قسمت از معماری از طریق یک بستر شبکه، عموماً اینترنت، به هم متصل می‌شوند.

لازم به ذکر است عموماً لفظ " معماری محاسبات ابرین " به معماری بخش پشتی آن اشاره دارد جایی که مستقیماً با خود ابر روبرو هستیم. در مقاله پیش رو نیز همین رویه پیش گرفته شده و به بحث اساسی‌تر که همان معماری ابر می‌باشد پرداخته شده است.

مدل لایه ای

به طور عمومی معماری محیط محاسبات ابرین را می‌توان به چهار لایه تقسیم نمود که عبارتند از: لایه سخت‌افزار/پایگاه داده، لایه زیرساخت، لایه سکو و لایه کاربرد که در شکل زیر نمایش داده شده است. اکنون هر یک از این لایه‌ها را به تفصیل مورد بررسی قرار می‌دهیم.



- **لایه سخت‌افزار**

این لایه مسئولیت مدیریت منابع سخت‌افزاری را بر عهده دارد که شامل سرورها، مسیریاب‌ها، سیستم های خنک کننده و غیره می‌باشند. در عمل این لایه عموماً در مراکز داده پیاده سازی می‌شود. یک مرکز داده عموماً از هزاران سرور که از طریق مسیریاب‌ها، سوئیچ‌ها و دیگر ابزارآلات شبکه به هم متصل هستند، تشکیل شده است. موضوعات و مسائل عمومی این لایه، پیکربندی، مدیریت ترافیک، مدیریت توان و خنک سازی می‌باشند.

- **لایه زیرساخت**

لایه زیرساخت که به لایه مجازی سازی هم مشهور است یک استخر از منابع محاسباتی و ذخیره سازی ایجاد می‌نماید. این استخر بوسیله تقسیم بندی منابع فیزیکی به روش مجازی سازی و از طریق ابزارهایی چون KVM، Xen و یا VMware به وجود می‌آید. لایه زیرساخت یکی از مؤلفه های بسیار مهم در بحث محاسبات ابرین می‌باشد زیرا بسیاری از قابلیت های کلیدی مانند انتساب منابع به شکل پویا تنها از طریق تکنولوژی مجازی سازی قابل دستیابی هستند.

- **لایه سکو (Platform)**

این لایه که در بالای لایه زیرساخت قرار می‌گیرند سیستم عامل‌ها و چارچوب های برنامه های کاربردی را در بر می‌گیرد. هدف این لایه به حداقل رساندن حجم برنامه هایی است که می‌بایست مستقیماً بر روی لایه ماشین های مجازی قرار گیرند. به عنوان مثال Google App Engine بر روی لایه سکو قرار می‌گیرد تا از رابط های برنامه نویسی برنامه های کاربردی پشتیبانی نموده تا بدین طریق بتوان پایگاه داده‌ها و یا منطق حرفه را برای برنامه های عمومی تحت وب پیاده سازی نمود.

- **لایه کاربرد**

در بالاترین سطح این سلسله مراتب لایه کاربرد قرار گرفته است که شامل برنامه های واقعاً کاربردی ابر می‌باشد. بر خلاف برنامه های کاربردی سنتی، این برنامه های کاربردی می‌توانند از قابلیت گسترش خودکار به منظور دستیابی به کارایی و دسترسی پذیری بیشتر و هزینه عملیاتی کمتر بهره ببرند.

در مقایسه با محیط های دیگر میزبانی و تحویل سرویس مانند مزرعه سرورهای اختصاصی (Dedicated Servers Farm) معماری ابرها ماجولارتر می‌باشد. لایه‌ها با اتصال سست با هم ارتباط دارند و این باعث می‌شود تا بتوان هر لایه را به شکل مستقل توسعه داد. این طراحی شبیه به مدل مرجع OSI که مربوط به پروتکل های شبکه است، می‌باشد. ماجولار بودن معماری به ابرها این اجازه را می‌دهند تا طیف وسیعی ازنیازمندی های کاربردی را مورد حمایت قرار دهند و به علاوه سربار های مدیریتی و نگهداری را کاهش دهند.

معماری باز محاسبات ابرین

می دانیم محاسبات ابرین با به کارگیری چندین تکنولوژی به مهمترین هدف خود که به اشتراک گذاری منابع مبتنی بر نیازمندی های حرفه می‌باشد می‌پردازد. در عمل دو تکنولوژی نقش بسیار مهمی را در این حوزه بازی می‌کنند که تکنولوژی مجازی سازی و معماری سرویس گرا می‌باشند.

تکنولوژی مجازی سازی مسئولیت ساخت تصاویر مختلفی از سیستم عامل، میان افزار و برنامه های کاربردی و انتساب آن‌ها به ماشین های فیزیکی مربوطه را برعهده دارد. این تصاویر می‌بایست قابلیت جابجایی را در محدوده محیط سیستم داشته باشند. علاوه بر این مسئولیت، این تکنولوژی استفاده مجدد از مجوزهای استفاده از سیستم عامل یا نرم‌افزار های کاربردی را امکانپذیر می‌کند؛ به این صورت که به محض اینکه کاربری به استفاده خود از سیستم عامل پایان داد سیستم بلافاصله می‌تواند منبع را آزاد کرده و در اختیار کاربر دیگری قرار دهد.

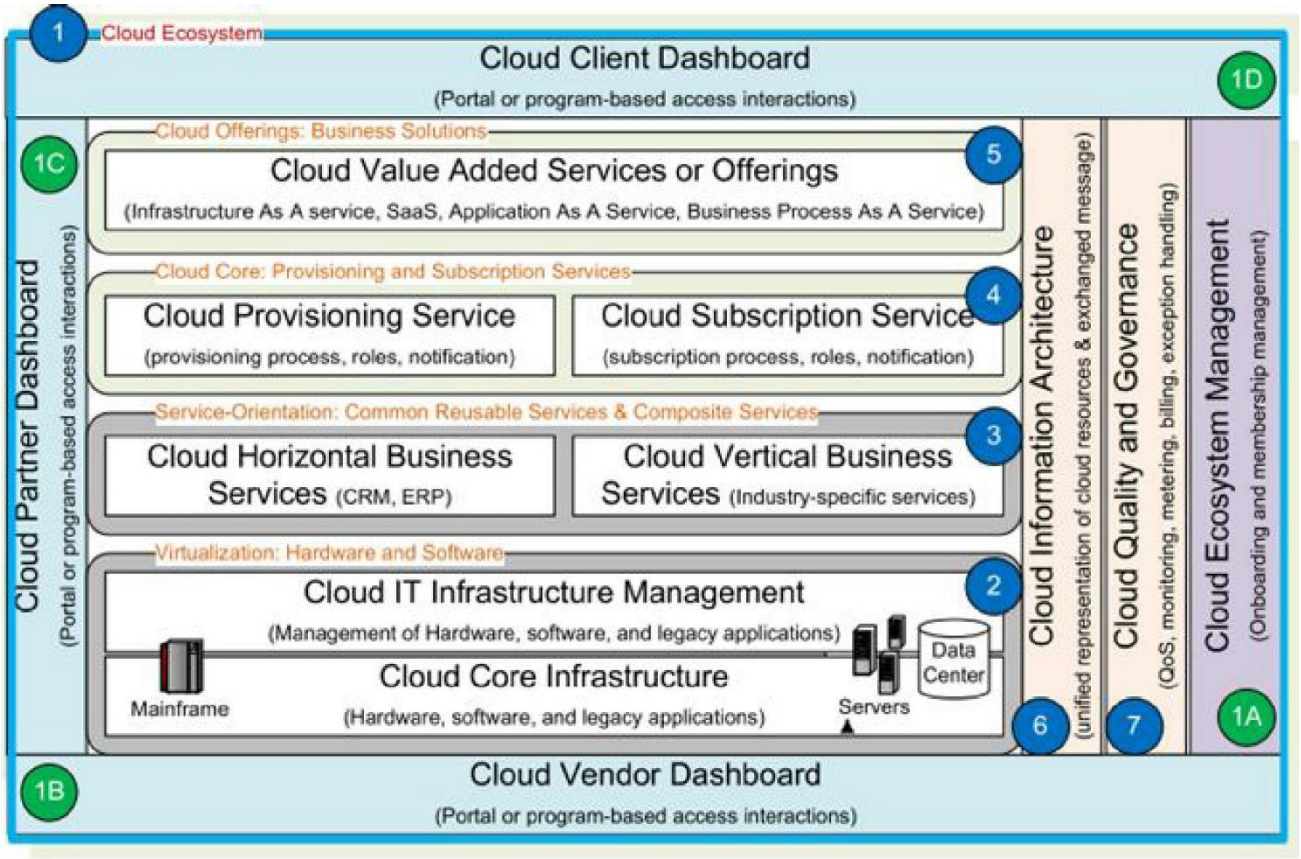
معماری سرویس گرا تکامل یک سیستم یا معماری نرم‌افزار با هدف ایجاد قابلیت استفاده مجدد، مولفه بندی، قابلیت توسعه و انعطاف پذیری می‌باشد. برای ایجاد یک سکوی محاسبات ابرین با قابلیت گسترش بالا نیاز است تا از این نوع معماری برای ساخت مولفه هایی با قابلیت استفاده مجدد و با رابط های استاندارد بهره گرفته شود.

اهداف معماری باز

در این معماری سه هدف برای ایجاد یک معماری باز خوب متصور است. اولین هدف تعیین یک مسیر و روش مشخص برای ایجاد سکوی تامین سرویس‌ها به شکل مقیاس پذیر و قابل پیکربندی می‌باشد. هدف دوم ارائه یک مجموعه سرویس های عمومی و اشتراکی برای ساخت سکو های ابر می‌باشد تا فراهم کنندگان سرویس های حرفه بتوانند ابرهای خود را بر روی این سرویس‌ها بنا کنند. هدف سوم اینست که بتوان با کمک یک زیرساخت فناوری اطلاعات مناسب و یک سیستم مدیریتی، ارزش حرفه ای ابر را به حداکثر میزان آن رساند.

هفت اصل در معماری محاسبات ابرین

در این معماری یک چارچوب یکپارچه تولید و نوآوری پیشنهاد شده که از طریق آن فروشندگان، فراهم کنندگان، شرکاء و مشتریان ابر در کنار هم و بر اساس هفت اصل اساسی کار می‌کنند و این اصول به ده ماجول معماری منتهی می‌شوند که ارتباط آن‌ها را در شکل زیر مشاهده می‌نمایید. این معماری باز تمام بخش های ابر از جمله زیرساخت، مدیریت، سرویس گرایی، هسته ابر جهت تامین و مدیریت مشترکین، معماری اطلاعاتی و تحلیل کیفیت آن را در بر می‌گیرد. در ادامه به معرفی هفت اصل مورد اشاره پرداخته می‌شود.



- **اصل ۱: مدیریت یکپارچه اکوسیستم ابر**

یک معماری باید از مدیریت اکوسیستم ابر پشتیبانی نماید.این اکوسیستم شامل تمامی سرویس‌ها و راه حل های فروشندگان مختلف، شرکا و کاربران نهایی سیستم می‌باشد تا منابع را در محیط ابر به اشتراک بگذارند.

- **اصل ۲: مجازی سازی زیرساخت ابر**

برای بکارگیری مجازی سازی در محیط ابر دو رهیافت وجود دارد. اولی مجازی سازی سخت‌افزار است که در جهت مدیریت تجهیزات سخت‌افزاری به شکل Plug & Play بکار گرفته می‌شود. بنابراین تجهیزات سخت‌افزاری مختلفی را می‌توان به سیستم اضافه و یا از آن حذف نمود بدون آنکه به عملکرد سیستم در حال اجرا خدشه ای وارد شود که مسلماً ظرفیت محاسباتی و فضای ذخیره سازی ابر نسبت به این اضافه و کم شدن‌ها به شکل پویا تغییر می‌یابد. دومین رهیافت مجازی سازی نرم‌افزار است. به عنوان مثال وقتی برای به اشتراک گذاری نرم‌افزار، از تکنولوژی مجازی سازی کد نرم‌افزار و یا سیستم مدیریت تصویر نرم‌افزار بهره می‌بریم.

❖ **اصل ۳: استفاده از سرویس گرایی برای سرویس های مشترک قابل استفاده مجدد**

همانطور که قبلاً گفته شد علاوه بر مجازی سازی، سرویس گرایی یکی دیگر از فناوری هایی است که ابر به کمک آن می‌تواند نیازمندی های حرفه را به کمک سرویس های موجود، برنامه های ترکیبی و سرویس های مشاپ شده پاسخگو باشد. دو نوع سرویس عمومی قابل استفاده مجدد وجود دارد: سرویس های حرفه افقی و عمودی ابر. سرویس های حرفه افقی، سرویس های مختلفی را شامل می‌شوند که پیچیدگی میان افزارها، پایگاه داده‌ها و ابزارها را مخفی می‌کنند. به علاوه میان افزارها و ابزارهای توسعه را در غالب سرویس‌ها ارائه می‌نمایند. سرویس هایی از قبیل نظارت، مدیریت صورت حساب‌ها و یا حتی سرویس هایی نظیر مدیریت ارتباط با مشتریان (CRM) و یا برنامه ریزی منابع سازمان (ERP). سرویس های حرفه عمودی شامل تمامی سرویس های کاربردی مخصوص به صنعت می‌باشد. سرویس هایی نظیر پرداخت و ارسال کالا. هر دو نوع این سرویس‌ها در CCOA قابلیت استفاده مجدد دارند تا بتوان خروجی های مورد انتظار ابر از جمله Infrastructure As a Service، SaaS، Application As a Service و Business Process As a Service را که در اصل پنجم توضیح داده می‌شوند را مهیا نمود.

❖ **اصل ۴: تامین سرویس‌ها و به اشتراک گذاری آن‌ها با قابلیت توسعه بالا**

تامین سرویس‌ها به شکل قابل توسعه یک ویژگی منحصر به فرد برای سیستم های محاسبات ابرین است. بدون قابلیت توسعه، بخش تامین سرویس ابر تنها می‌تواند پاسخگوی نوع خاصی از به اشتراک گذاری منابع باشد.

❖ **اصل ۵: قادرسازی ابر برای داشتن خروجی هایی با قابلیت پیکر بندی مناسب**

خروجی های ابر محصولات و سرویس های نهایی هستند که توسط سکوی ابر تامین شده‌اند. از آنجا که خروجی های ابر اهداف تجاری خاصی را هدف می‌گیرند، به آن‌ها راه حل های تجاری ابر نیز گفته می‌شود. مطابق با دسته بندی انجام شده برای به اشتراک گذاری منابع که پیش‌تر ارائه شد، این معماری خروجی سیستم خود را در چهار سطح ارائه می‌دهد:SaaS ، IaaS،

AaaS و BPaaS.

❖ **اصل ۶: نمایش اطلاعات به شکل یکسان و داشتن چارچوب تبادل پیام**

نحوه نمایش اطلاعات و همچنین تبادل پیام در منابع محاسبات ابرین در تاثیرگذار بودن قابلیت های ابر بسیار مهم هستند. منظور از منابع در CCOA تمامی موجودیت های حرفه (به عنوان مثال مشتریان، شرکا و فروشندگان) و منابع حمایتی از جمله ماجول های مربوط به مجازی سازی و هسته ابر را دربر می‌گیرد.

❖ **اصل ۷: کیفیت ابر و نظارت بر آن**

آخرین و مهم ترین ماجول در CCOA، کنترل کیفیت و نظارت بر ابر می‌باشد که شکل آن قبلا نشان داده شده است. این ماجول مسئول شناسایی و تعریف معیارهای کیفی برای محیط محاسبات ابرین می‌باشد و یک مجموعه راهنمایی های استاندارد برای نظارت بر طراحی، استقرار، اجرا و مدیریت ابر ارائه می‌دهد. از نقطه نظر معیارهای کیفی، پارامترهای مربوط به کیفیت سرویس‌ها (QoS) مستقیماً می‌توانند جهت تعریف ویژگی های مربوط به موجودیت های ابر مانند قابلیت اطمینان، زمان پاسخ، امنیت و قابلیت مجتمع سازی به کار روند.

۱۱-۳-۹- مدل های استقرار

همانطور که در بخش ۳-۷ دیدیم مدل های گوناگونی برای تحویل سرویس‌ها وجود دارد، برای استقرار و بکارگیری ابرهای نیز چندین مدل گوناگون وجود دارد که بسته به مورد کاربری می‌توان هر یک از آن‌ها را بکار گرفت. این مدل‌ها شامل ابرهای خصوصی، عمومی، ترکیبی، انجمنی و یا خاص-منظوره می‌باشند. که در ادامه شرح داده خواهند شد.

ابر خصوصی (Private Cloud)

این ابرها عموماً متعلق به یک شرکت منفرد و یا شرکت های استیجاری هستند و سرویس‌ها فقط در داخل همان شرکت مورد استفاده قرار می‌گیرند. همچنین سرویس‌ها مستقیماً به مشتریان عرضه نمی‌شوند. در واقع این سازمان های هنوز نخواسته یا نتوانستهاند که سرویس هایشان را در اختیار عموم مردم قرار دهند.

نمونه: e-bay

ابر عمومی (Public Cloud)

سازمان‌ها می‌توانند از سرویس های ارائه شده توسط سازمان های دیگر استفاده نمایند و البته سرویس های درون سازمانی خود را نیز در معرض دید سازمان های دیگر قرار دهند. این کار به شرکت‌ها این اجازه را می‌دهد تا ساخت سرویس های خود را برون سپاری کنند و از این طریق هزینه های ساخت سرویس را کاهش دهند.

نمونه: ابرهای آمازون، Google Apps و Windows Azure

ابر ترکیبی (Hybrid Cloud)

با اینکه سازمان های می‌توانند با استفاده از سرویس های ارائه شده در ابرهای عمومی و برون سپاری نیازمندی هایشان از کاهش هزینه زیرساخت بهرهمند شوند، با این حال این کار همیشه مطلوب نیست و سازمان‌ها عموماً ترجیح می‌دهند کنترل نسبی بر روی داده‌ها و سرویس های خود داشته باشند. در این شرایط آن‌ها می‌توانند برای سرویس های حساس خود از مدل خصوصی و در همان زمان، برای سایر سرویس‌ها از مدل عمومی استفاده کنند که به این مدل، ابر ترکیبی گفته می‌شود.

نمونه: ابرهای زیادی که با این مدل کار کنند وجود ندارند.

ابر انجمنی (Community Cloud)

در این مدل چندین سازمان که تقریباً حرفه و نیازمندی های آن‌ها مشترک می‌باشد. منابع و سرویس هایشان را با هم به اشتراک می‌گذارند و یک ابر انجمنی را تشکیل می‌دهند.

نمونه: Open Cirrus

ابر خاص منظوره (Special Purpose)

ابرهای ارائه دهنده IaaS سرویس های همه منظوره ای را ارائه می‌دهند که می‌توانند مورد استفاده دامنه وسیعی از مشتریان با سناریو های کاربردی متعدد قرار گیرد. در مقابل این گونه ابرها، ابرهای دیگری مثل ارائه دهندگان PaaS وجود دارند که دامنه مشتریان محدود تری دارند و برای اهداف خاصی طراحی گردیده‌اند که به این گونه ابرها، خاص منظوره اطلاق می‌شود.

۱۱-۴- نمونه‌ها و کاربردهای محاسبات ابرین

۱۱-۴-۱- سرویس دهنده گان اصلی

همانطور که در فصل ۳ بیان شد، سرویس های ارائه شده در محاسبات ابرین را می‌توان به انواع مختلفی تقسیم بندی نمود. در واقع می‌توان برای تفکیک انواع سرویس از مدل XaaS یا " هر چیزی به عنوان سرویس " استفاده نمود. X می‌تواند با مفاهیم مختلفی از جمله نرم‌افزار، سکو، زیرساخت، نیروی انسانی، امنیت و غیره جایگزین شود. امروزه سه مدل اصلی تحویل سرویس، ساختار به عنوان سرویس (IaaS)، سکو به عنوان سرویس (PaaS) و نرم‌افزار به عنوان سرویس (SaaS) در محاسبات ابرین استفاده می‌شود که این سه مدل اصلی در واقع بنیان سرویس های محاسبات ابرین را تشکیل می‌دهند. همچنین، داده به عنوان سرویس (DaaS)، نیروی انسانی به عنوان سرویس(HaaS) از جمله سایر مدل های مطرح شده برای تحویل سرویس به شمار می‌آیند. در ادامه این مدل‌ها به همراه تعدادی از سرویس دهندگان اصلی آن‌ها معرفی شده‌اند.

۱۱-۴-۲- IaaS

سرویس های ارائه شده در این دسته در پایین ترین سطح و بسیار نزدیک به سخت‌افزار قرار گرفته‌اند. سرویس های درون این بخش را منابع اصلی مانند فضای ذخیره سازی، زیرساخت شبکه و یا توان پردازشی تشکیل می‌دهند. این منابع در دو دسته کلی "مجموعه منابع فیزیکی" و "مجموعه منابع مجازی" قرار می‌گیرند. هر دو این مجموعه‌ها یک رابط برنامه نویسی را در اختیار سرویس های لایه های بالایی قرار می‌دهند تا از طریق آن بتوانند در اختیار گیری و حذف منابع، گسترش بنابر تقاضا، مقابله با از کار افتادن سیستم و بسیاری فعالیت های دیگر را به شکل خودکار انجام دهند. بخش PRS قسمتی است که به سخت‌افزار وابسته می‌باشد بنابراین به یک شرکت ارائه کننده سخت‌افزار گره خواهد خورد در حالیکه بخش VRS مستقل از شرکت های این چنینی خواهد بود. از نمونه های وابسته به سخت‌افزار می‌توان به Emulab و iLO اشاره نمود و سرویس های Nimbus، Tycoon، Eucalyptus، EC2 و OpenNebula از نمونه های مستقل از سخت‌افزار می‌باشند.

در جدول زیر تعدادی از سرویس دهندگان شناخته شده در حوزه IaaS به همراه توصیفی کوتاه از نوع سرویس ارائه شده آن‌ها آورده شده است.

سازمان	سرویس/ابزار	توصیف	لایه/سطح
آمازون	Elastic Compute Cloud (EC2)	سرور مجازی	IaaS – سرویس منبع مجازی
	Dynamo	سیستم ذخیره سازی مبتنی بر کلید- ارزش	IaaS – سرویس زیرساخت پیشرفته
	Simple Storage Service (S3)	سیستم ذخیره سازی دسته ای	IaaS – سرویس زیرساخت پایه
	SimpleDB	پایگاه داده به عنوان سرویس	IaaS – سرویس زیرساخت پیشرفته
	CloudFront	تحویل محتوا	IaaS – سرویس زیرساخت پیشرفته

	SQS	سرویس صف و زمانبندی	IaaS – سرویس زیرساخت پیشرفته
AppNexus	AppNexus Cloud	سرور مجازی	IaaS – سرویس منبع مجازی
گوگل	Google Big Table	سیستم توزیع شده برای ذخیره سازی	IaaS – سرویس زیرساخت پیشرفته
	Google File System	سیستم فایل توزیع شده	IaaS – سرویس زیرساخت پایه
اچ-پی	iLO	مدیریت خاموشی سرور	IaaS – سرویس منبع فیزیکی
	Tycoon	سیستم مدیریت منابع محاسباتی در کلاسترها	IaaS – سرویس منبع مجازی
Joyent	Accelerator	سرور مجازی	IaaS – سرویس منبع مجازی
	Connector	سرور مجازی از قبل تنظیم شده	IaaS – سرویس زیرساخت پیشرفته
	BingoDisk	دیسک ذخیره سازی	IaaS – سرویس زیرساخت پایه
Bluelock	Bluelock Virtual Cloud Computing	سرور مجازی	IaaS – سرویس منبع مجازی
	Bluelock Virtual Recovery	بازیابی مصیبت و شکست	IaaS – سرویس زیرساخت پیشرفته
Emulab	Emulab Network Testbed	بستر آزمایش شبکه	IaaS – سرویس منبع فیزیکی
ENKI	ENKI virtual private data centers	منابع دیتا سنتر مجازی بنابر تقاضا	IaaS – سرویس منبع مجازی
EU Reservoir project	Open Nebula	موتور مجازی زیرساخت (متن باز)	IaaS – سرویس منبع مجازی
FlexiScale	FlexiScale Cloud Computing	سرور مجازی	IaaS – سرویس منبع مجازی
GoGrid	Cloud Hosting	سرور مجازی	IaaS – سرویس منبع مجازی
	Cloud Storage	فضای ذخیره سازی	IaaS – سرویس زیرساخت پایه
Nirvanix	Nirvanix Storage Delivery Network	دیسک ذخیره سازی	IaaS – سرویس زیرساخت پایه
OpenFlow	OpenFlow	شبیه سازی شبکه	IaaS – سرویس زیرساخت پایه
RackSpace	Mosso Cloud Sites	سرور مجازی از پیش تنظیم شده	IaaS – سرویس زیرساخت
	Mosso Cloud Storage	دیسک ذخیره سازی	IaaS – سرویس زیرساخت پایه
	Mosso Cloud Servers	سرور مجازی	IaaS – سرویس منبع مجازی
SkyTap	Skytap Virtual Lab	محیط آزمایشگاه مجازی فناوری اطلاعات	IaaS – سرویس زیرساخت
Terremark	Infinistructure	سرور مجازی	IaaS – سرویس منبع مجازی
UCSB	EUCALYPTUS	نسخه متن باز EC2 آمازون	IaaS – سرویس منبع مجازی
10gen	Mongo DB	پایگاه داده برای ذخیره سازی ابرین	IaaS – سرویس زیرساخت پیشرفته
	Babble Application Server	سرور برنامه های تحت وب برای استقرار ابرین	IaaS – سرویس زیرساخت پیشرفته

همانطور که مشاهده می‌شود تعداد زیادی از سرویس دهندگان از جمله شرکت های بزرگ آمازون، گوگل و اچ -پی در این حوزه فعالیت می‌کنند و این مسئله نشان گر اهمیت این مدل سرویس در محاسبات ابرین می‌باشد. در واقع بدون زیرساخت محاسبات ابرین لایه های بالایی قادر به سرویس دهی نخواهند بود. به همین دلیل شکل گیری محاسبات ابرین نیز از این مدل آغاز گردید و تا به امروز شرکت های بسیاری سرویس های خود را در این حوزه ارائه نموده‌اند. لازم به ذکر است که با

بررسی های انجام گرفته بر روی این نمونه‌ها و آنچه در ادامه نیز خواهد آمد مشکلاتی شناسایی شدند که در بخشی مجزا با عنوان "مشکلات ابرها ی موجود " به آن‌ها پرداخته خواهد شد.

۱۱-۴-۳- PaaS

اگر یک لایه بالاتر آییم با بخش سکو به عنوان سرویس روبرو خواهیم شد.. چیزی که در اینجا از آن به عنوان سکو یاد شده به دو محیط متفاوت بر می‌گردد. محیط توسعه سیستم و محیط اجرا آن. در مورد محیط اول می‌توان به پروژه شرکت سان به نام

Caroline و یا چارچوب Django اشاره نمود و برای محیط اجرا می‌توان به نمونه هایی چون AppEngine شرکت گوگل یا سیستم Azure شرکت مایکروسافت اشاره نمود. البته آنچه از تحلیل دو نمونه ذکر شده به دست می‌آید این است که محیط های اجرایی، خود محیط توسعه مخصوص به خود را در بر می‌گیرند. بنابراین برای اجرای یک سیستم تحت AppEngine شما می‌توانید از محیط توسعه مخصوص به آن هم استفاده نمایید و البته محیط اجرای Azure Umbrella نیز ابزارهای متفاوتی را برای توسعه سرویس‌ها در اختیار شما قرار خواهد داد.

در جدول زیر تعدادی از سرویس دهندگان شناخته شده در حوزه PaaS به همراه توصیفی کوتاه از نوع سرویس ارائه شده آن‌ها آورده شده است.

سازمان	سرویس/ابزار	توصیف	لایه/سطح
Akamai	EdgePlatform	تحویل برنامه کاربردی، محتوا و سایت	PaaS
مایکروسافت	Azur	محیط توسعه و اجرا برای برنامه های کاربردی مایکروسافت	PaaS
	Live Mesh	بستری برای به هنگام سازی، اشتراک و دسترسی به دامنه وسیعی از دستگاه هایی با سیستم عامل مایکروسافت	PaaS
فیس بوک	Facebook Platform	بستر آزمایش شبکه	PaaS
گوگل	App Engine	محیط اجرایی قابل گسترش برای برنامه های تحت وب نوشته شده در زبان پایتون	PaaS
NetSuite	SuiteFlex	جعبه ابزاری برای سفارشی سازی برنامه های کاربردی کسب و کار آنلاین همین شرکت	PaaS
Salesforce	Force.com	ساخت و تحویل برنامه های کاربردی در کلاس کسب و کار	PaaS
Sun	Caroline	بستر قابل گسترش افقی برای توسعه و استقرار سرویس های تحت وب	PaaS
Zoho	Zoho Creator	جعبه ابزاری برای ساخت و تحویل برنامه های کاربردی در کلاس کسب و کار و به شکل بنابرتقاضا	PaaS

۱۱-۴-۴- SaaS

تمامی برنامه های کاربردی که بر روی ابر کار می‌کنند و یک سرویس مستقیم را به مشتریان عرضه می‌دارند در این لایه قرار می‌گیرند. توسعه دهندگان این سرویس‌ها می‌توانند برای توسعه و اجرای برنامه های خود از PaaSها و یا مستقیماً از IaaSها استفاده نمایند. اگر بخواهیم می‌توانیم سرویس های ارائه شده در این لایه را به دو بخش سرویس های پایه و سرویس

های مرکب تقسیم نماییم. از نمونه های سرویس های پایه که همگی با آن‌ها آشنا هستیم می‌توان به سرویس OpenId و سرویس نقشه گوگل اشاره نمود. یکی از راه های توسعه سرویس های مرکب استفاده از ویرایشگرهای مشاپ می‌باشد و البته نرم‌افزار های قدرتمندتر و پیچیده تری نیز در این دسته قرار می‌گیرند از جمله Google Docs و یا Microsoft Office Live که نسخه آنلاین برنامه آفیس می‌باشد.

در جدول زیر تعدادی از سرویس دهندگان شناخته شده در حوزه SaaS به همراه توصیفی کوتاه از نوع سرویس ارائه شده آن‌ها آورده شده است.

سازمان	سرویس/ابزار	توصیف	لایه/سطح
گوگل	Google Docs	بسته نرم‌افزاری آفیس آنلاین	SaaS
	Google Maps API	رابط برنامه نویس سرویس نقشه گوگل به توسعه دهندگان این امکان را می‌دهد تا نقشه گوگل را در سایتهای خود جاسازی کنند	SaaS – سرویس ساده
	OpenSocial	یک رابط برنامه نویسی کاربردی مشترک برای برنامه های شبکه های اجتماعی	SaaS – سرویس مرکب
OpenID Foundation	OpenID	یک سیستم توزیع شده که به کاربران این اجازه را می‌دهد تا تنها با یک شناسه دیجیتال بتوانند از سایتها مختلف استفاده نمایند.	SaaS – سرویس ساده
مایکروسافت	Office Live	بسته نرم‌افزاری آفیس آنلاین	SaaS
Salesforce	Salesforce.com	بسته نرم‌افزاری مدیریت روابط مشتریان	SaaS

۱۱-۴-۵- DaaS

همانطور که گفته شد جدا از لایه های مطرح شده در پشته مرجع محاسبات ابرین، انواع دیگری از سرویس‌ها نیز وجود دارند که البته می‌توان آن‌ها را با ملاحظاتی در داخل هر یک از لایه های مطرح شده گنجاند. با این حال آن‌ها به خودی خود دارای استقلال هویتی هستند و می‌توانند جداگانه مورد بحث قرار گیرند. یکی از مهمترین این انواع، " داده به عنوان سرویس " می‌باشد که از جهاتی شباهت زیادی به SaaS دارد. در این نوع سرویس‌ها " داده " به شکل بنابر تقاضا ارائه می‌شود. شاید بپرسید این چیز جدیدی نیست و از مدتها قبل شرکت هایی وجود داشتند که داده‌ها و اطلاعات را در اختیار متقاضیان آن‌ها قرار می‌دادند. اما باید بگوییم این سرویس از این جهت با آن‌ها متفاوت است که داده‌ها در اینجا در ابر، زنده هستند و با گذر زمان تغییر می‌کنند. در حالت اول متقاضیان داده هایی را می‌خریدند و به سیستم خود وارد می‌نمودند و مورد تحلیل و ارزیابی قرار می‌دادند. در این حالت ارتباط آن‌ها با منبع داده‌ها، تا زمان بعدی درخواست داده جدید، قطع بود و از به روز رسانی داده‌ها بهره ای نمی‌بردند. در DaaS شرکت‌ها مجبور نیستند حجم عظیمی از داده‌ها را درخواست دهند حال آنکه تنها به بخش کوچکی از آن‌ها احتیاج دارند. آن‌ها می‌توانند داده های موجود در ابر را در همان محل اصلی خود مورد جستجو قرار دهند و فقط بخشی را که واقعا به آن نیاز دارند را به شکل کاملاً به روز شده دریافت نمایند. از نمونه های این نوع سرویس می‌توان به Xignite،Infochimps و غیره اشاره نمود.

در جدول زیر تعدادی از سرویس دهندگان شناخته شده در حوزه DaaS به همراه توصیفی کوتاه از نوع سرویس ارائه شده آن‌ها آورده شده است.

سازمان	سرویس/ابزار	توصیف	لایه/سطح
Hoover's	Hoover's	داده های مربوط به مشاغل، صنایع و افراد دست اندر کار	DaaS
Xignite	Xignite	داده های مالی بازار داد و ستد	DaaS
Urban Mapping	Urban Mapping	داده های جغرافیایی. ارزشمند برای کمپانی های املاک و مستغلات	DaaS
socrata	socrata.com	داده های حکومتی (عمومی)	DaaS

۱۱-۴-۶- HaaS

برخی از سرویس‌ها بر جمع آوری و استخراج داده از جمعیتی از انسآن‌ها متکی هستند. هر فردی از اجتماع می‌تواند از ابزارها و فناوری های مناسب برای حل مسئه مشخص شده استفاده نماید. در برخی نمونه‌ها هوش بشر به عنوان حل کننده زیر مسائل بنابر تقاضا مورد استفاده قرار می‌گیرد مانند سرویس Mechanical Turk شرکت آمازون و در برخی دیگر از هوش جمعی برای پیش بینی رخدادها و یا گسترش ایده های مردم پسند استفاده می‌گردد.

در جدول زیر تعدادی از سرویس دهندگان شناخته شده در حوزه HaaS به همراه توصیفی کوتاه از نوع سرویس ارائه شده آن‌ها آورده شده است.

سازمان	سرویس/ابزار	توصیف	لایه/سطح
آمازون	Mechanical Turk	به کارگیری قدرت کار بشر به شکل گسترش پذیر	HaaS
Digg.com	Digg.com	جمع آوری خبر	HaaS
The University of Iowa	Iowa Electronic Markets	پیش بینی آینده بازار طبق رخداد های اقتصادی و سیاسی	HaaS
Youtube	Youtube	پرتال تصویری	HaaS

۱۱-۴-۷- کاربرد محاسبات ابرین

نمونه هایی از کاربردهای محاسبات ابرین در این بخش مطرح گردیده‌اند. این کاربردها در سه دسته کلی پایپ- لاین پردازشی، سیستم های پردازشی دسته ای و وب سایت‌ها ارائه می‌شوند. در هر دسته، نمونه هایی آورده شده است.

- پایپ- لاین پردازشی
  - پایپ-لاین پردازش مستندات
  - پایپ-لاین پردازش تصاویر
  - پایپ-لاین تبدیل تصاویر
  - شاخص گذاری
  - داده کاوی
- سیستم های پردازشی دسته ای
  - تحلیل گزارشات
  - ساخت های شبانه خودکار

- تست واحد و تست استقرار خودکار

❖ وب سایت ها

- سایت های هوشمند قابل گسترش
- سایت های لحظه ای
- سایت های فصلی

کاربرد در سیستم های فوق مقیاس وسیع

عبارت "محاسبات ابرین" از جنبه های مختلفی در کنار عبارات "سیستم های فوق مقیاس وسیع" و یا "سیستمی از سیستم‌ها" قرار گرفته است و این، حاکی از تاثیر محاسبات ابرین بر روی سیستم های فوق مقیاس وسیع و بالعکس می‌باشد. گاهی از محاسبات ابرین به عنوان یک معماری SoS یاد شده و زمانی دیگر از خود ابر به عنوان یک سیستم فوق العاده پویا از سیستم‌ها. البته آنچه واضح است این است که از ابر می‌توان برای توسعه سیستم های فوق وسیع استفاده نمود. در حال حاضر سرویس های دسته IaaS و PaaS به طور عملی در ابرها مورد استفاده قرار می‌گیرند ولی سرویس های لایه های بالاتر کمتر به شکل عملی به کار گرفته شده‌اند. از مثال هایی که می‌توان در زمینه ارائه نمود راه حل های مبتنی بر ابر ارائه شده توسط شرکت Salesforce و کاربرد عملی آن‌ها مثلاً در سیستم مراقبت بهداشت که به دلیل ویژگی های با ارزش به عنوان یکی از مصادیق سیستم های فوق مقیاس وسیع مطرح می‌باشد.

معرفی salesforce.com

این شرکت از پیش تازان این حوزه می‌باشد و به عنوان اولین شرکت خالص ابرینِ میلیارد دلاری مطرح شده است. CRM ارائه شده توسط این شرکت به تنهایی دارای ۱.۱ میلیون نفر کاربر در سرتاسر جهان می‌باشد و درآمد سه ماهۀ منتهی به آوریل ۲۰۰۸ این شرکت بالغ بر ۲۴۸ میلیون دلار بوده است. به عنوان یک نمونه از کاربرد و تاثیر یک راه حل مبتنی بر ابر بر یک تجارت، به بررسی سیستم مراقبت بهداشت شرکت CRC Health می‌پردازیم.

مطالعه موردی – سیستم مراقبت بهداشت – Health care

شرکت CRC Health به عنوان بزرگترین تامین کننده ملی سرویس های درمان بیماران الکلی و مصرف کننده مواد مخدر مطرح است. این شرکت برای مدیریت و پذیرش بیماران و همچنین پیگیری تحت وب این اطلاعات نیاز به یک سکوی یکپارچه داشته است. علاوه بر این مدیریت این شرکت در جهت افزایش سود دهی و کاهش هزینه‌ها سیاست خود را بر استفاده از عملیات های ساده و پرهیز از فرآیند های هزینه بر و پیچیده گذاشته است. این شرکت برای مدیریت داده های بیماران عموماً از سیستم Act و صفحه گسترده‌ها استفاده می‌کرده است. اما این روش محدودیت هایی را به همراه داشته است از جمله اینکه در یک لحظه تنها یک اپراتور تلفنی می‌توانست یک صفحه گسترده را باز کند و این باعث کاهش کارایی، افزایش ابهام و کاهش قابلیت گسترش سیستم می‌شد.

بنابراین این شرکت تصمیم گرفت از راه حل ارائه شده توسط شرکت Salesforce استفاده نماید و در این راستا یک رابط کاربری را بر روی Force.com توسعه داد. این تصمیم علاوه بر داشتن خصوصیات مورد نظر سیستم قبلی از جمله سادگی و کم هزینه بودن فرآیندها مزایای بیشمار دیگری را نیز برای این شرکت به ارمغان آورد از جمله افزایش امنیت تا سطح مورد نیاز برای HIPPA و دیگر آیین نامه های صنعتی، امکان ردیابی ساده و موثر تحت وب از طریق CRM شرکت و

همچنین اینکه Open API های موجود در این سکو امکان یکپارچه سازی کامل را با سیستم های قدیمی موجود مانند Outlook و eFax و... را فراهم می‌نمود.

این نمونه از کاربر راه حل های مبتنی بر ابر در سیستم های فوق مقیاس وسیع بود اما این تمام ماجرا نیست؛ محاسبات ابرین به عنوان یک تکنولوژی داغ روز در طراحی سیستم های فوق مقیاس وسیع نیز کاربرد دارد که در بخش بعدی به بررسی آن می‌پردازیم.

طراحی سیستم های مقیاس وسیع

برای توسعه سیستم های مقیاس وسیع قطعاً بکارگیری و یکپارچه سازی تکنولوژی های روز یکی از ملزومات است و البته در این راه با چالش های فراوانی روبرو خواهیم بود که بسیار حائز اهمیت هستند. به عنوان مثال به لایه ای برای ترکیب سرویس‌ها نیاز است و این لایه در مقیاس پذیری سیستم نقش به سزایی خواهد داشت و یا مباحث مربوط به تضمین کیفیت سرویس از مباحث باز و چالش برانگیز این حوزه است، همچنین کشف سرویس های غیر متمرکز به دلیل وسعت سیستم کار بسیار دشواری است.

آنچه واضح است اینست که این مسئله یکپارچه سازی به یکباره قابل حل نمی‌باشد زیرا لایه زیرساخت محاسباتی مدام در حال تغییر است به عنوان مثال وب پس از مدتی با وب- ۲ و وب معنایی جایگزین گردید، بنابراین توسعه دهندگان باید بدانند که کی یک تکنولوژی داغ روز مورد اطمینان است تا از آن برای توسعه سیستم استفاده نمایند در غیر اینصورت راه حل ارائه شده پس از آمدن یک تکنولوژی جدید و کارا دیگر معتبر نخواهد بود.

شکل زیر روند تکامل وب را نشان می‌دهد.



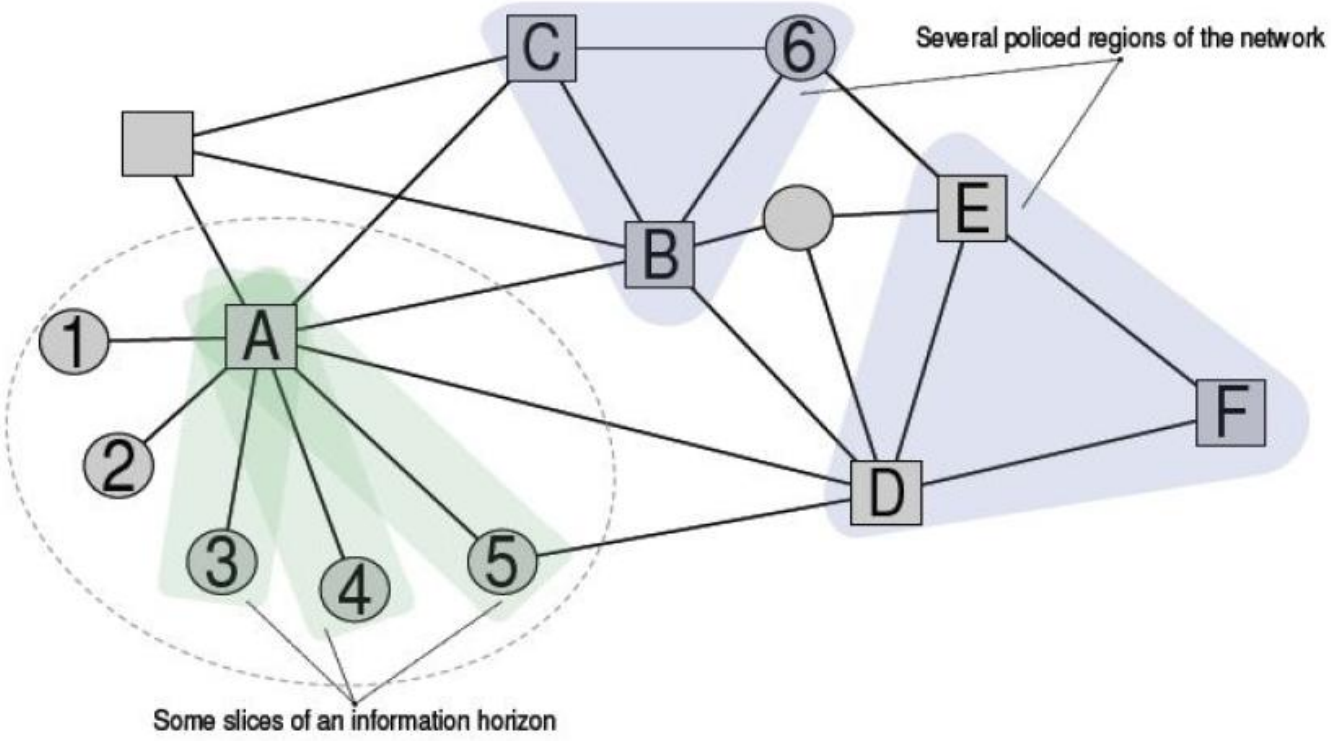
رهیافتی مدل رانه برای طراحی سیستم های مقیاس وسیع

طراحی مدل رانه این اینگونه مشکلات را هدف قرار می‌دهد، در واقع به جای اینکه توسعه دهندگان تمرکز خود را بر روی تکنولوژی های پیاده سازی قرار دهند، بهتر است تمرکز خود را بر روی الگوی مدل سازی قرار دهند. الگویی که با فراهم سازی یک زبان برای ساخت مدل به انتساب مفاهیم با مدل‌ها می‌پردازد بدون اینکه از تکنولوژی پیاده سازی سخنی به میان آورد. البته نگرانی در پیاده سازی این مدل‌ها وجود ندارد زیرا در نهایت این مدل‌ها را می‌توان از طریق یک فرآیند نیمه خودکار در یک مولد کد، به کد پیاده سازی تبدیل نمود. در صورت استفاده از این رهیافت به راحتی می‌توان با ایجاد و جایگزینی یک مولد کد جدید برای یک تکنولوژی جدید، از تکنولوژی های داغ روز بهره برد. این رهیافت قبلاً در تولید نرم‌افزار های سنتی هم مورد استفاده قرار می‌گرفت در واقع سعی می‌شد تا ویژگی های نرم‌افزار را در دو دسته مدل های مستقل از سکو ۵۰ و وابسته به سکو (Platform) توصیف نمود. این مدل‌ها از طریق مبدل های مدل به هم قابل تبدیل هستند.

در این رهیافت در ابتدا الگوی مدل سازی با نام BAM برای توصیف یک سیستم محاسبات ابرین بر روی یک بستر شبکه ای کاملاً پویا، ارائه شده است که در نهایت با استفاده از یک مولد کد که تکنولوژی خاصی را هدف گرفته است به سیستم اجرایی بدل خواهد شد.

محاسبات ابرین داده محور توسط BAM

محاسبات ابرین توصیف کننده برنامه های کاربردی است که از ترکیب سرویس هایی که در سطح نود های زیادی توزیع شده‌اند به دست آمده‌اند. برخلاف مدل های محاسباتی توزیع شده دیگر، محاسبات ابرین، به توپولوژی و ارتباطات شبکه وابستگی بسیار کمی دارد. شکل زیر نمایش دهنده یک ابر می‌باشد که در آن دایره‌ها و مربع‌ها نشاندهنده نود هایی هستند که دو نوع سرویس مختلف را ارائه می‌دهند. یال های بین نودها نیز نشان دهنده خطوط ارتباطی بین نودها می‌باشند. ارتباطات بی نظم نشان داده شده در شکل معرف این موضوع است که سیستم ابر بر روی یک بستر سست و کاملاً پویا که در طول زمان مدام در حال تغییر می‌باشد، واقع شده است. در این مرحله چالش اصلی بهره گیری از این زیرساخت متلاطم به گونه ای قابل پیش بینی می‌باشد.



تعریف و توصیف برنامه های کاربردی تحت ابر توسط BAM پشتیبانی می‌شود، همچنین در آن قابلیت تحلیل فرمال رفتار

سیستم‌ها فراهم شده است. یک توصیف BAM به طور خلاصه شامل موارد زیر است:

- یک شمای پایگاه داده که داده هایی که به وسیله برنامه پردازش می‌شوند را تعریف می‌کند.
- یک مجموعه از قوانین سازگاری که می‌بایست توسط پایگاه داده رعایت شوند.
- یک مجموعه از عملیات بر روی داده‌ها که وضعیت یک پایگاه داده را تغییر می‌دهند.

برای توصیف یک برنامه در ابتدا کاربر بدون اینکه دغدغه چگونگی توزیع برنامه اش را بر روی ابر داشته باشد، نیازمندی را در قالب مدل بالا ارائه می‌نماید. یادآوری می‌شود با اینکه در اینجا صحبت از شمای پایگاه داده و عملیات بر روی داده‌ها شده است، اما به هیچ وجه منظور، یک پیاده سازی یا تکنولوژی خاص نمیباشد و تمامی این مفاهیم به وسیله جبر و فرمول های منطقی بیان می‌شوند.

پس از آنکه نیازمندی های داده ای تعیین شدند، کاربر شما را مطابق ابر دلخواه خود تقسیم بندی می‌کند. این عمل از طریق شناسایی انواع نودها و همچنین چگونگی اتصال میان آن‌ها امکانپذیر می‌باشد. این تقسیم بندی به شکلی انجام می‌شود که قوانین سازگاری در هر یک از قسمت‌ها قابل دستیابی باشد.

یک مدل BAM می‌تواند الگوهای تعاملی میان مؤلفه های مختلف را نمایش دهد و پیاده سازی یک سیستم BAM به معنی نوشتن کدی است که این الگوهای تعامل را پیاده سازی می‌کند، برخی از این کدها مخصوص مدل BAM می‌باشند اما برخی دیگر به حل مسائل عمومی در زمینه سیستم های توزیع شده مربوطند. در اینجا هدف اصلی استفاده از آخرین فناوری‌ها برای حل زیر مسائل عمومی، تولید عملکردهای خاص مدل و سپس یکپارچه سازی آن‌ها می‌باشد. زیر مسائل عمومی مطرح در این مسئله به همراه فناوری استفاده شده برای پاسخ به آن شامل موارد زیر می‌باشند:

- کشف نود: در ابر هر نود می‌بایست از جایگاه نود های دیگری که قرار است به او سرویس بدهند باخبر باشد البته با این فرض که دانش متمرکزی از وضعیت شبکه در دست نیست. برای این مسئله از فناوری PNRP استفاده می‌شود.
- ترکیب سرویس: برای انجام یک عمل مفید لازم است سرویس‌ها با هم در تعامل باشند. برای این مورد از فناوری .NET Remoting بر روی نود های ابر استفاده می‌شود.
- مانایی داده: نودها می‌بایست بوسیله یک لایه مانایی قدرتمند از داده های محلی خود نگهداری کنند. برای تامین این لایه از فناوری LINQ و SQL بهره برده می‌شود.
- پشت صحنه وضعیت دار: حرکت کاربر در صفحات وب ارتباط با وب-سروری را ایجاد می‌کند که فعالیت‌ها وضعیت داری را اجرا می‌کند. برای این مورد از فناوری VOLTA استفاده می‌شود.

هر یک از این فناوری‌ها نقش به سزایی در حل زیر مسائل عمومی دارند و بنابراین نود های ابر بدون بکارگیری آن‌ها قادر به پیاده‌سازی نیستند. از این بابت می‌توان ابر را یک SoS فوق پویا نامید.

در این مقاله از طریق یک API مدل BAM ایجاد شده در مراحل قبل به فایل های Visual Studio تبدیل می‌شوند که آن‌ها بوسیله تعدادی مولد کد مورد پردازش قرار می‌گیرند. سپس همانطور که گفته شد از Microsoft Volta برای تبدیل خودکار یک برنامه به زبان C # به صفحات وب پویای وضعیت دار استفاده می‌شود. در نهایت با استفاده از یک موتور الگوی C # برای یکپارچه سازی مؤلفه‌ها استفاده می‌شود و سیستم BAM مورد نظر پیاده سازی می‌شود.

چه کسانی می‌توانند از ابر استفاده کنند؟

برای آنکه امکان پذیری و کاربردی بودن مسأله ای بررسی شود، لازم است نمونه هایی عملی از استفاده از آن موضوع بررسی و بیان شود، لذا در ادامه تعدادی از مطالعات موردی معتبر و برخی ویژگی های مربوط به آن‌ها، در استفاده عملی از توان و پتانسیل محاسبات ابرین ارائه می‌شود.

- ❖ پیتر هارکینز در واشینگتن–پست
  - ۲۰۰ عدد EC2 آمازون (۱۴۰۷ ساعت کار سرور – دو ماه شبانه روز)
  - تبدیل ۱۷۴۸۱ صفحه از مستندات سفرهای هیلاری کلینتون
  - تنها در ۹ ساعت با هزینه ۱۴۴ دلار
- ❖ روزنامه نیویورک تایمز
  - ۱۰۰ عدد EC2 آمازون
  - برنامه Hadoop
  - تشخیص ۴ ترا بایت عکس خام (با فرمت TIFF)
  - تبدیل به ۱.۱ میلیون فایل PDF
  - در ۲۴ ساعت با هزینه ۲۴۰ دلار
- ❖ وزارت دفاع امریکا
  - هم اکنون سرویس ابرین ارائه می‌دهد.
  - بستر Rapid Access Computing Environment (RACE)
  - با دسترسی پذیری ۹۹.۹۹۹ ٪
  - افزایش سرعت استقرار (نصب سرور جدید در ۲۴ ساعت به جای ۶ ماه)

۱۱-۴-۸- نتیجه گیری

در این فصل سرویس های ارائه شده در مدل های مختلف محاسبات ابرین و همچنین کاربرد های احتمالی که این سرویس‌ها در سیستم های کامپیوتری می‌توانند داشته باشند، مطرح گردیدند. همانطور که گفته شد با توجه به تعداد سرویس های ارائه شده در مدل IaaS می‌توان به اهمیت این مدل نسبت به سایر مدل‌ها پی برد. در واقع نتیجه چیزی جز این نیز نخواهد بود زیرا بدون وجود زیرساختی مناسب با مشخصه های ادعا شده، قرارگیری لایه های بالاتر از جمله PaaS و SaaS ناممکن می‌نمود. محاسبات ابرین می‌تواند در زمینه های متعددی کارایی بالایی داشته و در بهینه سازی سیستم نقش به سزایی داشته باشد. از جمله:

- زمانی که مقیاس پذیری بالا مورد انتظار باشد، زیرا فراهم سازی منابع با کمترین هزینه در محاسبات ابرین امکان پذیر است.
- در سیستم های چند– مستاجری که تعداد زیادی از کاربران از سیستمی با یک منبع کد استفاده می‌نمایند.
- در محاسبات پیچیده و توزیع شده که نیاز به منابع متعدد و کم هزینه وجود دارد.

- در ذخیره سازی داده های بسیار حجیم، زیرا محاسبات ابرین می‌تواند حافظه ارزان و تقریباً بی نهایت را برای یک سازمان به ارمغان آورد.

۱۱-۵- ترکیب سرویس و یکپارچه سازی سیستم در فضای ابر

۱۱-۵-۱- مقدمه

با گذشت زمان بر محبوبیت محاسبات ابرین افزوده شده است و غول های صنعت فناوری اطلاعات دنیا مانند گوگل، آمازون، مایکروسافت، آی- بی- ام هر یک زیر ساخت ابر مخصوص به خود را راه انداخته‌اند و بحث اصلی جایی شکل می‌گیرد که این زیرساخت‌ها به شکل جداگانه و جزیره ای تهیه شده‌اند و در برخی شرایط کمترین تعامل را با یکدیگر برقرار امکانپذیر نموده‌اند. در این شرایط جای خالی مفهوم ترکیب سرویس و یکپارچه سازی سیستم به شدت احساس می‌شود. در این بخش هدف ما بررسی وضعیت کنونی سیستم‌ها در قبال این مسئله می‌باشد. این بخش از گزارش به دلیل تاثیر به سزا بر شکل دهی روند تحقیقات و کارهای آینده، پر اهمیت می‌باشد. در ادامه مفاهیم اصلی در حوزه ترکیب سرویس و یکپارچه سازی ارائه شده و چالش های مطرح در این حوزه در بخش بعد مورد بررسی قرار خواهند گرفت و در نهایت نتایج این بررسی‌ها به عنوان بخش اصلی نتیجه گیری ارائه خواهند شد.

۱۱-۵-۲- ترکیب سرویس ابرین

سرویس های ساده محاسبات ابرین می‌توانند با یکدیگر ترکیب شده و سرویس های پیچیده تر، متنوع‌تر و کاربردی تری را تشکیل دهند. این مطلب تنها در مورد سرویس هایی که تاکنون با آن‌ها آشنا بودیم یعنی SaaS یا سرویس های نرم‌افزاری صادق نیست بلکه برای سرویس های لایه های پایینتر که در معماری لایه ای با آن‌ها آشنا شدیم نیز صادق است.

برای تشکیل یک سرویس مرکب می‌توان سرویس های داخل یک ابر را با هم ترکیب نمود و یا سرویس هایی از چندین ابر متفاوت که البته روش اول به دلیل سازگاری بیشتر سرویس‌ها، بیشتر مورد استفاده قرار می‌گیرد. لازم است در اینجا به نکته ظریفی در مورد تفاوت ترکیب سرویس های ابرین و ترکیب وب- سرویس‌ها در معنای عام توجه شود. بحث ترکیب سرویس‌ها در بستر چارچوب های دستی یا خودکار و یا به صورت مشاپ (Mashup)، بیشتر به سرویس های ساده یا مرکب عملیاتی و عموماً کاربردی و در سطوح بالای انتزاع مربوط می‌شود، در حالیکه آنچه در اینجا از آن به عنوان سرویس های ابرین یاد می‌شود بیشتر به سرویس هایی که معنای خود را از محاسبات ابرین گرفته‌اند و حتی به سطوح زیرساختی مربوط هستند بر می‌گردد، به عنوان مثال سرویس هایی در حوزه فضای ذخیره سازی یا محاسباتی. منظور ما از ترکیب سرویس ابرین، ترکیب این گونه سرویس‌ها و البته در کنار وب‌سرویس های دیگر در معنای عام می‌باشد. در ادامه به بیان نمونه هایی از ترکیب سرویس ابرین در دو نوع مطرح شده، می‌پردازیم.

۱۱-۵-۳- ترکیب سرویس های داخل یک ابر

اخیراً برخی از مهندسین نرم‌افزار شرکت آمازون تصمیم گرفتند تا چگونگی ساخت برنامه های تحت وب را با استفاده از ترکیب سرویس های آمازون به نمایش بگذارند. به عنوان نمونه آن‌ها برنامه GrepTheWeb را توسعه دادند که به عنوان مثال

از سرویس SQS برای جداسازی مولفه های سیستم و کنترل‌کننده‌ها، پیاده سازی MapReduce بر روی خوشه ای از EC2ها و همچنین از S3 و SimpleDB برای ذخیره و بازیابی داده‌ها استفاده می‌نماید.

ترکیب رابط برنامه نویس کاربردی OpenSocial شرکت گوگل با سکوی توسعه ابرین این شرکت یعنی Google AppEngine نمونه دیگری از امکان ترکیب تکنولوژی محاسبات ابرین با سرویس های دیگر برای به دست آوردن نرم فزارهای قدرتمندتر می‌باشد. برنامه های کاربردی OpenSocial ای که از منابع خارجی بهره ای نمی‌برند در معرض محدودیت هایی چون فضای کم ذخیره سازی می‌باشند در حالیکه ترکیب این برنامه‌ها با AppEngine اجازه ترکیب لایه ارائه سمت مشتری را با داده های خارجی و منطق پیچیده تری از برنامه را خواهد داد.

۱۱-۵-۴- ترکیب سرویس هایی از چندین ابر

نمونه هایی که دیده شد از ترکیب سرویس های داخل یک ابر مانند آمازون یا گوگل به وجود آمده بوند. اما این پایان ماجرا نیست، نمونه های خوب دیگری نیز از ترکیب سرویس هایی از ابرهای مختلف نیز وجود دارد.

مانند مثالی که از ترکیب OpenSocial و AppEngine گفته شد، منتها اینبار با ترکیب برنامه های تحت Facebook و سرویس های آمازون یا جوینت (Joyent) می‌توان محدودیت های ذکر شده را از میان برداشت. نمونه موجود مهمی که می‌توان به آن اشاره نمود، ترکیب سرویس های Salesforce و AppEngine می‌باشد. در واقع شرکت Salesforce یک کتابخانه برای AppEngine ارائه نموده است که کاربران می‌توانند از طریق آن از داخل برنامه های نوشته شده خود در گوگل، سرویس های Salesforce را فراخوانی نمایند. از این طریق کاربران می‌توانند برنامه هایی در کلاس حرفه با منطق حرفه پیچیده را در برنامه های نوشته شده خود استفاده نمایند.

۱۱-۵-۵- نتیجه گیری

با بررسی روشها و چارچوب های ترکیب سرویس در فضای غیر ابرین، می‌توان مشاهده نمود که طی چندین سال گذشته دستاوردهای بسیاری در این حوزه حاصل شده است، اگرچه با حرکت به سمت استفاده از سرویس های ابرین، تعدادی از این دستاوردها از دست رفته و تا حدودی به مراحل اولیه کار باز گشته‌ایم. در واقع با بررسی های انجام شده در این تحقیق به این نتیجه رسیدیم که روش‌ها و ابزار های ترکیب سرویس موجود در فضای ابر دارای کاستی‌ها و مشکلاتی هستند از جمله اینکه بحث خودکار سازی عملیات ترکیب سرویس‌ها و یا پشتیبانی از انقیاد پویا در سرویس های مرکب نادیده گرفته شده‌اند به علاوه اینکه تعدادی نقایص دیگر نیز که از ماهیت فعلی ابرهای موجود ناشی می‌شوند نظر ما را به خود جلب نمودند. در ادامه لیستی از مشکلات روش‌ها و ابزارهای ترکیب سرویس موجود را به شکل خلاصه مشاهده می‌نمایید.

- تنها دارای آداپتور های پیش ساخته برای اتصال و یکپارچگی با سرویس های سازمانی معتبر و معروف هستند.
- اشتراک و استفاده مجدد از راه حل های توسعه داده شده توسط جامعه توسعه دهندگان را پشتیبانی نمی‌کنند.
- خودکار نیستند و عموماً به دانش فنی زیادی نیاز دارند.
- از انقیاد زودرس (ایستا) استفاده می‌کنند.
- استقرار سرویس ترکیبی به محیط توسعه محدود است و در محیط های دیگر نمی‌تواند مستقر گردد.

- استاندارد یا قراردادی در جهت یکسان سازی رابط های سرویس‌ها (به خصوص سرویس های پایه) وجود ندارد.

۱۱-۶- چالش های مطرح در حوزه محاسبات ابرین

۱۱-۶-۱- چالش های عمومی

در دنیای محاسبات ابرین گذشته از مزایا و فوایدی که در استفاده از این سبک محاسباتی وجود دارد با چالش های پیچیده ای نیز مواجه هستیم. در ادامه سعی شده است تا لیستی از مهمترین چالش‌ها که در این تحقیق شناسایی شدند ارائه شود. نکته قابل توجه این است که تعدادی از این موارد که در اینجا به عنوان چالش مطرح شده‌اند در بخشهای قبلی از آن‌ها به عنوان مزیت محاسبات ابرین یاد شده است و این نشان دهنده این است که آن مزیت هنوز به طور کامل اثبات نگردیده و مورد توافق همگان نمی‌باشد.

امنیت و حریم خصوصی

این بزرگترین مانع بر سر راه پذیرفته شدن این سبک محاسباتی به طور گسترده می‌باشد. اینکه کاربران و سازمان‌ها داده های خود را در محلی غیر از سازمان خود نگهداری و پردازش کنند برای عده زیادی پذیرفتنی نیست و نمی‌توان مطمئن بود که افراد غیر مجاز قادر به دسترسی به داده هایشان نیستند. تحقیقات زیادی در این حوزه انجام شده و مقالات متعددی نیز چه در جهت مهم جلوه دادن چالش و چه در جهت ارائه راه حل ارائه شده‌اند ولی همانطور که گفته شد هنوز راه حل مناسب و سطح قابل قبول و پذیرفته شده ای از امنیت به دست نیامده است و این چالش به موضوعی داغ در این حوزه بدل شده است.

دسترسی پذیری

به دست آوردن دسترسی پذیری بسیار بالا، پس از بحث امنیت از مهمترین مسائل باز این حوزه می‌باشد. در ادامه در بخش مربوط به خطر نهفته خواهیم دید که به دلیل وابستگی سیستم های مبتنی بر ابر به زیرساخت ابرین خود، در صورت بروز مشکل در یک زیرساخت، حجم وسیعی از سیستم های وابسته به آن از کار خواهند افتاد و این می‌تواند یک فاجعه باشد. در واقع زیرساخت ابر و سرویس های پایه که توسط تعداد بسیاری از مشتریان در حال استفاده می‌باشد، می‌بایست از دسترسی پذیری بسیار بالایی برخوردار باشند که در حال حاضر اینگونه نیست و هر چه سریعتر و قبل از بروز مشکلات فراوان می‌بایست به این موضوع رسیدگی نمود.

قابلیت تعامل و همکاری

این مورد در سیستم های بزرگ و بیشتر در بحث یکپارچه سازی سیستم‌ها و ترکیب سرویس‌ها مطرح است و یکی از بزرگترین موانع بر سر راه ترکیب سرویس‌ها برای دستیابی به ارزش افزوده می‌باشد. در واقع تا زمانیکه این تعامل پذیری میان سرویس های ابرهای مختلف به وجود نیامده کاربران مجبورند تنها از سرویس های یک ابر خاص بهره بگیرند و یا از آن‌ها مانند جزیره های دور افتاده از هم استفاده نمایند.

قابلیت اطمینان

اینکه داده های ذخیره شده در ابر تا چه میزان قابل اعتماد هستند چالش دیگری است که با آن روبرو هستیم. صحت، سازگاری و جامعیت داده‌ها می‌بایست تا سطح بالایی تضمین شود تا این سیستم‌ها قابل ارائه به حرفه های جدی و حساس باشند.

فقدان استاندارد

همانطور که در گذشته نیز مطرح شد تقریباً در هیچ یک از زیر شاخه های این بحث استانداردی توسعه داده نشده است. از تعریف خود محاسبات ابرین گرفته تا مدل های سرویس و رابط سرویس‌ها. بسیاری از مشکلات از جمله سطح پایین تعامل پذیری سرویس‌ها از همین کاستی نتیجه می‌شوند و این حوزه می‌بایست بیشتر مورد توجه سازمان های استانداردسازی قرار گیرد.

انعطاف پذیری پایین در سفارشی سازی

در حال حاضر سرویس های ارائه شده در ابر واقعاً از سطح بسیار پایین سفارشی سازی پشتیبانی می‌کنند. یعنی شما باید سرویسی را که در اختیار دارید همانطور که ارائه شده است مصرف نمایید حق هیچ دخل و تصرفی در آن ندارید.

۱۱-۶-۲- چالش های پیش رو

درست است که با ظهور محاسبات ابرین تعداد زیادی از مشکلات و مسائل قدیمی موجود رفع گردیدند با این حال ما را با مسائل جدیدی مواجه ساخته است. به عنوان مثال:

- اگر شما بدون داشتن برنامه و طرح از محاسبات ابرین استفاده نمایید، با خطر جدی روبرو خواهید بود. این دقیقاً شبیه استفاده از برق می‌باشد. اگر یک شرکت یا یک خانواده با تصور اینکه برق منبع نا محدودی است، سهل انگارانه به مصرف برق اقدام نماید علاوه بر هدر دادن انرژی، خود را در معرض ریسک خرابی و قطعی برق قرار داده است. بنابراین داشتن برنامه از پیش تعیین شده بسیار با اهمیت می‌باشد.
- به دلیل پایین بودن میزان سرمایه گذاری اولیه لازم برای تشکیل سیستم های مبتنی بر ابر، احتمالاً تعداد زیادی از پروژه‌ها به سرعت و با عجله توسعه داده می‌شوند که این عجله می‌تواند در آینده دردسر ساز شود مانند خانواده ای که تعداد زیادی بچه دارد ولی از عهده تربیت آن بر نخواهد آمد.

بنابراین همانطور که گفتیم باید بپذیریم اگرچه محاسبات ابرین پاسخ سوالات متعددی را داده است با این حال خود سوالات جدیدی را پیش روی ما قرار داده است. در حقیقت با انتخاب یا عدم انتخاب محاسبات ابرین به تعادلی بین سوالات قدیم و جدید خواهیم رسید.

خطر نهفته در محاسبات ابرین

چند سال پیش، در اسفندماه، سرویس S3 شرکت آمازون که قبلا معرفی گردید یک بار به مدت ۴ ساعت از کار افتاد. این مطلب باعث شد تا مردم دوباره به موضوع امنیت در ابر فکر کنند. از زمان ارائه سرویس S3 تا به حال تعداد زیادی از توسعه‌دهندگان وب ۲.۰ برای کاهش هزینه سخت‌افزار، سایت خود را بر روی مراکز داده ای آمازون قرار داده‌اند. ولی زمانی که بحث امنیت به میان می‌آید این توسعه دهندگان اطمینان خود را از دست داده و تا حدودی پشیمان می‌شوند. زمانی که کاربران از ابر استفاده می‌کنند در حقیقت به شخص دیگری این اجازه داده‌اند تا داده های آنان را ذخیره کند و این خطر از

دست رفتن تجارت و داده های خصوصی آن‌ها را به همراه خواهد داشت. هم اکنون محاسبات ابرین به طور کامل در میان مردم پذیرفته نشده است و محصولات و سرویس های ارائه شده در محاسبات ابرین قابل باور نیستند و هنوز به پایداری لازم نرسیده‌اند و این تنها یکی از ریسک های این حوزه می‌باشد.

در حقیقت همانطور که قبلاً هم بیان شد نگران کننده ترین سوال همان امنیت و حفظ حریم خواهد بود. طبق گزارشات تالار جهانی حفظ حریم شخصی داده های موجود در ابرها شامل: رکورد کاربران، داده های مالیاتی، داده های مالی، ایمیل‌ها، رکورد های سلامتی و پزشکی، مستندات و فایل های ارائه تجاری و غیره می‌باشند. عمومی ترین نرم‌افزار های تجاری تحت وب را سیستم های مدیریت مشتریان و حقوق و دستمزد تشکیل می‌دهند و از این رو با داده های حساس سر و کار دارند و از دست دادن این داده‌ها مشکلات فراوانی را به همراه خواهد داشت.

۱۱-۶-۳- مشکلات ابرهای موجود

در بررسی های انجام شده بر روی نمونه های موجود از سیستم های محاسبات ابرین خصوصیات مشترکی از آن‌ها به دست آمد که در واقع می‌توان از آن‌ها به عنوان ضعف اینگونه سیستم‌ها یاد نمود.

گره خوردن کاربران به یک سرویس دهنده خاص

اگرچه در حال حاضر هزینه های مربوط به زیرساخت و راه اندازی ابتدایی سیستم‌ها کاهش یافته‌اند و هزینه مربوط به سخت‌افزار و یا حتی مجوز های نرم‌افزاری تا حدود زیادی حذف شده‌اند، با این حال باید قبول کنیم تمام تلاش و هزینه ای که برای ساخت سیستم پرداخت شده، صرف توسعه سیستمی بر پایه یک سکوی خاص ابرین شده است و بنابراین مهاجرت به یک ابر دیگر به معنی دوباره سازی و توسعه مجدد آن نرم‌افزار خواهد بود. به عنوان مثال برنامه ای که بر روی Amazon EC2 استقرار یافته است به دلیل وابستگی به یک چارچوب ذخیره سازی خاص، به راحتی قابل جابجایی به سکویی دیگر نخواهد بود.

وابستگی شدید بین مولفه ها

این مطلب از طریق بیان یک مثال مشابه به خوبی قابل لمس می‌گردد. فرض کنید قصد خرید یک کامپیوتر شخصی را دارید. دو انتخاب پیش روی شماست؛ یکی خرید یک کامپیوتر شخصی آماده وابسته به یک مارک خاص به صورت یکجا و دیگری خرید قطعات مورد نیاز به صورت جداگانه و در نهایت سر هم بندی (اسمبل) سیستم. مزایایی که سر هم بندی نسبت به خرید آماده دارد عبارتند از: وجود گزینه های متعدد و گسترده تری از قطعات، انعطاف پذیری بیشتر در سفارشی سازی محصول و صد البته هزینه کمتر. حال اگر منابع محاسباتی را جایگزین قطعات کامپیوتری کنیم با شرایط دیگری روبرو خواهیم بود. در اینجا با حداقل انعطاف پذیری روبرو هستیم. بنابراین اگر مشتری قصد استفاده از مثلاً سرویس S3 از شرکت آمازون را داشته باشد در اکثر اوقات مجبور است از سایر تکنولوژی‌ها و سرویس های ارائه شده از همان شرکت مانند EC2 یا Elastic Map Reduce نیز استفاده نماید.

فقدان پشتیبانی از SLA

در ابتدا توضیحاتی راجع به SLA ارائه نموده و در مورد فقدان آن بیشتر بحث می‌کنیم.

تعریف توصیف SLA

به عنوان یک قرارداد بین مشتری و تأمین کننده سرویس، توصیف SLA در زبان توصیف، نیازمندی های QoS تأمین شده مشروط بر مشتری سرویس را توصیف می‌کند. یک SLA شامل یک مجموعه از SLO58 هاست که محدودیت‌ها را بر روی پارامترهای QoS اعمال می‌کند و در واقع ترکیبی از یک یا چند معیار سنجش کیفیت هستند. در مدیریت SLA، از توصیف یک SLA به منظور تطبیق محدودیت های QoS با سایر SLAها که QoS تأمین شده بوسیله تأمین کنندگان سرویس را توصیف می‌کند، استفاده می‌شود.

از آنجا که یک پارامتر QoS باید قابل سنجش باشد، توصیف SLA اجازه بیان کردن توصیف، برای محدودیت های QoS شان را به مشتریان می‌دهد، برای مشتریان سرویس محتمل‌تر است که علاقه به کیفیت محتوای ویژگی های QoS داشته باشند تا کمیت. مستندات نگاشت به منظور مربوط کردن توصیف کیفی با توصیف کمی برای دلال ترکیب استفاده می‌شود. مثال زیر مستند نگاشت برای پارامترهای QoS فراخوانی قابلیت در دسترس بودن را نشان می‌دهد.

```
<parameter mapping type="customer">
    <parameter name="AVAILABILITY">
        <qualityLevel type="high">100-95</qualityLevel>
        <qualityLevel type="middle">95-85</qualityLevel>
        <qualityLevel type="low">85-0</qualityLevel>
        <qualityLevel type="customize"></qualityLevel>
    </parameter>
</parameter mapping>
```

با این مستند نگاشت، مشتریان سرویس محدودیت QoS را با توصیف کیفی در SLOs بیان می‌کنند.

به عنوان مثال یک SLO از توصیف SLA را در نظر می‌گیریم که شامل دو پارامتر QoS می‌باشد:

- سرویس قابلیت در دسترس پذیری: این سرویس با توصیف کیفی توصیف می‌شود.
- سرویس زمان پاسخ: این سرویس با مقدار کمی تعریف می‌شود.

مستند SLO ای به طور مثال در زیر بیان شده است:

```
<slo_level name="qosConstraint">
    <parameter name="AVAILABILITY" qualityType="high">
    </parameter>
    <parameter name="RESPONSETIME" qualityType= "customize">
        <value>0-50</value>
    </parameter>
</slo_level>
```

توصیف SLA، قابلیت کشف سرویس های وب و تعامل QoS بین تقاضای کاربر و سرویس های وب را تأمین می‌کند. کاربر سرویس ترکیبی، می‌تواند چندین SLO را با ترتیبی از اولویت‌ها در یک درخواست سرویس اعمال کند طوری که SLO با اولویت کمتر در زمانی که سرویس وب، محدودیتی با اولویت بالای SLO را نقض کند، به کار می‌رود. سرویس ترکیبی می‌تواند از سرویس وب کنونی با یک SLA با اولویت کمتر هنگامی که نقض SLA بالا رخ دهد، استفاده می‌کند.

فقدان SLA در ابرهای موجود

در حال حاضر SLA یک مانع بزرگ بر سر راه گسترش محاسبات ابرین می‌باشد. سرویس های زیرساختی مانند EC2 آمازون هنوز قادر نیستند تا SLA مورد نیاز کمپانی هایی که قصد استفاده از محاسبات ابرین را در حرفه خود به صورت جدی

دارند را امضا کنند. به علاوه عموماً حرفه ماهیتی پویا دارد و قطعاً یک SLA ایستا قادر به پاسخگویی به تغییرات حرفه نخواهد بود در حالیکه این یکی از قول هایی است که راجع به محاسبات ابرین داده شده است.

فقدان پشتیبانی از چند- مستاجری (Multy Tenancy)

مفهوم چند- مستاجری به معنی پشتیبانی از چندین کلاینت به شکل همزمان از طریق یک نسخه از سیستم و با هدف افزایش بهره وری می‌باشد. برای بکارگیری این مفهوم سه روش وجود دارد: مجازی سازی، استفاده از میانجی و به اشتراک گذاری. در حال حاضر، ابرهای موجود به طور کامل از چند-مستاجری حمایت نمی‌کنند. بنابراین برای بهره گیری از تمامی پتانسیل چند-مستاجری می‌بایست به مسائل زیر پاسخ مناسبی داده شود.

- به اشتراک گذاری منابع: برای کاهش هزینه صرف شده برای سخت‌افزار، نرم‌افزار و مدیریت منابع به ازای هر مستاجر.
- جداسازی به دلایل امنیتی: برای پیشگیری از دسترسی غیر مجاز، تضادها و مداخلات میان مستاجرین مختلف.
- سفارشی سازی: برای پشتیبانی از رابط کاربری، فرآیندها، داده‌ها و غیره که مختص هر مستاجر باشد.

فقدان انعطاف پذیری لازم در واسط کاربری

رابط کاربری یکی از مهمترین قسمت های یک سیستم می‌باشد و تجربیات کاربر از کار با آن به عنوان یک فاکتور مهم ارزیابی سیستم تجاری مطرح می‌باشد. در این شرایط کاربران در حوزه محاسبات ابرین یا SaaS با محدودیت فراوانی در انتخاب رابط کاربری روبرو هستند.

۱۱-۶-۴- نتیجه گیری

در این فصل چالش‌ها و مشکلات محاسبات ابرین از دو جنبه مورد بررسی قرار گرفت. ابتدا چالش هایی عمومی که بعضاً از مفهوم محاسبات ابرین به عنوان یک سبک محاسباتی جدید ناشی شده‌اند ارائه گردید و سپس مشکلاتی که عموماً در سیستم های ابرین کنونی وجود دارند مورد بررسی قرار گرفت. در حالت کلی این مشکلات را نمی‌توان به مفهوم عمومی محاسبات ابرین نسبت داد بلکه می‌توان از آن‌ها به عنوان نقصان در سیستم های کنونی یاد نمود. آنچه از دید ما از اهمیت بیشتری برخوردار است نبود استاندارد و از آنجا کاهش تعامل پذیری ابرها می‌باشد که هم در نمونه های کنونی و هم به شکل عام مطرح می‌باشد.

منبع: امیررضا غفاری؛ "سیستم های محاسبات ابرین: نمونه‌ها، کاربردها، چالش ها"؛ دانشگاه شهید بهشتی؛ ۱۳۸۹

فصل ۱۲

خوشه‌بندی

(Clustering)

۱۲-۱- مقدمه

دانشمندان موفق شده‌اند با الهام گرفتن از یک روایت کهن، شیوه کارآمد و در عین حال ارزانی را برای دستیابی به توآن‌های محاسباتی بسیار بالا، تکمیل کنند. به نوشته ماهنامه علمی "ساینتیفیک آمریکن " این شیوه هم‌اکنون در بسیاری از مراکز علمی و آزمایشگاه‌های تحقیقاتی، مورد استفاده قرار گرفته است.

در افسانه‌های قدیمی آمده است که روزی گذار کهنه سربازی گرسنه و بی‌پول به دهی فقرزده افتاد و برای رفع گرسنگی ابتکاری به خرج داد. او به مردم دهکده گفت که می‌تواند با استفاده از یک دیگ بزرگ آب جوش و یک تکه سنگ آش خوشمزه‌ای بپزد. مردم ده ابتدا با ناباوری به او که دیگ را بار گزارده بود نگریستند، اما بعد هر یک برای آنکه سهمی از آش داشته باشند، با اهدا یک تکه کوچک گوشت یا یک دسته سبزی، یا یکی دو تا هویج، یا مشتی برنج، در کار پختن و تهیه آش مشارکت کردند. دست آخر درون دیگ آنقدر ماده خوردنی جای گرفته بود که محصول نهایی را به اندازه کافی خوشمزه و مغذی می‌کرد. به نوشته این ماهنامه، محققان آزمایشگاه ملی " اوک ریج " با استفاده از همین تمثیل ابر کامپیوتر تازه‌ای موسوم به " سنگ " را تکمیل کرده‌اند که متشکل از ۱۳۰ کامپیوتر معمولی است که به صورت کلاستری عمل می‌کنند. یکی از این ۱۳۰ دستگاه به عنوان ورودی کل سیستم عمل می‌کند که از یک سو با شبکه‌ها و سیستم‌های دیگر در تماس است و از سویی دیگر با بقیه اعضا شبکه خود ارتباط برقرار می‌کند. این شبکه مسائلی را که بدان محول می‌شود، با استفاده از شیوه محاسبه موازی و با تقسیم کار میان اعضاء شبکه به انجام می‌رساند.

یکی از بزرگترین طرح‌هایی که این ابر کامپیوتر مونتاژ شده از عهده آن برآمده، تهیه نقشه جامعی از ایالات متحده است که در آن کل مساحت امریکا به ۷/۸ میلیون قطعه، هر یک به مساحت یک کیلومتر مربع، تقسیم شده و ۲۵ مولفه آب و هوایی مختلف برای نقاط گوناگون آن در نظر گرفته شده و در مجموع ۱۰۰۰ ناحیه آب و هوایی متفاوت در آن منظور شده است.

هرچند اندیشه به هم پیوستن کامپیوترهای معمولی و یا قدیمی برای دستیابی به توان عملیاتی بالاتر، اندیشه تازه‌ای نیست و سابقه آن به دهه ۱۹۵۰ باز می‌گردد، اما تنها در چند سال اخیر است که ظهور نرم‌افزارهای جدید امکان بهره‌گیری کلاستری از کامپیوترهای دیجیتالی را فراهم آورده است. به عنوان نمونه، هم‌اکنون در موزه تاریخ طبیعی آمریکا، ۵۶۰ کامپیوتر پنتیوم ۳ موجود است که محققان با به هم پیوستن آن‌ها، ابر کامپیوتر قدرتمندی را بوجود آورده‌اند که از آن برای بررسی در نحوه تطور اختران و ستارگان بهره گرفته می‌شود.

نکته حائز اهمیت در رهیافت تازه آن است که می‌توان از کامپیوترهای موجود در اوقاتی که کاربران اصلی آن‌ها از آن‌ها استفاده نمی‌کنند، بهره گرفت. به عنوان مثال، پروژه " ستی " که به وسیله دانشگاه کالیفرنیا و برای بررسی امکان وجود موجودات هوشمند در کیهان در حال اجراست، فعالیت خود را از طریق اینترنت و به کمک ۳ میلیون کامپیوتر شخصی متعلق به شهروندان، و در ساعات آخر شب که کامپیوترها مورد استفاده صاحبان آن‌ها نیستند، دنبال می‌کند.



شکل شماره ۱: تهیه نقشه جامع از آب و هوای ایالات متحده آمریکا با استفاده از ایجاد کلاستر

۱۲-۱-۱- توصیف

بیشتر اوقات برنامه‌های کاربردی به توان محاسباتی بالاتری نسبت به آنچه که یک کامپیوتر ترتیبی می‌تواند ارائه دهد، نیاز دارند. یکی از راه‌های غلبه بر این محدودیت بهبود بخشیدن سرعت عملیاتی پردازنده‌ها و سایر اجزا می‌باشد، بطوریکه آن‌ها بتوانند توان مورد نیاز برنامه‌های کاربردی که دارای محاسبات وسیع و گسترده هستند را فراهم نمایند. اگر چه در سال‌های اخیر این امکان تا اندازه‌ای مهیا شده است، لیکن سرعت نور، قوانین ترمودینامیک و هزینه‌های سنگین ساخت پردازنده موانعی

در جهت پیشرفت‌های آتی ایجاد کرده‌اند. یکی از راه‌حل‌های موثر و کم‌هزینه اتصال چندین پردازنده به یکدیگر و هماهنگ نمودن عملیات و توان محاسباتی آن‌ها می‌باشد. سیستم‌های بوجود آمده تحت عنوان " کامپیوترهای موازی " شهرت دارند و اجازه تقسیم یک کار محاسباتی بین چند پردازشگر را می‌دهند.

همانگونه که فیستر اشاره می‌کند، جهت بهبود عملکرد یک سیستم سه راه وجود دارد:

- کار و تلاش بیشتر
- کارکرد موثر و کارآمد
- کمک گرفتن

در اصطلاح تکنولوژی‌های محاسباتی، کار و تلاش بیشتر به مثابه استفاده از سخت‌افزار سریعتر (پردازنده‌ها و دستگاه‌های جانبی با کارآیی و سرعت بالا) می‌باشد. کارکرد موثر و کارآمد به مثابه انجام کارها بصورت کارا بوده و در رابطه با الگوریتم‌ها و تکنیک‌هایی که جهت حل مسائل و کارهای محاسباتی استفاده می‌شوند، صحبت به عمل می‌آورد. و در نهایت کمک گرفتن به بکارگیری چندین کامپیوتر جهت حل یک مسئله خاص اشاره دارد.

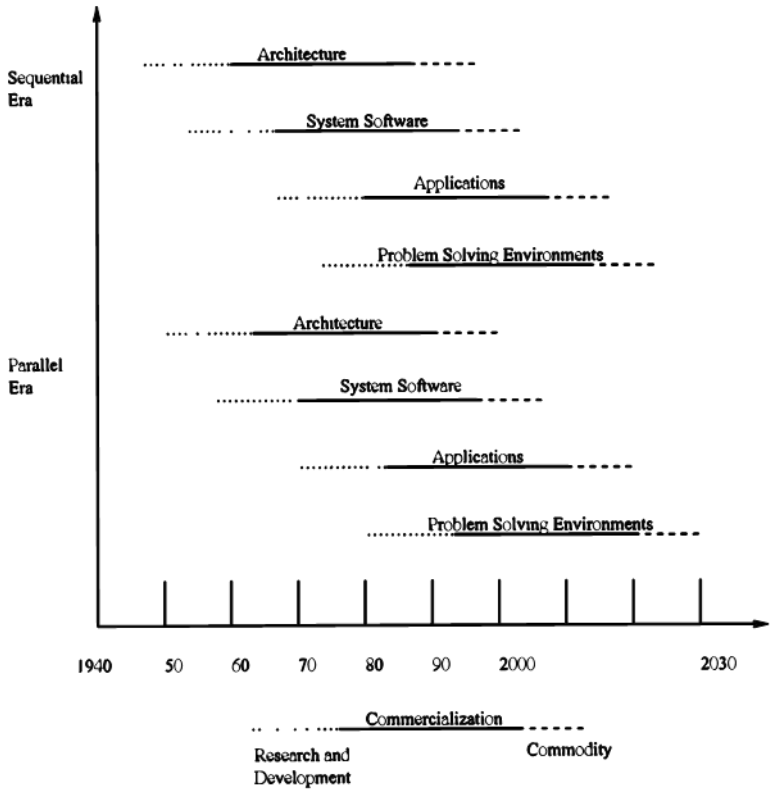
۱۲-۲- دوره‌های محاسبات

صنعت محاسبه یکی از صنایعی است که سریعترین رشد را داشته و از دستاوردهای فنی پرشتاب در حوزه‌های سخت‌افزار و نرم‌افزار بهره جسته است. پیشرفت‌های تکنولوژی در عرصه سخت‌افزار، رشد و توسعه تراشه‌ها، فن‌آوری‌های ساخت تراشه، ریزپردازنده‌های سریع و ارزان و همچنین پهنای باند بالا و شبکه‌های ارتباطی با تاخیر کم می‌باشند. در بین این موارد پیشرفت‌های اخیر در فن‌آوری VLSI (تجمع در مقیاس بسیار وسیع) نقش مهمی در رشد کامپیوترهای ترتیبی و موازی ایفا کرده است. فن‌آوری نرم‌افزار نیز به سرعت در حال رشد می‌باشد. نرم‌افزارهای پیشرفته‌ای چون سیستم‌عامل‌ها، زبان‌های برنامه‌نویسی، متدهای توسعه و ابزارها، همگی در دسترس می‌باشند. اینها باعث رشد و ساماندهی برنامه‌های کاربردی در جهت خدمت به نیازهای علمی، مهندسی و تجاری شده‌اند. همچنین باید خاطر نشان کرد که برنامه‌های بزرگ و قدرتمند نظیر پیش‌بینی وضع هوا و تحلیل و بررسی زلزله، عامل اصلی رشد و توسعه کامپیوترهای موازی قدرتمند بوده‌اند.

یکی از راه‌های مشاهده محاسبه تقسیم آن به دو عصر می‌باشد:

- عصر محاسبه ترتیبی
- عصر محاسبه موازی

شکل شماره ۲ تغییراتی که در عصرهای محاسبات بوجود آمده است را نشان می‌دهد. هر عصر محاسبه با یک توسعه در معماری‌های سخت‌افزاری و به دنبال آن نرم‌افزار سیستم (به ویژه در حوزه کامپایلرها و سیستم‌عامل‌ها) و برنامه‌های کاربردی شروع شده و در نهایت با رشد در PSEها (محیط‌های حل مسئله) به اوج خود رسیده است. هر جزء از سیستم محاسباتی دارای سه فاز R&D (تحقیق و توسعه)، تجاری‌سازی و تولید جنس می‌باشد. فن‌آوری که در ورای توسعه اجزای سیستم محاسبه در عصر ترتیبی وجود دارد به تکامل رسیده است و رشدهای مشابه‌ای هنوز باید در عصر موازی رخ دهند. یعنی، فن‌آوری محاسبه موازی هنوز جای رشد و توسعه دارد، زیرا به اندازه کافی پیشرفت نکرده است تا به عنوان یک تکنولوژی تولید کالا مطرح شود.



شکل شماره ۲: دو عصر محاسبات

دلیل اصلی ایجاد و استفاده کامپیوترهای موازی غلبه بر تنگنای سرعت کم پردازشگر واحد با استفاده از موازی‌سازی می‌باشد. علاوه بر این، نسبت بها / عملکرد یک کامپیوتر موازی کوچک بر مبنای کلاستر در مقایسه با یک مینی کامپیوتر، بسیار کوچکتر و در نتیجه از بهای مناسب‌تری برخوردار خواهد بود. خلاصه اینکه، توسعه و تولید سیستم‌هایی که سرعت متوسطی داشته و از معماری‌های موازی استفاده می‌کنند بسیار ارزانتر از ایجاد عملکرد معادل در یک سیستم ترتیبی می‌باشد.

در بخش‌های باقیمانده، گزینه‌های معماری برای ساختن کامپیوترهای موازی، محرک‌های تغییر در جهت محاسبه موازی کم‌هزینه، مدل کلی یک کامپیوتر کلاستر شده، اجزای بکار گرفته شده در ساخت کلاستر، میان‌افزار کلاستر، مدیریت و برنامه‌ریزی منابع، ابزارها و محیط‌های برنامه‌نویسی و سیستم‌های نماینده کلاستر مورد بحث قرار خواهند گرفت. در نهایت تکنولوژی‌هایی که در آینده در رابطه با کلاستر وجود خواهند داشت نیز توضیح داده می‌شوند.

۱۲-۳- معماری‌های مقیاس‌پذیر کامپیوتر موازی

در طول دهه‌های گذشته، سیستم‌های کامپیوتری بسیار متفاوتی که از عملکرد محاسباتی بالایی برخوردار بوده‌اند، پدیدار گشته‌اند. طبقه‌بندی آن‌ها بر مبنای چگونگی پردازنده‌ها، حافظه و اتصالات درونی بوده است. رایج‌ترین سیستم‌ها عبارتند از:

- پردازنده‌های موازی گسترده (MPP)
- چندپردازنده‌های متقارن (SMP)
- دسترسی به حافظه غیر همشکل و یکسان بودن کاشه (CC-NUMA)
- سیستم‌های توزیعی
- کلاسترها (Clusters)

جدول شماره ۱ مقایسه ویژگی‌های معماری و عملیاتی ماشین‌های بالا را نشان می‌دهد.

MPP معمولاً یک سیستم پردازش موازی بزرگ است که در معماری آن منبع مشترک وجود ندارد. این سیستم شامل چند صد واحد پردازش (گره) می‌باشد که از طریق یک شبکه یا سوییچ ارتباطی با سرعت بالا به یکدیگر متصل شده‌اند. هر گره (Node) می‌تواند تنوعی از اجزاء سخت‌افزاری داشته باشد، اما عموماً شامل یک یا چند پردازنده و یک حافظه اصلی است. بعلاوه، گره‌های ویژه می‌توانند وسایل جانبی نظیر دیسک‌ها و یا سیستم‌های پشتیبان داشته باشند. هر گره یک نسخه جداگانه از سیستم‌عامل را اجرا می‌کند.

Characteristic	MPP	SMP CC-NUMA	Cluster	Distributed
Number of Nodes	O(100)-O(1000)	O(10) – O(100)	O(100) or less	O(10)-O(1000)
Node Complexity	Fine grain or medium	Medium or coarse grain	Medium Grain	Wide Range
Internode Communication	Message passing shared variables for distributed shared memory	Centralized and Distributed Shared Memory (DSM)	Message Passing	Shared files , RPC , Message Passing and IPC
Job Scheduling	Single run queue on host	Single run queue mostly	Multiple queue but coordinated	Independent queues
SSI Support	Partially	Always in SMP and some for NUMA	Desired	No
Node OS copies and type	N micro-kernels monolithic or layered OSs	One monolithic SMP and many for NUMA	N OS platforms-homogeneous or micro-kernel	N OS platforms homogeneous
Address Space	Multiple – single for DSM	Single	Multiple or single	Multiple
Internode Security	Unnecessary	Unnecessary	Required if exposed	Required
Ownership	One organization	One organization	One or more organizations	Many organizations

جدول شماره ۱: خصوصیات اصلی کامپیوترهای موازی مقیاس‌پذیر

امروزه سیستم‌های SMP دارای ۲ الی ٦٤ پردازنده بوده و دارای معماری کاملاً اشتراکی می‌باشند. در این سیستم‌ها کلیه پردازنده‌ها از تمامی منابع موجود (bus، حافظه، سیستم ورودی / خروجی) به صورت اشتراکی استفاده می‌کنند. یک نسخه واحد از سیستم‌عامل بر روی این سیستم‌ها اجرا می‌شود.

CC-NUMA یک سیستم چندپردازنده‌ای مقیاس‌پذیر می‌باشد که دارای معماری دسترسی به حافظه غیرهمشکل بوده و کاشه در این سیستم coherent می‌باشد. دقیقاً همانند معماری SMP، هر پردازنده به تمامی حافظه اشراف کامل خواهد داشت. این نوع سیستم نام (NUMA) را به خاطر تعداد دفعات دسترسی غیر همشکل به نزدیک‌ترین و دورترین بخش‌های حافظه، به خود گرفته است.

سیستم‌های توزیع شده را می‌توان شبکه‌های قراردادی از کامپیوترهای مستقل در نظر گرفت که دارای image سیستم‌های مختلف می‌باشند و هر گره سیستم‌عامل خود را اجرا می‌کند. ماشین‌های مستقل در یک سیستم توزیعی به عنوان مثال می‌توانند ترکیبی از MPPها، SMPها، کلاسترها و کامپیوترهای شخصی باشند.

در ابتدایی‌ترین سطح، یک کلاستر مجموعه‌ای از ایستگاه‌های کاری یا کامپیوترهای شخصی است که با استفاده از یک نوع تکنولوژی شبکه به یکدیگر متصل شده‌اند. عموماً یک کلاستر، جهت اهداف پردازش موازی باید از ایستگاه‌های کاری و یا کامپیوترهای شخصی با سرعت و عملکرد بالا که بوسیله یک شبکه سریع به یکدیگر متصل شده‌اند تشکیل شده باشد. یک کلاستر به عنوان مجموعه یکپارچه‌ای از منابع عمل کرده و می‌تواند دارای یک Image واحد از سیستم باشد که کل گره‌ها را پوشش می‌دهد.

۱۲-٤- به سوی محاسبات موازی کم‌هزینه و انگیزه‌ها

در دهه ۱۹۸۰ باور بر این بود که کارآیی کامپیوتر با بوجود آوردن پردازنده‌های سریعتر و موثرتر به بهترین نحو بهبود خواهد یافت. این نظریه با نظریه پردازش موازی که به معنای متصل نمودن دو یا چند کامپیوتر جهت حل یک مسئله محاسباتی است، در رقابت بود. از اوایل دهه ۱۹۹۰ رویه روزافزونی در خصوص دوری از ابرکامپیوترهای موازی تخصصی و گران‌قیمت و حرکت به سمت شبکه‌های ایستگاه‌های کاری به وجود آمده است. در بین محرک‌های اصلی که اجازه چنین تفکری را داده‌اند، رشد سریع قابلیت دسترسی اجزاء با کارآیی بالا جهت ایستگاه‌های کاری و شبکه‌ها مهمترین عامل بوده است. این فن‌آوری‌ها شبکه‌های کامپیوتری (کامپیوترهای شخصی و یا ایستگاه‌های کاری) را به ابزاری مناسب جهت پردازش موازی تبدیل کرده‌اند و این امر در نهایت منجر به پایین آمدن هزینه تولید سیستم‌های ابرمحاسبه‌ای شده است.

تحقیقات وسیعی در ارتباط با کاربرد پردازش موازی به عنوان ابزاری جهت ارائه امکانات محاسبه‌ای با کارآیی بالا برای برنامه‌های کاربردی بزرگ و وسیع، صورت گرفته است. با این وجود تا این اواخر، منافع این تحقیقات به اشخاصی محدود می‌شد که به این نوع سیستم‌ها دسترسی داشتند. رویه محاسبه موازی، حرکت از سوی سکوهای ابرمحاسبه‌ای سنتی ویژه مانند Cray/SGI T3E، به سوی سیستم‌های ارزانتر چند منظوره می‌باشد که شامل اجزایی هستند که loosely coupled بوده و از کامپیوترهای شخصی یا ایستگاه‌های کاری ساخته شده‌اند که دارای یک یا چند پردازنده‌اند. این دیدگاه دارای چندین مزیت است، از جمله توانایی ساخت سکویی جهت یک بودجه فرضی که برای گروه کثیری از برنامه‌های کاربردی و بارهای کاری مناسب می‌باشد.

استفاده از کلاسترها جهت نمونه‌سازی اولیه، رفع خطا و اجرای برنامه‌های کاربردی موازی به جای سکوهای (Platforms) محاسبه موازی تخصصی و گران‌قیمت، بطور روزافزونی عمومیت یافته است. یکی از عوامل مهم که استفاده از کلاسترها را به یک قضیه عملی تبدیل کرده است، استاندارد کردن بسیاری از ابزارها و برنامه‌های سودمندی است که بوسیله برنامه‌های کاربردی موازی استفاده می‌شوند. نمونه این استانداردها کتابخانه انتقال پیام (MPI) و زبان موازی داده‌ای (HPF) می‌باشند. در این زمینه، استاندارد کردن این امکان را به برنامه‌های کاربردی می‌دهد که توسعه یافته، مورد آزمایش قرار گیرند و حتی بر روی شبکه‌ای از ایستگاه‌های کاری اجرا شوند. سپس در مرحله بعدی با تغییرات اندکی به سمت سکوهای موازی اختصاصی، جایی که زمان CPU ثبت و محاسبه می‌شود، منتقل شوند.

دلایلی که در ذیل آورده شده است نشان می‌دهند که چرا شبکه‌ای از ایستگاه‌های کاری به کامپیوترهای موازی مخصوص ترجیح داده می‌شوند:

- ایستگاه‌های کاری شخصی روز به روز قدرتمندتر می‌شوند. در واقع، کارآیی ایستگاه کاری در چند سال اخیر به مقدار زیادی افزایش پیدا کرده است و در هر ۱۸ تا ۲٤ ماه دو برابر می‌شود. این رشد برای سالهای متمادی ادامه خواهد یافت زیرا پردازنده‌های سریعتر و ماشین‌های چندپردازنده‌ای موثرتر به بازار خواهند آمد.
- بدلیل تکنولوژی‌های جدید شبکه و همچنین پروتکل‌هایی جدید که در یک شبکه محلی پیاده‌سازی می‌شوند، پهنای باند ارتباطی مابین ایستگاه‌های کاری در حال افزایش و تاخیر در حال کاهش می‌باشد.
- کلاسترهای ایستگاه‌های کاری جهت عمل یکپارچه‌سازی نسبت به کامپیوترهای موازی خاص ساده‌تر می‌باشند.
- ایستگاه‌های کاری عموماً توسط کاربرانشان کمتر به کار گرفته می‌شوند.
- ابزارهای توسعه برای ایستگاه‌های کاری در مقایسه با راه‌حل‌های اختصاصی جهت کامپیوترهای موازی کامل‌تر می‌باشند. این به جهت طبیعت غیر استاندارد اکثر سیستم‌های موازی است.
- کلاسترها به راحتی قابل رشد بوده و توانایی هر گره به راحتی با افزودن حافظه و یا نصب کردن پردازنده‌های اضافی قابل افزایش است.
- کلاسترهای ایستگاه‌های کاری ارزان بوده و به راحتی جهت سکوهای محاسباتی با توان بالا در دسترس می‌باشند.

از آنجایی که یک شبکه محلی عموماً دارای پهنای باند کم بوده و در شروع کار تاخیر پیام زیادی دارد، بنابراین محیط ایستگاه کاری جهت برنامه‌های کاربردی که نیاز به ارتباط زیاد ندارند مناسب‌تر می‌باشد. اگر برنامه کاربردی نیاز به قدرت ارتباط سریعتر داشته باشد، معماری‌های شبکه‌های محلی موجود مانند اترنت جوابگوی آن نخواهند بود.

در گذشته، در علوم و صنایع، ایستگاه کاری به یک سکوی UNIX گفته می‌شد و عملیات عمده ماشین‌هایی که تحت کامپیوترهای شخصی بنا شده بودند، جهت کارهای اجرایی و پردازش متن مورد استفاده قرار می‌گرفتند. با این وجود همگرایی سریعی در کارآیی پردازنده‌ها و عملیات در سطح kernel ایستگاه‌های کاری و کامپیوترهای خانگی در سه سال اخیر صورت پذیرفته است (معرفی ماشین‌های سریعی که پردازنده آن‌ها Pentium می‌باشد و سیستم‌عامل‌های Linux و Windows NT گواهی بر این ادعا می‌باشد). این همگرایی باعث شده است تا استفاده از سیستمهای PC-based به عنوان یک منبع محاسباتی کم هزینه جهت محاسبات موازی مورد استفاده قرار گیرد. این عامل بعلاوه هزینه نسبتاً پایین PCها و گستردگی آن‌ها از لحاظ قابلیت دسترسی در صنعت و علوم باعث شده است تا ایجاد تعدادی پروژه نرم‌افزاری که هدف اصلی آن‌ها کنترل کردن این منابع بصورت اشتراکی است، شروع شود.

۱۲-۵- دریچه‌ای به سوی فرصت‌ها

منابع موجود در شبکه‌ای میانه از ایستگاه‌های کاری نظیر پردازنده‌ها، رابط‌های شبکه، حافظه و دیسک سخت، فرصت‌های تحقیقاتی زیادی را بوجود می‌آورند. بطور مثال:

- **پردازش موازی:** از پردازنده‌های گوناگون جهت ایجاد سیستم‌هایی مشابه MPP/DSM که برای محاسبات موازی مورد استفاده قرار می‌گیرند، سود می‌جوید.

- **حافظه شبکه:** از حافظه موجود در هر یک از ایستگاه‌های کاری می‌توان به عنوان یک کاشه DRAM به هم پیوسته استفاده نمود. این موضوع می‌تواند بطور قابل ملاحظه‌ای حافظه مجازی و کارآیی سیستم فایل را بهبود ببخشد.

- ***RAID* نرم‌افزاری (آرایه‌ای از دیسک‌های کم‌هزینه):** با استفاده از آرایه دیسک‌های ایستگاه‌های کاری می‌توان فضای ذخیره‌سازی مقیاس‌پذیر با قابلیت دسترسی بالا و ارزان‌قیمت را ایجاد نمود. این کار با استفاده از شبکه محلی به عنوان زیرساختار ورودی/خروجی برای آرایه‌ای از دیسک‌های ایستگاه‌های کاری میسر می‌باشد. بعلاوه می‌توان جهت برنامه‌های کاربردی نظیر MPI-IO که در لایه میان‌افزار قرار داند از ورودی / خروجی موازی نیز پشتیبانی به عمل آورد.
- **ارتباطات چندمسیره:** با استفاده از چندین شبکه می‌توان انتقال اطلاعات بین گره‌ها را بصورت موازی انجام داد.

برنامه‌های کاربردی موازی و مقیاس‌پذیر نیاز به عملیات ممیز شناور با کارآیی بالا، ارتباطات با تاخیر کم و پهنای باند زیاد، پهنای باند قابل انعطاف و دسترسی سریع به فایل‌ها خواهند داشت. نرم‌افزار کلاستر می‌تواند این نیازمندی‌ها را با استفاده از منابعی که جهت هر کلاستر وجود دارند، مهیا کند. می‌توان سیستم فایلی که از ورودی و خروجی موازی پشتیبانی به عمل می‌آورد را با استفاده از دیسک‌هایی که جهت هر ایستگاه کاری وجود دارد بجای استفاده از RAID سخت‌افزاری گران‌قیمت، بوجود آورد. می‌توان کارآیی حافظه مجازی را با استفاده از حافظه شبکه به عنوان یک فضای ذخیره‌سازی جبرانی بجای دیسک سخت، بطور موثری بهبود بخشید. سیستم‌های فایل موازی و حافظه شبکه به نوعی شکاف بزرگ کارآیی مابین پردازنده‌ها و دیسک‌ها را کوچکتر کرده و تقلیل می‌دهند.

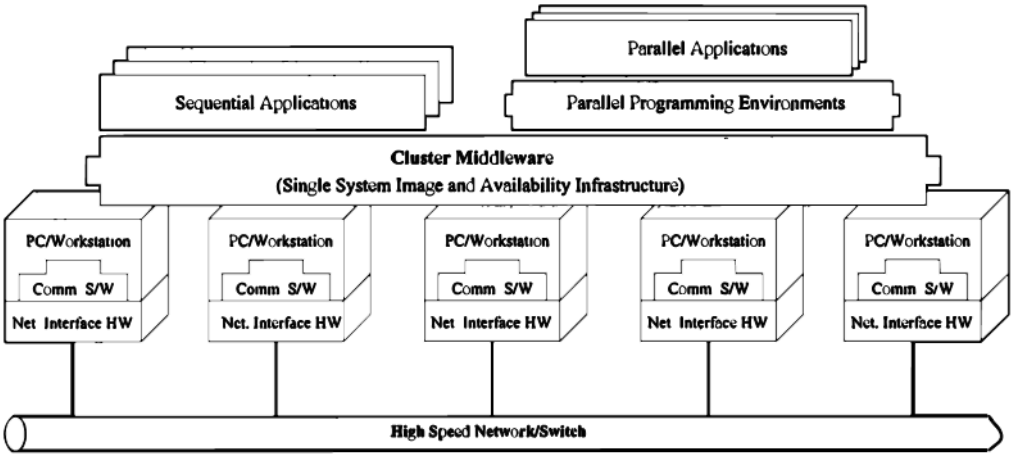
متصل نمودن گره‌های موجود در یک کلاستر با استفاده از شبکه اترنت استاندارد و یا شبکه‌های مخصوص با کارآیی بالا نظیر Myrinet امری متداول می‌باشد. این چند شبکه می‌توانند جهت انتقال اطلاعات بین گره‌های موجود در کلاستر بصورت موازی مورد استفاده قرار گیرند. نرم‌افزار ارتباط چندمسیره در گره‌ای فرستنده اطلاعات عمل مالتی‌پلکسینگ داده‌ها را انجام داده و سپس آن را از طریق شبکه‌های چندگانه ارسال می‌کند، سپس در گره مقصد و یا گیرنده نیز عمل دی‌مالتی‌پلکسینگ داده‌ها را انجام می‌دهد. به همین دلیل تمامی شبکه‌های موجود می‌توانند جهت انتقال اطلاعات سریع مابین گره‌های یک کلاستر مورد استفاده قرار گیرند.

۱۲-٦- کامپیوتر کلاستر و معماری آن

یک کلاستر گونه‌ای از سیستم پردازش موازی و یا توزیعی است که شامل مجموعه‌ای از کامپیوترهای مستقل متصل به هم می‌باشد که این کامپیوترها به عنوان یک منبع محاسباتی یکپارچه و واحد با یکدیگر کار می‌کنند.

یک گره کامپیوتر می‌تواند دارای سیستم تک‌پردازنده‌ای و یا چندپردازنده‌ای (کامپیوترهای شخصی، ایستگاه‌های کاری و یا SMP ها) باشد که دارای حافظه، امکانات ورودی / خروجی و سیستم عامل می‌باشند. عموماً کلمه کلاستر به دو یا چند

کامپیوتر (گره) که به یکدیگر متصل هستند اطلاق می‌شود. گره‌ها می‌توانند در یک قفسه واحد بوده و یا بصورت فیزیکی از یکدیگر مجزا بوده و از طریق شبکه محلی به یکدیگر متصل باشند. یک کلاستر از کامپیوترها که ارتباطات آن بر اساس شبکه محلی باشد می‌تواند به عنوان یک سیستم واحد برای کاربران و برنامه‌های کاربردی در نظر گرفته شود. چنین سیستمی می‌تواند یک راه‌حل کم‌هزینه جهت خصوصیات و فوایدی (خدمات سریع و قابل اطمینان) تنها در سیستم‌های اشتراک حافظه گران‌قیمت و خصوصی یافت می‌شدند، ارائه دهد. معماری نمونه یک کلاستر در شکل شماره ۳ نشان داده شده است.



شکل شماره ۳: معماری کامپیوتر کلاستر

تعدادی از عناصر مهم در کامپیوترهای کلاستر شده به قرار زیر می‌باشند:

- کامپیوترهای با کارآیی و قدرت بالا (کامپیوترهای شخصی، ایستگاه‌های کاری و یا SMP ها)
- سیستم‌عامل‌های موثر (بصورت لایه‌ای و یا ریزهسته (Microkernel))
- شبکه‌ها و یا سوییچ‌های پر سرعت (نظیر Myrinet و یا Gigabit Ethernet)
- کارت‌های شبکه (NIC)
- پروتکل‌های ارتباط سریع و سرویس‌ها (نظیر پیام‌های سریع و فعال (AFM))
- میان‌افزار کلاستر (تصویر سیستم واحد (SSI) و زیرساختار قابلیت دسترسی سیستم)
  - ✓ سخت‌افزار (نظیر کانال حافظه شرکت دیجیتال (DEC)، سخت‌افزار DSM و تکنیک‌های SMP)
  - ✓ هسته سیستم عامل و یا لایه Gluing (نظیر Solaris MC و GLUnix)
  - ✓ برنامه‌های کاربردی و زیرسیستم‌ها
    - برنامه‌های کاربردی (نظیر ابزارهای مدیریت سیستم و فرم‌های الکترونیکی)
    - سیستم‌های Runtime (نظیر DSM نرم‌افزاری و سیستم فایل موازی)
    - نرم‌افزار مدیریت منابع و زمان‌بندی (نظیر LSF (امکان تقسیم بار) و CODINE (محاسبه در محیط‌های شبکه‌ای توزیعی)
- ابزارها و محیط‌های برنامه‌نویسی موازی (نظیر کامپایلرها، PVM (ماشین مجازی موازی) و MPI (رابط انتقال پیام))
- برنامه‌های کاربردی

- ✓ ترتیبی
- ✓ موازی و یا توزیعی

سخت‌افزار رابط شبکه به عنوان پردازنده ارتباطی عمل نموده و وظیفه ارسال و دریافت پاکت‌های داده مابین گره‌های کلاستر از طریق سوئیچ و یا شبکه را به عهده دارد.

نرم‌افزار ارتباط، انتقال اطلاعات سریع و قابل اطمینان بین گره‌های موجود در کلاستر و همچنین دنیای خارج را مهیا می‌کند. اغلب کلاسترهایی که از شبکه‌ها و یا سوئیچ‌های مخصوص نظیر Myrinet بهره می‌گیرند، برای داشتن ارتباط سریع بین گره‌هایشان از پروتکل‌های ارتباطی نظیر پیام‌های فعال (Active Messages) استفاده می‌کنند. آن‌ها بصورت بالقوه مرحله سیستم‌عامل را نادیده گرفته و با این روش سربارهای ارتباطی بحرانی را از بین می‌برند و به همین دلیل قادر به دسترسی در سطح کاربر و بصورت مستقیم با رابط شبکه می‌باشند. گره‌های موجود در کلاستر می‌توانند بصورت گروهی و به عنوان یک منبع محاسباتی یکپارچه عمل کنند و همچنین می‌توانند بصورت کامپیوترهای مستقل نیز کار خود را انجام دهند. میان افزار کلاستر وظیفه ایجاد تصور تصویر سیستم یکتا (SSI) و قابلیت دسترسی از طریق یک مجموعه کامپیوترهای مستقل ولی متصل به هم را دارد.

محیط‌های برنامه‌نویسی ابزارهای موثر و قابل انتقال که کار کردن با آن‌ها ساده می‌باشد را جهت توسعه برنامه‌های کاربردی در اختیار می‌گذارند. آن‌ها شامل کتابخانه‌های انتقال پیام، اشکال‌زداها و Profilerها می‌باشند. نباید فراموش شود که کلاسترها می‌توانند جهت برنامه‌های کاربردی موازی و همچنین ترتیبی بکار گرفته شوند.

۱۲-۷- طبقه‌بندی کلاسترها

کلاسترها مشخصه‌های ذیل را با هزینه نسبتاً پایین ارائه می‌دهند:

- عملکرد بالا
- توسعه‌پذیری و میزان‌پذیری
- قابلیت دسترسی بالا
- توان عملیاتی (Throughput) بالا

تکنولوژی کلاستر به سازمان‌ها امکان تقویت قدرت پردازش خود را با بکارگیری فن‌آوری استاندارد (اجزاء سخت‌افزاری و نرم‌افزاری مناسب) که می‌توان با هزینه نسبتاً پایین خرید و یا بدست آورد، را می‌دهد. این ممکن توسعه‌پذیری را – یک مسیر ارتقاء که به سازمان‌ها اجازه می‌دهد تا توان محاسباتی خود را افزایش دهند – با حفظ سرمایه‌های موجود و بدون متحمل شدن هزینه‌های اضافی میسر می‌سازد. عملکرد برنامه‌های کاربردی نیز با حمایت محیط نرم‌افزاری مقیاس‌پذیر بهبود می‌یابد. مزیت دیگر کلاستر کردن توانایی غلبه بر خطاها و خرابی‌ها می‌باشد که این امکان را فراهم می‌کند تا یک کامپیوتر پشتیبان وظایف کامپیوتری که در کلاستر قرار دارد و دچار نقص شده است را به عهده گیرد.

کلاسترها بر مبنای عوامل زیادی که در زیر به آن‌ها اشاره شده است قابل طبقه‌بندی می‌باشند.

۱- **از لحاظ برنامه کاربردی:** علوم محاسبه‌ای و یا برنامه‌های کاربردی که دارای وظیفه مهم می‌باشند.

- کلاسترهایی با عملکرد بالا (HP Clusters)

- کلاسترهایی با قابلیت دسترسی بالا (HA Clusters)

تمرکز اصلی ما بر روی کلاسترهایی با عملکرد بالا و تکنولوژی‌ها و محیط‌های لازم جهت بکارگیری آن‌ها در محاسبات موازی خواهد بود.

۲- **مالکیت گره:** به صورت مالکیت شخصی و یا به عنوان یکی از گره‌های کلاستر.

- کلاسترهای اختصاصی
- کلاسترهای غیر اختصاصی

تمایز این دو مبتنی بر مالکیت گره‌ها در یک کلاستر می‌باشد. در نوع کلاسترهای اختصاصی یک شخص مشخص مالک یک ایستگاه کاری نمی‌باشد؛ منابع به اشتراک گذاشته می‌شوند بطوریکه محاسبه موازی در یک کلاستر می‌تواند صورت گیرد. نوع دیگر کلاستر غیر اختصاصی زمانی است که ایستگاه‌های کاری در تملک افراد بوده و برنامه‌های کاربردی با ربودن سیکل‌های بدون استفاده پردازنده اجرا می‌شوند. انگیزه این سناریو بر این حقیقت استوار است که اکثر سیکل‌های پردازنده‌های ایستگاه‌های کاری حتی در طول اوج ساعات کاری مورد استفاده قرار نمی‌گیرند. محاسبه موازی در مجموعه ایستگاه‌های غیر اختصاصی که بطور پویا تغییر می‌کنند، محاسبه موازی تطبیقی نامیده می‌شود.

در کلاسترهای غیر اختصاصی رقابتی بین صاحبان ایستگاه‌های کاری و کاربران دوری که جهت اجرا شدن برنامه‌های کاربردی خود به ایستگاه‌های کاری نیاز دارند، وجود دارد. اولی انتظار پاسخ متقابل سریع را از ایستگاه کاری خود دارد، در حالیکه دومی نگران برگشت سریع برنامه کاربردی با استفاده از سیکل‌های آزاد پردازنده می‌باشد. تقسیم منابع پردازشی مفهوم مالکیت گره را کم‌رنگ کرده و نیازمندی‌های پیچیده‌ای نظیر جابجایی فرآیند (پردازش) و استراتژی‌های توازن بار را معرفی می‌کند. چنین استراتژی‌هایی به کلاسترها امکان می‌دهند تا به حد کافی عملکرد تقابل را تحویل داده و همچنین منابع اشتراکی را جهت برنامه‌های کاربردی موازی و ترتیبی مورد نیاز فراهم کنند.

۳- **سخت‌افزار گره:** کامپیوترهای شخصی (PC)، ایستگاه‌های کاری و یا SMP.

- کلاستری از کامپیوترهای شخصی (CoPs) یا انبوهی از کامپیوترهای شخصی (PoPs)
- کلاستری از ایستگاه‌های کاری (COWs)
- کلاستری از SMPها (CLUMPs)

٤- **سیستم‌عامل گره:** Linux، NT، Solaris، AIX و غیره.

- کلاسترهای Linux (برای مثال Beowulf)
- کلاسترهای Solaris (برای مثال Berkeley NOW)
- کلاسترهای NT (برای مثال HPVM)
- کلاسترهای AIX (برای مثال IBM SP2)
- کلاسترهای Digital VMS
- کلاسترهای HP-UX
- کلاسترهای Microsoft Wolfpack

۵- **پیکربندی گره:** معماری گره و نوع سیستم‌عاملی که بر روی آن اجرا می‌شود.

- کلاسترهای متجانس: تمامی گره‌ها دارای معماری یکسان بوده و سیستم‌عامل یکسانی را اجرا می‌کنند.
- کلاسترهای غیر متجانس: گره‌ها معماری یکسانی نداشته و سیستم‌عامل‌های مختلفی را اجرا می‌کنند.

٦- **سطوح کلاستر کردن:** بر اساس مکان گره‌ها و تعداد آن‌ها.

- کلاسترهای گروهی (دارای ۲ الی ۹۹ عدد گره): گره‌ها توسط SANها (شبکه‌های منطقه‌ای سیستم) نظیر Myrinet به یکدیگر متصل شده و می‌توانند درون یک فریم و یا یک مرکز قرار بگیرند.
- کلاسترهای واحدی (دارای ۱۰ الی ۱۰۰ عدد گره)
- کلاسترهای سازمانی (شامل تعداد زیادی کلاسترهای واحدی)
- فوق‌کامپیوترهای ملی (بر اساس شبکه‌های گسترده و یا اینترنت): شامل تعداد زیادی کلاسترها و یا سیستم‌های سازمانی و واحدی می‌باشند.
- فوق‌کامپیوترهای بین‌المللی (بر پایه اینترنت): (دارای هزاران تا میلیونها گره)

ممکن است کلاسترهای شخصی به صورت داخلی به یکدیگر متصل شوند تا یک سیستم بزرگتر (کلاستری از کلاسترها) را بوجود آورند و در حقیقت خود اینترنت می‌تواند به عنوان یک کلاستر محاسبه‌ای مورد استفاده قرار گیرد. بکارگیری شبکه‌های گسترده از منابع کامپیوتری جهت محاسبات با عملکرد و کارآیی بالا منجر به تولد رشته جدیدی به نام Meta Computing (فراپردازش) شده است.

۱۲-۸- اجزا مناسب جهت کلاسترها

توسعه‌ها و بهبودهایی که در زمینه ایستگاه‌های کاری و عملکرد شبکه بوجود آمده‌اند و همچنین در دسترس بودن APIهای برنامه‌نویسی استاندارد، راه را جهت استفاده گسترده از سیستم‌های موازی بر پایه کلاستر، هموار می‌سازند. در این قسمت پیرامون اجزا سخت‌افزاری و نرم‌افزاری که عموماً در کلاسترها و گره‌ها مورد استفاده قرار می‌گیرند، بحث خواهیم نمود.

۱۲-۸-۱- پردازنده‌ها

در طول دو دهه گذشته، پیشرفت شگفت‌انگیزی در معماری ریزپردازنده‌ها به وقوع پیوسته است (برای مثال RISC، CISC، VLIW و بردارها) و این مسئله باعث شده است تا پردازنده‌های تک تراشه‌ای به اندازه پردازنده‌هایی که در ابرکامپیوترها بکار می‌روند، قدرتمند باشند. اخیراً محققین سعی بر یکپارچه‌سازی پردازنده‌ها و حافظه یا رابط شبکه در یک تراشه واحد دارند. یعنی می‌خواهند پردازنده‌ها و حافظه یا رابط شبکه را بصورت واحد در یک تراشه قرار دهند. پروژه حافظه هوشمند (IRAM) دانشگاه Berkeley در حال بررسی و کاوش طیف کلی مشکلات و موانع طراحی سیستم‌های کامپیوتری همه‌منظوره‌ای است که پردازنده و حافظه آن‌ها در یک تراشه واحد قرار داده می‌شوند – این مشکلات از مدارها، طراحی

VLSI و معماری‌ها گرفته تا کامپایلرها و سیستم‌عامل‌ها گسترده می‌باشند. شرکت Digital با معرفی پردازنده Alpha 21364 خود سعی در یکپارچه‌سازی پردازش، کنترل‌کننده حافظه و کارت رابط شبکه در یک تراشه واحد نموده است.

پردازنده‌های شرکت Intel عموماً در کامپیوترهای شخصی و یا PCها بکار برده می‌شوند. نسل اخیر از خانواده پردازنده‌های x86 شرکت Intel شامل Pentium Pro، Pentium II و Pentium III می‌باشد. این پردازنده‌ها اگرچه حد عملیاتی بالایی ندارند ولی با عملکرد پردازنده‌های سطح متوسط ایستگاه‌های کاری متناسب می‌باشند. در حد عملیاتی بالا، پردازنده Pentium Pro در عملیات مربوط به اعداد صحیح بسیار قوی نشان داده و در سرعت کلاک یکسان از پردازنده UltraSPARC شرکت Sun پیشی گرفته است. با این وجود عملیات ممیز شناور در آن، حد عملیاتی بسیار پایینی داشته است. پردازنده Pentium II Xeon همانند پردازنده‌های جدید Pentium II از یک گذرگاه حافظه 100MHz بهره می‌برد. این پردازنده با حافظه کاشه سطح دوم به ظرفیت ۵۱۲ کیلوبایت تا ۲ مگابایت موجود می‌باشد و با همان سرعتی که پردازنده عمل می‌کند، کار کرده و بر مشکلات اجرایی و اندازه حافظه کاشه سطح دوم در پردازنده‌های اولیه Pentium II غلبه کرده است. همکاری نوع تراشه 450NX جهت پردازنده‌های Xeon از گذرگاه‌های PCI پشتیبانی به عمل آورده که خود امکان استفاده از اتصالات گیگابیت را بوجود می‌آورد.

سایر پردازنده‌های رایج از جمله گونه‌های x86 (AMD x86، Cyrix86)، پردازنده Alpha شرکت دیجیتال، پردازنده PowerPC شرکت IBM، پردازنده SPARC شرکت Sun، پردازنده MIPS شرکت SGI و پردازنده PA محصول شرکت HP می‌باشند. از سیستم‌های کامپیوتری که بر اساس این پردازنده‌ها بنا شده‌اند نیز می‌توان در کلاسترها استفاده نمود. به عنوان مثال Berkeley NOW از خانواده پردازنده‌های SPARC محصول شرکت Sun جهت گره‌های موجود در کلاستر خود استفاده می‌نماید.

۱۲-۸-۲- حافظه و کاشه (Cache)

اساساً، حافظه ارائه شده در یک کامپیوتر شخصی ٦٤٠ کیلوبایت بوده و معمولاً بر روی بورد اصلی سیستم لحیم شده بود. در حالیکه امروزه یک کامپیوتر شخصی با حافظه ٦٤ یا ۱۲۸ مگابایت و یا بیشتر که از تکنولوژی DIMM استفاده می‌کنند در بازار ارائه می‌شود. امروزه ظرفیت بالقوه یک کامپیوتر شخصی صدها مگابایت می‌باشد.

سیستم‌های کامپیوتری انواع مختلف حافظه نظیر خروجی داده توسعه‌یافته (EDO)، حافظه پویای همزمان (SDRAM) و fast page و... را مورد استفاده قرار می‌دهند. EDO امکان شروع دسترسی بعدی در زمانی که داده قبلی در حال خوانده شدن است را می‌دهد و fast page اجازه چندین دسترسی همجوار بطور مفید و موثر را فراهم می‌کند.

مقدار حافظه مورد نیاز برای کلاسترها احتمالاً بوسیله برنامه‌های کاربردی مورد استفاده در کلاستر مشخص می‌شود. برنامه‌هایی که موازی‌سازی می‌شوند باید به گونه‌ای توزیع شوند که حافظه و همچنین پردازش آن‌ها جهت میزان‌پذیری مابین پردازنده‌ها توزیع شده باشد. به همین دلیل نیازی به داشتن حافظه‌ای که بتواند تمامی برنامه را در خود جای دهد بر روی هر سیستم نخواهیم داشت، ولی فقط کافی است از وقوع جابجایی زیاد بلاک‌های حافظه (از دست دادن صفحات) به دیسک جلوگیری به عمل آوریم زیرا دسترسی به دیسک تاثیر به سزایی بر عملکرد کلی سیستم خواهد داشت.

دسترسی به حافظه DRAM در مقایسه با سرعت پردازنده بسیار کند می‌باشد، و جهت امور بزرگتر بیشتر از یک سیکل ساعت پردازنده طول می‌کشد. اگر پردازنده مجدداً به یک کلمه از همان بلاک قبلی رجوع کند، کاشه‌ها (Caches) جهت دسترسی سریع به آن کلمه، بلاکی که اخیراً به آن دسترسی شده است را در خود نگاه می‌دارند. با این وجود حافظه بسیار سریعی که در کاشه مورد استفاده قرار می‌گیرد گران بوده و با بزرگتر شدن اندازه کاشه مدار کنترلی آن نیز پیچیده‌تر خواهد بود. بدلیل این محدودیت‌ها کل اندازه یک کاشه معمولاً بین ۸ کیلوبایت تا ۲ مگابایت تغییر می‌کند.

داشتن گذرگاه حافظه ٦٤ بیتی و همچنین نوع تراشه‌ای که از دو مگابایت کاشه خارجی پشتیبانی به عمل آورد در ماشین‌هایی که پردازنده‌های Pentium در آن‌ها بکار برده شده، غیر متداول نمی‌باشد. چنین بهبودهایی جهت بهره‌برداری از کل توان پردازنده Pentium و شبیه کردن معماری حافظه به همتای خود در ایستگاه‌های کاری Unix، لازم بود.

۱۲-۸-۳- دیسک و ورودی / خروجی

بهبود زمان دسترسی به دیسک نتوانسته با عملکرد پردازنده که هر سال ۵۰ درصد یا بیشتر رشد داشته است، همگام شود. اگرچه تراکم رسانه‌های مغناطیسی افزایش پیدا کرده و زمان انتقال اطلاعات در دیسک نیز تقریباً به اندازه ٦٠ تا ۸۰ درصد در سال کاهش پیدا می‌کند، ولی با این وجود بهبود کلی زمان دستیابی در دیسک که بستگی به پیشرفت در سیستم‌های مکانیکی دارد، کمتر از ۱۰ درصد در سال می‌باشد.

برنامه‌های کاربردی بزرگ با بار کاری زیاد اغلب نیاز به پردازش حجم زیادی از اطلاعات و مجموعه داده‌ها دارند. قانون Amdahl بیانگر این مطلب است که افزایش سرعت حاصل از پردازنده‌های سریع توسط کندترین جزء سیستم محدود می‌شود. بنابراین بهبود کارآیی و عملکرد ورودی / خروجی جهت هماهنگ شدن با عملکرد پردازنده ضروری می‌باشد. یکی از راه‌های بهبود عملکرد ورودی / خروجی انجام این عملیات بصورت موازی است که بوسیله سیستم‌های فایل موازی که بر پایه RAID سخت‌افزاری یا نرم‌افزاری بنا شده‌اند، پشتیبانی می‌شود. از آنجایی که RAID سخت‌افزاری گران می‌باشد، RAIDهای نرم‌افزاری را می‌توان با استفاده از دیسک‌هایی که برای هر ایستگاه کاری در کلاستر در نظر گرفته شده‌اند، ایجاد کرد.

۱۲-۸-٤- گذرگاه سیستم

گذرگاه اولیه کامپیوترهای شخصی (AT که امروزه به آن گذرگاه ISA نیز می‌گویند) با سرعت ساعت ۵ مگاهرتز عمل کرده و عرض آن نیز ۸ بیتی بود. توانایی‌های این نوع گذرگاه زمانی که برای اولین بار معرفی شد، با بقیه سیستم به خوبی تناسب داشت. کامپیوترهای شخصی، سیستم‌های مدولاری هستند و تا چند سال قبل تنها پردازنده و حافظه بر روی بورد مادر بصورت سخت‌افزاری وصل بودند و سایر قطعات بر روی کارت‌های کمکی قرار داشتند که از طریق یک گذرگاه سیستم به آن متصل می‌شدند. از آنجایی که گذرگاه ISA برای اولین بار استفاده می‌شد، عملکرد کامپیوترهای شخصی افزایش پیدا کرد. ولی همین گذرگاه بعدها به یک تنگنا تبدیل شد، زیرا توان عملیاتی ماشین را محدود می‌کرد. سپس عرض گذرگاه ISA به ١٦ بیت و سرعت ساعت آن نیز به ۱۳ مگاهرتز افزایش داده شد. با این وجود این مقدار هنوز قادر به پاسخ به درخواست‌های پردازنده‌های اخیر، رابط‌های دیسک و دستگاه‌های جانبی دیگر نمی‌باشد.

گروهی از سازندگان کامپیوترهای شخصی گذرگاه داخلی VESA، که ۳۲ بیتی بوده و سرعت آن با سرعت ساعت سیستم متناسب بود را عرضه کردند. گذرگاه PCI که شرکت Intel آن را معرفی کرد، بطور وسیعی به جای گذرگاه داخلی VESA مورد استفاده قرار گرفت. این گذرگاه امکان انتقال ۱۳۳ مگابایت اطلاعات در هر ثانیه را داده و در کامپیوترهای شخصی که از پردازنده Intel در آن‌ها استفاده شده، بکار برده می‌شود. گذرگاه PCI همچنین جهت استفاده در سکوهایی که بر پایه پردازنده Intel نیستند، نظیر دامنه کامپیوترهای Digital AlphaServer، تطبیق داده شده است. این مسئله، از آنجایی که ممکن است زیر سیستم ورودی / خروجی یک ایستگاه کاری از رابط‌ها و کارت‌های ارتباطی مناسب ساخته شده باشد، باعث ابهام در تشخیص امتیازات و تفاوت‌های کامپیوترهای شخصی (PCs) و ایستگاه‌های کاری شده است.

۱۲-۸-۵- اتصالات درونی در یک کلاستر

گره‌ها در یک کلاستر از طریق شبکه‌های پر سرعت و با استفاده از پروتکل‌های استاندارد شبکه نظیر TCP/IP و یا پروتکل‌های سطح پایین نظیر پیام‌های فعال (Active Messages) با یکدیگر ارتباط برقرار می‌کنند. در بیشتر مواقع اتصالات داخلی از طریق اترنت استاندارد برقرار می‌شوند. از لحاظ عملکرد و کارآیی (تاخیر و پهنای باند) این تکنولوژی قدمت خود را آشکار می‌کند. با این وجود، اترنت یک روش ارزان و ساده جهت اشتراک فایل‌ها و چاپگر می‌باشد. یک اتصال اترنت واحد نمی‌تواند بطور جدی جهت محاسباتی که از طریق کلاسترها انجام می‌شوند،مورد استفاده قرار گیرد. پهنای باند و تاخیر این تکنولوژی در مقایسه با توان محاسباتی ایستگاه‌های کاری امروزه متناسب و هماهنگ نمی‌باشند. معمولاً یک شخص پهنای باند ارتباطی بالاتر از ۱۰ مگابایت در ثانیه و تاخیر پیام کمتر از ۱۰۰ میکروثانیه را در یک کلاستر انتظار دارد. تعدادی از تکنولوژی‌های شبکه با کارآیی بالا در بازار موجود می‌باشند که در این بخش پیرامون بعضی از آن‌ها بحث خواهیم نمود.

اترنت، اترنت سریع و گیگابیت اترنت

اترنت استاندارد تقریباً مشابه شبکه‌سازی در ایستگاه‌های کاری می‌باشد. این فن‌آوری چه در بخش تجاری و چه در بخش علمی کاربرد وسیعی پیدا کرده است. با این وجود، پهنای باند 10Mbps دیگر برای استفاده در محیط‌هایی که کاربران حجم زیادی از داده‌ها را انتقال داده و یا حجم ترافیک سنگینی دارند، مناسب نمی‌باشد. نسخه پیشرفته آن که به اترنت سریع معروف است، پهنای باند 100Mbps را ارائه می‌دهد و جهت ارتقای مسیر نصب اترنت‌های موجود طراحی شده است. اترنت استاندارد و سریع را نمی‌توان بصورت همزمان بر روی یک کابل داشت، ولی هر دو از نوع کابل یکسانی جهت ارتباطات بهره می‌گیرند. زمانی که نصب ما بر اساس hub بوده و از زوج سیم به عنوان رسانه ارتباطی استفاده کنیم امکان ارتقای hub به گونه‌ای که از هر دو استاندارد پشتیبانی به عمل آورد امکان‌پذیر خواهد بود و همچنین می‌توان تنها کارت‌های اترنتی را در ماشین‌ها جایگزین نمود که واقعاً نیاز باشد.

اکنون جدیدترین نوع اترنت، Gigabit Ethernet است که جذابیت آن بیشتر به دلیل دو ویژگی مهم می‌باشد. اولاً سادگی اترنت حفظ شده و در همان حال انتقال ملایم به سرعت‌هایی در حد گیگابیت در هر ثانیه امکان‌پذیر شده است. و ثانیاً پهنای باند بسیار بالایی را جهت انباشته کردن قطعات چندگانه اترنت سریع ارائه می‌دهد و همچنین قادر به پشتیبانی از ارتباطات سرویس‌دهندههای سریع، زیرساختارهای سوییچی بین‌ساختمانی، اتصالات بین سوئیچی و شبکه‌های گروه کاری بسیار سریع، می‌باشد.

مد انتقال غیرهمزمان (*ATM*)

ATM یک تکنولوژی مدار مجازی سوئیچی می‌باشد و اساساً جهت صنایع مخابراتی بوجود آمده است. ATM شامل یک سری پروتکل‌ها و استانداردهای تعریف شده بوسیله اتحادیه بین‌المللی مخابرات می‌باشد. انجمن بین‌المللی ATM که یک سازمان غیر انتفاعی است، این کار را دنبال می‌کند. برخلاف سایر فن‌آوری‌های شبکه‌سازی، ATM برای استفاده در LANها و هم در WANها منظور شده است و برای هر دو روش هم‌شکلی را ارائه می‌دهد. ATM بر اساس پاکت‌های داده‌ای کوچک با طول ثابت به نام cell عمل می‌کند. ATM به گونه‌ای طراحی شده است که به cellها اجازه انتقال از چندین رسانه مختلف نظیر کابل‌های مسی و فیبر نوری را می‌دهد. این تنوع سخت‌افزاری منجر به بوجود آمدن سطوح مختلفی از عملکرد و کارآیی در اتصالات داخلی می‌شود.

زمانی که تکنولوژی ATM برای اولین بار مطرح شد، فیبر نوری به عنوان فن‌آوری اتصال بکار گرفته می‌شد. با این وجود این مسئله در محیط‌های رومیزی چندان مطلوب نمی‌باشد؛ به عنوان مثال ممکن است جهت اتصالات داخلی در یک محیط شبکه‌ای از زوج سیم استفاده کرده باشیم و ارتقاء این سیستم بهATM ی که از فیبر نوری استفاده می‌کند بسیار هزینه‌بر خواهد بود. دو نوع از رایج‌ترین فن‌آوری‌های کابل‌کشی در محیط‌های رومیزی کابل‌های تلفن CAT3 و نوع با کیفیت بهتر به نام CAT5 می‌باشند. CAT5 می‌تواند به همراه تکنولوژی ATM به گونه‌ای بکار گرفته شود که ارتقا شبکه‌های موجود نیازی به جایگزینی کابل‌ها نداشته باشد.

رابط ارتباطی مقیاس‌پذیر (*SCI*)

SCI یک استاندارد IEEE 1596-1992 می‌باشد که به منظور تامین حافظه اشتراکی توزیعی با تاخیر کم در یک کلاستر ایجاد شده است. SCI معادل گذرگاه پردازنده – حافظه – ورودی / خروجی بوده که با شبکه محلی ترکیب شده است. SCI به گونه‌ای طراحی شده است که از چندپردازش توزیعی با تاخیر کم و پهنای باند زیاد پشتیبانی به عمل می‌آورد. این استاندارد دارای معماری مقیاس‌پذیری است که به سیستم‌های بزرگ اجازه می‌دهد از تعداد زیادی قطعات ارزان با تولید انبوه ساخته شوند.

SCI یک معماری نقطه به نقطه با همگونی کاشه بر اساس دایرکتوری می‌باشد. این معماری می‌تواند تاخیر ارتباطات بین پردازنده‌ها را حتی در مقایسه با جدیدترین و بهترین فن‌آوری‌های موجود از قبیل کانال فیبری و ATM، کاهش دهد. SCI با حذف لایه‌های اجرایی مربوط به ترجمه پروتکل- نمونه نرم‌افزاری به این مهم نایل می‌گردد. یک ارتباط دور در SCI همانند قسمتی از یک بارگیری (load) یا ذخیره‌سازی (store) ساده پردازش در یک پردازنده به وقوع می‌پیوندد. عموماً دسترسی به یک آدرس دور منجر به یک فقدان در کاشه (Cache miss) می‌شود. این امر به نوبه خود کنترل‌کننده کاشه را وادار به اشاره به حافظه دور کرده تا از طریق SCI به آن داده دسترسی پیدا کند. داده با تاخیری کمتر از چند میکروثانیه در کاشه واکشی می‌شود و سپس پردازنده عملیات اجرایی خود را ادامه می‌دهد.

در حال حاضر شرکت Dolphin جهت SPARC Sbus کارت‌های SCI تولید می‌کند. با این وجود آن‌ها کارت‌های SCI جهت کامپیوترهای شخصی (PC) را نیز معرفی نموده‌اند. آن‌ها یک SCI MPI بر روی سکوی پردازنده SPARC محصول شرکت Sun تولید نموده‌اند که تاخیر پاکت با طول پیام صفر در آن ۱۲ میکروثانیه می‌باشد و قصد آماده‌سازی MPI

برای Window NT را نیز در برنامه خود دارند. یک نسخه SCI از زبان برنامه‌نویسی فرترن با عملکرد بالا نیز قابل دسترس از طریق شرکت Portland Group می‌باشد.

اگرچه SCI از لحاظ پشتیبانی از حافظه اشتراکی و توزیعی سریع مورد توجه می‌باشد، با این وجود به طور گسترده مورد استفاده قرار نمی‌گیرد زیرا مقیاس‌پذیری آن بوسیله نسل جدید سوئیچ‌ها و اجزای آن‌ها محدود شده و همچنین نسبتاً گران نیز می‌باشد.

Myrinet

Myrinet یک شبکه ارتباطی کاملاً دو طرفه با سرعت 1.28 Gbps می‌باشد که توسط شرکت Myricom عرضه شده است. این شبکه یک ارتباط با عملکرد بالا و اختصاصی می‌باشد. Myrinet از سوئیچ‌های مسیریابی cut-through با تاخیر کم استفاده می‌کند که توانایی ارائه تحمل‌پذیری خطا بوسیله نگاشت خودکار پیکربندی شبکه را می‌دهند. این مسئله همچنین تنظیم و برپا نمودن شبکه را آسانتر می‌کند. Myrinet از سیستم‌عامل Linux و NT پشتیبانی به عمل می‌آورد. علاوه بر پشتیبانی از TCP/IP، پیاده‌سازی MPICH از MPI نیز در بعضی از بسته‌هایی که بصورت شخصی توسعه داده شده‌اند نظیر پیام‌های فعال Berkeley موجود می‌باشد که قادر به تامین تاخیرهای کمتر از ۱۰ میکروثانیه هستند.

Myrinet در مقایسه با اترنت سریع نسبتاً گران‌تر است، ولی مزایای بیشتری نسبت به آن دارد: تاخیرهای بسیار کم (۵ میکروثانیه برای ارتباط نقطه به نقطه یک طرفه)، توان عملیاتی بسیار بالا، و یک پردازنده برنامه‌پذیر که بر روی بورد نصب شده و بسیار انعطاف‌پذیر می‌باشد. Myrinet می‌تواند پهنای باند مفید یک گذرگاه PCI ۱۲۰ مگابایت در ثانیه‌ای را با پاکت‌های ٤ کیلوبایتی اشباع سازد.

همانطور که در بالا اشاره شد، یک از مهمترین معایب Myrinet هزینه بیشتر آن نسبت به اترنت سریع است. هزینه اجزای شبکه محلی Myrinet که شامل کابل‌ها و سوئیچ‌ها نیز می‌باشد در حدود ۱۵۰۰ دلار برای هر میزبان خواهد بود. همچنین سوئیچ‌هایی با درگاه‌های بیشتر از ١٦ تا نیز قابل دسترس نمی‌باشند، بنابراین مقیاس‌پذیری پیچیده خواهد بود، اگرچه از زنجیر کردن سوئیچ‌ها جهت ایجاد کلاسترهای Myrinet بزرگتر استفاده می‌شود.

۱۲-۸-٦- سیستم‌عامل‌ها

سیستم‌عامل‌های مدرن دو سرویس اساسی به کاربران ارائه می‌دهند. اولاً، کاربرد سخت‌افزار کامپیوتر را ساده‌تر می‌سازند. سیستم‌عامل ماشین مجازی را می‌سازد که بطور چشمگیری با ماشین واقعی تفاوت دارد. در حقیقت قسمتی از انقلاب کامپیوتر در دو دهه گذشته مدیون موفقیت سیستم‌عامل در دور نگاه داشتن کاربران در برابر پیچیدگی‌های سخت‌افزار کامپیوتر است. ثانیاً یک سیستم‌عامل منابع سخت‌افزاری را بین کاربران به اشتراک می‌گذارد. یکی از مهمترین منابع پردازنده می‌باشد. یک سیستم‌عامل چندکاره نظیر Unix و یا Windows NT کارهایی که باید انجام شوند را بین پردازش‌ها تقسیم می‌کند و به هر پردازش، حافظه، منبع سیستمی، حداقل یک رشته (Thread) اجرایی و یک واحد اجرایی به ازای هر پردازش اختصاص می‌دهد. سیستم‌عامل هر رشته را برای مدت زمان کوتاهی اجرا کرده و سپس به نوبت با اجرای رشته‌های دیگر به دیگر رشته‌ها سوئیچ می‌کند. حتی بر روی یک سیستم تک کاربره، چندکاره بودن اهمیت خاصی دارد زیرا به کامپیوتر امکان می‌دهد تا

چندین کار و عمل را یکباره انجام دهد. به عنوان مثال یک کاربر می‌تواند در زمانی که یک پرونده در حال چاپ شدن است و یا یک کامپایلر در حال کامپایل کردن یک فایل بزرگ می‌باشد، بر روی پرونده‌ای دیگر عمل ویرایش را انجام دهد. هر پردازش کار خود را انجام می‌دهد و برای کاربر اینگونه به نظر می‌رسد که تمامی برنامه‌ها همزمان اجرا می‌شوند.

صرفنظر از فوایدی که در بالا ذکر شدند، مفهوم جدید سرویس‌های سیستم‌عامل پشتیبانی از چندین رشته کنترلی در یک پردازش است. این مفهوم ابعاد جدیدی جهت پردازش موازی به گونه‌ای که موازی‌سازی در سطح پردازش صورت گیرد و نه در سطح برنامه، باز نموده است. در نسل جدید سیستم‌عامل‌ها، هسته (kernel)، فضای آدرس و رشته‌ها از یکدیگر مجزا می‌شوند به گونه‌ای که یک فضای آدرس واحد بتواند چندین رشته اجرایی داشته باشد. برنامه‌نویسی پردازشی که چندین رشته کنترلی داشته باشد معروف به multithreading است. رابط رشته‌های POSIX محیط برنامه‌نویسی استانداردی است که جهت ایجاد همزمانی و همچنین موازی‌سازی در یک پردازش بکار برده می‌شود.

تعدادی از عوامل که بر طراحی سیستم‌عامل تاثیر گذارده‌اند، در چند سال گذشته مشاهده شده است که مهمترین آن‌ها حرکت به سوی modularity می‌باشد. سیستم‌عامل‌هایی نظیر Windows محصول شرکت مایکروسافت و OS/2 محصول شرکت IBM و سایرین به قطعات مجزایی تقسیم شده‌اند که هر یک از این قطعات دارای رابط کوچک با تعریف جامع می‌باشند و هر کدام از آن‌ها از طریق رابط پیام‌گذاری بین کاری با دیگران ارتباط برقرار می‌سازند. پایین‌ترین سطح ریز هسته (Micro-Kernel) می‌باشد که تنها سرویس‌های اساسی سیستم‌عامل از قبیل تغییر زمینه (context switching) را فراهم می‌کند. Windows NT به عنوان مثال دارای یک لایه انتزاعی سخت‌افزاری (HAL) در زیر ریز هسته است که به سایر قسمت‌های سیستم‌عامل اجازه می‌دهد تا بدون در نظر گرفتن پردازنده‌ای که در زیر قرار دارد اجرا شوند. این انتزاع سطح بالا از قابلیت حمل سیستم‌عامل یکی از محرک‌های اصلی به سمت ریز هسته و modularity می‌باشد. سایر خدمات بوسیله زیرسیستم‌هایی که بر روی لایه ریزهسته قرار دارند تامین می‌شوند. به عنوان مثال سرویس‌های فایل می‌توانند توسط سرویس‌دهنده فایل که به عنوان یک زیرسیستم در بالای ریزهسته قرار داده شده است، ارائه شوند.

این قسمت به بررسی سیستم‌عامل‌های متنوعی که در ایستگاه‌های کاری و کامپیوترهای شخصی مورد استفاده قرار می‌گیرند، می‌پردازد. فن‌آوری سیستم‌عامل در حال کامل شدن است و به سادگی می‌تواند گسترش یابد، همچنین می‌توان زیرسیستم‌های جدیدی را بدون تغییر ساختار زیرین سیستم‌عامل به آن اضافه نمود. سیستم‌عامل‌های امروزی در سطح هسته از چندرشته‌ای پشتیبانی به عمل می‌آورند و سیستم‌های چندرشته‌ای در سطح کاربر نیز بدون مداخله هسته قابل پیاده‌سازی خواهند بود. اکثر سیستم‌عامل‌های کامپیوترهای شخصی تثبیت شده‌اند و از قابلیت‌های شبکه‌سازی، چندرشته‌ای و چندکارگی برخوردار هستند.

سیستم‌عامل Unix و گونه‌های مختلف آن (مانند Sun Solaris، IBM AIX، HP UX) بصورت رایج در ایستگاه‌های کاری مورد استفاده قرار می‌گیرند. در این بخش راجع به سه سیستم‌عامل مهم بحث خواهیم نمود که در گره‌های کلاسترهایی از ایستگاه‌های کاری و یا کامپیوترهای شخصی بکار برده می‌شوند.

Linux

لینوکس سیستم‌عاملی شبیه به Unix است که اولین بار در سال ۹۲-۱۹۹۱ توسط یک دانشجوی فنلاندی به نام Linus Torvalds به مورد اجرا گذاشته شد. نسخه‌های اولیه لینوکس به سیستم‌عامل Minix بسیار وابسته بودند. با این وجود، تلاش تعدادی از برنامه‌نویسان، باعث توسعه و اجرای یک سیستم‌عامل قوی، قابل اعتماد و قابل قبول از لحاظ POSIX، گشته است.

اگرچه لینوکس بوسیله یک شخص ابداع شده، لیکن تعداد زیادی از برنامه‌نویسان اکنون درگیر توسعه آن می‌باشند. یکی از مزایای اصلی این توسعه توزیع شده این است که محدوده وسیعی از ابزارهای نرم‌افزاری، کتابخانه‌ها و برنامه‌های سودمند، موجود می‌باشد. این بدین دلیل است که هر برنامه‌نویس توانا می‌تواند به منبع سیستم‌عامل دسترسی داشته و ویژگی‌های آن را بر طبق خواسته خود تغییر داده و یا پیاده‌سازی نماید. کنترل کیفیت لینوکس بوسیله آزاد کردن هسته از یک نقطه واحد بدست می‌آید و قابلیت دسترسی آن از طریق اینترنت کمک می‌کند تا در مورد خطاها و سایر مشکلات یک منبع feedback سریع داشته باشیم.

نکات زیر بعضی از مزایای لینوکس را شرح می‌دهند:

- با وجود اینکه لینوکس بر روس سکوهای ارزان‌قیمت x86 اجرا می‌شود، توان و انعطاف‌پذیری Unix را دارا می‌باشد.
- لینوکس بر روی اینترنت وجود دارد و می‌توان بدون هزینه آن را download کرد.
- رفع اشکالات و بهبود کارآیی سیستم آسان می‌باشد.
- کاربران می‌توانند راه‌اندازهای سخت‌افزاری مناسب طراحی کنند که به نوبه خود به راحتی در دسترس دیگران می‌تواند قرار گیرد.

سیستم‌عامل لینوکس ویژگیهایی را که عموماً در پیاده‌سازی‌های Unix وجود دارند، فراهم می‌کند، نظیر: پشتیبانی از چندپردازنده‌ای، چندکاربری، حافظه مجازی demand-page و چندکارگی تقدمی. اکثر برنامه‌های کاربردی که برای Unix نوشته شده‌اند تنها نیاز به کامپایل مجدد خواهند داشت. علاوه بر هسته لینوکس، تعداد زیادی از برنامه‌های کاربردی و سیستمی نظیر نرم‌افزار GNU، Xfree86 که یک X-Server دامنه عمومی می‌باشد، بصورت مجانی موجود می‌باشند.

Solaris

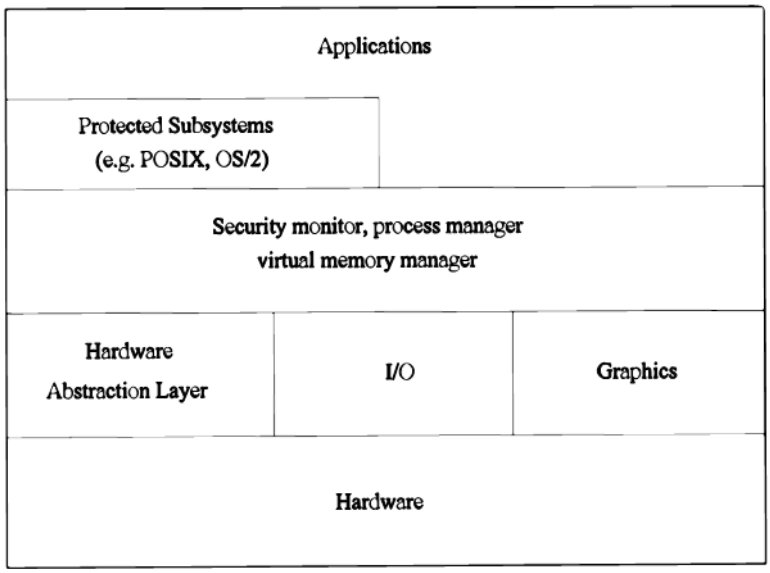
Solaris محصول شرکت SunSoft، سیستم‌عاملی مبتنی بر Unix است که از چندرشته‌ای و چندکاربری پشتیبانی به عمل می‌آورد. این سیستم‌عامل از سکوهای مبتنی بر SPARC و Intel x86پشتیبانی می‌کند. قسمت شبکه‌بندی آن شامل پشته پروتکل TCP/IP و ویژگی‌های لایه‌ای نظیر فراخوانی رویه دور (RPC) و سیستم فایل شبکه (NFS) می‌باشد. محیط برنامه‌نویسی Solaris شامل کامپایلرهای C و C++ که مورد قبول ANSI هستند و همچنین ابزارهایی جهت طراحی و رفع اشکال برنامه‌های چندرشته‌ای می‌باشد. هسته سیستم‌عامل Solaris از چندپردازشی و چندرشته‌ای پشتیبانی به عمل می‌آورد و همچنین دارای ویژگی‌های زمان‌بندی real-time ی است که برای برنامه‌های کاربردی صوتی و تصویری بسیار حیاتی هستند. Solaris از دو نوع رشته پشتیبانی می‌کند: پردازش‌های سبک وزن (LWP) و رشته‌هایی که در سطح کاربر می‌باشند. رشته‌ها به اندازه کافی سبک وزن هستند بطوریکه هزاران رشته می‌توانند وجود داشته باشند و همزمانی و تغییر زمینه می‌توانند بدون وارد شدن به هسته به سرعت بدست آیند.

Solaris علاوه بر سیستم فایل BSD، از چندین نوع سیستم فایل دیگر غیر از BSD نیز جهت افزایش کارآیی و راحتی استفاده، پشتیبانی به عمل می‌آورد. جهت عملکرد بهتر سه نوع سیستم فایل جدید وجود دارند: CacheFS، Autoclient و TmpFS. سیستم فایل کاشه CacheFS اجازه می‌دهد تا از یک دیسک سخت داخلی به عنوان کاشه مدیریت شده سیستم‌عامل جهت دیسک NFS راه دور و یا سیستم‌های فایل CD-ROM استفاده شود. با بکارگیری Autoclient و CacheFS کل فضای دیسک را می‌توان به عنوان کاشه مورد استفاده قرار داد. سیستم فایل موقتی TmpFS از حافظه اصلی جهت نگهداری سیستم فایل سود می‌برد. علاوه بر سیستم‌های فایلی که در بالا توضیح داده شدند، سیستم‌های فایل دیگری نیز نظیر Proc و Volume وجود دارند که جهت افزایش کارآیی سیستم از آن‌ها استفاده می‌شود.

Solaris از محاسبات توزیعی پشتیبانی کرده و قادر به ذخیره و بازیابی نمودن اطلاعات توزیعی جهت شرح سیستم و کاربران از طریق سرویس اطلاعاتی شبکه (NIS) و بانک اطلاعاتی، می‌باشد. OpenWindows که مربوط به رابط گرافیکی کاربر Solaris و ترکیبی از X11R5 و سیستم Adobe Postscript می‌باشد، به برنامه‌های کاربردی اجازه می‌دهد تا بر روی سیستم‌های دور اجرا شوند. این مهم در صورتی به وقوع می‌پیوندد که ما قادر به دنبال کردن وضعیت برنامه‌هایی که در سیستم‌های دور در حال اجرا می‌باشند از طریق برنامه‌های کاربردی داخلی خواهیم بود.

Windows NT

سیستم عامل Windows NT (تکنولوژی جدید)، در بازار کامپیوترهای شخصی بسیار معروف می‌باشد. NT یک سیستم‌عامل نوبه‌ای (preemptive)، چندکاربری، چندوظیفه‌ای و ۳۲ بیتی است. NT از چندین پردازنده پشتیبانی می‌کند و همچنین چندوظیفه‌ای را با استفاده از چندپردازش متقارن بدست می‌آورد. هر برنامه کاربردی ۳۲ بیتی در NT در فضای آدرس مجازی خود اجرا می‌شود. برخلاف نسخه‌های قبلی (نظیر Windows 95، Windows 98 و یا Windows for WorkGroups)، NT یک سیستم‌عامل کامل بوده و برنامه‌ای اضافه شده به DOS نیست. NT به کمک رشته‌ها از پردازنده‌های مختلف و ماشین‌های چندپردازنده‌ای پشتیبانی می‌کند. NT دارای مدل امنیتی بر مبنای object بوده و دارای سیستم فایل (NTFS) مختص به خود می‌باشد که به نوبه خود اجازه می‌دهد مجوزها را درون یک فایل یا دایرکتوری مقداردهی کنیم. طرح شماتیک معماری NT در شکل شماره ٤ نشان داده شده است. NT پروتکل‌ها و سرویس‌های شبکه را در داخل سیستم‌عامل پایه خود قرار داده است.



شکل شماره ٤: معماری Windows NT 4.0

به همراه NT چندین پروتکل شبکه نظیر IPX/SPX، TCP/IP و NetBEUI و APIهایی نظیر NetBIOS، DCE RPC و Winsock بصورت داخلی عرضه می‌شوند. برنامه‌های کاربردی TCP/IP از WinSock جهت ارتباط از طریق شبکه TCP/IP بهره می‌گیرند.

۱۲-۹- سرویس‌های شبکه / نرم‌افزارهای ارتباطی

نیازهای ارتباطی برنامه‌های کاربردی توزیعی بسیار متغیر و متفاوت بوده و از اتصالات نقطه به نقطه قابل اطمینان تا ارتباطاتی که در آن‌ها ارسال به چند نقطه مشخص بصورت غیر قابل اطمینان انجام می‌گیرد، امکان‌پذیر می‌باشند. زیرساختار ارتباطات باید از پروتکل‌هایی که جهت انتقال داده زیاد، داده جریانی، ارتباطات گروهی و همچنین پروتکل‌هایی که توسط اجزاء توزیعی مورد استفاده قرار می‌گیرند، پشتیبانی به عمل آورد.

سرویس‌های ارتباطی بکار گرفته شده، مکانیزم اولیه مورد نیاز توسط کلاستر جهت انتقال داده‌های کاربری و همچنین کنترلی را ارائه می‌دهند. این سرویس‌ها همچنین پارامترهای مهم کیفیت سرویس نظیر تاخیر، پهنای باند، قابلیت اطمینان، تحمل‌پذیری در برابر خطا و کنترل لغزش را جهت یک کلاستر تامین می‌کنند. عموماً سرویس‌های شبکه بصورت پشته‌ای سلسله‌مراتبی از پروتکل‌ها طراحی می‌شوند. در چنین سیستم لایه‌ای، هر لایه از پروتکل در پشته از سرویس‌هایی که لایه پایینی آن فراهم کرده، استفاده می‌کند. بهترین مثال در رابطه با چنین معماری شبکه‌ای، سیستم هفت لایه‌ای ISO OSI می‌باشد.

طبق عادت، سرویس‌های سیستم‌عامل (لوله‌ها و سوکت‌ها) جهت ارتباط بین پردازش‌ها در سیستم انتقال پیام، بکار می‌روند. به عنوان یک نتیجه، ارتباط بین مبداء و مقصد عملیات پرهزینه‌ای نظیر عبور پیام از لایه‌های زیاد، کپی کردن داده، کنترل حفاظت و معیارهای ارتباط قابل اطمینان، در بر دارد. اغلب کلاسترها با شبکه و یا سوئیچ‌های خاص نظیر Myrinet، از پروتکل‌های ارتباطی سبک وزن نظیر پیام‌های فعال جهت ارتباط سریع بین گره‌های خود، استفاده می‌کنند. آن‌ها بصورت بالقوه مرحله سیستم‌عامل را نادیده گرفته و با این روش سربارهای ارتباطی بحرانی را از بین می‌برند و به همین دلیل قادر به دسترسی در سطح کاربر و بصورت مستقیم با رابط شبکه می‌باشند.

سرویس‌های شبکه در کلاسترها، اغلب از API (رابط برنامه‌نویسی برنامه‌های کاربردی) ارتباطی نسبتاً سطح پایین ساخته می‌شوند که خود می‌توانند جهت پشتیبانی محدوده وسیعی از کتابخانه‌ها و پروتکل‌های ارتباطی سطح بالا مورد استفاده قرارگیرند. این مکانیزم‌ها وسایل پیاده‌سازی تعداد زیادی از روش‌های ارتباطی نظیر RPC، DSM و رابط‌های انتقال پیام و مبتنی بر جریان نظیر MPI و PVM را فراهم می‌کنند.

۱۲-۱۰- میان‌افزار کلاستر و تصویر سیستم واحد

اگر مجموعه‌ای از کامپیوترهای مرتبط طوری طراحی شود که بصورت یک منبع واحد نمایان شود، گوییم که دارای یک تصویر سیستم واحد (SSI) می‌باشد. SSI توسط یک لایه میان‌افزار حمایت می‌شود که مابین سیستم‌عامل و محیط سطح کاربر قرار گرفته است. این میان‌افزار اساساً از دو زیرلایه موجود در زیرساختار نرم‌افزاری تشکیل شده است:

- زیرساختار تصویر سیستم واحد
- زیرساختار قابلیت دسترسی سیستم

زیرساختار SSI در تمامی گره‌ها به سیستم‌عامل‌ها چسبیده است تا دستیابی منفرد به منابع سیستم را عرضه کند. زیرساختار قابلیت دسترسی به سیستم در میان تمامی گره‌های کلاستر، خدمات کلاستر در زمینه بازرسی محلی، غلبه بر خطا بصورت خودکار، بازیابی از خرابی و پشتیبانی از تحمل کردن خطا را فعال می‌سازد.

موارد ذیل از مزایا / فواید یک میان‌افزار کلاستر و بخصوص SSI می‌باشند:

- کاربر نهایی را از دانستن این موضوع که یک برنامه کاربردی در کجا به کار می‌رود، مبرا می‌سازد.
- اپراتور را از دانستن اینکه یک منبع (نمونه‌ای از منبع) در کجا قرار گرفته، رها می‌سازد.
- اپراتور یا برنامه‌نویس سیستم که باید در ناحیه‌ای خاص کار کنند را محدود نمی‌سازد. رابط کاربر نهایی (فرا رابط – بررسی جز به جز اطلاعات مشترک را آسان می‌سازد) می‌تواند به ناحیه‌ای که مشکل از آنجا ناشی شده است وارد شود.
- احتمال خطاهای اپراتور را می‌کاهد، با این نتیجه که کاربران نهایی متوجه قابلیت اطمینان بهبودیافته و قابلیت دسترسی بالای سیستم می‌شوند.
- متمرکز نمودن یا عدم تمرکز اداره و کنترل سیستم را ممکن می‌سازد تا نیازی به مجریان ماهر برای اداره سیستم نباشد.
- بطور وسیعی مدیریت سیستم را آسان می‌سازد؛ می‌توان اعمالی که، چندین منبع را تحت تاثیر قرار می‌دهند، را با یک دستور واحد بدست آورد، حتی زمانی که منابع در میان چندین سیستم و روی ماشین‌های متفاوت واقع شده باشند.
- ارتباط پیامی مستقل از مکان را مهیا می‌سازد. چون SSI نگاشتی پویا از پیام‌های مسیریابی، آنچنانکه در واقعیت رخ می‌دهد، ایجاد می‌کند، بنابراین اپراتور می‌تواند مطمئن باشد که اعمال در سیستم جاری اجرا خواهند شد.
- در ردیابی موقعیت تمامی منابع کمک زیادی می‌کند، در نتیجه هیچ نیازی نیست که اپراتورهای سیستم در حین انجام وظایف مدیریت سیستم، نگران موقعیت و مکان فیزیکی خود باشند.

فواید SSI همچنین می‌تواند برای برنامه‌نویسان سیستم بکار رود. SSI، زمان، تلاش و دانش لازم جهت اجرای اعمال را کاسته و به کارمندان فعلی اجازه می‌دهد تا سیستم‌های بزرگتر و پیچیده‌تری را اداره کرده و مورد استفاده قرار دهند.

۱۲-۱۰-۱- لایه‌ها / سطوح تصویر سیستم واحد

مفهوم SSI می‌تواند برای برنامه‌های کاربردی، زیرسیستم‌های ویژه و یا کل کلاستر سرویس‌دهنده بکار رود. خدمات تصویر سیستم واحد و قابلیت دسترسی سیستم می‌توانند بوسیله یک یا تعداد بیشتری از لایه‌ها / سطوح زیرین عرضه شوند:

- سخت‌افزار (نظیر کانال حافظه شرکت دیجیتال (DEC)، DSM سخت‌افزاری و تکنیک‌های SMP)
- ابزار تحتانی (Underware) هسته سیستم‌عامل یا لایه چسبیده (نظیر Solaris MC و GLUnix)
- برنامه‌های کاربردی و زیرسیستم‌ها در میان‌افزار
  - ✓ برنامه‌های کاربردی (نظیر ابزارهای مدیریتی سیستم و فرم‌های الکترونیکی)
  - ✓ سیستم‌های اجرایی (نظیر DSM نرم‌افزاری و سیستم فایل موازی)
  - ✓ نرم‌افزار زمان‌بندی و مدیریت منابع (نظیر LSF و CODINE)

همچنین این نکته باید ذکر شود که، سیستم‌های اجرایی و برنامه‌نویسی مانند PVM نیز می‌توانند به عنوان میان‌افزار کلاستر بکار روند.

لایه‌های SSI هم برنامه‌های کاربردی آگاه از کلاستر (نظیر برنامه‌های کاربردی موازی که توسط MPI ایجاد شده‌اند) و هم برنامه‌های کاربردی ناآگاه (معمولاً برنامه‌های ترتیبی) از آن را تداوم می‌بخشند. این برنامه‌های کاربردی (بخصوص نوع آگاه از کلاستر) شفافیت عملکردی و کارآیی مقیاس‌پذیر را طلب می‌کنند (یعنی وقتی قابلیت کلاستر افزایش پیدا می‌کند، باید سریعتر اجرا شوند). کلاسترها در یک جهت عملکردی، همچون یک سیستم SMP یا MPP با درجه بالای SSI عمل کرده و در جهت دیگر می‌توانند به عنوان یک سیستم توزیع شده با تصویرهای سیستم متعدد، عمل کنند.

خدمات SSI و قابلیت دسترسی سیستم نقش عظیمی را در موفقیت کلاسترها ایفا می‌کنند. در بخش بعدی، به طور مختصر در مورد لایه‌هایی که این زیرساختار را تداوم می‌بخشند، بحث می‌کنیم. بحث جزئی‌تر در مورد زیرساختار کلاستر را می‌توانید در بخشهای دیگر همراه با شاخص‌های مناسب جهت اطلاعات بیشتر پیدا کنید.

لایه سخت‌افزار

سیستم‌هایی نظیر کانال حافظه شرکت دیجیتال (DEC) و DSM سخت‌افزاری، SSI را در سطح سخت‌افزار عرضه داشته و این امکان را به کاربر میدهند که کلاستر را به عنوان یک سیستم حافظه مشترک بنگرد. کانال حافظه شرکت دیجیتال که یک ارتباط کلاستر اختصاصی می‌باشد، حافظه مشترک مجازی بین گره‌ها را از طریق نگاشت فضای آدرس بین‌گره‌ای مهیا می‌سازد.

هسته سیستم‌عامل (ابزار تحتانی) یا لایه چسبیده

سیستم‌عامل‌های کلاستر از اجرای کارآمد برنامه‌های کاربردی موازی در محیطی مشترک با برنامه‌های کاربردی ترتیبی، حمایت به عمل می‌آورند. یکی از اهداف، یکی کردن منابع در یک کلاستر به منظور ایجاد اجرای بهتر برای هر دو مورد برنامه‌های کاربردی موازی و ترتیبی می‌باشد. برای تحقق این هدف، سیستم‌عامل باید به زمان‌بندی گروهی برنامه‌های موازی تداوم بخشد و منابع بلااستفاده (نظیر پردازنده، حافظه و شبکه) در سیستم را شناسایی کرده و دسترسی کلی به آن‌ها را عرضه دارد. سیستم‌عامل باید از جابجایی پردازش به منظور توازن بار پویا و ارتباط بین‌پردازشی سریع جهت برنامه‌های کاربردی

سطح کاربر و سیستم، پشتیبانی به عمل آورد. سیستم‌عامل باید این اطمینان را حاصل کند که این ویژگی‌ها بدون نیاز به درخواست یا تقاضای دستورات یا فراخوانی سیستم جدید، یا دارا بودن از syntax یکسان در دسترس کاربر باشند. هسته‌های سیستم‌عامل‌هایی که از SSI حمایت می‌کنند شامل SCO UnixWare و Sun Solaris-MC می‌باشند.

یک SSI کاملاً گسترده در کلاستر به تمام منابع فیزیکی و منابع هسته این امکان را می‌دهد که از تمام گره‌های داخل سیستم قابل رویت و دسترس باشند. SSI کامل می‌تواند به عنوان ابزار تحتانی (SSI در سطح سیستم‌عامل) بدست آید. به عنوان دیگر، هسته سیستم‌عامل هر گره کمک می‌کند تا نگرش یکسانی از تمامی رابط‌های هسته، در تمامی گره‌ها بوجود آید.

SSI کامل در سطح هسته، می‌تواند در زمان و هزینه صرفه‌جویی کند، زیرا برنامه‌ها و کاربردهای موجود جهت کار کردن نیازی به دوباره نوشته شدن در این محیط جدید، ندارند. این برنامه‌های کاربردی بدون نیاز به تنظیم اجرایی در هر گره به اجرا در می‌آیند و پردازش‌ها می‌توانند به منظور توازن بار بین گره‌ها و همچنین جهت پشتیبانی از تحمل‌پذیری خطا در صورت لزوم، از گره‌ای به گره دیگر مهاجرت کنند.

اکثر سیستم‌عامل‌هایی که از SSI حمایت می‌کنند به عنوان یک لایه در بالای سیستم‌عامل‌های موجود منظور می‌شوند و تخصیص منابع کلی را به اجرا در می‌آورند. این استراتژی به آسانی سیستم را قابل انتقال ساخته، زمان پیشرفت و ارائه نسخه جدیدتر را می‌کاهد و ردیابی ارتقاء نرم‌افزاری فروشنده را نیز به دنبال خواهد داشت. GLUnix دانشگاه Berkeley این فلسفه را دنبال می‌کند و ثابت می‌کند که سیستم‌های جدید می‌توانند سریعاً از طریق نگاشت سرویس‌های جدید به قابلیت عملکردی که توسط لایه پایین‌تر ایجاد شده، ساخته شوند.

لایه برنامه‌های کاربردی و زیرسیستم‌ها (میان‌افزار)

SSI همچنین توسط موارد کاربردی و زیرسیستم‌هایی که اجزای چندگانه و مشترک یک برنامه کاربردی را برای کاربر یا مجری به عنوان یک کاربرد منفرد ایجاد و معرفی می‌کنند، حمایت می‌شود. SSI سطح کاربردی بالاترین و از جهتی مهمترین می‌باشد زیرا آن چیزی است که کاربر نهایی آن را می‌بیند. برای مثال، یک ابزار کنترلی کلاستر، یک نقطه منفرد از مدیریت و کنترل سرویس‌های SSI را عرضه می‌دارد. اینها می‌توانند به عنوان ابزاری بر مبنای رابط گرافیکی کاربر ساخته شوند که پنجره‌ای واحد برای کنترل و مونیتورینگ کلاستر به عنوان یک گره کلی منحصر به فرد یا اجزای ویژه سیستم، ارائه می‌کند.

زیرسیستم‌ها، ابزارهای نرم‌افزاری را برای ایجاد یک سیستم کلاستری کارآمد با استفاده آسان، ارائه می‌کنند. سیستم‌های اجرایی مانند سیستم‌های فایلی کلاستر باعث می‌شوند دیسک‌هایی که به گره‌های کلاستر متصل هستند همچون یک سیستم ذخیره‌سازی بزرگ منفرد به نظر رسند. SSI ارائه شده توسط سیستم‌های فایل اطمینان می‌دهد که هر گره در کلاستر نگرشی یکسان از داده‌ها را داراست. سیستم‌های برنامه‌نویسی کاری سراسری، منابع را اداره می‌کنند و زمان‌بندی فعالیت‌های سیستم و اجرای برنامه‌های کاربردی را، درحالی که خدمات با قابلیت دسترسی بالا همراه با شفافیت را ارائه می‌دهند، امکان‌پذیر می‌سازند.

۱۲-۱۰-۲- حدود SSI

کلیدی که ساختار SSI را مهیا می‌سازد، در توجه به نکات زیر قرار دارد:

- هر تصویر سیستم واحد دارای حد است؛ و
- پشتیبانی از تصویر سیستم واحد می‌تواند در سطوح مختلف در یک سیستم وجود داشته باشد - که یکی قادر است روی دیگری بنا شود.

برای مثال، یک زیرسیستم (سیستم‌های مدیریت منبع نظیر LSF و CODINE) می‌تواند مجموعه‌ای از دستگاه‌های مرتبط را به گونه‌ای ایجاد کند که بصورت یک دستگاه بزرگ به نظر آیند. وقتی هر عملکردی درون حدود SSI زیر سیستم اجرا شود، تصور یک ابرکامپیوتر قدیمی را بوجود می‌آورد. اما اگر هر چیزی خارج از حد SSI آن اجرا شود به نظر می‌رسد که کلاستر تنها گروهی از کامپیوترهای متصل است. نمونه زیرسیستم یا برنامه کاربردی دیگر، می‌تواند مجموعه‌ای از همان دستگاه‌ها را بوجود آورد که همانند یک سیستم بزرگ ذخیره‌سازی یا پایگاه داده‌ها به نظر رسند. مثلاً، یک سیستم فایل کلاستر که با استفاده از دیسک‌های محلی مربوط به گره‌ها ایجاد شده است، می‌تواند به عنوان یک سیستم ذخیره‌سازی بزرگ (RAID نرم‌افزاری) یا سیستم فایل موازی به نظر آید و دسترسی سریعتر به اطلاعات را ارائه کند.

۱۲-۱۰-۳- اهداف طراحی میان‌افزار

اهداف طراحی سیستم‌های بر مبنای کلاستر به طور عمده در موارد شفافیت کامل در مدیریت منابع، اجرا و کارآیی مقیاس‌پذیر و قابلیت دسترسی سیستم در حمایت از برنامه‌های کاربردهای کاربر، متمرکز می‌شوند.

شفافیت کامل

لایه SSI باید به کاربر اجازه دهد تا یک کلاستر را بدون آگاهی از معماری واقعی سیستم و به راحتی و بطور کارآمد مورد استفاده قرار دهد. محیط عملیاتی آشنا به نظر می‌رسد (با ایجاد نگرش و حس یکسان از سیستم موجود) و استفاده از آن راحت است. کاربر نگرشی از یک سیستم فایل سراسری، پردازنده‌ها و شبکه پیدا می‌کند. به عنوان مثال در یک کلاستر با یک نقطه ورودی منفرد، کاربر می‌تواند از هر گره وارد شود و اداره‌کننده سیستم می‌تواند نرم‌افزار را در گره هر کسی نصب یا بارگذاری کند و همچنین کاربر در تمام کلاستر قابل رویت می‌باشد. توجه داشته باشید که در سیستم‌های توزیعی لازم است که یک شخص نرم‌افزار یکسانی را برای هر گره نصب کند. جزییات مدیریت منابع و اعمال کنترلی نظیر تخصیص منابع، بازپس‌گیری منابع و کپی‌برداری توسط پردازش‌های کاربر غیر قابل رویت می‌باشند. این امر به کاربر اجازه می‌دهد که به منابع سیستم همچون حافظه، پردازنده و شبکه به طور شفاف دسترسی داشته باشد. این امر بدون توجه به اینکه آیا منابع بطور محلی در دسترس هستند یا در منطقه‌ای دور میسر خواهد بود.

اجرای مقیاس‌پذیر

همانگونه که کلاسترها به راحتی قابل گسترش هستند، اجرای آن‌ها نیز باید به همان راحتی گسترش و بهبود یابد. این مقیاس‌پذیری باید بدون نیاز به پروتکل‌ها و APIهای جدید بوجود آید. برای استخراج بیشترین کارآیی، سرویس SSI باید از طریق توزیع حجم کار بطور مساوی میان گره‌ها به توازن بار و موازی‌سازی تداوم ببخشد. برای مثال، ورودی نقطه منفرد باید درخواست‌های ورود، اجرای دور و Ftp را بین گره‌های کم‌بار توزیع کند. کلاستر باید این خدمات را با سربار کم ارائه

دهد و همچنین باید اطمینان دهد که زمان لازم برای اجرای عملیات مشابه در کلاستر بیشتر از زمان اجرای همان عملیات در یک ایستگاه کاری منفرد نخواهد بود (فرض کنید گره‌های کلاستر و ایستگاه‌های کاری پیکربندی‌های مشابهی دارند).

قابلیت دسترسی بهبودیافته

خدمات میان‌افزار باید در هر زمان از قابلیت دسترسی بالایی بهره‌مند باشند. در هر زمان یک نقطه شکست یا خرابی باید بدون تحت تاثیر قرار دادن برنامه کاربر، قابل احیا باشد. این امر با بکارگیری تکنولوژی‌های بررسی و تحمل‌پذیری خطا (خدمات دستگاه جانشین روشن و آماده به کار، قرینه‌سازی، غلبه بر خطا و برگرداندن خطا) به منظور قادر ساختن روش ترمیم بازگشتی، حاصل می‌شود.

وقتی خدمات SSI با استفاده از منابع قابل دسترس در چندین گره ارائه می‌شوند، خرابی هر گره نباید عملکرد سیستم را تحت تاثیر قرار دهد و یک سرویس ویژه باید از یک یا تعداد بیشتری اهداف طرح‌شده حمایت به عمل آورد. برای مثال، وقتی یک سیستم فایل در میان گره‌های زیادی با میزان مشخصی از افزونگی توزیع می‌شود، زمان از کار افتادن یک گره، آن بخش از سیستم فایل می‌تواند بصورت شفاف به گره دیگری منتقل شود.

۱۲-۱۰-٤- خدمات کلیدی SSI و زیرساختار قابلیت دسترسی

یک کلاستر، در حالت ایده‌آل، باید دامنه وسیعی از خدمات SSI و قابلیت دسترسی را عرضه کند. این خدمات توسط یک یا تعداد بیشتری از لایه‌هایی که در طول ابعاد گوناگونی از یک حوزه کاربردی گسترش یافته‌اند، ارائه می‌شوند. بخش‌های ذیل راجع به خدمات SSI و قابلیت دسترسی که توسط زیرساختارهای میان‌افزار ارائه می‌شوند، بحث می‌کنند.

خدمات پشتیبانی از *SSI*

نقطه واحد ورودی: یک کاربر جهت اتصال به کلاستر بجای اینکه به گره‌های جداگانه متصل شود، نظیر سیستم‌های توزیعی (مانند telnet node1.Beowulf.myinstitute.edu)، می‌تواند به عنوان یک سیستم واحد (مانند telnet Beowulf.myinstitute.edu) با آن ارتباط برقرار کند.

سلسله مراتب فایل منفرد (SFH): در زمان ورود به سیستم، کاربر، یک سیستم فایل را به عنوان سلسله‌مراتب واحدی از فایل‌ها و دایرکتوری‌هایی که تحت یک دایرکتوری ریشه قرار دارند، مشاهده می‌کند. مثال‌ها: xFS و Solaris MC Proxy.

نقطه منفرد مدیریت و کنترل: تمامی کلاستر را می‌توان از یک پنجره منفرد که از یک ابزار رابط کاربر گرافیکی بهره می‌برد، کنترل کرد. این مورد بسیار شبیه به یک ایستگاه کاری NT است که توسط ابزار مدیریت وظیفه یا مونیتورینگ PARMON منابع کلاستر را کنترل کرده و اداره می‌کند.

شبکه‌سازی مجازی منفرد: به این معنا است که هر گره می‌تواند از طریق حوزه کلاستر به هر اتصال شبکه دسترسی داشته باشد، حتی اگر شبکه از لحاظ فیزیکی به تمام گره‌های کلاستر متصل نباشد.

فضای حافظه منفرد: این مورد تصور حافظه مشترک با استفاده از حافظه‌های گره‌های موجود در کلاستر را بوجود می‌آورد.

سیستم مدیریت کار منفرد: یک کاربر می‌تواند از هر گره و با استفاده از مکانیزم ارائه کار بصورت شفاف، کاری را به کلاستر ارائه دهد. کارها می‌توانند طوری برنامه‌ریزی شوند که در یکی از حالات دسته‌ای، محاوره‌ای یا موازی به اجرا در آیند. سیستم‌های نمونه LSF و CODINE می‌باشند.

رابط کاربر منفرد: کاربر باید قادر به استفاده از کلاستر از طریق رابط کاربر گرافیکی واحد باشد. رابط باید دارای همان ظاهر و احساسی باشد که در ایستگاه‌های کاری قابل دسترس است. (مانند Solaris OpenWin و یا Windows NT GUI)

توابع پشتیبانی از قابلیت دسترسی

فضای ورودی / خروجی منفرد (SIOS): این امر به هر گره امکان می‌دهد تا عملیات ورودی / خروجی را روی دیسک‌ها یا دستگاه‌های جانبی مستقر در نقطه‌ای دور یا در همان محل به مورد اجرا بگذارد. در این طرح SIOS، دیسک‌هایی که در گره‌های کلاستر قرار دارند، RAIDها و دستگاه‌های جانبی یک فضای آدرس منفرد را تشکیل می‌دهند.

فضای پردازش منفرد: پردازش‌ها دارای یک شناسه فرآیندی در گستره کلاستر می‌باشند. یک پردازش بر روی هر گره می‌تواند فرآیندها یا پردازش‌های کوچکتری را روی همان گره یا گره‌های دیگر (از طریق یک انشعاب Unix) بوجود آورد یا با هر کدام از پردازش‌های دیگر روی یک گره دور (از طریق علائم، سیگنال‌ها یا لوله‌ها (Pipes)) ارتباط برقرار کند. این کلاستر باید از مدیریت پردازش سراسری پشتیبانی کرده و امکان مدیریت و کنترل پردازش‌ها را، به گونه‌ای که گویی در دستگاه‌های محلی اجرا می‌شوند، بوجود آورد.

انتقال یا مهاجرت پردازش و بررسی: مکانیزم‌های بررسی امکان ذخیره‌سازی حالت پردازش و نتایج محاسبات میانی را بصورت دوره‌ای یا پریودیک بوجود می‌آورند. وقتی یک گره از کار می‌افتد، فرآیندهایی که بر روی گره از کار افتاده قرار دارند می‌توانند مجدداً روی گره سالم دیگری بدون از دست دادن محاسبات قبلی خود آغاز شوند. انتقال پردازش امکان توازن بار پویا بین گره‌های موجود در یک کلاستر را ایجاد می‌کند.

۱۲-۱۱- مدیریت منابع و زمان‌بندی (*RMS*)

مدیریت منابع و زمان‌بندی (RMS) همان عمل توزیع برنامه‌های کاربردی در میان کامپیوترها به منظور بالا بردن توان عملیاتی آن‌هاست. این عمل همچنین بهره‌گیری موثر و کارآمد از منابع موجود را ممکن می‌سازد. نرم‌افزاری که RMS را اجرا می‌کند از دو جزء تشکیل شده است: یک مدیر منبع و یک زمان‌بند منبع. بخش مدیر منبع با مسائلی همچون استقرار و تخصیص منابع محاسباتی، تعیین اعتبار و همچنین وظایفی نظیر ایجاد و انتقال پردازش روبرو می‌باشد. بخش زمان‌بند منبع با وظایفی نظیر در صف قرار دادن برنامه‌های کاربردی و همچنین واگذاری و استقرار منابع در ارتباط می‌باشد.

RMS به چند دلیل بوجود آمده است که عبارتند از: توازن بار، بکارگیری چرخه‌های اضافی CPU، ایجاد سیستم‌های تحمل‌پذیر خطا، دستیابی اداره شده به سیستم‌های قدرتمند و غیره. اما دلیل اصلی وجودشان توانایی آن‌ها در ارائه و مهیا نمودن توان عملیاتی افزایشی و قابل اطمینان برنامه‌های کاربردی بر روی سیستم‌هایی است که اداره می‌کنند.

معماری اصلی RMS یک سیستم سرویس‌دهنده – سرویس‌گیرنده است. در ساده‌ترین فرم، هر کامپیوتر که منابع محاسبه‌ای را به اشتراک گذاشته، یک برنامه کمکی سرویس‌دهنده را اجرا می‌کند. این برنامه‌های کمکی، وظیفه نگهداری جدول‌های به روزی را که اطلاعات محیطی، که RMS در آن ساکن می‌باشد را در خود ذخیره می‌کنند، را دارند. یک کاربر

با محیط RMS از طریق یک برنامه سرویس‌گیرنده ارتباط برقرار می‌کند که این محیط می‌تواند یک مرورگر وب یا یک رابط شخصی X-Windows باشد. برنامه کاربردی می‌تواند در حالت محاوره‌ای یا دسته‌ای اجرا شود که حالت دوم بطور رایجتری مورد استفاده قرار می‌گیرد. در حالت دسته‌ای اجرای یک برنامه کاربردی، تبدیل به کاری می‌شود که جهت پردازش تسلیم سیستم RMS می‌گردد. برای تسلیم یک کار دسته‌ای، کاربر باید جزییات کار را برای سیستم سرویس‌گیرنده RMS مهیا سازد. این جزییات ممکن است شامل اطلاعاتی از قبیل، محل مجموعه داده‌های ورودی و قابل اجرا که خروجی استاندارد نیز باید در آنجا مستقر شود، نوع سیستم، حداکثر طول اجرا خواه کار به منابع ترتیبی یا موازی نیاز داشته یا نداشته باشد و غیره، باشند. به محض اینکه کاری به محیط RMS عرضه می‌شود، این محیط از جزییات کار به منظور استقرار، زمان‌بندی و اجرای کار به طریق مناسب بهره می‌گیرد.

محیط‌های RMS خدمات میان‌افزار را به کاربران عرضه می‌دارند تا محیط‌های ناهمگن ایستگاه‌های کاری، SMPها و سکوهای موازی اختصاصی را قادر سازند تا به آسانی و به طور کارآمد مورد استفاده قرار گیرند. خدماتی که توسط یک محیط RMS ارائه می‌شوند، می‌توانند شامل این موارد باشند:

انتقال یا مهاجرت پردازش: این امر در جایی است که یک پردازش می‌تواند معلق شده، انتقال یابد و در کامپیوتر دیگری در داخل محیط RMS مجدداً شروع شود. عموماً، انتقال پردازش به یکی از این دو دلیل زیر انجام می‌شود: یک منبع محاسبه‌ای دارای بار بیش از حد می‌باشد و منابع آزاد دیگری که قابل بهره‌برداری هستند، موجود می‌باشند یا در ارتباط با پردازش کاهش فشار کاربران که در زیر بیان می‌شود.

بررسی و بازدید: این امر وقتی است که فعالیت لحظه‌ای از وضعیت برنامه در حال اجرا ذخیره شود و بعداً در صورت لزوم بتوان از آن برای شروع مجدد برنامه از همان نقطه استفاده کرد. به طور کلی، بررسی و بازدید به عنوان وسیله‌ای برای ایجاد اطمینان در نظر گرفته شده است. زمانی که بخشی از یک محیط RMS از کار می‌افتد، برنامه‌هایی که در آن اجرا می‌شوند، می‌توانند بجای شروع مجدد از نقطه انقطاع، از یک نقطه میانی در اجرایشان شروع شوند.

کشف و بکارگیری سیکل‌های بلااستفاده: کلاً تشخیص داده شده است که بین ۷۰٪ تا ۹۰٪ مواقع، اکثر ایستگاه‌های کاری بیهوده و بلااستفاده هستند. سیستم‌های RMS می‌توانند برای بهره‌گیری از سیکل‌های بلااستفاده پردازنده تنظیم شوند. به عنوان مثال، می‌توان کارها را در طول شب یا آخر هفته به ایستگاه‌های کاری داد. با این شیوه، کارهای خارجی بر کاربران محاوره‌ای تاثیر نمی‌گذارد و سیکل‌های بلااستفاده پردازنده نیز قابل بهره‌برداری می‌شوند.

تحمل‌پذیری خطا: یکی سیستم RMS می‌تواند با کنترل کارها و منابع خود، سطوح گوناگون تحمل‌پذیری در برابر خطا را مهیا سازد. در ساده‌ترین شکل، پشتیبانی از تحمل‌پذیری خطا می‌تواند به این مفهوم باشد که یک کار ناموفق می‌تواند مجدداً آغاز یا اجرا شود بنابراین این تضمین را حاصل می‌کند که بطور کامل انجام خواهد شد.

کاهش برخورد برای کاربران: اجرای یک کار در ایستگاه‌های کاری عمومی می‌تواند اشکالات عمده‌ای را در قابلیت استفاده از ایستگاه‌های کاری بوسیله کاربران محاوره‌ای ایجاد کند. برخی از سیستم‌های RMS می‌کوشند تا تاثیر کار در حال اجرا بر کاربران محاوره‌ای را یا از طریق کاهش اولویت زمان‌بندی محلی یک کار یا از طریق معلق گذاشتن آن، کاهش دهند. کارهای معلق می‌توانند بعدها دوباره شروع شده یا به منابع دیگر در سیستم انتقال یابند.

توازن بار: کارها می‌توانند بین تمامی سکوهای محاسبه‌ای موجود در یک سازمان ویژه، توزیع شوند. این امر امکان استفاده کارآمد و موثر از تمامی منابع، بجای تعداد کمی از آن‌ها که ممکن است تنها منابعی باشند که کاربر از آن‌ها مطلع است، را بوجود خواهد آورد. انتقال پردازش نیز می‌تواند بخشی از استراتژی توازن بار باشد که این استراتژی ممکن است برای انتقال پردازش‌ها از سیستمی که دارای بار بیش از حد است، به سیستم‌های با بار کمتر مورد استفاده قرار گیرد.

صف‌های کاربردی چندگانه: صف‌های کار می‌توانند برای کمک به اداره منابع در یک سازمان خاص بکار برده شوند. هر صف می‌تواند با ویژگی‌های خاصی طراحی شود. برای مثال، کاربران مهم، دارای اولویت اجرای کارهای کوتاه قبل از کارهای طولانی می‌باشند. همچنین صف‌های کار می‌توانند برای اداره استفاده از منابع تخصصی همچون سکوی محاسبه موازی یا یک ایستگاه کاری گرافیکی با کارآیی بالا تنظیم شوند. این صف‌ها در یک سیستم RMS می‌توانند برای کاربران آشکار باشند. کارها از طریق کلمه‌های کلیدی که هنگام ارائه مشخص می‌شوند، به صف‌ها اختصاص می‌یابند.

بسته‌های تجاری و تحقیقاتی فراوانی جهت RMS موجود می‌باشند. لیست تعداد کمی از انواع رایج آن‌ها در جدول شماره ۲ آمده است. چندین مطالعه دقیق از سیستم‌های RMS موجود می‌باشد.

Project	Commercial Systems – URL
LSF	http://www.platform.com/
CODINE	http://www.genias.de/products/codine/tech_desc.html
Easy-LL	http://www.tc.cornell.edu/userDoc/SP/LL12/Easy/
NQE	http://www.cray.com/products/software/nqe
	Public Domain systems – URL
CONDOR	http://www.cs.wisc.edu/condor/
GNQS	http://www.gnqs.org/
DQS	http://www.scri.fsu.edu/~pasko/dqs.html
PRM	http://gost.isi.edu/gost-group/products/prm/
PBS	http://pbs.mrj.com/

جدول شماره ۲: بعضی سیستم‌های رایج مدیریت سیستم

۱۲-۱۲- ابزارها و محیط‌های برنامه‌نویسی

قابلیت دسترسی ابزارهای برنامه‌نویسی استاندارد و همچنین برنامه‌های سودمند،کلاسترها را تبدیل به یک انتخاب عملی بعنوان یک سکوی پردازش موازی، نموده است. در این بخش در مورد تعداد کمی از رایجترین ابزارها بحث می‌کنیم:

۱۲-۱۲-۱- رشته‌ها (Threads)

رشته‌ها، یک الگوی رایج برای برنامه‌نویسی همزمان در ماشین‌های تک‌پردازنده‌ای و نیز ماشین‌های چندپردازنده‌ای می‌باشند. در سیستم‌های چندپردازنده‌ای، رشته‌ها اساساً جهت بکارگیری همزمان از تمامی پردازنده‌های موجود به کار

می‌روند. در سیستمهای تک‌پردازنده‌ای، رشته‌ها برای استفاده موثر از منابع سیستم بکار می‌روند. این امر با بهره‌گیری از رفتار آسنکرون یک برنامه کاربردی برای روی هم انداختن (overlap) قسمت محاسبه و ارتباط حاصل می‌شود. برنامه‌های کاربردی که چندرشته (Multithread) شده‌اند پاسخ سریعتری را به ورودی کاربر ارائه داده و سریعتر اجرا می‌شوند. برخلاف پردازش چندبخشی که به forked معروف است، ایجاد رشته هزینه کمتری داشته و جهت اداره کردن آسان‌تر می‌باشد. رشته‌ها همانطور که داخل فضای آدرس پردازش بالاترشان (parent) بوجود می‌آیند، با استفاده از متغیرهای مشترک ارتباط برقرار می‌کنند.

به دلیل وجود استاندارد IEEE برای رابط رشته‌های POSIX که معمولاً Pthreads نامیده می‌شود، رشته‌ها بطور بالقوه قابل انتقال می‌باشند. رابط چندرشته‌ای استاندارد POSIX در PCها، ایستگاه‌های کاری، SMPها و کلاسترها قابل دسترس و موجود می‌باشد. یک زبان برنامه‌نویسی مانند Java از حمایت چندرشته‌ای در داخل خود بهره‌مند می‌باشد که پیشرفت و توسعه آسان برنامه‌های کاربردی چندرشته‌ای را ممکن می‌سازد. رشته‌ها بطور گسترده‌ای در توسعه برنامه‌های کاربردی و نرم‌افزارهای سیستم، بکار برده می‌شوند.

۱۲-۱۲-۲- سیستم‌های انتقال پیام (MPI و PVM)

مجموعه برنامه‌های انتقال پیام این امکان را ایجاد می‌کنند که برنامه‌های موازی کارآمد برای سیستم‌های حافظه توزیعی نوشته شوند. این مجموعه‌ها یا کتابخانه‌ها روال‌هایی را برای آغاز و طراحی ساختار محیط پیام‌دهی، همچنین ارسال و دریافت بسته‌های اطلاعات عرضه می‌دارند. امروزه، دو نوع از رایجترین سیستم‌های انتقال پیام سطح بالا برای کاربردهای علمی و مهندسی، PVM (ماشین مجازی موازی) از لابراتوار ملی Oak Ridge و MPI (رابط انتقال پیام) که توسط انجمن MPI تعریف شده، می‌باشند.

PVM یک محیط و همچنین مجموعه برنامه یا کتابخانه انتقال پیام است که می‌تواند برای اجرای برنامه‌های کاربردی موازی در سیستم‌هایی که از ابرکامپیوترهای مدل بالا گرفته تا کلاسترهای ایستگاه‌های کاری گسترده شده‌اند، بکار رود. در حالی که MPI ویژگی انتقال پیام می‌باشد، که طوری طراحی شده است تا برای محاسبه موازی حافظه توزیعی که از انتقال صریح پیام استفاده می‌کند، استاندارد باشد. این رابط می‌کوشد تا استانداردی عملی، قابل انتقال، کارآمد و قابل انعطاف برای انتقال پیام بوجود آورد. MPI در اکثر سیستم‌های HPC که شامل دستگاه‌های SMP هستند، موجود می‌باشد.

استاندارد MPI ترکیبی از بهترین بخش‌های سیستم‌های انتقال پیام رایج در زمان طراحی و بوجود آمدنش می‌باشد. این استاندارد نتیجه کار انجمن MPI – هیاتی متشکل از فروشندگان و کاربران که در SC’92 جهت تعریف استاندارد انتقال پیام شکل گرفت – می‌باشد. اهداف طرح MPI عبارت بود از قابلیت انتقال، کارآیی و توان عملیاتی. استاندارد تنها به تعریف مجموعه برنامه انتقال پیام یا کتابخانه می‌پردازد و از میان موارد دیگر، تعیین وضعیت اولیه، آغازسازی و کنترل پردازش‌ها را به سازندگان شخصی واگذار می‌کند. MPI مانند PVM در گستره وسیعی از سکوها، از سیستم‌هایی با کوپل قوی (Tightly Coupled) تا متاکامپیوترها، در دسترس می‌باشد. انتخاب اینکه برای تحقق یک برنامه کاربردی موازی از PVM استفاده شود یا MPI، فراتر از حوزه این تحقیق می‌باشد، اما بطور کلی طراحان برنامه‌های کاربردی، MPI را انتخاب می‌کنند، چرا که سریعاً به استاندارد Defacto در رابطه با انتقال پیام مبدل می‌شود. مجموعه برنامه‌ها یا کتابخانه‌های MPI و PVM در

زبان‌های Fortran 77، Fortran 90، ANSI C و C++، موجود می‌باشند. همچنین رابط‌هایی نیز جهت زبان‌های دیگر وجود دارد. یکی از نمونه‌های این رابط‌ها MPI Java می‌باشد.

۱۲-۱۲-۳- سیستم‌های حافظه اشتراکی توزیعی (DSM)

کارآمدترین و پرکاربردترین الگوی برنامه‌نویسی در سیستم‌های حافظه توزیعی انتقال پیام می‌باشد. مشکلی که در استفاده از این الگو وجود دارد این است که در مقایسه با سیستم‌های برنامه‌نویسی حافظه مشترک، برای برنامه‌نویسی مشکل و پیچیده می‌باشد. سیستم‌های حافظه مشترک یک الگوی برنامه‌نویسی عمومی و ساده ارائه می‌دهند اما از لحاظ مقیاس‌پذیری دارای نقص می‌باشند. یک راه‌حل مقرون به صرفه دیگر، ساخت یک سیستم DSM بر روی سیستم حافظه توزیعی می‌باشد که مدل برنامه‌نویسی کلی و ساده را از یک طرف ارائه داده و مقیاس‌پذیری سیستم‌های حافظه توزیعی را نیز پشتیبانی خواهد کرد.

DSM برنامه‌نویسی متغیر مشترک را ممکن ساخته و می‌توان آن را با استفاده از راه‌حل‌های نرم‌افزاری یا سخت‌افزاری ایجاد نمود. مشخصات سیستم‌های DSM نرم‌افزاری عبارتند از:

- معمولاً به عنوان یک لایه جداگانه در بالای رابط ارتباطی ساخته می‌شوند.
- کاملاً از ویژگی‌های برنامه‌های کاربردی بهره می‌گیرند.
- صفحات مجازی، objectها و نوع زبان‌ها جزو واحدهای به اشتراک گذاشته شده می‌باشند.

DSM نرم‌افزاری می‌تواند صرفاً در هنگام اجرا، در هنگام compile و یا از طریق شیوه‌های ترکیبی پیاده‌سازی شود. دو نمونه از سیستم‌های DSM نرم‌افزاری عبارتند از: TreadMarks و Linda. ویژگی‌های سیستم‌های DSM سخت‌افزاری عبارتند از:

- اجرا و کارآیی بهتر و بالاتر (خیلی سریعتر از DSM نرم‌افزاری).
- عدم ایجاد بار اضافی بر روی کاربران و لایه‌های نرم‌افزاری.
- دانه‌بندی (Granularity) متناسب در رابطه با اشتراک.
- گسترش طرح‌های انسجام حافظه نهان (Cache).
- پیچیدگی سخت‌افزاری افزایش یافته.

دو نمونه از سیستم‌های DSM سخت‌افزاری DASH و Merlin می‌باشند.

۱۲-۱۲-٤- برنامه‌های رفع اشکال و پیش‌نمای (Profiler) موازی

به منظور طراحی و تولید برنامه‌های کاربردی موثر و صحیح با قدرت اجرایی بالا، داشتن روش رفع اشکال موازی که کاربرد آن ساده باشد و همچنین ابزارهای پیش‌نمای اجرا، بسیار مطلوب می‌باشد. اکثر فروشندگان سیستم‌های HPC برنامه‌های رفع اشکال و تحلیل‌گر اجرا را برای سکوهای خود مهیا می‌سازند. بطور ایده‌آل، این ابزارها باید قادر به کار در محیط ناهمگن باشند تا طراحی، توسعه و پیاده‌سازی یک برنامه کاربردی در مثلاً شبکه‌ای از ایستگاه‌های کاری را ممکن سازند و پس از آن، محصولات را بتوان بر روی سکوی HPC اختصاصی نظیر Cray T3E اجرا نمود.

برنامه‌های رفع اشکال

تعداد برنامه‌های اشکال‌زدایی موازی که می‌توانند در یک محیط طراحی ناهمگن با سکوی متقابل مورد استفاده قرار گیرند، بسیار محدود است. بنابراین در سال ۱۹۹۶ اقدامی آغاز شد که یک استاندارد اشکال‌یابی موازی با سکوی متقابل که دارای مشخصه‌ها و رابطی بود که کاربران تقاضا داشتند، را تعریف می‌کرد. انجمن اشکال‌زدایی با کارآیی بالا (HPDF) به عنوان پروژه کنسرسیوم ابزارهای موازی شکل گرفت. این انجمن مشخصات یک نسخه از HPD را آماده کرد که عملکرد، معنا و ترکیب را برای یک برنامه اشکال‌یابی موازی بصورت خط فرمان تولید می‌کرد. بطور ایده‌آل، یک برنامه اشکال‌زدایی موازی باید بتواند امور زیر را انجام دهد:

- اداره چندین پردازش و چندین رشته درون یک پردازش
- نمایش هر پردازش در پنجره خود
- نمایش کد اصلی، ردیابی پشته و قالب پشته برای یک یا تعداد بیشتری پردازش
- توانایی جستجو در objectها، زیرروال‌ها و توابع
- قرار دادن نقاط توقف در سطح کد اصلی و دستگاه
- اشتراک نقاط توقف بین گروهی از پردازش‌ها
- تعریف نقاط مشاهده و ارزیابی
- نمایش آرایه‌ها و قطعات آن‌ها
- کنترل ماهرانه مقادیر ثابت و متغیر در کد

TotalView

TotalView محصولی تجاری از Dolphin Interconnect Solutions است که امروزه تنها برنامه اشکال‌یابی موازی بر مبنای رابط کاربر گرافیکی بوده و بطور گسترده‌ای در دسترس می‌باشد. این محصول از سکوهای HPC چندگانه نیز حمایت به عمل می‌آورد. TotalView از بیشتر زبان‌های علمی متداول (C، C++، Fortran 77 / 90 و HPC)، مجموعه برنامه‌های انتقال پیام (MPI و PVM) و سیستم‌عامل‌ها (Solaris، Sun OS، IBM AIX، Digital Unix و SGI IRIX) پشتیبانی می‌کند. با اینکه TotalView می‌تواند در چندین سکو اجرا شود، تنها در محیط‌های همگن بکار می‌رود، به این مفهوم که بطور عمده هر پردازش برنامه کاربردی موازی که اشکال‌زدایی شده باید تحت همان نسخه از سیستم‌عامل به اجرا در آید.

۱۲-۱۲-۵- ابزارهای بررسی کارآیی

هدف اساسی ابزارهای بررسی اجرا و کارآیی کمک به برنامه نویس جهت فهم مشخصات اجرایی یک برنامه کاربردی می‌باشد. بخصوص این ابزارها باید بخش‌هایی از یک برنامه کاربردی را که اجرای ضعیفی از خود نشان داده و تنگناهای برنامه را ایجاد می‌کنند تجزیه تحلیل کرده و محل آن‌ها را پیدا کنند. چنین ابزارهایی برای درک عملکرد برنامه‌های کاربردی ترتیبی معمولی مفیدند و می‌توانند زمانی که سعی در تجزیه و تحلیل مشخصات اجرایی برنامه‌های کاربردی موازی داریم، بسیار یاری‌رسان و سودمند باشند. اکثر ابزارهای کنترل و مونیتورینگ اجرا از برخی یا تمامی بخش‌های صفحه بعد تشکیل شده‌اند:

- وسیله‌ای برای وارد ساختن فراخوآن‌های واسطه به روال‌های کنترل اجرا در داخل برنامه کاربردی کاربر.
- یک مجموعه برنامه یا کتابخانه در رابطه با کارآیی زمان اجرا که متشکل است از یک سری روال‌های کنترل‌کننده که جنبه‌های گوناگون اجرای یک برنامه را اندازه‌گیری و ضبط می‌کنند.
- یک سری ابزار برای پردازش و نمایش داده‌های اجرایی.

یک موضوع خاص در مورد ابزارهای کنترل اجرا، نفوذ فراخوآن‌های ردیاب و تاثیر آن‌ها بر اجرای برنامه‌های کاربردی می‌باشد. توجه به این نکته بسیار مهم است که ابزارهای واسطه بر مشخصات اجرایی برنامه کاربردی موازی تاثیر گذاشته و در نتیجه نگرشی نادرست از عملکرد آن فراهم می‌سازند. جدول شماره ۳ معمولترین ابزارهای بکار گرفته شده جهت تجزیه و تحلیل اجرای برنامه‌های انتقال پیام را نشان می‌دهد.

۱۲-۱۲-۶- ابزارهای اداره کردن کلاستر

کنترل و مونیتور کردن کلاسترها، کاری است دشوار که می‌تواند بوسیله ابزارهایی که امکان می‌دهند تا تمامی کلاسترها را در سطوح مختلف از طریق یک رابط کاربر گرافیکی مشاهده نمود، سهل و آسان گردد. نرم‌افزار مدیریت خوب برای بهره‌گیری از یک کلاستر بعنوان یک سکو محاسبه‌ای با توانایی بالا، ضروری می‌باشد.

پروژه‌های بسیاری وجود دارند که در مورد اداره سیستم در کلاسترها که از محاسبات موازی پشتیبانی به عمل می‌آورند، تحقیق می‌کنند؛ از جمله این پروژه‌ها می‌توان به Berkeley NOW، SMILE که مخفف کلمات Scalable Multicomputer Implementation using Low-cost Equipment است و PARMON اشاره نمود. ابزار اداره سیستم در Berkeley NOW، اطلاعات را جمع‌آوری کرده و در یک پایگاه داده‌های رابطه‌ای ذخیره می‌کند. این ابزار از یک Java applet استفاده می‌کند تا برای کاربران امکان کنترل یک سیستم از سوی مرورگرشان را فراهم سازد. ابزار اداره SMILE را K-Cap می‌نامند. محیط آن متشکل از گره‌های محاسبه‌ای (که کارهای محاسبه‌ای فشرده را اجرا می‌کنند)، یک گره مدیریت (یک سرویس‌دهنده فایل و مدیر کلاستر و همچنین یک کنسول مدیریت) و یک سرویس‌گیرنده که می‌تواند کلاستر را کنترل کند، می‌باشد. K-Cap از یک Java applet به منظور اتصال به گره مدیریت از طریق یک آدرس URL از پیش تعریف شده در کلاستر استفاده می‌کند.

Tool	Supports	URL
AIMS	Instrumentation , monitoring library, analysis	http://science.nas.nasa.gov/Software/AIMS
MPE	Logging library and snapshot performance visualization	http://www.msc.anl.gov/mpi/mpich
Pablo	monitoring library and analysis	http://www-pablo.cs.uiuc.edu/Projects/Pablo/
Paradyn	Dynamic instrumentation runtime analysis	http://www.cs.wisc.edu/paradyn
SvPablo	Integrated instrumentor, monitoring library and analysis	http://www-pablo.cs.uiuc.edu/Projects/Pablo/
Vampir	Monitoring library performance visualization	http://www.pallas.de/pages/vampir.htm
Dimemas	Performance prediction for message passing programs	http://www.pallas.com/pages/dimemas.htm

Paraver	Program visualization and analysis	http://www.cepba.upc.es/paraver

جدول شماره ۳: ابزارهای ارزیابی و مشاهده کارآیی و اجرا

گزارشگر وضعیت گره (NSR)، مکانیزمی استاندارد برای اندازه‌گیری و دستیابی به اطلاعات وضعیت کلاسترها مهیا می‌کند. ابزارها و برنامه‌های کاربردی موازی می‌توانند از طریق رابط NSR به NSR دست یابند. PARMON یک محیط وسیع برای کنترل کلاسترهای بزرگ است که از تکنیک‌های سرویس‌دهنده – سرویس‌گیرنده جهت فراهم آوردن دسترسی شفاف به تمام گره‌هایی که باید کنترل شوند، استفاده می‌کند. دو جزء بزرگ PARMON عبارتند از: parmon سرویس‌دهنده (فراهم‌آورنده فعالیت‌های منبع سیستم و تامین‌کننده اطلاعات بکارگیری) و parmon سرویس‌گیرنده (یک Java applet یا برنامه کاربردی که قادر به جمع‌آوری و نشان دادن اطلاعات کلاستر بصورت همزمان می‌باشد).

۱۲-۱۳- موارد کاربردی کلاستر

قبلاً در بخش‌های گذشته این تحقیق در مورد دلایل اینکه چرا مایلیم یک کلاستر اجرایی سطح بالا را بوجود آوریم تا یک سکوی محاسبه‌ای برای تمامی انواع کاربردهای موازی و توزیعی فراهم سازد، بحث نمودیم. کلاس برنامه‌های کاربردی که یک کلاستر معمولاً با آن‌ها سر و کار دارد، کاربردهای چالشی عظیم یا فوق محاسبه‌ای نامیده می‌شوند. GCAها (کاربردهای چالشی عظیم) مشکلات اساسی در علم و مهندسی همراه با تاثیر علمی و اقتصادی گسترده می‌باشند. بطور کلی آن‌ها بدون استفاده از کامپیوترهای موازی با جدیدترین تکنولوژی، غیر قابل کنترل و اجرا شناخته می‌شوند. میزان نیازهای منبع آن‌ها نظیر زمان پردازش، حافظه و نیازهای ارتباطی باعث تمایز GCAها شده است.

یک مثال معمولی از یک مسئله مبارزه بزرگ یا چالشی عظیم، شبیه‌سازی برخی پدیده‌هایی است که از طریق تجربه قابل اندازه‌گیری نیستند. GCAها شامل مسائل ساختاری بلورشناسی و Microtomographic، دینامیک پروتئین و بیوکاتالیزها، شیمی کوانتومی نسبیت آکتنیدها، تولید فرآیند و طراحی مواد مجازی، مدل‌سازی آب و هوای جهان و شبیه‌سازی رویدادهای مجزا، می‌باشند.

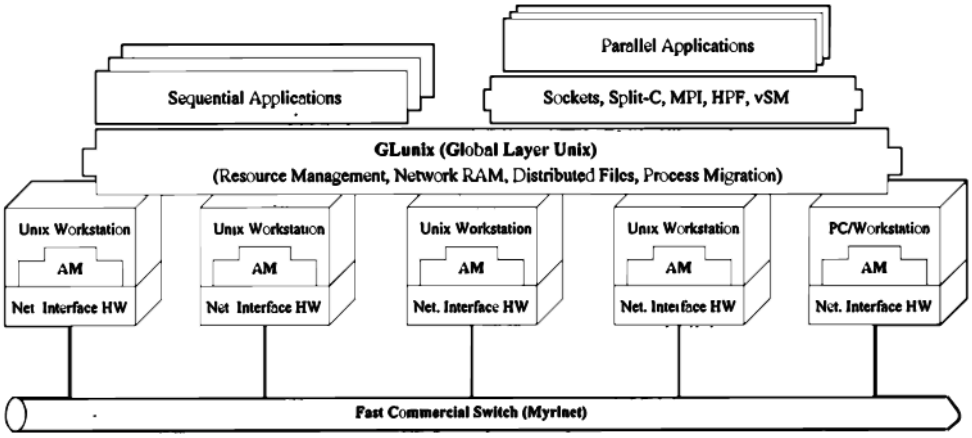
۱۲-۱٤- سیستم‌های کلاستری نمونه

پروژه‌های بسیاری موجود می‌باشند که راجع به توسعه ماشین‌های ابرمحاسبه‌ای که از اجزای آماده استفاده، سود می‌برند، تحقیق می‌کنند. ما بطور خلاصه به شرح اقدامات مشهور ذیل می‌پردازیم:

- پروژه شبکه ایستگاه‌های کاری (NOW) در دانشگاه کالیفرنیا، برکلی.
- پروژه ماشین مجازی با کارآیی بالا در انشگاه ایلینویز در Urbana-Champaign.
- پروژه Beowulf در مرکز هوافضای Goddard مربوط به ناسا.
- پروژه Solaris-MC در Sun Labs مربوط به شرکت Sun Microsystems واقع در Palo Alto , CA.

۱۲-۱٤-۱- پروژه شبکه ایستگاه‌های کاری بِرکلی (Berkeley NOW)

پروژه Berkeley NOW ساختمان یک سیستم محاسبه‌ای موازی با مقیاس بزرگ را نشان می‌دهد که از ایستگاه‌های کاری تجاری که تولید انبوه می‌شوند و جدیدترین قطعات شبکه بر اساس سوئیچ، بهره می‌گیرد. به منظور رسیدن به هدف ترکیب ایستگاه‌های کاری توزیعی و تبدیل آن به یک سیستم واحد، پروژه NOW شامل تحقیق و توسعه در رابطه با سخت‌افزار رابط شبکه، پروتکل‌های ارتباط سریع، سیستم‌های فایل توزیعی، زمان‌بندی توزیعی و کنترل کار می‌باشد. معماری سیستم NOW در شکل شماره ٥ نشان داده شده است.



شکل شماره ٥: معماری سیستم NOW

ارتباط بین پردازش‌ها

پیام‌های فعال (AM) از primitiveهای اصلی ارتباطات در پروژه Berkeley NOW می‌باشند. پیام‌های فعال رابط‌های AM قبلی را تعمیم داده است تا طیف وسیعتری از برنامه‌های کاربردی نظیر برنامه‌های سرویس‌دهنده – سرویس‌گیرنده، سیستم‌های فایلی و سیستم‌عامل‌ها را حمایت کند و برای برنامه‌های موازی نیز پشتیبانی مداومی را ارائه دهد. ارتباط AM اساساً یک فراخوانی زیرروال از راه دور ساده شده می‌باشد که می‌تواند در طیف وسیعی از سخت‌افزارها بطور موثری پیاده‌سازی شود. NOW شامل مجموعه‌ای از Primitiveهای ارتباط موازی با تاخیر کم است که شامل: سوکت‌های Berkeley، سوکت‌های Fast، زبان C موازی با فضای آدرس‌دهی مشترک (Split-C) و MPI می‌باشند.

لایه سراسری Unix (GLUnix)

GLUnix یک لایه سیستم‌عامل است که به منظور فراهم آوردن اجرای شفاف از راه دور، حمایت از کارهای ترتیبی و موازی محاوره‌ای،توازن بار و سازگاری با اجزای برنامه‌های کاربردی موجود، طراحی شده است. GLUnix یکی سیستم چند کاربره است که در سطح کاربر پیاده‌سازی می‌شود تا به راحتی به تعدادی از سکوهای مختلف منتقل شود. هدف GLUnix مهیا ساختن یک فضای نام گسترده در کلاستر است و از PIDهای شبکه (NPIDs) و شماره‌های گره مجازی (VNNs) استفاده می‌کند. NPIDها شناسه‌های پردازش واحد بصورت سراسری برای برنامه‌های موازی و ترتیبی در سراسر سیستم می‌باشند. VNNها به منظور تسهیل ارتباطات میان پردازش‌های یک برنامه موازی بکار می‌روند. در اینجا از یک سری ابزارهای کاربر برای بکارگیری و اداره NPIDها و VNNها که معادل run، kill و غیره در Unix می‌باشند، حمایت می‌شود. یک GLUnix API امکان بکارگیری و ارتباط با NPIDها و VNNها را فراهم می‌سازد.

RAM شبکه

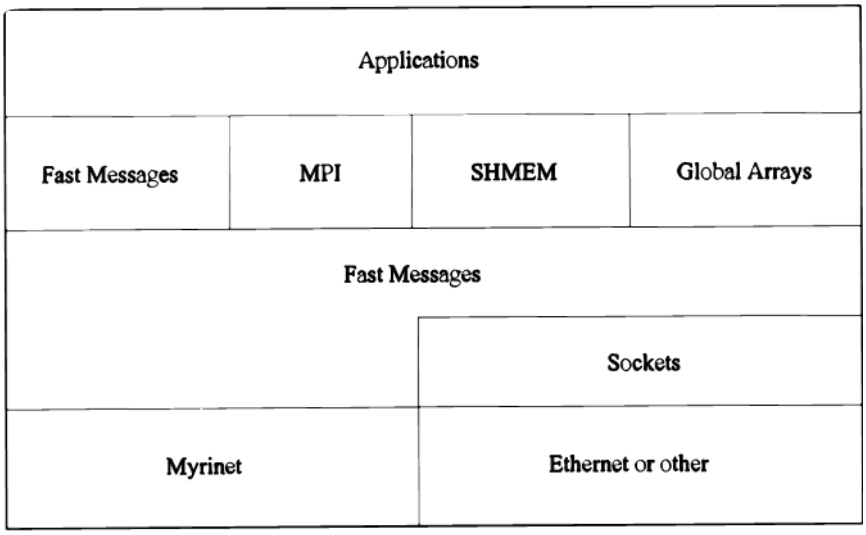
RAM شبکه این امکان را برای ما فراهم می‌سازد تا از منابع آزاد روی ماشین‌های بلااستفاده به عنوان یک دستگاه فراخوانده شده برای ماشین‌های پرکار استفاده کنیم. سیستم طراحی شده، بدون سرویس‌دهنده می‌باشد و هر ماشینی می‌تواند در زمان بیکاری یک سرویس‌دهنده باشد و یا می‌تواند در زمان نیاز به حافظه بیشتر نسبت به آنچه که از لحاظ فیزیکی در دسترس است، یک سرویس‌گیرنده باشد. دو سیستم نمونه طراحی و معرفی شده‌اند. یکی از آن‌ها از راه‌انداز قطعه Solaris برای پیاده‌سازی یک فراخواننده خارجی در سطح کاربر بهره می‌گیرد که این راه‌انداز صفحات را با برنامه‌های کمکی صفحه‌ای از راه دور تعویض می‌کند. سیستم دیگر با استفاده از signal عملیات مشابهی را بر روی نواحیی که به همان طریق نگاشته شده‌اند، ارائه می‌دهد.

xFS: سیستم فایل شبکه بدون سرویس‌دهنده

xFS یک سیستم فایل توزیعی و بدون سرویس‌دهنده می‌باشد که می‌کوشد تا با توزیع عملیات سرویس‌دهنده میان سرویس‌گیرندهها دسترسی با تاخیر پایین و پهنای باند بالا به داده‌های سیستم فایل را فراهم سازد. وظایف نمونه یک سرویس‌دهنده شامل حفظ انسجام حافظه پنهان (Cache)، استقرار و تعیین مکان داده‌ها و تامین نیازهای دیسک می‌باشند. عمل تعیین مکان و استقرار داده‌ها در xFS بوسیله مسئول بودن هر سرویس‌گیرنده برای تامین نیازها در یک زیرمجموعه از فایل‌ها، بین آن‌ها توزیع شده است. جهت دسترسی به پهنای باند بالا، داده فایل از روی چندین سرویس‌گیرنده بدست می‌آید.

۱۲-۱٤-۲- پروژه ماشین مجازی با کارآیی بالا (HPVM)

هدف پروژه HPVM انتقال کارآیی ابرکامپیوتر به یک سیستم ارزان قیمت قابل استفاده (COTS) می‌باشد. همچنین پروژه HPVM، پنهان کردن پیچیدگی‌های یک سیستم توزیعی در ورای یک رابط شفاف را هدف قرار داده است. این پروژه، نرم‌افزاری را مهیا می‌کند که محاسبات با توانایی بالا را روی کلاسترهای کامپیوترهای شخصی و ایستگاه‌های کاری، ممکن می‌سازد. معماری HPVM (شکل شماره ٦) از تعدادی بخش‌های نرم‌افزاری با رابط برنامه کاربردی سطح بالا نظیر MPI، SHMEM و آرایه‌های سراسری تشکیل یافته است، که این بخش‌ها به کلاسترهای HPVM امکان می‌دهند تا با سیستم‌های MPP اختصاصی رقابت کنند.



شکل شماره ٦: معماری لایه‌ای HPVM

پروژه HPVM پرداختن به مسائل زیر را هدف قرار داده است:

- تحویل ارتباطات با توان اجرایی بالا به APIهای سطح بالا و استاندارد
- هماهنگ نمودن زمان‌بندی و مدیریت منبع
- مدیریت عدم تجانس (Heterogeneity)

یک بخش حیاتی و مهم از HPVM، پروتکل ارتباطی با پهنای باند زیاد و تاخیر کم است که بر اساس Berkeley AM عمل کرده و به عنوان پیام‌های سریع (FM) شناخته می‌شود. برخلاف لایه‌های پیام‌دهی دیگر، FM، رابط برنامه کاربردی سطحی نمی‌باشد بلکه در زیرساختار قرار دارد. FM دربرگیرنده توابعی برای ارسال پیام‌های کوتاه و بلند و استخراج پیام از شبکه می‌باشد. خدماتی که توسط FM ارائه می‌شوند، سلسله مراتب حافظه که FM آن‌ها را برای نرم‌افزاری که با خود او ساخته شده فراهم می‌سازد، را تضمین و کنترل می‌کنند. همچنین FM ارسال قابل اطمینان و به ترتیب بسته‌ها و همینطور کنترل زمان‌بندی عمل ارتباط را تضمین می‌کند.

رابط FM در اصل بر روی یک Cray T3D و کلاستری از ایستگاه‌های Sparc که توسط سخت‌افزار Myrinet به هم متصل شده بودند، پیاده‌سازی شد. سخت‌افزار Myricom's Myrinet یک کارت رابط شبکه قابل برنامه‌نویسی است که قادر به ارائه اتصالات ۱٦۰ مگابایت در ثانیه با تاخیرهای سوئیچ زیر یک میکروثانیه می‌باشد. FM دارای یک رابط نرم‌افزاری سطح پایین است که اجرای ارتباط سخت‌افزاری را حمل می‌کند؛ با این حال رابط لایه‌های سطح بالاتر عملکرد بیشتر، قابلیت انتقال برنامه‌های کاربردی و سهولت استفاده را ارائه می‌دهد.

۱۲-۱٤-۳- پروژه *Beowulf*

هدف پروژه Beowulf، تحقیق در مورد پتانسیل کلاسترهای کامپیوترهای شخصی برای اجرای کارهای محاسبه‌ای بود. Beowulf به دسته‌ای از کامپیوترهای شخصی (PoPC) اطلاق می‌شود که بصورت کلاستری از کامپیوترهای شخصی می‌باشند و بسیار شبیه به COW / NOW هستند. PoPC بر استفاده از اجزای تولید انبوه در بازار، پردازنده‌های اختصاصی (به جای استفاده از سیکل‌های ایستگاه‌های کاری بلااستفاده) و استفاده از یک شبکه ارتباطی خصوصی تاکید دارد. یک هدف کلی Beowulf، کسب بهترین نسبت هزینه / کارآیی سیستم برای یک کلاستر است.

نرم‌افزار سیستمی

مجموعه ابزارهای نرم‌افزاری که در پروژه Beowulf توسعه و تحول یافته‌اند، به عنوان Grendel شناخته می‌شود. این ابزارها برای مدیریت منبع و پشتیبانی کاربردهای توزیعی بکار می‌روند. توزیع Beowulf شامل چندین محیط برنامه‌نویسی و مجموعه برنامه‌های (کتابخانه‌های) توسعه به صورت بسته‌های جداگانه می‌باشد. این موارد شامل PVM، MPI و BSP و همچنین SYS V-Style IPC و Pthreads می‌باشند.

ارتباط بین پردازنده‌ها در Beowulf از طریق TCP/IP و بر روی اترنتی که در داخل کلاستر است، صورت می‌پذیرد. بنابراین کارآیی ارتباطات میان‌پردازنده‌ای توسط ویژگی‌های اجرایی اترنت و نرم‌افزار سیستمی که انتقال پیام را اداره می‌کند، محدود می‌شود. از Beowulf برای بررسی امکان بکارگیری چندین شبکه اترنت بصورت موازی جهت بدست آوردن پهنای

باند مورد نیاز برای انتقال داده‌ها بصورت داخلی، استفاده می‌شود. هر ایستگاه کاری در Beowulf دارای دسترسی شفاف کاربر به شبکه‌های اترنتی موازی چندگانه می‌باشد. این معماری بوسیله تکنیک‌های " چسباندن کانال (Channel bonding) " حاصل می‌شود که به عنوان پیشرفت‌هایی برای هسته Linux پیاده‌سازی می‌شوند. پروژه Beowulf نشان داده است که بیش از سه شبکه می‌توانند با هم متحد شوند تا توان عملیاتی چشمگیری را بدست آورند بنابراین به بکارگیری تکنیک چسباندن کانال اعتبار می‌بخشند. تکنولوژی‌های جدید شبکه مانند اترنت سریع، حتی کارآیی بهتر ارتباطات میان پردازنده‌ای را تضمین می‌کنند.

به دلیل ارائه یک تصویر سیستم واحد به کاربران و برنامه‌های کاربردی، Beowulf هسته Linux را گسترش داده است تا این امکان را برای مجموعه بدون انسجام گره‌ها فراهم سازد تا در تعدادی از فضای نام‌های سراسری سهیم شوند. در اغلب موارد در یک طرح توزیع‌شده، داشتن یک PID که در سرتاسر یک کلاستر واحد می‌باشد و چندین هسته را می‌پوشاند، برای پردازش‌ها مفید خواهد بود. Beowulf دو طرح شناسه سراسری پردازش (GPID) را پیاده‌سازی می‌کند. اولین طرح مستقل از مجموعه برنامه‌های (کتابخانه‌های) خارجی می‌باشد و دومین طرح که GPID-PVM نام دارد برای سازگاری با قالب شناسه کاری PVM طراحی شده و PVM را به عنوان وسیله حمل و نقل سیگنال خود مورد استفاده قرار می‌دهد. در حالی که گسترش GPID برای کنترل در سطح کلاستر و اشاره کردن به پردازش‌ها موثر می‌باشد، اما بدون دید سراسری، پردازش‌ها دارای کاربرد اندکی خواهند بود. به منظور رسیدن به این هدف، پروژه Beowulf مکانیزمی را توسعه و ارائه می‌دهد که به برنامه‌های سودمند نسخه‌های بدون تغییر Unix استاندارد (مانند ps) امکان می‌دهد تا بر روی یک کلاستر کار کنند.

۱۲-۱٤-٤- Solaris MC: یک سیستم عامل با توانایی اجرایی سطح بالا برای کلاستر

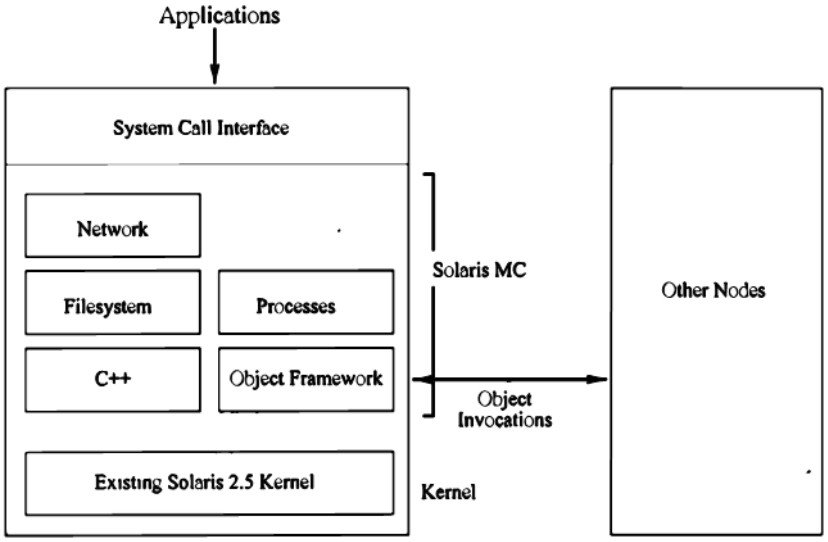
Solaris MC (MC به معنای چندین کامپیوتر می‌باشد) یک سیستم عامل توزیع شده برای یک سیستم چند کامپیوتری، یعنی کلاستری از گره‌های محاسبه‌ای که بوسیله یک ارتباط سرعت بالا بهم متصلند، می‌باشد. این سیستم‌عامل یک تصویر سیستم منفرد را ارائه می‌دهد که باعث می‌شود کلاستر مانند یک ماشین منفرد برای کاربر، کاربردها و شبکه به نظر آید. Solaris MC به عنوان یک لایه سراسری (پوشا) بر روی هسته Solaris موجود، همانگونه که در شکل شماره ۷ نشان داده شده است، ساخته می‌شود. Solaris MC مدل انتزاعی سیستم‌عامل را از روی کلاستر توسعه بخشیده و Solaris ABI/APIموجود را حفظ می‌کند و در نتیجه برنامه‌های کاربردی Soalaris 2.x و راه‌اندازهای ابزار موجود را بدون تغییر اجرا می‌کند. Solaris MC از بخش‌های متعددی تشکیل یافته است که عبارتند از: زبان C++ و چارچوب شیءگرا ؛ و پردازش سراسری، سیستم فایل و شبکه‌بندی.

مشخصه‌های جالب Solaris MC شامل موارد زیر می‌باشند:

- گسترش سیستم‌عامل Solaris موجود
- حفظ توافق Solaris ABI/API موجود
- فراهم ساختن پشتیبانی برای قابلیت دسترسی بالا
- کاربرد زبان C++، IDL و CORBA در هسته اصلی
- بکارگیری تکنولوژی Spring

Solaris MC از یک چارچوب شیءگرا برای ارتباط بین گره‌ها استفاده می‌کند. این چارچوب شیءگرا بر پایه CORBA بوده و فراخوانی‌ها را به روش object راه دور، مهیا می‌سازد. این روش برای برنامه‌نویسان مانند فراخوانی‌ها در C++ استاندارد، به نظر می‌آید. این چارچوب فرضیه مرجع شیءای را ارائه می‌کند که عبارت است از: زمانی که هیچ مرجع دیگری (محلی یا راه دور) برای شیء موجود نباشد، اطلاعیه‌ای برای سرویس‌دهنده شیء ارسال خواهد شد. مشخصه دیگر چارچوب شیءای Solaris MC این است که از چندین اداره‌کننده شیء حمایت می‌کند.

یک جزء کلیدی در تایید تصویر یک سیستم منفرد در Solaris MC، سیستم فایل سراسری می‌باشد. این سیستم، دسترسی نامتناقض (Consistent) را از چندین گره به فایل‌ها و ویژگی‌های آن‌ها مهیا ساخته و از حافظه نهان (Cache) برای اجرا و کارآیی بالا، بهره می‌گیرد. این سیستم از یک سیستم فایل توزیعی جدید که سیستم فایل ProXy (PXFS) نامیده می‌شود استفاده می‌کند که یک سیستم فایل سراسری را بدون نیاز به تغییر سیستم فایل موجود ارائه می‌دهد.



شکل شماره ۷: معماری Solaris MC

دومین جزء مهم Solaris MC که از یک تصویر سیستم واحد پشتیبانی می‌کند، مدیریت پردازش سراسری آن است. این جزء عملیات پردازشی نظیر signalها را سراسری می‌کند. همچنین سیستم فایل proc/ را نیز جهت مهیا نمودن دسترسی به وضعیت پردازش برای فرمآن‌هایی نظیر " PS " و برنامه‌های اشکال‌زدایی، سراسری می‌کند. همچنین از اجرای راه دور که امکان آغاز پردازش‌های جدید روی هر گره در سیستم را فراهم می‌سازد، نیز پشتیبانی به عمل می‌آورد.

Solaris MC همچنین پشتیبانی خود جهت ایجاد شبکه و ورودی – خروجی را نیز سراسری می‌کند. امکان اتصال بیش از یک شبکه را فراهم کرده و از عمل مالتی‌پلکس اختیاری بین اتصالات شبکه حمایت می‌کند.

۱۲-۱۴-۵- مقایسه چهار محیط کلاستری

پروژه‌های کلاستر که در این تحقیق به آن‌ها اشاره شد، در هدف عمومی که تلاش برای ارائه یک منبع واحد از میان کامپیوترهای شخصی مرتبط یا ایستگاه‌های کاری است، سهیم می‌باشند. هر سیستم مدعی است که می‌تواند منابع ابرکامپیوتری را از اجزای COTS فراهم آورد. هر پروژه این منابع را به روش‌های گوناگونی ارائه می‌کند، در واقع هم از جهت چگونگی

ارتباط سخت‌افزار به یکدیگر و هم روشی که نرم‌افزار سیستم و ابزارها، خدمات را برای برنامه‌های کاربردهای موازی ارائه می‌دهند.

جدول شماره ٤ اجزای اصلی سخت‌افزاری و نرم‌افزاری که در هر سیستم استفاده می‌شوند را، نشان می‌دهد. Beowulf و HPVM قادر به استفاده از هر کامپیوتر شخصی می‌باشند، در حالی که پروژه Berkeley NOW و Solaris MC در سکوهایی عمل می‌کنند که Solaris در آنجا در دسترس باشد - در حال حاضر کامپیوترهای شخصی، ایستگاه‌های کاری شرکت Sun و سیستم‌های گوناگون همخوان با آن‌ها شامل این موارد می‌باشند. Berkeley NOW و HPVM از Myrinet با پروتکل ارتباطات سطح پایین و سریع (پیام‌های سریع و فعال) استفاده می‌کنند. Beowulf از چندین اترنت استاندارد بهره می‌گیرد و Solaris MC از NIC هایی که توسط Solaris حمایت می‌شوند و دامنه گسترش آن‌ها از اترنت تا ATM و SCI می‌باشد، استفاده می‌کند.

Project	Platform	Communications	OS	Other
Beowulf	PCs	Multiple Ethernet with TCP/IP	Linux and Grendel	MPI/PVM, Sockets and HPF
Berkeley NOW	Solaris-based PCs and workstations	Myrinet and Active Messages	Solaris + GLUnix + xFS	AM, PVM, MPI, HPF, Split-C
HPVM	PCs	Myrinet with Fast Messages	NT or Linux connection and global resource manager + LSF	Java-fronted, FM, Sockets, Global Arrays, SHMEM and MPI
Solaris MC	Solaris-based PCs and workstations	Solaris-supported	Solaris + Globalization layer	C++ and CORBA

جدول شماره ٤: مقایسه سیستم‌های کلاستری

هر سیستم از برخی میان‌افزارها تشکیل یافته است که به هسته سیستم‌عامل متصلند و برای فراهم ساختن یک لایه سراسری یا نگرش واحد از منابع توزیعی کلاستر، بکار می‌روند. پروژه Berkeley NOW از سیستم‌عامل Solaris استفاده می‌کند، در حالی که Beowulf از Linux همراه با یک هسته تغییریافته بهره می‌گیرد و HPVM نیز در دسترس Linux و هم در دسترس Windows NT می‌باشد. تمامی این چهار سیستم‌عامل تنوع گسترده‌ای از ابزارها و برنامه‌های کمکی را ارائه می‌دهند که معمولاً برای توسعه، آزمایش و اجرای کاربردهای موازی بکار می‌روند. این موارد شامل APIهای گوناگون سطح بالا برای انتقال پیام و برنامه‌نویسی حافظه مشترک می‌باشند.

۱۲-۱۵- کلاستری از *SMP*ها (*CLUMPS*)

پیشرفت در تکنولوژی‌های سخت‌افزاری در زمینه پردازنده‌ها، حافظه و رابط‌های شبکه، قابلیت دسترسی به ماشین‌های SMP حافظه مشترک با پیکربندی کوچک و ارزان قیمت (۲ تا ۸ پردازنده) را ممکن ساخته است. همچنین مشاهده می‌شود

که کلاسترهای چندپردازنده‌ها (CLUMPS) نوید می‌دهند که ابرکامپیوترهای آینده باشند. در CLUMPS، چندین SMP همراه با چندین رابط شبکه می‌توانند با استفاده از شبکه‌هایی با کارآیی و توانایی بالا به یکدیگر متصل شوند.

این امر دو مزیت را در بر دارد: بهره بردن از سیستم‌های SMP با تعداد کمی پردازنده و با کارآیی بالا و کاربرد و برنامه‌ریزی آسان، امکان‌پذیر است. علاوه بر این، کلاسترها می‌توانند با کمی تلاش نصب شوند (مثلاً یک کلاستر با ۳۲ پردازنده می‌تواند با بکارگیری هشت SMP ٤ پردازنده‌ای یا با چهار SMP ۸ پردازنده‌ای که عموماً قابل دستیابی هستند، بجای ۳۲ ماشین تک پردازنده‌ای، ساخته شود)، که اجرای آسان‌تر و پشتیبانی بهتری را برای محلی‌سازی داده‌ها درون یک گره به ارمغان می‌آورد.

این روند، نیاز تازه‌ای را برای ارتباط‌های درونی کلاستر معرفی می‌کند. برای مثال، یک NIC منفرد برای یک سیستم ۸ پردازنده‌ای کافی نخواهد بود و نیاز به چندین دستگاه شبکه را، ضروری می‌کند. علاوه بر این، لایه‌های نرم‌افزاری باید مکانیزم‌های مختلفی را برای انتقال داده‌ها پیاده‌سازی کنند (از طریق حافظه مشترک درون یک گره SMP و شبکه به گره‌های دیگر).

۱۲-۱٦- خلاصه و نتایج

در این فصل در مورد اجزای نرم‌افزاری و سخت‌افزاری گوناگون که عموماً در نسل حاضر سیستم‌های کلاستری استفاده می‌شوند، بحث نمودیم. همچنین به شرح چهار پروژه با جدیدترین تکنولوژی‌ها پرداختیم که به طرز ماهرآنه‌ای از دیدگاه‌های مختلفی که گستره آن‌ها از یک دیدگاه All-COTS تا ترکیبی از تکنولوژی‌های مختلف گسترده شده بود، استفاده می‌کردند. در این بخش یافته‌های خود را خلاصه کرده و نظراتی راجع به روندهای احتمالی آینده ارائه می‌دهیم.

۱۲-۱٦-۱- روندهای رشد نرم‌افزار و سخت‌افزار

در ۵ سال گذشته پیشرفت‌های مهمی صورت گرفته است که بارزترین آن‌ها عبارتند از:

- کارآیی شبکه با استفاده از پشتیبانی اترنت 100BaseT که کاملاً دو طرفه می‌باشد تا ۱۰ برابر افزایش یافته است.
- قابلیت دسترسی به مدارهای شبکه سوئیچی که شامل سوئیچ‌های full crossbar برای تکنولوژی‌های شبکه اختصاصی مانند Myrinet می‌باشند.
- کارآیی ایستگاه‌های کاری بطور چشمگیری افزایش پیدا کرده است.
- پیشرفت عملکرد ریزپردازنده به قابلیت دسترسی به کامپیوترهای شخصی رومیزی با عملکردی مشابه ایستگاه‌های کاری کم سرعت ولی بطور چشمگیری با قیمت پایین‌تر، منجر شده است.
- قابلیت دستیابی به سیستم‌عامل‌های سریع، با قابلیت عملیاتی و پایدار (Linux) با دسترسی به کد مبداء (Source) آن‌ها برای کامپیوترهای شخصی.
- شکاف اجرایی بین ابرکامپیوتر و کلاسترهای بر مبنای محصول به سرعت از بین می‌رود.
- ابرکامپیوترهای موازی هم‌اکنون به اجزای COTS بخصوص ریزپردازنده‌ها (DEC Alpha، Cray T3E، SGI) مجهز می‌باشند، در حالی که سیستم‌های قدیمی‌تر دارای قطعات سفارشی و شخصی بودند.

- افزایش کاربرد گره‌های SMP با دو الی چهار پردازنده.

گروهی از روندهای رشد سخت‌افزاری در بالا نشان داده شدند. مهمترین آن‌ها طرح و تولید ریزپردازنده‌ها می‌باشد. یک پیشرفت اساسی، کاهش اندازه ظاهری است که مدارها را قادر می‌سازد تا سریعتر کار کرده یا نیروی کمتری را صرف نمایند. همراه با این، رشد اندازه die می‌باشد که قابل تولید خواهد بود. این عوامل به این معناست که:

- متوسط تعداد ترانزیستورها بر روی یک تراشه تا حدود ٤٠ درصد در سال، در حال افزایش است.
- میزان رشد فرکانس ساعت در حدود ۳۰ درصد در سال می‌باشد.

پیش بینی می‌شود که در آینده رشد بسیار سریعی در حافظه و پردازنده‌ها وجود داشته باشد. مشکل در اینجاست که در حین سریعتر شدن پردازنده‌ها، حافظه‌ها نیز بزرگتر می‌شوند. بنابراین دسترسی به داده‌ها در حافظه یک تنگنا به شمار می‌رود. یک روش برای غلبه بر این تنگنا، قرار دادن DRAM در بانک‌ها و سپس انتقال داده‌ها از این بانک‌ها بصورت موازی می‌باشد. علاوه بر این، سلسله مراتب چند سطحی حافظه که بصورت حافظه‌های کاشه سازماندهی می‌شوند نیز، دستیابی به حافظه را عملی‌تر و سریعتر می‌سازند، ولی طراحی آن‌ها پیچیده است. تنگنای دسترسی برای دستیابی به دیسک نیز وجود دارد که می‌تواند با استفاده از دیسک‌های موازی و حافظه‌های نهان (Cache) تخفیف داده شود.

نسبت بین هزینه و کارآیی ارتباطات درونی شبکه، به سرعت در حال کاهش است. کاربرد تکنولوژی‌های شبکه نظیر ATM، SCI و Myrinet در ایجاد کلاستر برای پردازش موازی نویدبخش به نظر می‌رسد. این امر بوسیله پروژه‌های علمی و تجاری بسیاری نظیر پروژه Berkeley NOW و پروژه Beowulf ثابت شده است. با این وجود هیچ ارتباط شبکه‌ای خاصی به عنوان یک برنده آشکار پدیدار نشده است. Myrinet یک محصول تولیدی نمی‌باشد و هزینه بسیار زیادتری نسبت به اترنت در بر دارد، ولی مزایای زیادی را نسبت به آن داراست که عبارتند از: تاخیر بسیار کم، پهنای باند زیاد و پردازنده‌ای که بر روی برد قرار دارد و قابل برنامه‌ریزی است که انعطاف‌پذیری بیشتری را امکان‌پذیر می‌سازد. شبکه SCI برای ساخت سیستم حافظه مشترک توزیعی بکار رفته است ولی از قابلیت مقیاس‌پذیری برخوردار نیست. ATM نیز در کلاسترهایی بکار می‌رود که در اصل برای پردازش چندرسآن‌های استفاده می‌شوند.

دو گونه از رایج‌ترین سیستم‌عامل‌ها در دهه ۱۹۹۰، Linux و NT می‌باشند. Linux به دلیل دسترسی مجانی و کارآیی بهتر در مقایسه با دیگر سیستم‌عامل‌های رومیزی مانند NT، برای یک سیستم‌عامل تجاری یک جایگزین رایج شده است. هم اکنون Linux دارای بیش از ۷.۵ میلیون کاربر در سراسر جهان بوده و سیستم‌عامل انتخابی محققان می‌باشد.

NT دارای یک پایه نصبی قوی بوده و تقریباً یک سیستم‌عامل فراگیر شده است. NT 5.0 یک پشته TCP/IP سریعتر و باریکتر را خواهد داشت که از ارتباط سریعتر پیام‌ها حمایت می‌کند. سیستم‌های NT برای محاسبات موازی در موقعیتی مشابه با ایستگاه‌های کاری Unix در ۵ الی ۷ سال قرار دارند و تنها، موضوع زمان در اینجا قبل از ورود NT مطرح بود - یعنی سازندگان NT نیازی به صرف وقت یا پول برای تحقیق ندارند چرا که در حال اقتباس بیشترین بخش از تکنولوژی‌ای هستند که بوسیله گروه سیستم‌عامل Unix توسعه یافته است.

۱۲-۱۶-۲- روندهای رشد تکنولوژی کلاستر

ما در این تحقیق به بحث راجع به تعدادی از پروژه‌های کلاستر پرداختیم. این دامنه، از پروژه‌هایی که تولید شده ولی دارای قطعات اختصاصی هستند (Berkeley NOW) تا یک سیستم کاملاً تولیدی (Beowulf) گسترده می‌باشد. HPVM می‌تواند به عنوان یک سیستم ترکیبی در نظر گرفته شود زیرا از کامپیوترهای تولیدی و رابط‌های شبکه‌ای اختصاصی استفاده می‌کند. این نکته باید در نظر گرفته شود که پروژه‌هایی که بطور جزئی در این تحقیق به آن‌ها پرداخته شد، تنها تعداد کمی از متداول‌ترین و معروف‌ترین پروژه‌هایی هستند که از یک لیست بسیار بلند انتخاب شده بودند.

تمام پروژه‌های مورد بحث مدعی هستند که از قطعات تولیدی تشکیل شده‌اند. با اینکه این امر واقعیت دارد؛ شخصی ممکن است اینطور استدلال کند که، تکنولوژی‌های واقعاً تولیدی آن‌هایی هستند که در اکثر مکآن‌های علمی و صنعتی رایج باشند. اگر وضعیت به این شکل باشد، بنابراین محصول واقعی به معنای کامپیوترهای شخصی که در حال اجرای ویندوز ۹۸ همراه با اترنت 100Mbps می‌باشند، خواهد بود. به هر حال وقتی کاربردهای موازی را در نظر گرفته و نیازهای محاسبه‌ای و شبکه‌ای را مطالعه کنیم این نوع کلاسترهای کم قدرت قادر به فراهم ساختن منابع مورد نیاز نخواهند بود.

هر یک از پروژه‌های مورد بحث با روش‌هایی نه چندان متفاوت سعی در غلبه بر تنگناهایی دارند که در حین استفاده از سیستم‌های بر مبنای کلاستر به منظور اجرای کاربردهای موازی بوجود می‌آیند. بدون در نظر گرفتن خرابی، تنگنای اصلی منبع محاسبه‌ای (که ممکن است یک PC یا ایستگاه کاری Unix باشد) نیست، بلکه تنگنای اصلی تامین یک ارتباط با پهنای باند بالا و تاخیر کم و یک پروتکل ارتباطی سطح پایین و مفید برای فراهم ساختن APIهای سطح بالا می‌باشد.

پروژه Beowulf کاربرد چندین کارت اترنتی استاندارد را به منظور غلبه بر تنگنای ارتباطات بررسی می‌کند، در حالی که پروژه Berkeley NOW و HPVM از کارت‌های قابل برنامه‌ریزی Myrinet و پروتکل‌های ارتباطات AM/FM استفاده می‌کنند. Solaris MC از NICهای Myrinet و TCP/IP بهره می‌گیرد. انتخاب اینکه کدامیک بهترین راه‌حل است نمی‌تواند فقط بر اساس نحوه اجرا و کارایی آن باشد بلکه هزینه هر گره برای فراهم کردن NIC نیز باید در نظر گرفته شود. به عنوان مثال یک کارت اترنت استاندارد کمتر از ۵۰ دلار هزینه دارد، در حالی که کارت‌های Myrinet هر کدام فراتر از ۱۰۰۰ دلار هزینه در بر دارند. عامل دیگری که در این معادله باید در نظر گرفته شود، قابلیت دسترسی به اترنت سریع و پیدایش اترنت گیگابیتی می‌باشد. اینطور به نظر می‌رسد که تکنولوژی‌های اترنت احتمالاً رایج‌تر، دارای تولید بیشتر و در نتیجه ارزان‌تر از رابط‌های شبکه اختصاصی خواهند بود. به عنوان یک نکته، تمام پروژه‌هایی که راجع به آن‌ها بحث شده است پیشتاز تحول محاسبه‌ای کلاستر می‌باشند و تحقیق آن‌ها به گروه زیر کمک می‌کند تا تعیین کنند که کدام یک از تکنیک‌ها و تکنولوژی‌ها برای انتخاب بهترین می‌باشند.

۱۲-۱۶-۳- تکنولوژی‌های آینده کلاستر

پیدایش تکنولوژی‌های سخت‌افزاری در امتداد با تکامل منابع نرم‌افزاری به این معناست که سیستم‌های بر پایه کلاستر به سرعت در حال بستن شکاف عملیاتی با سکوهای محاسبه‌ای موازی و اختصاصی می‌باشند. سیستم‌های کلاستری که به دنبال سیکل‌های بلااستفاده کامپیوترهای شخصی و یا ایستگاه‌های کاری می‌باشند، به استفاده از هر قطعه سخت‌افزاری و نرم‌افزاری که در دسترس ایستگاه‌های کاری عمومی می‌باشد، ادامه خواهند داد. کلاسترهایی که به کاربردهای اجرایی سطح بالا

اختصاص یافته‌اند به عنوان کامپیوترهای قوی‌تر و جدیدتر مدام در حال تغییر و تحول خواهند بود و رابط‌های شبکه در دسترس بازار قرار می‌گیرند.

این احتمال وجود دارد که گره‌های مستقل کلاستر، SMPها باشند. امروزه کامپیوترهای شخصی و ایستگاه‌های کاری که دارای دو و یا چهار پردازنده‌اند، متداول شده‌اند. نرم‌افزاری که به گره‌های SMP امکان می‌دهد تا بهتر و کارآمدتر توسط برنامه‌های کاربردی موازی بکار روند، در آینده نزدیک گسترش پیدا کرده و به هسته سیستم‌عامل اضافه خواهند شد. این احتمال می‌رود که کاربرد گسترده اترنت گیگابیتی به وجود آمده و در نتیجه استاندارد بالفعل (Defacto) برای کلاستر شود. برای کاهش تاخیر انتقال پیام، سیستم‌های نرم‌افزاری کلاستر، هسته اصلی سیستم‌عامل را نادیده خواهند گرفت، بنابراین از نیاز به فراخوآن‌های سیستم گران قیمت اجتناب کرده و از کاربرد کارت‌های هوشمند شبکه بهره‌برداری می‌کنند. واضح است که این امر با استفاده از NICهای هوشمند و یا رابط‌های شبکه‌ای که روی تراشه قرار دارند نظیر آن‌هایی که بوسیله DEC Alpha 21364 جدید استفاده می‌شوند، حاصل می‌شود.

توانایی فراهم ساختن یک مجموعه توانا از ابزارهای توسعه و برنامه‌های کمکی و همچنین تامین خدمات معتبر و مستحکم، انتخاب سیستم‌عامل به کار رفته در کلاسترهای آتی را مشخص خواهد نمود. احتمال دارد سیستم‌عامل‌های بر پایه Unix متداول‌تر باشند، ولی پیشرفت و انتخاب Windows NT به این معناست که خیلی عقب نخواهد بود.

۱۲-۱۶-٤- استدلال نهایی

نیاز ما به منابع محاسبه‌ای در تمام زمینه‌های علمی، مهندسی و تجاری توانایی ما را برای بر آوردن این نیازها مورد آزمایش قرار می‌دهد. شاید استفاده از کلاسترهای کامپیوتر یکی از نویدبخش‌ترین راه‌هایی باشد که بوسیله آن می‌توانیم شکاف میان نیازهایمان و منابع موجود را پر کنیم. استفاده از سیستم‌های کلاستری بر مبنای COTS دارای مزایایی است که شامل این موارد می‌باشند:

- نسبت قیمت / اجرا در مقایسه با یک ابرکامپیوتر موازی اختصاصی
- رشد فزاینده‌ای که اغلب با الگوی تامین بودجه سالیانه همسان می‌باشد
- تامین یک سیستم با چند هدف: اینکه بتواند مثلاً برای امور دبیرخانه در طول روز و به عنوان یک وسیله ابرمحاسبه‌ای موازی در شب مورد استفاده قرار گیرد.

این مزایا و مزایای دیگر به تحول محاسبات کلاستری و قبول آن‌ها به عنوان یک وسیله فراهم‌سازی امکانات ابرکامپیوتری تداوم خواهند بخشید.

۱۲-۱۷- ضمیمه: تصاویر مختلف از کلاسترهای کامپیوتری



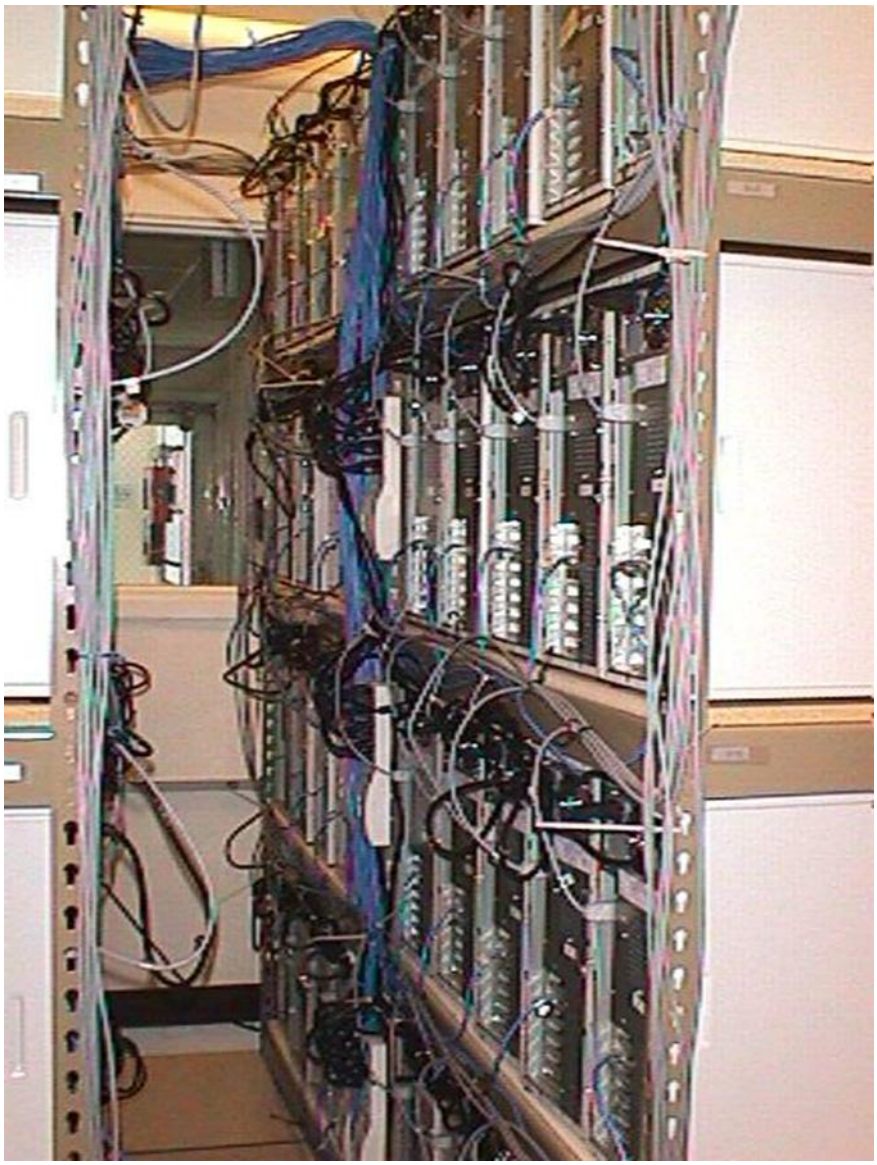
A. NASA Goddard’s PC 512 GB Bulk Data Server



B. Digital Domain’s 160 node DEC Alpha Cluster



C. Front View of a Los Alamos's Avalon DEC Alpha Cluster



D. Back View of a Los Alamos's Avalon DEC Alpha Cluster



E. Clemson University’s 16 node PC (200 MHz) Cluster

فصل ۱۳ آشنایی با مدارک شبکه

۱۳-۱- مقدمه

همانطور که می‌دانید در سراسر دنیا دوره‌های آموزشی شبکه مختلفی برگزار می‌گردد. هر کدام از این دوره‌ها هدفی خاص را دنبال می‌کند و در نهایت نیز به اخذ مدرک خاصی می‌نجامد. در واقع با دریافت یک مدرک و گواهینامه خاص، این امر اثبات می‌گردد که شما در آن زمینه خاص دارای مهارت و تبهر کافی می‌باشید. آزمون‌های شبکه عموما به صورت بین‌المللی انجام می‌گیرد و وابسته به شرکتی خاص در ایران نیست؛ لذا مدارک دریافتی اعتبار بین‌المللی دارند.

برخی از معروفترین موسسات ارائه کننده مدارک شبکه عبارتند از:

- **سیسکو (Cisco)**
- **مایکروسافت (Microsoft)**
- **کامپتیا (CompTIA)**
- **ناول (Novell)**

۱۳-۲- سیسکو (Cisco)



۱۳-۲- سیسکو (Cisco)

همانطور که می‌دانید شرکت Cisco بعنوان بزرگترین و معتبرترین شرکت در زمینه ساخت، طراحی و اجرای شبکه‌های کامپیوتری و تجهیزات آن در جهان شناخته شده است. از این رو برای آشنائی بیشتر متخصصان شبکه با اصول طراحی و کار با تجهیزات، این شرکت اقدام به برگزاری دوره‌های متعددی در زمینه‌های مختلف شبکه نموده است. همچنین برای آگاهی از صحت و کار آزمودگی دانش‌آموختگان این دوره‌ها پس از گرفتن آزمون از آن‌ها، به آن‌ها مدرک بین‌المللی ارائه می‌نماید.

لن بزاک و سندی لرنر (دارای مدرک لیسانس از دانشگاه ایالتی کالیفرنیا، فوق لیسانس اقتصادسنجی از دانشگاه کلرمونت و فوق لیسانس علوم کامپیوتر از دانشگاه استنفورد)، زوجی که در بخش کامپیوتر دانشگاه استنفورد کار میکردند، سیسکو را در سال ۱۹۸٤ تاسیس کردند. بزاک نرم‌افزار روترهای چند پروتکل را که توسط ویلیام یاگر (یک کارمند دیگر که کار سالها قبل از بزاک شروع کرده بود) نوشته شده بود تکمیل کرد.

با این وجود که سیسکو اولین شرکتی نبود که روتر (وسیله‌ای که ترافیک شبکه‌ها را از یکی به دیگری هدایت می‌کند) طراحی و تولید می‌کند، اولین شرکتی بود که یک روتر چند پروتکل موفق تولید می‌کند که اجازه ی ارتباط بین پروتکل‌های مختلف شبکه را می‌دهد. از زمانی که پروتکل اینترنت (IP) به یک استاندارد تبدیل شد، اهمیت روترهای چند پروتکل کاهش یافت. امروزه بزرگترین روترهای سیسکو طراحی شده‌اند تا پاکت‌های IP و فریمهای MPLS را هدایت کنند. در ۱۹۹۰، شرکت به سهامی عام تبدیل شد و سهام آن در بازار بورس NASDAQ عرضه شد.بزاک و لرنر با ۱۷۰ میلیون دلار از شرکت خارج شدند و بعد از مدتی جدا شدند. زمان انفجار اینترنت در ۱۹۹۹، سیسکو شرکت Cerent واقع در کالیفرنیا را با قیمت ۷ میلیارد دلار خریداری کرد. این شرکت گرانترین خرید سیسکو در آن زمان بود. تنها خرید گرانتر مربوط به ساینتیفیک آتلانتا می‌باشد.

در اواخر مارس ۲۰۰۰، در اوج رشد دات کام، سیسکو با ارزش مالی بالغ بر ۵۰۰ میلیارد دلار ارزشمندترین شرکت دنیا بود.در سال ۲۰۰۷، با ارزشی بالغ بر ١٦٥ میلیارد دلار همچنان یکی از ارزشمندترین شرکتها است.

با خرید شرکت‌های دیگر، توسعه ی داخلی و همکاری با دیگر شرکت‌ها، سیسکو به بازار بسیاری از قطعات دیگر شبکه (غیر از روتر) راه پیدا کرده است، مانند سوییچینگ اترنت، دسترسی از راه دور، روترهای شعبه‌ای، شبکه ی خودپردازهای بانک‌ها، امنیت، دیواره‌های آتش، تلفن اینترنتی و غیره. در ۲۰۰۳، سیسکو شرکت محبوب لینکسیس تولید کننده ی سخت‌افزار شبکه کامپیوتر را خریداری کرد و آن را در صدر تولید کننده‌های قطعات مربوط به کاربران عادی تبدیل کرد.

اسم "سیسکو" مخفف سانفرانسیسکو است. با توجه به اظهارات جان مرگریج،کارمند ۳٤ ساله و مدیر پیشین شرکت، موسسان شرکت زمانی که داشتند به سمت ساکرامنتو رانندگی میکردند تا شرکت را به ثبت برسانند، با تصویر پل گلدن گیت در نور آفتاب مواجه می‌شوند و اسم و نماد شرکت را بر این اساس انتخاب می‌کنند. نماد شرکت منعکس کننده اصلیت سان فرانسیسکویی آن است، که نشان دهنده پل گلدن گیت است که به سبک خاصی طراحی شده است. در اکتبر ۲۰۰٦، سیسکو نماد جدید خود را که از نماد قبلی ساده‌تر و ساختیافته‌تر بود به معرض نمایش گذاشت.

مدارک شرکت CISCO راهیست به سوی موقعیت‌های برجسته شغلی و تأییدی است بر مهارتی با استانداردهای بسیار عالی.دریافت مدرک CISCO (در هر سطحی) به معنی پیوستن به جامعه متخصصان ماهر در شبکه است که در دنیای صنعت و تکنولوژی شناخته شده و معتبرند.

سیسکو در ۱۵۰ کشور دنیا مرکزهایی آموزشی به منظور تعلیم افراد برای طراحی و نگهداری شبکه‌های کامپیوتری تاسیس کرده است. سیسکو مدارکی را برای متخصصین در زمینه‌های مختلف شبکه ارائه می‌کند. که شامل این مدارک می‌شود:

- ✓ CCSI - Cisco Certified Systems Instructor (آموزش دهنده سیستم‌های سیسکو)
- ✓ CCNA - Cisco Certified Network Associate (همکار شبکه سیسکو)
- ✓ CCDA - Cisco Certified Design Associate (همکار طراحی سیسکو)
- ✓ CCNP - Cisco Certified Network Professional (حرفه‌ای شبکه سیسکو)
- ✓ CCDP - Cisco Certified Design Professional (حرفه‌ای طراحی سیسکو)
- ✓ CCIP - Cisco Certified Internetwork Professional (حرفه‌ای شبکه بندی سیسکو)
- ✓ CCSP - Cisco Certified Security Professional (حرفه‌ای امنیت سیسکو)
- ✓ CCVP - Cisco Certified Voice Professional (حرفه‌ای تلفن اینترنتی سیسکو)
- ✓ CCIE - Cisco Certified Internetwork Expert (متخصص شبکه بندی سیسکو)

مدرک CCIE پیشرفته‌ترین و بالاترین مدرک ارایه شده توسط سیسکو در زمینه شبکه‌های کامپیوتری است. در هرم تحصیلی ارایه شده توسط شرکت سیسکو، مدرک CCNA به عنوان مدرک ورود به چرخه تحصیلی و کسب علوم شبکه‌ای در قاعده هرم قرار گرفته و عنوان نصب و پشتیبانی ادوات شبکه‌ای سیسکو را به خود اختصاص داده است. در همین سطح مدرک CCDA که ویژه طراحی مقدماتی شبکه‌های سیسکو می‌باشد نیز وجود دارد. در یک سطح بالاتر سه مدرک CCNP، CCDP و CCIP لایه میانی این هرم را تشکیل داده و عنوان مدیریت شبکه‌های پیشرفته و پیچیده سیسکو را به خود اختصاص داده‌اند و بالاخره این‌که مدرک CCIE با قرار گرفتن در راس این هرم تحصیلی، به عنوان طراح اصلی و مدیریت رده بالای شبکه‌های سیسکو شناخته می‌شود.

در دوره‌های آموزشی سیسکو، به طور معمول راه اندازی شبکه‌های کامپیوتری (سخت‌افزاری) پرداخته می‌شود. طراحی ساختار و راه اندازی و تنظیم و پشتیبانی از روترها و سوئیچ‌های سیسکو از مبحثهای این دوره آموزشی هستند. راه ورود به دنیای عظیم سیسکو شرکت در دوره آموزشی CCNA وکسب مدرک آن است. بعد از اینکه دوره ی CCNA را با موفقیت به پایان رساندید مجاز به شرکت در دوره‌های تخصصی و حرفه ای‌تر سیسکو بنام CCNP هستید. وقتی دو دوره فوق را با موفقیت پشت سر بگذارید. آماده شروع دوره‌ای خواهید شد که حرفه‌ای ترین و ارزشمندترین مدرک کمپانی سیسکو می‌باشد، این مدرک معتبر CCIE نام دارد.

در کشور ما شرکت‌ها و موسسات آموزشی متعددی اقدام به برگزاری این دوره‌ها نموده‌اند، ولی به علت اینکه شرکت سیسکو در آمریکا قرار دارد و ما هم تحریم هستیم (خدا لعنتشون کنه)، لذا هیچگونه مدرکی از طرف این شرکت در داخل ایران صادر نمی‌گردد و دانش‌آموختگان بایستی پس از گذراندن این دوره‌ها به یک کشور دیگر (معمولا شهر دبی) رفته، در امتحانات آنجا شرکت کرده و مدرک را در آن کشور اخذ نمایند. بله، همانطور که گفتم امتحان بین المللی در Test Center هایی گرفته می‌شود که متاسفانه کشور ایران را تحریم نموده و هیچ پایگاهی در داخل کشور ندارند، پس برای اخذ مدرک بین المللی باید از کشور خارج شوید، اما مساله فقط فقدان یک Test Center در کشور نیست، در آن سوی مرزها نیز شما

نمی‌توانید به صورت قانونی امتحان دهید و ناچارید با هویت غیرایرانی و به صورت غیرقانونی امتحان داده و از شرکت سیسکو مدرک بین المللی بگیرید.

مدرک بین المللی سیسکو افزون بر اینکه در ایران امتیازی بزرگ جهت یافتن شغل محسوب می‌شود، اعتبار علمی شما را در سرتاسر دنیا تضمین می کند.

۱۳-۲-۱- سطوح مدارک سیسکو

مدارک شرکت سیسکو به پنج سطح تقسیم می‌شوند. سطح بسیار مقدماتی و سطح بسیار پیشرفته آن به ترتیب عبارتند از Entry و Architect. اما گذشته از سطح Entry و Architect، سایر سطوح مدارک سیسکو (Associate و Professional و Expert) گرایش‌های مختلف مهندسی شبکه را پوشش می‌دهند.

- ✓ Entry
- ✓ Associate
- ✓ Professional
- ✓ Expert
- ✓ Architect

همچنین این مدارک به هشت گرایش مختلف تقسیم می‌شوند.

- ✓ Routing & Switching
- ✓ Design
- ✓ Network Security
- ✓ Service Provider
- ✓ Service Provider Operations
- ✓ Storage Networking
- ✓ Voice
- ✓ Wireless

۱۳-۲-۲- سطح Entry

سطح Entry با مدرک CCENT ابتدایی بوده و در ایران دوره‌ای با این عنوان برگزار نمی‌شود در عوض مدرک Network+ به عنوان پیش نیاز مهندسی شبکه سیسکو و مایکروسافت در ایران مورد توجه قرار داشته و معمولا اولین دوره‌ای است که متخصصان شبکه آن را می گذرانند.

البته CCENT معادل Network+ نبوده و سطح بالاتری دارد. CCENT را می‌توان نیمی از راه مدرک CCNA دانست، به عبارتی کسی که CCNA دارد، به CCENT هم مسلط است.

۱۳-۲-۳- سطح Architect

سطح Architect که چندی پیش توسط سیسکو ارائه شده است، بالاترین سطح مدرک مهندسی شبکه در بین کلیه مدارک بین المللی شبکه است، ظاهرا شرکت سیسکو با ارائه ی این سطح خواسته تا برترین متخصصان بین المللی شبکه را گلچین نماید، شاید بتوان CCA را به نوعی معادل فوق دکترای شبکه در گرایش Design دانست.

۱۳-۲-۴- سطح Associate

Associate یا دستیار، یعنی قرار گرفتن در ابتدای مسیر، گرایش شما هر چه که باشد می‌بایست پیش از اخذ هر مدرک و یا گذراندن هر دوره‌ای، CCNA با گرایش Routing & Switching را بگذرانید.

این سطح در قاعده هرم سیسکو جای گرفته و نخستین سطح مهارتی سیسکو، یعنی سطح آشنایی و مقدمات است. دانشجویان با اخذ این مدرک، دروازه سیسکو را بر روی خود می‌گشایند و خود را برای صعود از پله‌های پیشرفت و تخصص شبکه‌ای آماده می‌کنند.

بعد از آن چنانچه خواستار تغییر گرایش از Routing & Switching به سایر گرایش‌ها باشد، می‌بایست مدرک Associate آن گرایش را نیز اخذ کنید.

۱۳-۲-۵- سطح Professional و Expert

مثلا چنانچه به Security علاقه‌مند هستید باید مدرک CCNA با گرایش Security را کسب کرده و سپس به سطح بالاتر یعنی Professional صعود نموده و CCSP را بگذرانید و نهایتا مدرک سطح Expert یعنی CCIE با گرایش Security را اخذ کنید.

البته اخذ این مدارک به خصوص مدارک سطح Expert کاری فوق العاده سنگین بوده و نیازمند تجربه کاری در حدود ۱۰ سال و تمرکز عمیق روی منابع مطالعاتی است.

- معمولا مدارک سطح Associate نظیر CCNA و CCDA را معادل کارشناسی شبکه
- مدارک سطح Professional نظیر CCNP، CCSP و CCDP را معادل کارشناسی ارشد شبکه
- و مدارک سطح Expert نظیر CCDE و CCIE با گرایش‌های مختلف را معادل دکترای شبکه می‌دانند.

۱۳-۲-۶- CCNET (سطح Entry)



نخستین گام در شبکه‌های سیسکو با این سطح برداشته می‌شود، همچنین در این سطح یک مدرک موقت، به‌نام مدرک CCNET، برای کسانی که با مشاغل ساده‌تر ارتباط دارند، در نظر گرفته شده است. مدارک سطح همکار در حقیقت آغاز کار با شبکه است و دانشجویان این دوره‌ها در حقیقت کارآموز به‌شمار می‌آیند.

۱۳-۲-۷- مدرک CCNA (سطح Associate)



CCNA مخفف کلمات Cisco Certified Network Associate است که به معنای مدرکی است که دارنده آن، شرکت سیسکو را به عنوان همکار شبکه قبول دارد.

مدرک CCNA (CISCO Certified Network Associate) در رابطه با مهارت فنی در نصب و تنظیمات و راه بری شبکه‌های LAN و WAN و نیز ارتباطات شبکه توسط سیستم شماره گیری تلفن برای شبکه‌های کوچک (۱۰۰ گره و کمتر) از جمله IGRP, Serial, Frame Relay, IP RIP, VLANs, RIP, Ethernet, Access List می‌باشد.

اطلاعات اولیه و بنیادی که شما به هنگام آماده شدن و مطالعه جهت امتحان CCNA بدست می‌آورید اولین قدم در راه ورود به بازار حرفه‌ای شبکه است. مدرک CCNA مهارت و توانائی اولیه و مقدماتی فرد را در کار شبکه تأیید می‌کند، داوطلبانی که امتحان مربوطه را با موفقیت گذرانده‌اند از شرکت CISCO مدرک CCNA در یافت می‌کنند و می‌توانند این عنوان را در کارت ویزیت خود درج کنند.

دارندگان این مدرک، این توانایی‌ها را به‌دست می‌آورند:

- ✓ افزایش دانش و توانایی‌ها و تجربیات شبکه‌ای و تضمین موقعیت شغلی
- ✓ پیاده‌سازی سرویس‌های تلفنی برای شبکه‌های کوچک
- ✓ راه‌اندازی و پیکربندی و مدیریت شبکه‌های محلی (LAN) ساده با تجهیزات سیسکو
- ✓ برگزیدن یکی از سرویس‌های WAN، با توجه به نیاز شبکه و پیاده‌سازی و مدیریت کلی آن
- ✓ رفع اشکالات موجود در LAN و VLAN
- ✓ آشنایی و مهارت کلی با سیستم عامل روتر (IOS) شامل:
  - اجرای فرمآن‌هایی همچون به‌روزرسانی، پشتیبان‌گیری، دانلود نرم‌افزار ومدیریت IOS
  - تشریح فرمآن‌های مسیریاب، مانند تعیین رمز عبور و استفاده از فرمان راهنمایی مسیریاب.

پیش‌نیازهای اخذ مدرک

- ✓ با گذرانیدن دوره Network+ (یکی از دوره‌های CopmTIA، برای آشنایی پایه‌ای با مفاهیم اصلی شبکه)
- ✓ آشنایی کلی با لایه‌های OSI
- ✓ آشنایی با توپولوژی و همبندی شبکه
- ✓ آشنایی با پروتکل TCP/IP و اصول شبکه‌بندی (Subnetting)

- ✓ آشنایی کلی با تجهیزات سخت‌افزاری شبکه مانند: سوییچ، هاب و سخت‌افزار کامپیوتر
- ✓ ۶ ماه تا یک‌سال تجربه کاری در یک شبکه کوچک.

تذکر ۱: اخذ این مدرک مستلزم اخذ مدرک پیش نیاز نیست.

تذکر ۲: مدت اعتبار مدرک CCNA سه سال است.

۱۳-۲-۸- CCDA (سطح Associate)



یکی دیگر از مدارک سیسکو که در ایران کمتر به آن توجه شده است، مدرک CCDA یا Cicso Certified Design Associate است. این مدرک روی طراحی و مهندسی شبکه تمرکز دارد. CCDA تضمین‌کننده دانش طراحی و مهندسی شبکه‌های کوچک اداری است. دارندگان این مدرک توانایی بنیادی برای طراحی و نصب شبکه‌های کوچک سیسکو (۱۰۰ یا کمتر ایستگاه‌های کاری) را خواهند داشت و با استفاده از تجهیزات مسیریاب و سوییچ قادر به پیاده‌سازی LAN و WAN و سرویس‌های Dial Access برای شرکت‌ها و سازمان‌های گوناگون خواهند بود. همچنین قادر به ارزیابی راه‌حل‌هایی برای رفع اشکالات مربوط به انتقال ترافیک صوت بر روی شبکه خواهند بود.

این مدرک پیش‌نیازی ندارد، اما اخذ مدرک CCNA پیش از آن سفارش شده است.

۱۳-۲-۹- مدرک CCNP (سطح Professional)



CCNP مخفف عبارت Cisco Certified Network Professional است که معمولا افراد پس از گذراندن CCNA اقدام به گذراندن این دوره می‌کنند. این مدرک از سری مدارک سطح متخصص (Professional)، در رابطه با مهارت فنی در نصب و تنظیمات و راه بری شبکه‌های LAN و WAN و نیز ارتباطات شبکه توسط سیستم شماره گیری تلفن برای شبکه‌های بزرگ بوده و نشانگر دانش و مهارت پیشرفته در زمینه شبکه می‌باشد. این دسته از شبکه‌ها که اغلب در کارخانجات

صنعتی بزرگ، مراکز بزرگ بازرگانی و همچنین سازمان‌های بزرگ مستقر هستند و برخلاف شبکه‌های محلی کوچک و شبکه‌های دفتری به‌دلیل نوع استفاده افزایش شمار کاربران و نقشی که در پیشبرد اهداف نهایی آن سازمان ایفا می‌کنند، از حساسیت و اهمیت حیاتی برخوردار است. بنابراین، کسانی که با دریافت مدرک CCNP پا به عرصه کار با این‌گونه شبکه‌ها می‌گذارند، نسبت به دارندگان مدارک دیگر (مانند CCNA)، اهداف بزرگتر و به‌دنبال آن مشکلات و دردسرهای بیشتری را پیش‌رو دارند. در عوض، این افراد از دیدگاه جایگاه شغلی در ردههای بالاتر و از دیدگاه حساسیت نقشی که به‌عهده دارند، دارای مسوولیتی بزرگتر و از دیدگاه درآمد، وضعیتی مطلوبتر از دیگر دست‌اندرکاران طراحی و نصب شبکه دارند. تفاوت عمده این مدرک با CCNA این است که فرد پس از گذراندن این دوره توانائی شبکه‌بندی بین گره‌های بیشتری (از ۱۰۰ گره تا ۵۰۰ گره) و افزوده شدن تعداد بیشتری پروتکلهای شبکه نظیر PPP، PSTN، DDR، X25، ISL، ISDN، Frame Realy، IP، IGRP، IPX، Apple Talk، RIP، IP RIP، VLSM، BGP، 802.10، OSPF و IGRP دارد. مباحث این مدرک بر روی مواردی همچون امنیت، شبکه‌های متمرکز،کیفیت سرویس یا QoS (Quality of Service)، VPN (Virtual Private Networks) و تکنولوژی‌های Broadband تاکید دارد.

داوطلبان دریافت مدرکCCNP باید نخستین قاعده هرم تحصیلی شرکت سیسکو، یعنی مدرکCCNA، را (که مربوط به شبکه‌های محلی کوچک می‌شود) گذرانیده باشند. شخصی که به دریافت مدرک CCNP نایل می‌شود، از دیدگاه رده شغلی در میان همه شغل‌هایی که مربوط به مهندسی شبکه به‌ویژه نصب و راه‌اندازی شبکه با استفاده از تجهیزات سیسکو می‌شود، در رده دوم یعنی پس از مدرک CCIE که مربوط به مشاوران حرفه‌ای سیسکو است، قرار می‌گیرد. این بدان معنا است که شخص دارنده CCNP می‌تواند فاصله مقام خود را با ارشدترین سطح کارشناسی شبکه به یک گام برساند. کارشناس شبکه با ارتقای مدرک خود از CCNA به‌CCNP نه‌تنها تسلط خود بر مباحث مربوط به شبکه‌های LAN و Dial up را افزایش می‌دهد، بلکه از محدوده شبکه‌های محلی با کاربرد کوچک خارج شده و توانایی خود را در راه‌اندازی شبکه‌های WAN تثبیت می‌کند.

آزمون‌های مرتبط با دوره

برای کسب مدرکCCNP شرکت در ٤ دوره آموزشی و گذرانیدن موفقیت‌آمیز آزمون‌های هر کدام از آن‌ها الزامی است. مواد این دوره عبارت است از:

۱- ساخت شبکه‌های عادی سیسکو (BSCI)

در این دوره، نحوه اتصال و استفاده از مسیریاب‌های سیسکو در شبکه‌های LAN و WAN برای سایت‌های متوسط تا بزرگ آموزش داده می‌شود. در این دوره مباحث جامعی در زمینه پروتکل‌های EIGRP،BGP، OSPF،EGP و ISIS مطرح شده و داوطلبان با دو نوع پروتکل مسیریابی به‌نام‌های Distance Vector وLink State آشنا می‌شوند. در پایان این دوره، داوطلب می‌تواند سرویس‌هایIOS مناسب یک مسیریاب سیسکو را انتخاب و راه‌اندازی کند.

۲ - ساخت شبکه‌های چند لایه سیسکو(BCMSN)

در این دوره، شیوه ایجاد یک فضای شبکه بر پایه فناوری سوییچینگ چندلایه در سرعت‌های بالای اترنت(Ethernet) به مدیران شبکه‌ها آموزش داده می‌شود. این دوره شامل مفاهیم مسیریابی و سوییچینگ و فناوری‌های لایه دو و سه است.

داوطلبان پس از طی این دوره خواهند توانست یک فضای سوییچینگ چندلایه را برپا ساخته و به کنترل ترافیک شبکه با استفاده از سیستم‌های تشخیص هویت لایه‌های گوناگون بپردازند.

۳ – ساخت شبکه‌های راه‌دور(BCRAN)

در این دوره، داوطلب چگونگی پیکربندی و عیب‌یابی شبکه‌هایی را که در جاهای دیگر ایجاد شده و از طریق فناوری راه‌دور(Remote) به سایت مرکزی دسترسی دارند، فرا می‌گیرد. همچنین حالت عکس این کار یعنی دسترسی راه‌دور به سایت

مرکزی با مصرف کمترین پهنای‌باند نیز در این دوره مورد بحث قرار می‌گیرد. به‌طور کلی در BCRAN به شبکه‌های WAN توجهی ویژه می‌شود و روش پیکربندی تجهیزات سیسکو و برقراری ارتباط بهینه بین سایت مرکزی و دیگر شعبه‌ها و مسایل مربوط به کیفیت سرویس(QOS) در یک شبکه WAN تشریح می‌گردد. این دوره به‌ویژه برای مدیران شبکه‌ها که مسوول اجرا و عیب‌یابی زیرساخت یک شبکه WAN هستند، از اهمیت بالایی برخوردار است.

٤ – پشتیبانی و عیب‌یابی شبکه(CIT)

در این دوره، داوطلب چگونگی عیب‌یابی کامپیوترهای سرویس‌گیرنده یا سرویس‌دهنده را، که تحت پروتکل‌های گوناگون به‌هم متصل گشته‌اند و از سوییچ‌ها و مسیریاب‌های سیسکو استفاده می‌کنند، فرا می‌گیرد. بنابراین با گذرانیدن این دوره، می‌توان به تحلیل و شناسایی مشکلات در محیط‌های Fast Ethernet، VLAN، Frame Relay، ISDN BRI و ...، پرداخت و مشکلات پیچیده مربوط به سوییچ‌ها و مسیریاب‌های سیسکو را حل کرد.

سمت‌های مر بوط به یک متخصص CCNP:

- مدیر شبکه
- مهندس پشتیبانی سطح ۲
- مهندس سیستم سطح ۲
- تکنسین فنی شبکه
- مهندس استقرار

یک متخصص دارای مدرک CCNP دارای مهارتهای زیر می‌باشد:

- توانایی استفاده از تکنولوژی جهت ساخت یک Scalable Routed Network.
- ساخت شبکه با استفاده از تکنولوژیهای سوییچینگ چند لایه
- بهبود وضعیت ترافیک و کارآیی شبکه و کاهش امکان خرابی آن جهت LANها، WANهای Rout و سوییچ شده و شبکه‌های Remote Access.
- طراحی و راه اندازی اینترانتهای جهانی.
- عیب یابی محیطهای شبکه استفاده کننده از روترها و سوییچ‌های سیسکو جهت Client Hostها و سرویس‌های Multiprotocol.

تذکر ۱: اخذ این مدرک مستلزم اخذ مدرک پیش نیاز CCNA می‌باشد.

تذکر ۲: مدت اعتبار مدرک CCNP سه سال است.

۱۳-۲-۱۰- CCDP (سطح Professional)



مدرک CCDP یا Cicso Certified Design Professional یعنی طراح حرفه‌ای شبکه مورد تائید سیسکو. این مدرک، مدرکی برای طراحی حرفه‌ای و مسیریابی و سوییچ شبکه‌ها در محیط LAN و WAN با امکان سیستم شماره‌گیری برای شبکه‌های بزرگ است.

دارندگان این مدرک، دانش لازم برای طراحی پیشرفته شبکه‌های Routed و Switched که شامل LAN و WAN و سرویس‌های Dial Access است را دارا هستند (برای بین ۱۰۰ تا ۵۰۰ گره در شبکه). همچنین دارندگان این مدرک توانایی اعمال ماژول‌ها روی مسیریاب‌ها و انتخاب راه‌حل و طرحی مناسب برای محیط‌های کاری متفاوت (کاری، شخصی، شرکت‌ها و سازمان‌های گوناگون) را به‌دست خواهند آورد.

تذکر۱. داوطلبان برای کسب این مدرک باید دوره‌های مدرک CCNA و CCDA را با موفقیت پشت سر گذاشته باشند.

تذکر۲. اعتبار این مدرک از زمان اخذ آن به‌مدت ۳ سال است.

۱۳-۲-۱۱- CCIP (سطح Professional)



مدرک CCIP مخفف عبارت Professional Cisco Certified Inetrnetwork است. این مدرک، مدرک تخصصی در زمینه فناوری سرویس‌دهی شبکه‌ای است. دارندگان این مدرک صلاحیت لازم در زمینه تخصیص IP در شبکه‌ها را خواهند داشت و با فناوری‌ها و سرویس‌هایی مانند: IP routing، IP QoS، MPLS و BGP آشنایی پیدا می‌کنند. این مدرک تنها به مباحث IP و DSL می‌پردازد.

تذکر۱. داوطلبان برای کسب این مدرک باید دوره‌های مدرک CCNA را با موفقیت پشت سر گذاشته باشند.

تذکر۲. اعتبار این مدرک از زمان اخذ آن به‌مدت ۳ سال است.

۱۳-۲-۱۲- CCSP (سطح Professional)



CCSP مخفف عبارت Cisco Certified Security Professional است. این مدرک در زمینه مفاهیم بنیادین و پیچیده حفاظت و امنیت شبکه‌های سیسکو است. دارندگان این مدرک، توانایی مدیریتی در زمینه برقراری راه‌حل‌های امنیتی در شبکه و تجهیزات شبکه‌ای و کاهش ترافیک شبکه را به‌دست خواهند آورد.

تذکر۱. داوطلبان برای کسب این مدرک باید دوره‌های مدرک CCNA را با موفقیت پشت سر گذاشته باشند.

تذکر۲. اعتبار این مدرک از زمان اخذ آن به‌مدت ۳ سال است.

۱۳-۲-۱۳- CCVP (سطح Professional)



CCVP مخفف عبارت Cisco Certified Voice Professional است. این مدرک بر پایه فناوری اطلاعات پیشرفته بنا نهاده شده و برای کسانی مناسب است که علاقمند به فناوری صوت بر پایه شبکه هستند. دارندگان این مدرک توان ایجاد راه‌حل‌های تلفنی در شبکه‌های توسعه‌پذیر را خواهند داشت.

تذکر۱. داوطلبان برای کسب این مدرک باید دوره‌های مدرک CCNA یا ICDN را با موفقیت پشت سر گذاشته باشند.

تذکر۲. اعتبار این مدرک از زمان اخذ آن به‌مدت ۳ سال است.

۱۳-۲-۱۴- CCIE (سطح Expert)



بعد از گذراندن CCDP، شما می‌توانید مدرک CCIE را نیز اخذ کنید. CCIE مخفف عبارت Cisco Certified Internetwork Expert است. تفاوت اخذ این مدرک با بقیه مدارک شرکت سیسکو در نحوه برگزاری آزمون آن می‌باشد، چون این مدرک بصورت عملی و در آزمایشگاه برگزار می‌شود. این مدرک یکی از با پرستیژترین مدارک شبکه می‌باشد.

مدرک CCIE پایان مسیر و دوره آموزشی سیسکو می‌باشد. CCNA به‌عنوان نصب و پشتیبانی تجهیزات شبکه‌ای سیسکو و نیز به‌عنوان مدرک ورودی به چرخه مدارک سیسکو است. در همین سطح مدرک CCDA قرار گرفته که به‌عنوان طراحی مقدماتی و پایه‌ای شبکه‌های سیسکو است. در یک سطح بالاتر، ۶ مدرک CCNP، CCDP، CCIP، CCSP و CCVP در لایه میانی این هرم قرار گرفته است و به‌عنوان مدیریت و پشتیبانی شبکه‌های بزرگتر، پیشرفته‌تر و پیچیده‌تر سیسکو شناخته می‌شود. و در نهایت با صعود به راس هرم سیسکو، شاهد پیشرفته‌ترین و بالاترین مدرک ارایه‌شده توسط سیسکو یعنی CCIE خواهیم بود. که به‌عنوان دکترای حرفه‌ای شبکه است.

این مدرک با این که پیشرفته‌ترین مدرک شبکه و سیسکو است. اما برای اخذ آن هیچ پیش‌نیازی از طرف سیسکو در نظر گرفته نشده است. اما پیش از اخذ آن بهتر است که دانشجو۳ تا ۵ سال سابقه کار و تجربه در شبکه‌های بزرگ و پیچیده داشته باشد.

گرایش‌های CCIE

مدرک CCIE دارای ۵ گرایش در زمینه‌های گوناگون است. علاقمندان برای اخذ این مدرک باید یکی از گرایش‌ها را برپایه علاقمندی خود انتخاب کنند و بگذرانند. هرکدام از گرایش‌ها دارای یک آزمون نظری و یک آزمون عملی است که در یکی از نمایندگی‌های سیسکو برگزار می‌شود.

۱- CCIE Routing Switching

در این دوره، داوطلبان با انواع ارتباطات پیچیده Switching و Routing جهت افزایش پهنای باند، کاهش زمان پاسخ، افزایش کارایی و امنیت آشنا می‌شوند. همچنین نحوه نصب، نگهداری و رفع عیب از بزرگ‌ترین شبکه‌های LAN، WAN و سرویس‌های Dial Access را فرا می‌گیرند. مواردی چون Source Rout Briolging و DLSW+ (Data Link Switching) و PIX Firewall از جمله سرفصل‌های مهم این دوره به شمار می‌روند.

۲- CCIE Security

دوره امنیت در واقع از سال ۲۰۰۱ به سرفصل دروس CCIE اضافه شد که البته سه سال بعد شرکت سیسکو محتوای این دوره را به‌منظور هر چه نزدیک‌ترشدن به موضوعات امنیتی و فناوری روز، مورد بازبینی و ویرایش جدید قرارداد. در این دوره، ضمن بررسی انواع پروتکل‌های امنیتی شبکه و نقش سیستم‌عامل‌های مختلف در ارتباط با این پروتکل‌ها، مباحث پیچیده و مهمی چون: سیستم‌های کشف نفوذ (IDS)، سیستم‌های برقراری امنیت در سطح شبکه‌های بزرگVPN، پیاده‌سازی و پیکربندی سیستم‌های امنیتی برای شبکه‌های بی‌سیم و پروتکل‌هایEAP، AES متعلق به آن‌ها، مطرح می‌شود.

۳- CCIE Voice

در این دوره، اطلاعات جامعی در مورد تکنولوژی انتقال صوت از طریق پروتکل IP یعنی همان VOIP در محیط‌هایEnterprise از نصب و راه‌اندازی گرفته تا پشتیبانی و رفع عیب عرضه می‌شود.

۴- CCIE Service Provider

گذراندن این دوره بیانگر وجود اطلاعات و مهارت‌های فنی در بالاترین سطح آن در زمینه پروتکل IP و کلیه فناوری‌هایی است که براساس آن بنا شده‌اند: مثلIP Routing،Qos،Multicast،MPLS،MPLS VPN، MBGP و مهندسی ترافیک شبکه. به‌علاوه در این دوره، حداقل آخرین اطلاعات تخصصی در یک یا چند زمینه مهم ارایه سرویس‌های دیگر شبکه، مثلDSL،Optical Cable،Switching WAN،Content networking،IP telephony و Metro Ethernet عرضه می‌شود.

۵- CCIE Storage Networking

همان‌طور که از نام این دوره برمی‌آید، سرفصل‌های آموزشی آن مربوط به انواع ادوات و روش‌های ذخیره‌سازی اطلاعات است. از آن‌جا که مدیریت نگهداری از اطلاعات، مسایل مربوط به نگهداری آرشیو، نسخه‌های پشتیبان، سرعت دسترسی از روی دیسک و امثال آن در محیط‌های Enterprise دارای اهمیت حیاتی است، در این دوره سعی شده انتخاب‌های متفاوت قابل ارایه جهت ذخیره‌سازی اطلاعات در چنین محیط‌های بزرگی همانندFICON،FCIP،ISCSI و امثال آن مورد بررسی قرار گیرد.

۱۳-۲-۱۵- پرطرفدارترین گرایش ها

در بین ۸ گرایش ذکر شده، Routing & Switching مانند پایه‌ای برای سایر گرایش‌ها محسوب شده و در کشورهای مختلف دنیا همچون ایران پرطرفدارترین گرایش محسوب می‌شود.

در حال حاضر در ایران به گرایش هایی چون Voice, Security و Wireless نیز بها داده شده و دوره هایی برای این سه گرایش در آموزشگاه‌های مختلف برگزار می‌شود. البته مطمئن باشید در صورت انتخاب هر کدام از گرایش‌های سیسکو در صورت عبور از سطح Professional امنیت شغلی کافی را خواهید داشت.

اگر به مهندسی شبکه و دوره‌های مهندسی سیسکو علاقه مندید، برای انتخاب گرایش عجله نکنید، بعد از اتمام دوره‌ی CCNA با گرایش Routing & Switching، دید شما نسبت به مسیر بازتر شده و علاقه‌مندی خویش را بهتر خواهید شناخت.

۱۳-۲-۱۶- مزایای دستیابی به مدارک سیسکو

- دریافت مدرک بین المللی سیسکو (Certificate & Transcript)
- دریافت کارت شناسایی سیسکو (Wallet Card)
- امکان استفاده از لوگوی سیسکو
- موقعیت شغلی و استخدامی بهتر با توجه به تخصص و دانش مورد تأیید سیسکو در مورد محصولات و فن آوری این شرکت
- دریافت حقوق بیشتر با توجه به نوع تخصص
- اثبات دانش فنی و عملی در زمینه کار با جدیدترین تکنولوژیهای سیسکو
- دستیابی به بخش ویژه سایت سیسکو جهت دارندگان مدارک و امکان دریافت لوگوها و مشاهده وضعیت مدرک.

۱۳-۲-۱۷- وضعیت درآمد

بر اساس آماری که از مجله Certification در سال ۲۰۰۳ گرفته شده است، داشتن مدرکCCNA حدود ۱۶/۷ درصد باعث افزایش درآمد شده است. و دارندگان آن به طور متوسط درآمدی سالآن‌های معادل ۴۸ تا ۵۰ هزار دلار هستند.

مدرک CCNP، در حدود ۶۴ هزار دلار در سال وIP Telephony در حدود ۷۸ هزار دلار در سال درآمد داشته‌اند. با مقاسه درآمد مدارک سیسکو با مدارک مایکروسافت که در حدود۴۳ هزار دلار در سال است. می‌توان به سختی اخذ این مدارک، اعتبار و نیاز آن در سطح بین المللی پی‌برد.

طبق ادعای مسئولان دوره‌های آموزشی سیسکو، این دوره‌ها، به‌ویژه دوره CCIE، چنان تنظیم شده است که هرگونه نیاز اشخاصی که به کسب تخصص در امور شبکه تمایل دارند را برطرف می‌سازد. ضمن این‌که با تکیه‌ای که این دوره‌ها بر اصول علمی و فنی قضیه دارند، سعی شده است مفاد دروس صرفاً براساس تجهیزات خاصی که خود شرکت سیسکو ارایه می‌دهد بنا نشود و وابستگی کمتری به نوع تجهیزات شبکه‌ای مورد استفاده در هر یک از تکنولوژی‌های مورد بحث دوره‌ها لحاظ شود.

میانگین درآمد دارندگان مدرکCCIE در سال ۲۰۰۴ برابر ۱۰۵ هزار دلار در سال برآورد شده است که این رقم حاکی از یک افزایش ۱۲/۴ درصدی نسبت به سال ۲۰۰۳ است و به همین دلیل نه تنها موقعیت این مدرک را در زمینه میزان افزایش درآمد در سال در بین کلیه مدارک IT در مقام نخست قرار داده، بلکه بیانگر این مسئله است که اصولاً سطح درآمد هیچ مدرکی حتی معتبرترین و مشکل‌ترین مدارک متعلق به شرکت‌هایی چون اوراکل، IBM و مایکروسافت، به رقم میانگین یکصدهزار دلار در سال نرسیده است.

همچنین طبق آمار دیگری، مدرک CCIE در زمینه اشتغال‌زایی نیز مقام اول را به خود اختصاص داده و این امر بیانگر این نکته است که اولا هنوز تعداد زیادی از موقعیت‌های شغلی که توسط صاحبان این مدرک می‌تواند کسب شود، خالی است و در ثانی وجود چنین افرادی چه در رده مدیریت و چه در رده آموزش افراد، می‌تواند به رونق کسب‌وکار شبکه‌ای برای سایر مدارک و مشاغل مربوط به این حوزه منجر شود.

۱۳-۲-۱۸- خلاصه سطوح و مدارک سیسکو

Cisco Associate Level Certifications

Associate level Cisco certifications are the foundation for all higher level Cisco certifications.

- ✓ CCNA
- ✓ CCDA
- ✓ CCNA Security
- ✓ CCNA Voice
- ✓ CCNA Wireless
- ✓ CCNA Service Provider Operations

Cisco Professional Level Certifications

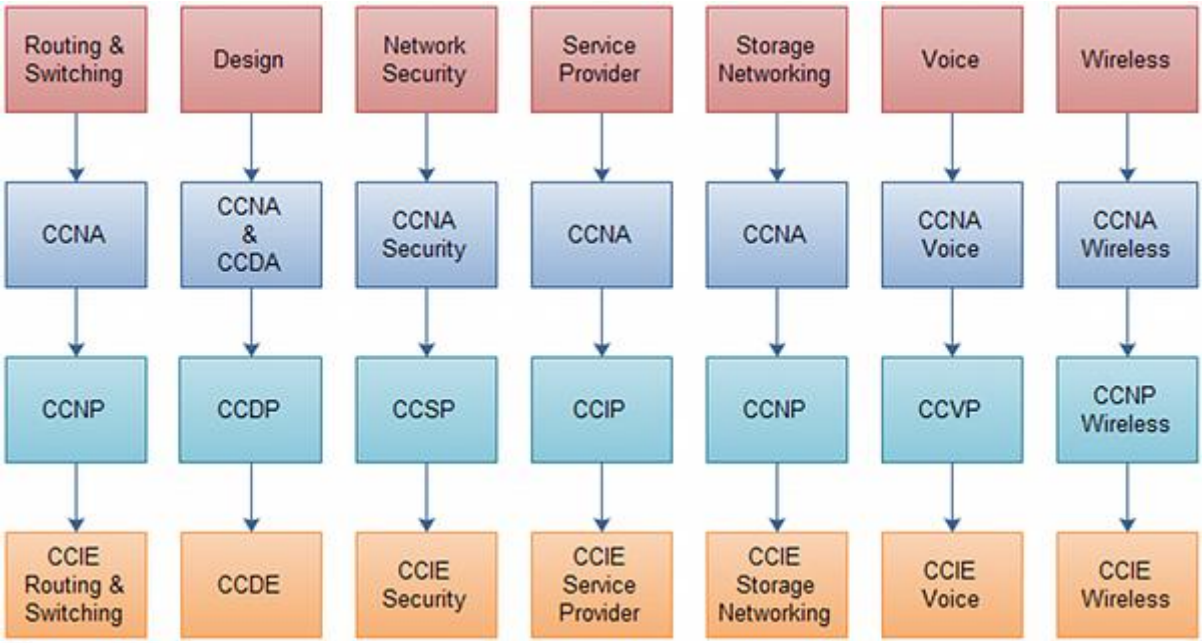
The Professional level is the advanced level of certification. Each certification (listed below) falls within a different certification path (or track) for meeting varying career needs.

- ✓ CCDP
- ✓ CCIP
- ✓ CCNP
- ✓ CCNP Security
- ✓ CCNP Service Provider Operations
- ✓ CCNP Voice (formerly known as CCVP)
- ✓ CCNP Wireless
- ✓ CCSP

Cisco Expert Level Certifications

Expert level Cisco certifications represent the highest level of skill and achievement for network or design professionals.

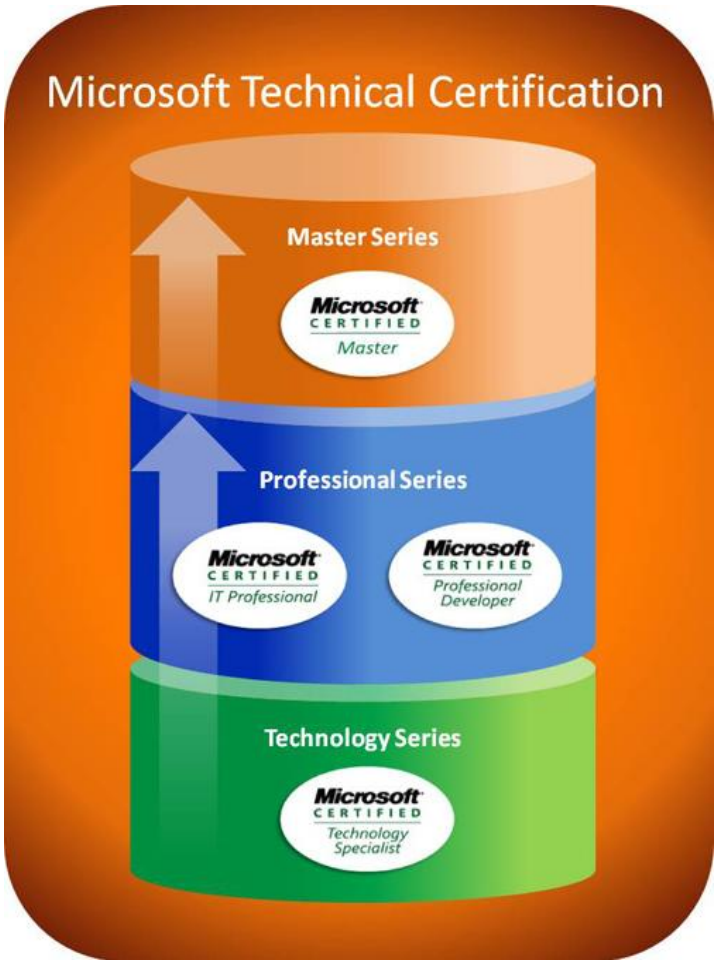
- ✓ CCIE Routing and Switching
- ✓ CCDE
- ✓ CCIE Security
- ✓ CCIE Service Provider
- ✓ CCIE Service Provider Operations
- ✓ CCIE Storage Networking
- ✓ CCIE Voice
- ✓ CCIE Wireless


Routing & Switching
Design
Network Security
Service Provider
Storage Networking
Voice
Wireless
CCNA
CCNA & CCDA
CCNA Security
CCNA
CCNA
CCNA Voice
CCNA Wireless
CCNP
CCDP
CCSP
CCIP
CCNP
CCVP
CCNP Wireless
CCIE Routing & Switching
CCDE
CCIE Security
CCIE Service Provider
CCIE Storage Networking
CCIE Voice
CCIE Wireless


ENTRY
PROFESSIONAL
ASSOCIATE
EXPERT
CCENT
CCNA NETWORK
CCNA SECURITY
CCNA VOICE
CCNA WIRELESS
CCDA DESIGN
CCNP NETWORK
CCNP SECURITY
CCNP VOICE
CCNP SERVICE PROVIDER
CCNP DESIGN
CCIE ROUTING AND SWITCHING
CCIE SECURITY
CCIE VOICE
CCIE STORAGE
CCIE SERVICE PROVIDER
CCDE DESIGN

Career Certifications				
Certification Paths	Entry-Level	Associate	Professional	Expert
Borderless Networks Solutions				
Routing & Switching	CCENT	CCNA	CCNP	CCIE Routing & Switching
Design	CCENT	CCNA & CCDA	CCDP	CCDE
Network Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Collaboration Solutions				
Voice	CCENT	CCNA Voice	CCNP Voice	CCIE Voice
Data Center Solutions				
Storage Networking	CCENT	CCNA	CCNP	CCIE Storage Networking
Service Provider Solutions				
Service Provider	CCENT	CCNA	CCIP	CCIE Service Provider
Service Provider Operations	CCENT	CCNA Service Provider Operations	CCNP Service Provider Operations	CCIE Service Provider Operations

۱۳-۳- مایکروسافت (Microsoft)



مدارک مایکروسافت که به مجموعه آن‌ها MCP (Microsoft Certified Professional) گفته می‌شود، طی امتحانات استانداردی، به افرادی داده می‌شود که در به کارگیری یا پیاده کردن یکی از محصولات یا فناوری‌های مایکروسافت مهارت کافی کسب کرده‌اند. کسب این مدارک، نشان دهنده آن است که صاحب مدرک در به کارگیری آن محصول، محصولات یا فناوری‌ها از نظر شرکت مایکروسافت تخصص کافی دارد. از سوی دیگر، صاحب مدرک می‌تواند به بعضی اطلاعات فنی موجود روی سایت مایکروسافت دسترسی مستقیم داشته باشد. مایکروسافت صاحبان این مدارک را به کنفرانس‌ها و سمینارهای فنی خود دعوت می‌کند و مجله‌ای را هم ویژه این افراد منتشر می‌کند.

۱۳-۳-۱- مدارک شبکه‌ای مایکروسافت

اگر بخواهیم به شبکه نه در مفهوم محض (مشابه نگاه مدرک Network+ کامپتیا) و نه در مفهوم کاملا انحصاری (مشابه تحلیل مدارک سیسکو) آن بنگریم، مدارک مهندسی مایکروسافت، یعنی MCSA و MCSE بهترین مدارکی هستند که دانشجو را به طور مستقیم به سمت مفاهیم کاربردی شبکه‌های ویندوزی رهنمون می‌کنند.این مدارک، دید مختصری از مباحث نظری فناوری شبکه، استانداردهای ارتباطی و تجهیزات شبکه‌ای را در اختیار قرار می‌دهند و با شتاب ملموسی وارد مباحث عملی طراحی، بر پایی و مدیریت شبکه‌های ویندوزی می‌شوند و حتی در پاره‌ای موارد نیز، به طور صریح شخص را جهت کسب اطلاعات و مفاهیم دقیق و مفصل تر، به سمت مدارک تخصصی هر شاخه، نظیر CCNA سیسکو (برای آشنایی

دقیق با ادوات شبکه و پیکر بندی آن‌ها) و +Network کامپتیا (برای کسب اطلاعات دقیق در مورد انواع شبکه پروتکل‌های ارتباطی)، و +Security کامپتیا (برای بررسی محض امنیت شبکه ای) سوق می‌دهد.

اگر نگارنده بخواهد از دید شخصی خود، مسیری را برای رسیدن به نام و عنوان متخصص شبکه (با مدیر شبکه اشتباه نشود) در نظر بگیرد، ه ترتیب فراگیری دوره‌های +NETWORK، MCSE (با گذاندن درس اختیاری +SECURITY) و MCSA را پیشنهاد می کند.

۱۳-۳-۲- MCP

مدرک MCP: Microsoft Certified Professional یا مدرک متخصص مایکروسافت اولین مرحله در جهت اخذ گواهینامه‌های دیگر مانند MCSE و MCSD می‌باشد. MCP پس از گذراندن اولین امتحان در یکی از دوره‌های مایکروسافت اعطا می‌گردد و پس از آن دارنده MCP می‌تواند در موارد انتخابی امتحان داده و تخصص خود را گسترش دهد.این دوره برای آندسته از افرادی است که توانائی راه اندازی یک محصول یا تکنولوژی مایکروسافت را به عنوان بخشی از راهکار تجاری یک ارگان دارا می‌باشند.

۱۳-۳-۳- MCSA

در بررسی مفاد و مدرک MCSA و MCSE به طور مرتب با چهار واژه اساسی کار با شبکه، یعنی Planning، Implementing، Managing و Maintaining روبه رو می‌شویم که ساختار این دو مدرک مایکروسافت را در قالب طراحی، پیاده سازی، مدیریت و نگهداری شبکه‌های ویندوزی تشکیل می‌دهند.

مدارک MCSA بیانگر تخصص در پیاده سازی، مدیریت و رفع عیب از شبکه‌های مبتنی بر ویندوز است. (یعنی همان واژه‌های چهارگانه شبکه به غیر از طراحی یا Planning). به منظور اخذ این مدرک، داشتن حداقل شش تا دوازده ماه تجربه کاری در زمینه ساختار و سیستم عامل‌های شبکه توصیه می‌شود.

مایکروسافت علت ارایه این مدرک را به این صورت تفسیر می کند که بسیاری از مهندسان و مدیران سیستم‌های شبکه، به صورت روزمره با مسایل مربوط به نگهداری و ارتقای سیستم عامل‌های سمت سرویس گیرنده و یا سرویس دهنده مواجه می‌شوند. در حالی که ممکن است در طول مدت دوران شغلی خود اصلا با مسایل مربوط به طراحی و ایجاد یک شبکه سر و کاری نداشته باشند.

بدین ترتیب مایکروسافت کوشیده است وجود یک رشته تخصصی برای نگهداری، مدیریت، ارتقا و رفع عیب شبکه را با این توجیه که هر شبکه یک بار طراحی و نصب می‌شود،اما هزاران بار نیاز به مدیریت و نگهداری دارد، لازم جلوه دهد. به هر حال و از آن جا که ممکن است دنبال کردن مسایل مربوط به ایجاد و راه اندازی یک شبکه، از ابتدای طراحی به کام کسانی که به مسائل نگهداری و مدیریت این سیستم‌ها علاقمند هستند چندان شیرین نباشد، وجود یک مدرک که بتواند صرفا به این جنبه شبکه بپردازد گریزناپذیر به نظر می‌رسد.به همین دلیل مایکروسافت، مدرک CSA را با چند تغییر و حذف دروس مربوط به طراحی، از مدرک MCSE مستقل کرد. دوره MCSE 2003 مربوط به سیستم عامل‌های تولید شده مایکروسافت درسال ۲۰۰۳ یعنی Windows XP (NT5.1) و Windows 2003 Server (NT5.2) و سرویس‌های آن می‌باشد.

تعداد امتحانات برای اخذ مدرک MCSA، ۴ امتحان می‌باشد.

۱۳-۳-۴- MCSE

MCSE، که مهمترین مدرک مایکروسافت در زمینه شبکه می‌باشد بیانگر تسلط کامل به طراحی و پیاده سازی سیستمهای مربوط به شبکه‌های Windows2003 و محصولات دوره‌های Back office می‌باشد و جهت آندسته از افرادی طراحی شده است که توانائی آنالیز نیازهای تجاری یک ارگان را دارا بوده و قادر به طراحی و راه اندازی ساختار شبکه برای راهکارهای تجاری مبتنی بر سیستم عاملهای مایکروسافت و نرم‌افزار Server مایکروسافت باشند.این مدرک برای مهندسان سیستم، مهندسان پشتیبانی فنی، تحلیلگران سیستم، تحلیلگران شبکه و مشاوران فنی مناسب است و نشانه حداقل یک سال تجربه کار راه اندازی و مدیریت شبکه‌های مایکروسافتی درابعاد متوسط تا بزرگ می‌باشد.

MCSE on windows 2003 برای متخصصین تکنولوژی اطلاعاتی است (IT) که به طور ایده آل در محیط‌های شبکه پیچیده کامپیوتری با اندازه متوسط تا بزرگ مشغول به کار می‌باشند. در واقع، این مدرک برای مهندسان سیستم، مهندسان پشتیبانی فنی، تحلیلگران سیستم، تحلیلگران شبکه و مشاوران فنی مناسب است. این مدرک، از پرطرفدارترین و معروف‌ترین مدارک فنی به حساب می‌آید. کسی که برای کسب این مدرک اقدام می‌کند، باید دست کم تجربه‌ای یک ساله در پیاده کردن و مدیریت یک سیستم عامل تحت شبکه با ۲۰۰۰ کاربر و در ۵ نقطه فیزیکی داشته باشد. علاوه بر آن، نامزد MCSE باید دست کم یک سال تجربه در زمینه پیاده کردن و مدیریت سیستم عامل روی رایانه شخصی و طراحی زیرساخت شبکه داشته باشند. افراد داوطلب دریافت این گواهینامه باید در مجموع هفت امتحان شامل پنج آزمون اصلی (Core) و دو امتحان انتخابی (Elective) را با موفقیت پشت سر بگذارند. این امتحان انتخابی شامل امتحانات compTIA نیز می‌گردد.(Network+/A+)

مدرک MCSE دارای دو گرایش زیر می‌باشد

MCSE 2003: Security
MCSE 2003: Messaging

تعداد امتحانات برای اخذ این مدرک، ۷ امتحان می‌باشد.

۱۳-۳-۵- مقاد آزمون MCSA و MCSE

همان گونه که قبلا گفته شد، مدرک MCSA به مفهوم مدیریت و نگهداری به صورت متمرکز و پیاده سازی به صورت مختصر پرداخته است. در حالی که در MCSE هر چهار عنصر طراحی، پیاده سازی، مدیریت و نگهداری به صورت متمرکز و تفصیلی مورد بررسی قرار گرفته است.

الف- دوره‌های شبکه ای

این دوره‌ها چهار آزمون مختلف را در بر می‌گیرند که برای مدرک MCSA فقط دو آزمون شماره ۲۹۰ و ۲۹۱ و برای مدرک MCSE هر چهار آزمون ۲۹۰ و ۲۹۱ و ۲۹۳ و ۲۹٤ باید گذرانده شود.

۱- آزمون ۲۹۰ (Managing & Maintaining Win2003 Environment)

این درس نگاهی مفصل به سیستم عامل ویندوز ۲۰۰۳ از جایگاه یک سرور شبکه دارد و قسمت‌های مختلف آن، از جمله مرکز کنترل، ابزارهای مدیریتی(Administration Tools) ، مانیتورینگ عملکرد سرور (دیسک، پردازنده، حافظه، کارت شبکه)، نحوه انجام امور مختلف مدیریتی، مثل مدیریت کاربران در اکتیو دایرکتوری شش، ایجاد نسخه‌های پشتیبان از

اطلاعات هارددیسک، پیکربندی سخت‌افزارهای داخلی و شبکه‌ای و به طور کلی تعامل با ویندوز ۲۰۰۳ مورد بررسی قرار می‌گیرد.

۲- آزمون ۲۹۱ (Implementing,Managing & Maintaining Win 2003 Network Infra)

همان گونه که از نام این آزمون بر می‌آید، مسائل مربوط به پیاده سازی سرویس‌های مختلف شبکه‌ای مثل DHCP، DNS، ROUTING، VPN و امثال آن، که از اساسی ترین ابزارهای ارتباطی میان کاربران و سرور محسوب می‌شسوند و در واقع وجود یک شبکه بدون نیاز به این سرویس‌ها معنای خاصی ندارد، در این دوره مورد بررسی قرار می‌گیرد.

دانشجویان پس از طی دوره ۲۹۰ و ۲۹۱ قادر خواهند بود انواع سرویس‌های شبکه‌ای مثل دامنه، اشتراک فایل و چاپگر، پراکسی، فایرول، اینترنت، اتصال راه دور، تعریف کاربران و گروه‌های کاربری را در شبکه ویندوزی ایجاد کند و امنیت استفاده و نگهداری از آن را در دست گیرند (تا سطح MCSA).

۳- آزمون ۲۹۳ (Planning & Maintaning Win 2000 Netwotk Infra)

این دوره ویژه داوطلبان MCSE است، در واقع مطالب مورد بحث در آزمون ۲۹۱ را با نگرشی بسیار عمیق تر، مورد بررسی قرار می‌دهد و به افراد، قدرت تحلیل مسایل و شرایط مختلف یک شبکه را می‌بخشد.

پس از طی این دوره، دانشجویان قادر خواهند بود شبکه‌های بزرگ مبتنی بر پروتکل TCP/IP را با توجه به نیازها و امکانات موجود طراحی کنند و سرویس‌ها، کنترل‌ها و روال‌های نظارت و مانیتورینگ عملکرد اجزای مختلف و امنیت آن‌ها را بر قرار سازند و آن را مدیریت نمایند.

٤- آزمون ۲۹٤ (Planning , Implementing , Maintaining Active Directory)

این دوره نیز که ویژه MCSE در نظر گرفته شده است، کلیه مسایل مربوط به اساس کنترل دامنه ویندوزی و کاربران را که اکتیو دایرکتوری نام دارد، پوشش می‌دهد. ظاهرا سرویس اکتیو دایرکتوری که در واقع اساسی ترین جز ویندوزهای سرور را تشکیل می‌دهد، آن قدر از طرف مایکروسافت مهم شناخته شده که یک دوره و آزنون مستقل بلرای کشف تمام نکات و جزئیات آن اختصاص داده است.

ب- سیستم عامل‌های کلاینت

در هر دو مدرک MCSA و MCSE دو آزمون ویژه سیستم عامل کلاینت، یعنی ویندوز ۲۰۰۰ حرفه‌ای و ویندوز اکس پی وجود دارد که داوطلبان باید حتما یکی از آن دو را بگذرانند.

در هر دو دوره، نحوه نصب و پیکر بندی کلاینت چه از لحاظ ارتباط با سخت‌افزار و چه از لحاظ استفاده از سرویس‌های شبکه‌ای یک سرور ۲۰۰۳، مثل استفاده از اینترنت به اشتراک گذاشته شده، فایل‌ها و چاپگرهای شبکه‌ای، اتصال به یک VPN و امثال آن در سیستم عامل‌های مربوطه آموزش داده می‌شود.

ج- طراحی شبکه (فقط MCSE)

در بخش طراحی شبکه، دو درس و آزمون برای مختلف برای داوطلبان MCSE در نظر گرفته شده که گذراندن یکی از آن‌ها برای کسب مدرک MCSE کافی است.

۱- Designing Win 2003 Active Directory Network Infra

این دوره که به آزمون ۲۹۷ مشهور است، سعی می‌کند به ساختار شبکه‌های ویندوزی و اکتیو دایرکتوری نگاهی تحلیلی و جامع‌تر داشته باشد. تمام مباحثی که قبل از بر با ساختن یک شبکه، مثل برآورد نیازمندی‌های سخت‌افزاری، نرم‌افزاری، پیش بینی و ارایه طرح هایی برای مشخص نمودن انواعگروه‌های کاربری، اتخاذ سیاست‌های امنیتی در سطح کلان، ارئه راهکارهای اساسی برای پیکربندی بنیادین سرویس‌های شبکه‌ای مثل DNS، DHCP و بسیاری از تصمیمات استرادژیک و ساختاری، در این دوره مورد بررسی قرار می‌گیرد.

۲- Designing Win 2003 Network Security

این دوره که به آزمون ۲۹۸ مشهور است، بر نحوه انتخاب و اتخاذ سیاست‌های امنیتی، تمرکز خاصی دارد. در این دوره تمام گزینه هایی که به شکلی با مقوله امنیت ارتباط دارند (نظیر انواع پروتکل‌های ارتباطی، سخت‌افزار، سرویس‌های مختلف، کاربران، پروتکل‌های امنیتی IPSec، SSL مباحث مربوط به فیلترینگ، فایروال، امنیت در شبکه‌های VPN، اینترنت، وب سرور IIS، روش‌های اعتبار سنجی و امثال آن) مورد تحلیل قرار می‌گیرد و داوطلبان با نحوه پیش بینی و برآورد نیازمندی‌های کلان آشنا می‌شوند.

د- دروس اختیاری

آزمون‌های اختیاری، به برنامه‌های جانبی و ابزارهای مایکروسافت که به عنوان نرم‌افزارهای کمکی برای ویندوز ۲۰۰۳ یا اکس پی جهت افزایش قابلیت‌های آن به کار می‌رود، مربوط می‌شود.

از بین این آزمونها، یک آزمون به دلخواه برای کسب هر دو مدرک باید گذرانده شود.بانک اطلاعاتی SQL Server، ایمیل سرور Exchange، سرور مدیریت سرویس (System Management Server)، پراکسی و فایروال ISA Server و چند محصول دیگر مایکروسافت، در این دروس اختیاری دیده می‌شود.

در ضمن مدرک +Security متعلق به موسسه آموزشی کامپتیا در این جمع به چشم می‌خورد.

۱۳-۳-۶- *MCITP*

دوره MCITP 2008 مربوط به سیستم عامل‌های تولید شده مایکروسافت از سال ۲۰۰۸ به بعد می‌باشد در حال حاضر جدیدترین دوره موجود که توسط مایکروسافت ارائه شده است بر روی سیستم‌های Windows Seven (NT 6.1) و Windows 2008 Server R2 (NT 6.1) و سرویس‌های آن می‌باشد. مدرک MCITP یعنی داشتن تخصص در مهندسی شبکه‌های مایکروسافت. چنانچه افراد بتوانند موفق به اخذ این مدرک شوند، مهارت‌های لازم را در ویندوز سرور ۲۰۰۸ پیدا خواهند کرد و آنگاه می‌توانند در بازارکار، در عناوین شغلی مدیریت شبکه، مدیریت IT، مدیریت امنیت شبکه و بالاخره طراحی شبکه، مشغول به کار شوند. در این دوره افراد با کلیه جزئیات مربوط به دسترسی کاربران درون شبکه، شناخت نیازهای یک شبکه به سرویس‌های مختلف، طراحی یک شبکه، مدیریت آن و در نتیجه رفع اشکالات مختلفی که در نحوه عملکرد سرویس‌ها یا ارتباطات درون شبکه‌ای و برون شبکه‌ای ایجاد می‌شود ، آشنا می‌شوند. در واقع به طور خلاصه می‌توان گفت، این مدرک به افرادی اعطاء خواهد شد که توانایی کارکردن بصورت حرفه‌ای با سرویس هایی مثل: Terminal Service، SharePoint، IIS، Clustering، DNS، Active Directory DHCP، RRAS و... را داشته باشند.

کد آزمون	نام دوره	سرفصل ها
70-680	Windows 7 Configuring	Install, Migrate, or Upgrade to Windows 7 Configuring System Images Deploying System Images Managing Devices and Disks Managing Applications Network Settings Windows Firewall and Remote Management BranchCache and Resource Sharing Authentication and Account Control DirectAccess and VPN Connections BitLocker and Mobility Options Windows Update and Windows Internet Explorer Monitoring and Performance Recovery and Backup
70-640	Windows Server 2008 Active Directory Configuration	Installation Administration Users Groups Computers Group Policy Infrastructure Group Policy Settings Authentication Integration Domain Name System with ADDS Domain Controllers Sites and Replication Domains and Forests Directory Business Continuity Active Directory Lightweight Directory Services Active Directory Certificate Services and Public Key Infrastructure Active Directory Right Management Services Active Directory Federation Services
70-642	Windows Server 2008 Network Infrastructure Configuration	Understanding and Configuring IP Configuring Name Resolution Configuring a DNS Zone Infrastructure Creating a DHCP Infrastructure Configuring IP Routing Protecting Network Traffic with IPSec Connecting to Networks Configuring Windows Firewall and Network Access Protection Managing Software Updates Monitoring Computers Managing Files Managing Printers
70-643	Windows Server 2008 Applications Infrastructure Configuration	Implementing and Configuring a Windows Deployment Infrastructure Configuring Server Storage and Clusters Installing and Configuring Terminal Services Configuring and Managing a Terminal Services Infrastructure Installing and Configuring Web Applications Managing Web Server Security Configuring FTP and SMTP Services Configuring Windows Media Services Configuring Windows SharePoint Services
70-647	Windows Server 2008 Enterprise Administrator	Planning Name Resolution and Internet Protocol Addressing Designing Active Directory Domain Services Planning Migrations , Trusts , and Interoperability Designing a Network Access Strategy Design a Branch Office Deployment Planning Terminal Services and Application Deployment

Server and Application Virtualization Planning and Designing a Public Key Infrastructure Designing Solution for Data Sharing , Data Security , and Business Continuity Designing Software Update Infrastructure and Managing Compliance		

خوب حالا اول MCSE 2003 یا MCITP 2008؟

با توجه به اطلاعات مربوط به استفاده از سیستم عامل‌های کلاینت و سرور در سطح دنیا، سیستم عامل‌های تولید شده توسط مایکروسافت در سال ۲۰۰۳ با توجه به وجود سیستم عامل‌های ۲۰۰۸ مایکروسافت هنوز هم محبوب هستند. علت این امر در واقع دانش کاربران، نیازهای آن‌ها و سخت‌افزارها کاربران می‌باشد بسیاری از کاربران هنوز آماده نشده‌اند تا بتوانند خودشان را با شرایط سیستم عامل جدید وقف دهند ممکن است بسیاری از کاربران بتوانند سخت‌افزار مورد نیاز را تهیه نمایند اما سطح دانش و راحتی کار با ویندوز XP باعث شده تا هنوز کاربران از ویندوز XP را استفاده کنند.

اما شرایط برای مدیرهای شبکه کمی متفاوت است در واقع در سه عامل دانش کاربران، نیازها و سخت‌افزار دراینجا بیشتر خودش را نشان می‌دهد برای شروع کسانی که می‌خواهند با سرور ۲۰۰۸ کار کنند بهتر است اول سرور ۲۰۰۳ شروع کنند علت چیست؟ ارتقا سرورها از ۲۰۰۳ به ۲۰۰۸ در یک سازمان دردسرهای زیادی را به همراه دارد از جمله این دردسرها را می‌توان به سطح دانش مدیران شبکه و سخت‌افزار شبکه دانست در لینک بالا می‌توان میزان استفاده از حافظه و پردازنده این دو سرور را با هم مقایسه کرد ویندوز سرور ۲۰۰۳ سریع‌تر و محیط ساده تری دارد اما از لحاظ امنیتی و کارایی سرور ۲۰۰۸ بهتر از ویندوز ۲۰۰۳ می‌باشد. همچنین برای یک سازمان سخت است تا بتواند یکجا هم مدیران شبکه و هم سخت‌افزارها را ارتقاء دهند.

اما باتوجه به تمام نکات بالا روز به روز به کاربران سیستم عامل‌های ۲۰۰۸ مایکروسافت افزوده می‌شود؛ پیشنهاد ما به شما این است که از MCSE 2003 شروع و آن را به MCITP 2008 ارتقاء (Upgrade) دهید.

روش ارتقاء

شما باید آزمون ۷۰-۶۴۹ (Upgrade Exam) را بگذرانند که در واقع جایگزین آزمونهای ۷۰-۶۴۰ ، ۷۰-۶۴۲ ، ۷۰-۶۴۳ خواهد بود. در ضمن باید آزمونهای Enterprise Server Administrator MCITP و Seven Client را نیز پشت سر بگذارید.

۱۳-۳-۷- وضعیت درآمد

طبق آمار مجله Certificatian، میانگین درآمد دارندگان این دو مدرک در سال ۲۰۰۴، حدود ۶۷ هزار دلار برای مدرک MCSE و ۵۸ هزار دلار برای مدرک MCSA است.

این عدد در مقایسه با میزان درآمد سالیانه ۹۰ مدرک معتبر بین المللی دیگر، در جایگاه شصت و هشتم برای مدرک MCSE قرار دارد. طبق همین آمار، میزان درآمد افراد شاغل در پست‌های طراحی یا مدیریت شبکه‌های ویندوزی با کسب مدرک MCSE، حدود ۱۲ درصد نسبت به زمان قبل از کسب آن افزایش یافته است. به هر حال با توجه به افزایش ۴ هزار

دلاری درآمد سالیانه دارندگان مدرک MCSE در سال ۲۰۰۴ نسبت به سال قبل، می‌توان در پی رشد و توسعه شبکه‌های ویندوزی به افزایش دوباره آن در سال‌های آینده نیز امید داشت.

۱۳-۳-۸- مزایای دستیابی به مدارک مایکروسافت

- دریافت مدرک بین المللی مایکروسافت (Certificate & Transcript)
- دریافت کارت شناسایی مایکروسافت (Wallet Card)
- دریافت Pin مخصوص مایکروسافت حاوی لوگوی مدرک مربوطه (Lapel Pin)
- امکان استفاده از لوگوی مایکروسافت
- موقعیت شغلی و استخدامی بهتر با توجه به تخصص و دانش مورد تأیید مایکروسافت در مورد محصولات و فن آوری این شرکت
- امکان دستیابی مستقیم به اطلاعات تکنیکی مربوط به محصولات از طریق ناحیه ویژه وب سایت MCP در مایکروسافت با اعطای Account مخصوص.
- عضویت در وب سایت اختصاصی MSDN online که اجازه دستیابی به بهترین منابع تکنیکی، ارتباط با جامعه MCP و دسترسی به منابع و سرویس‌های با ارزشی را به دارنده آن می‌دهد.
- دعوت به سمینارها، جلسات آموزش تکنیکی و رویدادهای خاص مایکروسافت.
- اشتراک OnLine مجله ارزشمند Microsoft Certified Professional Magazine Online

۱۳-۳-۹- دیگر مدارک مایکروسافت

MCDBA

MCDBA مخفف عبارت Microsoft Certified Database Administrator بوده و به مدیران پایگاه داده‌های SQL DATABASE اختصاص دارد؛ کسانی که به طراحی، پیاده سازی و مدیریت این کارگزار (Server) مشغولند. در حال حاضر، این مدرک روی SQL Server 2000 ارائه می‌شود.

MCT

دارندگان مدرک MCT (Microsoft Certified Trained) استادانی هستند که از سوی مایکروسافت، برای تدریس و آموزش دوره‌های مایکروسافت تاییده شده‌اند. برای دریافت این مدرک باید یکی از دیگر مدارک MCP را داشت.

MCAD

MCAD که مخفف عبارت Microsoft Certified Application Developer می‌باشد. مدرکی است برای کسانی که از فناوری‌های مایکروسافت برای توسعه و نگهداری برنامه‌های کاربردی، برنامه‌های تحت وب و سرویس‌های داده‌ای استفاده می‌کنند. افرادی که به XML یا.NET تسلط دارند و از آن‌ها برای ارائه برنامه‌های مختلف استفاده می‌کنند در این گروه قرار می‌گیرند. کسانی که برای دریافت این مدرک، نامزد می‌شوند باید یک یا ۲سال تجربه در این زمینه داشته باشند. برنامه‌نویسان، تحلیلگران برنامه و تولیدکنندگان نرم‌افزار می‌توانند برای کسب این مدرک اقدام کنند.

MCSD

دارندگان مدرک MCSD (Microsoft Certified Solution Develper) افرادی هستند که با فناوری‌ها، سیستم‌های عامل و معماری ویندوز، راهکارهای مناسبی را برای صاحبان صنایع و تجارت طراحی کرده و توسعه می‌دهند. دست کم یک تجربه ۲ ساله کاری برای خواستاران این مدرک لازم است. مهندسان نرم‌افزار. تحلیلگران و تولیدکنندگان برنامه‌های کاربردی و مشاوران فنی کسانی هستند که داشتن این مدرک را به آن‌ها توصیه می‌کنیم.

MOS

مدرک MOS (Microsoft Office Specialist) به کسانی داده می‌شود که در کار با مجموعه نرم‌افزارهای Office یعنی Word، Excel، Outlook، Powerpoint، Access و MS Project مهارت کافی داشته باشند. از آنجا که مجموعه Office در بیش از ۱۰۰کشور و با ۱۸ زبان در اختیار کاربران قرار می‌گیرند. می‌توان آن را فراگیرترین مدرک مایکروسافت دانست. بد نیست بدانید که ماهانه ۳۲۰۰۰ نفر در سراسر دنیا این مدرک را دریافت می‌کنند.

MOS

مدرک Microsoft Office Specialist Master Instructor به کسانی داده می‌شود که برای تدریس بخش‌های مختلف Office مهارت کافی داشته باشند. خواستاران این مدرک باید دست کم از ۲ سال تجربه تدریس این نرم‌افزارها بهره‌مند باشند.

Exchange

در این دوره افراد توانایی پیکربندی یکی از قدرتمندترین و معروفترین ایمیل سرورهای دنیا را فرا می‌گیرند. Exchange 2010 در حال حاضر به عنوان کارآمدترین ایمیل سرور دنیا شناخته می‌شود و افراد پس از گذراندن این دوره می‌توانند Exchange را برای سازمان‌های با مقیاس کوچک، متوسط و بزرگ راه اندازی نمایند.

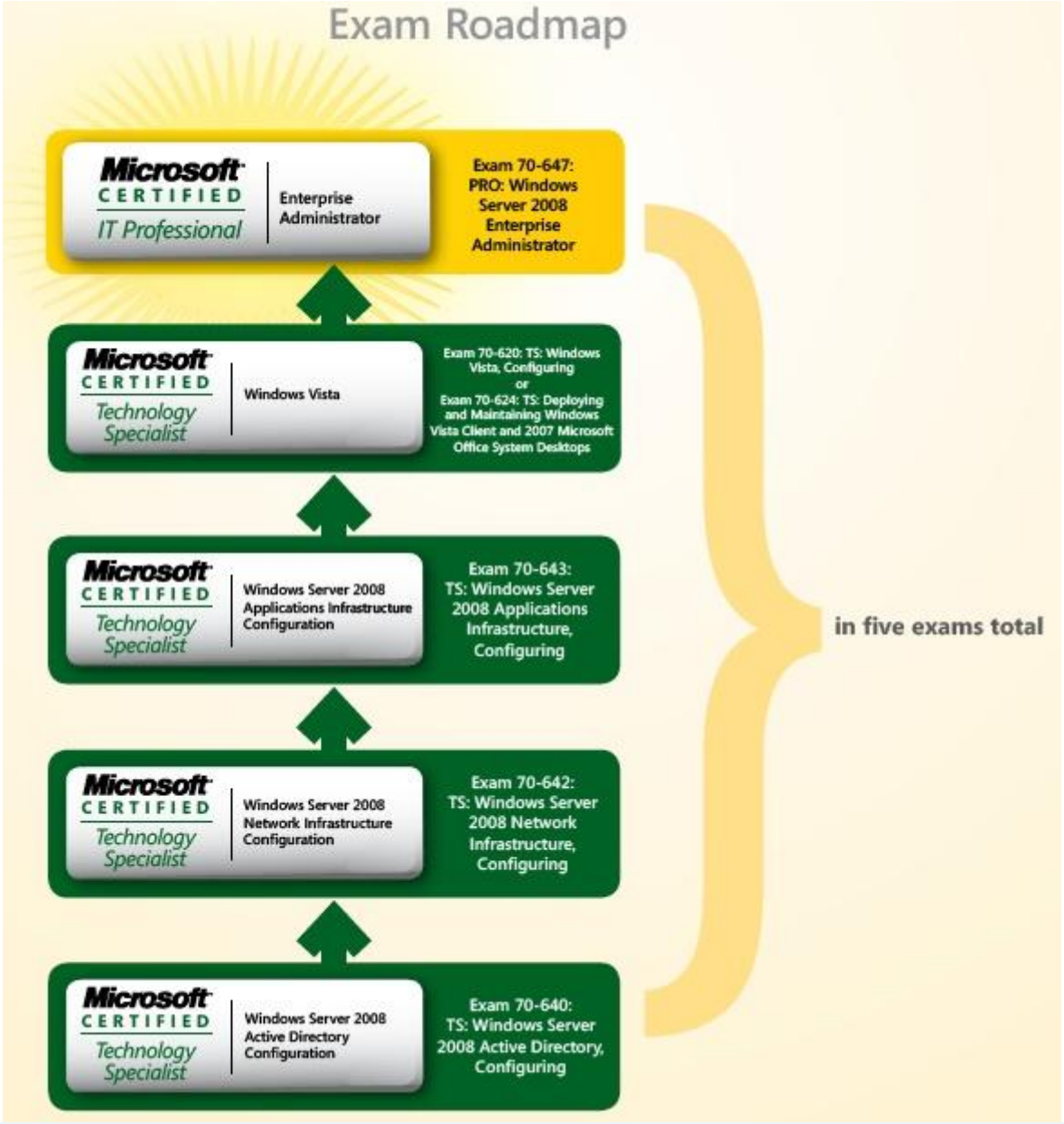
TMG

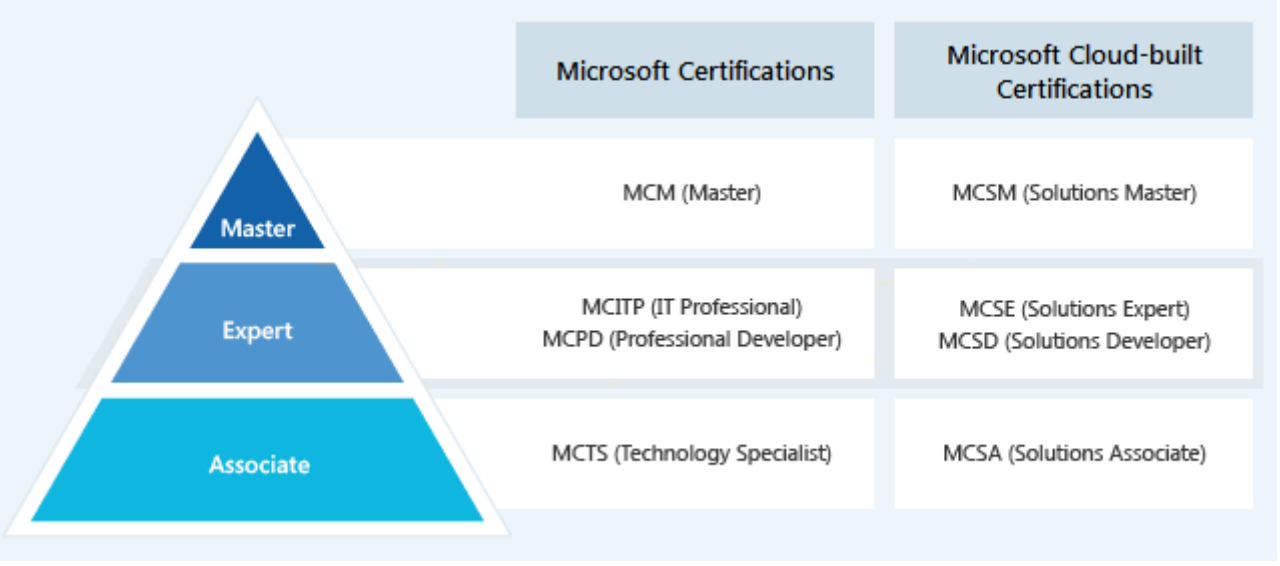
TMG شما را قادر می‌سازد تا از اینترنت به صورت امن و مطمئن و بدون نگرانی از تهدیدات نرم‌افزارهای جاسوسی و یا تهدیدات دیگر استفاده کنید. درگذشته این وظیفه را ISA عهده دار بود که از سال ۲۰۱۰ به بعد TMG بشکلی کاملتر این کار را انجام می‌دهد. افرادی که این دوره را طی کنند می‌توانند بر روی لبه شبکه خود تنظیمات امنیتی را طراحی و پیاده سازی نمایند.

MCSE Cloud

مدرکی جدید از مایکروسافت که به آموزش شبکه‌سازی در فضای Cloud و عموما به کمک مجازی‌سازی می‌پردازد.

۱۳-۳-۱۰- خلاصه مدارک مایکروسافت





MCSA Microsoft Certified Solutions Associate	MCSE Microsoft Certified Solutions Expert	MCSD Microsoft Certified Solutions Developer
MCSA Windows Server 2012	MCSE Business Intelligence	MCSD Windows Store Apps
MCSA SQL Server 2012	MCSE Communication Certification	MCSD Web Application
MCSA Windows 8	MCSE Desktop Infrastructure	MCSD Application Lifecycle Management
	MCSE SharePoint Certification	
	MCSE Data Platform	
	MCSE Server Infrastructure	
	MCSE Private Cloud certification	

۱۳-۴- کامپتیا (CompTIA)





۱۳-۴-۱- *Network+*

با پیشرفت علوم رایانه‌ای و فن آوری اطلاعات هر روزه استفاده از شبکه‌های رایانه‌ای فراگیرتر و گسترده‌تر می گردد. به تبع این امر، نیاز به متخصصین و تکنسین‌های شبکه نیز در این عرصه اجتناب ناپذیر می‌باشد. مدرک تخصصی تکنسین شبکه مربوط به شرکت کامپتیا یا Network+ بر آورنده چنین نیازی است. افراد دارای این مدرک دارای دانش مورد تایید در زمینه شبکه، توپولوژی‌ها، پروتوکل‌ها، استانداردها، راه اندازی و پشتیبانی شبکه می‌باشند که معادل نه ماه تجربه کار در شبکه می‌باشد.دنیای تکنولوژی این مدرک را به عنوان بهترین نقطه ورود به دنیای شبکه می‌شناسد. مهمترین شرکتهای کامپیوتری دنیا از جمله Microsoft، Novell، Cisco، Compaq، Lotus و 3Com این مدرک را به عنوان بخشی از روند اخذ مدرک خود دانسته و برخی از شرکت‌ها نیز این مدرک را جهت کارمندان خود جهت استخدام لازم می‌دانند.

تعداد امتحانات

اخذ مدرک + Network نشانه مهارت در زمینه عملکرد اجزای شبکه و نصب، راه اندازی و عیب یابی اولیه سخت‌افزارهای شبکه، پروتکل‌ها و سرویس‌های آن می‌باشد. آزمون این مدرک توانایی تکنیکال در حیطه مدیاها، پروتکل‌ها، استانداردها، راه اندازی و پشتیبانی شبکه و تکنولوژِهای جدید از جمله Wireless Networking و Gigabit Ethernet را مورد ارزیابی قرار می‌دهد.در حقیقت مباحثی که این مدرک در بر می‌گیرد شامل موارد زیر می‌گردد:

- ✓ Network+ Basics
- ✓ Network+ Hardware
- ✓ Network+Connections
- ✓ Networking Software
- ✓ Data Link Layer Protocols
- ✓ Network Layer Protocols
- ✓ Transport Layer Protocols
- ✓ TCP/IP Fundamentals
- ✓ TCP/IP Applications
- ✓ TCP/IP Configuration
- ✓ Remote Network Access
- ✓ Network Security
- ✓ Planning the Network
- ✓ Installing a Network
- ✓ Network Maintenance
- ✓ Network Troubleshooting Procedures
- ✓ Network Troubleshooting Tools
- ✓ Network Troubleshooting Scenarios

۱۳-۴-۲- A+

مدرک CompTIA A+ با شماره آزمون BR0-003 یک استاندارد فنی برای کارشناسان فنی پشتیبان کامپیوتر می‌باشد. متخصصان کامپیوتر با استفاده از این مدرک شایستگی‌های خود را در در نصب، نگهداری و پیشگیری از مشکلات، شبکه سازی، امنیت و اشکال زدایی در سطح بین المللی اثبات می‌کنند. متخصصان فنی که مدرک CompTIA A+ را کسب کرده‌اند، با استفاده از مهارتهای ارتباطی برای کار با Clientها بهترین خدمات رسانی را به مشتریان دارا می‌باشند.

مدرک A+ بیانگر وجود یک تخصص عمومی درباره سخت‌افزار در شخص صاحب این مدرک بوده و وی به عنوان تکنسین سخت‌افزار کامپیوتر شناخته می‌شود. برای شرکت در دوره‌های آمادگی کسب این مدرک، شرکت کامپتیا حداقل ۵۰۰ ساعت تجربه قبلی آشنایی و کار با سخت‌افزار کامپیوترهای شخصی را توصیه می‌کند. از نکات برجسته این دوره و مدرک مربوط به آن، این است که بسیاری از شرکت‌های معتبر تولیدکننده سخت‌افزار کامپیوتر، گذراندن آن را به کاربران خود و کسانی که قصد دارند در زمینه‌هایی مثل مونتاژ کامپیوتر فعالیت کنند توصیه می‌نمایند.

در حالی که در این دوره به هیچ آیتم خاصی که محصول کارخانه خاصی باشد اشاره نشده و صرفاً قطعات و قسمت‌های مختلف یک کامپیوتر از لحاظ فنی مورد بررسی قرار می‌گیرند. همچنین علاوه بر این موارد، نحوه نصب سیستم‌عامل، تنظیم، پیکربندی سخت‌افزار در آن و آماده نمودن یک دستگاه کامپیوتر برای اتصال به شبکه از جمله تجاربی است که یک داوطلب کسب مدرک A+ باید دارا باشد. هم‌اکنون بیش از یکصد شرکت تولیدی و یا آموزشی، مدرک A+ را به عنوان پیش‌نیاز

برای کار یا کسب مدارک خود معرفی نموده‌اند و شرکت‌های معتبری چون مایکروسافت، HP، سیسکو، آی‌بی‌ام و بسیاری دیگر در سایت خود از مدرک مذکور به عنوان یک مدرک پایه‌ای جهت پرداختن به امور فنی یک کامپیوتر نام برده‌اند.

مدرک CompTIA A+ یک قسمت از مدارک سازمان هایی مانند Microsoft، Hewlett-Packard، Cisco و Novell می‌باشد. دیگر کمپانی هایی که دارای این تکنولوژی هستند مانند CompuCom و Ricoh کسب مدرک CompTIA A+ را جزو الزامات متخصصان سرویس دهنده خود کرده‌اند.

دروس

در این دوره، ابتدا با چگونگی کار قطعات داخلی یک کامپیوتر و نحوه ارتباط سخت‌افزار و نرم‌افزار با یکدیگر آشنا می‌شویم. در قسمت بعد ساختار یک مادربُرد (MotherBoard) یا همان برد اصلی کامپیوتر که سایر قطعات به آن متصل یا روی آن سوار می‌شوند، مورد کالبد شکافی قرار می‌گیرد. سپس در بخش‌های بعد ابتدا مواردی چون حافظه‌های اصلی (RAM)، فلاپی‌درایو و سایر دستگاه‌های ورودی یا خروجی مثل ماوس یا پرینتر و سپس مبحث مهم نصب هارددیسک مورد بحث قرار می‌گیرد.

همچنین در مورد منبع تغذیه و قسمت‌های الکترونیکی یک کامپیوتر و نحوه رفع ایراد و مشکل از آن‌ها مطالبی به داوطلبان آموخته می‌شود. در فصول بعد ضمن آشنایی با مفاهیم سیستم‌عامل و نحوه ارتباط آن با سخت‌افزار موجود در سیستم، نحوه ایجاد هماهنگی بین آن دو و همچنین تنظیم بهینه سخت‌افزار و نرم‌افزار برای به حداکثر رساندن کارایی کلی و سرعت کامپیوتر مورد بررسی قرار می‌گیرد. در قسمت‌های بعد نوبت به بحث شبکه و نحوه آماده‌سازی و پیکربندی قسمت‌های مربوط به آن مثل کارت شبکه، مودم، کابل‌های اتصال تلفن و اترنت می‌رسد و در قسمت‌های آخر نیز مباحثی چون نحوه مقابله با ویروس‌های کامپیوتری و کلاً نحوه نگهداری و پشتیبانی از یک دستگاه کامپیوتر جهت آماده نگهداشتن آن برای مصارف گوناگون آموزش داده می‌شود.

آزمون ها

برای کسب این مدرک A+ آزمون‌های زیر را باید گذرانده باشید:

Exam 220-701 CompTIA A+ Essentials

این آزمون به سنجش مهارتهای اصلی تکنولوژی کامپیوتر، شبکه سازی و امنیت و همچنین مهارتهای ارتباطی و پیشرفته‌ای مورد نیاز برای تمامی تازه واردان IT می‌باشد.

Exam 220-702 CompTIA A+ Practical Application

این آزمون به منظور سنجش دانش و مهارت‌های توسعه یافته متخصصان‌ای تی که در آزمون CompTIA A+ Essential کسب کرده‌اند، می‌باشد. (که این مهارت‌های توسعه یافته شامل اشکال زدایی و استفاده از ابزارهایی برای حل مشکلات بوجود آمده می‌باشد.)

وضعیت درآمد

طبق آمار مجله certification، میانگین درآمد سالانه دارندگان مدرک A+ در سال ۲۰۰۴ تاکنون، معادل ۲۷ هزار دلار در سال بوده است که در مقایسه با دارندگان سایر مدارک مثل MCSE،Network+ یا CCNA از جایگاه جالب توجهی برخوردار نمی‌باشد. دلیل آن هم کاملاً مشخص است. داشتن مدرک A+ برای اشخاصی که مایلند در کار نصب و پشتیبانی

سخت‌افزار مشغول شوند لازم بوده ولی کافی نمی‌باشد. همچنین تخمین زده می‌شود که تاکنون در حدود چهارصدهزار نفر در سراسر دنیا موفق به کسب مدرک A+ شده‌اند که در یک نظرسنجی (از بیش از یکصد نفر) حدود ۹۰ درصد آن‌ها شرکت در دوره‌های تخصصی و موفقیت در گذراندن آزمون A+ را عامل مهمی در بالا رفتن سطح شغلی و افزایش درآمد خود دانسته‌اند. درصد رشد علاقه‌مندان به کسب مدرک A+ در سال ۲۰۰۴ به صورتی بوده است که این مدرک به همراه مدارک MCSE،CCNA و +Secutity جزء پرطرفدارترین مدارک این سال شناخته شده‌اند.

۱۳-۴-۳- Server+

+Server عنوان مدرکی است که در آن به حوزه تخصصی سرورها و نحوه نصب، استفاده و رفع عیب آن‌ها پرداخته می‌شود. شرکت CompTIA که ارایه‌دهنده این مدرک است، در سایت اینترنتی خود علاقمندان به زمینه‌های تخصصی شبکه خصوصاً مفاهیم مربوط به ساختار و بدنه سرورها و اصول سخت‌افزاری و پیکربندی آن‌ها را به دریافت این مدرک توصیه می‌نماید. طبق اظهارات مسؤولین امور آموزشی این شرکت، دارندگان مدرک مذکور بدون داشتن هیچگونه پیش‌نیازی قادرند اطلاعات جامع و مدونی را در رابطه با سرورها و عملکرد بخش‌های مختلف آن‌ها در دریافت، ارسال، پردازش و ذخیره‌سازی اطلاعات، کسب کنند. مفاهیمی چون RAID، SCSI و Muti CPU از جمله موارد مهمی هستند که در بررسی یک سرور مورد توجه قرار گرفته‌اند. دوره +Server قادر است دانش فنی دانشجویان خود را در زمینه نصب، پیکربندی، ارتقاء، نگهداری و رفع ایرادات یک سرور به حد بسیار مطلوبی افزایش دهد.

پس از طی این دوره، داوطلبان قادر خواهند بود انواع سرورهای مختلف و کلیه سخت‌افزارها و نرم‌افزارهای قابل نصب در آن‌ها را تشریح کنند، سرورهای مذکور را در یک محیط شبکه‌ای وارد و ارتباط لازم را برقرار کنند، سرورها را برای بهترین سرعت و کارایی آن‌ها پیکربندی و تنظیم نمایند، سخت‌افزارها و نرم‌افزارهای آن‌ها را به موقع ارتقاء دهند، عوامل محیطی و شبکه‌ای مؤثر بر کارایی و عملکرد یک سرور را شناسایی و بهینه کنند و هرگونه اتفاق غیرمنتظره قابل وقوع برای یک سرور را تشخیص داده و در جهت پیشگیری و یا رفع آن اقدام کنند. سرپرست شبکه‌ها در شرکت‌ها و مؤسسات تجاری با حداقل ۹ ماه سابقه کار در این شغل، بهترین و مناسب‌ترین افراد برای کسب مدرک +Server هستند. اگر چه این مدرک به‌طور رسمی هیچگونه پیش‌نیازی ندارد اما شرکت کامپتیا داشتن مدرک و یا حداقل داشتن اطلاعات و تجربه قبلی در حد مدرک +Network را به کارآموزان توصیه می‌نماید. همان‌طور که تمرکز مدرک +Network برروی سه لایه Physical، Data Link و Network از لایه‌های هفت‌گانه شبکه است، تمرکز مدرک +Server برروی سه لایه Physical،Data Link و Application و به صورت تخصصی‌تر به امور مربوط به سرورهاست.

مزایا

سایت کامپتیا، کسب اطلاعات فنی تخصصی در زمینه سرورها و در نتیجه قدرت انتخاب یک موقعیت شغلی مناسب را از مزایای کسب مدرک +Server می‌داند. همچنین با کسب این مدرک و یا +Network، راه داوطلبان جهت کسب مدارک بالاتر و جامع‌تری مثل +iNet که به طور کامل برروی هفت لایه شبکه متمرکز شده و به تمام آن‌ها می‌پردازد، هموار می‌شود. ضمن این‌که هزینه پایین‌تر آموزش و کسب مدرک دوره +Server نسبت به بسیاری از مدارک دیگر در زمینه شبکه از دیگر مزایای آن به شمار می‌آید. یک فرد متخصص سرور در سطح مدرک +Server می‌تواند در زمینه‌های متعدد مسایل فنی وارد

عمل شده و حداقل در حد مشاور فنی به همکاران خود توصیه‌های لازم را بنماید. به عنوان مثال می‌تواند به مدیران یا برنامه‌نویسان پایگاه‌های اطلاعاتی در نحوه چیدمان و پیکربندی سرور اصلی یک بانک اطلاعاتی، سرور پشتیبان و یا سروری که نقش دروازه (Gateway) را برای کاربران خارج از مرکز بازی می‌کند، یاری برساند.

اعتبار

از آن جایی که شرکت کامپتیا یک مؤسسه آموزشی است، در راه تعریف و ایجاد سیستم آموزشی، ارزشیابی و مدرک‌دهی خود از بسیاری از سازندگان سرورها و تجهیزات مربوطه به آن یاری گرفته است. شرکت‌های معتبری چونIBM،HP، اینتل و امثال آن از جمله این شرکت‌ها هستند. در زمینه ارزش مدرک هم، می‌توان به رسمیت شناخته شدن مدرک مذکور نزد کلیه شرکت‌های صاحب‌نام اشاره کرد. در این مورد حتی مایکروسافت که خود از جمله ارایه‌دهندگان سیستم آموزشی و کسب مدرک است، +Server را به عنوان یکی از گزینه‌های اختیاری ارائه مدرک MCSA معرفی کرده است.

مفاد آزمون

۱- Installatio (17%)

ارایه طرح نصب یک سرور در شبکه به همراه کلیه تمهیدات و پیش‌بینی‌هایی که باید در زمینه اختصاص اداوت سخت‌افزاری از مادربرد و سی‌پی‌یو گرفته تا کابل‌های اتصال شبکه UPS و SCSI، صورت پذیرد در این قسمت قرار دارند.

۲- Configuratio (18%)

در این مرحله، آموزش گام به گام پیکربندی و راه‌اندازی یک سرور از تنظیمات BIOS آن گرفته تا مسایل مربوط به آرایش ادوات ذخیره‌سازی RAID، نصب سیستم‌عامل، برقراری و تنظیم ارتباطات شبکه‌ای لازم با سرور، پیکربندی ادوات جانبی و سرویس‌های شبکه‌ای مثل SNMP و امثال آن جای می‌گیرند.

۳- Upgrading (12%)

تعویض یا ارتقاء هر یک از اجزاء یک سرور می‌تواند مراحل مختلفی را جهت اطمینان از دست‌یابی به بهترین حالت عملیاتی آن سرور دربرگیرد. به‌عنوان مثال با تعویض یا اضافه کردن یک CPU، باید از انطباق و همخوانی سرعت و قدرت caching آن در ارتباط با سایر CPUها مطمئن گردید. در زمان اضافه کردن یا تعویض هارددیسک باید طوری عمل کرد تا اختلالی در اطلاعات از قبل ذخیره شده در هارددیسک‌های دیگر پیش نیاید. اضافه کردن حافظه‌های اصلی، مراحل تست و آزمایش سایر قطعات و سیستم‌عامل را جهت سازگاری و پشتیبانی از آن طلب می‌کند.

۴- Proactive Maintenance (9%)

شامل کلیه عملیاتی است که پس از نصب و در حالی که سرور به حالت پایدار و بهره‌برداری رسیده است باید انجام شود. شیوه‌های ایجاد درایوها و فایل‌های پشتیبان، بررسی و تجزیه و تحلیل سرعت و کارایی سرور در زمآن‌های مختلف و اقدام در جهت افزایش آن از جمله این موارد می‌باشند.

۵- Environment (5%)

این مبحث شامل دو قسمت اصلی است. قسمت اول مربوط به برآورده کردن سیاست‌های مختلف امنیتی در دسترس کاربران و کامپیوترها به قسمت‌ها و سرویس‌های متعدد یک سرور است و قسمت دوم موارد حفاظتی مربوط به محیط استقرار شبکه و سرور مثل درجه حرارت و رطوبت محیط و خطرات ناشی از آتش‌سوزی، اتصال برق و امثال آن را بررسی می‌کند.

۶- Troubleshooting (27%)

این مبحث، بیشترین سهم از وظایف یک متخصص امور سرور و در نتیجه مدرک Server را به خود اختصاص می‌دهد. در این قسمت انواع اتفاقاتی که می‌تواند سبب بروز مشکلات سخت‌افزاری و نرم‌افزاری در سرورهای ویندوزی، یونیکسی، لینوکسی و OS.2 شود مورد بررسی قرار گرفته و راه‌های کشف علل آن و نحوه برخورد با مشکلات مربوط به سرعت، عدم هماهنگی در سخت‌افزار یا نرم‌افزار و سرویس‌هایی که سرور به کاربران ارایه می‌دهد و همچنین نحوه استفاده از ابزارهای مختلف جهت رفع آن‌ها به داوطلبان آموخته می‌شود.

۷- Disaster Recovery (12%)

کلیه اتفاقاتی که ممکن است سرور و شبکه تحت پوشش آن را در یک وضعیت بحرانی قرار دهد و تعدادی از سرویس‌های آن را به‌طور کامل مختل نماید یا باعث از دست رفتن اطلاعات حساس و حیاتی شود، در این بخش مورد بررسی قرار می‌گیرد، راه‌های پیشگیری از بروز چنین مواردی مثل نگهداری سخت‌افزارهای جایگزین و حفظ آمادگی جهت جایگزین کردن و یا برگرداندن اطلاعات پشتیبان و قطعات جایگزین و راه‌اندازی مجدد سرویس‌های مختل شده در اسرع وقت از جمله موارد مطرح شده در این فصل است.

وضعیت درآمد

طبق آخرین آمارهایی که توسط سایت Certification ارائه شده است، مدرک +Server از لحاظ میزان درآمد سالانه دارندگان آن با رقم ۵۴ هزاردلار در سال، از میان ۹ مدرک مختلف شرکت کامپتیا در رده ششم قرار دارد. این در حالی است که در این رده‌بندی، مدرک +Network که مباحثی شبیه مدرک مذکور اما با گرایش کمتر به سمت سرور و بیشتر به سمت بنیان شبکه دارد، با ۴۹ هزار دلار در رده هشتم جای گرفته است. طبق همین آمار مدرک MCSA مایکروسافت که تا حدودی و بیشتر از لحاظ نرم‌افزاری به +Server شبیه است با ۵۸ هزاردلار درآمد سالیانه، حکایت از اندک تفاوت بین این دو مدرک دارد و بیانگر اهمیت مدرک مذکور برای کسب موقعیت شغلی خوب و درآمد مناسب است.

۱۳-۴-۴- *Security+*

آزمون و مدرک بین المللی +CompTIA Security تعیین کننده استانداردهای مورد نیاز صنعت جهت مدیریت امنیت اطلاعات می‌باشد.با گذارندن این دوره شما مهارت‌های لازم جهت ایمن سازی سیستم‌ها و اطلاعات موجود بر روی آن‌ها و همچنین دانش لازم برای گذراندن آزمون را کسب خواهید نمود. دوره +Security از جدیدترین دوره هایی می‌باشد که مورد تایید مایکروسافت بوده و با استفاده از کتاب Security+ 2003 از انتشارات Microsoft Press تدریس می‌گردد.آزمون و مدرک این دوره توسط شرکت compTIA ارائه شده و از جمله آزمونهای مورد تایید مایکروسافت جهت یکی از آزمونهای Elective (انتخابی) مدرک مدیریت شبکه هاب مایکروسافت (MCSE:S) می‌باشد.این دوره برای سایر دوره‌های Security و امنیت شبکه پیش نیازی ضروری می‌باشد.(آزمون SYC-101 کامپتیا)

تعداد امتحانات:

این آزمون دربرگیرنده مواردی از جمله Communication Security, Infrastructure Security, Cryptography, Access Control, Authentication, External Attack And Operational And Organization Security می‌باشد.بسیاری از شرکتهای صاحب تکنولوژی نظیر Sun, IBM/Tivoli Software Group, Symantec, Motorola و Olympus Security Group این مدرک را جهت پرسنل خود الزامی دانسته و شرکتهایی نظیر مایکروسافت آنرا در سری آزمونهای مورد قبول خود جای داده‌اند که این امر نشانه ارزشگزاری دنیای فن آوری اطلاعات به این مدرک می‌باشد.

- ✓ General Security Concepts 30%
- ✓ Communication Security 20%
- ✓ Infrastructure Security 20%
- ✓ Basics of Cryptography 15%
- ✓ Operational/Organizational Security 15%

۱۳-۴-۵- Project+

تصور کنید پروژه اتوماسیون سیستم اداری یک سازمان بزرگ در حال شکل‌گیری است. در این پروژه افراد مختلفی از تحلیلگران، طراحان، برنامه‌نویسان، متخصصان شبکه و... در تیم فنی و اجرایی پروژه هستند. افراد دیگری نیز در این پروژه نقش مشاور در ساخت برنامه‌های مالی، تجاری و امثال آن را ایفا می‌کنند که هرکدام در رشته خود صاحب تجربه‌های مختلفی هستند. در این میان یک نفر به عنوان مدیر پروژه، نه تنها لازم است که آشنایی خوبی با تمام امور فنی و غیرفنی مذکور داشته باشد، بلکه باید اصول مدیریت و نحوه ایجاد هماهنگی بین اعضای دخیل در پروژه را به خوبی بشناسد. همچنین تسلط خوبی در تخصیص بهینه منابع، اعم از نیروی انسانی، بودجه، هزینه‌های پروژه و زمانبندی انجام و تکمیل مراحل مختلف آن داشته باشد. از این رو با توجه به اهمیت مدیریت در این‌گونه پروژه‌ها، این‌بار یک مدرک مدیریتی در عرصه پروژه‌های IT معرفی می‌شود.

مدرک Project+ یک مدرک مهم و منحصربه‌فرد در زمینه مدیریت پروژه‌های IT است. داشتن این مدرک بیانگر وجود تخصص و اطلاعات جامع در مورد کسب و کار مبتنی بر IT و جوانب مربوط به آن، از دید مدیریتی است. تاریخچه وجود این مدرک در کامپتیا به سال‌های چندان دوری برنمی‌گردد. در واقع کامپتیا در سال ۲۰۰۱ امتیاز مربوط به Project+ را به کلی از مؤسسه Garthergroup خریداری کرد.

سپس در سال ۲۰۰۳ کامپتیا با کمک متخصصان حوزه مدیریت IT، این مدرک را دوبار بازنویسی کرد تا سرانجام به شکل نهایی آن که اکنون تدریس می‌شود، درآمد. در حال حاضر مباحث موجود در این مدرک غیراز اطلاعات مربوط به مدیریت متداول پروژه‌های IT، بسیاری از سطوح دیگر مدیریت در این حوزه، مثل نقش‌های هماهنگ‌کننده، تحویل به مشتری، پشتیبانی مشتریان، روابط عمومی، بازاریابی، و... را دربر می‌گیرد.

البته سؤالی که در این‌جا مطرح می‌شود این است که آیا واقعاً افرادی که در سطح مدیریت پروژه‌های IT قرار دارند، غیراز مدیریت متداول IT به این‌گونه تخصص‌های جانبی دیگر نیازمند هستند یا نه؟ کامپتیا این سؤال را با هر دو گزینه آری و خیر پاسخ می‌دهد. در واقع کامپتیا معتقد است با توجه به نوع و گستردگی هر پروژه IT، یک مدیر پروژه علاوه‌بر داشتن

دانسته‌هایی در حوزه کاملاً تخصصی IT که همان مدیریت سنتی یا متداول نامیده می‌شود، باید در برخی شاخه‌های تجارت نیز از آگاهی‌ها و تجارب کافی برخوردار باشد.

هیچ پروژه IT، صرفاً به دنیای کامپیوتر و شبکه تعلق کامل ندارد. بسیاری از پروژه‌ها، برنامه‌هایی تجاری هستند که برای مقاصد مختلفی ازجمله حسابداری، منابع انسانی، بودجه، ارائه انواع خدمات به مشتریان، خرید و فروش و امثال آن به وجود آمده‌اند؛ پس افرادی که در سطوح بالای مدیریت این‌گونه برنامه‌ها و پروژه‌ها قرار می‌گیرند، نمی‌توانند با واژه‌ها، مفاهیم، و تکنیک‌های این رسته‌ها غریب و ناآشنا باشند.

در ویرایش دوم دروس +Project، بر سناریوهای مختلف قابل وقوع در راه انجام یک پروژه IT، تمرکز زیادی شده است. این سناریوها که جنبه‌های مختلف مدیریت، چه از لحاظ فنی و چه از لحاظ کسب و کار را دربرمی‌گیرد، کلیه رویدادها یا مشکلاتی را که می‌تواند در آغاز یا در هنگام انجام یک پروژه به‌وجود آید، مورد بررسی قرار داده و راه‌های مقابله با آن را آموزش می‌دهند.

اگر مباحث مورد کنکاش در +Project را به چند مرحله تقسیم‌بندی کنیم، در مرحله اول، مباحث مربوط به آغاز یک پروژه، از جمله تأمین منابع انسانی و تخصیص هر یک از آن‌ها به پست‌های مربوط به خودشان، تخمین هزینه‌ها و بودجه پروژه، تخمین زمان انجام پروژه و درواقع زمانبندی مراحل مختلف انجام یک پروژه و درنظرگرفتن حداکثر مهلت زمانی پایان هر مرحله (Deadline) مطرح می‌شود. همچنین برآورد کلیه نیازمندی‌های فنی و غیرفنی مربوط به زمان انجام پروژه در این مرحله صورت می‌گیرد.

در مرحله دوم که به طراحی پروژه (Planning) مربوط است، کلیه محصولاتی که قرار است در یک پروژه تولید شود، اعم از محصولات اصلی و یا اجزای آن‌ها، محدوده هر کدام، منابع و نیازمندی‌های لازم برای انجام و تکمیل هر یک از مراحل انجام پروژه که در بحث اول تعریف شده بود، مورد بررسی قرار می‌گیرد.

در مرحله سوم، که در واقع وارد مرحله مدیریت اجرایی پروژه می‌شود، کنترل و هماهنگی بین سایر اعضای اجرایی پروژه، در دستور کار مدیر پروژه قرار می‌گیرد. نظارت بر پیشرفت هر یک از مراحل تعریف شده برای یک پروژه و تغییر به موقع یا بروزرسانی طرح اولیه در صورت لزوم، ایجاد ارتباط مداوم با اعضا برای آگاهی از روند پیشرفت پروژه و تخصیص یا حذف منابع در صورت لزوم و تهیه گزارش‌های مدیریتی برای آگاهی از کارایی هر نفر یا تیم در انجام امور محوله، از جمله موارد مورد بحث در مرحله سوم به‌شمار می‌روند.

در مرحله چهارم، کلیه مسائل مدیریتی مربوط به مراحل بعد از پایان پروژه، یعنی نگهداری، پشتیبانی، ارتقا و امثال آن مطرح می‌شود. در این مرحله، داوطلبان +Project با نحوه زمانبندی، تخصیص منابع مالی و انسانی برای تست، تکمیل مستندسازی پروژه، و ساخت راهنمای ویژه کاربران (user Manual) آشنا می‌شوند. پس از طی این مراحل نیز مباحثی در زمینه بازاریابی و قراردادهای تجاری که بین سازندگان پروژه و فروشندگان آن رواج دارد، مطرح می‌گردد. در طی کلیه مراحل آموزش و آزمون مدرک +Project، ابزارهای معروف مدیریتی و آماری، اعم از صفحه‌های گسترده مثل اکسل، انواع برنامه‌ها و ابزارهای زمانبندی (Scheduler)، برخی بانک‌های اطلاعاتی، و برنامه‌های دیگر مورد استفاده قرار می‌گیرد و به‌کارگیری آن‌ها به افرادی که قصد کار در ردههای مدیریتی پروژه‌های IT را دارند، توصیه می‌شود.

ارزش مدرک

هر پروژه IT در هر سازمانی که قرار است اجرا شود، مستلزم ایجاد مقدماتی برای طرح و آغاز است. اکنون وجود یک مدیر با تجربه و مسلط بر جنبه‌های مختلف پروژه، یکی از اصول بدیهی و مقدماتی هر پروژه IT به حساب می‌آید. امروزه بسیاری از سازمان‌ها به این نتیجه رسیده‌اند که برای جلوگیری از خطر به بن‌بست رسیدن و شکست پروژه در مراحل میانی یا پایانی کار، ارزش داشتن یک مدیر با تجربه، بیش از داشتن چند نفر مسئول فنی بدون سابقه مدیریت در این زمینه است. وجود این مدیر باعث می‌شود ریسک شکست پروژه در مراحل بحرانی و حساس کاهش زیادی پیدا کرده و با تدبیری که این شخص در مراحل مختلف پروژه از خود نشان می‌دهد، بالاترین بهره‌وری از بودجه و نفرات به دست آید.

برای همه کسانی که به داشتن پست‌های مدیریتی در پروژه‌های IT علاقه زیادتری دارند، کسب مدرک +Project شانس اشتغال آن‌ها و همچنین میزان درآمد آن‌ها را نسبت به همتایانی که مدرک بین‌المللی با این عنوان کسب نکرده‌اند، افزایش می‌دهد. طبق نظر رسمی کامپتیا، کسانی که قصد کسب مدرک +Project را دارند، باید حداقل دو هزار ساعت تجربه کار مدیریتی در پروژه‌های IT را اندوخته باشند. البته در زمینه مدیریت و خصوصاً در رسته مدیریتIT، بسیاری از ارائه‌دهندگان فناوری یا مؤسسات آموزشی، مدرک‌های تخصصی مدیریت در هر یک از شاخه‌های IT ارائه نموده‌اند. با این حال مدرک +Project که جنبه عمومی‌تری نسبت به سایر مدارک دارد، می‌تواند پیش‌نیاز و در واقع یک گام اساسی برای شروع مدارج بالاتر و تخصصی‌تر مدیریت IT باشد.

وضعیت درآمد

میانگین درآمد متوسط دارندگان مدرک Project+ در سال ۲۰۰۴، در حدود ۷۰ هزار دلار گزارش شده است. این رقم نه‌تنها شاخص متوسطی را در بین کلیه مدارک بین‌المللی از خود نشان می‌دهد، بلکه در میان مدارک کامپتیا، در رتبه اول (و حتی بالاتر از پرطرفدارترین مدرک این مؤسسه، یعنی +Security با ۶۳ هزار دلار در سال) قرار دارد. البته میزان درآمد این مدرک از آن‌جایی که به عنصر خاصی در دنیای IT، مثل برنامه‌نویسی شبکه، بانک اطلاعاتی، امنیت و امثال آن مربوط نمی‌شود، با مدارک بین‌المللی دیگر قابل‌مقایسه نیست، اما با توجه به رشد درآمد سالیآن‌های که برای افراد صاحب این مدرک (در مقایسه با کسانی که بدون داشتن آن در مناصب مدیریتی مشغول به کار هستند)، دیده می‌شود، ارزش Project+ در ارتقای سطح شغلی کاملاً مشهود به نظر می‌رسد.

۱۳-۴-۶- مزایای دستیابی به مدارک کامپتیا

- دریافت مدرک بین المللی کامپتیا (Certificate & Transcript)
- دریافت کارت شناسایی کامپتیا (Wallet Card)
- امکان استفاده از لوگوی کامپتیا
- موقعیت شغلی و استخدامی بهتر با توجه به تخصص و دانش مورد تأیید کامپتیا
- دریافت حقوق بیشتر
- اثبات دانش فنی و عملی در زمینه کار مقدماتی با شبکه
- کسب دانش فنی و عملی لازم جهت اخذ مدارک بالاتر شبکه

– دستیابی به بخش ویژه سایت کامپتیا جهت دارندگان مدارک و امکان دریافت لوگوها و مشاهده وضعیت مدرک.

۱۳-۵- مدارک لینوکس

۱۳-۵-۱- مدارک لینوکس‌کاران

اصولا هر قدر از ویندوز دور می‌شویم، دنیا قشنگ‌تر می‌شود، البته نه همیشه! به‌ویژه وقتی مجبوریم با برخی امکانات ویندوزی خودمان را سازگار کنیم. اما لینوکس به‌عنوان یک مرجع در سیستم‌عامل‌های متن‌باز با داشتن نسخه‌های گوناگون از هر توزیع، هر روز در حال بهتر شدن است.

شاید در نگاه اول گمان کنید لینوکس یک سیستم عامل سخت و پیچیده است اما نسخه‌هایی که برای کاربران نهایی تهیه شده، چیزی از ظاهر ویندوز کم ندارد و صد البته از ویندوز بسیار کارآمدتر است. اما به‌هر حال میلیاردها دلار سرمایه مایکروسافت پیشتیبان لینوکس نیست تا نرم‌افزارهای همه‌گیر را روی آن همخوان کنند و برایش تبلیغات کنند.

لینوکس یک سیستم‌عامل متن‌باز است که در بیشتر نسخه‌ها رایگان عرضه می‌شود و برای دریافت، به‌روزرسانی و پشتیبانی آن‌ها نیازی به پرداخت پول نیست. از طرفی بیشتر نسخه‌های آن نیز منبع‌باز و از دسته نرم‌افزارهای آزاد هستند؛ یعنی برنامه‌نویس می‌تواند با تغییر در منابع آن با ایجاد نوعی تغییر کارایی، آن را تغییر دهد و چیزی را بسازد که می‌خواهد. این در تمام نسخه‌ها امکان‌پذیر نیست. (برای اطلاعات بیشتر در مورد لینوکس پیگیر صفحه لینوکس ما باشید.)

موضوع مدارک تخصصی، این بار به لینوکس رسیده. لینوکس نیز مانند دیگر جوانب رایانه دارای چند سطح مهارتی است که از کاربری معمولی و پس از تخصصی به فوق تخصصی می‌رسد. سطح اول برای انجام تمام کارهای اداری و امثال آن کافی است. مدارک لینوکس نیز یا توسط شرکت‌های سازنده نسخه‌های خاص ارایه می‌شوند؛ مانند RedHat که لینوکس ردهت و شرکت ناول که لینوکس SuSE را عرضه می‌کند

تمایل به کسب مدارک بین‌المللی لینوکس، روز به روز در جامعه طرفداران اُپن‌سورس و این سیستم‌عامل محبوب افزایش می‌یابد. این مدارک را برحسب ارایه‌دهندگان آن‌ها می‌توان به دو دسته تقسیم نمود. دسته اول مدارکی هستند که توسط ارائه‌دهندگان لینوکس و با گرایش بیشتر به محصول اختصاصی خودشان ارایه می‌شود، مثل مدارک مربوط به شرکت ردهت که لینوکس RedHat و مدرک شرکت ناول که لینوکس SuSE را شامل می‌شود. دسته دوم، مدارکی هستند که توسط مؤسسات آموزشی مثل CompTIA و یا انجمن‌های مهم طرفدار این سیستم‌عامل مثل انستیتوی حرفه‌ای لینوکس‌کاران عرضه می‌شود. در این مقاله نگاهی به هر دو گروه مدرک موجود در دنیای لینوکس خواهیم داشت.

۱۳-۵-۲- مدرک Linux+

این مدرک یکی از معتبرترین مدارک بین‌المللی در حوزه سیستم‌عامل لینوکس است. داوطلبانی که موفق به کسب مدارک مذکور شوند، قادر خواهند بود این سیستم‌عامل را نصب و پیکربندی کرده، برای مقاصد مختلف آن را آماده نموده و اشکالات پیش آمده را رفع کنند. شرکت کامپتیا حداقل شش‌ماه تجربه کاری مفید در محیط سیستم‌عامل لینوکس را پیش شرط اخذ این مدرک برای داوطلبان اعلام کرده است. یک فرد دارای مدرک Linux+ به عنوان شخصی که مفاهیم دنیای اُپن‌سورس را به طور کامل درک کرده و قادر است کلیه تنظیمات مربوط به لینوکس از جمله تنظیمات مدیریتی، اعطای مجوز

استفاده به کاربران، نصب و پیکربندی برنامه‌ها و نرم‌افزارهای مختلف و همچنین برقراری ارتباط با سایر کامپیوترها در محیط شبکه و مدیریت فایل‌ها و عملیات ذخیره‌سازی بر روی ادوات مربوطه را انجام دهد، شناخته می‌شود.

آزمون +Linux به خودی خود دارای هیچ پیش نیازی نیست اما باز هم شرکت کامپتیا داشتن اطلاعاتی در حد مدارک +Aیا +Network را به داوطلبان توصیه می‌کند. آزمون +Linux که شامل ۹۴سؤال با ۹۰ دقیقه زمان پاسخ است در کل ۹۰۰ امتیاز دارد که داوطلب باید حداقل ۶۵۵ امتیاز از آن را کسب کند.

مزایا

شرکت کامپتیا برای دارندگان مدرک +Linux، حرفه‌ای شدن برای کار در محیط لینوکس، ارتقاء سطح شغلی موجود یا ایجاد زمینه اشتغال بیشتر برای صاحب مدرک، بهترشدن مسیر کسب و کار و کمک به داوطلبان در انتخاب مسیر دانش‌اندوزی و همچنین ایجاد یک زمینه محکم برای تشویق دانشجویان به کسب مدارک سطوح بالاتر را از مزایای داشتن مدرک مذکور عنوان می‌کند.

مفاد آزمون +Linux

در آزمون مربوط به مدرک +Linux، هفت موضوع اصلی مورد توجه قرار می‌گیرند که هر کدام درصدی از آزمون را به خود اختصاص می‌دهند. به این شرح که:

۱- راهکارها و شیوه‌های استفاده از سیستم‌عامل لینوکس: ۴ درصد

۲- نصب لینوکس: ۱۲٪

۳- پیکربندی: ۱۵٪

۴- مدیریت: ۱۸٪

۵- نگهداری و پشتیبانی: ۱۴٪

۶- رفع مشکلات: ۱۸٪

۷- ارتباط با ادوات سخت‌افزاری: ۱۹٪

در بخش اول، داوطلبان با مزایای استفاده از این سیستم‌عامل و همچنین اصطلاحات دنیای لینوکس آشنا می‌شوند. در قسمت دوم، انواع روش‌های مربوط به دریافت فایل‌های نصب لینوکس و انجام عمل نصب چه از طریق CD قابل بوت سیستم‌عامل و چه از طریق پروتکل‌های شبکه‌ای مثل FTP،HTTP،SMB و NFS مورد بحث قرار می‌گیرد. در بخش سوم، نحوه تنظیم و پیکربندی ماجول‌های اصلی سیستم‌عامل برای استفاده از انواع سرویس‌های موجود مثل دسترسی راه‌دور، سرویس‌های اینترنت و شبکه مورد بررسی قرار می‌گیرد.

در فصل چهارم، نحوه تعامل مدیر سیستم با کاربران، گروه‌های کاربری و مقوله‌های امنیتی مربوط به آن شرح داده می‌شود. در قسمت پنجم، نحوه ایجاد فایل‌های پشتیبان از سیستم، مدیریت پردازش‌های در حال اجرا، تشخیص و خارج کردن پردازش‌های زاید با استفاده از ابزارهایی مثل فرمان Kill و مانیتورینگ عملکرد سیستم و سرویس‌های ارایه شده مورد بحث قرار می‌گیرد. در بخش ششم هم بیشتر مطالب مربوط به بخش قبل اما با گرایش به سمت نحوه برخورد با مشکلات و مواقع

بحرانی سیستم در نظر گرفته شده است. در قسمت آخر هم موضوع ارتباط لینوکس با انواع ادوات سخت‌افزاری داخلی و خارجی مثل هارددیسک، مادربرد، حافظه، CPU و سایر تجهیزات مورد بررسی قرار می‌گیرد.

۱۳-۵-۳- مدرک *Novell CLP*

پس از آن‌که شرکت ناول‌نت‌ور موفق به خرید شرکت SuSE، تولیدکننده آلمانی سیستم‌عامل لینوکس شد، عنوانی را به لیست مدارک بین‌المللی خود اضافه نمود تا بتواند شماری از کاربران و علاقه مندان به این سیستم‌عامل را به خود جذب نماید و قسمتی از بیش از دو هزار عنوان شغلی که برای پرداختن به این سیستم‌عامل در جهان درنظرگرفته شده را، تحت پوشش مدرک خود قرار دهد. مدرک CLP (Certified Linux Professional) مدرکی است که در سال ۲۰۰۴ و با گرایش مدیریت در محیط لینوکس معرفی شد.

این مدرک که بنابر ادعای ارایه‌دهندگان آن خالی از مفاهیم تئوریک خشک و خسته‌کننده بوده و بیشتر جنبه عملی و آشنایی با محیط کار واقعی لینوکس دارد، بر روی نسخه خاصی از لینوکس و آن هم لینوکس SuSE بنا شده است. شرکت ناول، کسب این مدرک را به کلیه کسانی که نقش راهبردی و فعال در زمینه مدیریت سیستم‌های بزرگ تجاری (Enterprise) با لینوکس دارند، توصیه می‌نماید.

مفاد آزمونCLP

برای کسب مدرکCLP، گذراندن سه دوره آموزشی مختلف به همراه آزمون‌های مخصوص هر کدام در نظر گرفته شده که عبارتند از:

۱- SuSE Foundamental:

در این دوره، تازه واردان و همچنین قدیمی‌ترهای دنیای لینوکس با مفاهیم روزمره و کاربردی این محیط به‌خصوص فایل‌سیستم و انواع دستورهای خط فرمان و مفاهیم مربوط به کاربران، شبکه و امثال آن آشنا می‌شوند.

۲- SuSE Administration:

در این دوره، مهارت‌های مدیریتی لینوکس مثل نصب و آماده‌سازی کامپیوترها برای ارتباط در یک محیط شبکه‌ای، مدیریت کاربران، گروه‌های کاربری و کنترل سطح دسترسی هر کدام از آن‌ها به منابع سیستم، نصب و حذف برنامه‌های مختلف، کاربا چاپگر، سرویس‌های شبکه‌ای و امثال آن مورد بحث قرار می‌گیرند.

۳-Advanced SuSE Administration:

برای کسانی که آشنایی مقدماتی با مفاهیم مدیریتی در لینوکس دارند، این دوره جهت تکمیل مهارت‌های آن‌ها برای تصدی مدیریت در کاربردهای حساس‌تر و بزرگ‌تر در نظر گرفته شده است. نحوه مدیریت و کامپایل کرنل، راه‌اندازی سرویس‌هایی مثلFTP، وب سرور، مدیریت داده‌های شبکه با استفاده از Open LDAP، مدیریت سرویس‌های پست‌الکترونیکی و پیام‌رسانی فوری ازجمله این تخصص‌ها می‌باشند.

۱۳-۵-۴- مدرک RHCE (RedHat Certified Engineer)

Redhat همواره یکی از بزرگ‌ترین و معتبرترین تولیدکنندگان سیستم‌عامل لینوکس بوده است. این شرکت که در ابتدا کار خود را با پرسنل اندکی که تعدادشان به ۲۰ نفر هم نمی‌رسید آغاز کرد، آنچنان حوزه فعالیت خود را در عرضه این سیستم‌عامل گسترش داد که در طی مدت محدودی، لینوکس خود را به شهرت جهانی رساند. هم‌اکنون انواع نسخه‌های لینوکس متعلق به ردهت، از نسخه‌های عادی آن گرفته تا نسخه‌های ویژه سرورهای Enterprise و اخیراً ویرایش‌های جدیدی که تحت نام فدورا به بازار ارایه شده است، همگی از کاربرد و محبوبیت وسیعی در بین علاقه‌مندان و کاربران محیط‌های اُپن‌سورس برخوردارند.

به همین دلیل یکی از معتبرترین مدارک بین‌المللی که در حوزه ویژه و تخصصی سیستم‌عامل لینوکس وجود دارد، مدرکی است که شرکت ردهت ارایه می‌دهد. دوره آموزشی ویژه این مدرک نحوه تعامل با لینوکس را به صورت عملی و تجربی به داوطلبان می‌آموزد. ردهت، آشنایی قبلی با مفاهیم اساسی شبکه چون LAN، WAN و همچنین انواع پروتکل‌ها و سرویس‌های استاندارد آن چون FTP، DNS، DHCP، NFS و امثال آن را توصیه می‌نماید.

افرادی که موفق به کسب مدرک RHCE شوند قادر خواهند بود سیستم‌عامل لینوکس ردهت را به راحتی نصب، پیکربندی و مدیریت نمایند. مفاهیم مورد بحث در مدرک RHCE در هفت فصل مختلف متمرکز شده‌اند که عبارتند از:

۱- سخت‌افزار و نصب

در این فصل به روند بوت شدن سیستم‌عامل و نحوه شناسایی یا معرفی سخت‌افزارهای مختلف توسط آن پرداخته می‌شود.

۲- پیکربندی و مدیریت

این فصل به نحوه پیکربندی ردهت جهت استفاده از سیستم‌عامل در مقاصد مختلف و با کاربردهای گوناگون و همچنین نحوه نصب پکیج‌های نرم‌افزاری مخصوص ردهت به نام RPM و مفاهیم دیگری مثل فایل‌سیستم، مدیریت کاربران و گروه‌های کاربری اختصاص دارد.

۳ - روش‌های دیگر نصب

در این فصل موضوع نصب لینوکس ردهت بر روی کامپیوترهای لپ‌تاپ و مسأله مهم بوت دوگانه یا چندگانه (MultiBoot) برای کاربرانی که قصد داشتن چند سیستم‌عامل دیگر را به همراه ردهت بر روی یک کامپیوتر دارند و همچنین نصب از طریق شبکه مورد بحث قرار می‌گیرد.

۴- کرنل و تنظیمات سیستم

در این مبحث، دانشجویان با فایل‌سیستم /Proc، سیستم Quota و همچنین نحوه کامپایل کردن، نصب و تنظیم کرنل لینوکس و مفاهیم دیگر این سیستم‌عامل چون LILO آشنا می‌شوند.

۵ - سرویس‌های استاندارد شبکه

این فصل، مباحث مربوط به پروتکل‌ها و سرویس‌های مختلف شبکه‌ای در لینوکس و نحوه تنظیم و راه‌اندازی آن‌ها در یک شبکه مبتنی بر لینوکس را شامل می‌شود. مواردی چون TCP/IP،FTP،NFS،DHCP و مفاهیمی چون وب سرور (آپاچی)، پراکسی سرور (اِسکوئید) و سیستم اشتراک فایل (سامبا) در این فصل مورد بررسی قرار می‌گیرند.

۶- Xwindows

کلیه اصول مربوط به واسط کاربر گرافیکی لینوکس و انواع سرویس‌ها و محیط‌های مربوط به آن در این بخش مورد بحث قرار می‌گیرد.

۷ – امنیت

این بخش کلیه مفاهیم امنیتی و سرویس‌ها و پروتکل‌های ویژه احراز هویت و دسترسی کاربران به منابع مختلف سیستم و نحوه استفاده و تنظیم آن‌ها را شامل می‌شود. همچنین در این فصل مسایل مربوط به دیواره‌های آتش و روترها نیز بررسی می‌شوند.

فصل ۱۴

ساخت شبکه‌های مجازی با نرم‌افزار Virtual Box

۱۴-۱- مقدمه

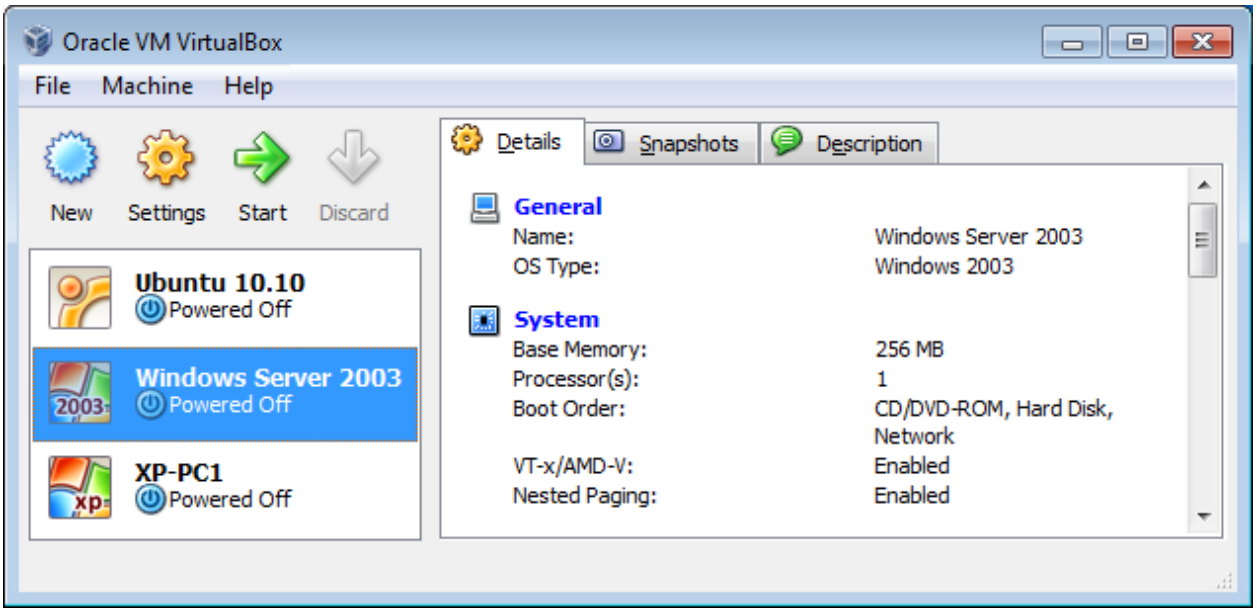
بسیاری از مباحث عملی مطرح شده در این جزوه، جهت انجام نیاز به دو یا چند کامپیوتر دارند به طوری که این کامپیوترها با یکدیگر شبکه شده باشند. اما از آنجایی که برای افراد سخت است که در خانه خود یک شبکه کامپیوتری راه اندازی کنند (به خاطر محدودیت‌های سخت‌افزاری)، لذا تصمیم گرفتیم که در ابتدای آموزش‌های عملی، آموزش شبیه سازی اجرای همزمان چندین سیستم عامل روی یک سیستم عامل به گونه‌ای که این سیستم عامل‌ها بتوانند با یکدیگر شبکه شوند را آموزش دهیم. مزیت این کار این می‌باشد که افراد می‌توانند چندین سیستم را به صورت نرم‌افزاری با یکدیگر شبکه نموده و مباحث عملی مطرح شده را به راحتی کار نمایند. مزیت دیگر نیز این است که در کلاس‌های آموزش عالی، معمولاً جهت جلوگیری از خرابی نرم‌افزاری کامپیوترها، آن‌ها را Freeze می‌کنند؛ تا تغییرات نرم‌افزاری را بی اثر سازند؛ اما با شبیه سازی می‌توان ابتدا نرم‌افزار شبیه ساز را نصب نمود و سپس به تعداد دلخواه روی آن سیستم عامل نصب کرد. نرم‌افزاری که ما در این فصل آموزش می‌دهیم، نرم‌افزار Oracle VM VirtualBox می‌باشد.

Oracle VM VirtualBox -۲-۱۴

جهت شبیه سازی اجرای همزمان چندین سیستم عامل، نرم‌افزارهای متعددی وجود دارند، نرم‌افزار هایی از قبیل: VMware Work Station، Microsoft Virtual PC، Oracle VM Virtual Box و.... اما دلیل اینکه ما نرم‌افزار Oracle VM VirtualBox را انتخاب نمودیم این است:

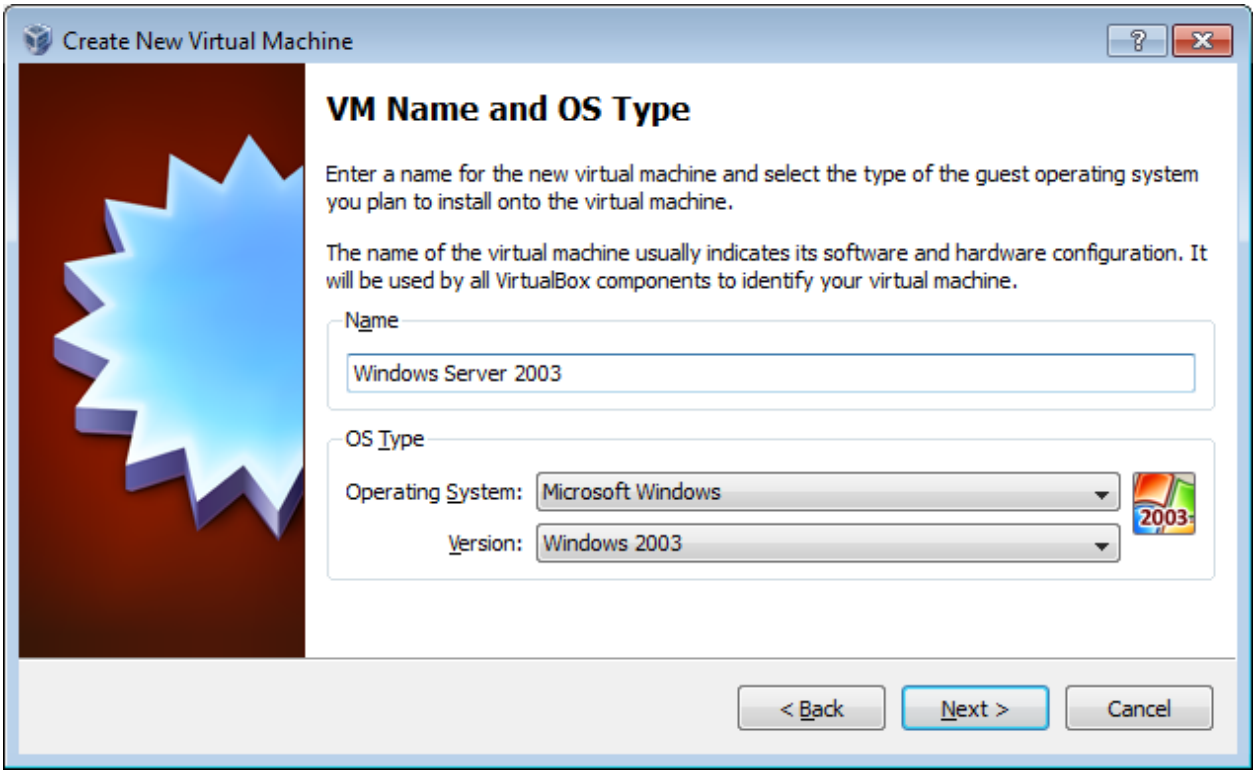
۱. نرم‌افزار پر قدرتی است.
۲. رایگان می‌باشد.
۳. کم حجم است (۷۵ مگابایت).
۴. بسیار سبک و راحت اجرا می‌شود.

در ادامه این نرم‌افزار را به اختصار Virtual Box می‌نامیم. VM در Oracle VM VirtualBox مخفف Virtual Machine و به معنای ماشین مجازی می‌باشد. در گام اول، این نرم‌افزار را دانلود نموده و آن را نصب نمایید. پس از نصب نرم‌افزار و باز کردن آن، صفحه‌ای مانند صفحه زیر مشاهده می‌نمایید:

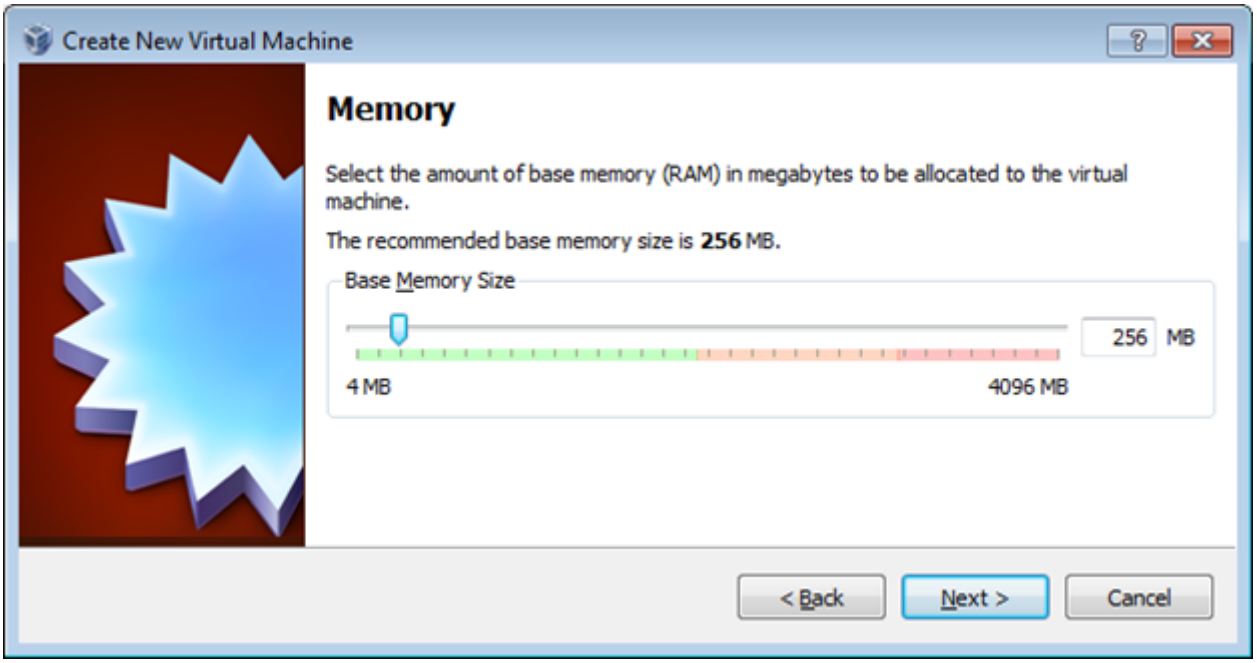


در سمت چپ، لیست سیستم عامل‌های نصب شده را مشاهده می‌نمایید و در سمت راست نیز با انتخاب هر سیستم عامل، قادر به مشاهده جزئیات آن خواهید بود. در بالا نیز دکمه هایی جهت ساخت سیستم عامل جدید (New)، انجام تنظیمات روی سیستم عامل‌های موجود (Settings) و راه اندازی یکی از سیستم عامل‌های موجود (Start) وجود دارد. با این نرم‌افزار امکان اجرای همزمان چندین سیستم عامل نیز وجود دارد.

ما بحث را با آموزش نصب یک سیستم عامل مجازی آغاز می‌کنیم. بدین منظور در صفحه اصلی روی دکمه New کلیک کنید. بدین ترتیب صفحه خوش آمد گویی باز می‌شود. روی Next کلیک کنید. در صفحه بعدی نوع سیستم عامل مورد نظر خود را انتخاب نموده و نامی دلخواه برای آن انتخاب نمایید. سعی نمایید که نام وارد شده پر مفهوم بوده و بیانگر خود سیستم عامل باشد. روی دکمه Next کلیک کنید.



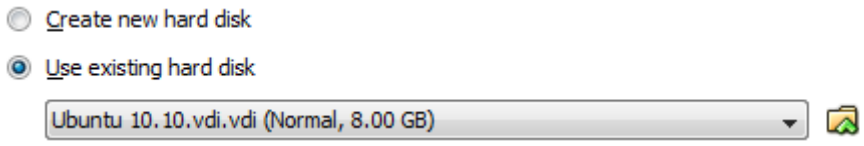
در صفحه بعد، میزان حافظه RAM که به این سیستم عامل تخصیص می‌دهید را بر حسب مگابایت وارد نمایید. توصیه می‌شود که همین مقدار پیش فرض را انتخاب نمایید. مقدار پیش فرض برای ویندوز سرور ۲۰۰۳، برابر با 256 MB می‌باشد.



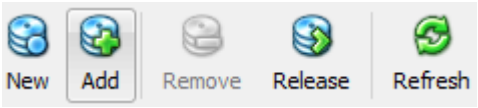
در صفحه بعد، بایستی یک فایل را به عنوان هارد دیسک سیستم عامل مورد نظر انتخاب نمایید. سیستم عامل مجازی این فایل را به صورت یک هارد دیسک مجزا می‌بیند و هر مقدار که اندازه سیستم عامل مجازی شما رشد کند (مثلاً با نصب نرم‌افزارهای مختلف)، اندازه این فایل نیز بزرگتر می‌شود.

اگر از قبل یک فایل به عنوان هارد دیسک دارید و اکنون می‌خواهید این فایل به عنوان هارد دیسک این سیستم عامل جدید استفاده شود (مثلاً قبلاً یک سیستم عامل مجازی نصب کرده‌اید و اکنون می‌خواهید این سیستم عامل را روی ۱۰

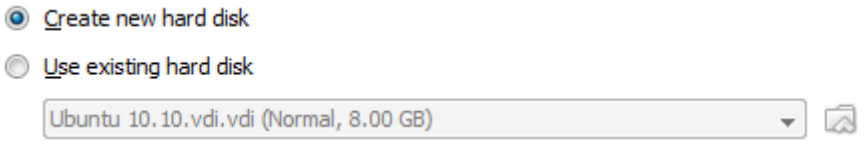
کامپیوتر استفاده نمایید، لذا فایل مربوط به هارد این سیستم عامل را روی هر ۱۰ کامپیوتر کپی می‌نمایید)، گزینه دوم یعنی Use Existing Hard Disk را انتخاب نموده و سپس روی علامت کلیک نمایید.



در صفحه باز شده، روی دکمه Add کلیک نموده و سپس فایل مورد نظر را انتخاب نمایید.



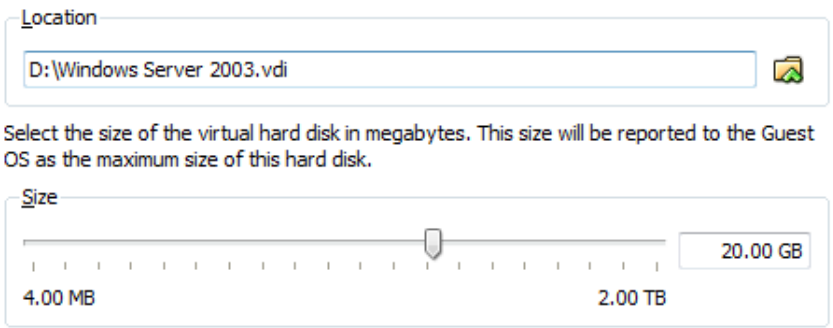
پس از انتخاب فایل مورد نظر، روی Select کلیک کنید. اما اگر هیچ فایلی به عنوان هارد دیسک ندارید و می‌خواهید فایلی جدید به عنوان هارد دیسک بسازید، گزینه Create New Hard Disk را انتخاب نموده و سپس روی Next کلیک نمایید.



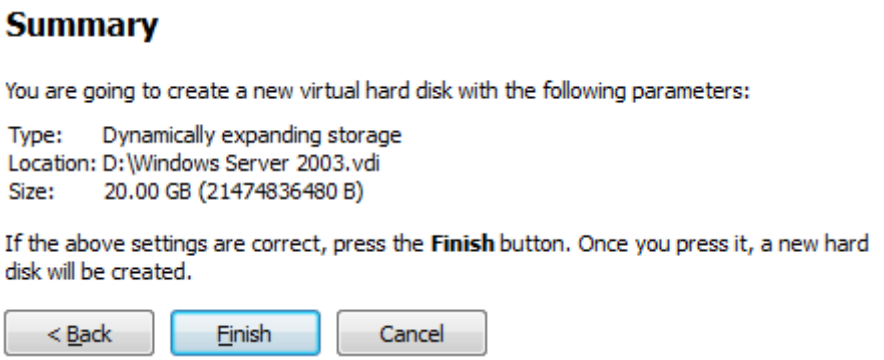
صفحه ایجاد هارد جدید باز می‌شود. پس از عبور از صفحه خوش آمد گویی، وارد صفحه نوع هارد دیسک از لحاظ روش گسترش سایز می‌شوید. در این صفحه اگر گزینه Dynamically Expanding Storage را انتخاب نمایید، هارد دیسک شما، ابتدا اندازه صفر دارد (قبل از نصب سیستم عامل مجازی) و به موازات رشد سیستم عامل مجازی، اندازه فایل نیز بزرگتر می‌شود. اما اگر گزینه Fixed-Size Storage را انتخاب نمایید، بدین معنا است که اگر اندازه هارد را مثلاً 10 GB انتخاب نمودید، فایل شما نیز از همان ابتدا 10 GB فضا اشغال می‌کند، حتی اگر هیچ سیستم عاملی هم نصب نکرده باشید. توصیه می‌شود گزینه Dynamically Expanding Storage را انتخاب نمایید. در نهایت روی Next کلیک کنید.



در صفحه بعدی بایستی اندازه هارد دیسک مورد نظر و محل فایل متناظر با آن را تعیین نمایید. توصیه می‌شود که اندازه پیش فرض را قبول نموده و فایل متناظر با هارد دیسک را نیز در جایی ذخیره نمایید که به اندازه کافی فضای خالی داشته باشد. سپس روی دکمه Next کلیک کنید.

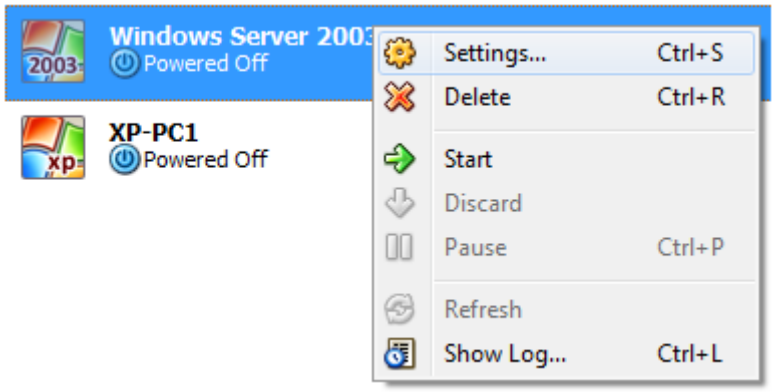


در پایان، نرم‌افزار، خلاصه‌ای از کارهای انجام شده را به شما نشان می‌دهد. جهت اتمام عملیات ساخت هارد و معرفی سیستم عامل جدید، روی دکمه Finish کلیک نمایید.

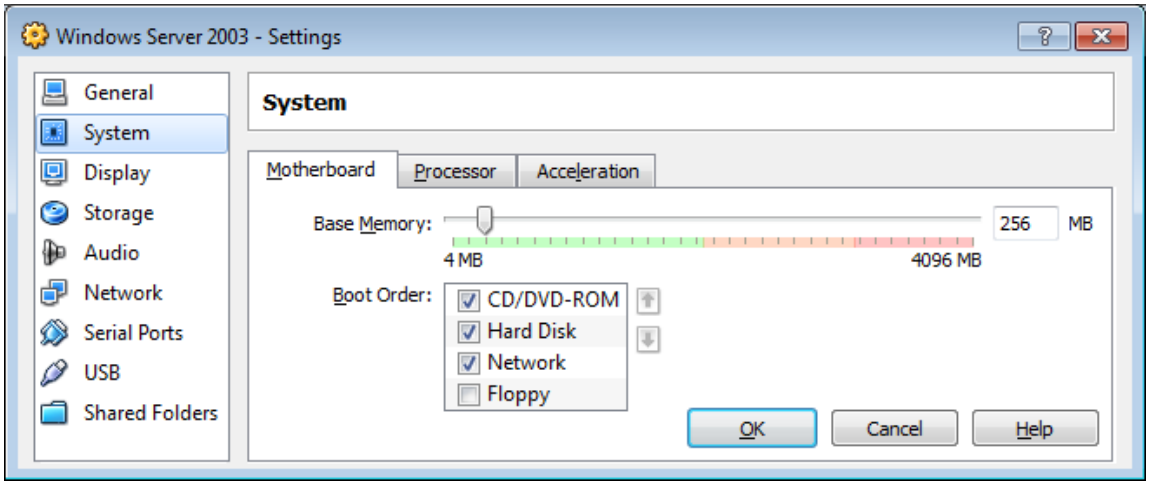


تا اینجا شما فقط سیستم عامل جدید خود را به همراه هارد دیسک آن و مقدار حافظه RAM به نرم‌افزار Virtual Box معرفی نموده‌اید. اما هنوز سیستم عامل خود را نصب نکرده‌اید.

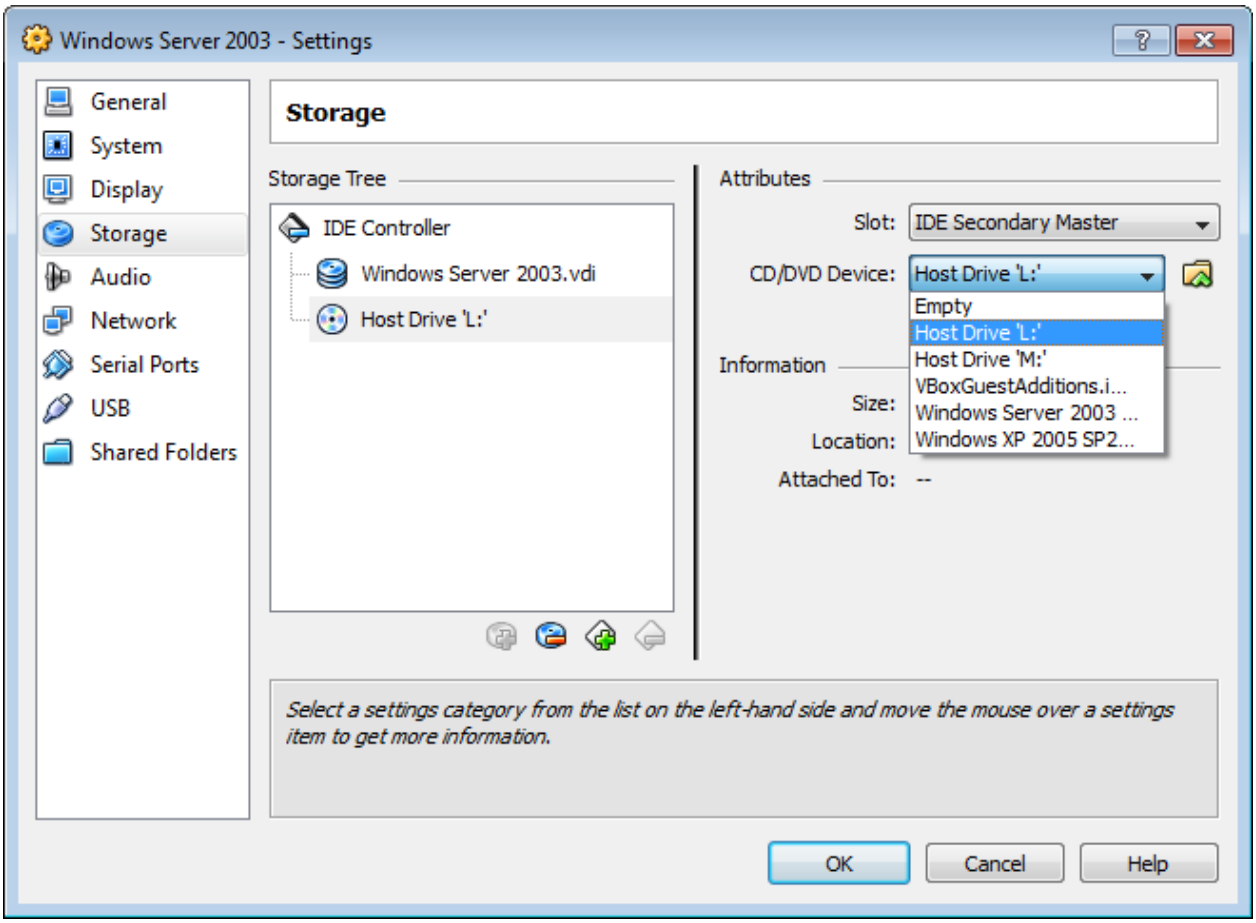
حال نوبت به عملیات نصب سیستم عامل جدید می‌رسد. عملیات نصب سیستم عامل مجازی، دقیقا مانند سیستم عامل‌های واقعی می‌باشد. بدین منظور بایستی ابتدا تنظیماتی را روی سیستم عامل مجازی خود انجام دهیم. لذا روی سیستم عامل مورد نظر راست کلیک نموده و گزینه Settings را انتخاب نمایید.



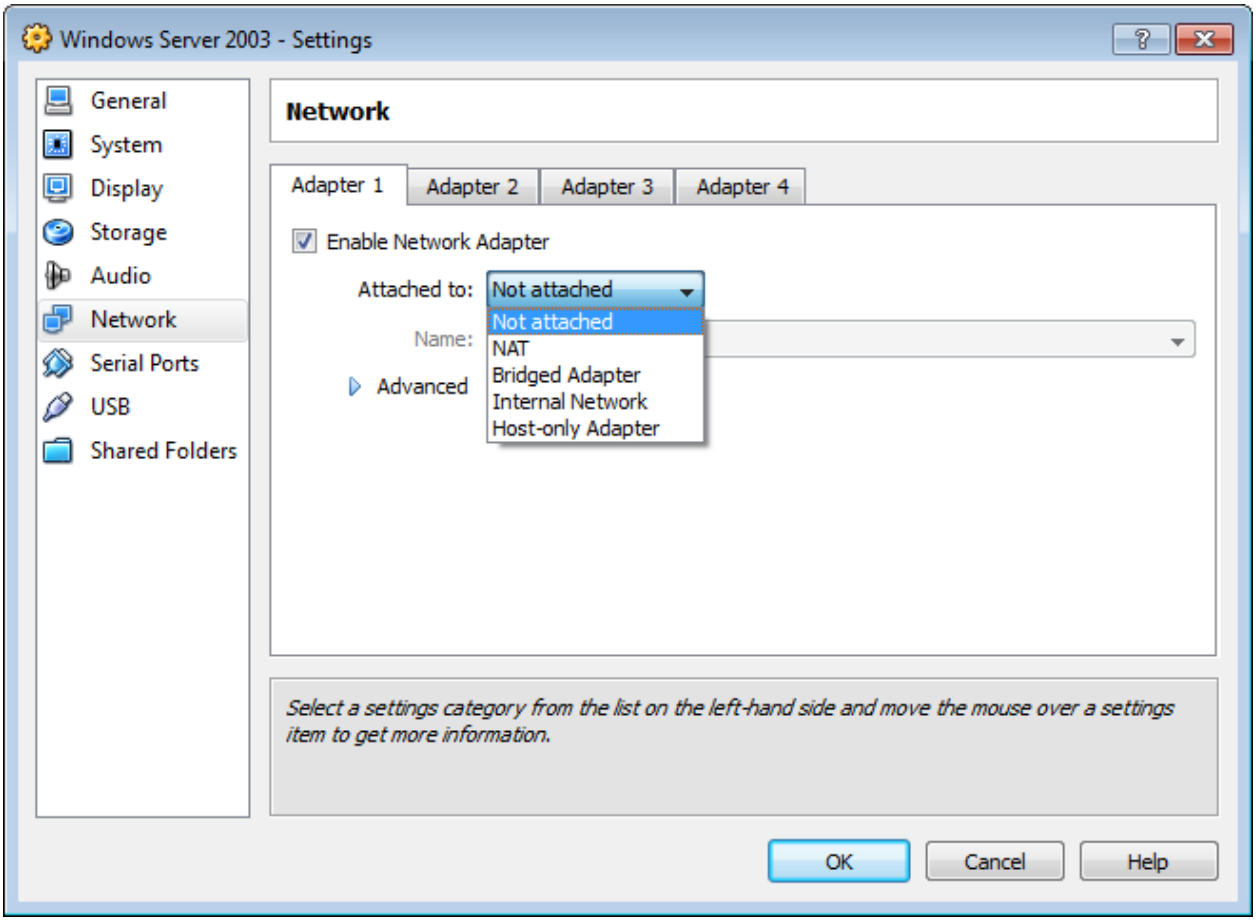
شما از طریق این قسمت می‌توانید تنظیماتی را روی سیستم مجازی خود انجام دهید. مثلاً از طریق قسمت System، می‌توانید میزان RAM مورد استفاده و نیز ترتیب دستگاه‌ها جهت بوت شدن (راه اندازی) سیستم عامل را تعیین نمایید. بهتر است مانند شکل زیر تعیین نمایید که بوت شدن ابتدا از هارد دیسک شروع شده و سپس به سراغ سی دی رام برود.



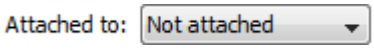
در مراحل قبل، مشخص نمودیم که سیستم عامل مجازی، از کدام فایل به عنوان هارد دیسک خود استفاده نماید. حال بایستی به سیستم عامل مجازی خود بگوییم که از کدام یکی از دیسک‌های نوری ما به عنوان سی دی رام خود استفاده نماید. در نرم‌افزار Virtual Box این امکان وجود دارد که بتوان یک فایل Image با پسوند.iso را به عنوان سی دی رام یک سیستم عامل مجازی انتخاب نمود. جهت انجام تنظیمات سی دی رام، ابتدا وارد قسمت Storage شوید. در سمت چپ، ابتدا Host Drive را انتخاب نموده و سپس در سمت راست، یکی از دیسک‌های نوری سیستم را به عنوان سی دی رام انتخاب نمایید. اینکه چگونه یک فایل Image را به عنوان سی دی رام انتخاب کنیم را جلوتر توضیح خواهیم داد. از آنجا که در اکنون اولویت اصلی ما نصب سیستم عامل می‌باشد، سی دی شامل سیستم عامل را درون درایو سی دی قرار داده و در قسمت Storage، این درایو سی دی را به عنوان سی دی رام سیستم عامل مجازی انتخاب می‌کنیم.



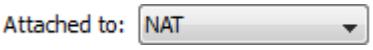
مهمترین قسمت تنظیمات سیستم عامل مجازی، تنظیمات شبکه آن می‌باشد. تنظیمات این بخش، تاثیر زیادی بر کار ما دارد؛ زیرا هدف ما از راه اندازی سیستم عامل مجازی، شبکه کردن چندین سیستم عامل به صورت مجازی می‌باشد. جهت انجام تنظیمات شبکه، وارد قسمت Network شوید. در Virtual Box، امکان تعریف ۴ کارت شبکه به صورت همزمان وجود دارد که ما در اینجا فقط با یک آداپتور کار داریم. چگونگی کارکرد شبکه را در ۵ وضعیت مختلف می‌توان تعیین نمود. در ادامه این ۵ حالت را توضیح می‌دهیم. فرض کنید که سیستم عامل اصلی ما، ویندوز ۷ می‌باشد که ما Virtual Box را روی آن نصب نموده‌ایم. روی Virtual Box نیز دو سیستم عامل Windows XP و Windows Server 2003 نصب نموده‌ایم که این دو سیستم عامل‌های مجازی ما می‌شوند.



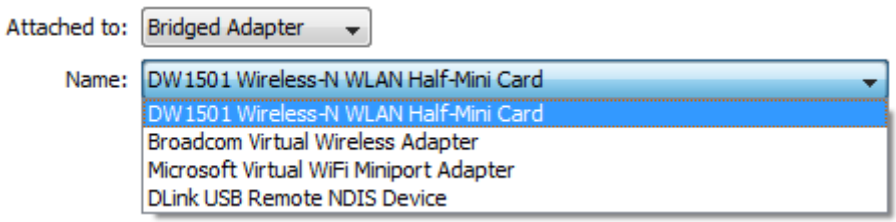
- **Not Attached:** این گزینه بدین معنا است که سیستم عامل مجازی ما، اصلا کارت شبکه ندارد.



- **NAT:** بدین معنی می‌باشد که سیستم عامل مجازی ما، با هیچ سیستم دیگری شبکه نیست، ولی امکان اتصال به اینترنت را دارد. یعنی دقیقا مانند یک سیستم عامل مستقل عمل می‌کند.



- **Bridge Adapter:** توسط این قسمت می‌توان تعیین نمود که سیستم عامل مجازی، بتواند توسط یکی از تجهیزات سیستم عامل اصلی (Windows 7) به اینترنت متصل شود. بعد از انتخاب این گزینه، بایستی تجهیزی که می‌خواهیم به کمک آن به اینترنت متصل شویم را نیز تعیین نماییم.

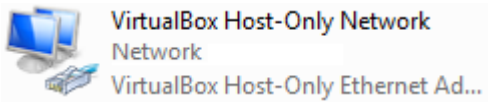


- **Internal Network:** از این گزینه برای شبکه کردن سیستم عامل‌های مجازی با یکدیگر استفاده می‌شود (در اینجا Windows XP و Windows Server 2003). اگر قصد داریم کارهای عملی این فصل را با سیستم عامل‌های مجازی انجام دهیم، بایستی چندین سیستم عامل مجازی را با یکدیگر شبکه کنیم که برای شبکه کردن آن‌ها بایستی از گزینه

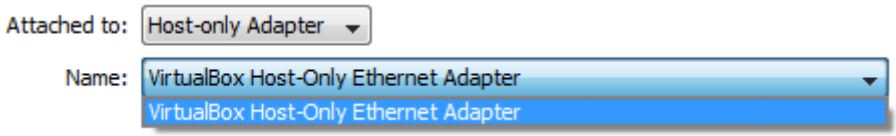
Internal Network استفاده نماییم. بعد از انتخاب این گزینه، بایستی نامی برای شبکه مجازی خود انتخاب کنیم که طبعا سیستم عامل هایی با یکدیگر شبکه می‌شوند که هم مجازی بوده و هم نام شبکه اشان با یکدیگر برابر باشد.



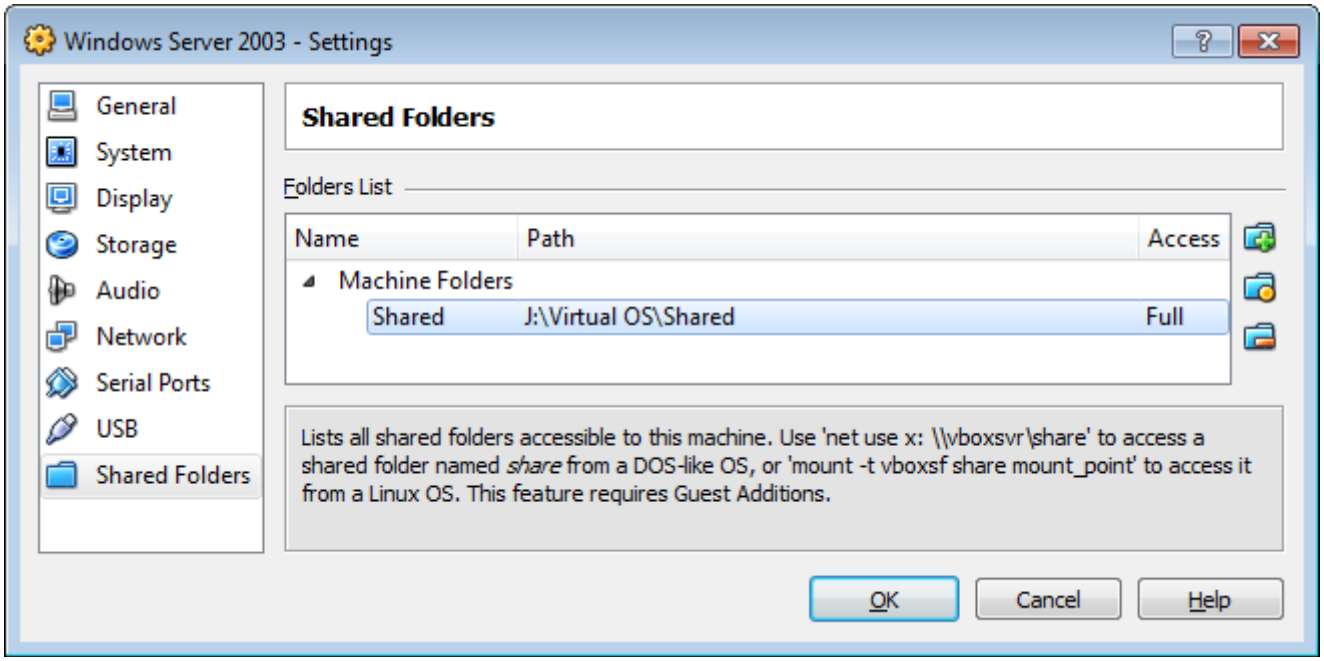
– **Host-Only Adapter:** از این گزینه برای شبکه کردن سیستم عامل مجازی (در اینجا Windows XP یا Windows Server 2003) با سیستم عامل واقعی (در اینجا Windows 7) استفاده می‌شود. نرم‌افزار Virtual Box هنگام نصب، یک آداپتور شبکه به سیستم عامل واقعی به نام VirtualBox Host-Only Network ایجاد می‌کند. که اگر قصد دارید با گزینه Host-Only Adapter، سیستم عامل مجازی را با سیستم عامل واقعی شبکه کنید، بایستی این کانکشن را فعال (Enable) سازید.



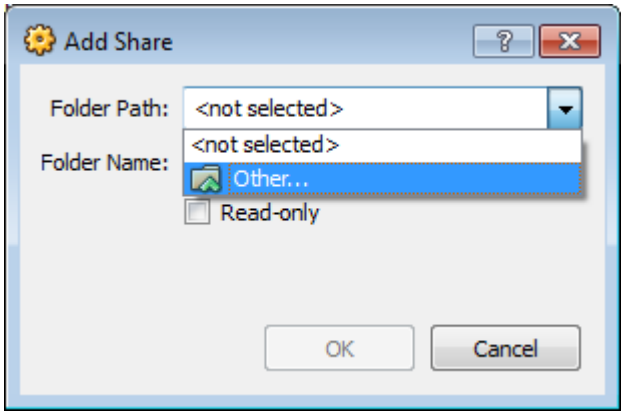
این امکان وجود دارد که روی سیستم عامل واقعی، چندین کانکشن Virtual Box وجود داشته باشد که در این صورت، پس از انتخاب گزینه Host-Only Adapter، بایستی کانکشن مورد نظر را نیز انتخاب نمایید.



یکی دیگر از امکانات Virtual Box، امکان به اشتراک گذاری پوشه‌ای خاص بین سیستم عامل واقعی و سیستم عامل مجازی می‌باشد تا بتوان برخی فایل‌ها را به راحتی بین هر دو سیستم عامل منتقل نمود. بدین منظور، ابتدا یک پوشه در سیستم عامل واقعی بسازید. سپس در بخش تنظیمات وارد قسمت Shared Folders شوید.



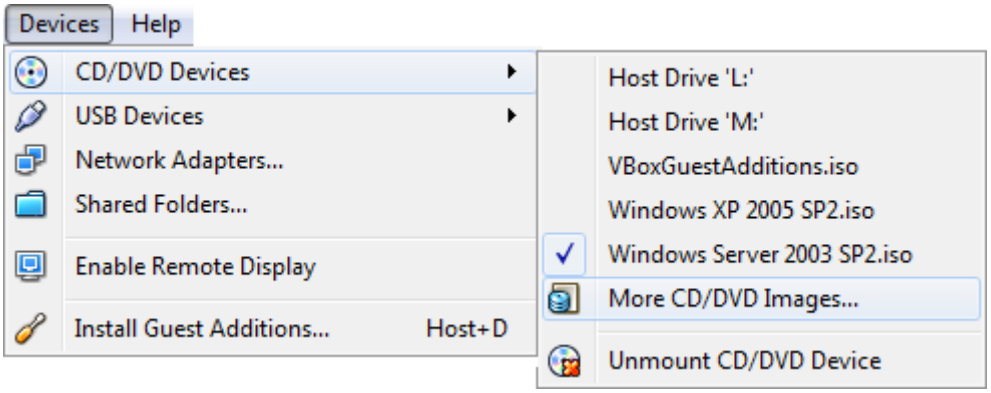
برای افزودن پوشه‌ای جدید برای اشتراک گذاری، روی دکمه کلیک نمایید. در صفحه باز شده، گزینه Other را انتخاب نموده و سپس پوشه مورد نظر را جهت به اشتراک گذاری انتخاب نمایید. این پوشه به صورت یک درایو Map شده در سیستم عامل مجازی نمایش داد می‌شود.



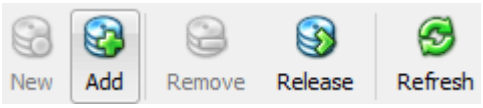
سپس سی دی ویندوز را در سی دی رام قرار داده و سپس سیستم عامل مجازی را انتخاب نموده و روی دکمه Start کلیک کنید.



صبر نمایید تا عملیات نصب سیستم عامل مجازی خاتمه یابد و سیستم عامل مجازی بالا بیاید. پس از بالا آمدن سیستم عامل مجازی، در هر لحظه امکان تغییر سی دی رام وجود دارد. حتی می‌توان یک فایل Image را به عنوان یک سی دی رام به سیستم عامل مجازی معرفی نمود. برای انجام این کار، در صفحه سیستم عامل مجازی، از منوی Devices، و قسمت CD/DVD Devices، یکی از سی دی رام‌های موجود را انتخاب کنید. اگر قصد دارید که یک فایل Image را به عنوان سی دی رام معرفی نمایید، گزینه More CD/DVD Images را انتخاب نمایید.



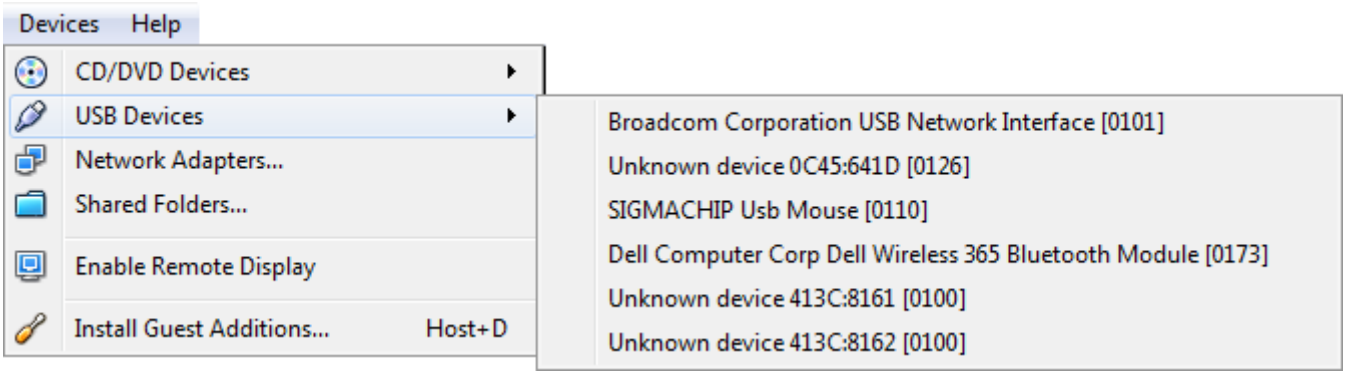
در صفحه باز شده، می‌توانید فایل‌های Imageای که تا کنون استفاده کرده‌اید را مشاهده نمایید. جهت انتخاب فایل Image جدید، روی دکمه Add کلیک نموده و سپس فایل Image را انتخاب کنید. بدین ترتیب محتوای این فایل Image به عنوان سی دی رام در سیستم عامل مجازی نشان داده می‌شود.



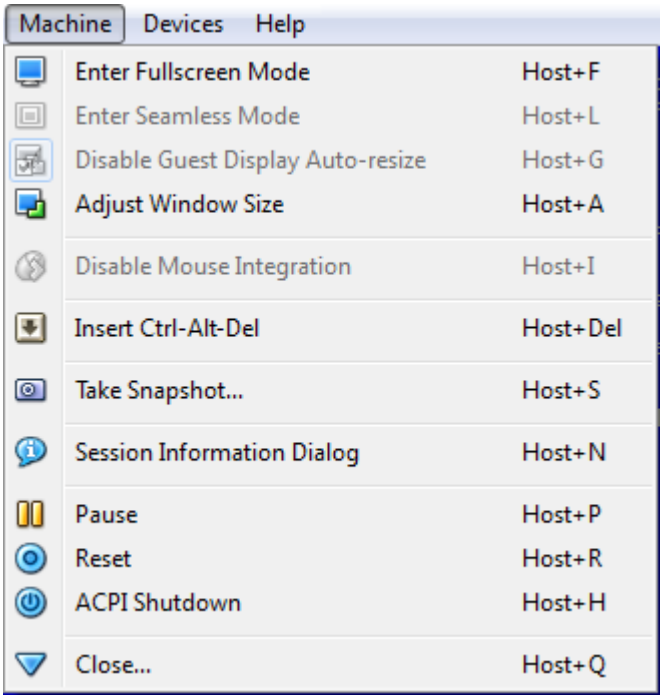
پس از نصب سیستم عامل مجازی و بالا آمدن کامل سیستم عامل، شما نیاز دارید برخی درایورها را نصب نمایید تا سیستم عامل مجازی بتواند به خوبی و با سرعت بالا کار کند. مثلاً بتواند Full Screen شود. این درایورها به صورت پیش فرض توسط نرم‌افزار Virtual Box عرضه شده است. جهت استفاده از آن، از قسمت Devices ➔ CD/DVD Devices، گزینه VBoxGuestAdditions.iso را انتخاب نمایید. محتویات این فایل Image در قالب سی دی رام نمایش داده می‌شود. محتویات آن را نصب نموده و سیستم عامل مجازی خود را Restart نمایید.



از طریق منوی Devices ➔ USB Devices نیز می‌توان تجهیزات USB را به سیستم عامل مجازی معرفی نمود.



منوی Machine نیز امکاناتی را نظیر Full Screen و کلیدهای CtrlA+lt+Del را در اختیار قرار می‌دهد. در کلیدهای میانبر، منظور از کلمه Host، دکمه Ctrl سمت راست می‌باشد که البته این دکمه قابل تغییر می‌باشد.



در قسمت پایین پنجره نیز دکمه هایی به ازاء تجهیزات وصل شده، مانند هارد دیسک، آداپتور شبکه و... تعبیه شده است.



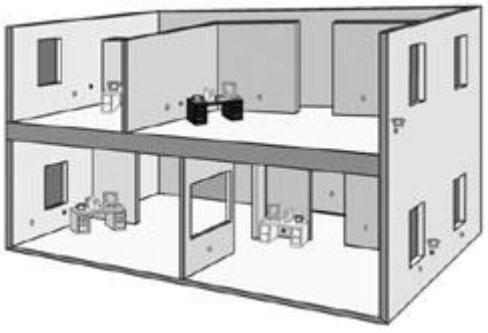
جهت پیاده سازی مناسب مثال‌های این جزوه، توصیه می‌شود که روی نرم‌افزار Virtual Box، دو عدد Windows XP و یک عدد Windows Server 2003 نصب شود.

فصل ۱۵

راه اندازی شبکه Workgroup و نحوه Share کردن داده ها

۱۵-۱- اشتراک گذاری

اگر در محیط کار یا منزل خود با بیش از یک کامپیوتر سروکار دارید، احتمالا به فکر افتادهاید که آن‌ها را به یکدیگر متصل کرده و یک شبکه کوچک کامپیوتری راه بیندازید.



از طریق یکی از کامپیوترها که به اینترنت وصل است، بقیه را نیز به اینترنت متصل کنید؛ از هر یک از کامپیوترها به فایل‌های خود از جمله عکس‌ها، آهنگ‌ها و اسناد دسترسی پیدا کنید؛ به بازی هایی بپردازید که به چند بازیکن با چند کامپیوتر نیاز دارند و بالاخره این که خروجی وسایلی چون DVD Player یا وب کم را به سایر کامپیوترها ارسال کنید.

در این فصل ضمن معرفی روش‌های مختلف اتصال کامپیوترها به یکدیگر، انجام تنظیمات دستی را برای بهره بردن از حداقل مزایای یک شبکه کامپیوتری به شما نشان می‌دهیم.

۱۵-۲- چگونه عملا چند کامپیوتر را به یکدیگر شبکه کنیم؟

چند وقت پیش یکی از دانشجویان سوالی پرسید، مبنی بر اینکه فرض کنید که در یک شرکت ۵ کامپیوتر داریم، چگونه آن‌ها را با یکدیگر شبکه کنیم؟

در ادامه مرسوم ترین راه جهت انجام این کار را توضیح می‌دهیم:

۱- خریداری یک سوییچ که تعداد پورت آن برابر با تعداد کامپیوترها باشد. معمولا تعداد پورت سوییچ‌ها، ۵ یا ۸ یا ۱۶ یا ۳۲ است. در زمان نوشتن این متن، قیمت سوییچ ۸ پورت حدود ۹۰،۰۰۰ و سوییچ ۱۶ پورت حدود ۱۶۰،۰۰۰ تومان می‌باشد.

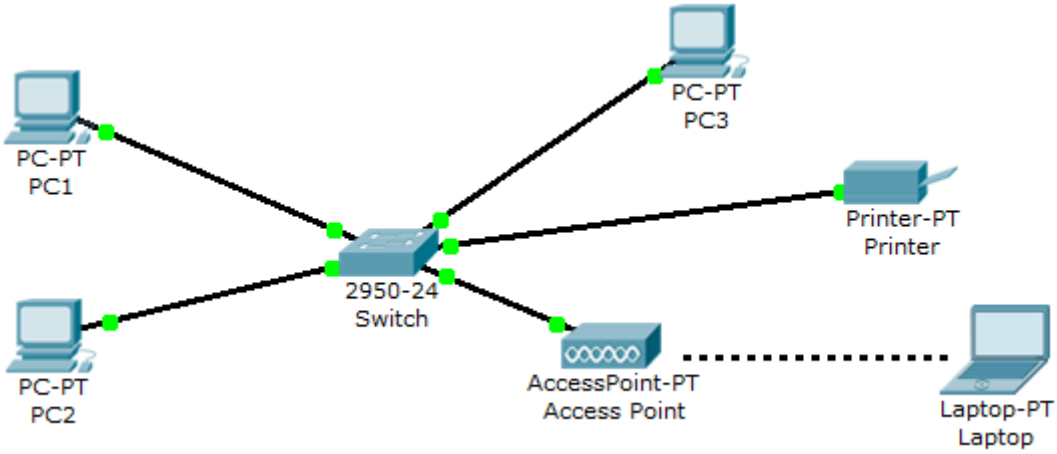
۲- خریداری کابل‌های شبکه از نوع Cross و با سوکت RJ-45 به تعداد کامپیوترها.

پس از تهیه نمودن این تجهیزات، سوییچ را در یک مکان مناسب قرار دهید، به طوری که به تمامی کامپیوترها نزدیک باشد. سپس یک سر کابل‌ها را به سوییچ متصل نموده و سر دیگر کابل را به قسمت کارت شبکه کامپیوتر متصل نمایید. در نهایت سوییچ و کامپیوترها را روشن نمایید.

با این کار، کامپیوترها به صورت سخت‌افزاری به یکدیگر شبکه شده‌اند. پس از روشن شدن کامپیوترها، آدرس IP کامپیوترها به گونه‌ای تنظیم نمایید تا قسمت Net ID کامپیوترها با یکدیگر برابر شده و در یک محدوده آدرس IP قرار بگیرند. بدین ترتیب کامپیوترها از لحاظ نرم‌افزاری نیز شبکه می‌شوند.

نکته: اگر کارت شبکه شما Wireless است، به یک Access Point جهت اتصال به سوییچ سیمی نیاز دارید.

در شکل زیر، ما سه کامپیوتر و یک چاپگر داریم که به صورت سیمی و یک لپتاپ داریم که به صورت بی‌سیم و با کمک Access Point به یک سوییچ وصل شده‌اند.



۱۵-۳- مراحل انجام کار

برای راه اندازی شبکه در منزل خود این سه کار را باید انجام دهیم:

۱- انتخاب فناوری مناسب شبکه مورد نظر، که در این فصل، استاندارد مورد نظر، اترنت است.

۲- خرید و نصب سخت‌افزار مناسب این کار، که اصلی ترین آن‌ها کارت شبکه برای هر یک از کامپیوترهای شبکه و یک هاب یا سوئیچ است.

۳- آماده سازی سیستم‌ها به نحوی که بتوانند همدیگر را ببینند و اصطلاحا با یکدیگر صحبت کنند.

از این سه مرحله، گزینه سوم از همه مهم‌تر است. گزینه اول و دوم را که در فصل‌های پیشین توضیح دادیم. در واقع ما در این لحظه، فرض می‌کنیم که شما تجهیزات سخت‌افزاری مورد نیاز جهت ایجاد یک شبکه محلی را فراهم کردهاید (مثلاً از یک سوئیچ استفاده کرده و آن را پیکربندی نموده و کامپیوترهای خود را به آن متصل کردهاید یا در ساده ترین حالت ۲ کامپیوتر را با یک کابل UTP به صورت مستقیم به هم وصل کرده اید). لذا فقط به بررسی تنظیمات نرم‌افزاری می‌پردازیم.

ویندوز XP قسمتی به نام Network Setup Wizard دارد که تنظیمات شبکه را برای شما انجام میدهد (این قسمت در Control Panel قرار دارد). به غیر از حالت، این متخصصان هستند که در ازاء دریافت دستمزد، شبکه شما را در محل راه می‌اندازند. نام گذاری کامپیوترها، به اشتراک گذاشتن چاپگرها، فایل‌ها و اتصالات اینترنتی، اساسی ترین کارهایی هستند که این افراد برای شما انجام می‌دهند. اما اگر با مشکلی مواجه بشوید یا تنظیمات کامپیوتر تان بهم بخورد، باید بتوانید خودتان شبکه را تنظیم کنید.

کلا بد نیست مفاهیم و اصول راه اندازی یک شبکه کامپیوتری را بدانید تا به هنگام ضرورت خودتان بتوانید دست به کار شوید.

به طور کلی کار هایی که باید انجام دهید تا یک شبکه ‘‘مرده’’ را ‘‘زنده’’ کنید و به بهره برداری از آن بپردازید، از این قرار است:

۱. نام گذاری کامپیوتر
۲. دادن آدرس IP
۳. به اشتراک گذاشتن فایل‌ها
۴. به اشتراک گذاشتن چاپگر
۵. انجام تنظیمات امنیتی
۶. به اشتراک گذاشتن اتصال اینترنت
۷. اتصال یک درایو به پوشه Share شده (Map Network Drive)

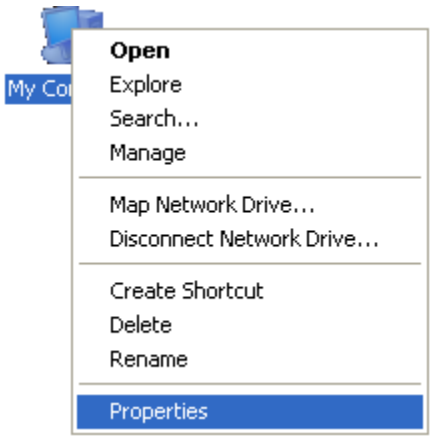
۱۵-۴- نام گذاری کامپیوتر

بعد از نصب سخت‌افزارهای مورد نیاز برای راه اندازی شبکه، نوبت به نصب نرم‌افزارهای آن می‌رسد. در اولین قدم باید برای تک تک کامپیوترهای موجود در شبکه خود اسمی منحصر به فرد و غیر تکراری انتخاب کنید.

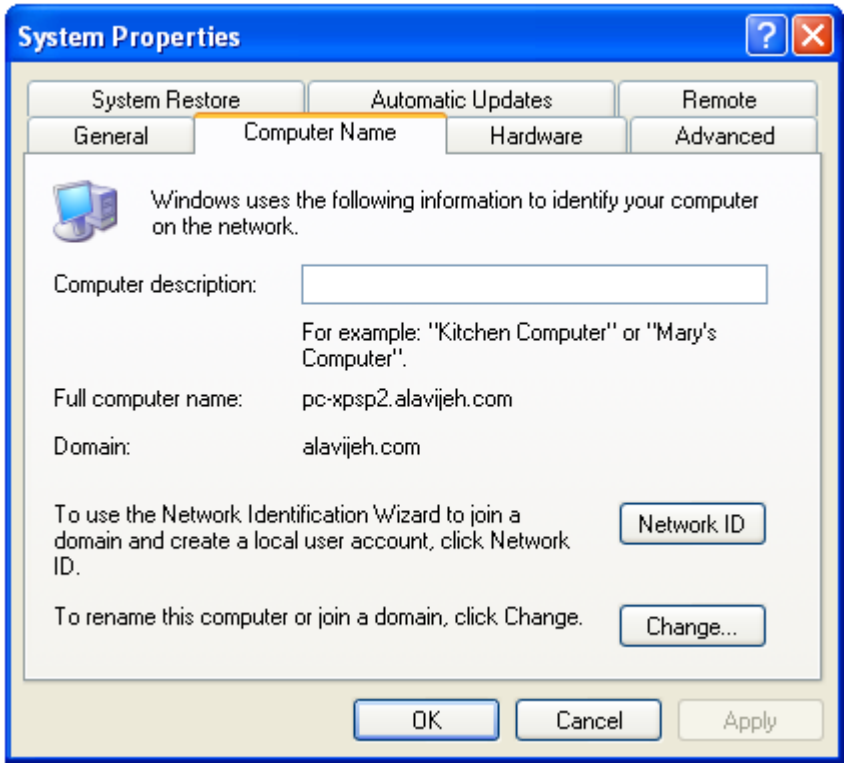
علاوه بر اسم کامپیوتر اسم گروه کاری یا Work Group هم مهم است. تمام کامپیوترهای یک شبکه باید عضو یک گروه کاری باشند.

برای نام گذاری کامپیوتر در ویندوز XP این مراحل را دنبال کنید:

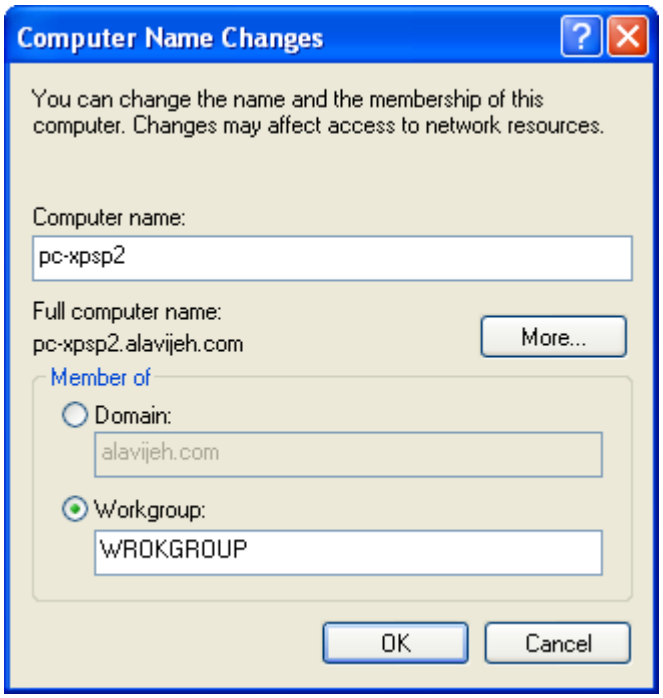
۱- بر روی My Computer راست کلیک کرده و گزینه Properties را انتخاب نمایید.



۲- در کادر محاوره ظاهر شده صفحه Computer Name را انتخاب کنید.



۳- بر روی دکمه Change کلیک کنید تا صفحه زیر باز شود.



همان طور که ملاحظه می‌کنید کامپیوتر یک اسم کامل دارد و یک گروه کاری.

۴- در کادر اول اسمی را تایپ کنید که می‌خواهید به کامپیوتر تان اختصاص دهید. این اسم هر چیزی می‌تواند باشد، فقط نباید تکراری باشد. مثلاً اسم کامپیوتر اول را PC1 بگذارید.

۵- در کادر دوم اسمی را که می‌خواهید به گروه کاری خود اختصاص دهید وارد کنید. مثلاً My office یا My Home یا هر چیز دیگر. حتی خود Work Group هم بد نیست.

۶- در پایان OK و دوباره OK را بزنید. اگر ویندوز خواست Restart کند، قبول کنید.

۱۵-۵- تنظیم آدرس IP

آدرس IP نشانی هر کامپیوتر در شبکه است. کامپیوتر از طریق این نشانی است که یکدیگر را در شبکه پیدا می‌کنند.

در هر شبکه آدرس IP هر کامپیوتر باید منحصر به فرد و غیر تکراری باشد.

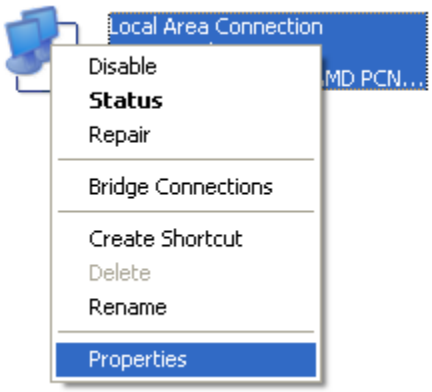
سپس به تعیین آدرس IP و آدرس Subnet Mask می‌پردازیم که توضیحات آن را در فصول قبل ارائه کردیم.

در یک شبکه کوچک، برای تمام کامپیوترها، سعی می‌کنیم کلاس آدرس IP را Class A در نظر بگیریم. لذا سه قسمت اول آدرس IP را یکسان می‌گیریم و فقط قسمت چهارم را برای هر کامپیوتر عدد متفاوتی را در نظر می‌گیریم.

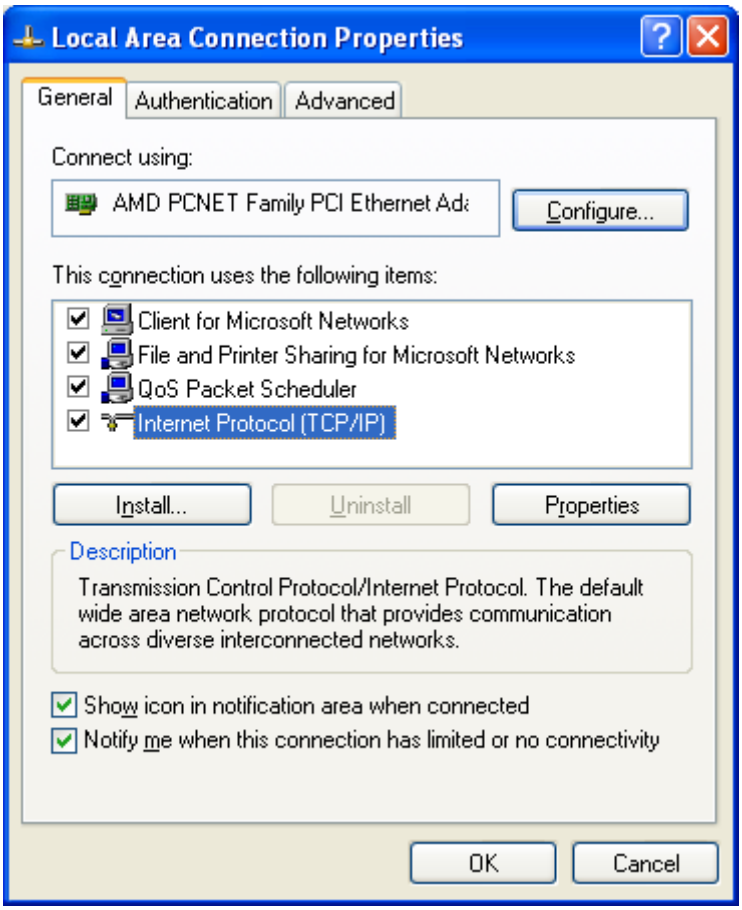
مثلاً در کامپیوتر اول آدرس ۱۹۲.۱۶۸.۰.۱ و برای کامپیوتر دوم آدرس ۱۹۲.۱۶۸.۰.۲ را می‌نویسیم و به همین ترتیب در بقیه کامپیوترها قسمت چهارم آدرس IP را عدد متفاوتی را می‌دهیم.

۱- Control Panel را باز کرده و Network Connections را انتخاب کنید

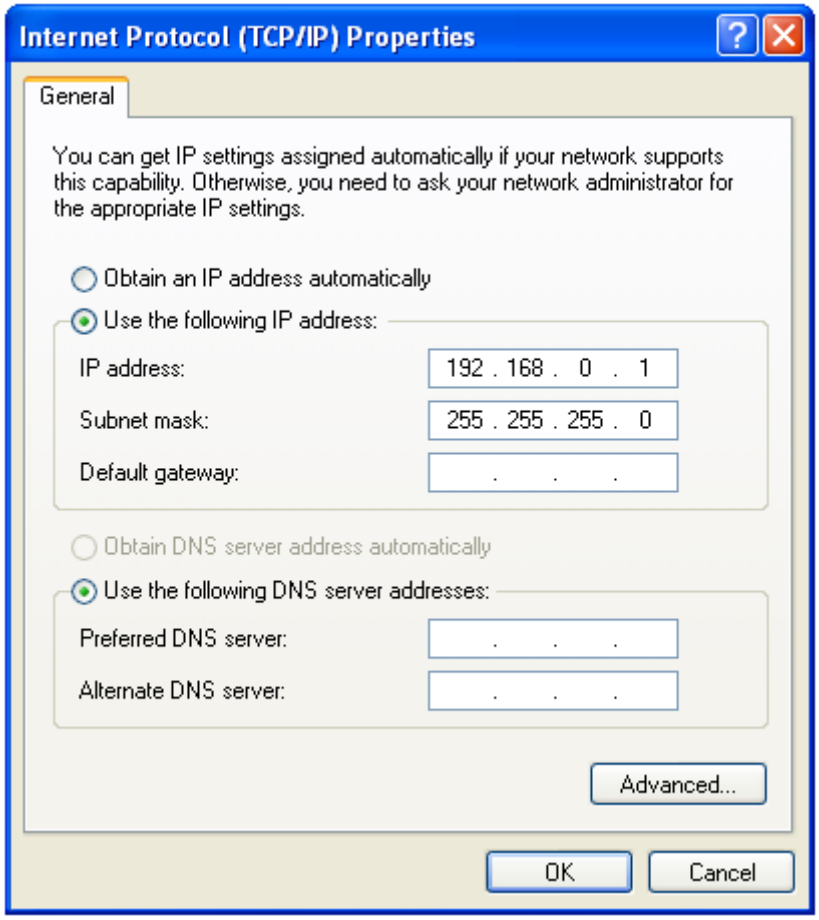
۲- بر روی آیکون Local area connection کلیک راست کرده و گزینه Properties را انتخاب کنید.



۳- در پنجره بعدی روی Internet Protocol (TCP/IP) کلیک کرده و کلید Properties را کلیک نماید.



۴- طبق توضیحات فوق IP مورد نظر و سایر اطلاعات را وارد کنید.



۲- دکمه OK و دوباره OK را بزنید.

بعد از این که به همین ترتیب به بقیه کامپیوترها هم آدرسIP دادید، نوبت به Share کردن فایل‌ها و پوشه‌ها می‌رسد. شبکه‌ای که نتواند فایل هایش را با دیگران سهیم کند، زیاد به درد نمی‌خورد. مثلاً می‌توانید مجموعه فایل‌های MP3 و موسیقی خود را در یکی از کامپیوترها بگذارید و با Share کردن آن‌ها، به بقیه کامپیوترها هم اجازه دسترسی بدهید.

۱۵-۶- به اشتراک گذاشتن فایل‌ها (File Sharing) و استفاده از آن‌ها

یکی از کاربردهای اصلی شبکه، به اشتراک گذاشتن فایل‌ها میان کامپیوترها است. این کار در ویندوز، به ویژه ویندوز XP، بسیار آسان است. توجه نمایید که تنها می‌توان پوشه‌ها و هر آنچه داخل آن است را به اشتراک گذاشت و امکان به اشتراک گذاری یک فایل به صورت مستقیم وجود ندارد.

اشتراک گذاری در ویندوز XP به دو صورت ساده و پیشرفته انجام می گیرد که ما هر دو روش را توضیح خواهیم داد. بین اشتراک گذاری ساده و پیشرفته تفاوت‌های زیر وجود دارد:

۱- در حالت ساده، نیازی به ایجاد رمز بر روی ویندوز نیست، اما در حالت پیشرفته بایستی برای تمامی کاربران تعریف شده روی سیستم، رمز عبور تعریف کنیم.

۲- در حالت ساده، امکان تعیین رمز عبور جهت دسترسی به پوشه Share شده وجود ندارد. اما در حالت پیشرفته، کاربر هنگام دسترسی به پوشه Share شده، بایستی یکی از نام‌های کاربری و رمزهای عبور تعریف شده در سیستم را وارد نماید.

۳- در حالت ساده، امکان تعیین سطح دسترسی برای کاربران مختلف وجود ندارد، اما در حالت پیشرفته می‌توان به ازاء هر کاربر سطح دسترسی متفاوت تعریف نمود.

۴- در حالت پیشرفته، می‌توان تعیین نمود که در هر لحظه، حداکثر چند نفر می‌توانند به پوشه دسترسی داشته باشند، اما در حال ساده این کار امکان پذیر نیست.

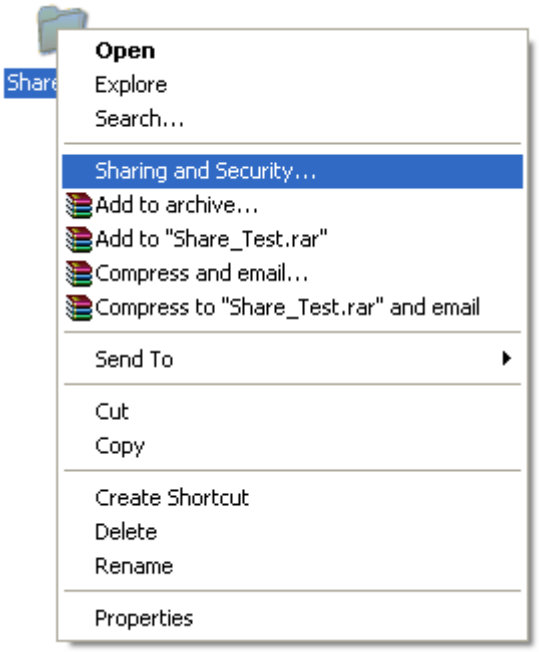
۵- در حالت پیشرفته، بر عکس حالت ساده امکان استفاده از Caching وجود دارد تا بتوان در زمانی که سرور فعال نیست، بازهم از پوشه Share شده استفاده نمود.

۱۵-۶-۱- اشتراک گذاری ساده

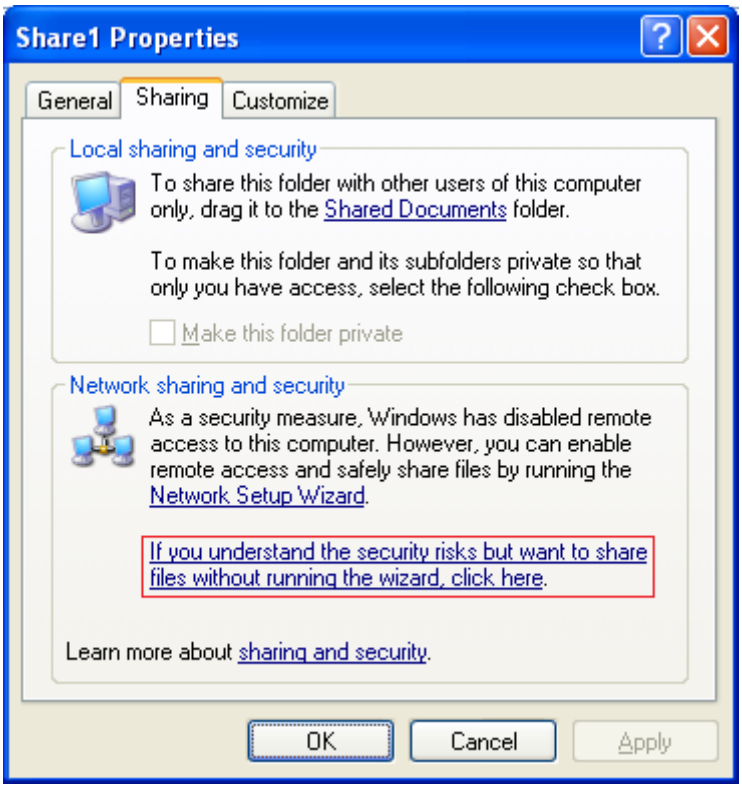
به صورت پیش فرض، اشتراک گذاری در ویندوز XP به صورت ساده انجام می گیرد.

به منظور اشتراک گذاری یک پوشه، روی آن راست کلیک نموده و گزینه Sharing and Security را انتخاب کنید.

راه دیگر راست کلیک روی پوشه، انتخاب گزینه Properties و سپس رفتن به سربرگ Sharing است.



سپس صفحه‌ای مانند زیر باز می‌شود. این صفحه می‌گوید که شما هنوز ساختار شبکه خود را تعیین ننمودهاید. در مورد چگونگی تعیین ساختار شبکه و ایجاد شبکه‌های Workgroup، در ادامه و در همین فصل صحبت خواهیم کرد. ابتدا روی گزینه If you understand … کلیک کنید.

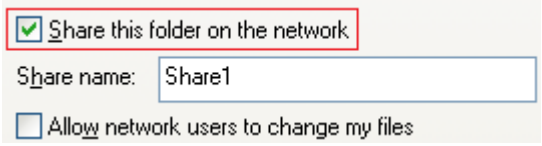


سپس در صفحه باز شده گزینه Just Enable file sharing (گزینه دوم) را انتخاب نموده و سپس روی OK کلیک کنید. اگر گزینه اول را انتخاب کنید، یک صفحه Wizard جهت تعیین چگونگی ساختار شبکه Workgroup باز می‌شود که در مورد آن بعدا صحبت خواهیم کرد.



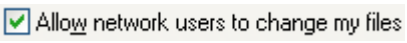
سپس گزینه Share this folder on the network را تیک زده و نامی برای پوشه Share شده در شبکه وارد نمایید. توجه نمایید که نام Share می‌توان**د** با نام اصلی پوشه متفاوت باشد. همچنین نمی‌توان دو یا چند نام Share یکسان داشت. دلیل نیز این است که کاربران راه دور، تنها نام پوشه‌های Share شده را می‌بینند و نمی‌توانند مسیر اصلی آن پوشه‌ها بر روی هارد شما را مشاهده نمایند. در شکل زیر، من نام پوشه به اشتراک گذاشته شده را Share1 گذاشته ام.

نکته: اگر در انتهای نام Share، علامت $ بگذارید، پوشه Share می‌شود، اما دیگر کاربران شبکه نمی‌توانند این پوشه را مشاهده نمایند.

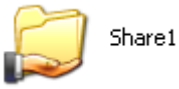


۱۵-۶- به اشتراک گذاشتن فایل‌ها (File Sharing) و استفاده از آن‌ها

اگر می‌خواهید دیگر کاربران شبکه بتوانند محتویات پوشه Share شده را تغییر دهند، گزینه Allow network users to change my files را تیک بزنید.



در نهایت روی OK کلیک کنید تا پوشه Share شده و شکل آن عوض شود.

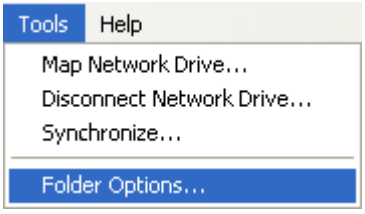


تا اینجا کار به اشتراک گذاری پوشه به پایان رسیده است. در مورد چگونگی استفاده از این پوشه در دیگر کامپیوترها بعدا صحبت خواهیم نمود.

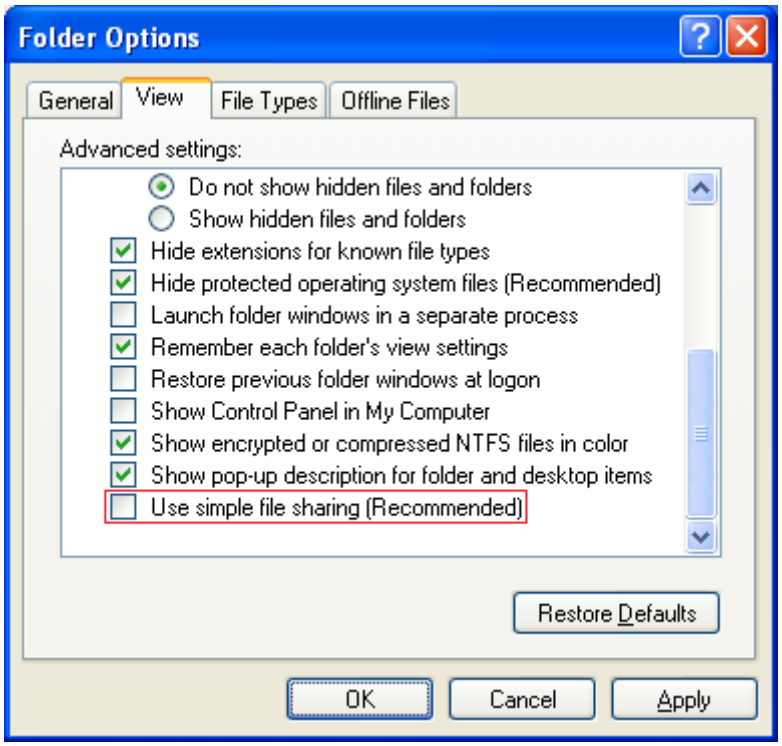
۱۵-۶-۲- اشتراک گذاری پیشرفته

جهت اشتراک گذاری پیشرفته، مراحل زیر را دنبال نمایید.

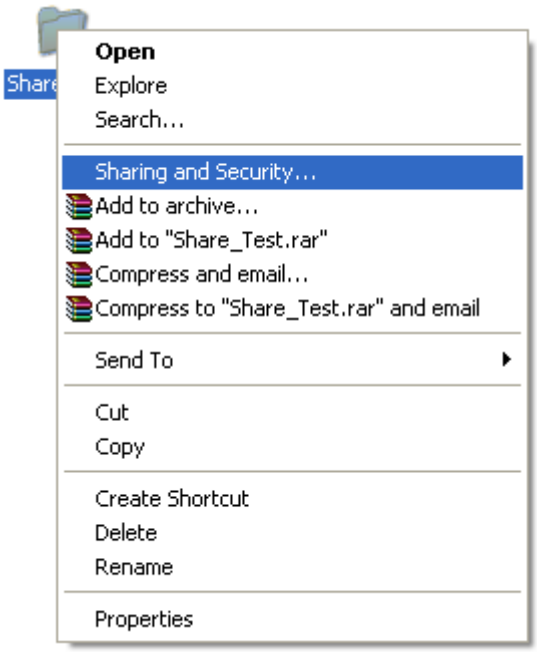
۱- ابتدا وارد My Computer شده، سپس از منوی Tools گزینه Folder Option را انتخاب نمایید.



۲- سپس وارد سربرگ View شده و تیک گزینه آخر یعنی گزینه Use Simple File Sharing را بردارید.



۳- سپس روی پوشه‌ای که می‌خواهید آن را Share کنید، راست کلیک کرده و سپس گزینه Sharing and Security را انتخاب کنید.

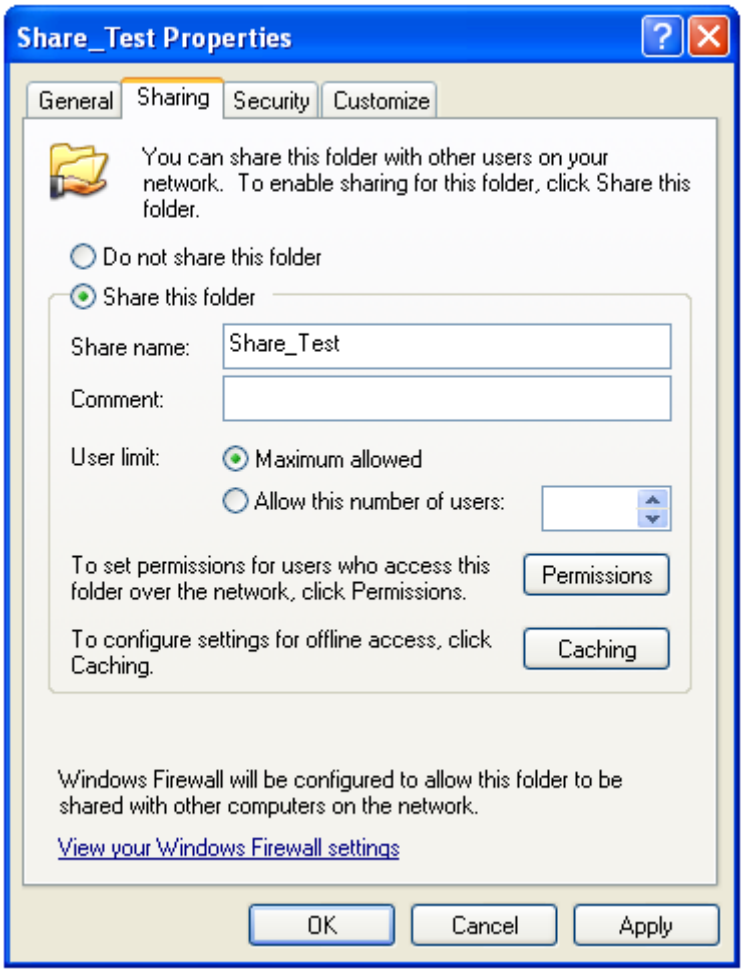


۴- در کادر محاوره ظاهر شده، به صفحه Sharing بروید. حالا گزینه Share This Folder را انتخاب کنید و اسمی را برای پوشه تایپ کنید که می‌خواهید در شبکه به آن اسم شناخته شود.

وقتی پوشه‌ای را به اشتراک می‌گذارید، تمامی کاربران شبکه می‌توانند پوشه Share شده را ببینند. اگر می‌خواهید پوشه Share شده را مخفی کنید، هنگام اشتراک گذاری، انتهای نام آن، یک علامت $ قرار دهید (توجه: نام پوشه را تغییر ندهید، بلکه هنگام اشتراک گذاری، در قسمت Share Name، انتهای نام پوشه یک علامت $ بگذارید). در این مثال می‌شود: Share_Test$

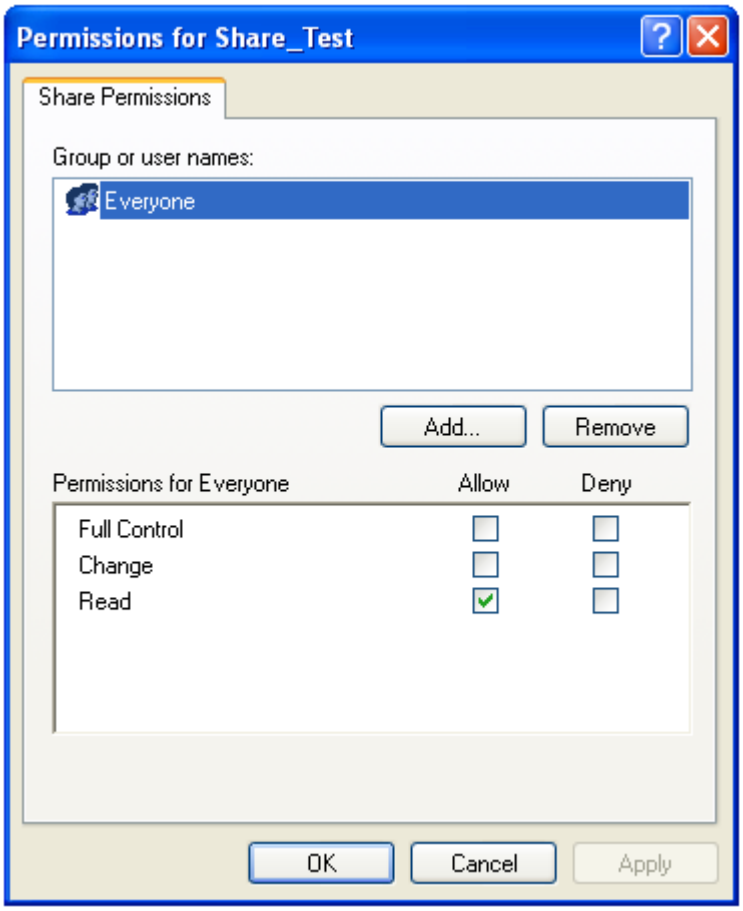
البته به طور پیش فرض در ویندوز XP، برخی قسمت‌ها به صورت مخفیانه به اشتراک گذاشته شده‌اند که عبارتند از:

- C$، D$، E$ و...: به اشتراک گذاری ریشه درایو ها
- Admin$: پوشه ویندوز
- IPC$: برای کاربران کاربردی ندارد و برای ارتباط بین برنامه‌های رایانه در شبکه و مدیریت از راه دور برنامه‌ها مورد استفاده قرار می‌گیرد.



۵- در همین صفحه، این قابلیت وجود دارد که تعیین نمایید که به طور همزمان چند نفر در شبکه به این پوشه دسترسی داشته باشند. ایجاد محدودیت روی دسترسی همزمان، تاثیر زیادی در کنترل ترافیک در شبکه‌های شلوغ دارد. برای تعیین محدودیت دسترسی همزمان، در همین صفحه گزینه Allow this number of users را انتخاب کرده و سپس در جعبه متن روبروی آن، تعداد را وارد نمایید.

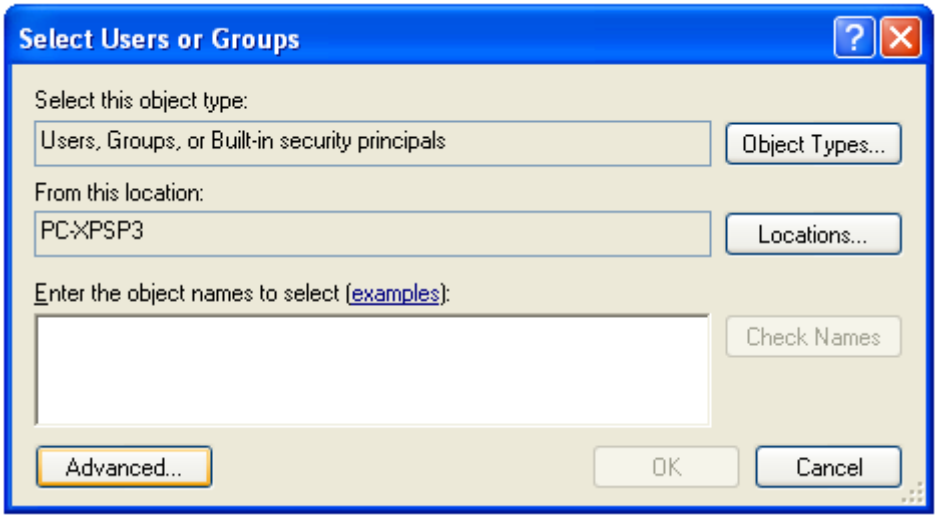
۶- وقتی پوشه‌ای را در شبکه به اشتراک می‌گذارید، این اختیار را دارید که نوع دسترسی به آن (و فایل‌های موجود در آن) را تعیین کنید. این دسترسی می‌تواند به صورت فقط خواندنی (Read-Only) باشد، یا دسترسی کامل (Full Control). وقتی دسترسی به صورت فقط خواندنی باشد، کاربر اجازه ندارد پوشه را حذف یا چیزی داخل آن کپی کند، اما می‌تواند محتوای پوشه را مشاهده و در صورت نیاز آن را در کامپیوتر خود کپی کند. حتی می‌تواند از همان جا به اجرا یا (مثلاً در مورد موسیقی) به پخش فایل‌ها بپردازد. در این رابطه در قسمت تنظیم امنیت بیشتر صحبت خواهیم کرد. اما به طور خلاصه، برای تنظیم دسترسی، در همین صفحه روی دکمه Permissions کلیک کنید.



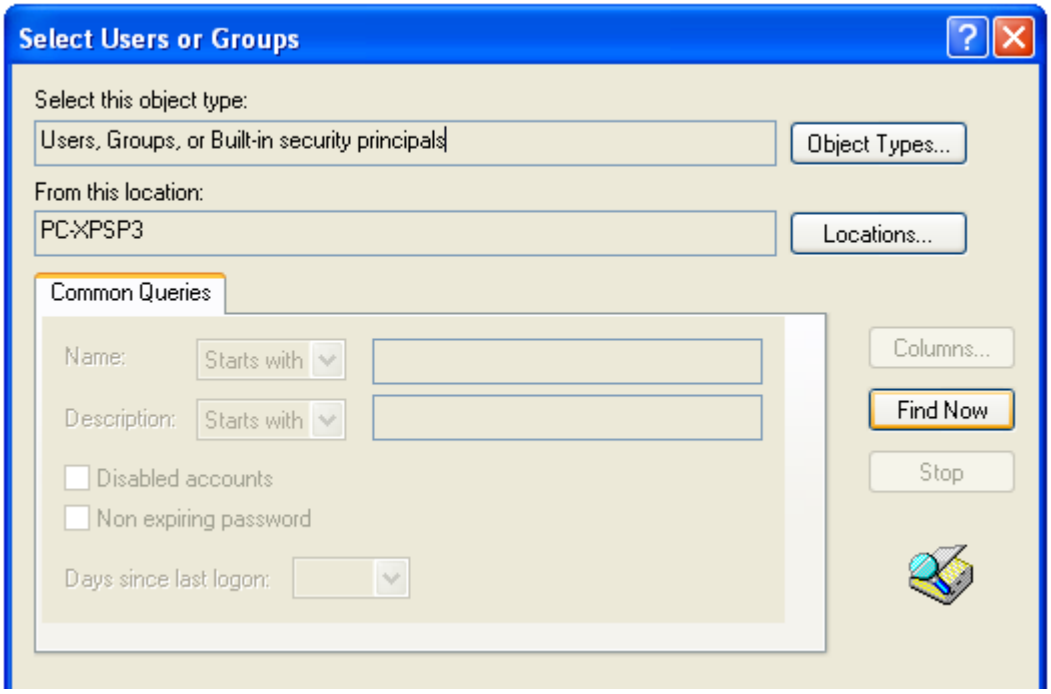
۷- سپس در این صفحه، سطح دسترسی هر کاربر را تعیین نمایید.

۸- می‌توانید دسترسی کاربر دیگری را نیز تعیین نمایید. برای این کار در همین صفحه روی دکمه Add کلیک کنید.

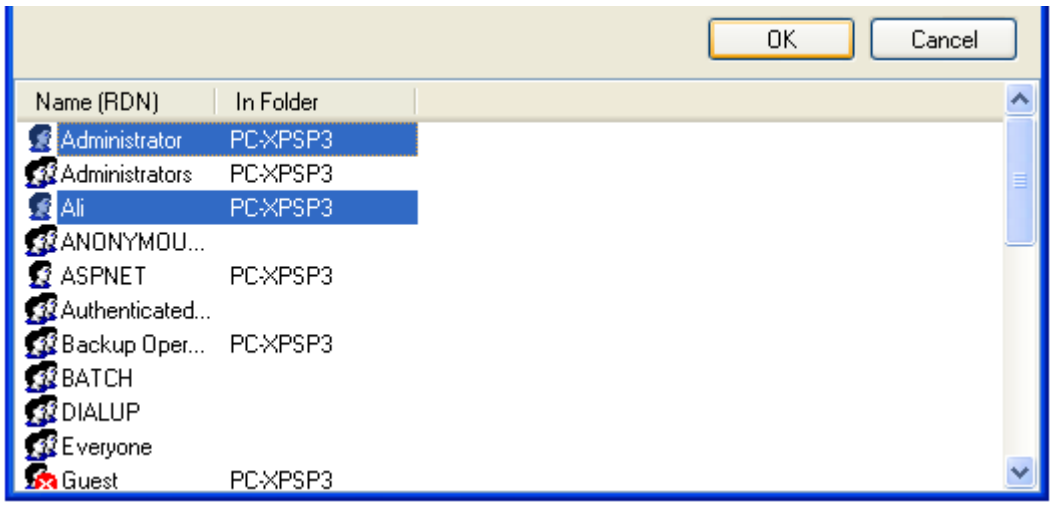
۸- سپس روی دکمه Advanced کلیک نمایید.



۹- سپس در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست تمام کاربران و گروه‌های موجود در کامپیوتر به نمایش درآید.



۱۰- سپس در صفحه باز شده، کاربر (کاربران) یا گروه (گروه های) مورد نظر را انتخاب کنید:



۱۱- سپس دو بار OK نمایید.

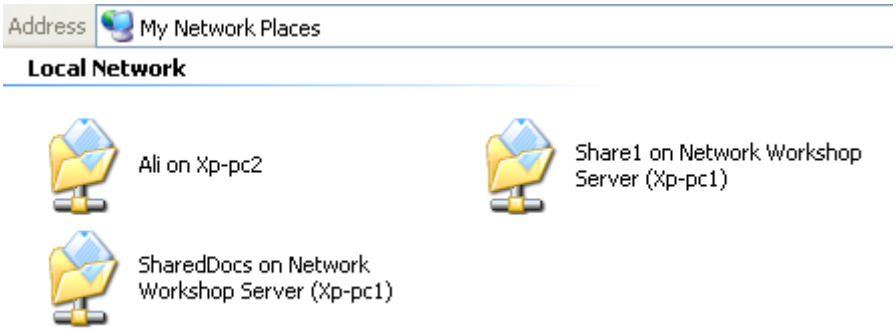
۱۲- توجه نمایید که نام Everyone که در صفحه دسترسی‌ها مشاهده نمودید؛ تمامی کاربران جزء این گروه هستند. لذا در دادن دسترسی به این گروه نهایت دقت را به عمل آورید. زیرا به طور مثال اگر گروه Everyone قابلیت نوشتن داشته باشد، و اگر از کاربری مانند Ali، اجازه نوشتن را بگیرید، بازهم کاربر Ali اجازه نوشتن را دارد.

۱۵-۶-۳- استفاده از پوشه Share شده

برای دسترسی به پوشه‌ای که به اشتراک گذاشته شده است، در کامپیوتر راه دور، از My Computer، لینک My Network Places را کلیک کنید.



اگر کسی در کامپیوتر خود پوشه‌ای را به اشتراک گذاشته باشد، اسم آن‌ها در پنجره شما ظاهر خواهد شد. از این جا به بعد، مثل این است که آن فایل‌ها و پوشه‌ها در کامپیوتر خود شما هستند.



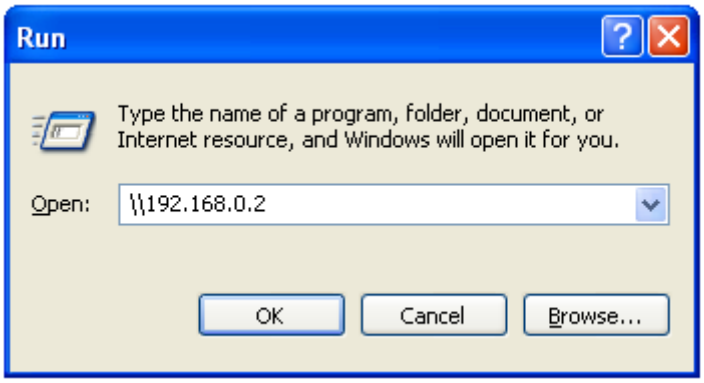
با دوبار کلیک روی اسم یک پوشه، می‌توانید محتوای آن را مشاهده کنید. البته با توجه به اینکه نوع اشتراک گذاری ساده یا پیشرفته باشد، ممکن است هنگام باز کردن یک پوشه، از شما نام کاربری و رمز عبور بخواهد که بایستی نام کاربری و رمز عبوری را وارد نمایید که در همان کامپیوتری که پوشه را به اشتراک گذاشته است، تعریف شده است.

توجه: نکته بسیار مهم در ویندوز XP این است که نام کاربری که وارد می‌کنید باید در هر دو ویندوز تعریف شده باشد. یعنی در این مثال هم در ویندوزی که پوشه را Share کرده و هم در ویندوزی که می‌خواهد از پوشه Share شده استفاده کند، بایستی کاربری به نام Ali وجود داشته باشد. هنوز دلیل این سیاست مایکروسافت را نمی‌دانم. واقعا چرا آخه؟!؟!؟!؟!؟!

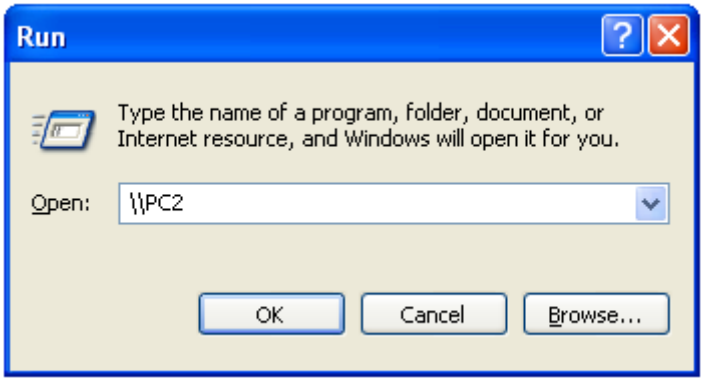


پس از باز کردن پوشه Share شده، اگر بخواهید می‌توانید فایل یا پوشه را به کامپیوتر خودتان کپی کنید. و اگر اجازه داشته باشید، می‌توانید فایلی را حذف نموده یا تغییر نام دهید.

البته راه دیگری نیز برای اتصال به دیگر کامپیوترها دارید و آن اینکه ابتدا وارد Run شده و ابتدا علامت \\ نوشته و سپس **اسم کامپیوتر یا آدرس IP** کامپیوتر مقصد را وارد نمایید.



یا



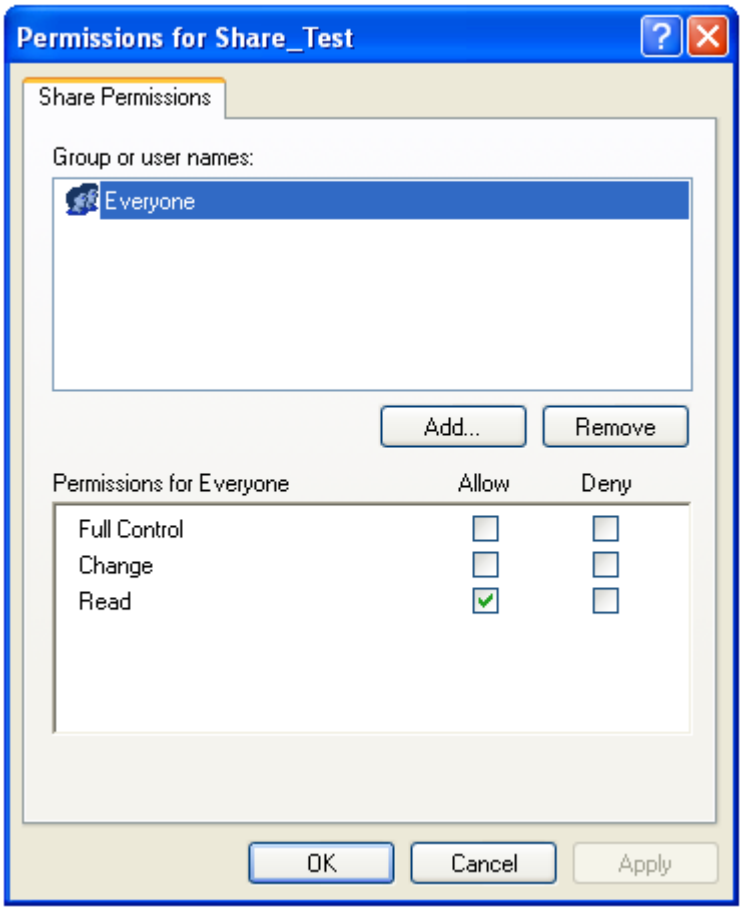
نکته: مزیت این روش این است که می‌توان به پوشه هایی که توسط علامت $ مخفی شده‌اند، توسط وارد نمودن نام آن، دسترسی پیدا نمود.

۱۵-۶-۴- تنظیمات امنیتی

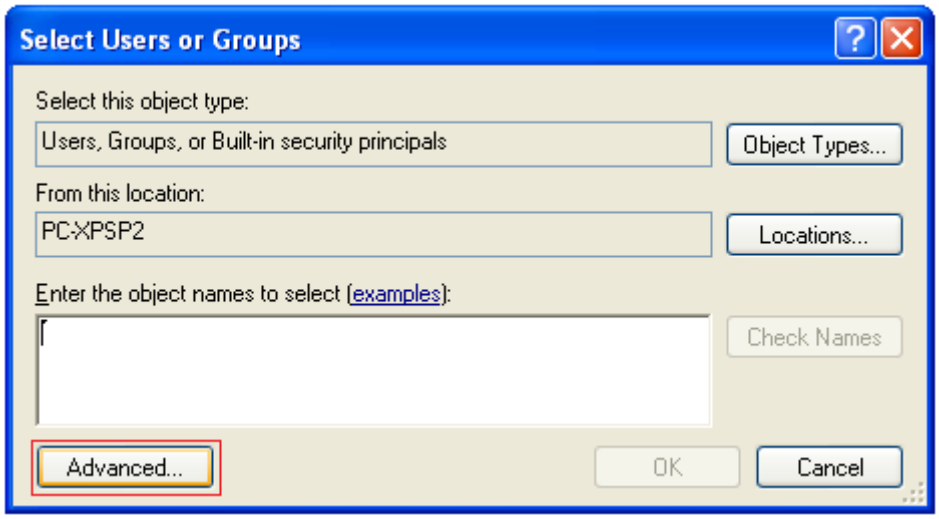
منظور از تنظیمات امنیتی تعیین سطح دسترسی است که یک کاربر از راه دور می‌تواند روی یک فایل یا پوشه Share شده داشته باشد. این کار در دو حالت اصلی "خواندن" و " نوشتن " می‌تواند باشد. وقتی می‌گوییم خواندن، یعنی کاربر می‌تواند محتوای پوشه را ببیند، فایل‌های آن را باز، اجرا، پخش یا مشاهده کند، و در صورت نیاز آن‌ها را به کامپیوتر خود کپی کند. اما نوشتن، یعنی این که کاربر می‌تواند فایل‌های خود را داخل آن پوشه کپی کند، در صورت لزوم فایل یا تمام پوشه را حذف کند، یا اسم فایل‌ها یا پوشه را تغییر دهد.

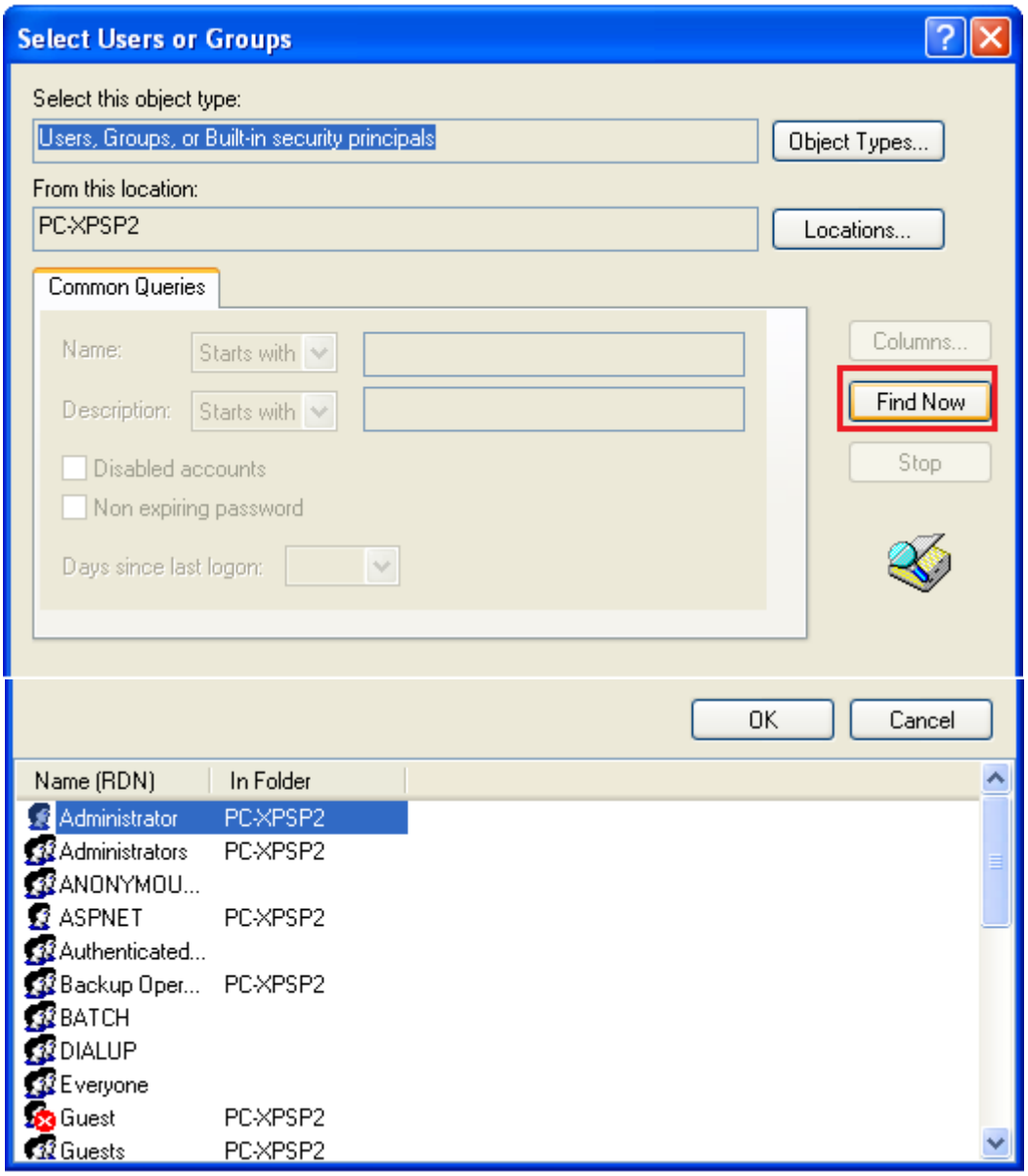
این کارها در ویندوز اکس پی به صورت کاملاً تفکیک شده و جزء به جزء قابل تنظیم هستند. مثلاً اجازه "دیدن محتوای پوشه" از اجازه "اجرای فایل‌های پوشه" کاملاً تفکیک شده‌اند، در حالی که عملاً هر دو این کارها جزو "خواندن" محسوب می‌شوند.

اگر در کادر محاوره‌ای مربوط به Share کردن پوشه، روی دکمه Permissions کلیک کنید، کادر محاوره دیگری ظاهر می‌شود. در این حالت، گزینه های Full Control، Change و Read را می‌بینید که هر کدام می‌توانند پذیرفته (Allow) یا رد (Deny) بشوند. به طور پیش فرض، فقط گزینه Read پذیرفته است، که یعنی کاربران فقط اجازه دیدن و استفاده از فایل‌ها را دارند، نه چیز دیگر.



اگر دقت کرده باشید، در کادر محاوره Permissions، فهرستی از کاربران ارائه شده است. در این شکل شما Everyone را می‌بینید که دسترسی وی Read تعیین شده است. یعنی هر کس که این پوشه Share شده را بخواهد، فقط می‌تواند آن را ببیند و استفاده کند. ولی شاید بخواهید برای کاربران مختلف دسترسی‌های متفاوت تعریف کنید. مثلاً کاربر Administrator می‌تواند دسترسی کامل داشته باشد. برای این منظور، با کلیک روی دکمه Add فهرستی از کاربران تعریف شده در سیستم را خواهید دید. کاربر یا گروه کاربری مورد نظر خود را انتخاب و OK کنید. حالا می‌توانید برای این کاربر، دسترسی متفاوتی تعریف کنید.





در اینصورت، هنگام اتصال از دیگر کامپیوترها به کامپیوتر شما، بایستی یک Username و Password وارد کرد که در اینصورت، شما دسترسی‌های Username وارد شده را خواهید داشت.

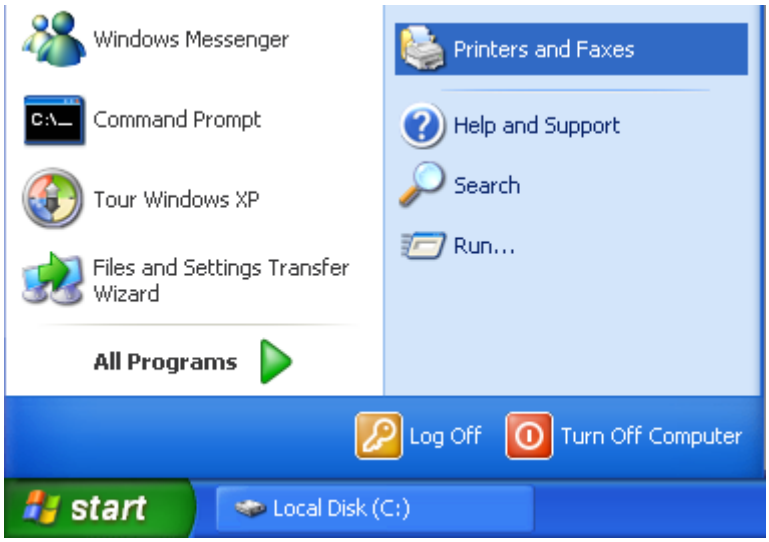
۱۵-۷- به اشتراک گذاشتن چاپگر

ابتدا با برخی از مفاهیم به اشتراک گذاری چاپگر آشنا می‌شویم:

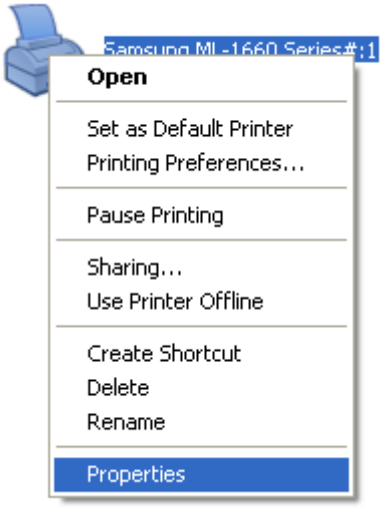
- **Print Server**: به سرویس دهنده‌ای گفته می‌شود که یک چاپگر در آن نصب و به اشتراک گذاشته می‌شود.
- **Print Queue**: به کارهای چاپی که در یک چاپگر منتظر چاپ شدن می‌باشند، گفته می‌شود.
- **Print Job**: به سندی که برای چاپ به یک چاپگر فرستاده می‌شود، اطلاق می‌گردد.

Share کردن چاپگر در ویندوز XP بسیار آسان است:

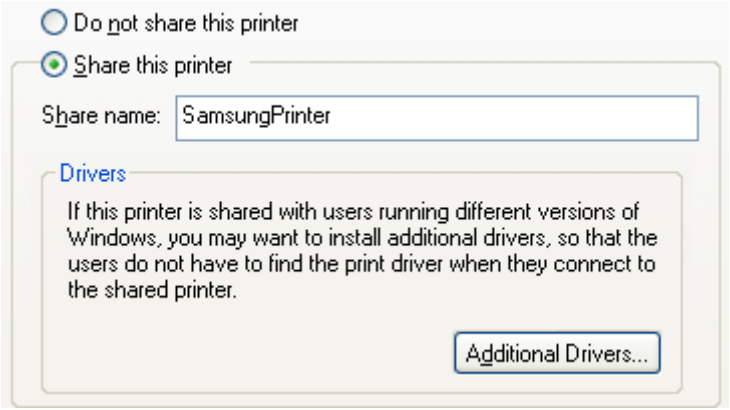
۱- از منوی استارت، گزینه Printers and Faxes را کلیک کنید.



۲- با کلیک راست روی آیکون چاپگری که قصد Share کردن آن را دارید، گزینه Properties را انتخاب کنید.

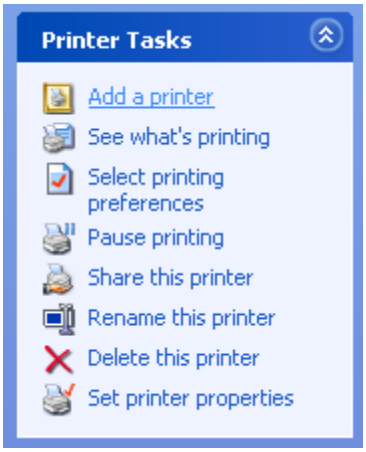


۳- در کادر محاوره ظاهر شده، به صفحه Sharing رفته و گزینه Share this printer را علامت بزنید.

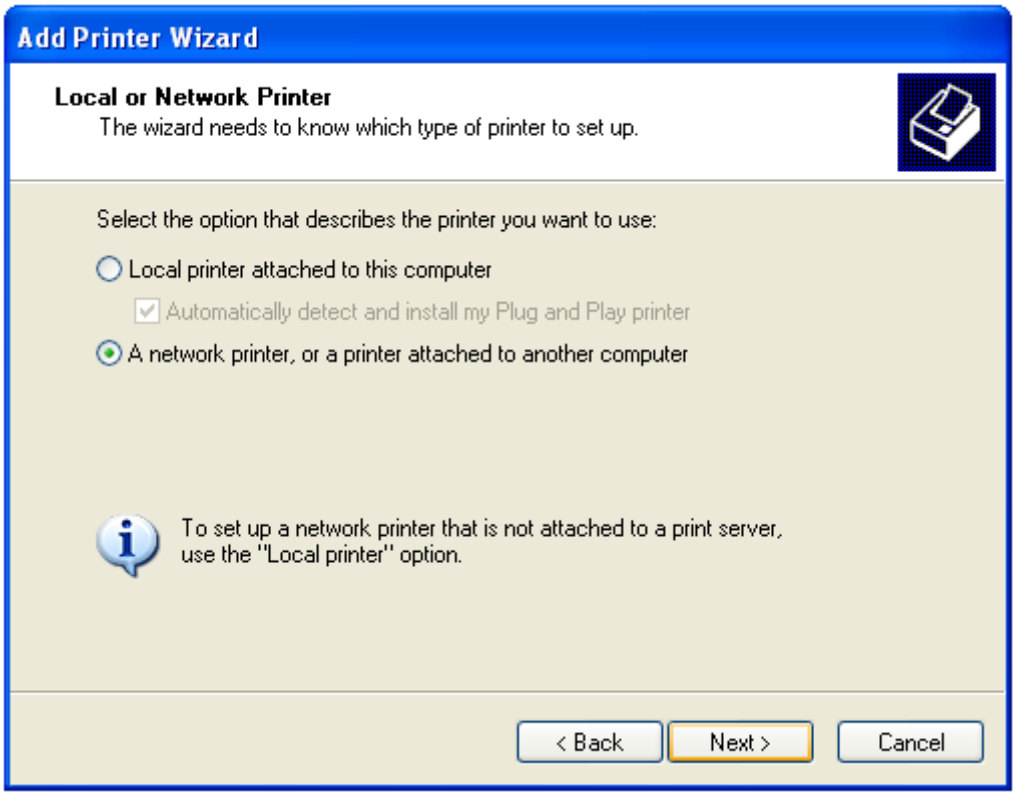


۴- بعد از دادن یک اسم مناسب برای چاپگر خود، دکمه OK را کلیک کنید.

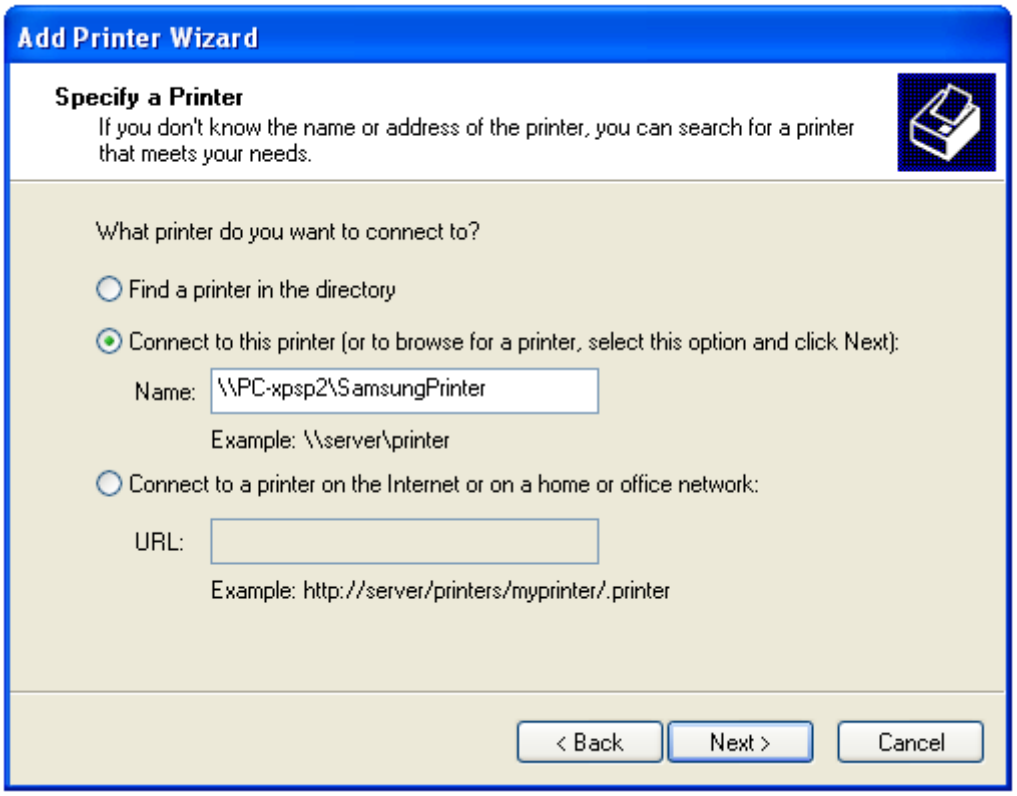
حالا اگر بخواهید از کامپیوتر خود به چاپگری دسترسی پیدا کنید که در شبکه Share شده است، باید به پنجره Printers and Faxes بروید و از ستون سمت چپ، Add a new printer را انتخاب کنید.



ویزاردی شروع به کار می‌کند که در یک مرحله از آن سؤال می‌شود که آیا چاپگر به کامپیوتر خودتان متصل است یا جزء چاپگرهای شبکه می‌باشد. شما باید گزینه مربوط به چاپگر شبکه را انتخاب و سپس Next را بزنید.



بعد در شبکه جستجو کنید و چاپگر مورد نظر را پیدا کنید. پس از نصب چاپگر، می‌توانید به چاپ اسناد خود بپردازید. درست مثل این که چاپگر به کامپیوتر خودتان متصل است.



۱۵-۸- به اشتراک گذاشتن اتصال اینترنت

یکی دیگر از منابعی که می‌توان با اشتراک گذاشت، اتصالات اینترنت می‌باشد. از آنجا که این بحث مفصل می‌باشد، آن را در یک فصل جداگانه قرار داده‌ایم. برای کسب اطلاعات بیشتر به فصل "*به اشتراک گذاشتن اتصال اینترنت*" مراجعه فرمایید.

۱۵-۹- اتصال یک درایو به پوشه Share شده (Map Network Drive)

فرض کنید که شما هر روز به پوشه‌ای نیاز دارید که این پوشه در کامپیوتری دیگر قرار دارد و برای دسترسی به آن نیاز دارید که از طریق Run ابتدا آدرس کامپیوتر مقصد را وارد کرده، سپس پوشه مورد نظر را پیدا کرده، وارد آن شده و از آن استفاده کنید. اما راه ساده تری نیز وجود دارد و آن اینکه در ویندوز این قابلیت وجود دارد که در My Computer یک درایو مجازی بسازید (مثل H:\)، سپس آن را به پوشه Share شده در شبکه Mount کنید، یعنی با بازکردن این درایو، محتویات پوشه Share شده را ببینید. بدین منظور ابتدا در کامپیوتر مقصد یک پوشه ساخته و آن را Share کنید.

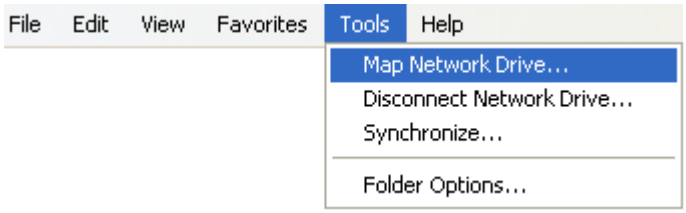

SharedFolder

سپس در این پوشه یک فایل متنی ایجاد کنید.

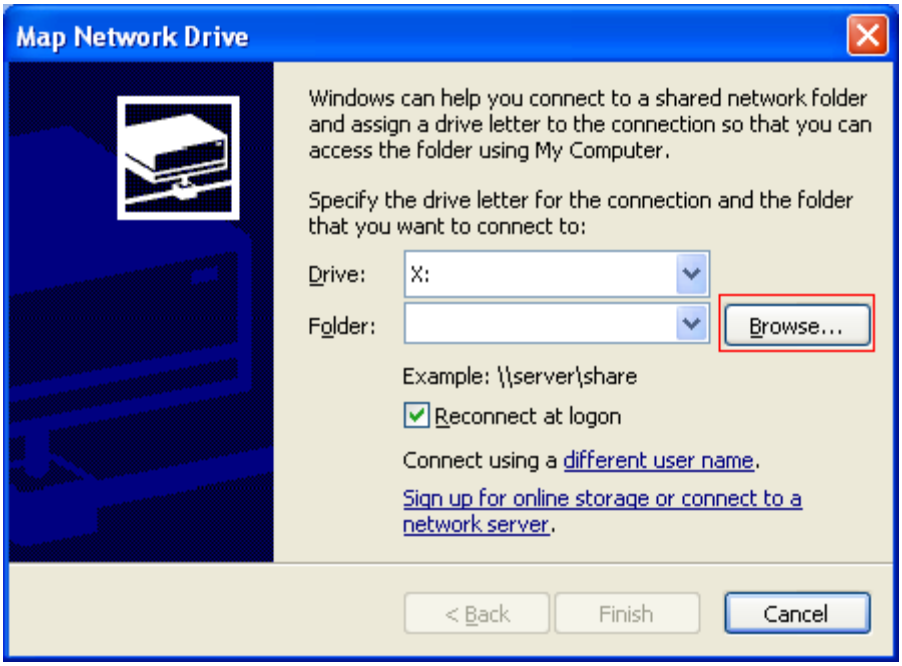

Information
Text Document
1 KB

حال به کامپیوتر خود رفته و از منوی Tools گزینه Map Network Drive را انتخاب کنید.

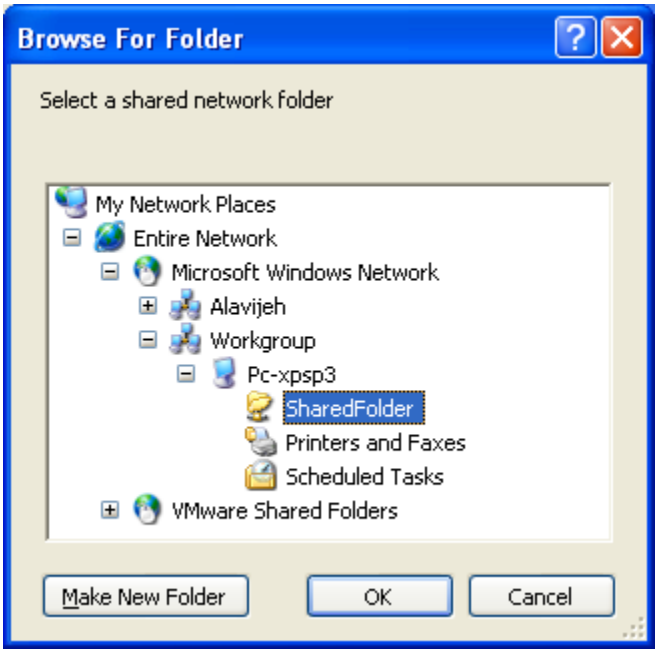
۱۵-۹- اتصال یک درایو به پوشه Share شده(Map Network Drive)



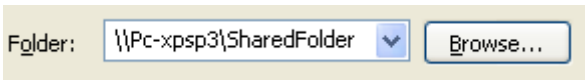
در صفحه باز شده، در قسمت Drive، مشخص کنید که درایو مجازی ساخته شده، با چه اسمی به نمایش درآید؟ (در این مثال X:\)، سپس در قسمت Folder، آدرس یا اسم کامپیوتر مقصد به اضافه نام پوشه Share شده را وارد نمایید. اما برای انتخاب پوشه Share شده به صورت تصویری، روی دکمه Browse کلیک کنید.



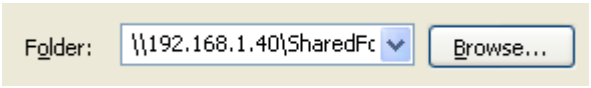
سپس در قسمت Microsoft Windows Network، ابتدا Workgroup مورد نظر، سپس کامپیوتر مورد نظر و سپس پوشه Share شده را انتخاب نمایید.



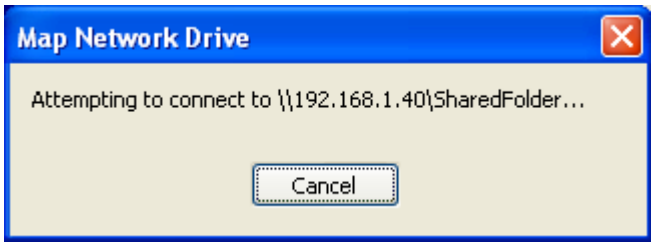
با این کار می‌بینید که آدرس مورد نظر در بخش Folder قرار می گیرد.



البته می‌توانید اسم کامپیوتر مقصد، آدرس IP آن را نیز وارد نمایید. توجه کنید که آدرس IP در مواقعی که سیستم‌ها آدرس IP خود را از DHCP Server می‌گیرند مناسب نیست.



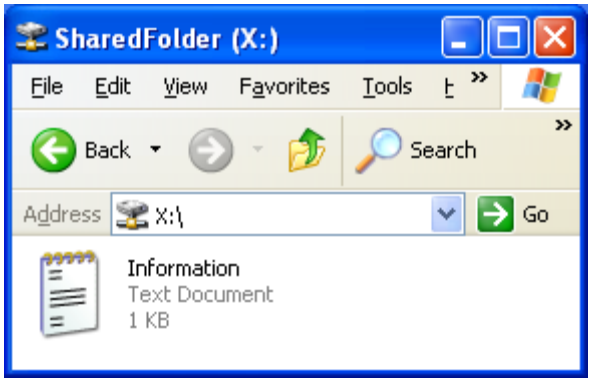
پس از OK کردن صبر کنید تا درایو مورد نظر ساخته شود.



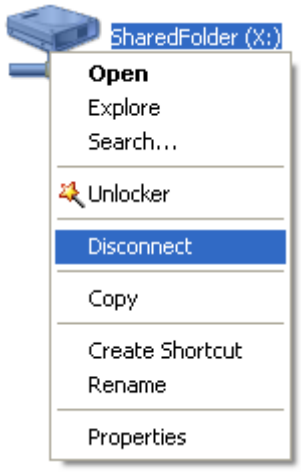
حال اگر وارد My Computer شوید، می‌بینید که درایو جدید X:\ ساخته شده است.



با بازکردن این درایو، محتویات پوشه Share شده را مشاهده خواهید نمود.



برای حذف این درایو از کامپیوتر خود، روی آن راست کلیک کرده و گزینه Disconnect را انتخاب نمایید.

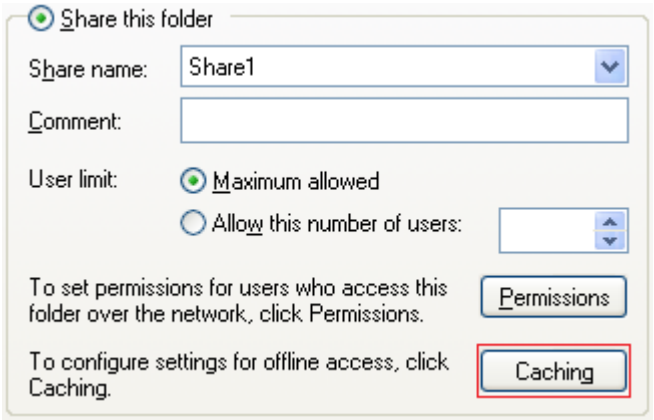


۱۵-۱۰- Caching در File Sharing

یکی از قابلیت‌های Sharing در ویندوز XP، استفاده از Caching است. Cache به معنای استفاده از یک داده، بدون دسترسی به منبع اصلی داده می‌باشد. مانند Cache کامپیوتر که به جای دسترسی به RAM، داده‌ها را از محلی به نام Cache می‌خواند. Cache در Sharing بدین معنا است که می‌توان به یک پوشه Share شده دسترسی داشت، بدون نیاز به اینکه کامپیوتر نگهدارنده آن پوشه روشن باشد.

۱۵-۱۰-۱- فعال سازی امکانات Caching

جهت استفاده از امکانات Caching، ابتدا بایستی هنگام Share کردن پوشه، بگویید که این پوشه قابلیت Cache شدن را داشته باشد. بدین منظور، هنگام Share کردن یک پوشه، در سربرگ Sharing گزینه Caching را انتخاب نمایید.

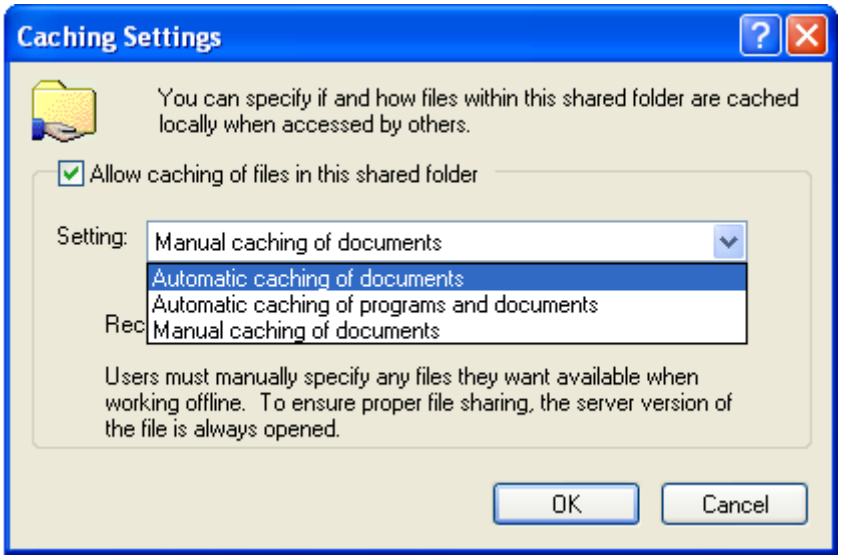


در صفحه باز شده، ابتدا گزینه Allow caching of files in this shared folder را تیک بزنید و سپس از لیست پایین، نوع Caching را انتخاب نمایید.

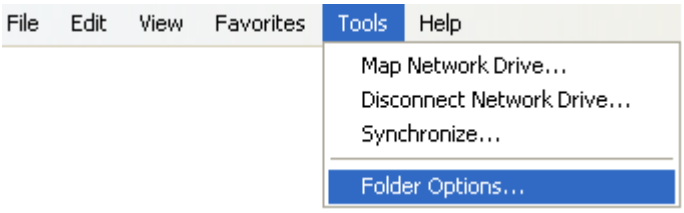
گزینه اول، Caching خودکار را فقط روی اسناد انجام می‌دهد.

گزینه دوم، Caching خودکار را روی تمامی فایل‌ها انجام می‌دهد.

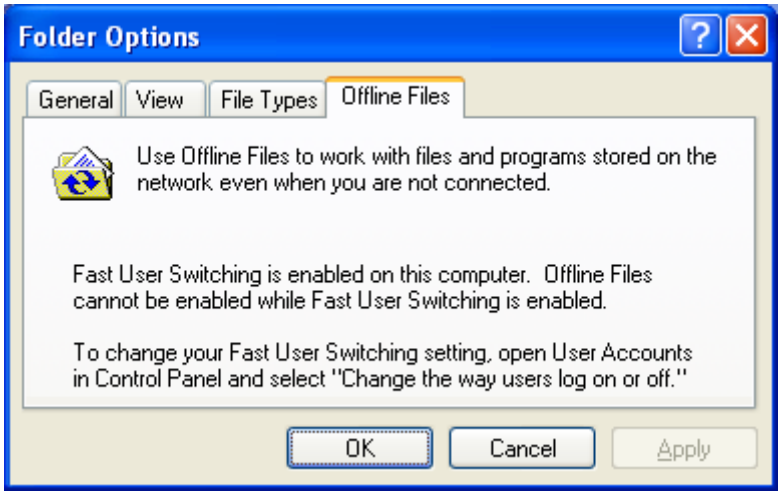
گزینه سوم، Caching را در زمانی انجام می‌دهد که کاربر به صورت دستی این کار را انجام دهد.



حال، Clientها (سیستم هایی که می‌خواهند از پوشه Share شده استفاده کنند) در صورتی می‌توانند از امکان Sharing استفاده کنند که سرویس مربوطه روی Client فعال باشد. برای این کار، در Client وارد My Computer شده و از منوی Tools گزینه Folder Option را انتخاب نمایید.



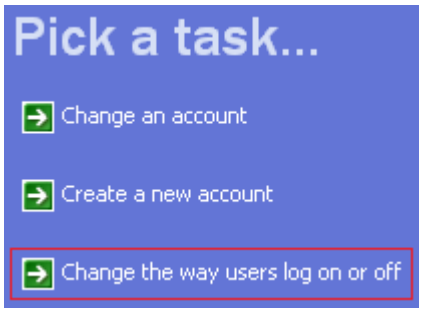
سپس وارد سربرگ Offline Files شوید. همانطور که در شکل زیر مشاهده می‌نمایید، سیستم می‌گوید که جهت فعال سازی قابلیت Caching، بایستی حالت Fast User Switching را غیر فعال نمایید. برای انجام اینکار بایستی وارد قسمت User Accounts شوید.



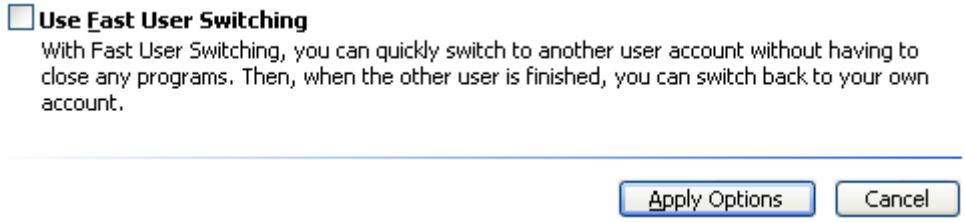
به منظور غیر فعال نمودن Fast User Switching، از Control Panel، وارد User Accounts شوید.



سپس در صفحه باز شده، روی Change the way users log on or off کلیک کنید.



سپس در صفحه باز شده، تیک گزینه Use Fast User Switching را بردارید و سپس روی Apply Options کلیک کنید.



پس از انجام این کار، مجددا از طریق Folder Option ➔ Tools مجددا وارد سربرگ Offline Files شوید. در این صفحه، تنظیمات زیر وجود دارد.

Enable Offline Files: سرویس Caching از فایل‌های Share شده را فعال می‌کند.

Synchronize all offline files when logging in: هنگام روشن شدن این کامپیوتر، عمل همزمانی را با دیگر کامپیوترها انجام می‌دهد.

Synchronize all offline files when logging off: مانند مورد فوق، با دو تفاوت. ۱- عمل همزمانی هنگام خروج از سیستم انجام می‌گیرد. ۲- هنگام خروج از سیستم، اگر قابلیت تغییر فایل را داشته باشیم و در فایل Share شده تغییری را اعمال کرده باشیم، این تغییر در سرور اعمال می‌شود.

Display a reminder every: بر اساس زمان تعیین شده، پیغامی را در مورد Offline Files به کاربر نشان می‌دهد.

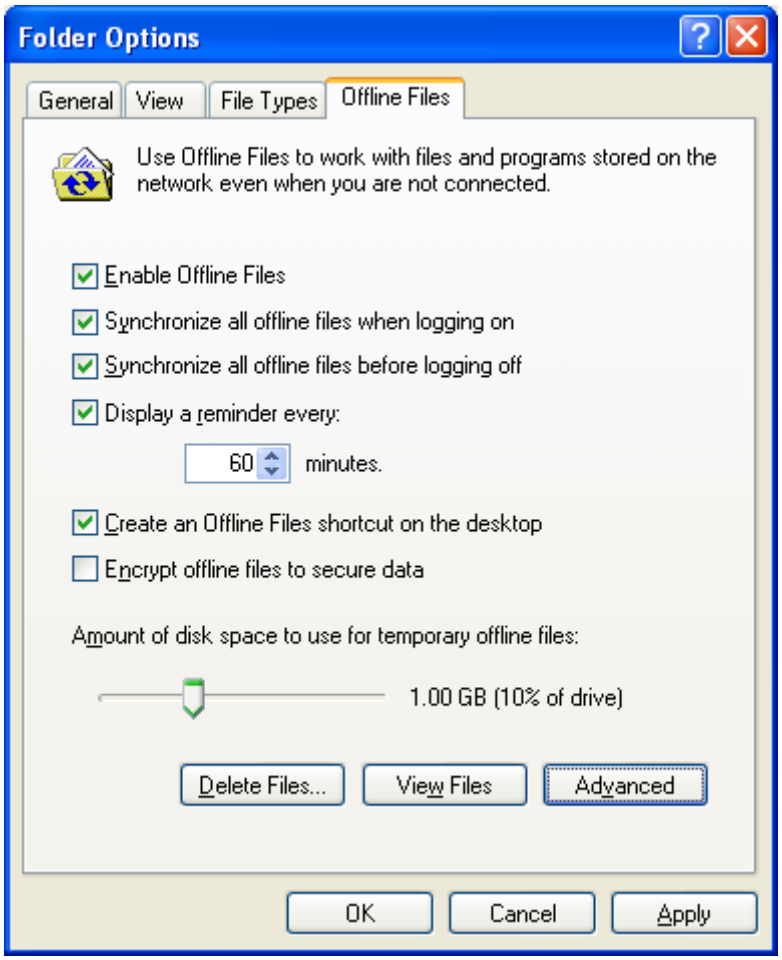
Create an Offline Files shortcut on the desktop: یک میانبر به پوشه‌های Cache شده ایجاد می‌کند که با باز کردن این میانبر می‌توان آن پوشه‌ها را مشاهده نمود.

Encrypt offline files to secure data: کد کردن فایل‌های کپی شده به منظور افزایش امنیت

Amount of disk space to use for temporary offline files: حداکثر مقدار فضا جهت کپی گرفتن از فایل‌های Share شده

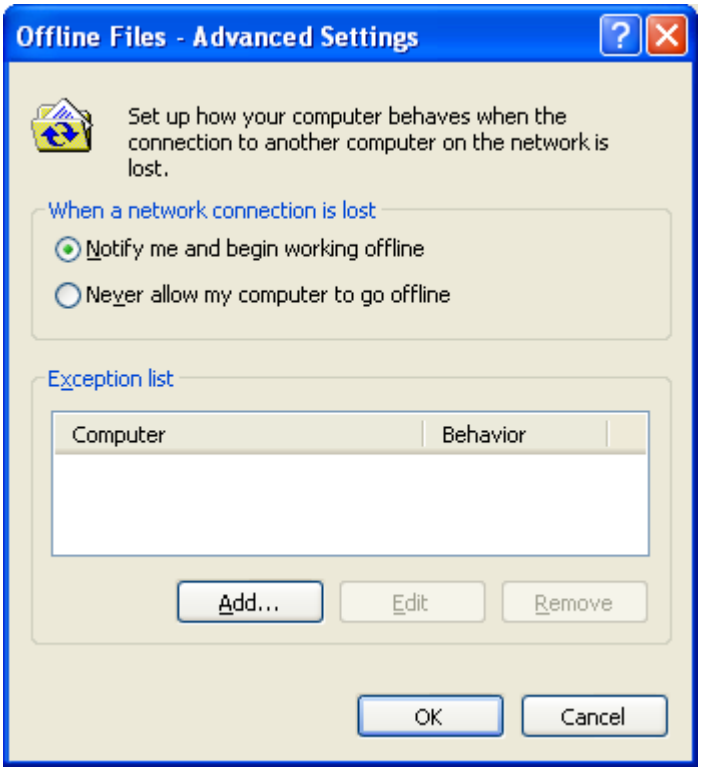
Delete Files: حذف فایل هایی که از دیگر کامپیوترها Cache شده و اکنون روی این کامپیوتر کپی شده است.

View Files: مشاهده فایل‌های کپی شده و Cache شده.

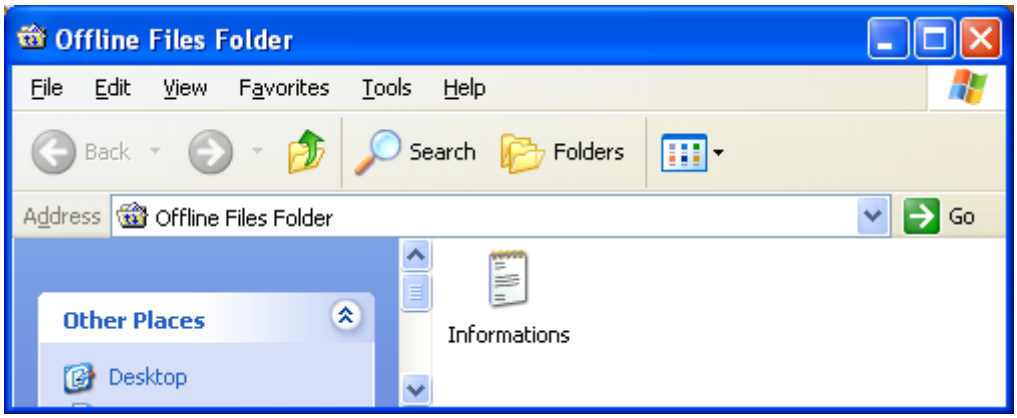


Advanced: انجام تنظیمات پیشرفته‌تر که با کلیک روی آن، صفحه زیر باز می‌شود. در این صفحه می‌توان کارهای زیر را انجام داد:

- نمایش پیغام هنگام شروع عملیات Offline و Caching
- عدم اجازه به کامپیوتر برای انجام عملیات Offline و Caching
- عدم کپی گیری از فایل‌های Share شده یک کامپیوتر راه دور خاص از طریق Exception list



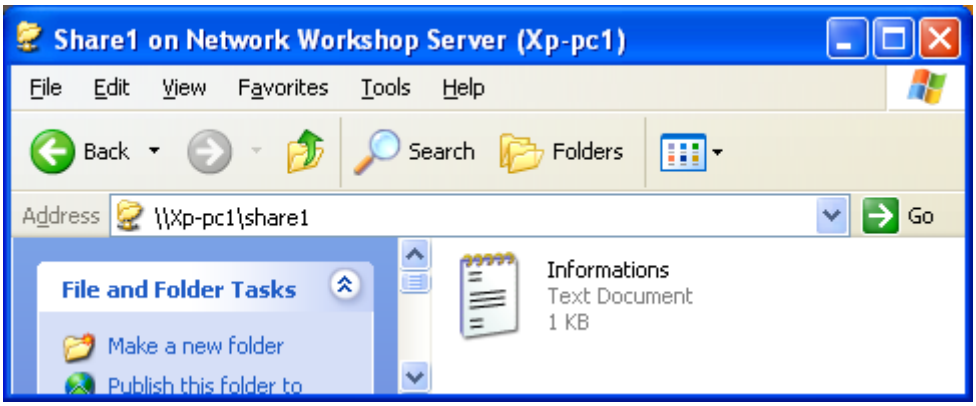
نکته: کپی یک فایل Share شده فقط زمانی به کامپیوتر شما منتقل می‌شود که شما آن را باز کرده باشید و به آن دسترسی پیدا نموده باشید. برای مثال من از طریق PC2 به پوشه Share شده که Share1 نام داشته و روی PC1 قرار دارد، دسترسی پیدا نموده و فایل Information.txt را باز نمودم. پس از باز نمودن این فایل، به دلیل فعال بودن قابلیت Offline، یک کپی از این فایل، به کامپیوتر من منتقل شد. اگر وارد بخش Offline Files که میانبر آن روی صفحه دسکتاپ قرار دارد وارد شوم، می‌توانم این فایل را ببینم.



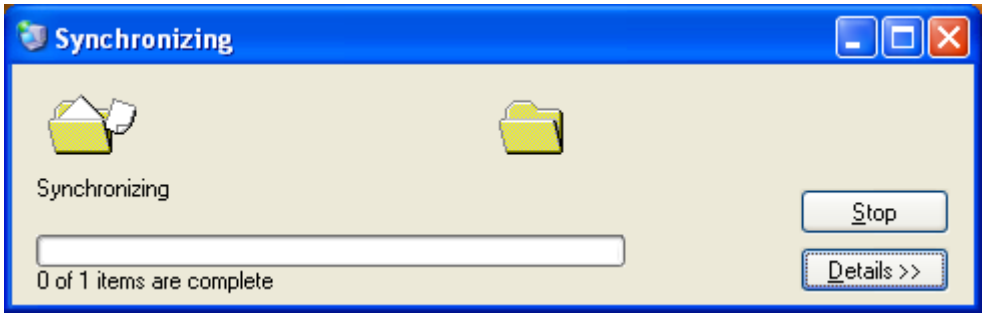
نکته جالب این است که اکنون حتی اگر اتصال من با شبکه قطع گردد، باز می‌توانم به فایل Share شده دسترسی پیدا کنم. همانطور که از شکل زیر پیداست، اتصال من با شبکه قطع است. آیکن آبی رنگ در شکل زیر، جهت امور Offline است که فرآیند همزمان سازی را به کمک آن و بدون نیاز به Log in یا Log off نمودن سیستم نیز می‌توان انجام داد.



اما از طریق My Network Places می‌توانم فایل Share شده را باز نمایم.



نکته جالب‌تر دیگر این است که می‌توانم این فایل را در صورتی که قابلیت تغییر فایل فعال شده را داشته باشیم، را تغییر نیز دهیم. فایل تغییر داده شده، به هنگام ایجاد اتصال با کامپیوتر اصلی نگهدارنده فایل و به کمک فرآیند همزمان سازی، جایگزین فایل اصلی می گردد. بسته به نوع تنظیمات، هنگام Log in یا Log off نمودن سیستم، عمل همزمانی انجام می گیرد.





البته اگر کامپیوتر راه دور دارای رمز عبور باشد، هنگام انجام عملیات همزمانی بایستی نام کاربری و رمز عبور وارد نمایید.

۱۵-۱۱- ساختار شبکه

تا اینجا مطالبی را که گفتیم مربوط به زمان بعد از انجام اتصالات فیزیکی یا به اصطلاح کابل کشی شبکه است. حالا ببینیم خود این کابل کشی به چه صورت می‌تواند انجام شود. همان طور که گفتیم، راه‌های مختلفی برای وصل کردن کامپیوترها به یکدیگر وجود دارد که آسان ترین و در دسترس ترین آن‌ها اترنت (Ethernet) است. لوازم و تجهیزات مورد نیاز برای ساخت یک شبکه اترنتی می‌تواند به سادگی اتصال دو کارت شبکه یا به پیچیدگی ارتباط چند روتر و سوئیچ باشد. و در واقع همین انعطاف پذیری این سیستم است که باعث شده شرکت‌های بزرگ و کوچک به سمت استفاده از آن بروند.

از مزایای سیستم شبکه بندی اترنت می‌توان به این موارد اشاره کرد:

۱. سریع ترین تکنولوژی شبکه بندی خانگی است (100 Mbps)
۲. اگر کامپیوترها فاصله زیادی از یکدیگر نداشته باشند، هزینه آن بسیار پایین است.
۳. قابل اطمینان است.
۴. نگهداری آن آسان است.

۵. تعداد دستگاه هایی که می‌توان به شبکه متصل نمود تقریباً نامحدود است.
۶. به لحاظ پشتیبانی و اطلاعات فنی بسیار فراگیر است.

برخی از نقاط منفی این تکنولوژی عبارتند از:

۱. برای وصل کردن بیشتر از دو کامپیوتر به یکدیگر، به تجهیزات اضافی نیاز است.
۲. در صورت نیاز به کابل کشی اضافی و نصب پریز، ممکن است هزینه‌ها بالا برود.
۳. راه اندازی و تنظیمات اولیه آن می‌تواند دشوار باشد.
۴. اصطلاحات فنی و تعداد انتخاب‌ها می‌تواند گمراه کننده باشد.

۱۵-۱۲- تجهیزات مورد نیاز

اترنت با سرعت 10 Mbps، 100 Mbps و 1000 Mbps موجود است و بیشتر کارت‌های شبکه می‌توانند با هر ۳ سرعت کار کنند، اما امروزه دلیلی ندارد از کارت‌های 10 Mbps استفاده کنید. و در بسیاری از مواقع تقریباً پیدا کردن کارت‌های 10 Mbps غیرممکن است. برای وصل کردن کارت‌های شبکه نیز دو نوع کابل وجود دارد که عبارتند از کابل هم محور (Coaxial) و کابل زوج به هم تابیده (UTP) که اولی تقریباً منسوخ شده و امروزه از UTP در انواع Cat5e، Cat5 و Cat6 استفاده می‌شود. (کاربرد کابل‌های Coaxial بیشتر در کابل‌های آنتن تلویزیون و یا شبکه‌های BUS است). کابل UTP کابلی است متشکل از ۸ سیم باریک دو به دو به هم تابیده، شبیه به سیم تلفن است. به دو سر این سیم کانکتور یا Jack می‌زنند که به RJ-45 معروف است. یک سر این سیم به کارت شبکه کامپیوتر و سر دیگر آن به دستگاهی دیگر وصل می‌شود؛ مثل سوئیچ، هاب یا کامپیوتر.

تمام کامپیوترهای موجود در یک شبکه، از طریق کابل‌های UTP به سوئیچ متصل هستند و سوئیچ جای تک تک کامپیوترها را می‌داند. بنابراین وقتی کامپیوتری اطلاعاتی را برای کامپیوتر دیگر ارسال می‌کند، این ارسال در واقع به واسطه سوئیچ تبادل می‌شود. یعنی سوئیچ اطلاعات را از کامپیوتر مبدا می‌گیرد و به کامپیوتر مقصد تحویل می‌دهد. سوئیچ‌ها اندازه‌های مختلفی دارند و این اندازه از روی تعداد پورت شان (یعنی تعداد کامپیوتری که می‌توان به آن‌ها وصل کرد) مشخص می‌شود. سوئیچ‌های ۴ پورتی، ۸ پورتی، ۱۶ پورتی، ۲۴ پورتی و بالاتر در بازار موجود می‌باشند. برای یک شبکه کوچک خانگی، معمولاً یک سوئیچ ۸ پورتی یا احتمالا ۱۶ پورتی کافی است.

اگر دوست ندارید سیم‌های شبکه کف اتاق را بپوشانند، می‌توانید سیم‌ها را از کانال هایی عبور دهید موسوم به Duct که روی دیوار نصب می‌شوند. سیم‌ها داخل داکت قرار می‌گیرند و در محل استقرار کامپیوتر، از داکت بیرون می‌آیند و به کارت شبکه کامپیوتر متصل می‌شوند. اگر بخواهید کار را از این هم تمیزتر انجام دهید، می‌توانید روی دیوار، پریزهای مخصوص شبکه (موسوم به Key Stone) را نصب کنید و با کابل‌های آماده (موسوم به Patch Cord)، کارت شبکه را به پریز متصل نمایید. بد نیست بدانید که برای وصل کردن فقط دو کامپیوتر به یکدیگر، نیازی به سوئیچ نیست و کافی است از طریق یک کابل UTP مخصوص، موسوم به Cross Over مستقیماً کارت شبکه دو کامپیوتر را به هم وصل کنید.

جدول زیر انواع کابل‌های UTP را نشان می‌دهد:

موارد استفاده	سرعت انتقال اطلاعات	گروه
سیستم‌های قدیمی تلفن، ISDN و مودم	حداکثر تا یک مگابیت در ثانیه	CAT1
شبکه‌های Token Ring	حداکثر تا چهار مگابیت در ثانیه	CAT2
شبکه‌های Token ring و 10 BASE-T	حداکثر تا ده مگابیت در ثانیه	CAT3
شبکه‌های Token Ring	حداکثر تا شانزده مگابیت در ثانیه	CAT4
اترنت (۱۰ مگابیت در ثانیه)، اترنت سریع (۱۰۰ مگابیت در ثانیه) و شبکه‌های Token Ring (16 مگابیت در ثانیه)	حداکثر تا یکصد مگابیت در ثانیه	CAT5
شبکه‌های Gigabit Ethernet	حداکثر تا یک هزار مگابیت در ثانیه	CAT5e

توجه نمایید که اگر برای راه اندازی شبکه خود از سوئیچ (نوع پیشرفته مدیریتی) استفاده نمایید، احتمالا نیاز به پیکربندی آن دارید. اما هاب هیچ تنظیم و مدیریتی نیاز ندارد. فقط کافی است کابل‌های شبکه را از یک طرف به هاب و از طرف دیگر به کارت شبکه وصل کرده و سپس هاب را روشن نمایید تا چراغ سبز رنگ روی کارت شبکه و چراغ متناظر با پورت مربوطه روی هاب روشن شود.

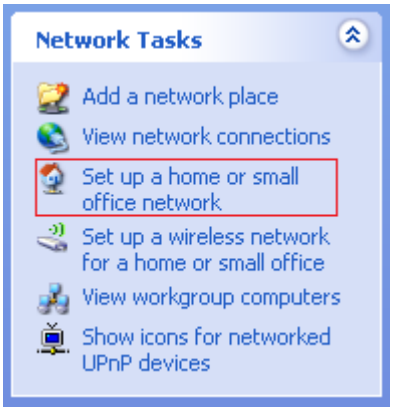
۱۵-۱۳- راه اندازی شبکه Workgroup جدید در ویندوز XP

در این قسمت، به آموزش این مبحث می‌پردازیم که چگونه ویندوز XP را جهت اتصال به یک Workgroup آماده سازیم. ممکن است این سوال برای شما مطرح شود که چرا این مبحث را در انتهای این فصل آورده‌ایم. موضوعی که مطرح است، این می‌باشد که ویندوز XP، به صورت خودکار، شبکه‌های محلی را می‌شناسد و به آن متصل می‌شود. اما گاهی مشکلاتی به وجود آمده و دیگر ویندوز XP قادر به متصل شدن به شبکه محلی نخواهد بود و بایستی تنظیمات آن را از ابتدا انجام دهیم. (به همین دلیل افراد حرفه‌ای رابطه خوبی با محصولات مایکروسافت نداشته و این شرکت را عوام فریب می‌نامند). شما نیز در صورتی که موفق به راه اندازی شبکه محلی خود نشدید، مراحل زیر را دنبال نمایید.

ابتدا وارد My Computer شده و سپس My Network Places را انتخاب نمایید.



سپس در این پنجره گزینه Set up a home or small office network را انتخاب نمایید.



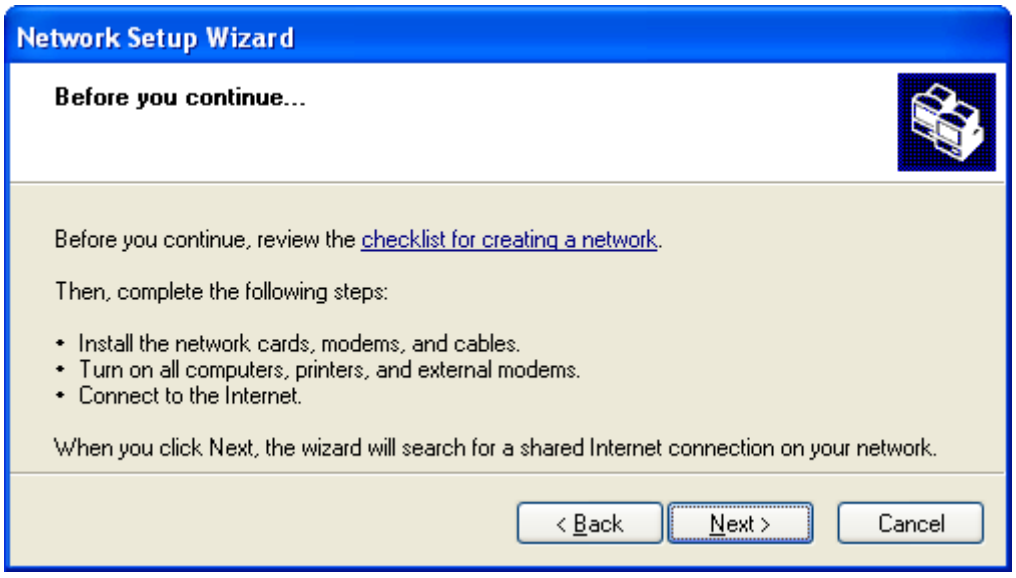
البته راه دیگر برای دسترسی به این قسمت این است که ابتدا وارد Control Panel شده و سپس گزینه Network Setup Wizard را انتخاب نمایید.



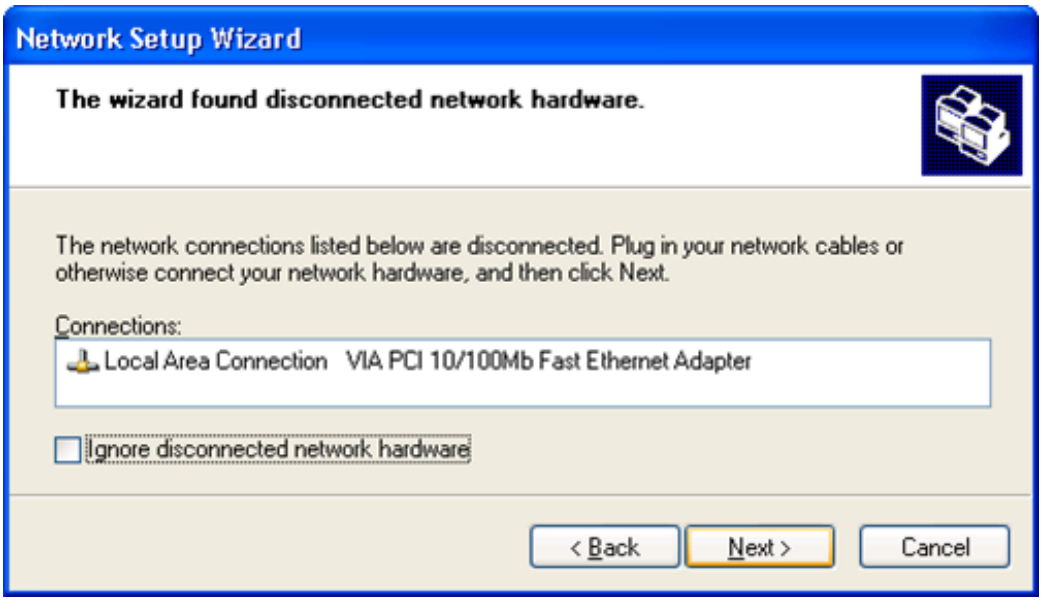
در صفحه خوش آمد گویی، Next بزنید:



صفحه بعدی، می‌گوید که قبل از نصب، تمامی کامپیوترها و دستگاه‌های جانبی را روشن نموده و همچنین به اینترنت متصل شوید. البته اگر به اینترنت متصل نشوید، باز هم می‌توان کار را ادامه داد.

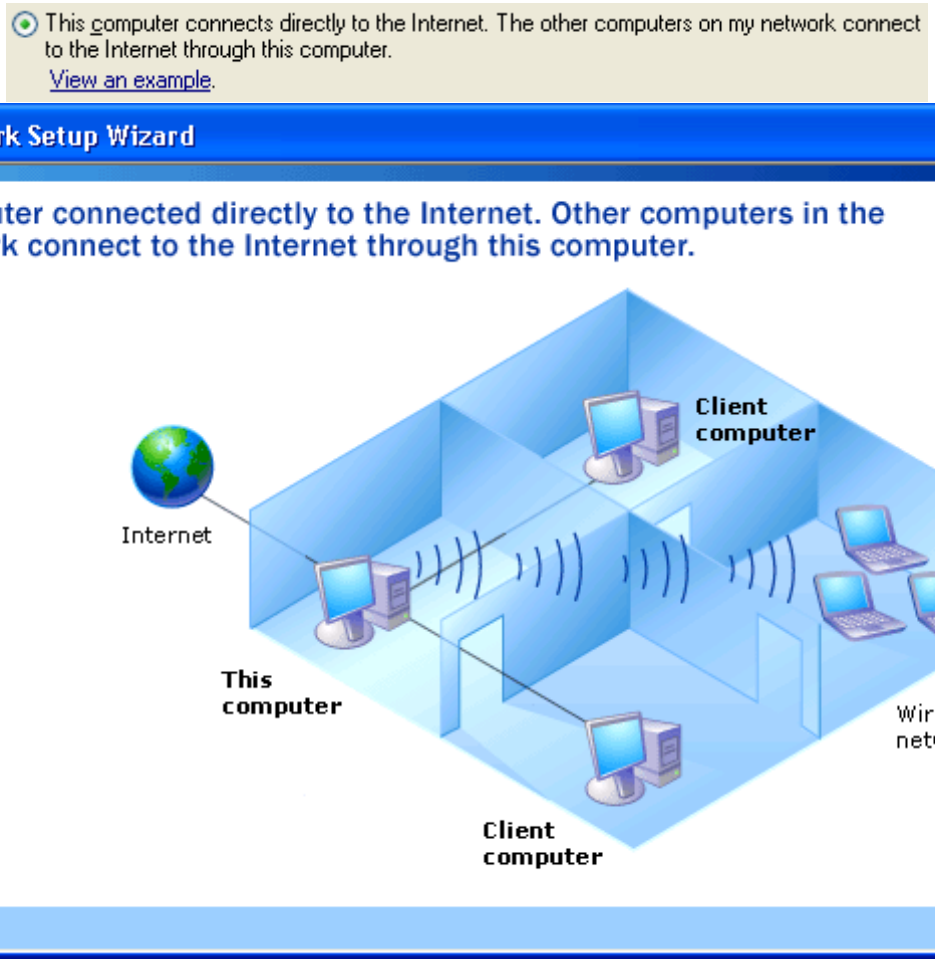


در صفحه باز شده مجددا Next بزنید. در صورتی که سیستم به شما پیام خطا داد، گزینه Ignore disconnected network hardware را فعال نموده و سپس Next بزنید.



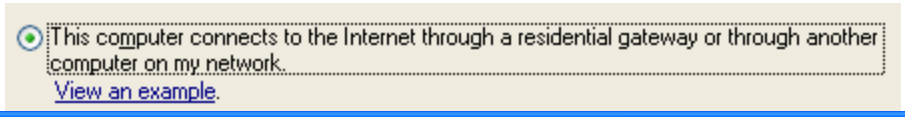
سپس در صفحه بعد بایستی نوع شبکه داخلی خود را انتخاب کنید. شما ۵ راه دارید، ۲ راه اول را در پنجره باز شده و ۳ راه دیگر را در پنجره بعد از صفحه بعد می‌توانید ببینید. در کنار هر حالت، گزینه‌ای تحت عنوان View an example وجود دارد که با انتخاب آن، مثالی مربوط به آن نوع شبکه را مشاهده خواهید کرد. در ادامه ما این ۵ حالت را به تصویر می‌کشیم:

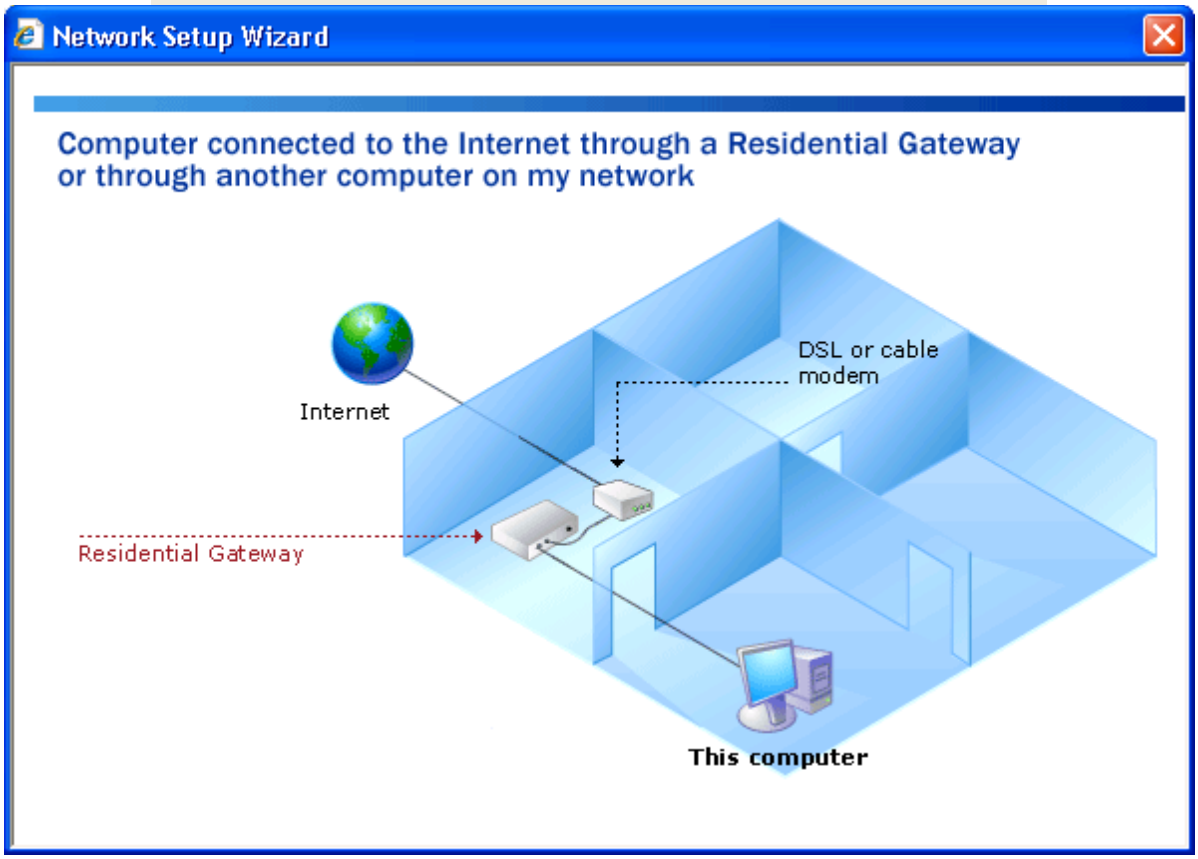
حالت اول



اتصال کامپیوتر شما به اینترنت و سپس به اشتراک گذاری اینترنت

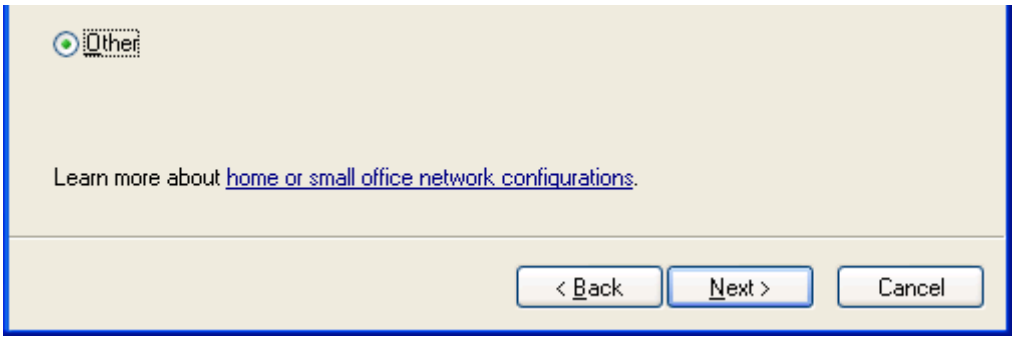
حالت دوم





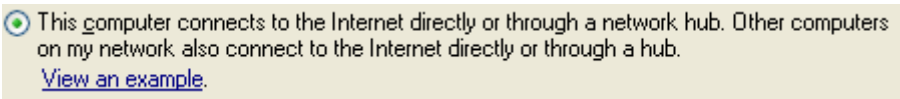
اتصال کامپیوتر شما به یک Gateway و دریافت اینترنت از آن

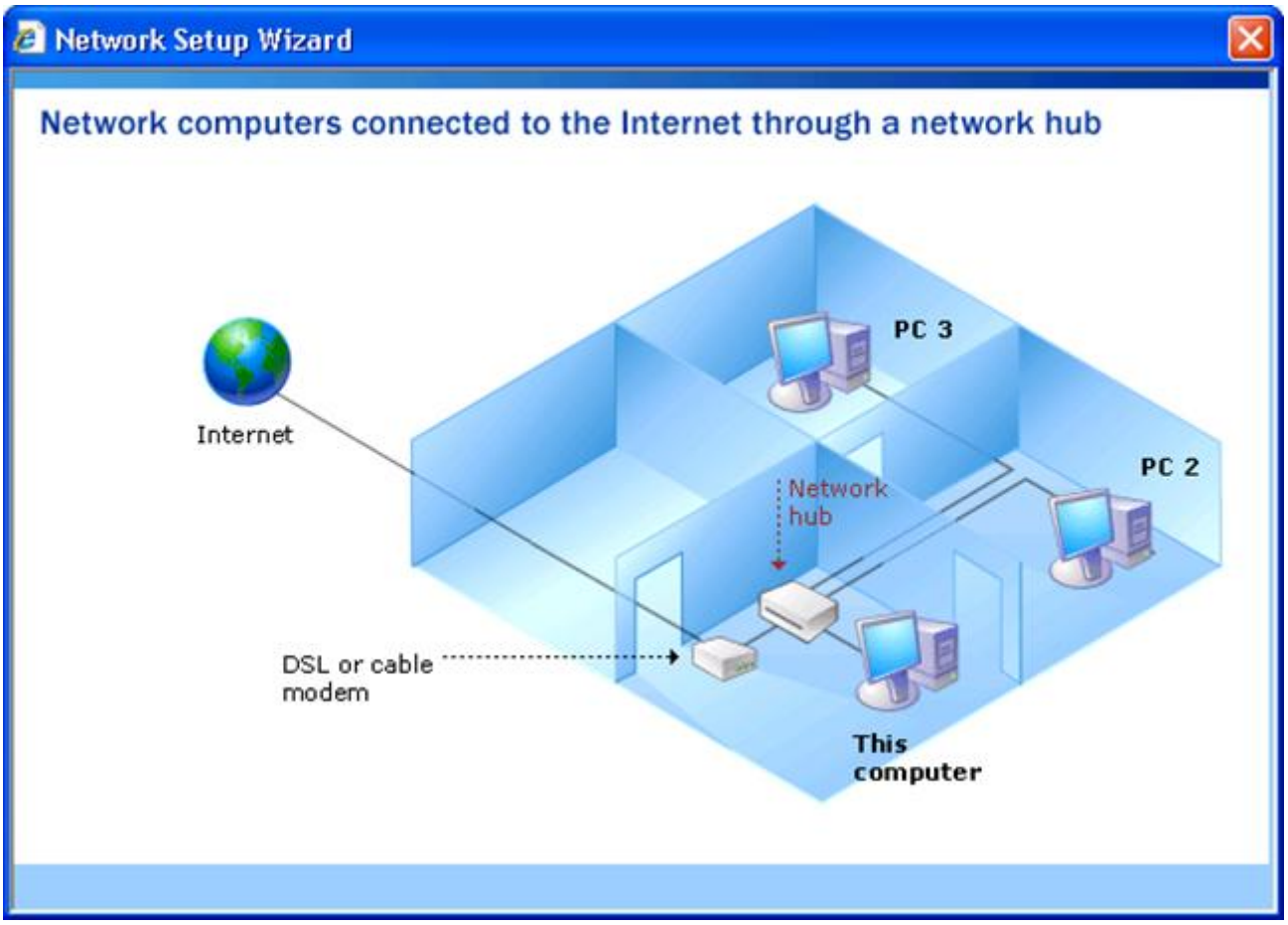
در صورتی که هیچ کدام از این دو حالت مد نظر شما نبود، گزینه Other را انتخاب کرده و به مرحله بعد بروید:



در صفحه باز شده، ۳ حالت دیگر برای انتخاب دارید.

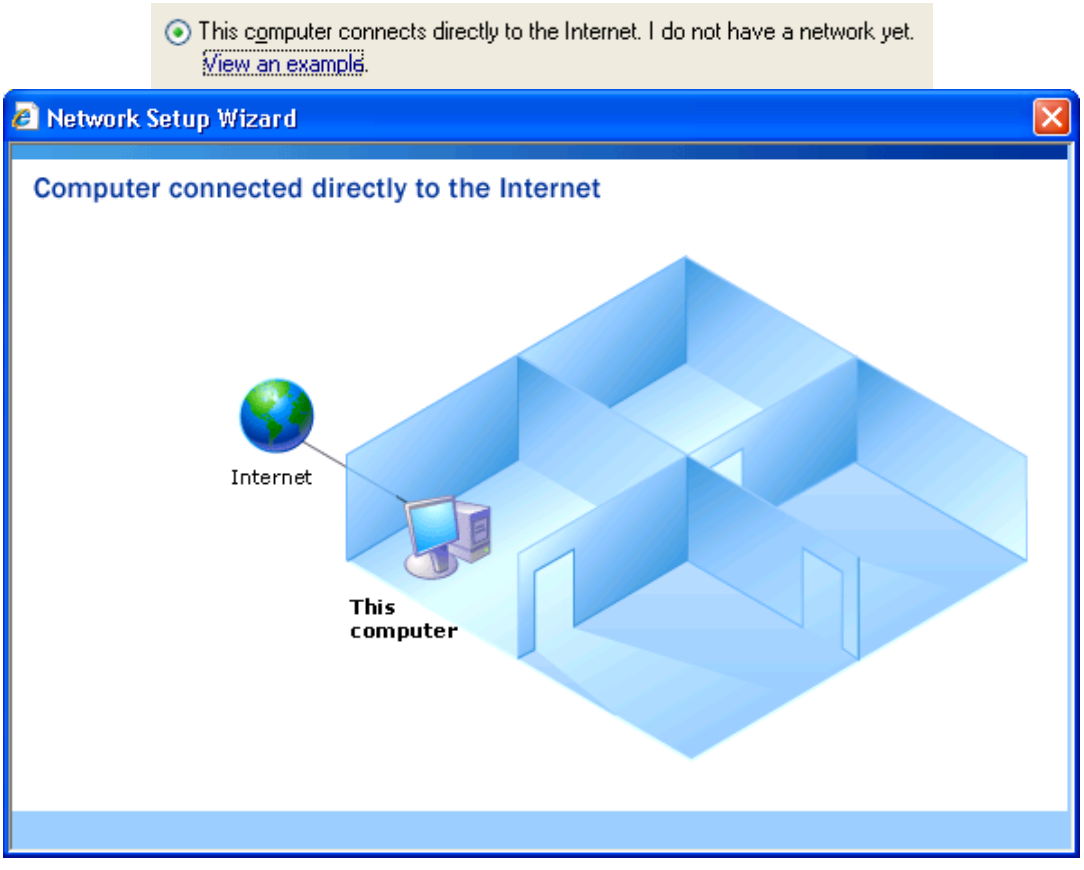
حالت سوم





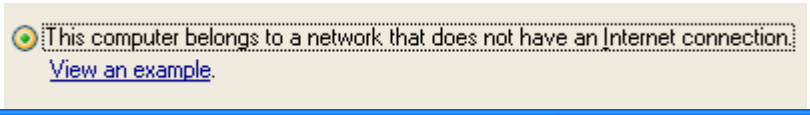
کامپیوترها به کمک یک Hub به یکدیگر متصل شده و خود Hub نیز به اینترنت وصل است

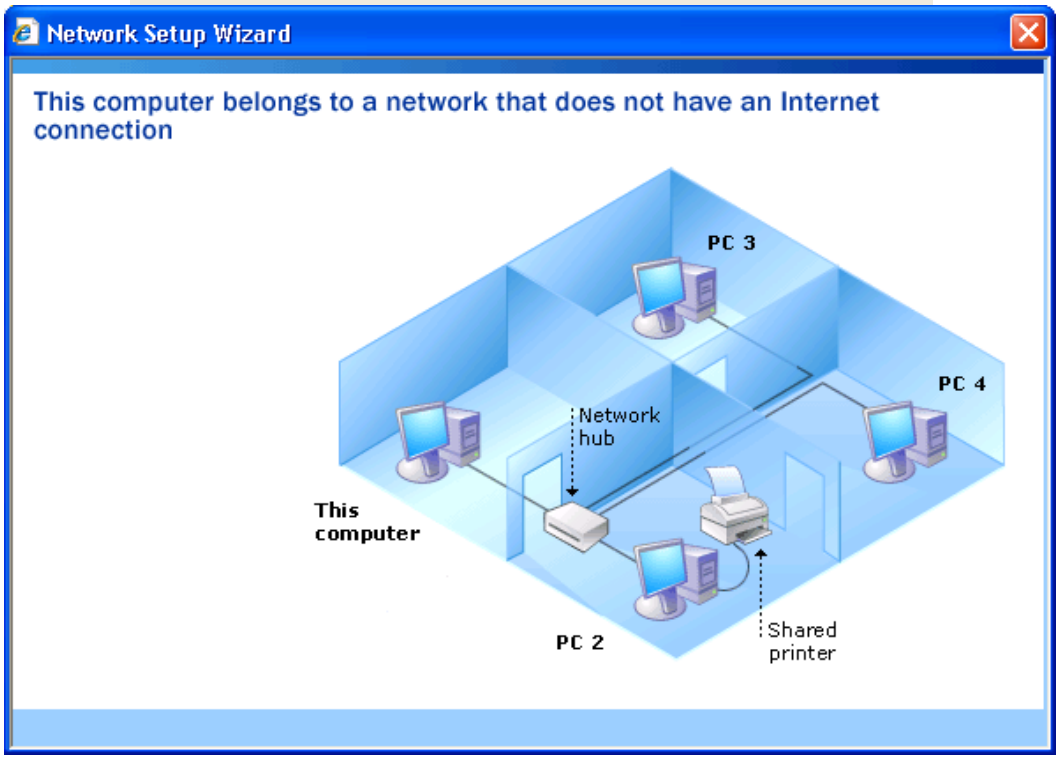
حالت چهارم



اتصال کامپیوتر خودتان به صورت مستقیم به اینترنت

حالت پنجم

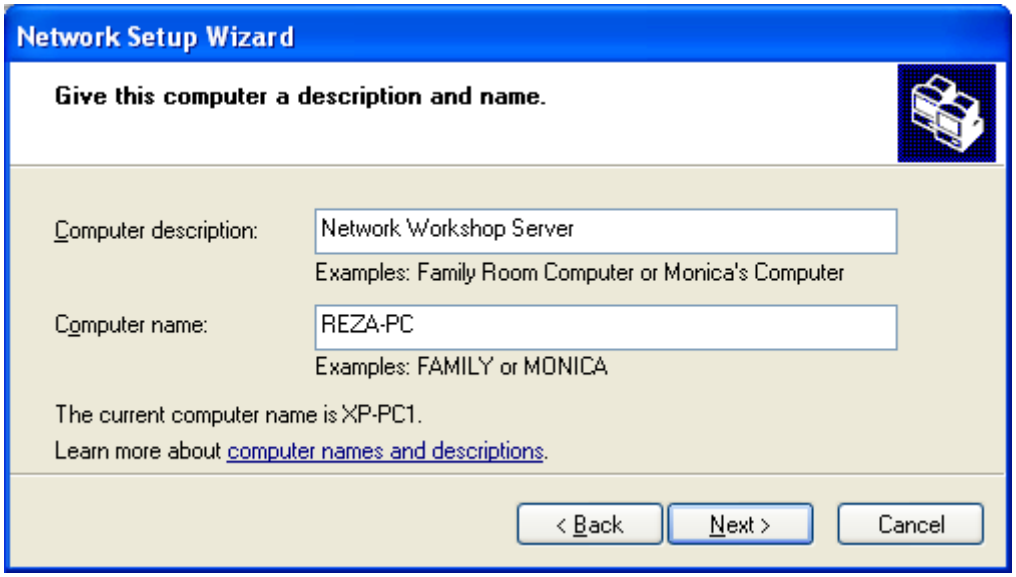




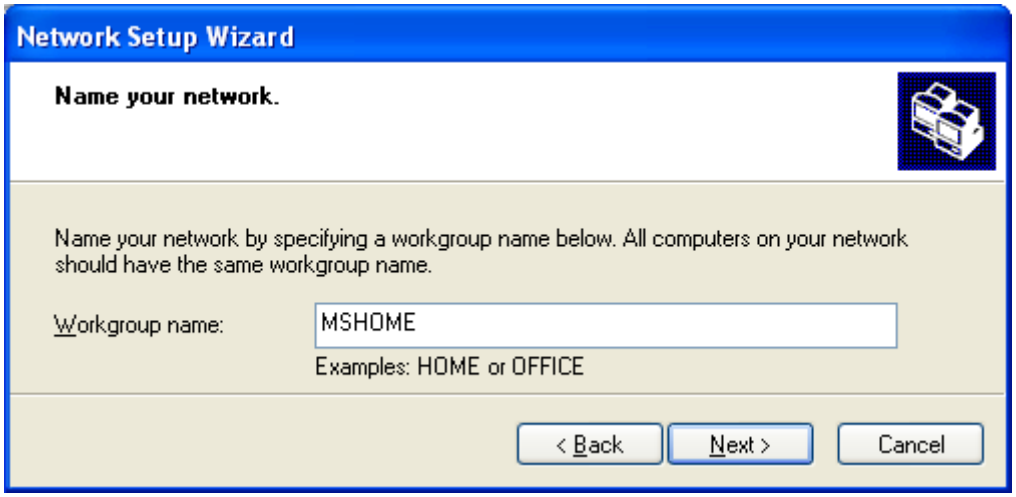
شبکه کردن کامپیوترها به صورت ساده

توجه فرمایید که این حالت پنجم از همه حالت‌ها رایج‌تر است و در شبکه‌های محلی استفاده می‌شود. لذا ما نیز همین حالت را انتخاب می‌کنیم.

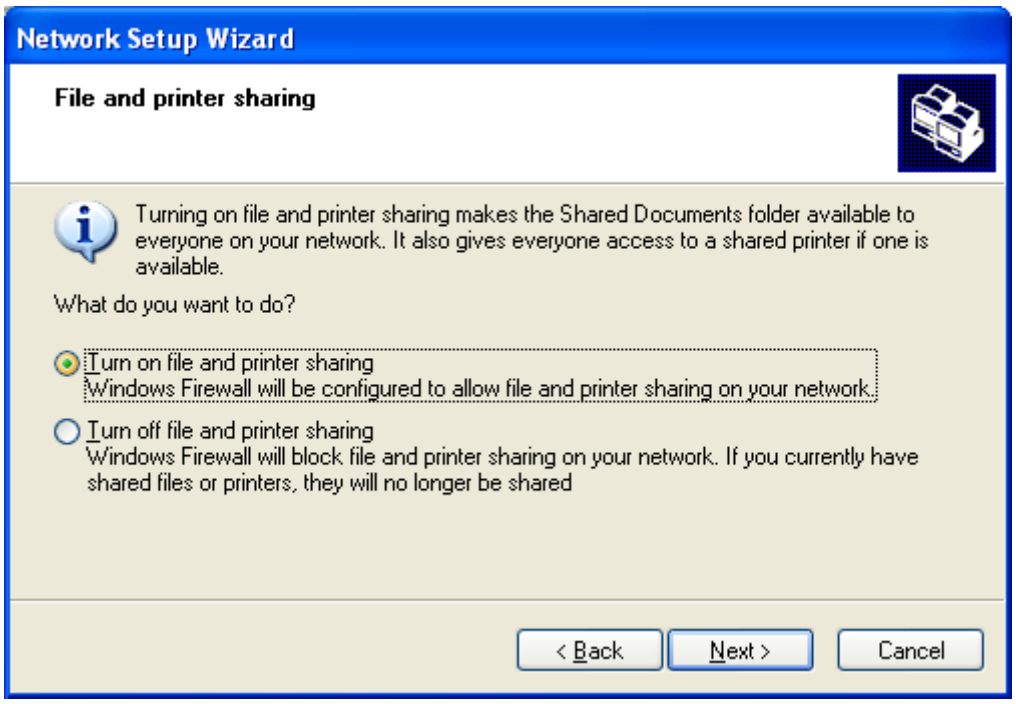
در صفحه بعدی، نام کامپیوتر در شبکه و توصیفی از آن را می‌نویسیم:



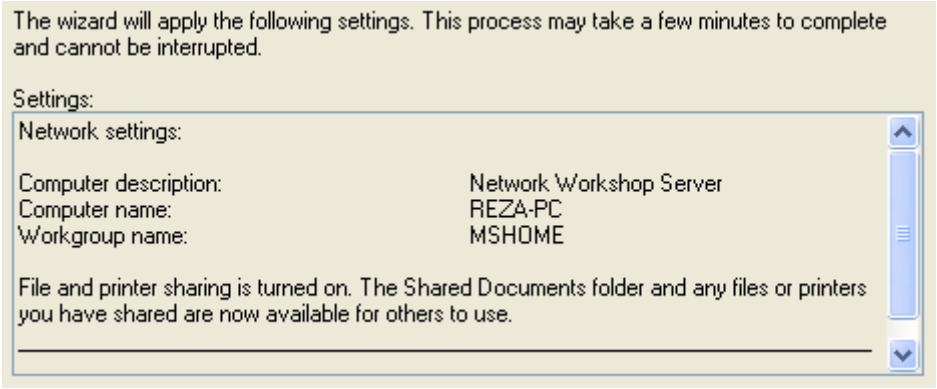
در صفحه بعدی، نام گروه کاری که کامپیوتر در آن قرار خواهد گرفت را وارد نمایید. گروه‌های کاری یک تقسیم بندی منطقی از شبکه است. مثلاً می‌توان یک گروه کاری برای پسران و یک گروه کاری برای دختران ایجاد نمود که **البته گروه کاری پسران ارجحیت خواهد داشت! بعله!**



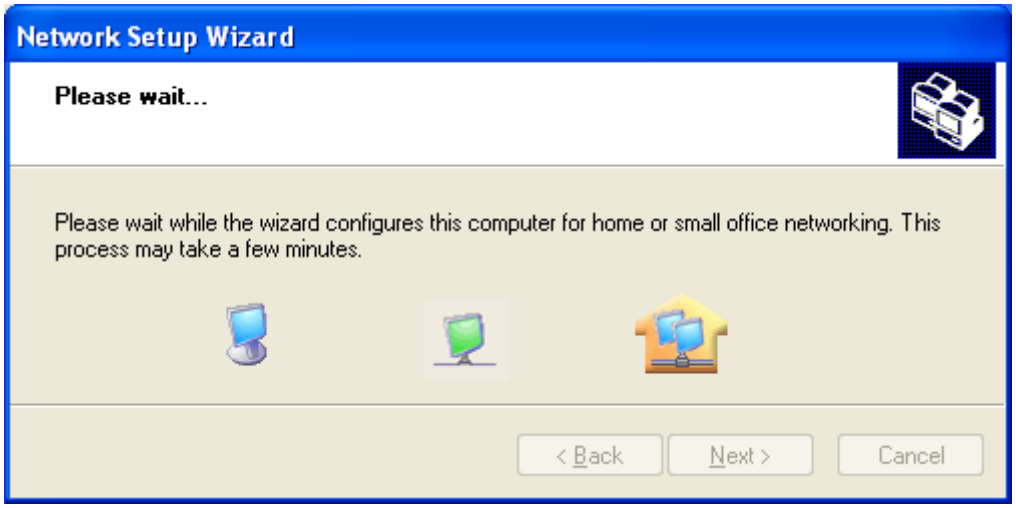
در صفحه بعد می‌توان تنظیم نمود که قابلیت اشتراک گذاری فایل و چاپگر فعال باشد یا نباشد که در شکل زیر آن را فعال کرده‌ایم.



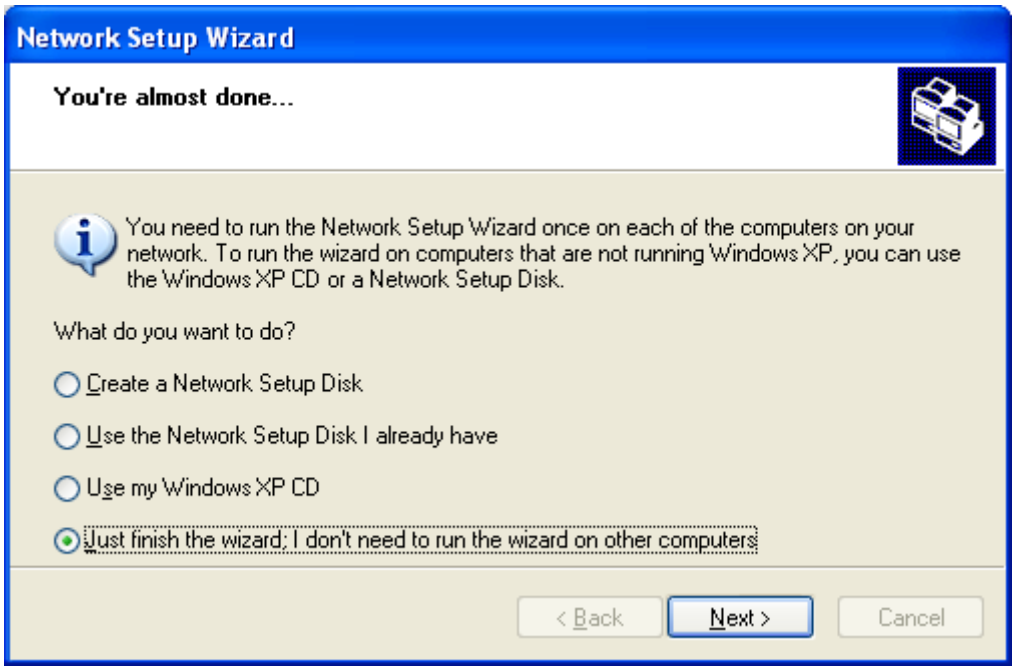
در مرحله بعد، خلاصه‌ای از تنظیمات انجام شده را مشاهده می‌کنید. برای رفتن به مرحله بعد Next بزنید:



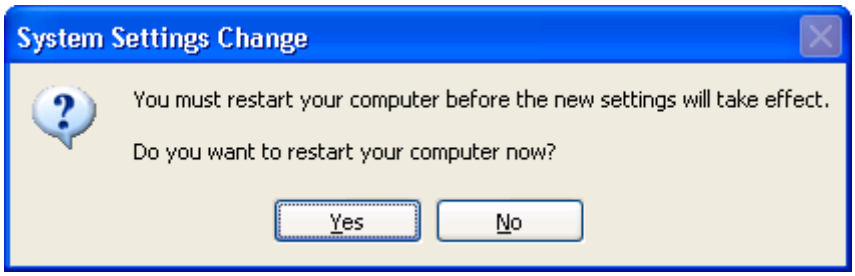
سپس سیستم شروع به راه اندازی شبکه خانگی یا محلی شما می کند.



در صفحه بعد، سیستم به شما اخطار می کند که روی دیگر کامپیوترهای موجود در شبکه نیز بایستی همین مراحل را انجام دهید؛ همچنین اخطار می‌دهد که اگر سیستم عامل آن‌ها ویندوز نباشد، به مشکل بر می‌خورید. گزینه آخر را انتخاب نمایید.



برای پایان نصب، Finish را بزنید. در نهایت سیستم خود را Restart نمایید.



حال در دیگر کامپیوترها می‌توانید این مراحل را انجام داده و به گروه کاری ساخته شده دسترسی پیدا کنید.

فصل ۱۶

به اشتراک گذاشتن اتصال اینترنت

۱۶-۱- مقدمه

همیشه به اشتراک گذاری اینترنت، یکی از دغدغه‌های راه اندازی شبکه بوده است. در گذشته نه چندان دور، سازمان‌های بزرگ یا اداره‌ها و شرکت‌ها، برای صرفه جویی در هزینه‌های اینترنت، آن را بین تمام کلاینت هایشان به اشتراک (Share) می‌گذاشتند. اینترنت یکی از منابعی است که می‌تواند در شبکه داخلی به صورت فردی یا گروهی مورد استفاده قرارگیرد لذا قابلیت به اشتراک گذاشتن این منبع بایستی وجود داشته باشد.

با گذشت زمان و با راه پیدا کردن شبکه‌ها به خانه‌های کاربران، یا به عبارتی خانگی شدن شبکه‌های کامپیوتری، کاربران عادی نیز به فکر اشتراک گذاری اینترنت بین سیستم‌های مختلف خود افتادند. اما این اقدام کمی برای یک کاربر آماتور و نا آشنا به شبکه کمی دشوار بوده و همواره نیاز بود تا متخصصان با قیمت‌های زیاد، آن را پیاده سازی کنند.

شرکت مایکروسافت در سیستم عامل‌های جدید خود امکانی را تحت عنوان ICS (Internet Connection Sharing)، به کاربران معرفی کرد تا به سادگی و بدون نیاز به هیچ دانش قبلی، و حتی متخصص این زمینه، بتوانند اینترنت خود را برای دستگاه‌های دیگر خود به اشتراک بگذارند.

اما همیشه سوالی بین کاربران وجود داشته که، بین چه دستگاه هایی می‌توان اینترنت را به اشتراک گذاشت.

به صورت کلی کامپیوترهای دسکتاپ، لبتاپ‌ها، Packet PC، PDA و... و هر چیزی که بتوان بر روی آن سیستم عامل نصب کنند، قادر خواهند بود از اینترنت Share شده استفاده نمایند. اما سیستم‌های دسکتاپ و لبتاپ بهترین گزینه به عنوان اشتراک گذارندهها هستند. اشتراک گذاشتن آن ممکن است به وسیله‌ی دستگاه اکسس پوینت یا از طریق یک رایانه شخصی که مجهز به کارت شبکه باشد انجام شود. اینترنت را می‌توان به صورت سیمی (موسم به LAN) یا به صورت بی‌سیم (موسوم به WiFi) بین دو یا چند کامپیوتر به اشتراک گذاشت.

۱۶-۲- روش‌های به اشتراک گذاری اینترنت

اینترنت را به دو روش متداول می‌توان اشتراک گذاشت:

۱. وب پروکسی (Web Proxy)
۲. مترجم آدرس شبکه یا NAT

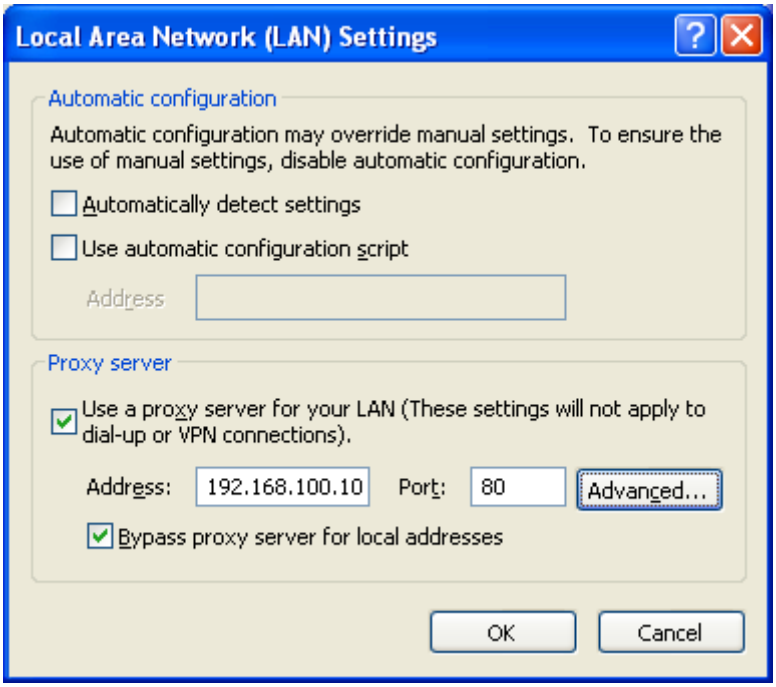
در ادامه به معرفی هر یک از روش‌های فوق می‌پردازیم.

۱۶-۳- وب پروکسی (Web Proxy)

در این روش یک نرم‌افزار به عنوان Proxy Server روی رایانه‌ای که به اینترنت متصل است، نصب می‌کنند و سپس سایر رایانه هایی که در شبکه می‌خواهند از اینترنت استفاده کنند، کلیه نرم‌افزارهای اینترنتی مانند Internet Explorer، Messenger، Opera، DAP، IDM و... در بخش Proxy خود بایستی آدرس **پروکسی سرور** و **پورت** را تنظیم کنند. با این کار کلیه درخواست‌های اینترنتی این رایانه‌ها از طریق آدرس و پورت تنظیم شده به رایانه اصلی (Proxy Server) و سپس از طریق آن به اینترنت ارسال شده و پاسخ آن‌ها نیز به همین روش دریافت می‌شود. ارتباط کاربران شبکه از طریق **لایه Application** انجام می‌شود. برای مثال، برای تنظیم Proxy Server در Internet Explorer، وارد قسمت زیر شوید:

Tools➔Internet Options ➔ Connection ➔ LAN Setting ➔ Proxy Server

حال از طریق این صفحه می‌توانید آدرس و پورت Proxy Server را وارد نمایید. در شکل زیر، آدرس Proxy Server برابر با ۱۹۲.۱۶۸.۱۰۰.۱۰ و شماره پورت برابر با ۸۰ می‌باشد.



۱۶-۳-۱- مزایای روش وب پروکسی

الف) اعتبار سنجی (Authentication): اعتبار سنجی به این معنی است که می‌توان برای کاربرانی که می‌خواهند از اینترنت در شبکه استفاده کنند، نام کاربری و کلمه عبور تعریف کرد و میزان دسترسی آن‌ها به اینترنت را محدود کرد.

ب) ثبت عملکرد کاربر (User Log): با این امکان می‌توان از کارکرد کاربران شبکه گزارش تهیه کرد. این گزارش شامل سایت هایی که کاربر دیده است، نوع استفاده از اینترنت از لحاظ سرویس‌های شبکه مانند FTP، Http، Chat و... و نیز حجم یا ترافیک استفاده از شبکه برای دانلود یا آپلود اطلاعات می‌باشد.

ج) دیوار آتشین شخصی (Personal Firewall): از طریق این گزینه می‌توان از نفوذ و دسترسی کاربران سایر شبکه‌ها به شبکه داخلی جلوگیری کرد و همچنین می‌توان سرویس‌های شبکه یا اسامی و سایت‌های اینترنتی خاصی را مسدود یا Block نمود.

د) نگهداری اطلاعات وب (Web Caching): کلیه سایت‌ها و اطلاعاتی که کاربران از شبکه دریافت می‌کنند، در بخشی از دیسک کپی شده و درخواست‌های بعدی کاربران شبکه، با این اطلاعات مقایسه می‌شوند. اگر درخواست‌ها در دیسک سخت وجود داشته باشند، به سمت کاربر ارسال می‌شوند و در غیر این صورت، درخواست مذکور به سمت اینترنت ارسال شده و نتایج حاصل به سمت کاربر ارسال می‌شود. به این عملیات Web Caching می‌گویند و برای بالا بردن سرعت استفاده از اینترنت و کاهش ترافیک شبکه مورد استفاده قرار می‌گیرد.

۱۶-۳-۲- معایب وب پروکسی

الف) زمان بر بودن تنظیم: برای اتصال به شبکه باید در همه رایانه‌ها تنظیمات خاصی را در بخش Proxy ویندوز انجام داد و در شبکه‌های بزرگ، انجام این کار وقت زیادی را می‌گیرد. البته برای تنظیم Proxy در Internet Explorer، می‌توان

با کمک Group Policy، این تنظیم را روی تمامی سیستم‌ها اعمال نمود. بدین منظور به فصل Group Policy مراجعه فرمایید.

ب) عدم شفافیت: نوع ارتباط، شبکه شفاف (Transparent Network) نیست؛ به این معنی که کاربران شبکه اطلاع دارند که از سمت سرویس دهنده به طور کامل کنترل می‌شوند.

ج) وابستگی به پروکسی سرور: در صورتی که نرم‌افزار پروکسی دچار مشکل شود، اینترنت تمامی کاربران قطع می‌شود.

از نرم‌افزارهای رایج به عنوان Proxy Server می‌توان به ISA Server، Win Route و CCProxy Server اشاره کرد.

۱۶-۴- مترجم آدرس شبکه یا NAT

در روش مترجم آدرس شبکه یا NAT (Network Address Translator) دیگر نیازی به نصب برنامه خاصی در ویندوز نیست، بلکه با استفاده از سرویس ویندوز ICS (Internet Connection Sharing) می‌توان اینترنت را برای کاربران در شبکه به اشتراک گذاشت. تنها نکته مهم برای برقراری ارتباط بین شبکه و سرور این است که بایستی آدرس Gateway تمامی رایانه‌های شبکه با آدرس رایانه سرور یکی باشد و در بخش DNS رایانه‌های شبکه، بایستی آدرس DNS Server را وارد نماییم تا عملیات تبدیل نام در شبکه انجام شود. این دقیقا همان کاری است که به صورت خودکار هنگام اتصال به اینترنت انجام می‌گیرد. مثلا زمانی که به یک ISP متصل می‌شویم.

۱۶-۴-۱- مزایا و معایب روش NAT

الف) نوع ارتباط شبکه شفاف است؛ به این معنی که کاربران از نوع سرویس دهنده اینترنت هیچ اطلاعی ندارند.

ب) رایانه‌های داخل شبکه نیاز به تنظیمات Proxy ندارند.

ج) در این روش، چون ارتباط کاربران در **لایه Network** انجام می‌شود، عملیات اعتبار سنجی، ثبت عملکرد کاربر، دیوار آتشین شخصی و نگهداری اطلاعات وب (Web Caching) را نمی‌توان انجام داد.

نکته: نرم‌افزار Microsoft ISA Server یکی از قوی ترین برنامه‌های به اشتراک گذاری اینترنت است که می‌تواند با هر دو روش فوق اینترنت را برای کاربران داخل شبکه به اشتراک بگذارد. این نرم‌افزار از یک دیوار آتشین (Firewall) بسیار قوی برای حفاظت رایانه‌های داخل شبکه استفاده می‌کند و می‌تواند تمامی کاربران داخل شبکه را بسیار قوی مدیریت کند. از دیگر ویژگی‌های مهم این نرم‌افزار، Cache Server قدرتمند آن می‌باشد.

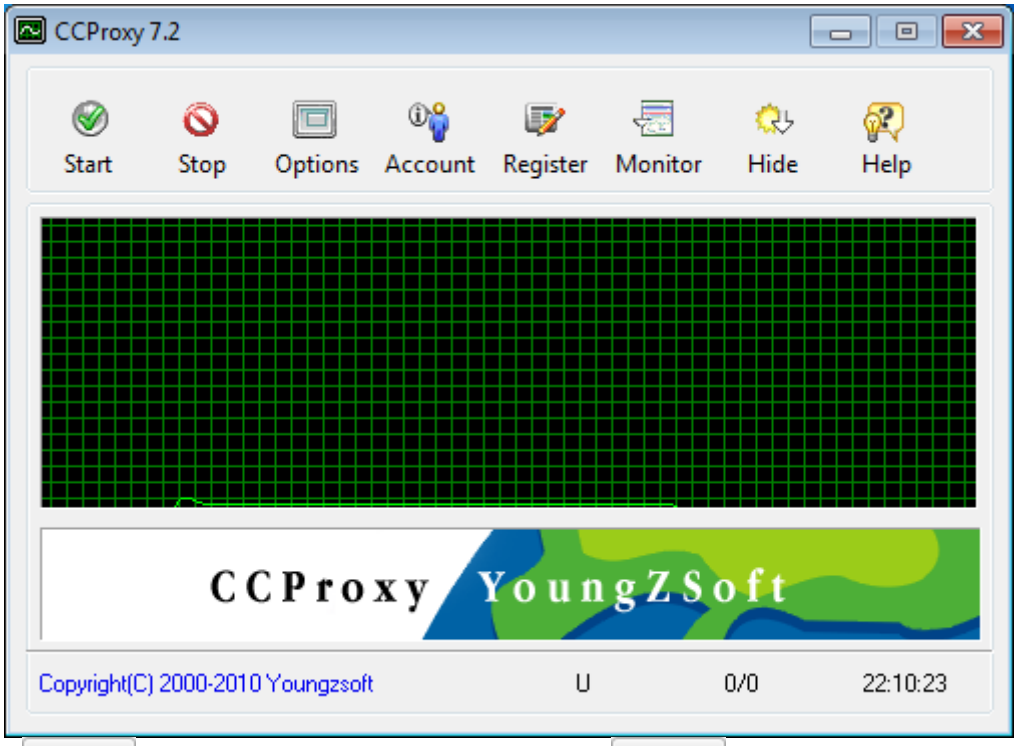
۱۶-۵- آموزش عملی وب پروکسی یا Proxy Server

گفتیم که یکی از روش‌های به اشتراک گذاری اینترنت، استفاده از وب پروکسی یا Proxy Server می‌باشد. در این قسمت، ما به آموزش یک نرم‌افزار Proxy Server به نام **CCProxy** می‌پردازیم. جهت استفاده از این نرم‌افزار، پس از نصب آن، حتما اقدام به ثبت آن نمایید زیرا نسخه ثبت نشده، تنها قادر به سرویس دهی به ۳ کاربر به صورت همزمان می‌باشد؛ اما نسخه ثبت شده هیچ محدودیتی در سرویس دهی ندارد. این نرم‌افزار بسیار کم حجم بوده (حدود 2 MB) و امکان دانلود آن از اینترنت وجود دارد.

۱۶-۵-۱- تنظیمات سرور

پس از نصب نرم‌افزار CCProxy روی کامپیوتری که به اینترنت وصل است (کامپیوتر سرور) و باز کردن آن، صفحه‌ای مانند زیر مشاهده می‌نمایید. کاربرد دکمه‌های اصلی نرم‌افزار به صورت زیر می‌باشد:

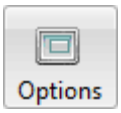
- Start: با کلیک روی این دکمه، نرم‌افزار شروع به سرویس دهی می‌کند و کلاینت‌ها می‌توانند از اینترنت آن استفاده نمایند.
- Stop: با کلیک روی این دکمه، نرم‌افزار عمل سرویس دهی را قطع می‌کند.
- Options: از طریق این قسمت می‌توان تنظیمات عمومی نرم‌افزار، مانند پورت‌های مورد استفاده را تغییر داد.
- Account: از طریق این قسمت می‌توان حساب‌های کاربران را مدیریت نمود.
- Register: از طریق این قسمت می‌توان اقدام به ثبت نرم‌افزار و حذف محدودیت‌های آن نمود.
- Monitor: از طریق این قسمت می‌توان عملیات آمار گیری را انجام داد.
- Hide: با کلیک روی این دکمه، صفحه اصلی نرم‌افزار مخفی شده و آیکون نرم‌افزار در System Tray باقی مانده و نرم‌افزار به سرویس دهی خود ادامه می‌دهد.
- Help: با کلیک روی این دکمه، یک فایل PDF باز می‌شود که در اصل همان Help نرم‌افزار می‌باشد.
- نکته: اگر برنامه را ببندید، سرویس دهی نرم‌افزار قطع می‌شود و دیگر کلاینت‌ها قادر به گرفتن اینترنت از سرور نیستند. جهت مخفی کردن نرم‌افزار، روی دکمه Hide کلیک کنید.



برای شروع سرویس دهی، روی دکمه 

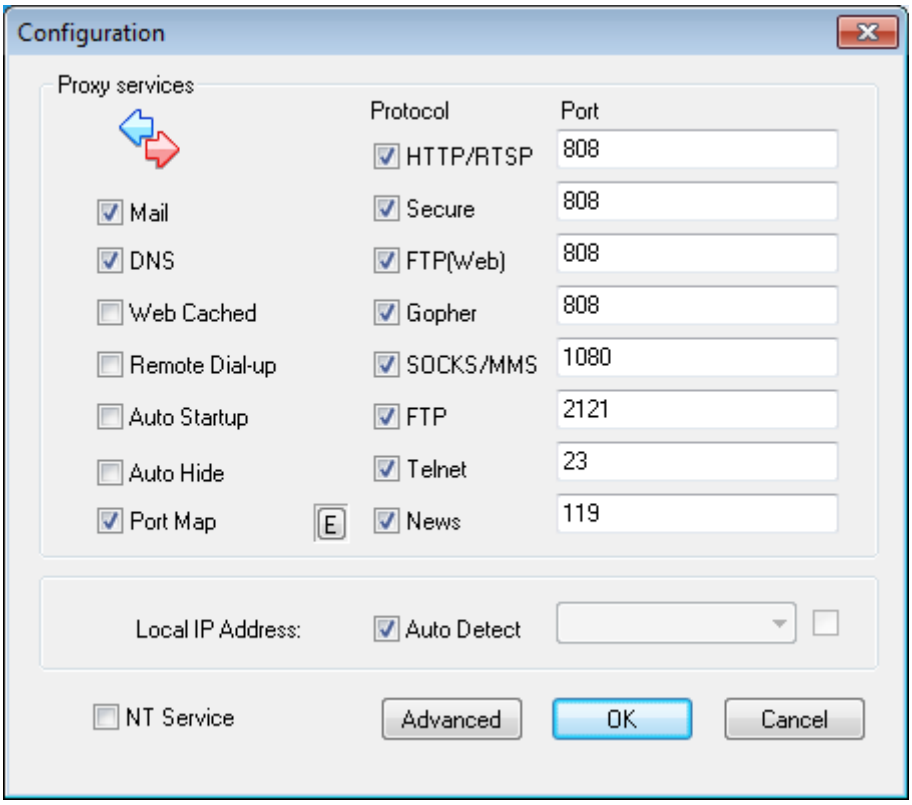
و برای قطع عمل سرویس دهی روی دکمه 

کلیک نمایید.

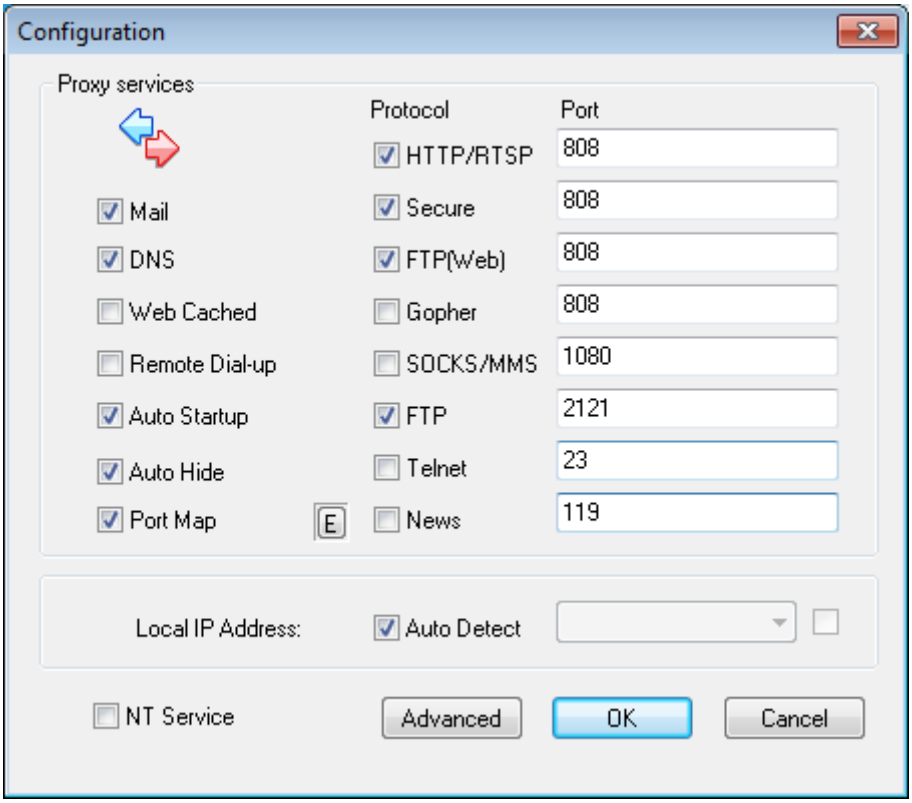
حال نوبت به تنظیمات عمومی برنامه می‌رسد. بدین منظور روی دکمه 

کلیک نمایید.

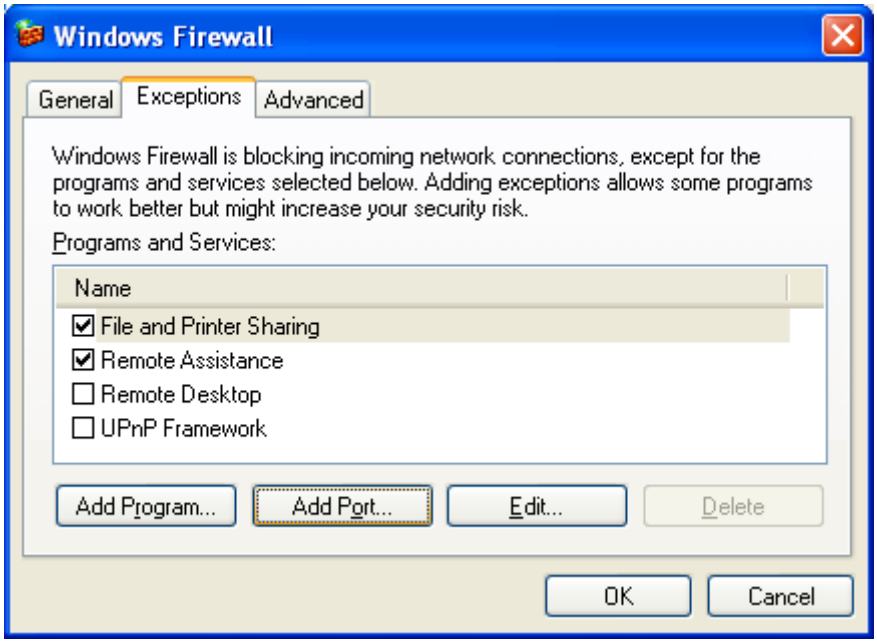
در صفحه باز شده، می‌توانید تنظیمات عمومی برنامه را مشاهده نمایید. اصلی ترین تنظیمات شامل سرویس‌های قابل ارائه توسط نرم‌افزار و شماره پورتی که هر سرویس اشغال می‌کند می‌باشد.



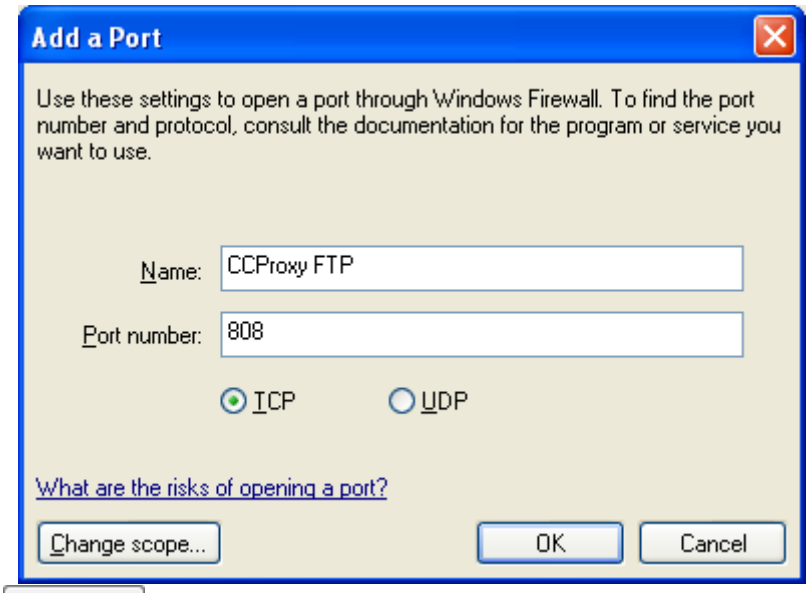
همانطور که در شکل فوق مشاهده نمودید، به صورت پیش فرض تمامی سرویس‌های قابل ارائه فعال می‌باشند، این امر هم باعث افت کارآیی نرم‌افزار می‌شود و هم باعث می‌شود برخی پورت‌ها بی دلیل اشغال شوند. به همین دلیل توصیه می‌شود سرویس هایی که به آن نیاز ندارید را غیر فعال نمایید. مثلاً سرویس Gopher یک سرویس قدیمی است که پروتکل Http جایگزین آن شده است. در صورت نیاز می‌توانید شماره پورت را نیز تغییر دهید؛ فقط توجه نمایید که شماره پورت‌های وارد شده نباید با شماره پورت دیگر نرم‌افزارها تداخل داشته باشد. ما سرویس‌های خود را به صورت زیر فعال نمودیم:



در صورتی که Firewall کامپیوتر شما فعال باشد، بایستی این شماره پورت‌ها (تصویر فوق) را به Firewall معرفی نمایید. بدین منظور ابتدا Firewall را از Control Panel باز نموده و سپس وارد سربرگ Exceptions شوید.

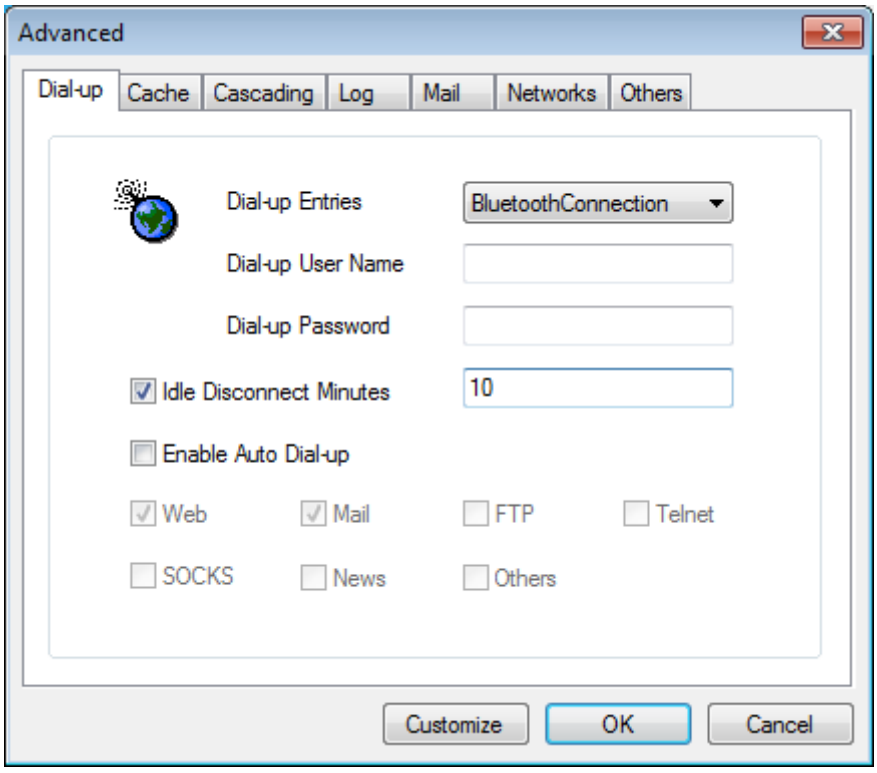


سپس روی دکمه Add Port کلیک نموده و سپس شماره پورت مورد نظر به همراه یک نام دلخواه برای آن وارد نمایید. به ازاء پورت‌های با شماره مختلف، این کار را چندین بار تکرار نمایید.



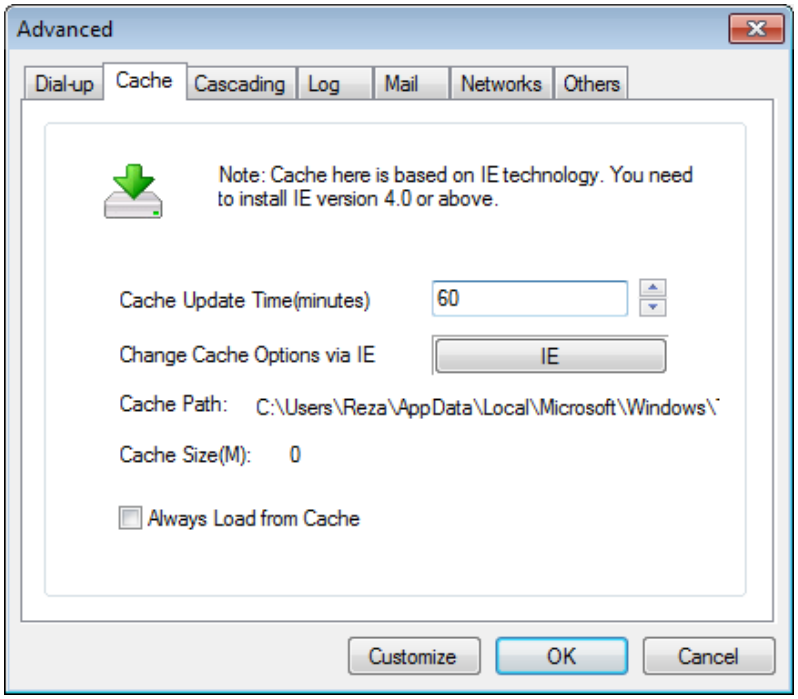
صفحه Options دارای تنظیمات پیشرفته تری نیز می‌باشد. بدین منظور روی دکمه Advanced کلیک نمایید. در صفحه باز شده، تعدادی سربرگ وجود دارد که آن‌ها را مختصرا توضیح می‌دهیم:

Dial-UP: در این سربرگ می‌توان مشخص نمود که از کدام Connection و با چه Username و Passwordی به اینترنت وصل شوید (خود سرور به اینترنت وصل شود و نه کلاینت ها). همچنین می‌توان مشخص نمود که اگر تا چند دقیقه هیچ درخواستی به Proxy Server ارسال نشد، اتصال سرور با اینترنت قطع شود (در این مثال ۱۰ دقیقه). امکان دیگری که این صفحه دارد، این است که می‌توان مشخص نمود که اگر درخواست‌های خاصی مانند Web، Email، FTP یا... به سمت سرور آمد و سرور به اینترنت متصل نبود، عمل اتصال به اینترنت و انجام عمل سرویس دهی به صورت خودکار انجام گیرد.

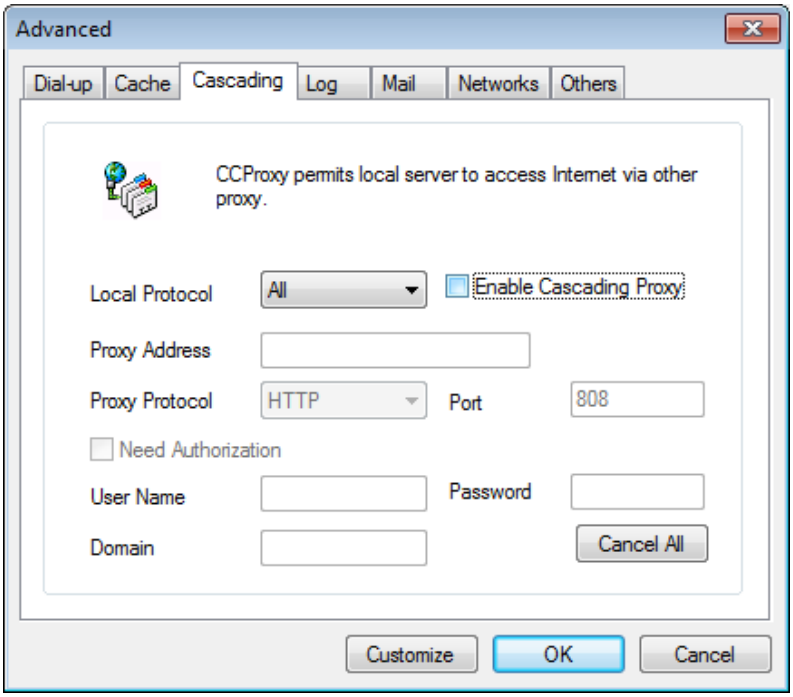


Cache: همانطوری که قبلاً توضیح دادیم، یکی از مزایای Web Proxyها، ذخیره صفحات وب یا اصطلاحا Caching می‌باشد. در این سربرگ شما می‌توانید تنظیمات Caching را تغییر دهید. مثلاً در شکل زیر مشخص شده است

که با باز شدن هر صفحه وب، اطلاعات آن صفحه به مدت ۶۰ دقیقه ذخیره شود و در درخواست‌های بعدی، در صورت امکان از این صفحات ذخیره شده استفاده نماید. مسیر ذخیره فایل‌های Cache شده نیز مشخص است. برای انجام تنظیمات بیشتر، روی دکمه IE کلیک نمایید.

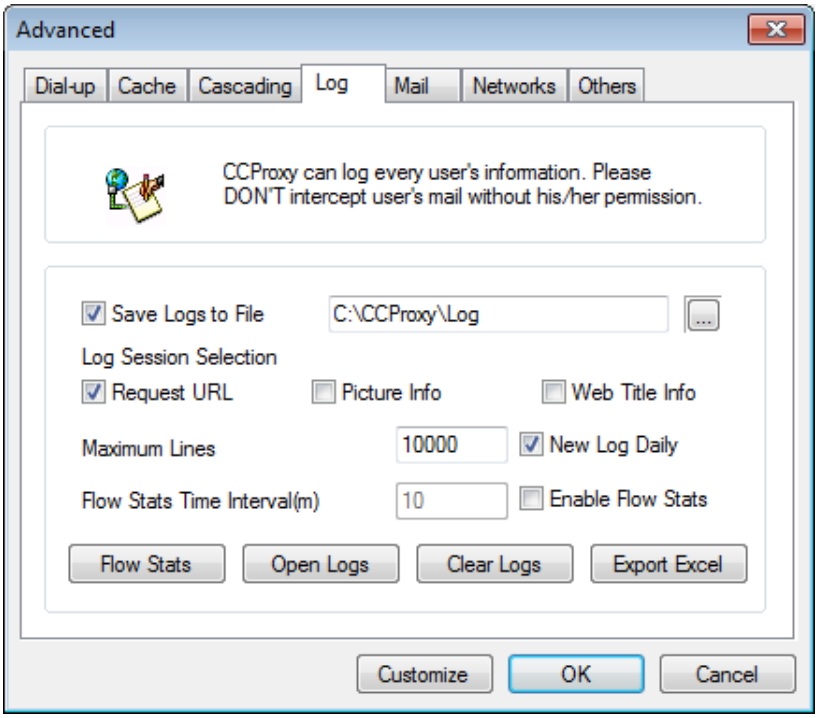


Cascading: این سربرگ زمانی استفاده می‌شود که خود Proxy Server ما، اینترنت را از یک Proxy Server دیگر دریافت نماید. در اینجا می‌توان تنظیمات مورد نیاز مانند آدرس و شماره پورت Proxy Server، نام کاربری، رمز عبور و... را تعیین نمود.

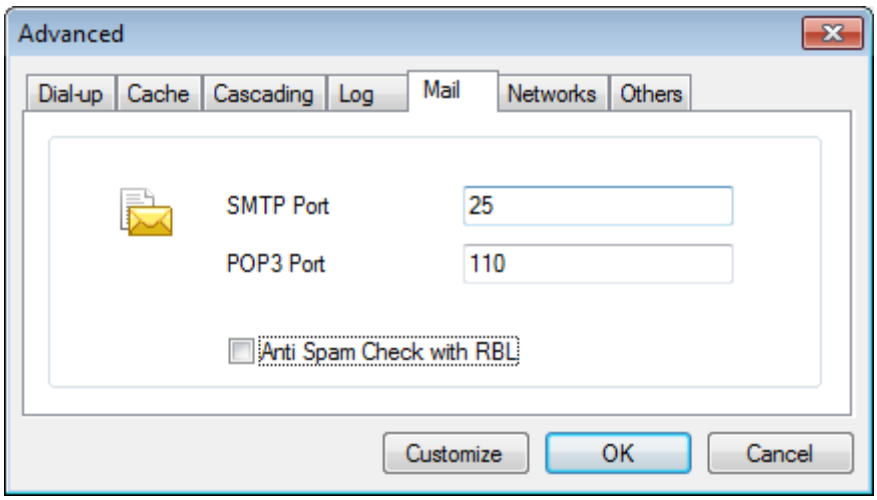


Log: همانطور که قبلاً نیز بحث شد، یکی از مزایای Web Proxy، امکان رد گیری اتفاقات انجام شده، مثلاً تلاش‌های کاربران برای مشاهده سایت‌های مختلف یا میزان داده‌های مورد استفاده هر کاربر می‌باشد. این اطلاعات در فایل هایی به نام

Log File ذخیره می‌شود. از طریق این صفحه می‌توانید تنظیمات Log Fileها را انجام دهید. ساختار Log Fileها بدین صورت است که نرم‌افزار به ازاء هر روز، دو فایل متنی می‌سازد، یکی برای سایت مورد دسترسی قرار گرفته (LogYYYYMMDD.txt) و دیگری برای میزان داده ارسالی و دریافتی هر کاربر (DataYYYYMMDD.txt). در این صفحه با کلیک روی دکمه Open Logs می‌توانید محتوای Log File را با Note Pad مشاهده نمایید. با کلیک روی دکمه Export Excel نیز می‌توانید Log File را به یک فایل Excel تبدیل نموده و داده‌ها را ساخت یافته مشاهده نمایید.



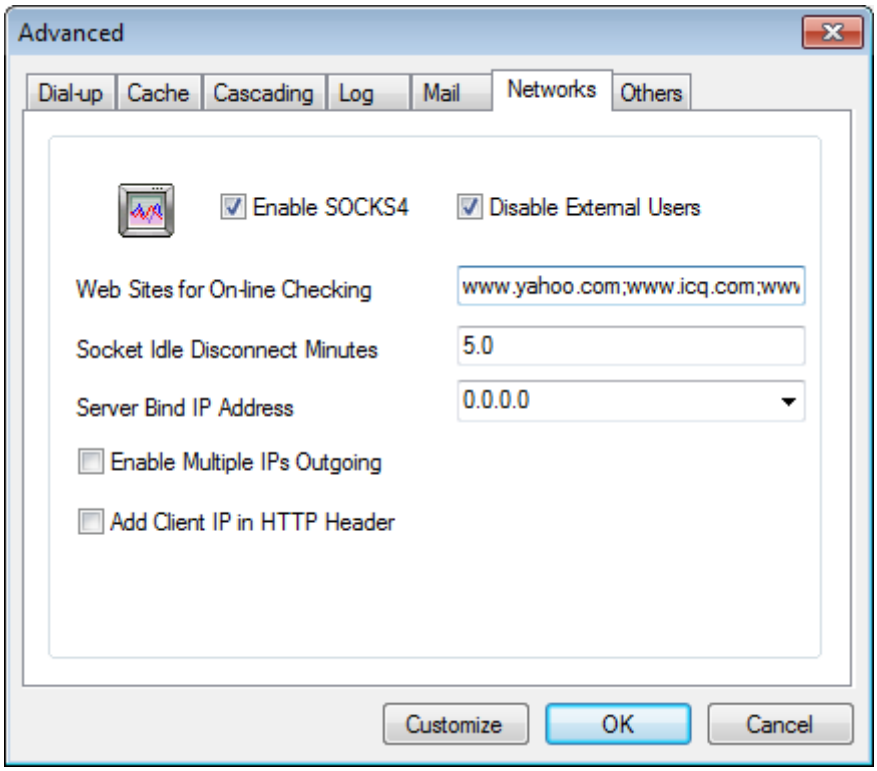
Mail: از طریق این سربرگ می‌توانید مشخص نمایید که سرویس‌های ایمیل SMTP و POP3 از طریق کدام پورت‌ها کار بکنند. این پارامترها بیشتر هنگام کار با نرم‌افزارهای مدیریت ایمیل مانند Outlook Express نمود پیدا می‌کنند. امکان بررسی وجود Spam در ایمیل‌ها نیز وجود دارد.



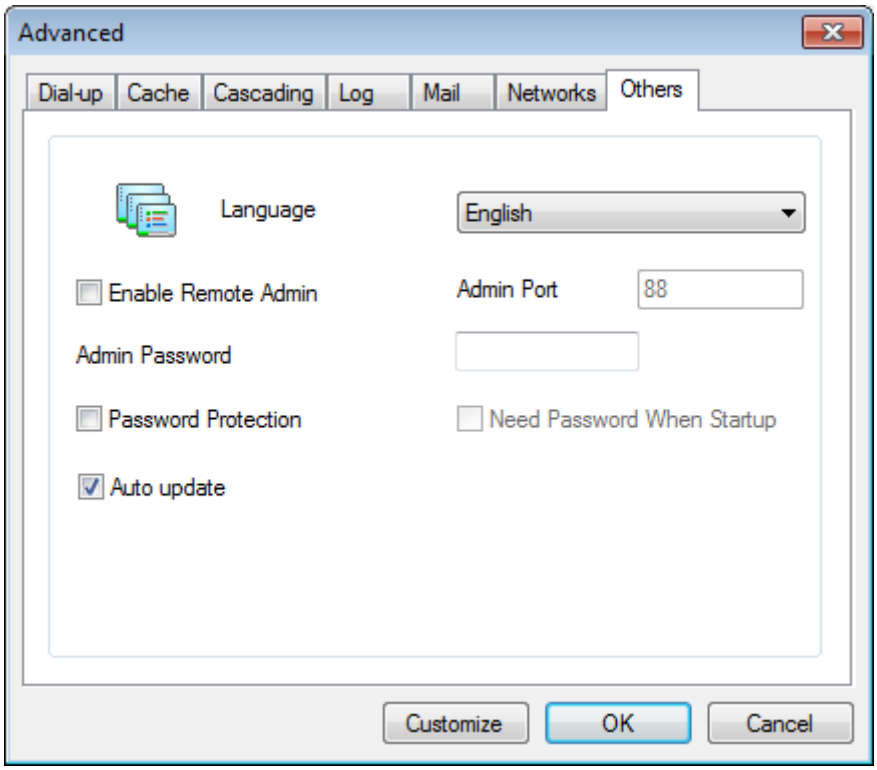
Networks: این سربرگ نیز تنظیمات خاصی را انجام می‌دهد که هر کدام را به اختصار توضیح می‌دهیم:

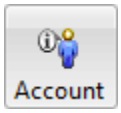
- Enable SOCKS4: فعال سازی سرویس‌های SOCKS4 و SOCKS4A که در Web Proxyها کاربرد دارد.
- Enable External Users: فعال کردن یا غیر فعال کردن دسترسی کاربران خارج از شبکه LAN.

- Web Sites For On-Line Checking: این نرم‌افزار نیاز دارد بداند که آیا سیستم سرور به اینترنت متصل است یا خیر؟ که بدین منظور بایستی سایت‌های خاصی را ملاقات نماید. در این قیمت می‌توانید سایت‌های خاصی را مشخص نمایید که در صورتی هیچ کدام از آن‌ها باز نشود، یعنی اینترنت ما قطع شده است.
- Socket Idle Disconnect Minutes: مدت زمان Time Out سوکت‌های بدون استفاده.
- Server Bind IP Address: زمانی که کامپیوتر سرور دارای چندین آدرس IP باشد (Multiple Host)، می‌توان آدرس IP خاصی را برای نرم‌افزار تعیین نمود. آدرس ۰.۰.۰.۰ بدین معناست که نرم‌افزار خودش یک آدرس IP را خودکار انتخاب نماید.
- Enable Multiple IPs Outgoing: اگر چندین آدرس IP دارید و می‌خواهید کاربران هنگام اتصال به اینترنت، هر کدام یک آدرس IP جدا داشته باشند، این گزینه را فعال نمایید.
- Add Client IP in HTTP Header: نرم‌افزار به سرآیند HTTP، "X-Forwarded-For" را اضافه می‌کند که "X-Forwarded-For" شامل آدرس IP کلاینت خواهد بود.

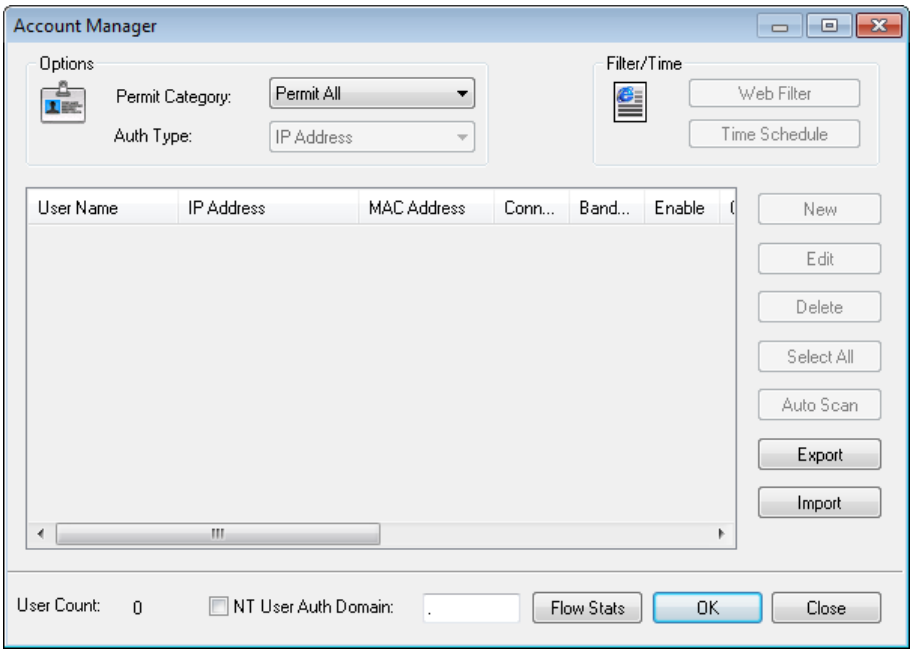


Others: از طریق این سربرگ می‌توان تنظیمات عمومی دیگری انجام داد، مانند زبان نرم‌افزار، رمز عبور مدیر (Admin)، امکان به روز رسانی خودکار و....



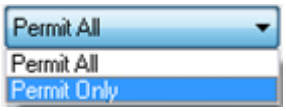
حال نوبت به تنظیمات حساب‌های کاربری می‌رسد. اگر تنظیمات این قسمت را وارد ننمایید، هر کامپیوتری که به شبکه متصل باشد، می‌تواند از اینترنت به اشتراک گذاشته شده استفاده نماید. اگر این امر مورد پسند شما نیست و دوست دارید کاربران را کنترل نمایید، در صفحه اصلی نرم‌افزار، روی دکمه 

کلیک کنید. در صفحه باز شده امکان انجام تنظیمات حساب‌های کاربری وجود دارد که آن‌ها را در ادامه توضیح می‌دهیم.



در ابتدای امر و در قسمت Permit Category مشخص می‌شود که اجازه‌های دسترسی جهت استفاده از اینترنت به اشتراک گذاشته شده چگونه باشد. در ابتدا گزینه Permit All انتخاب شده است، یعنی تمامی کاربران شبکه LAN حق

استفاده از این اینترنت را دارند. اما اگر می‌خواهید دسترسی‌ها به اینترنت را تحت کنترل خود در آورید، گزینه دوم یعنی Permit Only را انتخاب نمایید.



با انتخاب این گزینه، دکمه‌های این صفحه فعال شده و امکان مدیریت حساب‌های کاربری فراهم می‌شود. سپس بایستی نوع احراز هویت و اجازه دسترسی با اینترنت را مشخص نمایید. این کار از طریق قسمت Auth Type انجام می‌گیرد. معنای گزینه‌های این قسمت به صورت زیر است:

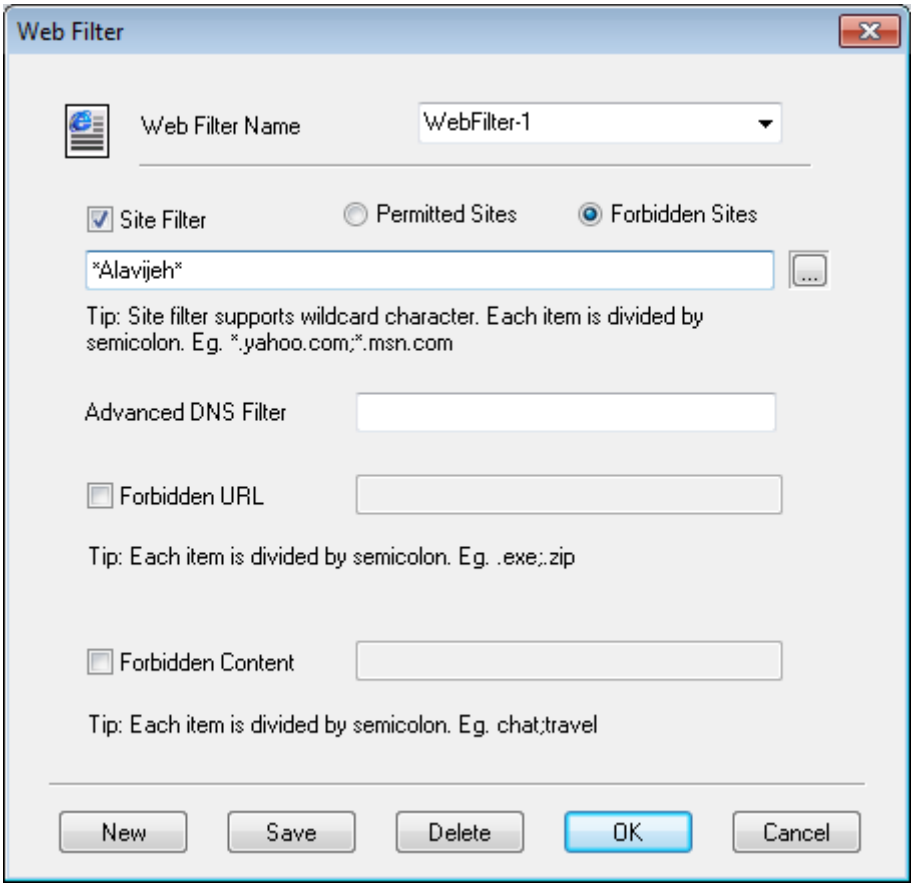
- **IP Address:** فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس IP سیستم آن‌ها در لیست زیر ثبت شده باشد.
- **MAC Address:** فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس MAC کارت شبکه آن‌ها در لیست زیر ثبت شده باشد.
- **User/Password:** فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن‌ها در لیست زیر ثبت شده باشد. این کاربران هنگام استفاده از اینترنت، بایستی نام کاربری و رمز عبور را وارد نمایند و اگر نام کاربری و رمز عبور وارد شده در لیست زیر موجود باشد، آن‌ها اجازه استفاده از اینترنت را پیدا می‌کنند.
- **User/Password + IP:** فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن‌ها به همراه آدرس IP سیستم آن‌ها در لیست زیر ثبت شده باشد. با این کار، تقریباً می‌توان گفت که کاربران را مجبور به استفاده از سیستمی خاص می‌کنیم، اما این امر همیشه صحیح نیست، زیرا آدرس IP کامپیوترها قابل تغییر است.
- **User/Password + MAC:** فقط کاربرانی حق استفاده از اینترنت را دارند که نام کاربری و رمز عبور آن‌ها به همراه آدرس MAC کارت شبکه آن‌ها در لیست زیر ثبت شده باشد. با این کار، کاربران را مجبور به استفاده از سیستمی خاص می‌کنیم.
- **IP + MAC:** فقط کاربرانی حق استفاده از اینترنت را دارند که آدرس IP سیستم آن‌ها به همراه آدرس MAC کارت شبکه آن‌ها در لیست زیر ثبت شده باشد. با این کار سیستم‌ها را مجبور می‌کنیم که هر سیستم، یک آدرس IP خاص داشته باشد که در صورت تغییر آدرس IP دیگر امکان اتصال به اینترنت وجود نداشته باشد.



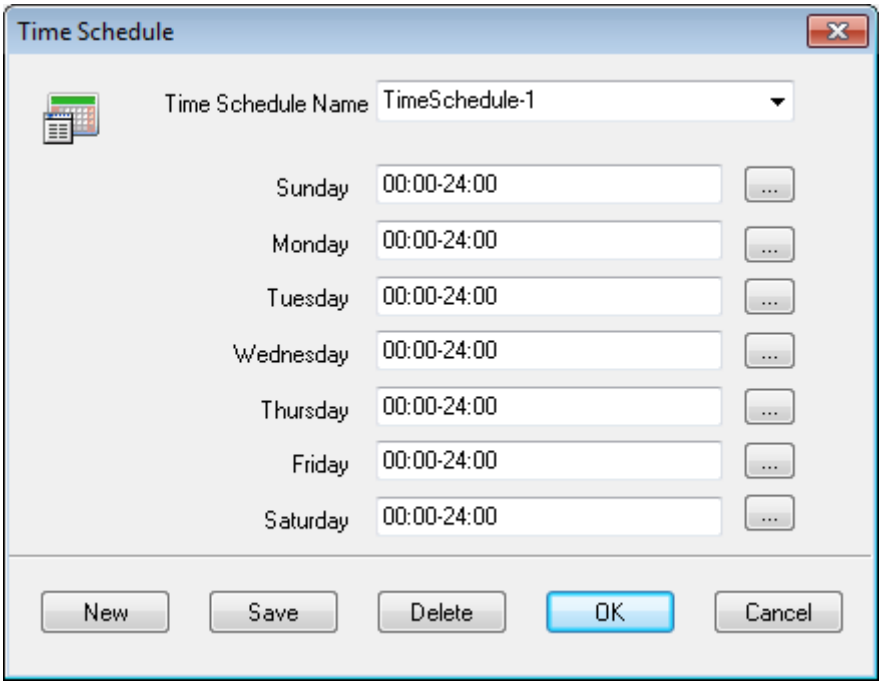
یکی دیگر از امکانات این نرم‌افزار، فیلتر کردن سایت‌های مورد دسترسی کاربران می‌باشد. بدین منظور روی دکمه 

کلیک نمایید. در این صفحه می‌توانید مشخص نمایید که فقط سایت هایی با ویژگی‌های زیر قابل باز شدن باشد (Permitted Sites) یا فقط سایت هایی با ویژگی‌های زیر مسدود و قدغن باشد (Forbidden Sites) که البته مورد دومی پر کاربردتر است. سپس در جعبه متن Site Filter، آدرس سایت‌های مورد نظر را وارد نمایید. برای استفاده از

کلی گویی می‌توان از علامت × (به معنای صفر یا چند حرف) استفاده کرد. در قسمت Forbidden URL می‌توان برخی URLهای ممنوعه را وارد نمود. مثلاً URL هایی که در آن‌ها حروف.exe یا.zip وجود دارد. این بخش بیشتر برای جلوگیری از عملیات دانلود می‌باشد. در قسمت Forbidden Content نیز می‌توان مشخص نمود که اگر یک صفحه درخواستی شامل متن و محتوای خاصی بود، آن را به سمت کاربر ارسال نکن. می‌توان چندین نوع فیلتر را تعریف نمود و هر کدام را به کاربری خاص نسبت داد. این کار در هنگام ایجاد کاربر جدید انجام می‌گیرد.



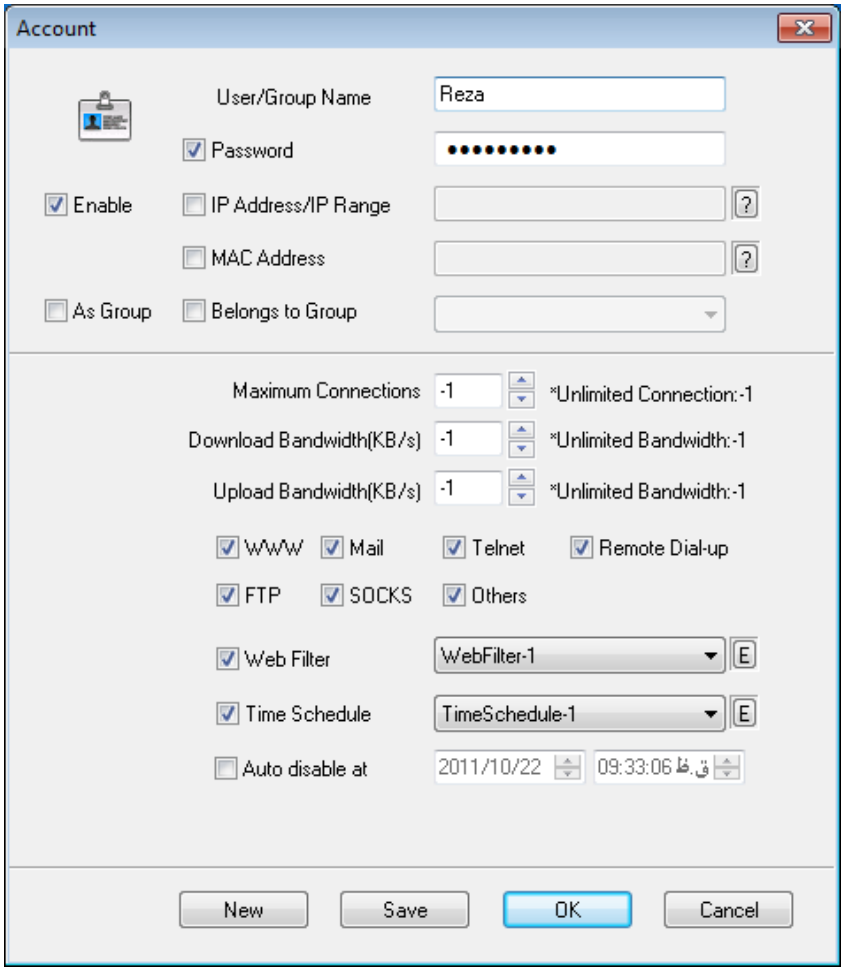
یکی دیگر از امکانات این نرم‌افزار، امکان زمانبندی سرویس دهی نرم‌افزار می‌باشد. بدین منظور در صفحه Accounts روی دکمه Time Schedule کلیک کنید. در صفحه باز شده می‌توانید مشخص نمایید که نرم‌افزار در چه روز هایی و از چه ساعت تا چه ساعت هایی، عمل سرویس دهی را انجام دهد. می‌توان چندین نوع زمان بندی را تعریف نمود و هر کدام را به کاربری خاص نسبت داد. این کار در هنگام ایجاد کاربر جدید انجام می‌گیرد.



حال نوبت به یکی از مهم ترین بخش‌های نرم‌افزار یعنی حساب‌های کاری کاربران می‌رسد. برای ایجاد حساب کاربری جدید، در صفحه Accounts روی دکمه New کلیک کنید. برای تغییر اطلاعات کاربران موجود نیز، پس از انتخاب کاربری خاص روی دکمه Edit کلیک نمایید. حذف کاربر نیز با دکمه Delete انجام می‌گیرد. بعد از باز شدن صفحه ثبت کاربر جدید یا تغییر اطلاعات کاربر، صفحه زیر را مشاهده می‌نمایید که معنای قسمت‌های مختلف به صورت زیر است:

- **User/Group Name:** نام کاربر یا نام گروه می‌باشد.
- **Password:** اگر این گزینه تیک خورده باشد، کاربر هنگام استفاده از اینترنت، بایستی نام کاربری و رمز عبور را وارد نماید. صفحه دریافت نام کاربری و رمز عبور هر نرم‌افزار متفاوت بوده (مانند IE، Opera، IDM و...) و خود نرم‌افزار آن‌ها را از کاربر دریافت می‌نماید.
- **IP Address/IP Range:** آدرس IP یا محدوده آدرس IP کامپیوتر هایی که کاربر می‌تواند از آن‌ها استفاده نماید.
- **MAC Address:** آدرس MAC کارت شبکه کامپیوتری که کاربر می‌تواند از آن استفاده نماید.
- **Enable:** فعال یا غیر فعال شدن کاربر یا گروه.
- **As Group:** اطلاعات وارد شده، مربوط به یک گروه می‌باشد و نه یک کاربر. این قسمت برای تعریف گروه به کار می‌رود. یعنی با این نرم‌افزار می‌توان کاربران را گروه بندی نمود و سیاست‌ها (مانند فیلترها و زمانبندی ها) را روی گروه‌ها را اعمال نمود و هر کاربری که عضو گروهی خاص شود، این سیاست‌ها روی وی اعمال خواهد شد.
- **Belongs to Group:** گروهی که کاربر عضو آن می‌باشد را مشخص می‌کند. با این کار دیگر امکان انجام تغییرات برای کاربر وجود ندارد و سیاست‌های گروه روی کاربر نیز اعمال می‌شود.

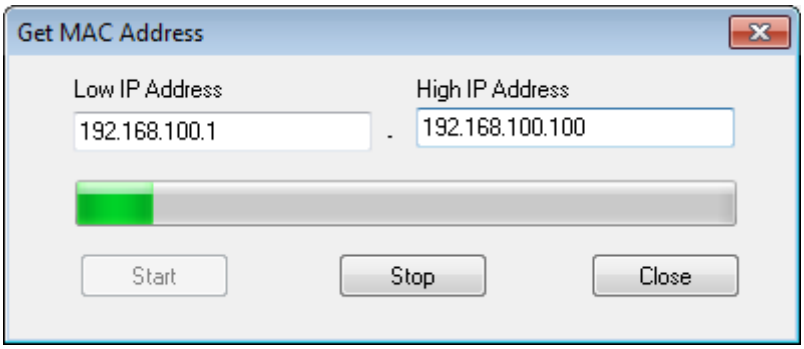
- **Maximum Connections:** مشخص می‌نماید که کاربر در هر لحظه چند درخواست اینترنتی می‌تواند وارد نماید (عدد ۱- به معنای بی نهایت است).
- **Download Bandwidth (KB/S):** مشخص می‌نماید که کاربر حداکثر با چه سرعتی می‌تواند عمل دانلود و باز کردن صفحات را انجام دهد. واحد بر حسب کیلو بایت بر ثانیه می‌باشد (عدد ۱- به معنای بی نهایت است).
- **Upload Bandwidth (KB/S):** مشخص می‌نماید که کاربر حداکثر با چه سرعتی می‌تواند عمل آپلود و ارسال اطلاعات را انجام دهد. واحد بر حسب کیلو بایت بر ثانیه می‌باشد (عدد ۱- به معنای بی نهایت است).
- **Services:** مشخص می‌نماید که کاربر حق استفاده از چه سرویس هایی را دارد. مثلاً www برای باز کردن صفحات وب و FTP برای کار با سرویس انتقال فایل می‌باشد.
- **Web Filter:** برای اعمال فیلتری خاص روی کاربر.
- **Time Schedule:** برای اعمال زمانبندی خاص روی کاربر.
- **Auto Disable At:** می‌توان مشخص نمود که کاربر در تاریخ و ساعت خاصی غیر فعال شود.



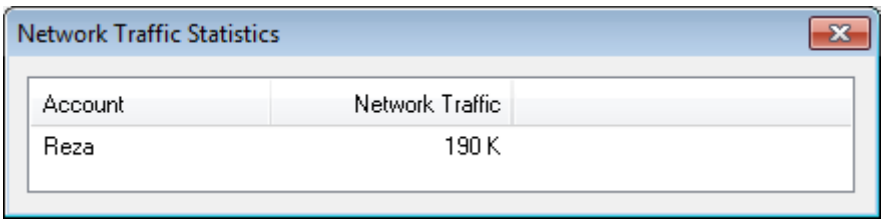
گفتیم که اگر در صفحه ایجاد کاربر جدید، کاربر را ملزم به ورود نام کاربری و رمز عبور نموده باشید، هنگامی که کاربر بخواهد از اینترنت استفاده کند، بایستی نام کاربری و رمز عبور را وارد نماید. مثلاً اگر بخواهید با Internet Explorer با اینترنت استفاده نمایید، صفحه دریافت نام کاربری و رمز عبور آن به صورت زیر می‌باشد:



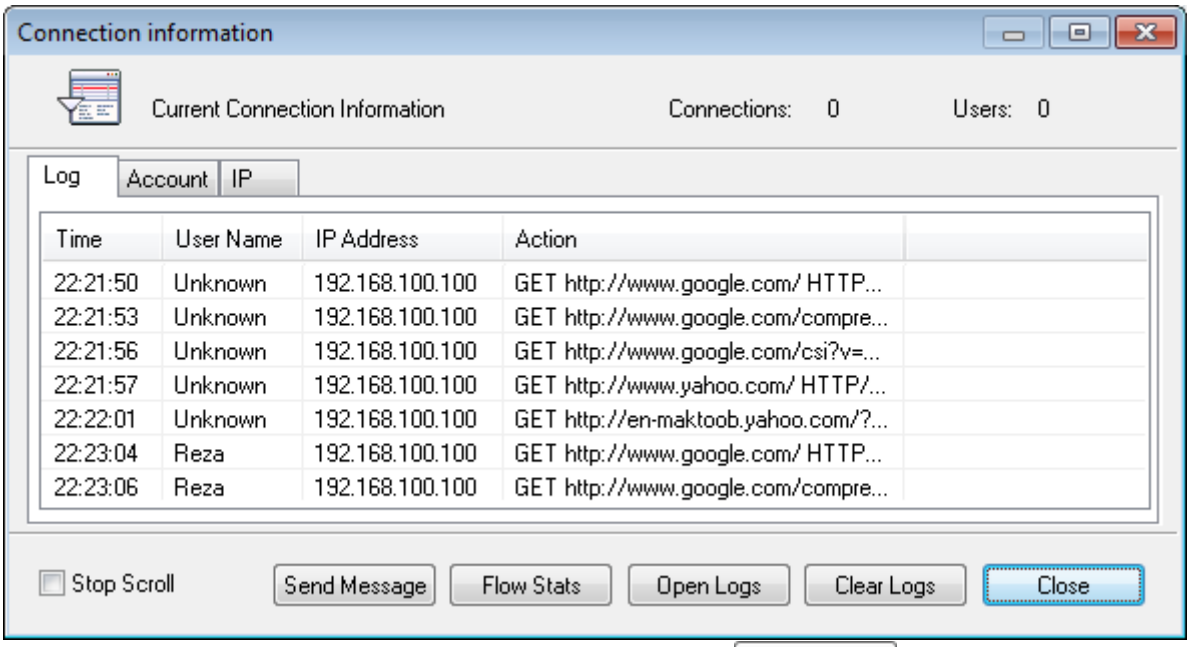
یکی دیگر از امکانات این نرم‌افزار، این است که می‌توان آدرس IP سیستم خاصی را داد و آدرس MAC آن سیستم را به دست آورد. بدین منظور، در صفحه Accounts روی دکمه Auto Scan کلیک نمایید. در صفحه باز شده، محدوده شروع و پایان جستجو را در قالب آدرس IP وارد نموده و سپس روی دکمه Start کلیک نمایید. بدین ترتیب نرم‌افزار دنبال کامپیوترهای موجود در محدوده وارد شده می‌گردد و با پیدا کردن هر کدام، آدرس MAC آن‌ها را به لیست کاربران اضافه می‌نماید.



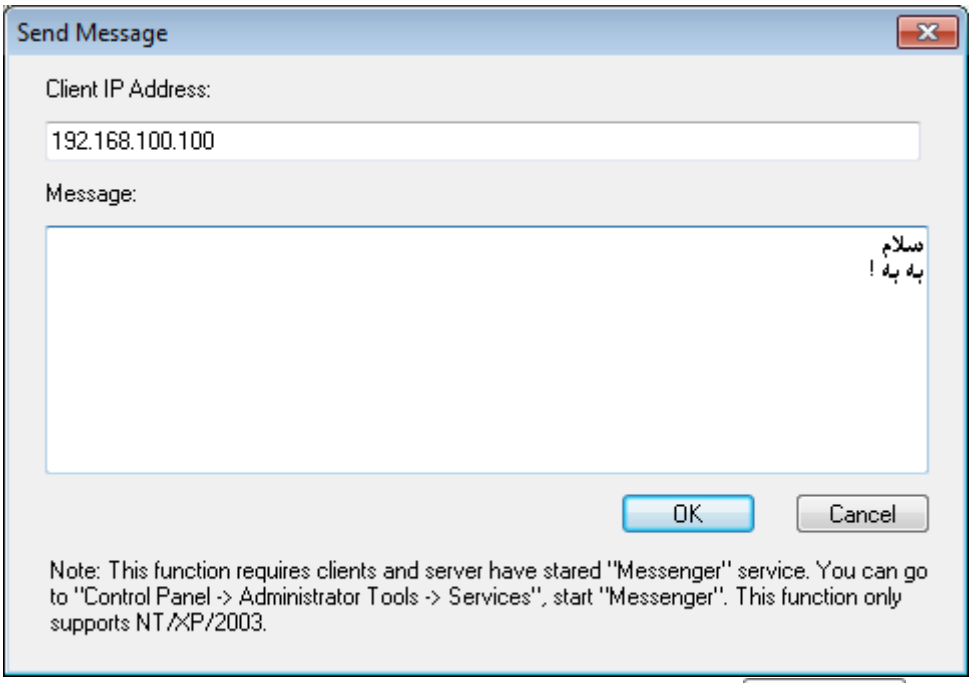
صفحه Accounts امکان دیگری که به ما می‌دهد، امکان مشاهده آمار ترافیک کاربران می‌باشد. بدین منظور در صفحه Accounts روی دکمه Flow Stats کلیک نمایید تا صفحه‌ای مانند صفحه زیر مشاهده کنید.



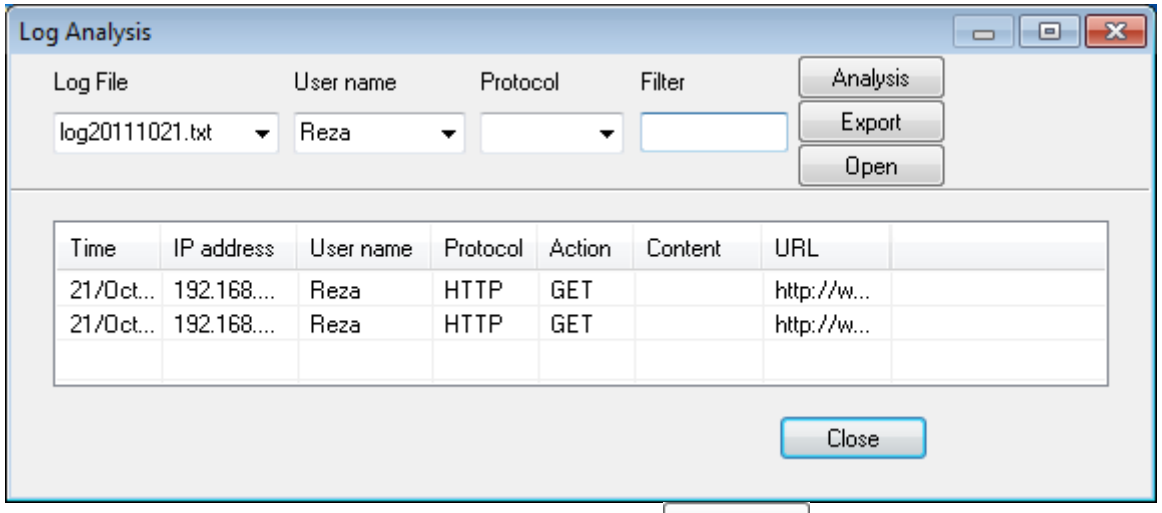
از دیگر امکانات اصلی این نرم‌افزار، امکان مشاهده وقایع اتفاق افتاده می‌باشد. بدین منظور در صفحه اصلی نرم‌افزار، روی دکمه Monitor کلیک نمایید. در صفحه باز شده، ۳ سربرگ مشاهده می‌نمایید که سربرگ Log تک تک وقایع اتفاق افتاده را نمایش می‌دهد.

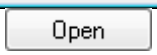


اگر در این صفحه روی دکمه Send Message کلیک کنید، صفحه‌ای مانند صفحه زیر باز می‌شود که امکان ارسال پیام به کامپیوتری خاص را به ما می‌دهد. البته این کار در صورتی قابل انجام است که سرویس پیام رسانی روی کلاینت‌ها فعال شده باشد.

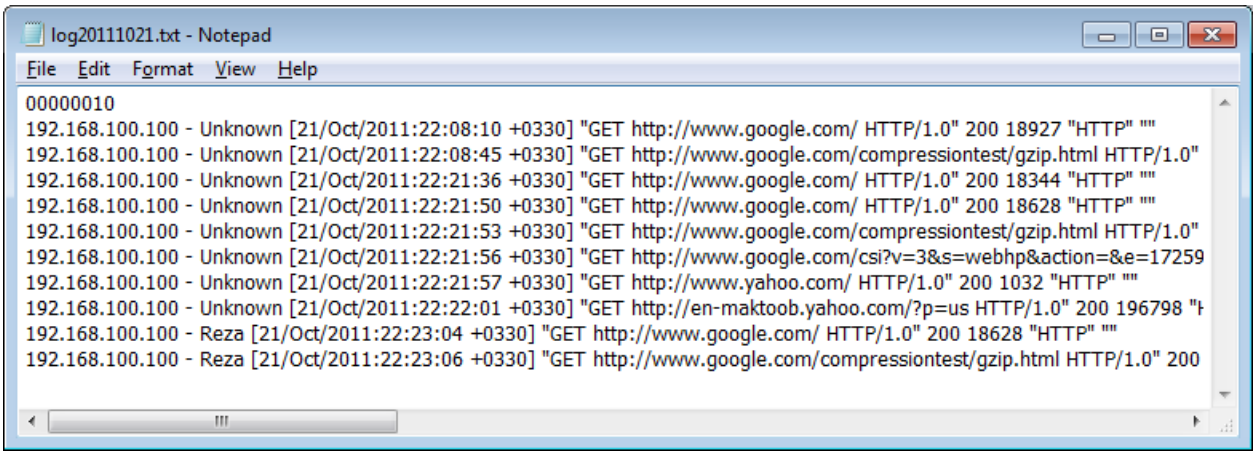


اما اگر روی دکمه Open Logs کلیک نمایید، صفحه آمارگیری و آنالیز اطلاعات باز می‌شود که این صفحه یکی از امکانات پر قدرت این نرم‌افزار می‌باشد. در این صفحه این امکان وجود دارد که بر اساس تاریخی خاص، کاربری خاص، پروتکلی خاص و کلمه کلیدی خاص، اطلاعات را فیلتر نمود. هر کدام از اطلاعات که وارد نشود، نرم‌افزار به دنبال کل اطلاعات می‌گردد. مثلاً اگر تاریخ وارد نشود، نرم‌افزار در تمامی تاریخ‌های موجود عمل جستجو را انجام می‌دهد.

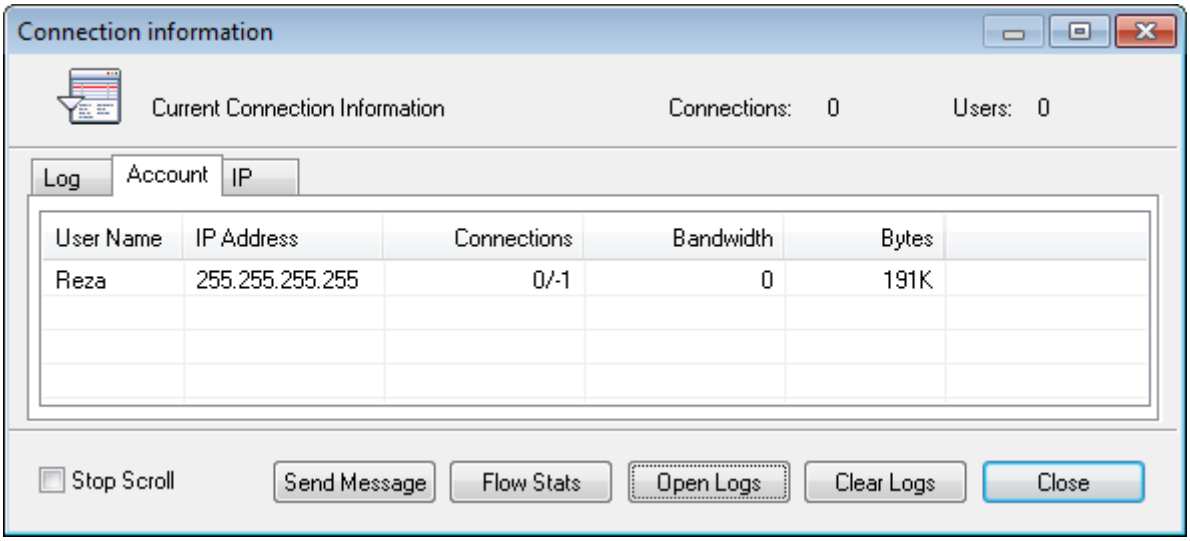


در همین صفحه با کلیک روی دکمه 

می‌توان خود Log File را در Note Pad مشاهده نمود.

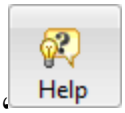


سربرگ دوم، سربرگ Account می‌باشد که در آن می‌توان حساب‌های موجود به همراه برخی اطلاعات آن را مشاهده نمود.



یکی دیگر از قسمت‌های نرم‌افزار، قسمت ثبت نرم‌افزار می‌باشد. برای ثبت نرم‌افزار، پس از خرید نرم‌افزار بایستی شماره سریال‌های داده شده را وارد نمایید. بدین منظور روی دکمه 

کلیک نمایید.

در پایان نوبت به قسمت Help یا راهنمای نرم‌افزار می‌رسد که با کلیک روی دکمه 

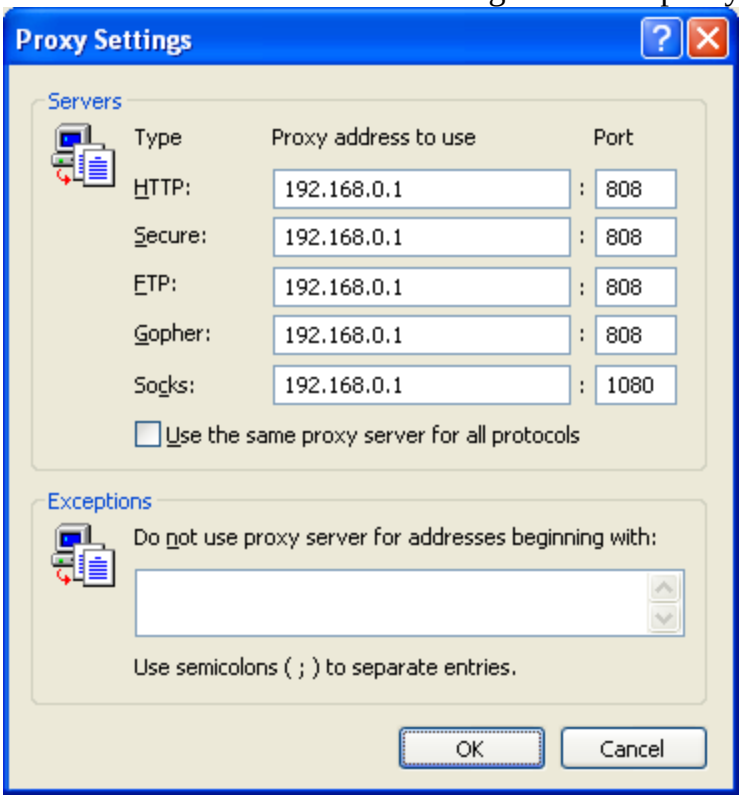
، یک فایل PDF در قالب راهنمای نرم‌افزار باز می‌شود.

۱۶-۵-۲- تنظیمات کلاینت ها

تا اینجا ما توضیح دادیم که چگونه سرور را تنظیم کنیم. اما کلاینت‌ها نیز برای استفاده از اینترنت به اشتراک گذاشته شده نیاز به تنظیماتی خاص دارند و این تنظیمات بدین صورت می‌باشد که اکثر نرم‌افزار هایی که از اینترنت استفاده می‌کنند، قسمتی به نام Proxy Server دارند کا بایستی این قسمت را پیدا نمود و سپس آدرس IP سرور که نرم‌افزار Web Proxy روی آن نصب است به همراه شماره پورت‌های سرویس‌های مختلف را وارد نمود. در ادامه محل تنظیمات Proxy Server برخی از نرم‌افزارهای معروف را نشان می‌دهیم.

Internet Explorer –

Tools ➔ Internet Options ➔ Connections ➔ LAN settings ➔ Use a proxy server ➔ Advanced



Fire Fox –

Tools ➔ Options➔ Advanced ➔ Network ➔ Settings

Internet Download Manager –

Options ➔ Proxy

Outlook: هنگام ساخت حساب جدید می‌توان تنظیمات را وارد نمود.

Cute FTP –

Edit ➔ Settings ➔ Connection ➔ Firewall

ICQ –

ICQ ➔ Menu Main ➔ Preferences ➔ Connection ➔ Server ➔ Use Firewall ➔ Proxy

- **MSN Messenger**

Tool ➔ Options ➔ Connection ➔ I use proxy server ➔ Type = SOCKS 5

- **Real Player**

View ➔ Preferences ➔ Proxy ➔ Streaming Settings ➔ Change Settings

- **Windows Media Player**

Tools ➔ Options ➔ Network ➔ Http ➔ Configure

- **AVG Update**

AVG ➔ Update Manager ➔ Settings ➔ Proxy ➔ User proxy server

- **Windows XP Update:** اگر آدرس سرور ۱۹۲.۱۶۸.۰.۱ باشد:

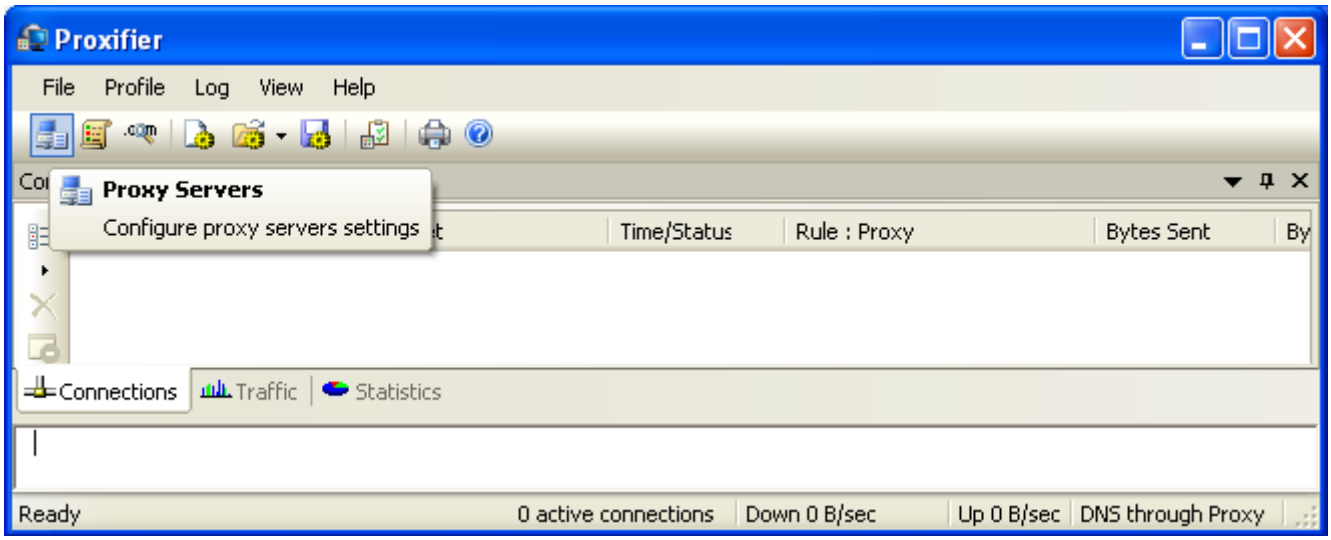
Command Prompt ➔ proxycfg -p 192.168.0.1:808

۱۶-۵-۳- نرم‌افزار مدیریت Client در استفاده از Proxy Server

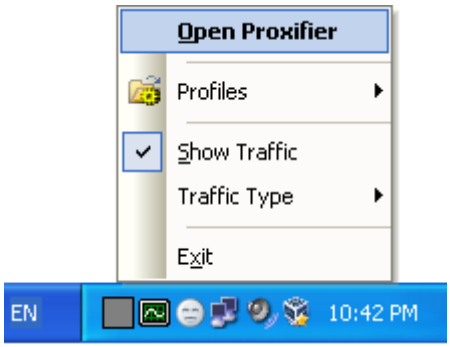
تا اینجا نحوه تنظیم کلاینت‌ها در مورد استفاده از Proxy Server مشخص شد. فرآیند کار بدین صورت بود که به ازاء هر نرم‌افزاری که می‌خواهد از اینترنت استفاده کند، وارد بخش تنظیمات Proxy آن می‌شدیم و سپس اطلاعات Proxy Server را وارد می‌نمودیم. اما مشکل بزرگی که در این کار وجود دارد، این است که در برخی نرم‌افزارها، اصلا بخشی برای تنظیمات Proxy Server وجود ندارد. در برخی دیگر نیز انجام این تنظیمات به دلیل مسائل امنیتی بسیار سخت می‌باشد. در مجموع این کار راحتی نیست که برای هر بار استفاده از Proxy Server، نرم‌افزارهای خود را تنظیم نماییم.

حالت مناسب و ایده آل این است که تنظیمات Proxy Server یک نقطه مرکزی را تغییر دهیم و با این کار، این تنظیمات روی تمامی نرم‌افزار هایی که از اینترنت استفاده می‌کنند اعمال شود؛ حتی نرم‌افزار هایی که قسمت تنظیمات Proxy Server را ندارند. خوشبختانه نرم‌افزار هایی برای انجام این کار ایجاد شده‌اند. نرم‌افزاری که در اینجا معرفی می‌کنیم، نرم‌افزار Proxifier V 3.0 است که حجم کمی دارد (حدود ۴ مگابایت) و به راحتی از اینترنت قابل دانلود می‌باشد (البته مانند CCProxy نیاز به Register شدن دارد). ویژگی مناسب نرم‌افزار Proxifier این می‌باشد که با انجام تنظیمات Proxy Server روی آن، از این پس هر نرم‌افزاری که قصد استفاده از اینترنت را داشته باشد، از این Proxy Server استفاده خواهد نمود و اینترنت خود را از Proxy Server مشخص شده دریافت خواهد کرد. مزیت دیگر این نرم‌افزار، قابلیت تعریف چندین Proxy Server می‌باشد. با این کار می‌توان اینترنت را همزمان از چندین Proxy Server دریافت نمود و این یعنی افزایش سرعت دسترسی به اینترنت و عدم اعمال بار زیاد روی یک Proxy Server خاص.

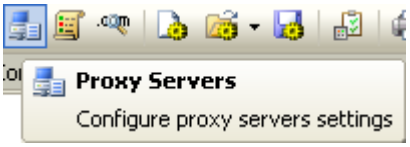
جهت استفاده از برنامه Proxifier، ابتدا آن را نصب نمایید. بعد از نصب برنامه و باز کردن آن، صفحه‌ای مانند صفحه زیر مشاهده خواهید نمود:



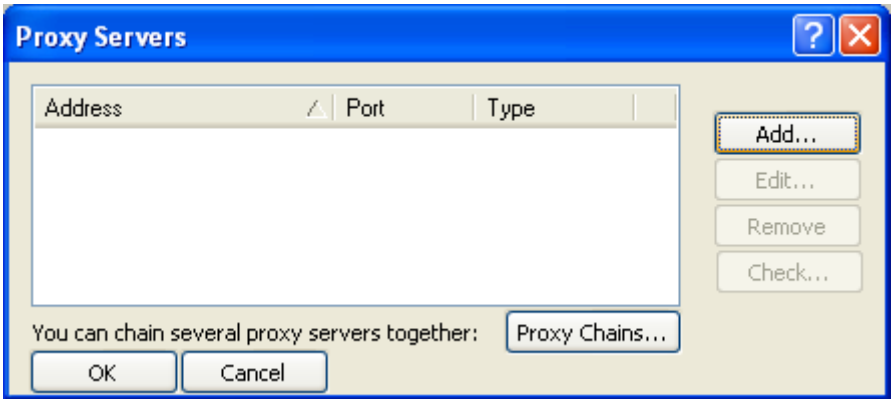
البته ممکن است که بعد از اجرای برنامه، برنامه به صورت خودکار Minimize شده و در System Try قرار گیرد. برای باز کردن آن به صورت زیر عمل نمایید:



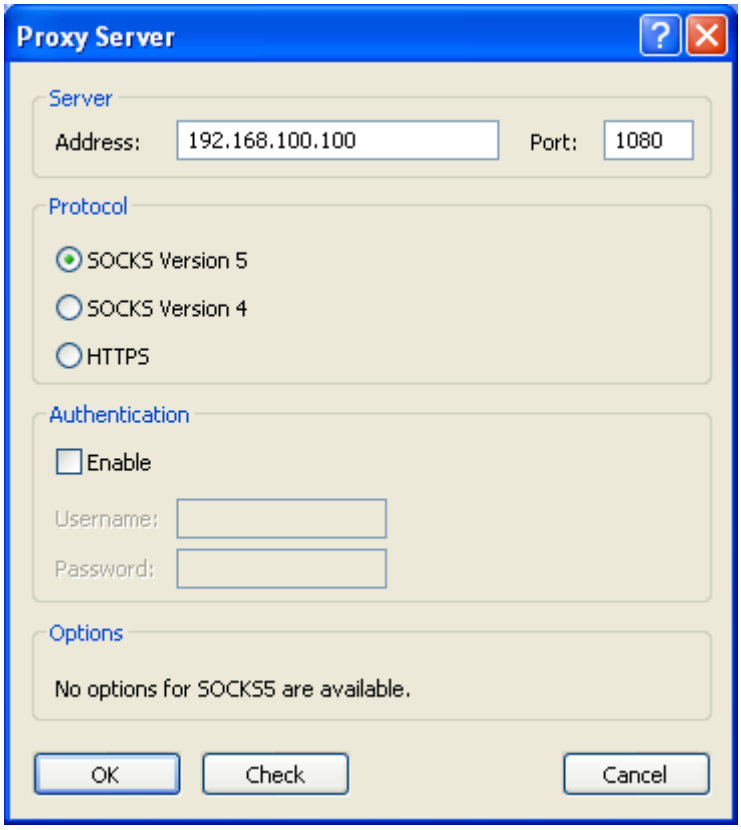
پس از باز شدن برنامه، وارد قسمت تنظیمات آن شوید. بدین منظور وارد بخش Proxy Servers شود:



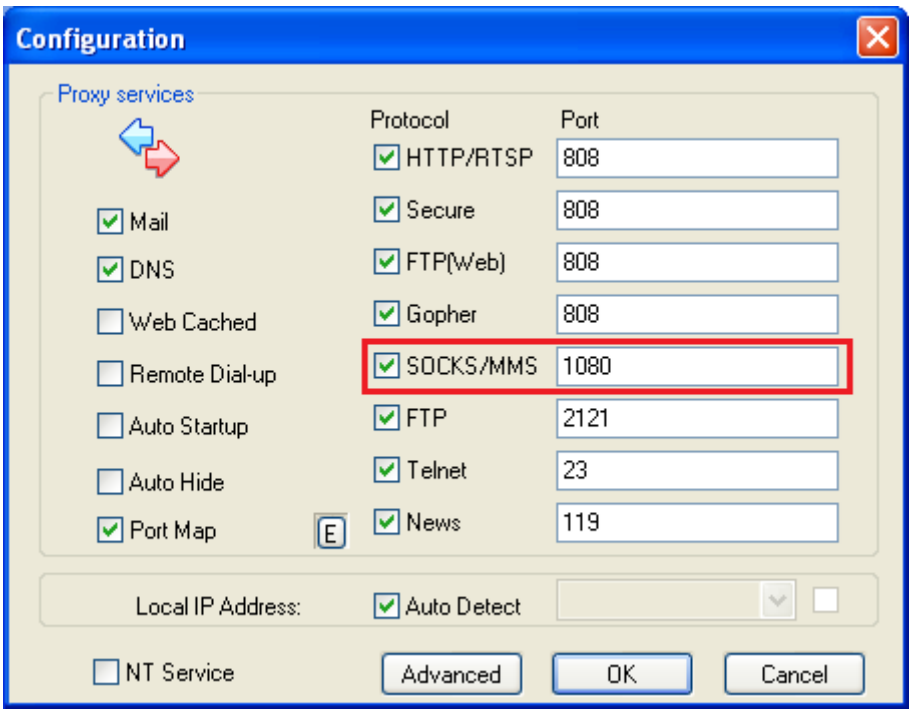
در صفحه باز شده می‌توانید لیستی از Proxy Serverهای ثبت شده را مشاهده نمایید (در این تصویر ما هنوز هیچ سروری اضافه نکرده ایم). جهت افزودن سرور جدید، روی دکمه Add کلیک نمایید.



در صفحه باز شده، در قسمت Address، آدرس IP کامپیوتر Proxy Server را وارد نمایید. در قسمت Port نیز آدرس پورت SOCKS/MMS که در نرم‌افزار CCProxy مشخص شده است را وارد نمایید. نوع پروتکل را نیز SOCKS Version 5 انتخاب کنید.

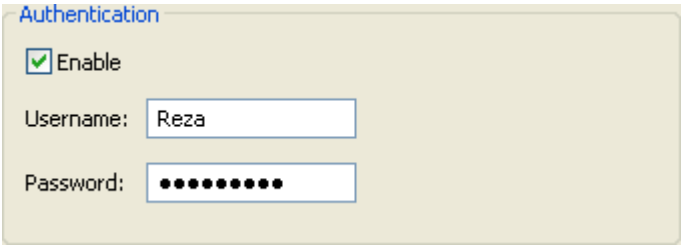


نکته بسیار مهم در شماره پورت است. **توجه: در اینجا بایستی شماره پورت SOCKS/MMS را وارد نمایید و نه شماره پورت HTTP.** برای یافتن این شماره پورت، وارد نرم‌افزار CCProxy شوید (همان نرم‌افزار سرویس پروکسی که در سرور اینترنت نصب شده است)، و از قسمت Options شماره پورت SOCKS/MMS را مشاهده نمایید. دقت فرمایید که این پورت فعال باشد.

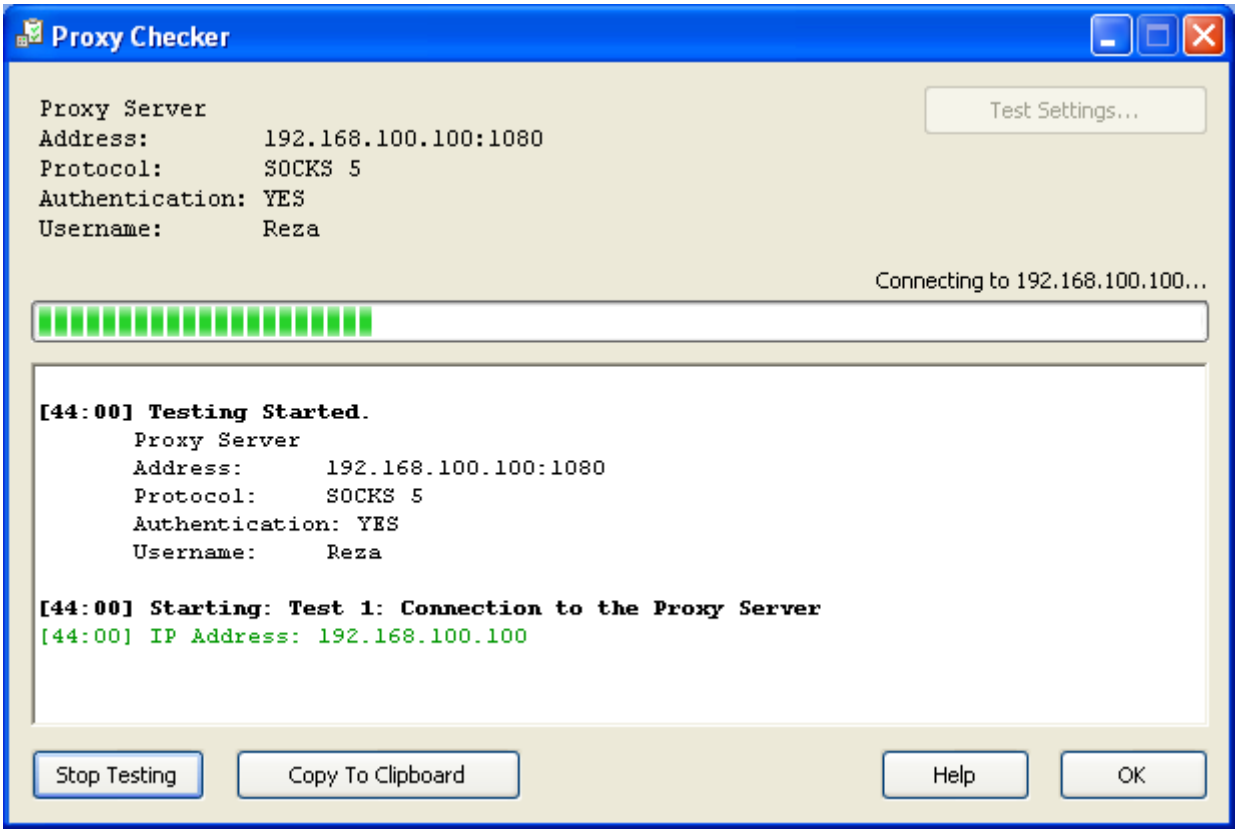


مجددا به نرم‌افزار Proxifier باز می‌گردیم. تا کنون مشخص نمودیم که سیستم ما به کدام سرور و به کدام پورت آن متصل شود؟ بحثی که باقی می‌ماند، تنظیم User Name و Password می‌باشد. اگر به یاد داشته باشید، در نرم‌افزار

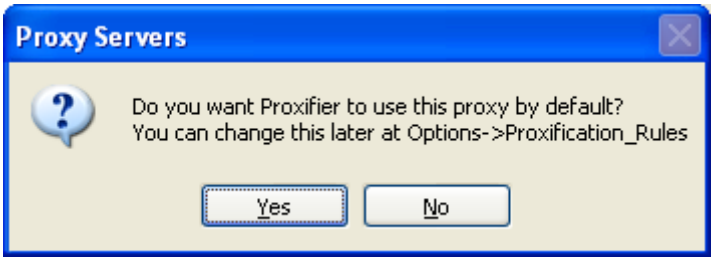
CCProxy این امکان وجود داشت که برای کاربران، User Name و Password تعریف نمود. یعنی تنها کاربرانی حق استفاده از اینترنت Share شده را داشته باشند که یک نام کاربری و رمز عبور داشته باشند. برای وارد کردن نام کاربری و رمز عبور، در نرم‌افزار Proxifier در همان صفحه افزودن سرور، نام کاربری و رمز عبور خود را در قسمت Authentication وارد نمایید.



اگر می‌خواهید از صحت تنظیمات خود مطلع شوید، در همین صفحه روی دکمه Check کلیک نمایید. با این کار صفحه کنترل صحت اتصال به Proxy Server باز می‌شود.



در نهایت، پس از افزودن سرور، سیستم از شما می‌پرسد که آیا این تنظیمات به عنوان تنظیمات پیش فرض ذخیره شود؟ سوال را تایید نماید.



با این کار، تنظیمات Proxy Server روی Client اعمال می‌شود و هر نرم‌افزاری که بخواهد از اینترنت استفاده کند، اینترنت خود را از Proxy Server تعیین شده دریافت خواهد نمود. **فقط به یاد داشته باشید که نرم‌افزار Proxyfier را هیچ گاه نبندید؛** زیرا با اینکار، تمامی نرم‌افزارها مانند حالت معمولی از اینترنت استفاده خواهند نمود و دیگر کاری به Proxy Server نخواهند داشت.

۱۶-۶- آموزش عملی روش NAT یا ICS

در ادامه چگونگی به اشتراک گذاری اینترنت از طریق ICS را توضیح می‌دهیم.

سیستم مایکروسافت موسوم به ICS محدودیت تعداد کلاینت ندارند و این یکی از بارز ترین ویژگی‌های این سیستم هست. هرچند برای شبکه‌های بالای ۵ کلاینت همیشه پیشنهاد می‌شود تا از سیستم‌های سروری (Proxy Server) استفاده کرد، اما ICS توانایی کنترل شبکه‌های کوچک را به خوبی دارد.

روش پیاده سازی ICS در تمام شبکه‌ها یکسان است، پس با این حساب اصلا مهم نیست شبکه شما Wireless هست یا سیمی، با اینکه اینترنت شما چگونه به دست شما میرسد.

۱۶-۶-۱- شروع به کار

شما از هر طریقی که اینترنت را دریافت کنید، (چه Wireless چه ADSL چه ISDN و...) سر انجام باید کارت شبکه‌ای به آن اختصاص یافته باشد.

نکته: گاهی پیش می‌آید که مودم‌های ADSL از طریق پورت USB به سیستم متصل می‌شوند، اما اگر دقت کنید در بخش تنظیمات ویندوز برای آن نیز یک کارت شبکه (حتی به صورت مجازی) وجود دارد.

نکته: در بعضی از مودم‌های ADSL که امروزه وجود دارند تنظیمات از طریق Connectionهایی مانند Dial-up تنظیم می‌شوند که البته بازهم تاثیری در روند کار ندارد. شما آن را به حکم یک کارت شبکه بشناسید.

نکته: برای ICS اصلا لزوم داشتن IP Public (به اصطلاح عامیانه Valid) یا Static وجود ندارد.

سرور: در بحث Share کردن اینترنت، سرور را به کامپیوتری خواهیم گفت که یک ویندوز XP بر روی آن نصب شده و قرار است کار اشتراک گذاری اینترنت را برای کلاینت‌ها انجام دهد. (این لفظ به معنای این نیست که شما یک ویندوز سرور احتیاج دارید)

شما برای شبکه خود مجبور هستید از یک کارت شبکه استفاده کنید (بسته به شبکه سیمی یا بی‌سیم). پس شما دو کارت شبکه در سرور خواهید داشت.

۱. کارت شبکه‌ای که اینترنت به آن وصل شده است. (به نکته اول و دوم در همین صفحه دقت کنید)

۲. کارت شبکه‌ای که به شبکه داخلی متصل است. (حال می‌تواند این شبکه فقط یک کامپیوتر دیگر باشد.)

کارت شبکه اینترنت: این لفظ را از این پس در مورد کارت شبکه‌ای به کار می‌بریم که به اینترنت متصل است.

کارت شبکه داخلی: این لفظ را از این پس در مورد کارت شبکه‌ای به کار می‌بریم که به شبکه داخلی (یا کامپیوتر مجاور به هر طریقی) متصل است.

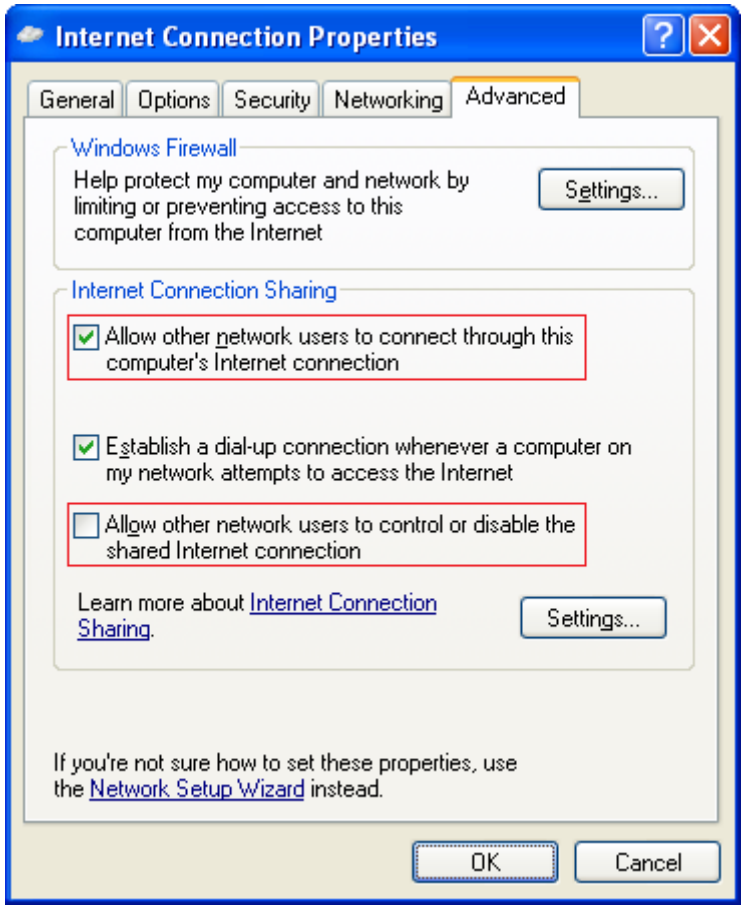
۱۶-۶-۲- مراحل راه اندازی

۱. از Control Panel وارد Network Connection شوید.

۲. بر روی کارت شبکه اینترنت راست کلیک کنید و سپس گزینه Properties را کلیک کنید.

۳. از سربرگ‌های موجود، سربرگ Advanced را انتخاب کنید. (در ویندوز ویستا و ویندوز ۷، این سربرگ به Sharing تغییر نام پیدا کرده است)

۴. در صفحه موجود در بخش Internet Connection Sharing، تیک Allow other network users to connect through this computer's Internet connection تا بزنید.



چند نکته که در راه اندازی ICS باید آنرا حتما رعایت کنید:

- اگر از چند کارت شبکه در کامپیوتر استفاده می‌کنید، شما می‌توانید از ICS تنها برای یک کارت شبکه داخلی استفاده کنید. در این صورت از منوی Home Networking Connection شبکه مورد نظر را انتخاب کنید.
- اگر به اعضای (کلاینت) شبکه اطمینان ندارید، تیک Allow other network users to control or disable the Shared internet connection را حتما بردارید.

مرحله مهم: بعد از فعال شدن ICS، کارت شبکه داخلی (همانی که قرار است از اینترنت Share شده استفاده کنند) و تمام کارت شبکه هایی که قرار است از اشتراک اینترنت استفاده کنند را در حالت Obtain an IP Address Automatically قرار دهید.

حال کارت شبکه داخلی خود را یک بار خاموش/روشن کنید (Disable/Enable) کرده و منتظر باشید که کارت شبکه IP بگیرد (اگر حالش را ندارید، کامپیوتر کلاینت را یکبار Restart کنید).

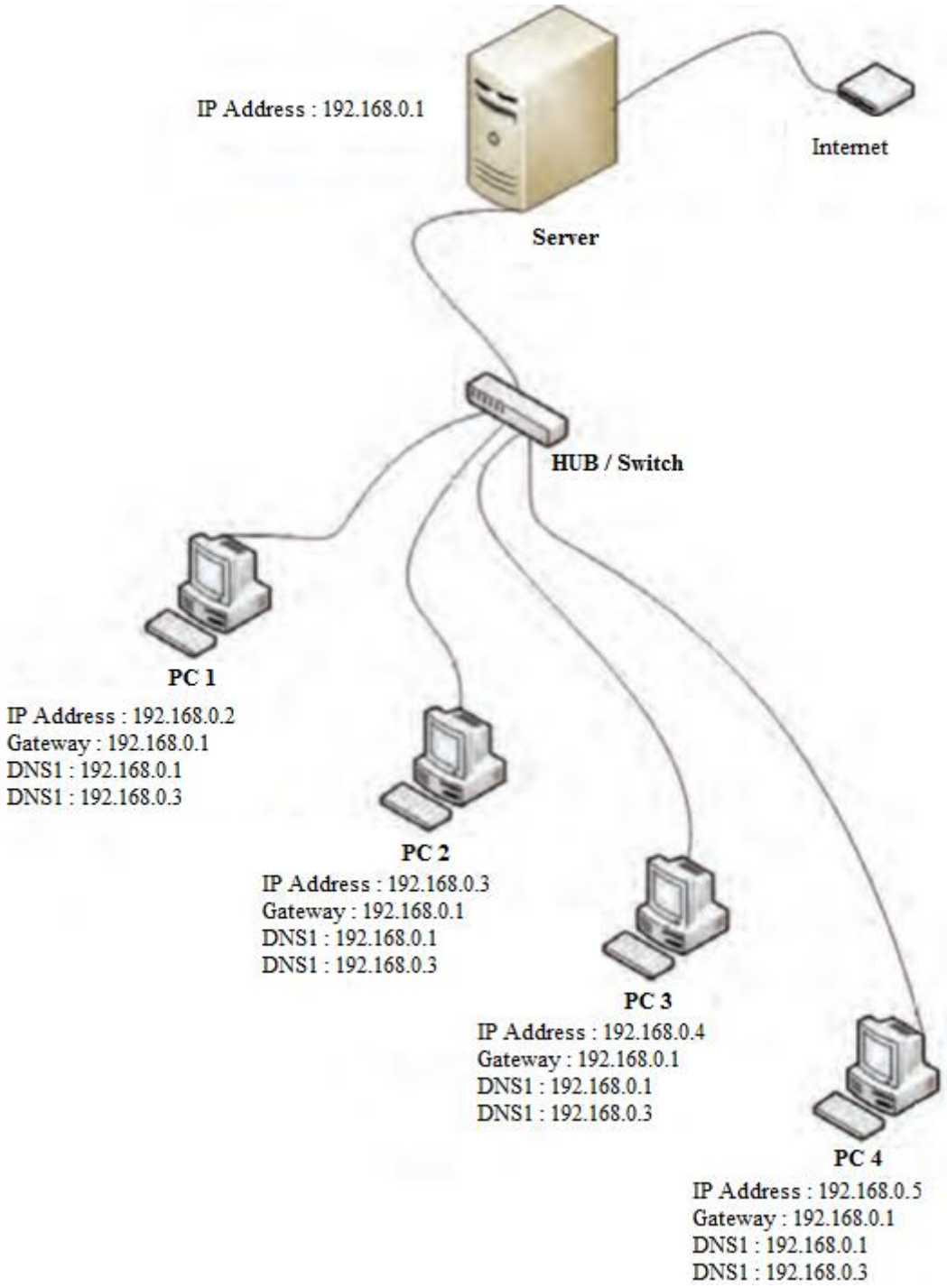
نکته: مطمئن شوید در صورتی که کارت شبکه‌های متفاوتی در سیستم دارید هیچ کدام از محدوده ۱۹۲.۱۶۸.۰.۰ نباشند.

کارت شبکه اینترنت شما در سرور حتما باید آدرس ۱۹۲.۱۶۸.۰.۱ را بگیرد (این کار به صورت خودکار انجام می‌گیرد) و به این ترتیب خود به بقیه کارت شبکه‌ها نیز IP می‌دهد که تماما از همین محدوده هستند. **البته اگر می‌خواهید آدرس‌دهی IP به صورت خودکار صورت نگیرد، IP کامپیوتر سرور را به صورت دستی تنظیم نمایید، سپس در کامپیوتر هایی که می‌خواهید از اینترنت استفاده کنند، آدرس Default Gateway آن‌ها را برابر با آدرس سرور قرار دهید (یعنی اگر آدرس سرور به صورت خودکار به ۱۹۲.۱۶۸.۰.۱ تغییر یافت، تمامی کلاینت‌ها نیز بایستی آدرس Gateway خود را به ۱۹۲.۱۶۸.۰.۱ تغییر دهند).** به یاد آورید که با تنظیم Gateway به سیستم می‌گفتیم که تمامی درخواست‌های خود را به سمت این کامپیوتر بفرستد.

به همین ساده گی اینترنت به صورت کامل به اشتراک گذاشته شد.

نکته: ممکن است در شروع کار ICS کمی کندی در روند اشتراک گذاری اینترنت مشاهده شود که به مرور زمان حل خواهد شد. (گاهی اوقات زمان زیادی می‌برد تا یک سایت باز شود و شما مجبور هستید بارها Refresh بزنید، اما مطمئنا پس از مدتی به صورت روان فعالیت خواهد کرد.)

شکل زیر، روند اشتراک گذاری اینترنت را بهتر نشان می‌دهد:


IP Address : 192.168.0.1
Internet
Server
HUB / Switch
PC 1
IP Address : 192.168.0.2
Gateway : 192.168.0.1
DNS1 : 192.168.0.1
DNS1 : 192.168.0.3
PC 2
IP Address : 192.168.0.3
Gateway : 192.168.0.1
DNS1 : 192.168.0.1
DNS1 : 192.168.0.3
PC 3
IP Address : 192.168.0.4
Gateway : 192.168.0.1
DNS1 : 192.168.0.1
DNS1 : 192.168.0.3
PC 4
IP Address : 192.168.0.5
Gateway : 192.168.0.1
DNS1 : 192.168.0.1
DNS1 : 192.168.0.3

فصل ۱۷

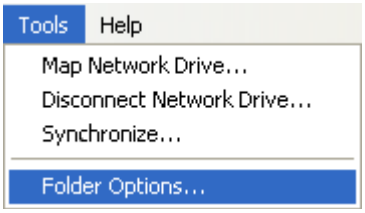
امنیت فایل‌ها و پوشه ها

۱۷-۱- انواع امنیت

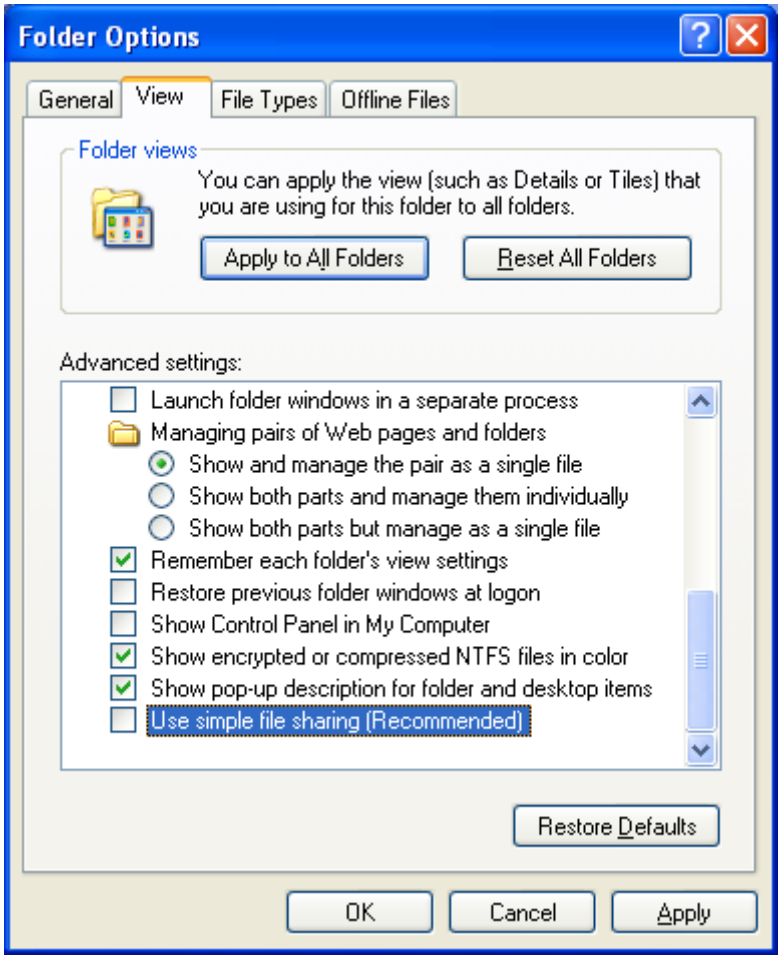
در فصل "راه اندازی شبکه‌های Workgroup" با نحوه به اشتراک گذاری اطلاعات و نیز نحوه ایجاد امنیت روی فایل‌های Share شده آشنا شدید. به عنوان مثال تعیین نمودید که در دسترسی به یک پوشه به نام TestFile، کاربری به نام Ali هیچگونه محدودیتی نداشته باشد، اما کاربری به نام Reza، فقط قابلیت دسترسی Read Only داشته باشد و قابلیت تغییر محتوای این پوشه را نداشته باشد. حال کاری که در عمل رخ می‌داد این بود که این محدودیت روی کاربر Reza فقط در حالت Sharing اعمال می‌شد. بدین معنا که اگر کاربر Reza به صورت محلی به سیستم Login می‌کرد، قابلیت تغییر پوشه TestFile را داشت. اما اگر کاربر Reza از طریق شبکه و به صورت Remote بخواهد به گوشه Share شده دسترسی داشته باشد، در اینصورت فقط قابلیت مشاهده پوشه را خواهد داشت؛ اما قابلیت تغییر اطلاعات این پوشه را ندارد. به عبارت دیگر این محدودیت در حالت Remote اعمال می‌شود و در حالت دسترسی Local این محدودیت اعمال نخواهد شد. اما در این فصل قصد داریم، گامی فراتر از این سطح امنیت برداریم و امنیت پوشه‌ای خاص (مثلاً TestFile) را به گونه‌ای تعیین نماییم، که کاربری به اسم Reza، چه به صورت Local و چه به صورت Remote خواست از این پوشه استفاده کند، یا قابلیت بازکردن پوشه را نداشته باشد یا فقط بتواند آن را به صورت Read Only باز کند.

۱۷-۲- تنظیمات امنیتی

برای رسیدن به این هدف (ایجاد تنظیمات امنیتی روی پوشه)، در گام اول بایستی تنظیمات و سرویس Sharing & Security را در ویندوز XP فعال کنید (این تنظیم در ویندوز سرور به صورت پیش فرض فعال است اما در ویندوز XP به صورت پیش فرض فعال نیست). بدین منظور ابتدا وارد My Computer شده، سپس از منوی Tools گزینه Folder Option را انتخاب نمایید.



سپس وارد سربرگ View شده و تیک گزینه آخر یعنی گزینه Use Simple File Sharing را بردارید.



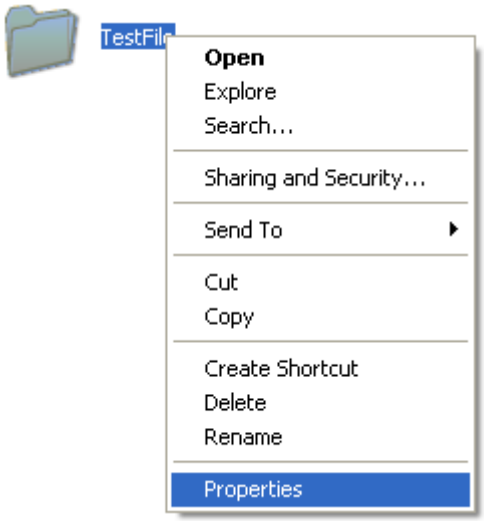
حال نوبت به ایجاد امنیت روی پوشه‌ای به نام TestFile می‌شود.



فرض کنید در این پوشه، فایلی به نام Sample Text.txt ایجاد کرده‌ایم تا تاثیر حالت امنیت Read Only را ببینیم.

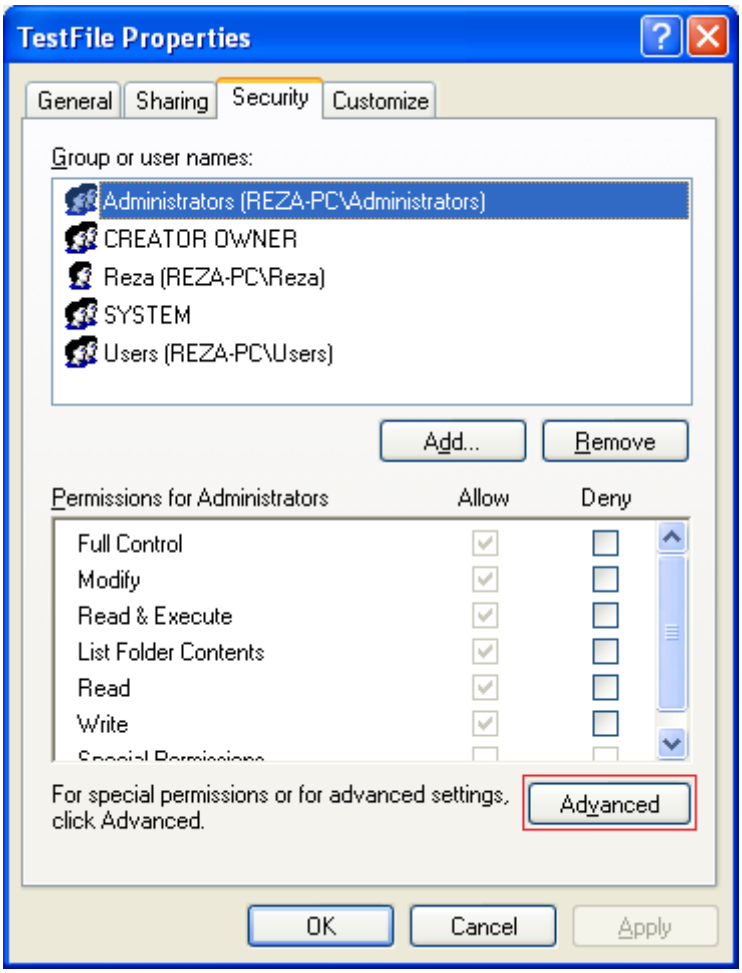


حال برای ایجاد امنیت، روی پوشه مورد نظر راست کلیک کرده و گزینه Properties را انتخاب کنید. (توجه: روی پوشه راست کلیک کنید و نه روی فایل، البته این امنیت گذاری روی فایل نیز جواب می‌دهد.)

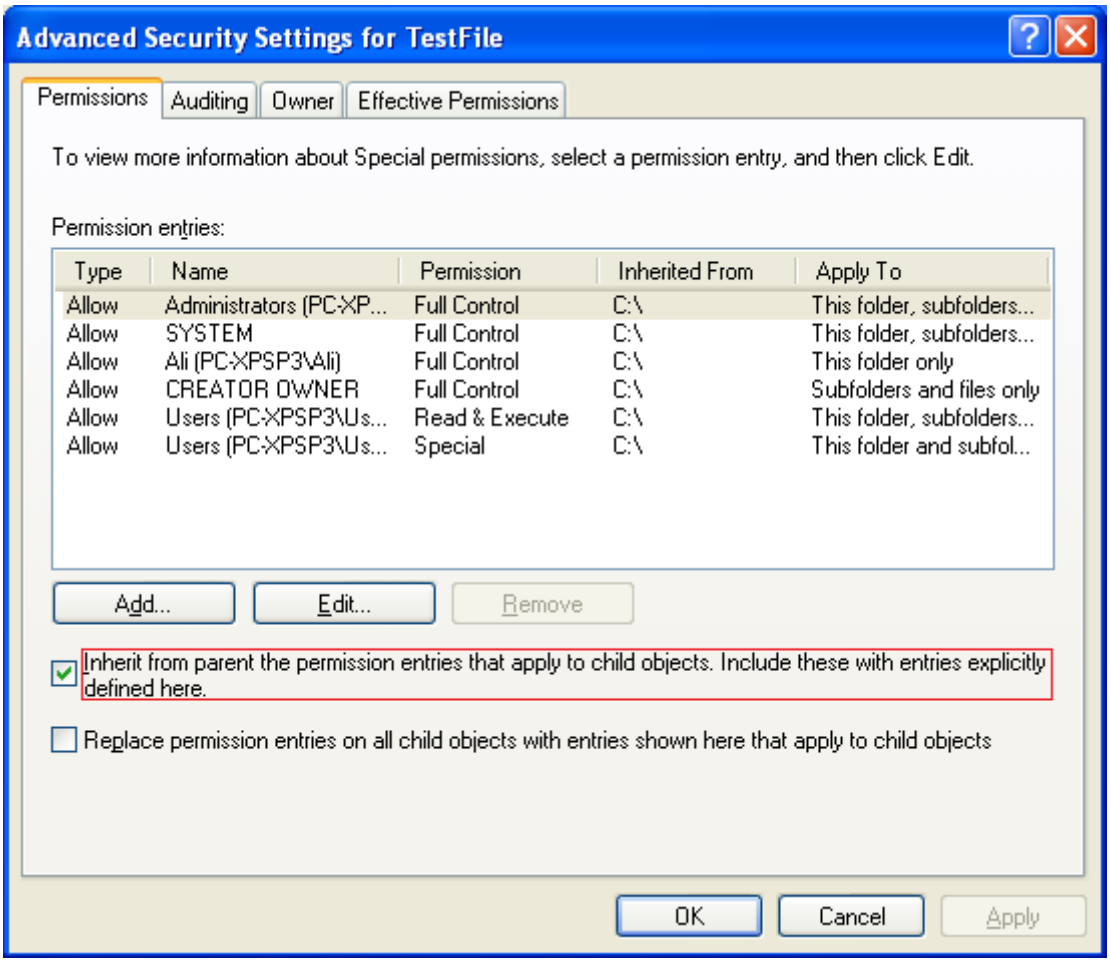


در صفحه باز شده، ابتدا وارد سربرگ Security شوید. در بالای صفحه اسامی کاربرانی که دسترسی آن‌ها به این پوشه اجازه داده شده است (Allow) یا دسترسی آن‌ها منع شده است (Deny) را مشاهده می‌نمایید.

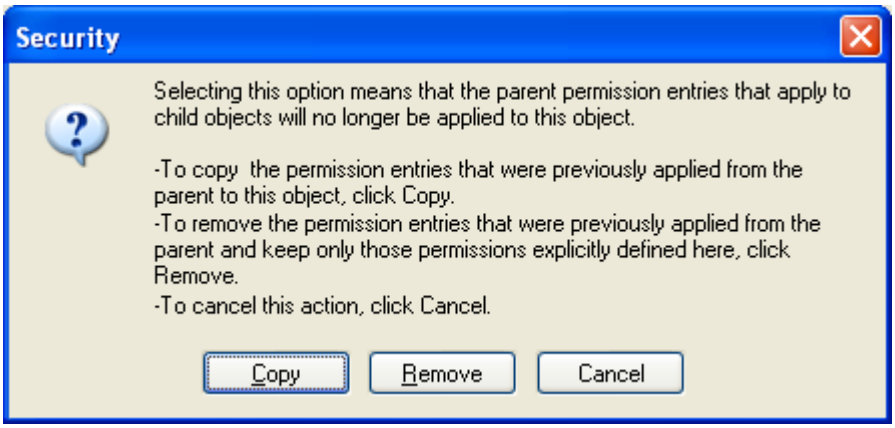
برای ایجاد امنیت روی دکمه Advanced کلیک کنید.



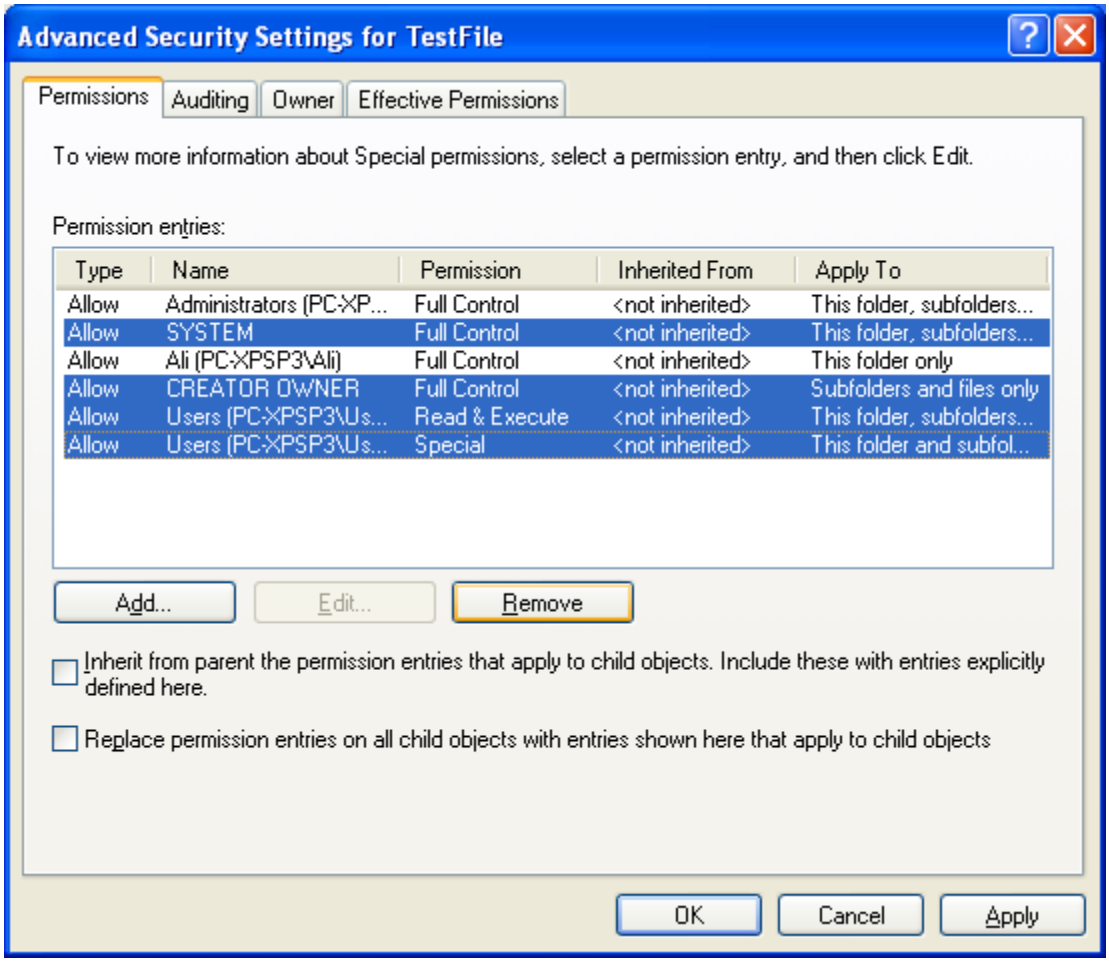
در صفحه باز شده، شما مجددا لیست دسترسی‌ها را با ظاهری متفاوت مشاهده خواهید نمود. در مرحله اول ابتدا تیک گزینه …Inherit from parent the permission را بردارید.



در سوالی که از شما می‌پرسد، گزینه Copy را انتخاب نمایید. در این صفحه، سیستم به شما می‌گوید که تنظیمات امنیتی را از حالت ارث بری برداشته (ارث بری را در انتهای فصل توضیح داده ایم) و سپس آن تنظیمات را به خود پوشه نسبت دهید (کپی کنید).



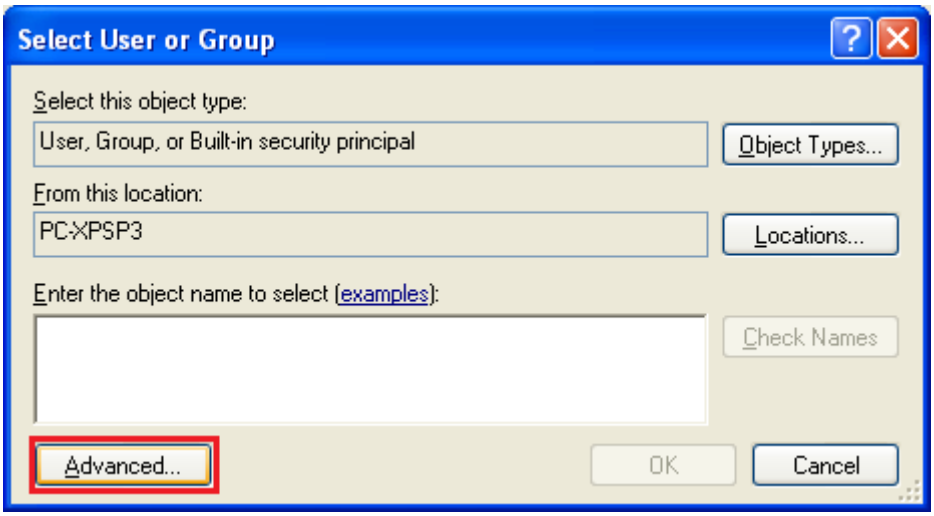
در صفحه تنظیمات دسترسی، فقط کاربرانی که می‌خواهید به این پوشه دسترسی داشته باشند را حفظ کرده و بقیه را حذف نمایید. بدین منظور، کاربرانی که می‌خواهید حذف کنید را انتخاب کرده و سپس روی دکمه Remove کلیک کنید. در این مثال، ما فقط دو کاربر Ali و Administrator را نگه داشته و بقیه را حذف کرده‌ایم.



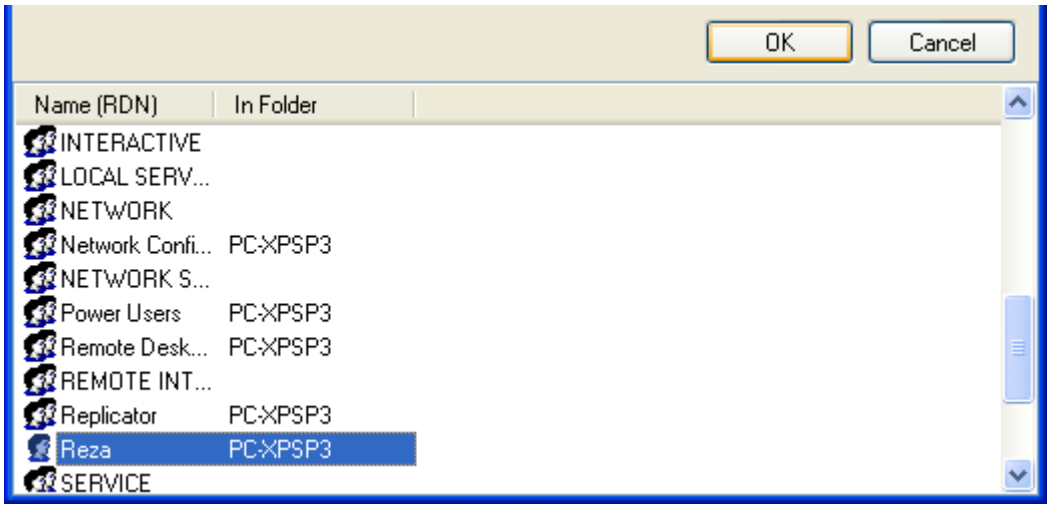
پس از OK کردن، مشاهده خواهید کرد که فقط دو کاربر Ali و Administrator باقی می‌مانند.

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (PC-XP...	Full Control	<not inherited>	This folder, subfolders...
Allow	Ali (PC-XPSP3\Ali)	Full Control	<not inherited>	This folder only

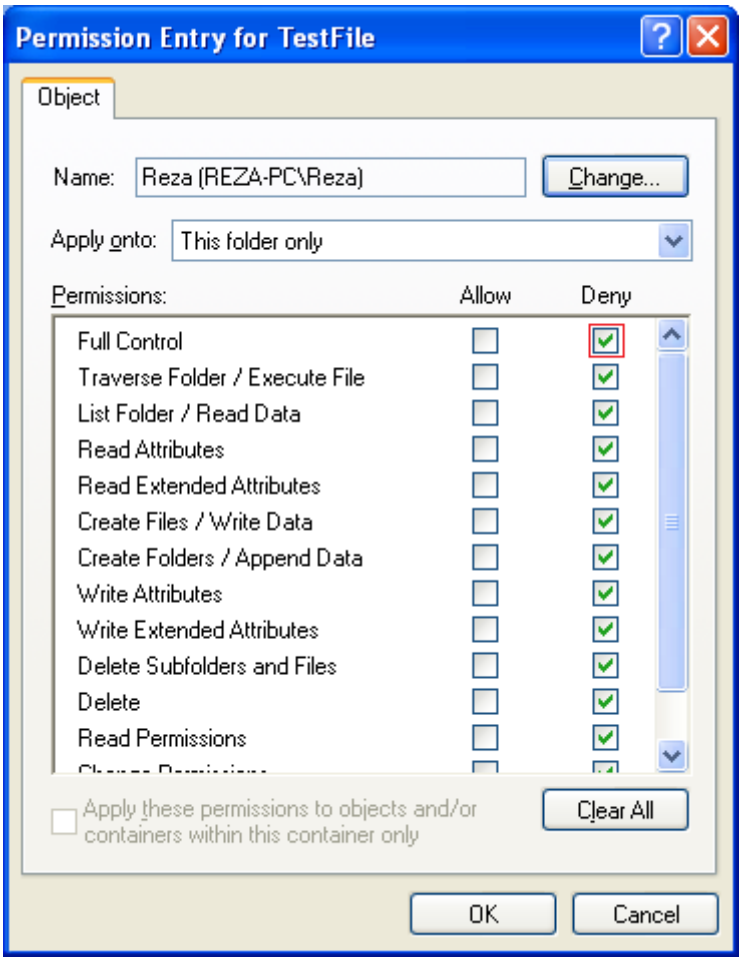
حال می‌خواهیم دسترسی کاربری مانند Reza را از این پوشه بگیریم. بدین منظور در همین صفحه ابتدا روی دکمه Add کلیک کنید. در صفحه باز شده برای انتخاب کاربر Reza، روی دکمه Advanced کلیک کنید.



در صفحه باز شده، ابتدا روی دکمه Find کلیک کنید تا لیست تمام کاربران به نمایش درآید. سپس کاربر Reza را انتخاب کرده و سپس دو مرتبه روی OK کلیک کنید.



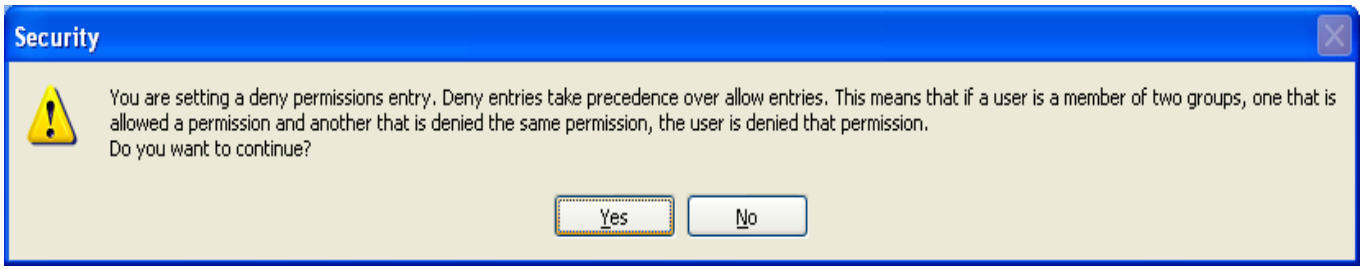
پس از OK کردن، صفحه‌ای مانند صفحه زیر نمایان می‌شود که در آن می‌توانید سطح دسترسی کاربر Reza را تعیین نمایید. در این صفحه دو کلمه دارید به نام Allow و Deny. ستون Allow برای دادن اجازه دسترسی و ستون Deny گرفتن اجازه دسترسی است. در این مثال ما گزینه Full Control را روی Deny تنظیم کرده‌ایم. بدین معنی که کاربر Reza هیچگونه دسترسی به این گوشه ندارد. در نهایت روی OK کلیک کنید.



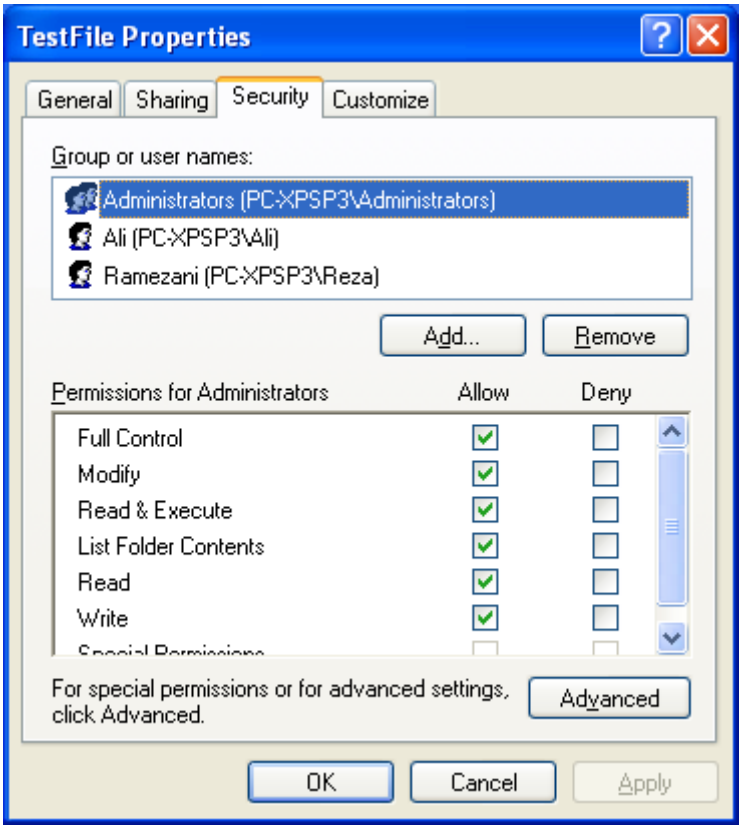
سپس مشاهده خواهید کرد که کاربر Reza نیز به لیست زیر و با نوع دسترسی Deny اضافه می‌شود. مجددا OK کنید.

Type	Name	Permission	Inherited From	Apply To
Deny	Ramezani (PC-XPSP...	Full Control	<not inherited>	This folder, subfolders...
Allow	Administrators (PC-XP...	Full Control	<not inherited>	This folder, subfolders...
Allow	Ali (PC-XPSP3\Ali)	Full Control	<not inherited>	This folder only

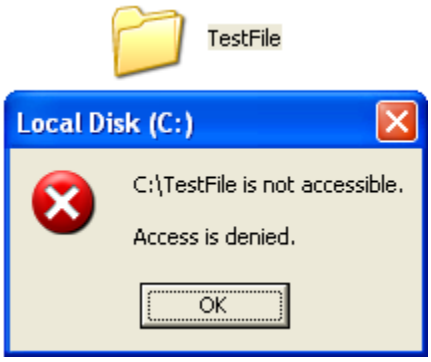
پس از OK کردن، سیستم از شما سوالی می‌پرسد؛ روی Yes کلیک کنید.



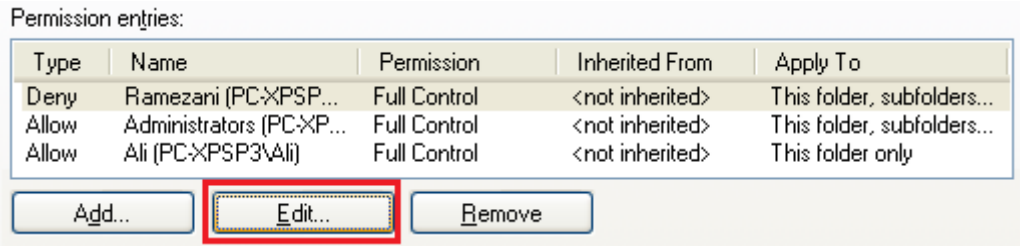
حال می‌بینید که کاربر Reza به لیست کاربران این پوشه اضافه می‌شود. در این صفحه هم کاربرانی که دسترسی Allow و هم کاربرانی که دسترسی Deny دارند را مشاهده می‌کنید. مجددا روی OK کلیک کنید.



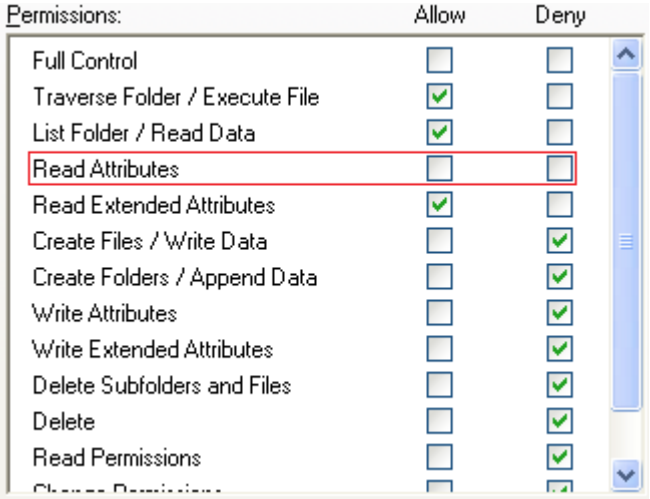
حال نوبت به دیدن تاثیر این سطح دسترسی می‌رسد. بدین منظور ابتدا از سیستم Log Out کرده و با کاربر Reza به سیستم Login کنید. مشاهده خواهید نمود که هنگام ورود به این پوشه، سیستم اجازه ورود شما را خواهد گرفت و پیام Access is Denied را مشاهده خواهید نمود.



حال می‌خواهیم به کاربر Reza اجازه دسترسی بدهیم، اما به صورت Read Only. بدین منظور از سیستم Log Out کرده و با کاربر Ali مجددا به سیستم Log In کنید. وارد صفحه تنظیمات امنیتی پوشه TestFile شده، کاربر Reza را انتخاب کرده و روی Edit کلیک کنید.



در صفحه باز شده فقط گزینه‌های مربوط به "دسترسی خواندنی" را Allow کرده و بقیه دسترسی هایی که مربوط به عملیات ویرایشی است را Deny کنید. اگر به شکل دقت کنید، گزینه Read Attributes نه در حالت Allow قرار دارد و نه در حالت Deny. حال به نظر شما سیستم کدام حالت را انتخاب می‌کند؟ جواب این است که سیستم از حالت **ارث بری** استفاده می‌کند. بدین معنی که فرض کنید این پوشه Test نام داشته و در ریشه درایو C:\ قرار دارد. حال اگر درایو C:\ برای دسترسی Read Attributes، حالت Allow را انتخاب کرده باشد، حالت Allow برای این پوشه نیز اعمال خواهد شد؛ در غیر اینصورت حالت Deny روی این گوشه اعمال خواهد شد. همچنین اگر این پوشه در مسیر C:\Folder1 باشد، دسترسی Read Attributes ابتدا از پوشه Folder1 خوانده می‌شود. اگر این صفت برای Folder1 نیز تعریف نشده باشد، آنگاه این سطح دسترسی از درایو C:\ خوانده خواهد شد.



توجه نمایید که در این روش امنیت گذاری، کاربر Reza چه به صورت محلی و چه به صورت راه دور به سیستم Login کنید، این محدودیت روی وی اعمال خواهد شد. بر عکس حالت امنیت Sharing که فقط در حالت دسترسی به فایل Share شده و از راه دور اعمال می‌شود.

فصل ۱۸

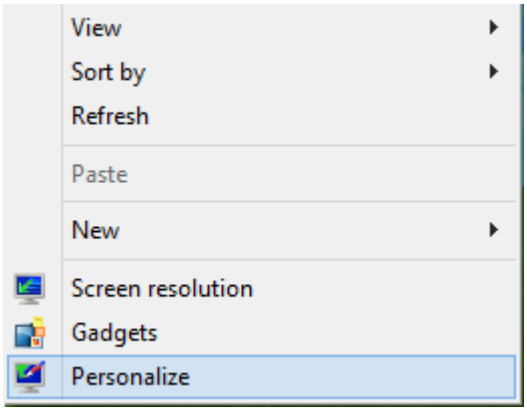
راه‌اندازی شبکه در ویندوز ۸

۱۸-۱- مقدمه

در فصل‌های گذشته در مورد شبکه سازی در ویندوز XP و مفاهیم مرتبطه صحبت شد و با کارهای مورد نیاز عملی مانند تغییر آدرس IP و تغییر نام کامپیوتر، به اشتراک گذاری پوشه‌ها، سطوح امنیتی اشتراک، نگاشت درایو شبکه و... آشنا شدید. در این فصل چگونگی انجام همین امور در ویندوز ۸ به صورت مختصر مورد بحث قرار خواهد گرفت.

۱۸-۲- آیکن My Computer

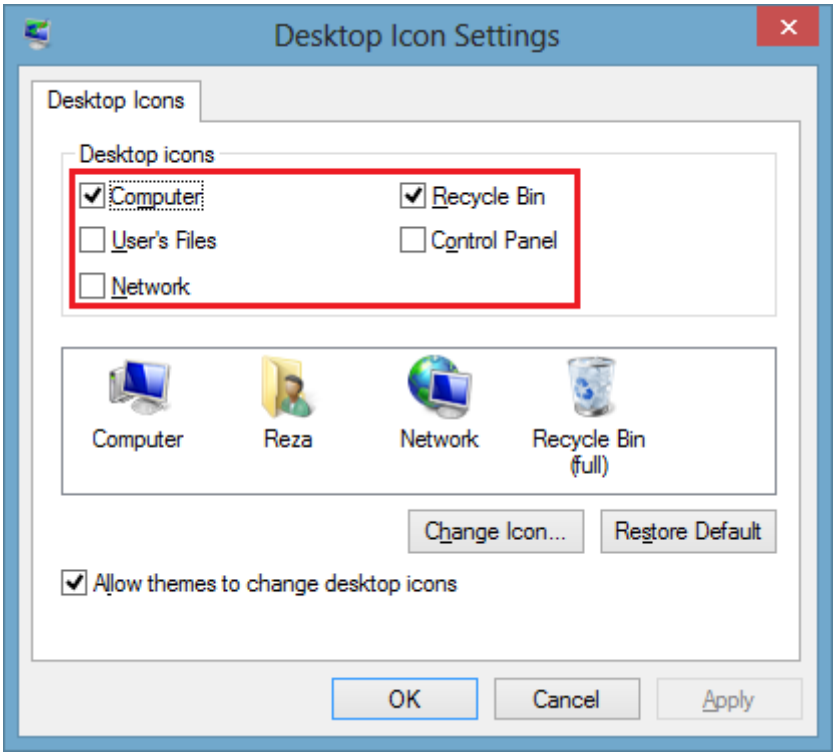
در ویندوز ۸، به صورت پیش فرض آیکن My Computer روی صفحه دسکتاپ قرار ندارد و خود بایستی آن را روی این صفحه قرار دهید. بدین منظور روی صفحه دسکتاپ راست کلیک کرده و روی گزینه Personalize کلیک کنید.



در صفحه بازشده روی دکمه Change Desktop Icons کلیک کنید.



سپس آیکن هایی که می‌خواهید روی صفحه دسکتاپ به نمایش در بیاید را انتخاب نموده و در نهایت روی OK کلیک کنید.



۱۸-۳- اتصال به شبکه

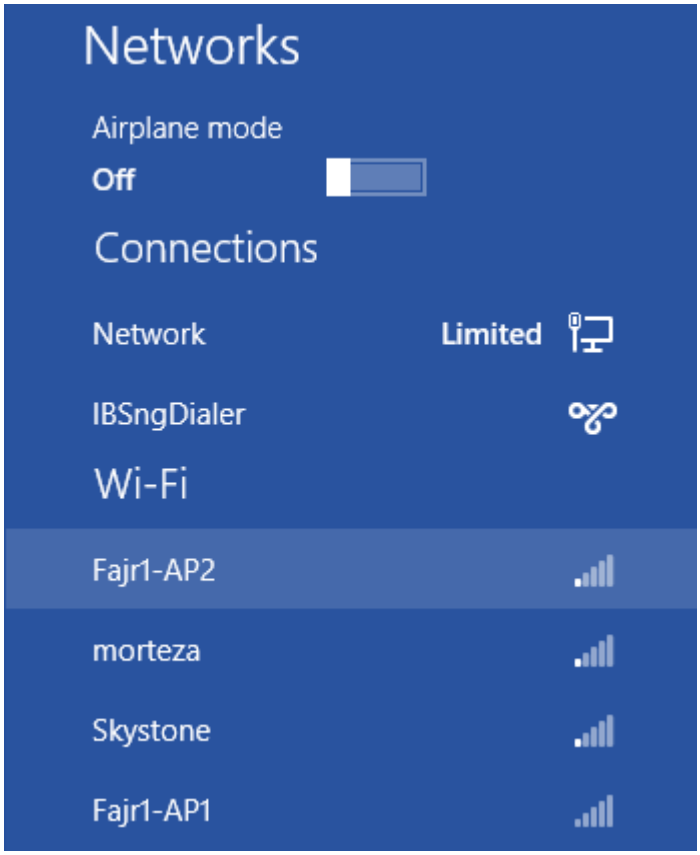
اولین گام در شبکه سازی ویندوز ۸، اتصال آن به شبکه‌ای خاص است. ممکن است این اتصال به صورت سیمی باشد یا به صورت بی‌سیم. اگر اتصال سیمی برقرار نمودید، آیکن شبکه شما بدون هیچگونه تنظیمات خاصی به شکل زیر در می‌آید:



اما اگر می‌خواهید به شبکه‌ای بی‌سیم متصل شوید، روی آیکن شبکه کلیک کنید.

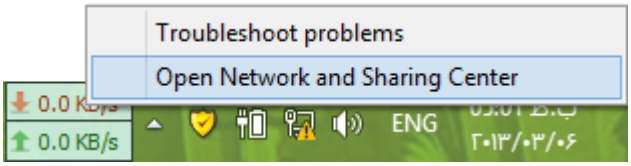


سپس شبکه مورد نظر بی‌سیم خود را انتخاب نمایید. اگر هنگام از شما رمز عبور خواست، رمز عبور تعیین شده برای آن شبکه را وارد نمایید.



۱۸-۴- مشاهده اتصالات شبکه

جهت ورود به صفحه تنظیمات شبکه، ابتدا روی آیکن شبکه راست کلیک نموده و سپس گزینه Open Network and Sharing Center را انتخاب کنید.



در صفحه به نمایش در آمده می‌توانید قسمت‌های مختلف مربوط به شبکه را تنظیم نمایید. در شکل، قسمت‌های مختلف با عدد بیان شده‌اند. معانی این اعداد بدین صورت است:

۱- مشاهده آداپتورها و اتصالات شبکه

۲- تعیین تنظیمات پیشرفته "به اشتراک گذاری"

۳- ساخت شبکه‌های Workgroup یا Homegroup

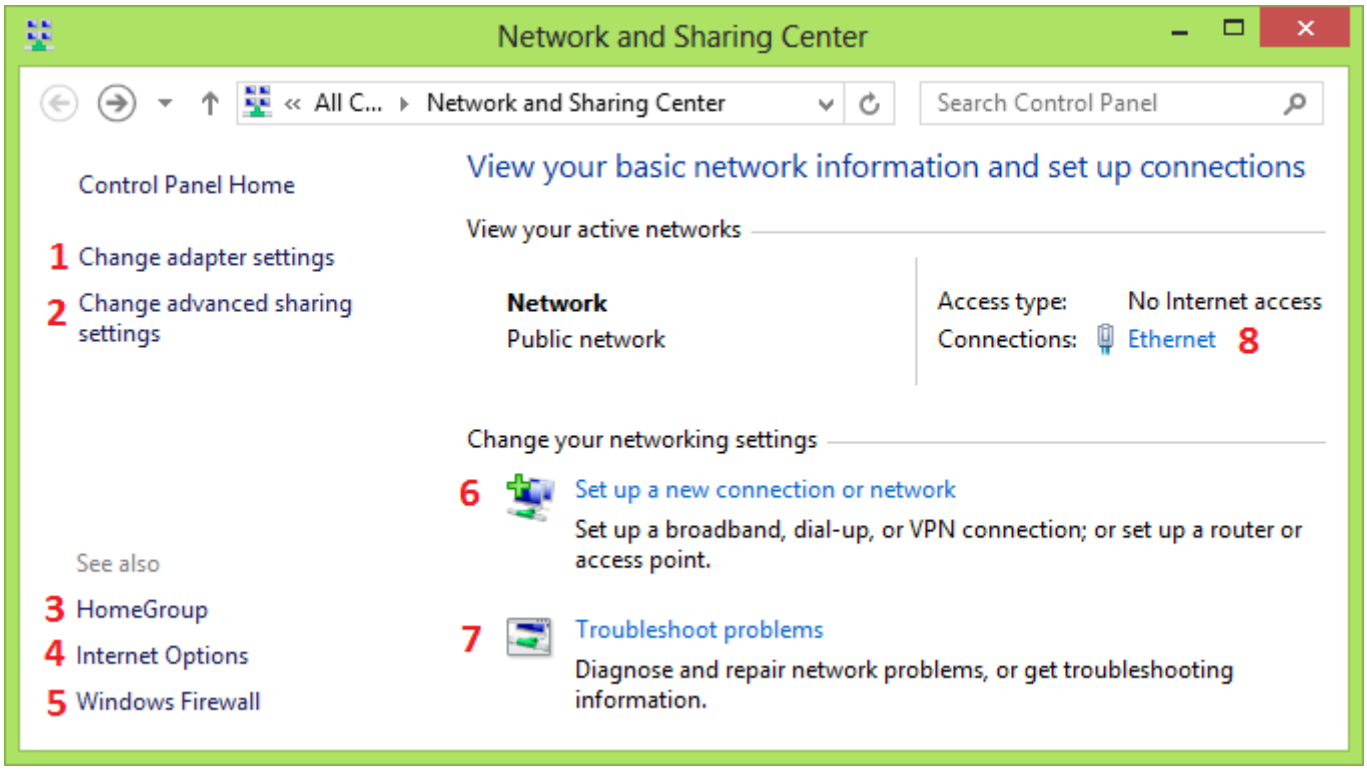
۴- تنظیمات اینترنت مربوط به Internet Explorer

۵- تنظیمات Firewall

۶- ایجاد اتصالات شبکه‌ای و اینترنت

۷- عیب یابی شبکه

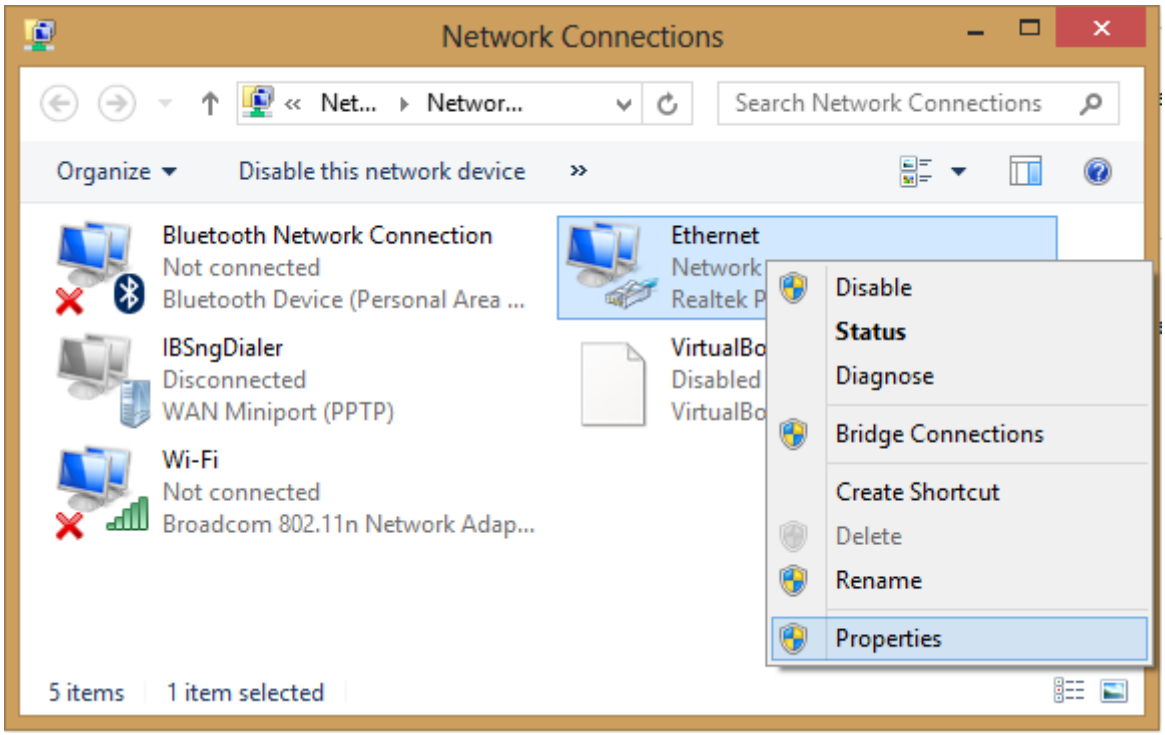
۸- اتصالات شبکه‌ای فعال فعلی



صفحه تنظیمات شبکه

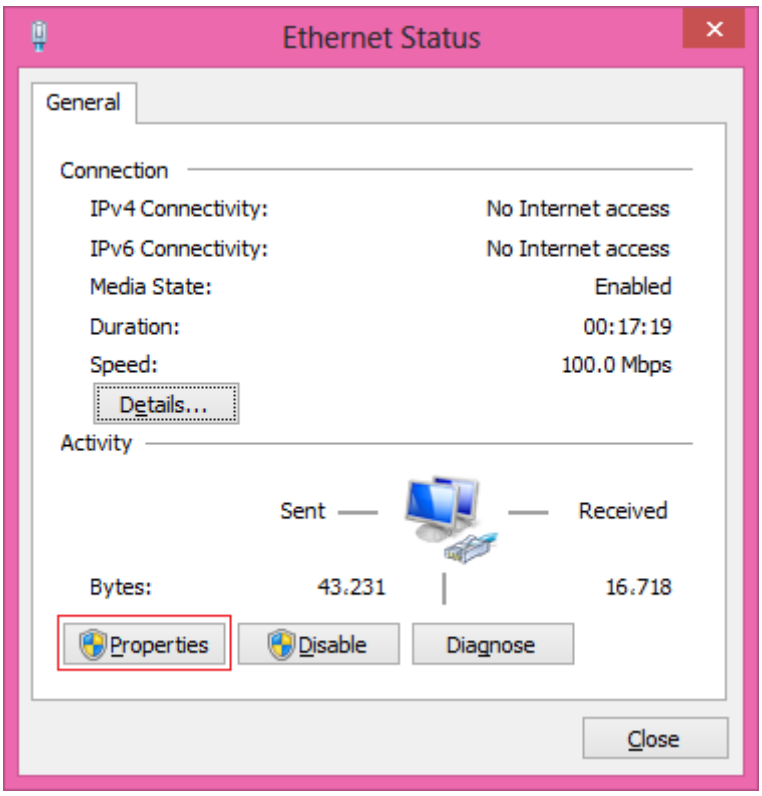
جهت مشاهده اتصالات شبکه در همین صفحه روی گزینه ۱، یعنی Change Adapter Settings کلیک کنید.

در صفحه بازشده، می‌توانید اتصالات شبکه‌ای موجود (فعال و غیرفعال) را مشاهده نمایید.

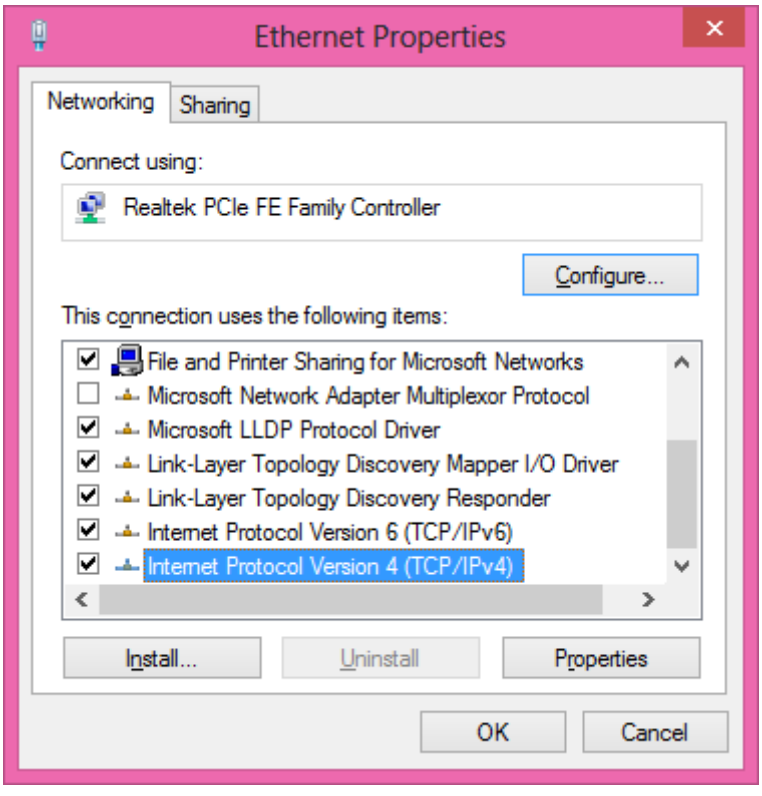


۱۸-۵- تغییر آدرس IP

جهت تغییر آدرس IP نیز در همان صفحه، گزینه شماره ۸ یعنی روی آداپتور فعال فعلی کلیک کنید. در صفحه بازشده، روی دکمه Propoerties کلیک نمایید. البته انجام این کار از طریق صفحه قبلی که لیست آداپتورها را نشان می‌داد، سپس راست کلیک روی آداپتور مورد نظر و انتخاب گزینه Properties نیز امکان پذیر است.



سپس صفحه تنظیمات شبکه آن باز می‌شود که بقیه آن مانند ویندوز XP است.

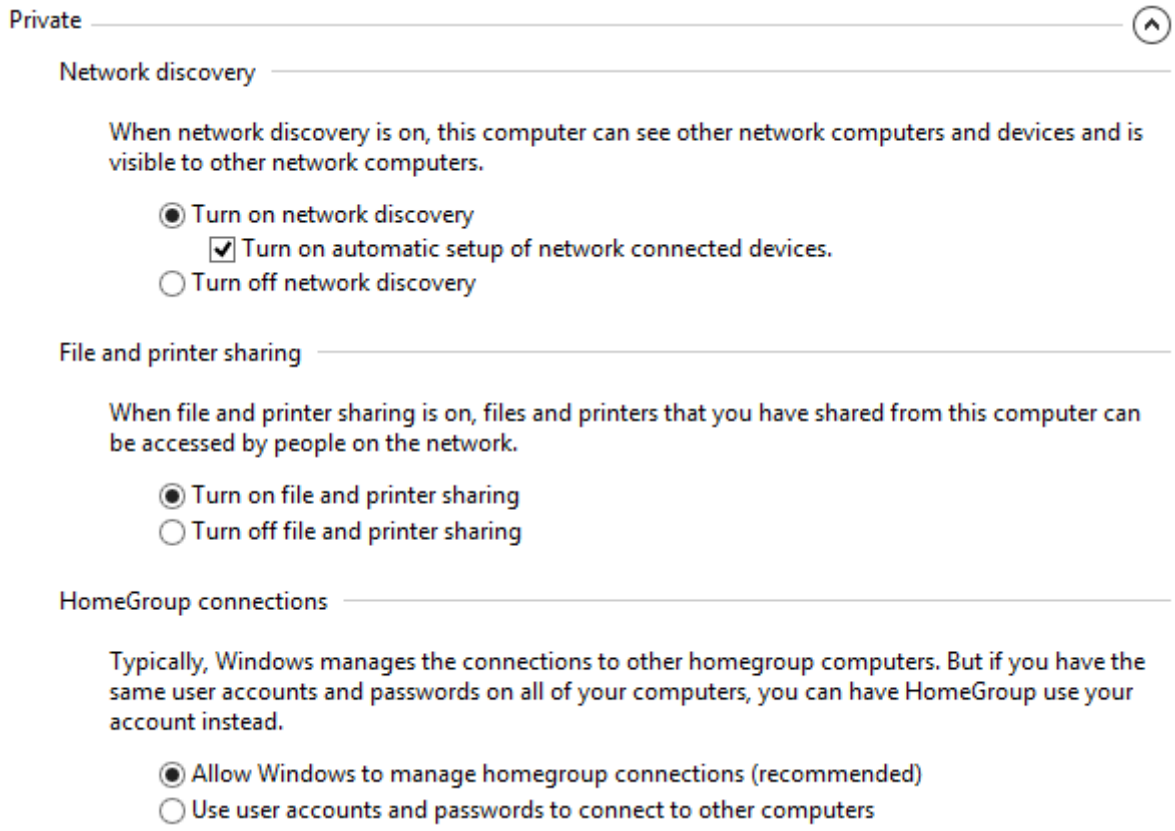


۱۸-۶- تنظیمات اشتراک گذاری پیشرفته

در صفحه تنظیمات شبکه با کلیک روی گزینه شماره ۲، یعنی Change Advanced Sharing Settings می‌توانید وارد صفحه تنظیمات پیشرفته اشتراک گذاری شوید. در این صفحه تنظیمات به ۳ دسته تقسیم می‌شوند.

۱۸-۶-۱- *Private*

تنظیمات این قسمت، مربوط به حفظ محرمانگی است که خود به ۳ دسته تقسیم می‌شود.



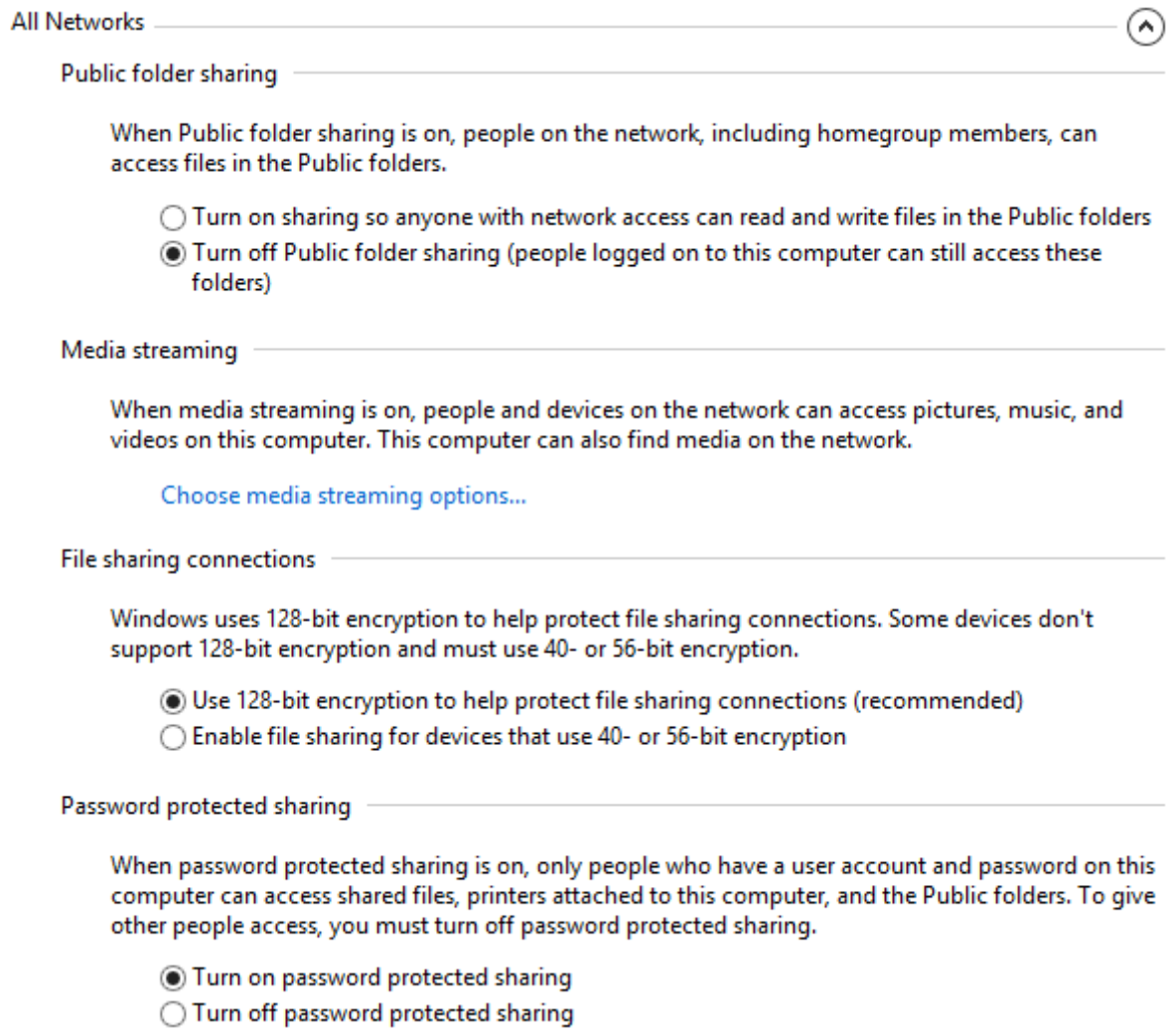
- **Network Discovery**: فعال بودن این گزینه (Turn on) باعث می‌شود که ویندوز شما بتواند دیگر کامپیوترها و تجهیزات متصل به شبکه را مشاهده نموده و آن‌ها را به شما نمایش دهید. همچنین از طرف دیگر، بقیه کامپیوترهای موجود در شبکه نیز بتوانند کامپیوتر شما را مشاهده نمایند.
- **File and Printer Sharing**: با فعال نمودن این گزینه (Turn on)، امکان به اشتراک گذاری پوشه‌ها و چاپگر در این ویندوز فراهم می‌شود.
- **HomeGroup Connections**: با انتخاب گزینه Allow…، ویندوز خود مدیریت شبکه خانگی را بر عهده می‌گیرد. این گزینه برای اتصال بدون نام کاربری و رمز عبور به کامپیوترهای عضو HomeGroup می‌باشد. اما اگر یک نام کاربری و رمز عبور یکسان روی تمام کامپیوترها تعریف نموده اید، با انتخاب گزینه Use… می‌توانید اتصال به دیگر کامپیوترها را خود مدیریت نمایید، بدون نیاز به عضویت در HomeGroup.

۱۸-۶-۲- *Guest or Public*

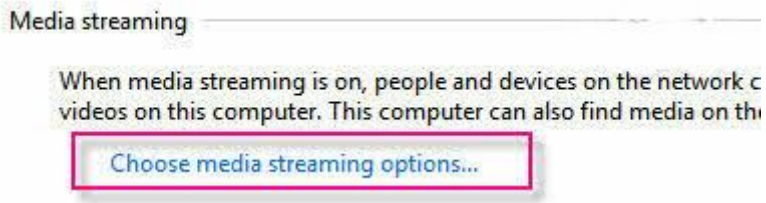
اطلاعات این بخش نیز، مانند بخش قبل می‌باشد، اما فقط برای کاربران Guest و اعضای گروه Public

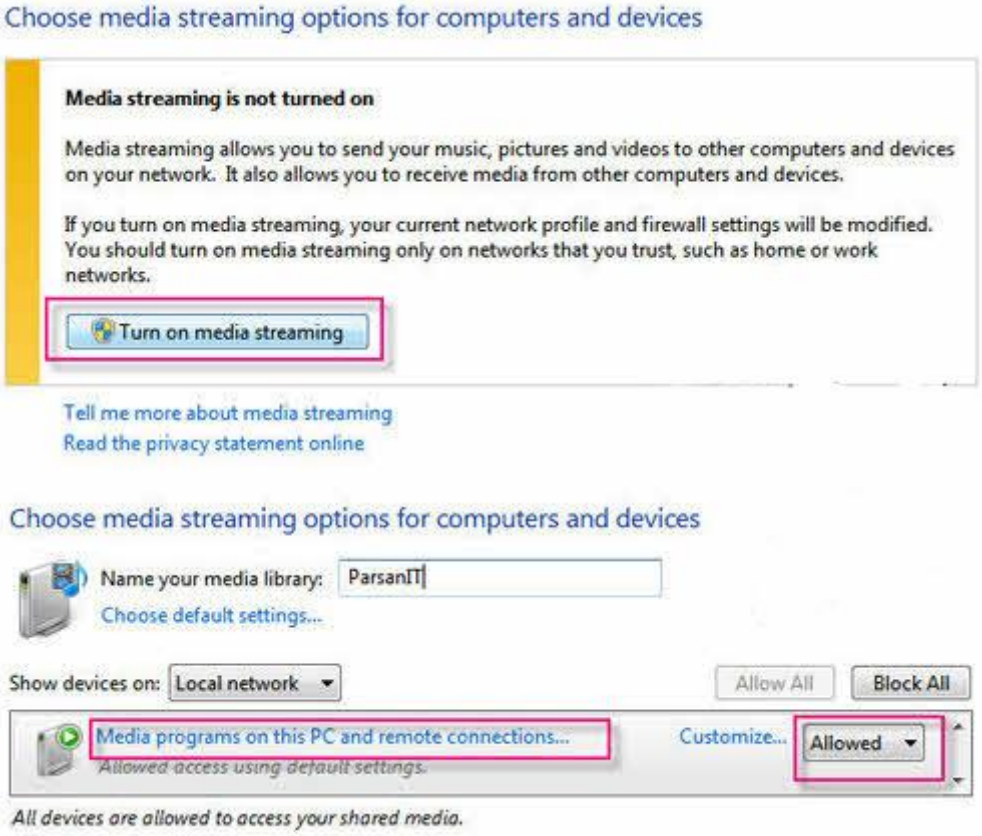
۱۸-۶-۳- *All Networks*

تنظیمات این قسمت نیز روی تمام کاربران کامپیوتر اعمال می‌شود که خود این قسمت ۴ بخش دارد.



- **Public Folder Sharing**: فعال کردن این گزینه (Turn On) باعث می‌شود که تمام کاربران عضو HomeGroup بتوانند به پوشه‌های اشتراکی عمومی دسترسی داشته باشند. پوشه‌های عمومی، پوشه هایی هستند که برای کاربردهای خاص، مانند برقراری ارتباط پیامی بین ویندوزها از آن‌ها استفاده می‌شود. مانند Users، IPC یا Admin. توصیه می‌شود این گزینه را غیر فعال نمایید.
- **Media Streaming**: در این قسمت قادر خواهید بود به تصاویر فایهای صوتی و ویدئویی دسترسی داشته باشید؛ همچنین دستگاه‌های مدیا که قابلیت کار در شبکه را دارند نیز می‌توانند با استفاده از تنظیمات این قسمت به این موارد دسترسی داشته باشند. در مورد قابلیت Media Streaming در فصلی جداگانه صحبت شده است.

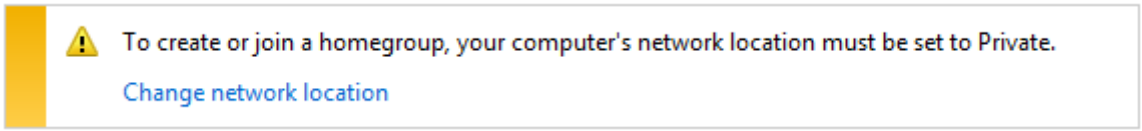




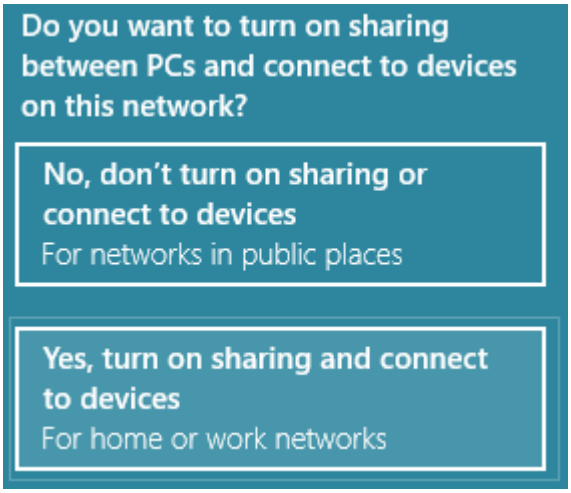
- **File Sharing Connections**: در این بخش می‌توانید طول کلید کد گذاری را تعیین نماید که دو حالت ۱۲۸ بیتی و ۴۰ یا ۵۶ بیتی وجود دارد. هر چه طول کلید، بزرگتر باشد، امنیت بالاتر می‌رود، اما از طرفی هم سرعت پایین می‌رود و هم این امکان وجود دارد که برخی تجهیزات نتوانند از کلیدهای فراهم شده استفاده کنند.
- **Password Protected Sharing**: فعال کردن این گزینه (Turn On) باعث می‌شود که وقتی دیگر کامپیوترها می‌خواهند از پوشه‌های به اشتراک گذاشته شده این ویندوز استفاده کنند، یکی از نام‌های کاربری و رمزهای عبور تعریف شده را وارد نمایند. غیر فعال کردن این گزینه باعث می‌شود که بقیه بتوانند بدون نام کاربری و رمز عبور، از اطلاعات به اشتراک گذاشته شده من استفاده کنند.

۱۸-۷- اتصال به HomeGroup

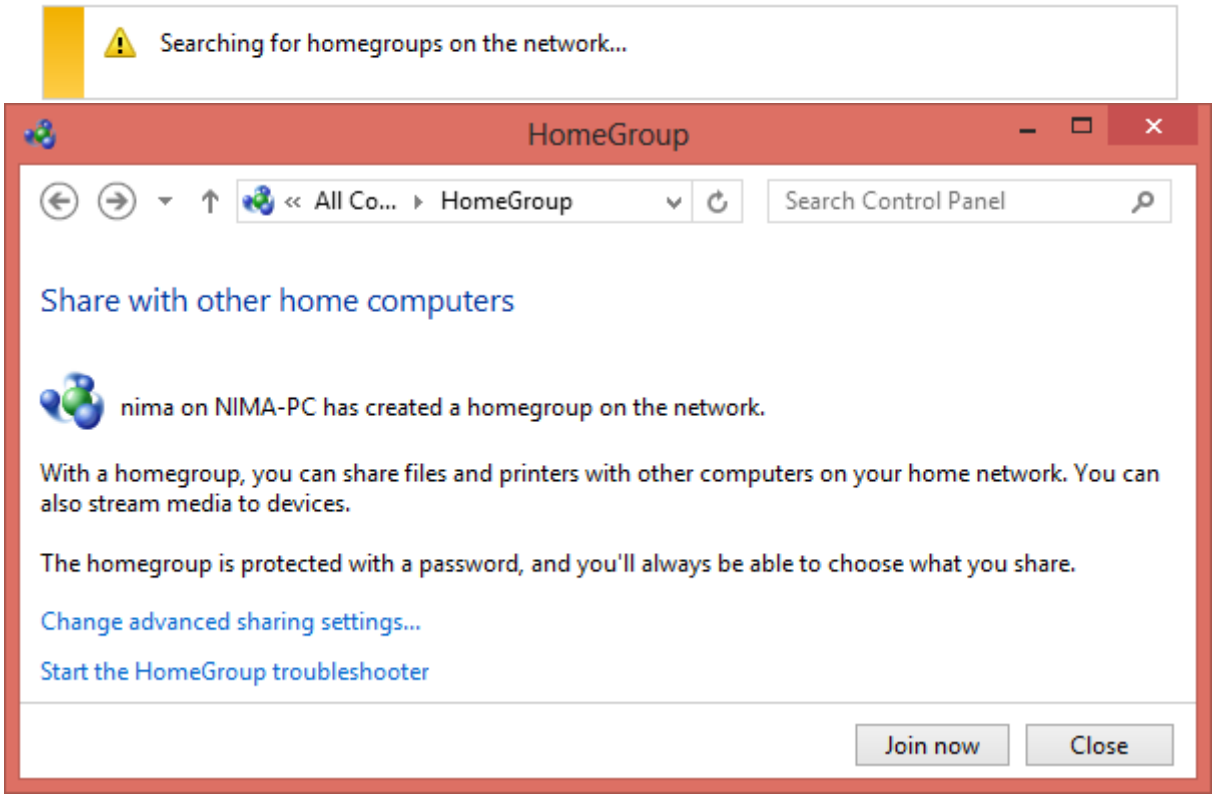
همانطور که در تنظیمات ویندوز XP نیز دیدید، می‌توان کامپیوتر را در گروه‌های مختلف قرار داد و از امکانات شبکه‌ای گروه‌ها استفاده نمود. جهت اتصال کامپیوترتان به یک HomeGroup ساخته شده، در صفحه تنظیمات شبکه، روی گزینه شماره ۳ یعنی HomeGroup کلیک کنید. وقتی برای اولین بار بخواهید به یک HomeGroup وصل شوید، سیستم به شما پیغام می‌دهد که بایستی اطلاعات Location خود را ثبت نمایید. بدین منظور روی قسمت Change Network Location کلیک کنید.



سپس در صفحه بازشده، گزینه Yes, turn on ... را انتخاب نمایید.

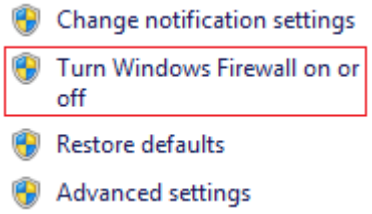


سپس به صفحه تنظیمات شبکه بازگشته و مجددا همین صفحه را باز نمایید. مشاهده خواهید کرد که ویندوز ۸ به دنبال شبکه‌های HomeGroup موجود می‌گردد. سپس می‌توانید به راحتی با انتخاب یکی از HomeGroupها (در صورت وجود) و با کلیک روی دکمه Join now به آن گروه متصل شوید.

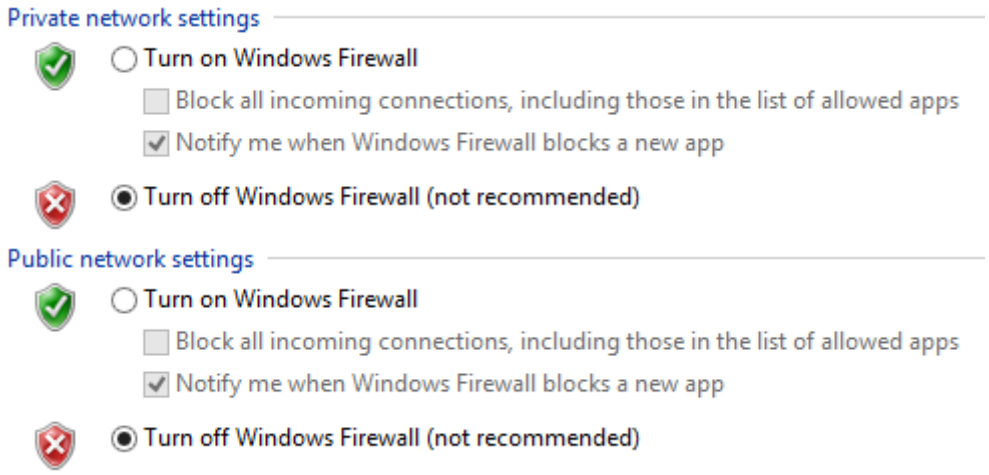


۱۸-۸- تنظیمات فایروول

تنظیمات فایروول در ویندوز ۸ تفاوت‌های زیادی نسبت به ویندوز XP پیدا کرده، اما هنوز اصول اولیه را حفظ نموده است. جهت ورود به صفحه تنظیمات فایروال، در صفحه تنظیمات شبکه، روی گزینه شماره ۵ یعنی Windows Firewall کلیک کنید. در صفحه بازشده، جهت خاموش یا روشن کردن فایروال، روی قسمت Turn Windows Firewall on or off کلیک کنید.

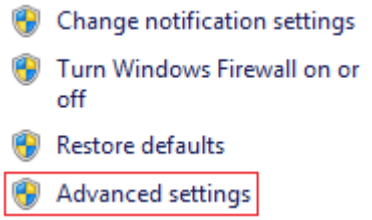


سپس در صفحه باز شده، جهت روشن کردن فایروال گزینه ..Turn on و جهت خاموش کردن آن از گزینه ..Turn off استفاده نمایید. همانطور که قبلا نیز دیدید، این تنظیمات امنیتی در دو سطح خصوصی و عمومی قابل اعمال است که تفاوت آن‌ها در کاربران و برنامه‌های احراز هویت شده یا نشده می‌باشد.

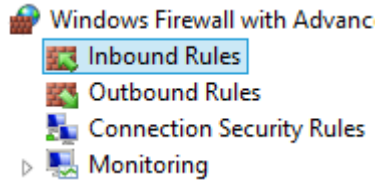


همچنین می‌توان تعیین نمود که پس از روشن شدن فایروال، آیا هیچ برنامه‌ای حق اتصال به سیستم ما را دارد؟ و نیز می‌توان نوع پیام رسانی‌های فایروال را تعیین نمود. توصیه می‌شود که اگر آنتی ویروسی دارید که دارای فایروال است، فایروال ویندوز ۸ را غیر فعال کنید.

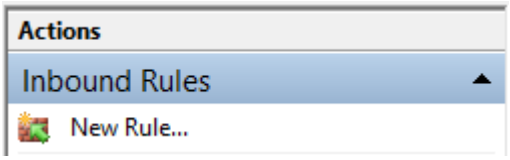
البته فایروال ویندوز ۸ تنظیمات پیشرفته تری نیز دارد که جهت انجام آن‌ها در صفحه قبل روی قسمت Advance Settings کلیک کنید.



در صفحه بازشده، می‌توانید قوانین خاصی را اعمال نمایید. مثلا اعلام کنید که نرم‌افزار خاصی اجازه دارد از فایروال عبور کرده و از شبکه و اینترنت استفاده کند. این قوانین به دو دسته تقسیم می‌شوند. یک Inbound که بیانگر نرم‌افزارها/پروتکل هایی هستند که روی سیستم خودمان قرار دارند و می‌خواهند از شبکه یا اینترنت استفاده کنند و دیگری Outbount که بیانگر نرم‌افزارها/پروتکل هایی هستند که در خارج از کامپیوتر ما قرار دارند و می‌خواهند از کامپیوتر ما استفاده کنند.

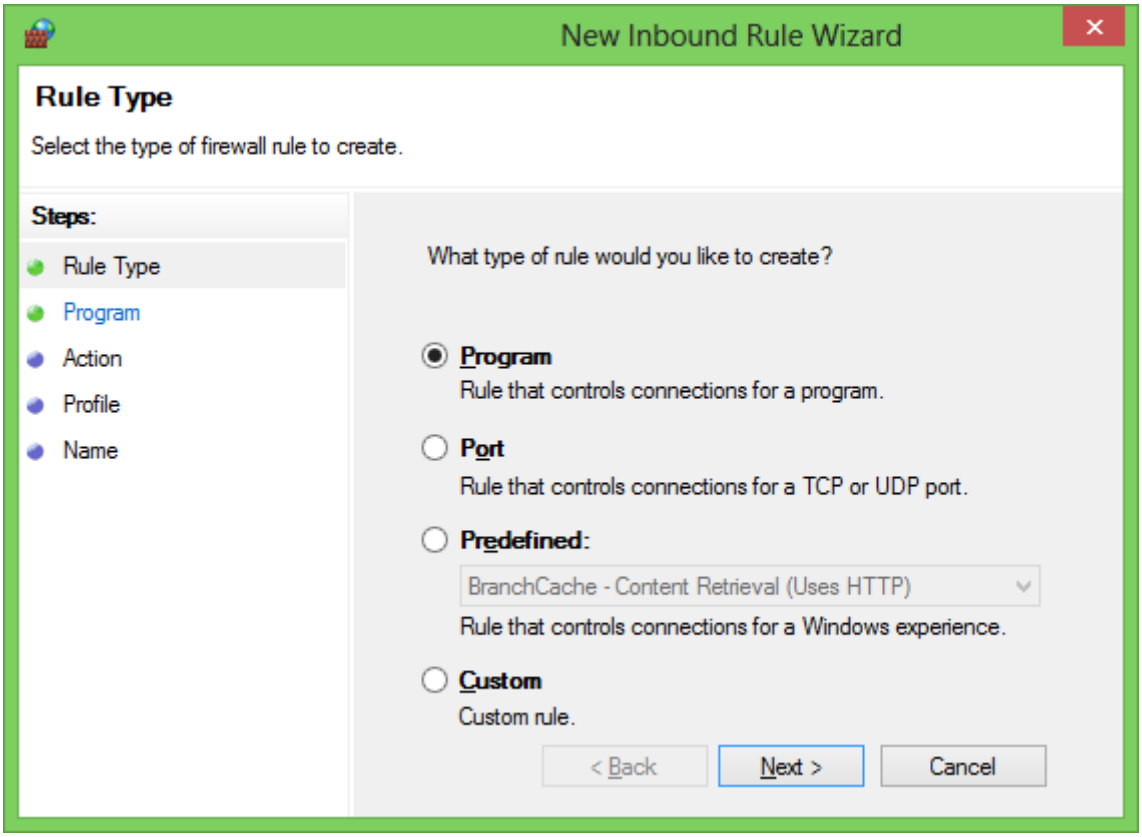


بعد از تعیین نوع قانون، جهت ایجاد قانونی جدید، روی دکمه New Rule در سمت راست صفحه کلیک کنید.



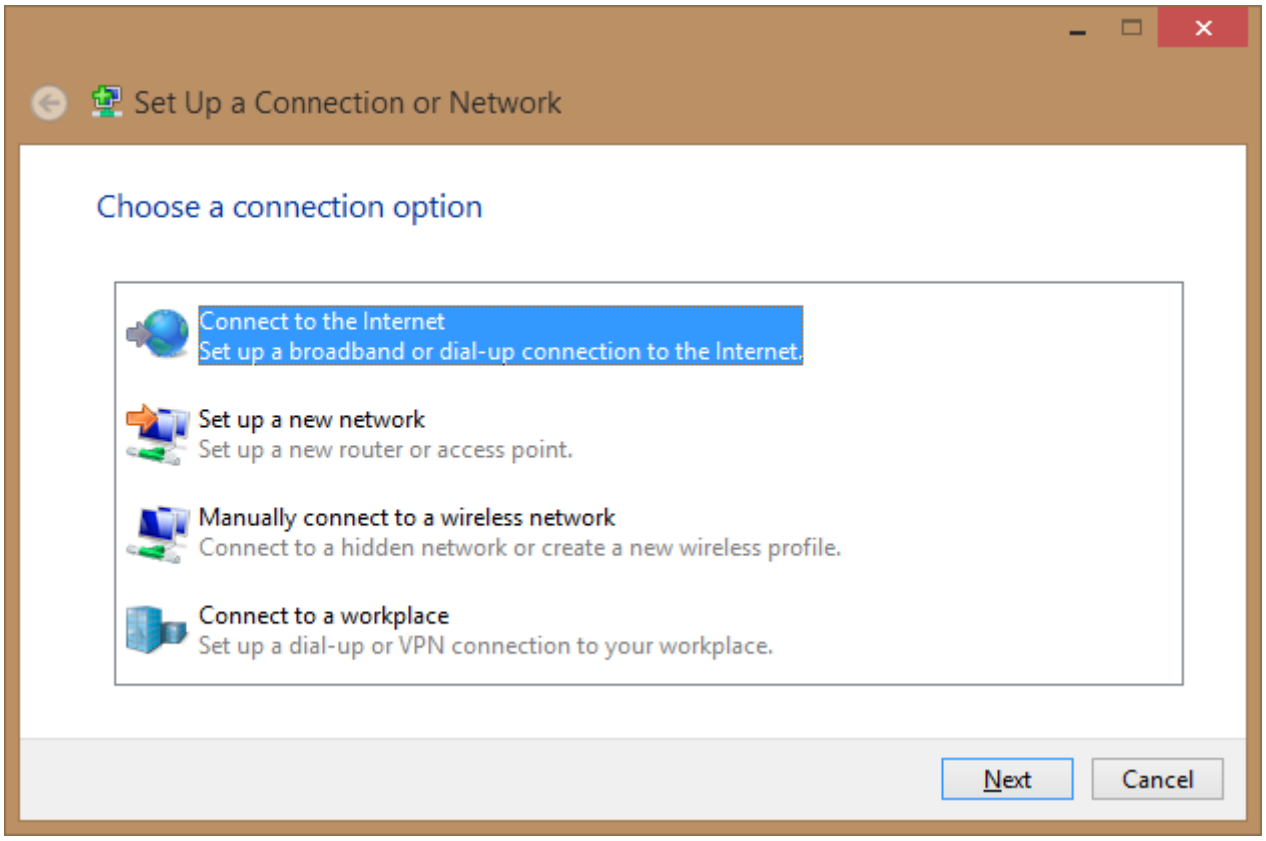
سپس نوع عنصری که می‌خواهد از فایروال عبور کند (برنامه، پورت یا پروتکل) را انتخاب کرده و با طی مراحل مرتبط، کار را به اتمام رسانید.

در این بخش دیگر وارد جزئیات چگونگی تعریف قانون نمی‌شویم. اما مراحل کار بسیار ساده است و با ورود به هر مرحله، اگر با فایروال آشنا باشید، متوجه می‌شوید که چه کاری باید انجام دهید.



۱۸-۹- راه اندازی اتصالات شبکه جدید

جهت ایجاد اتصالات شبکه‌ای جدید، در صفحه تنظیمات شبکه، روی گزینه شما ۶، یعنی Set up new connection… کلیک کنید تا صفحه زیر باز شود.

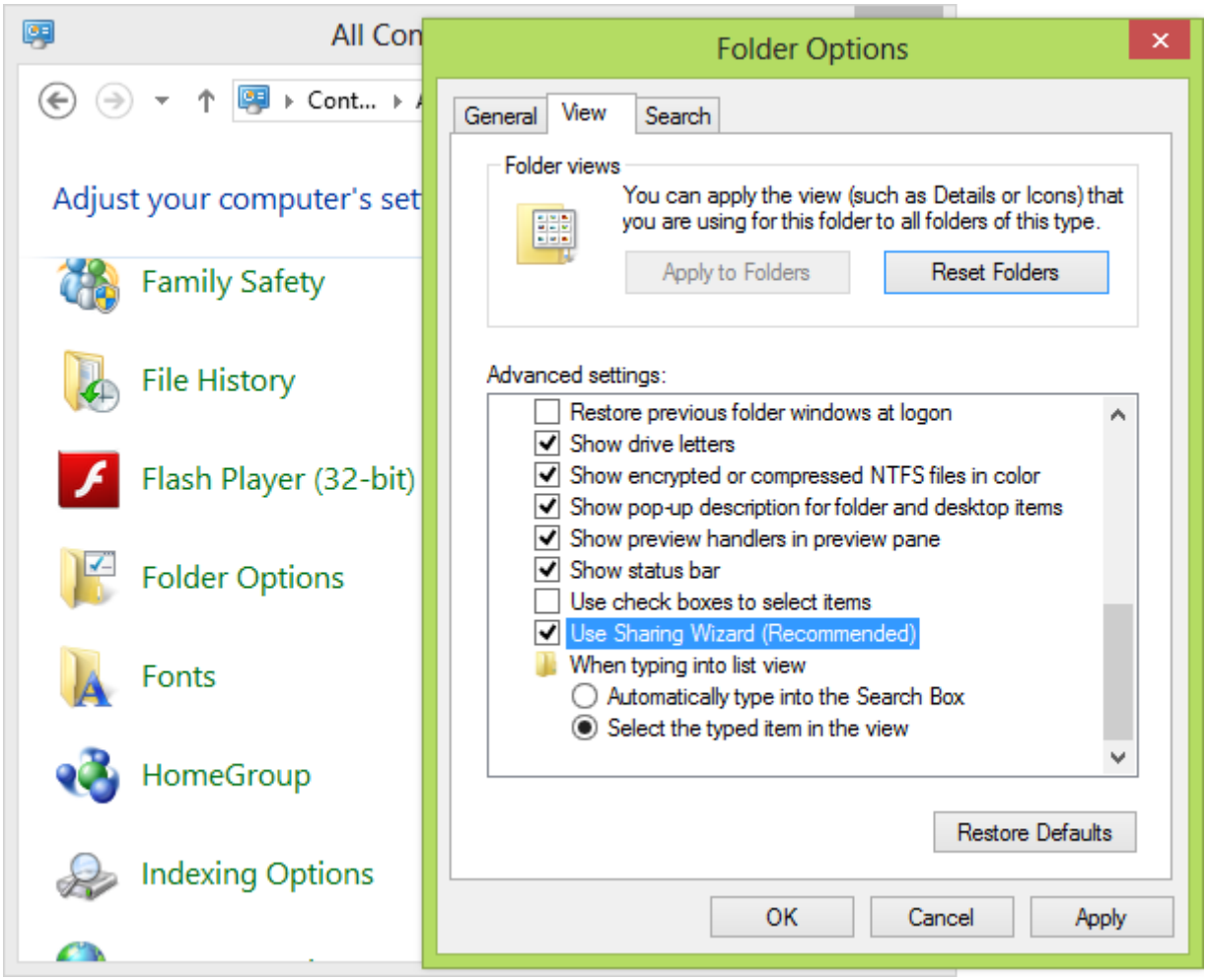


در این صفحه می‌توانید اتصالات مختلفی را ایجاد نمایید که عبارتند از:

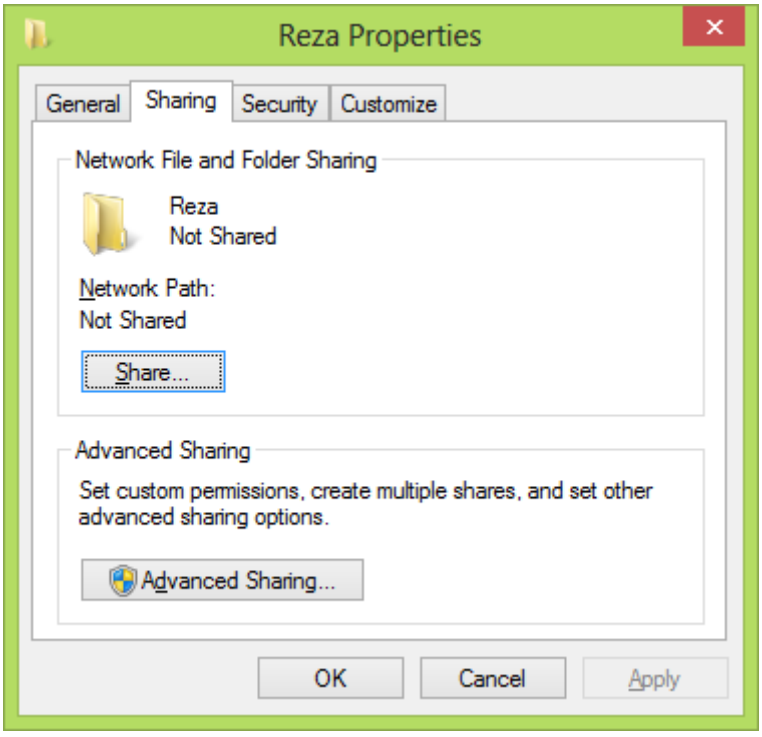
- **Connect to the Internet**: این مورد زمانی مناسب است که بخواهید توسط یکی از کامپیوترهای موجود در شبکه به اینترنت متصل شوید. این مورد به خصوص در مراکز دانشگاهی که دانشجویان جهت اتصال به اینترنت نیاز به نام کاربری و رمز عبور دارند، مناسب می‌باشد.
- **Setup a New Network**: با کمک این گزینه می‌توانید شبکه‌ای جدید به کمک مسیریاب یا به کمک Access Point ایجاد نمایید.
- **Manually Connect to a Wireless Network**: این گزینه جهت برپاسازی شبکه بدون اتصال فیزیکی (بی‌سیم) و به صورت Adhoc به کار می‌رود.
- **Connect to a Workplace**: از این گزینه جهت اتصال به شبکه‌ای دیگر به کمک خطوط Dial-UP یا اتصال VPN استفاده می‌شود. در مورد این دو مورد در فصول بعدی صحبت خواهد شد.

۱۸-۱۰- اشتراک گذاری پوشه‌ها

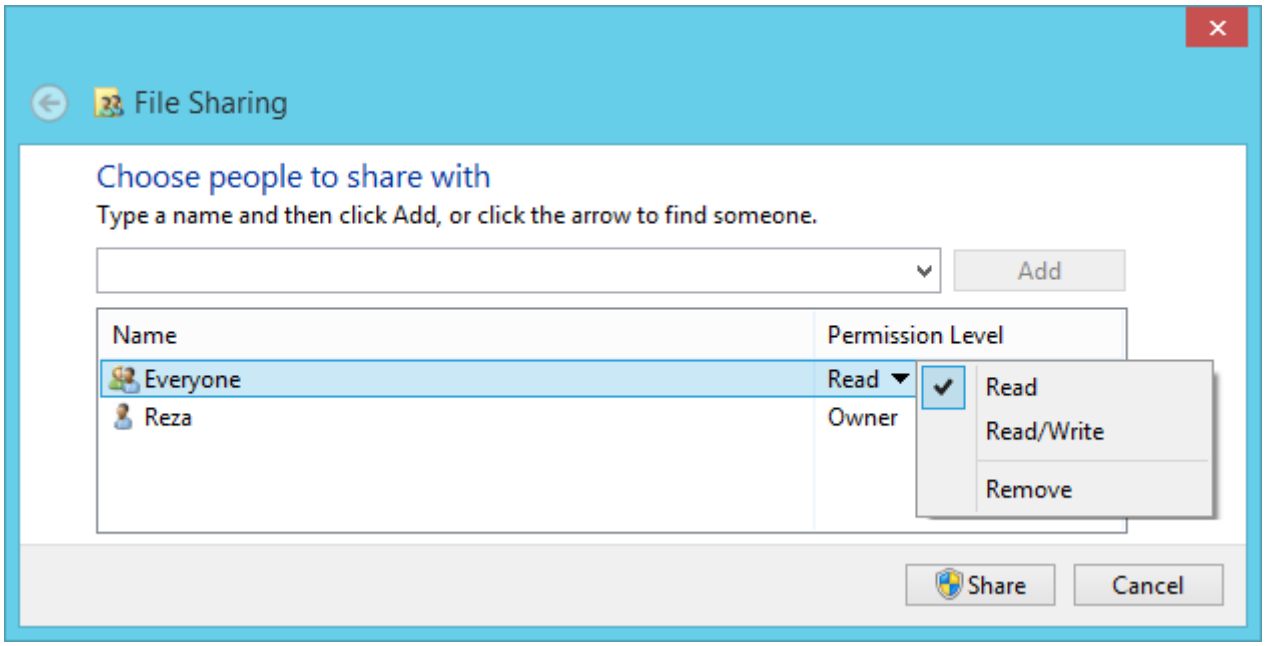
با مفاهیم اشتراک گذاری پوشه‌ها قبلا آشنا شده اید. این کار در ویندوز ۸ بسیار راحت است. بدین منظور ابتدا بایستی امکان اشتراک گذاری به صورت Wizard را فعال کنید. بدین منظور از Control Panel، وارد Folder Oprion شده و سپس در صفحه بازشده، گزینه Use Sharing Wizard را فعال نمایید.



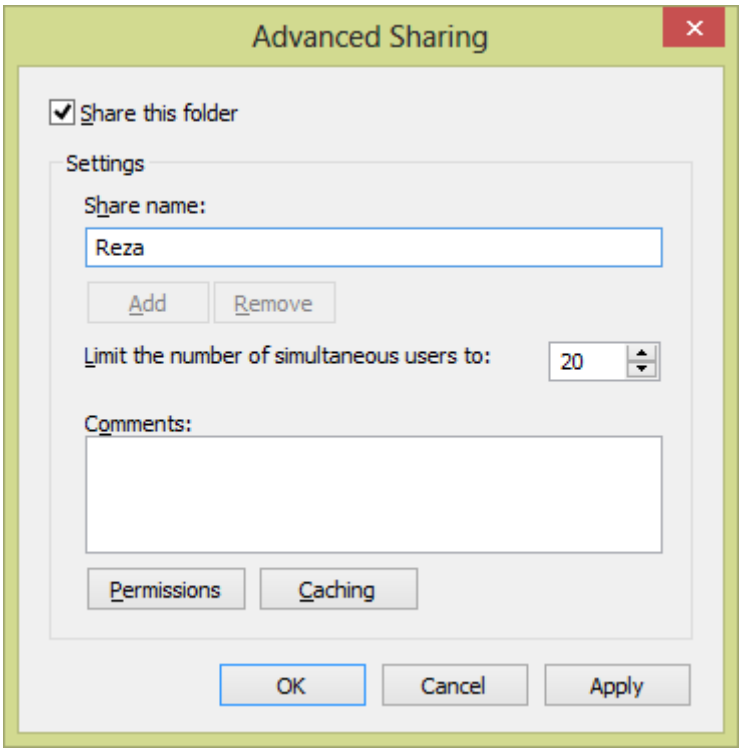
سپس جهت به اشتراک گذاری پوشه‌ای خاص، روی آن راست کلیک نموده و بعد از انتخاب گزینه Properties وارد سربرگ Sharing شوید. ویندوز ۸ دو نوع Sharing ساده و پیشرفته فراهم می‌کند. جهت به اشتراک گذاری ساده روی دکمه Share کلیک کنید.



سپس در صفحه بازشده، کاربرانی که حق استفاده از پوشه به اشتراک گذاشته شده را دارند را اضافه نموده و سپس سطح دسترسی هر یک را تعیین نمایید.



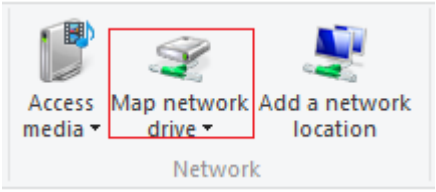
اما برای به اشتراک گذاری پیشرفته، روی دکمه Advanced Sharing کلیک نموده و سپس گزینه Share this folder را فعال نمایید.



بقیه قسمت‌ها مانند ویندوز XP است. مثلا از طریق Limit the number... می‌توان تعداد دسترسی همزمان را محدود کرد، از طریق دکمه Permissions می‌توان سطوح دسترسی خاص را اعمال نمود و از طریق دکمه Caching نیز امکان Cache کردن اطلاعات به اشتراک گذاشته شده را فراهم نمود.

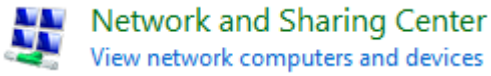
۱۸-۱۱- نگاشت درایو شبکه

جهت نگاشت درایو شبکه، همانند ویندوز XP دو راه وجود دارد. یکی اینکه ابتدا وارد My Computer شده و گزینه Map Network Drive را انتخاب نمایید.

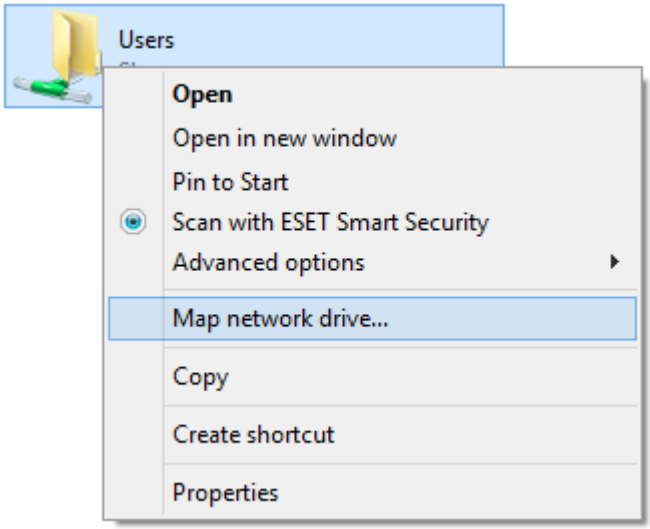


سپس یک پوشه روی شبکه را انتخاب نمایید که بقیه مراحل مانند ویندوز XP است.

راه دیگر این است که ابتدا وارد یکی از پوشه‌های به اشتراک گذاشته شده در شبکه شوید. از طریق Run یا Control Panel. در Run باید آدرس پوشه به اشتراک گذاشته شده در شبکه را وارد نمایید. برای Control Panel نیز وارد Control Panel شده و در قسمت جستجو عبارت View network computers and devices را وارد نموده و وارد گزینه به نمایش در آمده شوید.



سپس وارد کامپیوتر مقصد مورد نظر شوید و حرکت کنید تا به پوشه به اشتراک گذاشته شده در کامپیوتر مقصد شوید. سپس روی پوشه مورد نظر راست کلیک نموده و گزینه Map Network Drive را انتخاب نمایید.



بدین ترتیب یک درایو نگاشت شده به پوشه به اشتراک گذاشته شده، روی کامپیوترمان ایجاد می‌شود.

۱۸-۱۲- اشتراک گذاری چاپگر

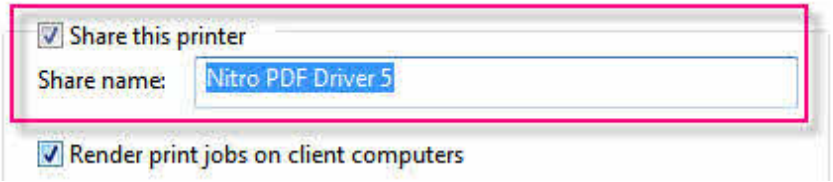
شاید شما در خانه یا دفتر خود یک چاپگر داشته باشید و بخواهید که تمامی سیستمهای شما در هر لحظه بتوانند از این چاپگر استفاده کنند. ساده ترین کار به اشتراک گذاری چاپگر است. برای این کار ابتدا به Control Panel رفته و View Devices and Printers را انتخاب نمایید.



سپس در قسمت Printer and faxes روی چاپگر مورد نظر که نام آن در لیست مقابلتان قرار دارد راست کلیک کرده و Properties را انتخاب نمایید.



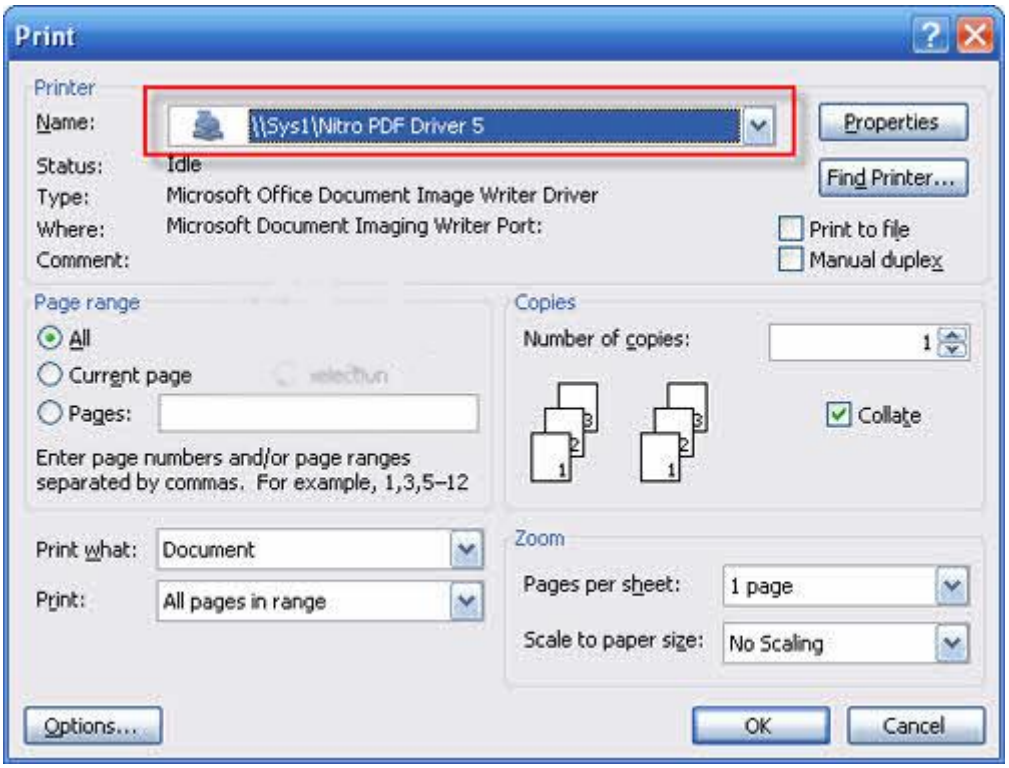
در صفحه جدید به زبانه Sharing رفته و روی عبارت Share this printer کلیک کنید. در کادری که فعال می‌شود نام دلخواهی انتخاب نماید. سپس روی OK کلیک کنید. مشاهده می‌کنید که این چاپگر به اشتراک گذاشته می‌شود. حال باید روی هر سیستم در شبکه چاپگر به اشتراک گذاشته شده را اضافه نمایید.



برای این منظور به سراغ سیستم مقابل (مقصد) رفته و از طریق View workingrup computers در my network places یا در قسمت سمت راست پنل Computer در ویندوز ۸ روی تصویر چاپگری که به لیستتان اضافه شده راست کلیک کرده و گزینه connect را کلیک کنید.



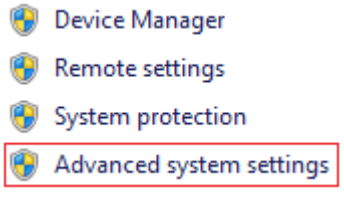
کادری مبنی بر درخواست نصب چاپگر بروی این سیستم باز می‌شود گزینه Yes را زده تا نصب چاپگر آغاز شود. ممکن است در خلال این نصب از شما فایل خواصی درخواست شود در این هنگام با گذاشتن سی دی چاپگر در درایو سی دی خود و ادامه مراحل این قسمت با موفقیت به پایان میرسد



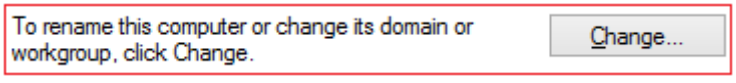
در اینجا چاپگر شما به اشتراک سیستم مقصد در آمد و از این پس می‌توانید از آن مانند سیستم متصل به آن استفاده کنید.

۱۸-۱۳- تغییر نام کامپیوتر، اتصال به دامنه

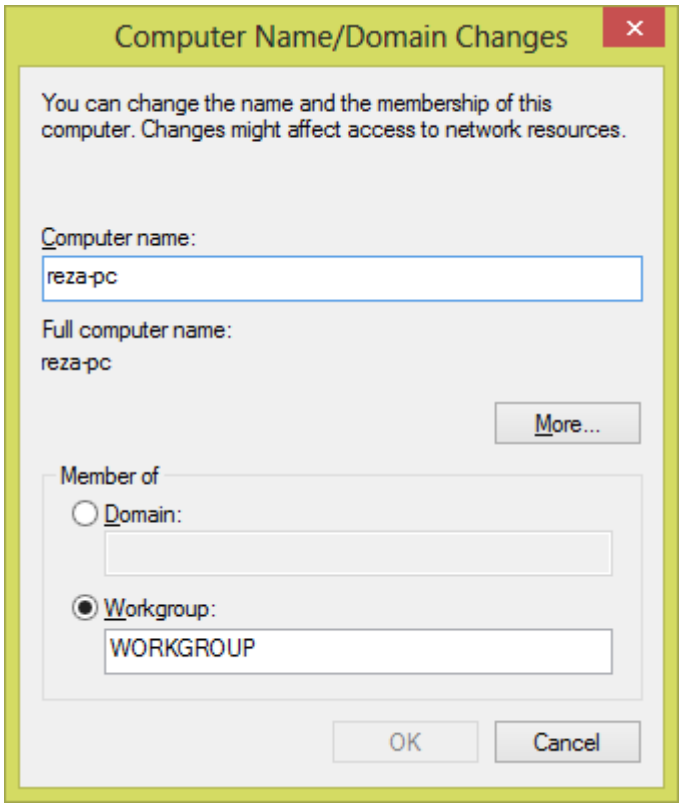
جهت تغییر نام کامپیوتر، ابتدا روی My Computer راست کلیک کرده و گزینه Properties را انتخاب نمایید. سپس گزینه Advances system settings را انتخاب نمایید.



سپس وارد سربرگ Computer Name شده و روی Change... کلیک کنید.



صفحه بازشده، همان صفحه‌ای است که در ویندوز XP هم وجود داشت و به کمک آن می‌توانستید نام کامپیوتر را تغییر داده، نام Workgroup را تغییر داده و یا به یک دامنه خاص متصل شوید.



فصل ۱۹

راه اندازی شبکه در لینوکس

۱۹-۱- مقدمه

لینوکس (Linux) به خانواده‌ای از سیستم‌عامل‌های شبه یونیکس اطلاق می‌شود که از هسته‌ی لینوکس استفاده می‌کنند که معروف‌ترین نمونه از نرم‌افزار آزاد و متن‌باز شناخته می‌شود. دراصل تنها باید هسته‌ی لینوکس را لینوکس نامید، اما به طور معمول این واژه به سیستم‌عامل‌های شبه یونیکس اطلاق می‌شود که بر مبنای هسته‌ی لینوکس و کتاب‌خانه‌ها و ابزارهای پروژه گنو ساخته شده‌اند. لینوکس قابل نصب بر روی انواع سخت‌افزارهاست، از ساعت (Linux Watch)، تلفن‌های همراه، تبلت‌ها، مسیریاب‌ها، و کنسول‌های بازی گرفته تا رایانه‌های رومیزی، رایانه‌های بزرگ و ابررایانه‌ها.

به مجموعه‌ای از نرم‌افزارهای بنا شده بر اجزای گفته شده توزیع لینوکس (Linux Distribution) می‌گویند که به طور معمول شامل ابزارهای گسترش نرم‌افزار، پایگاه‌های داده، سرویس دهندههای وب مثل آپاچی، محیط‌های رومیزی مانند گنوم و کی‌دی‌ای و اکس‌اف‌سی‌ای و مجموعه‌های اداری مانند اُپن آفیس هستند.

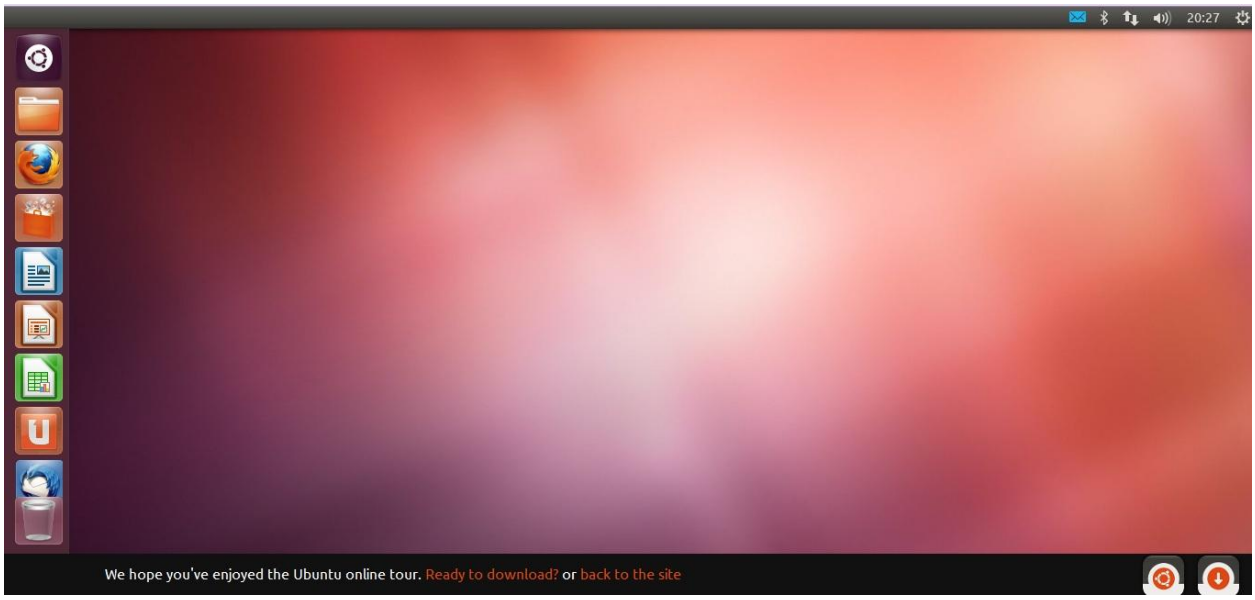
از توزیع‌های مهم لینوکس می‌توان به نسخه‌های زیر اشاره کرد:

- ✓ Debian
- ✓ Ubuntu
- ✓ Aurora
- ✓ Gentoo
- ✓ Arch Linux
- ✓ Fedora
- ✓ SUSE Linux

- ✓ Red Hat Enterprise Linux
- ✓ Centos
- ✓ Slackware

۱۹-۲- اوبونتو

اوبونتو یک سیستم عامل است که به کمک یک تیم جهانی از توسعه‌دهندگان نرم‌افزاری با تجربه آماده می‌شود. این سیستم عامل همه برنامه‌های مورد نیاز شما را داراست: یک مرورگر وب، مجموعه اداری دفتری، برنامه‌های چندرسآن‌های، پیغام‌رسآن‌های اینترنتی و بسیاری دیگر. اوبونتو یک جایگزین متن-باز برای ویندوز و مجموعه اداری آن است.



از آنجایی که ما قصد نداریم اوبونتو را به طور کامل آموزش دهیم فرض را بر این میگیریم که شما لینوکس کار کرده اید و با کار با آن کاملا آشنایی دارید و می‌خواهید با روش شبکه کردن لینوکس و به اشتراک گذاری فایل در لینوکس آشنایی پیدا کنید.

۱۹-۳- شبکه کردن لینوکس

قوانین شبکه کردن در تمامی سیستم عامل‌ها یکسان است. تمام قوانین مربوط به تخصیص IP که ما در ویندوز استفاده می‌کردیم در لینوکس اوبونتو هم کاربرد دارد.تنها تفاوت لینوکس با ویندوز محل قرار گرفتن این تنظیمات است.

همانطور که ما برای راه اندازی DHCP Server یا DNS Server نیاز به ویندوز سرور داریم، برای انجام این کارها در لینوکس هم نیاز به استفاده از نسخه ی مخصوص سرور لینوکس داریم، نسخه‌ای مانند Linux Ubuntu Server می‌تواند این کارها را به خوبی برای ما انجام دهد.

در لینوکس اوبونتو ۲ راه برای تخصیص IP وجود دارد.

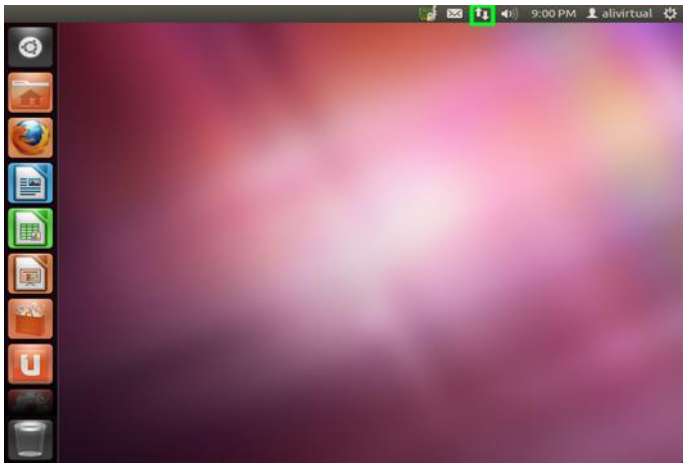
از طریق رابط گرافیکی

از طریق خط فرمان مختص لینوکس(در اینجا نسخه ی اوبونتو)

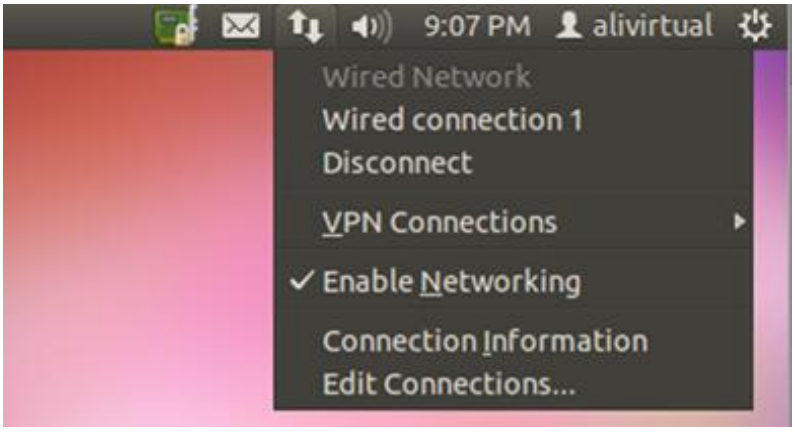
۱۹-۳-۱- تخصیص IP از طریق رابط گرافیکی

وقتی ما کامپیوتری که لینوکس اوبونتو روی آن نصب است را با کارت شبکه به شبکه متصل می‌کنیم خودش به صورت خودکار یک کانکشن از نوع Wired Connection ساخته و نوع تخصیص IP آن را روی Automatic DHCP قرار می‌دهد.

ما می‌توانیم کانکشن انواع شبکه‌ها،مثلا وایرلس، بلوتوث، سیمی، Vpn و ... را در لیونکس در یک جا ببینیم.در شکل زیر محل قرار گرفتن Network Setting را می‌توانیم ببینم که با علامت سبز رنگ مشخص شده است.



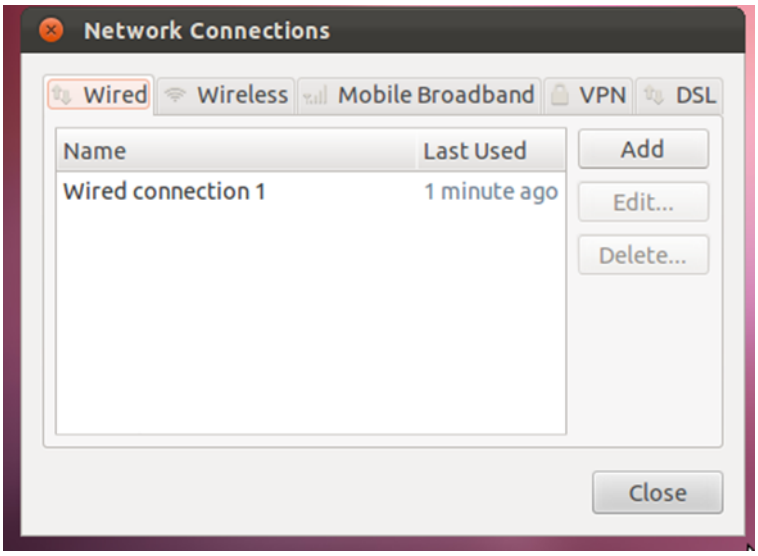
پس ازکلیک روی Network Setting پنجره‌ای مانند بالا زیر می‌شود که در آن می‌توان ارتباط داشتن شبکه با شبکه ی دیگر، اسم Connection، اطلاعات مربوط به Connection و تنظیمات مربوط به آن‌ها را مشاهده کرد. در قسمت Vpn هم می‌توانیم تنظیمات مربوط به Vpn را انجام بدهیم یا به آن وصل شویم.



لینوکس از Vpnهای نوع Pptp، Cisco Vpn و Open Vpn پشتیبانی می‌کند. یکی از تنظیمات این بخش Enable Networking است که با برداشتن تیک آن می‌توان کل قابلیت‌های شبکه را در سیستم خودمان ببندیم. با زدن دوباره ی تیک باز شبکه ی ما با همان تنظیمات قبلی اجرا می‌شود.

در این شکل میبینیم که سیستم ما به شبکه‌ای وصل است.اسم کانکشن آن Wired Connection 1 می‌باشد.

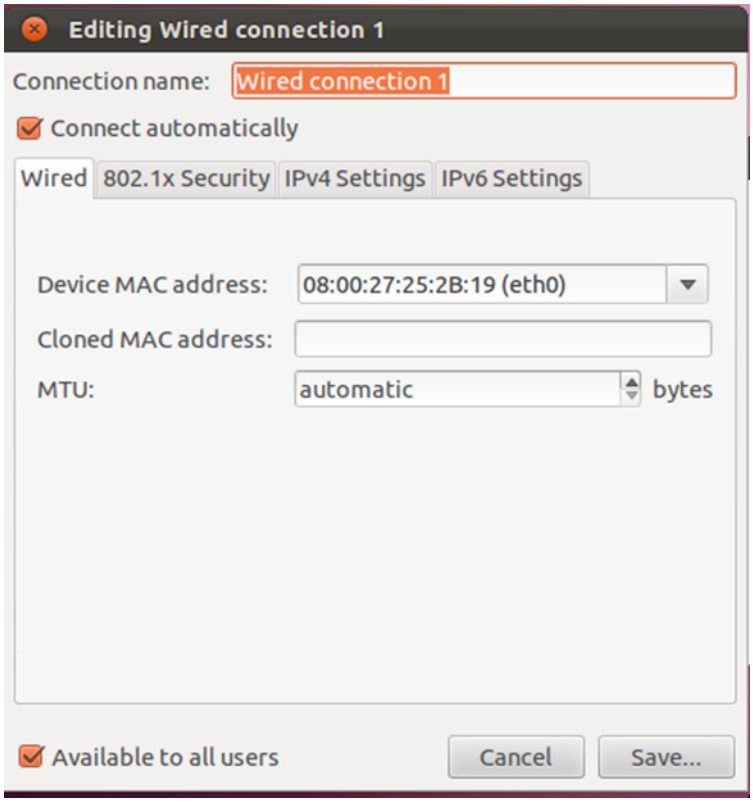
پس از کلیک روی Edit Connections کادری همانند شکل زیر باز می‌شود. این کادر به منظور ساختن انواع کانکشن‌ها در شبکه‌های مختلف است. ما برای شبکه کردن با کارت شبکه و کابل نیاز به قسمت Wired داریم.



توجه داشته باشید که پس از وصل کردن سیستم به شبکه، لینوکس به صورت خودکار کانکشن ایجاد می‌کند. حال اگر ما بخواهیم همان کانکشن را تنظیم کنیم کافیست بر روی آن کلیک کرده و به روی دکمه ی Edit کلیک کنیم.

برای ساختن یک کانکشن جدید باید از Add و برای حذف از دکمه ی Delete استفاده می‌کنیم.

پس از کلیک بر روی Edit کادری همانند شکل زیر باز می‌شود.

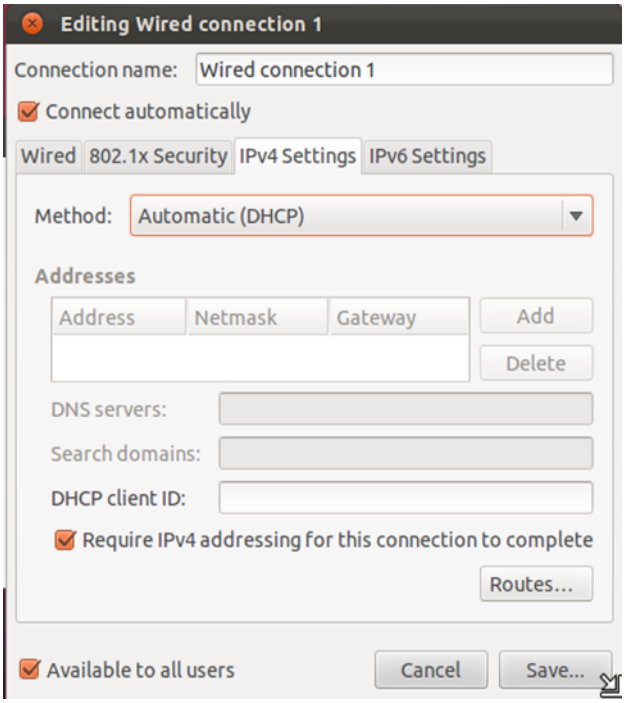


در شکل بالا همانطور که قابل مشاهده است، ما ۴ سربرگ در اختیار داریم که می‌توانیم تنظیمات مربوط به کارت شبکه، امنیت، IPV4 و IPV6 را پیکربندی کنیم.

برای مثال در این سربرگ می‌توانیم آدرس مک کارت شبکه را ببینیم و حتی به راحتی آن راClone کنیم.

برای تنظیم IP و Subnet Mask و ... باید به سربرگ IPV4 Setting برویم.

در صفحه ی بعد شکل مربوط به آن را خواهیم دید.



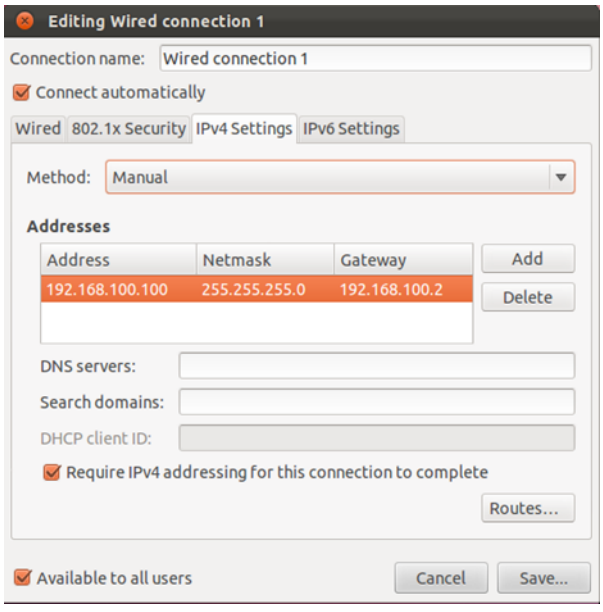
همانطور که مشاهده می‌نمایید تنظیمات سیستم ما به طور پیشفرض به روی DHCP ست شده است. برای عوض کردن این تنظیم باید بر روی لیست Method رفته و Manual را انتخاب کنیم.

پس از این کار، کادر غیرفعال پایین فعال شده و ما امکان نوشتن آدرس، Netmask و Gateway مربوط به شبکه ی خود را داریم.

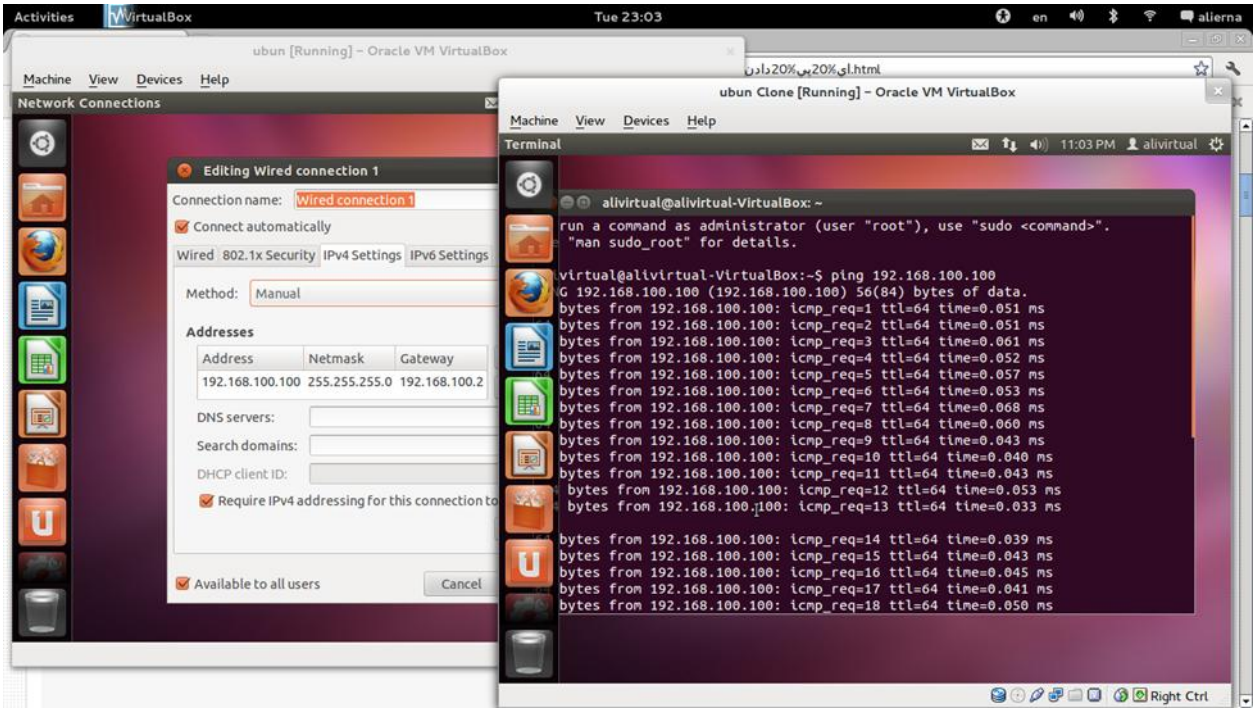
روند آدرس‌دهی و قوانین آن عینا مانند ویندوز بوده و هیچ مشکلی ایجاد نمی‌کند.

همانطور که میبینید ما در شکل زیر مشخصات شبکه را به طور دستی ست کردیم و حالا اگر آدرس درست باشد شبکه ی ما بدون هیچ مشکلی باید وصل شده باشد.

در آخر کار هم نیاز به زدن دکمه ی Save داریم.پس از Save کردن سیستم عامل پسورد کاربر را میخواهد که باید وارد کنیم.



در شکل زیر پینگ شدن کامپیوتری که IP داده‌ایم را میبینیم:



دیدیم که به راحتی از طریق رابط گرافیکی می‌توانیم IP بدهیم و از امکانات شبکه در لینوکس استفاده کنیم. اما حالا اگر بخواهیم با خط فرمان این کار را انجام دهیم چطور؟...

۱۹-۳-۲- تخصیص IP از طریق خط فرمان

خط فرمان در نسخه‌های مختلف لینوکس متفاوت است اما بسته به اینکه لینوکس ما از کدام نسخه ی پایه آمده باشد، نوع خط فرمان به چند دسته تقسیم می‌شود. برای مثال اوبونتو از لینوکس Debian درست شده، بنابراین خط فرمان آن با لینوکس هایی که مانند اوبونتو از Debian گرفته شده‌اند یکیست.اما لینوکس فدورا خط فرمانی متفاوت دارد که آن را از لینوکس قدیمی Red Hat به ارث برده است.

درست است که رابط کاربری گرافیکی هم در لینوکس‌های مختلف متفاوت است اما در کل شباهت هایی با هم دارند.

این مساله در خط فرمان به این صورت نیست و نمی‌توان هیچ وجه اشتراکی میان خط فرمآن‌های لینوکس‌ها، بجز عملکردشان پیدا کرد.

در اینجا ما برای شما روش استفاده از خط فرمان یکی از بهترین نسخه‌های لینوکس، یعنی اوبونتو را آموزش میدهیم.

۱.دستور ifconfig:

این دستور با فرض ifconfig شبکه‌ی Eth0، برای کارت شبکه‌ی اول IP برابر با 192.168.1.5 ست می کنه.

```
sudo ifconfig eth0 192.168.1.5 up
```

با همین دستور می‌توان به صورت زیر Netmask را هم می‌توانیم مقدار دهیم:

```
sudo ifconfig eth0 192.168.1.5 netmask 255.255.255.0 up
```

پس از انجام دادن تنظیمات بالا نیاز به Restart کردن شبکه هست. وحالا کد مربوط به Restart:

```
sudo /etc/init.d/networking restart
```

برای ست کردن Gateway دستوری به نام route وجود دارد:

```
sudo route add default gw 172.16.236.0
```

بعد از این دستور Default Gateway ما 172.16.236.0 می‌شود.

نکته ی مهم اینجاست که تمامی این تنظیمات پس از ریستارت شدن اوبونتو از بین می‌رود! حال برای ذخیره سازی این تنظیمات باید دستور زیر را هم وارد کنیم:

```
sudo gedit /etc/network/interfaces
```

حال فایلی باز می‌شود که به ما مقادیری مانند زیر را نشان میدهد:

```
iface eth0 inet static
Address 192.168.1.100
Netmask 255.255.255.0
Network 192.168.1.0
Broadcast 192.168.1.255
Gateway 192.168.1.254
```

کافیست مقادیر خودمان را جایگذین این مقدارها کنیم و تغییرات را ذخیره کنیم.

پس می‌توان نتیجه گرفت که دستورات اول فقط برای تست کردن شبکه بصورت موقت است و تمام کارها را می‌توان با دستور آخر انجام داد.

برای تنظیم DNS هم میتونید با دستور زیر فایل resolv.Conf را ویرایش کنید.

```
sudo gedit /etc/resolv.conf
```

در این دستور هم مانند دستور بالا باید فایل را ویرایش و به راحتی ذخیره کرد.

برای تنظیم Hostname بدین طریق عمل می‌کنیم:

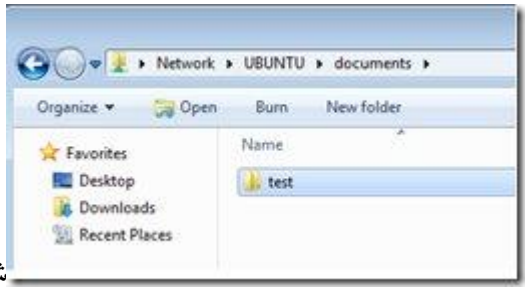
```
echo computername > /etc/hostname
```

تنظیم کارت شبکه برای آنکه از DHCPسرور آدرس IP بگیرد:

```
auto eth1
allow-hotplug eth1
iface eth1 inet dhcp
```

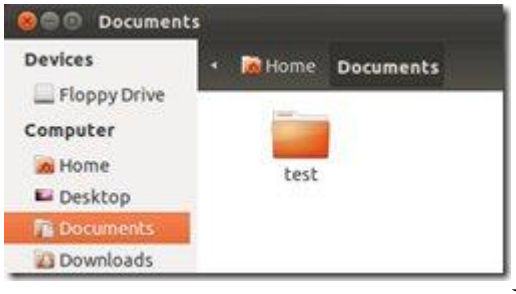
دستور Ping دقیقا به همان صورت که در ویندوز استفاده می‌شود قابل استفاده است.

۱۹-٤- به اشتراک گذاری پوشه در اوبونتو



آموز

ش زیر



نحوه اشتراک گذاری اطلاعات و پوشه‌های شما در اوبونتو را نشان میدهد و فرض بر این است که دو سیستم به هم متصل هستند و می‌خواهید یک پوشه را در اوبونتو به اشتراک بگذارید و در سیستم دیگر(اوبونتو یا ویندوز) آن پوشه را ببینید و از اطلاعات آن استفاده کنید.

(در شکل بالا پوشه Test به اشتراک گذاشته شده)

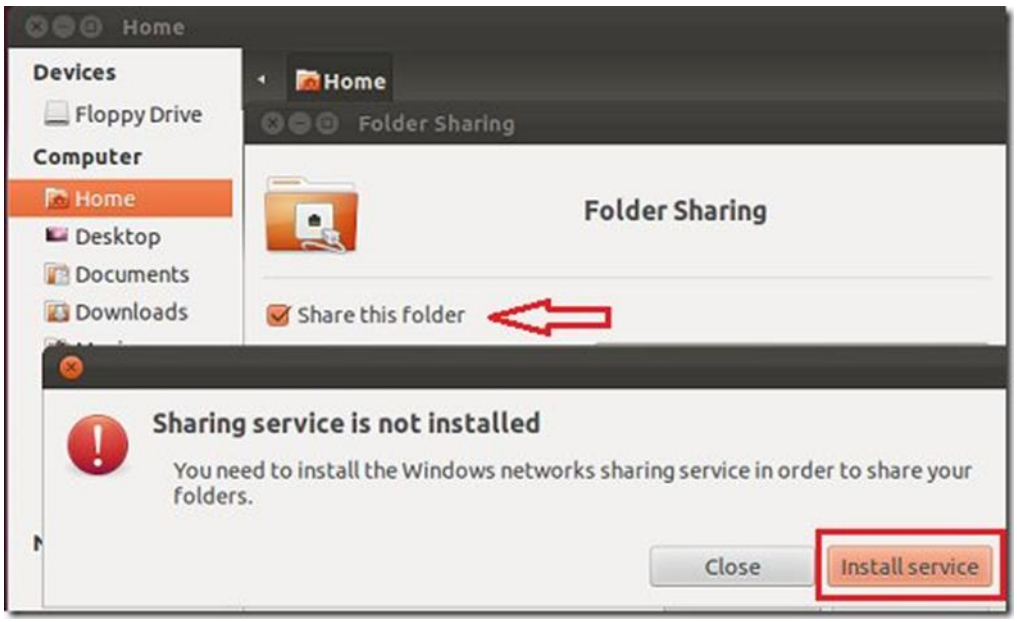
برای اشتراک گذاری یک فایل مراحل زیر را طی کنید:

بر روی پوشه ی مورد نظر راست کلیک کرده و گزینه Sharing Options را انتخاب کنید.



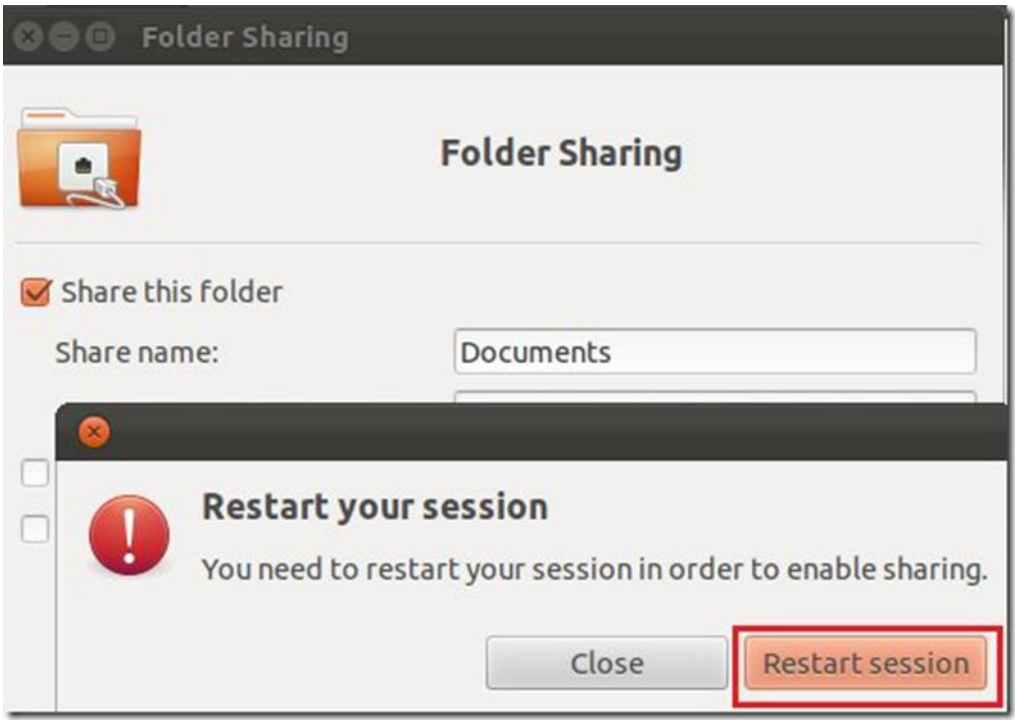
بعد از انتخاب و انجام این کار تیک کنار گزینه Share This Folder را بزنید و OK کنید.

حال بر روی گزینه Install Service کلیک کنید تا مخازن مربوط به اشتراک گذاری را نصب بکند.



برنامه Share بین ویندوز و اوبونتو برای اوبونتو Samba نام دارد و نیاز دارید Samba را هم از طریق Ubuntu Software Center نصب کنید.

بعد از نصب مخازن بر روی گزینه ی Restart Session کلیک کنید..



حالا تیک کنار گزینه Allow others to create and delete files in this folder را برای دادن حداکثر دسترسی به کامپیوتری که این فولدر را برای آن به اشتراک می‌گذارید بزنید.

(در صورت گذاشتن تیک گزینه بالا کامپیوتر میهمان می‌تواند فایل را پاک کند و یا پوشه‌ای جدید در فایل بسازد!)

اگر تیک کنار گزینه Guest Access را بزنید کامپیوتر میزبان بدون وارد کردن نام کاربری و پسورد به پوشه دسترسی پیدا می‌کند.

حالا به کامپیتور میهمان بروید (کامپیوتری که می‌خواهید فولدر را در آن ببینید ، ویندوز یا اوبونتو)

اگر سیستم میهمان اوبونتو بود: برای اشتراک گذاری اول باید در سیستم دیگر هم برنامه Sharing Service نصب بشود وبرای این کار بر روی یک پوشه راست کلیک کنید و Sharing Options را بزنید و پوشه را Share کنید تا برنامه Sharing Service نصب شود (همانند مرحله اول)

حالا به مرورگر فایل بروید (My Computer , Home و...) و از منوی سمت چپ گزینه Network را بزنید تا نام سیستم هایی که به شما شبکه شده‌اند را ببینید.

روی نام سیستمی که می‌خواهد به شما فایل را بدهد کلیک کنید و صبر کنید تا پوشه باز شود (در صورت زدن تیک کنار گزینه Guest Access از شما پسورد نمی‌خواهد و در غیر این صورت می‌خواهد)

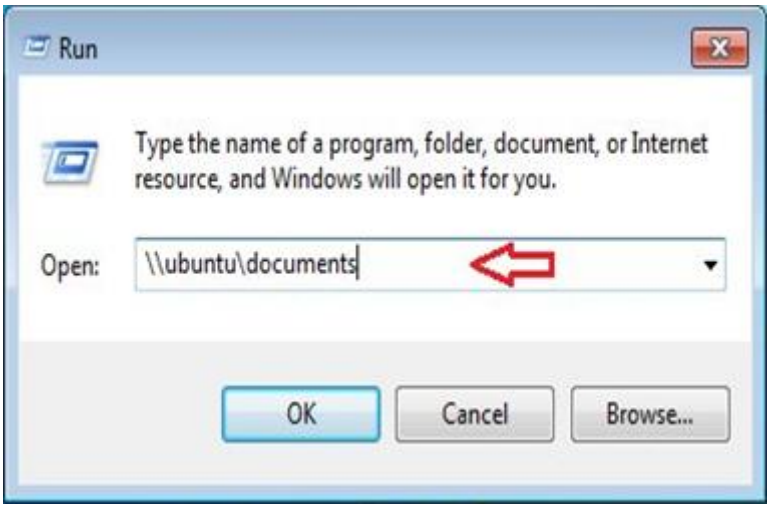
اگر سیستم میهمان ویندوز بود:به مسیر Start –> All Programs –> Accessories –> Run بروید و دستور زیر را در Run اجرا کنید:

\\Computer_Nameshare_Name

نام سیستم نام پوشه‌ای که به اشتراک گذاشتین

برای مثال در سیستم من:

\\Ali-PC\Documents



حالا بر روی OK کلیک می‌کنیم.

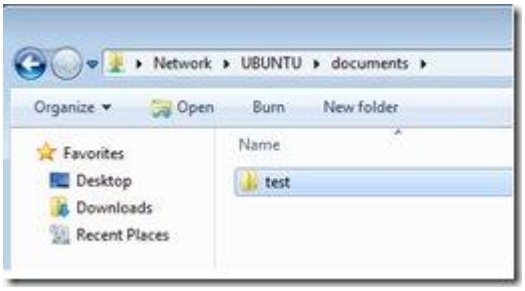
نکته: برای پیدا کردن نام کامپیوتر خود در لینوکس دستور Hostname را در خط فرمان لینوکس وارد کنید.

در اینجا Username و Password لینوکس را وارد می‌کنیم.



و پس از آن لینوکس و ویندوز آماده ی تبادل اطلاعات می‌شوند.





۱۹-۵- استفاده از ویندوز XP به عنوان سرور

۱) به **My Computer** خود رفته و یک فولدر را برای به اشتراک گذاشتن انتخاب کنید. سپس روی آن راست کلیک کرده و Sharing And Security را بیابید. سپس Network Setup Wizard را انتخاب کنید تا بعد از آن بتوانید عملیات

را شروع کنید و در حین ساختن شبکه جدید دقت کنید که Workgroup را چه چیزی تنظیم می‌کنید زیرا در تمامی سیستمهای متصل باید این مورد یکسان گذاشته شود.در انتها شما باید تیک Turn On File And Printer Sharing را بزنید و بعد از اتمام کار سیستم خود را ریستارت کنید!!!!!

۲) بعد از بوت شدن مجدد دوباره به فولدر قبلی رفته و به منوی Sharing And Security بازگردید و سپس Share This Folder On The Network را تیک بزنید.اسمی که می‌خواهید با آن به اشتراک گذاشته شود را انتخاب کنید و سپس اگر می‌خواهید که کاربران توانایی تغییر در فایل شما را داشته باشند " Allow Network Users To Change My Files" را تیک بزنید.

۱۹-۶- چگونه به سرور Samba متصل شویم؟

سرور خود را مطابق آنچه در بالا گفته شد پیکربندی کنید.

۱۹-۶-۱- کلاینت اوبونتو

روش اول را قبلا ذکر کردیم و ان رفتن به منوی Network و سپس Windows Network و پس از آن خلی گذاشتن فیلد نام و کلمه عبور و اتصال به شبکه می‌باشد.

راه جایگزین این است که از منوی Places گزینه Connect To Server را انتخاب کرده و سپس IP , Share Folder مورد نظر را وارد کنید و به شبکه متصل شوید.در این حالت نیازی به کلمه عبور نمی‌باشد.

۱۹-۶-۲- کلاینت ویندوز

در ویندوز نیز به آسانی می‌توانید به My Network Places رفته و سرورهای لینوکسی را مشاهده کرده و به آن‌ها متصل شوید و از فایل‌های آن استفاده کنید.

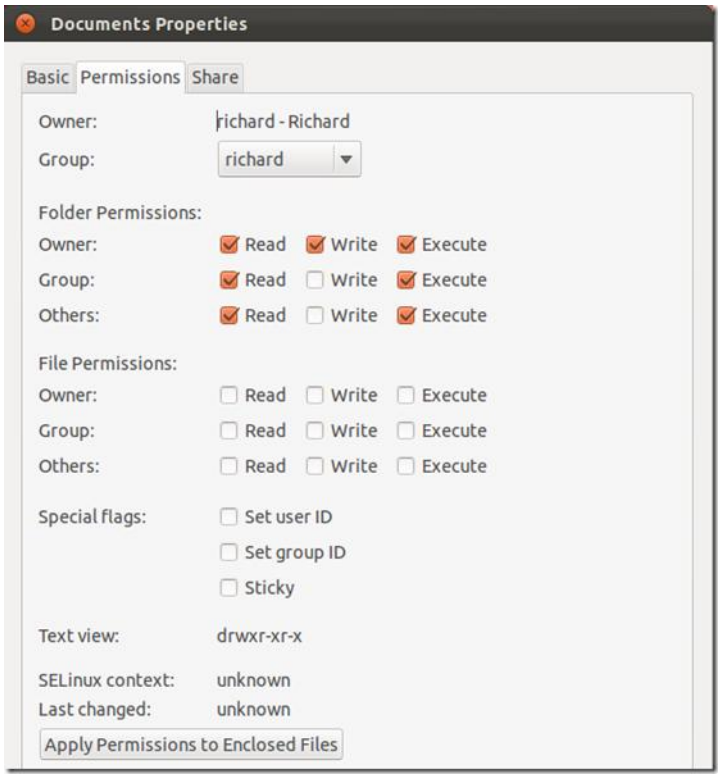
۱۹-۷- مدیریت سطح دسترسی در اوبونتو

سطح دسترسی یکی از مهمترین نکات مدیریت شبکه است. این مدیریت در اوبونتو به صورت پیشفرض غیر فعال استو باید آن را از طریق خط فرمان با یک دستور فعال کنیم تا بتوانیم از آن استفاده کنیم.

مدیریت حرفه‌ای سطوح دسترسی در اوبونتو بسیار سادست و تنها با خواندن این آموزش می‌توانید سطوح دسترسی را تغییر دهید. برای فعال کردن ابزار سطوح دسترسی دستور زیر را در ترمینال وارد کنید:

```
gsettings set org.gnome.nautilus.preferences show-advanced-permissions true
```

حالا کافیست برای تغییر سطوح دسترسی یک فایل روی آن کلیک راست کرده و Properties را انتخاب کنید. به سربرگ Permissions رفته و سطوح دسترسی رو بنا به نیاز خود تغییر میدهیم.



تغییر سطح دسترسی از طریق دستور chmod در محیط ترمینال نیز امکان پذیر است؛ که البته قدرت‌های بسیار بیشتری نسبت به حالت مشابه در ویندوز دارد.

۱۹-۷-۱- سطوح دسترسی در لینوکس

در جدیدترین و امن ترین فایل سیستم مایکروسافت یعنی NTFS 5.0 امکان تعیین سطوح مختلف دسترسی به دایرکتوری‌ها و فایل‌ها برای کاربران مختلف به صورت زیر وجود دارد:

۱- No Access

۲- Read

۳- Read & Execute

۴- Write

۵- Full Control

در حالت اول کاربر مورد نظر هیچگونه دسترسی به دایرکتوری مورد نظر ندارد. حالت دوم تنها می‌تواند فایل‌ها را ببیند ولی امکان اجرای فایل‌ها (ی اجرایی) را ندارد. در گزینه سوم این اختیار به کاربر داده شده است تا فایل‌ها را اجرا کند. در حالت چهارم یا Write کاربر قادر به انجام هر کاری جز تغییر سطوح دسترسی به دایرکتوری مورد نظر را دارد. به این حالت Modify هم گفته می‌شود و بالاخره در آخرین حالت کاربر می‌تواند هر آنچه را اراده می‌کند اعمال کند؛ این سطح دسترسی معمولا مخصوص Administrator بوده و به نااهلان داده نمی‌شود.

همانگونه که اشاره شد در این فایل سیستم امکان قطع کردن دسترسی کاربران به فایل‌ها وجود ندارد و تمام فایل‌های موجود در یک دایرکتوری به لحاظ سطح دسترسی تابع دایرکتوری خود هستند. اما در لینوکس استراتژی کاملا متفاوت است. دسترسی به هر فایل یا دایرکتوری توسط ۹ بیت اطلاعات اضافه‌ای که به فایل یا دایرکتوری چسبانده می‌شود برای ۳ کلاس ۳

بیتی کاربر، گروه کاربر و سایر کاربران، تعیین می‌شود که به ترتیب با کدهای u (کاربر)، g (گروه) و o (سایرین) مشخص می‌شوند. ۰ یا ۱ بودن بیت اول تعیین کننده دسترسی خواندن (Read) برای صاحب فایل (کاربر)، بیت دوم امکان نوشتن (Write) و ایجاد تغییر در فایل یا دایرکتوری مورد نظر و بالاخره بیت سوم امکان اجرای (eXecute) فایل‌های اجرایی را مشخص می‌کند. سه بیت دوم این دسترسی‌ها را برای کلاس گروه کاربر و سه بیت آخر دسترسی‌ها را برای سایر کاربران مشخص می‌کند. در صورتی که یک مجوز به کاربری داده نشده باشد به جای مجوز مورد نظر(یکی از حروف R، W یا X) هنگام نمایش مجوزها، علامت دش (-) دیده می‌شود. آنچه در زیر دیده می‌شود مجوز دسترسی کامل به یک فایل است. یعنی همه کاربران امکان خواندن، نوشتن و اجرای فایل را دارند:

کد: rwxrwxrwx

یا در حالتی که صاحب فایل دسترسی کامل، گروهش امکان خواندن و اجرا و سایرین هیچگونه دسترسی به فایل مورد نظر نداشته باشند این مجوزها به صورت زیر خواهد بود:

کد:

```
rwxr-x---
```

نمونه‌ای از این مجوزها را می‌توانید با اجرای فرمان ls -l مشاهده نمایید. توجه کنید که علاوه بر ۹ بیت ذکر شده، یک کاراکتر اضافه نیز در ابتدای این رشته وجود دارد که تعیین کننده نوع فایل است که برای فایل‌های عادی بصورت دش (-) و برای دایرکتوری‌ها بصورت d دیده می‌شود:

کد:

```
drwxr-xr-x
```

کد:

```
-rwxr-xr-x
```

نکته:

مجوز پیش فرض برای فایل‌های جدید بصورت زیر است:

کد:

```
rw-r--r--
```

و در صورتی که فایلی توسط یکی از کامپایلرهای موجود اجرایی شده باشد x (یا امکان اجرا کردن) به دسترسی‌ها اضافه می‌گردد. مجوز پیش فرض دسترسی به یک دایرکتوری جدید نیز مشابه همین حالت است:

کد: rwxr-xr-x

۱۹-۷-۲- تغییر سطح دسترسی

در صورتی که بخواهید مجوزهای پیش فرض را برای نشست جاری خود تغییر دهید می‌توانید از دستور umask استفاده کنید. برای تغییر مجوزهای یک فایل یا دایرکتوری کاربری که این اختیار را دارد (کاربر ریشه یا صاحب فایل یا دایرکتوری) می‌تواند با دستور chmod این کار رابوسیله یکی از دو روش زیر انجام دهد.

۱- در روش نخست پس از دستور chmod می‌توان با علامت‌های "+" یا "–" یک یا چند مجوز را به کلاس‌ها افزود و یا از آن‌ها گرفت. در این حالت کلاس‌ها با کدهایی که در بالا ذکر شد تعیین می‌شوند.مثلا:

کد:

```
#chmod go-rx anything
```

این دستور تعیین می‌کند که مجوز خواندن و اجرای فایلی به نام anything از کلاس گروه کاربر (u) و سایرین (o) گرفته شود و برعکس آن به صورت زیر است:

کد:

```
#chmod go+rx anything
```

۲- در روش دوم مجموع سه سطح دسترسی(خواندن،نوشتن و اجرا) به صورت یک عدد بین صفر تا هفت برای ۳ کلاس کاربر، گروهش و سایرین به صورت زیر تعیین می‌شود و پس از دستور chmod می‌آید. برای خواندن عدد چهار، برای نوشتن عدد دو و برای اجرا عدد یک منظور می‌شود. یعنی هفت(۱+۲+۴) نشان دهنده دسترسی کامل است در نتیجه مثلا ۷۷۷ نشان دهنده اعطای دسترسی کامل به همه کاربران است.مثلا:

کد:

```
#chmod 750 anything
```

این دستور نیز تعیین می‌کند که مجوزها بصورت زیر تغییر کنند:

کد:

```
rwxr-x---
```

به طور پیش فرض، هر کاربری که فایلی را ایجاد نماید، مالک آن فایل شناخته می‌شود. در صورتی که بخواهید مالکیت یک فایل را تغییر دهید، باید از دستور chown استفاده نمایید. هنگامی که مالکیت یک فایل یا دایرکتوری را به کاربری اعطا کنید، آن کاربر دارای تمام مجوزها برای انجام تغییرات و تغییر مجوزها روی آن فایل یا دایرکتوری است. به مثال‌های زیر توجه کنید:

کد:

```
#chown patoghu anything
#chown -R satsat /home/patoghu
```

در مثال نخست، مالکیت فایلی به نام anything به کاربر patoghu اعطا می‌شود. در مثال دوم، مالکیت دایرکتوری home/patoghu و تمام فایل‌ها و دایرکتوری‌های زیر آن به کارب patoghu اعطا می‌شود. توجه داشته باشید که در چنین مواردی از گزینه R در دستور استفاده می‌شود.

فصل ۲۰

معرفی برخی از نرم‌افزارهای ارتباطی

در این فصل به معرفی و آموزش برخی از نرم‌افزارهای ارتباطی خواهیم پرداخت.

۲۰-۱- نرم‌افزار NetMeeting



فرض کنید که شبکه محلی خود را راه اندازی کرده‌ایم. اما آیا کاربرد شبکه، فقط به اشتراک گذاری منابع است؟ آیا کاربران نمی‌توانند به صورت Online با یکدیگر ارتباط برقرار کنند؟ جواب کاملاً مشخص است. جواب شما چیست؟

یکی از نرم‌افزارهایی که برای برقراری ارتباط در شبکه به کار می‌رود، نرم‌افزار NetMeeting است. این نرم‌افزار به صورت رایگان و توسط Microsoft به همراه ویندوز XP عرضه شده است. از این نرم‌افزار برای چت کردن از طریق شبکه یا نمایش دسکتاپ یک کامپیوتر دیگر استفاده می‌شود.

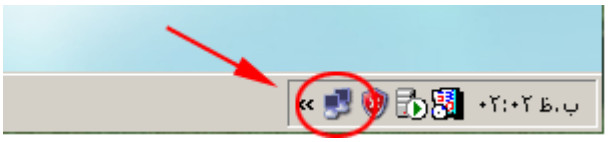
در ادامه بخش، به آموزش این نرم‌افزار می‌پردازیم.

برای این کار بایستی این نرم‌افزار را هم در Client و هم در Server اجرا کنیم. البته این مفهوم Client و Server با مفهوم Client و Server واقعی در شبکه متفاوت است. در این مبحث منظور از Server، کامپیوتری است که صفحه دسکتاپ آن را دیگران مشاهده خواهند کرد. همچنین منظور از Client نیز، کامپیوتر هایی هستند که صفحه دسکتاپ Server را مشاهده خواهند کرد.

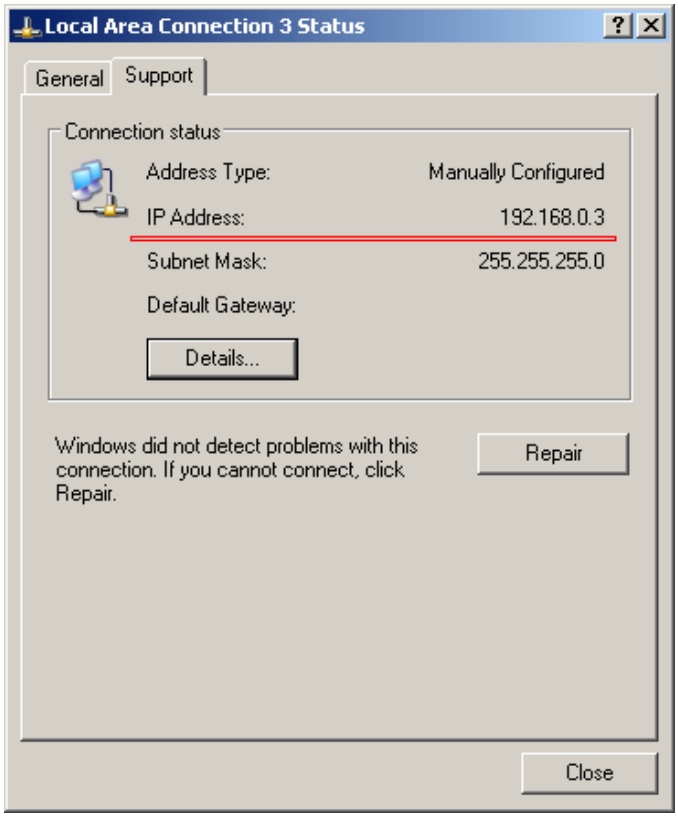
۲۰-۱-۱- مشاهده آدرس IP در سرور

پس از اجرای برنامه، Clientها بایستی به Server متصل شوند. برای این اتصال، Clientها به آدرس IP مربوط به Server نیاز دارند. برای پیدا کردن آدرس IP مربوط به Server، بر روی خود Server مراحل زیر را دنبال نمایید:

۱- بر روی آیکون کارت شبکه که در سمت راست نوار وظیفه قرار دارد، دو بار کلیک نمایید.



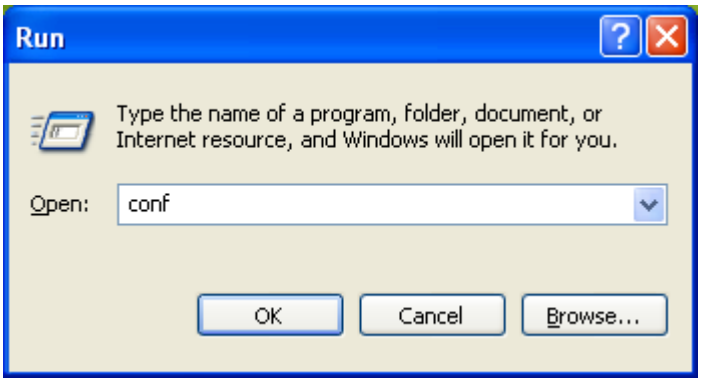
۲- در این حالت پنجره‌ای مانند روبرو نمایان می‌شود که دارای دو زبانه General و Support می‌باشد، زبانه دوم (Support) را انتخاب کنید. عبارت IP Address شماره IP سیستم شما را اعلام می‌کند.



۳- راه دیگر نیز این است که در محیط Command Prompt دستور IpConfig را وارد نمایید.

۲۰-۱-۲- اجرا و پیکربندی نرم‌افزار

حال نوبت به آموزش نرم‌افزار می‌رسد. برای اجرای برنامه، ابتدا وارد Run شده و سپس دستور Conf را اجرا نمایید:



راه دیگر نیز اجرای مستقیم نرم‌افزار از طریق منوی Start است.



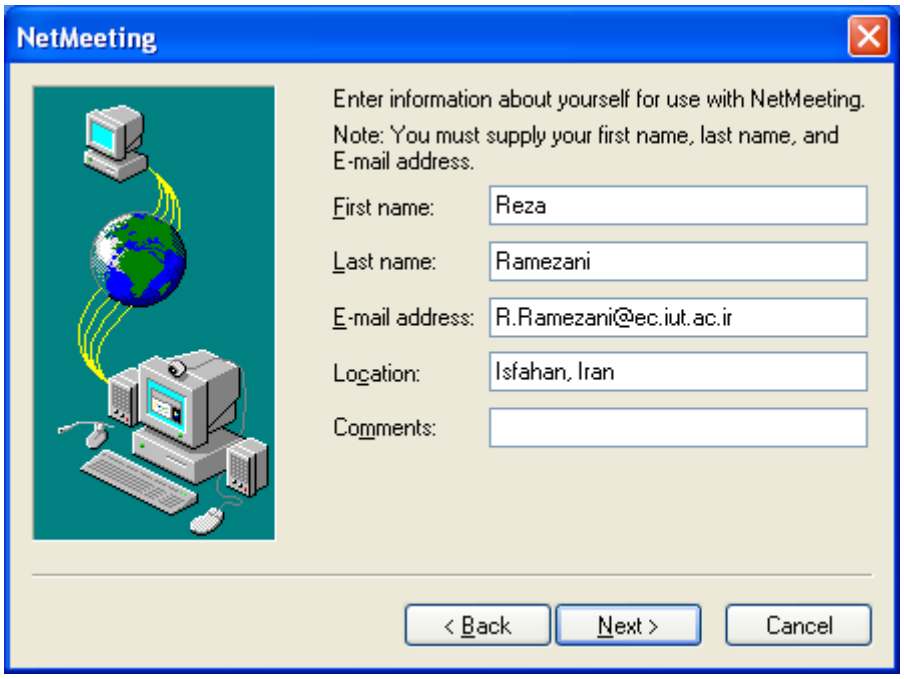
بعد از اجرا شدن صفحه زیر به ترتیب تا آخر NEXT را میزنیم.



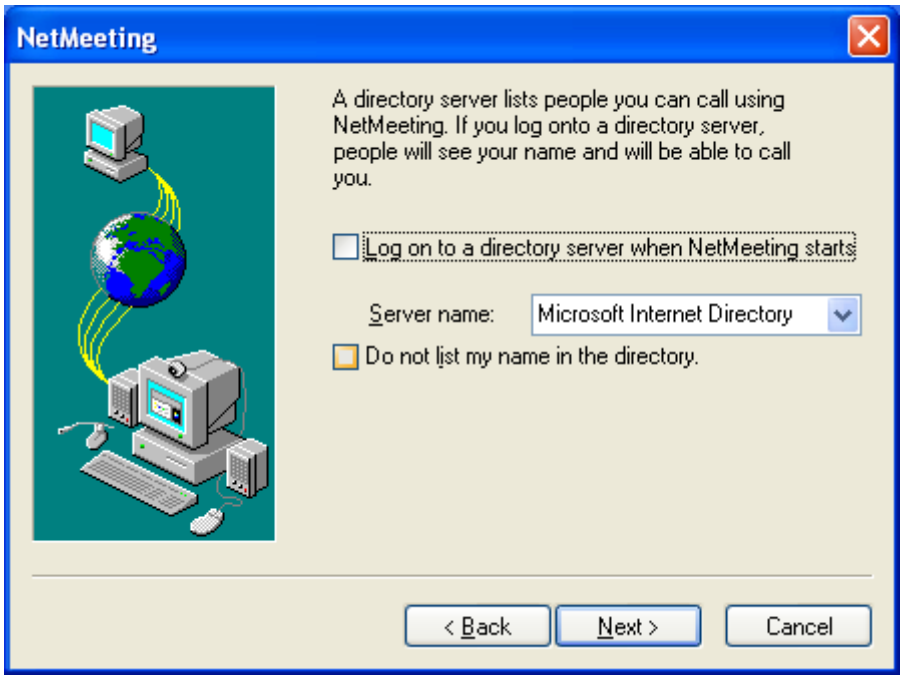
در قسمت زیر همانطور که می‌بینید، این قسمتها حتما باید پر شوند.

۱. **First Name**
۲. **Last Name**
۳. **Email Address**

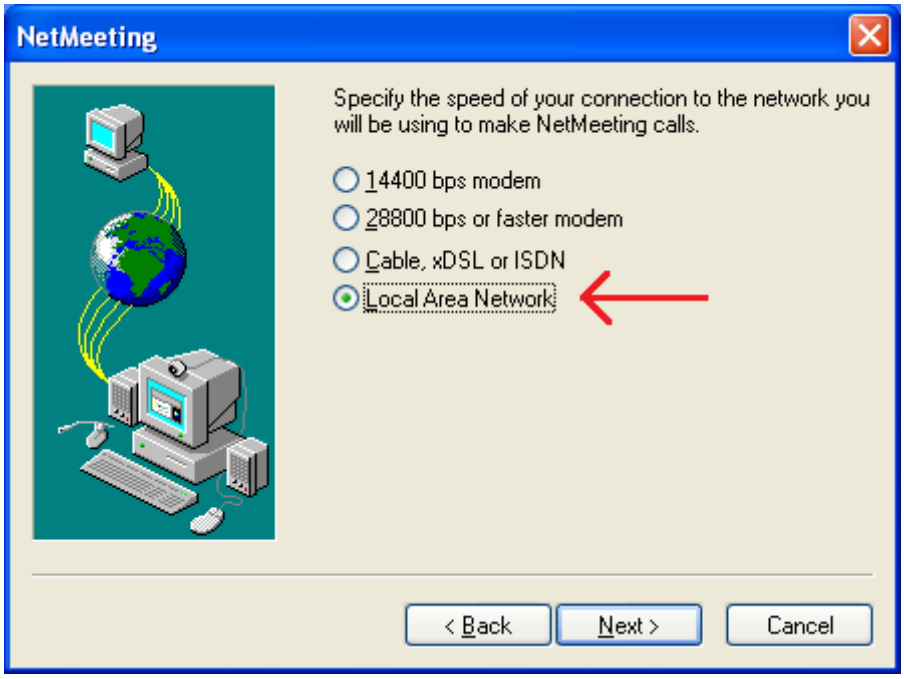
بقیه قسمت‌ها زیاد پر کردنش مهم نیست و ایمیل را هم می‌توانید یک مقدار فرضی وارد کنید و الزامی ندارد که حتما ایمیل خودتان باشد.



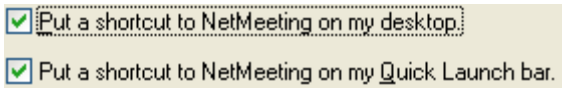
صفحه بعد امکان اتصال به Directory Server را به ما می‌دهد. بدون انتخاب آن، روی دکمه Next کلیک کنید.



چون در محیط شبکه محلی از این نرم‌افزار استفاده می‌کنید، گزینه آخر را انتخاب کرده و روی Next کلیک کنید.



در صفحه بعد می‌توانید محل قرار گیری میانبرهای نرم‌افزار را تعیین نمایید. روی Next کلیک کنید.



صفحه بعد، صفحه آغاز ویزارد میکروفون و اسپیکر می‌باشد. روی Next کلیک کنید.

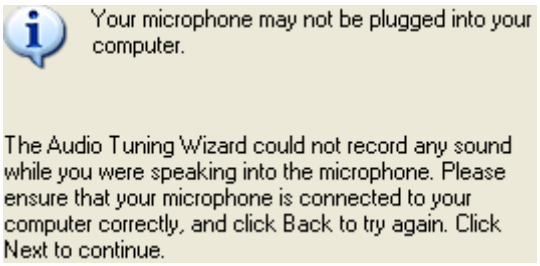
در صفحه جدید، با زدن دکمه Test، صدا را تست کرده و روی Next کلیک کنید.



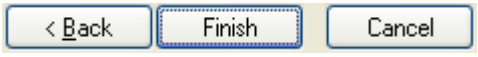
این صفحه مربوط به تست ضبط صدا می‌باشد. روی Next کلیک کنید.



این صفحه وضعیت میکروفون را نشان می‌دهد. روی Next کلیک کنید.



در نهایت روی Finish کلیک کنید.



کار تمام شده و برنامه اجرا می‌شود.



۲۰-۱-۳- نحوه کار با برنامه

در شکل زیر، صفحه اصلی برنامه را مشاهده می‌نمایید.



قسمت‌های مختلف برنامه به صورت زیر است:

A: Place Call، برای متصل شدن به کامپیوترهای محیط شبکه

B: End Call، برای خارج شدن و قطع اتصال برنامه از شبکه

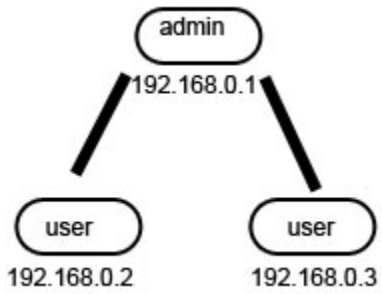
C: Transfer File، برای اشتراک گذاری و انتقال فایلها

D: White Board، برای نقاشی و.... (قابل مشاهده برای دیگران)

E: Chat، برای گفتمان و چت در محیط شبکه

F: Share Program، به اشتراک گذاری برنامه‌ها برای دیگر کاربران

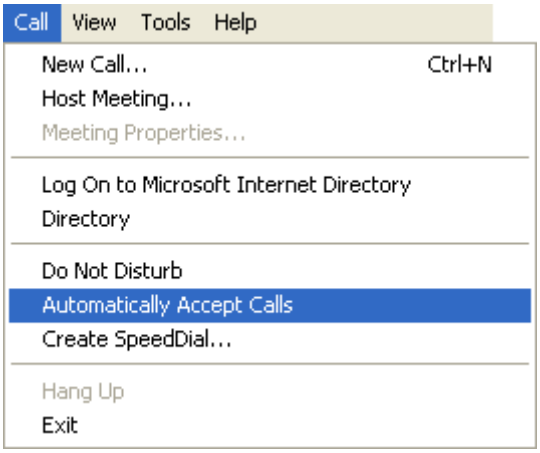
ما در محیط شبکه برای اتصال با برنامه NetMeeting به دیگر کامپیوترها، نیاز به IP داریم. هر کامپیوتر یک IP مخصوص به خود را دارد. مثلاً به صورت زیر:



فرض می‌کنیم که ما کامپیوتر شماره ۱ هستیم با آدرس ۱۹۲.۱۶۸.۰.۱ و می‌خواهیم به کامپیوتر شماره ۲ با آدرس ۱۹۲.۱۶۸.۰.۲ وصل بشویم. طبق شکل زیر عمل می‌کنیم. ابتدا آدرس IP کامپیوتر مقصد را وارد کرده و سپس روی دکمه Call کلیک می‌نماییم.



در این حالت، هر بار و هنگام اتصال از Client به Server، سیستم سوالی از کاربر Server منوط به پذیرش کاربر Client می‌پرسد. برای حذف این سوال، در برنامه اجرا شده در Server، از منوی Call گزینه Automatically Accept calls را انتخاب نمایید.



در کامپیوتری که قصد دارید تصویر آن را به اشتراک بگذارید، بر روی آیکون Share Program کلیک نمایید.



نکته: بعد از برقراری ارتباط NetMeeting موجود در سیستم‌ها با یکدیگر، انتخاب یکی از کامپیوترها برای Share تصویر، اختیاری بوده و لزومی ندارد دقیقاً کامپیوتر اصلی (مرکزی) را برای اشتراک تصویر در نظر بگیریم.

در کادر ظاهر شده عبارت Desktop را در سمت چپ و دکمه Share را در سمت راست انتخاب نمایید.



انتخاب عبارات دیگر (برنامه‌های در حال اجرا) موجب به اشتراک گذاشته شدن تصویر آن برنامه‌ها بر روی مانیتور سایر سیستم‌ها خواهد شد. در حالی که انتخاب کلمه Desktop کل محتویات صفحه نمایش شما را به اشتراک می‌گذارد.

بدین ترتیب تصویر کامپیوتر مورد نظر بر روی صفحه نمایش سایر کامپیوترها مشاهده خواهد شد. البته سیستم‌های دیگر، این تصویر را در ابعاد کوچکتر خواهند دید که برای بزرگ کردن اندازه آن می‌توان از کلیدهای ترکیبی CTRL+Enter یا ALT+Enter استفاده نمود.

جهت برداشتن Share تصویر نیز مجددا دکمه Share Program را فشرده، در کادر ظاهر شده، گزینه مورد نظر (Desktop) را انتخاب و دکمه Unshare یا Unshare All را کلیک می‌نماییم.

لازم به ذکر است بسته شدن نرم‌افزار NetMeeting موجب قطع ارتباط سیستم فعلی با سایر سیستم‌ها خواهد شد.

۲۰-۲- نرم‌افزار RaidCall

اگر بخواهم در یک جمله این نرم‌افزار را توصیف کنم، باید بگویم که این نرم‌افزار مخصوص افراد بیکار و بی‌عار است.



RaidCall یکی دیگر از نرم‌افزارهایی است که به منظور برقرار کردن ارتباط از طریق اینترنت توسط افرادی که در مکان‌های مختلفی قرار دارند، طراحی و ساخته شده است. ویژگی‌های برجسته RaidCall باعث شده است تا این برنامه بیشتر به منظور چت گروهی، چت صوتی با کیفیت بالا و همچنین برقراری ارتباطات گروهی برای بازی خورها به کار می‌رود (مخصوصاً بازی هایی که به کار گروهی هماهنگی احتیاج دارند یا بازی‌های اینترنتی مثل تراوین خان). اما می‌توان از آن برای هر نوع فعالیت دیگری اند بحث‌های طولانی درسی و کاری نیز استفاده نمود. صدای واضح و با کیفیت و امکان ضبط صدا از

ویژگی‌های برجسته این نرم‌افزار می‌باشد. این نرم‌افزار می‌تواند کیفیت صدای خوبی را بدون قطعی در اختیار شما قرار دهد و دیگر احتیاجی به اجاره ی سرور و یا ایجاد سرور و تنظیم آن توسط خودمان نیست.

۲۰-۲-۱- قابلیت‌های کلیدی نرم‌افزار Raidcall

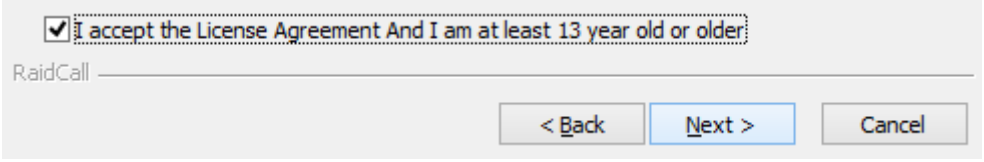
- محیط کاربری زیبا و طراحی شده مبتنی بر فلش
- ملحق شدن به یک شبکه اجتماعی جدید و ملاقات تعداد زیادی از دوستان در شبکه Raidcall
- یک سرویس صوتی رایگان و حرفه‌ای بر اساس محاسبات ابری
- اجرای روان و سریع
- حفظ حریم خصوصی اشخاص
- استفاده کم از منابع سیستم
- امکان ضبط صدا
- امکان گفتگوی مدیر با اعضا
- متکی بر محبوب ترین و قدرتمندترین موتور صوتی برای کاهش سر و صدا و ارتقاء کیفیت صدا
- استفاده از UDP به عنوان پروتکل‌های ارتباطی جهت تاخیر حداقلی و ناچیز در مقایسه با زمان تاخیر در پروتکل‌های TCP که توسط سیستم‌های VoIP مورد استفاده قرار می‌گیرد
- بهره وری بالا در برقراری ارتباط صوتی
- استفاده آزادانه و راحت از نرم‌افزار در زمان انجام بازی
- و...

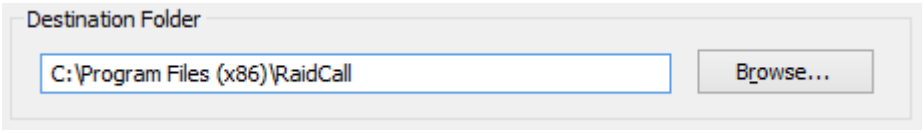
۲۰-۲-۲- نصب نرم‌افزار

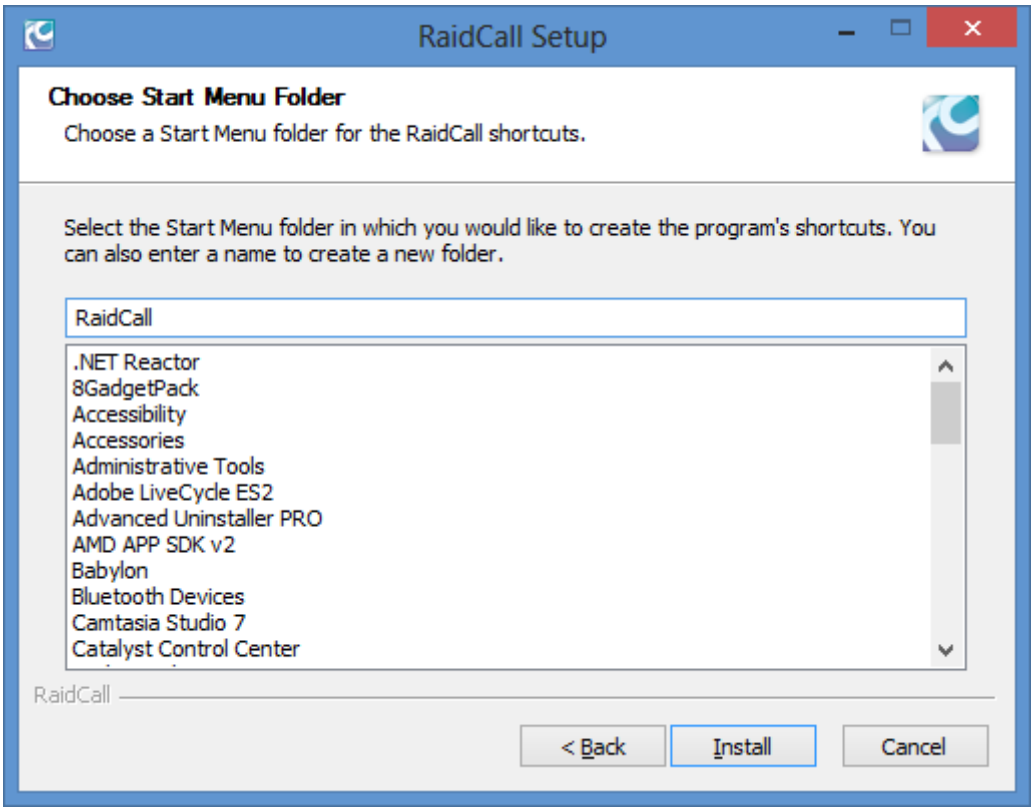
بعد از دانلود نرم‌افزار، در صفحه خوش آمد گویی روی Next کلیک کنید.

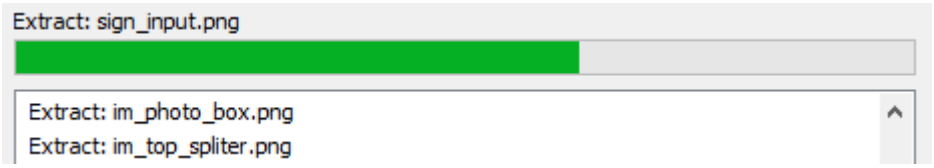


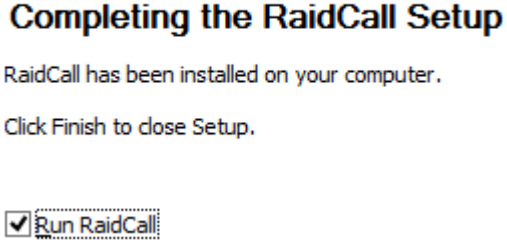
سایر مراحل نصب را دنبال نمایید.





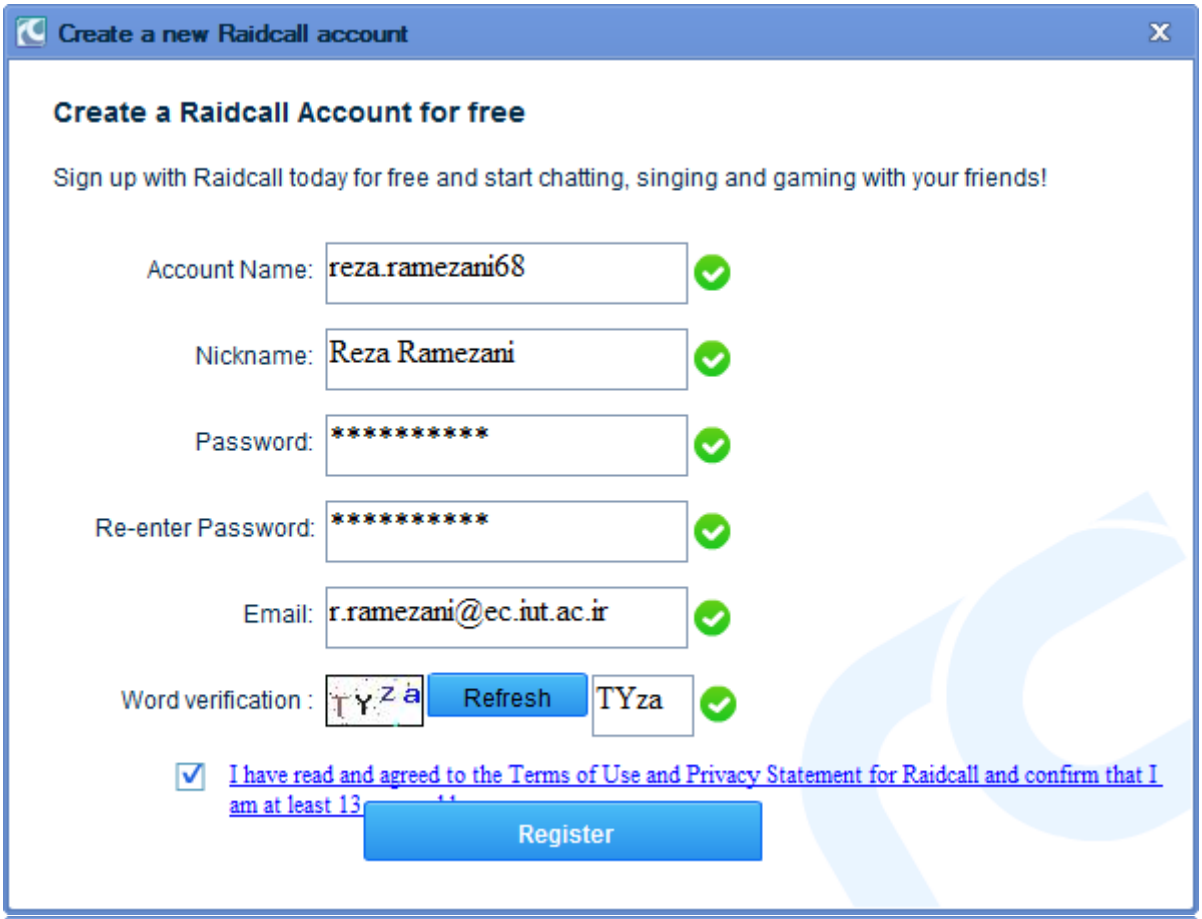






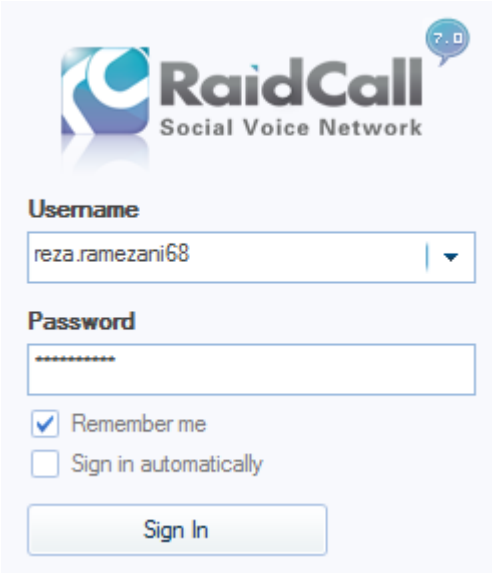
۲۰-۲-۳- ایجاد حساب کاربری

بعد از اجرای نرم‌افزار، نیاز به ساخت یک حساب کاربری دارید. روی گزینه Create a new account کلیک کنید تا صفحه ثبت نام باز شود.

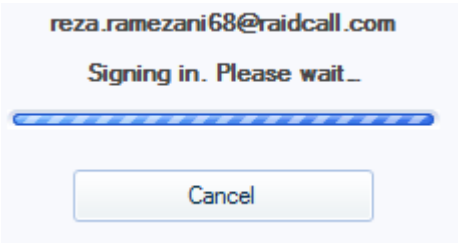




بعد از ثبت نام، به نرم‌افزار Login کنید.

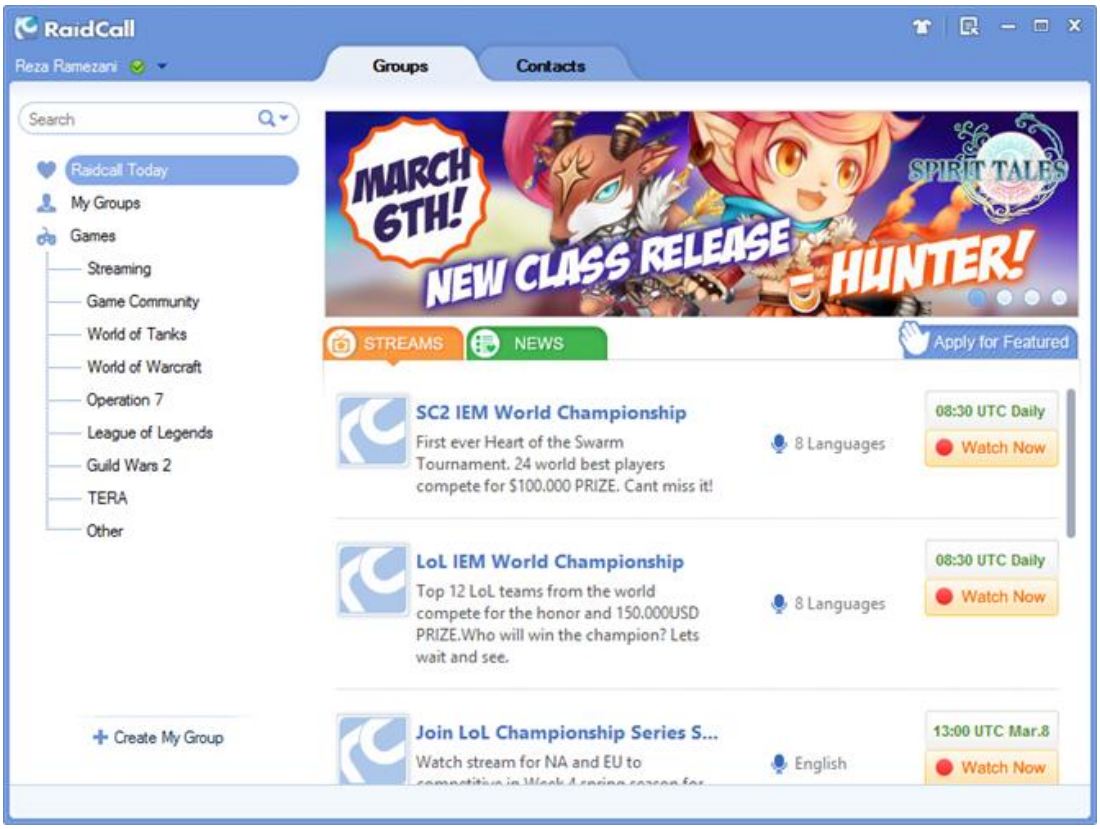


منتظر بمانید تا عمل Login انجام شود.



۲۰-۲-۴- اجرای نرم‌افزار

بعد از ورود صفحه زیر را مشاهده می‌کنید.



در این قسمت به شرح منوی Raidcall می‌پردازیم:

در قسمت Status که برای تعیین وضعیت کاربر هست؛ یعنی آزاد، مشغول و...

در قسمت My Profile هم می‌توانید تنظیمات کاربری از قبیل امضا، درباره خودتان و... را اعمال کنید.

با گزینه Sing out هم که آشنا هستید.

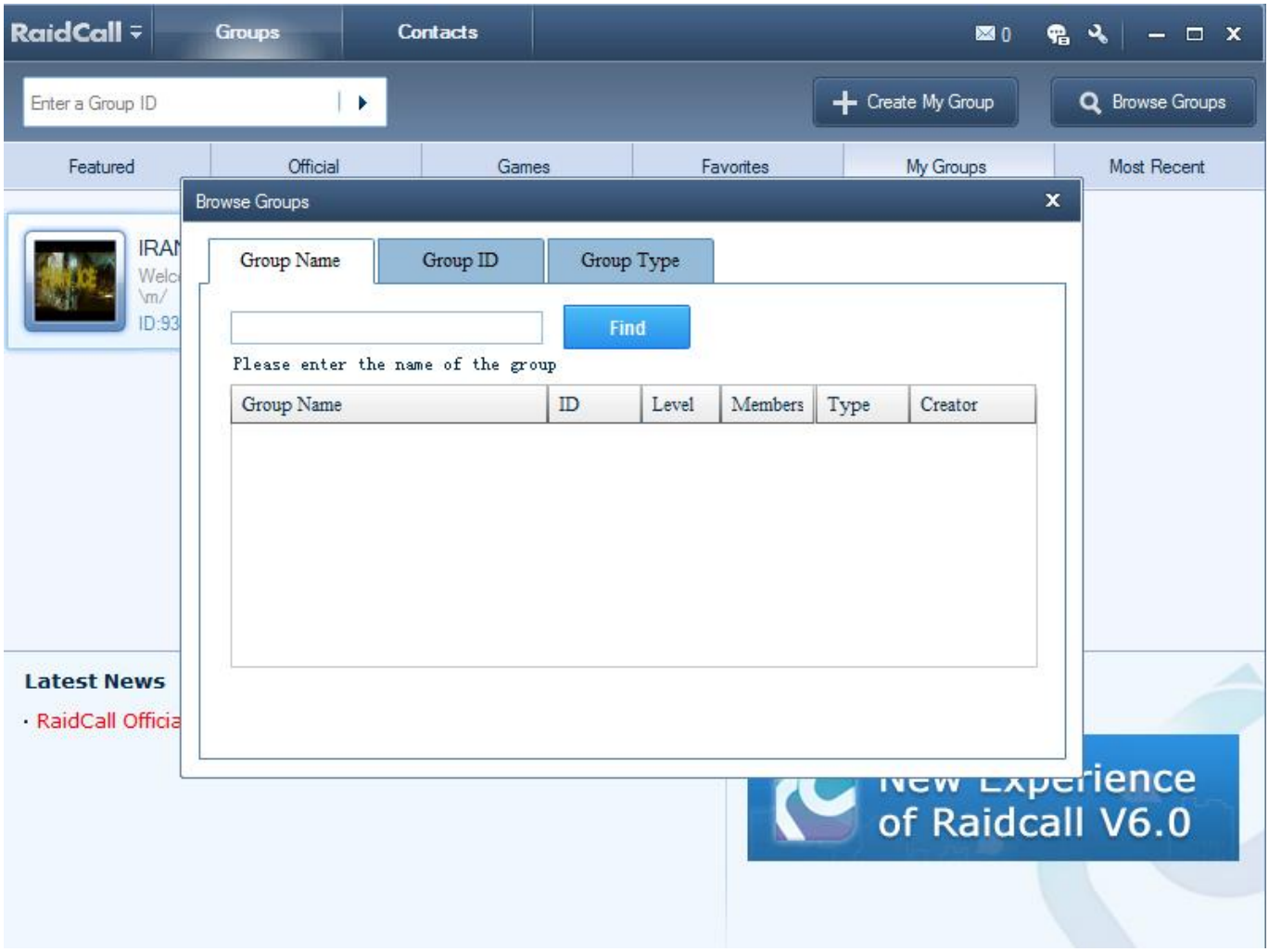


اگر بخواهید وارد یکی از سرورها شوید، می‌توانید هم ID آن انجمن و هم نام آن انجمن را وارد نمایید.

برای وارد کردن ID انجمن یا کنفرانس مورد نظر از اینجا اقدام کنید: مثلا در شکل زیر انجمن Iran Nice را مورد جستجو قرار داده‌ایم.



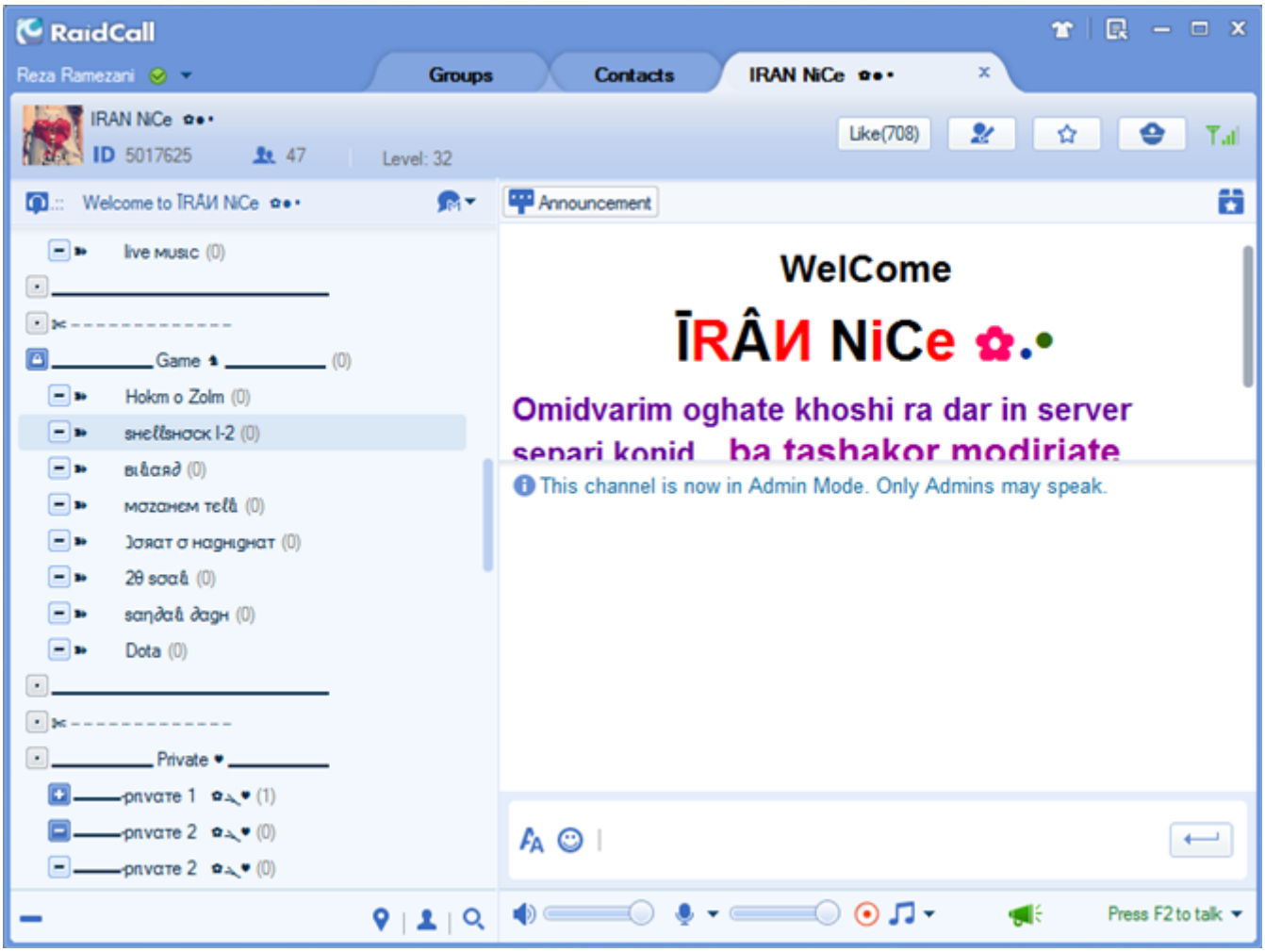
اگر فقط اسمش را دارید و برای مثال اسمش (International Server) هست، با کلیک روی دکمه Browes Groups این صفحه را می‌بینید:



در کادر می‌توانید اسم گروه رو وارد کنید و دکمه Find رو کلیک کنید. از لیست جست و جوها یکی رو انتخاب و دکمه Group Join برای عضو شدن در آن گروه و دکمه Enter صرفا برای ورود به اون گروه هست.درtab، Group Type هم می‌توان نوع گروه را بستگی به علاقت انتخاب کرد: بازی، سرگرمی و...

بعد از ورود به یک گروه این صفحه رو می‌بینید که در کادر سمت چپ می‌توانید با دابل کلیک وارد شوید.

حالا داخل این صفحه هر کاری بخواهید می‌توانید انجام دهید. مثلا کار علمی!!!



۲۰-۳- نرم‌افزار Skype



سال‌ها از اختراع بزرگ الکساندر گراهام بل می‌گذرد. اختراعی که موجب شد گوشه‌های دور دنیا به هم نزدیک شود. تلفن شروع فعالیت‌های مخابراتی دنیاست .

امروزه تلفن دیگر جواب گو نیازها نیست. تماس‌های تلفنی علاوه بر هزینه بالا از مشکلات متعددی مانند قطعی، سرعت پایین، پارازیت و... برخوردارند. دست اندر کاران حوزه IT در سال‌های اخیر توجه خود را بر روی سیستم **Voice Over Internet Protocol** که به اختصار **VOIP** خوانده می‌شود، معطوف کرده‌اند.

به طور خلاصه اگر سیگنال‌های آنالوگ را به داده‌های دیجیتال تبدیل و آن‌ها را از طریق اینترنت از مبدا به مقصد منتقل کنیم، به سیستمی رایگان برای مکالمه دست پیدا کرده‌ایم. سیستمی که برای استفاده از آن فقط کافی ست هزینه اینترنت را بپردازیم.

در این بخش سعی داریم شما را با یکی از سرویسهای تلفن اینترنتی به نام Skype آشنا کنیم و در ادامه نحوه استفاده از آن را کامل شرح می‌دهیم .

Skype، نرم‌افزاری رایگان برای تماس‌های اینترنتی شماست. شما نه تنها با یک نفر که می‌توانید کنفرانس‌های تلفنی خود را با بهترین کیفیت برگزار کنید. می‌توانید ویدئو کنفرانس داشته باشید. عکس‌ها، نوشته‌ها و فایل‌های خود را به اشتراک بگذارید.

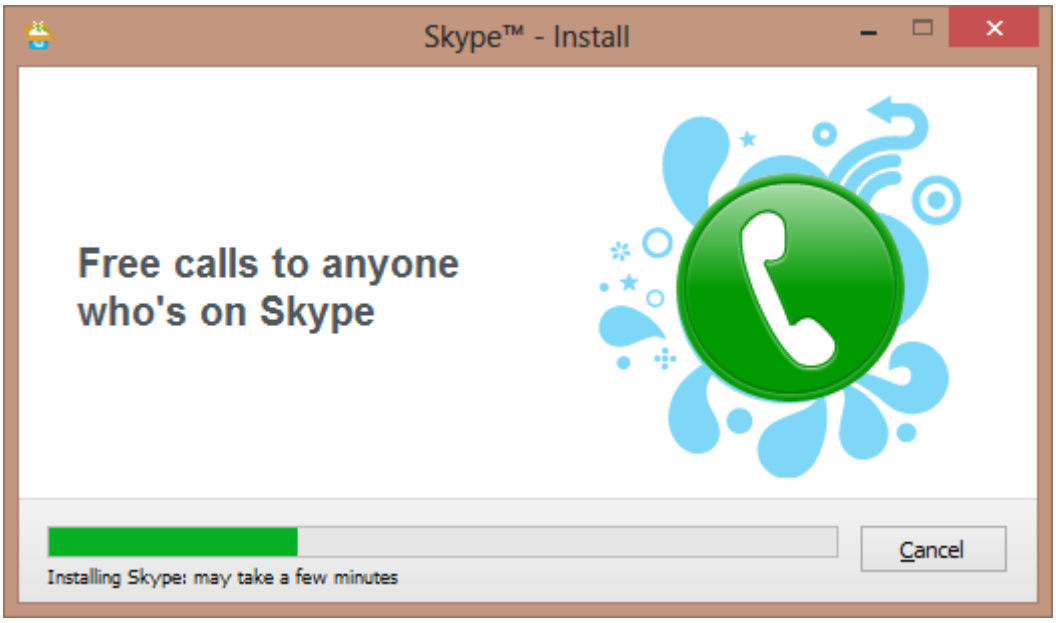
۲۰-۳-۱- نصب نرم‌افزار

ابتدا از سایت رسمی Skype، نرم‌افزار را دانلود کنید. به این صورت که وارد سایت Skype می‌شوید از منو بالای سایت به قسمت دانلود رفته و نرم‌افزار را دانلود و پس از آن، فایل را روی سیستم خود نصب می‌کنید.

برای نصب، ابتدا زبان را انتخاب کرده و سپس روی I agree – Install کلیک کنید.



صبر کنید تا عملیات نصب به پایان برسد. نصب این نرم‌افزار بسیار راحت است.

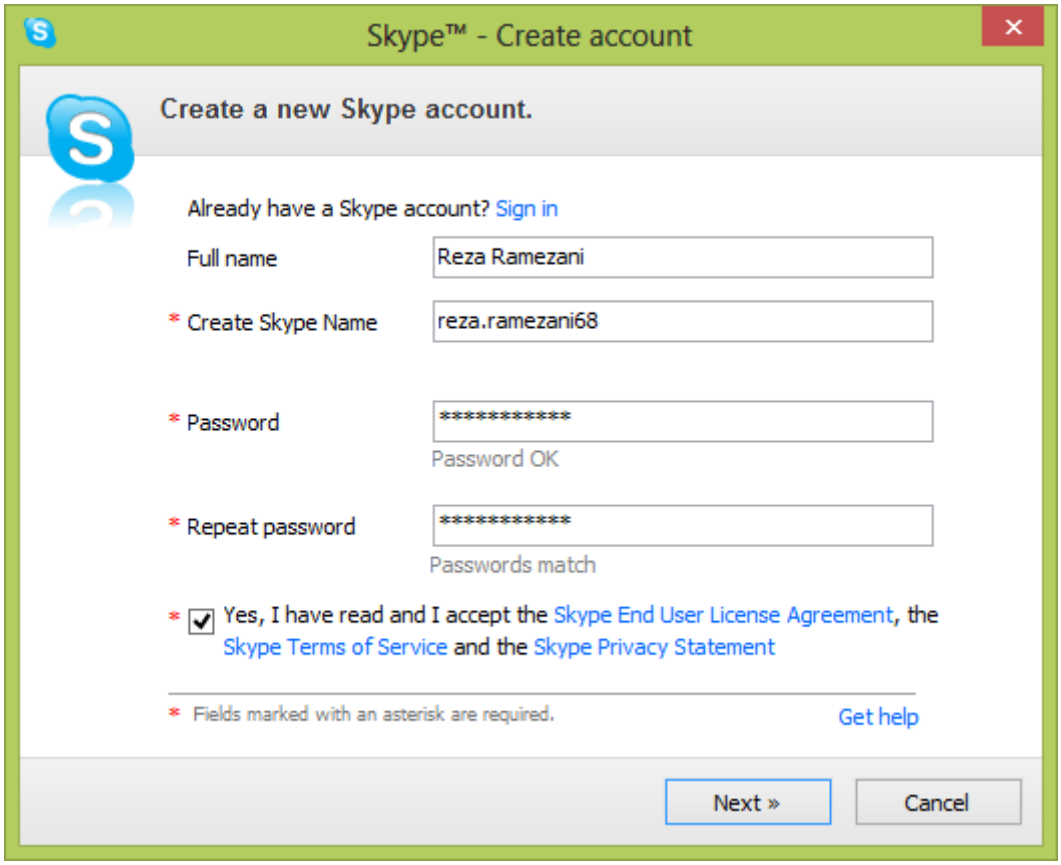


۲۰-۳-۲- ایجاد حساب کاربری

پس از نصب شدن برنامه، نوبت به ساختن اکانت می‌رسد. نرم‌افزار را باز کنید و مطابق تصویر زیر برای ایجاد یک حساب کاربری، روی گزینه Don't Have a Skype Name? کلیک کنید.

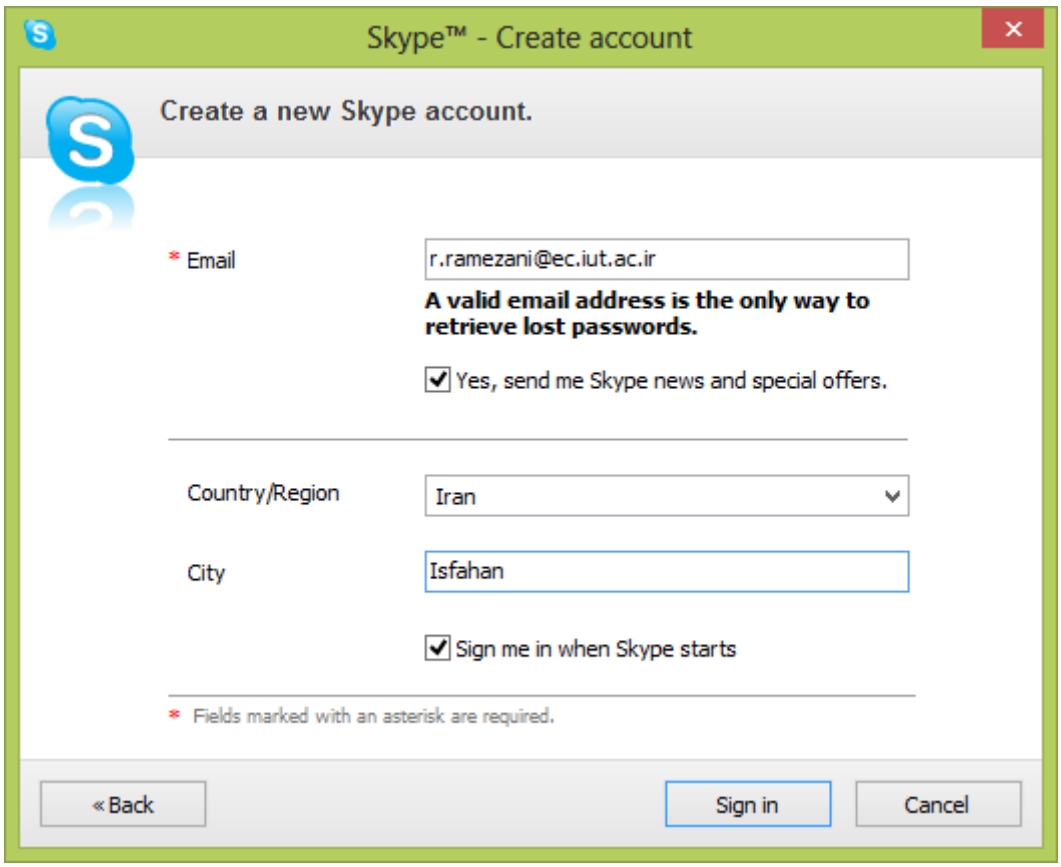


سپس مطابق تصویر زیر اسم کامل خود، اسمی که در Skype به آن شناخته می‌شوید و پسورد خود را پر کنید. توجه داشته باشید که اسم Skype شما باید بیشتر از ۶ کاراکتر و پسوردتان باید متشکل از اعداد و حروف باشد. چک مارک آخرین گزینه را هم فعال کنید. این گزینه به معنی پذیرش قوانین Skype است.



سپس Next را بزنید و در صفحه دوم ایمیل، کشور و شهرتان را بنویسید. کشور Iran هم در گزینه‌ها وجود دارد.

در نهایت روی Sign in کلیک کنید. اکانت شما به همین راحتی ساخته شد.

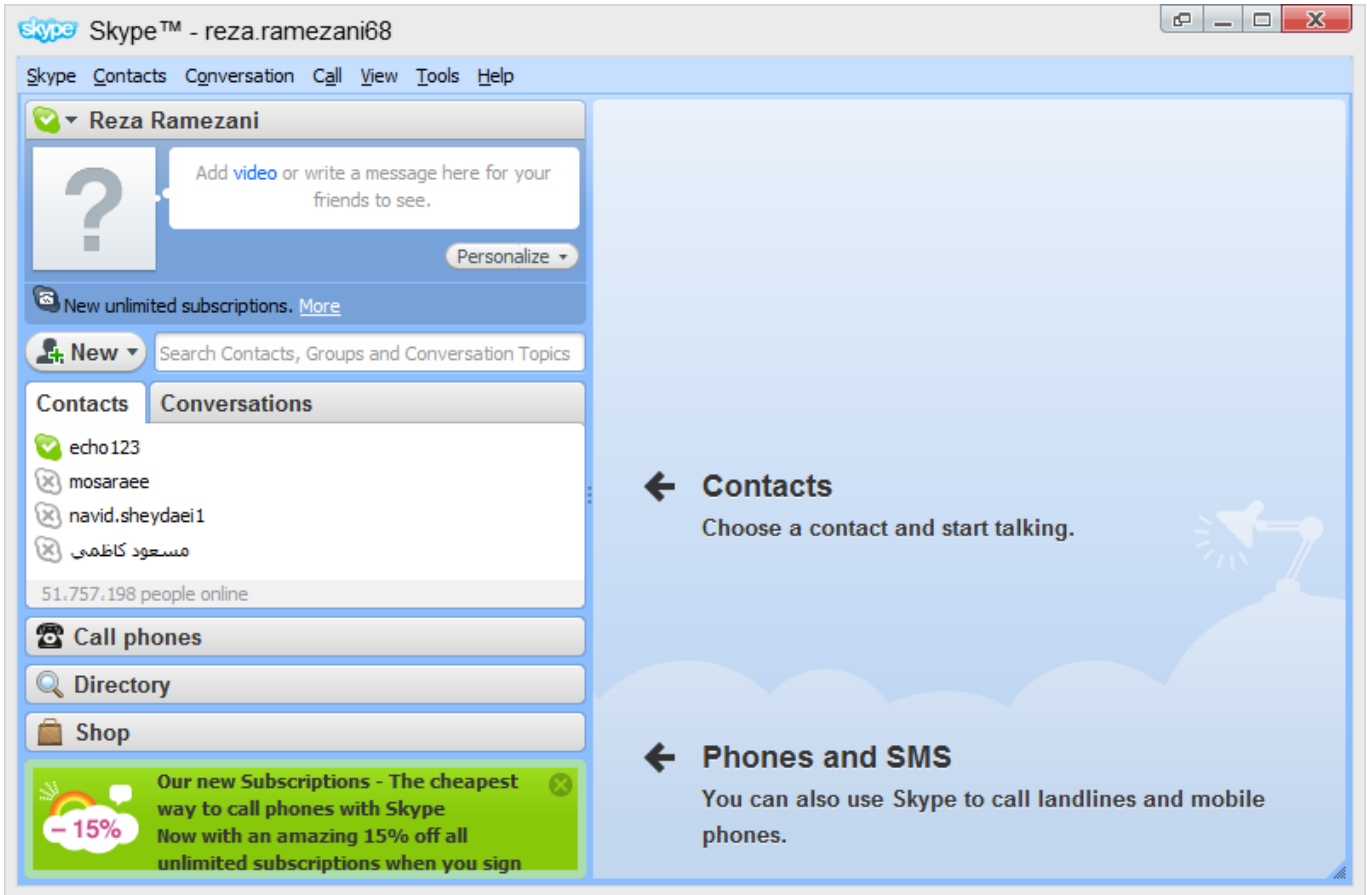


۲۰-۳-۳- اجرای نرم‌افزار

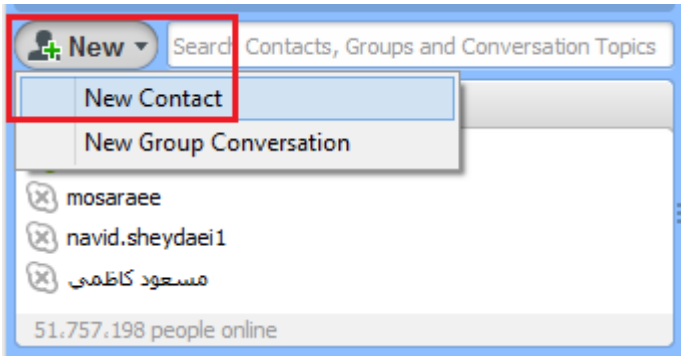
پس از ورود به نرم‌افزار برای اولین بار، صفحه خوش آمد گویی را می‌بینید که می‌توانید میکروفن و بلندگوهای خود را تست کنید. برای ورود به نرم‌افزار، روی قسمت Close this welcome screen … کلیک کنید.



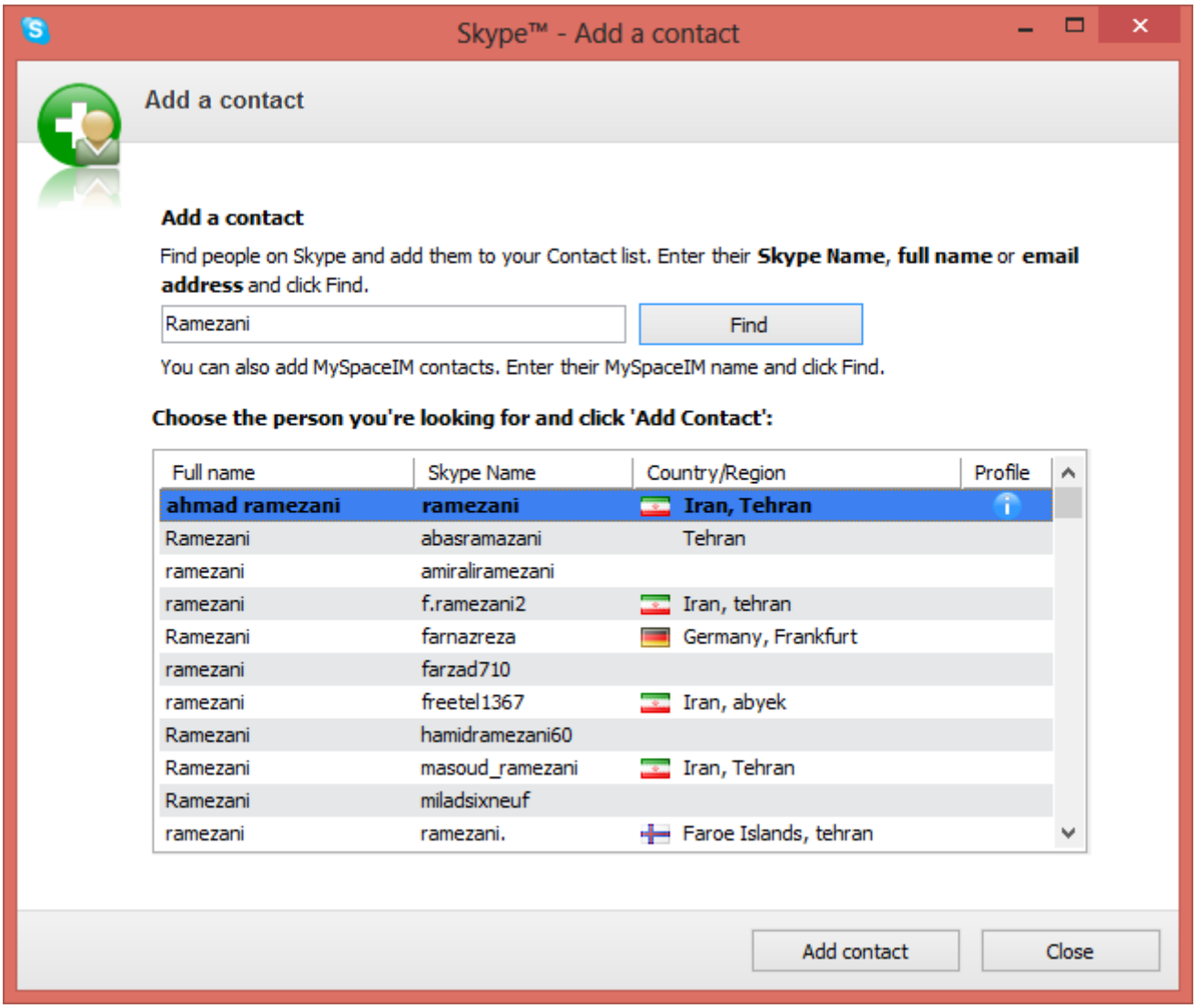
سپس صفحه اصلی نرم‌افزار باز می‌شود.



ابتدا بایستی مخاطبان جدید به لیست خود اضافه نمایید. برای این کار روی دکمه New Contact ← New کلیک کنید.



سپس در صفحه باز شده، نام، فامیل یا آدرس ایمیل مخاطب مورد نظر را وارد نمایید. در این مثال ما به دنبال Ramezani گشته‌ایم. سپس کاربر مورد نظر خود را انتخاب کرده و روی Add Contact کلیک کنید.

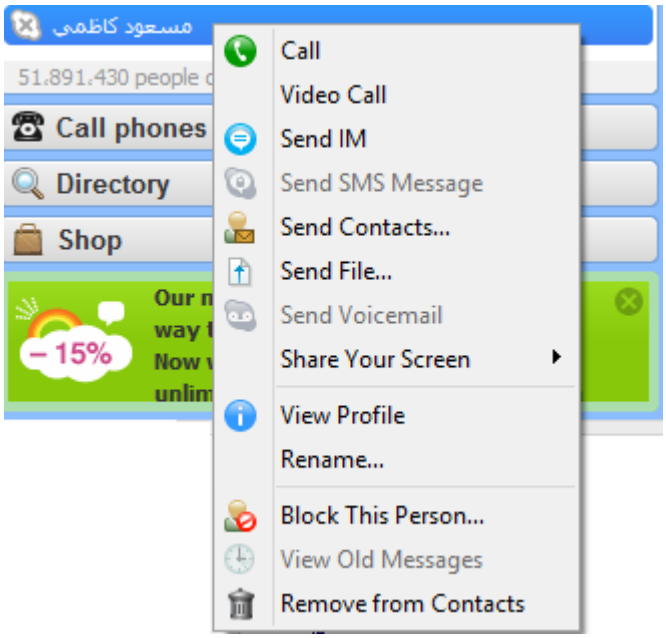


بعد از افزودن مخاطب مورد نظر می‌توانید به انجام مکالمه صوتی یا تصویری با آن‌ها بپردازید. البته مخاطب مورد نظر نیز باید Online باشد. بدین منظور روی نام مخاطب راست کلیک کرده و گزینه Call یا Video Call را انتخاب کنید.

نکته ۱: برخی از سرویس‌های Skype، پولی است.

نکته ۲: گزینه‌های دیگری که روی مخاطب می‌توان انجام داد، از روی شکل پیداست.

نکته ۳: مخاطب echo 123، مربوط به خود Skype و برای تست سیستم می‌باشد.



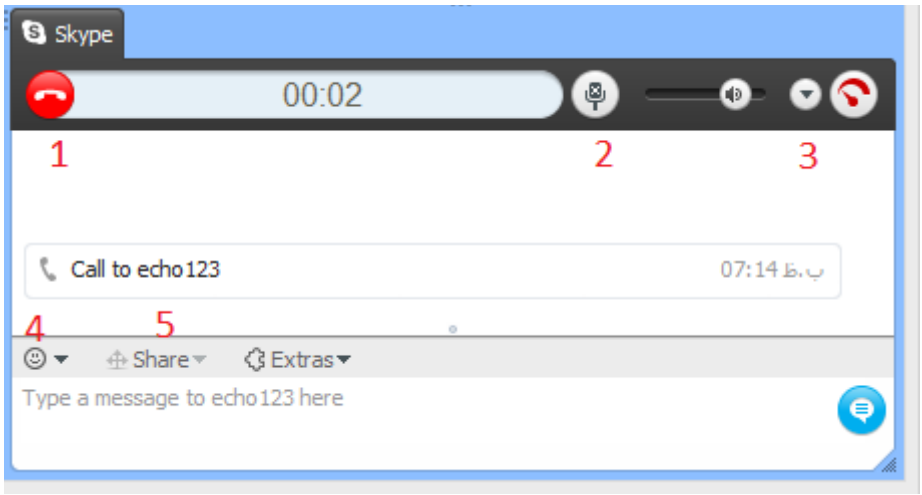
مطابق شکل بالا دو گزینه سبز رنگ، زیر توضیحات اکانت فرد مورد نظر قرار دارد. اگر سیستم شما مجهز به دوربین است و می‌خواهید تصویرتان را هم بفرستید روی گزینه **Video Call** و در غیر این صورت روی **Call** کلیک کنید.

فرد مورد نظر اگر آنلاین باشد، صفحه‌ای مانند زیر برایش باز می‌شود که در صورت تمایل می‌تواند به آن پاسخ بدهد.

گزینه اول از سمت چپ ارتباط صوتی ست. گزینه وسط ارتباط صوتی و تصویری ست و گزینه آخر قطع تماس است.



اکنون می‌خواهیم وارد جزئیات شده و بقیه امکانات این نرم‌افزار را معرفی کنیم.



هنگام مکالمه صفحه‌ای مانند شکل بالا خواهید داشت.

گزینه ۱: با کلیک کردن روی این قسمت به مکالمه خاتمه می‌دهید.

گزینه ۲: موقع صحبت کردن با دوستتان ممکن است بخواهید یک حرف در گوشی به کسی که کنارتان است بزنید! در این مواقع با دست جلوی دهنی تلفن رو میگیریم. با فعال کردن این گزینه میکروفن قطع می‌شود و صدای شما به آن طرف خط نمی‌رسد. پس با خیال راحت حرف در گوشی تان را بزنید!

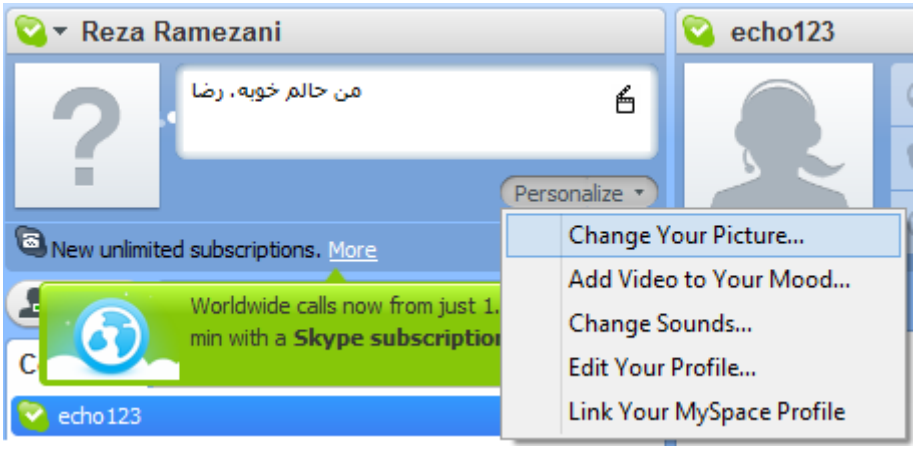
گزینه ۳: شما یک مکالمه صوتی را شروع کرده اید ولی وسط صحبت کردن نظرتان عوض می‌شود و می‌خواهید مکالمه ویدئویی هم داشته باشید. با فعال کردن این گزینه تصویرتان را برای دوستتان ارسال کنید.

گزینه ۴: شکلک‌های مختلف مناسب با حالت‌های مختلف را می‌توانید از اینجا انتخاب کنید.

گزینه ۵: از این قسمت می‌توانید اطلاعات مورد نظرتان را ذخیره و به صورت فایل برای دوستتان بفرستید.

شخصی سازی

مرحله بعدی تنظیم کردن پروفایل و شخصی سازی اکانت است. مطابق تصویر زیر در باکس مشخص شده می‌توانید وضعیت‌تان (همان Status) را بنویسید و از گزینه **Personalize** مواردی که دوست دارید را اضافه کنید.



۲۰-۴- نرم‌افزار oovoo

به علت گرانی تماس‌های تلفنی و سرعت پایین این ارتباطات در مقیاس بین المللی، تلفن‌های اینترنتی رواج بسیاری پیدا کرده‌اند. این ابزارها که اغلب به صورت رایگان ارائه می‌شوند تحولی در سیستم‌های ارتباطی به وجود آورده‌اند.

ابزار دیگری که این روزها خیلی باب شده و ابزار قدرتمندی‌ست نرم‌افزار oovoo است. oovoo با داشتن محیط راحت برای کاربر و امکانات بسیار می‌تواند مورد استفاده اکثر کاربران قرار بگیرد. عملکرد oovoo بسیار شبیه نرم‌افزار Skype است.

مبنای اصلی این نرم‌افزار ویدیو چت و کنفرانس‌های تصویری است، ولی در کنار آن می‌توان مانند یاهو مسنجر به چت معمولی پرداخت و یا فایل رد و بدل کرد. این نرم‌افزار کاملا رایگان نیست و برای استفاده از همه امکانات آن باید مبلغی بپردازید. البته اکثر امکاناتی که نیاز به پرداخت پول دارند در ایرن غیر فعال است.

با این ابزار می‌توانید از طریق اینترنت تلفن بزنید (شماره گیری برای ایران غیر فعال است) و نگران هزینه‌های سرسام آور تلفن‌های بین المللی نباشید. با این نرم‌افزار حداکثر می‌توانید ویدیو کنفرانسی با ۶ نفر برگزار کنید و مهم نیست هر کدام از افراد از چه ابزاری استفاده می‌کنند .هر کسی می‌تواند با موبایل، لپ تاپ و یا کامپیوتر خانگی به اینترنت وصل شود.

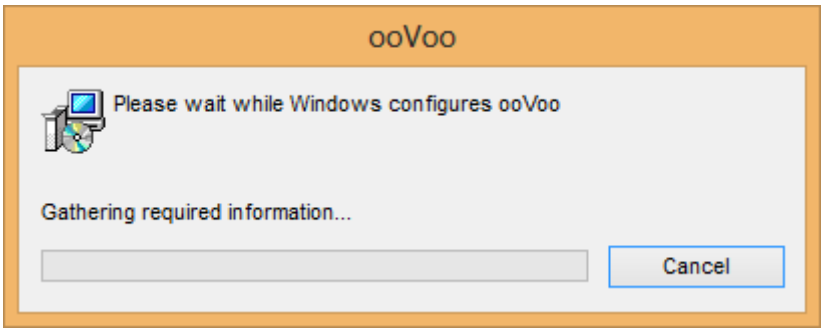
oovoo نسخه مخصوص موبایل خود را نیز ارائه کرده و اکثر گوشی‌های هوشمند مانند Samsung Epic، Apple iPhone 4 Motorola Droid X و HTC از آن پشتیبانی می‌کنند.

مشخصات اصلی به طور خلاصه:

- ✓ قابلیت چت نوشتاری
- ✓ قابلیت ارسال فایل
- ✓ امکان کنفرانس با حداکثر ۶ نفر
- ✓ امکان ضبط مکالمات هم به صورت صوتی و هم به صورت تصویری
- ✓ سازگار با سیستم عامل‌های Android و iPhone و Windows و Mac OS

۲۰-۴-۱- نصب نرم‌افزار

نصب این نرم‌افزار، بسیار راحت است. بعد از دانلود نرم‌افزار و اجرای فایل Setup، صبر کنید تا نرم‌افزار به صورت خودکار نصب شود. هنگام نصب هیچگونه اطلاعاتی مانند مسیر نصب و... از شما دریافت نمی‌گردد.

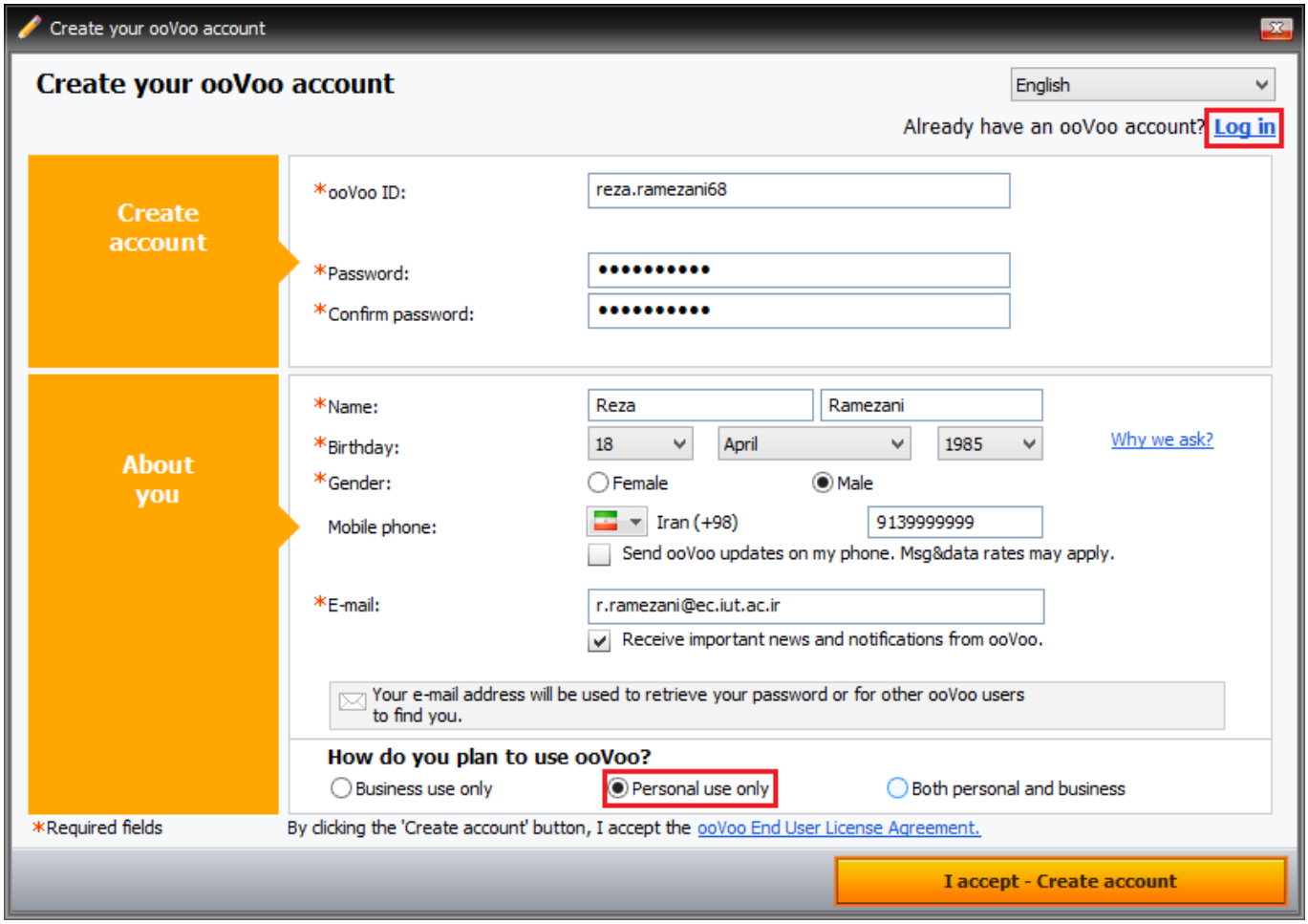


بعد از نصب نرم‌افزار، جهت اجرای آن، از مسیر C:\Program Files\ooVoo فایل ooVoo.exe را اجرا نمایید.

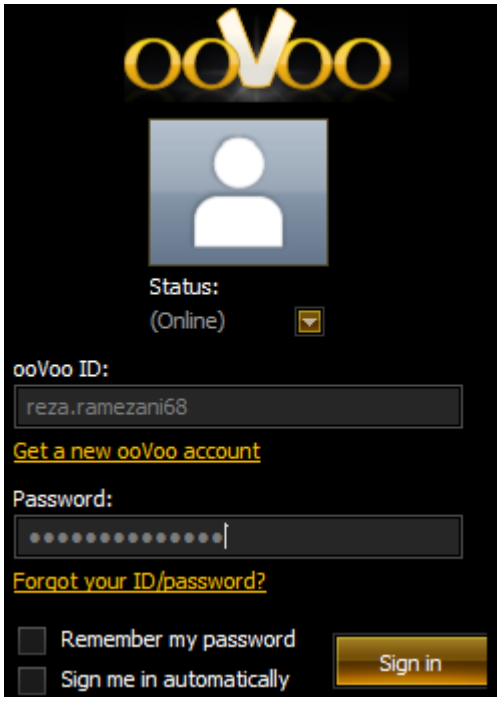


۲۰-۴-۲- ایجاد حساب کاربری

جهت استفاده از این نرم‌افزار، باید یک حساب کاربری داشته باشید. بدین منظور بعد از بازکردن نرم‌افزار برای اولین بار، مطابق شکل زیر، اطلاعات کاربری خود، شامل نام کاربری، رمز عبور و... را وارد نموده و سپس روی دکمه I accept – create an account کلیک کنید. اگر هم از قبل حساب کاربری دارید، روی Sign in کلیک کنید.



سپس جهت ورود به نرم‌افزار، نام کاربری و رمز عبور فراهم شده را وارد نمایید. از طریق قسمت Status نیز می‌توان تعیین نمود که بعد از ورود، وضعیت کاربری به صورت Online، Busy، Away یا Invisible باشد.



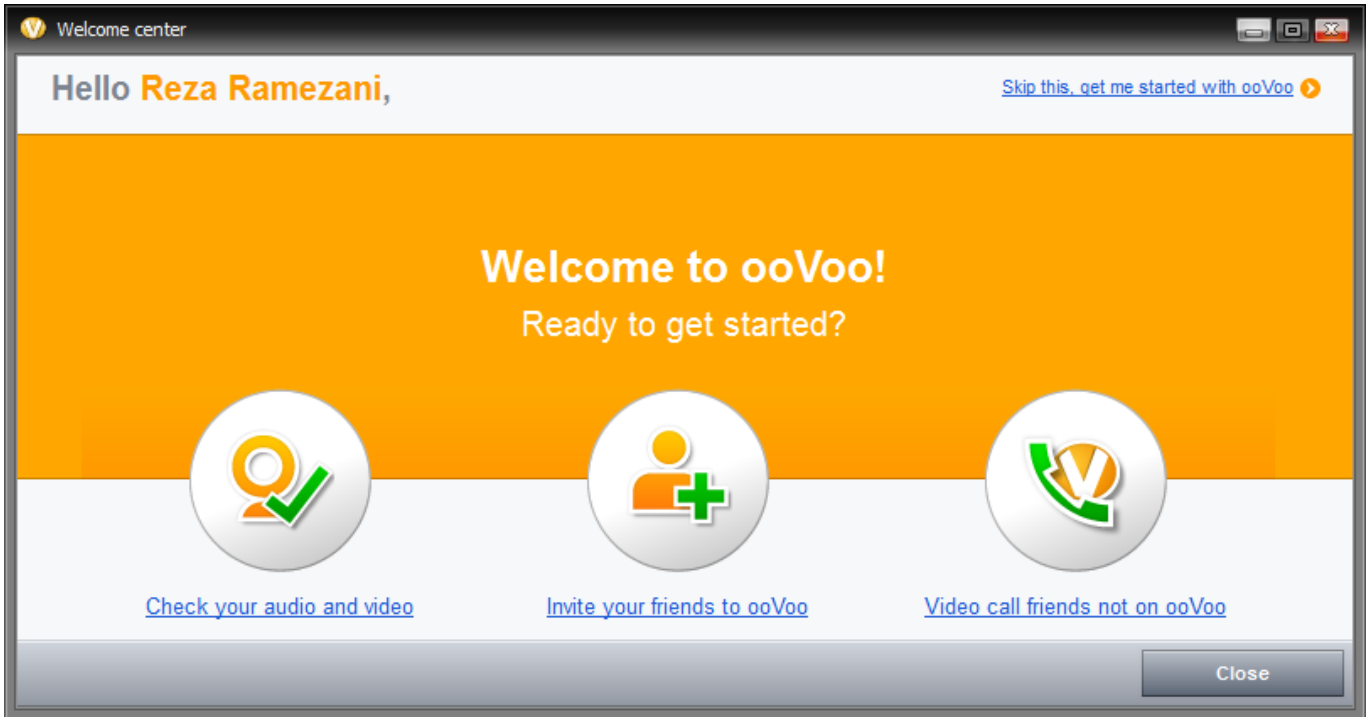
۲۰-۴-۳- اجرای نرم‌افزار

نحوه کار کردن با این نرم‌افزار مانند همه نرم‌افزارهای مبتنی بر وب بسیار آسان است. تمام این نرم‌افزارها User Friendly هستند و طوری طراحی شده‌اند که عموم کاربران بتوانند با آن کار کنند. اگر شما جزو کسانی هستید که هنوز نحوه کار کردن با اینگونه نرم‌افزارها را یاد نگرفته‌اید و هنگام مواجه با محیط نرم‌افزارهای جدید مضطرب می‌شوید، نگران نباشید. با خواندن این آموزش تصویری به راحتی یاد خواهید گرفت با دوستان خود در هر کجای دنیا ویدیو چت داشته باشید.

برای ورود به نرم‌افزار، نام کاربری و رمز عبور را وارد نموده و منتظر بمانید تا عمل اتصال انجام شود.



پس از ورود به نرم‌افزار، اگر برای اولین بار است که از نرم‌افزار استفاده می‌کنید، صفحه خوش آمد گویی و تست میکروفون و بلندگو و دعوت دیگر دوستان به oovoo ظاهر می‌شود.

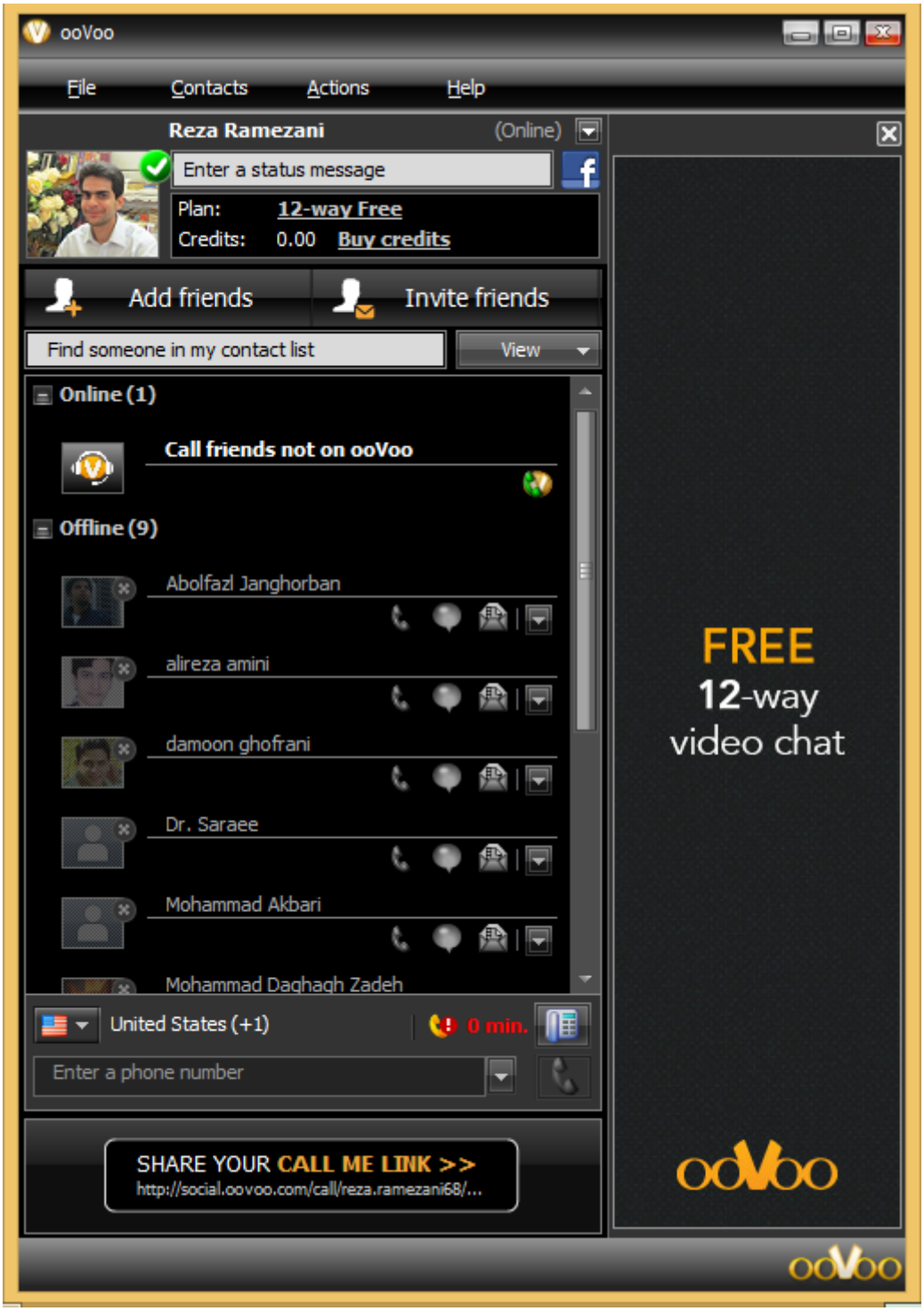


با کلیک روی دکمه Close، صفحه اصلی نرم‌افزار در مقابل شما نمایان می‌شود.

تمامی کارهای قابل انجام شامل

- ✓ افزودن مخاطب
- ✓ دعوت دیگر دوستان
- ✓ انجام مکالمه صوتی و تصویری
- ✓ انجام چت
- ✓ و...

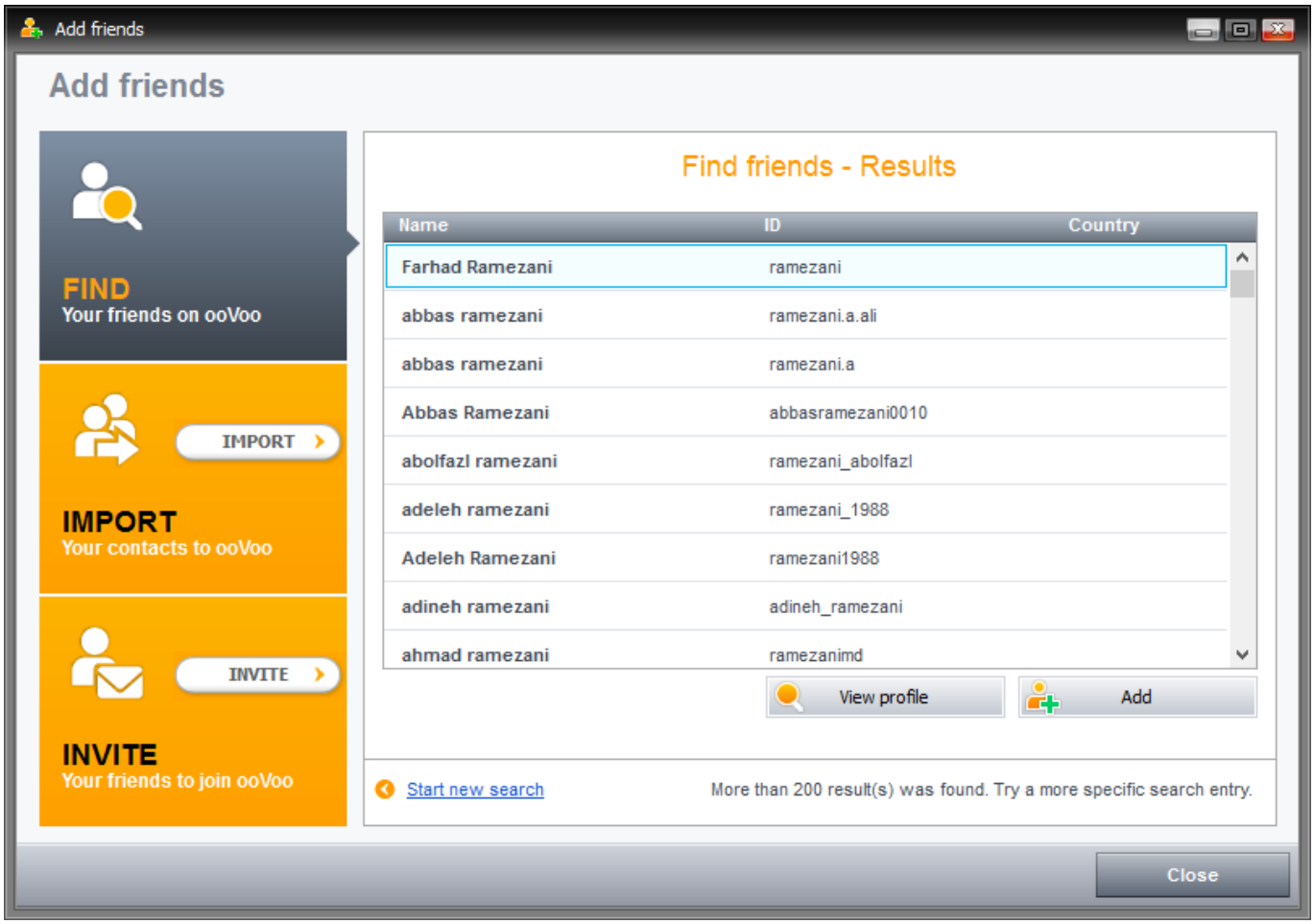
را از طریق همین صفحه، می‌توانید انجام دهید.



جهت افزودن مخاطب جدید، روی دکمه Add friends کلیک کنید.



سپس در صفحه باز شده، نام یا ایمیل فرد مورد نظر را وارد نموده و روی Search کلیک کنید. در نهایت روی فرد مورد نظر کلیک کرده و روی دکمه Add کلیک کنید. در شکل زیر، ما عبارت Ramezani را مورد جستجو قرار داده‌ایم. بعد از تایید فرد انتخاب شده، وی به لیست مخاطبان شما اضافه خواهد شد.



برای دعوت دوستان خود به استفاده از oovoo، روی دکمه Invite friends کلیک کنید.



در صفحه باز شده، می‌توانید با کمک حساب کاربری خود در سایت‌های اجتماعی، Skype، IM یا با کمک ایمیل، دوستان خود را دعوت به استفاده از oovoo نمایید.



مثلا می‌توانید با نام کاربری و رمز عبور Skype، وارد شده و دوستان خود در Skype را به oovoo دعوت کنید.

حال نوبت به برقراری ارتباط با مخاطبان می‌شود. برای داشتن ارتباط زنده، مخاطب مورد نظر باید Online باشد. برای شروع ویدیو چت روی اولین گزینه کنار ID دوستتان با نام Start oovoo Video Call کلیک کنید. با کلیک کردن روی این گزینه تماس آغاز می‌شود. این کار بار راست کلیک روی مخاطب مورد نظر نیز امکان پذیر است.

در پایین صفحه‌ی جدید سه گزینه داریم مطابق شکل:

- با کلیک کردن روی مربع قرمز تماس پایین میابد.
- با کلیک کردن روی مربع زرد می‌توانید چت متنی را آغاز کنید.
- با کلیک کردن روی مربع سبز می‌توانید برای طرف مقابل فایل ارسال کنید.



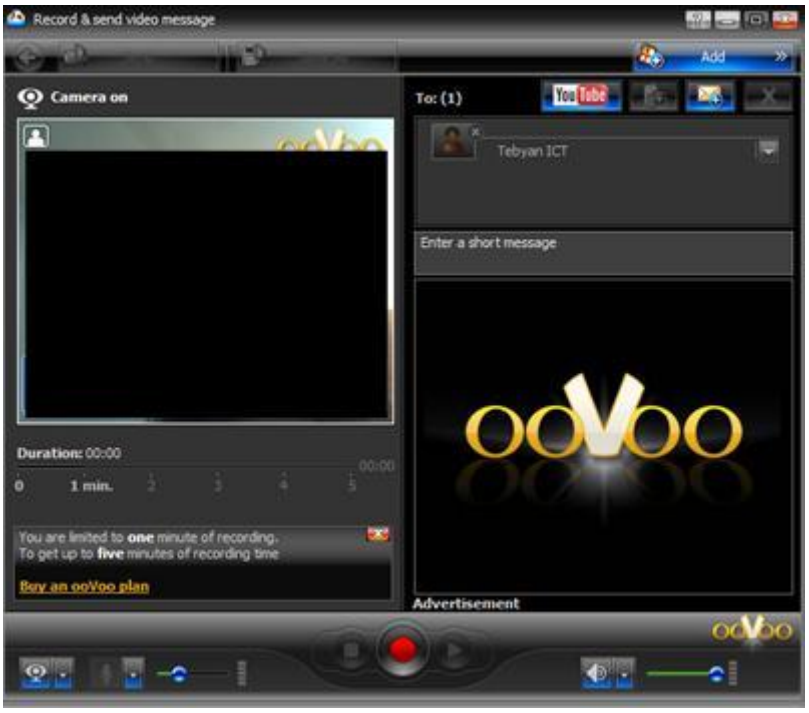
گزینه کنار Start oovoo video call را با نام Start text chat انتخاب کنید. با زدن این گزینه صفحه‌ای مطابق تصویر زیر خواهید داشت. همان طور که می‌بینید محیط برنامه بسیار ساده و مانند یاهو مسنجر است. در این صفحه نیز سه گزینه پایین کادر دارید:

- با کلیک کردن روی گزینه وسط ویدیو چت آغاز می‌شود.
- با کلیک کردن روی گزینه راست می‌توانید پیغام صوتی و تصویری را ضبط کنید و برای دوستتان بفرستید. (Record and send video message)
- با کلیک کردن روی گزینه چپ نیز می‌توانید فایل ارسال کنید.



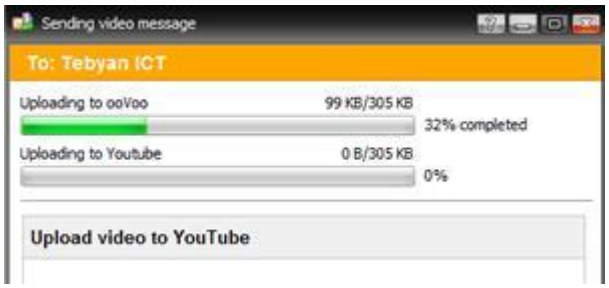
روی گزینه Record and send video message کلیک کنید. صفحه‌ای مطابق شکل زیر خواهید داشت. در محیط oovoo قادرید تا ۵ دقیقه فایل ویدیو ضبط کنید و به صورت آنلاین برای دیگران ارسال کنید.

با زدن کلید قرمز ضبط آغاز می‌شود. می‌توانید تنظیمات مربوط به کیفیت میکروفن و دوربین را تغییر دهید. روی شکل دوربین که در گوشه پایین چپ قرار دارد کلیک کنید و مطابق با سیستم و نوع دوربین تنظیمات را انجام دهید.

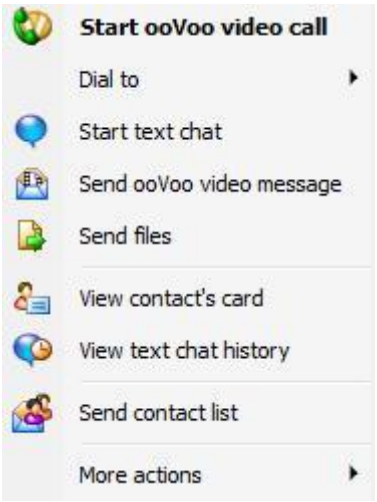


گزینه کناری نوع میکروفن رو مشخص می‌کند. اگر از میکروفن خارجی، هدست و... استفاده می‌کنید، می‌توانید اینجا انتخاب کنید. ولی بهتر است این گزینه‌ها را در حالت windows default device قرار دهید.

بعد از ضبط ویدیو، روی گزینه Send که در گوشه بالای چپ قرار دارد کلیک کنید. بعد از کلیک صفحهای مطابق زیر مشاهده می‌کنید، تا وقتی عملیات آپلود فایل ویدیو تمام نشده این صفحه را نبندید.



کنار اسم هر کدام از افراد درون لیست یک فلش وجود دارد. روی آن کلیک کنید تا منو آن باز شود. پنج گزینه اول را در بالا توضیح داده‌ایم.



بقیه گزینه‌ها عبارتند از:

- View Contact's Card پروفایل ID مورد نظر را باز می‌کند.
- View Text Chat History نوشته‌های پیشین شما را با فرد مورد نظر مشخص می‌کند.
- Send Contact List صفحه‌ای را باز می‌کند که در آن می‌توانید سایر دوستانتان را انتخاب کنید و مشخصات آن‌ها را برای فرد مورد نظر بفرستید.
- با کلیک روی گزینه More Actions قادر خواهید بود فرد مورد نظر را بلاک، حذف و یا تغییر نام دهید.

۲۰-۵- نرم‌افزار Net Support School



۲۰-۵-۱- معرفی نرم‌افزار

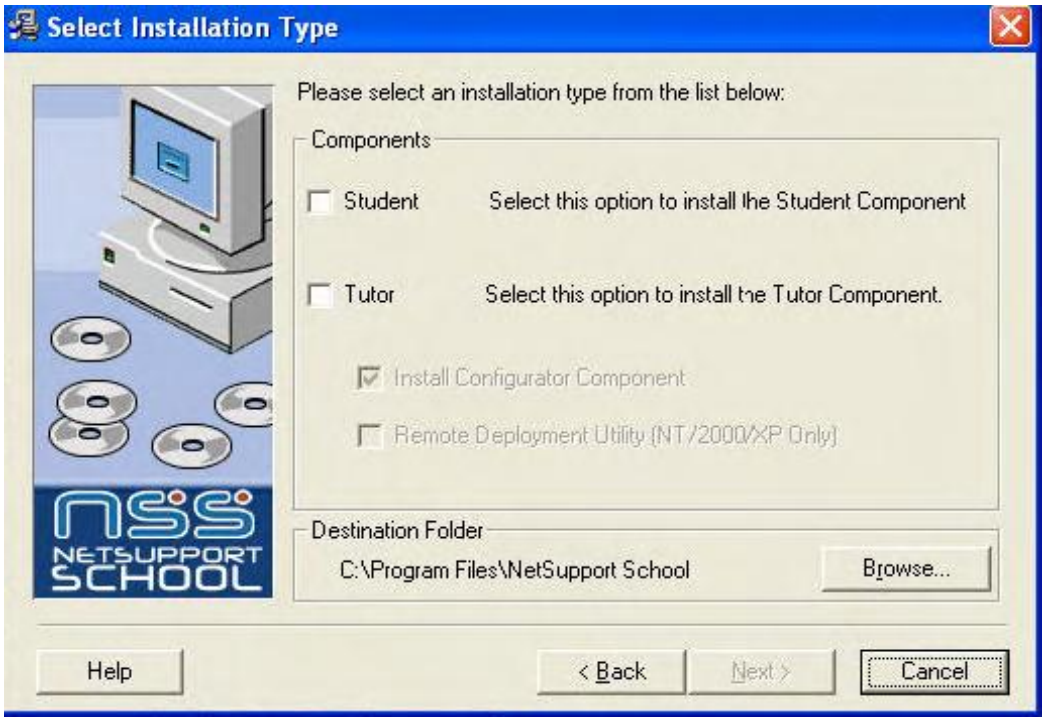
نرم‌افزار Net Support School یکی از قدرتمند ترین نرم‌افزار های مدیریتی در محیط شبکه در زمان تدریس می باشد. توسط این نرم‌افزار می توان کلیه دانش‌آموزان را در یک لحظه زیر نظر داشت. مهمترین کار این برنامه کمک به دبیر در حین تدریس در کلاس های عملی می باشد. دبیر توسط این برنامه در زمان تدریس می تواند کنترل کلیه سیستم های دانش‌آموزان را در اختیار بگیرد و صفحه جاری سیستم خود را بر روی صفحه دانش‌آموزان قرار داده و از این طریق تدریس بسیار آسان می شود. حتی توسط این نرم‌افزار دبیر قادر خواهد بود سیستم دانش‌آموزان را خاموش ویا روشن نماید.حتی به دبیر این قدرت را می دهد که در زمان ورود به اینترنت دانش‌آموزان را محدود کند وفقط بتوانند از سایتهای مجاز استفاده نمایند. در زمان تدریس دروس تئوری نیز احتیاجی به خاموش کردن مانیتورتوسط دانش‌آموزان وجود ندارد ودبیر می تواند از صفحه کنترلی خود مانیتور دانش‌آموزان را بطور موقت خاموش نماید. علاوه بر موارد اشاره شده در این فصل، این برنامه قادر به برگزاری آزمونهای الکترونیکی نیز می باشد به عبارت بهتر به همراه این برنامه برنامه دیگری به نام Net Support School Test Designer نصب می شود که معلم می تواند به کمک آن سوال های خود را طرح نموده و سپس دانش‌آموزان از طریق کامپیوتر خود به این سوال‌ها جواب دهند. در آخر زمان امتحان نیز نمرات کلیه دانش‌آموزان توسط سیستم اعلام می شود. توسط این برنامه می توان ۸ نوع سوال مختلف از جمله سوال چهار گزینه ای، صحیح و غلط، جای خالی، نامگذاری تصویر و غیره را مطرح نمود. یعنی آزمون های این برنامه می تواند از هر نوع آزمو ن کتبی کامل‌تر و جامع‌تر باشد.

۲۰-۵-۲- نصب نرم‌افزار

۱- فایل Setup برنامه را اجرا می کنیم.

۲- مراحل نصب را یکی یکی طی می کنیم سپس با شرایط تعیین شده موافقت می کنیم ودر مرحله بعد ی نصب از ما Username و Serial Number را می پرسد که آنرا نیز وارد می کنیم

۳- در مرحله آخر نصب برنامه برای سیستم دانش‌آموزان نسخه Student وبرای سیستم دبیر نسخه Tutor ، را انتخاب می کنیم.



توجه:

اگر شما بخواهید سیستم عامل کامپیوتر خود را Upgrade نمایید، ابتدا نرم‌افزار Net Support را از حالت نصب خارج کنید و پس از Upgrade کردن سیستم عامل خود آنرا مجددا نصب نمایید. برای نصب این نرم‌افزار سیستم کامپیوتر شما باید Administrator باشد وگرنه اجازه نصب به شما داده نخواهد شد.

۲۰-۵-۳- اجرای نرم‌افزار

برای اجرای نرم‌افزار Net Support دو روش وجود دارد اول اینکه از روی Desktop میانبرمربوط به این نرم‌افزار را اجرا کنیم. راه دیگر این است که از گزینه Start➔Allprograms➔Net Support School➔Net Support School Tutor استفاده نماییم.



وقتی که برای اولین بار این برنامه بر روی سیستم دبیر اجرا می شود پنجره خوش آمد گویی ظاهر می شود. وبرای مراحل بعدی دیگر این پنجره نمایش داده نمی شود. بعد از نصب برنامه Net Support بر روی سیستم دانش‌آموزان اگر دبیر برنامه Net Support نسخه مخصوص دبیر را اجرا کند، بطور اتوماتیک کلیه صفحات کاری دانش‌آموزان بر روی سیستم دبیر ظاهر خواهد شد. در این پنجره دکمه Start را انتخاب می کنیم تا وارد پنجره Class Wizard شویم.





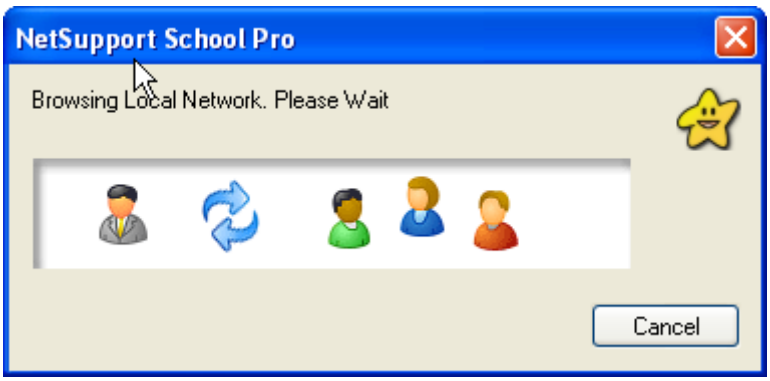
در پنجره Class Wizard شما قادر به تنظیمات اصلی محیط تدریس خواهید بود.

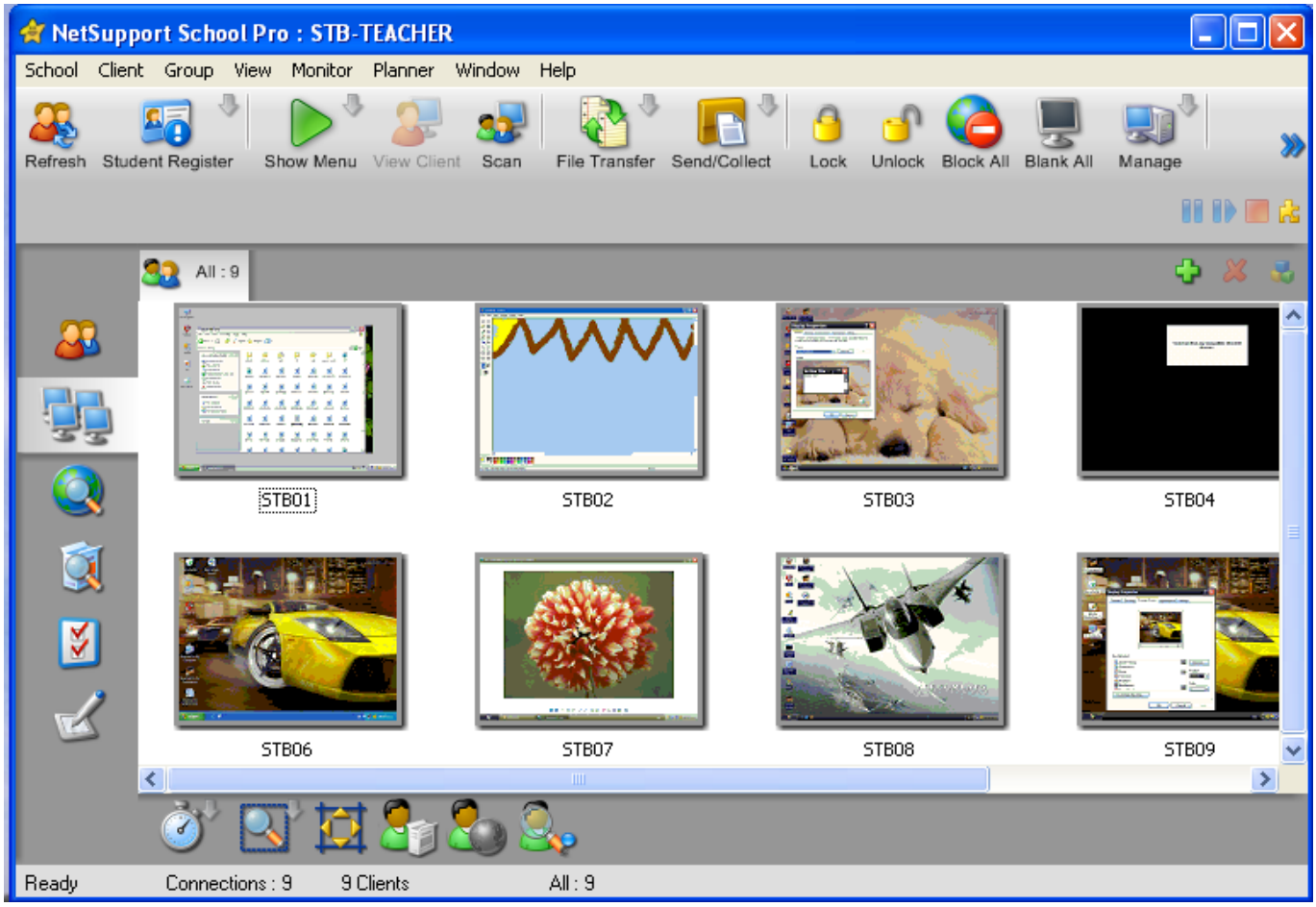
جزئیات این پنجره

- شما می توانید در بخش Teacher Name نام دبیر را وارد کنید
- در قسمت Lesson Title عنوان درسی راکه قرار است داده شود نوشت.
- در جلوی گزینه Room شماره کلاسی که درس برای آن کلاس در نظر گرفته شده است.

- در بخش Load An Exiting Lesson Plan با کلیک بر روی دکمه Browse شما می توانید برنامه درسی را که از قبل آنرا ذخیره کرده اید بارگذاری نمایید و بطور متناوب شما می توانید یک طرح درس جدید را ایجاد کنید.
- با تنظیم گزینه What Time Does This Lesson Finish? زمانی راکه شما می‌خواهید کلاستان به پایان برسد وارد کنید. سپس یک زمان سنج در حین تدریس شما بر روی صفحه ظاهر می شود و اگر شما نمی خواهید که مدت زمان تدریس شما به زمان سنج وابسته باشد گزینه Open Lesson را انتخاب نمایید.
- با انتخاب گزینه Create A Student Register شما می توانید قبل از شروع درس با قرار دادن اسامی دانش‌آموزان بجای شماره سیستم کامپیوتر آن‌ها را بیشتر وادار به تلاش کنید. و بر روی صفحه کنترلی دبیر نیز نام دانش‌آموزان بجای شماره آن‌ها نمایش داده می شود.
- اگر گزینه Automatically Reconnect انتخاب شده باشد، سیستم دانش‌آموزان به هر دلیلی Restart شود بطور اتوماتیک مجددا بر روی صفحه کنترل دبیر ظاهر می شوند. در غیر اینصورت پس از قطع ارتباط باید دبیر از گزینه Refresh استفاده کند.
- برای نمایش بهتر: اگر گزینه Optimize Show For Performance را انتخاب کنیم اطلاعات در موقع نمایش برروی صفحه دانش‌آموزان بهتر و واضح‌تر به نمایش در می آیند.
- واگر بخواهیم اطلاعات با قابلیت اعتماد بیشتر نمایش داده شوند گزینه Optimize Show For Reliability را انتخاب می کنیم.
- و در آخر اگر نیازی به تنظیم مجدد این پنجره ندارید میتوانید از پایین این پنجره گزینه Don’t Show This Dialog Again را انتخاب کنید تادر اجراهای بعدی این پنجره دیگر ظاهر نگردد.

اگر در پنجره Class Wizard بر روی دکمه Go کلیک کنیم برنامه Net Support بر روی شبکه به دنبال Client هایی می گردد که اولا به شبکه متصل باشند ثانیا بر روی آن‌ها برنامه Net Support نسخه مخصوص دانش‌آموزان نصب شده باشد.



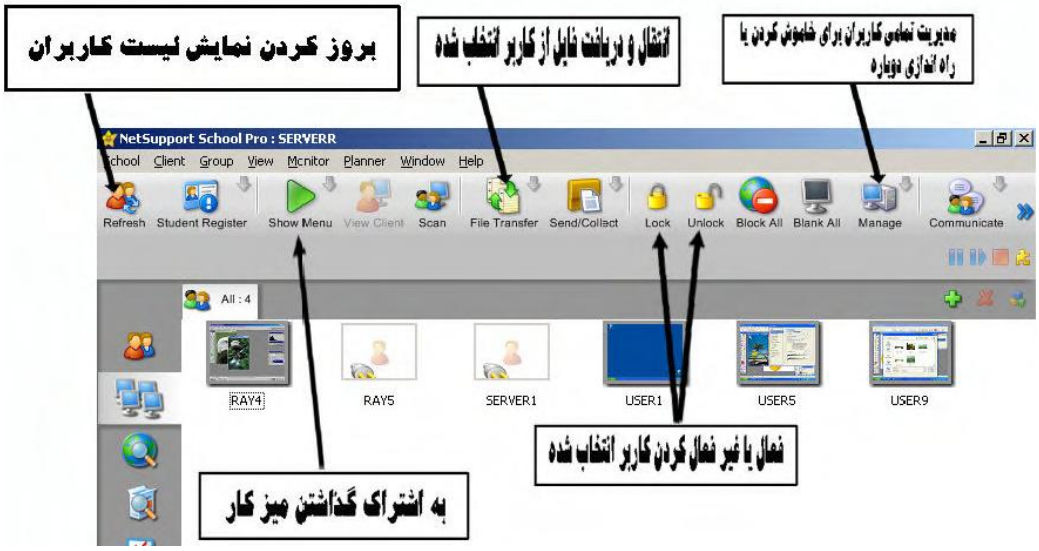


۲۰-۵-۴- معرفی محیط اصلی Net Support

همانطور که در شکل صفحه اصلی پنجره Net Support مشاهده می شود، در این پنجره پس از نوار عنوان پنجره نوار منو که شامل گزینه های School، Client، Group، View، Monitor، Planner، Window و Help می باشد.

پس از نوار منو نوار ابزار Standard قرار دارد که پر استفاده ترین دستورات بشکل ابزارهایی بر روی این نوار قرار داده شده‌اند.

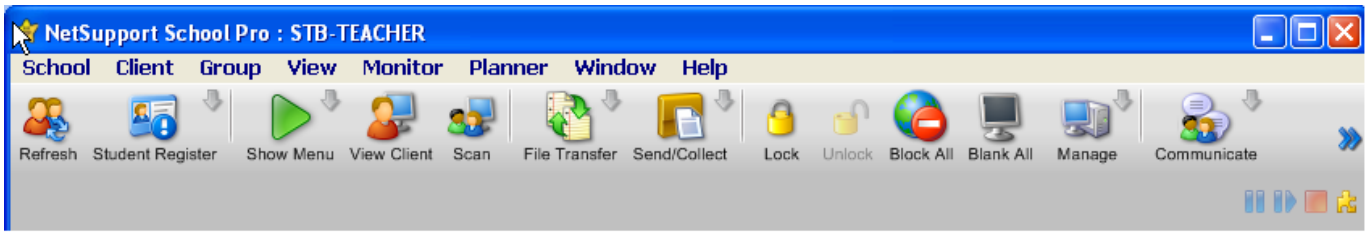
به طور کلی این نرم‌افزار دارای این قسمت‌ها است:





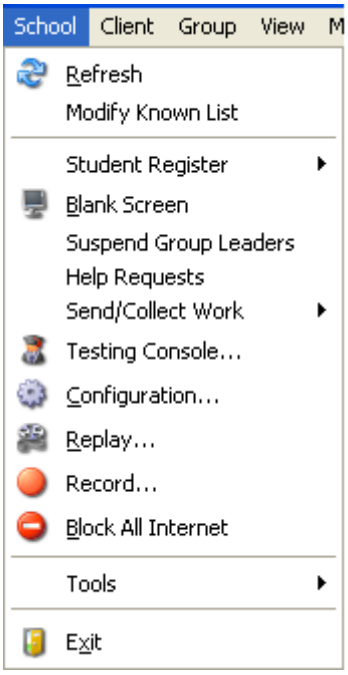
دو گروه ابزار نیز در اطراف صفحه کنترل قرار دارند که یک گروه آن به حالت عمودی ویک گروه به حالت افقی در زیر صفحه کنترل قرار دارند که به ترتیب همه گزینه‌ها در زیر توضیح داده شده است.

۱. نوار ابزار اصلی



در این نوار ابزار ابزارهایی برای جستجوی مجدد برای یافتن Client های جدید نمایش موضوع درسی، نمایش صفحه کاری دانش‌آموزان، دریافت وارسال اطلاعات به سیستم های دانش‌آموزان، فرستان نمونه سوال وجمع آوری آن، قفل کردن سیستم دانش‌آموزان به عنوان تنبیه (وجدانا قبلانا تو مکتب دانش‌آموزها تنبیه می‌شدند، دانش‌آموزهای امروزی هم تنبیه می‌شوند. بعد بگید چرا نمی‌رویم به جام جهانی؟!؟!)، قفل کردن شبکه Internet سیستم های دانش‌آموزان، خاموش کردن صفحه کاری دانش‌آموزان در حین درس تئوری، مدیریت سیستم دانش‌آموزان برای خاموش وروشن کردن سیستم های آنان و... وجود دارد که در صفحات بعدی بطور کامل توضیح داده می شود.

۲. منوی School



Refresh: از این گزینه برای جستجو در شبکه برای یافتن Client جدید استفاده می شود. اگر سیستم دانش آم وزی در اثر عوامل مختلف از قبیل نوسان برق یا Restart شدن ناگهانی سیستم کامپیوتر ویا به علت قطع شدن کابل شبکه از صفحه کنترل Net Support حذف شود برای شناسایی مجدد سیستم دانش‌آموز بجای خارج شدن از محیط Net Support از این گزینه استفاده می شود.

Modify Known List: توسط این گزینه می توان لیست اسامی دانش‌آموزانی را که در صفحه کنترل پنجره قابل مشاهده هستند را در فایل Client.Nns ذخیره کرد. این لیست این قابلیت را دارد که اگر تغییراتی بر روی لیست اسامی دانش‌آموزان وارد شد اطلاعات قبلی را برورز رسانی کند واطلاعات جدید را جایگزین اطلاعات قبلی نماید.

Student Register: بصورت پیش فرض برنامه Net Support اسامی کامپیوترها را در پنجره کنترل نمایش می دهد.اگر چه این امکان وجود دارد که بتوان بجای اسامی کامپیوترها از اسامی واقعی دانش‌آموزان برای نمایش در صفحه کنترل استفاده کرد.گزینه Student Register: این قابلیت را فراهم می کند که دبیر بتواند این تنظیم را انجام دهد واسامی واقعی دانش‌آموزان بجای نام کامپیوتر آن‌ها نمایش داده شود.

Blank Screen: این گزینه به دبیر این امکان را می دهد که بجای اینکه به دانش‌آموزان بگوید که در زمان درس تئوری مانیتور های خود را خاموش کنند می تواند از منوی School و با استفاده از گزینه Blanck Screen بطور موقت تمام صفحات مانیتورها را به حالت خاموش تبدیل کند ویا اگر دبیر بخواهد برروی سیستم دانش‌آموزی عملیاتی را انجام دهد که او متوجه نشود باز میتواند از این گزینه استفاده نمایید. برای غیر فعال کردن این گزینه مجدد بر روی آن کلیک میکنیم تا غیر فعال گردد وصفحات کاری دانش‌آموزان مجددا به حالت قبلی برگردد.

Suspend Group Leaders: در طول بررسی گروه های کاری که توسط این نرم‌افزار ایجاد شده‌اند دبیر ممکن است که سوالی را بخواهد از گروه خاصی بپرسد. ما میتوانیم توسط این گزینه به شکل محلی گر وهی را انتخاب کنیم وعملیات مربوط به آن گروه را رهبری کنیم.

Help Requests: با انتخاب این گزینه اگر دانش‌آموزی احتیاج به راهنمایی در مورد خاصی داشت این پنجره بر روی صفحه کاری دبیر ظاهر می شود وسوال مطرح شده نمایش داده می شود وتوسط آیکن Chat دبیر می تواند با دانش‌آموز ارتباط برقرار کرده و به سوال او پاسخ دهد.

Send/Collect Work: با انتخاب این گزینه درآینده شما قادر خواهید بود که یک یا تعدادی سند را به یک یا تعدادی از Client های موجود در شبکه بفرستید.با انتخاب این گزینه شما می توانید پاسخ سوال دانش‌آموزان را جمع آوری نمایید. یعنی فایل سوال را بفرستید و پس از مدت زمان معینی دوباره فایلها را جمع آوری کنید (با جواب)

Testing Console: توسط این گزینه شما می توانید برای دانش‌آموزان یک آزمون تستی را درست کنید و برای این آزمون تستی زمان پاسخ گویی را نیز تنظیم کنید.که دانش‌آموزان فقط در مدت زمانی که شما برای آن‌ها در نظر گرفته اید بتوانند به سوال‌ها پاسخ بدهند. در حقیقت این بخش آزمونهای طراحی شده بوسیله ی Net Support School Test Designer را اجرا می کند.

Configuration: توسط این گزینه می توان نحوه اتصا ل به سیستم های دانش‌آمو زان را درزمان مشاهده آنان تنظیم کرد که کنترل دردست دبیر باشد یا اینکه درحالت اشتراکی هردو بتوانند کار کنند.

Replay: توسط فرمان Replay ما می توانیم فایلی را ایجادکنیم که توسط آن فایل پاسخ سوال های دانش‌آموزان را مشاهده کنیم.

Record: بعد از انتخاب این گزینه این امکان به دبیر داده می شود که گزینه های Include Audio و Record Physical Font را انتخاب کند که کدام موضوع را برای ضبط شدن در مسیری که در کادر In Directory وارد می‌کند را انتخاب نماید.

Block All Internet: توسط این گزینه می توان نحوه اتصال سیستم دانش‌آموزان به اینترنت را کنترل کرد. اگر این گزینه را انتخاب کنیم دیگر دانش‌آموزان مجاز به استفاده از اینترنت نیستند.

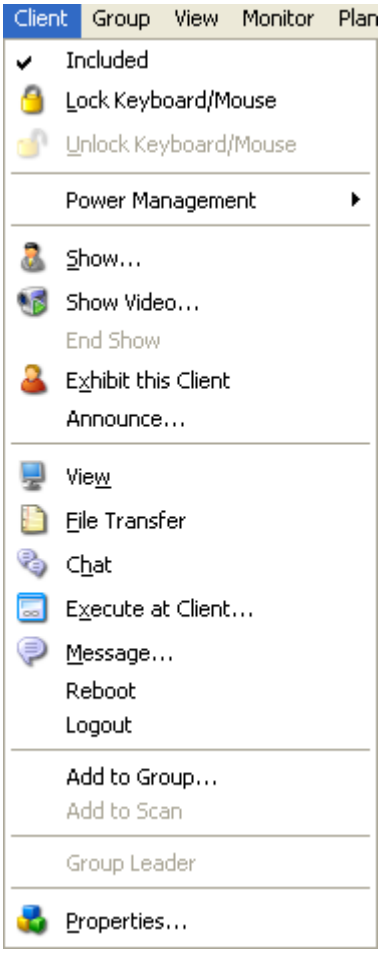
Tools: توسط این گزینه می توانیم با دکمه Add که برروی پنجره این دستور قرار داده شده است می توانیم مسیر اجرای یک برنامه را دراین پنجره با نام دلخواه ذخیره کنیم وهر بارکه به این برنامه نیاز داشتیم به سراغ گزینه Tools رفته ونامی را که برای اجرای برنامه در نظر گرفته بودیم انتخاب کنیم.

Exit: آخرین دستور در منوی School گزینه Exit است که از این گزینه برای خروج از برنامه Net Support می توان استفاده کرد.

۳. منوی Client

Included: اگر Client خاصی انتخاب شده باشد در کنار گزینه Included یک علامت تیک قرار داده می شود وگزینه های منوی Client فعال می شوند.

Lock Keyboard/Mouse: با انتخاب این گزینه صفحه کلید و ماوس دانش‌آموزیا دانش‌آموزانی که انتخاب شده‌اند قفل می شود ودیگر قادر به انجام عملی نیستند.



Unlock Keyboard/Mouse: با انتخاب گزینه Lock Keyboard/Mouse گزینه Unlock Keyboard/Mouse فعال شده ومیتوان سیستم را که ماوس وصفحه کلید آن قفل شده است از این حالت خارج ساخت.

Power Management: با انتخاب این گزینه زیر منوی آن شامل دو گزینه Power On و Power Off نمایش داده می شود اگر Client ی را که درحالت انتخاب است روشن باشد گزینه Power Off آن فعال است که توسط این گزینه می توان آن سیستم را خاموش کردو اگر سیستمی خاموش باشد گزینه On Power آن سیستم فعال است که توسط این گزینه می توان آن سیستم را روشن نمود.

Show: با انتخاب این گزینه می توان صفحه نمایش دبیر را بر روی سیستم یا سیستم هایی که انتخاب شده باشند به نمایش درآورد.

Show Video: توسط این گزینه می توان یک فایل ویدیویی را از مسیری که می توان مشخص کرد برای دانش‌آموزان به نمایش درآورد.

End Show: اگر فیلمی توسط گزینه Show Video در حال نمایش باشد می توان آنرا با گزینه End Show متوقف کرد.

Exhibit This Client: با این گزینه سیستم دانش‌آموزی را که در حالت انتخاب است بر روی صفحه مانیتور دیگر دانش‌آموزان قرار می دهد تا آن‌ها بتوانند صفحه نمایش او را مشاهده کنند.

View: با انتخاب این گزینه صفحه کاری دانش‌آموز بصورت تمام صفحه بر روی صفحه کنترل ظاهر می شود.

File Transfer: با این گزینه می توان فایل یا فایل هایی را برای دانش‌آموزان ارسال کرد یا فایل یا فایل هایی را از سیستم دانش‌آموزان گرفت. این گزینه برای نقل و انتقال فایل بین سیستمها به کار می رود.

Chat: توسط این دستور می توان یک ارتباط همزمان با دانش‌آموزان داشت.با انتخاب این گزینه یک پنجره گفتگو بر روی صفحه دانش‌آموز و دبیر ظاهر می شود که می توانند با یکدیگر بصورت نوشتاری در ارتباط مستقیم باشند.

Execute At Client: توسط این گزینه می توان بدون خارج شدن از برنامه Net Support و در زبانه Execute با انتخاب دکمه Add پس از باز شدن پنجره و انتخاب مسیر فایل اجرایی که مورد نظر است که بر رو ی سیستم دانش‌آموز به اجرا درآید آنگاه دکمه Execute را انتخاب می کنیم بلا فاصله برنامه مورد نظر بر روی سیستم دانش‌آموز اجرا می شود بدون اینکه آن دانش‌آموز برنامه مربوطه را داشته باشد.

Message: توسط این فرمان میتوان برای یک یا تعدادی Client که در حالت انتخاب باشند پیغامی را فرستاد.

Reboot: توسط این گزینه می توان سیستم دانش‌آموزی را مجددا راه اندازی کرد.

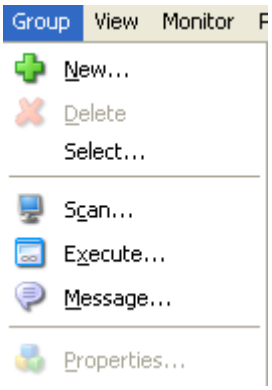
Logout: توسط این گزینه می توان برای تغییر حساب کاربری سیستم مورد نظر اقدام کرد ومحیط کاربری او را تغییر داد.

Add To Group: برای اضافه کردن یکی از Clientها به یک گروه از این دستور استفاده می شود.

Add To Scan: از این گزینه برای اضافه کردن یک سیستم برای چک کردن مشخصات آن استفاده می‌شود.

Properties: توسط این گزینه مشخصات مربوط به Client مورد نظر به نمایش گذاشته می شود مانند شماره IP وغیره...

۴. منوی Group



New: توسط این گزینه می توان گروه جدیدی را ایجاد نمود.پس از انتخاب این گزینه پنجره Add A Group باز می شود در داخل این پنجره دو کادر Name,Description وجود دارد که در کادر Name نام گروه مورد نظر را وارد می کنیم و در کادر Description توضیحاتی در باره این گروه داده می شود.پس از وارد کردن نام گروه مورد نظر دکمه Next را انتخاب می کنیم. در پنجره بعدی لیست اسامی Clientها به نمایش درمی آید. هر Client ی را که انتخاب کردیم توسط دکمه Add به لیست مورد نظر خود اضافه می کنیم ودر انتها دکمه Finish را انتخاب میکنیم وگروه مورد نظر ساخته می شود.

Delete: از این گزینه برای حذف یک گروه استفاد ه می شود. به این صورت که ابتدا باید گروه ایجاد شده برروی صفحه کنترل را انتخاب کرد وسپس از منوی Group گزینه Delete را انتخاب میکنیم آنگاه گروه انتخاب شده حذف می شود.

Select: با انتخاب این گزینه پنجره Net Support School Pro ظاهر می شود واسامی کلیه گروههای ایج اد شده را نمایش می دهد هر گروهی را که شما انتخاب کنید آن گروه به روی صفحه کنترل نمایش داده می شود. وبا استفاده از دکمه New می توانید گروه جدیدی را تشکیل بدهید.

Scan: با انتخاب این گزینه پنجره ای ظاهر می شود که داخل آن لیست اسامی Clientها به نمایش درآمده ا ست وبصورت پیش فرض همه آن‌ها در حالت انتخاب هستند. روی این پنجره گزینه Scan Interval قابل تنظیم است کار این گزینه تنظیم مدت زمان Refresh صفحه نمایش دانش‌آموزان است که این زمان بر حسب ثانیه تنظیم می شود. دو گزینه دیگرنیز برای انتخاب وجود دارند اگر گزینه Display One Client At A Time را انتخاب کنید در هر لحظه فقط سیستم یک دانش‌آموز که انتخاب شده است به نمایش در می آید واگر گزینه Display Multiple Client At A Time را انتخاب کنید این امکان به شما داده می شود که تعیین کنید که در هر لحظه چند سیستم را بتوانید با هم مشاهده کنید.

Execute: پس از انتخاب این گزینه از طریق دکمه Local Browse نام ومسیر فایل اجرایی را از روی سیستم دبیر پیدا کرده و با اضافه کردن آن با دکمه Add To List به لیست برنامه های اجرایی وبا انتخاب دکمه Execute برنامه مورد نظر بر روی سیستم یا سیستم های انتخاب شده اجرا می شود.

Message: با انتخاب این دکمه پنجرهای فعال می شود که می توان یکی از سه حالت زیر را برای یک یا چند Client ی که در یک گروه قرار دارند آن انتخاب کرد. با انتخاب گزینه All Available Client می توان پیغامی را برای تمامی Client های قابل دسترس فرستاد با انتخاب گزینه All Connected Clients می توان پیامی را برای تمامی سیستم های متصل به Net Support ارسال کرد و بالاخره با انتخاب گزینه Currency Selected Clients پیام مربوطه فقط به سیستمی که در حالت انتخاب است فرستاده می شود و در کادر مقابل گزینه Show This Meesage For ……(Sec) مدت زمان به نمایش در آمدن پیام مورد نظر را بر حسب مشخص می کنیم.

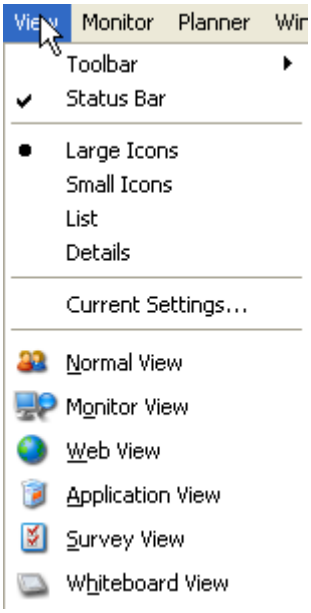
Properties: با انتخاب این گزینه پنجره ای با دو زبانه ظاهر می شود. در زبانه General این پنجره مشخصات مربوط به گروه که شامل عن اصر گروه وتوضیحات راجع به آن‌ها نمایش دا ده می شود. ودر زبانه Members لیست تمام Clientها نمایش داده می شود و با انتخاب دکمه Add میتوان عنصر جدیدی را به گروه اضافه کرد و با انتخاب دکمه Remove عضو مورد نظری را می توان از گروه حذف کرد.

۵. منوی View

Toolbar: توسط این گزینه می توان نوار ابزار هایی را که داریم بر روی پنجره مربوطه حذف و یا نصب کرد

Status Bar:توسط این گزینه نوار ابزار وضعیت بر روی پنجره Net Support نمایش داده می شود. در بخش میانی این زیر منو با انتخاب گزینه Larg باعث می شود که ایکن صفحه نمایش دانش‌آموزان بصورتی که صفحات آن‌ها قابل نمایش باشد نشان داده می شود. با انتخاب گزینه Small باعث می شود که فقط اسامی Clientها بصورت کوچک

نمایش داده شود. با انتخاب گزینه List اسامی Clientها بصورت یک لیست وستونی نمایش داده می شود و بالاخره با انتخاب گزینه Details اسامی Clientها بهمراه مشخصات آن‌ها به نمایش در می آیند.



Current Setting: با انتخاب این گزینه پنجره تنظیمات رایج ظاهر می شود. بطور مثال دا در این پنجره می توان تایید کرد که اگر پنجره کنترل بسته شود ابتدا اتصال بین سیستم‌ها قطع شود وسپس پنجره کنترل بسته شود.

Normal View: در حالت نمایش Normal پنجره های دانش‌آموزان بصورت فقط اسامی آن‌ها که در حالت اتصال هستند یا نه به نمایش در می آید.

Monitor View: دراین حالت نمایش مانیتور های دانش‌آموزان با در صد بزرگنمایی که ما تعیین می کنیم نمایش داده می شوند.

Web View: در این حالت نمایش نشان داده می شود که کدام یک از دانش‌آموزان در محیط اینترنت مشغول به کار می باشد.

Application View: دراین حالت نمایشی مشخص می شود که هر کدام از دانش‌آموزان در کدام نرم‌افزار مشغول به کار هستند بصورتی که آیکن نمادین آن نرم‌افزار برروی نام دانش‌آموز حک می شود.

Survey View: با انتخاب این گزینه می توان سوالی با پاسخ مشخص مثل بله، خیر و غیره را از دانش‌آموزان پرسید ونتیجه ودرصد پاسخ دهی را متوجه شد. (نظر سنجی)

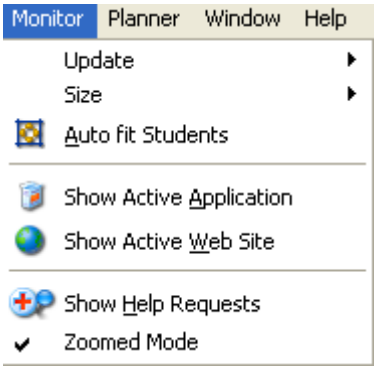
White Board View: دراین حالت نمایش یک صفحه سفید را که قلم ی بر روی آن وجود دارد می توان از آن برای انجام عمل تدریس استفاده کرد همانند یک صفحه وایت برد. لازم به ذکر است که گزینه های زیر منوی View در سمت چپ پنجره کنترل بصورت ابزار هایی قرار داده شده‌اند و قابل استفاده مستقیم هستند.

۶. منوی Monitor

Update: توسط این گزینه میزا ن زمان بروزرسانی صفحه کاری پنجره تنظیم می شود.

Size: توسط گزینه سایزمی توان اندازه صفحه کاری دانش‌آموزان را بر روی صفحه کنترل تنظیم کرد که با چه اندازه ای نمایش داده شوند تا تمام صفحات کاری بصورت یکجا قابل مشاهده باشد.

Auto Fit Student: توسط این گزینه تنا سب واندازه صفحات کاری دانش‌آموزان طوری تنظیم می شود که دبیر بتواند بتواند تمام مانیتور های دانش‌آموزان را بر روی صفحه کنترل خود داشته باشند.



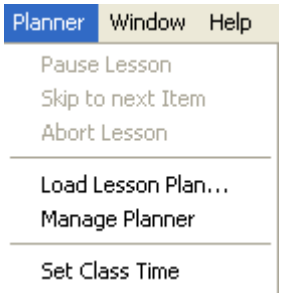
Show Active Application: با انتخاب این گزینه آیکن مشخصه ی نرم‌افزاری را که بصورت فعال دانش‌آموزان با آن در حال کار کردن هستند در کنار مانیتور آن‌ها نمایش می دهد.

Show Active Web Site: با این گزینه نیز آیکن مشخصه وب سایتی را که دانش‌آموزان با آن در حال کار کردن هستند نمایش می دهد.

Show Help Request: با این گزینه اگر در مورد خاصی احتیاج به راهنمایی داشتیم از این گزینه استفاده می کنیم.

Zoomed Mode: اگر این گزینه فعال باشد پس از اینکه دبیر بر روی سیستم دانش‌آموزی با ماوس اشاره کند صفحه کاری او بزرگ می شود تا بهتر قابل نمایش باشد.

۷. منوی Planner



توسط گزینه های این منو دبیر می تواند بر روی طرح درسی که آماده کرده است کنترل داشته باشد.

Pause Lesson: برای توقف موقت برنامه تدریس از این گزینه استفاده می شود.

Skip To Next Item: برای پرش از روی یک موضوع درسی و رفتن به روی موضوع بعدی از این دستور استفاده می‌شود.

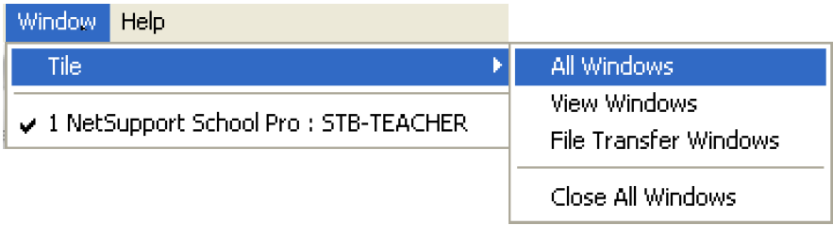
Abort Lesson: برای صرف نظر از اجرای برنامه درسی از این فرمان استفاده استفاده می کنیم.

Load Lesson Plan: از این فرمان برای فراخوانی طرح درس ایجاد شده استفاده می کنیم.

Manage Planner: توسط این فرمان می توان برنامه درسی را که طراحی کرده ایم می توان ویرایش کرد و یا به آن برنامه درسی موضوعی را اضافه کرد ویا حذف نمود.

Set Class Time: توسط این گزینه می توان مدت زمان اجرای برنامه درسی را برای دانش‌آموزان تنظیم کرد.

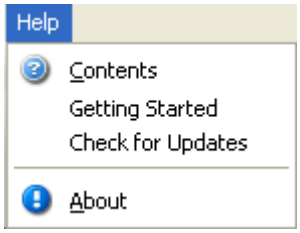
۸. منوی Window



درمنوی Window گزینه ای به نام Tile وجود داردکه با انتخاب گزینه All Windows میتوان تمامی پنجر ه‌ها بصورت کاشی کاری در صفحه نمایش بصورت مرتب قرار داد. برای نمایش یک پنجره از گزینه View Windows استفاده می کنیم.

با گزینه Close All Windows تمام پنجره های دانش‌آموزان که باز هستند بسته می شود.

۹. منوی Help



توسط پنجره Help برنامه Net Support می توان در باره کلیه مسایل و مشکلات احتمالی که پیش می آیند اطلاعات جامعی را بدست آورد.

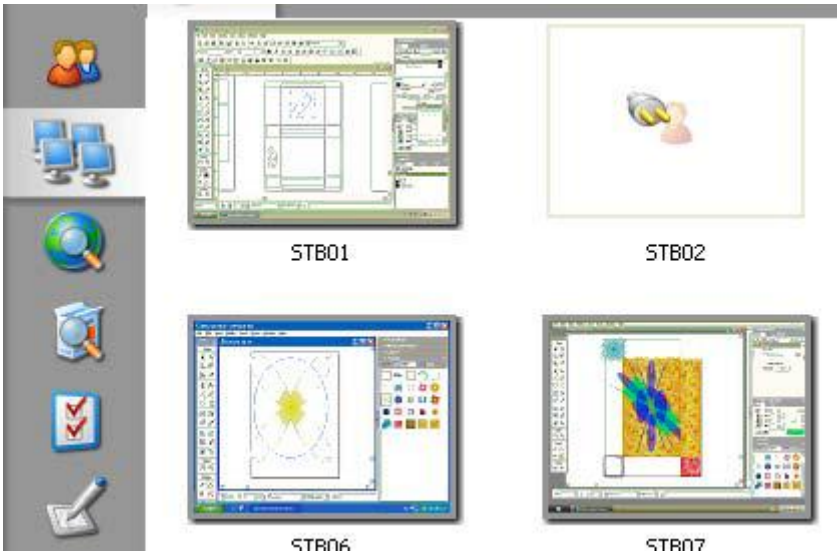
۱۰. نمایش لیست اسامی دانش‌آموزان (Normal View)



در حالت نمایش Normal پنجره های دانش‌آموزان بصورت فقط اسامی آن‌ها که در حالت اتصال هستند یا نه به نمایش در می آید.

۱۱. نمایش صفحات مانیتور دانش‌آموزان (Monitor View)

دراین حالت نمایش، مانیتور های دانش‌آموزان با در صد بزرگنمایی که ما تعیین می کنیم نمایش داده می شوند.



۱۲. برقراری ارتباط با اینترنت

از طریق این ابزار دانش‌آموزان می توانند با اینترنت ارتباط بر قرار کنند.



برای وارد کردن یک آدرس اینترنتی در محیط Net Support وهمچنین برای محدود کردن ورود دانش‌آموزان به سایر سایت‌ها از این ابزار استفاده می شود و پس از انتخاب این ابزار پنجره زیر ظاهر می شود.



که توسط قسمت Approved Sites و انتخاب علامت + می توان سایت های مورد نظر را که برای دانش‌آموزان مجاز است اضافه کرد. و در قسمت Restriched Sites و با انتخاب علامت + می توان سایت های غیر مجاز را معرفی کرد که دانش‌آموزان مجاز به استفاده از این سایت‌ها نباشند.

۱۳. پایش دانش‌آموزان

توسط این ابزار بدون اینکه مانیتور های دانش‌آموزان دیده شود ما می توانیم تشخیص دهیم که هر کدام از دانش‌آموزان در چه محیط نرم‌افزاری مشغول به کار هستند. به نحوی که آیکون هر نرم‌افزار در کنار آیکون هر دانش‌آموز مشاهده می شود.



۱۴. نظر سنجی

توسط این ابزار می توان از کلاس نظر سنجی نمود. یعنی سوالاتی با پاسخ مشخص مثل بله، خیر یا صحیح و غلط از دانش‌آموزان پرسید و نتایج آنرا به صورت تک تک و یا کل کلاس، به صورت در صد مشاهده نمود.



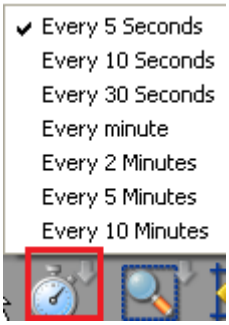
۱۵. تخته سفید

این ابزار در حقیقت یک وایت برد می باشد. یعنی هنگامی که روی این ابزار کلیک کنیم می توان بوسیله موس و یا قلم نوری (بسیار بهتر از موس) هر مطلبی را نوشت و با کلیک روی آیکون آدمک با فلش سبز هر چه روی صفحه نوشته شده بر روی مانیتور دانش‌آموزان نیز دیده می شود. در حقیقت این یکی از بهترین ابزارهای این نرم‌افزار است. البته این قسمت ابزارهای گوناگونی دارد مثلاً می توان نوشته‌ها را به صورت عکس ذخیره نمود و یا رنگ قلم را به دلخواه انتخاب کرد و...



۱۶. به روز رسانی صفحات

توسط این ابزارمدت زمانی را که طول می کشد تا صفحات مانیتور دانش‌آموزان نو سازی شود و آخرین تغییرات در آن اعمال شود تنظیم می شود. پیش فرض برنامه روی ۵ ثانیه قرار دارد.



۱۷. بزرگنمایی

توسط این ابزار می توان بزگنمای ی صفحه نمایش دانش‌آموزان را تنظیم نمود. اندازه صفحات آن‌ها را به اندازه مورد نظر خود تغییر دهیم.



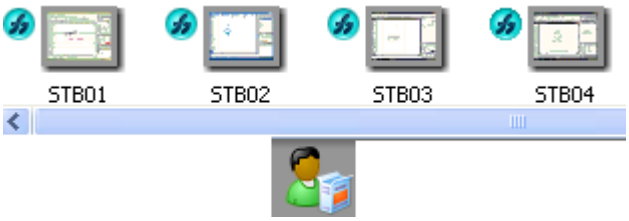
۱۸. اندازه خودکار

با انتخاب این ابزار صفحه مانیتور دانش‌آموزان به اندازه ای بزرگ می شود که همه مانیتورها بر روی صفحه کنترل قابل مشاهده باشند.



۱۹. پایش دانش‌آموزان

با انتخاب این ابزار می توان مشاهده نمود که هر کدام از دانش‌آموزان با چه نرم‌افزاری مشغول به کار هستند.



توسط این ابزار می توان مشاهده کرد که هرکدام از دانش‌آموزان که وارد محیط اینترنت شده‌اند در چه سایتی مشغول به کار هستند.



از این ابزار برای بزرگنمایی صفحه نمایش دانش‌آموزی که مورد نظر است استفاده می شود.



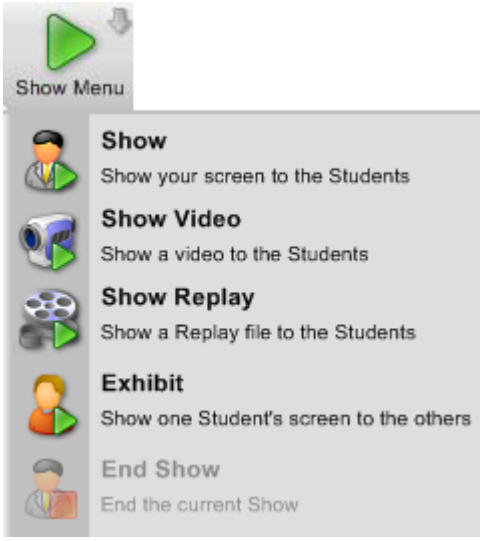
۲۰. Refresh

توسط این فرمان می توان Client هایی که جدیدا وارد شبکه شده باشند یا آن‌هایی که در اثر عوامل مختلف موقتا خارج شده باشند را مجددا شناسایی کرد همچنین این فرمان در منوی School نیز یافت می شود.

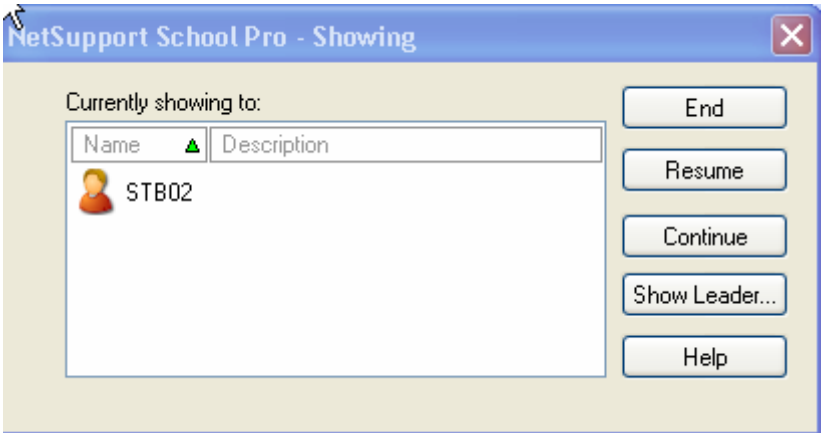


۲۱. نمایش صفحه دبیر روی صفحه دانش‌آموزان

از این منو جهت نمایش تصویر سیستم دبیر بر روی سیستم دانش‌آموزان و همچنین برای نمایش فایل ویدیویی و پایان نمایش استفاده می شود.



Show: برای نمایش نرم‌افزار مورد تدریس از این گزینه به این ترتیب استفاده می شود. ابتدا دبیر نرم‌افزار مر بوطه را بر روی سیستم خود فعال می کند و سپس وارد محیط نرم‌افزار Net Support شده واز گزینه Show Menu گزینه Show را انتخاب میکند آنگاه هر عملی که دبیر انجام می دهد بر روی سیستم دانش‌آموزان نمایش داده می شود ودانش‌آموز هیچ عملی را نمی تواند انجام دهد. برای خروج از حالت نمایشی وتدریس دبیر باید بر روی نوار وظیفه (گوشه سمت راست در پایین صفحه نمایش) بر روی آیکن که  درست شبیه آیکن Show Menu است دابل کلیک کرده تا پنجره زیر ظاهر شود سپس از داخل این پنجره با انتخاب گزینه End سیستم های دانش‌آموزان به صفحه های قبلی خود بر می گردند.



۲۲. نمایش صفحه دانش‌آموز روی صفحه دیگر دانش‌آموزان

Exhibit: توسط این گزینه می توان صفحه کاری یکی از دانش‌آموزان را بر روی تمام صفحات کاری دانش‌آموزان دیگر انداخت و آن را نمایش داد.

End Show: از این گزینه نیز برای پایان نمایش جاری استفاده می کنیم.

۲۳. نمایش صفحه دانش‌آموز روی صفحه دبیر

توسط این ابزار می توان صفحه کاری Client انتخاب شده (دانش‌آموز) را بصورت تمام صفحه مشاهده کرد.

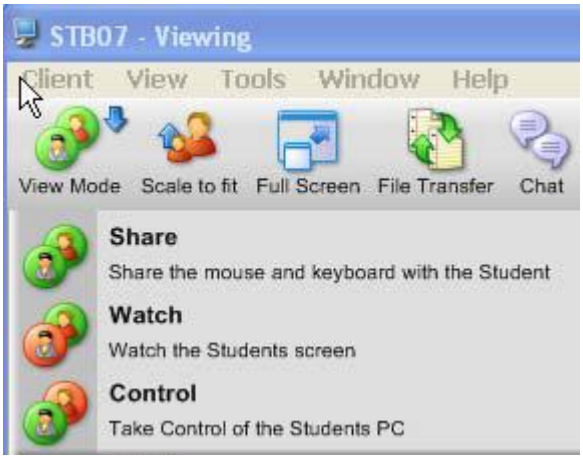


و در پنجره ای که مر بوط به صفحه کاری دانش‌آموزان است نوار ابزار زیر ظاهر می شود.روش دیگر برای دیدن صفحه کاری یک دانش‌آموز دابل کلیک بر روی آیکن مربوط به آن Client می باشد.



۲۴. نمایش

با انتخاب گزینه View Mode منوی زیر با سه گزینه فعال می شود.

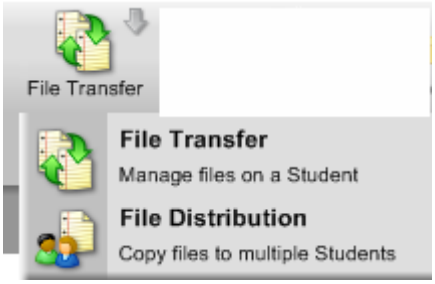


Share: با انتخاب گزینه Share باعث می شود که وقتی صفحه دانش‌آموزهم توسط دبیر قابل کنترل باشد وهم دانش‌آموز بتواند با صفحه کلید وماوس خود کار کند

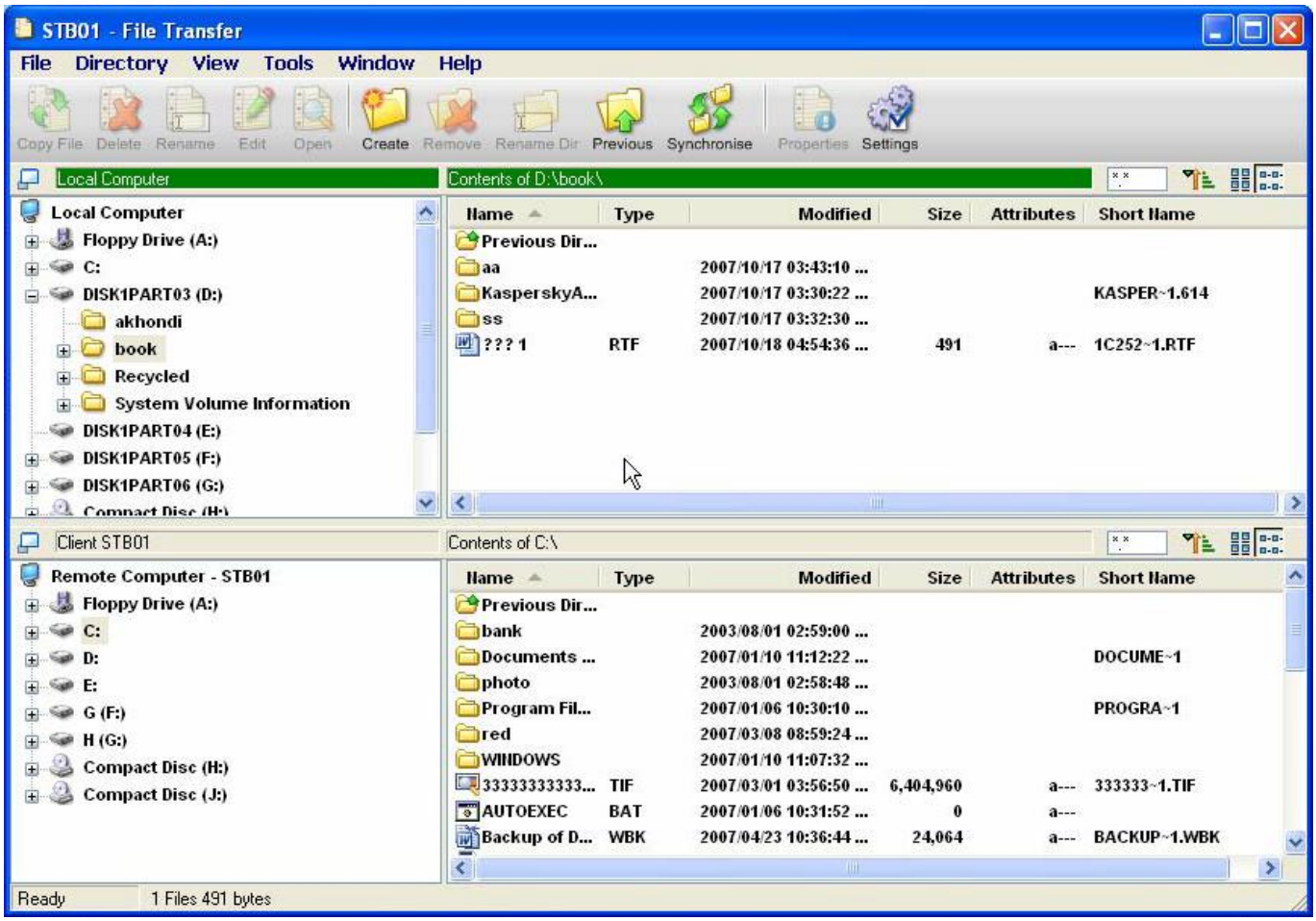
Watch: توسط این گزینه دبیر فقط میتواند کار دانش‌آموز را مشاهده کند و هیچگونه امکان تغییر از سوی دبیر وجود ندارد.

Control: با انتخاب این گزینه دانش‌آموز نمی تواند کاری را انجام دهد و فقط این دبیر است که کنترل را در دست داردو در صفحه کاری د انش آموزان می تواند کار کند.

۲۵. انتقال فایل



توسط گزینه File Transfer می توان در داخل پنجره ای فایل یا فایل هایی را برای دانش‌آموزان کپی کرد ویا برعکس بعد از انتخاب این گزینه ساختار درختی سیستم دبیر در بخش بالای پنجره وساختار درختی سیستم انتخاب شده دانش‌آموز مورد نظر در پا یین صفحه به نمایش در می آید که می توان فایل یا فایل هایی را برای انجام عمل کپی از مسیر مبدا به مقصد انتخاب کرد علاوه بر این عمل در این پنجره می توان پوشه جدیدی نیز ساخت.



۲۶. قفل

توسط ابزار Lock می توان Client یا Client های انتخاب شده را غیر فعال کرد به نحوی که سیستم دانش‌آموزان از هر نظر غیر فعال می شود؛ به صورتی که نه صفحه کلید فعال می شود و نه ماوس کار می کند. و با ابزار Unlock می توان سیستم های قفل شده را آزاد کرد.



۲۷. بلوکه کردن اینترنت

توسط این ابزار می توان مانع دسترسی کلیه دانش‌آموزان به اینترنت شد. اگر دانش‌آموزی برنامه Internet Explorer را اجرا نماید سیستم پیغام اخطاری مبنی بر قفل بودن اینترنت به دانش‌آموز می دهد.



۲۸. قفل مانیتور

با این ابزار می توان برای ارائه دروس تئوری کلیه مانیتورها را به حالت خاموش (سیاه) در آورد. وبدون اینکه نیازی به خاموش کردن مانیتورها از سوی دانش‌آموزان باشد وبا کلیک مجدد روی این ابزار دوباره سیستم‌ها به حالت عادی تبدیل می شوند.



۲۹. مدیریت دانش‌آموزان

با انتخاب این ابزار می‌توان بر روی سیستم‌های دانش‌آموزان عملیات مدیریتی انجام داد که در قسمت زیر شرح داده شده است.



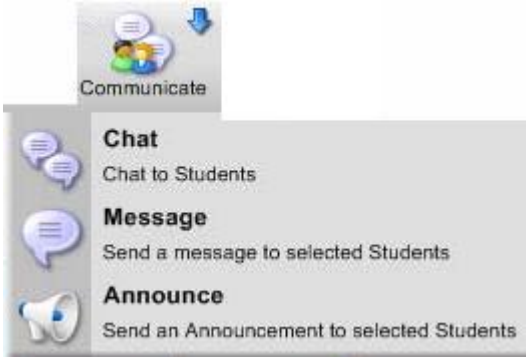
Power On: با انتخاب این گزینه اگر یک یا چند Client در Domain مربوطه قبلا وارد شده باشند می توان آن هارا روشن کرد.

Power Off: توسط این گزینه می توان Client های انتخاب شده روشن را خاموش کرد.

Reboot: با این گزینه می توان سیستم یا سیستم های انتخاب شده را مجددا راه اندازی کرد

Logout: با این گزینه می توان محیط کار بری Client مربوطه را تغییر داد.

۳۰. ارتباطات



با انتخاب گزینه Communication میتوان با دانش‌آموزان ارتباط نوشتاری وصوتی برقرار کرد.

Chat: با انتخاب گزینه Chat شما می توانید همزمان با دانش‌آموز از طریق پنجره ای ارتباط نوشتاری داشته باشید

Massage: از این گزینه جهت فرستادن پیام برا ی Client مورد نظر استفاده می شود.

Announce: اگر سیستم دانش‌آموزان دارای سیستم های پخش صوت باشد از این طریق می توان برای آن‌ها فایل های صوتی را ارسال کرد.

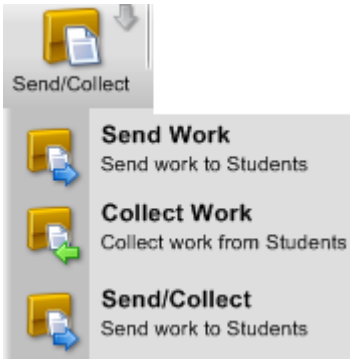
۳۱. طرح درس



با گزینه Execute Plan فایلی را که قبلا برای انجام عمل تدریس خود طراحی کرده ایم می توانیم به اجرا در آوریم.

و توسط گزینه Manage Plans می توانیم طرح درسی را که پیاده کرده بودیم ویرایش کنیم ویا طرح درس جدیدی را بسازیم.

۳۲. تکالیف



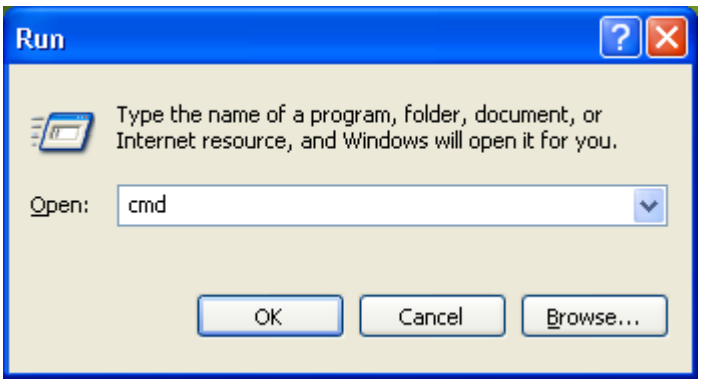
توسط این منو می توان تکالیفی را برای دانش‌آموزان فرستاد و پس از انجام مجدداً آن‌ها را جمع آوری نمود. مثلاً یک فایل ورد را که حاوی سوالات است را از طریق Send Work فرستاد و پس از مدت زمان مشخصی همان فایل را از کامپیوتر دانش‌آموزان مجدداً جمع آوری نمود (از طریق Collect Work). این حالت برای امتحاناتی که شامل چند سوال است بسیار مناسب است.

فصل ۲۱

دستورات پر کاربرد شبکه

۲۱-۱- محل اجرای دستورات

در این فصل به معرفی برخی دستورات شبکه می‌پردازیم. برای اجرای این دستورات بایستی از محیط Command Prompt استفاده نمایید. برای این کار وارد Run شده و تایپ کنید cmd.



۲۱-۲- دستور IPConfig

ipconfig، یکی از دستورات مفید به منظور بررسی وضعیت پیکربندی TCP/IP در کامپیوترهای سرویس دهنده و یا سرویس گیرنده‌ای است که بر روی آنان ویندوز نصب شده است. در یونیکس و لینوکس از دستور ifconfig در این رابطه استفاده می‌شود. در سیستم هایی که بر روی آنان ویندوز 9x و یا ME نصب شده است، می‌توان از دستور winipcfg استفاده نمود.

استفاده از ipconfig

برای استفاده از دستور فوق، کافی است نام آن را از طریق پنجره command prompt تایپ نمود. عملکرد ipconfig و اطلاعاتی که در اثر اجرای آن نمایش داده خواهد شد به نوع سوئیچ استفاده شده، بستگی دارد.

استفاده از ipconfig بدون سوئیچ، اطلاعات پیکربندی TCP/IP در ارتباط با هر یک از آداپتورهای موجود بر روی سیستم را نمایش خواهد داد:

- **آدرس IP**
- **Subnet Mask**
- **Default Gateway**
- **اطلاعات سرویس دهنده DNS**
- **Domain**

تایپ دستور	خروجی
C:\> ipconfig	**Ethernet adapter MyLan1:** Connection-specific DNS Suffix.: IP Address.....: 10.10.1.1 Subnet Mask.....: 255.0.0.0 Default Gateway.....: **PPP adapter My ISP:** Connection-specific DNS Suffix.: IP Address.....: 10.1.1.216 Subnet Mask.....: 255.255.255.255 Default Gateway.....: 10.1.1.216

دستور فوق، اطلاعات مربوط به اتصالات از نوع PPP که از آنان در Dialup و VPN استفاده می‌شود را نیز نمایش خواهد داد.

استفاده از ipconfig به همراه سوئیچ all، علاوه بر نمایش اطلاعات اشاره شده در بخش قبل، اطلاعات دیگری را نیز نمایش خواهد داد:

- آدرس سخت‌افزاری کارت شبکه (آدرس MAC)
- اطلاعات مربوط به DHCP

تایپ دستور	خروجی
C:\> ipconfig /all	**Windows 2000 IP Configuration** Host Name.....: srco Primary DNS Suffix.....: srco. ir Node Type.....: Broadcast IP Routing Enabled.....: No WINS Proxy Enabled.....: No DNS Suffix Search List.....: srco. ir **Ethernet adapter MyLan1:** Connection-specific DNS Suffix.:

	Description.....: D-Link DFE-680TX CardBus PC Card **Physical Address.....: 00-50-BA-79-DB-6A** **DHCP Enabled.....: No** IP Address.....: 10.10.1.1 Subnet Mask.....: 255.0.0.0 Default Gateway.....: DNS Servers.....: 127.0.0.1 **PPP adapter My ISP:** Connection-specific DNS Suffix.: Description.....: WAN (PPP/SLIP) Interface Physical Address.....: 00-53-45-00-00-00 00-53-45-00-00-00 DHCP Enabled.....: No IP Address.....: 10.1.1.216 Subnet Mask.....: 255.255.255.255 Default Gateway.....: 10.1.1.216 DNS Servers.....: x1.y1.z1. w1 x2.y2.z2. w2

سایر سوئیچ‌های دستور ipconfig: با استفاده از دستور ipconfig و برخی سوئیچ‌های آن (release، renew)، می‌توان اطلاعات مربوط به پیکربندی TCP/IP ارائه شده توسط سرویس دهنده DHCP را که در اختیار یک سرویس گیرنده قرار داده شده است را آزاد و یا آنان را مجددا از سرویس دهنده درخواست نمود (در مورد DHCP در فصل‌های آینده صحبت خواهیم کرد). فرآیند فوق به منظور تشخیص عملکرد صحیح سرویس دهنده DHCP در شبکه بسیار مفید و سرور است. (آیا سرویس دهنده DHCP وظایف خود را به خوبی انجام می‌دهد؟ آیا یک سرویس گیرنده قادر به برقراری ارتباط با سرویس دهنده DHCP به منظور درخواست و دریافت اطلاعات پیکربندی TCP/IP می‌باشد؟). دستور ipconfig دارای سوئیچ‌های مفید متعددی است که می‌توان با توجه به نوع خواسته خود از آنان استفاده نمود:

سوئیچ	عملکرد
/release [adapter]	آدرس IP پیکربندی شده توسط DHCP را آزاد می‌نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP برای تمامی آداپتورهای موجود بر روی کامپیوتر، آزاد می‌گردد. در صورتی که قصد آزاد سازی اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم، می‌بایست به همراه سوئیچ فوق نام آداپتور نیز مشخص گردد. (مثلاً ipconfig / release MyLan1)
/renew [adapter]	یک آدرس IP را بر اساس اطلاعات جدیدی که از طریق DHCP دریافت می‌نماید، پیکربندی مجدد می‌نماید. در صورتی که سوئیچ فوق را به تنهایی و بدون مشخص نمودن adapter تایپ نماییم، پیکربندی IP تمامی آداپتورهای موجود بر روی کامپیوتر، مجدداً" انجام خواهد شد. در صورتی که قصد ایجاد مجدد اطلاعات پیکربندی مربوط به یک آداپتور خاص را داشته باشیم، می‌بایست به همراه سوئیچ فوق

	نام آداپتور نیز مشخص گردد. (مثلاً ipconfig / renew MyLan1)
/flushdns	حذف محتویات DNS Resolver Cache
/registerdns	Refresh نمودن تمامی اطلاعات تولید شده توسط DHCP برای آداپتور و ریجستر نمودن اسامی DNS
/displaydns	نمایش محتویات DNS Resolver Cache
/showclassid [adapter]	نمایش تمامی DHCP Class ID مجاز برای آداپتور
/setclassid [adapter] [classidtoset]	تغییر DHCP Class ID

تشخیص نام آداپتور: نام آداپتور را می‌توان با کلیک (Right click) بر روی Network Neighborhood و انتخاب گزینه Properties، از طریق پنجره Network and Dial-up Connections مشاهده نمود (اسامی آدپتورها، نام آیکون‌ها می‌باشند).

مفهوم DNS Cache: زمانی که یک سیستم، ترجمه (تبدیل نام Host به آدرس) را از طریق یک سرویس دهنده DNS دریافت می‌نماید، برای مدت زمان کوتاهی آن را در یک Cache ذخیره می‌نماید. در صورتی که مجددا از نام استفاده شود، پشته TCP/IP محتویات Cache را به منظور یافتن رکورد درخواستی بررسی می‌نماید. بدین ترتیب امکان پاسخگوئی سریعتر به درخواست ترجمه نسبت به حالتی که در خواست برای یک سرویس دهنده DNS ارسال می‌شود، فراهم می‌گردد. با توجه به این که اندازه Cache نمی‌تواند از یک میزان منطقی و تعریف شده تجاوز نماید، هر رکورد موجود در Cache پس از مدت زمانی خاص حذف می‌گردد. در صورت اعمال هرگونه تغییرات در DNS (مثلاً تغییر یک رکورد DNS)، می‌توان با استفاده از دستور ipconfig /flushdns تمامی رکوردهای موجود در Cache را حذف نمود. بدین ترتیب در صورت درخواست یک نام Host، با سرویس دهنده DNS مشورت می‌گردد و نتایج مجددا" در Cache ذخیره خواهند شد. دستور ipconfig /displaydns، محتویات Cache را نمایش خواهد داد. از اطلاعاتی که نمایش داده می‌شود، می‌توان به منظور تشخیص این موضوع که آیا برای ترجمه نام به آدرس از Cache و یا سرویس دهنده DNS استفاده شده است، کمک گرفت.

موارد استفاده از دستور Ipconfig: از دستور فوق در مواردی که قصد تشخیص این موضوع را داریم که آیا سرویس دهنده DNS و DHCP در شبکه به درستی وظایف خود را انجام می‌دهند، استفاده می‌شود (علاوه بر مشاهده اطلاعات پیکربندی TCP/IP). مثلاً با استفاده از سوئیچ‌های release و renew، می‌توان براحتی تشخیص داد که آیا در زمینه دریافت اطلاعات پیکربندی از یک سرویس دهنده DHCP مشکل خاصی وجود دارد. از سوئیچ‌های مرتبط با DNS می‌توان به منظور اعمال تغییرات پیکربندی، بهنگام سازی cache محلی و یا رجیستر نمودن اطلاعات پیکربندی جدید با یک سرویس دهنده DNS، استفاده نمود.

۲۱-۳- دستور Ping

Ping دستوری است که مشخص می‌کند که آیا یک کامپیوتر خاص که ما IP یا Hostname (نام کامپیوتر) آن را می‌دانیم، روشن و فعال (Active) هست یا نه، یا اینکه ما قابلیت اتصال به وی را داریم یا نه؟ و اینکه اگر فعال باشد مدت زمان رسیدن بسته‌های TCP/IP از آن کامپیوتر به کامپیوتر ما چقدر است.

استفاده از این دستور به صورت زیر است:

Ping [IP-or-Hostname]

که به جای IP-or-Hostname باید آدرس IP و یا Hostname کامپیوتر مورد نظر را بگذاریم.

مثلاً Ping iut.ac.ir (سایت دانشگاه صنعتی اصفهان) را در command prompt تایپ کردم و به نتایج زیر رسیدم:

Pinging iut.ac.ir [217.219.19.121] with 32 bytes of data:

Reply from 217.219.19.121: bytes=32 time=1402ms TTL=105
Reply from 217.219.19.121: bytes=32 time=941ms TTL=105
Reply from 217.219.19.121: bytes=32 time=981ms TTL=105
Reply from 217.219.19.121: bytes=32 time=851ms TTL=105
Ping statistics for 217.219.19.121:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:

Minimum = 851ms, Maximum = 1402 ms, Average = 1043ms

این نتایج نشان می‌دهد که iut.ac.ir فعال است.

در نتیجه به دست آمده، منظور از bytes، مقدار بایت‌های ارسالی و دریافتی در هر بسته است. منظور از time، مدت زمانی است که طول کشیده تا بسته مورد نظر به مقصد برسد و منظور از TTL، تعداد گام‌های اعتبار بسته ارسالی است.

حالا به کامپیوتری با آدرس IP شماره ۲۱۷.۲۱۹.۱۹.۱۲۱ (که همان iut.ac.ir است)، Ping می‌کنیم. نتایج همان است فقط با تغییراتی در سطر اول. (البته time که معنای مدت زمان رسیدن بسته را می‌دهد، با توجه به ترافیک شبکه، کم و زیاد خواهد شد). برای Ping کردن به این IP، دستور Ping ۲۱۷.۲۱۹.۱۹.۱۲۱ را صادر می‌کنیم.

فرض کنید که به یک IP که فعال نیست، Ping کنیم. نتیجه به صورت زیر خواهد بود:

Pinging 217. 66.196.1 with 32 bytes of data :

Request timed out .

Request timed out .

Request timed out .

Request timed out .

Ping statistics for 217. 66.196.1:

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

که نشان می‌دهد که آن IP در آن لحظه فعال نیست.

البته تمام مطالبی که در بالا ذکر شد، در حالتی است که مستقیماً به اینترنت وصل شدهاید و یا اگر از طریق شبکه محلی به اینترنت وصل هستید، شبکه شما به درستی پیکربندی شده باشد. اصولا Ping یکی از بهترین دستورات برای پیدا کردن ایراد در شبکه است.

Optionهای مختلف دستور Ping:

۱) Ping –t

با استفاده از پارامتر **"t"** می‌توان تعیین کرد تا دستور **Ping** تا زمان **interrupted** شدن توسط کاربر به Ping کردن ادامه دهد. یعنی کار ارسال بسته تا بینهایت ادامه یابد، مگر اینکه کاربر آن را متوقف کند.

۲) Ping –a

با استفاده از پارامتر **"a"** نیز می‌توان نام هاست IP مورد نظر را پیدا کرد. به عبارتی این پارامتر نام هاست متناظر با IP را نمایش میدهد.

۳) Ping –n

با استفاده از پارامتر **"n"** نیز می‌توان تعداد دفعات ارسال **Echo Request messages** را که به طور پیش فرض **چهار بار** می‌باشد افزایش یا کاهش داد.

۴) Ping –l

با استفاده از پارامتر **"l"** نیز می‌توان حجم بسته **Echo Request messages** را که به طور پیش فرض **۳۲ بایت** می‌باشد تغییر داد. بیشترین مقدار مجاز برای این پارامتر **۶۵،۵۲۷** می‌باشد.

۵) Ping –i

با استفاده از پارامتر **"i"** نیز می‌توان مدت زمان زنده بودن بسته سرگردان را تعیین کرد. به عبارت دیگر این پارامتر - TTL Time To Live بسته **Echo Request messages** را تعیین می‌کند.

۶) Ping –v

با استفاده از پارامتر **"v"** نیز می‌توان مقدار TOS - Type Of Service در هدرای پی **Echo Request messages** را تعیین کرد. مقدار پیش فرض ۰ می‌باشد. محدوده مجاز این مقدار نیز ۰ تا ۲۵۵ می‌باشد.

۷) Ping -w

با استفاده از پارامتر **"w"** نیز می‌توان مدت زمان انتظار برای دریافت پاسخ از هاست بر حسب milliseconds را تعیین نمود.

۲۱-۴- دستور Tracert/Traceroute

همانطور که از نام این ابزار پیداست، از tracert برای پیدا کردن مسیر بین دو Host یا به عبارتی دو دستگاه دارای آدرس شبکه که همدیگر را می‌بینند استفاده می‌شود. یعنی اینکه بسته ارسالی ما برای رسیدن از مبدا به مقصد از چه دستگاه هایی عبور می‌کند. این دستور از طریق پروتکل ICMP این عمل را انجام می‌دهد و آن بدین صورت است که بسته Echo Request توسط کامپیوتر ما به دستگاه مقصد ارسال می‌شود و در هر مرحله‌ای از این مسیر، بسته Echo Reply ایجاد شده و به

کامپیوتر مبدا (کامپیوتر ما) ارسال می‌شود. باید این نکته را خاطرنشان کنم هریک از چهار سیستم عامل معروف امروزی دارای دستور ویژه خود در این ابزار هستند که در زیر لیست آن‌ها را آورده ایم:

Windows Server 2000/2003	tracert
Novell NetWare	iptrace
Linux/UNIX/ Macintosh	traceroute

این دستور علاوه بر اینکه اطلاعات جامعی از هر یک از مسیر یاب‌های مسیر تا رسیدن به مقصد به ما می‌دهد بلکه نام آن مسیر یاب‌ها را در صورتی که در آن‌ها تنظیم شده و در دسترس قرار گرفته باشد نشان خواهد داد. همچنین زمان رفت و برگشت بسته ICMP ما از مبدا تا مسیر یاب بین راه، بر مبنای میلی ثانیه نیز توسط این دستور مشخص خواهد شد. این اطلاعات به ما کمک خواهد کرد تا کشف کنیم در کجای مسیر ارتباطی بین دو نقطه از شبکه مشکل وجود دارد. در زیر یک نمونه موفق از استفاده از این دستور در ویندوز ۲۰۰۳ را مشاهده می‌کنید:

```
C:\>tracert 24.7.70.37
Tracing route to c1-p4.sttlwa1.home.net [24.7.70.37] Over a maximum of 30 hops:

1 30 ms 20 ms 20 ms 24.67.184.1
2 20 ms 20 ms 30 ms rd1ht-ge3-0.ok.shawcable.net [24.67.224.7]
3 50 ms 30 ms 30 ms rc1wh-atm0-2-1.vc.shawcable.net [204.209.214.193]
4 50 ms 30 ms 30 ms rc2wh-pos15-0.vc.shawcable.net [204.209.214.90]
5 30 ms 40 ms 30 ms rc2wt-pos2-0.wa.shawcable.net [66.163.76.37]
6 30 ms 40 ms 30 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]
Trace complete.
```

درست مانند سایر دستورات که در این بخش با آن پرداخته ام دستور tracert هم دارای ستون هایی است که اطلاعات مورد نیاز ما در آن تفکیک شده‌اند. ستون اول شماره هاپ (گام‌های طی شده) را مشخص کرده است؛ به روایت دیگر یعنی جایی که بسته ICMP ارسالی کامپیوتر ما با آن رسیده است. سه ستون دیگر نمایانگر زمان ارسال و برگشت بسته ارسالی به میلی ثانیه و آخرین ستون نام Host مقصد و آدرس IP دستگاه پاسخ دهنده را مشخص می‌کند. بدیهی است درصورت وجود مشکل در مسیر ارتباطی به مقصد Trace routeهای ما موفقیت آمیز نخواهند بود. در مثال زیر نمونه‌ای از آن را مشاهده می‌کنید:

```
C:\>tracert comptia.org
Tracing route to comptia.org [216.119.103.72]
Over a maximum of 30 hops:

1 27 ms 28 ms 14 ms 24.67.179.1
2 55 ms 13 ms 14 ms rd1ht-ge3-0.ok.shawcable.net [24.67.224.7]
3 27 ms 27 ms 28 ms rc1wh-atm0-2-1.shawcable.net [204.209.214.19]
4 28 ms 41 ms 27 ms rc1wt-pos2-0.wa.shawcable.net [66.163.76.65]
5 28 ms 41 ms 27 ms rc2wt-pos1-0.wa.shawcable.net [66.163.68.2]
6 41 ms 55 ms 41 ms c1-pos6-3.sttlwa1.home.net [24.7.70.37]
7 54 ms 42 ms 27 ms home-gw.st6wa.ip.att.net [192.205.32.249]
8 * * * Request timed out.

9 * * * Request timed out.
```

10 * * * Request timed out.

در این مثال بسته ارسالی ICMP ما تنها موفق شده تا هفت مرحله پیش برود و در مرحله هشتم به مشکل برخورد کرده است که دلیل آن می‌تواند این باشد که دستگاهی که در مرحله هشتم قراردارد قطع است و یا اینکه دستگاه موجود در مرحله هفتم کار می‌کند. اما امکان مشخص کردن هاپ بعدی را ندارد. عوامل بسیاری می‌تواند وجود داشته باشد که دستگاه مرحله هفت قادر به انجام وظیفه نگردیده است که ممکن است مشکل در جدول Route آن باشد و یا Connection صحیحی برای آنان ایجاد نشده باشد. با توجه به موارد بالا متوجه می‌شوید که توسط این دستور شما بررسی مشکل را تنها بر روی یک یا دو دستگاه محدود کردهاید. این دستور همچنین می‌تواند به شما کمک کند تا شبکه‌های در مسیر با بار زیاد و متراکم را محدود سازید.

۲۱-۵- دستور NetStat

NetStat مخفف Network Statistics، یک ابزار خط فرمان است که اتصالات شبکه را (هم به داخل و هم به خارج)، جداول هدایت کردن بسته‌ها و تعدادی از آمار رابطه‌های شبکه‌ای را نشان می‌دهد. همچنین این ابزار برای پیدا کردن مشکلات در شبکه و برآورد گر حجم اطلاعات رد و بدل شده در شبکه به عنوان یک اندازه گیر عملکرد استفاده می‌شود.

پارامترهای ورودی

پارامترهایی که در ورودی همراه دستور وارد می‌شوند باید با – شروع شوند (در ویندوز امکان استفاده از علامت / نیز وجود دارد):

بدون پارامتر: نمایش Connectionهای فعال

a–: نمایش تمامی اتصالات TCP و UDP فعال در کامپیوتر.

b–: نمایش برنامه درگیر با اتصالات شبکه‌ای نمایش داده شده در لیست خروجی. (در ویندوز ۲۰۰۰ و ویندوزهای قبل از آن و سایر سیستم عامل‌های غیر ویندوزی امکان پذیر نیست)

e–: نمایش آمار مربوط به اترنت، از قبیل تعداد بایت‌ها و بسته‌های دریافتی و ارسالی. این پارامتر می‌تواند با s– نیز ترکیب شود.

f–: نمایش FQDN برای آدرس‌های خارجی. (فقط در ویندوز Vista و سیستم عامل‌های جدیدتر)

g–: نمایش کارت‌های شبکه و آمار آن‌ها. (در ویندوز موجود نیست، ipconfig می‌تواند این کار را در ویندوز انجام دهد)

n–: نمایش ارتباط‌های TCP فعال، هر چند که IPها و پورت‌ها را به صورت عددی نمایش می‌دهد و تلاشی برای تشخیص نام آن‌ها نمی‌کند.

m–: نمایش آمار مربوط به استریم‌ها.

o–: نمایش اتصال‌های TCP فعال به همراه PID مربوط به آن اتصال.

p–: در ویندوز، پروتکل مربوط به اتصال را نمایش می‌دهد. (TCP، UDP، ICMP، IP،...)

p-: در لینوکس فرآیندهای مربوط به اتصال را نشان می‌دهد. (مانند کلید b- در ویندوز عمل می‌کند) (برای اجرای صحیح دستور باید دسترسی پایه یا root داشت.)

P-: در سولاریس، پروتکل مربوط به اتصال را نمایش می‌دهد. (TCP، UDP، ICMP، IP،...)

r-: جدول هدایت IPها را نشان می‌دهد. (معادل دستور **route print** در ویندوز است.)

s-: نمایش آمار به تفکیک پروتکل.

v-: وقتی که با b- استفاده شود، توالی اجزای برنامه‌ها را نشان می‌دهد.

h- یا help--: نمایش راهنمایی برای دستورات موجود. (مناسب برای سیستم‌های شبه یونیکس)

/?: نمایش راهنمایی برای دستورات موجود. (فقط در ویندوز)

۲۱-۶- دستور Net

دستور Net بیشتر برای کار با Objectهای شبکه‌ای مورد استفاده قرار می‌گیرد. با این دستور بایستی کلمه‌ای دیگر مثل User یا Computer وارد کنید تا سیستم متوجه بشود که می‌خواهید با چه نوع Objectی کار کنید.

- چگونگی یافتن راهنمای دستورات زیر: ابتدا دستور Net، سپس کلمه Help و سپس نوع دستور را وارد نمایید. مثلا برای یافتن راهنمایی در مورد دستور Net File، بنویسید: Net Help File

نام دستور	شرح دستور
Net Accounts	با این دستور، وضعیت تنظیمات پسوردها (مثل طول عمر) نشان داده می‌شود.
Net Computer	کامپیوترها را به پایگاه داده‌ی Domain مورد نظر اضافه و یا کم می‌کند.
Net Continue	سرویسی که توسط دستور Net Pause معلق شده است را دوباره راه اندازی می‌کند.
Net File	نام تمامی فایل‌های باز و اشتراک گذاشته شده بر روی سرور را نمایش می‌دهد.
Net Group	لیست گروه‌های محلی تعریف شده را بیان می‌کند و نیز می‌شود فهمید در هر کدام از این گروه‌ها چه حساب هایی وجود دارد و نیز می‌شود به یک گروه خاص حسابی اضافه کرد. می‌خواهیم ببینیم که چه گروه‌های محلی تعریف شده است. می‌نویسیم: Net localgroup که نتیجه می‌شود: Aliases for \\Computer-name *Administrators Backup Operators Debugger Users *DHCP Administrators DHCP Users Guests *Power Users Replicator Users The command completed successfully. دقت کنید که ویندوز معمولاً هنگام ارائه نتایج دستورات Net، می‌آید و اول اسم هر گروه یک × قرار می‌دهد تا با حساب‌ها اشتباه نشود. حالا می‌خواهیم ببینیم که مثلاً در گروه Administrators چه حساب هایی هست. می‌نویسیم:

	Net localgroup Administrators که نتیجه می‌شود: Alias nameAdministrators Comment Administrators have complete and unrestricted accessto thecomputer/Domain Members Administrator Ali Reza The command completed successfully. پس سه تا حساب در حد Admin داریم. حالا می‌خواهیم مثلاً حساب Ali را از لیست Adminها خارج کنیم، می‌نویسیم: Net localgroup Administrators Ali /delete و با این کار حساب Ali از گروه حذف می‌شود (می توانید دوباره لیست بگیرید و ببینید که کاربر Ali دیگر در این گروه نیست). حالا می‌خواهیم دوباره حساب Ali را به این گروه اضافه کنیم، می‌نویسیم: Net localgroup Administrators Ali /add این دستور از جمله مهم ترین دستوراتی است که باید یاد بگیرید. گاهی با حسابی وارد می‌شویم و می‌خواهیم که این حساب را به حد Admin برسانیم و روش کار همین دستور آخری است (اینکه اجازه این کار را داریم یا نه، بحثی است که در این مبحث نمی‌گنجد). وقتی حسابی وارد گروه Admin می‌شود، تمام مزایای این گروه را به دست می‌آورد.
Net Help	این دستور در واقع Help دستور Net است.
Net Helpmsg	وقتی که یک دستور Net به صورتی اجرا می‌شود که خطایی پیش بیاید، ویندوز یک شماره خطای ۴ رقمی به ما می‌دهد که برای دریافت جزئیات بیشتر در مورد این خطا باید از دستور Net helpmsg استفاده کنیم.
Net Localgroup	گروهای محلی را نمایش، اصلاح یا اضافه می کند.
Net Name	این دستور به یک پیام نام اختصاص می‌دهد و یا نام آن را پاک می کند.
Net Pause	سرویس‌های درحال اجرا را متوقف می کند.
Net Print	اطلاعات مربوط به یک صف مشخص را نمایش می‌دهد؛ اطلاعات مربوط به تمامی صف‌های مربوط به سرور نوشته شده را نمایش می‌دهد؛ اطلاعات مربوط به یک کار مشخص را نشان می‌دهد و یا کار مشخص شده را کنترل می کند.
Net Send	فرض کنید که می‌خواهیم یک Message به فرد خاصی که به سیستم وارد شده است و یک Session دارد بفرستیم (اینکه فردی Session دارد یا نه، به کمک دستور Net Session قابل بررسی است). بدین منظور از این دستور می‌توانیم استفاده کنیم. مثلاً اگر بخواهیم به Administrator که الآن در سیستم هست، پیغام Salam Mashti را بفرستیم، می‌نویسیم:

	Net Send Administrator Salam Mashti در این حالت کاربر Administrator، پیغام ما را می‌گیرد. اگر بخواهیم به همه افرادی که الآن Session دارند، همین پیغام را بفرستیم، می‌نویسیم: Net Send /Users Salam Mashti و پیغام را همه می‌گیرند. این دستور باید به صورت Local یعنی از طریق یک Shell اجرا شود.
Net Session	به کمک این دستور مشخص می‌شود که چه کسانی الآن در سیستم یک Session دارند. به عبارت دیگر، برای مشاهده اینکه چه کسانی به صورت Remote به سیستم وارد شده‌اند. این دستور را تایپ کنید: Net Session تا لیست این افراد نمایان شود. اگر بخواهیم همه Sessionها را خاتمه بدهیم، می‌نویسیم: Net Session /delete این دستور، رابطه این کامپیوتر با سایر کامپیوترهای شبکه قطع می‌کند (نه ارتباط فیزیکی، بلکه اتصالاتی که مثلاً با برنامه Remote Desktop ایجاد شده اند). اگر فقط بخواهیم یک Session را با یک کامپیوتر خاص تمام کنیم، می‌نویسیم: Net Session \\xxx.xxx.xxx.xxx /delete این در حالتی است که با آن کامپیوتر Session داشته باشم. دقت کنید که به جای دستور Net Session می‌توانید از دستور Net Sessions یا Net Sess استفاده کنید.
Net Share	این دستور به ما کمک می‌کند که Shareها را به صورت محلی مدیریت کنیم (دستور بالایی به صورت Remote استفاده می‌شود). می‌خواهیم ببینیم که الآن چه Share هایی وجود دارد. می‌نویسیم: Net Share و جواب می‌گیریم: Share name ResourceRemark
Net Start	سرویس‌های شبکه را آغاز یا لیست می‌کند.
Net Statistics	آمار مربوط به پایگاه‌های کاری یا سرورها را نشان می‌دهد.
Net Stop	سرویس‌ها را متوقف می‌کند
Net Time	ما از این دستور برای فهمیدن زمان روی یک سرور استفاده می‌کنیم. اگر به صورت محلی استفاده می‌کنید، بنویسید: Net Time ولی اگر به صورت Remote، می‌خواهید زمان یک کامپیوتر را پیدا کنید، بنویسید: Net time \\xxx.xxx.xxx.xxx که xxx.xxx.xxx.xxx همان آدرس IP است که برای آن Session داریم.

Net Use	این دستور دو کاربرد مهم دارد. اولین کاربرد، Connect یا Disconnect شدن به یک کامپیوتر با پورت ۱۳۹ باز (یعنی Firewall آن پورت را نبسته باشد) و NetBIOS فعال است. مثلاً اگر بخواهیم با حساب Administrator و با پسورد ۱۲۳ به کامپیوتری با آدرس IPی xxx.xxx.xxx.xxx متصل شده و به پوشه Share شده‌ای به اسم IPC$ دسترسی یابیم، (این Share معمولاً هست، به همین دلیل از این Share استفاده کردیم)، می‌نویسیم: Net use \\xxx.xxx.xxx.xxx\IPC$ “123” /User:”Administrator” این کاربرد اول بود که این را قبل از دستور Net view انجام می‌دهیم. می‌توانستیم یک null Session تشکیل دهیم، به این صورت که قسمت مربوط به Username و Password را خالی بگذاریم. به این صورت: Net use \\xxx.xxx.xxx.xxx\IPC$ “” /User: “” حالا Session تشکیل شده است. کاربرد بعدی اینه که بعد از اینکه دستور بالا را اجرا کردیم و بعد دستور Net view را اجرا کردیم و لیست کامل Shareها را بدست آوردیم، بیاییم و یکی از این Shareها را استفاده کنیم. مثلاً اگر اسم Share که لیست شده، SharedDocs باشد، و بخواهیم یک درایو جدید (Map Drive) را به آن نسبت بدهیم که بتوانیم با آن کار کنیم، می‌نویسیم: Net use * \\xxx.xxx.xxx.xxx\SharedDocs معنی کاراکتر * این است که اگر مثلاً آخرین درایو در کامپیوتر من (با احتساب سی-دی درایو) مثلاً G باشد، درایوی که برای اتصال به پوشه Share شده استفاده می‌شود، درایو بعدی یعنی H می‌باشد. می‌توانستیم اینطوری هم بنویسیم: Net use H: \\xxx.xxx.xxx.xxx\SharedDocs خوب حالا می‌توانیم مثل یک درایو محلی با آن پوشه Share شده کار کنیم. وقتی کارمان با Share تموم شد، باید Disconnect کنیم، با این دستور: Net use /delete H:
Net User	این دستور به ما کمک می‌کند که به صورت محلی بدانیم که چه حساب هایی در سیستم تعریف شده است و نیز اینکه اطلاعاتی در مورد هریک بدست آورده و نیز حساب جدید تعریف کنیم. اول می‌خواهیم بدانیم چه حساب هایی تعریف شده، می‌نویسیم: Net User که نتیجه می‌شود: User accounts for \\computer-name Administratorali Reza ASPNET Guest The command completed successfully. خوب حالا مثلاً می‌خواهیم راجع به حساب Reza اطلاعاتی بگیرم، می‌نویسیم: Net User Reza

	و جواب می گیریم: User name Guest User name Reza Full Name Comment User's comment Country code 000 (System Default) Account active 0es Account expires Never Password last set 24/11/2010 06:33:06.â Password expires Never Password changeable 24/11/2010 06:33:06.â Password required No User may change password Yes Workstations allowed All Logon script User profile Home directory Last logon 26/12/2010 07:54:48 Logon hours allowed All Local Group Memberships *Administrators *Debugger Users *HelpLibraryUpdaters *HomeUsers Global Group memberships *None The command completed successfully. می بینید که در سطر ۲ تا مانده به آخر (سطر Local Group Membership) دقیقا بیان شده است که این حساب به چه گروه هایی تعلق دارد. دقت کنید که به جای دستور Net User، از دستور Net Users هم می‌توانید استفاده کنید. حالا می‌خواهیم یک حساب جدید اضافه کنیم. اسم حساب می‌خواهیم Ali بوده و رمز عبور آن 123 باشد، می‌نویسیم: Net User Ali 123 /Add حالا می‌خواهیم همین حساب را پاک کنیم: Net User Ali /delete دقت کنید که در دستور پاک کردن دیگر لزومی به وارد کردن رمز عبور نیست.
Net View	فرض کنید که یک Netbios Session تشکیل داده‌ایم (یعنی به یک کامپیوتر ره دور متصل شده ایم؛ مثلاً توسط تایپ آدرس IP آن در Run) (گاهی Null Session هم جواب می‌دهد) و حالا می‌خواهیم ببینیم که چه منابعی برایمان Share شده است، می‌نویسیم: Net view \\xxx.xxx.xxx.xxx

	و مثلاً جواب می گیریم: Shared resources at \\xxx.xxx.xxx.xxx Share name Type Used asComment SharedDocsDisk The command completed successfully. می بینید که SharedDocs، پوشه‌ای است که Share شده است. حالا با دستور Net use می‌توانیم از Share استفاده کنیم.

۲۱-۷- دستور nslookup

nslookup.exe ابزاری است که به مدیران شبکه امکان تست و رفع اشکال سرویس DNS را می‌دهد. Nslookup یک برنامه از نوع خط فرمان (command-line) است که مخفف Name Server Lookup می‌باشد. به وسیله NSLookup می‌توان از Name Serverهای مختلف اطلاعات مربوط به دامنه‌های مورد نظر را در صورت امکان بدست آورد. اطلاعاتی که درباره دامنه از طریق NSLookup مشاهده می‌کنیم، در واقع همان اطلاعاتی است که در ZoneFile مربوط به دامنه وجود دارد.

آشنایی کامل با امکانات این دستور برای یک مدیر شبکه که با سرویس DNS سروکار دارد خیلی مهم و حیاتی است.

nslookup را می‌توان به دو شکل **Interactive** و **غیر Interactive** استفاده کرد.

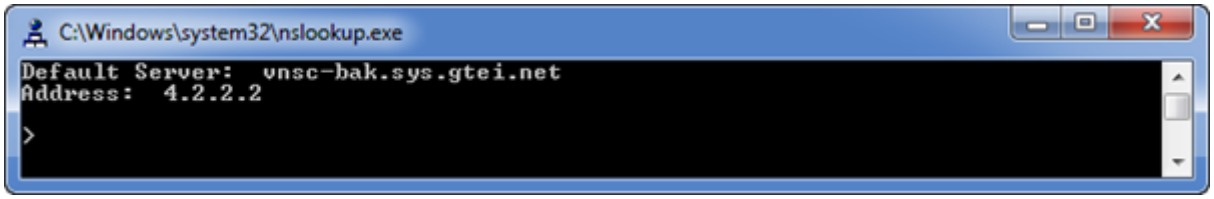
حالت **غیر Interactive** تنها زمانی کاربرد دارد که فقط قصد اجرای یک دستور را دارید و علاقه دارید پس از اتمام آن دوباره به محیط command برگردید.

شکل دستور nslookup در محیط **غیر Interactive** به صورت است:

nslookup [-option] [hostname] [server]

برای استفاده از nslookup به صورت **Interactive** کافی است دستور **nslookup** را وارد کنید.

پس از ورود به محیط دستور nslookup محیطی مانند شکل زیر نمایش داده می‌شود:



دستور nslookup پس اجرا شدن، با توجه با تنظیمات TCP/IP کامپیوتر شما، DNS پیش فرض کامپیوتر را به عنوان سرور انتخاب می‌کند و سعی می‌کند با استفاده از ارسال درخواست Reverse نام سرور را نیز پیدا کرده و به شما نمایش دهد.

اگر موفق به تبدیل IP به نام شود، در قسمت Default Server، نام سرور را نمایش می‌دهد در غیر این صورت Unknown نمایش داده می‌شود، اینکه nslookup موفق با تبدیل IP به نام شود یا نه تاثیری بر دستوراتی که در ادامه وارد می‌کنید ندارد و تنها برای اطلاع شما است.

در قسمت Address هم آدرس IP سرور را نمایش می‌دهد در خط بعد با نمایش علامت > منتظر دریافت دستور می‌شود. حال شما می‌توانید دستورات دلخواه خود را وارد نمایید.

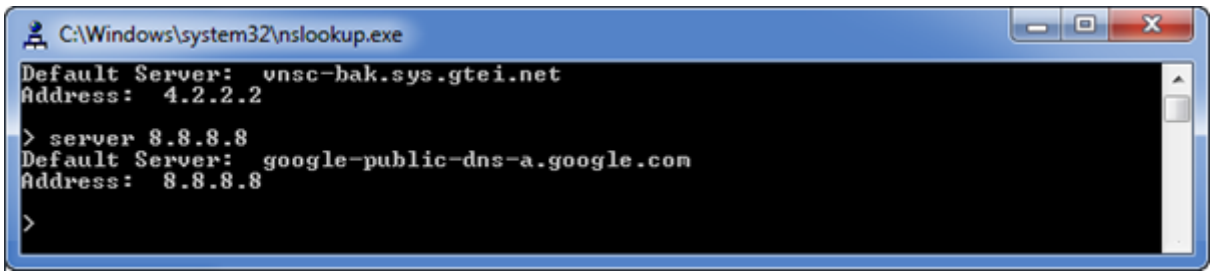
برای مشاهده لیست دستورات و توضیحات آن‌ها می‌توانید از علامت ? یا دستور Help استفاده کنید.

برای خروج از nslookup نیز می‌توانید از کلیدهای Ctrl+C یا دستور Exit استفاده کنید.

اگر قصد تست کردن سرور دیگری غیر سرور مشخص شده در قسمت Address دارید می‌توانید از دستور زیر استفاده کنید. بدین ترتیب دستوراتی که در ادامه وارد می‌کنیم، به این سرور ارجاع داده می‌شود:

server <server ip/name>

مثال: برای اینکه سوالاتی که در آینده از nslookup می‌پرسیم به DNS سروری با آدرس ۸.۸.۸.۸ ارجاع شود باید به این صورت عمل کنید:



برای اینکه نوع رکوردی که می‌خواهید از DNS سرور پرسیده شود را تغییر دهید، باید به کمک دستور Set Type یا Set Querytype این کار را انجام دهید و مقدار Type را به یکی از موارد زیر تغییر دهید:

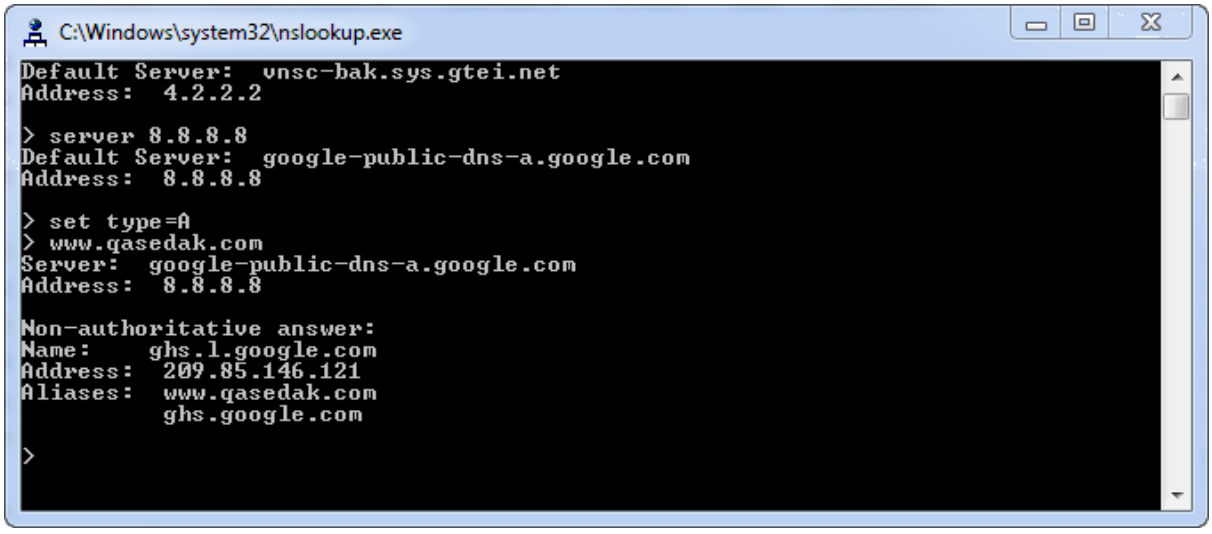
A, CNAME, MX, NS, PTR, SOA, SRV A, AAAA, AA+AAA, ANY

مفهوم این کلمات در فصل DNS Server آمده است.

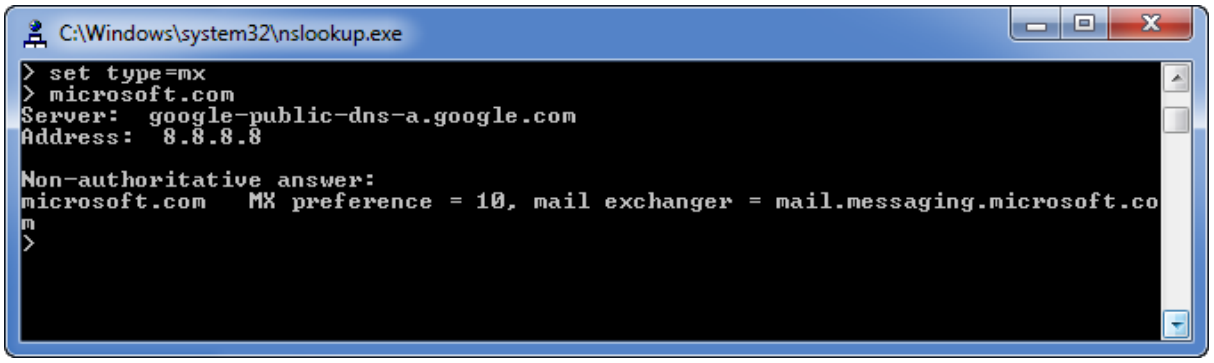
در صورتی که متغیر Type را مشخص نکنید، از حالت پیش فرض یعنی AA+AAA استفاده می‌شود.

پس از مشخص نمودن نوع سئوال می‌توانید درخواست خود را تایپ و کلید Enter را بزنید. بدین ترتیب پرس و جوهای شما به پرس و جوهای خاصی محدود می‌شود. مثلاً فقط IP کامپیوترها یا فقط Mail Serverها.

مثال (۱): برای تبدیل نام www.qasedak.com به IP



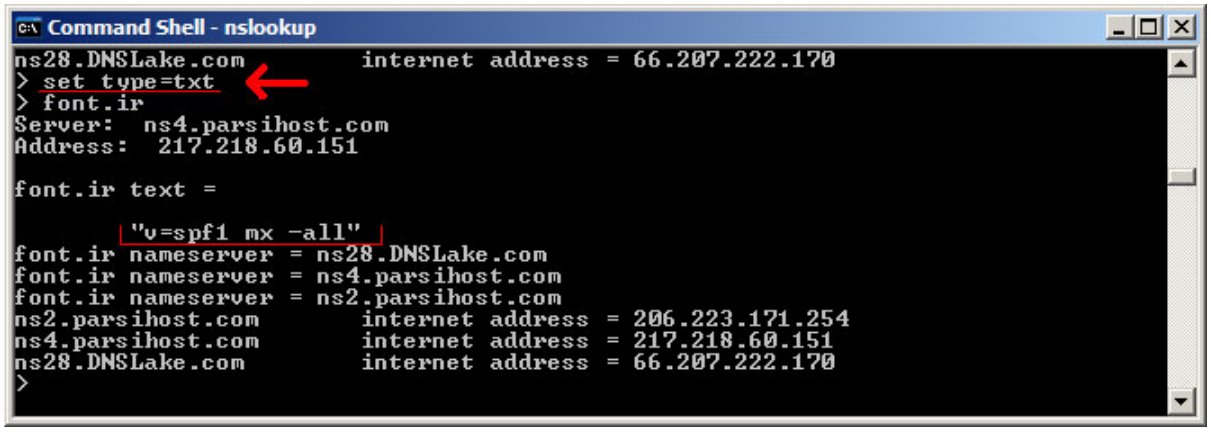
مثال (۲): برای اطلاع از Mail Serverهای موجود در دامنه Microsoft.com



نکته مهم: اگر nslookup در جواب، عبارت Non-authoritative answer را نمایش داد، به این معنی است که سروری که از آن سوال شده، جواب را از Cache خوانده و به سراغ سرور مسئول دامنه نرفته و اگر این عبارت وجود نداشت یعنی اینکه سوال مستقیماً از سرور مسئول دامنه پرسیده شده است. معمولاً اگر در این حالت یک بار دیگر سئوال را تکرار کنید عبارت Non-authoritative نمایش داده می‌شود.

مثال (۳): پرس و جوی رکوردهای TXT

دستور set type=txt را تایپ می‌کنیم و درباره دامنه font.ir پرس و جو می‌کنیم.



همانطور که در شکل می‌بینید، دستور فوق اطلاعات مربوط به رکورد TXT دامنه را نمایش می‌دهد.

دیگر امکانات دستور nslookup

۱) تست ZoneTransfer

برای اینکه عمل ZoneTransfer را توسط nslookup شبیه سازی کنید می‌توانید از دستور ls استفاده کنید. مثال: ls -d <zone name>

۲) Timeout

در صورت کندی اینترنت یا DNS سرور می‌توانید زمان Timeout را بالا ببرید. مقدار پیش فرض ۲ ثانیه است. مثال: set timout=<timeout second>

برای مشاهده تنظیمات فعلی nslookup، از دستور set all استفاده کنید.

۲۱-۸- دستور Whoami

دستور Whoami (Who am I?) نام دامنه، نام رایانه، نام کاربر و نام گروه هایی که کاربر عضو آن می‌باشد را نشان می‌دهد:

whoami [{/user | /groups | /priv} / all]

پارامتر ها:

User: برای نمایش نام کاربر به همراه نام دامنه

Groups: نام گروه هایی که کاربر عضو آن می‌باشد را نشان می‌دهد.

Priv: مجوز هایی که با کاربر داده شده است را نشان می‌دهد. مانند قابلیت تغییر ساعت ویندوز، نصب و حذف برنامه‌ها، تغییرات در تنظیمات شبکه و...

All: تمامی موارد فوق.

۲۱-۹- دستور Getmac

این دستور برای نمایش آدرس فیزیکی کارت شبکه به همراه لیستی از پروتکل‌های شبکه‌ای که به کارت شبکه مربوط می‌شود، استفاده می‌شود. آدرس فیزیکی ۱۲ رقم طول دارد که کاراکترها بر مبنای هگزا دسیمال (مبنای ۱۶) می‌باشد که توسط خط تیزه از هم جدا می‌شوند. مثلاً به آدرس روبرو دقت نمایید: 00-15-18-00-04-F9. آدرس فیزیکی تجهیزات شبکه بوده و تکراری نیست. همچنین این آدرس‌ها قابلیت تغییر نیز ندارند. مثال:

```
C:\> GetMac
Physical Address        Transport Name
=================       ==========================================
08-00-27-0A-90-59       \Device\Tcpip_{F6ED027D-A0B6-49B9-84C5-2736E61146CA}
```

پارامتر ها:

s/: برای مشخص کردن نام رایانه یا آدرس IP

u/: برای مشخص کردن نام کاربر به همراه نام دامنه

p/: برای مشخص کردن کلمه عبور. معمولاً این پارامتر به همراه پارامتر u/ استفاده می‌شود و مورد آن زمانی است که بخواهیم آدرس فیزیکی یک رایانه راه دور را ببینیم. به همین دلیل باید نام کاربری و کلمه عبور رایانه راه دور را داشته باشیم.

۲۱-۱۰- دستور SFC

دستور SFC یا System File Checker نسخه و صحت کلیه پروندههای سیستمی ویندوز را از روی سی دی ویندوز بررسی می‌کند و اگر مغایرتی بین این پروندهها پیدا کند، آن را مجددا از روی سی دی کپی کرده و آن را اصلاح می‌کند. قالب دستور به صورت زیر است:

```
Sfc [/scannow] [/scanboot]
```

پارامتر ها:

scannow/: این دستور تمامی پرونده هایی که توسط ویندوز محافظت می‌شود را بلافاصله اسکن و بررسی می‌نماید.

scanboot/: این دستور تمامی پرونده هایی که توسط ویندوز محافظت می‌شود را هر بار که رایانه راه اندازی می‌شود را اسکن و بررسی می‌نماید.

۲۱-۱۱- دستور SystemInfo

این دستور گزارش کاملی از کلیه تجهیزات سخت‌افزاری و سیستم عامل نشان می‌دهد.

فصل ۲۲

آموزش نصب ویندوز سرور ۲۰۰۳

برای نصب ویندوز ۲۰۰۳ چند مرحله پیش رو داریم:

۲۲-۱- ابتدا باید طرحی برای نصب داشته باشیم.

یعنی باید موارد زیر را در نظر بگیریم.

۱. به چه منظور ویندوز سرور نصب می‌کنیم؟ بر همین اساس نسخه‌ای مناسب از ویندوز سرور تهیه کنیم.
۲. موارد مورد نیاز سیستم را باید چک کنیم.
۳. باید سازگاری نرم‌افزار و سخت‌افزار را چک کنیم.
۴. باید نحوه پارتیشن بندی را چک کنیم.
۵. فایل سیستم مناسب را انتخاب کنیم.
۶. تصمیم گیری در مورد اینکه شبکه ما به صورت Workgroup باشد و یا Domain.
۷. تهیه چک لیست قبل از نصب برای چک کردن موارد بالا.

۲۲-۲- شروع عملیات نصب در مرحله متنی

راه‌های نصب متفاوتی برای نصب ویندوز ۲۰۰۳ وجود دارد؛ ولی مهم نیست که از کدام روش استفاده می‌شود چون تمام روشها تقریباً به یک گونه می‌باشد.

نصب با یک صفحه آبی شروع می‌شود و با انتخاب پارتیشن مربوطه و نحوه فایل سیستم و غیره ادامه پیدا می‌کند؛ که ما از ابتدا با شماره گذاری مراحل ادامه می‌دهیم.

بوت نمودن سیستم از طریق تنظیم صفحه Setup با فشردن کلید DEL یا با نمایش منوی بوت از طریق فشردن کلید F8 انجام می‌گیرد. مراحل زیر را دنبال نمایید.

۱. روشن کردن کامپیوتر در حالی که Boot شدن سیستم از طریق CD-ROM بوده و سی دی ویندوز درون CD-ROM می‌باشد.



۲. در ابتدا اگر خواهان نصب ابزارهای SCSI هستید، باید کلیدF6 را فشار داده و فلاپی را داخل فلاپی درایو قرار دهید تا درایورهای مورد نیاز آن بر روی فلاپی ریخته شود.



۳. و اگر بخواهید ASR (بازگردانی خودکار سیستم) را اجرا کنید کافیست در این مرحله کلید F2 را فشار دهید.



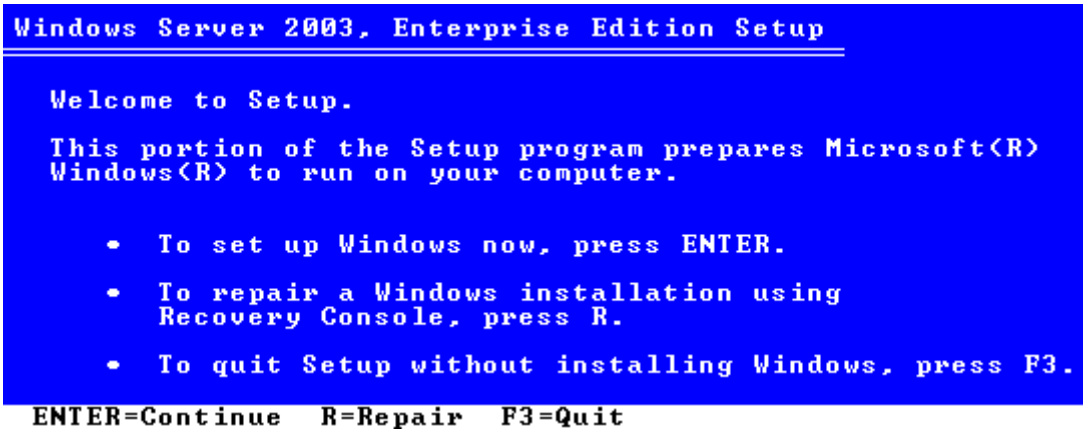
۴. در این مرحله‌ی نصب، تمام فایل‌ها و درایورها، بار گذاری می‌شود.



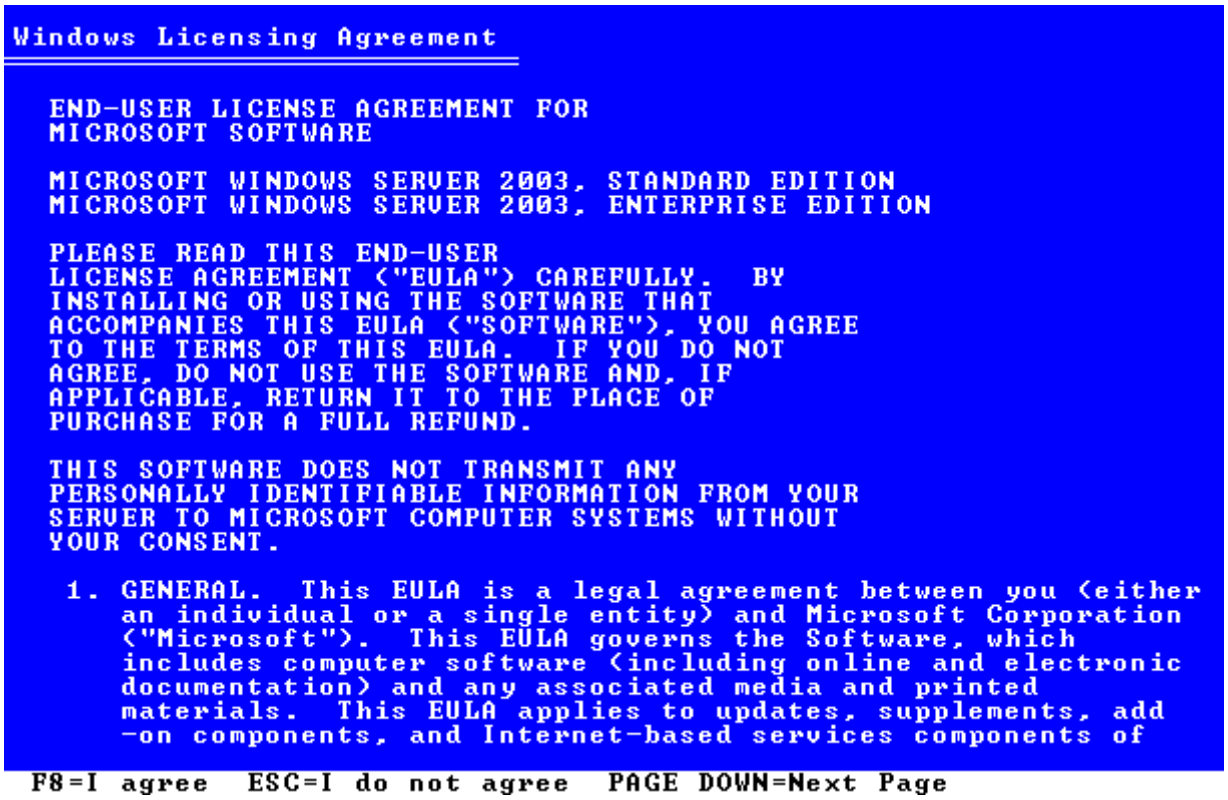
۵. سپس صبر نمایید تا فرآیند نصب و راه اندازی ویندوز شروع شود.



۶. حال به شما اجازه داده می‌شود که اگر از قبل بر روی کامپیوتر خود سیستم عامل دیگری داشته‌اید، آن را با فشردن کلید R تعمیر کنید و اگر می‌خواهید تازه سیستم عامل نصب کنید. کافیست با فشردن کلید ENTER، ادامه دهید.



۷. مرحله بعدی خواندن شرایط نرم‌افزار و فشار دادن کلید F8 برای قبول شرایط است. سعی کنید که تا حد ممکن این توافق نامه را مطالعه فرمایید. فشردن کلید F8 به معنای پذیرش این توافق نامه است.

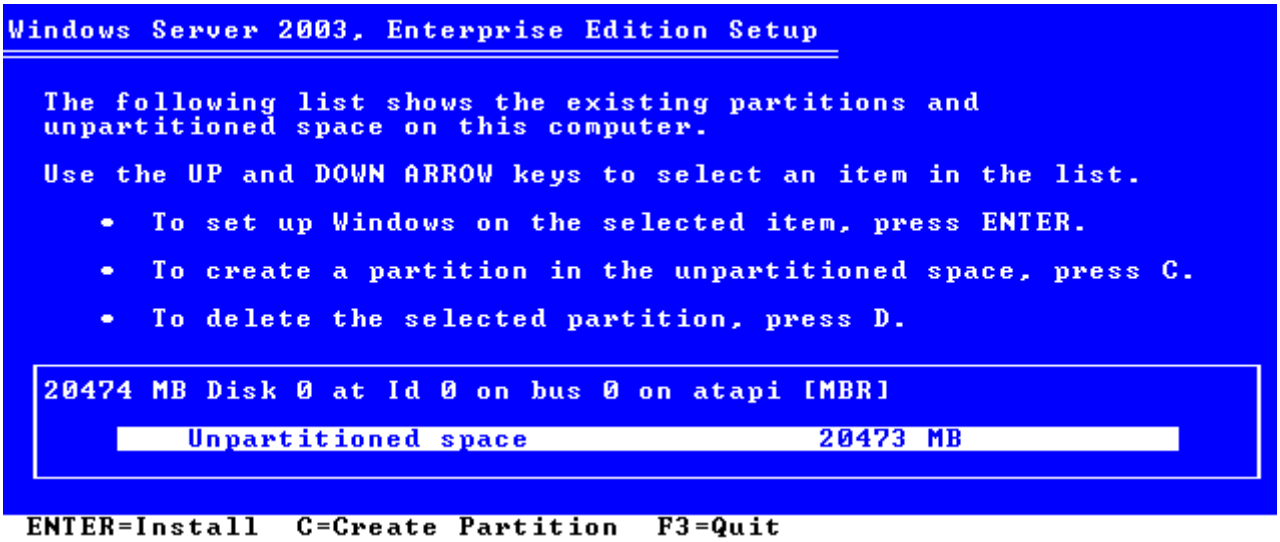


۸. حال نوبت انتخاب پارتیشن مورد نظر برای نصب ویندوز است که نحوه انتخاب آن به شرایط زیر بستگی دارد.

الف) اگر هارد شما به کلی پارتیشن بندی نشده باشد، شما در این حالت بایستی پارتیشن مورد نظر را درست کرده و سپس ویندوز را بر روی آن نصب کنید.

به پارتیشنی که هنوز پارتیشن بندی نشده باشد، UnPartitioned می‌گویند.

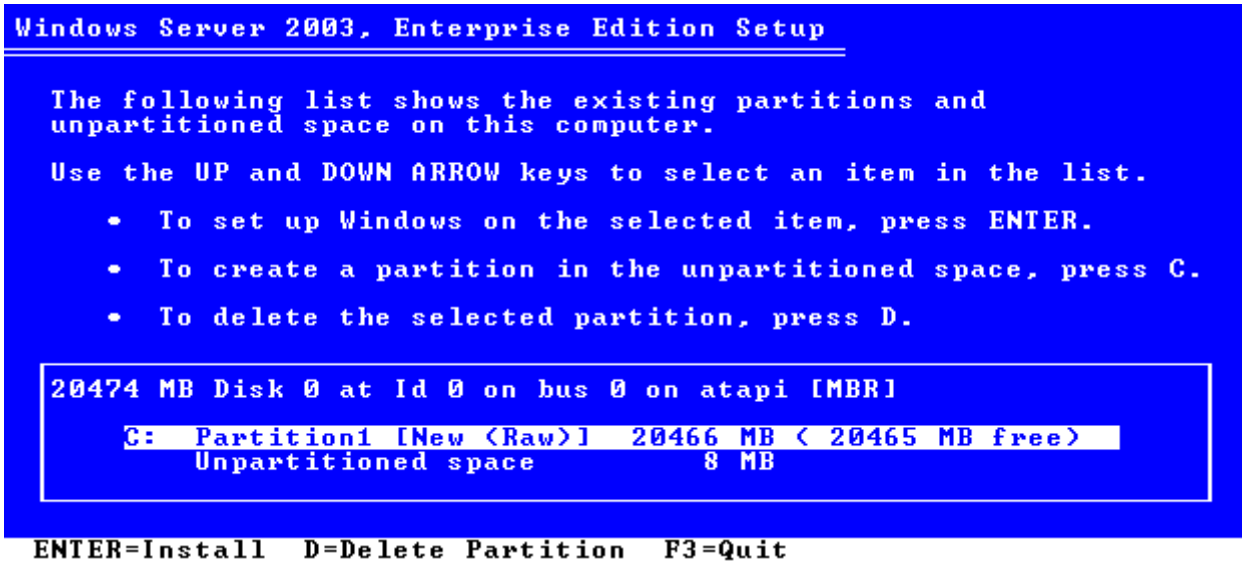
ابتدا پارتیشنی که UnPartitioned است را با فشردن دکمه C انتخاب نمایید. حرف C مخفف Create Partition است.



سپس اندازه جدید پارتیشن را بر حسب MB وارد نموده و کلید Enter را فشار دهید.



پارتیشن جدید با اندازه وارد شده، ساخته شده و می‌توانید آن را مشاهده نمایید.

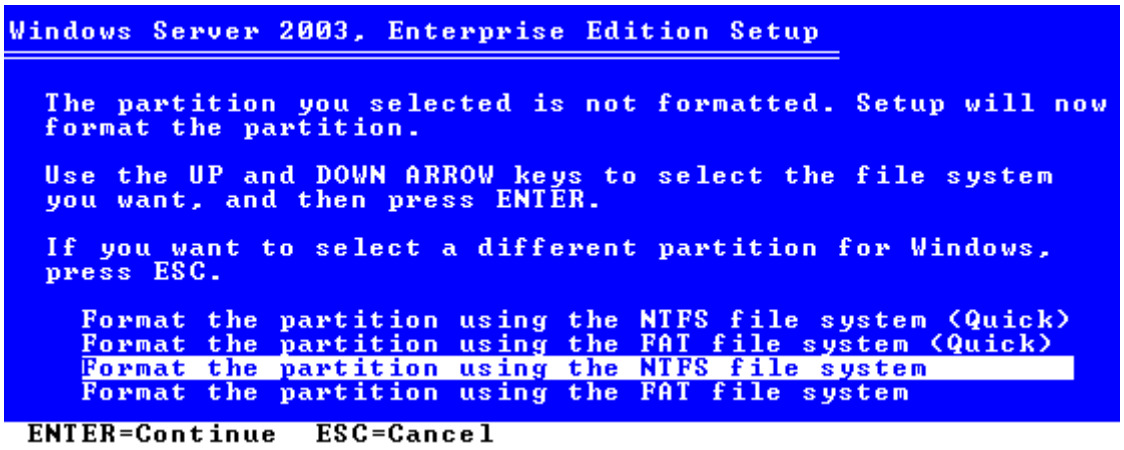


ب) اگر هارد شما از قبل پارتیشن بندی شده باشد و آن پارتیشن بندی مورد قبول شما باشد می‌توانید ویندوز را بر روی پارتیشن مورد نظر نصب کنید. بدین منظور کلید Enter را فشار دهید.

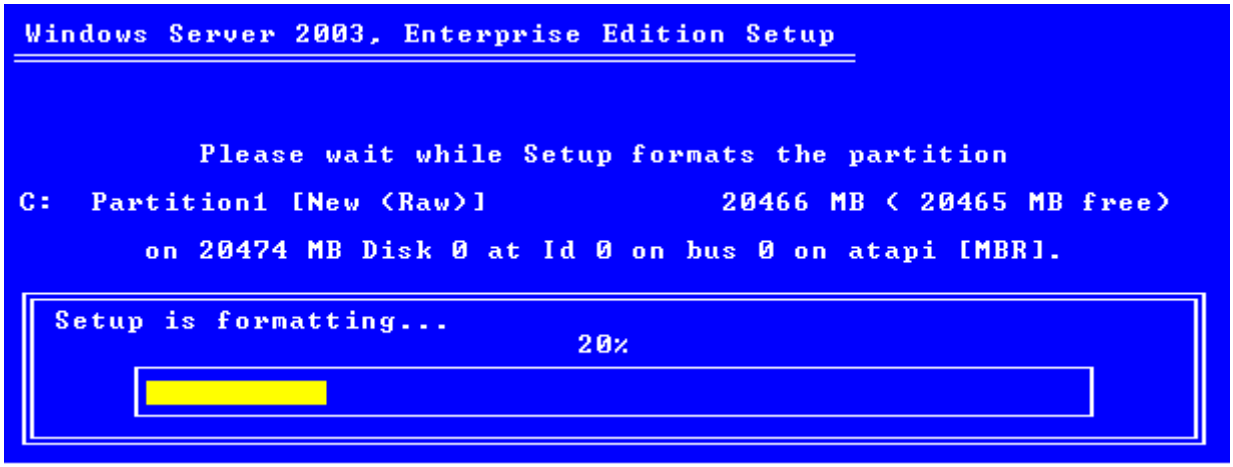
ج) اگر پارتیشن بندی مورد تمایل نباشد، می‌توانید پارتیشن‌ها را پاک کرده و دوباره پارتیشن بندی کنید و سپس ویندوز را بر روی آن پارتیشن نصب کنید. (حذف پارتیشن با دکمه D انجام می‌گیرد)

۹. در این مرحله باید نوع فایل سیستم خود را در هنگام فرمت کردن انتخاب کنیم. ویندوز ۲۰۰۳ با فایل سیستمهای NTFS، FAT32 و FAT کار می‌کند. ولی باید بدانیم اگر می‌خواهیم سیستم عامل دیگری به غیر از ۲۰۰۳ از هارد ما استفاده کند، مثل ویندوز ۹۸ که NTFS را پشتیبانی نمی‌کند باید نوع فایل سیستم خود را FAT یا FAT32 انتخاب کنیم و گرنه NTFS بهترین گزینه می‌باشد. (اکیدا توصیه می‌کنم که از فایل سیستم NTFS استفاده نمایید.)

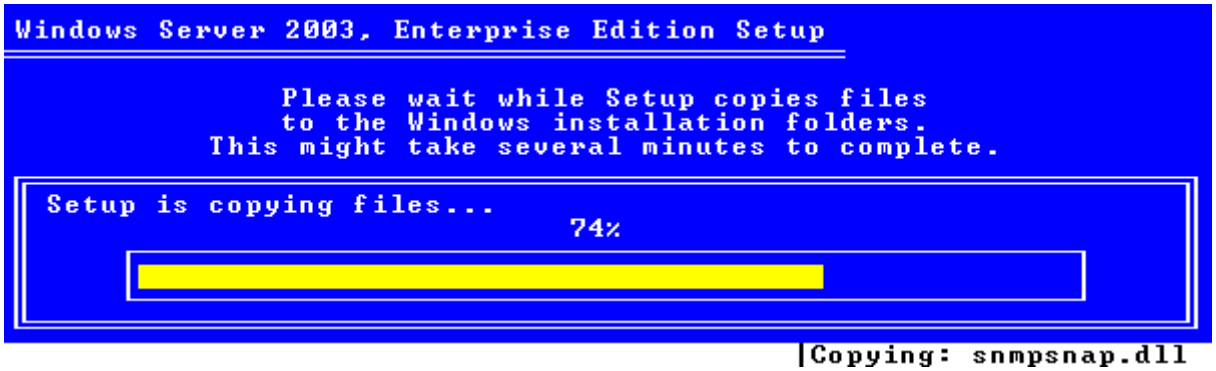
در این مرحله شما حق انتخاب فرمت به صورت سریع و کند را دارید که بر اساس میلتان می‌توانید یک حالت را انتخاب کنید.



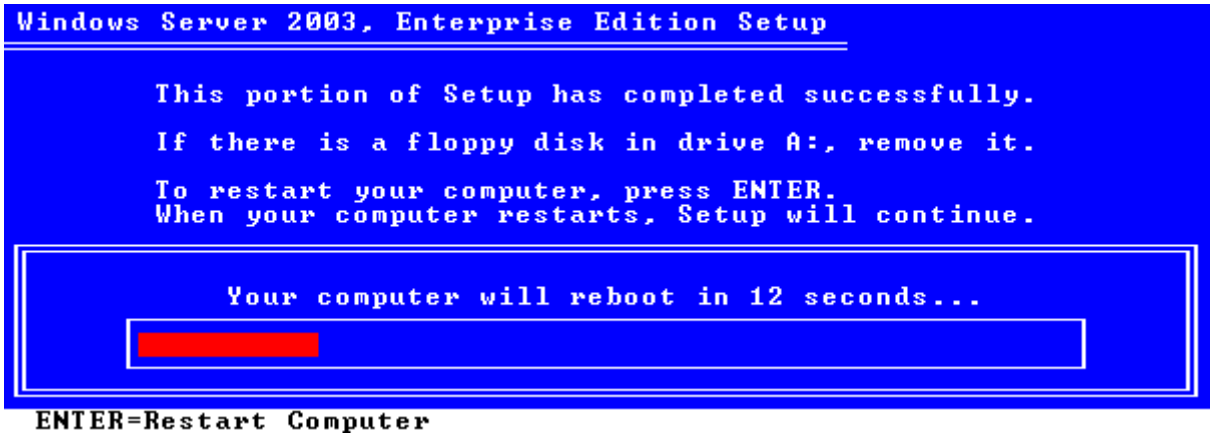
صبر نمایید تا عملیات فرمت کردن پارتیشن انتخابی به پایان برسد.



۱۰. بعد از گذشت از مرحله قبل، حالا نوبت مرحله‌ای می‌رسد که در آن فایل‌ها از روی سی دی ویندوز سرور به داخل هارد دیسک کپی می‌شود.



۱۱. بعد از کپی فایل‌های مورد نیاز که به صورت خودکار انجام می‌گیرد، کامپیوتر Restart شده و نصب ویندوز در مرحله گرافیکی ادامه پیدا می‌کند.



۲۲-۳- مرحله نصب گرافیکی GUI

بعد از Restart شدن کامپیوتر، نصب در حالت گرافیکی ادامه پیدا می کند.

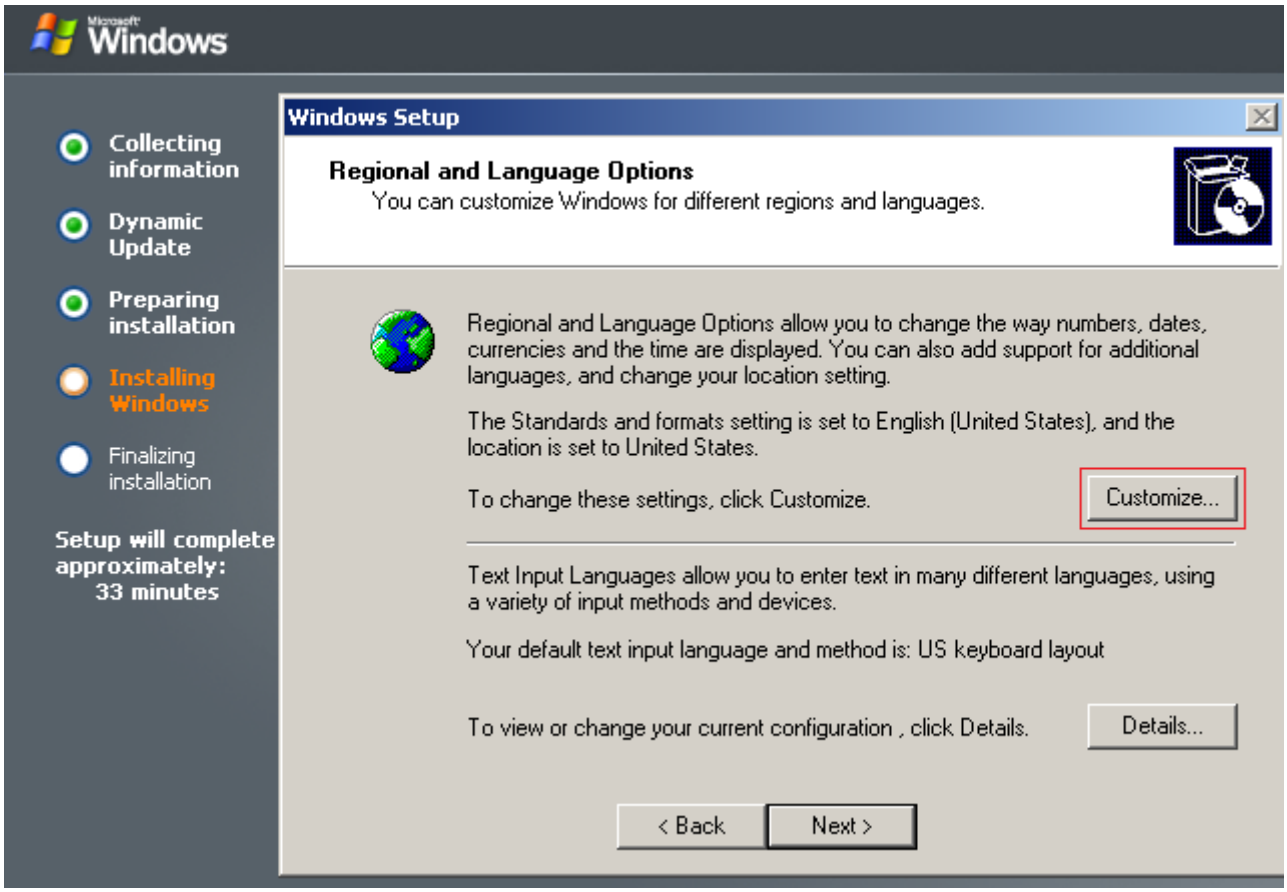




در ابتدا نصب کننده، مشغول بار گذاری درایورها می‌شود. بسته به اینکه چه سخت‌افزاری در کامپیوتر پیدا می‌شود، درایورهای متفاوتی بار گذاری خواهد شد. در این مرحله نیازی نیست که ما کاری را انجام دهیم. صبر نمایید تا عملیات نصب پیش برود.

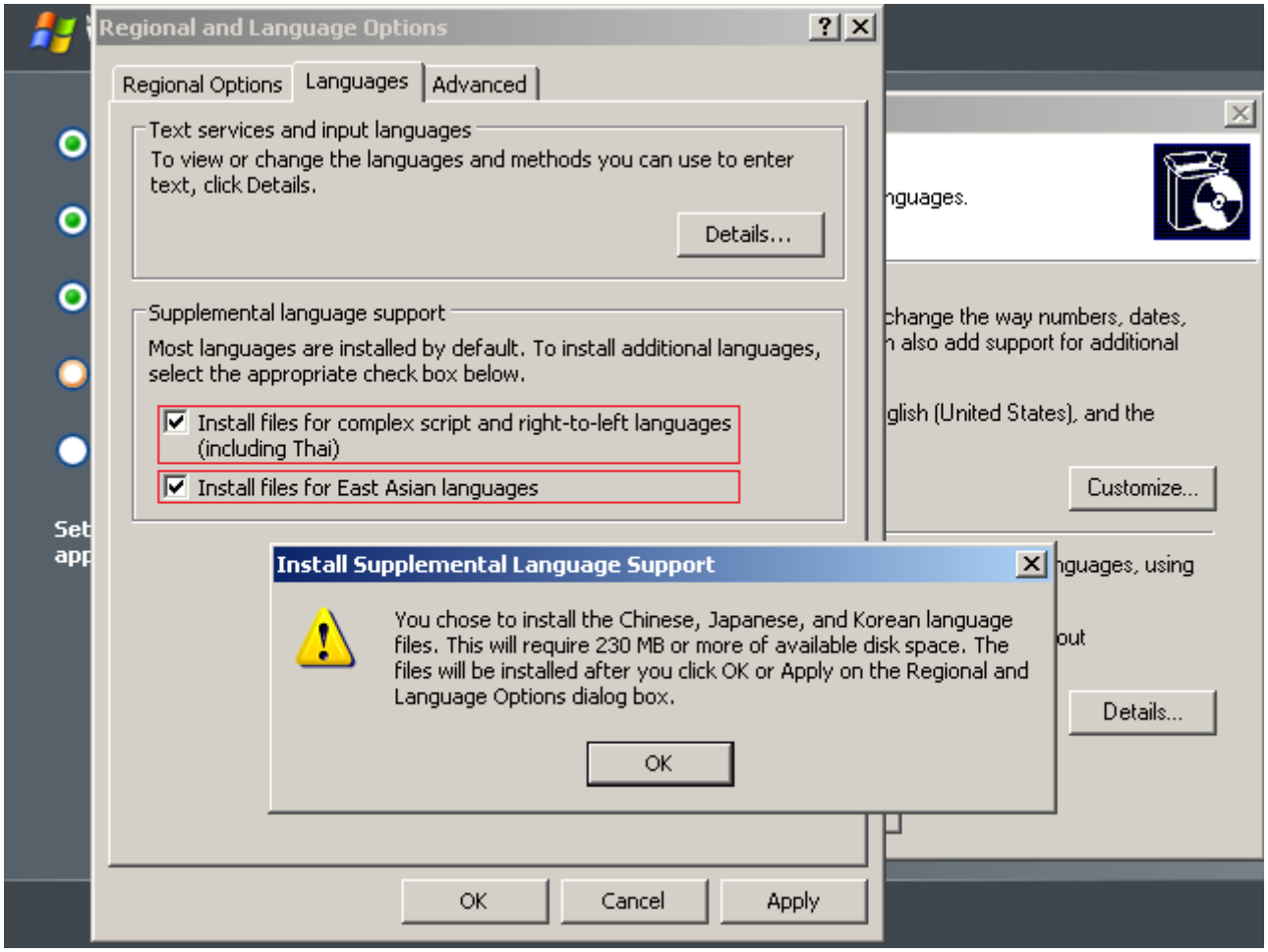


۱. سپس صفحه زیر ظاهر می‌شود که جهت تنظیمات زبان و ناحیه جغرافیایی استفاده می‌شود. در این مرحله می‌توانیم بر اساس موقعیت جغرافیایی خود می‌توانیم تاریخ، زمان، زبان، اعداد و نوع صفحه کلید و چیزهای مربوط به منطقه جغرافیایی را تنظیم نماییم. بدین منظور دکمه Customize را فشار دهید.

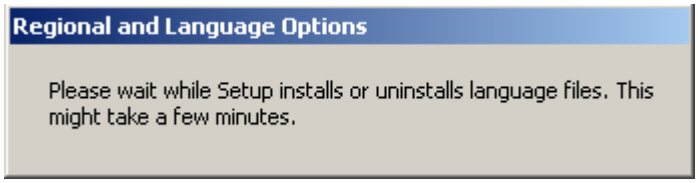


نکته:

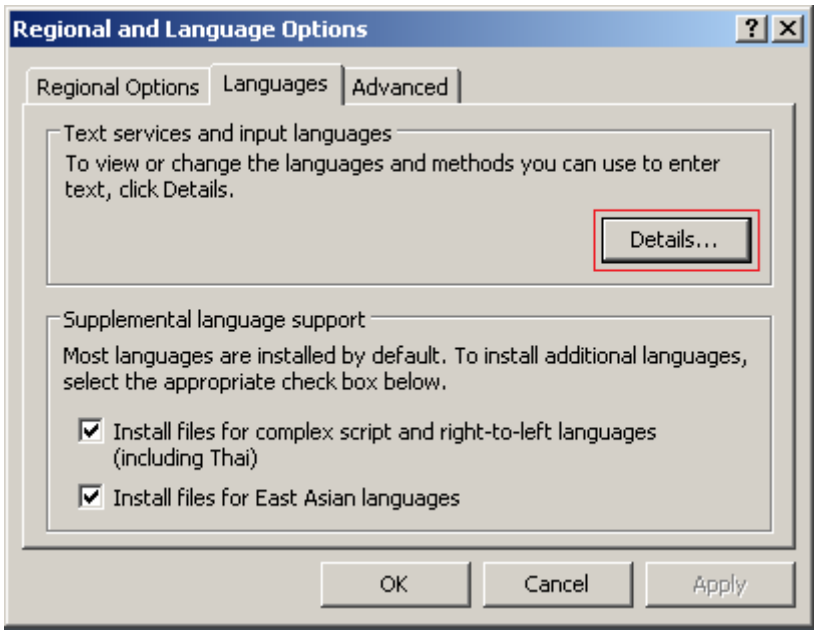
بدین دلیل که ما در منطقه آسیا زندگی می‌کنیم و دارای یک زبان Complex (زبان شامل حروف غیر لاتین) هستیم، باید دو تیک مربوط به انتخاب زبان‌های آسیایی را انتخاب کنیم که با این کار، یک پیغام ظاهر می‌شود. این پیغام نشان می‌دهد که حدود ۲۳۰ مگابایت اطلاعات بر روی هارد دیسک شما کپی خواهد شد. پس از OK کردن پیغام ظاهر شده، روی دکمه Apply کلیک کنید تا زبان‌های آسیایی نصب شوند.



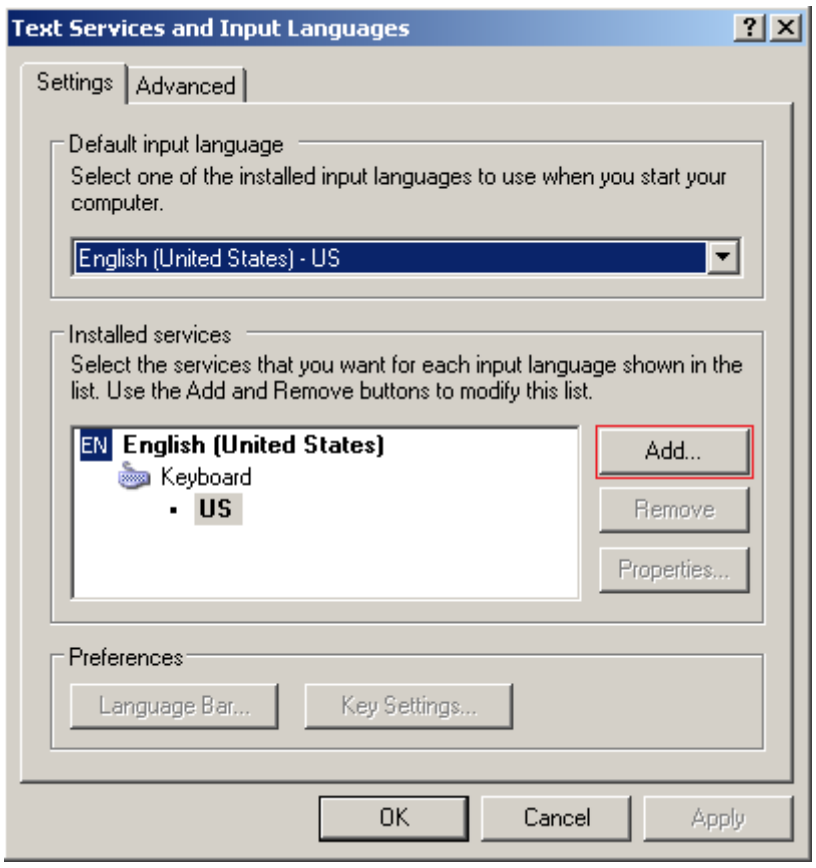
صبر نمایید تا عملیات نصب زبان‌ها به پایان رسد.



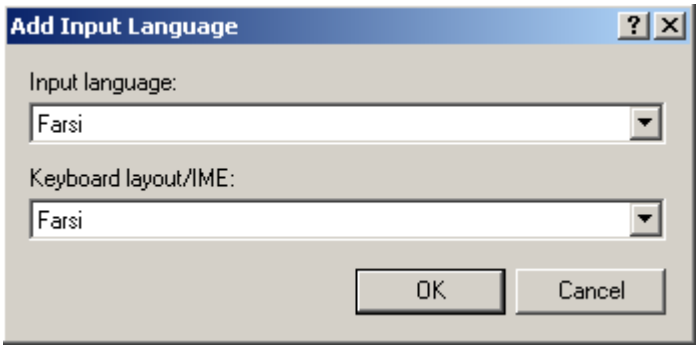
سپس جهت افزودن زبان Farsi به سیستم عامل خود، روی دکمه Details کلیک کنید.



در صفحه باز شده، جهت افزودن زبان Farsi روی دکمه Add کلیک کنید.



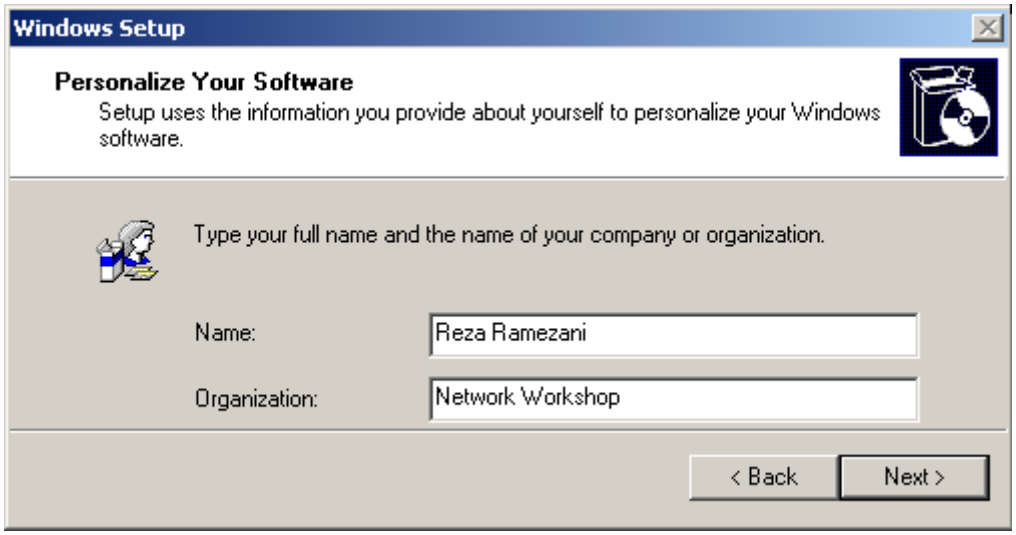
سپس زبان Farsi را انتخاب نموده و روی OK کلیک کنید.



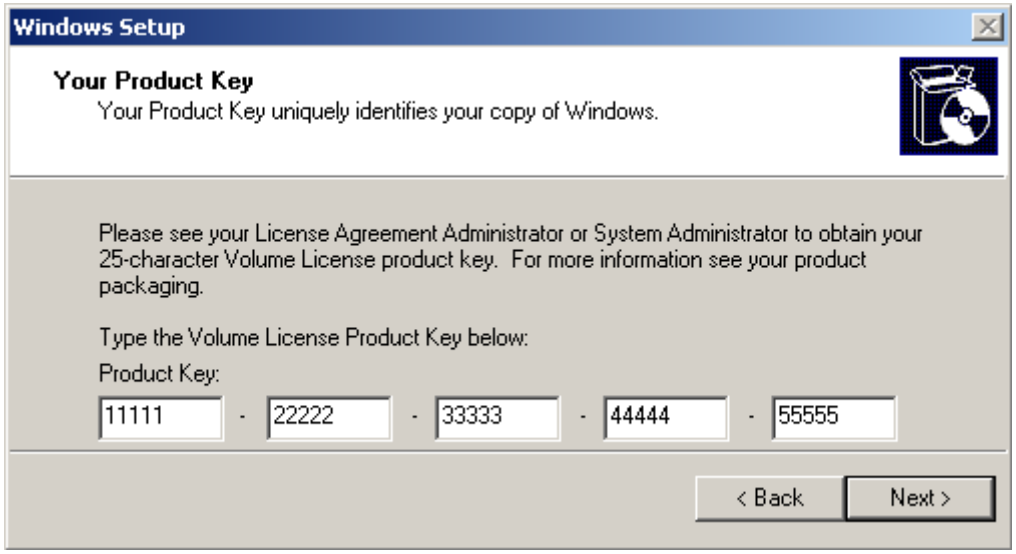
با این کار مشاهده می‌نمایید که زبان Farsi، به لیست زبآن‌های شما اضافه می‌گردد. در نهایت روی دکمه OK کلیک نموده و با کلیک روی دکمه Next به صفحه بعد بروید.



۲. در این مرحله نام خودمان و نام ارگان مربوطه را وارد می‌کنیم.

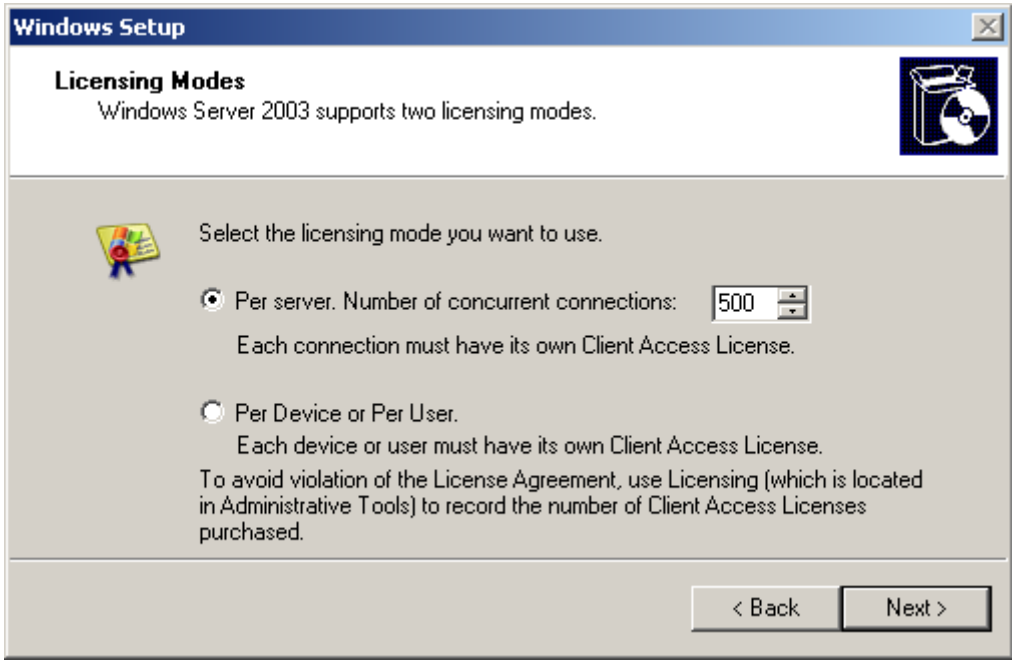


۳. سپس شماره سریال ویندوز را وارد کنید. سعی نمایید که ویندوز سرور را به صورت قانونی خریداری نمایید و از شماره سریال‌های کرک شده استفاده نکنید که کار خیلی زشتیه!!!!



۴. در مرحله بعد، از ما تعداد و نوع مجوز محصول را از ما می‌پرسد. گزینه دوم می‌گوید که به ازاء هر سیستم موجود در شبکه، یک ویندوز سرور خریداری خواهیم کرد. گزینه اول می‌گوید که ما یک مجوز جهت نصب ویندوز سرور روی تعداد زیادی کامپیوتر (مثلا ۵۰۰ کامپیوتر) خریداری نموده‌ایم.

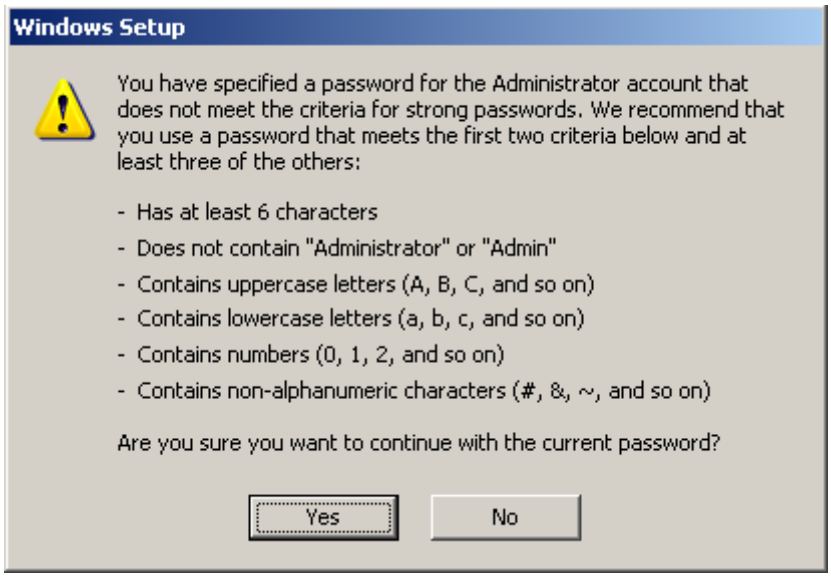
توجه: خرید یک مجوز برای نصب یک ویندوز سرور روی ۵۰۰ کامپیوتر، ارزان‌تر از خرید ۵۰۰ ویندوز سرور برای ۵۰۰ کامپیوتر می‌باشد.



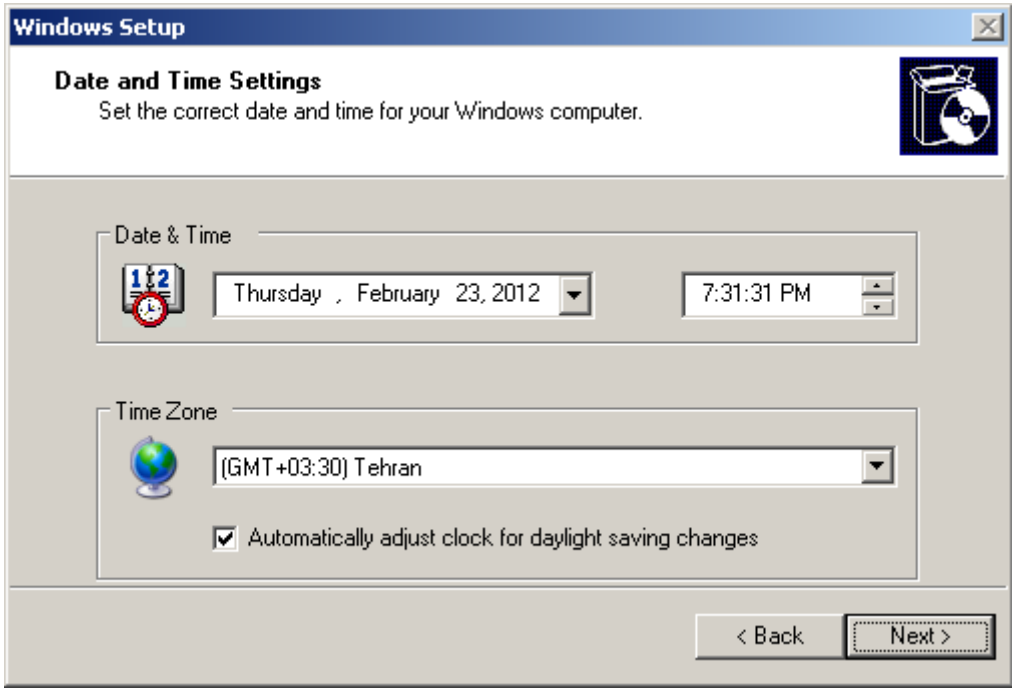
۵. مرحله پنجم، مرحله تعیین نام کامپیوتر و انتخاب رمز عبور برای کاربر Administrator است. کاربر Administrator، به عنوان مدیر سیستم شناخته شده و هیچ محدودیتی در کار با سیستم ندارد.



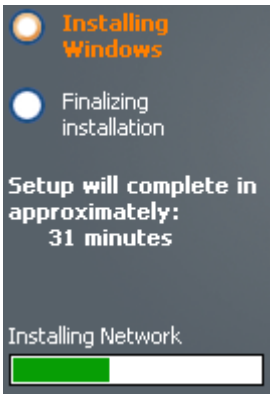
۶. در شکل بالا، من رمز ۱۲۳۴۵۶۷۸۹ وارد نمودم. اگر رمزی که وارد می‌کنیم، رمز پیچیده‌ای نباشد، با کلیک روی دکمه Next، سیستم یک سوال از شما می‌پرسد، مبنی بر اینکه انتخاب رمز عبور ساده برای Administrator، خطرناک است؛ آیا می‌خواهید همین رمز ساده را انتخاب کنید؟ با کلیک روی دکمه Next به صفحه بعد خواهید رفت.



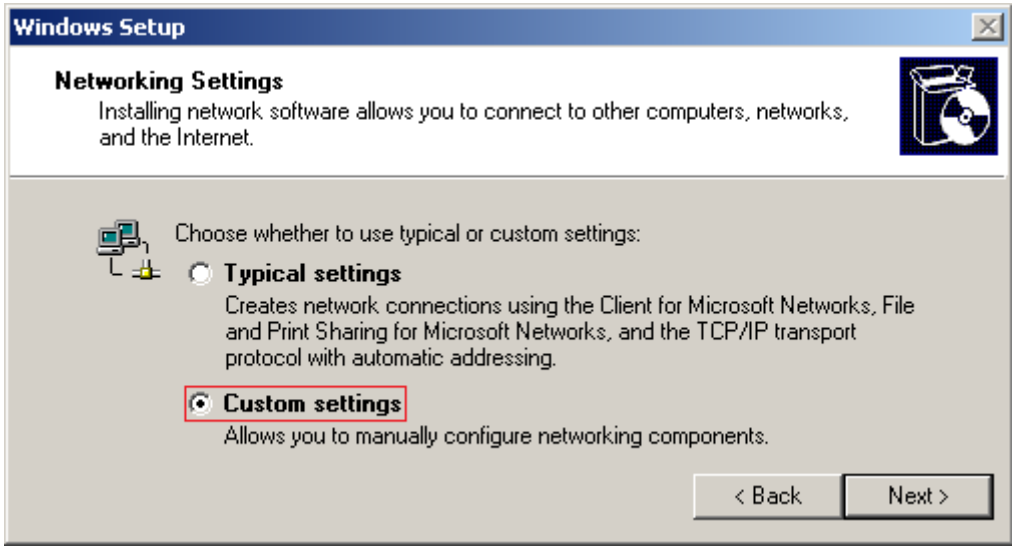
۷. در مرحله بعد پایتخت کشور خود را انتخاب نمایید. این صفحه جهت تنظیمات تاریخ و زمان سیستم می‌باشد.



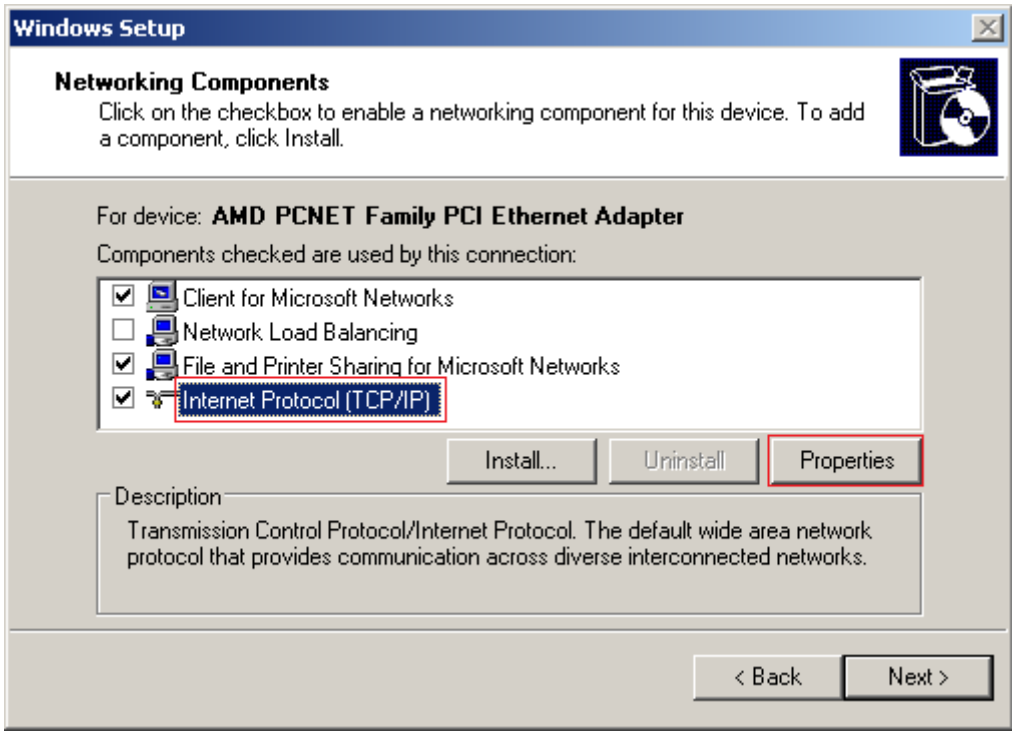
۸. نصب در این مرحله، اجزا شبکه را نصب می‌کند.



۹. اگر کارت شبکه داشته باشید و ویندوز بتواند آن را تشخیص دهد، یک صفحه مربوط به تنظیمات شبکه باز می‌شود. اگر تنظیم خاصی مد نظر شما نیست با انتخاب Typical settings مراحل نصب را ادامه دهید. اما اگر می‌خواهید تنظیمات کارت شبکه را انجام دهید، بعد از انتخاب گزینه Custom settings، روی دکمه Next کلیک کنید.



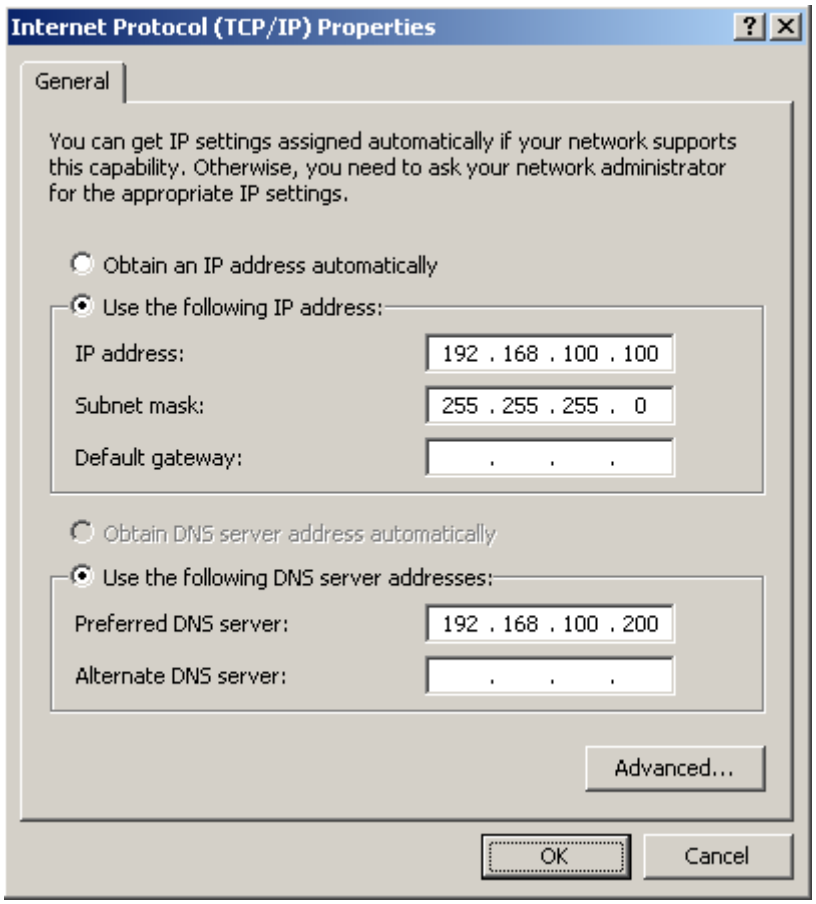
اگر Custom را انتخاب کنید صفحه تنظیمات کارت شبکه باز می‌شود. جهت انجام تنظیماتی چون آدرس IP، Subnet Mask، DHCP و DNS Server، پس از انتخاب گزینه Internet Protocol (TCP/IP)، روی دکمه Properties کلیک کنید.



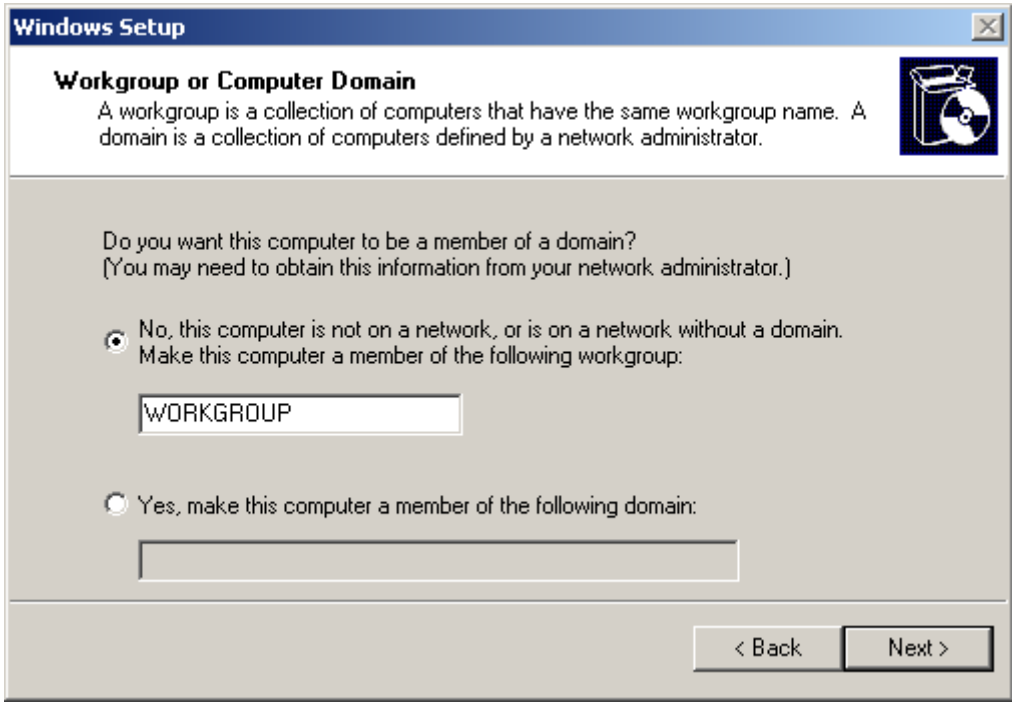
سپس در صفحه باز شده، مقادیر مربوط به IP Address، Subnet Mask، Default Gateway و DNS Server را وارد نمایید.

با این صفحه در فصل ۲ آشنا شده‌ایم.

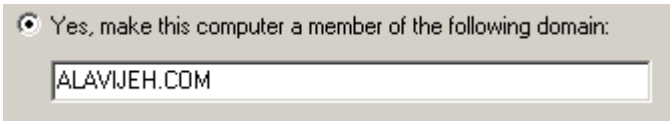
در نهایت، پس از تنظیم آدرس IP، روی OK کلیک نموده و با زدن دکمه Next به صفحه بعد بروید.



۱۰. در مرحله بعد، نوع شبکه بندی خود را انتخاب نمایید. اگر شبکه شما به صورت یک شبکه Workgroup است، گزینه اول را انتخاب نموده و نام شبکه Workgroup را وارد نمایید. شبکه‌های Workgroup، همان شبکه‌های Peer to Peer یا نظیر به نظیر هستند.



اما اگر شبکه شما، نظیر به نظیر نبوده و به صورت Domain می‌باشد، ابتدا گزینه دوم را انتخاب نموده و سپس نام Domain را وارد نمایید. شبکه‌های Domain، همان شبکه‌های Server Based یا مبتنی بر سرور می‌باشند.

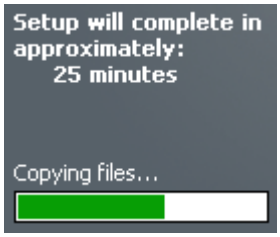


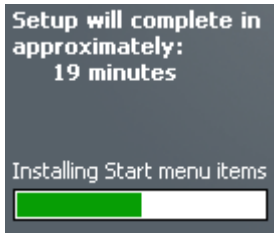
اگر نوع شبکه خود را Domain، انتخاب نمودهاید، هنگام کلیک روی دکمه Next، سیستم از شما یک نام کاربری و یک رمز عبور سوال می‌کند. در این صفحه بایستی نام کاربری و رمز عبوری را وارد نمایید که در سرور تعریف شده است.

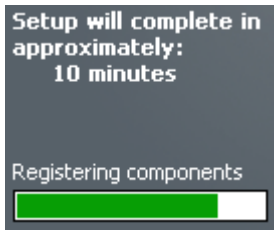
اگر هیچ سروری ندارید، در صفحه قبل، گزینه Workgroup را انتخاب نموده و سپس Next را بزنید.

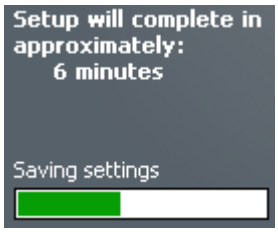


۱۱. دیگر تا کپی کردن فایل‌ها و انجام خودکار تنظیمات مربوطه، در مراحل نصب نیازی به انجام کاری نیست و صبر نمایید تا مراحل نصب به صورت اتوماتیک تمام شود و کامپیوتر دوباره راه اندازی گردد. این تمام کار هایی بود که ما برای نصب ویندوز ۲۰۰۳ نیاز بود انجام دهیم.





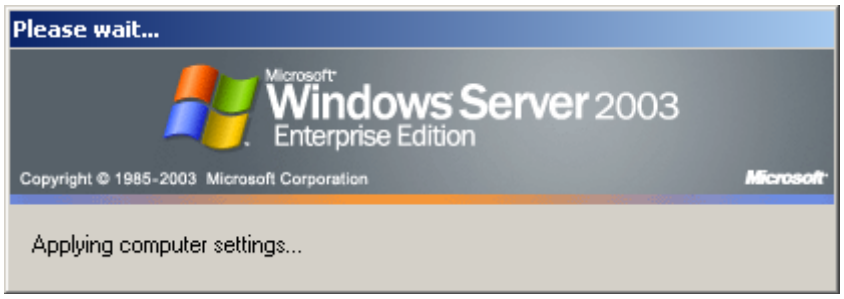




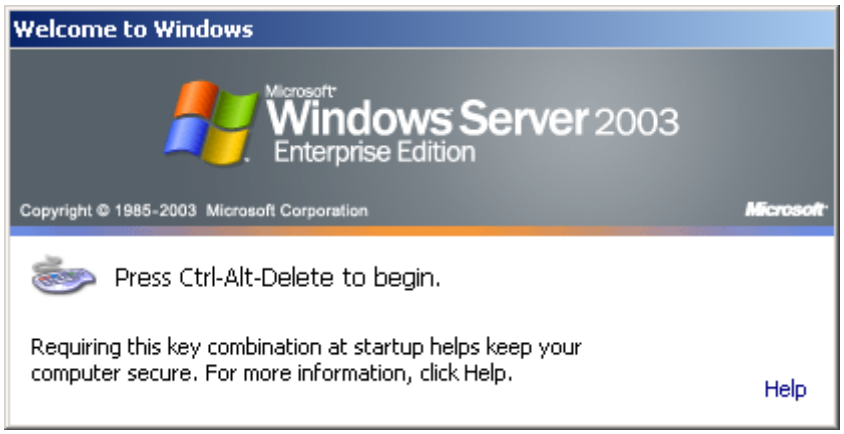
و در نهایت کامپیوتر با سیستم عامل ویندوز ۲۰۰۳ بالا می‌آید.



صبر نمایید تا تنظیمات اولیه اعمال گردد.



سپس صفحه "آمادگی جهت ورود به ویندوز سرور" باز می‌شود. پس از باز شدن این صفحه، کلیدهای CtrlA+lt+Delete را فشار دهید تا صفحه دریافت نام کاربری و رمز عبور نمایان شود.



در صفحه باز شده، نام کاربری و رمز عبور را وارد کرده و با فشردن دکمه OK وارد ویندوز شوید. اگر برای اولین بار است که ویندوز بالا می‌آید، بایستی نام کاربری Administrator و رمز عبور وی که در هنگام نصب ویندوز تعیین نموده‌اید را وارد نمایید. پس از وارد نمودن اطلاعات، روی OK کلیک کنید.



در نهایت اگر برای بار اولی باشد که ویندوز بالا می‌آید، صبر نمایید تا نصب و تنظیمات اولیه برخی نرم‌افزارهای پایه ویندوز سرور ۲۰۰۳ به پایان برسد.



در نهایت ویندوز سرور ۲۰۰۳ بالا می‌آید.

در مورد چگونگی کار با ویندوز سرور ۲۰۰۳، در فصل‌های بعدی صحبت خواهیم کرد.

فصل ۲۳

کاربران، گروه‌ها، واحدهای سازمانی

در این فصل در مورد کاربر (User)، گروه (Group) و واحد سازمانی (Organizational Unit) صحبت خواهد شد.

۲۳-۱- کاربر (User)

احتمالا تا کنون با مفهوم کاربر (User) آشنا شده‌اید. هر کاربر بیانگر یک فرد است که قابلیت کارکردن با سیستم را دارد. به عبارت دیگر، شما می‌توانید به هر فردی یک حساب کاربری (Username و احتمالا Password) تخصیص داده و تعیین کنید که این فرد با این حساب کاربری از کدام سیستم‌ها می‌تواند استفاده کند. البته کاربردهای User بالاتر از این است. مدیران سیستم می‌توانند سطح دسترسی خاصی برای کاربر تعیین کرده و بدین ترتیب محدودیت‌ها یا خط مشی‌ها را بر روی کاربر اعمال نمایند. به عنوان مثال یک نرم‌افزار فروش را در نظر بگیرید که چند کاربر با آن کار می‌کنند، مانند صاحب فروشگاه، مدیر مالی و فروشنده. حال این صحیح نیست که سطوح دسترسی آن‌ها با هم برابر باشد. به عنوان مثال مدیر سیستم حق دارد تعیین کند که چه کسانی از سیستم استفاده کنند (تعیین کاربران)؛ مدیر امور مالی می‌تواند حقوق کارمندان را تعیین کند و این درست نیست که فروشنده قابلیت تغییر حقوق را داشته باشد. همین بحث در مورد User و در سیستم عامل‌ها نیز وجود دارد. User یعنی یک نام کاربری (و احتمالا رمز عبور) و سطوح دسترسی کاربر که توسط مدیران سیستم تعیین می‌گردد. به عبارت دیگر، هر نام کاربری، بیانگر شخصی است که قابلیت انجام کارهایی خاص و از پیش تعیین شده را دارد. در سیستم عامل ویندوز، کاربران زیادی وجود دارد که در یک دید کلی می‌توان آن‌ها را به دو دسته تقسیم کرد:

۱. کاربران پیش فرض (مانند Administrator و Guest)

۲. کاربرانی که بعدا ایجاد می‌شوند.

به هنگام نصب ویندوز، دو کاربر Administrator و Guest به صورت اتوماتیک بر روی ویندوز ایجاد می‌شوند. این ۲ کاربر را نمی‌توانیم پاک کنیم. اما بر حسب نیاز مدیر می‌شود آن‌ها را تغییر نام داد. کاربر Guest به صورت پیش فرض غیر فعال هست و دارای پایین ترین سطح دسترسی می‌باشد.

نکاتی که به هنگام ایجاد یک User Account باید رعایت کنیم:

۱. اسامی آن منحصر به فرد باشد.

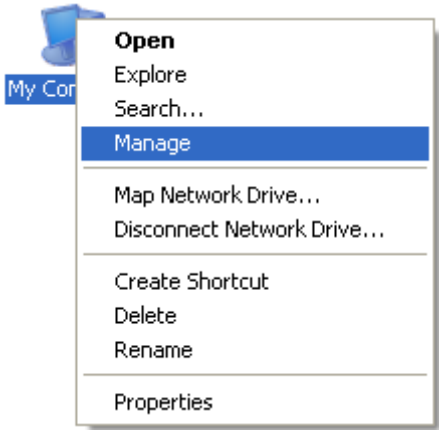
۲. به هنگام ایجاد User، اسم User تا بیش از ۲۰ کاراکتر نمی‌تواند باشد.

۳. برای ایجاد حساب از بعضی کاراکترها نمی‌توان استفاده کرد. / \ { } = + @#$ و....

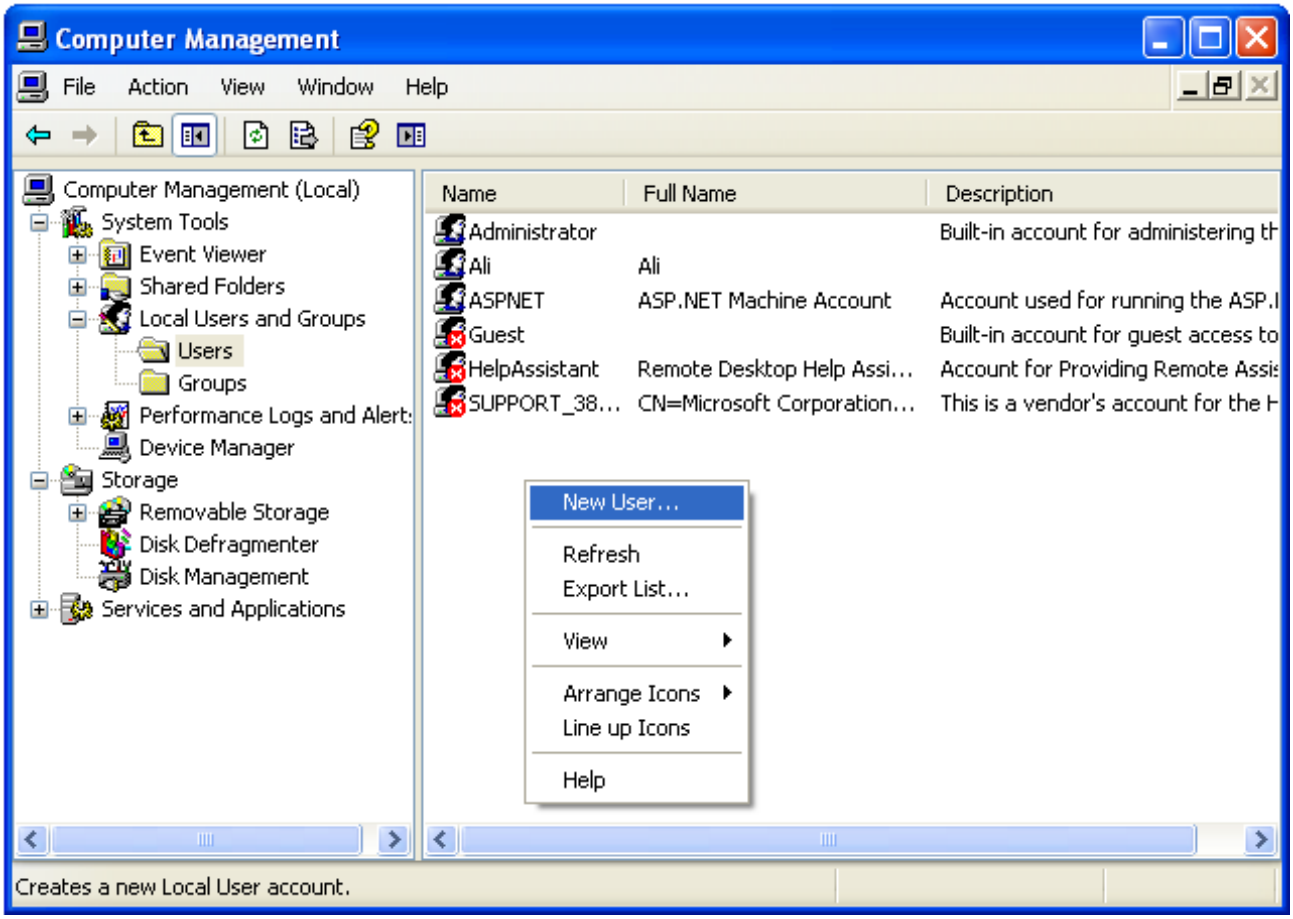
۴. اسامی کاربر با حروف بزرگ یا کوچک فرقی ندارد، اما Password فرق دارد.

۲۳-۲- نحوه ساخت کاربر

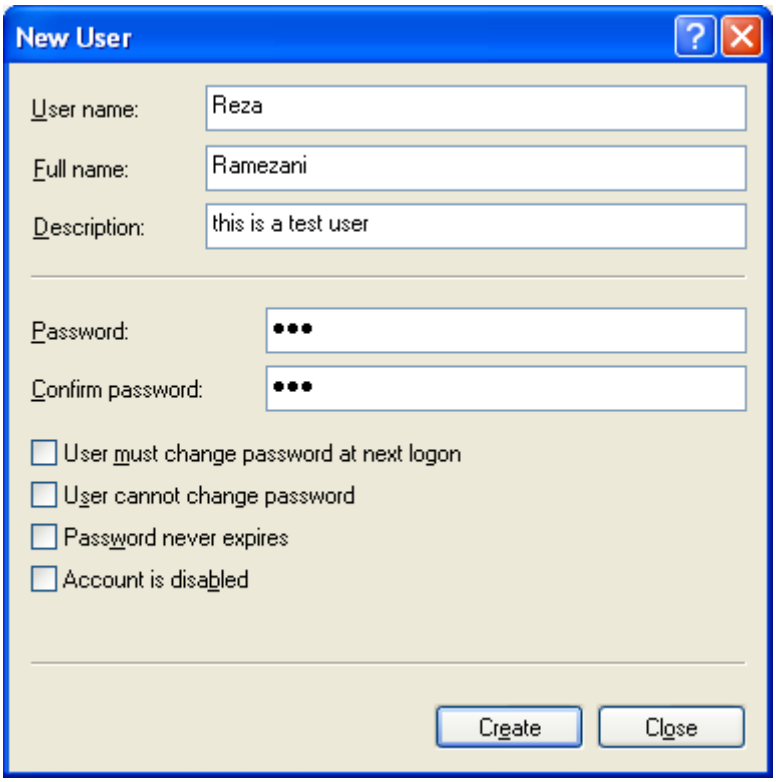
اگر از ویندوز XP استفاده می‌کنید، یا اگر در ویندوز سرور هستید، اما هنوز Active Directory را نصب نکرده‌اید، وارد مسیر زیر شود: ابتدا روی My Computer راست کلیک کرده و سپس گزینه Manage را انتخاب کنید.



سپس در صفحه باز شده، ابتدا وارد Local Users and Groups شده و سپس وارد قسمت Users شوید. در اینجا منظور از کلمه Local این است که کاربران تعریف شده در این قسمت فقط در حالت محلی معتبر اند؛ یعنی افراد فقط زمانی می‌توانند از این نام کاربری استفاده کنند که بخواهند به صورت محلی از همین سیستم استفاده کنند. برای ساخت کاربر در جای خالی صفحه راست کلیک کرده و گزینه New User را انتخاب کنید.



سپس در صفحه باز شده، اطلاعات کاربر، نظیر نام کاربری و رمز عبور را وارد کرده و سپس روی Create کلیک کنید.



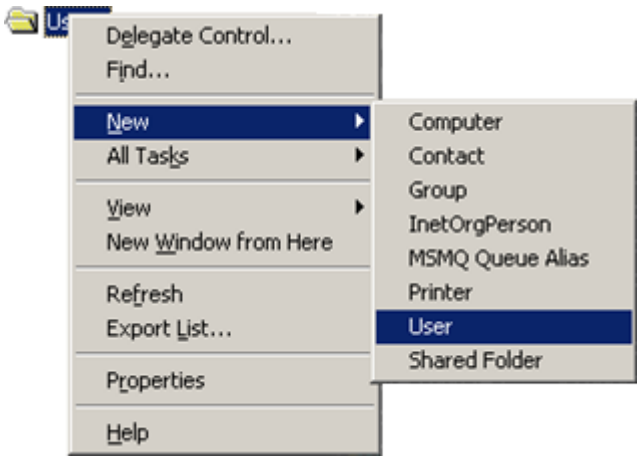
اما اگر از ویندوز سروری استفاده می‌کنید که Active Directory روی آن نصب است (در مورد Active Directory در فصل‌های بعد صحبت خواهیم کرد)، روش و محل تعریف Userها کمی متفاوت است. در این حالت، کاربران تعریف

شده، هم در حالت محلی و هم در شبکه Domain قابل شناسایی است. برای تعریف کاربر، از منوی Start، گزینه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.

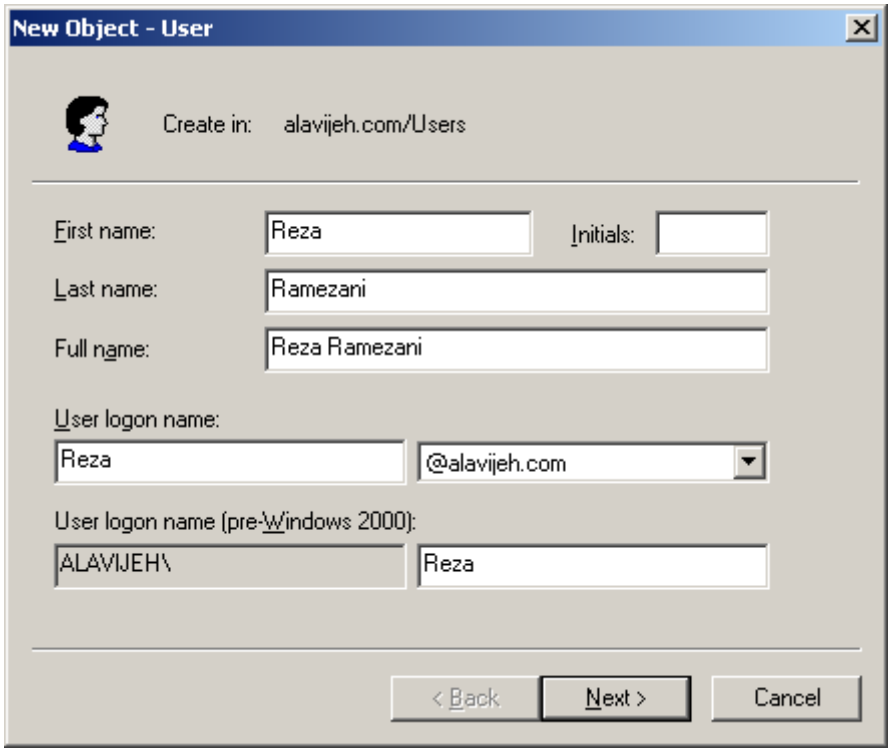


نکته: توجه نمایید که شکل گزینه فوق را تنها در صورتی می‌توانید مشاهده نمایید که Active Directory از قبل نصب شده باشد.

سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می‌دهد، بسط داده، روی قسمت Users راست کلیک کرده و سپس User ➔ New را انتخاب نمایید.



سپس در قسمت بالا، نام و نام خانوادگی کاربر را وارد نمایید. سپس در قسمت User logon name، نام کاربری کاربر که هنگام ورود به سیستم باید وارد کند را در این قسمت وارد نمایید. سپس روی Next کلیک کنید.



سپس در این صفحه، رمز عبور کاربر را وارد نمایید. توجه نمایید که در ابتدا به صورت پیش فرض، در ویندوز سرور، رمز عبور بایستی دارای حداقل ۷ حرف بوده و نیز به صورت Complex (پیچیده) باشد (این تنظیمات در Group Policy تعیین

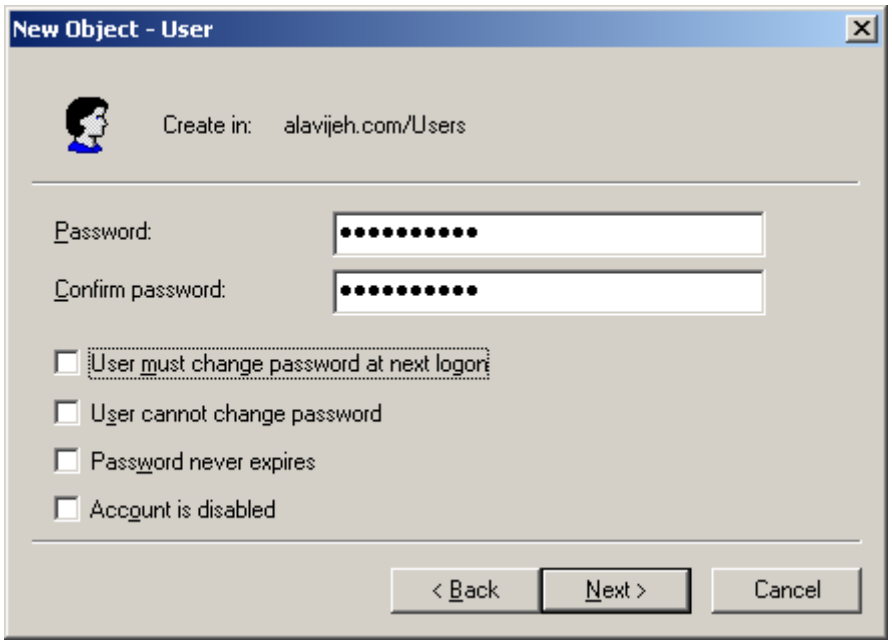
می‌گردد که بعدا در مورد آن صحبت خواهیم کرد). در این مثال ما رمز عبور را abc@abc123 وارد کردیم. در زیر ۴ گزینه وجود دارد که به توضیح مختصر آن می‌پردازیم:

۱. **User must change password at next logon:** با فعال کردن این گزینه، سیستم کاربر را مجبور می‌کند که هنگام **اولین** Login به سیستم، رمز عبور خود را تغییر دهید. **توجه:** اگر بخواهید سیستمی را به Domain خود Join کنید و هنگام Join کردن از این نام کاربری استفاده کنید؛ و همچنین اگر تاکنون با این کاربر Login نکرده‌اید و این گزینه را نیز فعال کرده باشید، سیستم اجازه ورود شما را خواهد گرفت.

۲. **User cannot change password:** با فعال کردن این گزینه، کاربر قادر به تغییر دادن رمز عبور خود نخواهد بود. بهتر است این گزینه را غیر فعال کنید.

۳. **Password never expires:** با فعال کردن این گزینه، رمز عبور کاربر هیچ گاه منقضی (Expire) نخواهد شد. در غیر اینصورت به صورت پیش فرض، پس از ۴۲ روز، کاربر مجبور به تغییر رمز عبور خود است. علت این امر بالا بردن امنیت رمز عبور است.

۴. **Account is disabled:** با فعال کردن این گزینه، کاربر غیرفعال شده و قابلیت ورود به سیستم را از دست خواهد داد.



در مرحله آخر، اطلاعات مختصری در مورد کاربر را مشاهده خواهید نمود. برای ساخت کاربر، روی دکمه Finish کلیک نمایید.

بدین ترتیب کاربر مورد نظر ساخته شده و قابلیت استفاده از آن را با رمز عبور تعیین شده دارید.

۲۳-۳- گروه (Group)

مفهوم گروه در یک عبارت ساده می‌شود "مجموعه‌ای از کاربران". اما بهتر است بدانید که گروه چه کاربردی دارد؟ فرض کنید که یک نرم‌افزار فروش، بیش از ۱۰۰۰ قابلیت مختلف دارد که می‌توان به هر کاربری، قابلیت کارکردن با برخی از این امکانات را داد. حال فرض کنید که ما ۱۰۰ فروشنده داریم و این فروشندهها بایستی با ۴۵۰ تا از امکانات این نرم‌افزار کار

کنند (که مدیر آن را تعیین می‌کند). بدین منظور ما بایستی ۴۵۰۰۰ = ۱۰۰ × ۴۵۰ خصوصیت برای سطح دسترسی تعیین کنیم. حال بهترین ایده این است که ما **یک گروه** تعریف کنیم و این سطوح دسترسی را برای این گروه تعیین نماییم. سپس می‌توان کاربران مورد نظر را تعریف کرده و این کاربران را عضو این گروه کرد. بدین ترتیب، این گروه هر سطح دسترسی که داشته باشد، این سطح دسترسی به کاربران موجود در گروه نیز اعمال خواهد شد. و با انجام این کار، ما فقط ۴۵۰ خصوصیت برای سطح دسترسی تعیین می‌کنیم. البته می‌توان مثلاً ۱۰ گروه تعریف نمود و سطح‌های دسترسی متفاوت برای هر گروه مشخص کرد؛ سپس کاربران را عضو این گروه‌ها نمود. بدین ترتیب کاربر جزء هر گروهی که باشد، سطح دسترسی آن را به ارث می‌برد.

گروه‌ها قابلیت‌های مختلفی دارند، مانند:

۱. می توانند عضو گیری کنند.
۲. می توانند اعضای خود را حذف کنند.
۳. هر گروه می‌تواند عضو گروه دیگری شود.
۴. به برخی از اعضای خود سطح دسترسی خاصی (متفاوت با دیگر اعضای گروه) بدهند.

فقط توجه فرمایید که زمانی که گروهی عضو گروهی دیگر شود، گروه فرزند نمی‌تواند سطح دسترسی بیشتر از سطح دسترسی گروه پدر داشته باشد. فرض کنید که گروه G1 قابلیت استفاده از 5GB فضا داشته باشد و گروه G2 نیز عضوی از گروه G1 داشته باشد. حال برای اعضای گروه G2 نمی‌توان فضایی بیشتر از 5GB در نظر گرفت. همچنین ذکر این نکته نیز مفید است که در یک لحظه، یک کاربر می‌تواند عضو چند گروه باشد.

گروه‌ها نیز مانند کاربران دو دسته‌اند.

۱. گروه‌های پیش فرض (مانند Backup Group و Admins Group)
۲. گروه هایی که بعدا (به منظورهای مختلفی) ایجاد می‌شوند.

البته دسته بندی‌های دیگری نیز برای گروه وجود دارد.

یکی از انواع گروه که می‌توان در ویندوز Server ایجاد کرد، Local Group است که این Local Group به ۲ دسته تقسیم می‌شود:

گروه اول توسط مایکروسافت از قبل پیش بینی و طراحی شده که به عنوان Built in local group ایجاد شده و گروه دوم Built-in system group هست. حالا معرفی این ۲ گروه:

۲۳-۳-۱- *Built-In Local Group*

۱-Administrators:

کاربرانی که عضو این گروه هستند می‌توانند هر گونه عملیاتی بر روی کامپیوتر انجام دهند. زمانی که یک کامپیوتر را عضو Domain می‌کنیم، گروه Domain Admin عضو گروه محلی Administrators می‌شود.

۲- Backup Operators:

اعضای این گروه قادر هستند از تمامی فایل‌های ویندوز هم Backup بگیرند و هم Restore کنند.

۳-Guests:

گروه مهمان هستند که مجوز و سطح دسترسی محدود تری نسبت به سایرین دارند.

۴- Network Configuration Operators:

اعضای این گروه می‌توانند کلیه تنظیمات و فرمآن‌های شبکه را اجرا کنند.

۵-Power Users:

اعضای این گروه توانایی ایجاد کاربر جدید و Share کردن منابع را دارند.

۶- Remote Desktop Users:

اعضای این گروه مجوز دسترسی راه دور به کامپیوتر دیگر را در صورت تعریف شدن عملیات Remote دارند.

۷- Replicator Group:

اعضای این گروه در صورت وجود Domain یا در محیط یک شبکه می‌توانند عملیات Replication و مدیریت فایل‌ها را انجام دهند.

۸- Users Group:

این گروه می‌توانند با مجوز تعیین شده به منابع دسترسی پیدا کنند. به صورت Default همه Userها عضو این گروه هستند.

۹- Debugger Users:

اعضای این گروه می‌توانند هم به صورت Remote هم به صورت Local بر روی کامپیوتر مورد نظر اشکال یابی کنند.

۱۰- Help Service Group:

اعضای این گروه می‌توانند از کلیه امکانات Help و فرمآن‌های موجود در داخل ان استفاده نمایند. البته این گروه خیلی کشکیه....

۲۳-۳-۲- *Built-In System Group*

این گروه به صورت Default وجود داشته و نمی‌توانیم آن‌ها را حذف یا اضافه کنیم. عضویت در این گروه‌ها را هیچ کس حتی Admin هم نمی‌تواند مشخص کنه و بسته به حالت‌های مختلف که هر بار کاربر Login می‌کند، می‌تواند عضو یکی از این گروه‌ها باشد.

انواع گروه Built-In System Group

۱- Every One:

تمامی کاربرانی که به کامپیوتر دسترسی پیدا می‌کنند، عضو این گروه هستند. ضمن اینکه اگه مجوزی به این گروه بدهیم، شامل همه کاربران اعم از Admin و غیر آن می‌شود.

۲- Authenticated Users:

کاربرانی که با User name و Password وارد شبکه می‌شوند جز این گروه هستند.

۳- Anonymous Log On:

کاربرانی که بدون User name و Password وارد شبکه می‌شوند جز این گروه هستند.

۴- Creator Owner:

زمانیکه هر شیئ ایجاد کنیم، عضو این گروه قرار میگیریم.

۵- Dial up:

هر کاربری که از طریق Dial up وارد شبکه شود عضو این گروه است. (برای اطلاعات بیشتر به فصل "برقراری ارتباط از راه دور" مراجعه فرمایید.)

۶- Interactive Group:

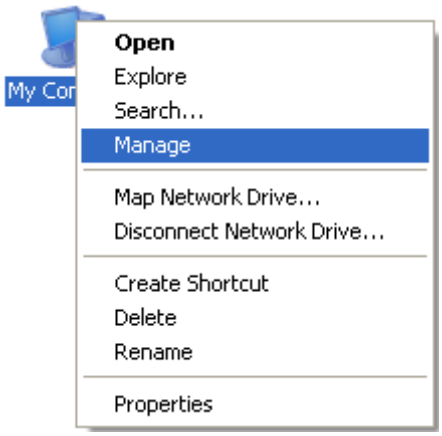
هر User که به صورت Local به کامپیوتر دسترسی پیدا کند عضو این گروه هست.

۷- Network Group:

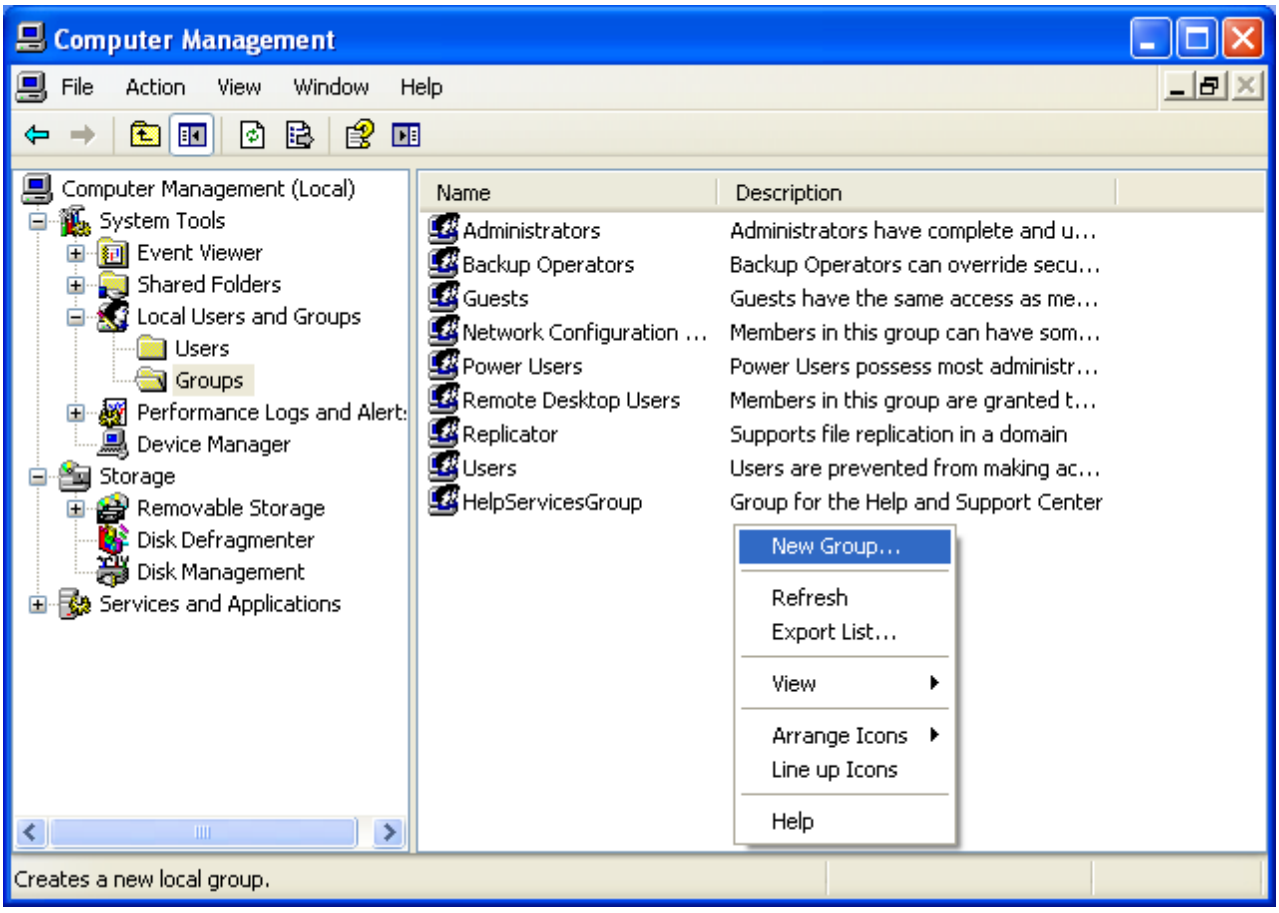
هر User که به صورت شبکه به کامپیوتر یا از طریق کامپیوتر به شبکه وصل شود عضو این گروه قرار میگیرد.

۲۳-۴- نحوه ساخت گروه

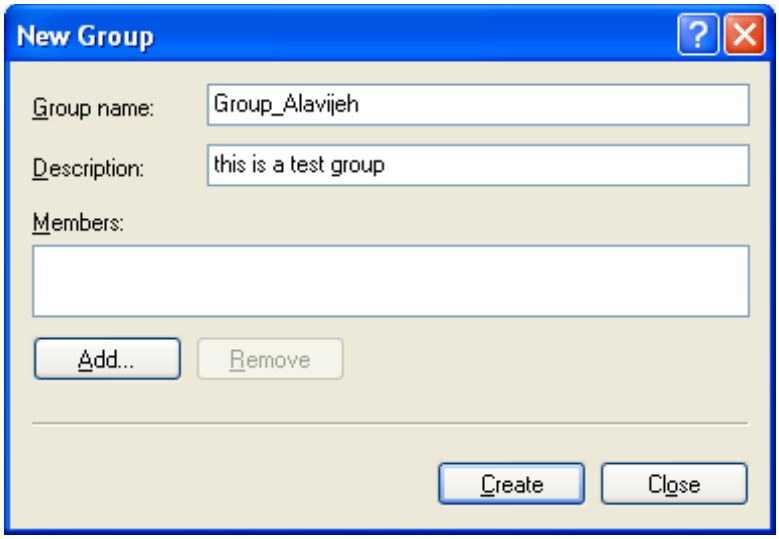
همانند بخش ساخت کاربر، اگر از ویندوز XP استفاده می‌کنید، یا اگر در ویندوز سرور هستید، اما هنوز Active Directory را نصب نکرده‌اید، وارد مسیر زیر شود: ابتدا روی My Computer راست کلیک کرده و سپس گزینه Manage را انتخاب کنید.



در صفحه باز شده، وارد Local Users and Groups شده و سپس وارد قسمت Groups شوید. برای ساخت گروه جدید، در جای خالی صفحه راست کلیک کرده و گزینه New Group را انتخاب کنید.



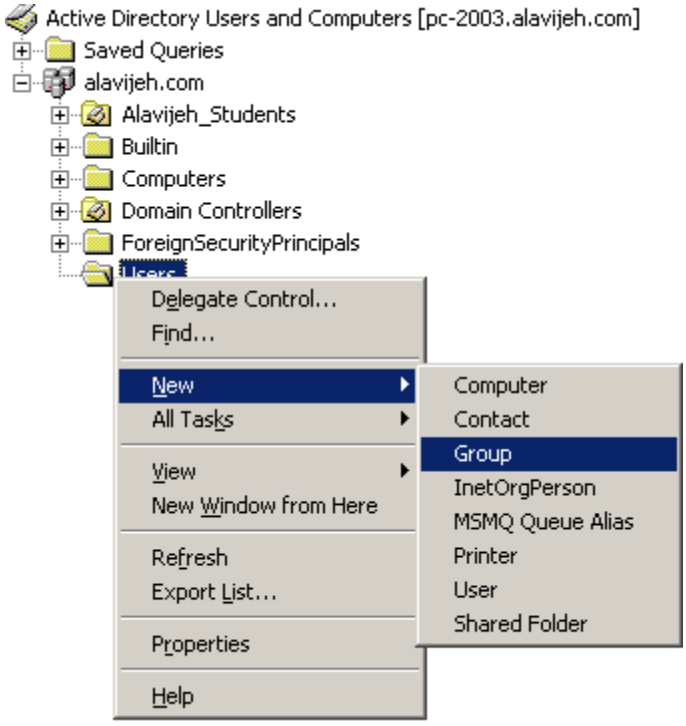
سپس در صفحه باز شده، یک نام و یک توصیف برای گروه خود وارد نمایید. در پایین صفحه این قابلیت وجود دارد که کاربران یا گروه هایی را عضو این گروه کنید. نحوه عضو گیری را جلوتر توضیح می‌دهیم.



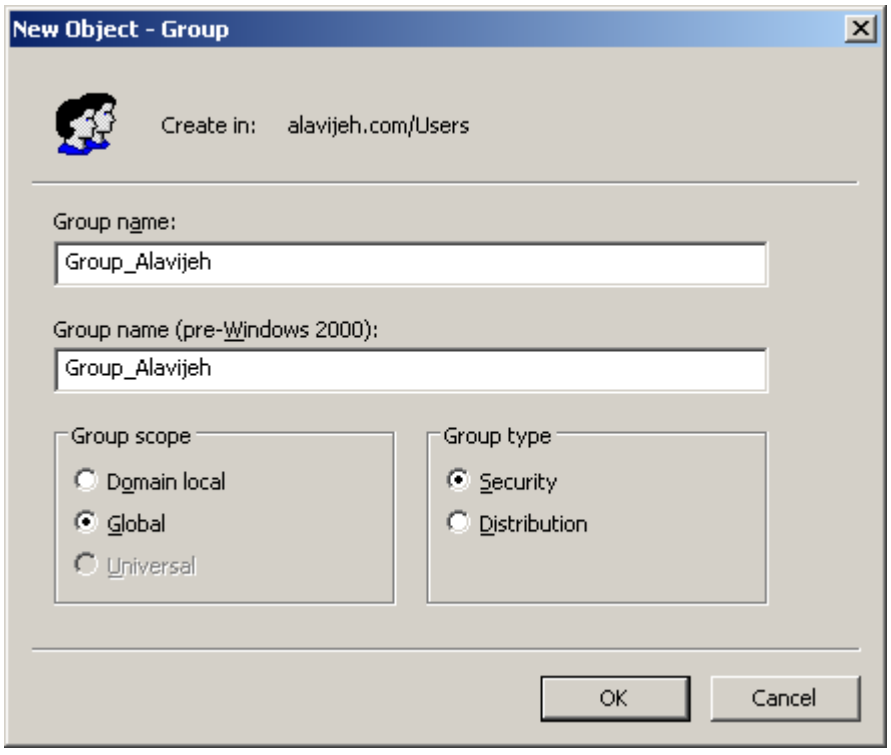
اما اگر از ویندوز سروری استفاده می‌کنید که Active Directory روی آن نصب است، روش و محل تعریف Groupها کمی متفاوت است. برای تعریف گروه جدید، از منوی Start، گزینه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.



سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می‌دهد، بسط داده، روی قسمت Users راست کلیک کرده و سپس Group ➔ New را انتخاب نمایید.



سپس در صفحه باز شده، نام گروه، توصیف گروه، حوزه کاری گروه و نوع گروه را تعیین نمایید.



حال به توضیح مختصری در مورد حوزه و نوع گروه می‌پردازیم.

الف) Group Types: بیانگر نوع گروه بوده و گروه‌ها از این نظر به دو نوع تقسیم می‌شوند:

۱- Security Groups: گروه‌های هستند که از آن‌ها بیشتر برای مجوز دادن استفاده می‌شود. همچنین از این نوع گروه می‌توان برای ایجاد لیست توزیع E-Mail استفاده نمود.

۲- **Distribution Groups:** توانایی ایجاد لیست توزیع Email را دارد و از آن نمی‌توان جهت اعطای مجوزهای دسترسی به منابع استفاده کرد. از اینرو زمانی از این نوع گروه‌ها استفاده کنید که اعضای آن نیاز به مجوز دسترسی به منابع را نداشته و فقط جهت لیست توزیع E-Mail از آن‌ها استفاده می‌شود.

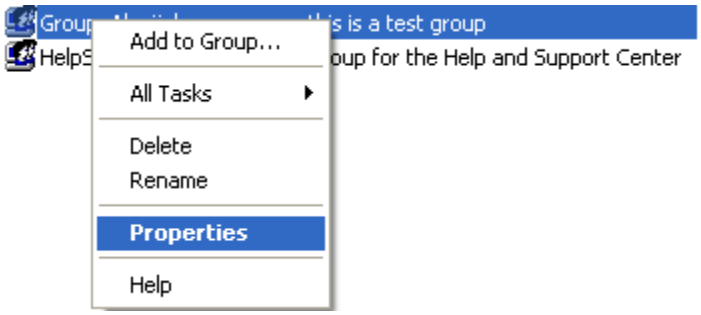
ب) Group Scopes: حوزه و محدوده کاری گروه را مشخص می‌کند.

۱- **Global Groups:** گروه هایی هستند که به منظور دسته بندی منطقی کاربران مورد استفاده قرار می‌گیرند که معمولاً بر اساس نوع کار یا محل جغرافیایی کاربران می‌باشد. به عنوان مثال می‌توانید کاربرانی که در واحد فروش کار می‌کنند را در یک گروه و کاربرانی که در واحد خرید کار می‌کنند را در گروهی دیگر گروه بندی نمایید.

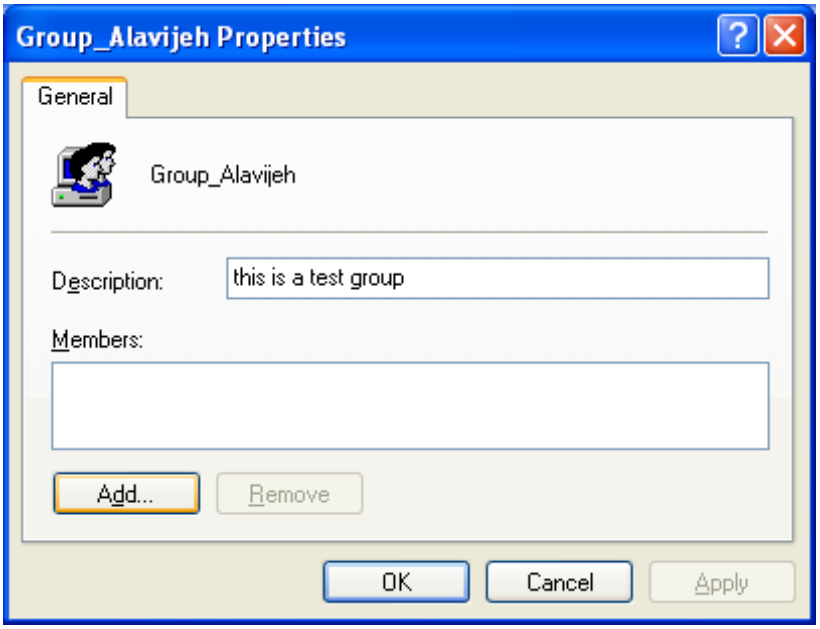
۲- **Domain Local Groups:** معمولاً برای اعطای مجوز استفاده می‌شود.

۳- **Universal Groups:** برای مجوز دادن به کاربران در شبکه هایی که بیش از یک Domain دارند، استفاده می‌شود.

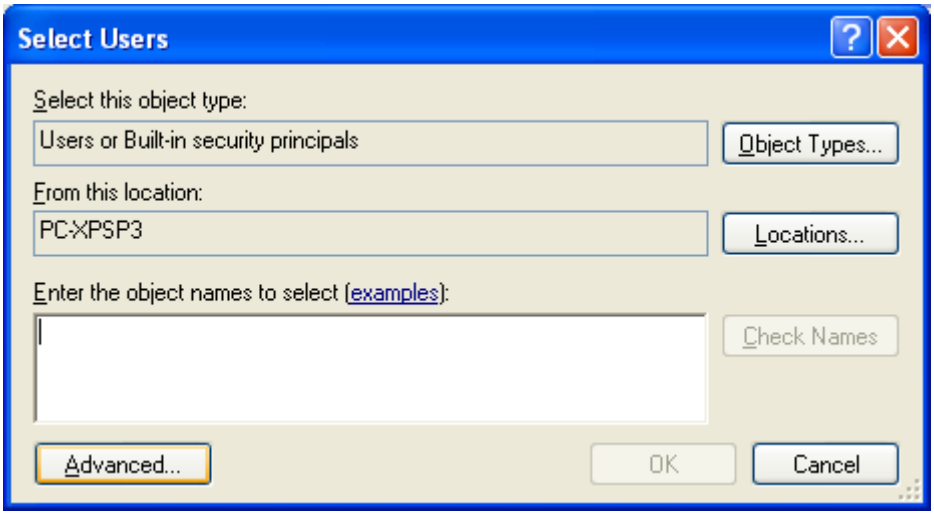
پس از ساخت گروه، نوبت به عضو گیری برای گروه می‌شود. بدین منظور روی گروه راست کلیک کرده و گزینه Properties را انتخاب کنید.



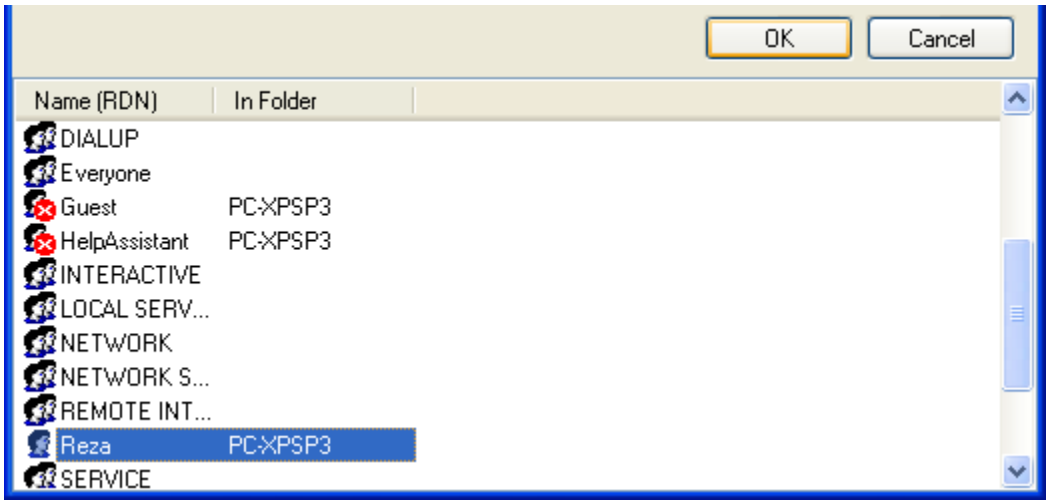
در پنجره باز شده، ابتدا وارد سربرگ Members شده و روی دکمه Add کلیک کنید.



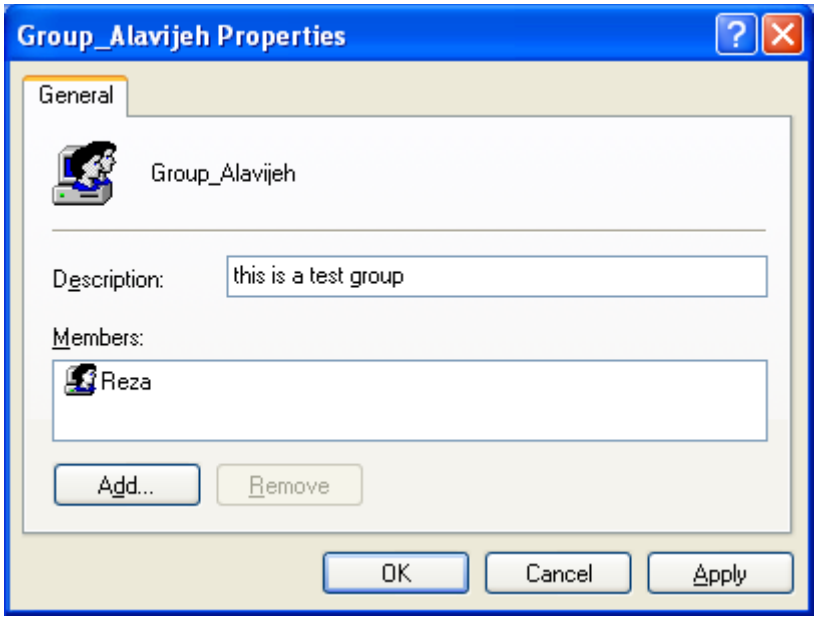
سپس برای انتخاب کاربر یا گروهی خاص برای عضو کردن در این گروه روی دکمه Advanced کلیک کنید.



سپس در صفحه باز شده، روی دکمه Find Now کلیک کرده، کاربران یا گروه‌های مورد نظر را انتخاب کرده و سپس دو مرتبه OK کنید تا اعضای انتخاب شده عضوی از این گروه شوند. در این مثال ما کاربر Reza را عضو این گروه کرده‌ایم.



سپس اعضای این گروه را مشاهده خواهید نمود.



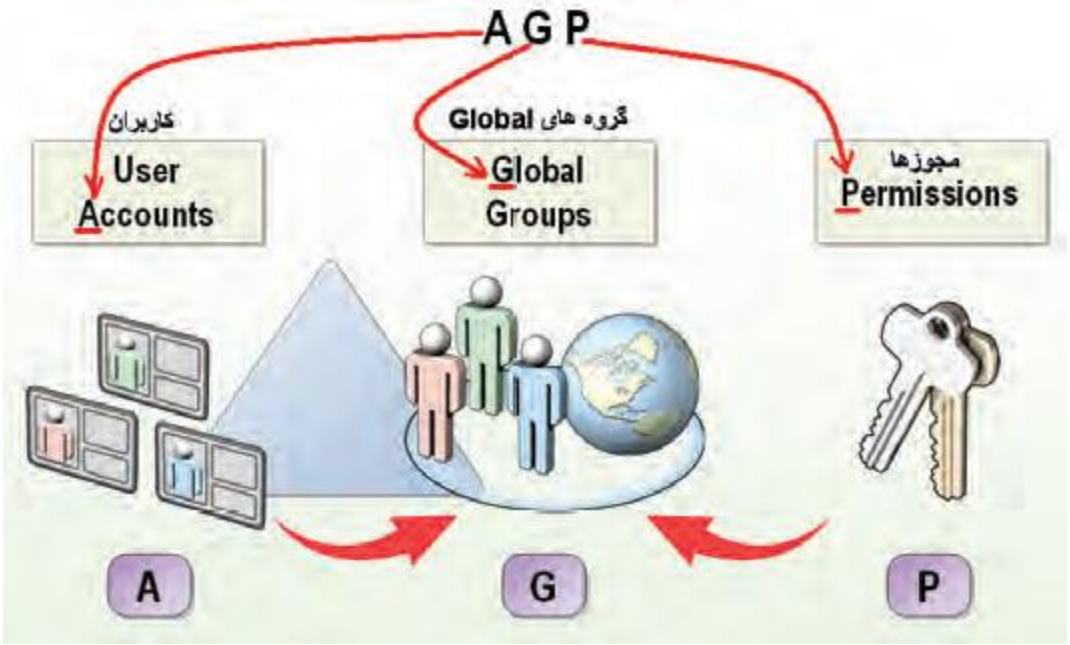
همچنین می‌توان کاربر یا گروهی خاص را به روشی دیگر عضوی از یک گروه کرد. بدین منظور ابتدا روی کاربر یا گروه مورد نظر راست کلیک کرده، گزینه Properties را انتخاب کرده و سپس وارد سربرگ Member Of شود. در صفحه باز شده، روی دکمه Add کلیک کرده و سپس گروه یا گروه هایی که قصد عضویت در آن را دارید انتخاب نمایید.



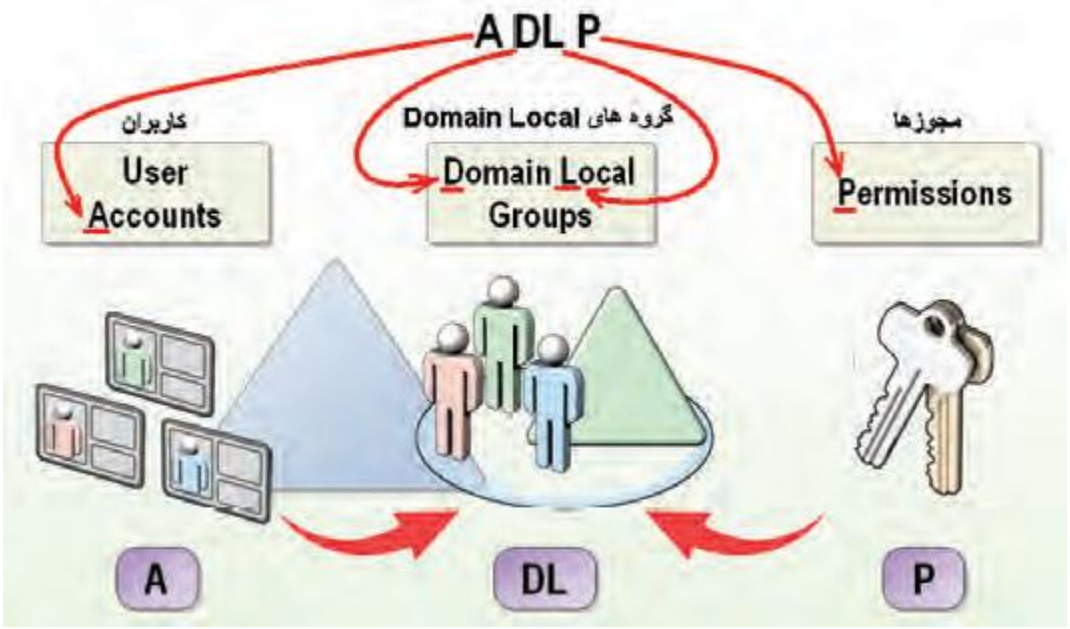
۲۳-۴-۱- روش‌های اعطای مجوز به کاربران

از روش‌های مختلفی برای اعطای مجوز به کاربران به کمک گروه‌ها می‌توان استفاده نمود.

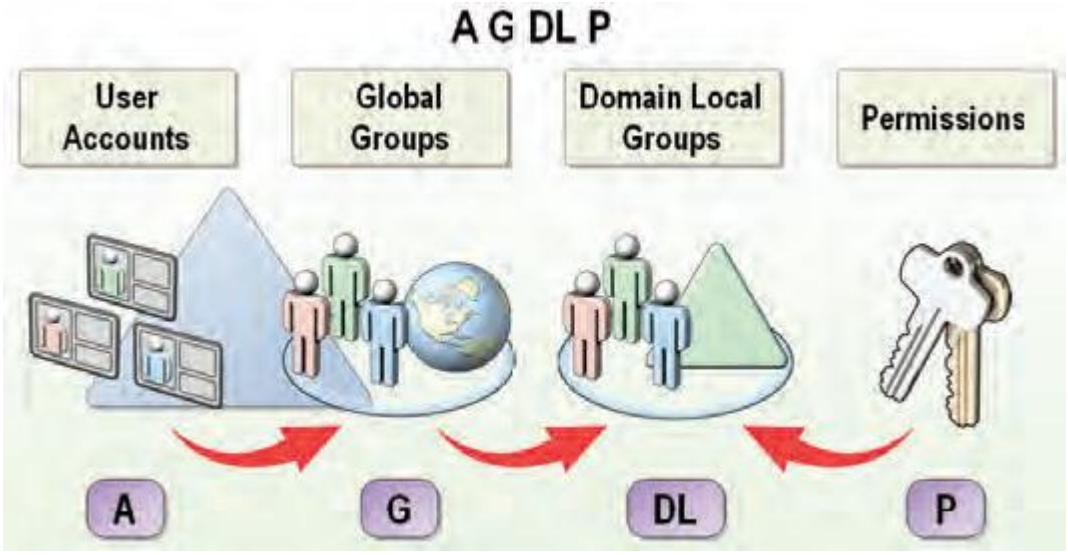
- **روش AGP:** در این روش کاربران (Account ها) را در گروه‌های مختلف از نوع Global دسته بندی می‌کنند. این دسته بندی از نظر **نوع کار و محل جغرافیایی کاربران** انجام می‌شود. سپس مجوز (Permission) لازم به گروه‌ها اعطا می‌شود. از این روش در شبکه هایی که تعداد Objectها زیاد نیست می‌توان استفاده کرد.



- **روش ADLP:** در این روش کاربران (Account ها) را در گروه‌های مختلف از نوع Domain Local دسته بندی نموده و سپس مجوزهای لازم را به گروه‌های مورد نظر اعطا می‌کنند. از این روش بیشتر زمانی که یک Domain بیشتر نداشته باشیم استفاده می‌شود.

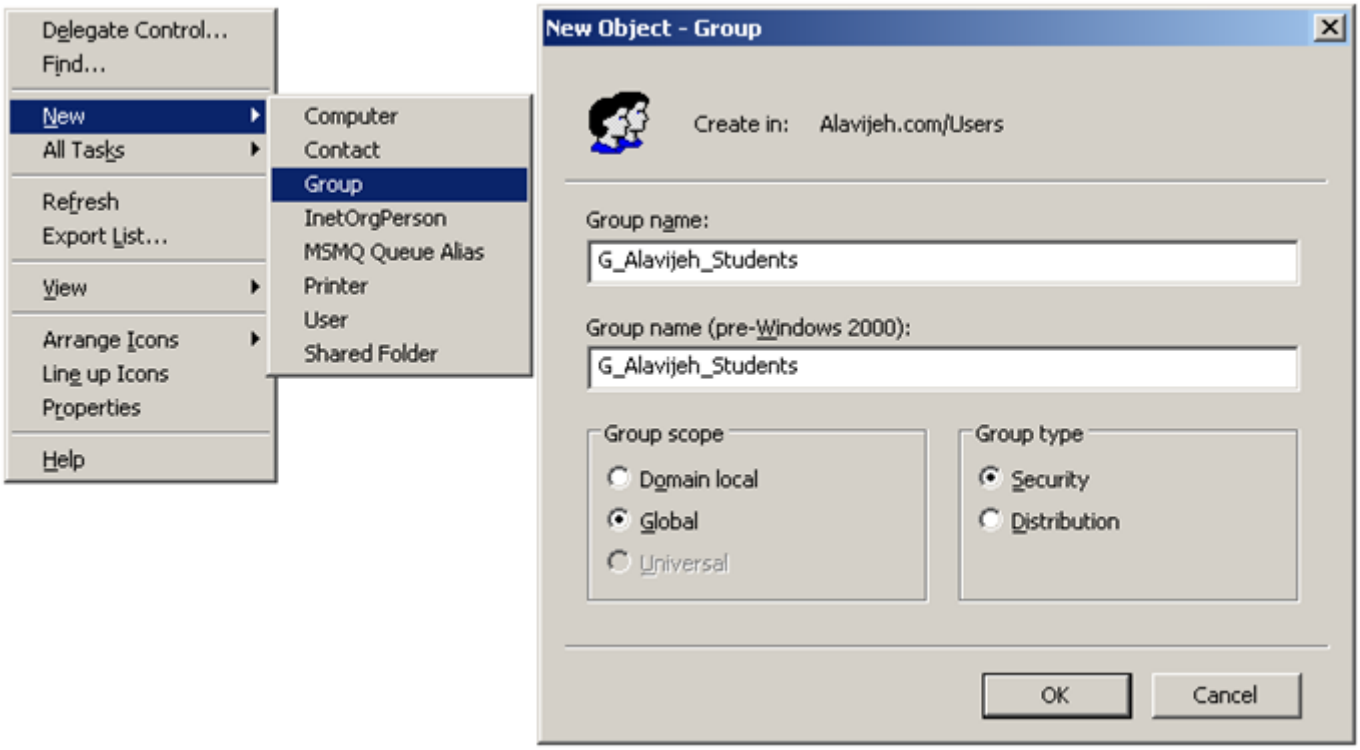


- **روش AGDLP:** در این روش کاربران را در گروه‌های مختلف از نوع Global دسته بندی می‌کنند. سپس گروه‌های از نوع Domain Local ایجاد کرده و به آن‌ها مجوز لازم را اعطا می‌کنند. حال تمامی گروه‌های Global که لازم است مجوزهای مربوطه را داشته باشند به عضویت گروه‌های Domain Local در می‌آورند. از این روش در شبکه هایی که تعداد Object هایی زیادی دارند و یا شبکه هایی که از چندین دامنه تشکیل شده‌اند می‌توان استفاده کرد.

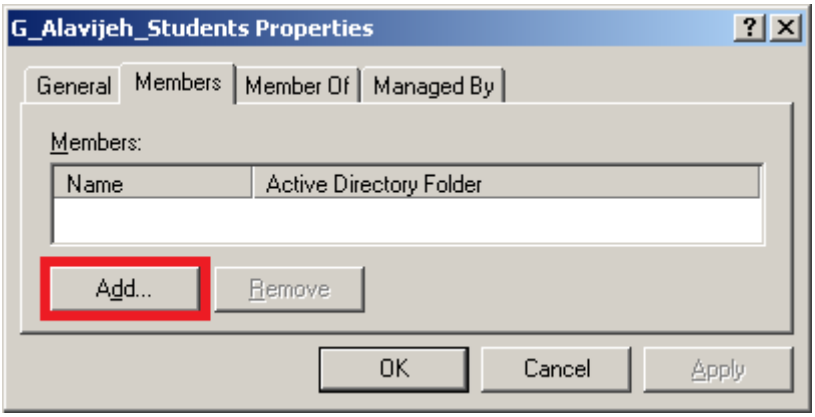


۲۳-۴-۲- پیاده سازی روش‌های مختلف اعطای مجوز به کاربران

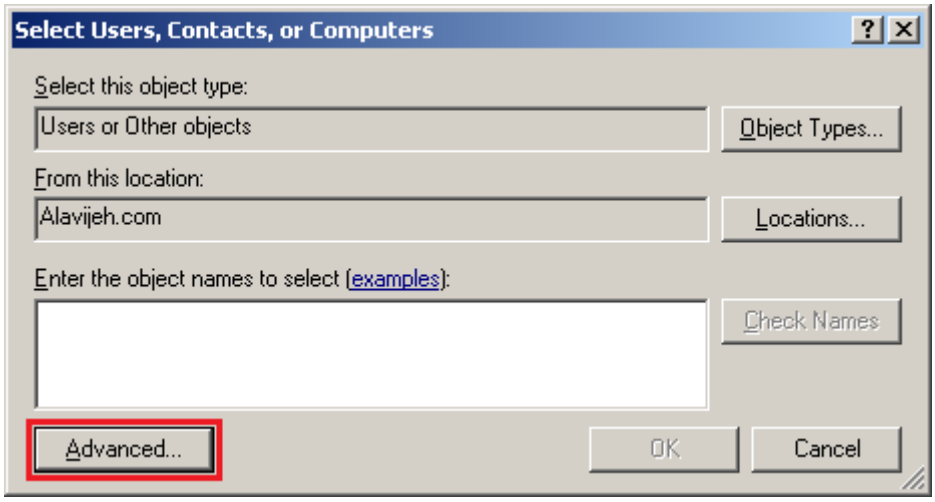
پیاده سازی روش AGP: در این روش ابتدا یک گروه از نوع Global به همان شیوه‌ای که در مراحل قبل یاد گرفتید، با نام G_Alavijeh_Students ایجاد کنید.



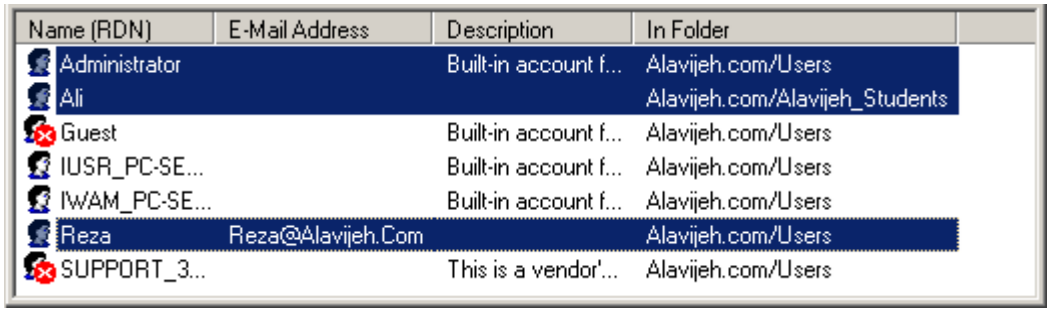
سپس روی این گروه راست کلیک کرده و Properties را انتخاب نمایید. سپس وارد سربرگ Members شوید. در زبانه Members لیست اعضای این گروه را مشاهده کنید.



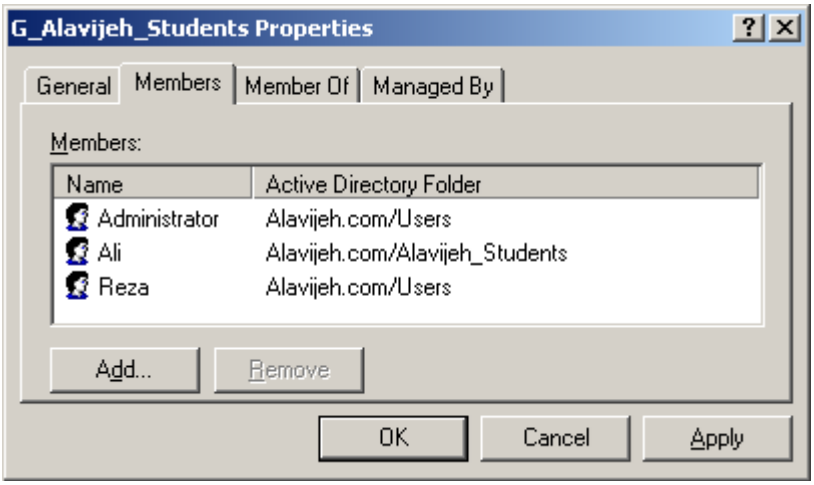
حال بایستی کاربرانی را عضو این گروه نمایید. بدین منظور روی دکمه Add کلیک کنید تا شکل زیر ظاهر شود.



در پنجره فوق می‌توانید اسامی کاربران را تایپ کرده و به لیست اضافه نمائید و یا برای انتخاب کاربران از لیست روی کلید Advanced کلیک کرده و سپس روی گزینه Find Now کلیک نمائید تا لیستی از کاربران و گروه‌ها نمایش داده شوند. حال کاربران مورد نظر را به کمک کلیدهای Ctrl و یا Shift انتخاب کرده و به لیست اضافه نمائید.

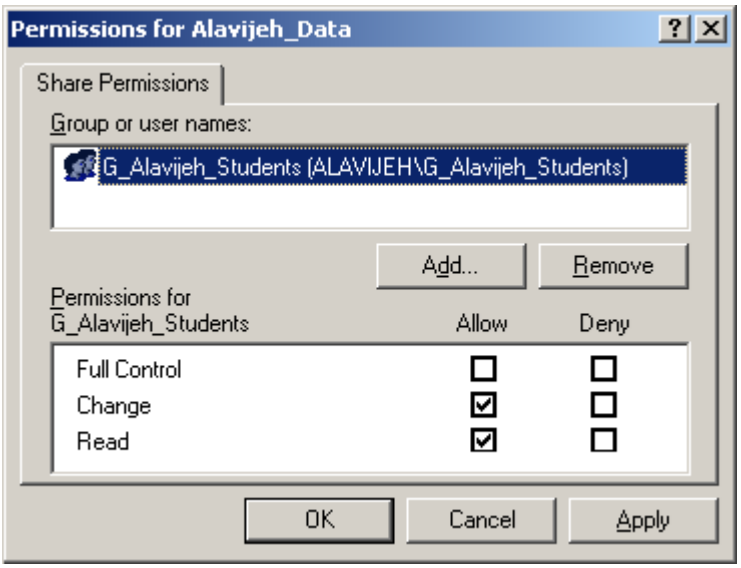


مشاهده خواهید کرد که این کاربران در زبانه Members لیست شده‌اند. روی گزینه OK کلیک کنید.

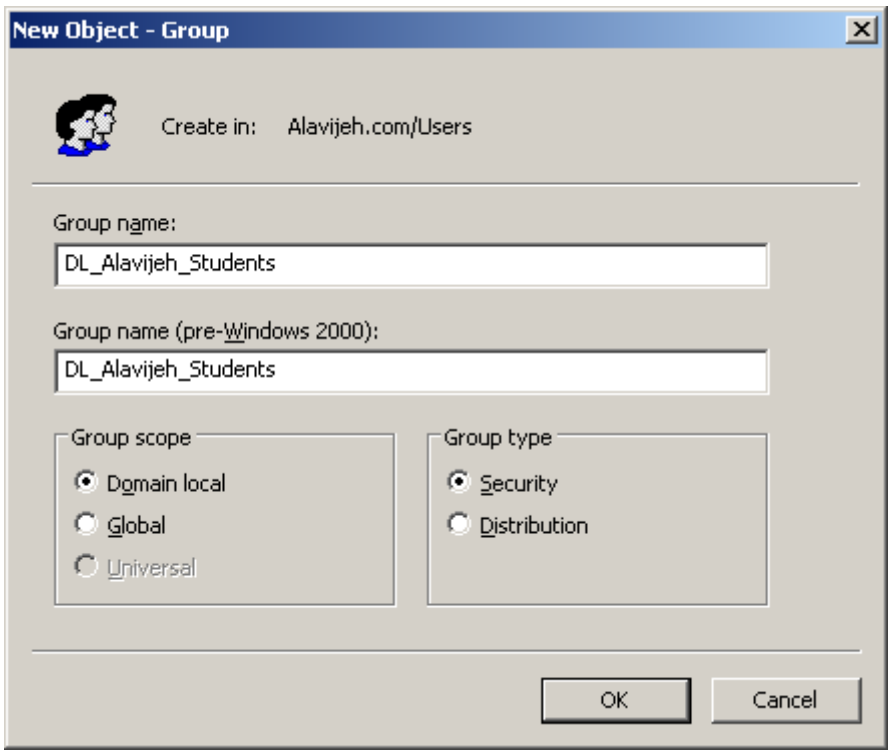


حال در هر جایی که منابع قرار دارند به این گروه مجوز می‌دهید. به عنوان مثال فرض کنید که یک پوشه به اشتراک گذاشته شده با نام Alavijeh_Data وجود دارد. روی این پوشه کلیک راست کرده و زبانه Sharing And Security را انتخاب کنید. در پنجره ظاهر شده روی دکمه Permissions کلیک کنید تا پنجره انتخاب کاربر گشوده شود.

در این پنجره گروه Every One را حذف کرده و سپس گروه G_Alavijeh_Students را به لیست اضافه کرده و مجوزهای لازم را به آن انتساب دهید.



پیاده سازی روش ADLP: این روش مشابه روش قبلی می‌باشد با این تفاوت که گروه را با نام DL_Alavijeh_Students ایجاد کرده و نوع آن را Domain Local انتخاب می‌کنیم. (بقیه مراحل مانند فوق صورت می‌گیرد.)



پیاده سازی روش AGDLP: در این روش ابتدا یک دسته بندی منطقی برای کاربران در نظر گرفته و سپس گروه‌های از نوع Global را ایجاد می‌کنیم و کاربران را براساس آن دسته بندی به عضویت گروه‌های مختلف (گروه‌های از نوع Global) در می‌آوریم. سپس یک گروه از نوع Local Domain ایجاد کرده و تمامی گروه‌های از نوع Global را عضو این گروه Local Domain می‌کنیم. در نهایت مجوزهای لازم روی منبع مورد نظر را به گروه Local Domain اعطا می‌نماییم. به عنوان مثال یک گروه با نام Alavijeh_Local_Users از نوع Local Domain ایجاد نموده و مجوز Print را

روی یک چاپگر به اشتراک گذاشته شده به آن اعطا می‌کنیم. البته بایستی گروه هایی که از نوع Global هستند و آن‌ها را قبلاً ساخته‌ایم را عضو گروه Alavijeh_Local_Users (گروهی از نوع Local Domain) کنیم.

۲۳-۵- واحدهای سازمانی یا Organizational Unit (OU)

Organizational Unit یا واحد سازمانی (به اختصار OU)، یک نوع پیشرفته و گسترش یافته Group است. گروه‌ها فقط می‌توانند User و Group را در خود نگهداری کنند؛ اما OU می‌تواند شامل هر نوع موجودیتی باشد، مانند: User، Group، Computer، Printer، Organizational Unit و....

البته تفاوت‌های دیگری نیز بین Organizational Unit و Group وجود دارد. مهمترین تفاوت این است که ما قابلیت تعریف Group Policy (سیاست گروهی) روی Organizational Unit را داریم، اما امکان تعیین Group Policy روی Group وجود ندارد.

در صورتی که با Group Policy آشنایی ندارید، به فصل Group Policy مراجعه فرمایید.

البته فقط به این نکته توجه داشته باشید که مفهوم User و Group در تمامی ویندوزها وجود دارد. اما مفهوم Organizational Unit فقط در ویندوز سرور و در Active Directory آن وجود دارد. لذا اگر در کار ویندوز سرور، تازه کار هستید، احتمالا مفهوم Organizational Unit برای شما جدید خواهد بود.

اما به نظر شما مهمترین کاربرد Organizational Unit چیست؟ به نظر بنده که مهمترین کاربرد Organizational Unit، نگهداری قسمت‌های منطقی یک سازمان است. فرض کنید که یک شرکت برنامه نویسی راه اندازی کرده‌اید. این شرکت شامل ۲ گروه عملیاتی ۱- برنامه نویسان و ۲- تحلیلگران است. در هر کدام از این گروه‌ها، چند نفر مشغول کارند. هر کدام از آن‌ها یک یا چند کامپیوتر دارند و هر گروه نیز یک چاپگر برای خود دارد. یک راه منطقی این است که هر کدام از این موارد را در یک دسته قرار دهیم. از آنجا که گروه قابلیت نگهداری اجزاء شبکه مانند چاپگر و کامپیوتر را ندارد، لذا مجبوریم از واحد قوی تری به نام Organizational Unit استفاده کنیم. لذا هر کدام از این دو گروه را در OUهای جدا قرار می‌دهیم. از طرف دیگر، قدرت مدیریت عناصر در ویندوز سرور، بسیار قوی‌تر از ویندوزهای غیر سروری است و از طرفی نیز OU فقط در ویندوز سرور وجود دارد.

به عنوان یک مزیت دیگر OU نسبت به گروه، می‌توان به این مورد اشاره کرد که در ویندوز سرور این قابلیت وجود دارد که مدیریت یک OU را به یک کاربر خاص واگذار (Delegate) کرد. مثلاً یک کاربر خاص را مامور مدیریت این OU کنیم که این کاربر سطوح دسترسی و خط مشی اعضای این OU را تعیین کند.

به طور خلاصه مزایای Organizational Unit (نسبت به گروه) به صورت زیر است:

۱. OU می‌تواند شامل هر نوع موجودیتی باشد، مانند: User، Group، Computer، Printer، Organizational Unit و....
۲. قابلیت تعریف Group Policy (سیاست گروهی) روی Organizational Unit وجود دارد.
۳. OU فقط در ویندوز سرور وجود دارد که ویندوز سرور خیلی قوی‌تر از ویندوزهای غیر سروری است.
۴. قابلیت دسته بندی واحدهای منطقی سازمان در آن وجود دارد.

۵. می توان مدیریت یک OU را به یک کاربر خاص واگذار (Delegate) کرد.

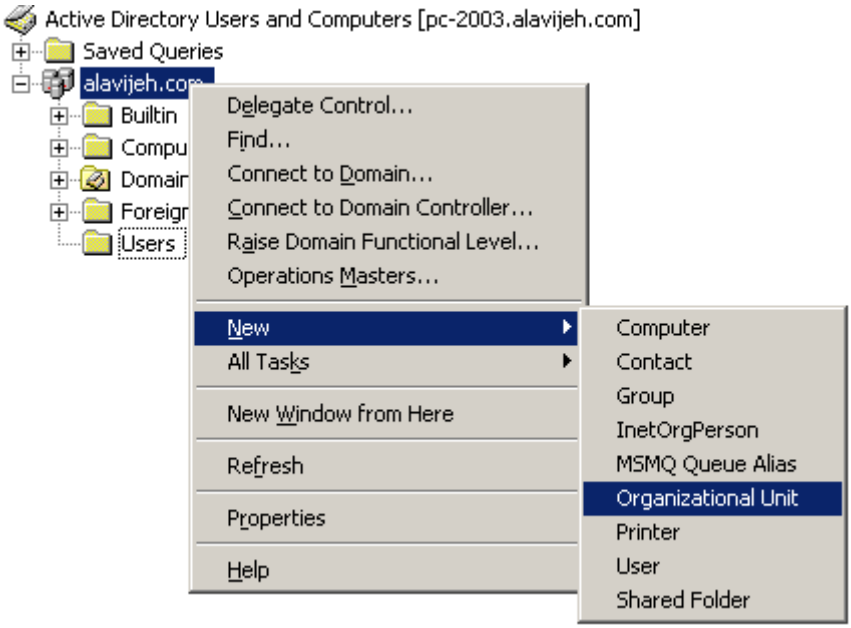
۲۳-۶- نحوه ساخت واحد سازمانی

توضیح دادیم که ساخت OU فقط در ویندوز سرور امکان پذیر است. برای ساخت OU، مراحل زیر را طی کنید:

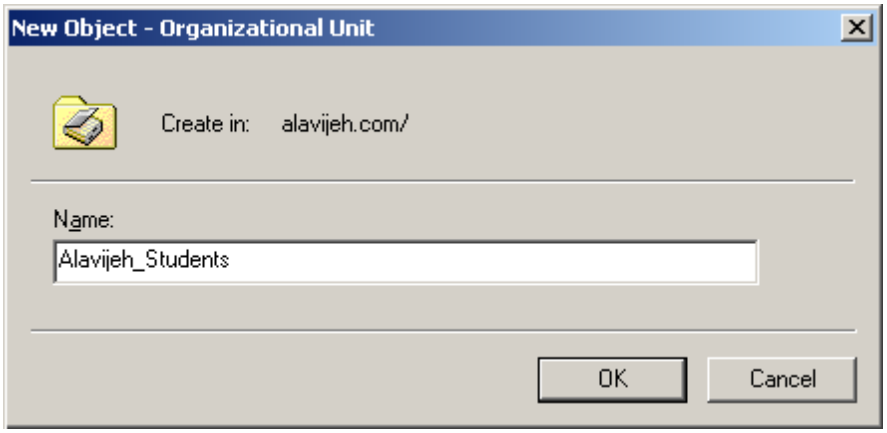
در قسمت Start بر روی Administrative Tools کلیک و سپس گزینه Active Directory Users and Computers را انتخاب نمائید.



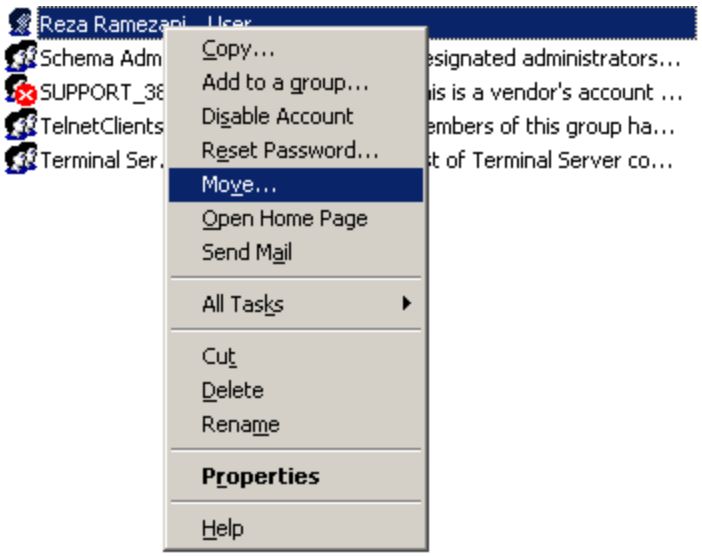
مطابق شکل زیر، روی نام سرور راست کلیک کرده و از منوی New گزینه Organization Unite را انتخاب نمایید.



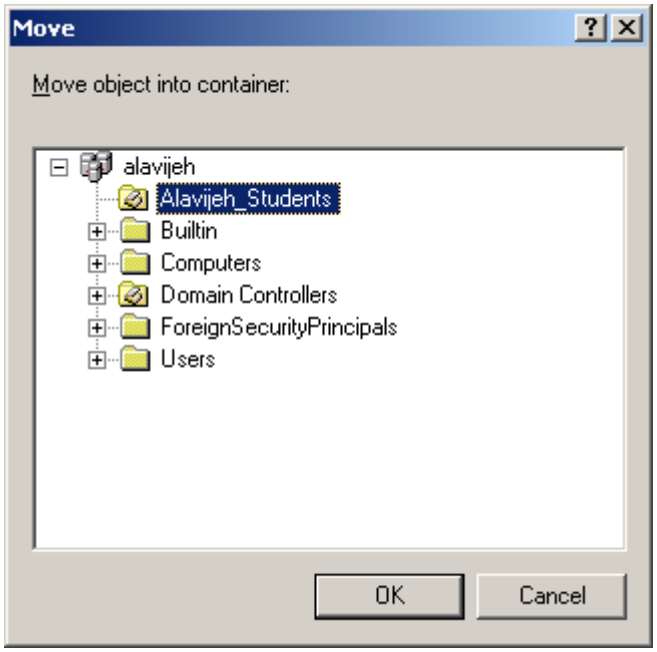
سپس یک نام برای واحد سازمانی خود (مثلاً Alavijeh_Students) وارد نمایید.



در ویندوز سرور ۲۰۰۳، هر کاربری که جدید ساخته شود به صورت پیش فرض در گروه Users قرار می‌گیرد پس برای اینکه بتوانید User یا Group ایجاد شده را عضو OU جدید کنید، آن را توسط موس داخل OU ساخته شده (در این مثال Alavijeh_Students) بیندازید. برای انتقال کاربر، روی آن راست کلیک کرده، گزینه Move را انتخاب کرده، مقصد را انتخاب نموده تا کاربر به آن انتقال یابد. در صورتیکه کاربری ایجاد نکردهاید بر روی Organization Unit ساخته شده راست کلیک کرده و از آنجا یک کاربر جدید بسازید تا از همان ابتدا عضو آن واحد سازمانی قرار گیرد.



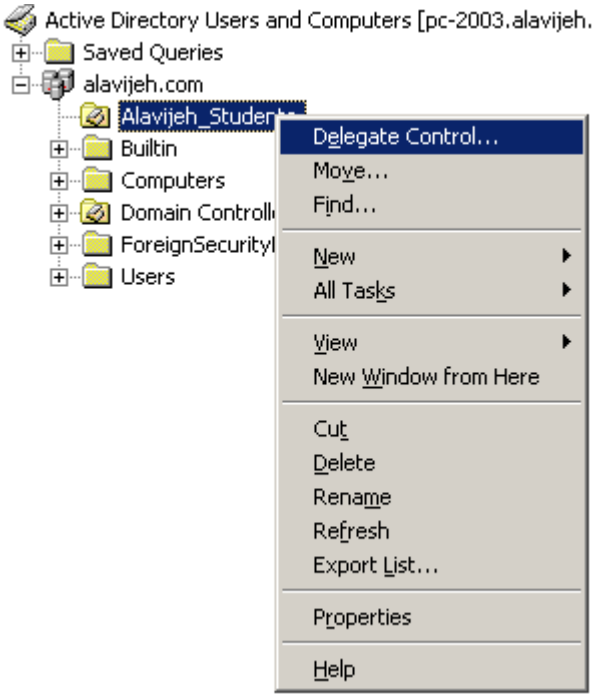
انتخاب مقصد کاربر:



اکنون Organization Unit ساخته شده و اعضای آن نیز مشخص می‌باشند حال باید برای آن‌ها Group Policy تعریف گردد. برای درک مفهوم Group Policy و آشنایی عملی با آن، به فصل Group Policy مراجعه نمایید.

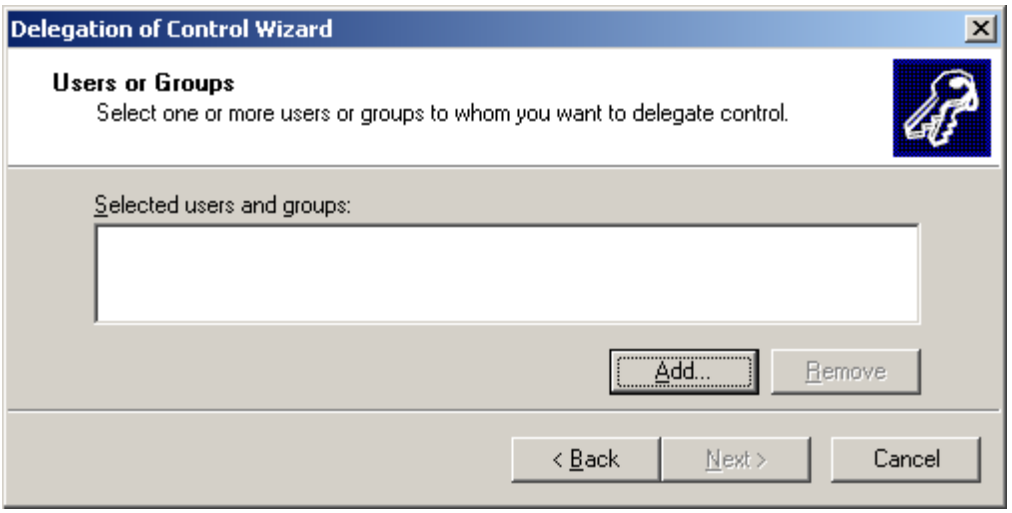
۲۳-۷- واگذاری مدیریت OU

در قسمت فوق اشاره کردیم که یکی از مزایای OU نسبت به Group این است که OU این قابلیت را دارد که می‌توان مدیریت OU را به یک کاربر واگذار کرد تا این کاربر خاص، خودش مدیریت OU را به عهده بگیرد. بدین منظور بر روی OU ساخته شده راست کلیک کرده و گزینه Delegate Control را انتخاب کنید.

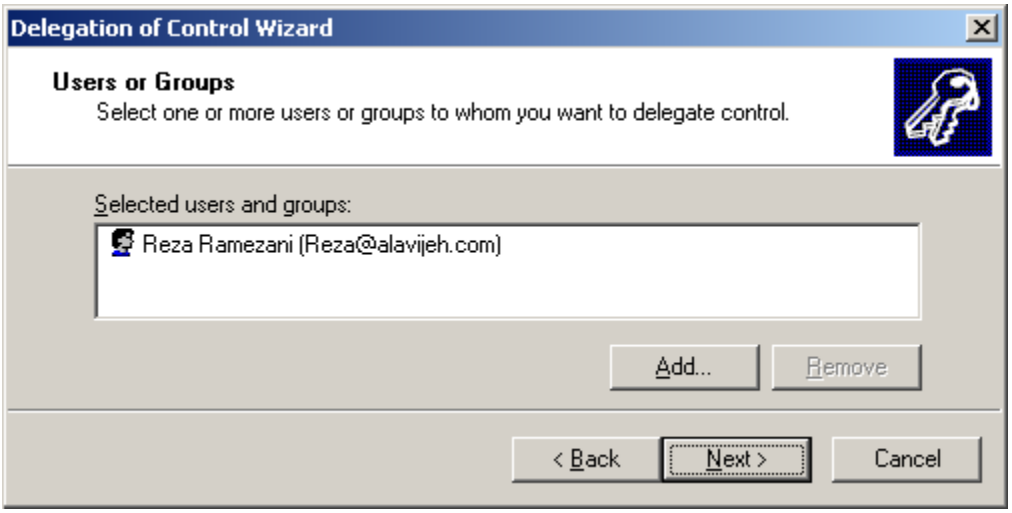


در صفحه خوش آمد گویی، دکمه Next را انتخاب کنید.

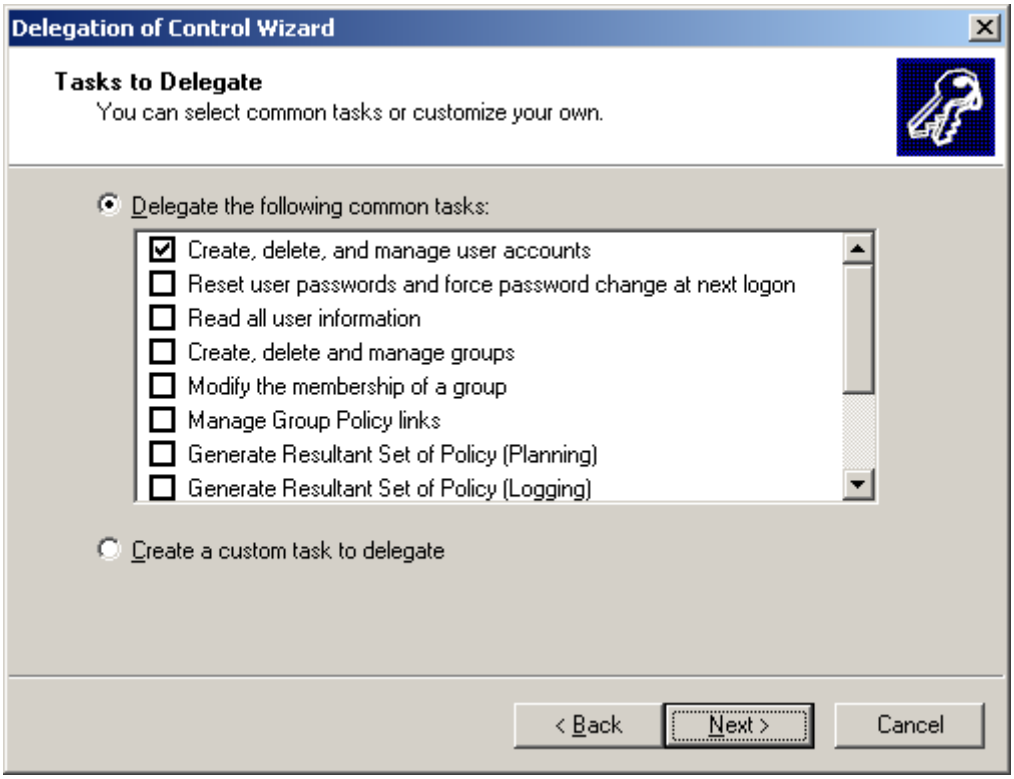
سپس در صفحه باز شده، کاربرانی که می‌خواهند مدیریت این OU را بر عهده بگیرند انتخاب کنید. بدین منظور روی دکمه Add کلیک کنید.



پس از انتخاب کاربری خاص، این کاربر در لیست مدیران OU قرار می‌گیرد. سپس روی دکمه Next کلیک کنید.



سپس در صفحه باز شده، سطوح دسترسی و قابلیت‌های مدیریتی کاربر انتخاب شده را تعیین نمایید. در مثال زیر، ما قابلیت ساخت و حذف اعضای OU را به کاربر داده‌ایم. سپس روی Next کلیک کنید.



در پایان بر روی دکمه Finish کلیک کنید. بدین ترتیب کاربر انتخاب شده قابلیت مدیریت OU ساخته شده را دارد.

فصل ۲۴

DNS Server

در این فصل در مورد DNS که یکی از مهمرین سرویس‌های شبکه و اینترنت است صحبت خواهد شد.

۲۴-۱- معرفی DNS (Domain Name Server)

DNS، ابزاری جهت تبدیل Host Name (نام کامپیوتر) به IP Address مربوطه می‌باشد. به عبارت دیگر، DNS در شبکه مانند ۱۱۸ عمل نموده و نام یک کامپیوتر را دریافت کرده و آدرس IP معادل آن را باز می‌گرداند.

هر کامپیوتر در شبکه یک Host نامیده می‌شود و علاوه بر IP Address دارای یک عنوان مشخص کننده دیگر به نام Host Name یا نام کامپیوتر می‌باشد. یک کامپیوتر برای بدست آوردن IP Address متناظر با Host Name، از کامپیوتری در شبکه به نام DNS Server کمک می‌گیرد. DNS Server، حاوی نام و آدرس IP کامپیوتر مورد نظر می‌باشد که پس از مقایسه درخواست با اطلاعات موجود در Database خود، IP Address مورد نظر را بر می‌گرداند.

جهت استفاده از DNS به اجزای زیر نیازمند خواهیم بود:

۱. DNS Client یا درخواست کننده IP Address
۲. DNS Server که حاوی اطلاعات مربوط به نام Host و IP Address، منابع موجود و نوع آن در شبکه می‌باشد. که به این بانک اطلاعاتی، Resource Record یا به اختصار RR گفته می‌شود.

لازم به ذکر است که DNS Serverهای موجود در اینترنت، جهت تبدیل نام به IP Address در شبکه اینترنت استفاده می‌شود.

۲۴-۲- تاریخچه DNS

DNS، زمانی که اینترنت تا به این اندازه گسترش پیدا نکرده بود و صرفاً در حد و اندازه یک شبکه کوچک بود، استفاده می‌گردید. در آن زمان، اسامی کامپیوترهای میزبان (سرور ها) به صورت دستی در فایلی با نام HOSTS درج می‌گردید (برای پیدا کردن این فایل در ویندوز، به آدرس C:\Windows\System32\drivers\etc مراجعه نمایید). فایل فوق بر روی یک سرویس دهنده مرکزی قرار می‌گرفت. هر سایت و یا کامپیوتر که نیازمند ترجمه اسامی کامپیوترهای میزبان بود، می‌بایست از فایل فوق استفاده می‌نمود. همزمان با گسترش اینترنت و افزایش تعداد کامپیوترهای میزبان، حجم فایل فوق نیز افزایش و امکان استفاده از آن با مشکل مواجه گردید (افزایش ترافیک شبکه). با توجه به مسائل فوق، در سال ۱۹۸۴ تکنولوژی DNS معرفی گردید.

۲۴-۳- پروتکل DNS

DNS، یک "بانک اطلاعاتی توزیع شده" است که بر روی ماشین‌های متعددی مستقر می‌شود (مشابه ریشه‌های یک درخت که از ریشه اصلی انشعاب می‌شوند). در صورت استفاده از ویندوز ۲۰۰۳ و اکتیو دایرکتوری، قطعا از DNS به منظور ترجمه اسامی کامپیوترها به آدرس‌های IP، استفاده می‌شود. شرکت مایکروسافت ابتدا نسخه اختصاصی و اولیه سرویس دهنده DNS خود را با نام WINS (Windows Internet Name Service) طراحی و پیاده سازی نمود. و سپس به علت قدیمی بودن آن به سمت DNS حرکت کند. DNS مسئولیت حل مشکل اسامی کامپیوترها (ترجمه نام به آدرس) در یک شبکه و مسائل مرتبط با برنامه‌های Winsock (برنامه‌های سوکت که در ویندوز نوشته می‌شوند و در آن برای آدرس‌دهی یک کامپیوتر از آدرس IP کامپیوتر استفاده می‌شود) را بر عهده دارد.

اغلب برنامه هایی که براساس پروتکل TCP/IP نوشته می‌شوند، از اینترفیس Winsock استفاده می‌نمایند. این نوع برنامه‌ها نیازمند آگاهی از نام کامپیوتر مقصد برای ارتباط نبوده و با آگاهی از آدرس IP کامپیوتر مقصد قادر به ایجاد یک ارتباط خواهند بود.

کامپیوترها جهت کار با اعداد (خصوصا IP) دارای مسائل و مشکلات بسیار ناچیزی می‌باشند. در صورتی که انسان در این رابطه دارای مشکلات خاص خود است. به هرحال به خاطر سپردن اسامی کامپیوترها به مراتب راحت‌تر از بخاطر سپردن اعداد (کد) است. از آنجایی که برنامه‌های Winsock نیازمند آگاهی از نام کامپیوتر یا Host Name نمی‌باشند، می‌توان با رعایت تمامی مسائل جانبی از روش فوق برای ترجمه اسامی استفاده کرد. فرآیند فوق را ترجمه اسامی (Hostname Resolution) می‌گویند.

۲۴-۴- DNS Namespace

DNS از یک ساختار سلسله مراتبی برای سیستم نام گذاری خود استفاده می‌نماید. با توجه به ماهیت سلسله مراتبی بودن ساختار فوق، چندین کامپیوتر می‌توانند دارای اسامی یکسان بر روی شاخه‌های مختلف بوده و هیچگونه نگرانی از عدم ارسال پیام‌ها وجود نخواهد داشت. ویژگی فوق درست نقطه مخالف سیستم نامگذاری NetBIOS است. در مدل NetBIOS قادر به انتخاب دو نام یکسان برای دو کامپیوتر، حتی در سطوح مختلف سلسله مراتب کامپیوترها، نخواهیم نبود.

NetBIOS یک پروتکل قدیمی می‌باشد که برای برقراری ارتباط میان کامپیوترها توسط شرکت IBM ایجاد شد (پروتکل‌ها مجموعه قوانین و مقرراتی هستند که برای انجام یک فرآیند خاص در شبکه‌های کامپیوتری تعریف می‌شوند). قابلیتی که این پروتکل ایجاد می‌کند، این است که، امکان دیدن نام کامپیوتر هایی که در یک گروه کاری (Workgroup) قرار دارند را فراهم می‌کند.

بالاترین سطح در DNS با نام Root Domain (یا Hint Root) نامیده شده و اغلب به صورت یک "." و یا یک فضای خالی "" نشان داده می‌شود. بلافاصله پس از ریشه با اسامی موجود در دامنه بالاترین سطح (Top Level) برخورد خواهیم کرد. مثلاً دامنه‌های .com، .net، .org و .edu

اینترنت به چندین ناحیه سطح بالا (Top-Level Domain) که هر کدام تعداد زیادی کامپیوتر را در بر می‌گیرد، تقسیم می‌شود. هر ناحیه به چندین زیر ناحیه (Sub Domain) و آن‌ها نیز به نوبه خود به زیر ناحیه‌های کوچکتر تقسیم می‌شوند. ناحیه هایی که زیر ناحیه ندارند "برگ" نامیده می‌شوند.

ناحیه‌های سطح بالا (Top Level) دو گونه اند: عمومی و کشورها.

ناحیه‌های عمومی مانند:

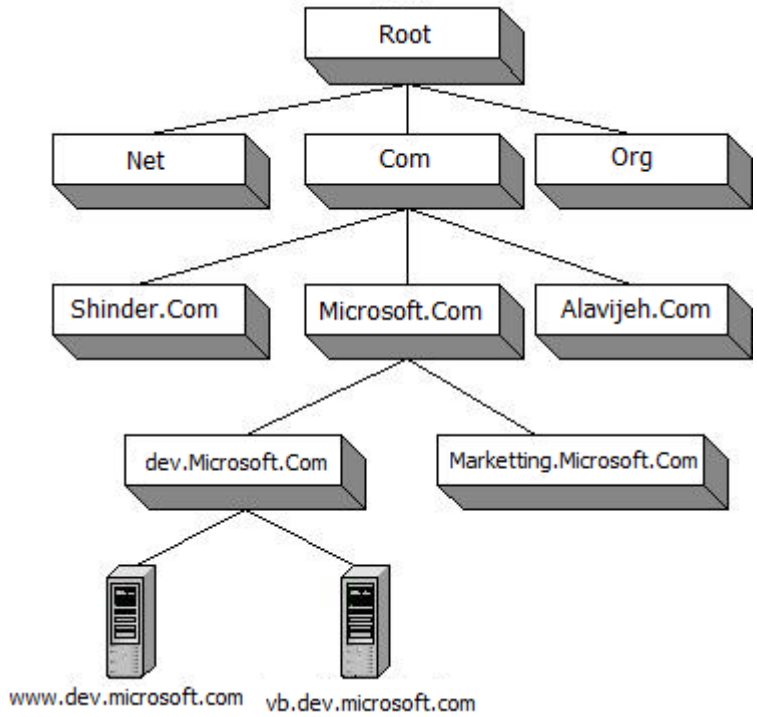
- Com (مخفف Commercial، تجاری)
- Edu (مخفف Educational، مؤسسات آموزشی)
- Net (مخفف Network Provider، شرکتهای خدمات شبکه و اینترنت) و غیره...

ناحیه‌های کشورها مانند:

- ir (کشور ایران)
- de (کشور آلمان)
- ja (کشور ژاپن)

سازمان هایی که تمایل به داشتن یک وب سایت بر روی اینترنت دارند، می‌بایست یک دامنه را که به عنوان عضوی از اسامی حوزه Top Level می‌باشد را برای خود اختیار نماید. هر یک از حوزه‌های سطح بالا دارای کاربردهای خاصی می‌باشند. مثلاً سازمان‌های اقتصادی در حوزه.Com و موسسات آموزشی در حوزه.Edu و... دامنه خود را ثبت خواهند نمود.

شکل زیر ساختار سلسله مراتبی DNS را نشان می‌دهد.



در هر سطح از ساختار سلسله مراتبی فوق می‌بایست اسامی با یکدیگر متفاوت باشد. مثلاً نمی‌توان دو حوزه.Com و یا دو حوزه.Net را تعریف و یا دو حوزه Microsoft.Com در سطح دوم را داشته باشیم. استفاده از اسامی تکراری در سطوح متفاوت مجاز می‌باشد.

حوزه‌های Top Level و Second Level تنها بخش هایی از سیستم DNS می‌باشند که می‌بایست به صورت مرکزی مدیریت و کنترل گردند. به منظور ثبت نمودن دامنه مورد نظر خود می‌بایست با سازمان و یا شرکتی که مسئولیت ثبت نمودن دامنه را برعهده دارد ارتباط برقرار نموده و از آن‌ها درخواست نمود که عملیات مربوط به ثبت نمودن دامنه مورد نظر ما را انجام دهند. در گذشته تنها سازمانی که دارای مجوز لازم برای ثبت نمودن حوزه‌های سطح دوم را در اختیار داشت شرکت NSI (Network Solutions Incorporated) بود. امروزه امتیاز فوق صرفاً در اختیار شرکت فوق نبوده و شرکت‌های متعددی اقدام به ثبت نمودن حوزه‌ها می‌نمایند.

مشخصات دامنه و اسم Host

هر کامپیوتر در DNS به عنوان عضوی از یک دامنه در نظر گرفته می‌شود. به منظور شناخت و ضرورت استفاده از ساختار سلسله مراتبی به همراه DNS، لازم است با FQDN با جزئیات بیشتری آشنا شویم.

۲۴-۴-۱- معرفی FQDN (Fully Qualified Domain Names)

یک FQDN، محل یک کامپیوتر خاص را در DNS مشخص خواهد نمود. با استفاده از FQDN می‌توان به سادگی محل کامپیوتر در دامنه مربوطه را مشخص و به آن دستیابی نمود. FQDN یک نام ترکیبی است که در آن **نام ماشین** (Host) و **نام دامنه** مربوطه با یکدیگر ترکیب شده‌اند (بحثی شبیه آدرس شبکه و آدرس کامپیوتر در شبکه در مبحث آدرس IP). مثلاً اگر شرکتی با نام Shiraziha در حوزه سطح دوم دامنه خود را ثبت نماید (Shiraziha.Com) در صورتی که سرویس دهنده وب بر روی Shiraziha.Com اجراء گردد، می‌توان آن را www نامید (www نام Host ماشین مربوطه است و شناسه خدماتی نیست) کاربران با استفاده از www.Shiraziha.Com به آن دستیابی پیدا نمایند. یک نام FQDN از دو عنصر اساسی تشکیل شده است:

- **Label:** شامل نام حوزه و یا نام یک Host است.
- **Dots:** نقطه‌ها که باعث جداسازی بخش‌های متفاوت خواهد شد.

هر Lable توسط نقطه از یکدیگر جدا خواهند شد. هر Lable می‌تواند حداکثر دارای ۶۳ بایت باشد (طول هر Lable بر حسب بایت مشخص شده است نه بر حسب طول رشته؛ علت این است که DNS در ویندوز ۲۰۰۳ از کاراکترهای UTF-8 استفاده می‌نماید نه کاراکترهای اسکی) طول FQDN باید حداکثر ۲۵۵ بایت باشد.

همانطوری که در شکل زیر مشاهده می‌کنید، تمامی اسامی اینترنتی به یک نقطه ختم می‌شوند. البته لازم به توضیح است که کاربران اینترنتی معمولاً این نقطه را در انتهای اسامی اینترنتی وارد نمی‌کنند و این نقطه به صورت اتوماتیک به اسامی اضافه می‌شود.

این قسمت از اسامی اینترنتی با نام Root Level (سطح ریشه) شناخته می‌شود پس می‌توان نتیجه گرفت که آخرین نقطه در اسامی اینترنتی بخشی از آن اسم نیز می‌باشد (برخلاف سایر نقطه‌ها که به عنوان جدا کننده مورد استفاده قرار می‌گیرند).

قسمت دوم از سمت راست این اسامی معمولاً اسامی دو یا سه کاراکتری هستند که بیانگر **نوع فعالیت** Domain و یا **محل جغرافیایی** آن Domain می‌باشند. به عنوان مثال.Com بیانگر فعالیت‌های تجارتی،.ir بیانگر کشور ایران،.Edu

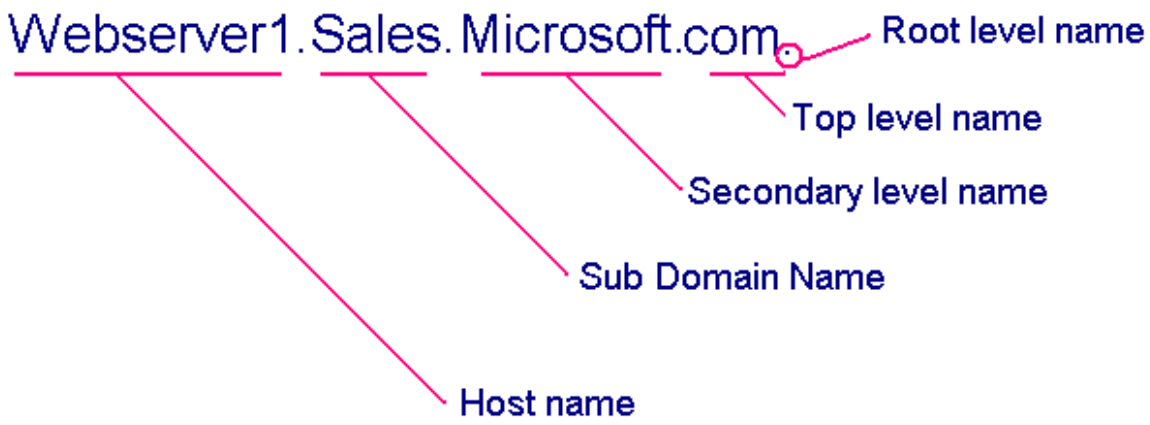
بیانگر فعالیت‌های آموزشی،.Ca بیانگر کشور کانادا و... می‌باشند. به اسامی مربوط به این سطح اسامی Top level (سطح بالا) گفته می‌شود.

قسمت بعد در اسامی اینترنتی مربوط به اسامی شرکت‌ها و اشخاص و... می‌باشد. این اسامی به وسیله اشخاص و یا شرکت‌ها اجاره می‌شوند. شرکت‌های خاصی این اسامی را اجاره می‌دهند. به عنوان مثال Microsoft یا Softgozar اسامی مربوط به این سطح می‌باشد که به آن‌ها اسامی Secondary (ثانویه) گفته می‌شود. نظارت بر اسامی اینترنتی و تشخیص آن‌ها به عهده شرکت Internic می‌باشد.

ایجاد Sub Domainها (زیر دامنه ها) به شرکت‌های مربوطه واگذار می‌شود (خود فرد یا شرکت صاحب دامنه). به عنوان مثال در داخل Microsoft، یک زیر دامنه به نام Training ایجاد شده است. ایجاد و نگهداری این زیر دامنه به عهده شرکت مایکروسافت می‌باشد: Training.Microsoft.Com

اسامی Hostها یا Sub Domainها از پائین ساختار درختی شروع شده و به ریشه ختم می‌گردد.

به عنوان مثال در شکل زیر یک Host با نام www وجود دارد که FQDN آن www.Microsoft.com می‌باشد. یا یک Host دیگری به نام WebServer وجود دارد که FQDN آن WebServer.Training.Microsoft.com. می‌باشد. شکل زیر قسمت‌های مختلف این اسم را تشریح می‌کند.



۲۴-۴-۲- استفاده از نام یکسان دامنه برای منابع اینترنت و اینترانت

به منظور حفاظت ناحیه (Zone)های DNS از دستیابی غیر مجاز، نباید هیچ گونه اطلاعاتی در رابطه با منابع داخلی بر روی سرویس دهنده DNS نگهداری نمود. بنابراین می‌بایست برای یک دامنه از دو Zone متفاوت استفاده نمود. یکی از Zoneها، منابع داخلی را دنبال می‌کند و Zone دیگر، مسئولیت پاسخگوئی به منابعی است که بر روی اینترنت قرار دارند. عملیات فوق قطعا حجم وظایف مدیریت سایت را افزایش خواهد داد.

۲۴-۴-۳- پیاده سازی نام یکسان برای منابع داخلی و خارجی

یکی دیگر از عملیات پیاده سازی دامنه‌های یکسان برای منابع داخلی و خارجی، Mirror نمودن منابع خارجی به صورت داخلی است. مثلاً فرض نمائید که Test.Com نام انتخاب شده برای دستیابی به منابع داخلی (اینترانت) و منابع خارجی (اینترنت) است. می‌خواهیم از اسامی یکسان برای سرویس دهندگان استفاده نماییم. اگر درخواستی برای www.Test.Com

صورت پذیرد، مسئله به کامپیوتری ختم خواهد شد که قصد داریم برای کاربران اینترنت قابل دستیابی باشد. در وضعیت هایی که نخواهیم کاربران اینترنت قادر به دستیابی به اطلاعات شخصی و داخلی سازمان باشند. حل مشکل فوق، Mirror نمودن منابع اینترنت به صورت داخلی است و ایجاد یک Zone در DNS برای دستیابی کاربران به منابع داخلی ضروری خواهد بود. زمانیکه کاربری درخواست www.Test.Com را صادر نماید، در ابتدا مسئله نام از طریق سرویس دهنده داخلی DNS برطرف خواهد شد که شامل Zone داخلی مربوطه است. زمانی که یک کاربر اینترنت قصد دستیابی به www.Test.Com را داشته باشد، درخواست وی به **سرویس دهنده اینترنت** DNS ارسال خواهد شد؛ که در چنین حالتی آدرس IP سرویس دهنده خارجی DNS برگردانده خواهد شد.

۲۴-۴-۴- استفاده از اسامی متفاوت برای دامنه‌های اینترنت و اینترانت

در مدل فوق نیازی به نگهداری Zoneهای متفاوت برای هر یک از آن‌ها نبوده و هریک از آن‌ها دارای یک نام مجزا و اختصاصی مربوط به خود خواهند بود. مثلاً می‌توان نام **اینترنتی** حوزه را Test.Com و نام اینترانتی آن را Test.Local قرار داد.

برای نامگذاری هر یک از زیر دامنه‌ها می‌توان اسامی انتخابی را براساس نوع فعالیت و یا حوزه جغرافیایی انتخاب نمود.

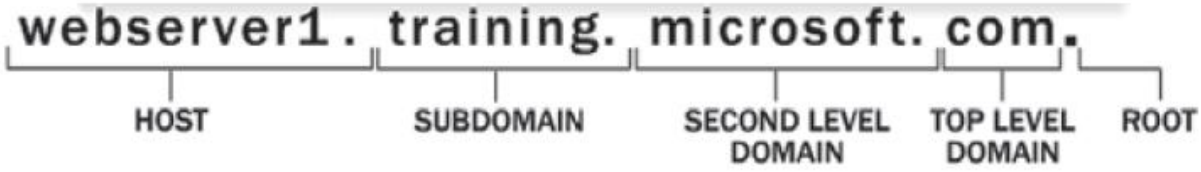
۲۴-۵- اجزاء DNS

یک DNS Server دارای اجزاء زیر می‌باشد:

۱- **Name Server:** به DNS Server، Name Server نیز اطلاق می‌شود و یک سرور ۲۰۰۳ است (در این جزوه) که سرویس DNS روی آن نصب گردیده است.

۲- **Zone:** یک DNS Server اطلاعات مربوط به Domainهای مختلف را می‌تواند نگهداری کرده و به کاربران در ارتباط با آن‌ها سرویس دهد. برای نگهداری اطلاعات Domain در DNS از Zone استفاده می‌شود. به عبارت دیگر بانک اطلاعاتی DNS سرور همان Zone می‌باشد.

در FQDN (شکل زیر)، به هر کدام از گزینه‌های Secondary Level مثل Microsoft یا Yahoo، یک Domain گفته می‌شود. زمانی که این Domainها را در DNS می‌خواهیم پیاده سازی کنیم، باید آن‌ها را با Zone ایجاد نماییم. بنابر این در شکل و نمودارها از واژه Domain و در عمل از Zone استفاده می‌شود.



Zoneها به دو دسته کلی تقسیم می‌شوند.

- **Forward Lookup Zones:** Zone هایی هستند که برای تبدیل اسم به IP استفاده می‌شوند.
- **Revers Lookup Zones:** Zone هایی هستند که برای تبدیل IP به اسم استفاده می‌شوند.

۳- **Resource Records:** در یک Zone اطلاعات مربوط به یک Domain نگهداری می‌شود. این اطلاعات به صورت رکورد ثبت و نگهداری می‌شوند. به عنوان مثال اسم و IP یک Host در یک رکورد از نوع Host قرار می‌گیرند. رکورد از نوع Host بیشترین استفاده را در DNS دارا می‌باشد، ولی از انواع رکوردها در یک Zone می‌توان استفاده نمود که تعدادی از این نوع رکوردها عبارتند از:

- **Host Record:** از این رکورد به منظور تبدیل اسم به IP استفاده می‌شود.
- **Point Record:** از این رکورد به منظور تبدیل IP به اسم استفاده می‌شود.
- **SRV Record:** از این رکورد به منظور معرفی سرویس دهنده هایی که سرویس‌های خاص را ارائه می‌کنند، استفاده می‌شود.
- **NS Record:** از این رکورد برای معرفی Name server (DNS) استفاده می‌شود.
- **SOA Record:** از این رکورد برای معرفی اطلاعاتی در ارتباط با یک Zone استفاده می‌شود.
- **Alias Record:** از این رکورد برای استفاده از اسم مستعار بجای FQDN استفاده می‌شود.

۲۴-۶- ناحیه‌ها یا Zoneها (Zones of Authority)

DNS دارای ساختاری است که از آن برای گروه بندی و دنبال نمودن ماشین مربوطه، براساس نام Host در شبکه استفاده خواهد شد. به منظور فعال نمودن DNS در جهت تامین خواسته‌ای مورد نظر، می‌بایست روشی جهت ذخیره نمودن اطلاعات در DNS وجود داشته باشد. اطلاعات واقعی در رابطه با دامنه‌ها در فایلی با نام Zone Database ذخیره می‌گردد. این نوع فایل‌ها، فایل‌های فیزیکی بوده که بر روی سرویس دهنده DNS ذخیره خواهند شد. یعنی برای نگهداری اطلاعات Domain در DNS از Zone استفاده می‌شود. به عبارت دیگر بانک اطلاعاتی DNS Server همان Zone می‌باشد. به هر کدام از گزینه‌های سطح دوم FQDN (مانند Microsoft در www.Microsoft.Com) یک Domain گفته می‌شود. زمانی که این Domainها را در DNS می‌خواهیم پیاده سازی کنیم، باید آن‌ها را با Zone ایجاد کرد. بنابر این در شکل‌ها و نمودارها از واژه Domain و در عمل از Zone استفاده می‌شود. آدرس محل قرار گیری فایل‌های فوق %systemroot%\system32\dns\ خواهد بود. Zoneهای استاندارد به دو نوع عمده تقسیم می‌شوند:

- Forward Lookup Zone
- Reverse Lookup Zone

۲۴-۶-۱- *Forward Lookup Zone*

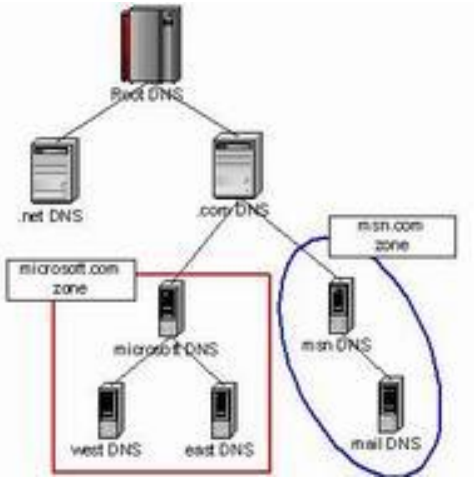
از این نوع Zone برای ایجاد مکانیزمی برای ترجمه اسامی Hostname به آدرس IP برای سرویس گیرندگان DNS استفاده می‌گردد. Zoneها دارای اطلاعاتی هستند که به صورت رکوردهای خاص در بانک اطلاعاتی مربوطه ذخیره خواهند شد. این نوع رکوردها را رکوردهای منبع یا Resource Record می‌گویند. رکوردهای فوق اطلاعات مورد نیاز در رابطه با منابع قابل دسترس در هر Zone را مشخص خواهند کرد.

۲۴-۶-۲- Reverse Lookup Zones

Zoneهای از نوع Forward امکان ترجمه نام یک کامپیوتر به یک IP را فراهم می‌نمایند. یک Reverse Lookup این امکان را به سرویس گیرندگان خواهد داد که عملیات مخالف عملیات گفته شده را انجام دهند: ترجمه یک آدرس IP به یک نام.

۲۴-۶-۳- تفاوت بین Domain و Zone

Zoneها با دامنه‌ها (Domain) یکسان نبوده و یک Zone می‌تواند شامل رکورد هایی در رابطه با چندین دامنه باشد. یعنی می‌تواند اطلاعات تبدیل آدرس چندین دامنه را در یک Zone قرار دارد، اما بهتر است که همیشه هر Zone فقط اطلاعات یک دامنه را نگهداری کند. مثلاً فرض کنید، دامنه www.Microsoft.Com دارای دو زیر دامنه با نام East و West باشد. (East.Microsoft.Com , West.Microsoft.Com). مایکروسافت دارای دامنه اختصاصی msn.Com بوده که خود شامل دارای یک زیر دامنه با نام mail.Microsoft.Com است.



دامنه‌های همجوار و غیر هم جوار در شکل فوق نشان داده شده است. دامنه‌های همجوار همدیگر را حس خواهند کرد (برای یکدیگر ملموس خواهند بود). در رابطه با مثال فوق دامنه‌های موجود در Microsoft.Com، همجوار و دامنه‌های Msn.Com و Microsoft.Com غیر هم جوار هستند.

Zone، بخش خاصی از فضای نام است که دارای Resource Record منحصر به فرد می‌باشد.

۲۴-۶-۴- انواع Zone

۱. **Primary Zone:** که Zone اصلی می‌باشد.
۲. **Secondary Zone:** که یک کپی از Primary Zone می‌باشد.
۳. **Stub Zone:** شامل بخش‌های خاصی از Recordها (بخش خاصی از Primary Zone) می‌باشد.

۲۴-۶-۵- ویژگی‌های یک Zone

هر ناحیه (Zone)، خواه ناحیه‌ای سطح بالا یا ناحیه‌ای سطح پایین (جزء دامنه‌های بالاتر) باشد، دارای تعدادی رکورد منبع (Resource Record) است.

برای یک کامپیوتر متداول ترین رکورد منبع، **آدرس IP** (رکورد نوع A) آن است.

هر رکورد منبع پنج بخش دارد:

Domain_Name – Time_To_Live – Class – Type – Value

- **(Domain_Name)** نام ناحیه‌ای است که این رکورد متعلق به آن است.
- **(Time_To_Live)** دوام و اعتبار رکورد را (بر اساس واحد زمان) مشخص می‌کند.
- **(Class)** برای اطلاعتت اینترنتی این فیلد همیشه IN است.
- **(Type)** نوع رکورد منبع را مشخص می‌کند.
- **(Value)** این فیلد می‌تواند یک عدد، نام ناحیه یا یک رشته متنی باشد.

مهمترین انواع (Type) رکوردهای منبع:

نوع	مفهوم	مقدار
SOA	Start Of Authority	پارامترهای منطقه
A	IP Address Of A Host	عدد صحیح ۳۲ بیتی
MX	Mail Exchange	تقدم دریافت ایمیل
NS	Name Server	نام سرویس دهنده ناحیه
CNAME	Canonical Name	نام ناحیه
PTR	Pointer	نام مستعار برای آدرس IP
HINFO	Host Description	مشخصات CPU و سیستم عامل
TXT	Text	متن تفسیر نشده

از نظر تئوری، برای نگهداری تمام اطلاعات DNS و پاسخ دادن به درخواست‌ها، یک سرویس دهنده DNS کافیست. اما در عمل، بار کاری چنین کامپیوتری آنقدر سنگین خواهد شد که عملاً آن را بلا استفاده می‌کند.

برای اجتناب از چنین وضعیتی، فضای نام DNS به چندین منطقه (Zone) با مرزهای مشخص و غیر مشترک تقسیم می‌شود.

وقتی یک تبدیل کننده می‌خواهد آدرس ناحیه‌ای را بداند، ابتدا درخواست خود را به سرویس دهندههای نام محلی خود می‌دهد.

اگر این ناحیه در محدوده قانونی سرویس دهنده نام مزبور بود، سرویس دهنده نام رکوردهای منبع معتبر را به آن بر می‌گرداند.

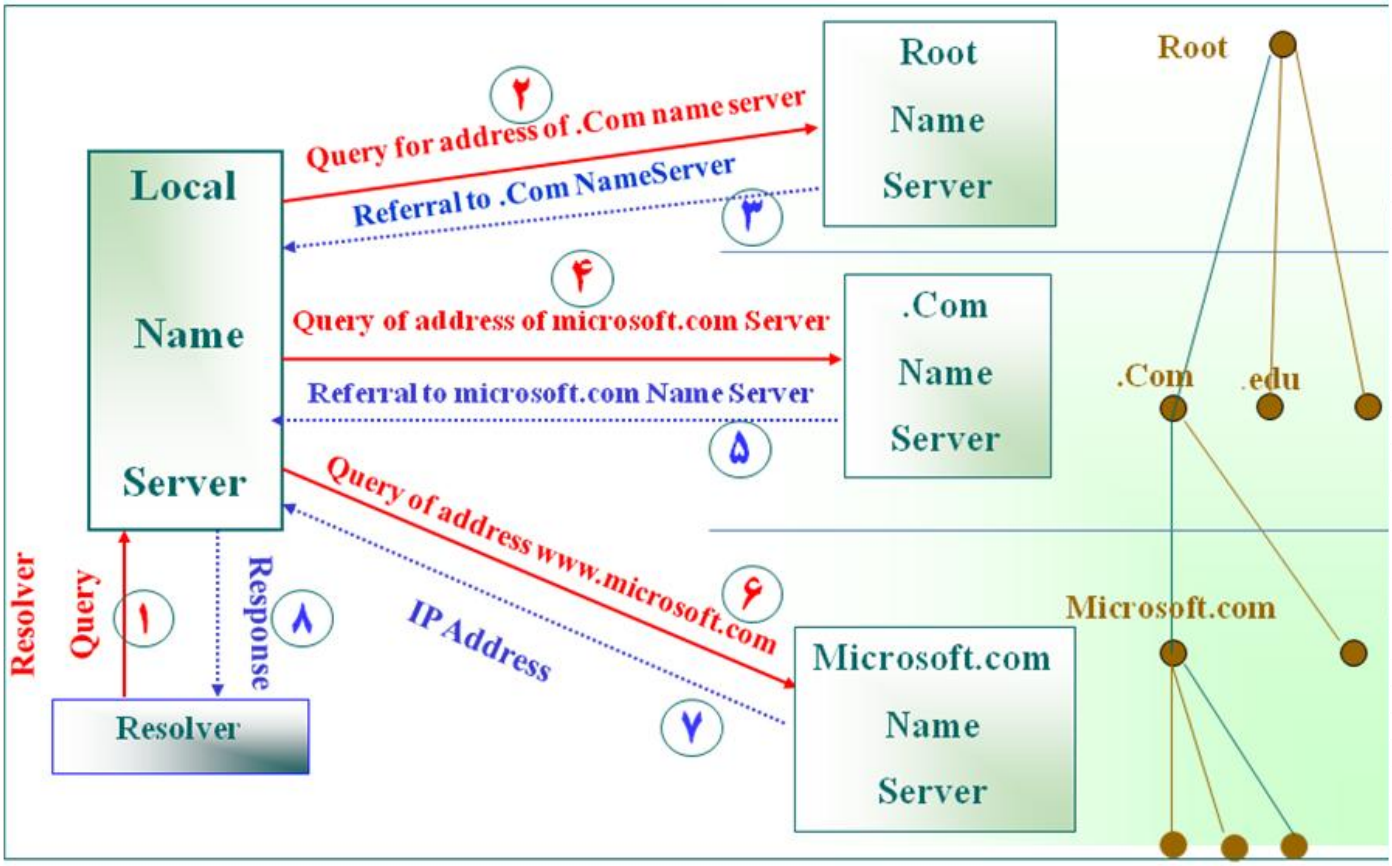
ولی اگر آن ناحیه در قلمرو سرویس دهندههای محلی نباشد، سرویس دهنده نام این درخواست را به سرویس دهنده نام سطح بالای ناحیه مزبور می‌فرستد.

۲۴-۷- انواع روش تبدیل Hostname به IP Address

یک سرویس گیرنده به منظور استفاده از DNS و اخذ پاسخ لازم از دو روش متفاوت استفاده می‌نماید. در مباحث زیر، منظور از کامپیوتر ISP، کامپیوترهای همان شرکتی است که کلاینت اینترنت خود را از آن می‌گیرد. مانند جهان گستر یا جهان روی خط.

۲۴-۷-۱- Non-Recursive Query (تکراری)

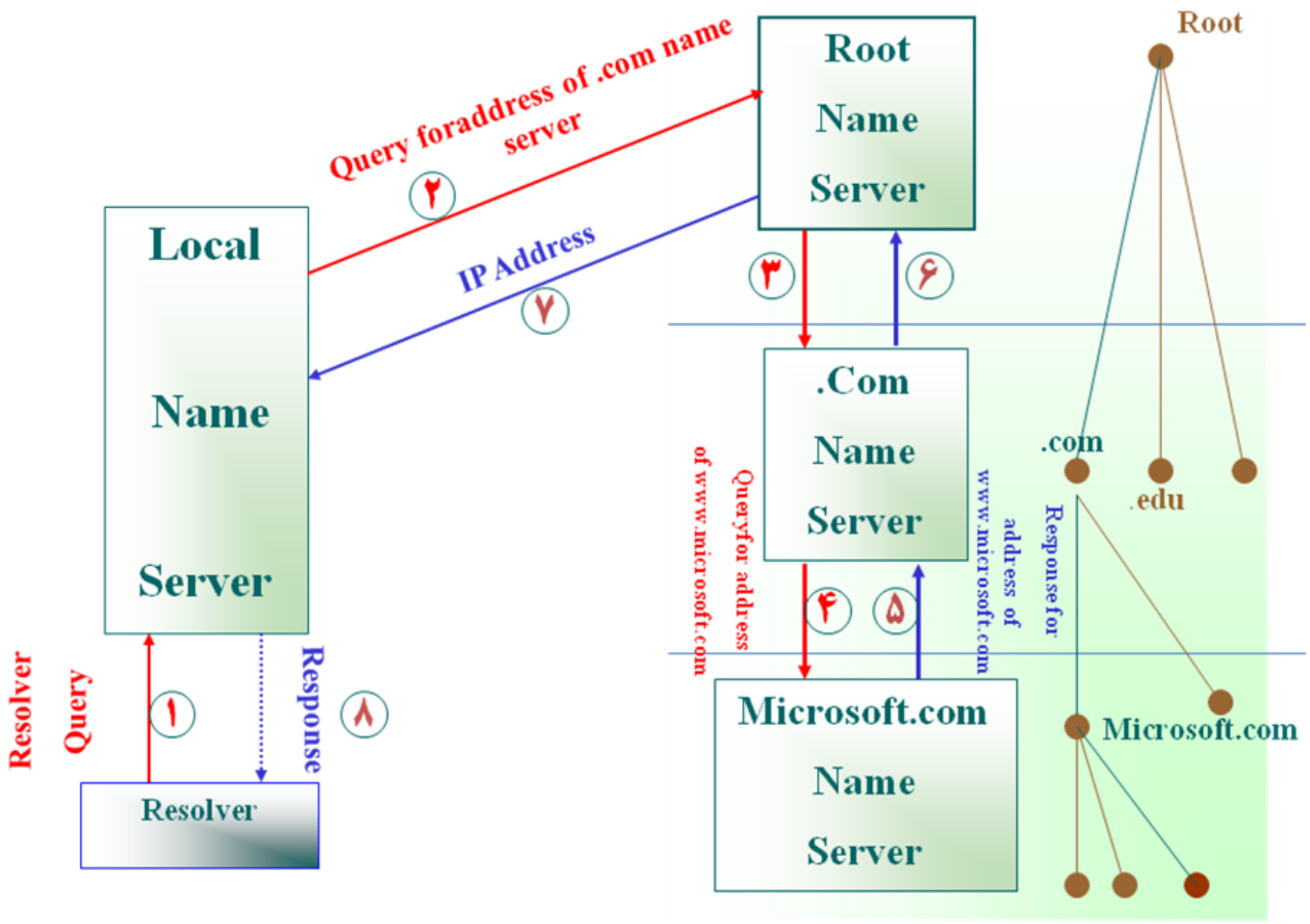
در این روش، کامپیوتر کلاینت، نام سرور مورد نظر را به سرور ISP خود می‌دهد و آدرس IP معادل آن را دریافت می‌کند. در این روش سرویس دهندههای موجود در ISP درگیر جزئیات می‌شوند. خود کامپیوترهای ISP با استفاده از DNS Server خود، از نگهدارندههای آدرس سطح بالاتر، آدرس کامپیوترهای سطح پایین‌تر را می‌پرسند و این کار را تا پیدا کردن آدرس نهایی تکرار می‌کنند. مثلاً برای آدرس www.Microsoft.com، ISP، از نگهدارنده.Com آدرس Microsoft.Com و سپس از Microsoft.Com، آدرس www.Microsoft.com را پرسیده و آدرس نهایی را به کاربر باز می‌گرداند. به عنوان مثالی دیگر، فرض کنید که قصد دارید آدرس Ramezani.ec.iut.ac.ir را به روش Non-Recursive Query (تکراری) استخراج کنید. بدین منظور، ابتدا کامپیوتر کلاینت درخواستی به کامپیوتر ISP داده و کامپیوتر DNS Server موجود در ISP نیز آدرس IP مربوط به DNS Server نگهدارنده آدرس‌های.**ir** را درخواست می‌کند (این سرور Hint Root است). پس از دریافت آدرس سرور نگهدارنده آدرس‌های.ir، مجددا کامپیوتر ISP درخواستی به سرور.ir داده و آدرس IP سرور ac.ir را تقاضا می‌کند. کامپیوتر ISP پس از یافتن آدرس IP مربوط به ac.ir، درخواستی به آن داده و آدرس iut.ac.ir را می‌طلبد. سپس آدرس ec.iut.ac.ir را از iut.ac.ir و آدرس Ramezani.ec.iut.ac.ir را از ec.iut.ac.ir تقاضا می‌کند. پس از پیدا شدن آدرس Ramezani.ec.iut.ac.ir، کامپیوتر ISP، آدرس نهایی را به کامپیوتر کلاینت می‌دهد.



ترجمه www.Microsoft.Com به روش تکراری

۲۴-۷-۲- Recursive Query (بازگشتی)

در این روش، نه کامپیوتر کلاینت و نه کامپیوتر ISP درگیر جزئیات یافتن آدرس IP نمی‌شوند. در این مثال، هر کامپیوتر DNS Serverی، آدرس کامپیوتر زیر مجموعه خود پیدا کرده و آن را بر می‌گرداند. مثلاً برای یافتن آدرس Ramezani.ec.iut.ac.ir، کامپیوتر کلاینت درخواست این آدرس را به ISP می‌دهد و ISP نیز این نام (Ramezani.ec.iut.ac.ir) را به نگهدارنده.ir می‌دهد. سپس نگهدارنده.ir نام را به نگهدارنده ac.ir می‌دهد. ac.ir نیز نام را به iut.ac.ir می‌دهد. iut.ac.ir نیز نام را به ec.iut.ac.ir می‌دهد و از آنجایی که ec.iut.ac.ir آدرس Ramezani را دارد (زیرا زیر مجموعه آن است)، آدرس آن را به iut.ac.ir می‌دهد. iut.ac.ir نیز آدرس را به ac.ir می‌دهد و ac.ir نیز آدرس را به نگهدارنده ir می‌دهد. در نهایت نیز ir آدرس را تحویل ISP داده و ISP نیز آدرس را به کلاینت می‌دهد. شکل زیر همین فرآیند را برای www.Microsoft.Com نشان می‌دهد.



ترجمه www.Microsoft.Com به روش بازگشتی

Cash Server -۸-۲۴

یکی دیگر از اجزای مورد استفاده در DNS، Cash Server می‌باشد که نقش زیادی در افزایش سرعت و کاهش ترافیک شبکه خواهد داشت. Cash Server پاسخ درخواست هایی را که قبلاً توسط DNS Clientها از آن پرسیده شده در حافظه خود نگه می‌دارد. به این ترتیب در صورتی که مجددا نیز به آن داشته باشد لازم به انجام مراحل Resolution نمی‌باشد و می‌تواند بلافاصله IP Address متناظر را برگرداند.

۹-۲۴- پروتکل DNS و مدل مرجع OSI

پروتکل DNS معمولاً از پروتکل UDP به منظور حمل داده استفاده می‌نماید. پروتکل UDP نسبت به TCP دارای سربار کمتری می‌باشد. هر اندازه سربار یک پروتکل کمتر باشد، سرعت آن بیشتر خواهد بود. در مواردی که حمل داده با استفاده از پروتکل UDP با مشکل و یا بهتر بگوئیم خطا مواجه گردد، پروتکل DNS از پروتکل TCP به منظور حمل داده استفاده نموده تا این اطمینان ایجاد گردد که داده به درستی و بدون بروز خطا به مقصد خواهد رسید.

فرآیند ارسال یک درخواست DNS و دریافت پاسخ آن، متناسب با نوع سیستم عامل نصب شده بر روی یک کامپیوتر است. برخی از سیستم‌های عامل اجازه استفاده از پروتکل TCP برای DNS را نداده و صرفاً می‌بایست از پروتکل UDP به

منظور حمل داده استفاده شود. بدیهی است در چنین مواردی همواره این احتمال وجود خواهد داشت که با خطا هایی مواجه شده و عملاً امکان ترجمه نام یک کامپیوتر و یا Domain به آدرس IP وجود نداشته باشد.

پروتکل DNS از پورت ۵۳ به منظور ارائه خدمات خود استفاده می‌نماید. بنابراین یک سرویس دهنده DNS (DNS Server) به پورت ۵۳ گوش داده و این انتظار را خواهد داشت که هر سرویس گیرنده‌ای که تمایل به استفاده از سرویس فوق را دارد از پورت مشابه استفاده نماید. در برخی موارد ممکن است مجبور شویم از پورت دیگری استفاده نماییم. وضعیت فوق به سیستم عامل و سرویس دهنده DNS نصب شده بر روی یک کامپیوتر بستگی دارد.

۲۴-۱۰- ساختار سرویس دهندگان نام دامنه‌ها در اینترنت

یک سرویس دهنده DNS، ضرورتی به آگاهی از تمامی اسامی دامنه‌های ثبت شده نداشته و صرفاً میزان آگاهی وی به یک سطح بالاتر و یک سطح پائین‌تر از خود محدود می‌گردد.

InterNic، مسئولیت کنترل دامنه‌های ریشه را برعهده داشته که شامل تمامی دامنه‌های سطح بالا می‌باشد. در این بخش، تمامی سرویس دهندگان درDNS ریشه قرار داشته و آن‌ها دارای آگاهی لازم در خصوص دامنه‌های موجود در سطح پائین‌تر از خود می‌باشند (مثلاًmicrosoft.Com). سرویس دهندگان DNS ریشه، مشخص خواهند کرد که کدام سرویس دهنده DNS در ارتباط با دامنه‌های.Com و یا.ir می‌باشد.

هر Domain شامل یک Primary DNS و یک Secondary DNS می‌باشد. Primary DNS، تمامی اطلاعات مرتبط با Domain خود را نگهداری می‌نماید. Secondary DNS به منزله یک Backup بوده و در مواردی که Primary DNS با مشکل مواجه می‌شود از آن استفاده می‌گردد (این سرور همان Alternate DNS Server می‌باشد که در مورد آن در بحث تنظیم آدرس IP در فصل دوم صحبت کردیم). به فرآیندی که بر اساس آن یک سرویس دهنده Primary DNS اطلاعات خود را در سرویس دهنده Secondary DNS تکثیر می‌نماید، **Zone Transfer** گفته می‌شود. با توجه به این که هم اینک میلیون‌ها وب سایت وجود دارد و هر روز نیز به تعداد آن‌ها اضافه می‌گردد، عملاً روشی وجود ندارد که بتوان با یک سرویس دهنده DNS، تمامی آدرس‌های IP را در آن ذخیره و این سرویس دهنده نیز قادر باشد به هر درخواستی جهت اتصال به اینترنت پاسخگو باشد. علاوه بر این، ایده استفاده از یک سرویس دهنده متمرکز می‌تواند هدف خوبی برای مهاجمان به منظور از کار انداختن آن باشد.

در مقابل استفاده از یک سرویس دهنده DNS متمرکز، سرویس دهندگان DNS توزیع شده‌اند. بنابراین یک سرویس دهنده DNS دارای تمامی اسامی Hostها و آدرس‌های IP برای تمامی شبکه اینترنت نخواهد بود. سازمان ICANN (برگرفته از Internet Corporation for Assigned Names and Numbers)، مسئولیت ثبت تمامی اسامی دامنه‌ها بر روی اینترنت را برعهده دارد.

مثال:

برای آشنائی با فرآیند یافتن نام یک وب سایت، فرض کنید قصد مشاهده وب سایت http://www.Google.Com را داشته باشیم. پس از تایپ آدرس فوق، مرور گر آدرس درخواستی را برای سرویس دهنده DNS که توسط پیکربندی TCP/IP بر روی کامپیوتر شما مشخص شده است ارسال می‌نماید (هنگام اتصال به اینترنت، بر اساس تنظیمات شرکت

سرویس دهنده اینترنت یا ISP، آدرس DNS Server شما نیز تغییر خواهد نمود). فرض کنید سرویس دهنده DNS شما نسبت به آدرس IP وب سایت فوق آگاهی نداشته باشد. بنابراین آن را برای سرویس دهنده DNS مربوط به ICANN ارسال می‌نماید. DNS فوق آدرس IP وب سایت فوق را نمی‌داند، ولی از آدرس IP سرویس دهنده DNS مرتبط با نام دامنه‌ای که به Com. ختم می‌شود آگاهی دارد. در ادامه، آدرس سرویس دهنده DNS مربوط به دامنه درخواستی (در این مثال Google.Com) برای مرور گر شما ارسال خواهد شد و در نهایت درخواستی برای سرویس دهنده DNS مربوط به دامنه ارسال تا آدرس IP کامپیوتری با نام www مشخص و برای متقاضی بازدید از وب سایت برگردانده شود.

۲۴-۱۱- DNS و WINS (Windows Internet Naming Service)

۲۴-۱۱-۱- DNS

سرویس DNS، توسط کامپیوتر هایی که بر روی آنان یک سرویس دهنده DNS اجراء شده است، ارائه می‌گردد. سیستم‌های عامل ویندوز تقریباً با هر نوع سرویس دهنده DNS استاندارد سازگار می‌باشند. (مثلاً سرویس دهندگانی که بر روی سیستم عامل یونیکس اجراء می‌گردند). ویندوز دارای نسخه اختصاصی خود در رابطه با سرویس دهنده DNS بوده که می‌توان آن را بر روی هر نوع سیستم عامل ویندوز (۲۰۰۳ و یا دات نت)، نصب نمود.

۲۴-۱۱-۲- تفاوت بین DNS و WINS

WINS، به منظور ترجمه اسامی کامپیوترها به آدرس‌های IP، استفاده می‌گردد (دقیقا مانند DNS، اما WINS قدیمی‌تر بوده و با برخی سیستم‌ها سازگاری ندارد). اسامی استفاده شده در WINS، نوع خاصی از نام‌های مبتنی بر ویندوزهای قدیمی (۹x و Me) می‌باشند. DNS، به مراتب متداول‌تر بوده و از آن به منظور ترجمه اسامی میزبان استفاده می‌شود. در محیط ویندوز، تفاوت زیادی بین دو نوع نام (اسامی خاص مبتنی بر ویندوز و اسامی میزبان) وجود نداشته و هر دو نوع، معادل می‌باشند. از نسخه ویندوز ۲۰۰۰ به بعد، تاکید مضاعف بر استفاده از DNS در دستور کار قرار گرفته و مایکروسافت، استفاده محدود و کم رنگ WINS را به عنوان یک سیاست محوری در ویندوز دنبال می‌نماید.

به منظور پیکربندی IP هریک از کامپیوترهای موجود در شبکه، می‌بایست آدرس IP و حداقل یک سرویس دهنده DNS را مشخص کرد. در این رابطه نمی‌توان از نام سرویس دهنده DNS در مقابل آدرس IP، استفاده نمود. (روشی به منظور ترجمه اسامی به آدرس IP بدون یک سرویس دهنده DNS وجود ندارد).

DDNS (DNS پویا)، امکان به هنگام سازی پویای سرویس دهنده DNS را برای کامپیوترها فراهم می‌نماید. بدین ترتیب، بانک اطلاعاتی DNS شامل آخرین اطلاعات مرتبط با آدرس هایIP موجود در شبکه، شده و سرویس دهنده DNS، قادر به ارائه سرویس خود به صورت پویا و متاثر از آخرین تغییرات انجام شده در شبکه، خواهد بود.

به منظور کاهش حجم عملیات مربوط به Name Resolution در یک محیط عملیاتی بزرگ، می‌توان از یک سرویس دهنده ثانویه و یا سرویس دهندگان Caching، استفاده کرد (که قبل‌تر توضیح داده شد). سرویس دهنده ثانویه، دارای بانک اطلاعاتی اختصاصی خود نبوده و از بانک اطلاعاتی DNS موجود بر روی یک سرویس دهنده DNS اولیه، استفاده می‌نماید. سرویس دهندگان ثانویه، گزینه‌ای مناسب برای ارائه خدمات مربوط به Name Resolution بوده ولی قادر به بهنگام سازی پویای DNS نخواهند بود. (برخی از انواع سرویس دهندگان ثانویه قادر به دریافت اطلاعات بهنگام شده و ارسال آنان برای

سرویس دهنده اولیه، می‌باشند). سرویس دهندگان Caching DNS، زمانیکه یک درخواست Name Resolution را دریافت می‌نمایند، با یک سرویس دهنده DNS به منظور اتمام عملیات خود، ارتباط برقرار خواهد کرد. سرویس دهنده Caching، در ادامه آدرس IP را استفاده و آن را به منظور پاسخ به درخواستی مشابه، ذخیره می‌نماید.

۲۴-۱۲- نصب DNS در ویندوز سرور ۲۰۰۳

نرم‌افزار سرویس دهنده DNS ویندوز، امکان ذخیره داده‌های DNS را در یک فایل متنی و یا در اکتیودایرکتوری، فراهم می‌نماید. با انتخاب اکتیو دایرکتوری، دارای گزینه‌ای مبنی بر نصب DNS بر روی هر Domain Controller خواهیم بود. در چنین مواردی در صورت بروز اشکال در اکتیو دایرکتوری، امکان بازیابی سریع اطلاعات وجود خواهد داشت (می توان DNS را بر روی یک Domain Controller دیگر نصب تا زمینه استفاده از اطلاعات DNS موجود در اکتیو دایرکتوری، فراهم گردد).

۲۴-۱۲-۱- تنظیم آدرس IP

قبل از نصب DNS، بایستی تنظیمات TCP/IP را انجام دهیم. اولین کار تنظیم آدرس IP به صورت Static است. البته این کار را می‌توان بعدا نیز انجام داد.

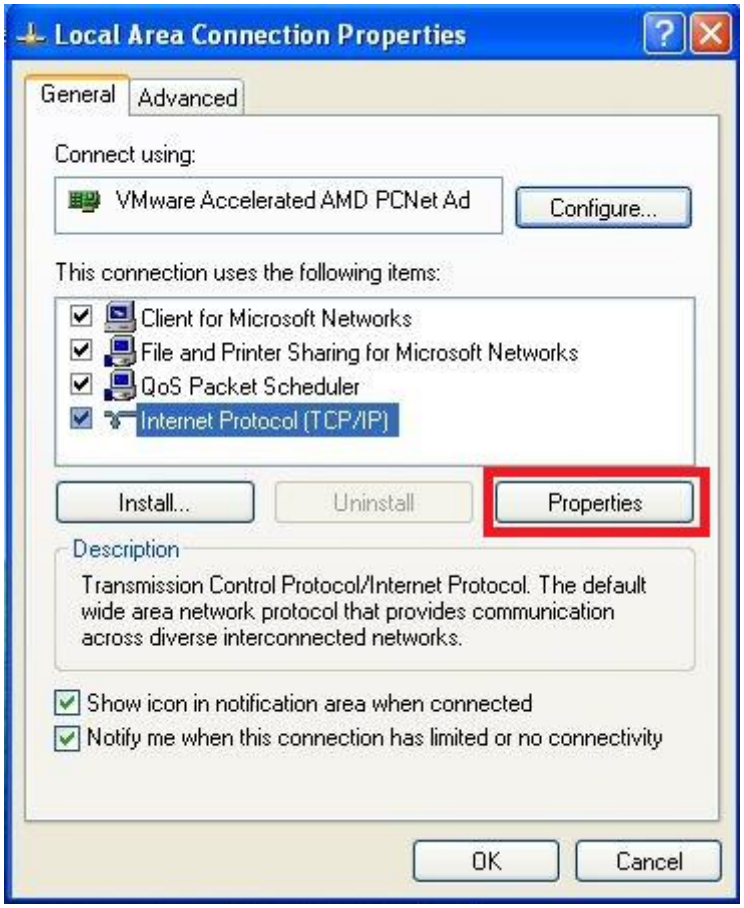
برای انجام تنظیمات IP، وارد مسیر زیر شوید:

Control Panel ➔ Network Connections

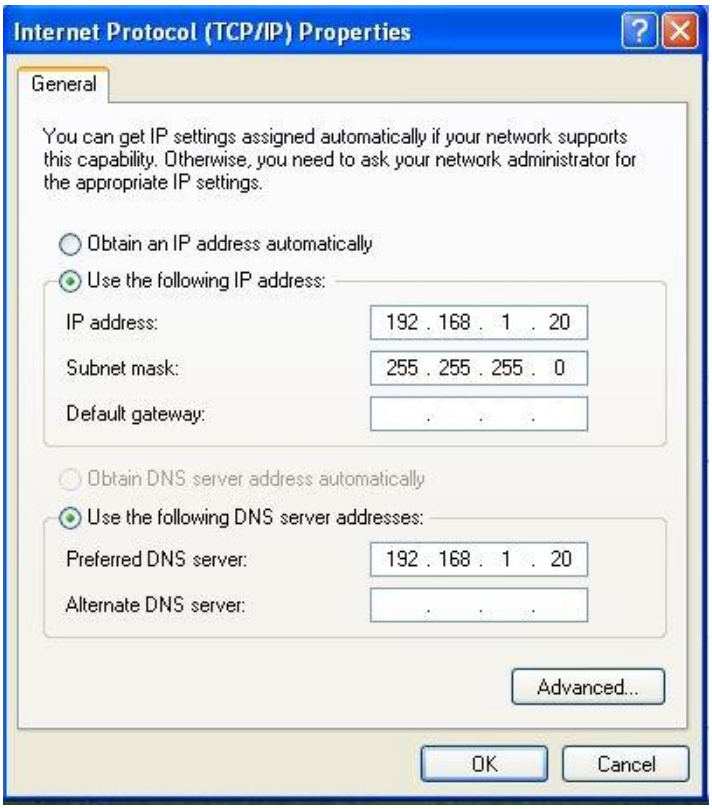
روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.



در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل، آدرس IP را به صورت دستی تنظیم کنید. در قسمت Preferred DNS نیز آدرس DNS Server که نصب کردهاید را وارد نمایید.

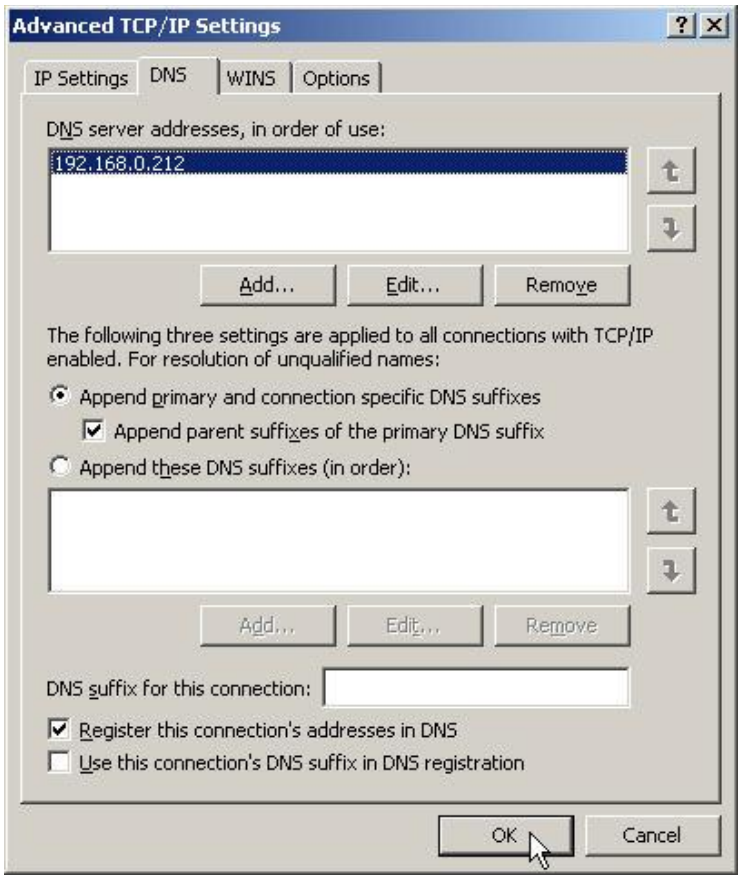


سپس روی دکمه Advanced کلیک کرده و سربرگ DNS را انتخاب کنید. سپس ۳ کار زیر را انجام دهید:

۱- گزینه Append primary and connection specific DNS suffixes را انتخاب کنید.

۲- خانه Append parent suffix of the primary DNS suffix را چک مارک کنید.

۳- خانه Register this connection's address in DNS را نیز چک مارک کنید.



سپس OK کنید تا پنجره بسته شود. حال نوبت به نصب DNS می‌شود.

۲۴-۱۲-۲- نصب DNS از طریق آدرس‌دهی

برای انجام کار به صورت زیر عمل کنید:

Start → Setting → Control Panel → Add/Remove Program →Add/Remove Components →Select Networking Service (do not tick) →Details → Tick DNS (Domain name system) →Ok →Next → Finish

۲۴-۱۲-۳- نصب DNS از طریق شکل

برای انجام کار به صورت زیر عمل کنید:

Start → Administrative Tools → Configure Your Server Wizard



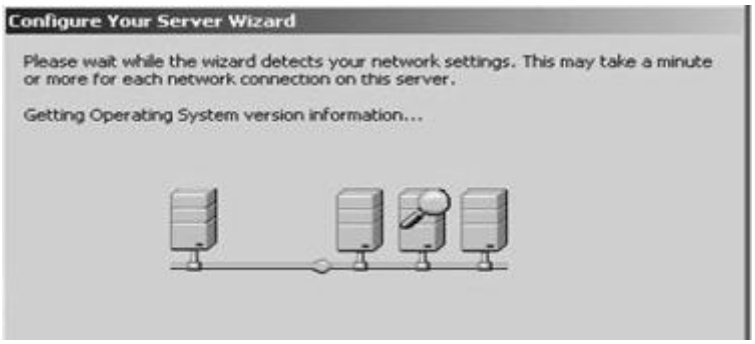
صفحه خوش آمدگویی باز می‌شود. در این صفحه Next بزنید تا به صفحه بعد بروید.



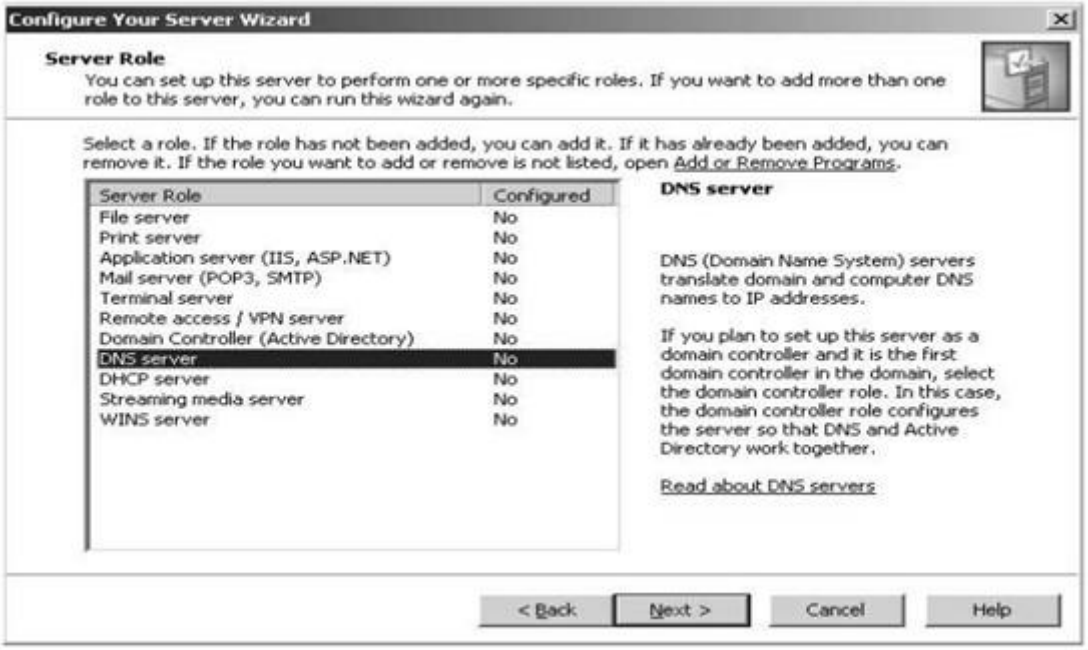
مجددا Next بزنید تا به صفحه بعد بروید.



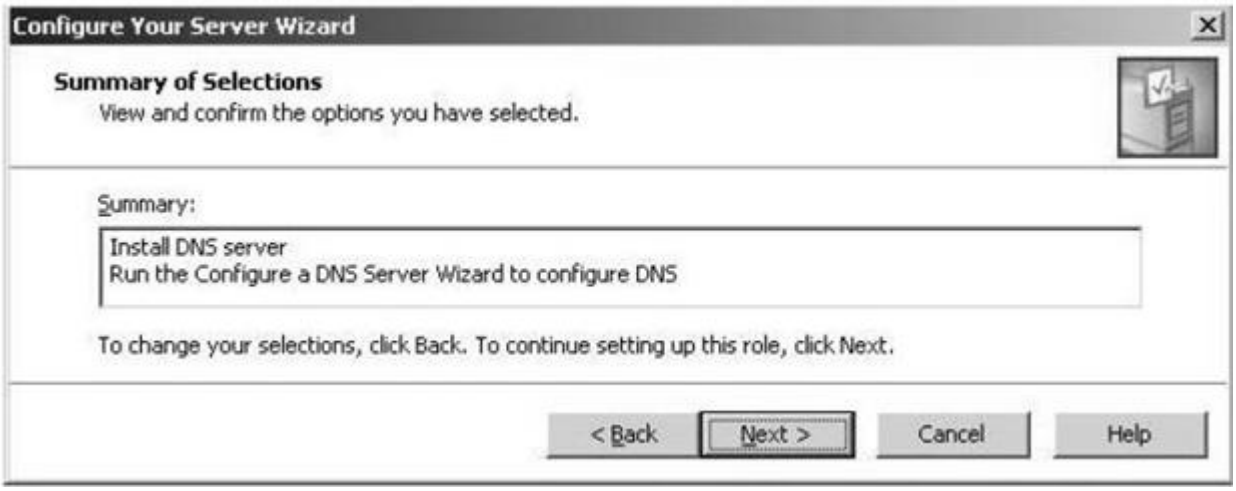
صبر نمایید تا این صفحه بسته شود.



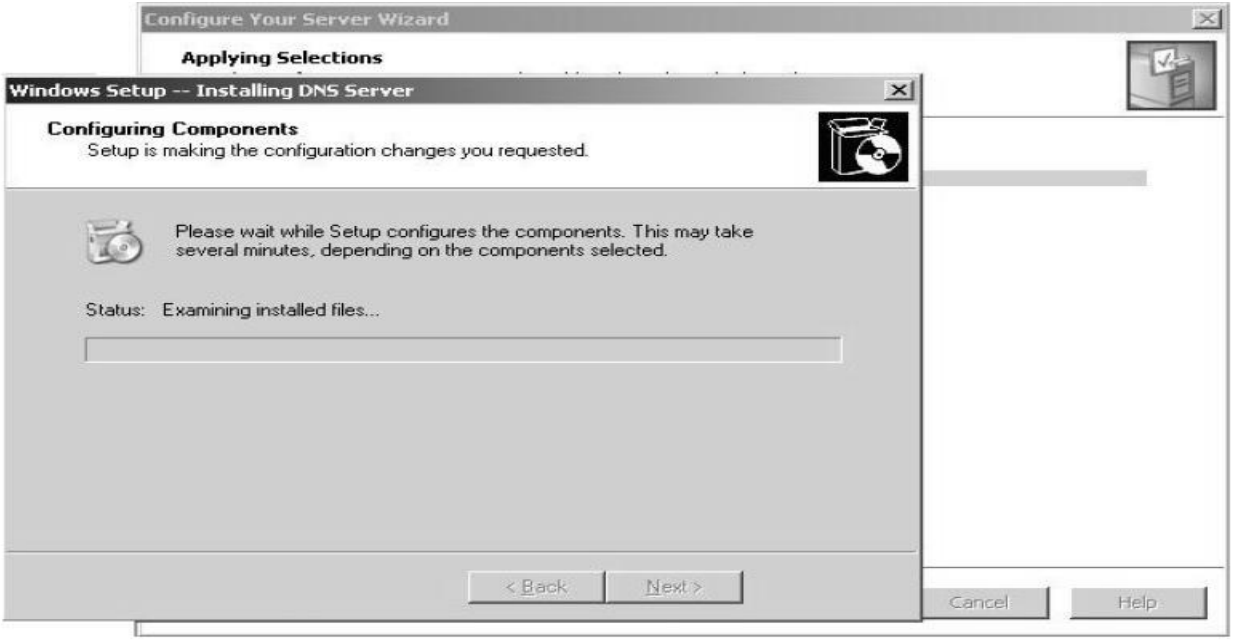
در صفحه باز شده، گزینه DNS را انتخاب نمایید؛ تا سرور شما نقش DNS Server را بپذیرد.



مجددا Next بزنید تا به صفحه بعد بروید.



مدتی صبر نمایید تا سیستم، DNS Server را نصب نماید.



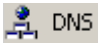
در نهایت روی دکمه Finish کلیک کنید تا عملیات نصب، پایان پذیرد.

بعد از انجام عملیات نصب DNS آن را اجرا می‌کنیم تا از کارکرد درست کابل شبکه اطمینان به عمل آوریم.

۲۴-۱۳- پیکربندی DNS Server

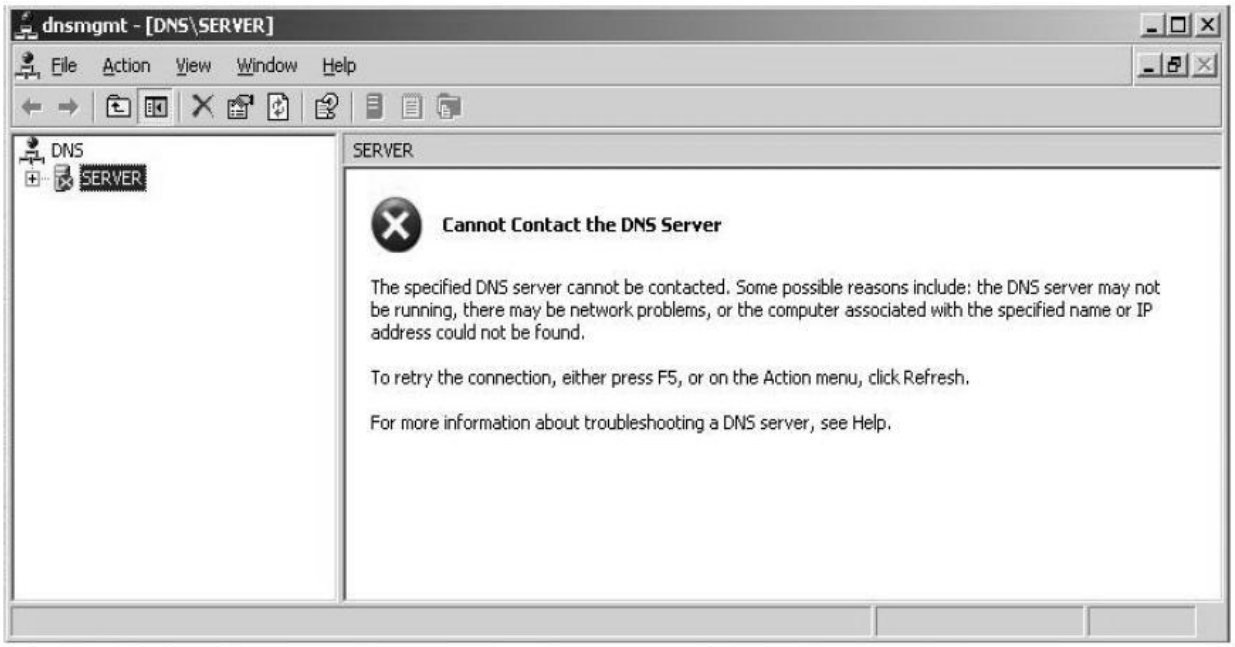
برای پیکربندی DNS Server، مراحل زیر را دنبال نمایید:

Start→Administrative Tools→ DNS



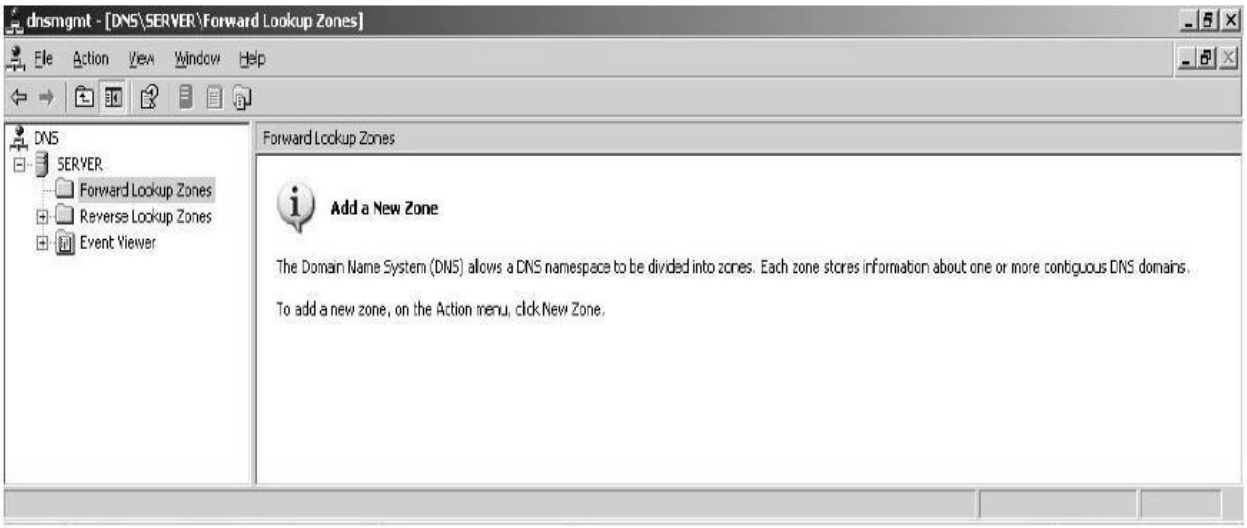
بعد از اجرای DNS دو حالت وجود دارد که به صورت زیر می‌باشند:

اگر شکل DNS – [with problem] را مشاهده کردید در اینصورت از صحت عملکرد کابل شبکه خود اطمینان حاصل فرمایید و یا اینکه کابل شبکه را جدا کرده و آن را مجددا وصل کنید.



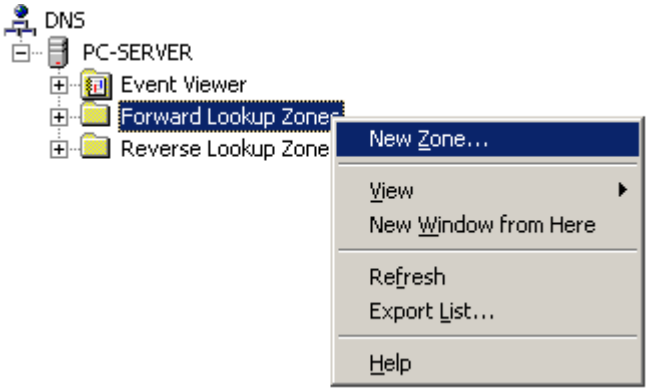
شکل DNS – [with problem]

اگر شکل DNS – [no problem] را مشاهده کردید، در اینصورت در ادامه بحث، همراه ما باشید.

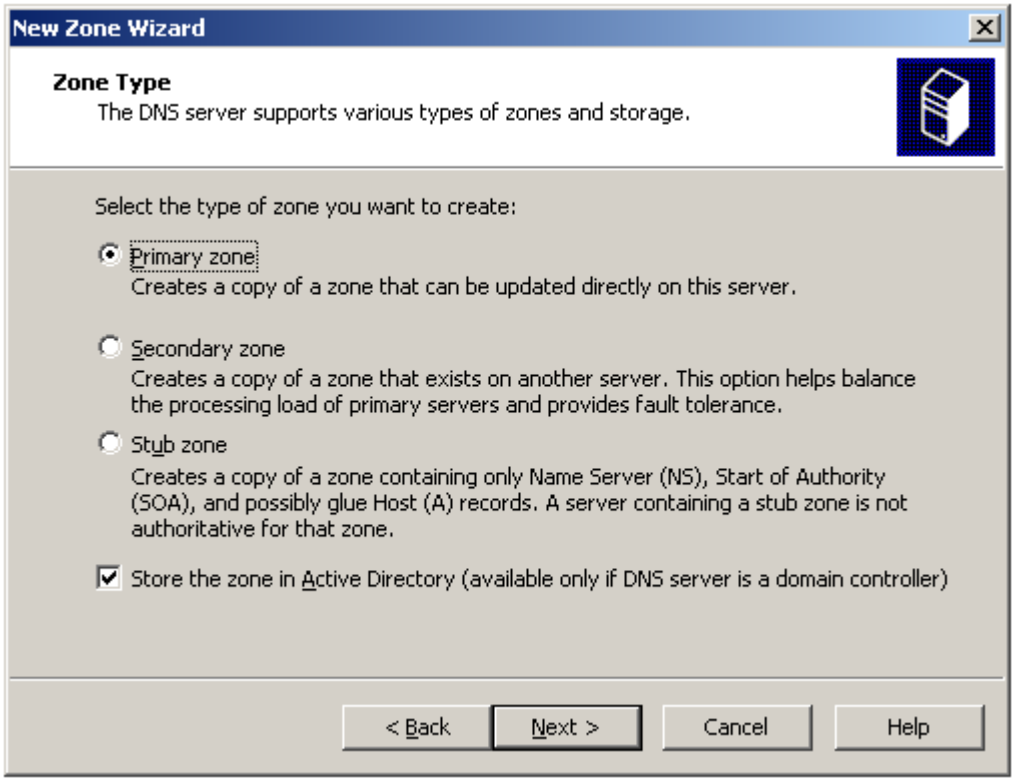


شکل DNS – [no problem]

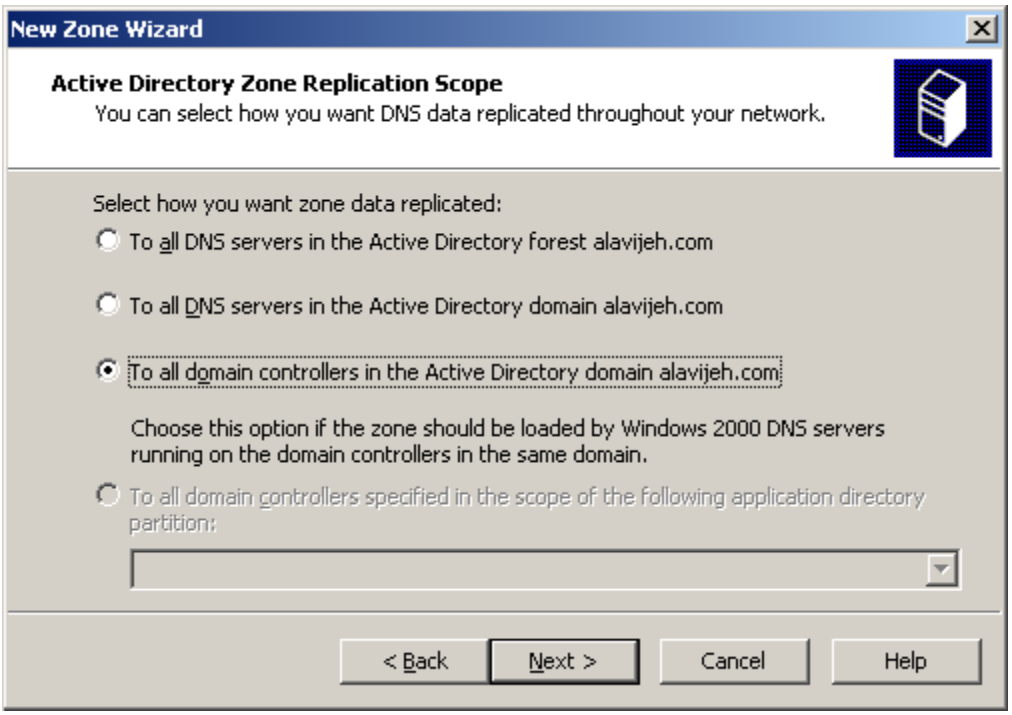
پس از اجرای صحیح، پنجره‌ای ظاهر می‌شود که در قسمت درختی آن نام سرویس دهنده و در زیر آن دو عبارت Forward Lookup Zones (تبدیل Hostname به IP Address) و Reverse Lookup Zones (تبدیل IP Address به Host Name) نمایش داده می‌شود. برروی Forward راست کلیک کرده و گزینه New Zone را انتخاب کنید (Zone محلی برای نگهداری اطلاعات اسامی یک یا چند دامنه یا زیر دامنه است).



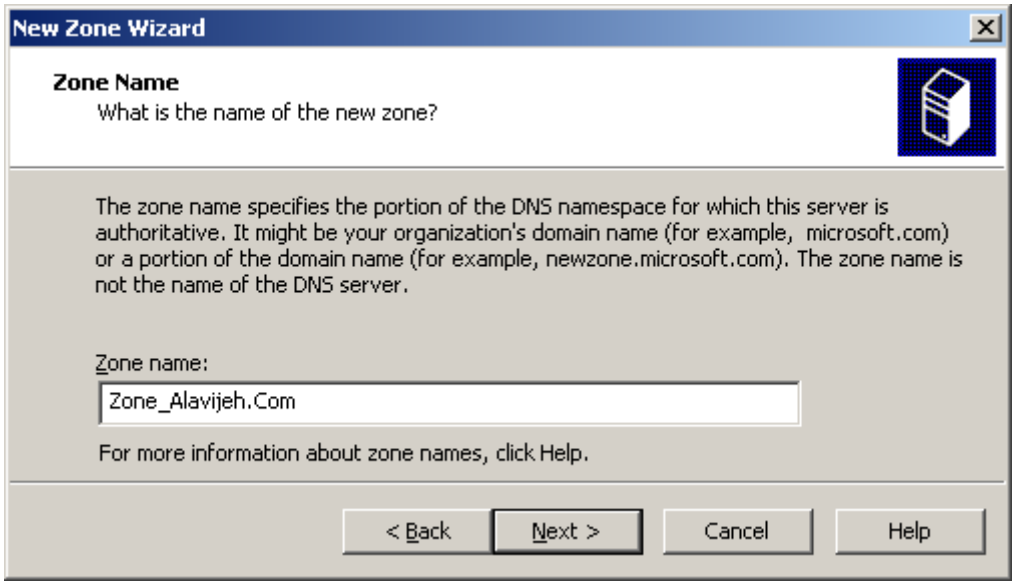
بعد از انجام این کار باید نوع ناحیه را مشخص کنیم، پیش فرض (Standard) را قبول کرده و دکمه Next را بزنید. گزینه Standard Secondary مربوط به Backup DNS و گزینه Stub zone، شامل بخشی از Primary Zone می‌باشد. اگر این اولین Zoneی است که دارید ایجاد می‌کنید، فقط قابلیت انتخاب گزینه Primary zone را دارید.



اگر Active Directory را نصب کرده باشید، صفحه زیر را مشاهده خواهید نمود. گزینه آخر را انتخاب کرده و Next بزنید. این صفحه بیان می‌کند که شما قصد دارید این Zone با کدام قسمت‌ها عمل Replicate را انجام دهد؟



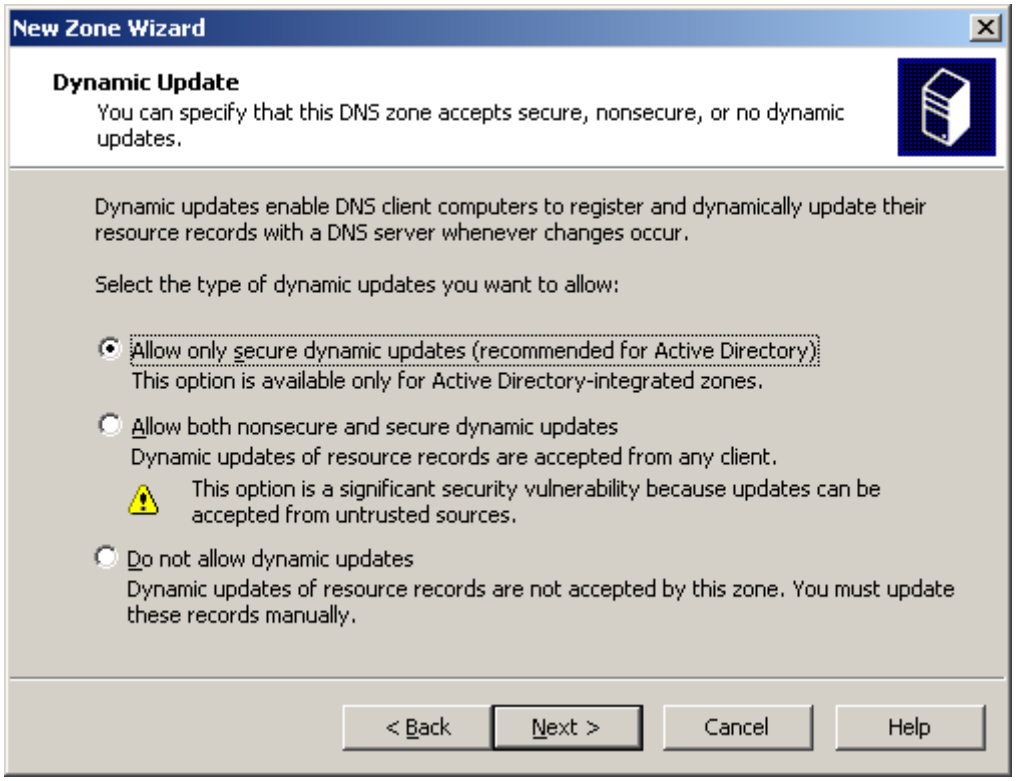
در پنجره بعدی نام Zone خود را وارد کنید، مثلاً Zone_Alavijeh.Com. البته توصیه می‌شود که نام Zone با نام دامنه‌ای که دارید برابر باشد یا بسیار به آن شبیه باشد تا یک دسته بندی منطقی از Zoneها داشته باشید.



در پنجره بعدی، فایل DNS ساخته می‌شود. نام فایل را وارد کرده و Next را بزنید.

:Dynamic Update

به فرآیندی گفته می‌شود که براساس آن Clientها اطلاعات خود را به صورت اتوماتیک درون DNS ثبت می‌کنند. در پنجره بعدی مشخص نمایید که به روز رسانی اطلاعات DNS به چه صورت باشد؟ اگر Active Directory نصب شده باشد، توصیه می‌شود که به روز رسانی امن را انتخاب کنید (گزینه ۱). گزینه دوم عملیات به روز رسانی را هم به صورت امن و هم به صورت نا امن (از منابع تایید نشده) انجام می‌دهد. گزینه سوم نیز به روز رسانی را انجام نمی‌دهد. در نهایت روی Next کلیک کنید.



:Forwarder

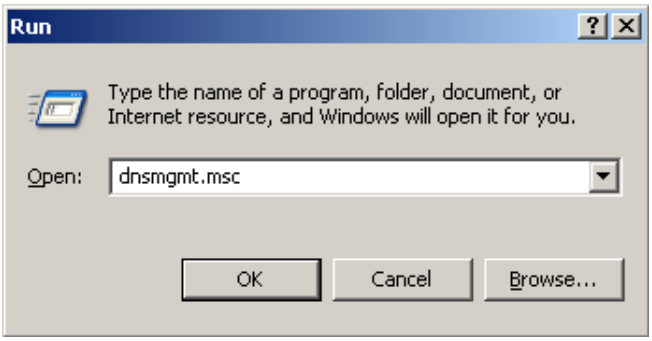
در صورتی که DNS Server موفق به پاسخگویی به Clientها نشود، می‌تواند آن را به یک DNS دیگر که Forwarder نام دارد، بفرستد. در صورتیکه نمی‌خواهید اطلاعات را Forward کنید گزینه دوم یعنی No, it should not forward queries را انتخاب کنید. با انتخاب این گزینه DNS Server جهت عملیات Resolution به Root Serverها مراجعه می‌کند.

برای ادامه کار دکمه Next را بزنید.

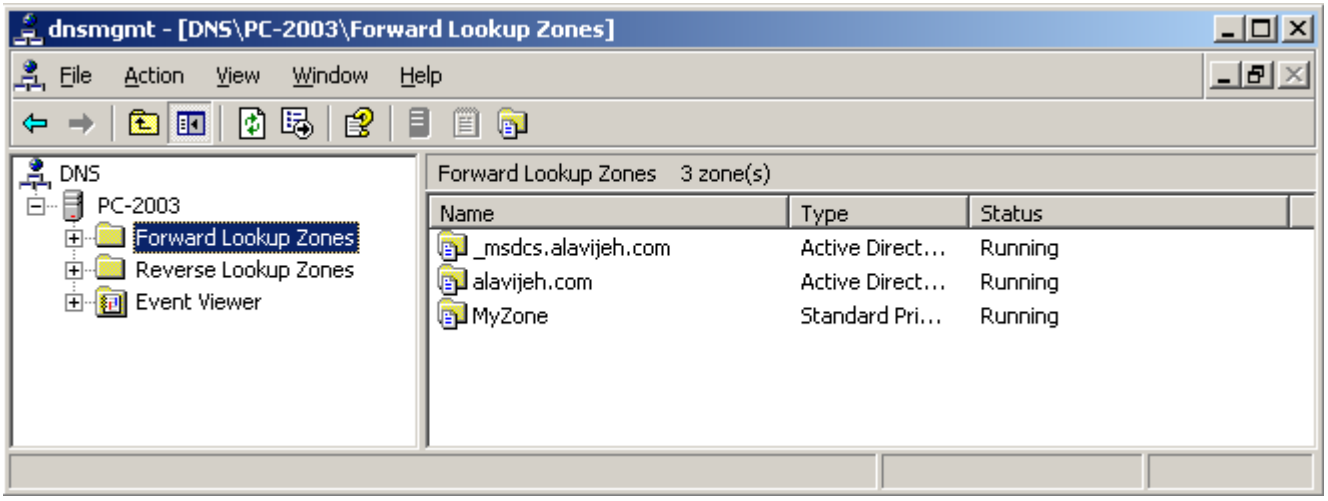
با زدن دکمه Next، DNS Server به دنبال Root Hintهای تعریف شده که در واقع آدرس سرورهای Root می‌باشد، خواهد گشت. در نهایت دکمه Finish را کلیک کنید تا مراحل تکمیل گردد.

۲۴-۱۴- تنظیمات DNS Server

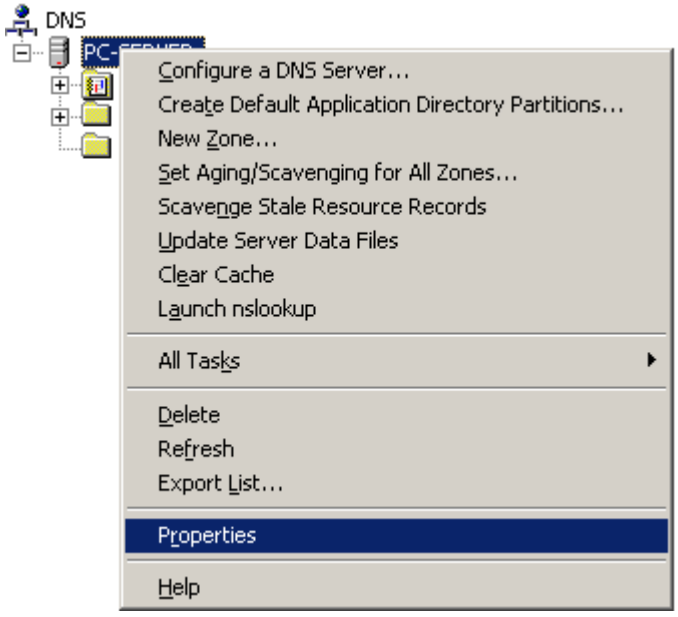
در درون گزینه RUN تایپ کنید: dnsmgmt.Msc، یا از طریق Start➔Administrative Tools➔DNS، صفحه کاربری DNS را باز نمایید.



در پنجره باز شده در سمت چپ یک ساختار درختی شامل نام DNS Server و زیر مجموعه‌های آن یعنی Forward lookup zones، Reverse lookup zones و Event viewer قرار دارد.



بر روی نام سرور راست کلیک کنید و گزینه Properties را انتخاب کنید.



پنجره‌ای شامل چند Tab برای تنظیمات DNS Server باز می‌شود.

از طریق این Tabها می‌توانید تنظیمات مربوط به DNS Server را انجام دهید. توجه نمایید که برخی از این سربرگ‌ها بسیار تخصصی بوده و در موارد و شرایط خاصی استفاده می‌شوند؛ لذا ما نیز آن‌ها را با جزئیات مورد بررسی قرار نمی‌دهیم.

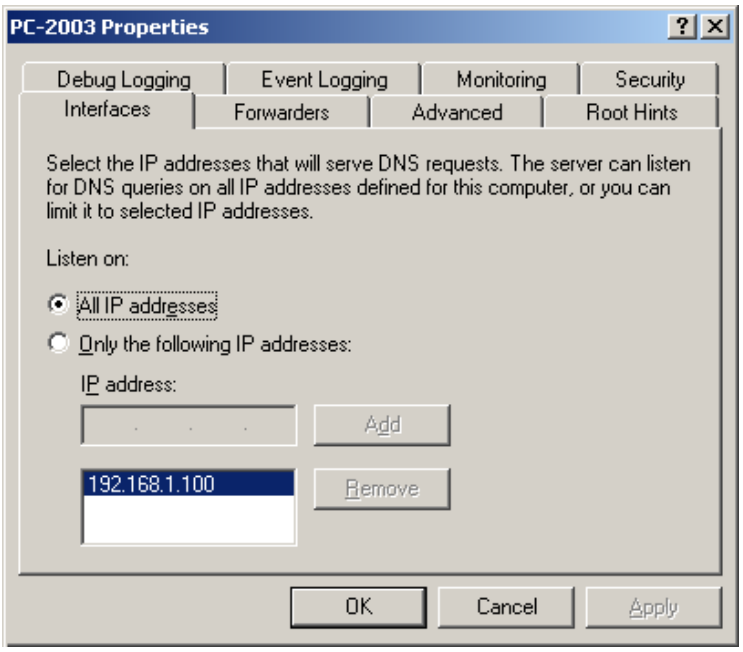
نکته حائز اهمیت این می‌باشد که کار کردن با تنظیمات DNS Server در صورتی مفید خواهد بود که کاربر مفاهیم پایه و اولیه DNS Server، آدرس‌های IP، Address Resolution، سلسله مراتب آدرس‌دهی و آدرس یابی، پروتکل‌های TCP و UDP، فرآیند امنیت و سطوح دسترسی را به خوبی درک کرده و با آن‌ها آشنا باشد.

لذا توصیه اکید بنده، قبل از ورود به تنظیمات DNS Server این می‌باشد که ابتدا حتما با مفاهیم فوق آشنا شده و سپس وارد قسمت تنظیمات DNS Server شوید.

در ادامه، به معرفی سربرگ‌های تنظیمات DNS Server خواهیم پرداخت.

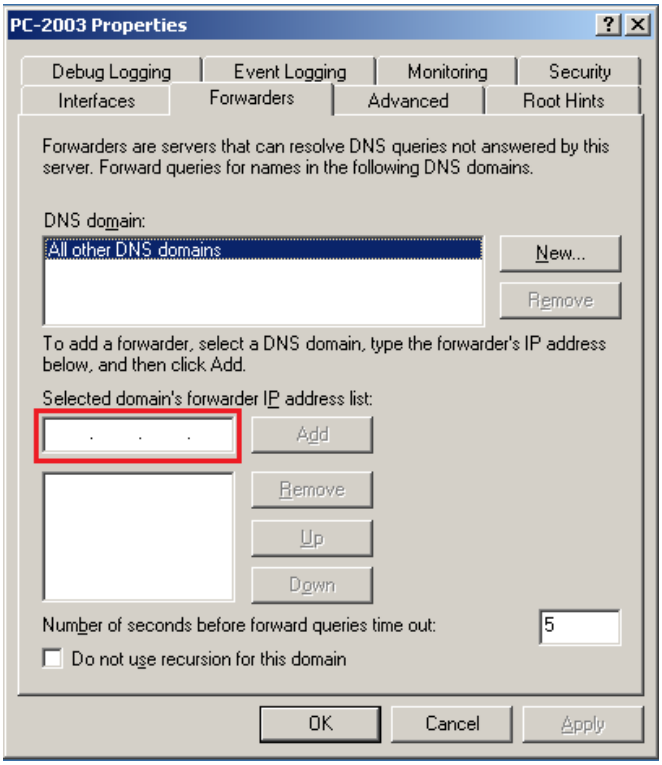
۱- Interfaces

این سربرگ نشان دهنده آدرس IP کارت شبکه‌ای است که این سرور از طریق آن درخواست‌های Clientها را دریافت می‌کند.



۲- Forwards

مشخص کننده آدرس DNS server هایی می‌باشد که در صورتی که این سرور موفق به Resolve، name به IP نشود از آن‌ها به منظور عملیات Resolution کمک می‌گیرد.

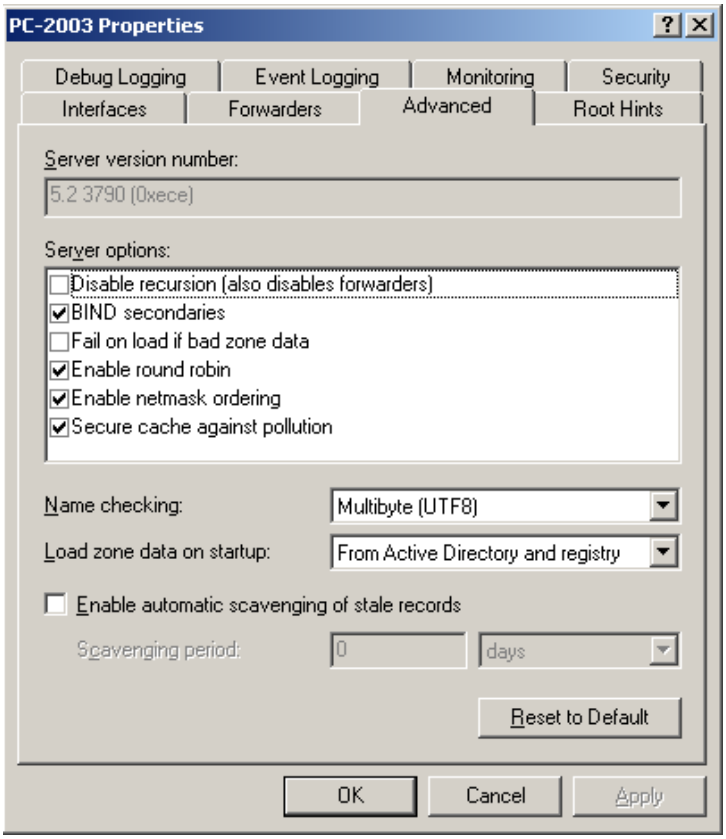


فعال سازی DNS Forwarding برای اتصالات اینترنت

برای این کار، در همین صفحه، در جای مخصوص آدرس IP، آدرس IPمربوط به سرور DNS که قرار است به عنوان ISP ما باشد را وارد کرده و OK را می‌زنیم (قسمت قرمز رنگ تصویر بالا).

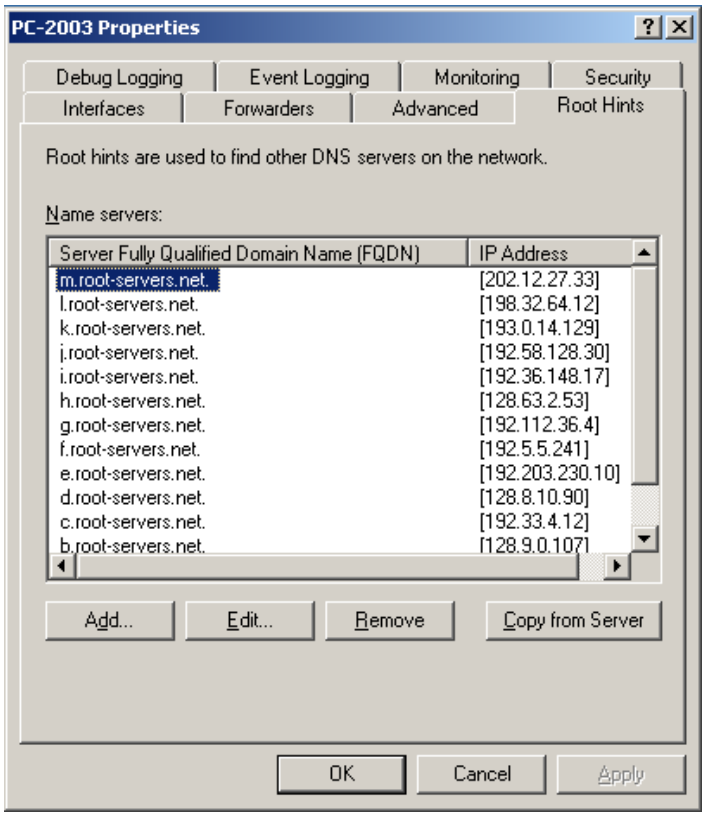
۳- Advanced

حاوی optionهای خاصی در مورد سرور می‌باشد. مثل تنظیمات امنیتی و کنترل بار (Load) زیاد.



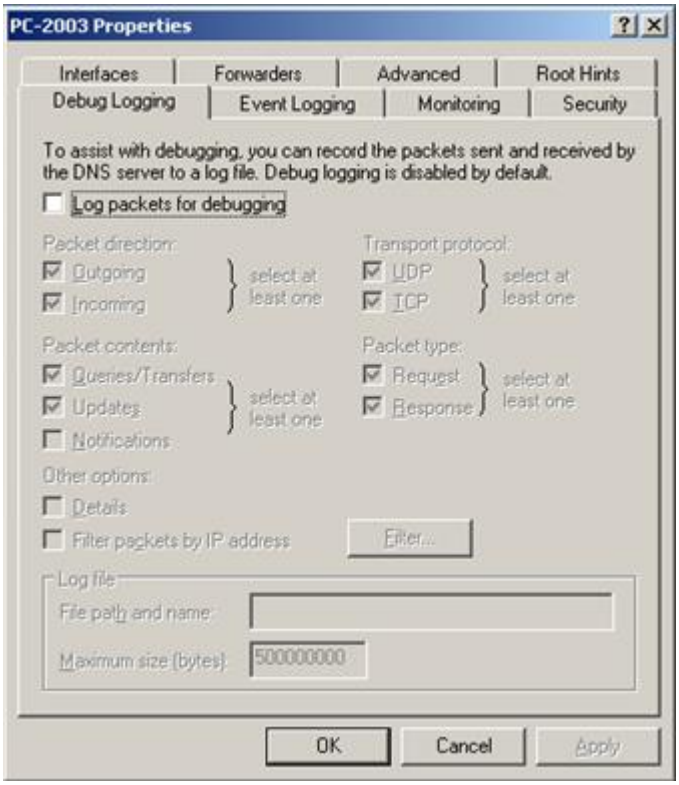
۴- Root hints

آدرس سرورهای Root می‌باشد که به صورت پیش فرض در آن گنجانده شده است ولی می‌توانید آدرس جدیدی نیز به آن اضافه کنید.



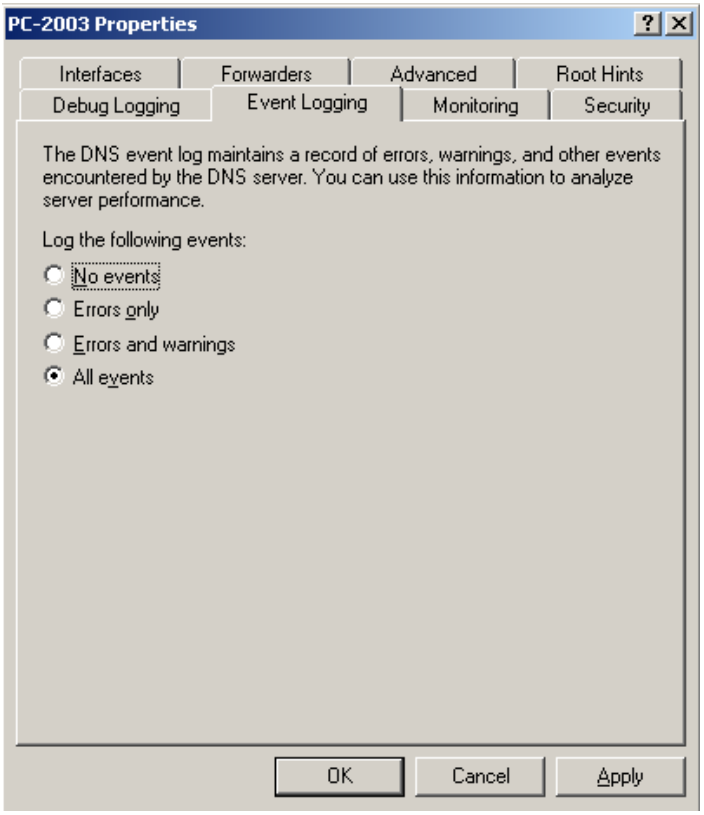
۵- Debug logging

در این سربرگ می‌توانید نوع Packet هایی که می‌خواهید اطلاعات آن‌ها ذخیره شود، مشخص کنید. این اطلاعات درون یک Log file ذخیره می‌شود و به طور پیش فرض این ابزار غیر فعال می‌باشد.



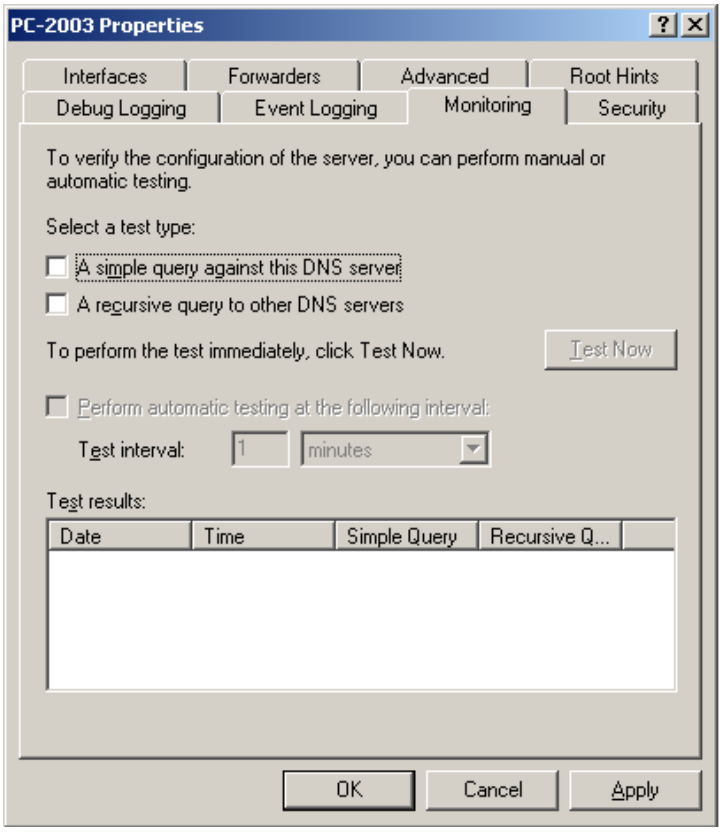
۶- Event logging

در این سربرگ، نوع Event هایی را که می‌خواهید درون Event viewer ذخیره گردند را مشخص کنید.



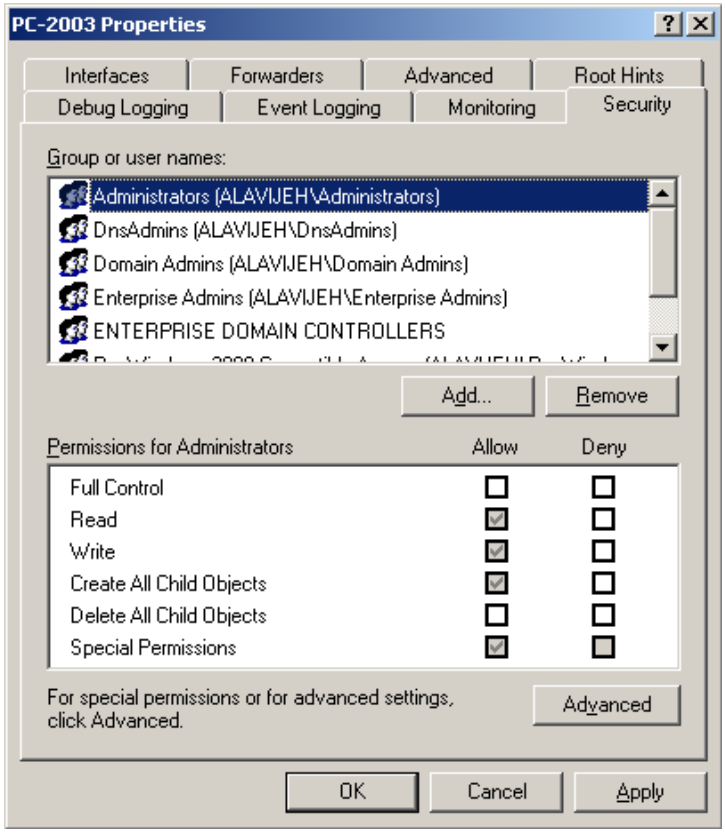
۷- Monitoring

این سربرگ، امکاناتی در جهت تست صحت کارکرد DNS را برای شما فراهم می‌کند.



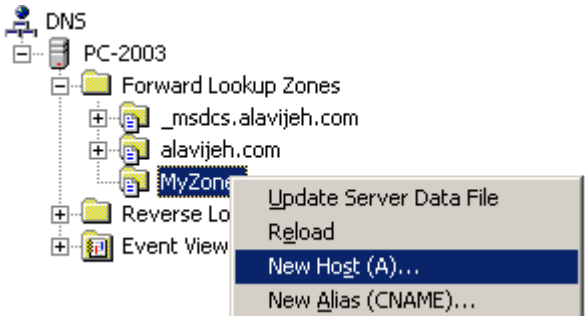
۸- Security

مشخص کننده گروه‌ها و اعضای آن‌ها، از جمله DNS Admin که توانایی ایجاد و اعمال تغییرات در DNS را دارا است، می‌باشد.

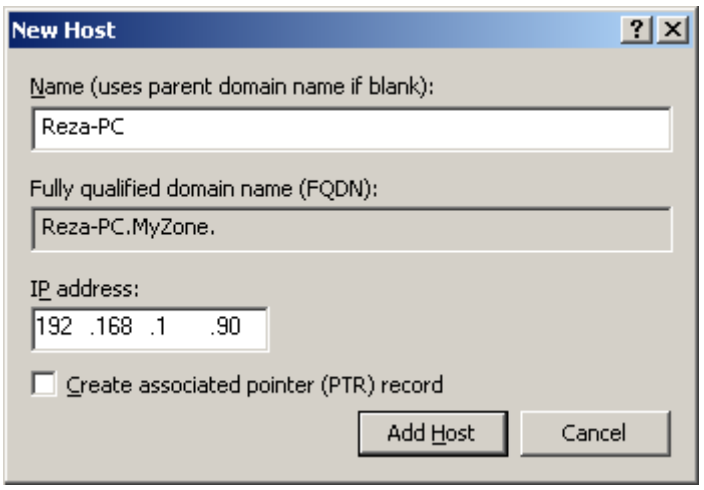


۲۴-۱۵- ایجاد Host جدید

اکنون وقت آن می‌رسد که رکورد جدیدی را تعریف کرده و اطلاعات یک کامپیوتر + آدرس IP آن را وارد نمایید. بدین منظور روی Zone ساخته شده، راست کلیک کرده و گزینه New Host را انتخاب کنید. مطابق شکل، قابلیت تعریف انواع رکورد وجود دارد. انواع رکورد را در ابتدای این فصل معرفی کرده‌ایم. در اینجا قصد داریم رکوردی از نوع A (Hostname ➔ IP Address) بسازیم.



سپس در صفحه باز شده، ابتدا نام کامپیوتر و سپس آدرس IP معادل آن را وارد نمایید. سپس روی دکمه Add Host کلیک کنید.



با این کار، این رکورد به مجموعه اطلاعات DNS Server اضافه خواهد شد.

(same as parent folder)	Start of Authority (SOA)	[1], winserver2003., hostmaster.
(same as parent folder)	Name Server (NS)	winserver2003.
Reza-PC	Host (A)	192.168.1.90

بدین ترتیب هنگامی که نیاز به آدرس کامپیوتر Reza-PC داشته باشید، این DNS Server آدرس ۱۹۲.۱۶۸.۱.۹۰ را باز خواهد گرداند.

۲۴-۱۶- تست کردن DNS Server

پس از نصب DNS Server، نوبت به تست صحت کارکرد آن می‌شود. بدین منظور می‌توانیم از دستورات Ping یا NSLookUP در Command Prompt استفاده کنیم. قبل از استفاده از این دستورات، ارتباط خود را با اینترنت قطع نمایید تا عملیات Name Resolution در داخل شبکه خودتان انجام گیرد. ۱) C:\> **Ping** ComputerName ۲) C:\> **NSLookUP** ComputerName

فصل ۲۵

مفاهیم اولیه در Active Directory

۲۵-۱- آشنایی با زیرساخت‌های Active Directory

یک دایرکتوری (Directory) مجموعه ذخیره شده از اطلاعات درباره‌ی اشیایی است که به نوعی با یکدیگر مرتبط هستند. یک سرویس دایرکتوری (Directory Service) تمامی اطلاعاتی را که برای استفاده و مدیریت این اشیا لازم است، در یک محل متمرکز ذخیره نموده و بدین ترتیب نحوه‌ی یافتن و مدیریت این منابع را تسهیل می‌بخشد. یک Directory Service، زمینه‌ای را فراهم می‌آورد تا دسترسی به منابع در سطح شبکه به بهترین نحو ممکن سازمان یابد. کاربران و مدیران ممکن است که نام دقیق یک شیئ مورد نیاز (مانند چاپگر یا کاربر) را ندانند، اما با دانستن یک یا چند ویژگی از یک شیئ و با استفاده از Directory Service می‌توانند لیستی از اشیاء با ویژگی مورد نظر خود را جستجو کنند.

در این بخش به معرفی سرویس Active Directory پرداخته و به صورت مقدماتی با خصوصیات، اشیا موجود و اجزای آن (فیزیکی و منطقی) آشنا می‌شویم.

۲۵-۲- آشنایی با سرویس دایرکتوری (Active Directory)

Active Directory، یک سرویس دایرکتوری بوده که در Windows Server قرار داده شده است.

Active Directory، شامل یک دایرکتوری بوده که اطلاعات مربوط به شبکه را ذخیره می‌کند، علاوه بر آن دارای تمامی سرویس هایی است که اطلاعات را قابل استفاده کرده و در دسترس قرار می‌دهد.

۲۵-۲-۱- ویژگی‌های Active Directory

۱. ذخیره‌ی متمرکز داده (Centralized data store)

۲. مقیاس پذیری (Scalability)

۳. قابلیت توسعه (Extensibility)

۴. قابلیت مدیریت (Manageability)

۵. استفاده و تمرکز بر سیستم نام گذاری دامنه (Integration with Domain Name System)

۶. مدیریت تنظیمات سرویس گیرنده (Client configuration management)

۷. مدیریت بر مبنای سیاست (Policy-based administration)

۸. تکرار اطلاعات (Replication of information)

۹. شناسایی ایمن و انعطاف پذیر (Flexible, secure authentication and authorization)

۱۰. برنامه‌ها و زیر ساختارهای مبتنی بر دایرکتوری (Directory-enable applications and infrastructures)

۱۱. تطبیق با سایر سرویس‌های دایرکتوری (Interoperability with other directory services)

۱۲. ترافیک رمز گذاری شده و امضا شده (Signed and encrypted LDAP traffic)

۲۵-۲-۲- مزایای *Active Directory*

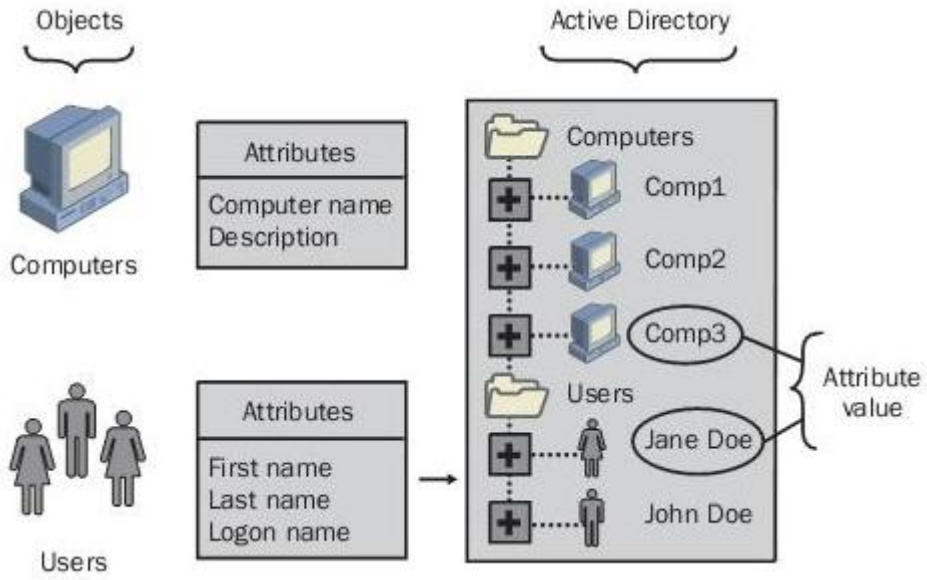
استفاده از Active Directory، دارای مزایای زیر است:

- **کاهش مجموع هزینه مالکیت:** پارامتر فوق به هزینه مالکیت یک کامپیوتر، مرتبط می‌گردد. هزینه فوق شامل: هزینه‌های مربوط به نگهداری، آموزش، پشتیبانی فنی، ارتقاء سخت‌افزار و نرم‌افزار است. Active Directory، با پیاده سازی سیاست‌ها باعث کاهش برخی از هزینه‌های فوق، می‌گردد. بکارگیری یک سیاست به همراه Active Directory، این امکان را فراهم می‌آورد که پیکربندی محیط مربوطه و نصب برنامه‌ها، از یک مکان مرکزی، انجام شود. بدین ترتیب زمان مربوط به پیکربندی و نصب برنامه‌ها بر روی هر کامپیوتر، کاهش پیدا خواهد کرد.
- **مدیریت انعطاف پذیر:** واحدهای سازمانی درون یک Domain را می‌توان بر اساس سیاست‌های موجود در Active Directory، تقسیم نمود. بدین ترتیب، واحدهای سازمانی، امکان تعریف کاربرانی خاص به منظور مدیریت بخش هایی خاص از شبکه را بدست می‌آورند.
- **Scalability:** با استفاده از Active Directory، امکان استفاده از سرویس‌های دایرکتوری برای سازمان هایی با ابعاد متفاوت، فراهم می‌گردد.
- **تسهیل در مدیریت:** Active Directory، ابزارهای مدیریتی خاصی را ارائه که مدیران شبکه، با استفاده از آنان قادر به مدیریت منابع موجود در شبکه خواهند بود.

۲۵-۳- اشیای موجود در Active Directory

هر داده‌ای که در Active Directory ذخیره می‌شود، به صورت اشیایی (Objects) متفاوت، سازمان می‌یابد. یک شیئ مجموعه مجزایی از صفات است که منابع شبکه را مشخص می‌کند. صفات (Attributes)، خصوصیات اشیای موجود در یک دایرکتوری را شامل می‌شود. به عنوان نمونه صفات یک User account)) می‌تواند شامل نام، نام خانوادگی و نام Log on برای آن کاربر باشد. در حالی که صفات یک Computer Account ممکن است که شامل نام و مشخصات آن شیئ باشد.

بعضی از اشیا، که از آن‌ها به نام Container یاد می‌شود، خود دربردارنده اشیایی دیگرند. به عنوان مثال یک Domain، خود یک Container است که می‌تواند شامل اشیایی مانند حساب کاربران و کامپیوترها باشد. در شکل زیر، پوشه‌ی کاربران، یک Container بوده که دارای اشیای مربوط به حساب کاربران است.



اجزای Active Directory

برای ایجاد یک ساختار دایرکتوری، اجزای زیادی مورد نیاز است. این اجزا به دو دسته‌ی منطقی و فیزیکی تقسیم می‌شوند.

۲۵-۳-۱- اجزای منطقی

اجزای منطقی عبارتند از:

۱. دامنه‌ها (Domains)
۲. واحدهای سازمانی (Organizational Units)
۳. درخت‌ها (Trees)
۴. جنگل‌ها (Forests)

۲۵-۳-۲- اجزای فیزیکی

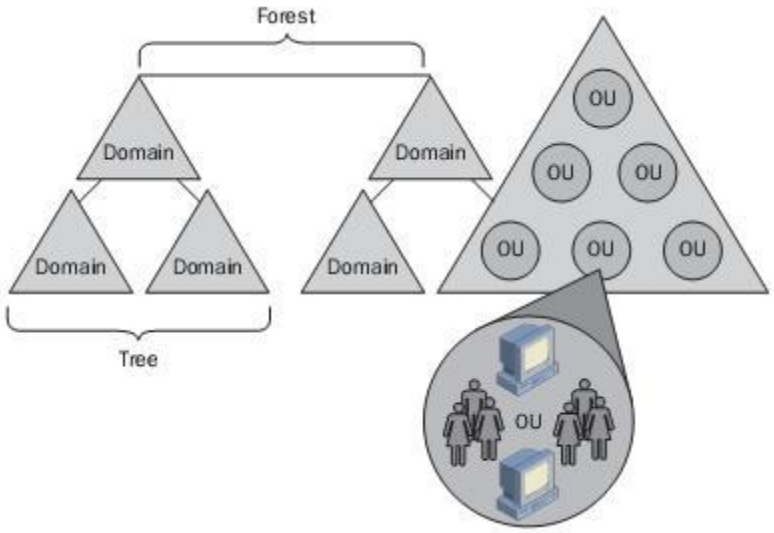
اجزای فیزیکی که ساختار فیزیکی Active Directory را شکل می‌دهند عبارتند از:

۱. سایت‌ها (Physical Subnets)
۲. Domain Controllerها (DC)

۲۵-۴- ساختار منطقی

در Active Directory، می‌توان منابع را به صورت یک ساختار منطقی سازمان داد (ساختاری که منعکس کننده‌ی مدل‌های انتزاعی سازمانی باشد). گروه بندی منطقی منابع این امکان را فراهم می‌آورد تا یک منبع با استفاده از نامش به سادگی

پیدا شود و این امر ما را از یادآوری محل فیزیکی منبع بی نیاز می‌سازد. در شکل زیر رابطه‌ی Domainها، OUها، treeها و Forestها دیده می‌شود.



۲۵-۴-۱- دامنه - Domain

هسته‌ی اصلی ساختار منطقی در Active Directory، Domain یا دامنه بوده که قادر به ذخیره‌ی میلیون‌ها شیئ است. تمامی Domainها در دو ویژگی زیر مشترک‌اند.

اول اینکه تمام اشیای شبکه در یک Domain قرار دارند و دوم اینکه هر Domain اطلاعات مربوط به همان Domain را دارا است.

Domain یک محدوده‌ی امنیتی است. دسترسی به اشیای Domainها از طریق لیست‌های کنترل دسترسی یا ACL (Access Control List)) میسر می‌شود. ACLها شامل مجوز هایی هستند که مرتبط با اشیای مورد نظر است. این مجوزها بیان می‌کنند که کدام یک از کاربران می‌توانند به یک شی دسترسی داشته باشند و این دسترسی از چه نوع و در چه سطحی است. در خانواده‌ی Windows Server، اشیاء شامل فایل‌ها، پوشه‌ها، اشتراکات، چاپگرها و سایر اشیای Active Directory است. این نکته می‌بایست در نظر گرفته شود که هیچ یک از تنظیمات و سیاست‌های امنیتی مانند اختیارات مدیریتی، سیاست‌های امنیتی و ACLها نمی‌توانند از یک Domain به Domain دیگر تغییر یابند. این امر بدان معنا است که یک مدیر در سطح یک Domain تنها دارای اختیاراتی است که وی را محدود به وضع سیاست‌ها در همان Domain می‌کند.

سطح عملیاتی دامنه (Domain Functional Level) که تحت عنوان حالت دامنه (Domain Mode) در Windows 2003 شناخته می‌شود، ویژگی‌های خاصی را در پهنه دامنه (Domain-Wide) و در محیط شبکه فراهم می‌آورد.

چهار سطح عملیاتی دامنه وجود دارد:

۱. **Windows 2000 Mixed**
۲. **Windows 2000 Native**
۳. **Windows 2003 Interim**
۴. **Windows Server 2003**

سطح عملیاتی "**Windows 2000 Mixed**" به یک Domain Controller (DC) با سیستم عامل Windows Server 2003 اجازه می‌دهد تا با سایر DCها در همان Domain که دارای سیستم عامل‌های Windows NT4، Windows 2000 و Windows server 2003 هستند ارتباط داشته باشند.

سطح عملیاتی "**Windows 2000 Native**"، تنها امکان ارتباط DCهای Windows 2003 با Windows 2000 را فراهم می‌آورد.

سطح عملیاتی "**Windows 2003 Interim**" ارتباط DCهای Windows Server 2003 با DCهای NT4 را ممکن می‌سازد.

سطح عملیاتی "**Windows Server 2003**" تنها DCهای ویندوز سرور ۲۰۰۳ را با یکدیگر مرتبط می‌سازد.

تنها در زمانی می‌توان سطح عملیاتی یک Domain را بالا برد که تمامی Domain Controllerها در آن Domain نسخه‌های مناسبی از Windows را اجرا کنند. به عنوان نمونه اگر سطح عملیاتی Domain به صورت " Windows Server 2003" باشد، در این صورت می‌بایست که تمامی DCها در این Domain دارای سیستم عامل Windows Server 2003 باشند.

ویژگی‌های یک Domain

Domain، یک گروه بندی منطقی از کامپیوترهای شبکه‌ای است که از یک محل مشترک به منظور ذخیره سازی اطلاعات امنیتی، استفاده می‌نمایند. استفاده از Domain، تمرکز در مدیریت منابع شبکه را بدنبال خواهد داشت. بدین ترتیب پس از ورود کاربران به شبکه و تائید صلاحیت آنان، زمینه استفاده از منابع به اشتراک گذاشته شده در سایر کامپیوترهای موجود در Domain، با توجه به مجوزهای تعریف شده، فراهم می‌گردد. Domain، در مفهوم مشابه Workgroup بوده ولی امکانات و ویژگی‌های بمراتب بیشتر و مفید تری را ارائه می‌نماید:

- **Single logon:** با استفاده از Domain، فرآیند ورود به شبکه صرفاً یک مرتبه انجام و کاربران قادر به استفاده از منابع متفاوت موجود در شبکه شامل: فایل‌ها، چاپگرها و برنامه‌ها، خواهند بود. Account مربوط به تمامی کاربران در یک مکان متمرکز، ذخیره می‌گردد.
- **Single User Account:** کاربران یک Domain، صرفاً از یک Account به منظور دستیابی به منابع موجود بر روی کامپیوترها، استفاده خواهند کرد (بر خلاف Workgroup که نیازمند یک account مجزا به منظور دستیابی به هر یک از کامپیوترها است).
- **مدیریت متمرکز:** با استفاده از Domain، امکان مدیریت متمرکز فراهم خواهد شد. Account مربوط به کاربران و منابع اطلاعاتی موجود، از طریق یک نقطه متمرکز، مدیریت خواهد شد.
- **Scalability:** استفاده از Domain، امکان گسترش و توسعه در شبکه را افزایش خواهد داد. روش دستیابی کاربران به منابع و نحوه مدیریت منابع در یک شبکه بسیار بزرگ مشابه یک شبکه کوچک خواهد بود.

مزایای استفاده از Domain

استفاده از Domain، دارای مزایای زیر است:

- **سازماندهی اشیاء:** اشیاء موجود در یک Domain را می‌توان بر اساس واحدهای موجود در یک سازمان، سازماندهی نمود. یک واحد سازماندهی شده شامل مجموعه‌ای از اشیاء در یک Domain است. اشیاء، نشان دهنده عناصر فیزیکی موجود در یک شبکه بوده و می‌توانند به یک و یا بیش از یک Domain مرتبط گردند. کاربران، گروه هایی از کاربران، کامپیوترها، برنامه‌ها، سرویس‌ها، فایل‌ها و لیست‌های توزیع شده نمونه هایی در این زمینه می‌باشند. مثلاً یک Domain در شبکه مربوط به یک سازمان، می‌تواند به منظور تسهیل در مدیریت منابع موجود در شبکه، منابع هر یک از دپارتمآن‌های موجود در سازمان را در یک واحد، سازماندهی نماید. هر واحد، می‌تواند توسط کاربران خاصی در دپارتمان مربوطه مدیریت گردد. بدین ترتیب مدیر شبکه قادر به مدیریت گروه هایی از واحدها در مقابل منابع انفرادی، خواهد بود.
- **مکان یابی آسان اطلاعات:** به موازات نشر (تعریف و پیکربندی) یک منبع، امکان دستیابی آن از طریق لیستی از اشیاء یک Domain، برای کاربران فراهم و بدین ترتیب مکان یابی یک منبع به سادگی انجام و زمینه استفاده از آن فراهم خواهد شد. مثلاً در صورتی که چاپگری در یک Domain نصب شده باشد، کاربران قادر به دستیابی به آن از طریق لیستی از اشیاء موجود در Domain مربوطه خواهند بود. در صورتی که چاپگر در Domain مربوطه تعریف نشده باشد، کاربران شبکه جهت استفاده از آن می‌بایست از محل نصب آن آگاهی داشته باشند.
- **دستیابی آسان و موثر:** تعریف و بکارگیری یک سیاست گروهی در ارتباط با یک Domain، نحوه دستیابی کاربران به منابع تعریف شده در Domain را مشخص می‌نماید. بدین ترتیب استفاده از منابع به همراه رویکردهای امنیتی، یکپارچه می‌گردد.
- **تفویض اختیار:** با استفاده از Domain، امکان واگذاری مسئولیت مربوط به مدیریت اشیاء در تمام Domain و یا در بخش هایی خاص، فراهم می‌گردد.

ساختار Domain

هر Domain توسط یک کنترل‌کننده Domain، مدیریت می‌گردد. به منظور تسهیل در مدیریت چندین Domain، می‌توان Domainها را در ساختار هایی با نام درخت (Tree) و جنگل (Forest)، گروه بندی کرد.

کنترل‌کننده دامنه (DC)

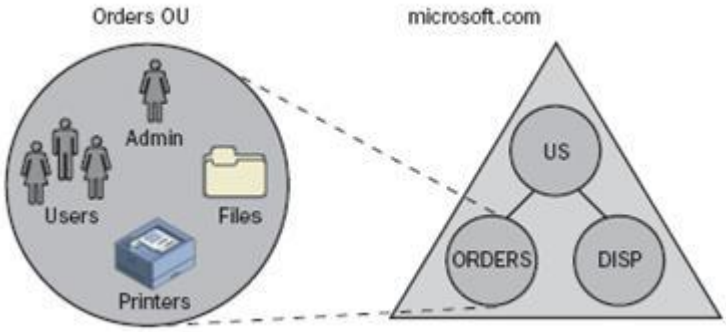
کامپیوتری که برروی آن سرویس دهنده ویندوز سرور اجراء و مدیریت Domain را برعهده می‌گیرد، کنترل‌کننده Domain نامیده می‌شود. کنترل‌کننده Domain، تمام عملیاتی امنیتی مرتبط با کاربران و Domain را مدیریت می‌نماید.

۲۵-۴-۲- واحدهای سازمانی - OUs (Organization Units)

OU خود یک Container بوده که اشیای یک دامنه (Domain) را در گروه‌های مدیریتی سازمان دهی می‌کند. یک OU برای اعمال و اجرای وظایف مدیریتی (مانند مدیریت منابع و کاربران) به کار رفته و می‌تواند شامل اشیایی مانند حساب‌های کاربران، گروه‌ها، کامپیوترها، چاپگرها، برنامه‌ها، فایل‌های به اشتراک گذاشته شده و حتی سایر OUها از همان Domain باشد. ساختار سلسله مراتبی یک OU در یک Domain، مستقل از ساختار سلسله مراتبی OU درDomainهای دیگر است. می‌توان با اضافه کردن یک OU در داخل OU دیگر (Nesting)، مدیریتی سلسله مراتبی را سازمان داد. در

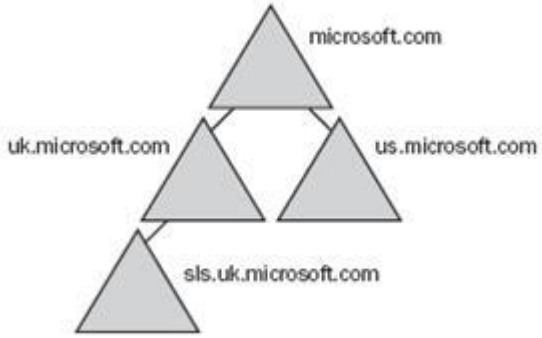
شکل زیر، Domain با نام Microsoft.com منعکس کننده‌ی سازمانی بوده که دارای سه واحد سازمانی است: US، Orders و Disp.

Orders و Disp در واحد سازمانی US آشیآن‌های شده‌اند. به صورت پیش فرض تمامی اشیای فرزند (OUهای Disp و Order) مجوزهای خود را از والدین به ارث می‌برند (US OU). ایجاد مجوز در سطوح بالاتر و استفاده از امکانات وراثت، وظایف مدیریتی را کاهش می‌دهد.



۲۵-۴-۳- درخت‌ها - Trees

یک درخت (Tree)، سازمان دهی یا گروه بندی منطقی یک یا چند دامنه بوده که از طریق ایجاد یا اضافه کردن چند دامنه‌ی فرزند (Child Domain) به دامنه‌ی پدر (Parent Domain) فعلی به وجود می‌آید. دامنه‌ها در یک درخت، دارای یک فضای اسمی (Contiguous Namespace) یا ساختار نامی سلسله مراتبی مشترک هستند. بر اساس استانداردهای DNS، نام یک دامنه‌ی فرزند، ترکیبی از نام خود دامنه‌ی فرزند به همراه نام دامنه‌ی پدر است. در شکل زیر، Domain با نام Microsoft.com به عنوان دامنه‌ی والد و Domainهای us.microsoft.com و uk.microsoft.com دامنه‌های فرزند آن هستند. علاوه بر آن خود دامنه‌ی uk.microsoft.com دارای یک دامنه‌ی فرزند با نام sls.uk.microsoft.com است (به روند دنباله دار نام دامنه‌ها دقت کنید).



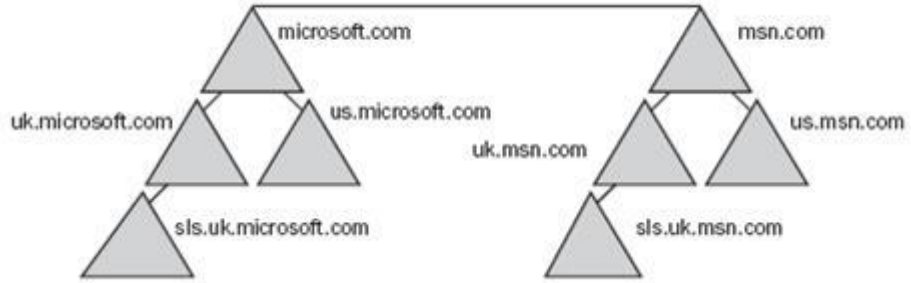
۲۵-۴-۴- جنگل‌ها - Forests

یک جنگل (Forest) دسته بندی یا سازماندهی سلسله مراتبی از یک یا چند درخت (Domain Tree) کاملاً مستقل و مجزا از هم است. یک جنگل دارای ویژگی هایی است:

۱- درخت‌ها در یک جنگل با توجه به دامنه هایشان، دارای ساختار نامی متفاوت هستند.

۲- دامنه‌ها در یک جنگل به صورتی کاملاً مستقل از هم عمل می‌کنند، ولی یک جنگل امکان ارتباط در تمامی سازمان را برقرار می‌سازد.

در شکل زیر دو درخت microsoft.com و msn.com از یک جنگل دیده می‌شوند. می‌توان مشاهده کرد که فضای نامی در هر درخت دنباله دار است.

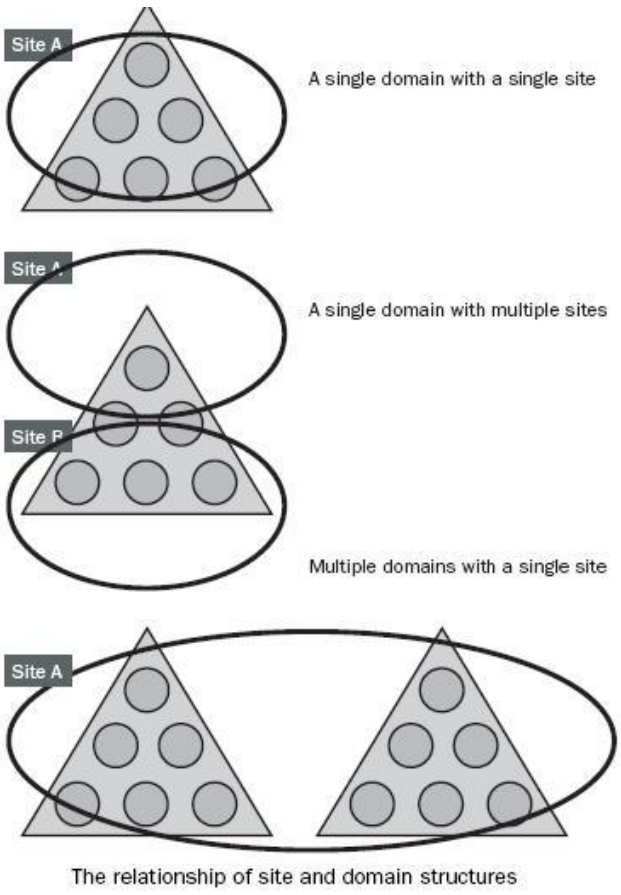


سطح عملیاتی جنگل (Forest Functional Level)، ویژگی‌های خاصی را در سطح جنگل و در محیط شبکه فراهم می‌آورد (Forest-wide Active Directory Features).

۲۵-۵- ساختار فیزیکی

۲۵-۵-۱- سایت‌ها (Sites)

یک سایت اجتماع یک یا چند زیر شبکه IP (Subnet) است که به وسیله‌ی یک اتصال فیزیکی **مطمئن و سریع** به هم مرتبط شده‌اند تا بتوان تا آنجا که ممکن است در جهت بهبود ترافیک شبکه اقدام کرد. سایت‌ها تنها شامل اشیای کامپیوتری و ارتباطی هستند که به منظور تنظیم چگونگی تکرار در سایت (Replication) به کار گرفته شده‌اند. همان گونه که در شکل زیر نشان داده شده است، یک دامنه مجزا می‌تواند شامل یک یا بیش از یک سایت (از لحاظ جغرافیایی) باشد، و یک سایت مجزا می‌تواند شامل حساب‌های کاربران و کامپیوتر هایی باشد که متعلق به چندین دامنه هستند.



The relationship of site and domain structures

۲۵-۵-۲- کنترل کننده دامنه - DC (Domain Controller)

یک Domain Controller، کامپیوتری است که دارای سیستم عامل Windows Server باشد و یک نسخه از دایرکتوری دامنه (Local Domain Database) یا Replica را در خود ذخیره کند. هر دامنه می‌تواند بیش از یک Domain Controller داشته باشد. یک Domain Controller تنها می‌تواند به یک دامنه سرویس دهد. یک DC وظیفه‌ی شناسایی کاربرانی را که تلاش برای Log On به دامنه دارند، را بر عهده دارد. علاوه بر آن سیاست‌های امنیتی برای یک دامنه را نیز تنظیم و حفظ می‌کند.

۲۵-۶- برخی ویژگی‌های Active Directory

در خانواده‌ی ویندوز سرور ۲۰۰۳، با مفاهیم جدیدی در ارتباط با Active Directory روبرو می‌شویم. این مفاهیم شامل موارد زیر است:

۱. تکرار (Replication)
۲. ارتباطات مطمئن (Trust Relationships)
۳. سیاست‌های گروهی (Group Policies)

اکنون به توضیح موارد فوق می‌پردازیم:

۲۵-۶-۱- تکرار یا Replication

کاربران و سرویس‌ها می‌بایست در هر زمانی و از هر کامپیوتری در Domain، به اطلاعات دایرکتوری دسترسی داشته باشند. انعکاس (Replication) این امر را تضمین می‌نماید که هر تغییری در یک Domain controller، در سایر DCها از همان Domain نیز منعکس می‌شود. اطلاعات دایرکتوری در Domain controllerهای داخل و بین سایت‌ها تکرار می‌شود.

چه اطلاعاتی تکرار می‌شود؟

آنچه که در دایرکتوری ذخیره می‌شود (در فایل Ntds.dit) به صورت منطقی به چهار دسته تقسیم می‌شود. به هر یک از این دسته‌های اطلاعاتی، لفظ Directory Partition اطلاق می‌گردد. یک پارتیشن دایرکتوری را با عنوان متن نامی (Naming Context) نیز می‌شناسند. دایرکتوری دارای پارتیشن‌های زیر است:

۱. **Schema Partition:** این پارتیشن اشیایی را مشخص می‌سازد که می‌توانند در دایرکتوری ساخته شوند. علاوه بر آن، این پارتیشن ویژگی‌ها و صفات این اشیا را نیز مشخص می‌سازد. این اطلاعات و داده‌ها در کل یک Forest مشترک بوده و در تمامی DCهای موجود در یک Forest تکرار می‌شود.

۲. **Configuration Partition:** این پارتیشن ساختار منطقی چیدمان Active Directory را بیان می‌دارد و شامل داده هایی درباره‌ی ساختار Domain و یا توپولوژی تکرار است. این داده‌ها نیز در تمامی Domainهای موجود در یک Forest مشترک بوده و در تمامی DCهای موجود در آن جنگل تکرار می‌شوند.

۳. **Domain Partition:** این پارتیشن تمامی اشیای موجود در یک Domain را تعریف می‌کند. این داده‌ها و اطلاعات مخصوص به یک Domain بوده و منحصر به فرد در همان Domain است و بنابراین در دیگر Domainهای موجود در یک Forest تکرار نخواهد شد.

۴. **Application Directory Partition:** این پارتیشن شامل اطلاعات پویای کاربردی است. ذخیره‌ی این اطلاعات در این پارتیشن موجب کنترل حوزه‌ی تکرار و محل نسخه‌های تکرار (Replica) می‌گردد و این امر کوچکترین تأثیر نا مطلوبی در کارآیی شبکه را به دنبال نخواهد داشت. این پارتیشن می‌تواند هر نوع شی را دارا باشد (به غیر از اشیای امنیتی که شامل کاربران گروه‌ها و کامپیوترها می‌باشد.) بدین ترتیب داده می‌تواند به صورتی مشخص به DC هایی هدایت شود که برای کارهای مدیریتی در نظر گرفته شده‌اند و این امر ترافیک غیر ضروری تکرار (Replication) را کاهش می‌دهد.

یک Domain Controller، موارد زیر را ذخیره کرده و تکرار می‌نماید:

۱. داده‌ی موجود در Schema Partition در سطح Forest

۲. داده‌ی موجود در Configuration Partition، به تمامی Domainها در سطح یک Forest

۳. داده‌ی موجود در Domain partition (تمامی اشیای دایرکتوری و مشخصات آن ها) برای همان Domain. این داده‌ها در تمامی Domain Controllerهای اضافی موجود در آن Domain تکرار خواهد شد. به منظور یافتن بهینه‌ی اطلاعات، بخشی از نسخه‌ی تکرار (Replica) که شامل صفاتی از تمام اشیایی است که به صورتی دائمی در

Domain مورد استفاده قرار می‌گیرند، در کاتالوگ سراسری (Global Catalog) نیز تکرار می‌گردد. کاتالوگ سراسری محلی مرکزی برای نگهداری اطلاعات در مورد اشیا در یک درخت یا جنگل است.

یک Global Catalog اطلاعات زیر را ذخیره و تکرار می‌نماید:

۱. داده‌های موجود در Schema Partition برای یک Forest
۲. داده‌های موجود در Configuration Partition برای تمامی Domainها در یک Forest
۳. بخشی از Replica که شامل صفاتی از تمام اشیای دایرکتوری است که معمولاً در یک Forest مورد استفاده قرار می‌گیرند (این اطلاعات تنها بین Global Catalogها تکرار می‌شود).
۴. تمامی Replica که شامل کل صفات تمام اشیای دایرکتوری در Domainهایی است که کاتالوگ سراسری در آن قرار دارد.

اطلاعات چگونه منعکس می‌شود؟

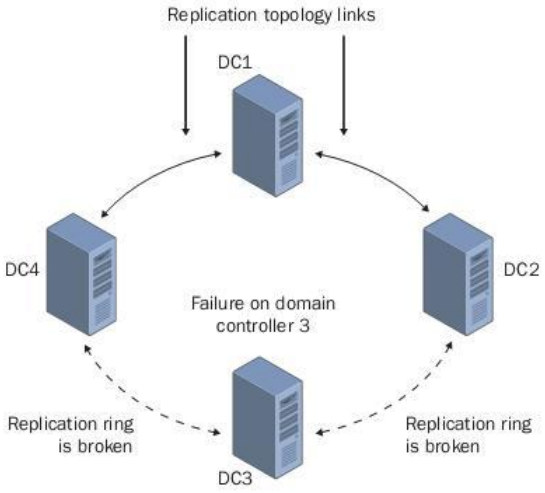
Active Directory اطلاعات را به دو صورت منعکس می‌کند:

- **IntraSite (در داخل یک سایت)**
- **InterSite (بین سایت ها)**

انعکاس در داخل سایت (IntraSite Replication)

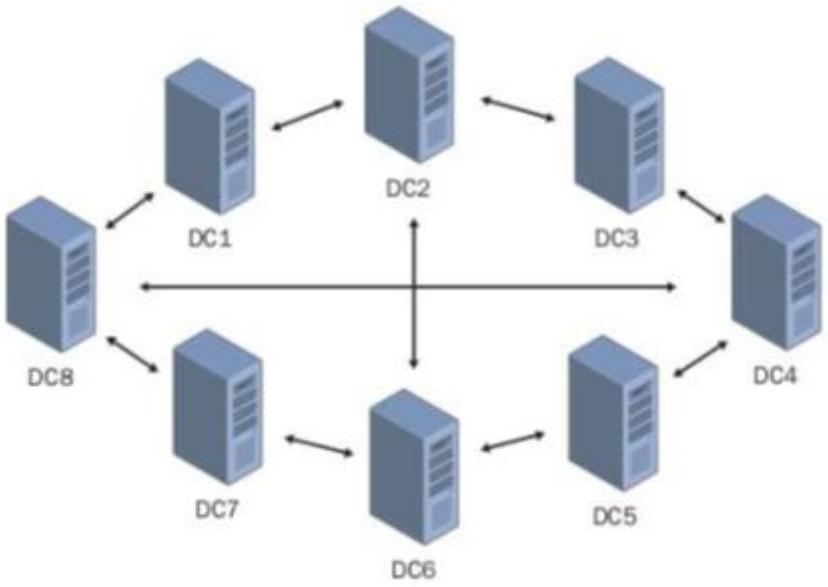
در داخل یک سایت، سرویسی از ویندوز سرور ۲۰۰۳ تحت عنوان Knowledge Consistency Checker که به اختصار آن را KCC می‌نامیم، به صورت خودکار یک توپولوژی برای تکرار در میان Domain controllerها در همان دامنه و با استفاده از یک ساختار حلقه ایجاد می‌کند. KCC یک پروسه‌ی خودکار است که در تمامی DCها اجرا می‌شود. توپولوژی اعمال شده مسیری برای به روز رسانی‌های دایرکتوری فراهم می‌آورد تا از یک DC به DC دیگر جریان یابد و این انتقال تا زمانی ادامه می‌یابد که DCهای موجود در یک سایت به روز رسانی‌های دایرکتوری را دریافت نمایند. KCC تصمیم می‌گیرد که کدام یک از سرورها برای انجام عمل انعکاس با یکدیگر مناسب‌تر هستند و سایر DCها را به عنوان شرکای انعکاس آن‌ها در نظر می‌گیرد. این تصمیم گیری بر اساس مواردی چون نحوه‌ی اتصال، سابقه‌ی انعکاس موفق و بر مبنای تطابق با نسخه‌های انعکاس جزئی و یا کامل است. هر DC می‌تواند بیش از یک شریک برای انعکاس داشته باشد. بعد از آن KCC اشیای ارتباطی را می‌سازد که ارتباط میان شرکای انعکاس را نمایش خواهد داد.

ساختار حلقه تضمین می‌کند که حداقل دو مسیر انعکاس از یک DC به DC دیگر وجود دارد. به همین دلیل اگر یکی از DCها از کار بیفتد، عمل انعکاس (Replication) به سایر DCها ادامه خواهد یافت. شکل زیر توپولوژی انعکاس در داخل سایت را نشان می‌دهد.



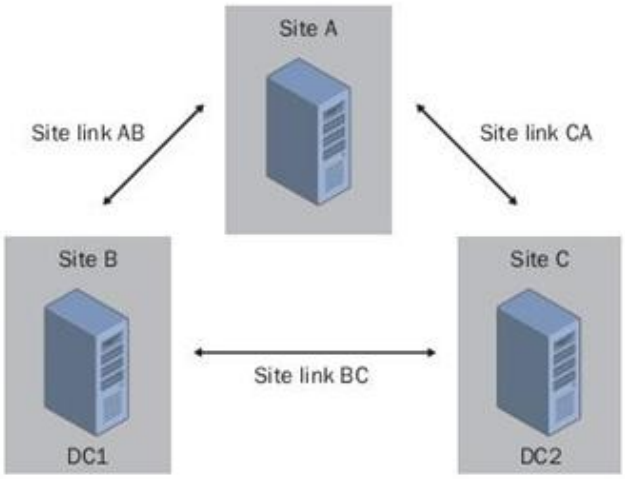
KCC توپولوژی انعکاس در داخل سایت را هر ۱۵ دقیقه یکبار بررسی کرده و از کارکرد آن اطمینان حاصل می‌کند. با اضافه یا خارج کردن یک DC از شبکه، KCC توپولوژی انعکاس را مجددا پیکربندی می‌کند تا این تغییرات در آن منعکس شود.

هنگامی که بیش از **هفت** Domain Controller به یک سایت اضافه می‌شوند، KCC اشیای ارتباط اضافی را در ساختار حلقه دخیل می‌کند تا این اطمینان حاصل شود که اگر تغییری در هر یک از DCها ایجاد شود، هیچ یک از DCها بیش از سه Hop (گام) از DC دیگر فاصله نداشته باشند. این ارتباطات بهینه به صورت تصادفی ایجاد می‌شوند و الزامی برای ساخت آن‌ها در هر DC نیست. شکل زیر این مورد را نشان می‌دهد.



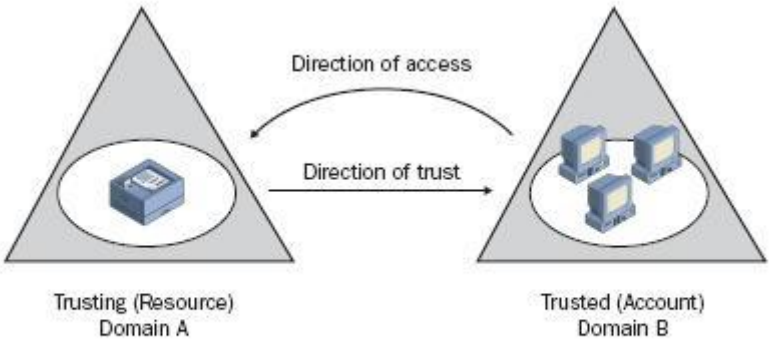
انعکاس بین سایت‌ها (InterSite Replication)

به منظور اطمینان از برقراری انعکاس میان سایت‌ها، می‌بایست که سایت‌ها به صورت دستی و از طریق ایجاد اتصالات سایتی (Site Link) به هم مرتبط شوند. اتصالات سایتی ارتباطات شبکه را نشان داده و وقوع انعکاس را ممکن می‌سازند. یک KCC مجزا در یک سایت تمامی ارتباطات میان سایت‌ها را برقرار می‌سازد. این امر در شکل زیر نشان داده شده است.



۲۵-۶-۲- ارتباطات مطمئن (Trust Relationships)

یک Trust، اتصالی میان دو دامنه است که در آن دامنه‌ی اعتماد کننده (Trusting Domain)، اطلاعات مربوط به دسترسی و شناسایی را از دامنه‌ی مورد اعتماد (Trusted Domain) کسب می‌کند. دو دامنه وجود دارند که موجب برقراری یک رابطه‌ی مطمئن و یا یک Trust می‌شوند: دامنه‌ی اعتماد کننده (Trusting) و دامنه‌ی مورد اعتماد (Trusted). دامنه‌ی اعتماد کننده، دامنه‌ای است که منابع را در اختیار داشته و به سایر دامنه‌ها برای استفاده از این منابع اعتماد دارد. دامنه‌ی مورد اعتماد در حقیقت استفاده کننده از منابع است. این مسئله در شکل زیر بهتر نمود می‌یابد.



Trusting and trusted domains linked with a one-way trust

Trustها ویژگی‌های زیر را دارا هستند:

۱. **چگونگی ایجاد (Method Of Creation):** Trust ها می‌توانند به صورت صریح (Explicitly) یا ضمنی (Implicitly) ساخته شوند. هیچ Trustی نمی‌تواند به هر دو صورت ساخته شود.

۲. **ترآن‌هادگی (Transitivity):** یک Trust ترآن‌هاده یعنی آنکه اگر Domain A به Domain B و Domain B به Domain C اعتماد یا Trust دارد، آنگاه Domain A نیز به Domain C اعتماد می‌کند. یک Trust غیر ترآن‌هاده یعنی آن که اگر Domain A به Domain B و Domain B به Domain C اعتماد یا Trust دارد، بین Domain A و Domain C هیچ ارتباط مطمئن یا Trust برقرار نیست.

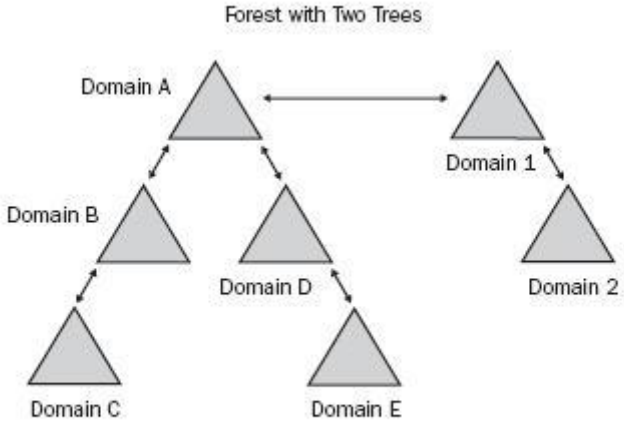
۳. **جهت (Direction):** Trust ها می‌توانند یک طرفه(One-Way) یا دو طرفه (Two-Way) باشند. در یک اعتماد یک طرفه، Domain A به Domain B، Trust دارد. در یک Trust دو طرفه اگر Domain A به Domain B اعتماد داشته باشد، آنگاه Domain B نیز به Domain A اعتماد دارد.

ویندوز سرور ۲۰۰۳ از انواع Trust هایی که در زیر آمده است پشتیبانی می‌کند.

- Parent-Child Trust
- Tree-Root Trust
- Shortcut Trust
- External Trust
- Forest Trust
- Realm Trust

Parent-Child Trust با ایجاد یک درخت و به صورت اتوماتیک میان تمامی دامنه‌های موجود در آن درخت به وجود می‌آید. با اضافه شدن یک دامنه‌ی جدید به یک درخت، پروسه‌ی ایجاد اتوماتیک Trust صورت می‌پذیرد. این نوع Trust دو طرفه و ترآن‌هاده است.

Tree-Root Trust نیز به صورت اتوماتیک و با اضافه شدن یک درخت به ساختار جنگل (A New Root Tree) برقرار می‌شود شکل زیر این Trustها را نشان می‌دهد. این نوع Trust نیز دو طرفه و دارای خاصیت ترآن‌هادگی است.



Domain structure showing tree-root and parent-child trusts

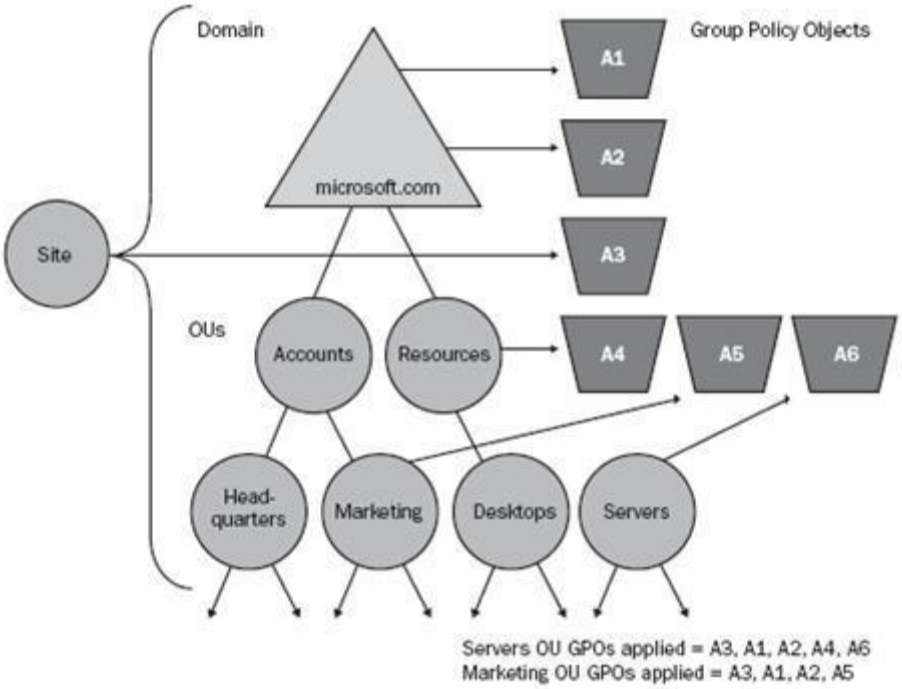
۲۵-۶-۳- سیاست‌های گروهی (Group Policies)

سیاست‌های گروهی، مجموعه‌ای از تنظیمات برای کاربران و کامپیوترها است که می‌تواند به کامپیوترها، سایت‌ها، دامنه‌ها و OUها اعمال گردد تا بدین ترتیب عملکرد کاربران بهتر مشخص گردد.GPOها مجموعه‌ای از سیاست‌های گروهی تنظیم شده است. برای معلوم کردن تنظیمات Desktop برای گروهی از کاربران مشخص، اشیای سیاست گروهی (Group Policy Objects or GPOs) ساخته می‌شوند. هر کامپیوتر با سیستم عامل ویندوز دارای یک GPO داخلی بوده (Local GPO) و علاوه بر آن می‌تواند با یک سری از سیاست‌های غیر محلی (مبتنی بر Active Directory) مرتبط گردد.GPOهای غیر محلی بر GPO داخلی اولویت می‌یابند.GPOهای غیر محلی یا به کاربران (بدون در نظر گرفتن کامپیوتری که به آن Log On می‌کنند) و یا به کامپیوترها (بدون در نظر گرفتن کاربری که به آن Log On می‌کنند) اعمال می‌گردد و مربوط به اشیای خاص Active Directory (دامنه‌ها، سایت‌ها و OU ها) است. این نوع از سیاست‌ها به صورت

سلسله مراتبی و از گروه با کمترین محدودیت (Site) به گروه با بیشترین محدودیت (OU) اعمال می‌شود. در حقیقت چگونگی و ترتیب اعمال به صورتی که در زیر آمده، است:

۱. **Local GPO:** هر سیستم عامل ویندوز تنها دارای یک سیاست گروهی است که به صورت محلی ذخیره شده است.
۲. **GPOs Linked To Sites:** هر GPO که به یک سایت مرتبط باشد در مرحله‌ی بعد اعمال می‌شود. این اعمال برای تمامی سیاست‌های مرتبط با یک سایت همزمان صورت می‌گیرد و مدیر یک شبکه تعیین کننده‌ی ترتیب اعمال است.
۳. **GPOs Linked to Domains:** اولویت اعمال این دسته از سیاست‌ها نسبت به دو مورد اول بیشتر است. اما اولویت اعمال چندین سیاست مربوط به یک دامنه را مدیر شبکه تعیین می‌کند.
۴. **GPOs linked to OUs:** GPO هایی که در بالای ساختار سلسله مراتبی یک OU قرار دارند زودتر اعمال می‌شوند. پس از آن، GPOهای مربوط به OUهای فرزند اعمال شده و در نهایت GPOهای مربوط به OU شامل کاربران و کامپیوترها اعمال می‌شود. در هر سطح از OU می‌توان بیش از چند GPO را اعمال نمود (حتی می‌توان هیچ GPO را اعمال نکرد).

شکل زیر چگونگی اعمال سیاست گروهی برای دو OUی نمونه‌ی Server و Marketing را نشان می‌دهد.



فصل ۲۶

نصب و راه اندازی Active Directory

۲۶-۱- نصب Active Directory

از جمله امکانات قدرتمند Windows Server 2003 Advanced، Active Directory است که امکان مدیریت کاربران، کامپیوترها، گروه‌ها و بطور کلی تمامی عناصر موجود در یک شبکه را فراهم می‌کند. در واقع اگر بخواهیم کامپیوتری به یک سرور واقعی تبدیل شود و بتواند یک دامنه را کنترل کند (Domain Controller)، بایستی Active Directory را روی آن نصب کرد. (البته نباید اینگونه تصور نمود که Active Directory تمامی مشکل یک مدیر شبکه را حل می‌نماید). با استفاده از قابلیت‌های Active Directory می‌توان مشخص کرد کدام User با کدام Computer تحت کدام Domain به چه کاری بپردازد. یعنی میزان دسترسی آن به منابع موجود در شبکه چه مقدار باشد و تا چه میزان در این کار اختیار دارد و اجازه دسترسی دارد (مثلاً امکان نوشتن یا جابجا نمودن و حتی امکان دسترسی به دیگر کاربران و اینکه خود در چه سطحی از مدیریت نمودن شبکه قرار بگیرد). با استفاده از قابلیت Active Directory در Windows Server 2003 Advanced مدیریت شبکه بسیار آسان است.

چند نکته مهم در استفاده از Active Directory:

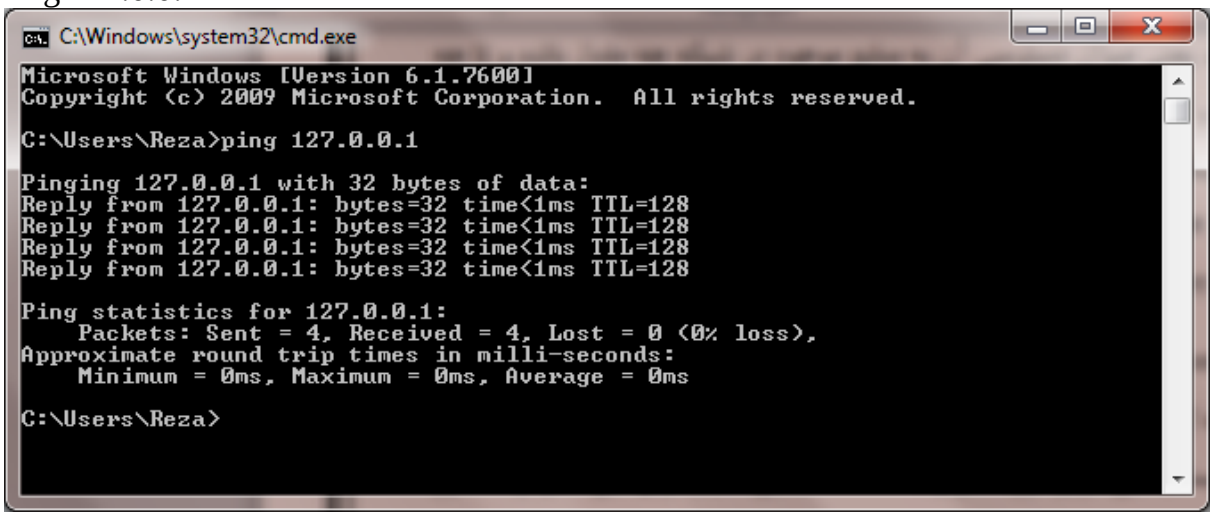
۱. اولین عاملی که باید در Active Directory مد نظر داشت این است که سیستم فایل ما باید از نوع NTFS باشد تا امکان استفاده از Active Directory را داشته باشیم. بنابراین اگر سیستم فایل ما از نوع FAT باشد، ابتدا باید نوع سیستم فایل درایو مورد نظر را به NTFS تبدیل کنیم. برای این کار از دستور Convert موجود در Command Prompt استفاده کنیم.

Run➔ CMD➔ Convert D: /fs:NTFS

درایو مورد نظر :D می‌باشد.

۲. صحت تنظیمات کارت شبکه و پروتکل کامپیوتر مورد نظر نیز کنترل شود. برای اینکار در Command Prompt دستور زیرا را وارد کنید. نتیجه کار باید مانند شکل زیر باشد:

C:\> Ping 127.0.0.1

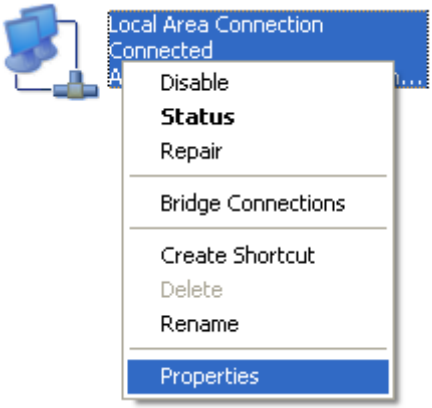


۳. سپس باید DNS Server را نصب کنید. وظیفه DNS Server تبدیل اسامی Host به آدرس IP است. توجه نمایید که در صورت عدم نصب DNS Server، سرور و Active Directory قادر به انجام وظایف خود نیست. برای آشنایی با DNS Server و نحوه نصب آن به فصل DNS Server مراجعه فرمایید.

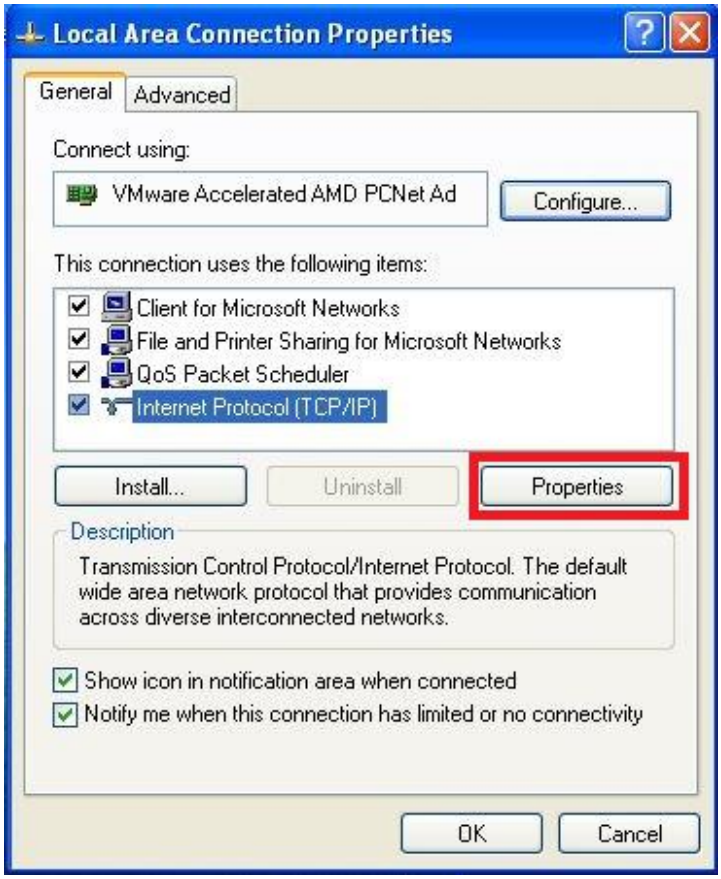
۴. IP Address را باید حتما به صورت دستی (ایستا) تنظیم کنیم. زیرا IP سرور نباید متغیر باشد. برای اینکار وارد مسیر زیر شوید:

Control Panel ➔ Network Connections

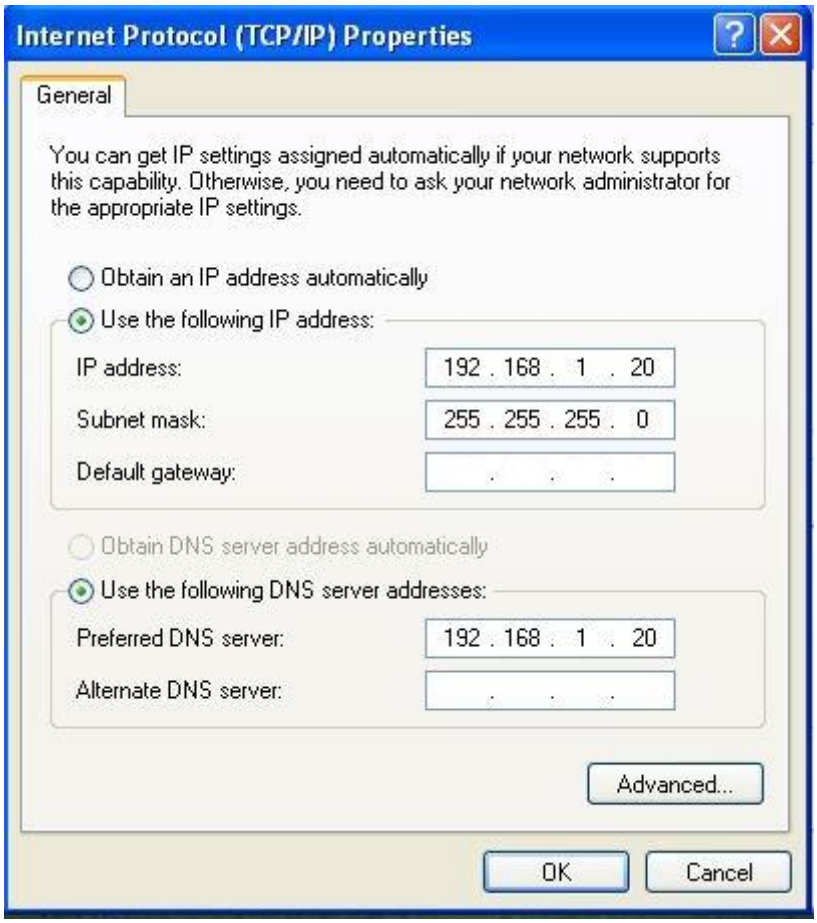
روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.



در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل زیر، آدرس IP را به صورت دستی تنظیم کنید. در قسمت Preferred DNS نیز آدرس DNS Server که نصب کردهاید را وارد نمایید. در نهایت روی دکمه OK کلیک کنید.



۵. بهتر است که در شبکه Clientهای خود را از خانواده Windows NT (XP , 2000 Pro , NT Work Station) باشد. در اینصورت به بهترین وجه می‌توان امنیت شبکه و کامپیوترهای آن را تامین نمود.

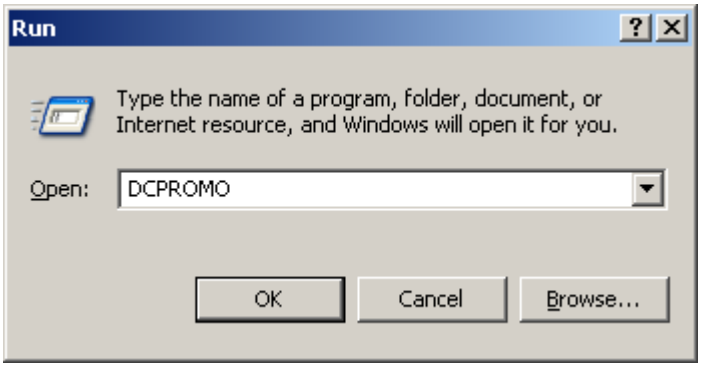
۶. باید حداقل 1 GB فضای خالی داشته باشیم.

در صورتی که موارد فوق را به درستی انجام داده باشیم، سیستم ما آماده نصب Active Directory می‌باشد. درصورت نصب Active Directory، سرور ما تبدیل به یک Domain Controller خواهد شد.

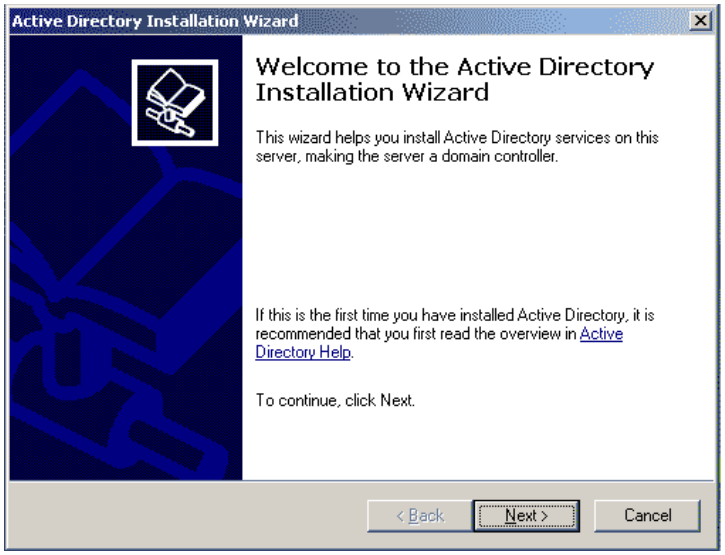
قابل ذکر است که این طریق نصب، طریقه نصب به صورت حرفه‌ای می‌باشد و در صورتی که بخواهید می‌توانید به صورت خیلی آسان از طریق پنجره‌ی Manage Your Server از داخل Administrative Tools این کار را به راحتی تمام و به صورت Wizard انجام دهید.

برای شروع نصب منوی Start را باز کرده و در RUN عبارت زیر را تایپ می‌کنیم: DCPROMO

DCPromo مخفف Domain Controller Promotion و به معنای ارتقای کنترل‌کننده دامنه می‌باشد.

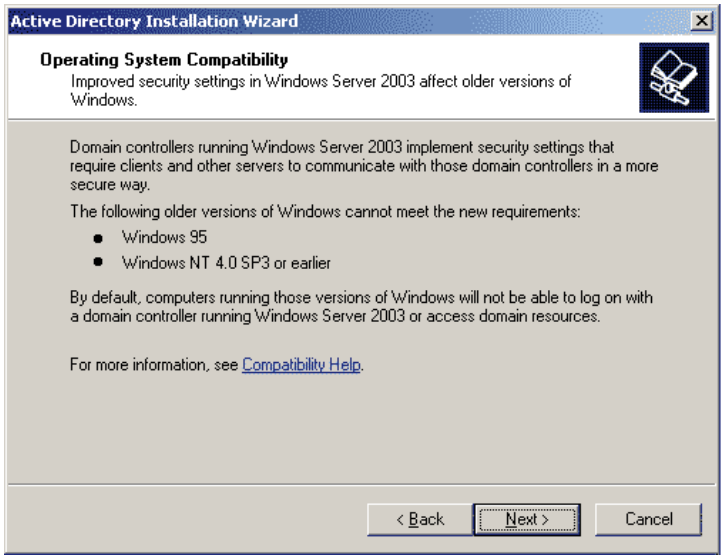


در ابتدا صفحه خوش آمد گویی مبنی بر نصب Active Directory ظاهر خواهد شد.



بر روی دکمه‌ی Next کلیک می‌کنیم و به صفحه بعدی هدایت می‌شوید.

در این صفحه به شما هشدار می‌دهد که در صورتی که در شبکه خود کامپیوتر هایی با سیستم عامل‌های Win 95 و یا Win NT SP 3.0 یا قدیمی‌تر داشته باشید، نمی‌توانند به DC وصل شوند و عملیات Login را انجام دهند و نمی‌توانند از منابع به اشتراک گذاشته شده در شبکه استفاده کنند.



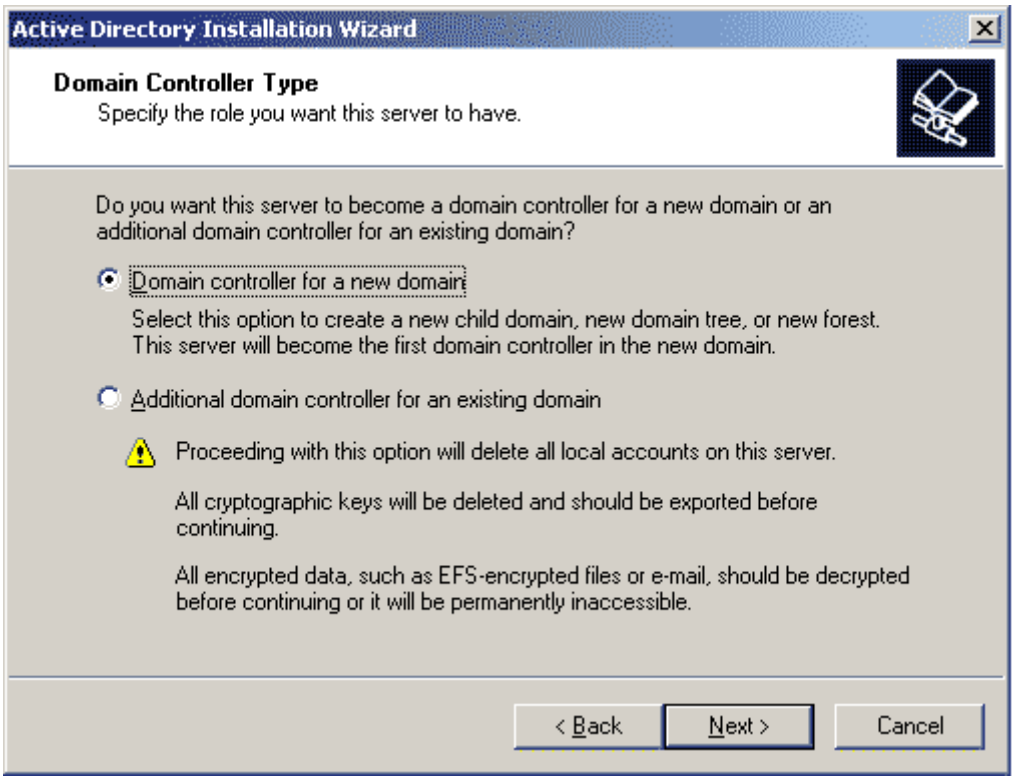
بر روی دکمه Next کلیک کرده و به صفحه بعدی بروید.

در این صفحه که عکس آنرا در پایین مشاهده می‌کنید دو گزینه وجود دارد:

در صورتی که شما گزینه Domain controller for a new domain را انتخاب کنید، یعنی اینکه می‌خواهید اولین DC را برای Domain خود ایجاد کنید.

و در صورتی که گزینه Additional domain controller for an existing domain را انتخاب نمایید، بدین معناست که شما از قبل یک DC، دارید و اکنون می‌خواهید یک DC جدید اضافه نموده و احتمالا آن را زیر شاخه‌ای از آن قرار دهید.

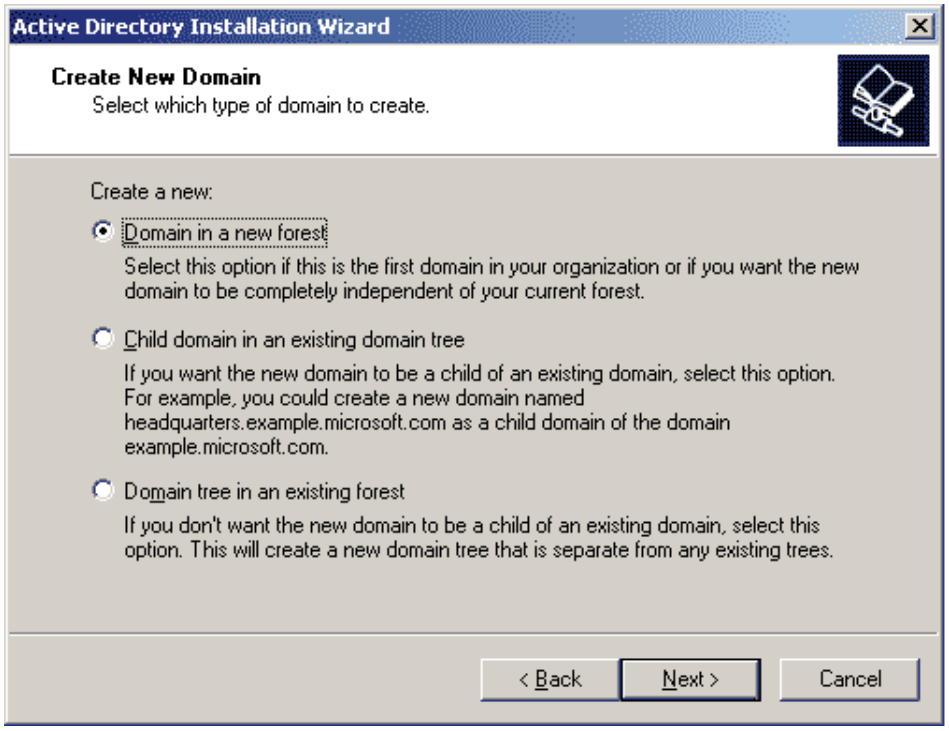
گزینه اول را انتخاب کرده و دکمه Next را کلیک نمایید.



در صفحه بعدی با توجه به اینکه در صفحه قبل گزینه اول را انتخاب کردهاید، ۳ گزینه پیش رو دارید:

در صورتی که Domainای که راه اندازی می‌کنید، اولین Domain برای یک Forest جدید می‌باشد، گزینه Domain in a new forest را انتخاب کنید. در این حالت یک Forest جدید ساخته خواهد شد. گزینه دوم (Child Domain in an existing domain tree) برای مواقعی می‌باشد که می‌خواهید یک Child Domain را در داخل یک Domain Tree که از قبل وجود داشته است، ایجاد کنید. و اما گزینه سوم (Domain tree in an existing forest) برای زمانی می‌باشد که شما نمی‌خواهید Domainای که ایجاد می‌شود به عنوان Child برای یک Domain Tree باشد و می‌خواهید این دامنه جدید به عنوان دامنه ریشه (نه فرزند دامنه‌ای دیگر) به کار گرفته شود.

گزینه اول را انتخاب کرده و بر روی Next کلیک کنید.



در اینجا مجددا توضیح مختصری درباره مفاهیم فوق می‌دهیم: ساختار Active Directory از یک مجموعه به نام Forest (جنگل) تشکیل می‌شود. هر Forest می‌تواند شامل یک یا تعدادی Domain Tree باشد. هر Domain Tree از یک یا چند Domain تشکیل می‌شود، به طوری که اولین Domain را با نام Root Domain و سایر Domainها را با نام Child Domain می‌شناسیم. هر Domain یک نام برای خود خواهد داشت که در سطح خود (نسبت به پدر) یکتا است و اسامی Domainهای موجود در یک Tree به یکدیگر وابسته خواهند بود؛ یعنی نام فرزند با یک نقطه به ابتدای نام پدر خواهد چسبید. مثلاً اگر نام Domain پدر Alavijeh.Com و نام Domain فرزند Computer باشد، نام کامل فرزند (FQDN) می‌شود: Computer.Alavijeh.Com

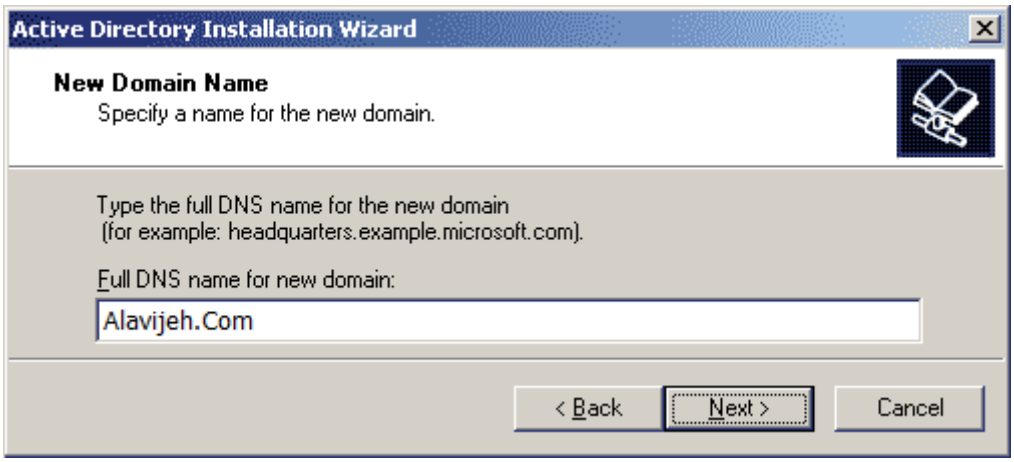
در این صفحه که بسیار مهم می‌باشد شما می‌بایست نامی را که می‌خواهید برای Domain خود داشته باشید وارد نمایید. که بطور مثال بنده در این عکس Alavijeh.Com را در نظر گرفته ام. سپس روی دکمه Next کلیک کنید. دقایقی طول می‌کند تا سیستم تکراری بودن یا معتبر بودن نام وارد شده را بررسی کند.

برای انتخاب این اسم بایستی موارد زیر را در نظر داشته باشید:

۱. نام هیچ کامپیوتری در شبکه را برابر با نام Domain نگذارید.

۲. سعی کنید نامی را انتخاب کنید که بعدا زمانی که شبکه خود را به اینترنت وصل می‌کنید مشکل نداشته باشید. به عنوان مثال در صورتی که نام Domain خود را Microsoft.Com انتخاب کنید و شبکه خود را به اینترنت وصل کنید در داخل DNS یکسری مشکلات دارید و باید تنظیماتی را انجام دهید. (پیشنهاد می‌کنم که هر نامی را که دوست دارید انتخاب کنید و در انتهای آن.local را اضافه کنید چراکه پسوند.local در اینترنت وجود ندارد.)

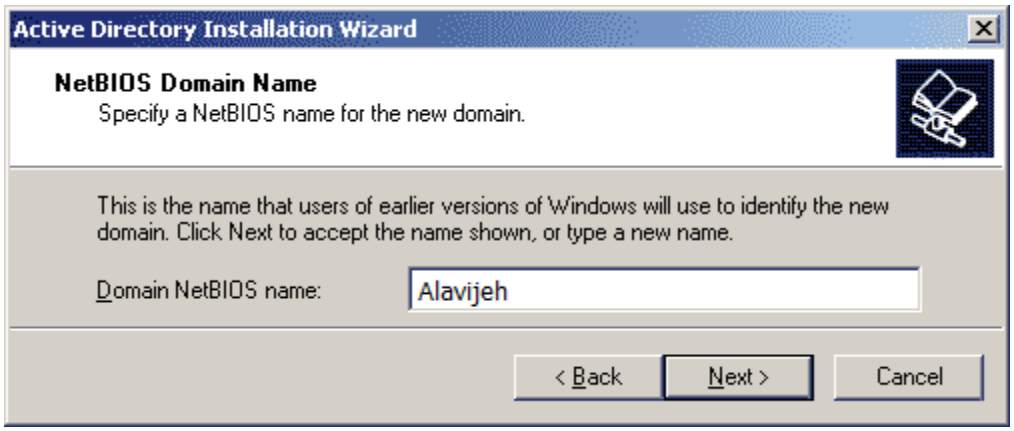
بعد از انتخاب نام و وارد کردن آن بر روی Next کلیک کنید تا وارد صفحه بعد شوید.



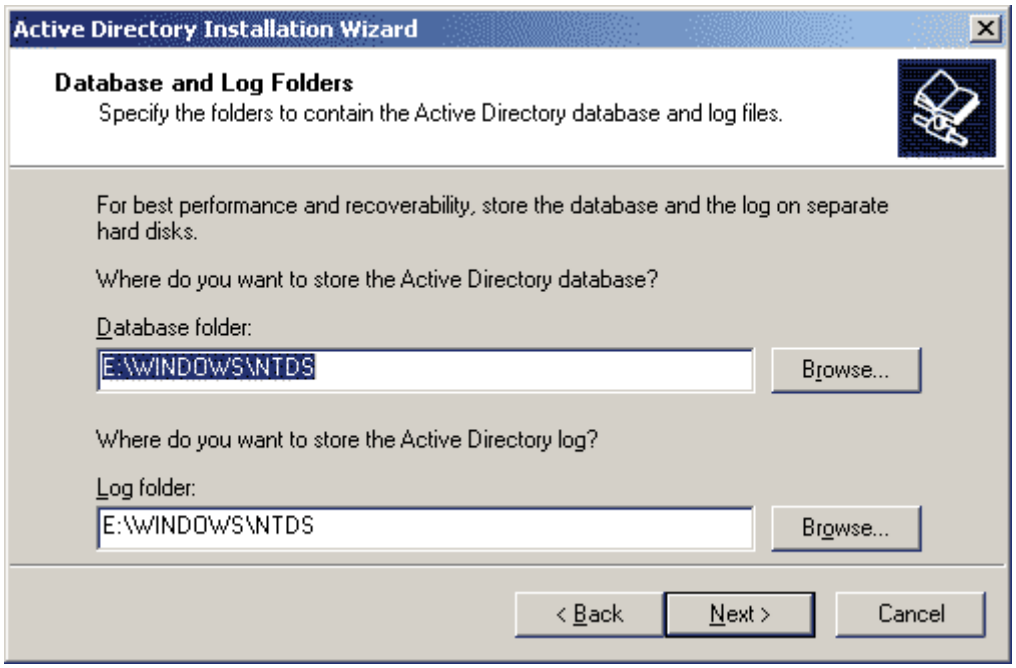
در صفحه بعدی نامی که وارد کردید تا قبل از نقطه به عنوان NetBIOS Name انتخاب می‌شود تا نسخه‌های قدیمی ویندوز از طریق آن Domain جدید را شناسایی کنند.

نکته در رابطه با NetBIOS Name: می‌دانیم که NetBIOS Name فرمت قدیمی نام گذاری مایکروسافت می‌باشد که این اسم از ۱۶ کاراکتر تشکیل می‌شود که ۱۵ تای ابتدایی آن را کاربر انتخاب می‌کند و آخرین کاراکتر را خود سیستم با توجه به سرویس‌های مختلف اضافه می‌کند.

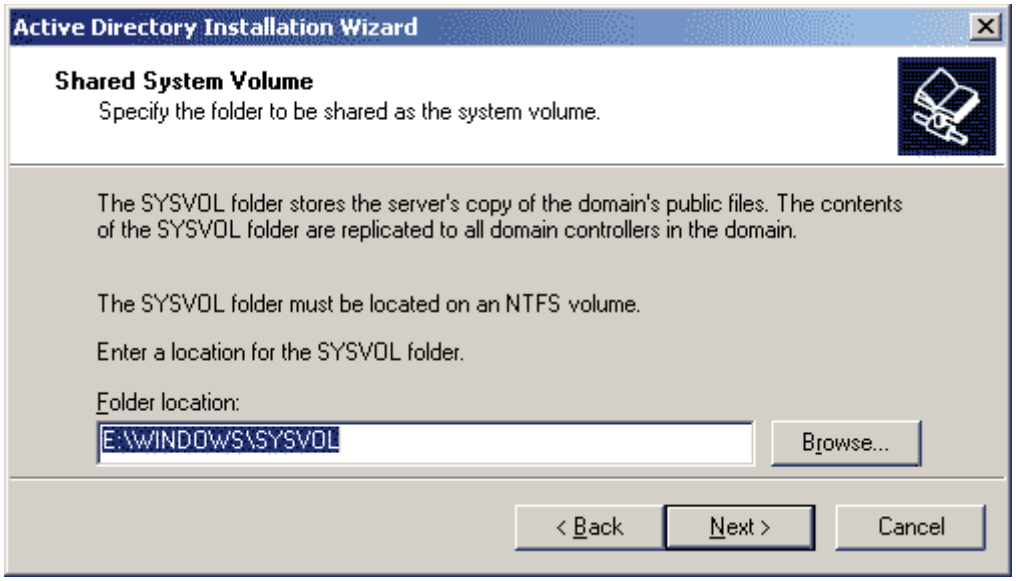
در این صفحه نیز بروی Next کلیک کنید.



در صفحه بعدی شما می‌توانید محل ذخیره Database، Active Directory و همچنین محل ذخیره Log فایل‌های مربوط به این سرویس را مشخص کنید.



قابل ذکر است که پایگاه داده اکتیو دایرکتوری به نام NTDS.DIT و به صورت پیش فرض در پوشه ویندوز ذخیره می‌شود. در صفحه بعدی شما محل ذخیره پوشه SYSVOL را مشخص می کنید.

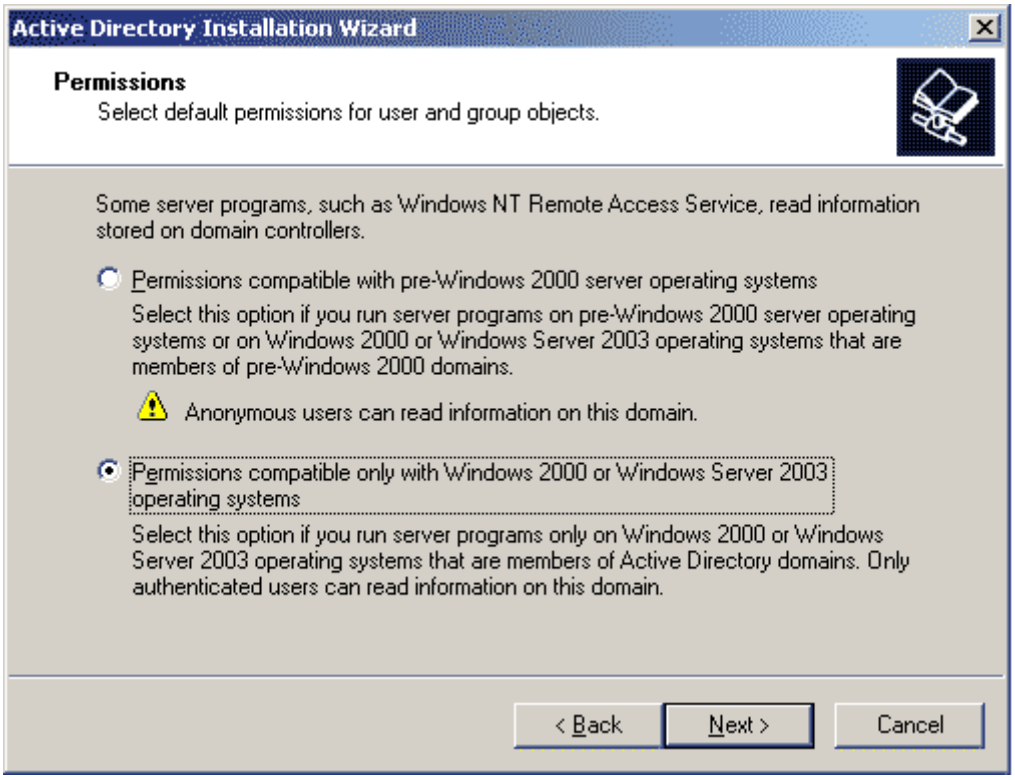


نکاتی در رابطه با پوشه SYSVOL:

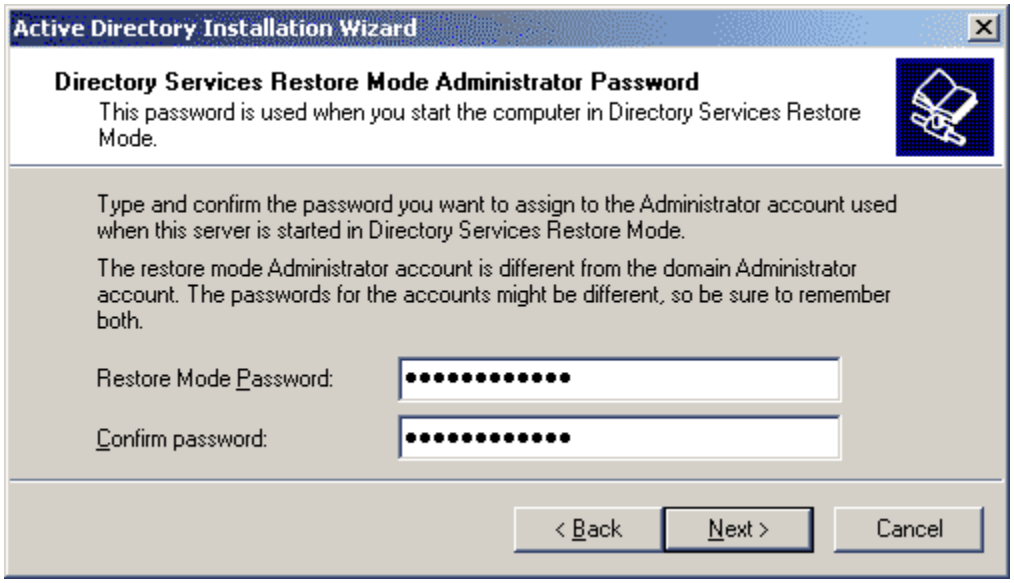
به هنگام نصب AD (اکتیو دایرکتوری) پوشه‌ای بر روی کامپیوتر DC ایجاد می‌شود که این پوشه به صورت پیش فرض Share شده می‌باشد. قابل ذکر است که محل این پوشه حتما باید بر پارتیشنی به فورمت NTFS باشد. فایلهای موجود در این پوشه حاوی سیاستهای کلی تعریف شده در داخل ساختار AD می‌باشد و همچنین DCها برای اینکه بتوانند با یکدیگر عملیات Replication انجام دهند از این پوشه استفاده می کنند.

مر حله بعدی نصب DNS می‌باشد که می‌توانیم بگوییم که خود سیستم به صورت خودکار به همراه نصب AD، DNS هم نصب کند یا اینکه قبل از نصب AD سرویس DNS را خودمان به صورت دستی بر روی کامپیوتر مورد نظر نصب کنیم. و باید توجه داشته باشیم که وجود DNS برای AD الزامی است.

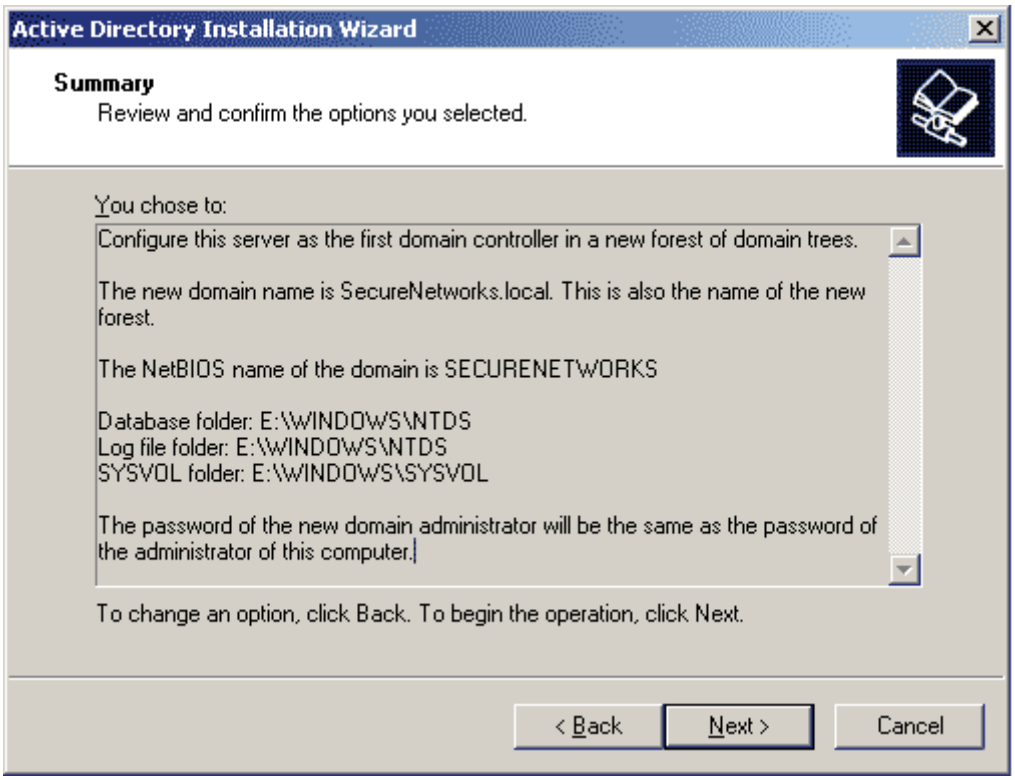
در مرحله بعدی انتخاب کلاینت هایی می‌باشد که با سرور ما ارتباط برقرار می‌کنند که گزینه اول برای پلاتفرم‌های قبل از ۲۰۰۰ می‌باشد و دومین گزینه پلاتفرم‌های ۲۰۰۰ و ۲۰۰۳ را پشتیبانی می‌کند که در شکل زیر مشاهده می‌کنید:



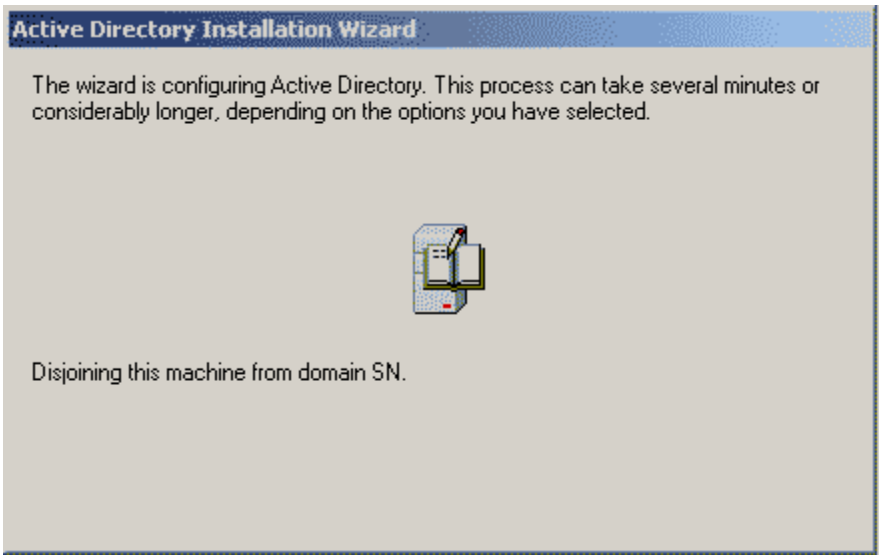
در صفحه بعدی که در شکل زیر مشاهده می‌کنید می‌بایست Passwordای را برای حالت DSRM یا (Directory Services Restore Mode) انتخاب کنید تا در صورتی که کامپیوتر را در این حالت Boot کردید از این Password استفاده کنید.



و در صفحه نهایی تمامی تنظیماتی را که در صفحه‌های پیشین وارد نمودید به طور یکجا و به صورت Information نشان می‌دهد. در صورتی که مشکلی نمی‌بینید و تمامی تنظیمات درست است بر روی Next کلیک کنید تا عملیات نصب آغاز شود.



پس از Next کردن صفحه زیر برای شما نمایان خواهد شد که عملیات مختلف راه اندازی DC و نصب AD را نشان می‌دهد:



پس از پایان یافتن عملیات نصب بر روی Finish کلیک نمایید و با پیغامی که ظاهر می‌شود دستگاه خود را Restart کنید تا تمام عملیات انجام شده بر روی سیستم شما اعمال شود.



اجازه می‌دهیم سیستم مجدد راه اندازی شود.

پس از طی مراحل فوق شما موفق به نصب قویترین سرویس مایکروسافت بر روی ویندوز سرور خود شدهاید.

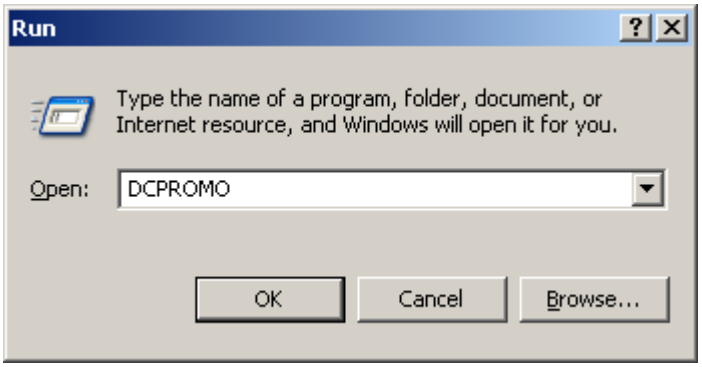
پس از راه اندازی سیستم می‌توانیم با استفاده از کلمه کاربری مدیر سیستم (Administrator) و کلمه رمزی که در هنگام نصب وارد کرده‌ایم وارد سیستم شویم.

در هنگامیکه این سرویس بر روی ویندوز سرور نصب می‌گردد کلیه Accountها، Groupهای ویندوز غیرفعال شده و جای خود را به گروه‌ها و Userهای Active Directory می‌دهند.

حال کافیست پیکربندی آن را انجام دهید.

۲۶-۲- حذف Active Directory

حذف Active Directory بسیار شبیه نصب آن است. همانطور که برای نصب Active Directory از دستور DCPromo استفاده کردیم، برای حذف نیز همین دستور را در Run وارد می‌کنیم:

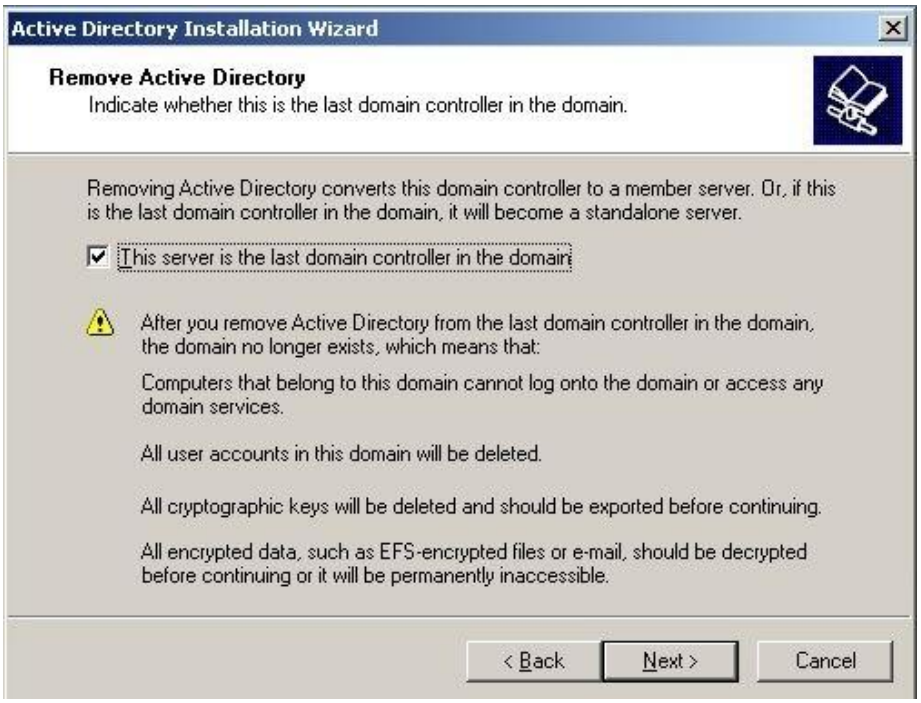


پس از کلیک کردن روی دکمه OK، صفحه خوش آمد گویی می‌شود. بر روی دکمه Next کلیک کنید.

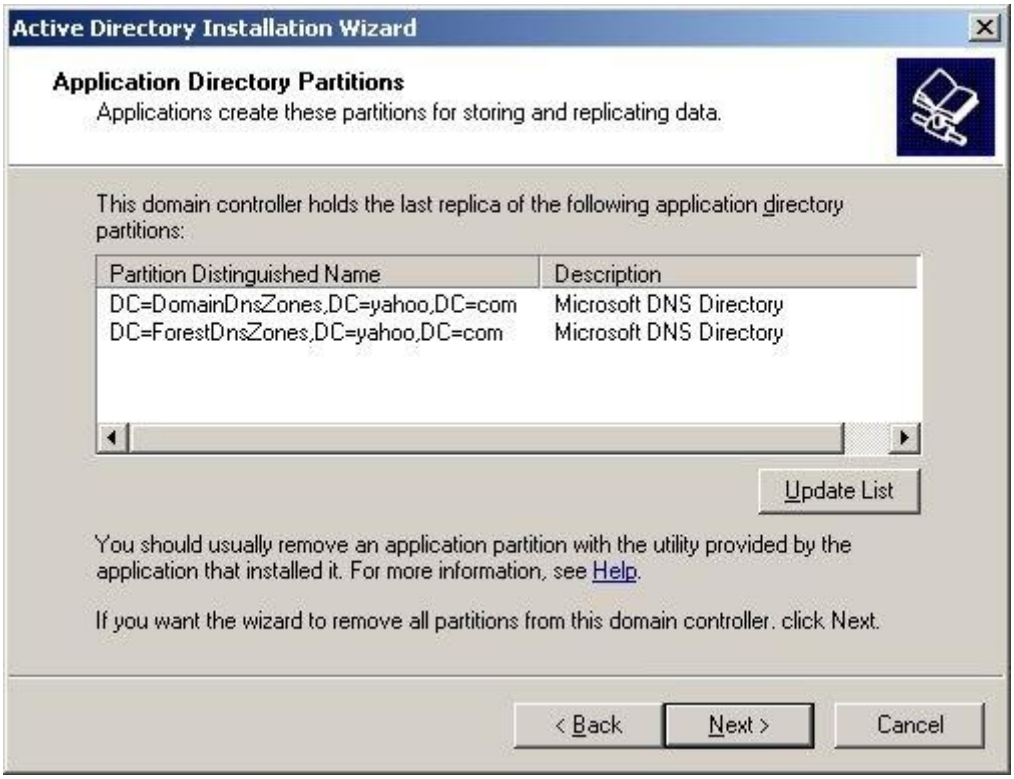
سپس پیغام زیر ظاهر می‌شود. روی دکمه OK کلیک کنید:



در این صفحه بایستی مشخص کنید که این کامپیوتر یک کنترل‌کننده دامنه (DC) می‌باشد. با حذف DC، این کامپیوتر تبدیل به یک کامپیوتر عادی عضو شبکه می‌شود. برای ادامه عملیات حذف، روی دکمه Next کلیک کنید:



مجددا روی دکمه Next کلیک کنید:



سپس در این صفحه بایستی مشخص نمایید که قصد دارید دایرکتوری برنامه‌های کاربردی اکتیو دایرکتوری را حذف نمایید. عمل حذف دایرکتوری برنامه‌های کاربردی اکتیو دایرکتوری بعد از پایان پذیرفتن عملیات حذف اکتیو دایرکتوری رخ می‌دهد.



باز هم روی دکمه Next کلیک کنید. در این پنجره از کاربر کلمه رمزی را برای کاربر مدیر کامپیوتر درخواست می‌شود که بعد از حذف این سرویس و راه اندازی مجدد سیستم، کاربر می‌بایستی توسط این کلمه عبور وارد سیستم گردد.



سپس روی دکمه Next کلیک کنید:



بعد از رفتن به مرحله بعد، سیستم شروع به حذف Active Directory خواهد کرد. در این قسمت بایستی چند دقیقه‌ای صبر کنیم تا سیستم کارش به اتمام برسد.



پس از اتمام حذف Active Directory، روی دکمه Finish کلیک کنید.

در نهایت سیستم را Restart کنید:



۲۶-۳- مفاهیم Active Directory Backup

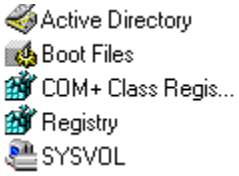
امروزه تهیه پشتیبان از فایل‌ها، اسناد و داده‌ها در هر شبکه و سیستمی، خواه شبکه کوچک باشد یا بزرگ، ضروری به نظر می‌رسد؛ حتی تهیه پشتیبان بر روی رایانه‌های شخصی هم گاهی واجب می‌باشد. در همین راستا پشتیبان گیری از Active Directory هم در جهت نگهداری و پشتیبانی از آن یکی از اصول پایه و مهم به شمار می‌آید؛ زیرا Active Directory قلب یک شبکه Client/Server به حساب می‌آید.

تهیه پشتیبان از Active Directory را به ۲ صورت گرافیکی و توسط خط فرمان می‌توان انجام داد که در این آموزش هر دو صورت بررسی خواهد شد.

پشتیبان گیری مرتب و طبق زمانبندی مناسب سبب می‌شود تا در مواقع بحرانی از دست دادن داده و اطلاعات شانس بیشتری در جهت برگرداندن آن‌ها داشته باشید.

برای تهیه پشتیبان از Active Directory می‌بایست از System State پشتیبان تهیه کنید، پشتیبان گیری از Active Directory هیچ گونه خللی در کار Domain Controller و شبکه ایجاد نمی‌کند.

System State دارای اجزای مختلفی می‌باشد، که این اجزا بر روی سیستمی که نقش Domain Controller ایفا می‌کند متفاوت از دیگر سیستم‌ها می‌باشد. در این جا، اجزای تشکیل دهنده آن در یک کنترل‌کننده دامنه را مورد بررسی قرار می‌دهیم:



۱. Active Directory
۲. Boot Files
۳. COM+ Class Registration Database
۴. Registry
۵. SYSVOL
۶. Certificate Service Database

نکته:

موارد ۱ و ۵ فقط بر روی Domain Controller وجود دارند که جزیی از System State هستند.

مورد ۶ فقط بر روی سیستمی که CA سرور باشد وجود خواهد داشت.

اکثر اجزای در بالا ذکر شده را می‌توان از طریق نامشان به کاربردشان پی برد و فقط به توضیحی کوتاه در مورد SYSVOL می‌پردازیم:

SYSVOL یک پوشه به اشتراک گذاشته شده می‌باشد که حاوی قالب‌های Group Policy و اسکریپتهای Logon می‌باشد.

هر چند System State دربر دارنده اکثر تنظیمات سیستم می‌باشد، ولی الزاما حاوی تمام فایل‌ها و اطلاعات مورد نیاز برای برگرداندن کامل سیستم به قبل از خرابی و مشکل نمی‌باشد. البته برای برگرداندن اطلاعات Active Directory تهیه پشتیبان از آن کافی است؛ برای تهیه پشتیبان کامل از سیستم می‌توان از ابزارهایی نظیر Norton Ghost بهره جست.

نکته مهم: در هنگام تهیه پشتیبان از Active Directory باید به زمان مشخص شده برای Tombstone (سنگ قبر) توجه داشته باشیم، از آن رو که نمی‌توان آن پشتیبان گرفته شده را بعد از مدت زمان مشخص شده برای Tombstone باز گرداند. زمان پیش فرض ۶۰ روز می‌باشد که اگر ویندوز بروز رسانی شده باشد تا ۱۸۰ روز هم قابل افزایش می‌باشد. پس سعی کنید در بازه‌های زمانی کوتاه پشتیبان گیری صورت گیرد و حداقل ۲ پشتیبان در زمان Tombstone داشته باشید.

Tombstone چیست؟

وقتی یک Object را از Active Directory پاک می‌کنیم در مرحله اول بطور فیزیکی از پایگاه داده حذف نمی‌شود؛ بلکه Active Directory مشخصه (isDeleted (attribute را True کرده و آن را به یک Container خاص به نام CN=Deleted انتقال می‌دهد، حالا این Object یک Tombstone می‌باشد که با استفاده از ابزارهای معمول قابل مشاهده نمی‌باشد.

می توان با استفاده از این خاصیت، Objectهایی که اشتباها پاک شده‌اند را حتی بدون استفاده از Backup&Restore بازیابی کرد. یکی از ابزارهایی که می‌تواند Tombstoneها را باز گرداند، AdRestore می‌باشد.

شرکت مایکروسافت داشتن حداقل ۲ سرور Domain Controller را توصیه کرده است، چنانکه در صورت خرابی سرور اصلی، سرور پشتیبان وظایف آن را به عهده می‌گیرد و خللی در کار شبکه به وجود نمی‌آید؛ البته فقط یک سرور می‌تواند در بر دارنده Operations Master Roleها باشد و در صورت از دست دادن کامل DC اصلی این‌ها را به DC دیگر انتقال می‌دهیم. DCهای پشتیبان را Additional Domain Controller می‌نامند و هنگام نصب Active Directory در پنجره Active Directory Type باید Additional Domain Controller for existing Domain را انتخاب کرد.

هر چند داشتن Additional Domain Controller ریسک از دست دادن اطلاعات را کاهش می‌دهد، ولی برای باز گردانی اطلاعات به صورت Authoritative (در ادامه بررسی می‌شود) به کپی پشتیبان System State نیاز خواهید داشت.

ایجاد تغییراتی برای آزمایش:

برای اینکه پشتیبان گیری و بازگرداندن آن قایل لمس باشد، یک کاربر با نام Reza ایجاد کنید.

۲۶-۴- پشتیبان گیری از Active Directory

همان طور که اشاره شد برای پشتیبان گیری از Active Directory باید از System State پشتیبان تهیه کنیم، برای این منظور کاربری که قصد گرفتن پشتیبان دارد باید عضو گروه Domain Admins باشد تا بتواند این عملیات را انجام دهد.

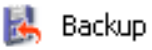
توجه داشته باشید که برای تهیه پشتیبان باید حتما به صورت Local از ابزار Backup Utility استفاده کنید زیرا پشتیبان System State را نمی‌توان از راه دور تهیه کرد، البته می‌توان از Remote Desktop جهت اجرای این ابزار به صورت Local بهره جست.

۲۶-۴-۱- پشتیبان گیری توسط رابط گرافیکی

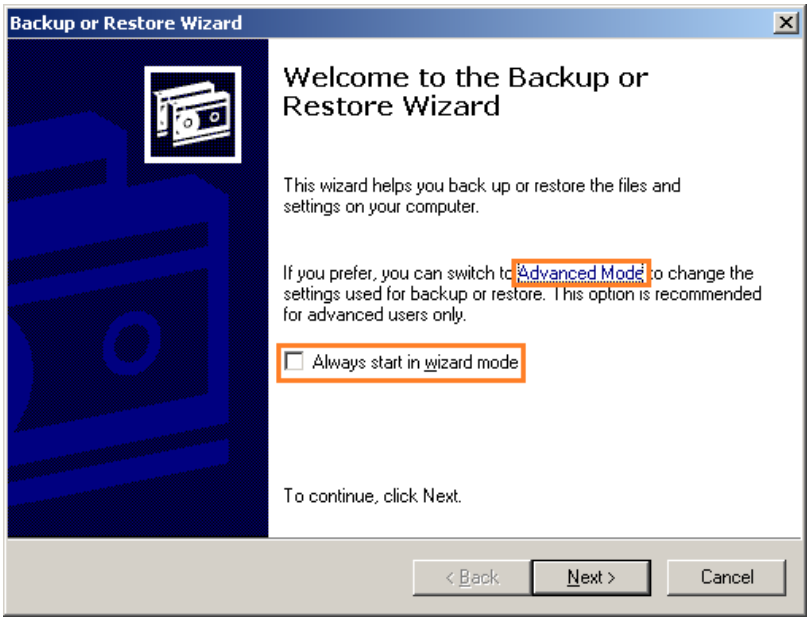
برای تهیه پشتیبان مراحل زیر را طی می کنیم:

۱. از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می کنیم:

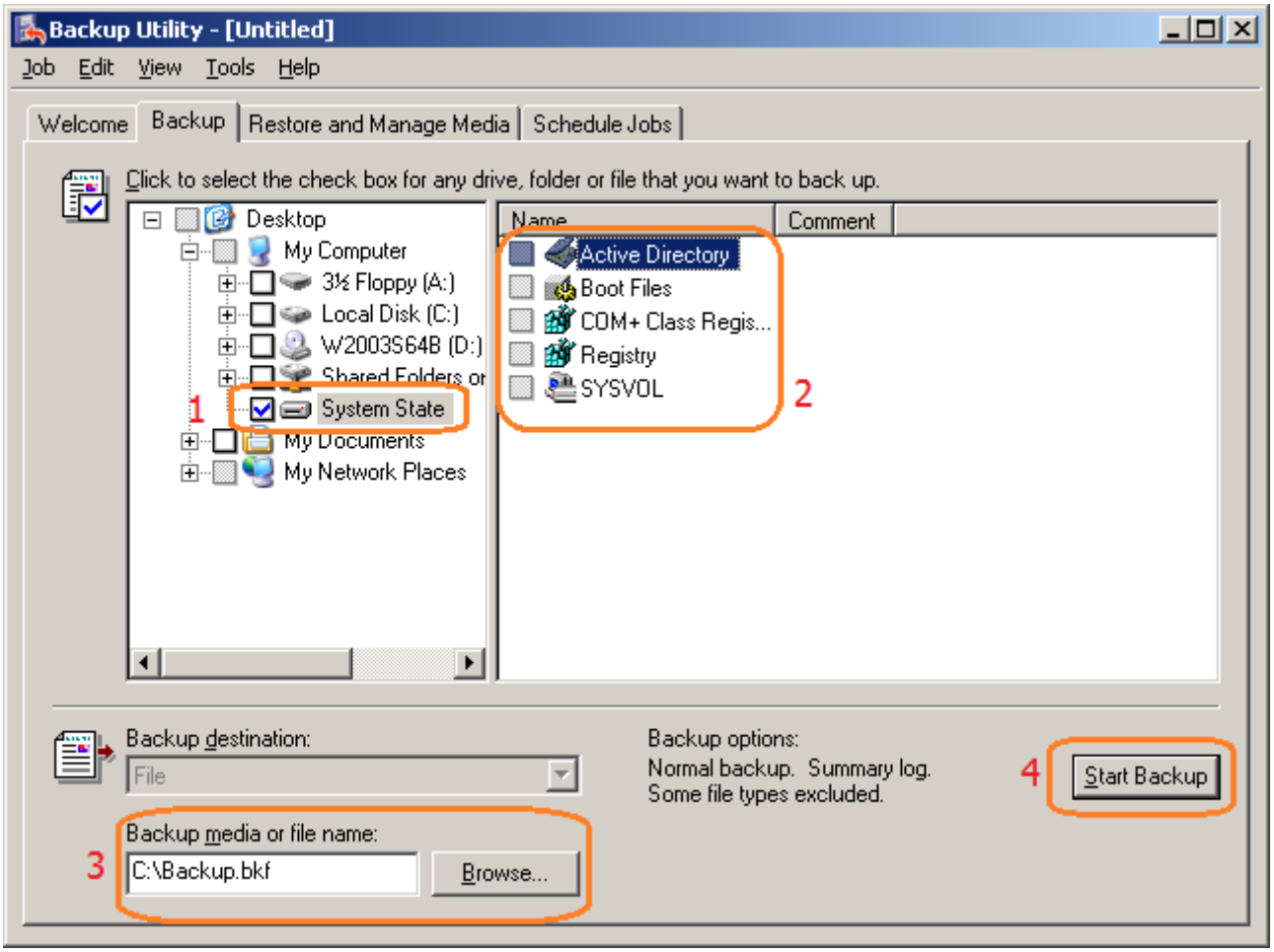
Start Menu ➔ All Programs ➔ Accessories ➔ System Tools ➔ Backup



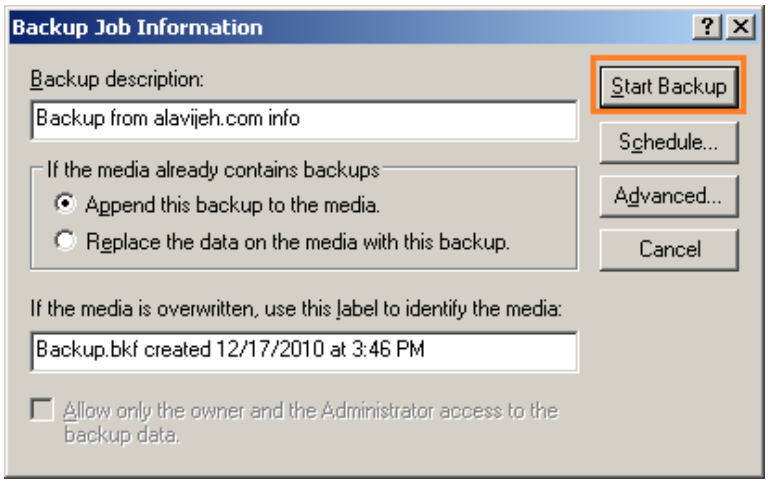
۲. در پنجره Backup or Restore Wizard طبق عکس زیر بر روی Advance mode کلیک کنید. اگر می‌خواهید همیشه در حالت پیشرفته اجرا شود، تیک Always start in wizard mode را بردارید.



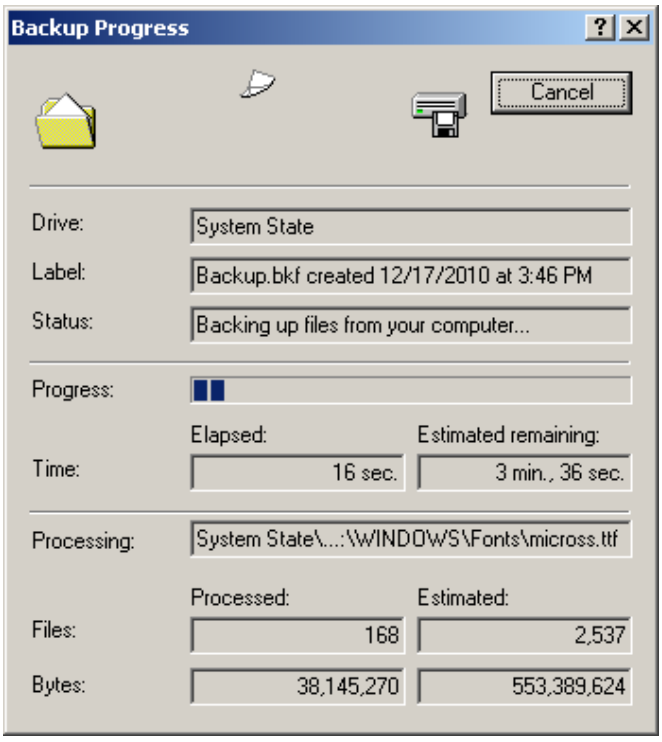
۳. وارد سربرگ Backup شده و طبق عکس زیر، System State را انتخاب و تیک آن را بزنید. سپس از دکمه Browse محلی که می‌خواهید پشتیبان در آنجا ذخیره شود را مشخص و نامی مناسب برای آن انتخاب کنید، سپس بر روی Start Backup کلیک کنید.



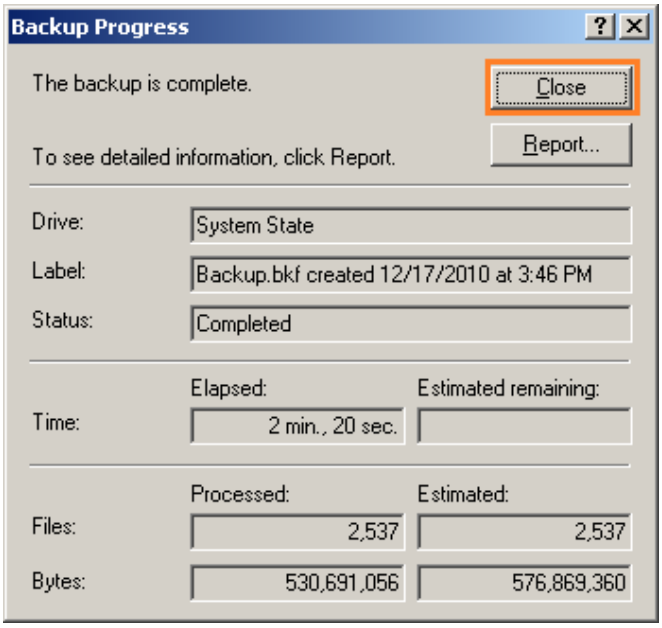
۴. در پنجره Backup Job Information بر روی Start Backup کلیک کنید. همچنین می‌توانید برای یک پشتیبان گیری مرتب در همین مرحله بر روی Schedule کلیک کنید و زمانبندی مناسب را انجام دهید.



۵. با کلیک روی Start Backup، عملیات کپی گیری شروع می‌شود. صبر کنید تا این عمل تمام شود.



۶. در این مرحله پشتیبان گیری شروع و پایان می‌پذیرد، در آخر بر روی Close کلیک کنید.

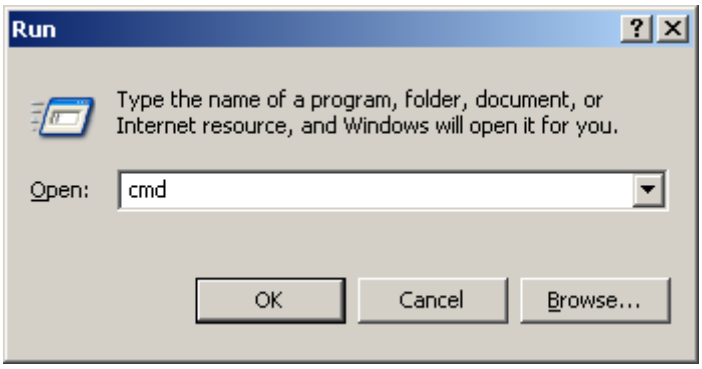


توجه: توصیه می‌شود پشتیبان را حتما در حالت Normal انجام دهید و از انواع دیگر پشتیبان گیری مانند Incremental یا Differential خودداری کنید.

۲۶-۴-۲- پشتیبان گیری توسط خط فرمان

برای تهیه پشتیبان توسط خط فرمان (Command Line) مراحل زیر را طی کنید:

۱. از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.



۲. در خط فرمان با استفاده از دستور ntbackup به صورت زیر می‌توان پشتیبان تهیه کرد:

Ntbackup backup systemstate /J 'Backup Job' /F 'C:/systemstate.bak'



ntbackup: ابزار پشتیبان گیری از طریق خط فرمان می‌باشد.

Backup: مشخص کننده این است که عملیات پشتیبان گیری صورت می‌پذیرد.

Systemstate: مشخص کننده این است که از System State پشتیبان گرفته می‌شود.

F/: نام فایل پشتیبان و محل آن را مشخص می‌کند.

ایجاد تغییراتی برای آزمایش:

اکنون برای آزمایش باز گردانی اطلاعات کاربر Reza که ایجاد کرده بودید را حذف کنید.

۲۶-۵- بازگرداندن اطلاعات Restore Active Directory

در ویندوز سرور ۲۰۰۳ برای باز گردانی پایگاه داده Active Directory در صورت تنظیمات اشتباه، خرابی یا از دست دادن اطلاعات، به دلیل مشکلات سخت‌افزاری و نرم‌افزاری شیوه‌های مختلفی وجود دارد. در ساده ترین حالت در صورت وجود چندین DC می‌توان DC دیگری را نصب و سپس به واسطه Replication بین DCها تمامی اطلاعات به DC جدید منتقل خواهد شد؛ راه دیگر استفاده از ابزار پشتیبان گیری برای بازگرداندن اطلاعات می‌باشد.

توجه داشته باشید که وقتی از یک Domain Controller پشتیبان تهیه می‌کنید، از تمامی داده‌های Active Directory به همراه پوشه SYSVOL و Registry بر روی سرور پشتیبان گرفته می‌شود. پس در موقع بازگرداندن آن، هر آنچه پشتیبان گرفته شده همچون تنظیمات Group Policy و رجیستری هم به حالت قبل باز می‌گردد.

۲۶-۵-۱- شیوه‌های بازگرداندن پشتیبان

برای بازگرداندن پشتیبان Active Directory، 3 روش وجود دارد:

۱. **Primary**
۲. **Normal (NonAuthoritative)**
۳. **Authoritative**

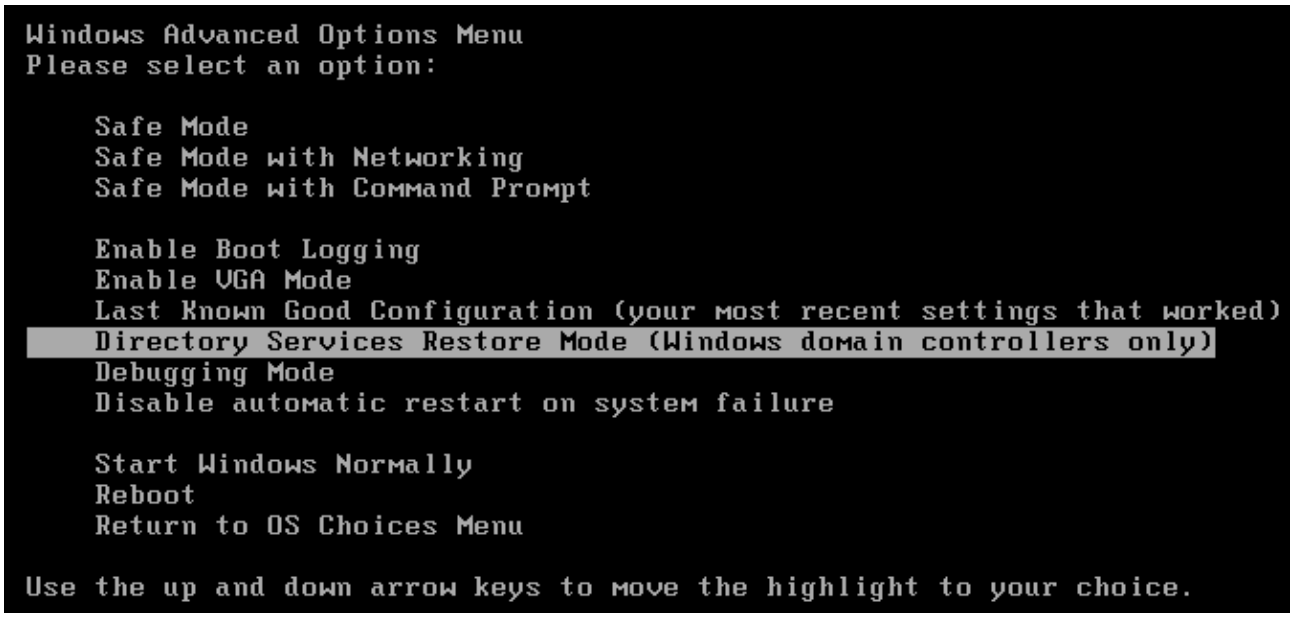
۱. **Primary:** این شیوه اولین Domain Controller را مجددا ایجاد می‌کند، وقتی هیچ راه دیگری برای ایجاد دوباره Domain وجود ندارد. این شیوه زمانی کاربرد دارد که هیچ DC دیگری در شبکه وجود ندارد و می‌خواهید DC اصلی را توسط پشتیبان مجدد ایجاد کنید.
۲. **Normal:** این شیوه دوباره Active Directory را به حالت قبل از پشتیبان گیری بر می‌گرداند و سپس به واسطه Replicate بین DCها بروز می‌شود. این شیوه زمانی استفاده می‌شود که چندین DC در شبکه وجود دارد و می‌خواهید یک DC را به آخرین وضعیت مناسب آن بر گردانید.
۳. **Authoritative:** این شیوه پشت سر Normal استفاده می‌شود. بدین معنی که مراحل همانند Normal صورت می‌پذیرد؛ منتها در آخر کار، یک سری داده‌ای مشخص را نشانه دار می‌کنید تا در Replicate بین DCها برعکس Normal بازنویسی نشوند.

فرض کنید اشتباها یک OU را حذف کرده‌اید و در Replicate بین دومین‌ها این OU در تمام DCهای دیگر هم حذف شده است، هم اکنون برای باز گرداندن آن فقط می‌توانید از شیوه Authoritative استفاده کنید، زیرا به علت وجود DC از شیوه Primary نمی‌توان استفاده کرد، در صورت استفاده از Primary کلیه اطلاعات بعد از پشتیبان گیری از بین می‌رود؛ در صورت استفاده از شیوه Normal به خاطر Replicate بین DCها، OU که در DCهای دیگر پاک شده است در DC جدید هم پاک می‌شود پس باید با مشخص کردن آن به صورت Authoritative از بازنویسی آن جلوگیری کرد.

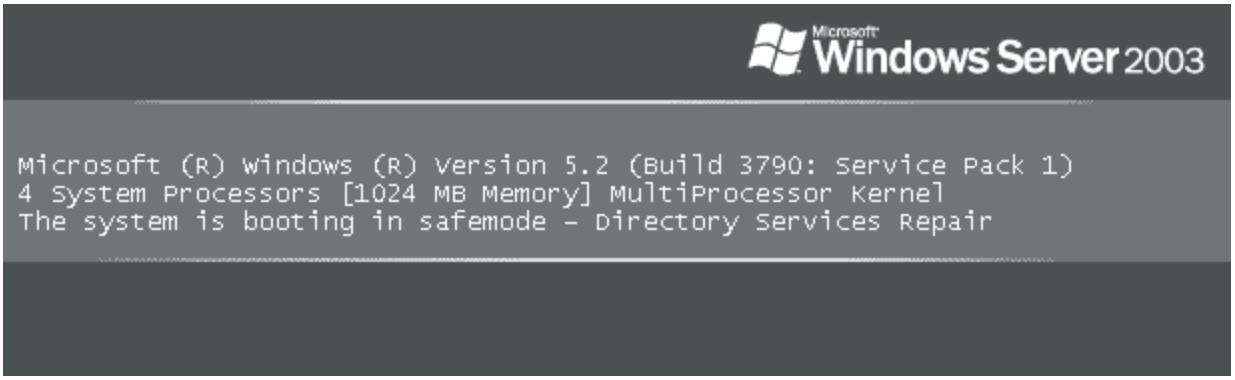
۲۶-۵-۲- نحوه بازگرداندن به صورت Primary

برای بازگرداندن پشتیبان مراحل زیر را طی کنید:

۱. Domain Controller (کامپیوتر سرور) را در حالت Directory Services Restore Mode شروع مجدد کنید. یعنی قبلاً از بالا آمدن ویندوز، کلید F8 را فشار دهید تا صفحه زیر نمایان شود. در این صفحه گزینه Directory Services Restore Mode را انتخاب نمایید.



۲. بدین ترتیب سیستم در حالت Safe Mode و AD Repair بالا می‌آید.

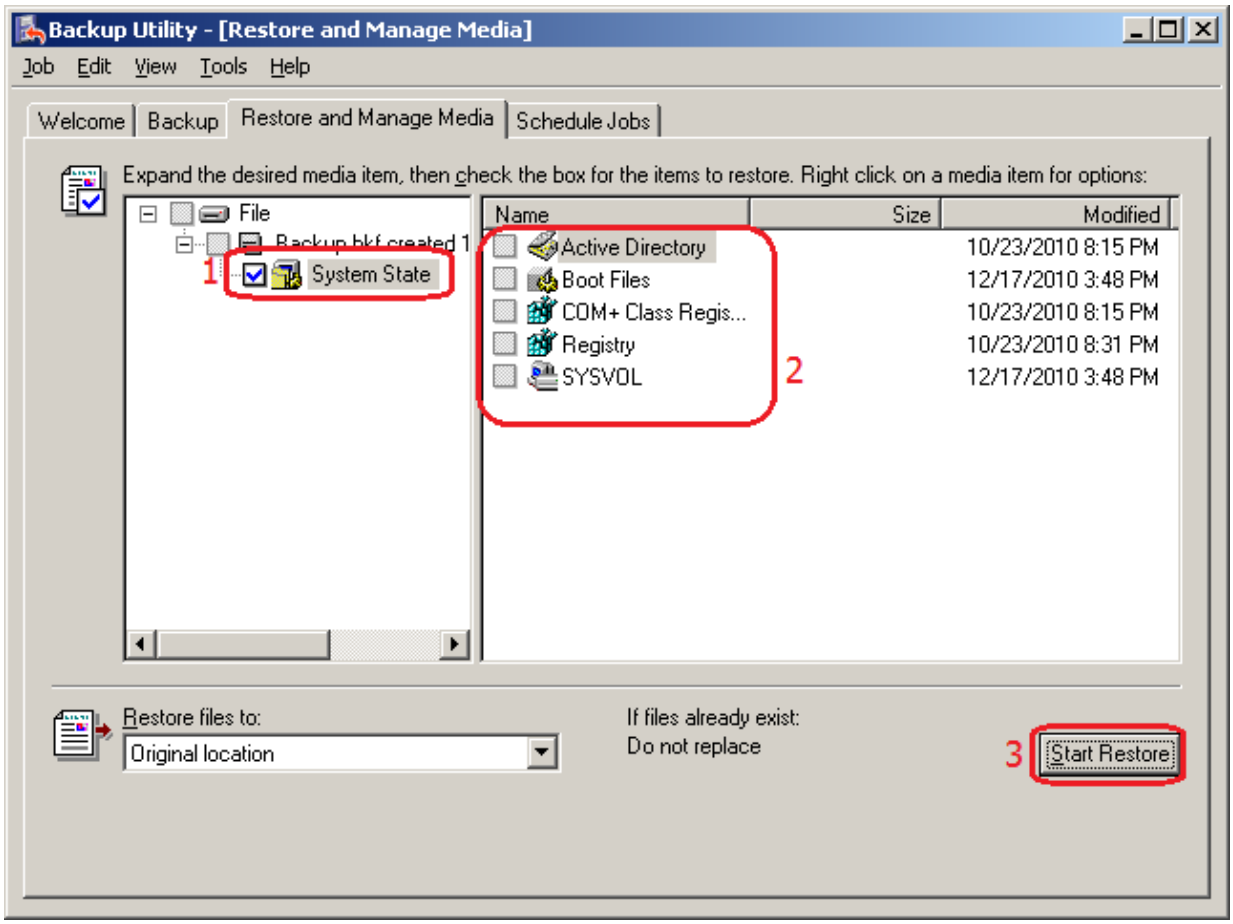


۳. از منوی شروع آدرس زیر را جهت اجرای Backup Utility طی می‌کنیم:

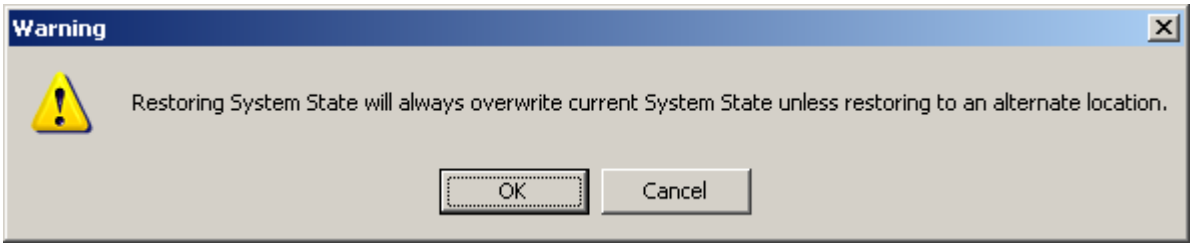
Start Menu ➔ All Programs ➔ Accessories ➔ System Tools ➔ Backup



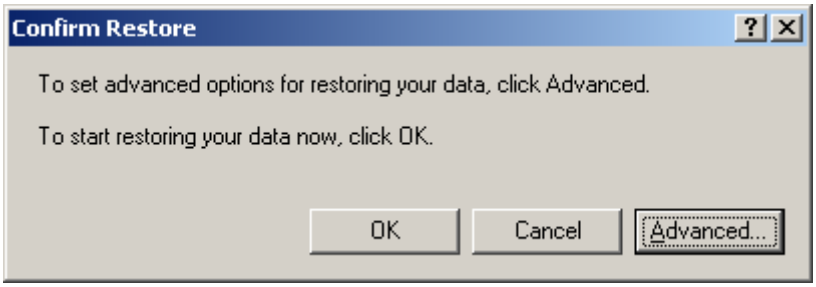
۴. در پنجره Backup or Restore Wizard بر روی Advance mode کلیک کنید. (به تصاویر بالایی مراجعه نمایید). در سربرگ Restore and Manage Media هر آنچه که می‌خواهید بازگردانید (که در اینجا System State می‌باشد) را انتخاب و سپس بر روی Start Restore کلیک کنید.



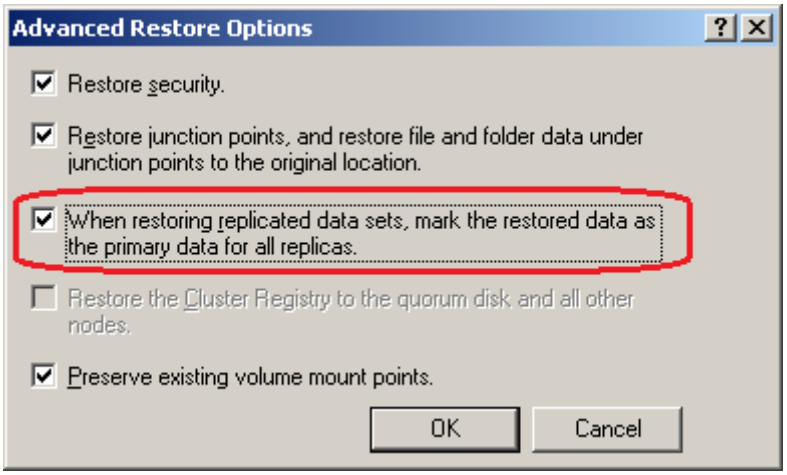
۵. یک صفحه هشدار دهنده باز می‌شود که OK را می‌بایست انتخاب کنید.



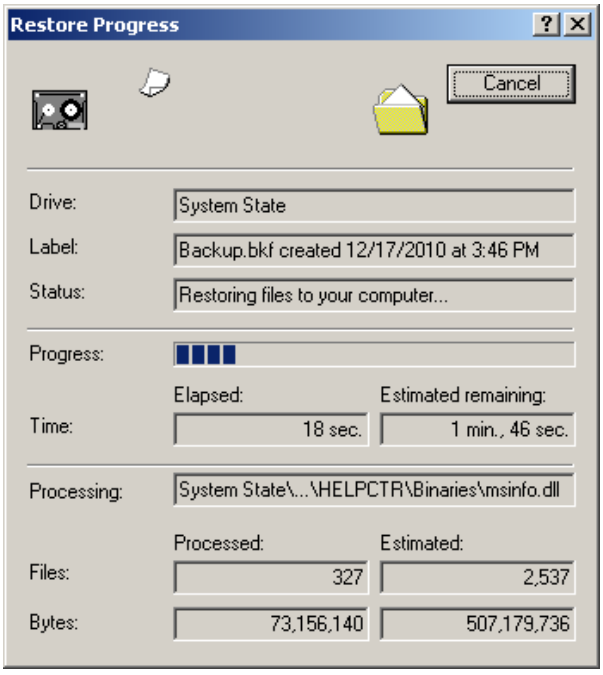
۶. در Confirm Restore بر روی Advanced کلیک کنید.



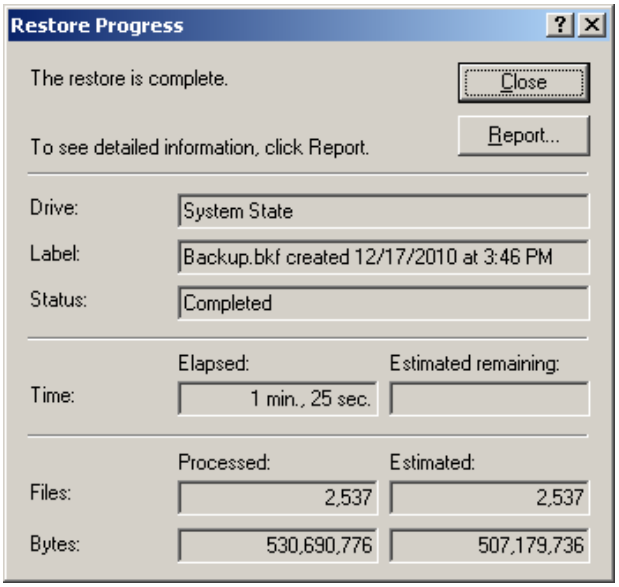
۷. در پنجره Advanced Restore options، گزینه When restoring replicated data sets, mark the restored data as the primary data for all replicas را انتخاب و سپس بر روی OK کلیک کنید.



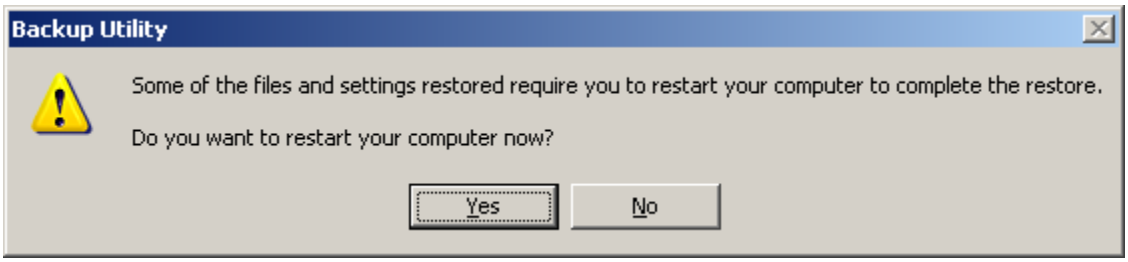
۸. صبر نمایید تا سیستم اطلاعات را Recovery کند.



۹. در این مرحله باز گردانی پشتیبان پایان می‌پذیرد. بر روی Close کلیک کنید.



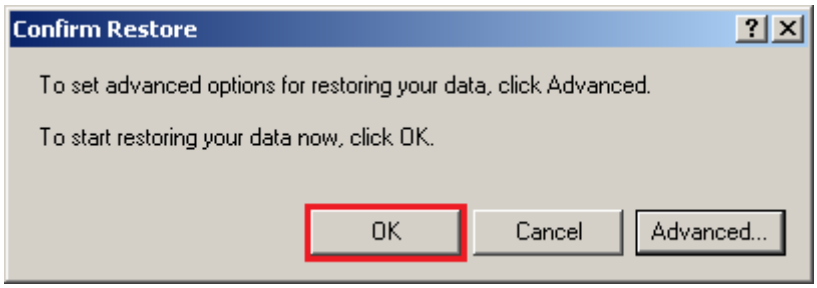
۱۰. در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می‌شود که شما Yesرا انتخاب کنید.



۲۶-۵-۳- نحوه بازگرداندن به صورت Normal

برای بازگرداندن پشتیبان مراحل زیر را طی کنید:

مانند روش باز گردانی Primary، مراحل را طی نمایید تا پنجره Confirm Restore باز شود. اما این بار روی دکمه OK کلیک کنید.

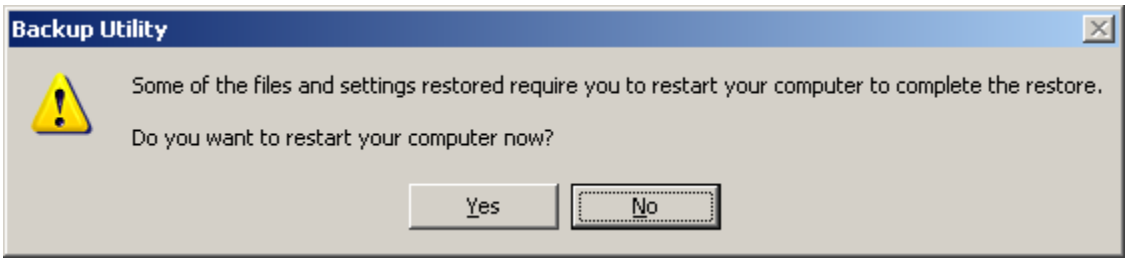


بقیه مراحل مانند روش Primary می‌باشد.

۲۶-۵-۴- نحوه بازگرداندن به صورت Authoritative

۱. مانند روش باز گردانی Normal، مراحل را طی نمایید (یعنی در صفحه Confirm Restore روی OK کلیک کنید) و ادامه دهید تا پنجره Backup Utility باز شود

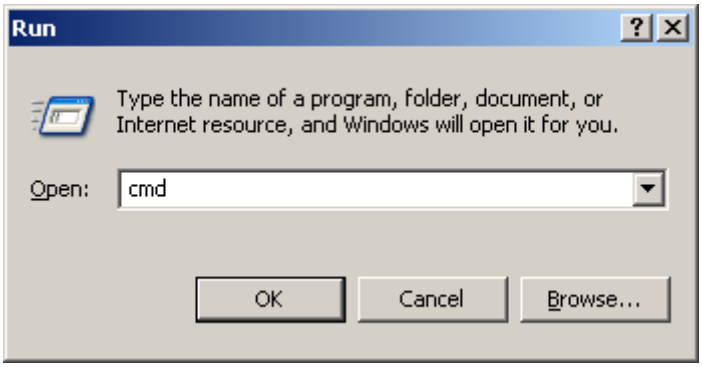
۲. در پنجره Backup Utility پیغامی مبنی بر شروع مجدد سیستم ظاهر می‌شود، که بر عکس شیوه Normal می‌بایست No را انتخاب کنید.



تفاوت شیوه Normal با Authoritative از همین مرحله آغاز می‌شود که یک سری داده را برای جلوگیری از بازنویسی در Replicate بین DCها نشانه دار می‌کنید.

۳. از منوی Start برنامه CMD را از آدرس زیر اجرا کنید.

Start ➔ Run ➔ Enter 'CMD' ➔ OK



۴. در خط فرمان Ntdsutil را اجرا کنید. سپس در اعلان Ntdsutil، عبارت Authoritative Restore را تایپ و اجرا کنید.

توجه: در اعلان Authoritative Restore برای نشانه گذاری بدین ترتیب عمل کنید:

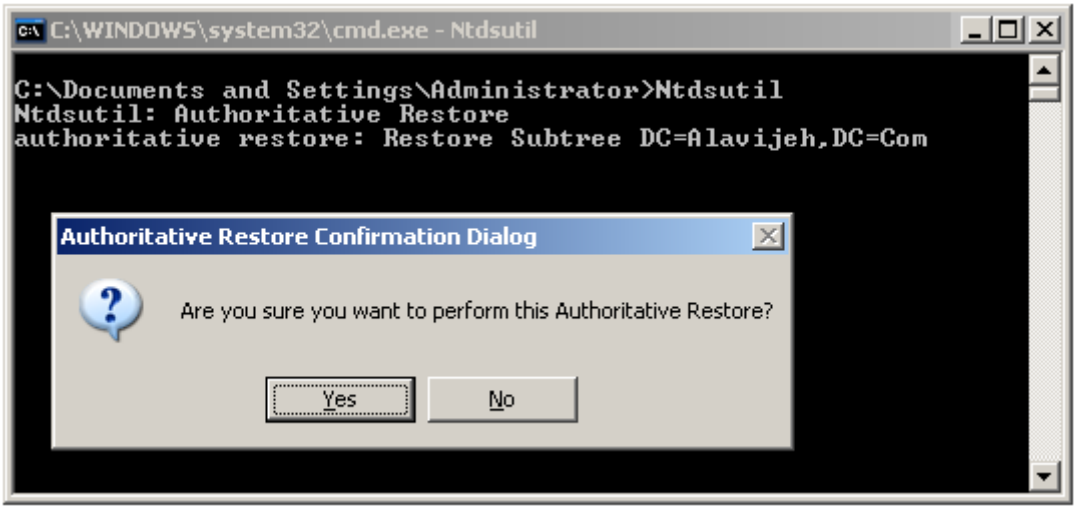
Restore SubTree Distinguished_Name_Of_Object

Distinguished Name، آدرس عنصر (Object) مورد نظر در Active Directory می‌باشد.

برای مثال برای نشانه گذاری دامنه Alavijeh.Com که در برای آزمایش حذف کرده بودید، بدین ترتیب عمل می‌کنیم:

Restore Subtree DC=Alavijeh,DC=Com

سپس در پنجره ظاهر شده Yes را انتخاب کنید.



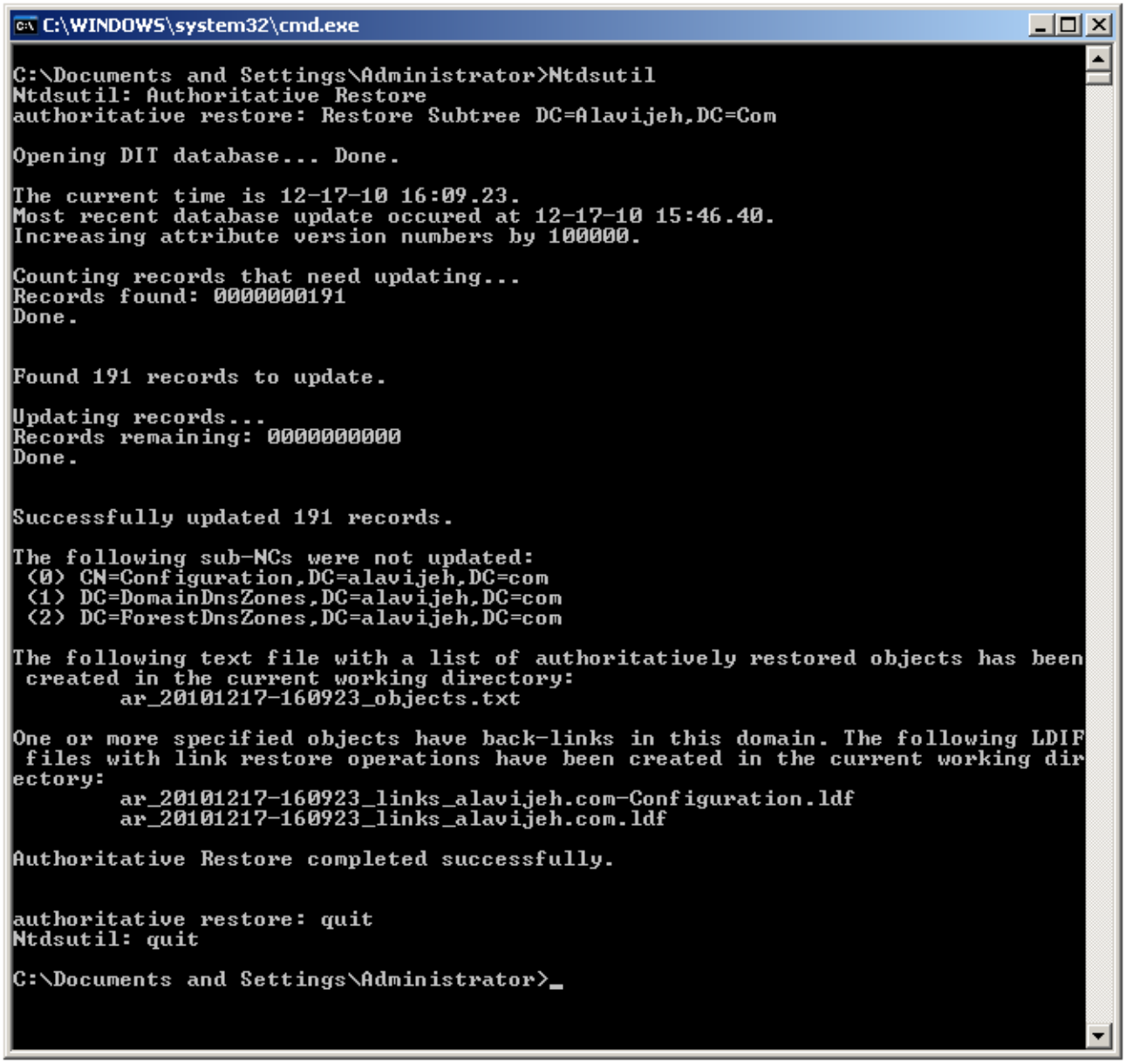
نکته: نشانه گذاری کل پایگاه داده و تنظیمات به صورت Authoritative به این نحو انجام می‌شود:

Restore Database

۵. Object مورد نظر با موفقیت نشانه گذاری شد، حال دو مرتبه quit را تایپ و اجرا کنید تا از اعلان ntdsutil خارج شوید.

توجه داشته باشید که Objectی همانند OU به همراه تمامی Objectهای دیگری که در بر دارد مانند گروه‌ها و کاربر هایش نشانه گذاری می‌شود.

به شکل صفحه بعد دقت نمایید.



۶. Domain Controller را شروع مجدد کنید (Restart) و سیستم عامل را در حالت عادی اجرا کنید.

فصل ۲۷

DHCP Server

در این فصل در مورد DHCP که یکی از مهمرین سرویس‌های شبکه و اینترنت است صحبت خواهد شد.

۲۷-۱- آشنایی با DHCP Server

DHCP Server به شما امکان می‌دهد تا آدرس‌های IP، Gateway، DNS، Subnet Mask، WINS و... را به صورت اتوماتیک از سرور دریافت کنید. در واقع اگر کارت شبکه‌ی شما در حالت خودکار تنظیم شده باشد، هنگام بوت شدن، درخواستی را به DHCP Server ارسال کرده و آدرس‌های مورد نیاز خود را دریافت می‌کند. به این صورت تمامی روند دادن آدرس IP به صورت خودکار انجام خواهد شد. یک ایستگاه کاری (Client) در شبکه برای اتصال به سرور و تماس با دیگر کامپیوترها نیاز به یک آدرس منطقی به نام آدرس IP دارد. وقتی در یک شبکه محلی تعداد زیادی کامپیوتر وجود داشته باشد، یک مدیر شبکه امکان تخصیص و تنظیم آدرس IP برای همه آن‌ها به صورت دستی را نخواهد داشت و وقت بسیار زیادی برای تنظیم آدرس IP تک تک ایستگاه‌ها صرف خواهد شد. سرویس DHCP این امکان را فراهم می‌آورد که یکی از سیستم‌ها (در اینجا سرور Windows 2003) به صورت اتوماتیک و بدون دخالت مدیر شبکه به سیستم‌های کاری یا Clientها آدرس IP اختصاص دهد. DHCP مخفف کلمات Dynamic Host Configuration Protocol است؛ یعنی پروتکل تنظیم پویای میزبآن‌ها (Host). منظور از Host در این جمله همان کامپیوتر یا ایستگاه‌های داخل شبکه است.

۲۷-۱-۱- ویژگی‌های DHCP

۱. **جلوگیری از Conflict:** اگر به صورت حرفه‌ای با شبکه کار کرده باشید، حتما با پیغامی مبنی بر وجود دو آدرس IP یکسان در شبکه برخورد کردهاید. این اتفاق زمانی رخ می‌دهد که دو سیستم واقع در یک شبکه، از یک آدرس IP استفاده کنند. اما این مشکل با استفاده از DHCP حل خواهد شد و بدین ترتیب می‌توانیم مطمئن باشیم چنین اتفاقی نخواهد افتاد.

نکته: بعد از راه اندازی DHCP Server و با تنظیمات پیش فرض آن، باز هم احتمال رخ دادن Conflict وجود دارد.

۲. **سرعت بخشیدن به کارها:** در یک شبکه‌ی بزرگ که از DHCP استفاده نمی‌کنند، اگر شما بخواهید آدرس DNS Server را تغییر بدهید، چه اتفاقی می‌افتد؟ اتفاق خاصی نمی‌افتد ولی باید آدرس DNS تک تک سیستم‌ها

را تغییر دهید. در صورتی که اگر یک DHCP Server در شبکه وجود داشته باشد، کافی است آدرس DNS مورد نظرتان را در آن وارد کنید.

۳. **مدیریت متمرکز:** که باز هم می‌توانیم مثال بالا را برای آن ذکر کنیم. به جای عوض کردن آدرس DNS تک تک سیستم‌ها، می‌توانید از طریق یک سیستم و به صورت متمرکز، به خواسته‌های خود جامه‌ی عمل بپوشانید.

۴. **ضرورت:** در بعضی از شرایط، مجبور به استفاده از DHCP Serverها هستیم. مثلاً هنگامی که شما از یک ISP اینترنت دریافت می‌کنید، مدیر آن برای دادن آدرس IP به منزل شما مراجعه نمی‌کند. تمامی این فرایندها از طریق راه دور و البته DHCP Server صورت می‌گیرد.

۲۷-۱-۲- جایگاه سرویس دهنده DHCP در یک شبکه مبتنی بر ویندوز ۲۰۰۳

به منظور بکارگیری DHCP در یک محیط ویندوز ۲۰۰۳، از رویکردهای متفاوتی استفاده می‌گردد. با توجه به اینکه DHCP پروتکلی است که دارای محدودیت‌های امنیتی خاص خود است، سرویس DHCP نباید به خارج ارائه گردد. همچنین به Domain Serverهای حیاتی و ماشین‌های سرویس گیرنده مهم، می‌بایست آدرس‌های IP ثابتی نسبت داده شود که ارتباطی با DHCP نخواهد داشت. سرویس DHCP Client بر روی ماشین‌های حساس، غیرفعال گردد. در زمان نصب ویندوز ۲۰۰۳ (هم سرویس دهنده و هم سرویس گیرنده)، سرویس DHCP Client فعالیت خود را آغاز و به عنوان یک سیستم محلی اجراء خواهد شد. سرویس دهندگان DHCP و سایر ماشین‌های حساس دیگر که از آدرس‌های IP ثابتی استفاده می‌نمایند به این سرویس نیاز نداشته و لازم است که سرویس فوق، متوقف و وضعیت فعالیت آن در زمان راه اندازی سیستم به حالت دستی (Manually) تغییر یابد.

۲۷-۱-۳- پیکربندی سرویس دهنده DHCP

سرویس دهنده DHCP به صورت اتوماتیک آدرس‌های IP و سایر اطلاعات مرتبط با پیکربندی TCP/IP را در اختیار سرویس گیرندگان DHCP-Enabled، قرار می‌دهد. سرویس دهنده DHCP به عنوان یک سیستم محلی اجراء می‌گردد. به منظور کاهش احتمال بروز خرابی و اشکالات حاصل از عوامل جانبی، پیشنهاد می‌گردد که سرویس دهنده DHCP بر روی یک Domain Server که یک Domain Controller نمی**باشد**، نصب گردد. جایگاه سرویس دهندگان DHCP، بسیار حساس و مهم بوده و می‌بایست تمامی آنان دارای آدرس‌های IP ثابت باشند. سرویس DHCP Client می‌بایست برروی این نوع از سیستم‌ها متوقف و وضعیت اجراء آن در زمان راه اندازی سیستم، به صورت دستی در نظر گرفته شود.

۲۷-۱-۴- پیکربندی سرویس گیرندگان DHCP

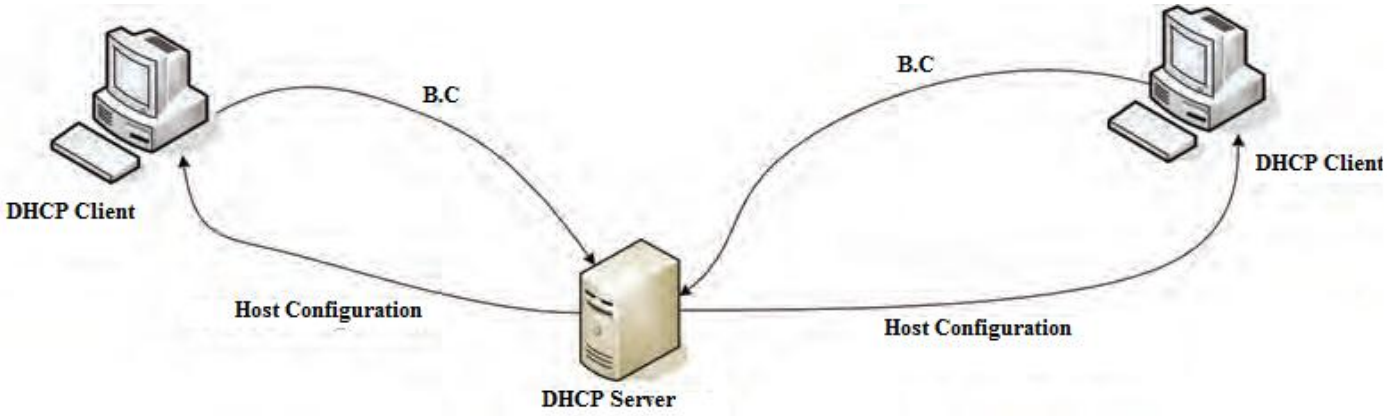
سرویس DHCP Client، به صورت اتوماتیک درخواست هایی را برای سرویس دهنده DHCP به منظور دریافت یک آدرس IP و نسبت دهی آن به ماشین سرویس گیرنده، انجام می‌دهد. درخواست فوق، در زمان راه اندازی سیستم (Booting) انجام و در صورت ضرورت و قبل از اتمام تاریخ اعتبار آن (نصف زمان تاریخ انقضاء)، تکرار خواهد شد. سرویس DHCP Client به عنوان یک سیستم محلی بر روی ماشین سرویس گیرنده اجراء خواهد شد. پیشنهاد می‌گردد که از خدمات DHCP بر روی ماشین‌های سرویس گیرنده حساس و مهم **استفاده نگردد**. این نوع از ماشین‌های سرویس گیرنده، می‌بایست از

آدرس‌های IP ثابتی استفاده و بر روی آنان سرویس DHCP Client متوقف و نحوه راه اندازی آنان در زمان راه اندازی، به صورت دستی یا ایستا تعیین گردد.

منظور از DHCP Client، سرویسی است که در طی فرآیند راه اندازی (Boot)، با سرویس دهنده DHCP ارتباط برقرار کرده و پیکربندی لازم را از آن دریافت می‌کند. بدیهی است که این سرویس بایستی روی کلیه ایستگاه هایی که پیکربندی آن‌ها می‌خواهد به طور خودکار انجام شود، فعال گردد.

در سیستم عامل ویندوز، نسخه‌های XP، 2000، 2003، 2008، Vista و ۷، با مراجعه به کنسول سرویس‌ها (Services.msc)، می‌توان فعال بودن این سرویس را بررسی کرد. وضعیت سرویس باید در حالت Started باشد.

همانطور که از شکل زیر پیدا است، DHCP Client پس از فعال شدن روی ایستگاه‌ها با استفاده از Broadcast (به اختصار BC) سرویس دهنده را پیدا کرده و بعد از طی مراحلی کوتاه، پیکربندی لازم را از سرویس دهنده دریافت می‌کند.



حال چنانچه DHCP Server در شبکه نباشد و یا در زمان مناسب، به دلایلی مانند ترافیک، شبکه نتواند پاسخ لازم را به کلاینت بدهد، در آن صورت بسته به رفتار سیستم عامل کلاینت، ممکن است یکی از حالات زیر اتفاق بیفتد:

الف) سرویس گیرنده پیکربندی نمی‌شود. در سیستم عامل‌های مایکروسافت Win 95 و NT 4.0 چنین اتفاقی می‌افتد که با مراجعه به Command Prompt و وارد نمودن دستور ipconfig یا winipcfg می‌بینیم که آدرس به صورت 0.0.0.0 است و این موضوع نشان می‌دهد که آدرس IP در سرویس گیرنده پیکربندی نشده است.

ب) سرویس گیرنده به طور خودکار و تصادفی یک آدرس به خود می‌دهد. سیستم عامل‌های Me، Win 98، XP، 2000، 2003، 2008، Vista و ۷ چنین رفتاری دارند که با مراجعه به Command Prompt و وارد کردن دستور ipconfig یا winIPcfg می‌بینیم که آدرس تصادفی در محدوده 169.254.X.Y (یعنی از ۱۶۹.۲۵۴.۰.۱ تا ۱۶۹.۲۵۴.۲۵۵.۲۵۴) با Subnet Mask کلاس B یعنی ۲۵۵.۲۵۵.۰.۰ تنظیم شده است. به این روش تخصیص آدرس به صورت تصادفی، اصطلاحا APIPA (Automatic Private IP Addressing) می‌گویند. البته کلاینت بعد از انتخاب یک آدرس تصادفی، با دیگر کلاینت‌های موجود در شبکه برای بررسی تکراری بودن آدرس IP مذاکره می‌کند.

متاسفانه روش APIPA مکانیزم مناسبی برای پیکربندی در شبکه‌ها نیست. زیرا:

- غیر از IP و Subnet Mask، پارامتر دیگری را تنظیم نمی‌کند (از قبیل Router یا DNS)
- ترافیک شبکه را افزایش می‌دهد (می خواهد بررسی کند که آیا آدرس تکراری است یا خیر)

- غیر از محدوده 169.254.X.Y، محدوده دیگری را نمی‌توان روی آن تنظیم کرد. به عبارت دیگر، APIPA قابل تنظیم نیست.

نکته: در فرآیند APIPA، پس از آن که سرویس گیرنده آدرس را به صورت تصادفی برای خود انتخاب کرد، آن را تا مدت کوتاهی (حدود ۵ دقیقه) نگه داشته و سپس مجددا به دنبال DHCP Server می‌گردد؛ که البته این جستجو با Broadcast انجام می‌شود. حال اگر بتواند از آن جواب بگیرد، در آن صورت پیکربندی خود را طبق دستور العمل سرویس دهنده انجام می‌دهد و در غیر اینصورت، یعنی نگرفتن پاسخ از DHCP Server، همان آدرس تصادفی قبلی را استفاده می‌کند و این فرآیند مرتبا تکرار می‌شود؛ یعنی حدوداً هر ۵ دقیقه یکبار، به روش Broadcast به دنبال DHCP Server می‌گردد و این امر افزایش ترافیک بیش از حد در شبکه‌های متوسط و بزرگ را به همراه خواهد داشت.

ج) سرویس گیرنده به طور خودکار با آدرس از پیش تعیین شده تنظیم شود. در سیستم عامل ویندوز نسخه‌های XP و ۲۰۰۳ (و نسخه‌های جدید تر) چنین قابلیتی وجود دارد که اگر سرویس گیرنده‌ای، DHCP Server را پیدا نکند، با آدرس و سایر پارامترهای دیگری که از قبل تعریف شده است، خود را تنظیم کند. این حالت اصطلاحا Alternate Configuration نام دارد.

۲۷-۲- نصب DHCP Server

قبل از اینکه اقدام به نصب DHCP نماییم، لازم است حداقل یک IP Address به صورت Static یا دستی برای دستگاهی که قرار است سرویس DHCP را برای شبکه فراهم آورد تعریف کرد. این دستگاه در این بحث، همان ویندوز سرور ۲۰۰۳ می‌باشد. در صورتیکه این کار انجام نپذیرد، در هنگام نصب DHCP، سیستم مذکور پیغام زیر را می‌دهد.

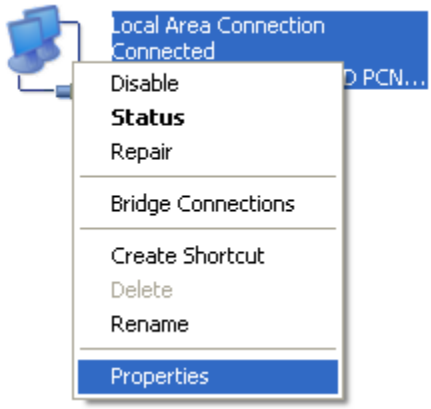


۲۷-۲-۱- تنظیم IP Address برای سرور (به صورت دستی)

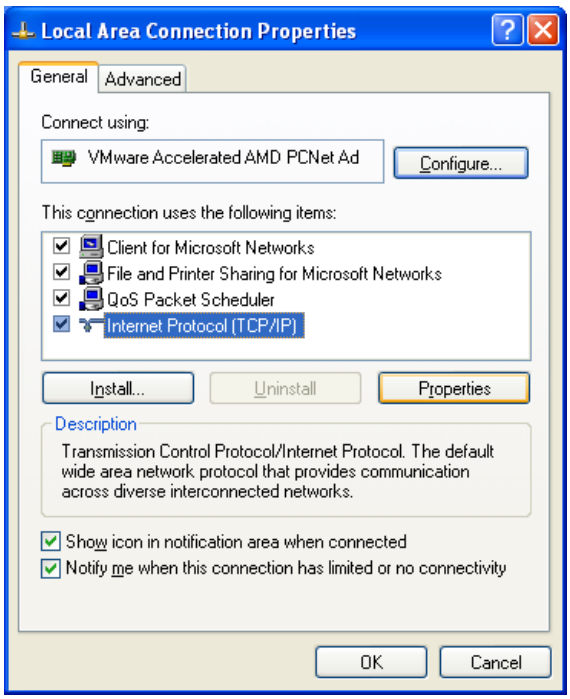
از مسیر زیر پنجره Local Area Connection را باز کنید (البته چندین راه برای این کار وجود دارد).

Start ➔ Control Panel ➔ Network Connections ➔ Local Area Connection

روی گزینه Local Area Connection راست کلیک کرده و گزینه Properties را انتخاب کنید تا پنجره Local Area Connection Properties فعال گردد.

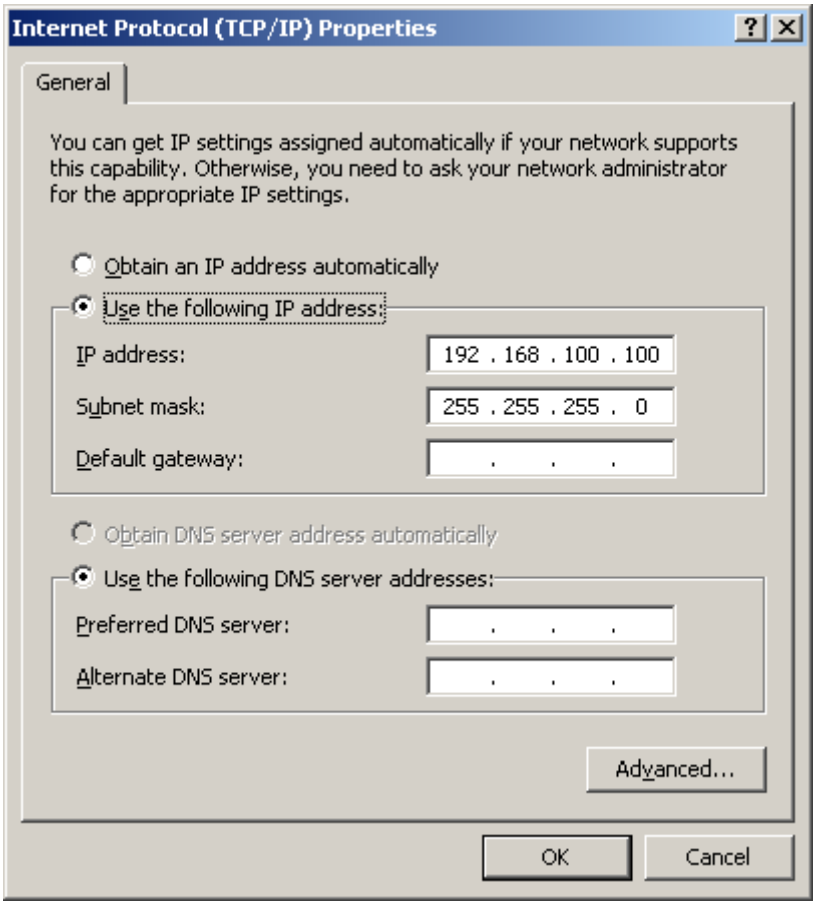


در شکل زیر، گزینه Internet Protocol (TCP/IP) را انتخاب و دکمه Properties را بزنید تا پنجره Internet Protocol (TCP/IP) Properties باز شود.



مطابق شکل زیر، می‌توانید آدرس IP که قبلاً بررسی و انتخاب نمودهاید را وارد نمائید. (مثلاً ۱۹۲.۱۶۸.۰.۱۰۰)

در این صفحه، دو قسمت Subnet Mask و Default Gateway را نیز می‌توانید تنظیم نمایید. (تنظیم Subnet Mask ضروری است، ولی تنظیم Default Gateway اختیاری است). در پایان این قسمت دکمه OK را بزنید.



اکنون سرور دارای یک IP Address می‌باشد و می‌توانید برای نصب DHCP Server اقدام نمائید.

۲۷-۲-۲- نصب DHCP Server

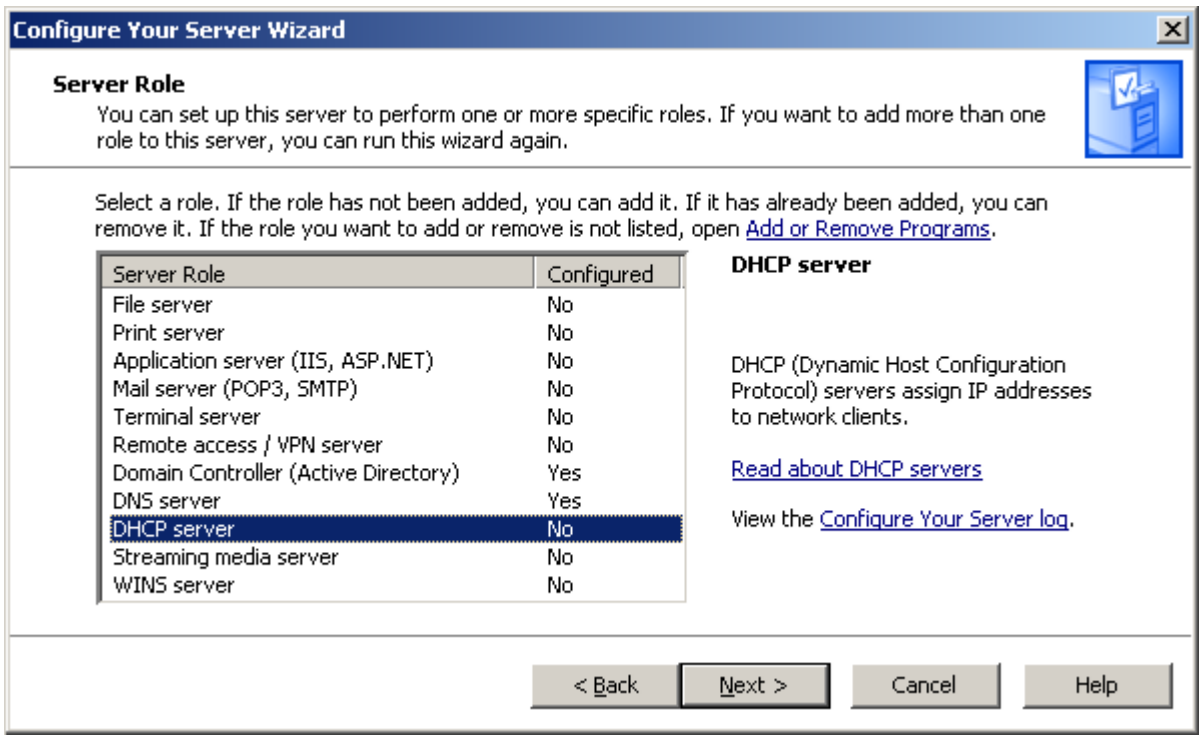
برای شروع نصب، در ویندوز سرور وارد مسیر Start ➔ Administrative Tools ➔ Configure Your Server Wizard شوید.



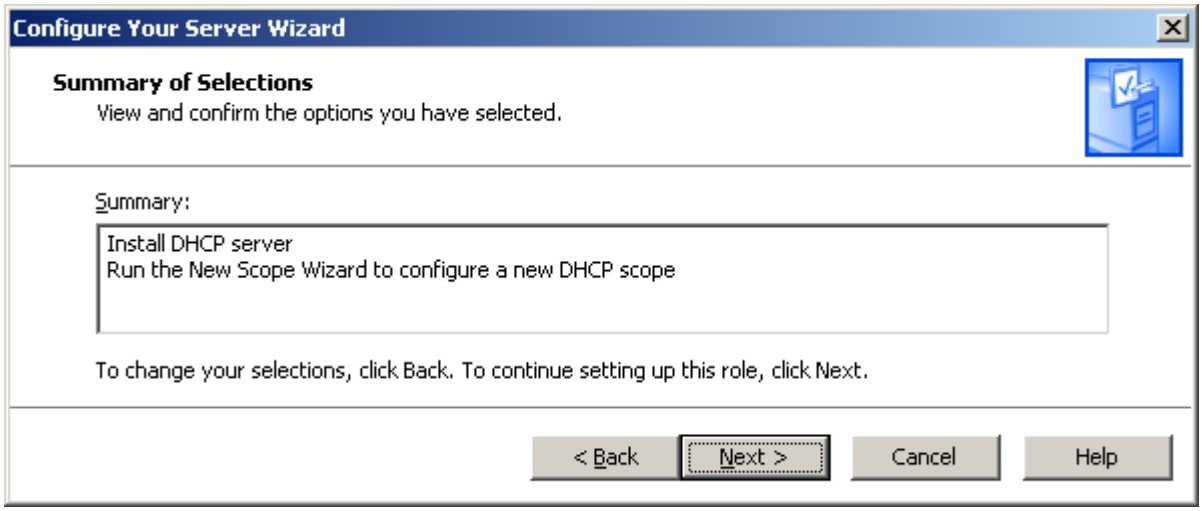
در صفحه خوش آمد گویی، دکمه Next را بزنید.

مجددا Next را بزنید.

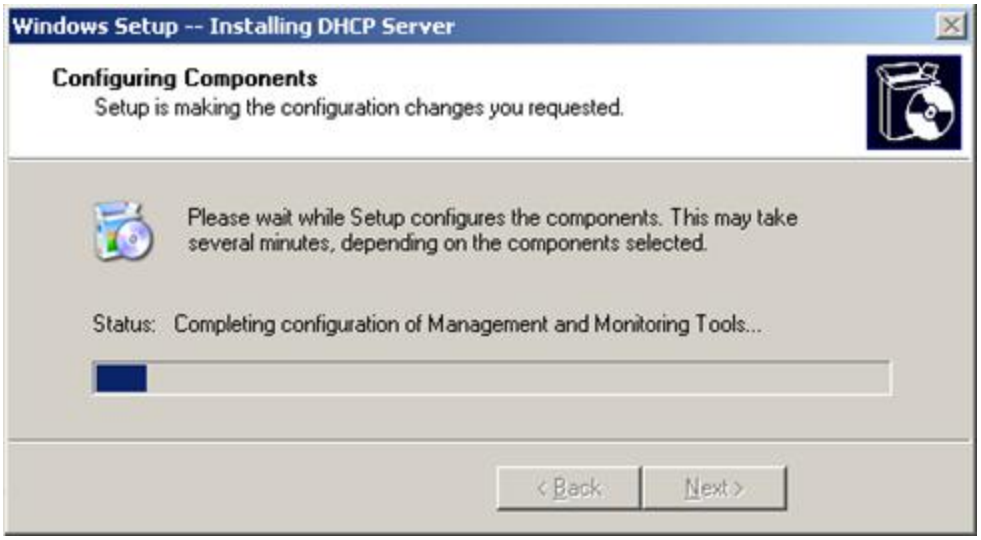
در صفحه باز شده، گزینه DHCP Server را انتخاب کنید، این بدان معناست که می‌خواهید نقش DHCP Server را به این کامپیوتر بدهید. سپس روی دکمه Next کلیک کنید.



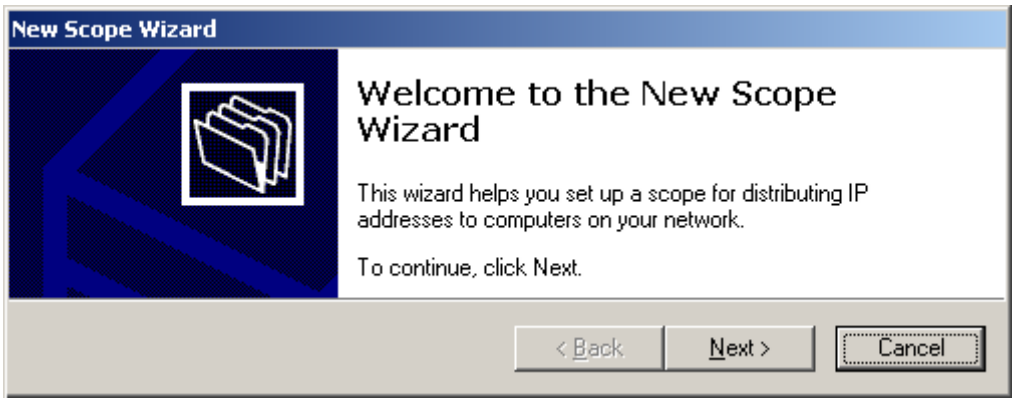
مجددا روی دکمه Next کلیک کنید.



صبر کنید تا سیستم، DHCP Server را نصب کند. در صورتی که سیستم از شما CD ویندوز را خواست، آن را در دستگاه قرار دهید.



در مرحله بعد، سیستم می‌خواهد تنظیماتی را انجام دهد. اما فعلا دکمه Cancel را انتخاب نمایید. زیرا ما قصد داریم این کار را به صورت دستی انجام دهیم.



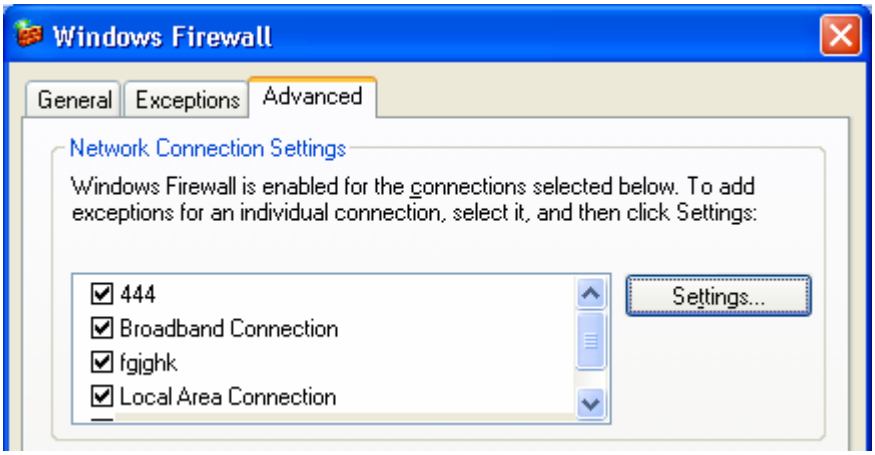
روی دکمه Finish کلیک کنید. توجه نمایید که تا اینجا، عملیات نصب به صورت ناقص انجام شده است. چگونگی تکمیل فرآیند نصب را جلوتر توضیح می‌دهیم.

۲۷-۲-۳- پیکربندی Firewall

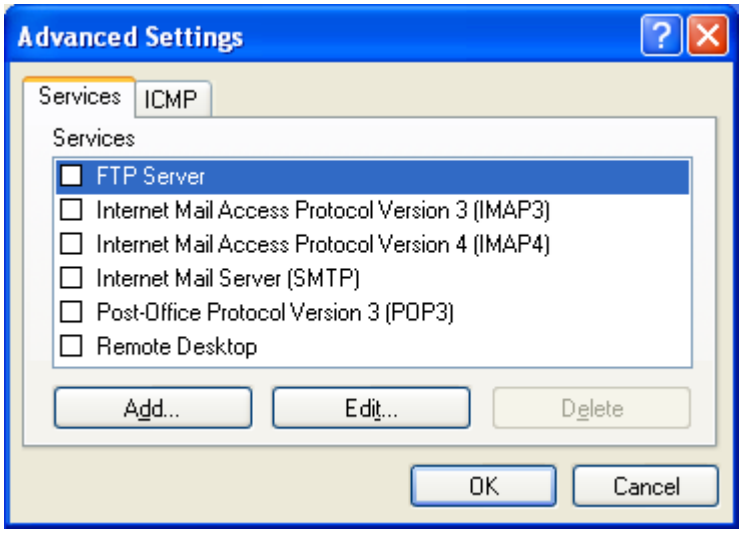
در این مرحله، نوبت به پیکربندی Firewall جهت قادر ساختن آن به منظور دریافت درخواست Clientها برای آدرس IP می‌باشد. یعنی باید به Firewall بگوییم که درخواست‌های تخصیص IP را Reject (رد درخواست) نکند. بدین منظور، ابتدا از طریق Control Panel وارد Windows Firewall شوید. البته اگر Firewall شما غیر فعال باشد، نیازی به تنظیم این بخش نیست.



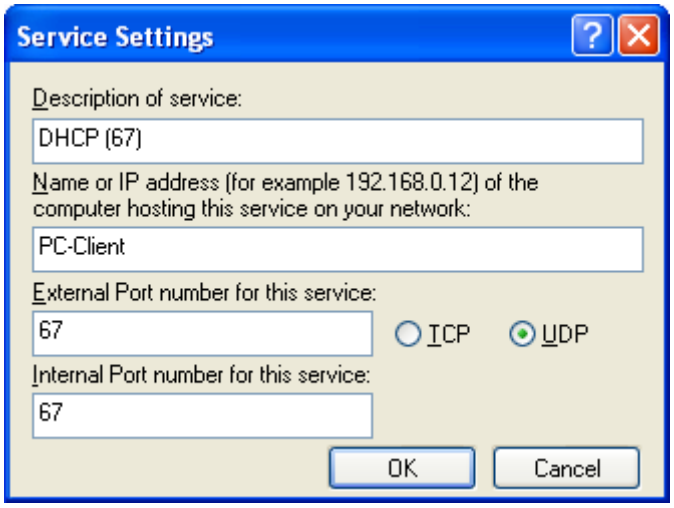
کاری که شما بایستی انجام دهید، این است که به Firewall بگویید که درخواست‌های DHCP را رد نکند. این درخواست‌ها از طریق پورت شماره ۶۷ و به صورت UDP وارد می‌شود. برای تنظیم این مورد، پس از باز شدن Windows Firewall، وارد سربرگ Advanced شده و سپس روی دکمه Settings کلیک کنید.



سپس در صفحه باز شده، برای افزودن پورت شماره ۶۷، روی دکمه Add کلیک کنید.



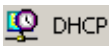
سپس در صفحه باز شده، در جعبه متن اول، نامی دلخواه برای این سرویس وارد نمایید. در جعبه متن دوم، نیز نام کامپیوتر یا آدرس IP کامپیوتری که این سرویس روی آن قرار دارد را وارد نمایید. در دو جعبه متن باقیمانده، عدد ۶۷ را وارد نمایید (عدد ۶۷ بیانگر شماره پورتی است که برای DHCP استفاده می‌شود). در قسمت آخر نیز UDP را انتخاب نمایید. زیرا روش انتقال درخواست DHCP به صورت UDP می‌باشد. در نهایت روی OK کلیک کنید.



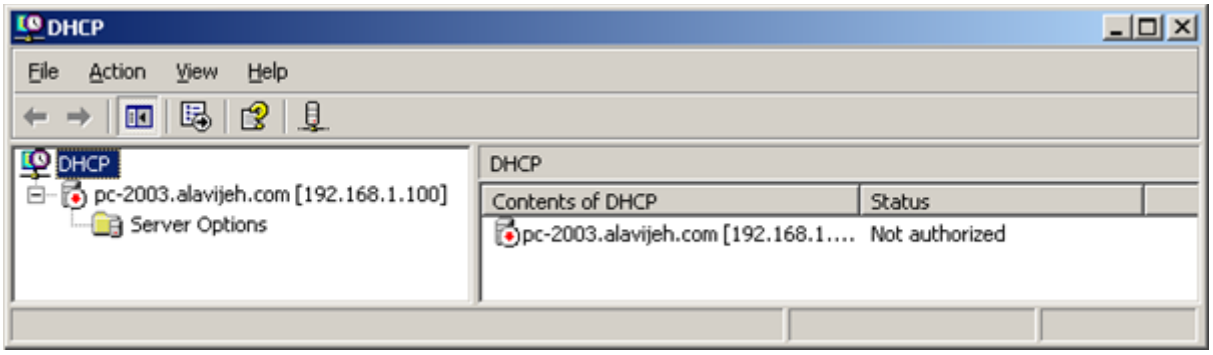
البته اگر Firewall را غیر فعال کنید، نیازی به معرفی پورت به Firewall نخواهد بود.

۲۷-۳- پیکربندی DHCP Server

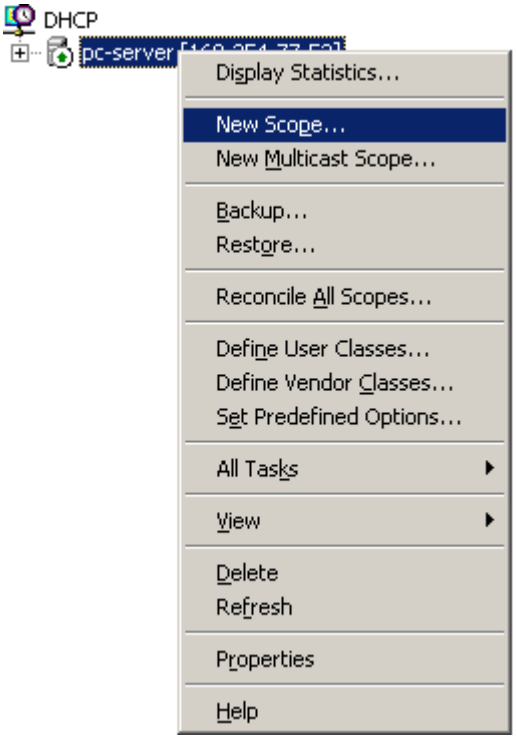
برای پیکربندی، از منوی Start، منوی Administrative Tools، گزینه DHCP را انتخاب نمایید.



با این کار پنجره DHCP باز می‌شود.



برای شروع پیکربندی، ابتدا بایستی یک Scope را ایجاد نمایید. در مباحث تئوری DHCP، گفتیم که DHCP Server، به Clientها آدرس IP تخصیص می‌دهد. DHCP Server، بایستی آدرس IP را بر اساس قواعدی مشخص انتخاب نماید و نمی‌تواند آن را بدون نظم (به قول شیرازی‌ها: هِرلِی) انتخاب نماید. بدین منظور ما بایستی یک Scope تنظیم نماییم. منظور از Scope، محدوده‌ای از آدرس‌های IP است که DHCP Server، IPها را از این محدوده انتخاب خواهد کرد. برای ساخت Scope جدید، روی نام سرور راست کلیک کرده و گزینه New Scope را انتخاب نمایید.



یک Wizard برای تعریف Scope شامل دو بخش است:

الف) مشخصات اولیه شامل:

- **Name Description:** یک نام یا توضیح دلخواه است که برای توصیف Scope استفاده می‌باشد.

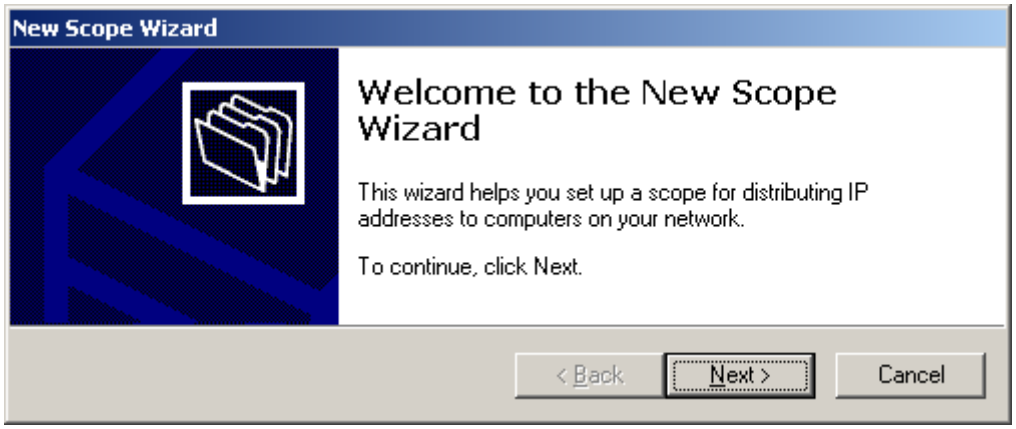
- **IP Address Range Assigned to Client & Subnet Mask:** بیانگر محدوده آدرسی می‌باشد که آدرس کلاینت‌ها از این محدوده انتخاب می‌شود. آدرس شروع و پایان محدوده بایستی هر دو در یک کلاس آدرس IP باشند.
- **IP Address Range Excluded (Not Assign to Clients):** محدوده آدرسی است هیچ آدرسی از داخل آن، نباید به کاربر داده شود. این محدوده بایستی جزئی از محدوده قبلی باشد.
- **Lease Duration:** مدت زمانی است که اطلاعات پیکربندی به کلاینت اجاره داده می‌شود. البته زمانی که مدت دریافت اطلاعات کلاینت به نصف زمان اجاره برسد، کلاینت نسبت به تمدید آن اقدام می‌کند.

ب) مشخصات ثانویه (معروف به Scope Options) که شامل موارد زیر می‌باشد:

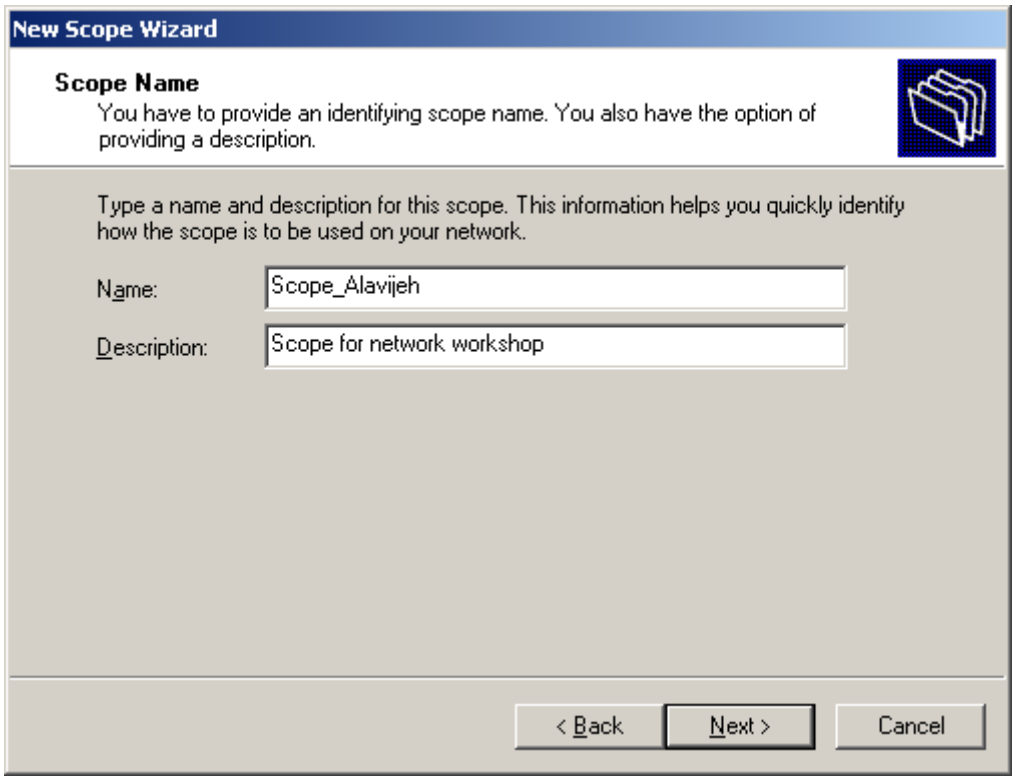
- **Router IP Address (Default Gateway):** آدرس روتری است که کلاینت‌ها به واسطه آن به شبکه‌های دیگر راه پیدا می‌کنند. در رایانه‌های مبتنی بر سیستم عامل ویندوز، این پارامتر تحت عنوان Default Gateway شناخته می‌شود.
- **DNS Server IP Address:** آدرس کامپیوتری است که عملیات تبدیل نام کامپیوتر به آدرس IP را انجام می‌دهد.
- **Domain Name**
- **Win Server IP Address**
- **Node Type**

سه مورد فوق در حالت‌های خاص استفاده می‌شوند. لذا وارد جزئیات نمی‌شویم.

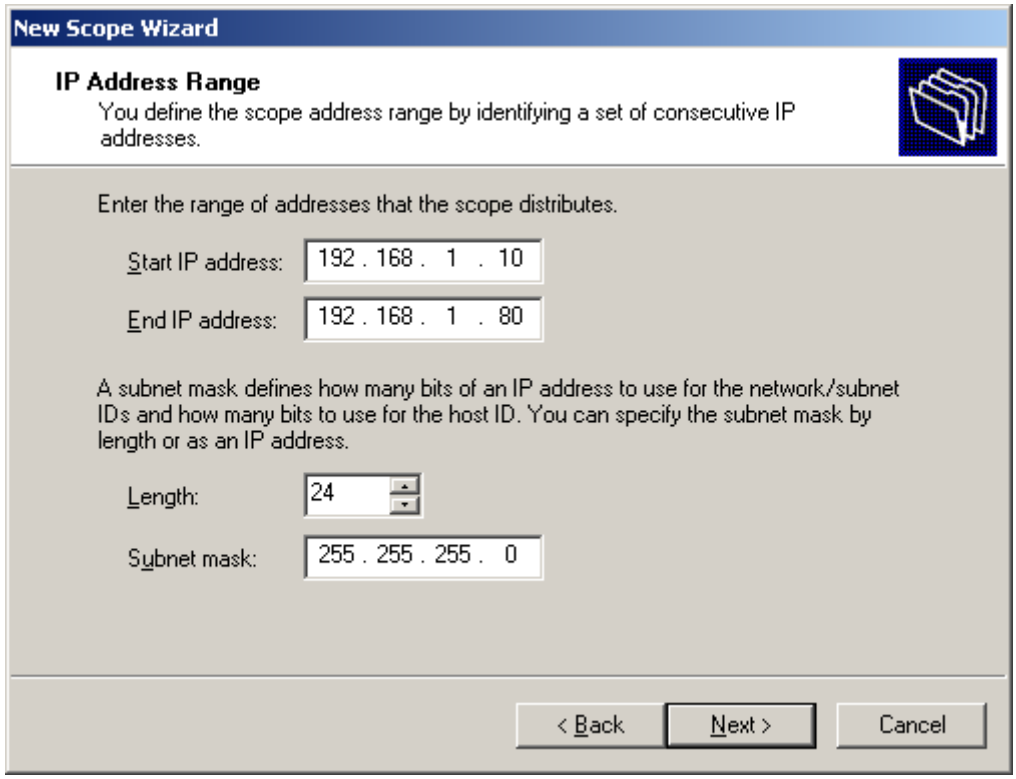
در صفحه باز شده، Next را بزنید.



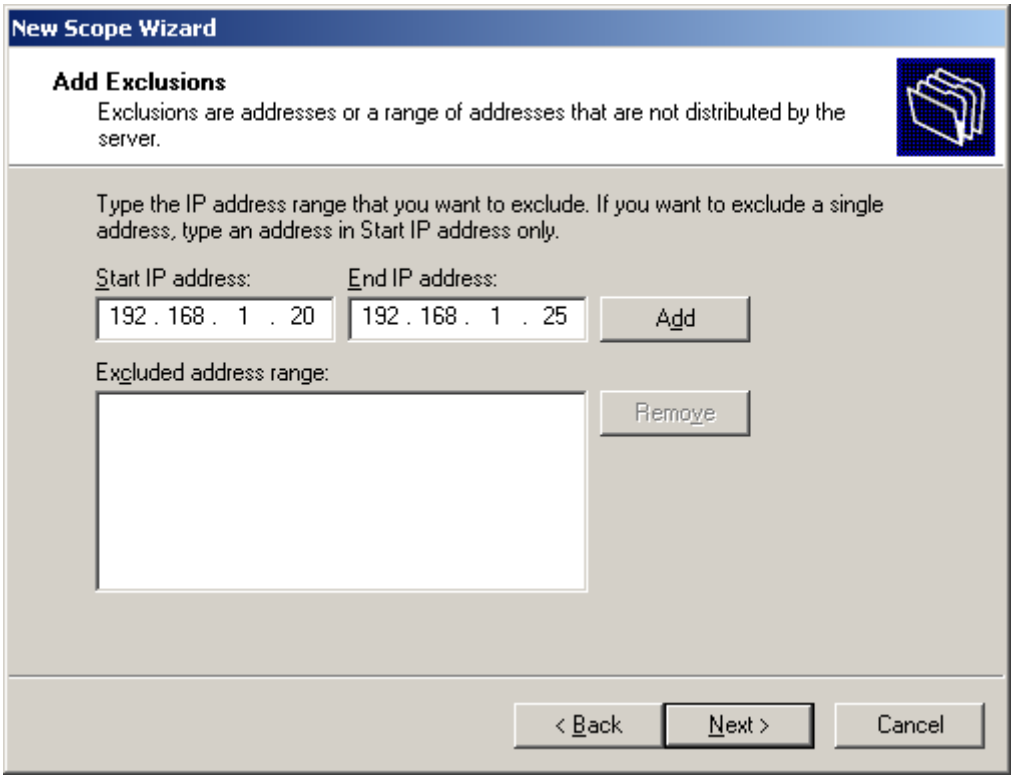
در صفحه بعدی، یک نام برای Scope به همراه یک توصیف (Description) برای آن Scope وارد نمایید.



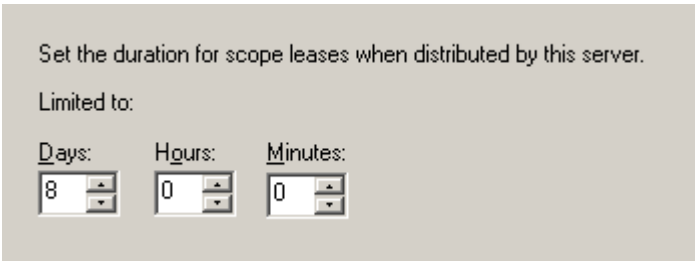
در صفحه بعد، در قسمت Start IP Address، شروع محدوده IP و در قسمت End IP Address، پایان محدوده IP را وارد نمایید. قسمت پایین نیز، بخش Length بیانگر تعداد ۱های Subnet Mast است (مفهوم Subnet Mast را در فصول قبل توضیح داده ایم). با تغییر مقدار Length، عدد مربوط به Subnet Mask در زیر آن تغییر خواهد کرد.



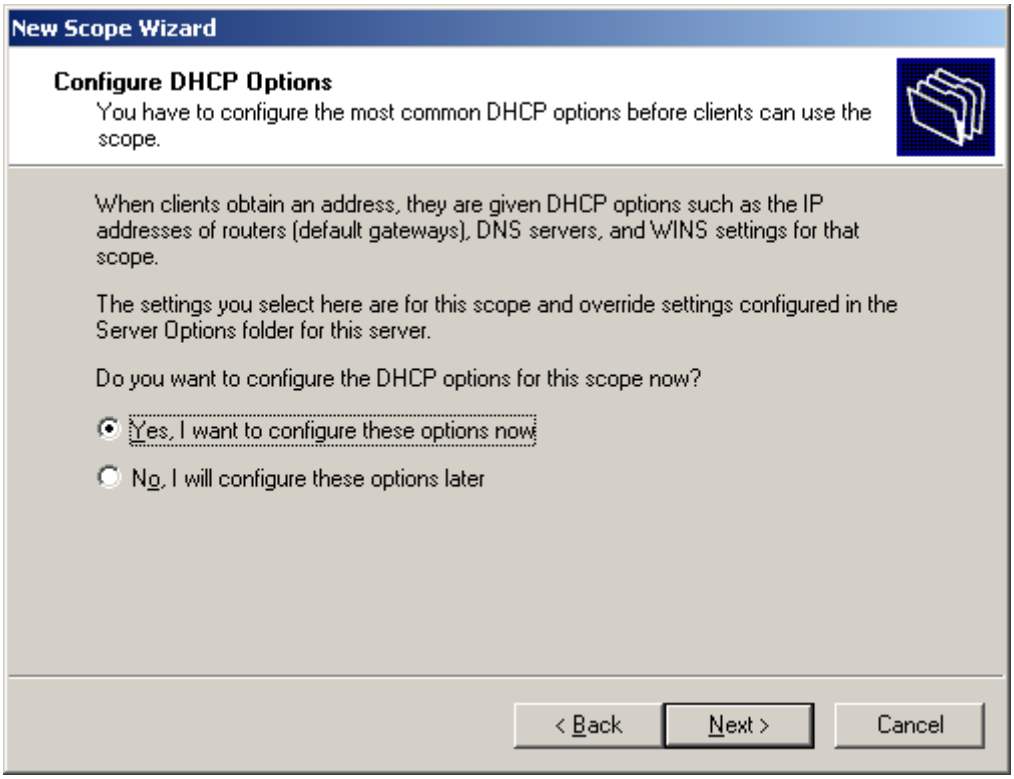
در صفحه بعد، می‌توانید محدوده IPای را وارد نمایید که قصد دارید DHCP Server آن را به Clientها تخصیص ندهد. به عبارت دیگر آن را Exclude نماید.



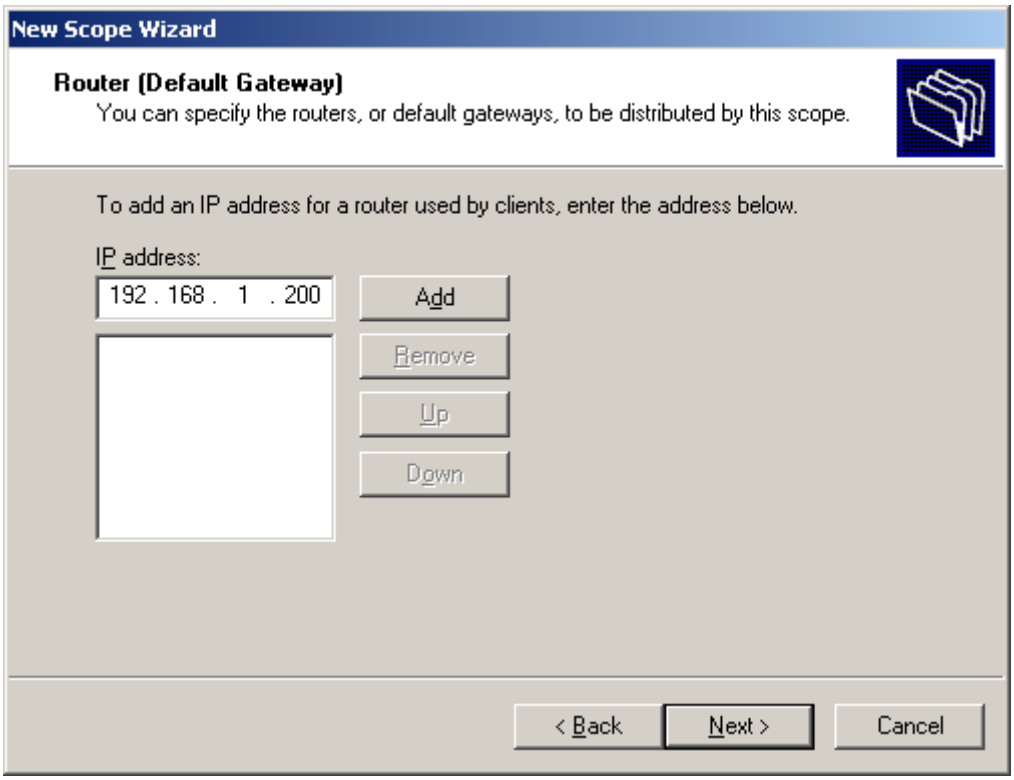
در صفحه بعدی، مدت زمانی که یک آدرس IP تخصیص داده شده معتبر خواهد بود را تعیین می‌کند. البته زمانی که نصف این زمان بگذرد، Client درخواست تمدید IP Address می‌کند. طول این زمان به طور پیش فرض ۸ روز است. اما می‌توان گفت که چنان چه در یک شبکه میزان جابجایی رایانه‌ها نسبتا کم باشد و از طرفی نیز محدوده آدرس نسبت به رایانه‌ها زیادتر باشد، در آن صورت مدت زمان اجاره را طولانی انتخاب کنید و در صورتی که جابجایی رایانه‌ها زیاد باشد (مثلاً می‌خواهیم ایستگاه‌های قدیمی را از رده خارج کرده و ایستگاه‌های جدیدی جایگزین کنیم و یا به عنوان مثال تعداد رایانه‌های Notebook که به شبکه وارد می‌شوند و از آن خارج می‌گردند زیاد است) و از طرفی محدوده آدرس‌ها نسبت به تعداد رایانه‌ها محدود باشد، در اینصورت مدت زمان اجاره را کوتاه انتخاب می‌کنیم. به بیانی دقیق‌تر مدت زمان اجاره بستگی به میزان عرضه و تقاضای آدرس IP دارد. هر چه نسبت عرضه به تقاضا بیشتر باشد، مدت زمان را طولانی‌تر و هر چه نسبت عرضه به تقاضا کمتر باشد، مدت زمان را کوتاه‌تر انتخاب می‌کنیم.



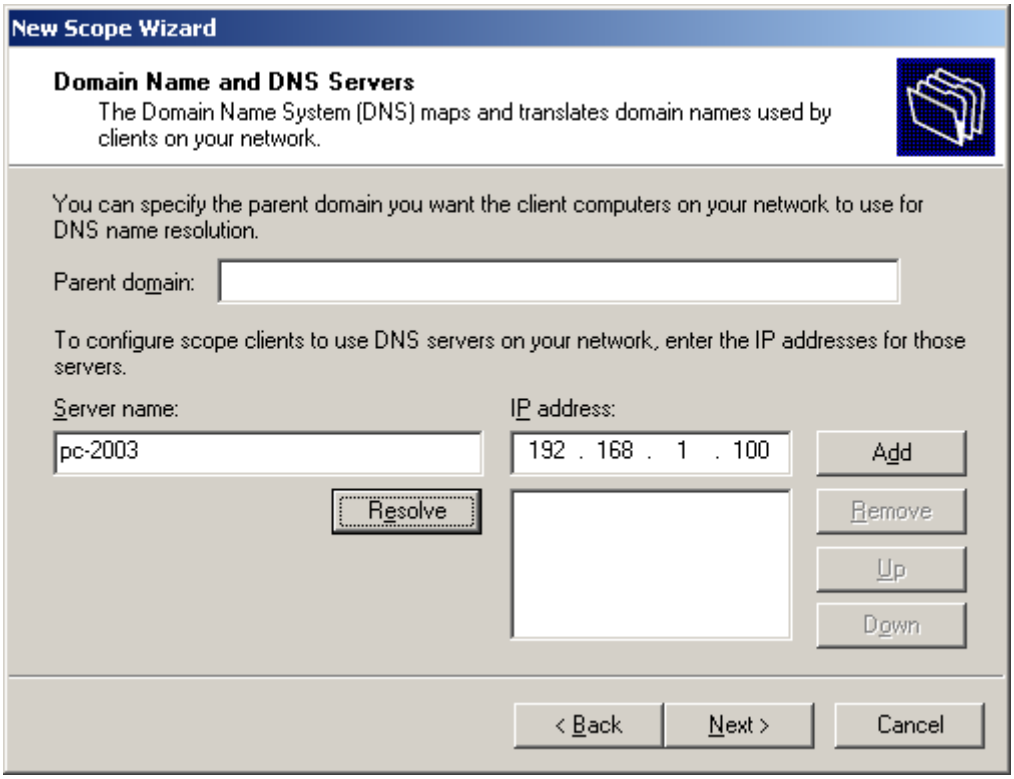
در صفحه بعدی تعیین نمایید که می‌خواهید تنظیمات دیگری را نیز انجام دهید.



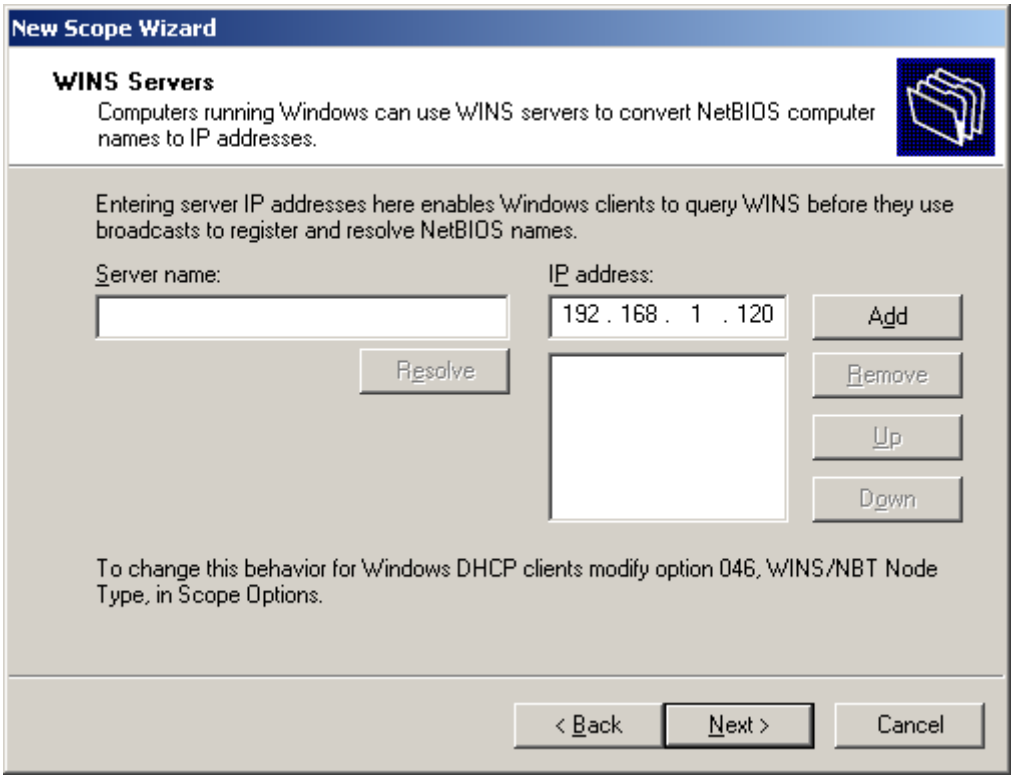
در صفحه بعدی، آدرس IP مربوط به Router یا Gateway پیش فرض را وارد نمایید.Gateway کامپیوتری است که بسته‌های ارسالی ما، ابتدا به سمت آن می‌رود و وجود آن در شبکه اختیاری است.



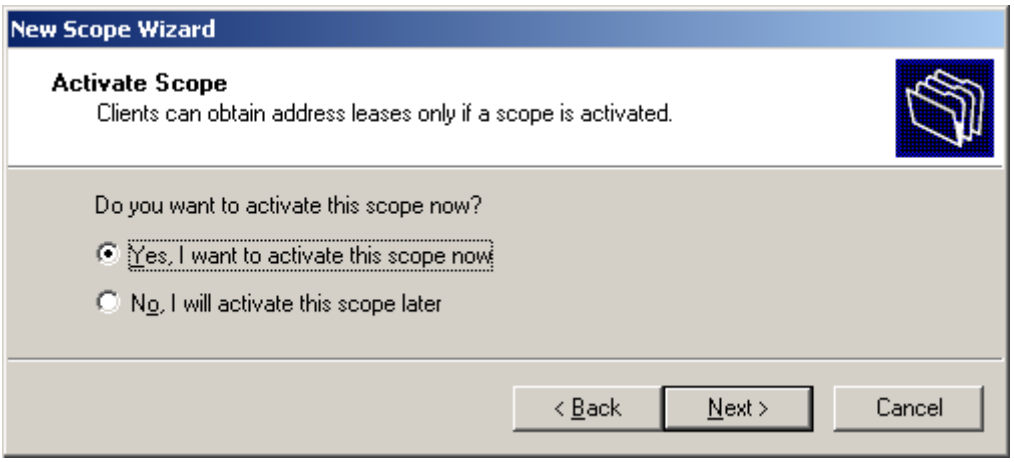
در صفحه بعد، آدرس IP مربوط به DNS Server را وارد نمایید. DNS Server وظیفه تبدیل اسامی Host Name به آدرس IP را بر عهده دارد. اگر آدرس IP را نمی‌دانید، نام DNS Server را وارد کرده و سپس روی دکمه Resolve کلیک نمایید. با این کار، DHCP Server آدرس DNS Server را نیز به Clientها می‌دهد.



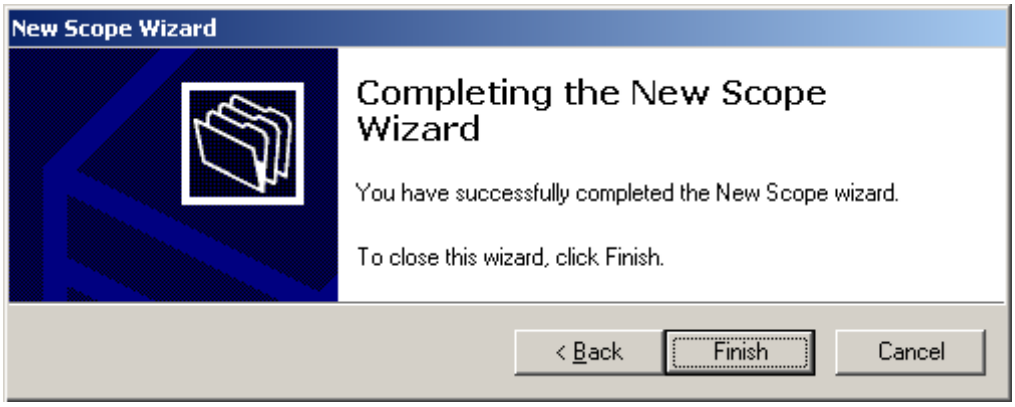
در صفحه بعد، آدرس IP مربوط به WINS Server را وارد نمایید. WINS Server وظیفه تبدیل اسامی NetBIOS Name به آدرس IP را بر عهده دارد. (برای اطلاعات بیشتر به فصل DNS Server مراجعه نمایید.)



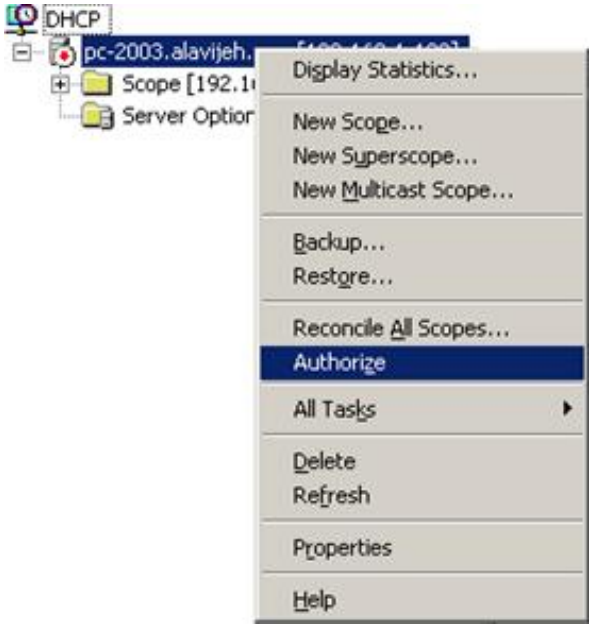
در صفحه بعد تعیین نمایید که قصد دارید این Scope را فعال نمایید.



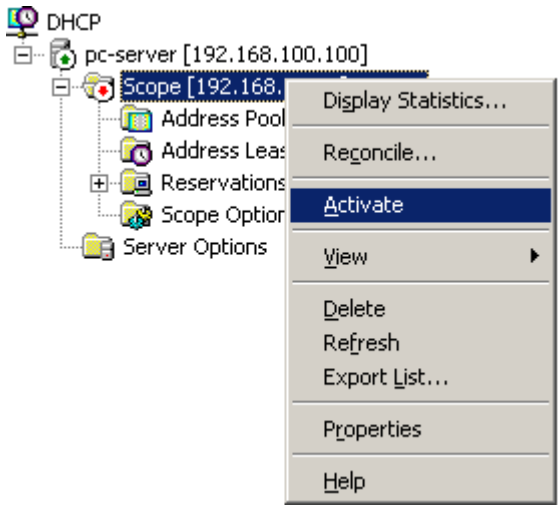
سپس برای پایان نصب، روی دکمه Finish کلیک نمایید.



تا این مرحله، Scope ساخته شده فعال است. اما هنوز خود DHCP Server فعال (Authorize) نشده است. باید حتما DHCP Server خود را فعال کنید. این کار برای جلوگیری از تداخل وجود چند DHCP Server در شبکه است. بدین منظور در صفحه DHCP، روی نام سرور راست کلیک کرده و گزینه Authorize را انتخاب نمایید.



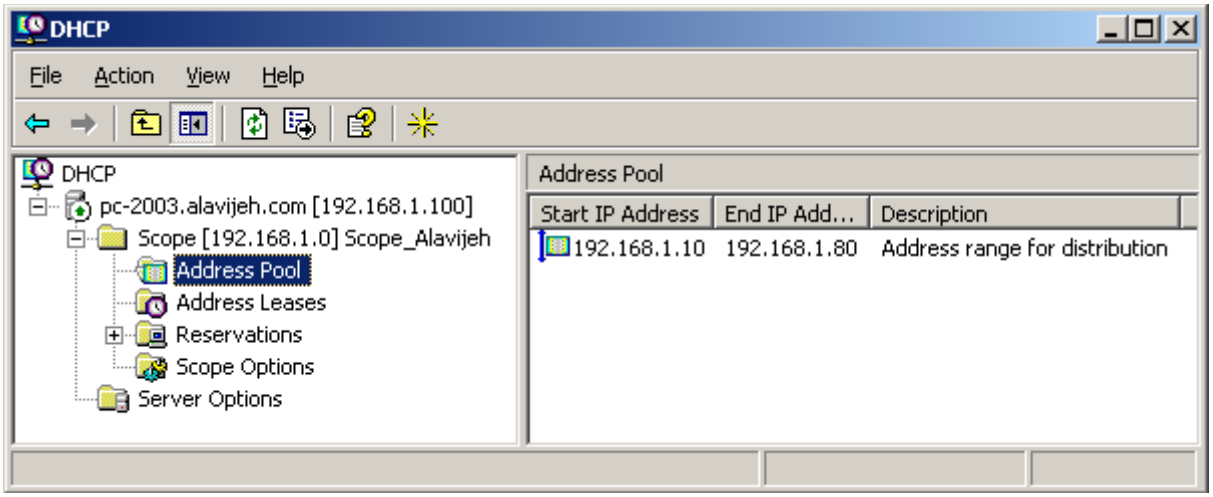
سپس بایستی Scope ساخته شده را فعال کنید. لذا روی Scope ساخته شده راست کلیک کرده و گزینه Activate را انتخاب نمایید.



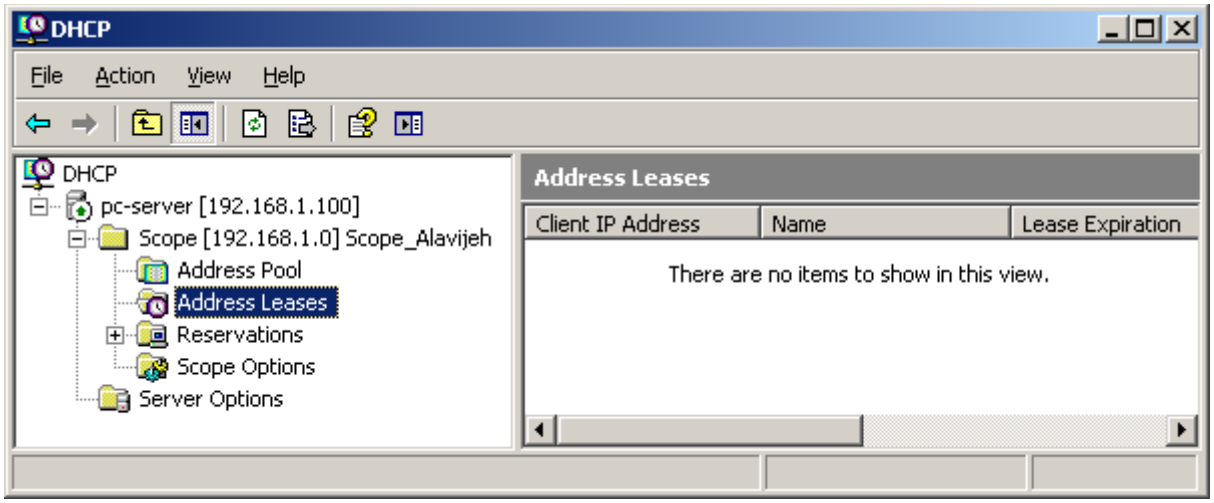
۲۷-۳-۱- قسمت‌های مختلف DHCP Server

در ادامه به معرفی قسمت‌های مختلف DHCP Server می‌پردازیم.

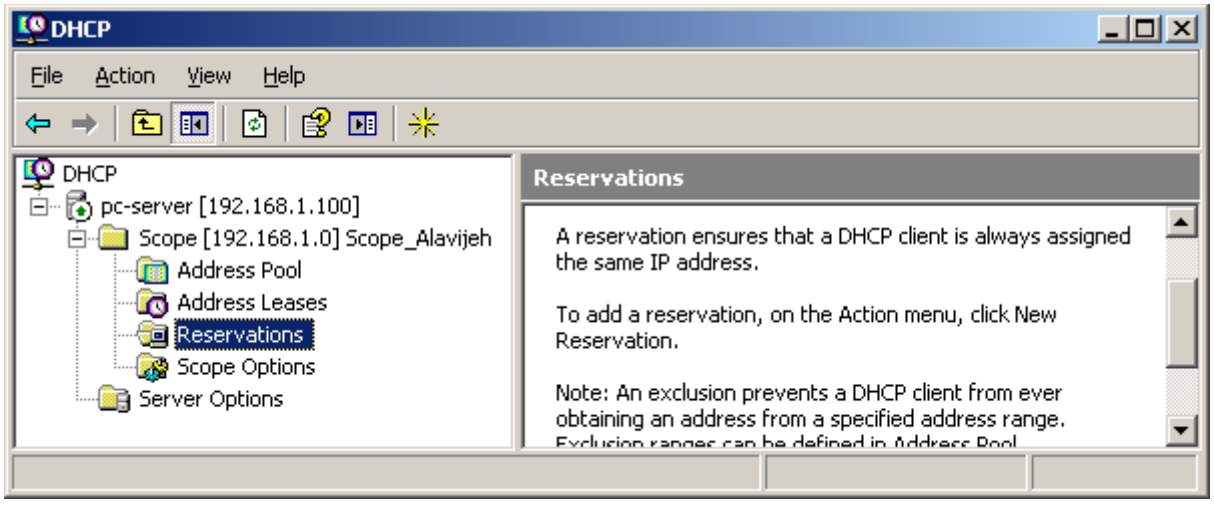
۱. **Address Pool (استخر آدرس):** این قسمت بیانگر محدوده آدرس‌های قابل تخصیص و محدوده آدرس‌های غیر قابل تخصیص (Exclude) است.



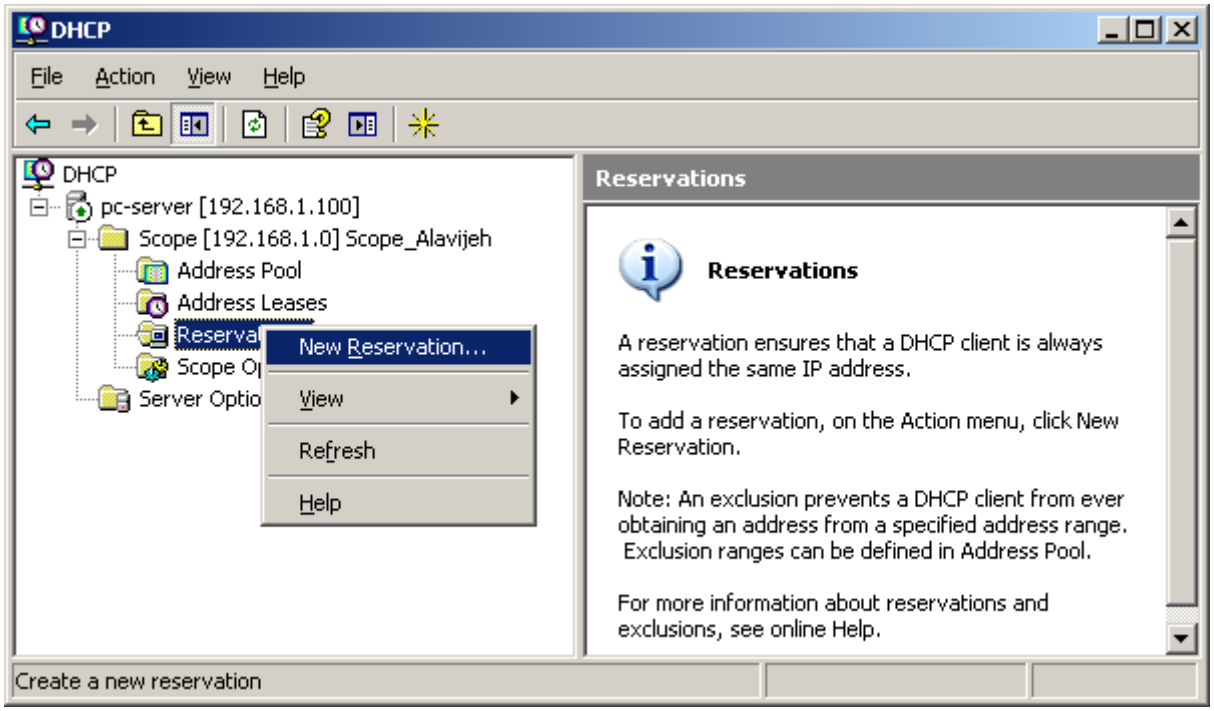
۲. **Address Leases (آدرس‌های اجاره داده شده):** بیانگر آدرس IPهایی می‌باشد که تا کنون به Clientها تخصیص داده شده است.



۳. **Reservation (رزرو شده ها):** توسط این قسمت می‌توانید آدرس هایی خاص را همیشه به کامپیوتر هایی خاص نسبت بدهید. به عبارت دیگر زمانی که Clientی خاص درخواست IP بدهد، همیشه IPی ثابت و مشخص به وی تحویل داده خواهد شد.



برای ایجاد IP رزرو شده جدید، روی گزینه Reservation راست کلیک کرده و گزینه New Reservation را انتخاب نمایید.

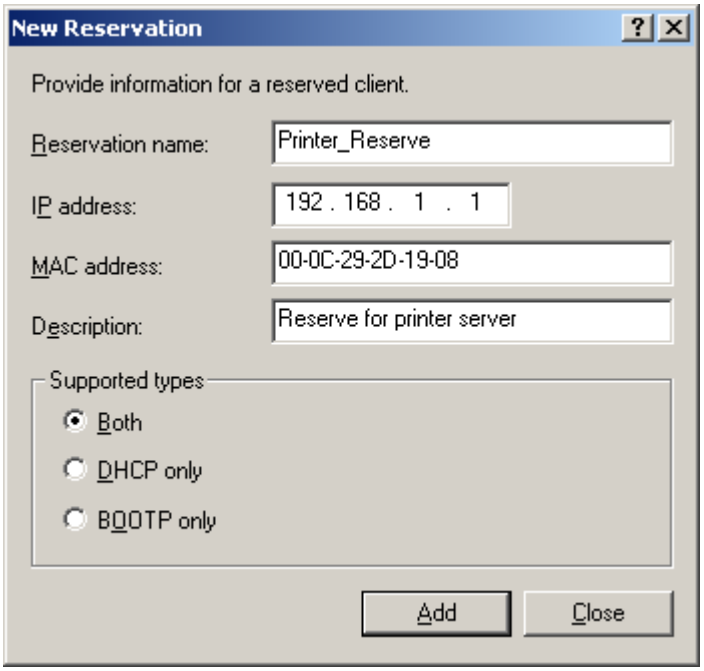


در صفحه باز شده، موارد زیر را وارد نمایید.

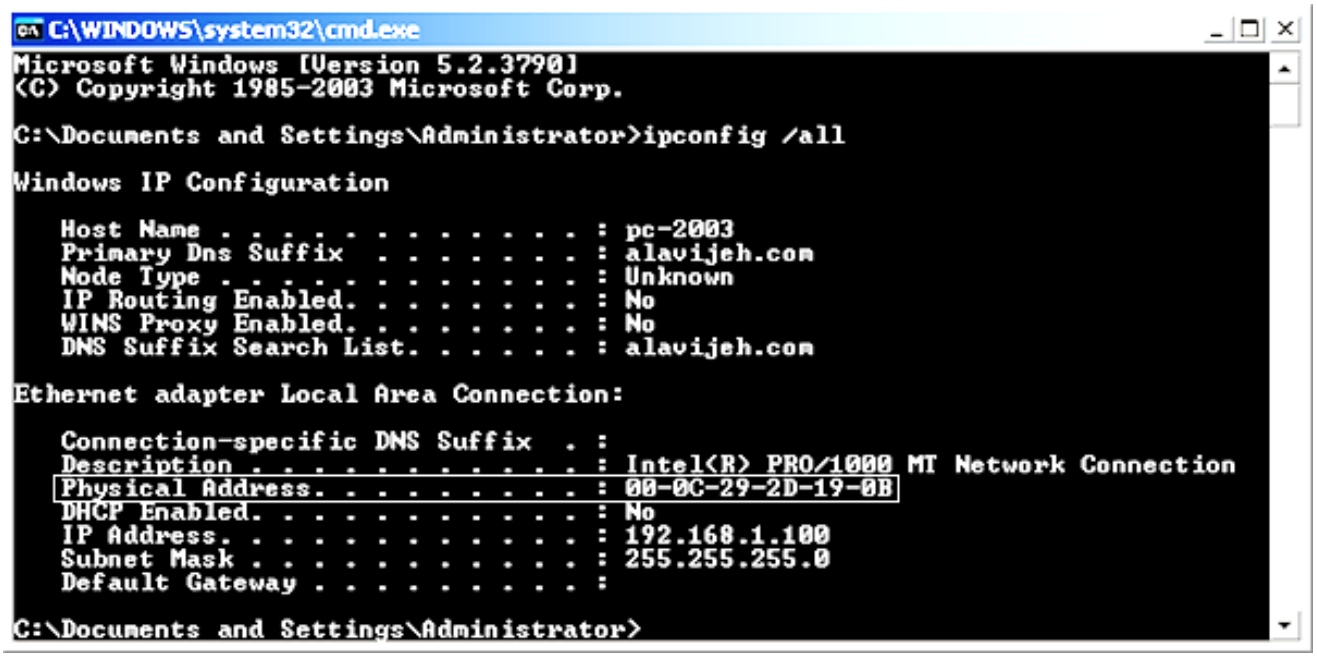
۱. Reservation Name: نامی دلخواه برای آدرس تخصیص داده شده

۲. IP Address: آدرس IP که می‌خواهید تخصیص دهید.

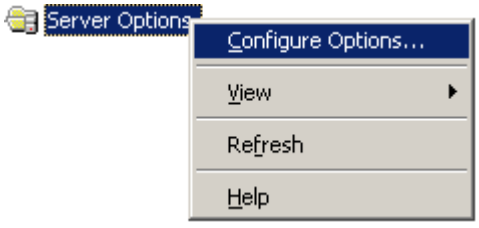
۳. MAC Address: بیانگر آدرس سخت‌افزاری کارت شبکه Client است که می‌خواهیم **همیشه** این آدرس IP را به آن اختصاص دهیم. برای به دست آوردن آدرس MAC یک کامپیوتر راه دور، می‌توان از دستور GetMac استفاده نمود.

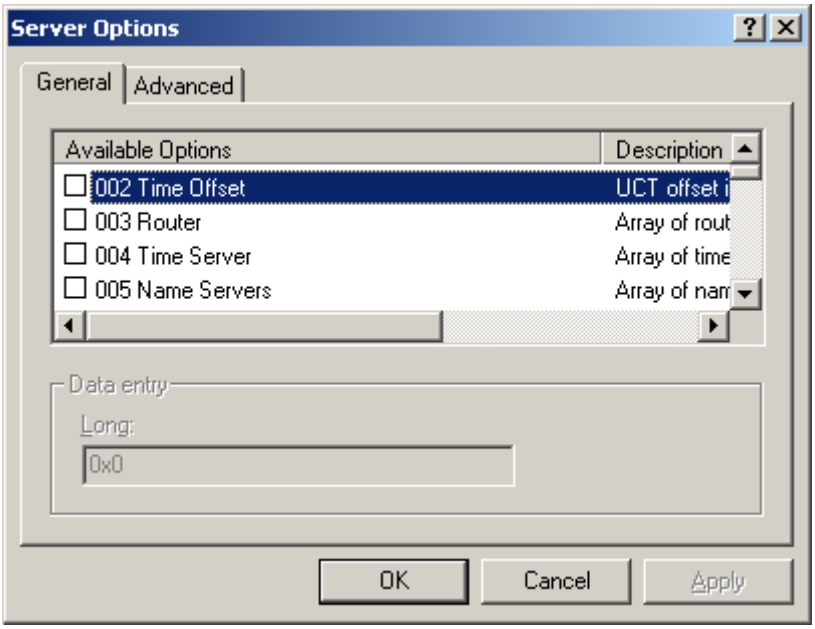


برای یافتن آدرس MAC، در Client بدین صورت عمل کنید: در **Client** وارد محیط Command Prompt شده و دستور IpConfig /All را وارد نمایید. با این کار آدرس IP را در قسمت Physical Address مشاهده خواهید نمود. آن را در جعبه متن فوق، به همراه علامت –، وارد نمایید.



۴. **Scope Option:** از طریق این قسمت می‌توانید تنظیمات تخصصی مربوط به DHCP Server را تعیین نمایید.





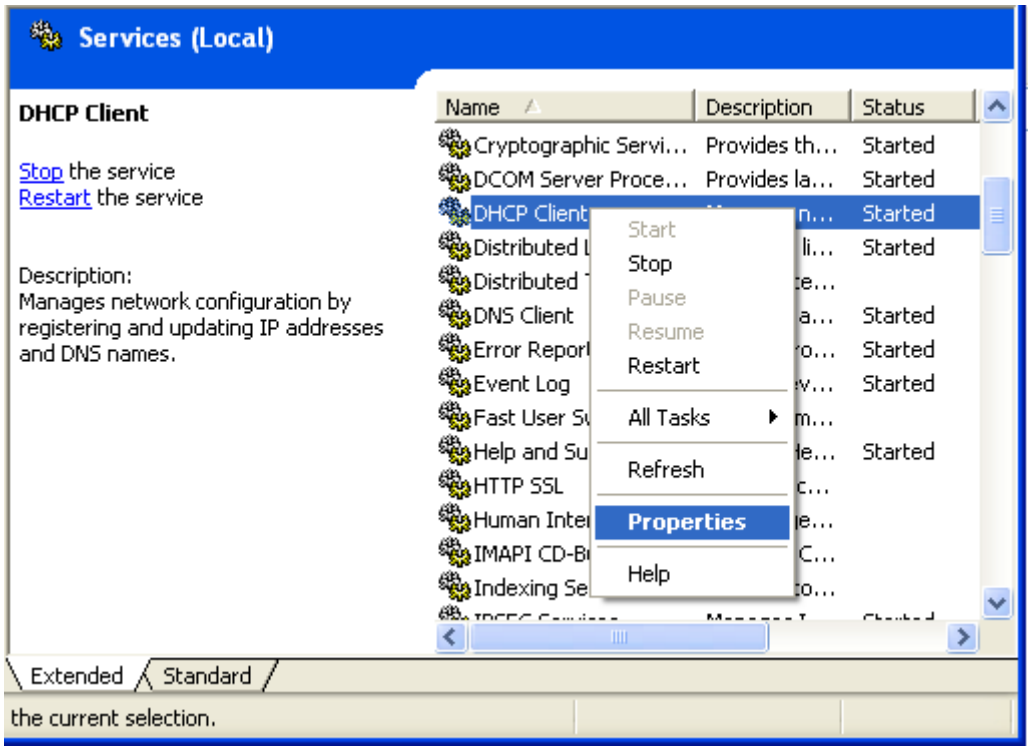
۲۷-۳-۲- تنظیم Client جهت استفاده از DHCP Server

از نظر تئوری با انجام موارد فوق، از این پس Clientها قادر به دریافت IP خود از سرور می‌باشند. (در صورتی که نحوه دریافت IP خود را روی Automatic تنظیم کرده باشند). اما همیشه در عمل این موضوع رخ نمی‌دهد و بایستی تنظیماتی را در Client انجام دهیم.

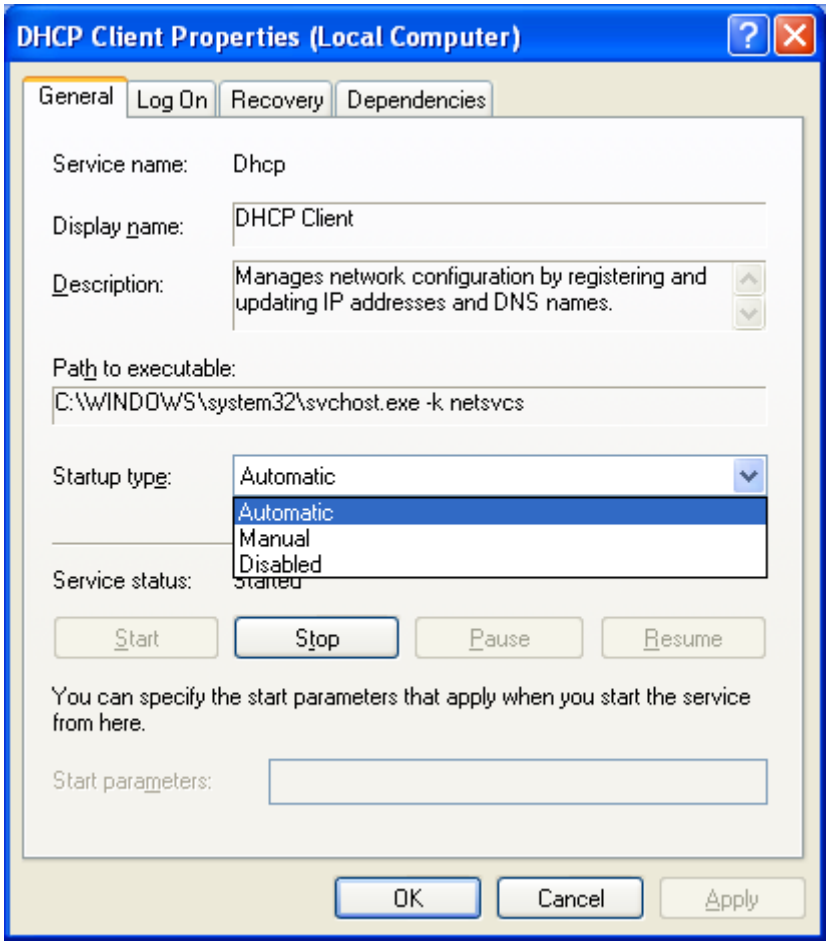
اولین گام فعال کردن DHCP Service (سرویس DHCP) است. برای این کار، در Client وارد مسیر زیر شوید:

Control Panel ➔ Administrative Tools ➔ Services

سپس روی گزینه DHCP Server راست کلیک کرده و گزینه Properties را انتخاب نمایید.



سپس در صفحه باز شده، از قسمت Startup type، گزینه Automatic را انتخاب کرده و OK کنید.

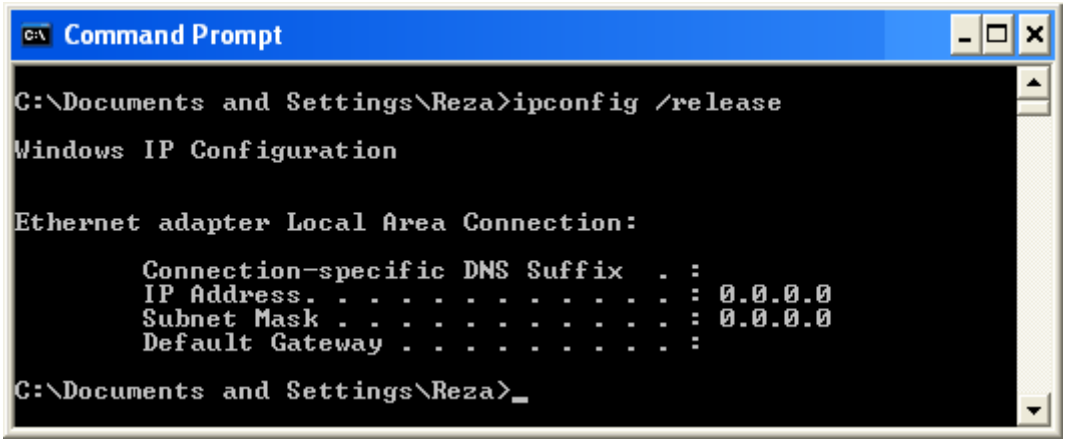


پس از OK کردن، توسط دکمه Start Service، سرویس DHCP Server را اجرا کنید. (البته ابتدا DHCP Server را انتخاب نمایید).

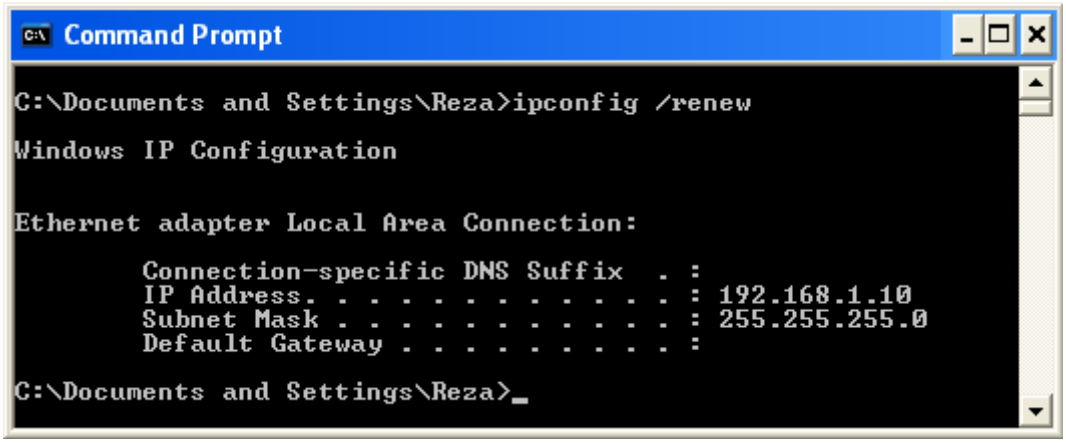


در گام بعدی بایستی آدرسی جدید از DHCP Server درخواست نمایید. این کار به دو صورت امکان پذیر است. راه اول این است که Client را Restart نمایید.

اما اگر می‌خواهد بدون راه اندازی مجدد Client، آدرس IP را به صورت خودکار بدست آورید، بایستی ابتدا آدرس IP خود را از بین ببرید. برای این کار ابتدا وارد محیط Command Prompt شده و سپس دستور IPConfig /release را وارد نمایید.

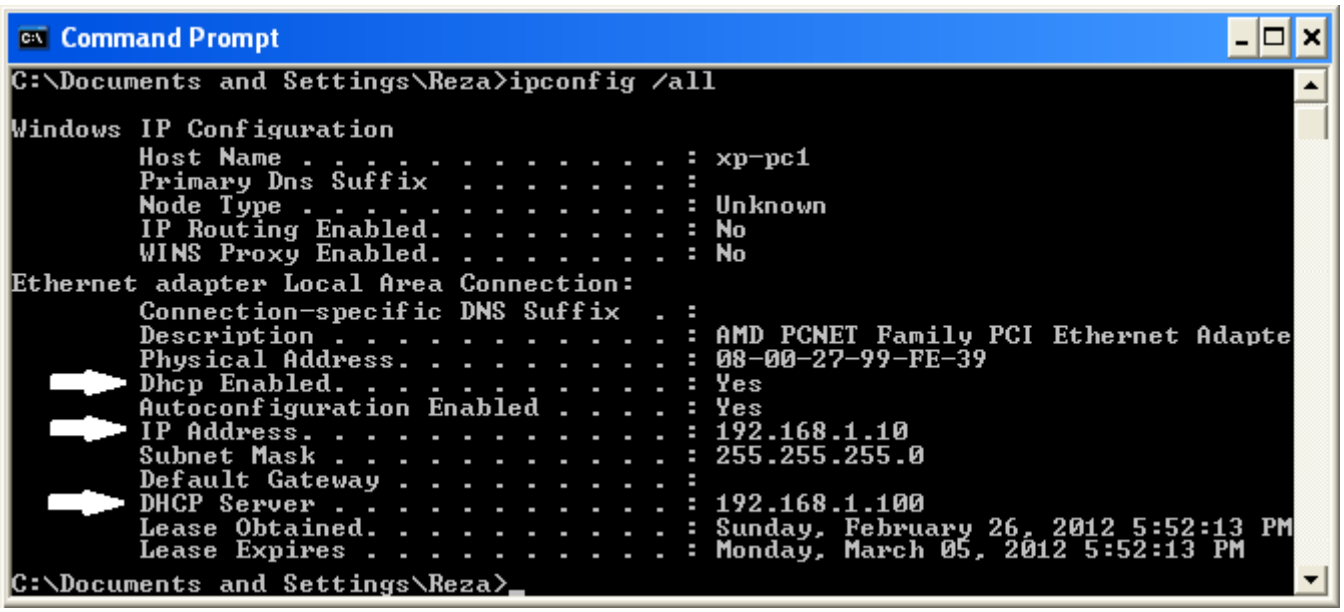


با این کار، دیگر Client آدرس IP ندارد. برای درخواست آدرس IP، دستور IPConfig /renew را وارد نمایید. با این کار، آدرس IP جدیدی از سمت Server به Client تخصیص داده می‌شود.

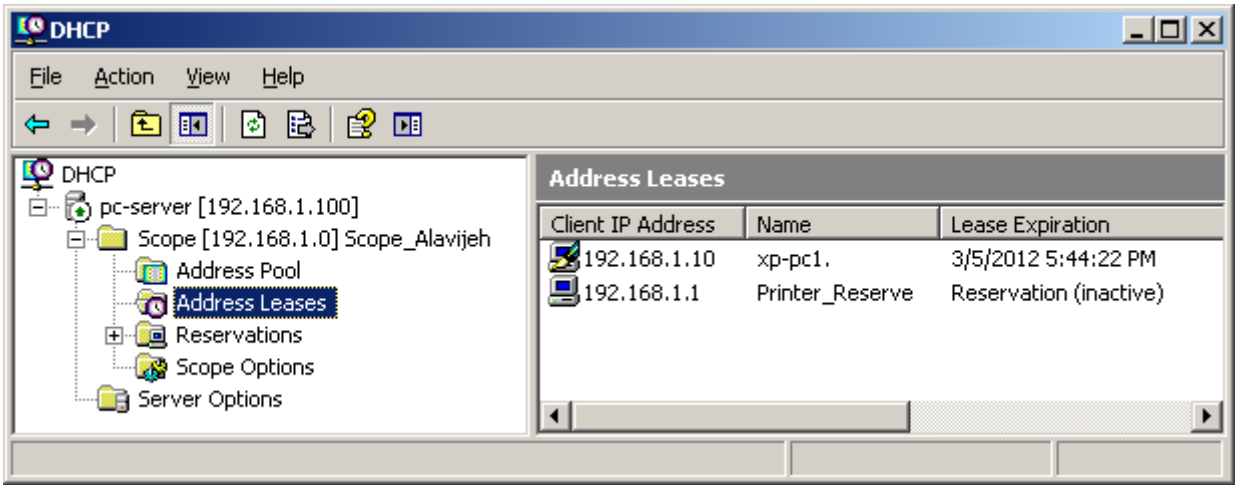


برای دیدن اطلاعات دقیق تر، در Client دستور IPConfig /All را وارد نمایید.

در شکل به قسمت DHCP Server و IP Address توجه فرمایید.

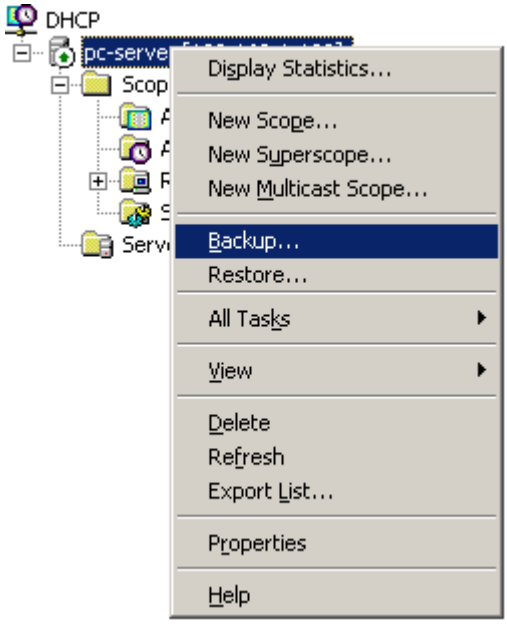


حال اگر مجددا به Server سری بزنید و وارد پنجره DHCP شوید، در قسمت Address Leases، مشاهده خواهید که Server به صورت خودکار، به Client یک آدرس IP تخصیص داده است.

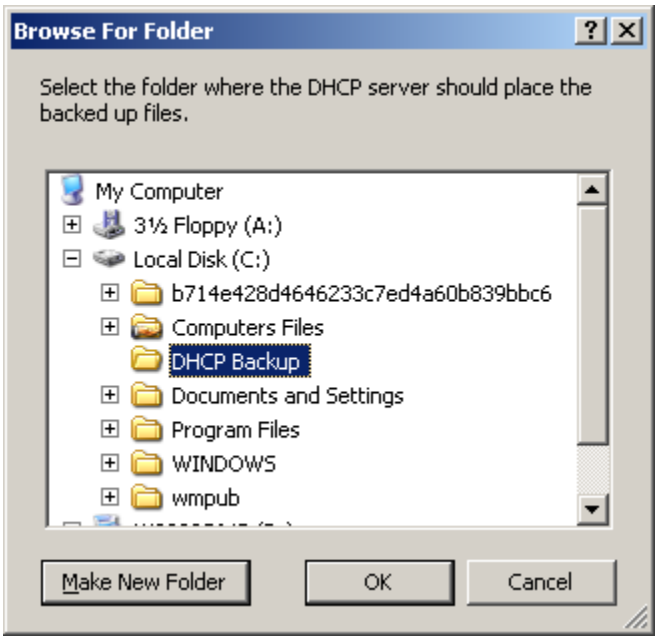


DHCP Backup & Restore -۴-۲۷

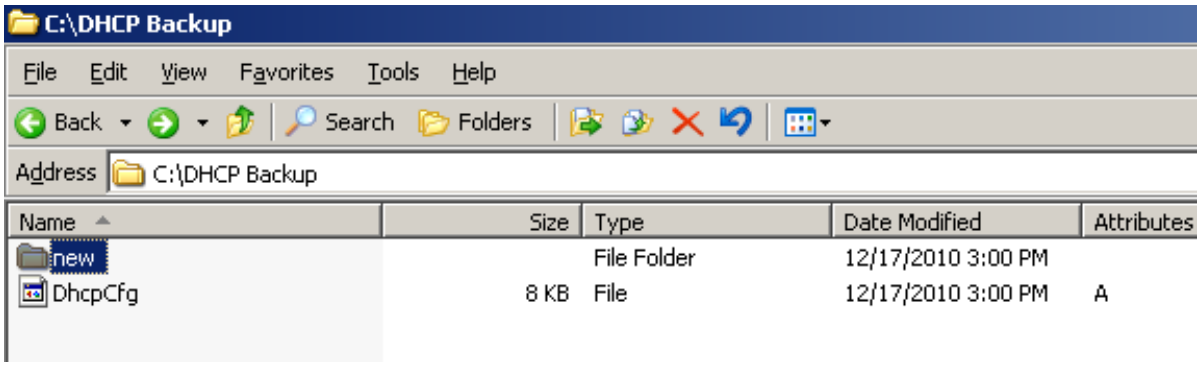
گاهی ممکن است به دلایل مختلفی بخواهید که سرویس DHCP موجود بر روی یک سرور را به سروری دیگر انتقال دهید. در این حالت بایستی ابتدا از اطلاعات مرتبط با سرویس DHCP در سرور اول پشتیبان تهیه نموده، سرویس DHCP را غیر فعال کرده و سپس فایل‌های پشتیبان تولید شده را به سرور دوم انتقال دهید. یا حتی ممکن است بخواهید یک کپی پشتیبان از DHCP خود داشته باشید (البته ویندوز خودش به صورت خودکار هر ۳۰ دقیقه یکبار از DHCP کپی پشتیبان می‌گیرد). بدین منظور ابتدا وارد DHCP ➔ Administrative Tools ➔ Start شده، روی سرویس DHCP راست کلیک کرده و گزینه Backup را انتخاب کنید.



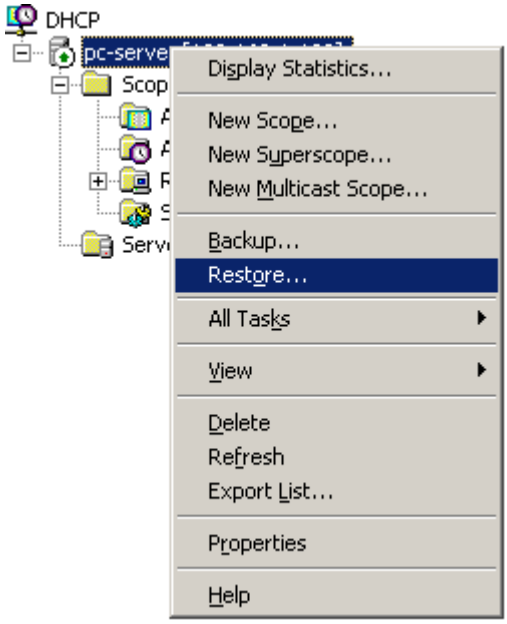
سپس در صفحه باز شده، مسیری را برای ذخیره فایل‌های کپی پشتیبان تعیین نمایید. در این مثال، آدرس مورد نظر C:\DHCP Backup است.



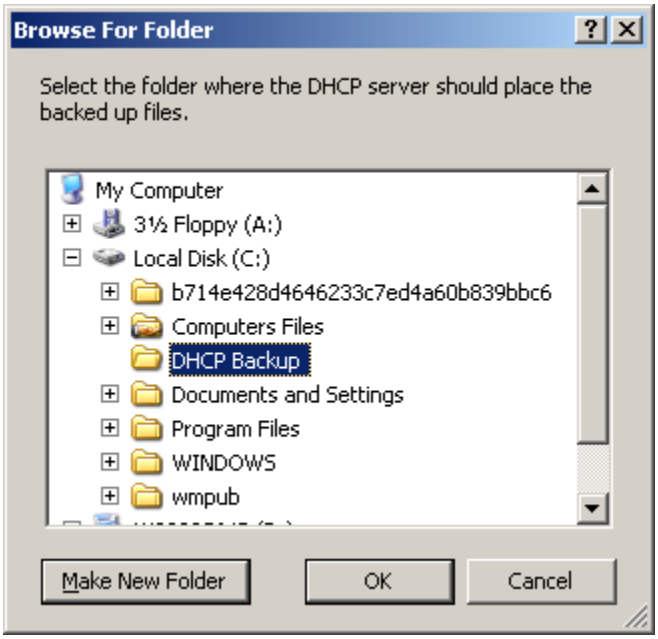
در اینصورت، سیستم در مسیر تعیین شده، فایل هایی را ایجاد خواهد نمود.



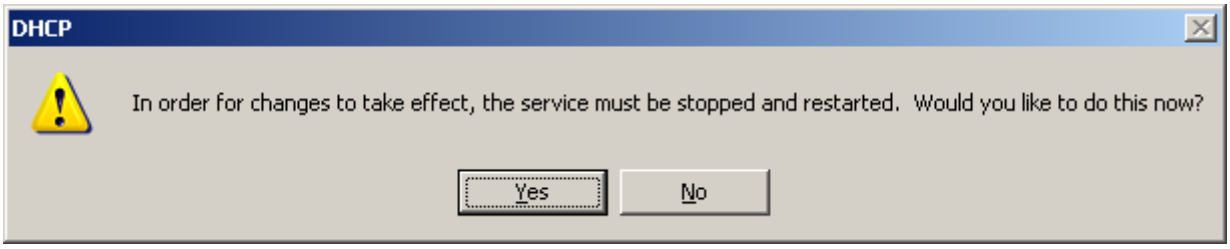
حال نوبت به باز گردانی (Restore) اطلاعات DHCP می‌شود. بدین منظور روی سرویس DHCP مورد نظر (در کامپیوتر خودتان یا در یک کامپیوتر دیگر) راست کلیک کرده و گزینه Restore را انتخاب کنید.



در صفحه باز شده، مسیری که فایلهای Backup در آن قرار دارد را انتخاب نمایید. در این مثال، این مسیر برابر با C:\DHCP Backup است.



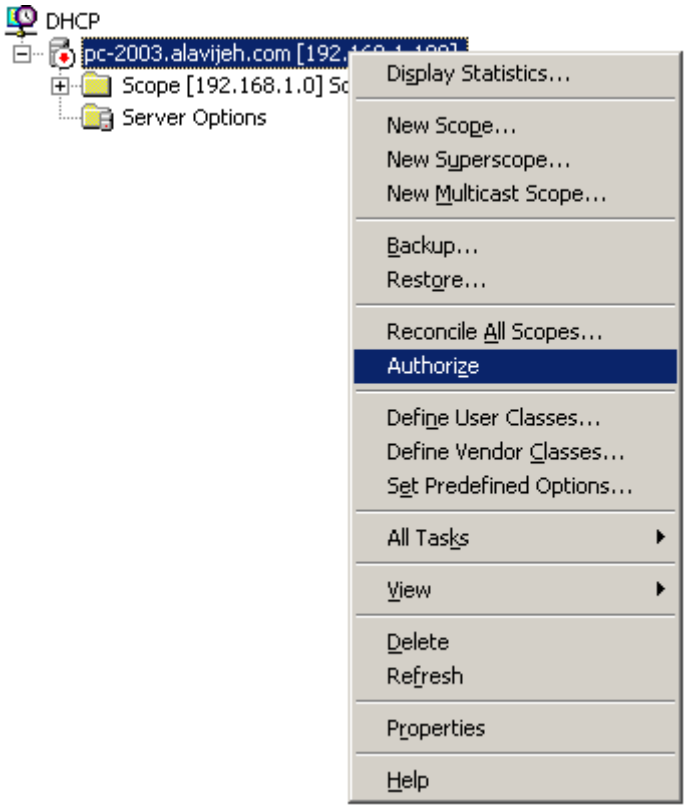
پس از انتخاب مسیر، سیستم می گوید که برای مشاهده تاثیرات Backup، بایستی سرویس DHCP، ابتدا Stop و مجددا Restart شود. روی OK کلیک کنید.



مدتی صبر نمایید تا تغییرات در شبکه اعمال شود.



بعد از اتمام عملیات باز گردانی اطلاعات، این بار نوبت به Authorize نمودن سرور DHCP می‌باشد. به منظور انجام این کار کافیست طبق تصویر زیر عمل کنید:



اگر عمل Restore را در سرور دیگری انجام دهید، حال اگر کلاینت‌های موجود در شبکه، راه اندازی مجدد (Restart) گردند، سرور دوم را به عنوان سرور DHCP خود بر می‌گزینند. فقط توجه داشته باشید که در این حالت بایستی DHCP اولیه را غیر فعال کنید.

فصل ۲۸

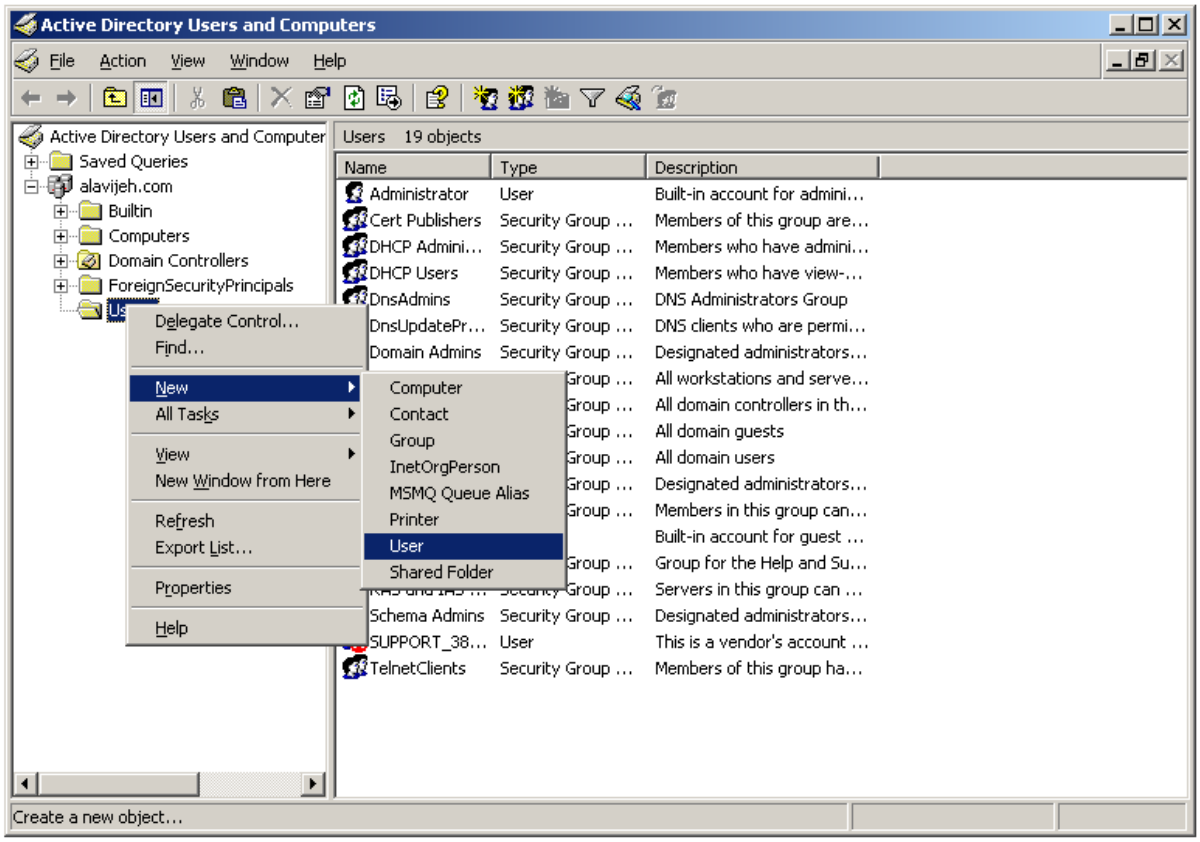
اتصال Client به Domain

۲۸-۱- تنظیمات Server

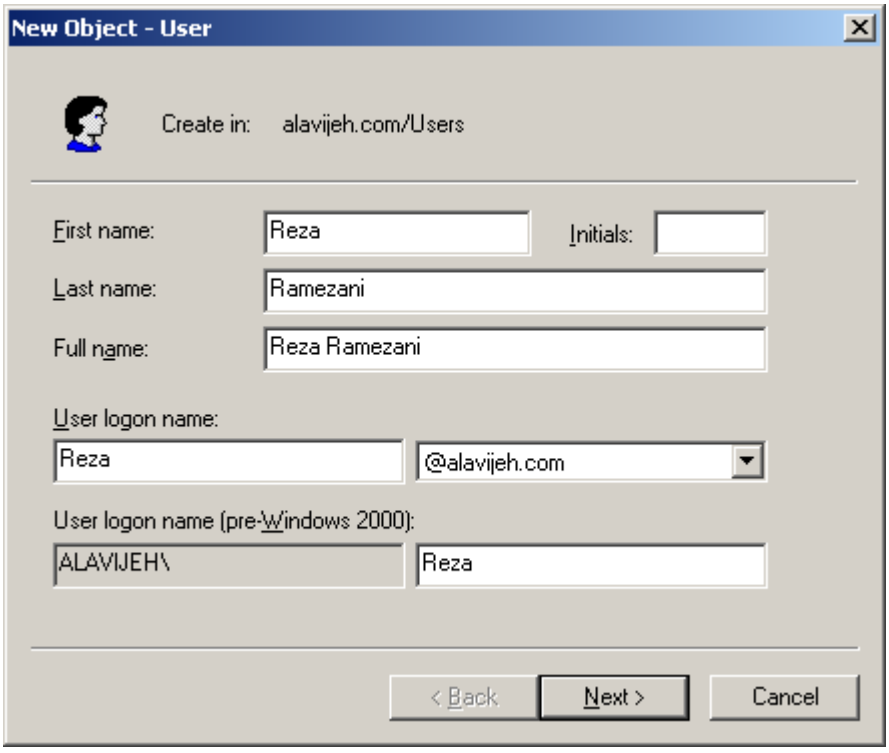
پس از راه اندازی Server (نصب Active Directory)، نوبت به این کار می‌رسد که Clientها را به Server متصل کرده و آن را عضوی از Domain کنیم. بدین منظور ابتدا یک نام کاربری و رمز عبور برای Client و در Server تعریف کنید تا به کمک آن Client بتواند به سرور Login کرده و به آن متصل شود. برای این کار، در سرور از منوی Start، گزینه Administrative Tools و سپس گزینه Active Directory Users and Computers را انتخاب نمایید.



سپس در صفحه باز شده، قسمتی که نام دامنه را نشان می‌دهد، بسط داده، روی قسمت Users راست کلیک کرده و سپس User ➔ New را انتخاب نمایید.



سپس در قسمت بالا، نام و نام خانوادگی کاربر را وارد نمایید. سپس در قسمت User logon name، نام کاربری کاربر که هنگام ورود به سیستم باید وارد کند را در این قسمت وارد نمایید. سپس روی Next کلیک کنید.



سپس در این صفحه، رمز عبور کاربر را وارد نمایید. توجه نمایید که در ابتدا به صورت پیش فرض، در ویندوز سرور، رمز عبور بایستی دارای حداقل ۷ حرف بوده و نیز به صورت Complex (پیچیده) باشد (این تنظیمات در Group Policy تعیین

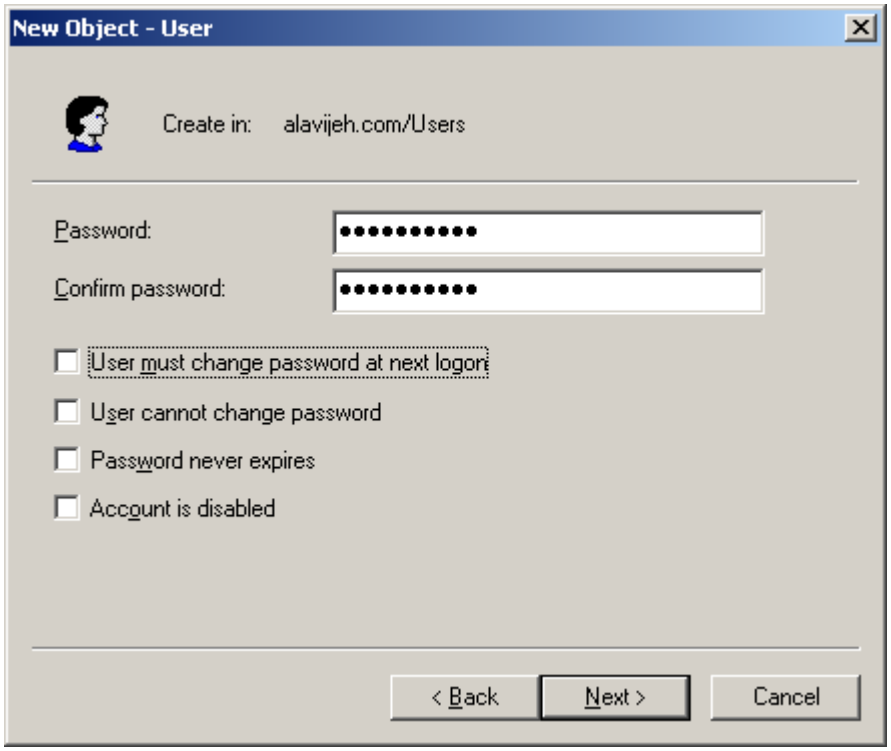
می‌گردد که در فصل‌های بعدی توضیح می‌دهیم). در این مثال ما رمز عبور را abc@abc123 وارد کردیم. در زیر ۴ گزینه وجود دارد که به توضیح مختصر آن می‌پردازیم:

۱. **User must change password at next logon:** با فعال کردن این گزینه، سیستم کاربر را مجبور می‌کند که هنگام **اولین** Login به سیستم، رمز عبور خود را تغییر دهید. **توجه:** اگر بخواهید سیستمی را به Domain خود Join کنید و هنگام Join کردن از این نام کاربری استفاده کنید؛ و همچنین اگر تاکنون با این کاربر Login نکرده‌اید و این گزینه را نیز فعال کرده باشید، سیستم اجازه ورود شما را خواهد گرفت.

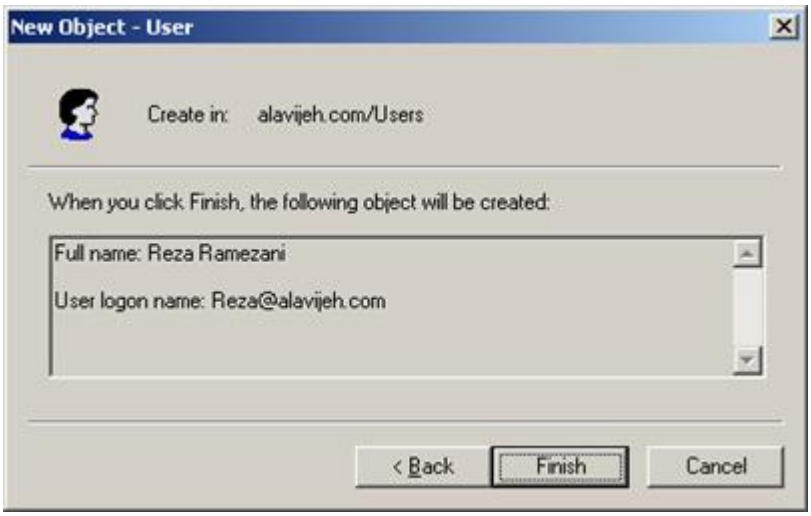
۲. **User cannot change password:** با فعال کردن این گزینه، کاربر قادر به تغییر دادن رمز عبور خود نخواهد بود. بهتر است این گزینه را غیر فعال کنید.

۳. **Password never expires:** با فعال کردن این گزینه، رمز عبور کاربر هیچ گاه منقضی (Expire) نخواهد شد. در غیر اینصورت به صورت پیش فرض، پس از ۴۲ روز، کاربر مجبور به تغییر رمز عبور خود است. علت این امر بالا بردن امنیت رمز عبور است.

۴. **Account is disabled:** با فعال کردن این گزینه، کاربر غیرفعال شده و قابلیت ورود به سیستم را از دست خواهد داد.



در مرحله آخر، اطلاعات مختصری در مورد کاربر را مشاهده خواهید نمود. برای ساخت کاربر، روی دکمه Finish کلیک نمایید.

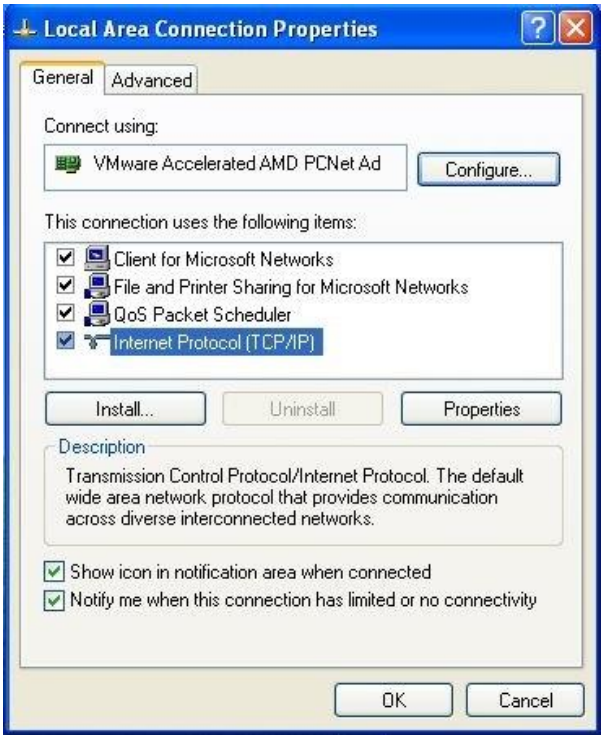


۲۸-۲- تنظیمات Client

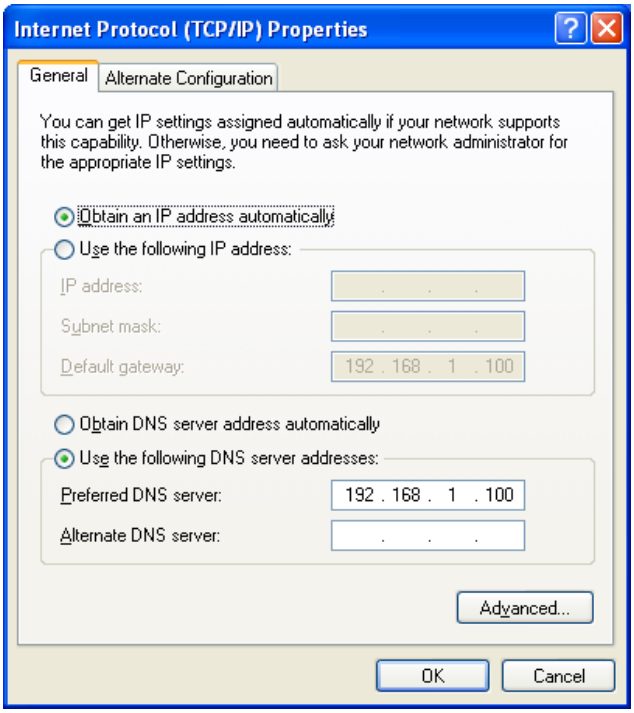
پس از تعریف نام کاربری و رمز عبور در Server، نوبت به انجام تنظیماتی در Client می‌شود. برای شروع ابتدا از متصل بودن Client مطلع شوید. بدین منظور در Client در Network Connection ➔ Control Panel روی Local Area Connection، دو بار کلیک کنید. در صورت اتصال Client به شبکه، بایستی صفحه‌ای مانند صفحه زیر مشاهده کنید. سپس باید تنظیمات IP Address و DNS Address مربوط به Client را انجام دهید. برای این کار روی دکمه Properties کلیک کنید.



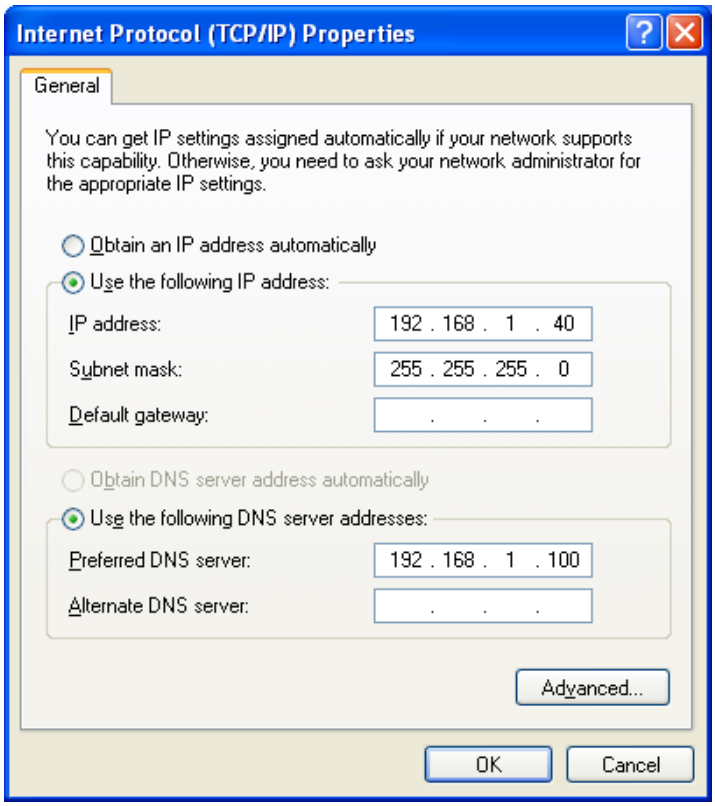
برای تنظیم کردن IP، ابتدا گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک کنید.



حال نوبت به تنظیم آدرس IP در Client می‌شود. در این مرحله، اگر در شبکه خود از DHCP Server استفاده می‌کنید، بایستی صفحه را به صورت زیر تنظیم نمایید (برای اطلاعات بیشتر به فصل DHCP و قسمت اتصال Client مراجعه نمایید). تنها نکته مهم این است که در قسمت Preferred DNS Server، بایستی حتما آدرس DNS Server را وارد نمایید. البته **توجه** فرمایید که اگر DHCP Server آدرس DNS Server را نیز بدهد، نیازی به پر کردن این قسمت نیست (آیا به خاطر دارید که هنگام ایجاد Scope جدید در DNS Server، می‌توانستیم آدرس DNS Server را نیز تعیین نماییم؟).

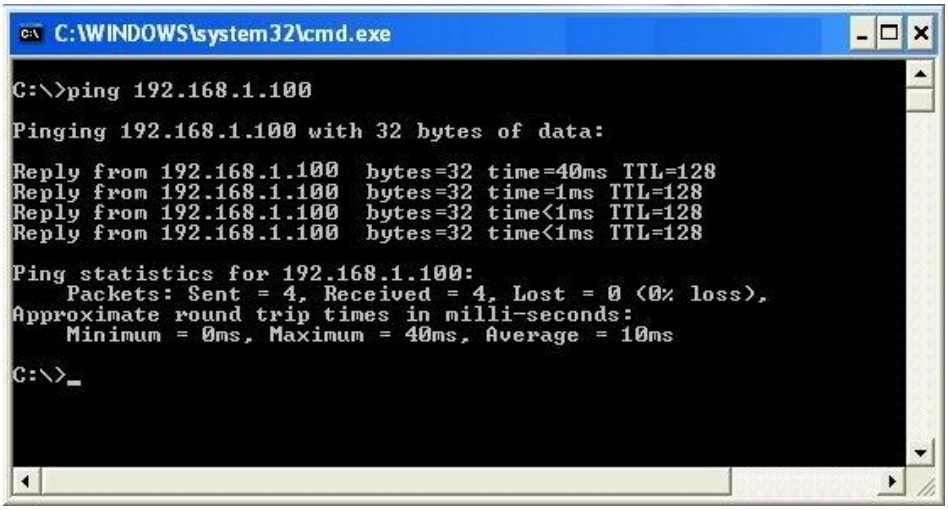


اما اگر قصد دارید IP Address مربوط به Client را به صورت دستی تنظیم کنید، بایستی آن را به گونه‌ای وارد کنید که به صورت منطقی در شبکه سرور (Domain Controller) قرار گیرد. یعنی آدرس‌های IP کلاینت و سرور باید قسمت شبکه اشان با هم برابر باشد (یعنی قسمت Network Address آن‌ها با هم برابر باشد). مثلاً دو آدرس‌ای پی ۱۹۲.۱۶۸.۱.۱۰۰ و ۱۹۲.۱۶۸.۱.۴۰ هر دو از نظر منطقی در یک شبکه قرار دارند. همچنین حتما باید در قسمت Preferred DNS Server، آدرس سروری که DNS روی آن نصب شده است را وارد نمایید. توجه نمایید که اگر این قسمت را به درستی وارد نکنید، Client قابلیت اتصال به Domain را پیدا نخواهد کرد.

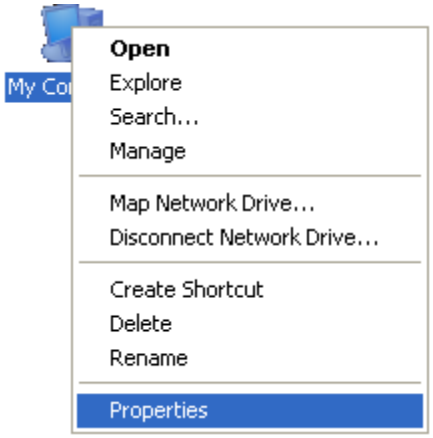


برای تست ارتباط شبکه کافیست همانند تصویر زیر، با استفاده از دستور Ping از صحت ارتباط کلاینت با سرور، اطمینان حاصل نماییم. بدین منظور دستور زیر را وارد نمایید:

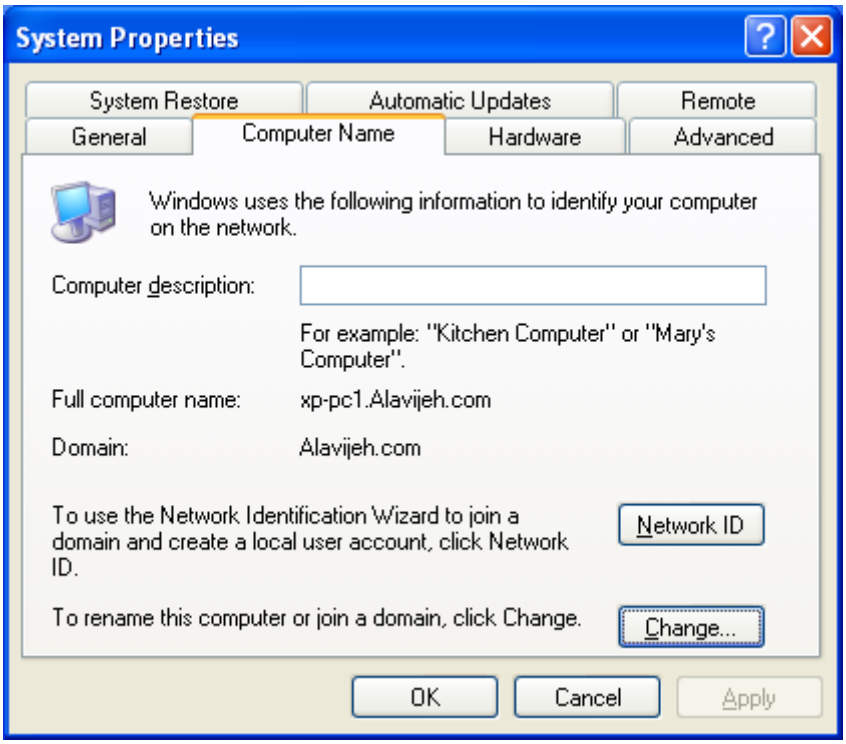
C:\> **Ping** آدرس/نام سرور



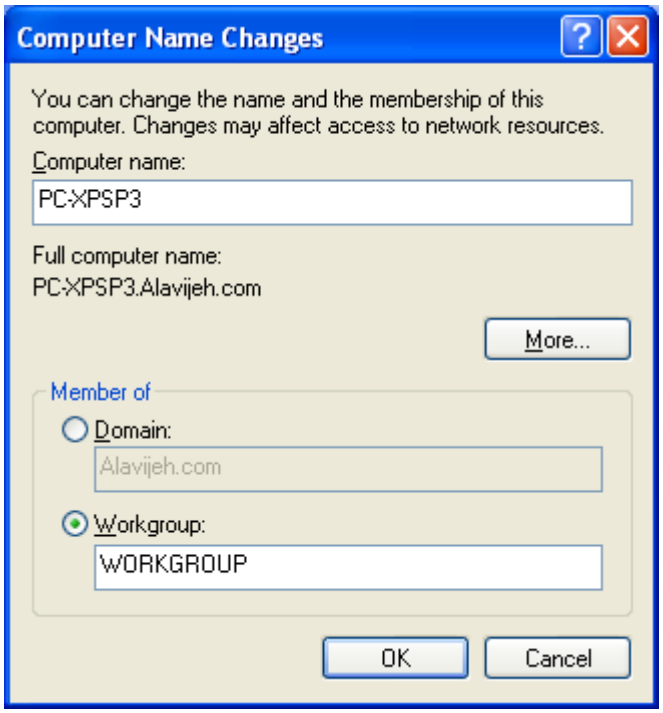
پس از اطمینان از صحت قابلیت اتصال Client به Server، بایستی تنظیمات نهایی Client را انجام دهید تا Client عضوی از دامنه شود. برای این کار روی My Computer راست کلیک کرده و گزینه Properties را انتخاب کنید.



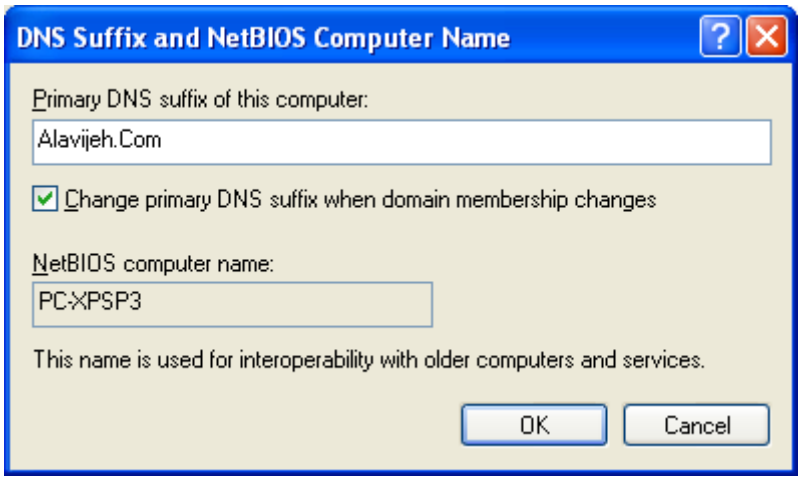
سپس سربرگ Computer Name را انتخاب کرده و سپس روی دکمه Change کلیک کنید.



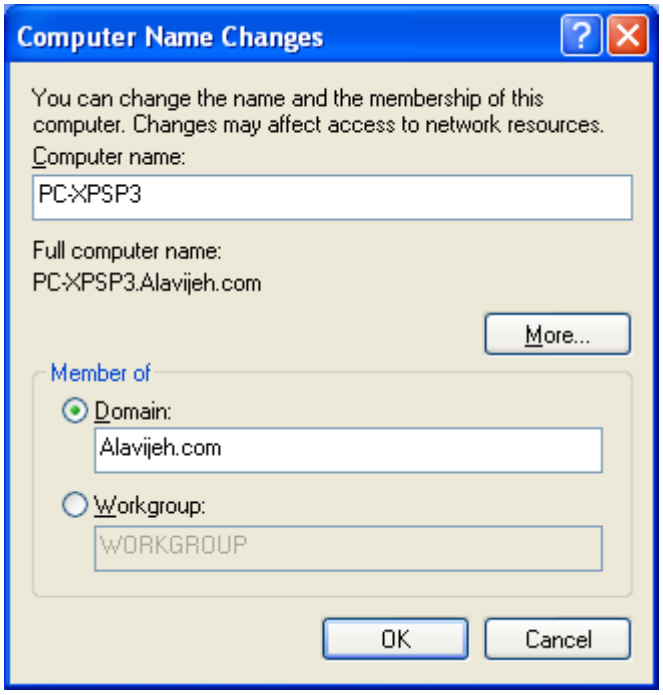
سپس در صفحه باز شده، مشاهده خواهید کرد که کامپیوتر شما عضوی از Workgroup است.



سپس روی دکمه More کلیک کرده و نام Domain Controller را وارد نمایید.



سپس روی دکمه OK کلیک کنید. سپس در صفحه باز شده، گزینه Domain را انتخاب کرده و سپس در جعبه متن مربوطه، نام کامل Domain Controller را وارد نمایید.



بعد از کلیک کردن روی دکمه OK، بایستی نام کاربری و رمز عبوری را که در سرور ثبت کردهاید را در پنجره باز شده وارد نمایید.



بعد از OK کردن، اگر نام کاربری و رمز عبور درست باشد، سیستم به شما پیغام خوش آمد گویی به دامنه را میدهد.



با دیدن پنجره فوق اطمینان حاصل مینماییم که کار به اتمام رسیده است. سپس باید Client را Restart کنید:

پس از Restart شدن Client، صفحهای مانند صفحه زیر وارد میشود.



باز فشردن کلیدهای Ctrl + Alt + Delete، صفحه‌ای مانند صفحه زیر باز می‌شود. از طریق این صفحه می‌توانید ۲ روش برای ورود به سیستم انتخاب کنید:

۱. **This Computer:** که برای این کار بایستی نام کاربری و رمز عبوری را وارد نمایید که بر روی همین Client ثبت شده است. (مانند روش قبل)

۲. **To Domain:** در این روش بایستی نام کاربری و رمز عبوری را وارد نمایید که بر روی Server تعریف شده باشد. در این صورت شما فقط کارهایی را بر روی سیستم می‌توانید انجام دهید که مدیر شبکه اجازه انجام آن کارها را به شما داده باشد.



فصل ۲۹

Active Directory Users And Computers

۲۹-۱- آشنایی با انواع Accountها و ابزارهای مدیریتی

در Active Directory، Accountها به ۳ دسته تقسیم می‌شوند:

۱. **User Account:** به ازاء هر کاربر در Domain یک User Account باید ایجاد کنید. از این نوع Accountها برای Log On کردن به Domain و دسترسی به منابع آن استفاده می‌شود.

۲. **Computer Account:** به ازاء هر کلاینت، هر سرور و هر DC که عضو Domain هست یک Computer Account وجود دارد و در آن‌ها برای اعمال کردن Policyها از Authentication استفاده می‌شود.

۳. **Group Account:** برای مدیریت راحت کاربران (عضویت افراد در گروه ها) و اعطای مجوز به آن‌ها و همچنین اعمال Policy از این نوع Accountها استفاده می‌شود.

۲۹-۲- مدیریت در Active Directory user and computer

برای مدیریت و اجرای این بخش مسیر زیر را دنبال می‌کنیم.

Start➔Administrative Tools➔ Active Directory Users and Computers



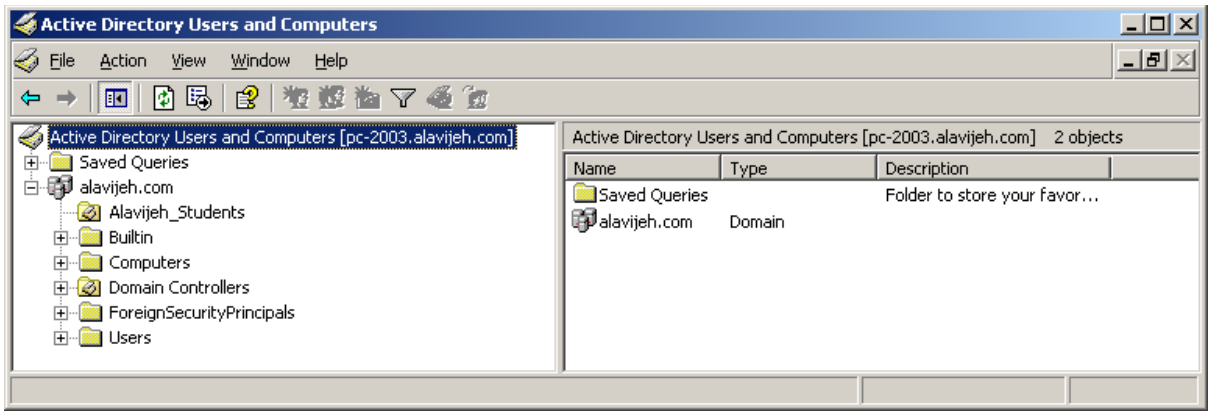
پس از اجرا، پنجره Active Directory Users and Computers اجرا می‌شود که به شکل زیر است:

همچنین قابل ذکر است که:

تمامی کاربران و گروه‌های که در Domain ایجاد می‌شوند، داخل پوشه Users قرار می‌گیرند.

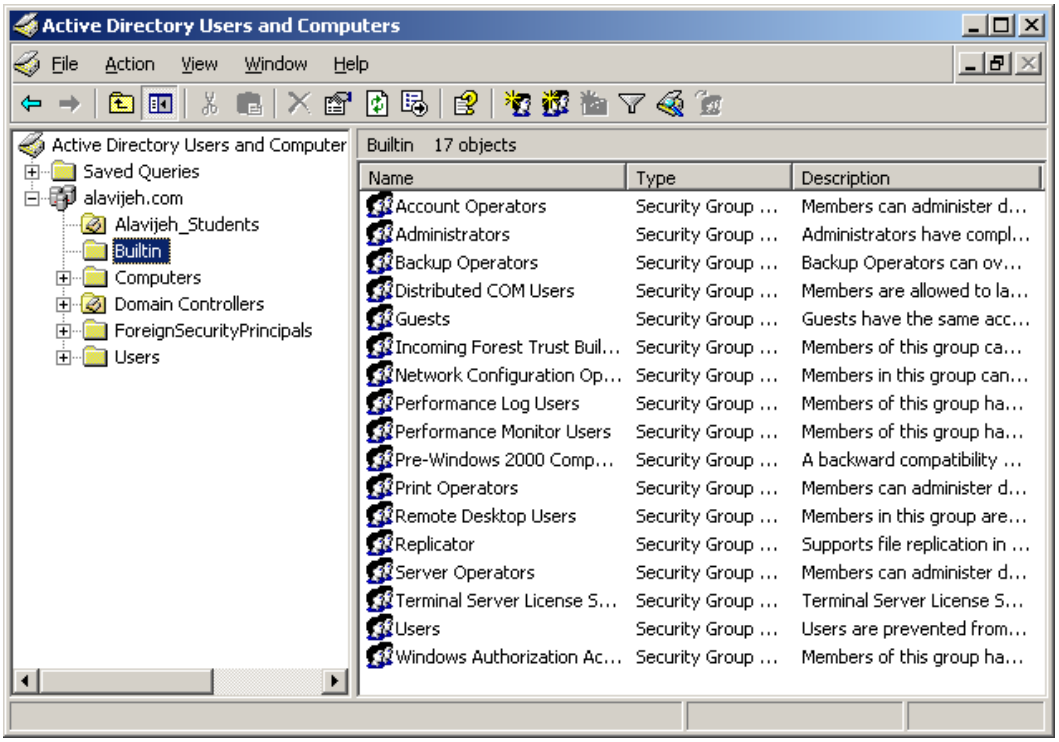
به ازاء تمامی کامپیوتر هایی که عضو Domain می‌شوند، یک Computer Account در پوشه Computers ایجاد می‌شود.

تمامی گروه هایی که به صورت پیش فرض ایجاد می‌شوند، در پوشه Builtin قرار می گیرند.



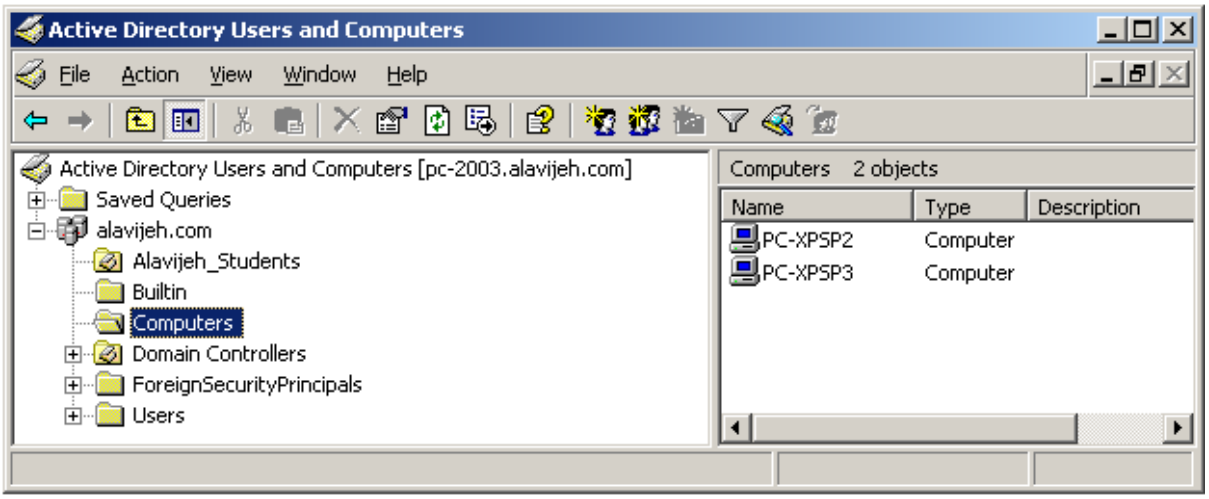
۲۹-۲-۱- آشنایی با گروه‌های Builtin

گروه‌های Builtin، گروه هایی هستند که زمان نصب Active Directory به صورت پیش فرض همراه با برنامه نصب و ایجاد می‌شوند و می‌توان آن‌ها را در پوشه‌های Builtin و Users مشاهده کرد.



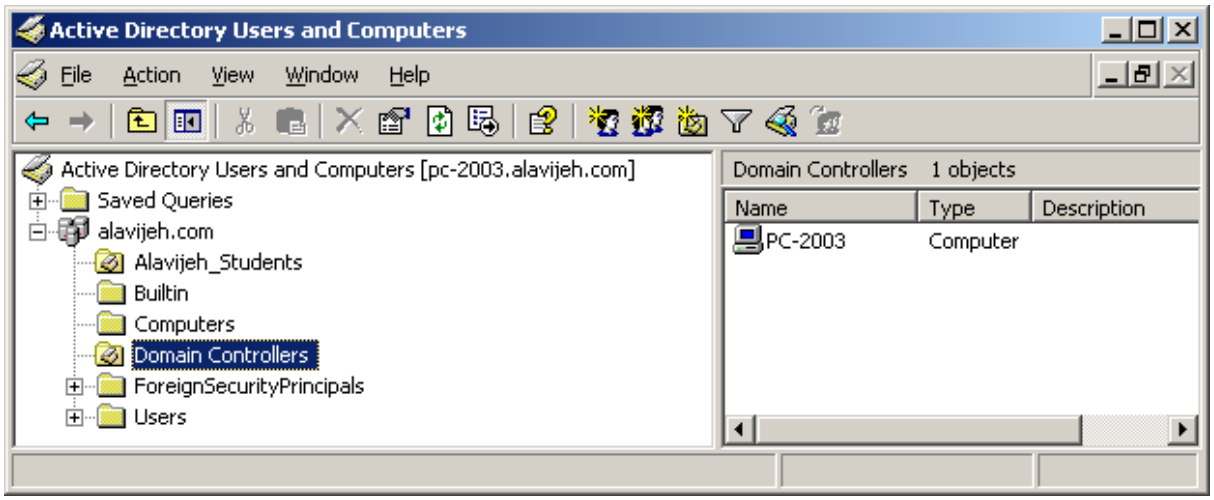
۲۹-۲-۲- پوشه Computers

به ازاء تمامی کامپیوتر هایی که عضو یک Doman می‌شوند، یک Computer Account در پوشه Computers مانند شکل زیر ایجاد می‌شود.



۲۹-۲-۳- Domain Controllers

هر کامپیوتری که عضو Domain می‌شود، به صورت خودکار برای آن کامپیوتر یک Computer Account در پوشه Computers در داخل Domain ایجاد می‌شود. اما برای کامپیوتر هایی که DC باشند، یک Account در Domain Controllers ایجاد می‌شود. در شکل زیر، ما فقط یک Domain Controller داریم.



۲۹-۲-۴- ForeignSecurityPrincipals

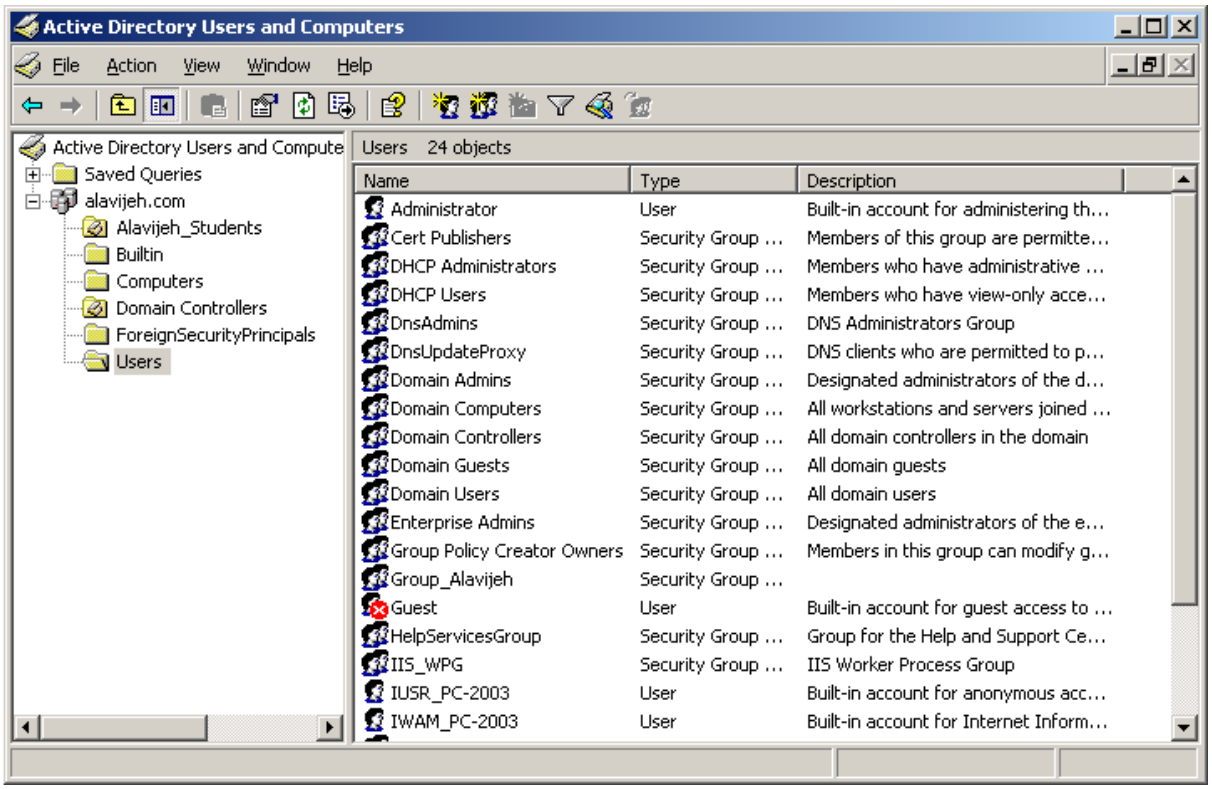
یک نگهدارنده است که تایید کنندههای امنیتی و هویتی را نگهداری می‌کند که این تایید کنندههای امنیتی و هویتی با Objectها و عناصر دامنه‌های خارجی Trust (روابط اعتمادی) شده، مجتمع شده‌اند.



۲۹-۳- مدیریت کاربران و گروه ها

بخش Users یکی از مهمترین و اصلی ترین بخش‌های Active Directory Users and Computers است.

نظارت، مدیریت و کنترل کاربران در هر سازمانی مهمترین بخش است و این مدیریت در اینجا توسط قسمت Users انجام می‌شود. با انتخاب قسمت Users، لیست تمامی کاربران و گروه‌های سیستم را مشاهده خواهید نمود. تصویر بیانگر یک کاربر و تصویر بیانگر یک گروه است. وجود یک علامت ضربدر قرمز رنگ نیز (مانند) بیانگر غیرفعال بودن یک کاربر یا یک گروه می‌باشد.



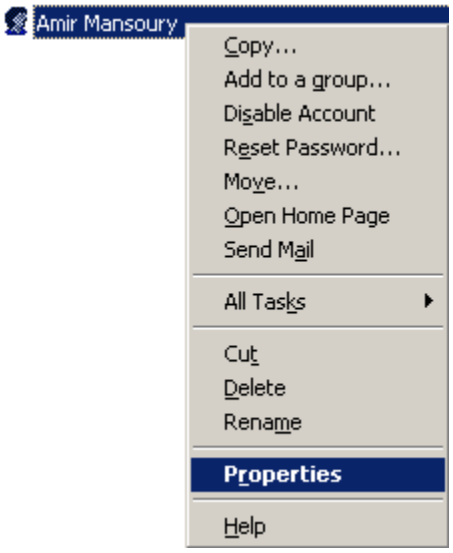
۲۹-۳-۱- تعریف کاربر، گروه و واحد سازمانی جدید

برای آشنایی با چگونگی تعریف کاربر، گروه یا واحد سازمانی جدید، به فصل User, Group, Organizational Unit مراجعه فرمایید.

۲۹-۴- مدیریت و تنظیمات کاربری

پس از ایجاد کاربر، مهمترین بخش آن مدیریت و تنظیمات کاربر جدید و دیگر کاربران می‌باشد. برای مدیریت کاربران به ترتیب مراحل زیر را دنبال می‌کنیم.

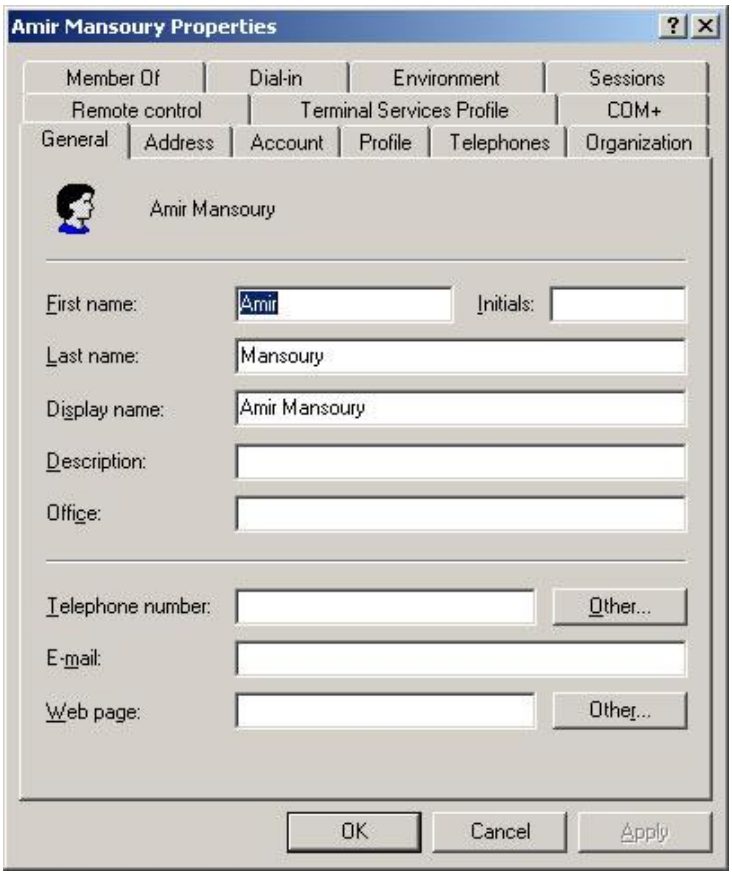
از پوشه User بر روی کاربر مورد نظر کلیک راست کرده و سپس گزینه Properties انتخاب کنید.



با این کار، پنجره زیر نمایان می‌شود. در این بخش هر Tab مرتبط با یکسری تنظیمات است که به صورت جدا به آن‌ها میپردازیم.

۲۹-۴-۱- General

این بخش شامل اطلاعات کاربر بطور کلی می‌باشد که شامل نام، نام خانوادگی، اسم نمایش داده شده، توضیحات، آدرس ایمیل و.... می‌باشد.



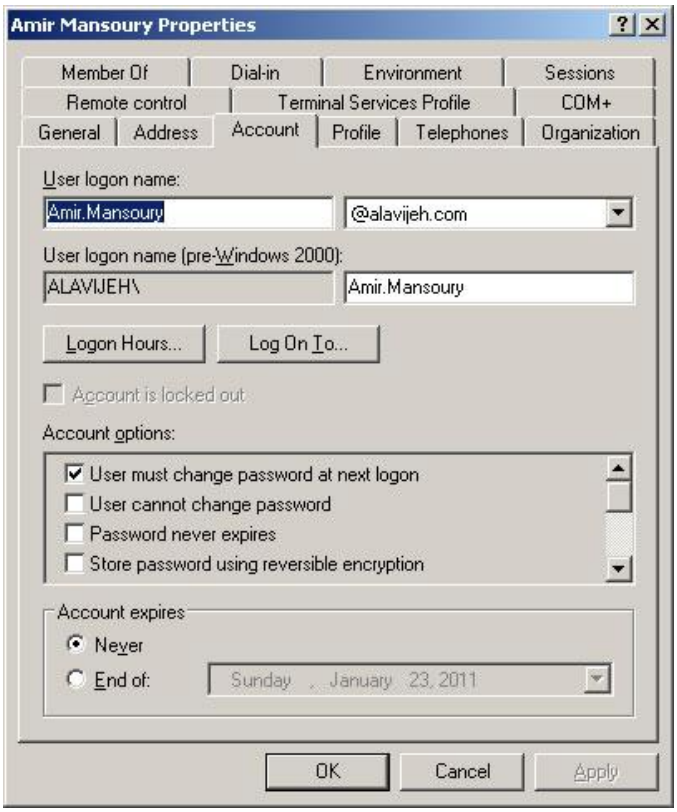
۲۹-۴-۲- Account

در این بخش تنظیمات زیر قابل انجام است:

بخش User Logon Name که همان نام کاربری است.

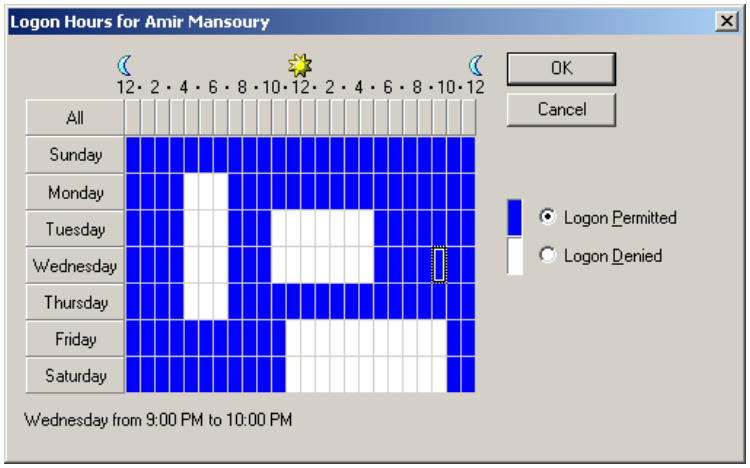
بخش Account Expires که توسط این گزینه می‌توانید برای کاربر محدودیت زمانی ایجاد کنید. بدین منظور که کاربر بعد از تاریخی خاص منقضی (Expire) شده و دیگر توانایی Login کردن را نداشته باشد. در ویندوز سرور بطور پیش فرض این گزینه بر روی Never تنظیم شده است. در صورت نیاز، می‌توانید زمان Expire شدن را تنظیم نمایید.

اما یکی از مهمترین مبحث‌ها در سیستم‌های کاربری، ساعت ورود و خروج کاربران به سیستم می‌باشد. شما به عنوان مدیر یک مجموعه باید بتوانید برای کاربران، ساعت‌های معینی را مشخص کنید تا کاربران فقط در این زمآن‌ها بتوانند به سیستم وارد شوند. برای این کار از Login Hours استفاده می‌کنیم.



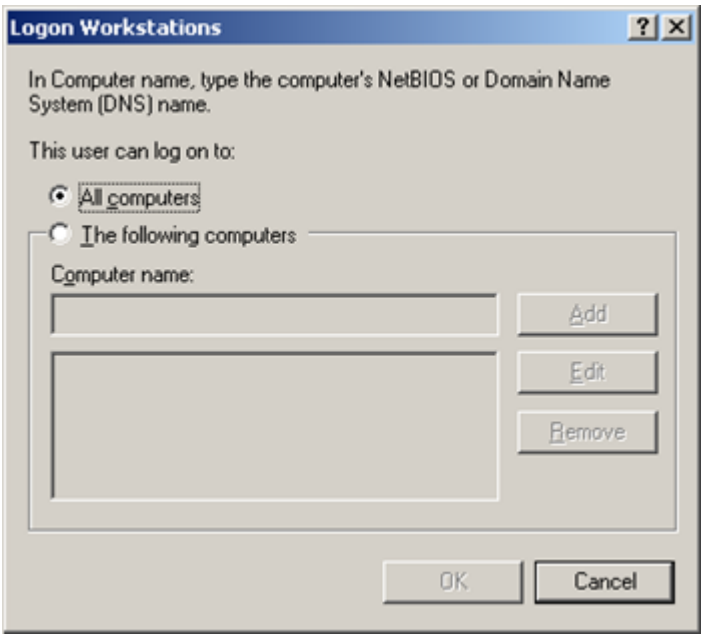
۲۹-۴-۳- *Logon Hours*

اگر روی دکمه Logon Hours کلیک کنید، شکلی مطابق شکل زیر به نمایش در می‌آید. این پنجره به شما نشان می‌دهد که کاربر در چه ساعات و در چه روزهایی، می‌تواند اجازه Login کردن به Domain را داشته باشد. شما می‌توانید هر کاربر را دارای محدودیتی زمانی در یکی از روزهای هفته و طی ساعاتی خاص بکنید. خانه هایی که با رنگ آبی پرشده‌اند بیانگر این موضوع هستند که کاربر در این ساعات و در این روزها اجازه Login کردن به Domain را دارد. شما می‌توانید با انتخاب یک خانه یا Select کردن خانه‌های متفاوت و گوناگون برای کاربر محدودیت ایجاد کنید. لذا باید آن خانه‌ها را به رنگ سفید در بیاورید که نشان دهنده آن است که کاربر در آن ساعات و در آن روزها اجازه Login به Domain را ندارد. بدین منظور بعد از انتخاب زمآن‌های مورد نظر، روی قسمت Logon Denied کلیک کنید. البته باید توجه داشت که در ویندوز سرور، پیش فرض تمامی خانه‌ها آبی رنگ هستند.

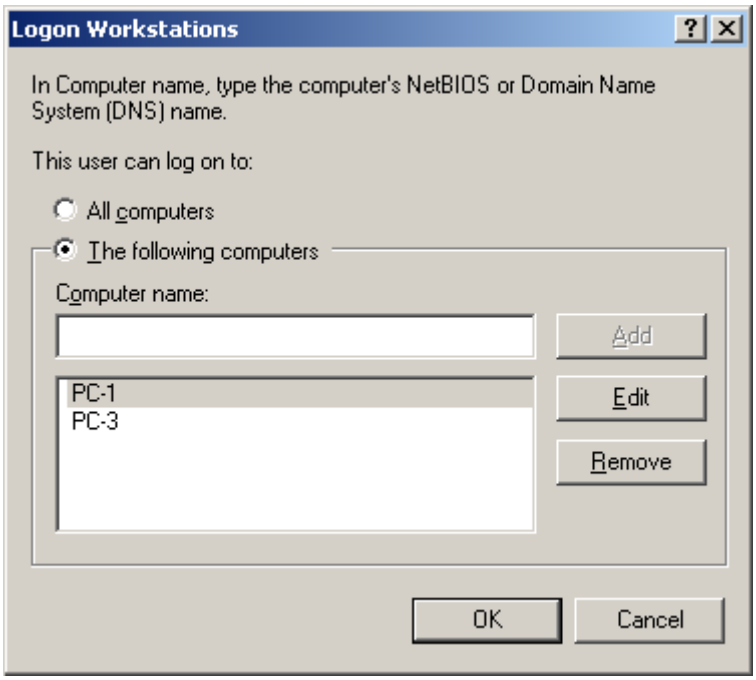


۲۹-۴-۴- *Log On To*

با انتخاب این گزینه می‌توانید برای کاربران محدودیتی ایجاد کنید که بر اساس این محدودیت، برخی کاربران فقط از طریق کامپیوتر هایی خاص بتوانند اقدام به Login کردن بکنند. بدین منظور در سربرگ Account روی دکمه Log On To کلیک کنید. در صفحه باز شده، مشخص است که کاربر از هر سیستمی می‌تواند Login کند.

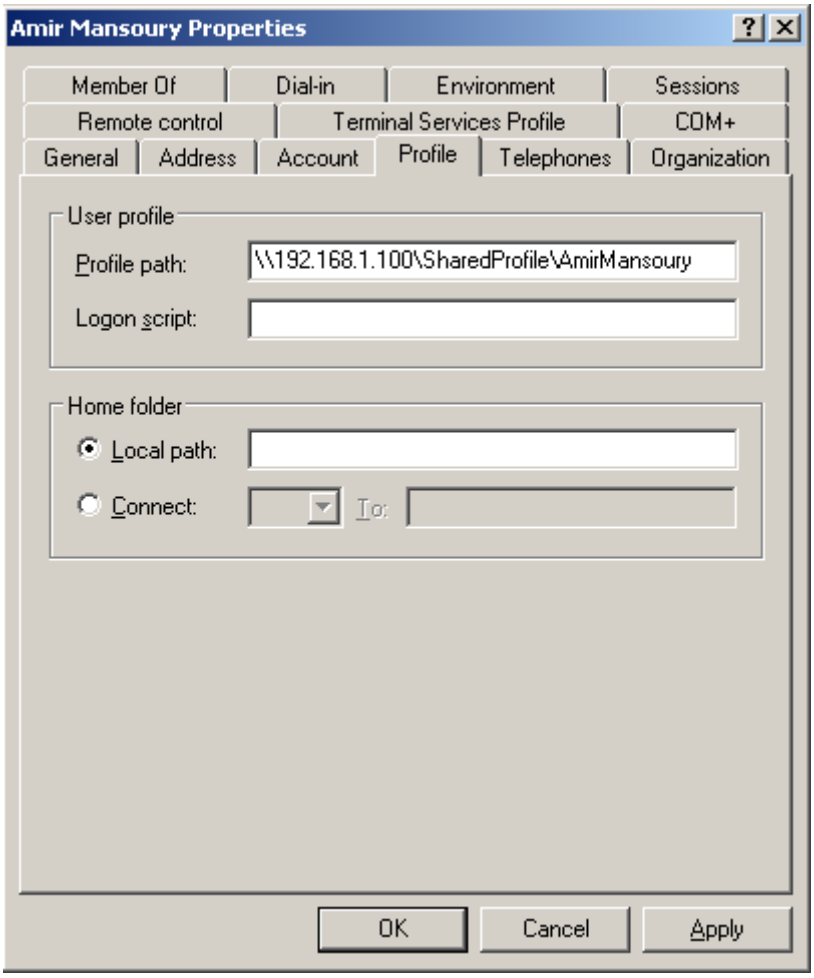


اما اگر خواستید که کاربر را محدود به سیستم هایی خاص کنید، ابتدا گزینه The following computers را فعال کرده و سپس **نام** کامپیوترهای مورد نظر **(Hostname)** را Add نمایید. مثلاً بر اساس شکل زیر، کاربر فقط می‌تواند از سیستم‌های PC-1 و PC-3 به سیستم Login کند.



Profile -۵-۴-۲۹

شما در این بخش این امکان را دارید که برای هر کاربر مشخص نمایید که فایل‌های شخصی و مرتبط با آن در جایی خاص قرار بگیرد و آن فرد از هر طریقی در هر کجا که به سیستم Login کند، بتواند به آن‌ها دسترسی داشته باشد. مثلاً اگر فایلی Shortcut را روی صفحه دسکتاپ خود قرار داد یا چینش نوار استارت خود را تغییر داد، این تغییرات را از هر سیستمی که Login می‌کند، بتواند ببیند. بدین منظور ابتدا در کامپیوتر سرور، یک پوشه را Share کرده (توجه نمایید که کاربران این پوشه باید قابلیت Read و Write را داشته باشند. لذا در تنظیمات Permission این پوشه، به کاربر Every One، قابلیت Read و Write را بدهید.) و سپس در این پوشه، یک پوشه دیگر به نام کاربر قرار دهید. سپس در بخش Profile Path **آدرس پوشه Share شده در شبکه** را وارد نمایید. توجه: در اینجا نباید مسیر فیزیکی پوشه در سرور را وارد نمایید. بلکه باید مسیر پوشه Share شده که دیگر کاربران شبکه برای دسترسی به این پوشه، آن مسیر را وارد می‌کنند، وارد کنید. در این مثال، ما در مسیر D:\SharedProfile یک پوشه ساخته و آن را Share می‌کنیم. حال پوشه D:\SharedProfile\AmirMansoury را می‌سازیم تا اطلاعات پروفایل کاربر در این پوشه قرار گیرد. حال بایستی مسیر پوشه Share شده در شبکه را وارد کنیم. با فرض اینکه آدرس IP سرور برابر ۱۹۲.۱۶۸.۱.۱۰۰ باشد، مسیر پوشه Share شده در شبکه برابر با \\192.168.1.100\SharedProfile\AmirMansoury خواهد بود.

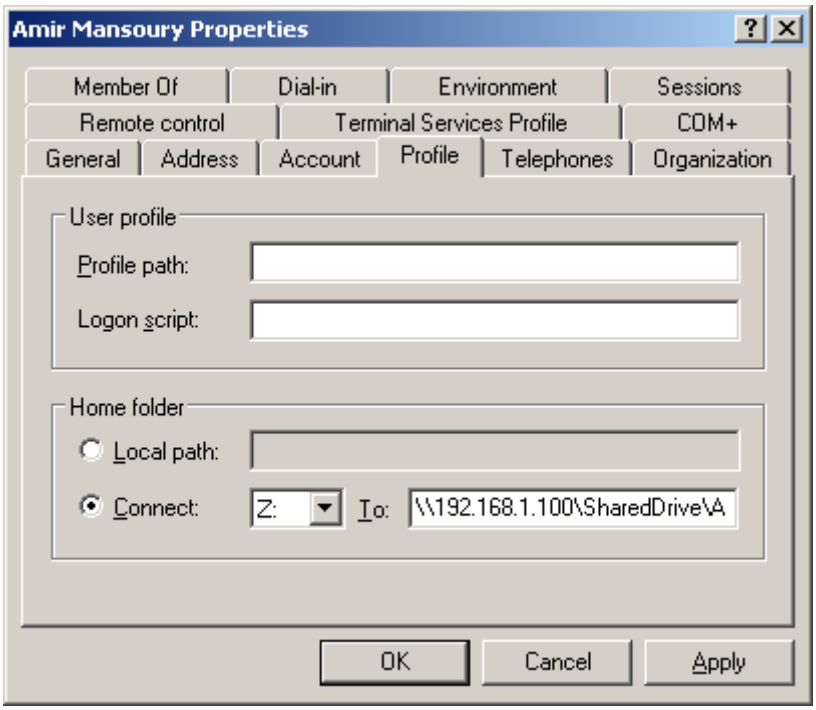


۲۹-۴-۶- *Home Folder*

امکان دیگری که این سربرگ دارد این است: وقتی که کاربر به Domain وارد می‌شود، پشت هر سیستمی که باشد، درایوهای دیسک سخت همان کامپیوتر را می‌بیند. به عنوان مثال اگر در درایو D:\ کامپیوتر PC-1 فایلی بسازد، سپس کاربر Logout کرده و اینبار با PC-3 وارد Domain شود، قادر به مشاهده فایل موجود در درایو D:\ نخواهد بود. ما در این بخش می‌خواهیم برای کاربر درایوی بسازیم که با هر سیستمی که Login کرد، بتواند این درایو را ببیند و اطلاعات آن در بین همه سیستم‌ها مشترک باشد. یعنی می‌خواهیم درایوی بسازیم که وابسته با کاربر باشد و نه وابسته به کامپیوتر.

بدین منظور، مانند قسمت قبل، ابتدا در کامپیوتر سرور، یک پوشه را Share کرده (توجه نمایید که کاربران این پوشه باید قابلیت Read و Write را داشته باشند. لذا در تنظیمات Permission این پوشه، به کاربر Every One، قابلیت Read و Write را بدهید.) و سپس در این پوشه، یک پوشه دیگر به نام کاربر قرار دهید. سپس در بخش Connect، **آدرس پوشه Share شده در شبکه** را وارد نمایید. توجه: در اینجا نباید مسیر فیزیکی پوشه در سرور را وارد نمایید. بلکه باید مسیر پوشه Share شده که دیگر کاربران شبکه برای دسترسی به این پوشه، آن مسیر را وارد می‌کنند، وارد کنید. در این مثال، ما در مسیر D:\SharedDrive یک پوشه ساخته و آن را Share می‌کنیم. حال پوشه D:\SharedDrive\AmirMansoury را می‌سازیم تا اطلاعات پروفایل کاربر در این پوشه قرار گیرد. حال بایستی مسیر پوشه Share شده در شبکه را وارد کنیم. با فرض اینکه آدرس IP سرور برابر ۱۹۲.۱۶۸.۱.۱۰۰ باشد، مسیر پوشه Share شده در شبکه برابر با

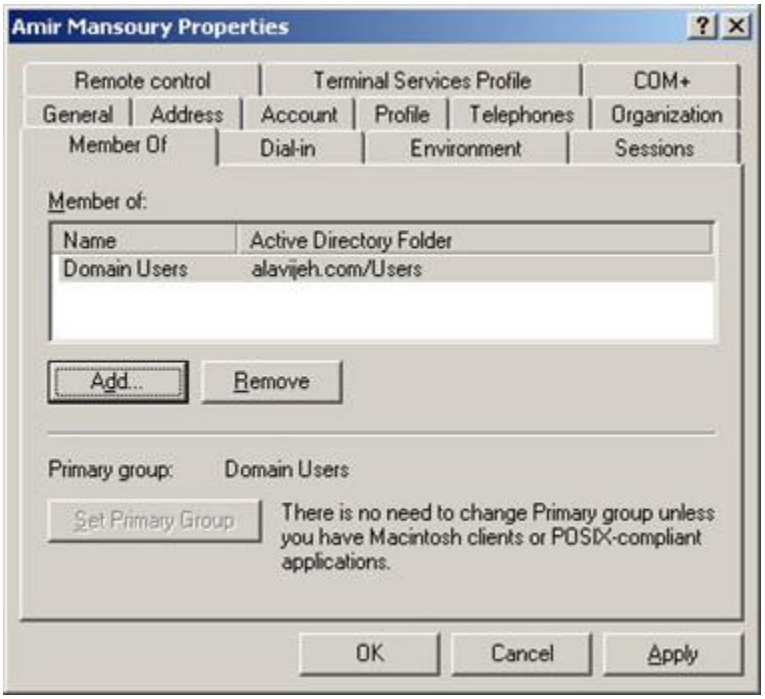
\\192.168.1.100\SharedDrive\AmirMansoury خواهد بود. همچنین در این قسمت باید مشخص نمایید که درایو ساخته شده، با چه حرفی نمایان شود. به صورت پیش فرض، این مقدار برابر Z:\ خواهد بود.



تنها نکته‌ای که باقی می‌ماند این است که با این کار، به صورت پیش فرض، کاربران هیچ گونه محدودیتی (از نظر میزان فضا) در استفاده از درایو خود ندارند و می‌توانند به حدی در آن اطلاعات بریزند تا درایو نگهدارنده این پوشه (در این مثال درایو D:\ موجود در سرور) پر شود. لذا بایستی کاربر را محدود کرد. بدین منظور بایستی از Disk Quota استفاده نمود. برای آشنایی با چگونگی این کار، به بخش Disk Quota در آخر همین فصل مراجعه نمایید.

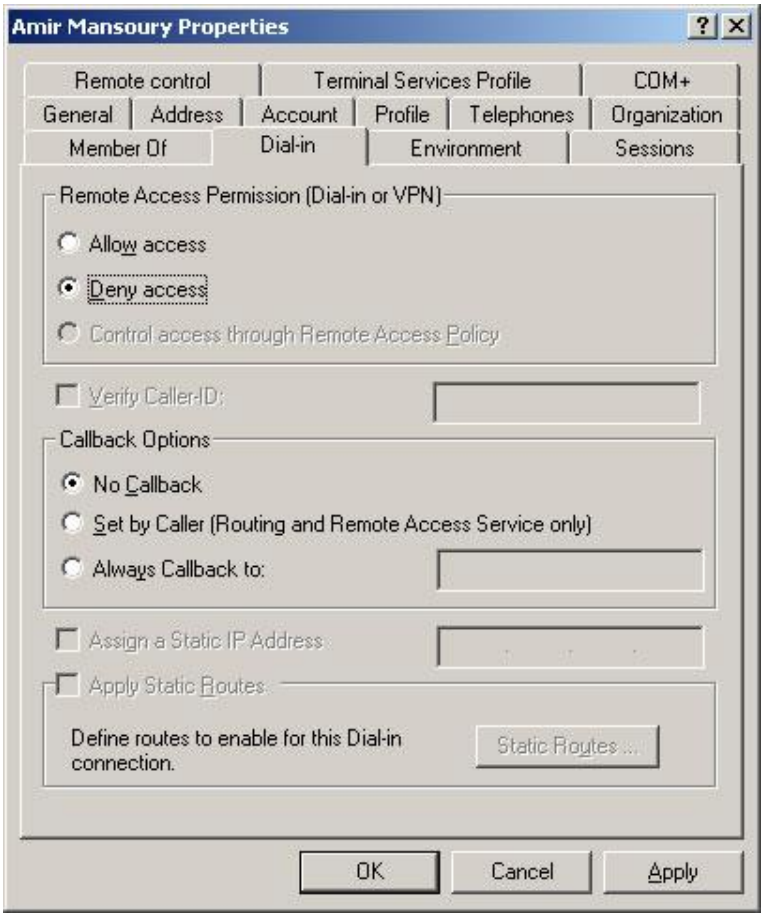
۲۹-۴-۷- *Member of*

از طریق این سربرگ می‌توانید مشاهده کنید که کاربر عضو چه گروه هایی است. با کلیک روی دکمه Add، و سپس انتخاب یک گروه (گروه های) خاص، می‌توانید این کاربر را عضو این گروه (گروه ها) کنید. با کلیک روی دکمه Remove نیز کاربر از عضویت گروه خارج می‌شود.



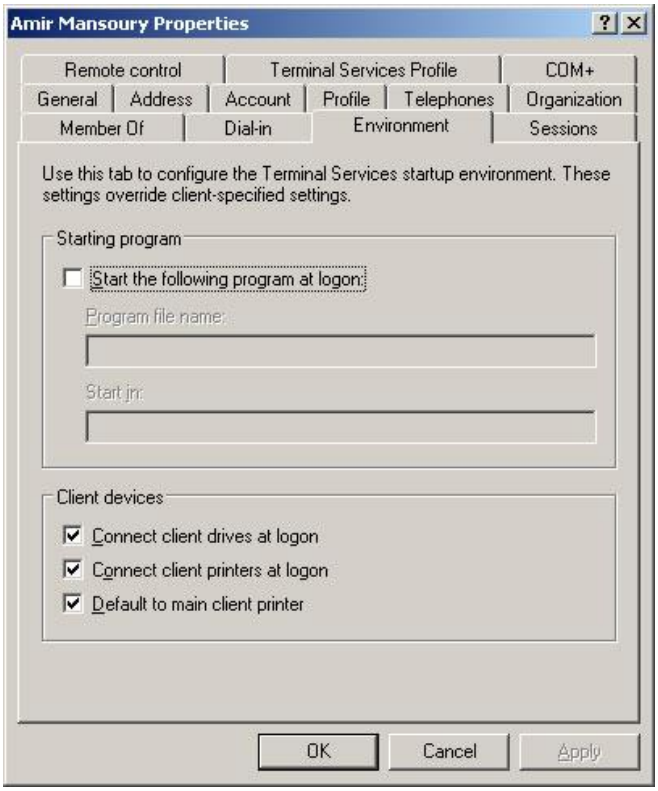
۲۹-۴-۸- Dial-in

این بخش برای راه‌های اتصال به شبکه از راه‌های دیگر مثلاً به شیوه شماره گیری یا VPN می‌باشد. از طریق این قسمت می‌توانید تعیین کنید که آیا این کاربر قابلیت اتصال به شبکه از طریق شماره گیری یا VPN را دارد یا خیر؟ برای اطلاعات بیشتر به فصل Dialup , VPN مراجعه نمایید.



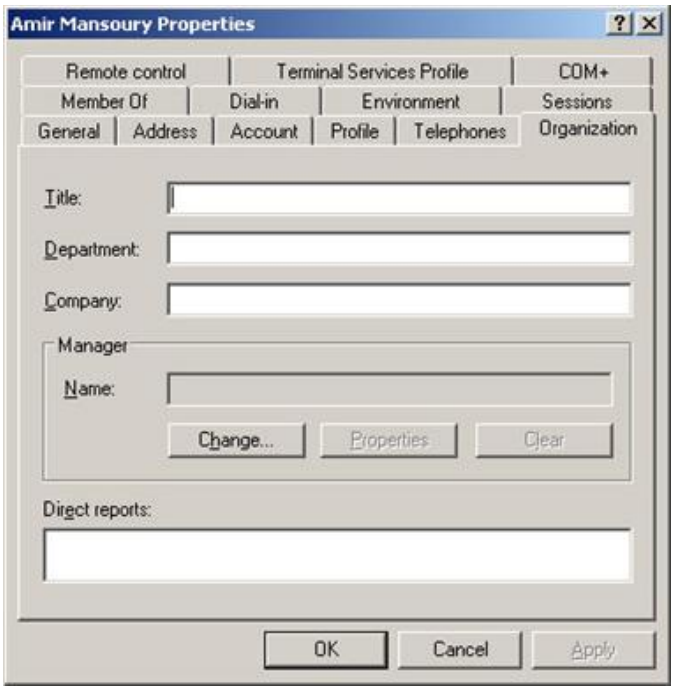
Environment – ۹-۴-۲۹

در این بخش می‌توانید مشخص کنید که همزمان با Login کردن کاربر، چه برنامه‌ای برای آن کاربر شروع به اجرا شدن بکند. همچنین در Client Devices می‌توانید امکان استفاده از برخی تجهیزات سخت‌افزاری و استفاده از وسایل جانبی را به کاربر بدهید.



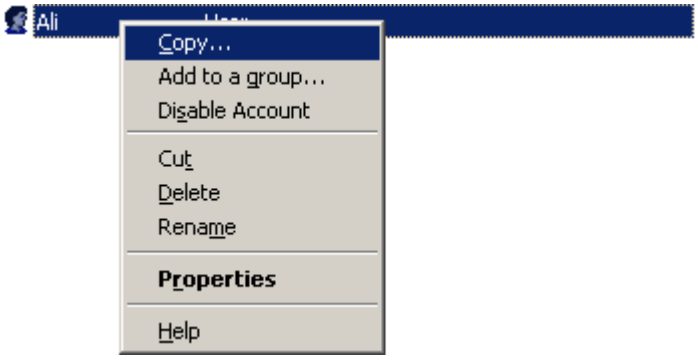
Organization – ۱۰-۴-۲۹

در این بخش اطلاعات سازمانی کاربر وارد و مدیریت می‌شود (این اطلاعات سازمانی با بحث واحد سازمانی یا OU متفاوت است). از قبیل سِمت کاری، نام شرکت و همچنین واحد کاری که کاربر در آن مشغول به کار است.

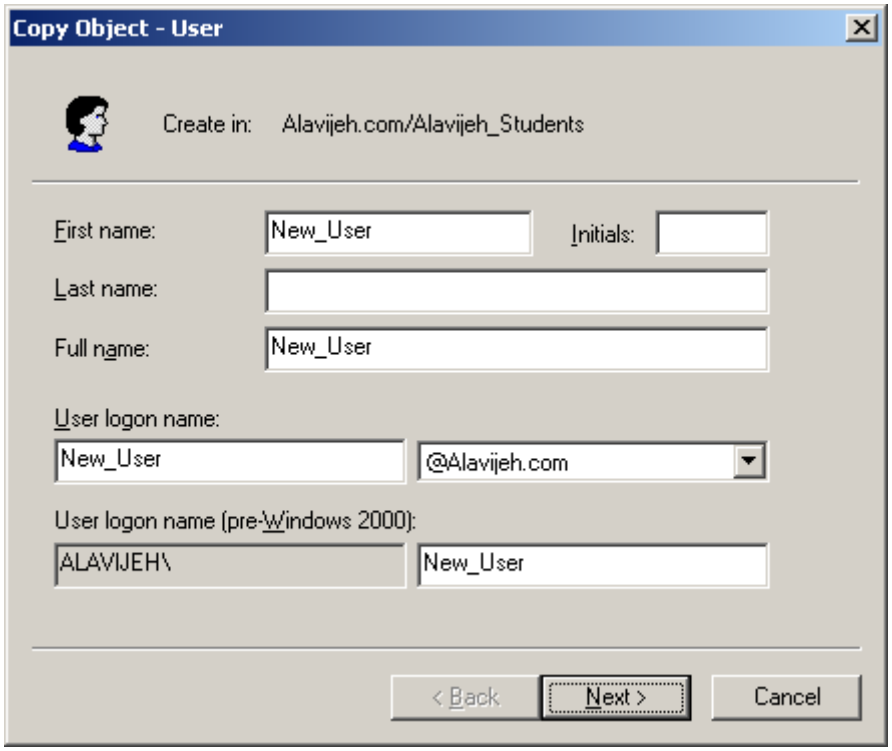


۲۹-۴-۱۱- تکثیر کاربران

فرض کنید نیاز داریم تعداد زیادی کاربر بسازیم که تمامی این کاربران ویژگی‌ها و سیاست‌ها و دسترسی‌های مشترک دارند. اینکه بخواهیم که کاربران را تک تک تعریف نموده و ویژگی‌های هر یک را نیز تک تک تعریف کنیم، کمی سخت و با ضریب اشتباه بالا می‌باشد. راه عاقلانه این می‌باشد که یک کاربر بسازیم (مثلاً به اسم User_Temp) و تنظیمات را روی آن اعمال کنیم. سپس کاربر مورد نظر را Disable می‌نماییم (به دلیل مسائل امنیتی حتما کاربر مذکور را غیر فعال نمایید). سپس هر گاه به کاربری نیاز داشتید که مشخصاتش معادل یا شبیه این کاربر باشد، می‌توانیم از این کاربر یک کپی بگیریم و کاربر جدید را فعال سازیم. بدین منظور روی نام کاربر مرجع راست کلیک نموده و گزینه Copy را انتخاب نمایید.



سپس صفحه‌ای باز می‌شود و مشخصات کاربر جدید را می‌خواهد. توجه داشته باشید که تمام اطلاعات کاربری کاربر قدیمی (مانند سطوح دسترسی، سیاست‌ها و...) برای کاربر جدید نیز کپی می‌شود؛ و نیازی به تنظیم مجدد آن نمی‌باشد.



۲۹-۵- آشنایی با انواع گروه‌های Biult-in

گروه‌های Biult-in، گروه‌های هستند که بطور پیش فرض در زمان نصب Active Directory ایجاد می‌شوند؛ که بطور خلاصه برخی از آن‌ها را معرفی می‌کنیم.

Builtin Global User

این نوع گروه‌ها در پوشه Users و در ابزار Active Directory Users and Computers قرار داشته و عبارتند از:

۱. **Domain Users:** این گروه شامل تمامی کاربران Domain است. هر کاربری که در Domain ایجاد می‌شود، به صورت خودکار به عضویت این گروه در آمده و می‌تواند از هر کامپیوتری به Domain وارد شود. اگر می‌خواهید که کاربری از راه دور نتواند به Domain وارد شوند و برای وارد شدن به Domain از خود کامپیوتر DC استفاده کند، وی را از عضویت این گروه خارج کنید.

۲. **Domain Administrators:** اعضای این گروه می‌توانند Domain را مدیریت کنند. این افراد به عنوان مدیر Domain شناخته می‌شوند. فقط Administrator مربوط به همان Domain، به صورت پیش فرض عضو این گروه می‌باشد.

Built-in Domain Local

این گروه‌ها در پوشه Built-in در ابزار Active Directory Users and Computers قرار دارند که عبارتند از:

۱. **Administrators:** اعضای این گروه می‌توانند DCها را مدیریت کنند. این اعضا تمامی مجوزها بر روی این کامپیوترها را دارا می‌باشند.

۲. **Account Operators:** اعضای این گروه عملیات مدیریتی همچون ایجاد، حذف و... را روی Accountها انجام میدهند. بطور مثال می‌توانند یک گروه را ایجاد و کاربرانی را به عضویت آن گروه در بیاورند.

۳. **Print Operators:** اعضای این گروه می‌توانند چاپگرهای Domain را مدیریت کنند.

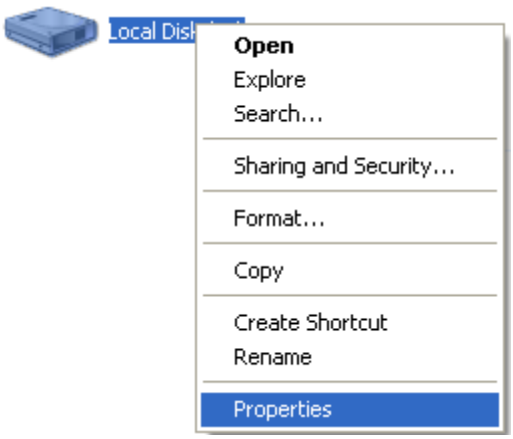
۴. **Backup Operators:** اعضای این گروه می‌توانند عملیات Backup گرفتن از اطلاعات و برگرداندن اطلاعات (Restore کردن) را انجام دهند.

۲۹-۶- آموزش کار با Disk Quota

Disk Quota امکانی است در ویندوز که به کمک آن می‌توان به تمام کاربران یک مجموعه یا به تعدادی از کاربران، یک مقدار خاص از فضای هارد دیسک اختصاص داد. در این صورت، آن‌ها قادر به استفاده بیشتر، از فضای تعیین شده نمی‌باشند.

توجه: این امکان فقط بر روی پارتیشن‌های که به فورمت NTFS هستند کار می‌کند.

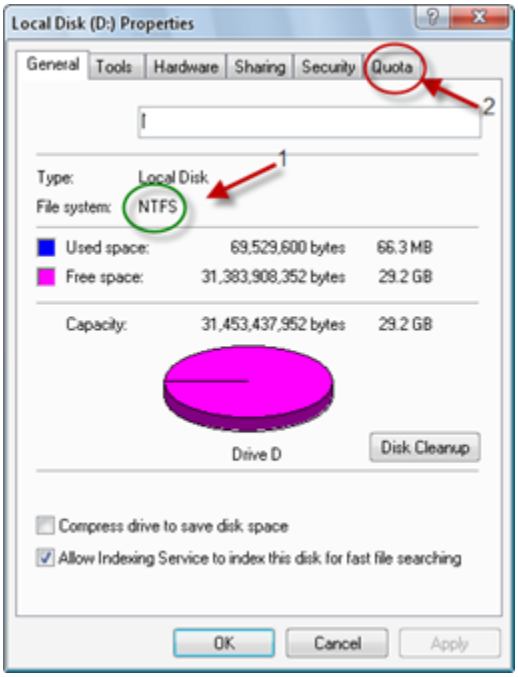
برای شروع کار، بر روی پارتیشنی که می‌خواهید این کار را انجام دهید کلیک راست کرده و گزینه Properties را انتخاب کنید.



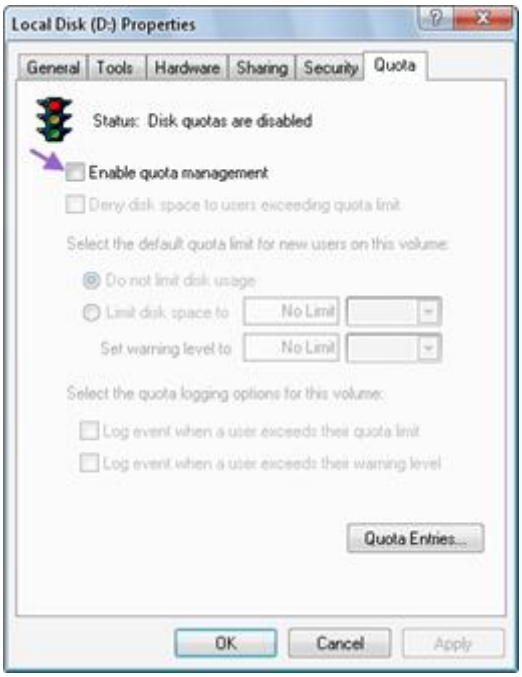
بعد از انتخاب این گزینه، شکل زیر باز می‌شود که شما باید کارهای زیر را انجام دهید.

۱. باید توجه داشته باشید فرمت پارتیشن شما NTFS باشد.

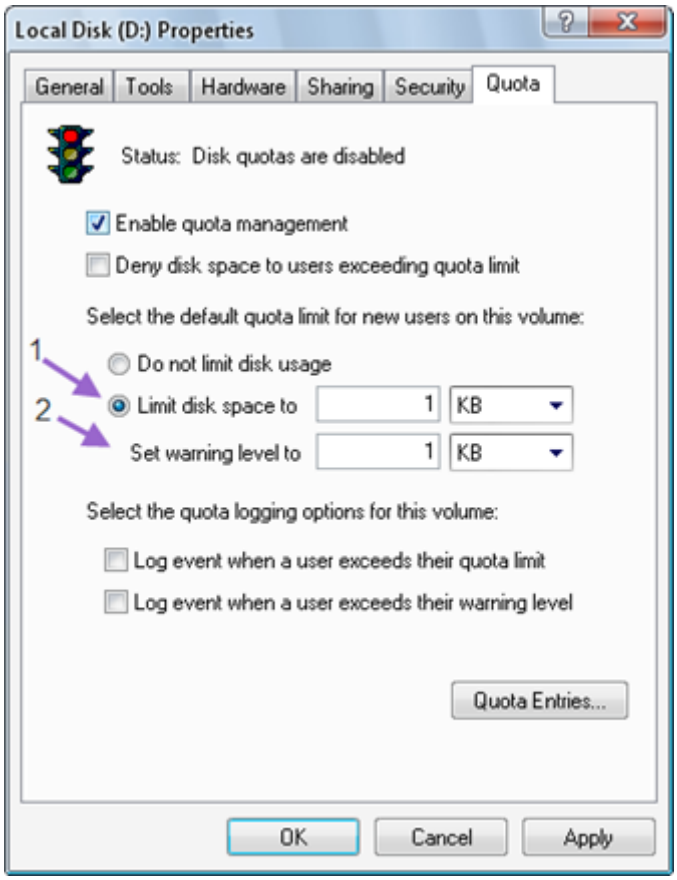
۲. سربرگ Quota را انتخاب کنید.



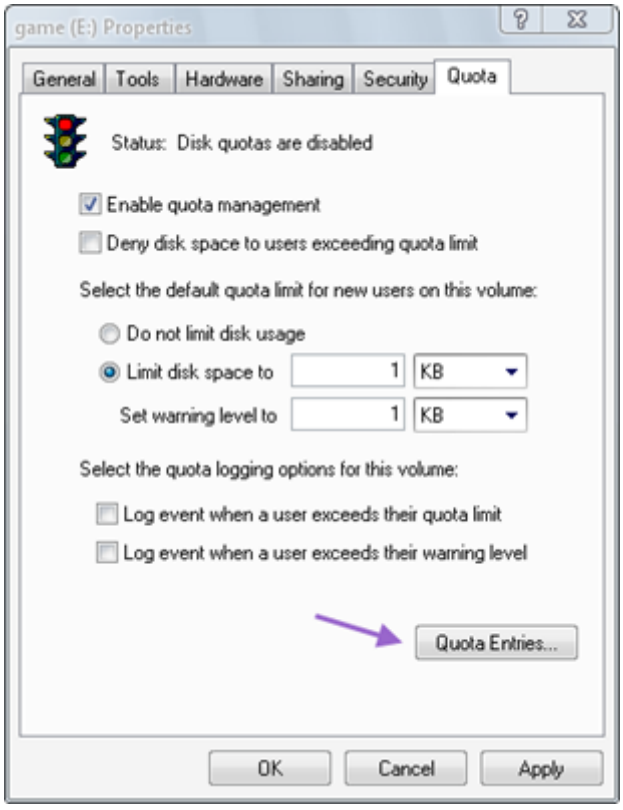
در این شکل، طبق فلش، گزینه Enable quota management را فعال کنید.



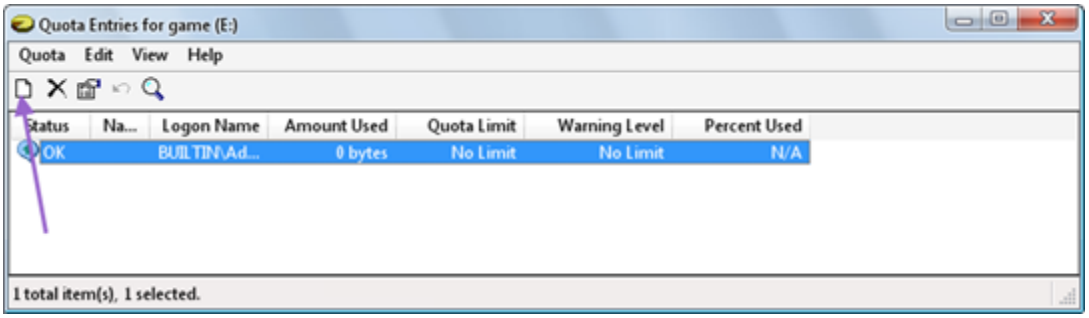
طبق شکل زیر، با انتخاب گزینه اول شما می‌توانید حداکثر فضایی که می‌خواهید به کاربران بدهید را وارد کنید و در گزینه دوم نیز می‌توانید عددی را وارد کنید که اگر فضای کاربر از آن عبور کرد، سیستم اخطار دهد.



مقدار فضایی که در شکل قبل تعیین، روی تمام کاربران اعمال می‌شود. اگر می‌خواهید به کاربری خاص، مقدار فضای دیگری را بدهید، در همین صفحه روی دکمه Quota Entries کلیک کنید.

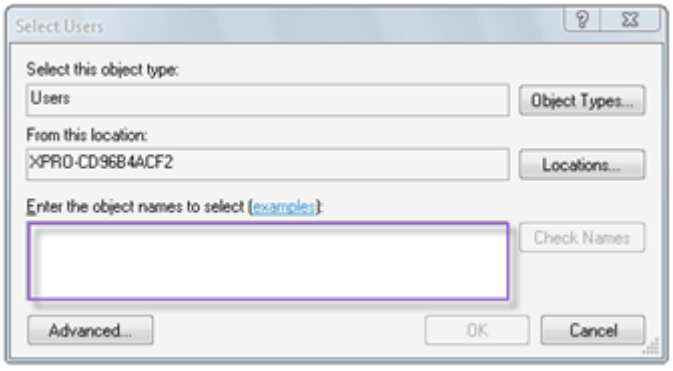


در صفحه باز شده، طبق شکل بر روی گزینه New کلیک کنید.

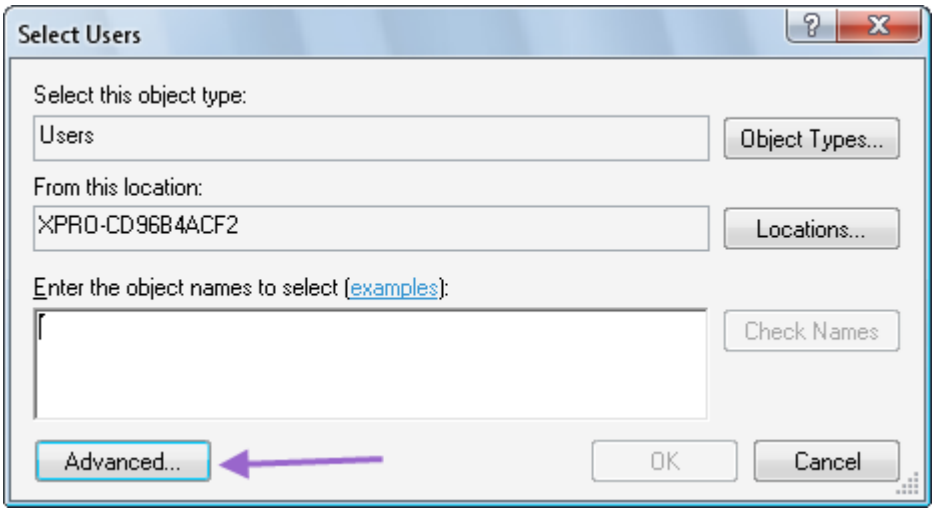


در صفحه باز شده، شما باید نام کاربر مورد نظر را وارد کرده و تایید کنید.

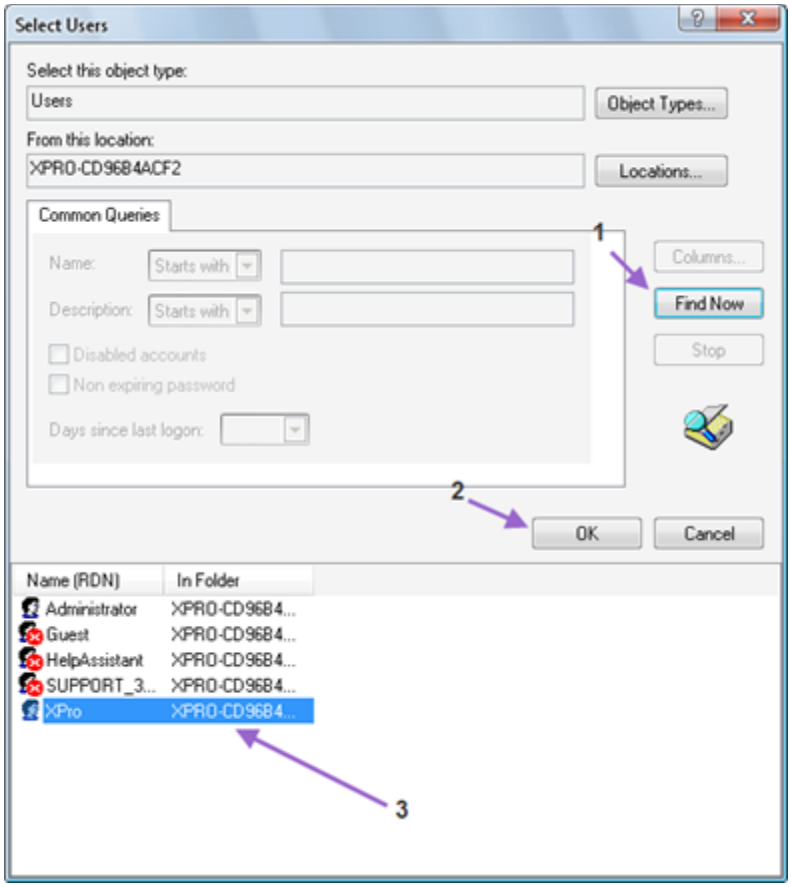
توجه: اگر شما مدیر ویندوز نباشید نمی‌توانید برای دیگر کاربران، فضا تعیین کنید.



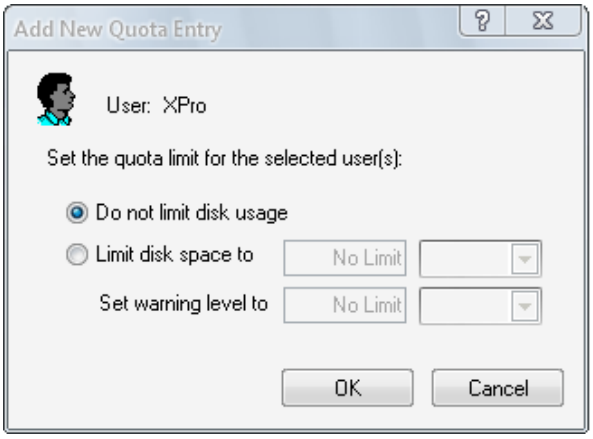
اگر نام کاربر را نمی‌دانید، طبق شکل ابتدا روی دکمه Advanced کلیک کنید.

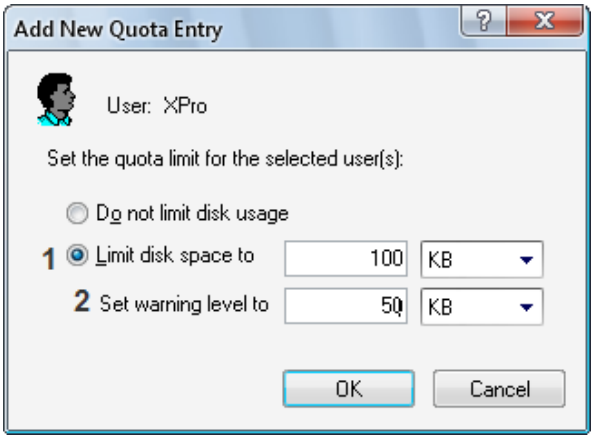


سپس روی دکمه Find کلیک کرده، کاربر(کاربران) مورد نظر را انتخاب کرده و در نهایت روی OK کلیک کنید.



حال اگر می‌خواهید کاربر(کاربران) انتخاب شده، محدودیتی در استفاده از فضای دیسک نداشته باشند، گزینه Do not limit disk usage، و اگر می‌خواهید محدودیتی روی فضای قابل استفاده آن‌ها ایجاد کنید، ابتدا گزینه Limit disk space to را فعال کرده و سپس مقادیر مورد نظر را وارد نمایید.





پس از تایید، کاربر جدید به لیست اضافه شده و شما می‌توانید آن را ببینید.

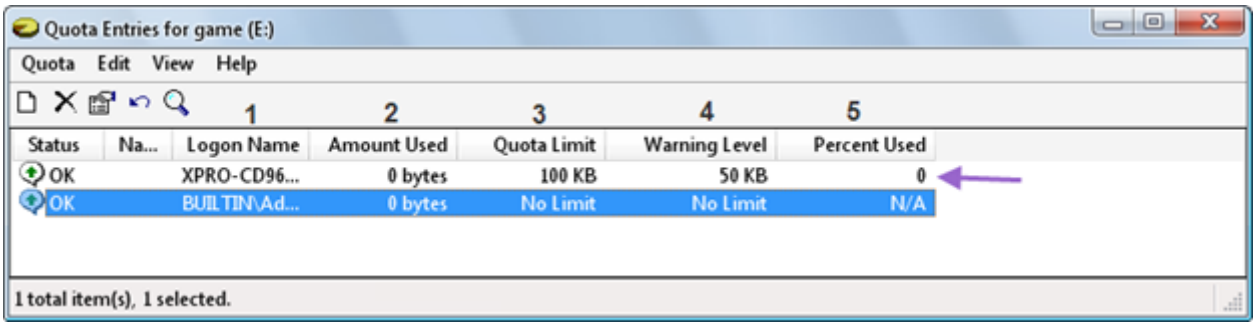
در شماره ۱ اسم کاربر نمایش داده می‌شود.

در شماره ۲ کل فضای استفاده شده نمایش داده می‌شود.

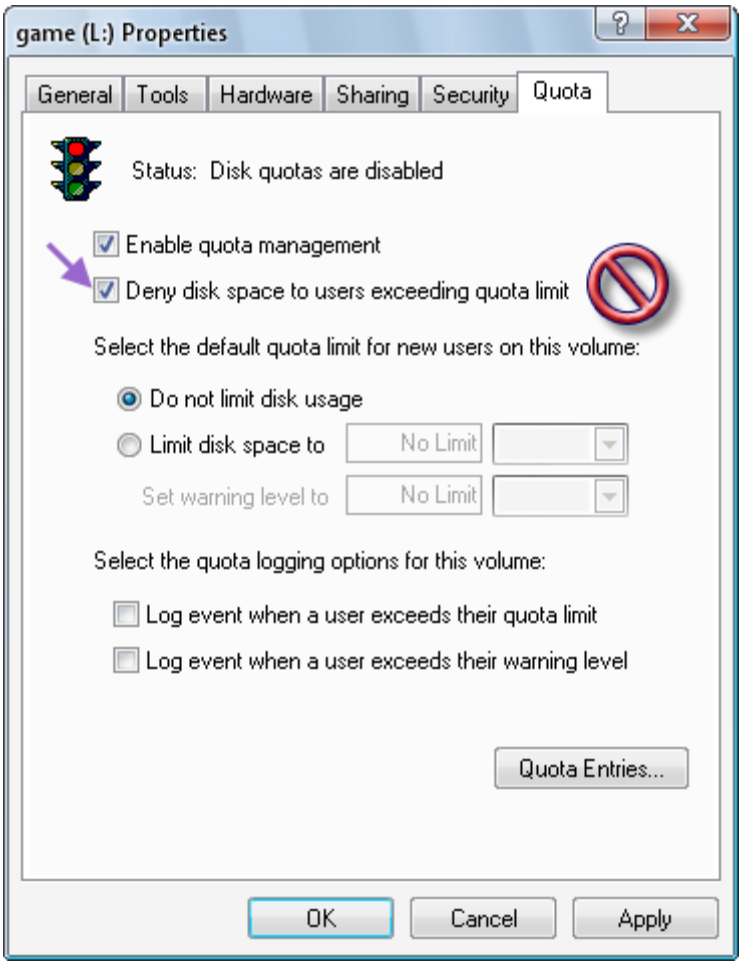
در شماره ۳ کل فضای اختصاص داده شده به کاربر نمایش داده می‌شود.

در شماره ۴ اگر کاربر از حد مجاز تعیین شده عبور کند، اخطار می‌دهد.

در شماره ۵ درصد استفاده شده از کل فضا را نشان می‌دهد.



این کار فقط در حد مانیتورینگ است. و برای عملی کردن این کار باید طبق شکل زیر عمل کرد.



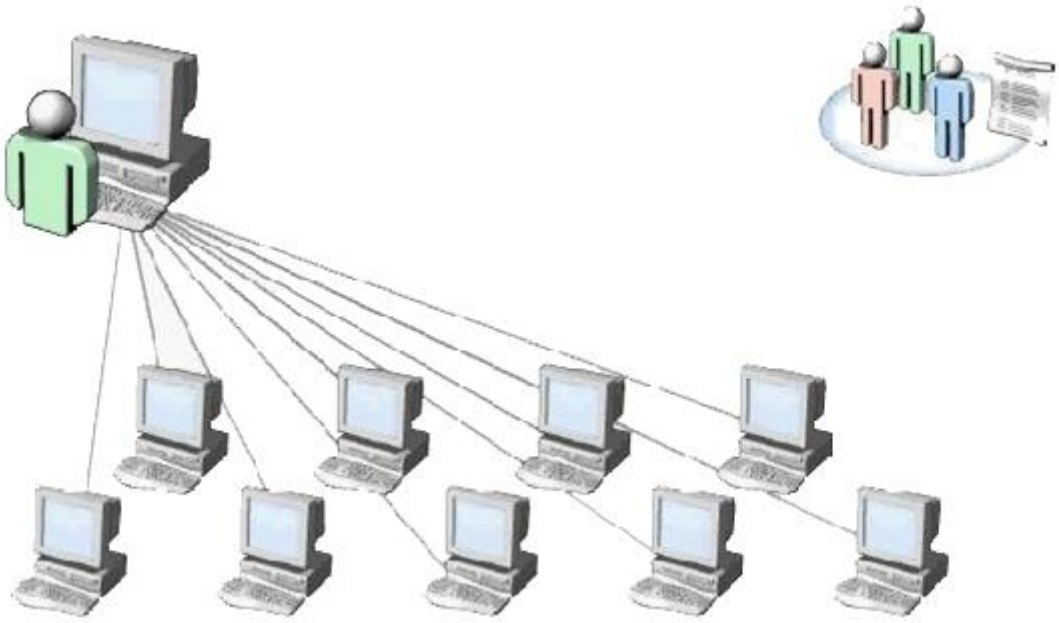
در این شکل با تیک زدن جای مشخص شده تمام کاربران انتخاب شده توسط شما به مقدار فضایی که دارند محدود می‌شوند.

فصل ۳۰

سیاست گروهی (Group Policy)

۳۰-۱- تعریف Group Policy

وقتی صحبت از قلب ویندوز به میان می‌آید، عموما تصویری از Registry در ذهن ایجاد می‌شود. Registry ابزار قدرتمندی است که قلب و هسته اصلی اعمال تغییرات در ویندوز است. اما در این بین Group Policy نیز ابزاری حیاتی و در عین حال ساده و User Friendly (کاربر پسند) است که می‌تواند تغییرات بسیار جامع و کاملی را شامل شود. در مقایسه با Registry می‌توان گفت که سادگی کار و وجود توضیحات کافی Group Policy را برتر از Registry جلوه می‌دهد.Group Policy در ویندوز سرور ۲۰۰۳، یک روش کارآمد و مفید به منظور مدیریت متمرکز و انجام تنظیمات بر روی Clientها می‌باشد.Group Policy به سرورها و مدیران شبکه قدرت تنظیم و اعمال اجباری سیاست‌های خود بر روی کاربران و کامپیوتر هایی که به عنوان Client در شبکه قرار دارند را می‌دهد.



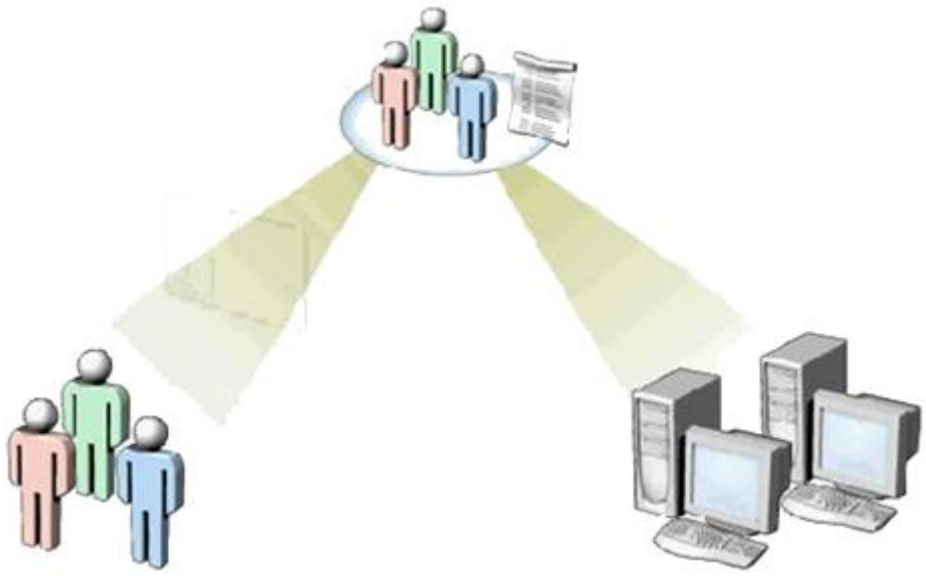
برخی از سیاست‌ها که توسط Group Policy بر روی کامپیوتر، کاربر یا گروهی خاص و بدون دخالت کاربر و از روی سرور انجام می‌شود عبارتند از:

۱. نصب برنامه‌های کاربردی روی سیستم
۲. تنظیم اجباری رجیستری به تفکیک کاربر یا به تفکیک کامپیوتر (منظور دستگاه Clientی که به شبکه Login می‌کند)
۳. تنظیمات موارد امنیتی (Security Setting)
۴. اجرای اسکریپت هایی هنگام Log in یا Log off
۵. اجرای اسکریپت هایی هنگام بالا آمدن یا خاموش شدن سیستم
۶. حذف و اضافه نمودن گزینه‌ای Taskbar و Start Menu و کنترل پانل
۷. برخی تنظیمات برای سرویس هایی که از راه دور نصب می‌گردند.

به عبارت دیگر یک مدیر شبکه با این امکان به جای اینکه روی تک تک سیستم‌ها تنظیماتی را انجام دهد، می‌تواند از طریق سرور و برای گروه‌های مختلف سیاست‌های گوناگون را تنظیم و اعمال نماید؛ به طوری کاربر هیچگونه دخالتی در این خصوص نداشته باشد.

نکته: دقت کنید که تنظیمات Group Policy تنها بر روی سیستم عامل‌های Windows XP Professional، Windows 2000 و Windows Server 2003 اعمال می‌شوند و بر روی ویندوزهای قدیمی نظیر خانواده 9X و یا Millennium پیاده سازی نخواهند شد.

برخی از تنظیمات Group Policy مخصوص کاربر و برخی دیگر از تنظیمات مخصوص کامپیوتر است. یعنی اگر تنظیمات روی کاربر اعمال گردد، آن کاربر از هر کامپیوتری که وارد شبکه گردد، آن سیاست‌ها و تنظیمات روی وی اعمال می‌شود و به کامپیوتر بستگی ندارد و برخی از سیاست‌ها Policy) ها(که روی کامپیوتر اعمال می‌شود به کاربر بستگی ندارد.



یک کامپیوتر با ویندوز سرور، به صورت پیش فرض، یک Local Group Policy دارد و می‌تواند تعدادی NonLocal Group Policy نیز داشته باشد.

- **Local Group Policy:** حتما با معنای واژه Local آشنایی دارید؛ یک Local Group Policy یعنی Group Policy هر کامپیوتر در خودش ذخیره شود و در واقع زمانی چنین روشی اتخاذ می‌شود که در محیط Active Directory Domain نیستیم. یک Local Group Policy فقط روی همان کامپیوتری که در آن قرار دارد اعمال می‌شود و nonLocal Group Policyها ارجحیت بیشتری نسبت به Local Group Policyها دارند. حال اگر در محیط دامنه Active Directory باشیم، سیاست‌های nonLocal ارجحیت بیشتری بر سیاست‌های Local دارند. پس اهمیت Local Group Policy زمانی است که کامپیوتر در یک شبکه بدون Active Directory حضور دارد. محل ذخیره سازی این تنظیمات %Systemroot%\System32\GroupPolicy است.
- **Non-Local Group Policy:** این سیاست‌ها باید در Active Directory ساخته شوند و به یک Site، Domain، OU مرتبط شوند. به صورت پیش فرض، با نصب Active Directory، دو Group Policy ساخته می‌شوند که عبارتند از:

۱. **Default Domain Policy:** این سیاست روی تمام دامنه (Domain) شامل کامپیوترها، Userها و Domain Controllerها اعمال می‌شود.

۲. **Default Domain Controllers Policy:** این سیاست روی تمام Domain Controller OU اعمال می‌شود. یادآوری می‌کنم که حساب Domain Controllerها روی یک OU جدا به نام Domain Controller نگه داری می‌شود. در صورتی که جای پوشه sysvol مقدار پیش فرض باشد، این سیاست‌ها در %Systemroot%\Sysvol\Domain Name\Policies\GPO GUID\Adm% ذخیره می‌شوند که که در این آدرس GUID یک ID یکتا است.

نکته مهم: یک GPO که برای یک سایت تعریف شده باشد، روی تمام کامپیوترهای آن سایت اعمال می‌شود. بنابراین، بدون توجه به دامنه‌ای که آن کامپیوتر در آن عضو است، می‌توان یک Group Policy اعمال کرد. (بدیهی است در یک جنگل باید باشند)

۳۰-۲- نحوه فعال شدن Group Policy

ابزار متداول ویرایش Group Policy، نرم‌افزار Group Policy Object Editor است. آنکه چگونه این ابزار را باز کنید، به این بستگی دارد که این سیاست‌ها به کجا قرار است اعمال شود و نوع Group Policy چیست.

۱. LGPO - Local Group Policy Objects:

- در RUN وارد کنید MMC و از منوی file گزینه Add/Remove Snap-In را انتخاب کنید.
- در زبانه Standalone Tab در صفحه Add/Remove Snap-In دکمه Add را بزنید.
- Group Policy Object Editor را Add کنید و دقت کنید که Local Computer انتخاب شده است.
- Finish را بزنید و سپس با زدن OK صفحه را ببندید.

نکته: با استفاده از GPedit.msc می‌توانید وارد LGPO شوید. از این رو، گاهی در لغت GPedit را به جای GPOE به کار می‌برند که منظور همان GPOE است.

۲. LGPO روی کامپیوتر دیگر:

- مراحل ۱ را انجام دهید با این تفاوت که با جای Local Computer، کامپیوتر دلخواه را انتخاب کنید.

۳. GPO روی یک سایت:

- به Administrative Tools بروید و کنسول Active Directory Site & Services را باز کنید.
- در درخت کنسول (نوار سمت چپ کنسول) روی سایتی که می‌خواهید Group Policy اعمال کنید، کلیک راست کنید و Properties را بزنید.
- به زبانه (Tab) مربوط به Group Policy بروید و برای اضافه کردن یک GPO گزینه Add را بزنید. می‌توانید برای ویرایش موارد موجود Edit را بزنید و...

۴. GPO روی یک OU یا دامنه:

- به Administrative Tools بروید و کنسول Active Directory Users & Computers را باز کنید.
- در درخت کنسول (نوار سمت چپ کنسول) روی دامنه یا OU که می‌خواهید Group Policy اعمال کنید، کلیک راست کنید و Properties را بزنید.
- به زبانه (Tab) مربوط به Group Policy بروید و برای اضافه کردن یک GPO گزینه Add را بزنید. می‌توانید برای ویرایش موارد موجود Edit را بزنید.

تنظیماتی که شما در Group Policy انجام می‌دهید درون Group Policy Object یا به اختصار (GPO) ذخیره می‌شود. با هم نگاهی کوتاه به تنظیمات درون GPO می‌اندازیم.

Administrative Templates:

محل انجام تنظیمات Windows Components، Desktop، Start Menu and Taskbar، Control Panel، Shared Panel و Network System می‌باشد.

برای مثال در این قسمت می‌توان از تنظیماتی همچون نحوه اجرای Welcome Screen، تنظیمات مربوط به درایورها، Interface مربوط به کاربران و تنظیمات مربوط به Editing Registry می‌باشد.

Security:

قوانینی است که می‌توانیم بر روی یک کامپیوتر و یا چندین کامپیوتر اعمال کنیم و از منابع موجود بر روی شبکه محافظت کنیم. Security Setting می‌تواند اعمالی همچون نحوه شناسایی کاربران در شبکه و یا نوع منابعی که کاربران اجازه‌ی استفاده از آن‌ها را دارند، نوع اطلاعاتی که باید درون Event Viewer ذخیره گردد و هم چنین عضویت در گروه‌های مختلف را کنترل نماید.

Software Installation:

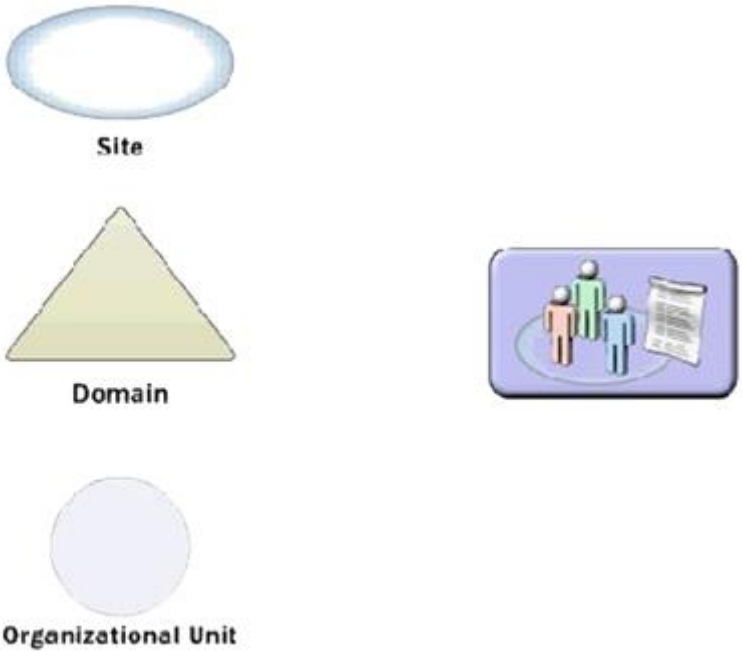
با استفاده از این گزینه می‌توانیم برنامه‌های مورد نظر را Install, Uninstall و یا پشتیبانی نماییم. با استفاده از Scripts، می‌توانید Scriptهایی را اختصاص دهید که به طور اتوماتیک در زمان خاموش و روشن شدن دستگاه و یا زمانی خاص اجرا شود. می‌توانید Scriptهای خود را به زبان‌های برنامه نویسی مختلفی که درون ویندوز پشتیبانی می‌شود مانند VB script یا Java script بنویسید.

Remote Installation Service:

این امکان را به شما می‌دهد که تنظیمات مربوط به نصب سیستم عامل را برای کاربران انجام دهید.

با استفاده از Internet Explorer Maintenance می‌توانید تنظیمات مربوط به نرم‌افزار IE و نحوه اجرای آن برای کاربران را مشخص نماید. از جمله این تنظیمات می‌توان از تنظیمات Proxy، اتصالات اینترنت و تنظیمات Security مربوط به Explorer را نام برد و در نهایت برای مدیریت اطلاعات مهم مانند محتویات Desktop وMy Document و سایر Folderهای مهم می‌توانید از گزینه‌ی Folder Redirection استفاده کرده و این Folderها را به یک محل خاص درون شبکه انتقال دهید و کاربران در تمامی حالات به آن دسترسی داشته باشند.

در ویندوز سرور، این امکان وجود دارد که Group Policy خود را به گروه هایی مهم همچون Site، Domain، Organizational Unit متصل و یا اصطلاحا لینک کنید. GPO (Group Policy Object) می‌تواند به بیش از یک قسمت لینک و یا اعمال شود. همچنین هر یک از این گروه‌ها می‌تواند به بیش از یک GPO متصل گردد. GPO بر اساس اولویتی که ماهیت‌ها و عناصر درون ساختار AD فعال می‌شوند، فعال می‌شود. به صورت پیش فرض GPO ابتدا بر روی Site، سپس Domain و در نهایت OU فعال می‌گردد. یعنی اگر روی OU سیاستی فعال کنید، سپس روی Domainی که OU عضو آن است، سیاستی متضاد با سیاست OU فعال کنید، **اولویت سیاست OU بیشتر بوده** و آن سیاست اعمال می‌شود، البته به شرطی که از سیاست اعمال شده Domain تجاوز نکند. مثلاً به Domain مقدار GB 1 فضا بدهیم، اما OU بخواهد از GB 2 فضا استفاده کند!



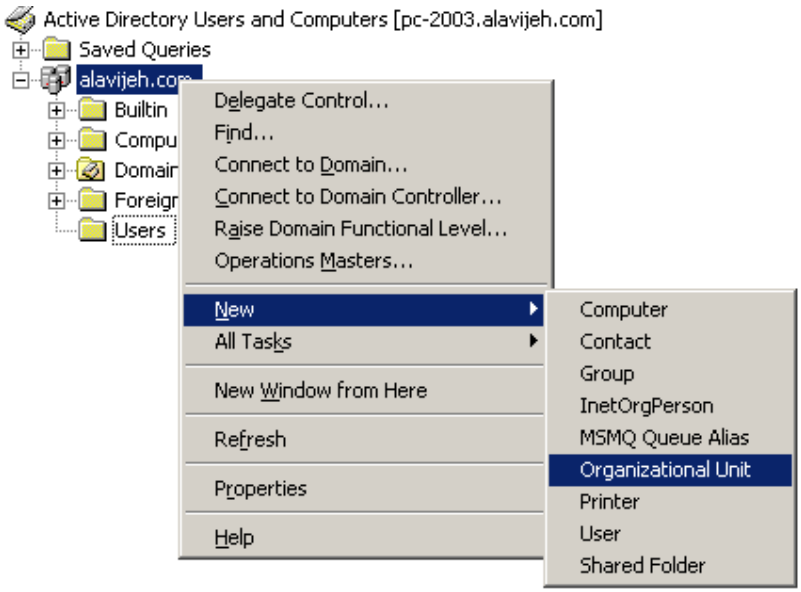
امروزه با توجه به گسترش و افزایش تعداد کاربران و کامپیوترها در شبکه، یک مدیر تنظیمات لازم را برای یک فرد یا یک کامپیوتر انجام نمی‌دهد، بلکه مدیر شبکه ابتدا گروه هایی ساخته و کاربرانی را عضو این گروه‌ها می‌کند و در این حالت می‌تواند سیاست‌ها و تنظیمات را روی این گروه‌ها اعمال کند. در این مقاله بر اساس امکانی که در ویندوز سرور ۲۰۰۳ وجود دارد، قصد داریم یک Organization Unit بسازیم (OU یا واحد سازمانی را مانند ظرفی در نظر بگیرید که هر چیزی می‌تواند در آن قرار گیرد، مانند کاربر، کامپیوتر، چاپگر و....) و تنظیمات را روی آن اعمال نماییم. پس ابتدا روش ساخت یک Organization Unit را شرح می‌دهیم.

۳۰-۳- ایجاد Organization Unit

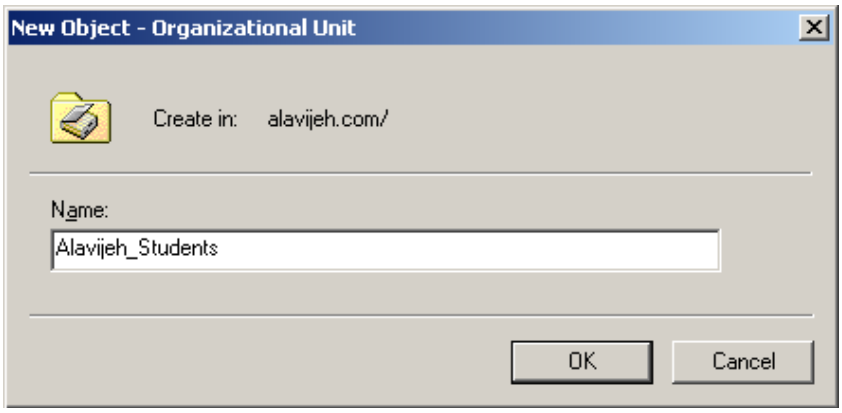
قبل از اینکه بخواهید Policy هایی را برای کاربران تعیین و اعمال نمایید و به منظور صرفه جویی در زمان یک Organization Unit ایجاد نمایید و کاربران مورد نظر را به عضویت آن در آورید تا نیاز نباشد برای هر کاربر جداگانه Group Policy تعریف و تنظیم شود. برای ساخت Organization Unit مراحل زیر را انجام دهید:

در قسمت Start بر روی Administrative Tools کلیک و سپس گزینه Active Directory Users and Computers را انتخاب نمائید.

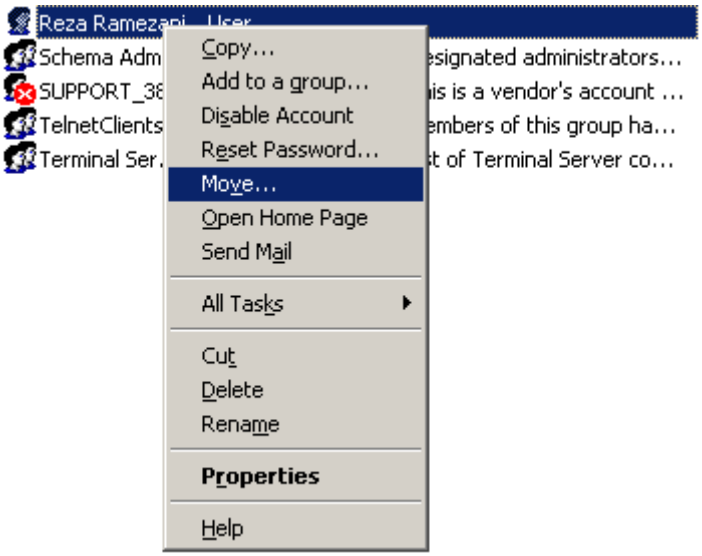
مطابق شکل زیر، روی نام سرور راست کلیک کرده و از منوی New گزینه Organization Unite را انتخاب نمایید.



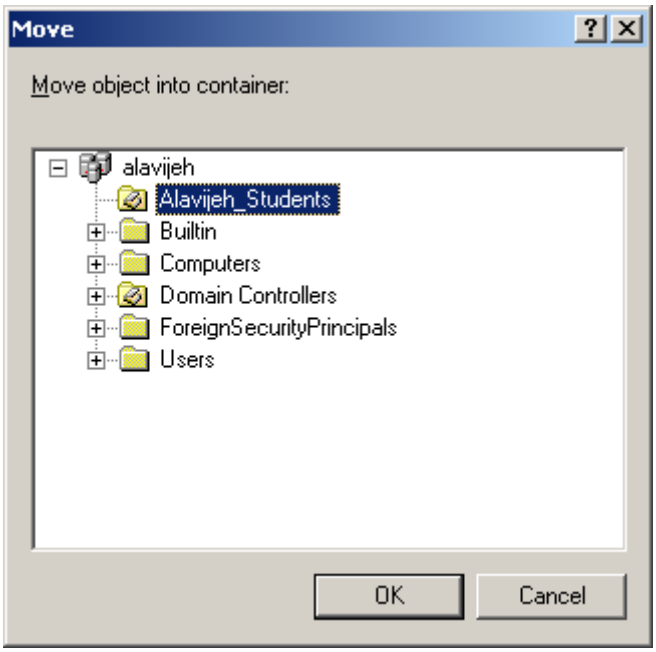
سپس یک نام برای واحد سازمانی خود (مثلاً Alavijeh_Students) وارد نمایید.



در ویندوز سرور ۲۰۰۳، هر کاربری که جدید ساخته شود به صورت پیش فرض در گروه Users قرار می‌گیرد پس برای اینکه بتوانید User یا Group ایجاد شده را عضو OU جدید کنید، آن را توسط موس داخل OU ساخته شده (در این مثال Alavijeh_Students) بیندازید. برای انتقال کاربر، روی آن راست کلیک کرده، گزینه Move را انتخاب کرده، مقصد را انتخاب نموده تا کاربر به آن انتقال یابد. در صورتیکه کاربری ایجاد نکردهاید بر روی Organization Unit ساخته شده راست کلیک کرده و از آنجا یک کاربر جدید بسازید تا از همان ابتدا عضو آن واحد سازمانی قرار گیرد.



انتخاب مقصد کاربر:



اکنون Organization Unit ساخته شده و اعضای آن نیز مشخص می‌باشند حال باید برای آن‌ها Group Policy تعریف گردد. برای درک مفهوم Group Policy و آشنایی عملی با آن، چند مثال را بطور عملی توضیح می‌دهیم.

۳۰-۴- مثال‌های عملی از Group Policy

در ادامه مثال هایی را در مورد چگونگی کار با Group Policy معرفی می‌نماییم.

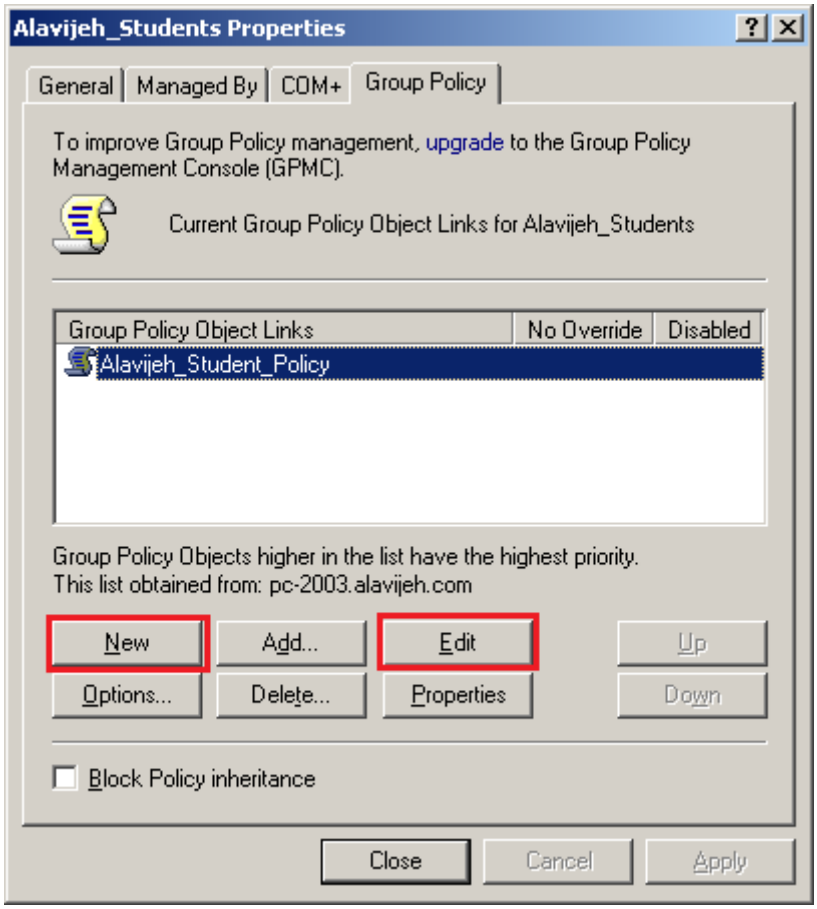
۳۰-۴-۱- تنظیم Proxy برای کاربران به صورت گروهی

فرض کنید در شبکه محلی (LAN) اداره یا سازمان متبوع خود، اینترنت راه اندازی کرده‌اید و می‌خواهید فقط برای گروهی از کاربران و با استفاده از قابلیت Group Policy پروکسی (Proxy) تنظیم نمایید. اگر شبکه شما دارای یک Domain Controller (DC) باشد و همچنین Active Directory راه اندازی کرده‌اید، از این پس نیازی نیست برای تک تک کاربران پروکسی تنظیم کنید. بلکه مراحل زیر را طی کنید:

روی Organization Unit ساخته شده راست کلیک و گزینه Properties را انتخاب نمایید

در صفحه ظاهر شده (در این مثال Alavijeh_Students Properties) به قسمت Group Policy بروید.

در این قسمت و مطابق شکل زیر دکمه New را بزنید و یک نام (مانند Alavijeh_Student_Policy) برای آن تعیین کنید.

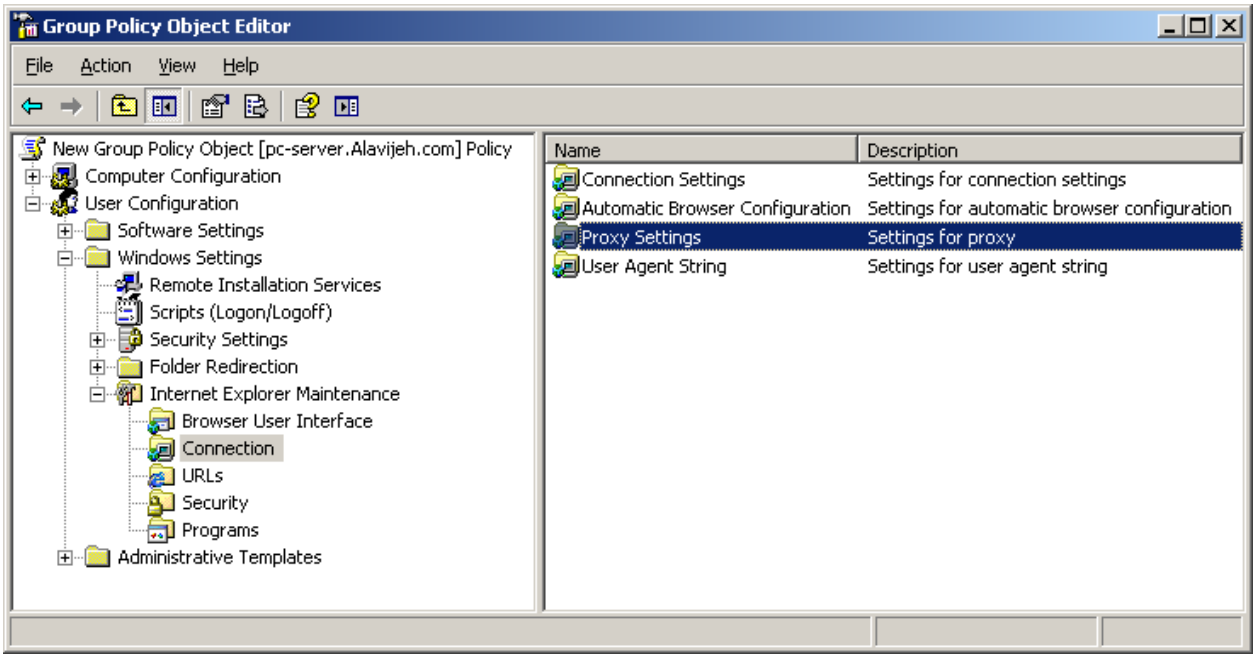


اکنون وقت تنظیم پروکسی می‌باشد. برای این منظور مراحل را به ترتیب زیر ادامه دهید:

در همان صفحه (مطابق شکل فوق)، Policy تعریف شده را انتخاب و گزینه Edit را بزنید

در صفحه Group Policy Object Editor به مسیر زیر بروید.

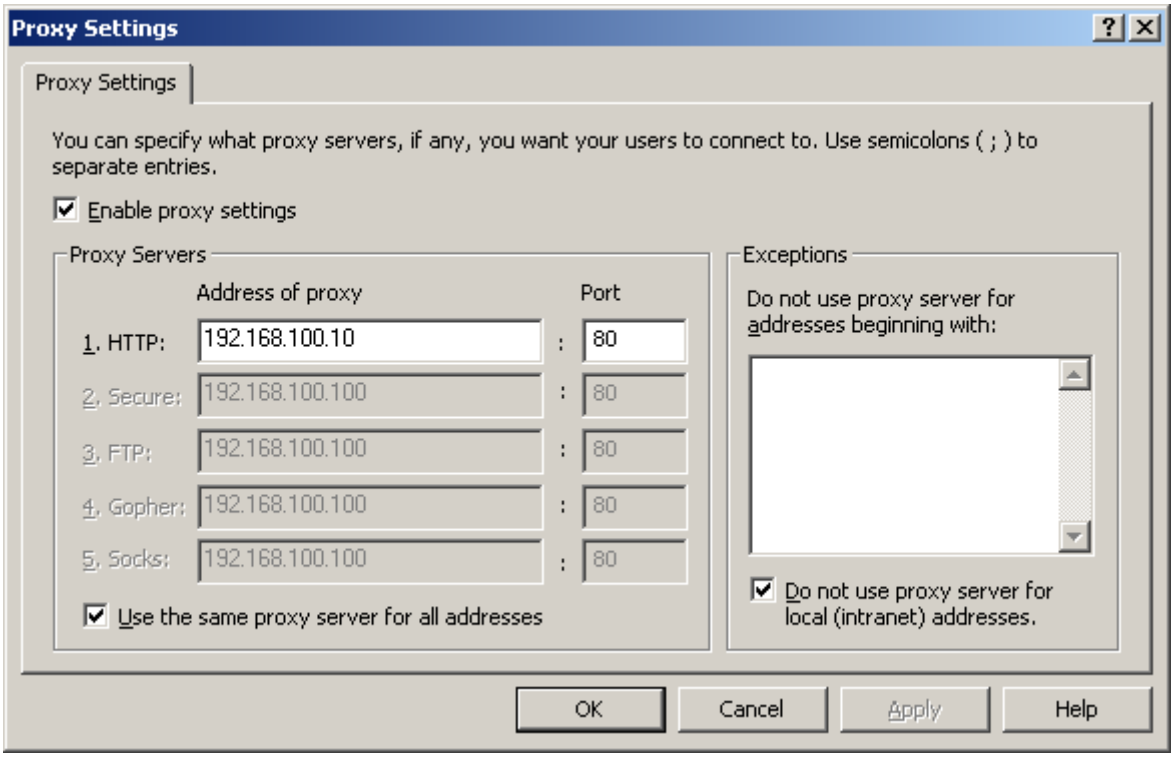
User Configuration➔Windows Settings➔Internet Explorer Maintenance➔Connection



در صفحه سمت راست گزینه Proxy Setting را انتخاب نمائید.

در صفحه Proxy Setting ابتدا تیک Enable Proxy Setting را بزنید (به شکل زیر توجه کنید)

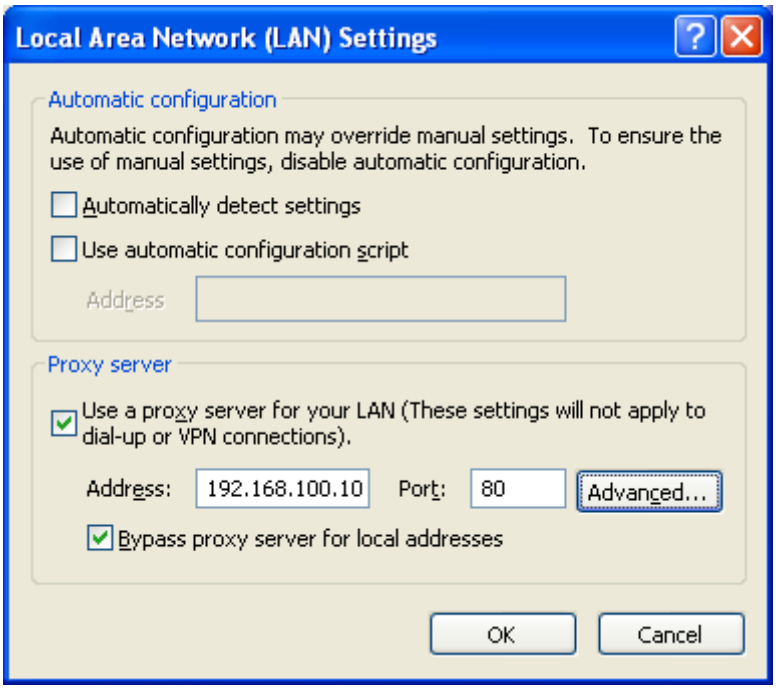
سپس مطابق شکل زیر، در قسمت HTTP آدرسی که قرار است کاربران به آن متصل شوند و اینترنت را از آنجا دریافت کنند را وارد کنید.



همانطور که در شکل زیر ملاحظه می‌کنید، از این پس، کاربرانی که با نام کاربری و رمز عبوری که در Domain موجود باشد به شبکه Login کنند و عضو Organization Unit ساخته شده توسط شما نیز باشند، به صورت اتوماتیک در Internet Explorer خود در قسمت Proxy Server آدرس ۱۹۲.۱۶۸.۱۰۰.۱۰ با پورت ۸۰ وارد شده است.

Tools➔Internet Options ➔ Connection ➔ LAN Setting ➔ Proxy Server

این همان آدرسی است که در قسمت قبل (به شکل فوق توجه کنید) تنظیم شده است.



۳۰-۴-۲- تغییر Title Bar اینترنت اکسپلورر

شاید بخواهید در صفحه Internet Explorer تمام کاربرانی که در شبکه محلی از اینترنت استفاده می‌کنند، نام سازمان یا اداره متبوع خود را در Title Bar بنویسید، به طوریکه هر کاربری که به شبکه با نام کاربری و رمز عبور معتبر در Domain وارد می‌شود و Internet Explorer را باز می‌کند نام سازمان را در بالای صفحه آن ببیند. برای تنظیم این مورد مراحل زیر را انجام دهید:

روی Organization Unit ساخته شده کلیک راست نمایید و گزینه Properties را بزنید.

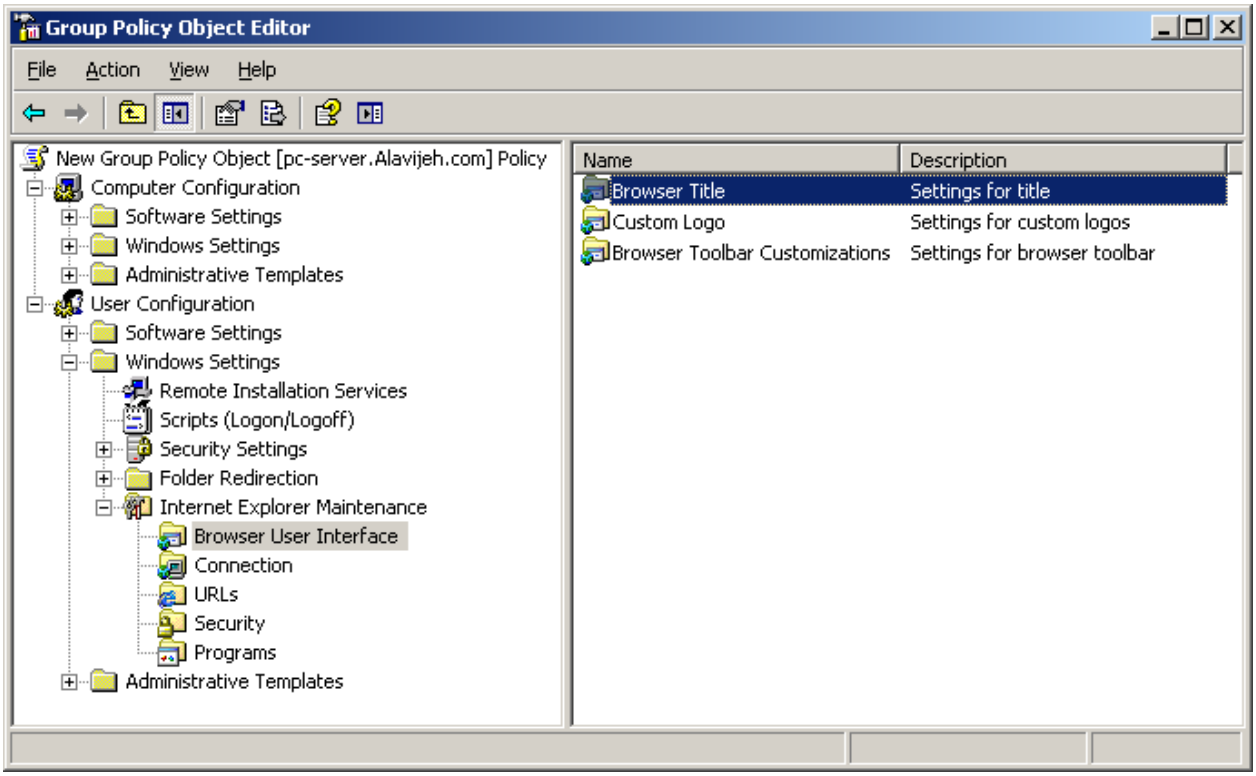
در صفحه ظاهر شده به قسمت Group Policy بروید.

Group Policyای که در قسمت قبل ایجاد شد را انتخاب و مجدد دکمه Edit را بزنید.

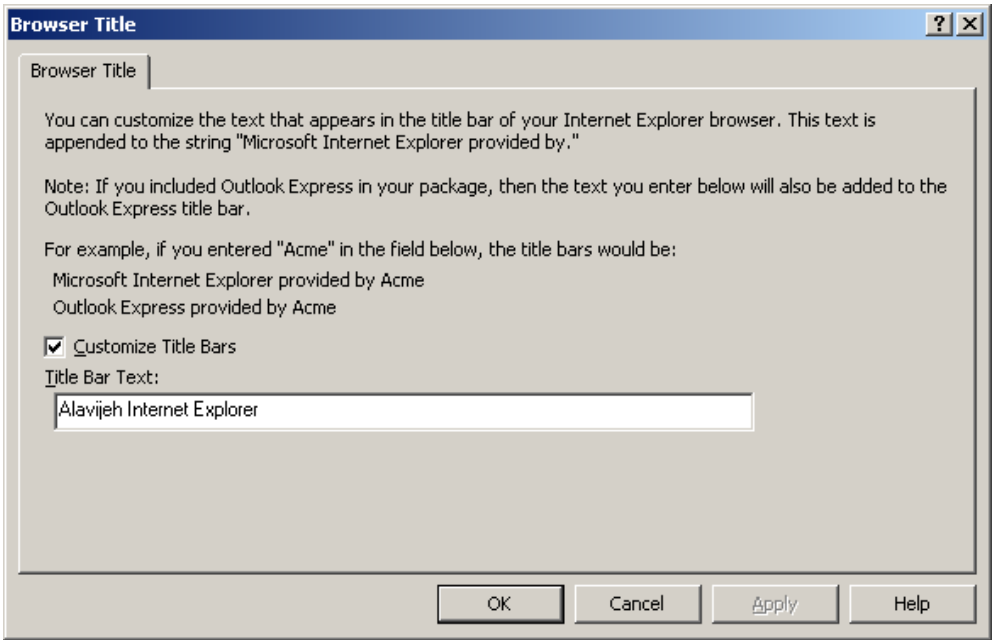
در صفحه Group Policy Object Editor به مسیر زیر بروید:

User Configuration➔Window Setting➔Internet Explorer Maintenance➔Brower User Interface

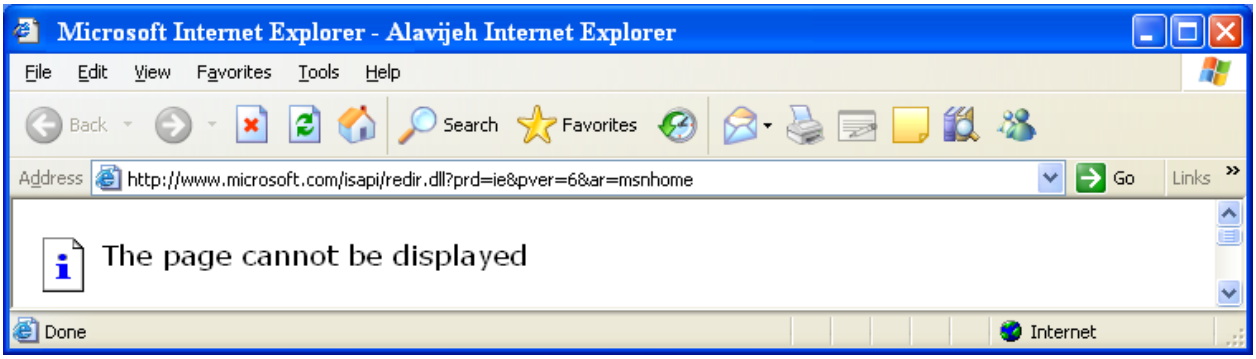
از صفحه سمت راست گزینه Browser Title را انتخاب کنید.



مطابق شکل زیر، ابتدا تیک مربوط به Customize Title Bars را زده و متن دلخواه خود را داخل Title Bar Text بنویسید.



برای دیدن نتیجه لازم است با Username و Password کاربری که عضو گروه ساخته شده است، به شبکه Login کنید تا نتیجه را مانند آنچه در شکل زیر آمده است، ملاحظه نمایید.



۳۰-۴-۳- تنظیمات نوار وظیفه و منوی شروع (Start Menu and Taskbar)

ویندوز کلیه تنظیمات مربوط به منوی شروع (Start Menu) و نوار وظیفه (Task bar) را در محل مشخصی از Group Policy قرار داده است که می‌توانید همه چیز در این دو مورد را در همان قسمت تنظیم نمایید.

به عنوان مثال شاید لازم باشد در شبکه محلی شما بنابر طراحی انجام شده، دکمه RUN روی منوی شروع کاربران نباشد یا نتوانند از شبکه خارج شوند، یعنی بخواهید به صورت مرکزی دکمه Log Off را از منوی شروع کلیه کاربران عضو یک گروه بردارید.

برای تنظیم کردن این موارد و براساس نیازتان مراحل زیر را انجام دهید:

روی Organization Unit ساخته شده راست کلیک کنید سپس دکمه Properties را بزنید

Group Policy ساخته شده را انتخاب و گزینه Edit را بزنید.

در صفحه Group Policy Object Editor به مسیر زیر بروید:

User Configuration➔Administrative Templates➔Start Menu Tools Bar

در پنجره‌ای که در سمت راست ظاهر می‌شود تنظیماتی مانند آنچه در زیر اشاره می‌شود را می‌توانید انجام دهید:

۱. حذف یا اضافه کردن دکمه RUN
۲. حذف یا اضافه کردن نام کاربری
۳. حذف یا اضافه کردن دکمه Log Off
۴. حذف یا اضافه کردن Shutdown و بسیاری تنظیمات دیگر.

در شکل زیر، نمونه‌های مختلف را مشاهده می‌نمایید:

Remove user's folders from the Start Menu	Not configured
Remove links and access to Windows Update	Not configured
Remove common program groups from Start Menu	Not configured
Remove My Documents icon from Start Menu	Not configured
Remove Documents menu from Start Menu	Not configured
Remove programs on Settings menu	Not configured
Remove Network Connections from Start Menu	Not configured
Remove Favorites menu from Start Menu	Not configured
Remove Search menu from Start Menu	Not configured
Remove Help menu from Start Menu	Not configured
Remove Run menu from Start Menu	Not configured
Remove My Pictures icon from Start Menu	Not configured
Remove My Music icon from Start Menu	Not configured
Remove My Network Places icon from Start Menu	Not configured
Add Logoff to the Start Menu	Not configured
Remove Logoff on the Start Menu	Not configured

Remove and prevent access to the Shut Down command	Not configured
Remove Drag-and-drop context menus on the Start Menu	Not configured
Prevent changes to Taskbar and Start Menu Settings	Not configured
Remove access to the context menus for the taskbar	Not configured
Do not keep history of recently opened documents	Not configured
Clear history of recently opened documents on exit	Not configured
Turn off personalized menus	Not configured
Turn off user tracking	Not configured
Add "Run in Separate Memory Space" check box to Run dialog box	Not configured
Do not use the search-based method when resolving shell shortcuts	Not configured
Do not use the tracking-based method when resolving shell short...	Not configured
Gray unavailable Windows Installer programs Start Menu shortcuts	Not configured
Prevent grouping of taskbar items	Not configured
Turn off notification area cleanup	Not configured
Lock the Taskbar	Not configured
Force classic Start Menu	Not configured

هر آیتمی در بخش Administrative Templates، سه حالت دارد:

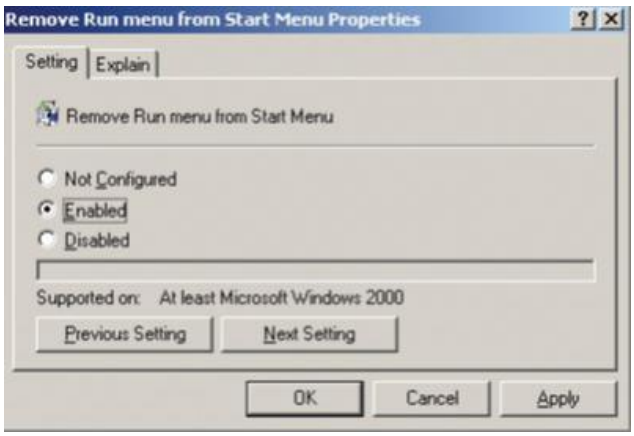
۱. **Not Configured:** به معنای آنکه تغییر به Registry اعمال نشده است.

۲. **Enabled:** به معنای آنکه سیاست اثر گذار است و Registry تغییر یافته است.

۳. **Disabled:** به معنای آنکه تغییر یافته و سیاست اثرگذار نیست.

اما به عنوان مثال برای حذف دکمه RUN در همان پنجره روی گزینه Remove Run Menu From Start Menu دو بار کلیک کنید تا پنجره‌ای مطابق شکل زیر مشاهده شود.

در این پنجره اگر گزینه Enable را انتخاب کنید، دکمه Run برای کلیه کاربرانی که به شبکه وارد می‌شوند حذف می‌شود و یا برای اینکه دکمه Shut Down را از روی منوی شروع بر داریم، در همین قسمت گزینه Remove and Prevent Access to the Shutdown را فعال می‌کنیم.



۳۰-۴-۴- تنظیمات و حذف و اضافه گزینه‌های مربوط به Control Panel

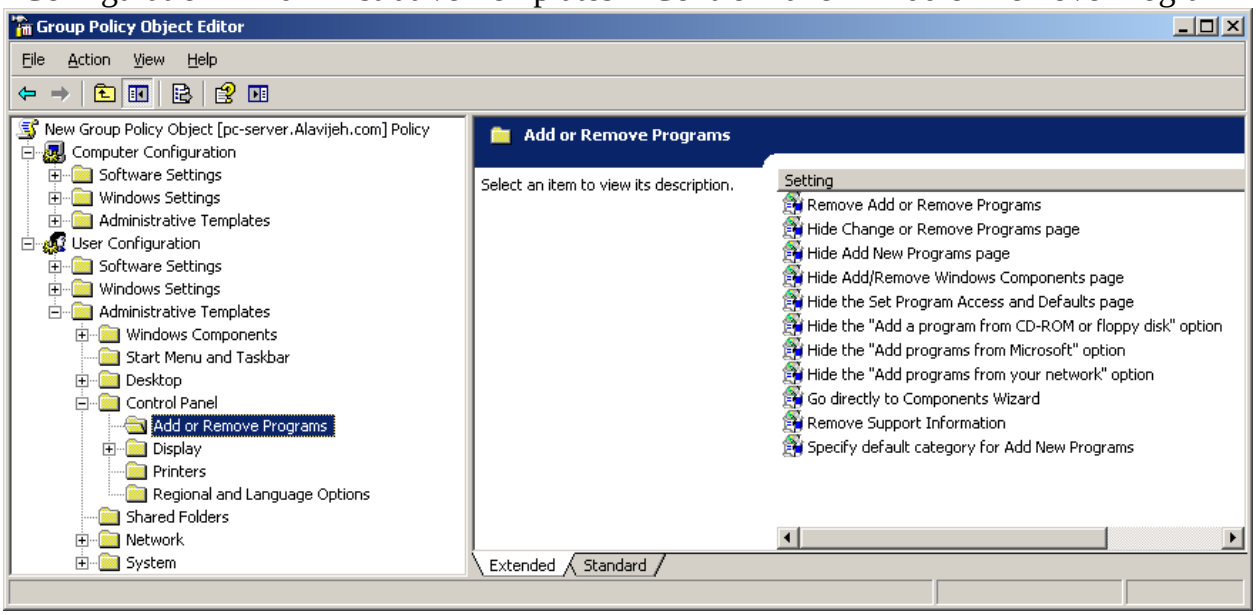
با توجه به تکرار مراحل قبلی که چندین بار به آن اشاره شد یعنی با Edit کردن Group Policy ساخته شده و در صفحه Group Policy Object Editor از طریق مسیر زیر می‌توان کلیه تنظیمات و محدودیت‌های مربوط به کنترل پانل را برای کاربران انجام داد.

User Configuration➔Administrative Templates➔Control Panel

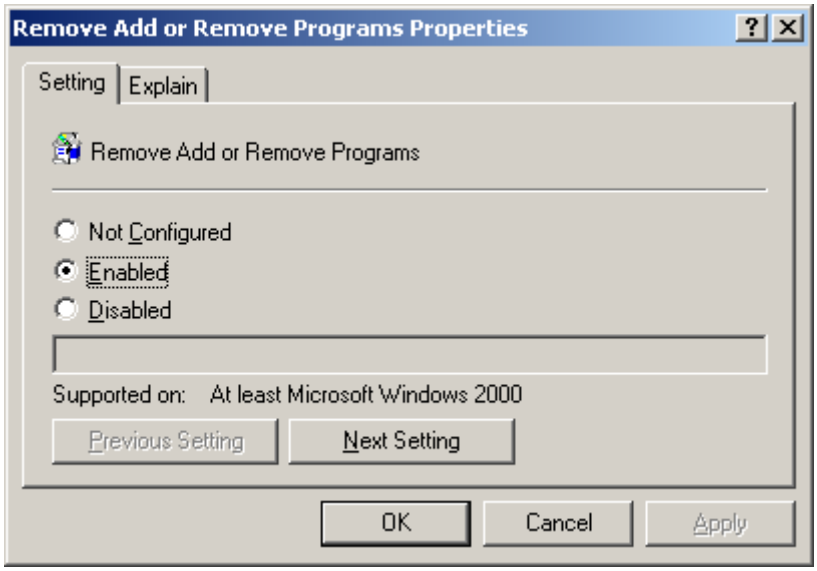
به عنوان مثال اگر بخواهید دکمه Add \ Remove Program از داخل کنترل پانل سیستم‌های موجود در شبکه حذف نمایید مراحل زیر را انجام دهید:

ابتدا به مسیر زیر بروید:

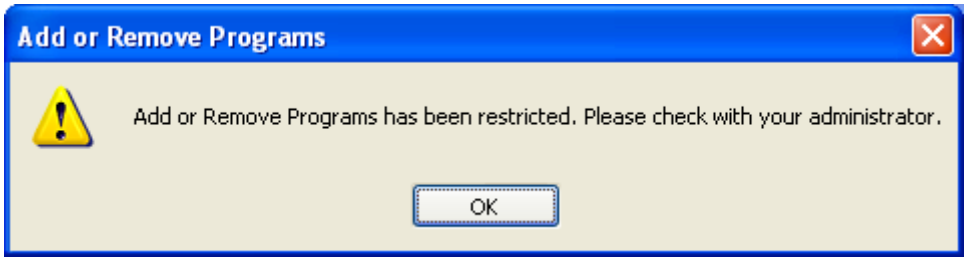
User Configuration➔Administrative Templates➔Control Panel➔Add or Remove Program



سپس از صفحه سمت راست، همانطور که در شکل زیر مشاهده می‌کنید، گزینه Remove Add or Remove Program را با دوبار کلیک انتخاب کنید و سپس در پنجره‌ای که باز می‌شود گزینه Enable را بزنید.



بعد از این تنظیم اگر کاربری که جزء گروه ایجاد شده (در این مثال Alavijeh_Students) باشد وارد Control Panel سیستم خود شود، با توجه Policy که در این مثال تعریف شده نمی‌تواند گزینه Add or Remove Program را اجرا نماید و در صورت اجرای آن، با پیغامی که در شکل زیر مشاهده می‌کنید مواجه می‌گردد.



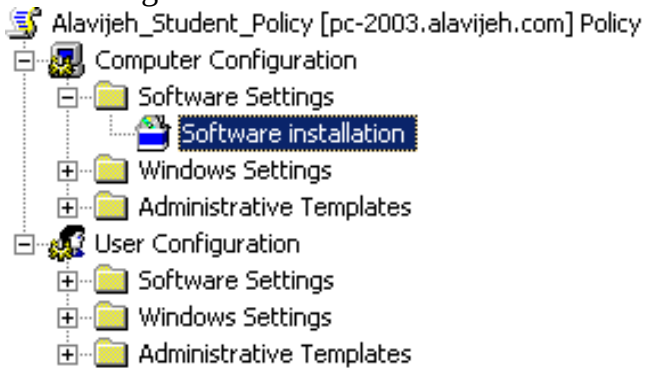
۳۰-۴-۵- نصب برنامه‌های کاربردی

می خواهیم برنامه‌ای را تعیین کنیم که تمامی کاربران بتوانند در شبکه نصب کنند. معمولاً آنچه که می‌خواهیم روی کامپیوترهای کلاینت نصب کنیم سه دسته می‌شوند:

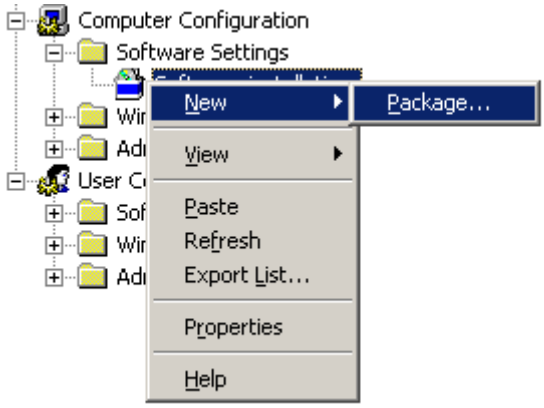
۱. فایل‌های MSU که مربوط به روز رسانی‌های ویندوز می‌باشند. آن‌ها را با WSUS منتشر می‌کنیم و در اینجا بررسی نمی‌شوند.
۲. فایل‌های MSI که با کمترین زحمتی قابل نصب روی تمام کلاینت‌های مورد نظر هستند و در اینجا روی این فایل‌ها تمرکز می‌کنیم.
۳. فایل‌های غیر از MSI مانند EXE که می‌خواهیم روی تمام کلاینت‌های مورد نظر نصب شوند و قدری کار بیشتر نیاز است.

بدین منظور مجددا مانند قبل وارد صفحه Edit ➔ Group Policy واحد سازمانی یا Domain ساخته شده شوید. سپس وارد مسیر زیر شوید:

User | Computer ➔ Software Settings ➔ Software Installation



سپس روی Software installation راست کلیک کرده و از قسمت New گزینه Package را انتخاب نمایید.

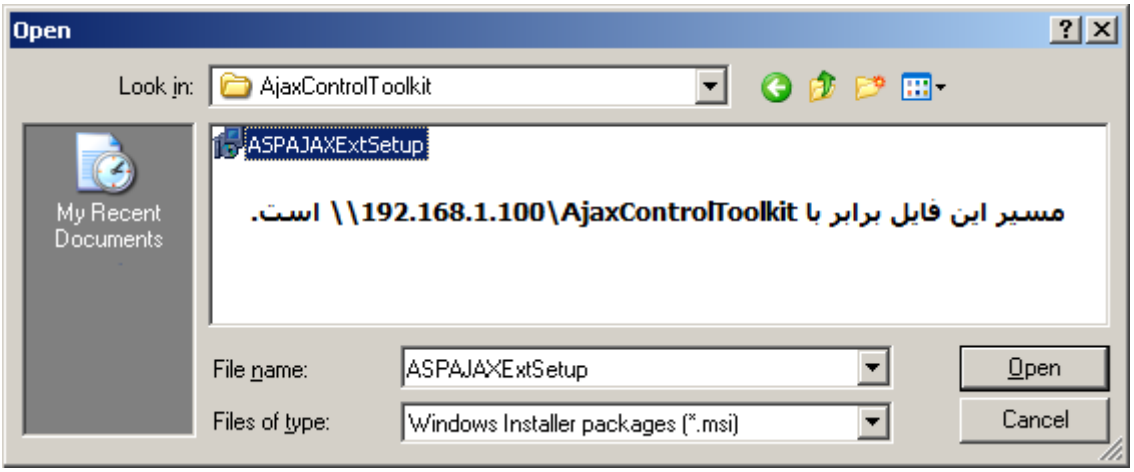


بر حسب آنکه نوع فایل MSI است یا نه، در اینجا باید مراحل مختلفی را انجام دهیم. اگر MSI باشد، فایل را انتخاب می‌کنیم و مراحل ساخت Package را ادامه می‌دهیم. اما اگر نوع فایل ZAP باشد، باید ابتدا یک ZAP فایل بسازیم که در ادامه توضیح می‌دهیم.

مهم: در هنگام انتخاب مسیر فایل Installation و ZAP فایل، **فراموش نکنید و تاکید می‌کنم فراموش نکنید** که مسیر فایل را در شبکه وارد کنید. مثلاً از طریق My Network Places مسیر را وارد کنید یا مثلاً:

\\Server1\office\word.msi

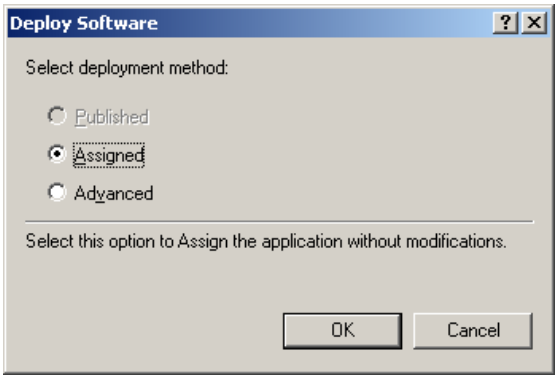
بنابراین بدیهی است که باید فایل‌ها Share باشند. البته اگر فراموش کنید، ویندوز با پیام هشداری به شما یادآوری می‌کند.



پس از ساخت Package سه گزینه در دسترس داریم:

- **Published:** اگر یک Package به صورت Published تنظیم شود، اولین باری که کاربر Login کند Add/Remove Program برای او نمایش داده خواهد شد و کاربر می‌توان**د انتخاب کند که برنامه نصب شود یا خیر.**
- **Assigned:** اگر یک Package به صورت Assigned به کاربری تنظیم شود، اولین باری که کاربر Login کند برنامه نصب می‌شود و پیش از اولین بار اجرا، نهایی می‌شود. اگر یک Package به صورت Assigned به کامپیوتری تنظیم شود، اولین باری که ویندوز Start می‌شود، Package نصب می‌شود و پیش از اولین اجرا نهایی می‌شود. برای تمام کاربران آن کامپیوتر نرم‌افزار قابل دسترسی خواهد بود.
- بدیهی است از آنجا که کامپیوترها نمی‌توانند تصمیم بگیرند که آیا یک Package نصب شود یا خیر، گزینه Published برای کامپیوترها غیر فعال است.
- فایل‌های ZAP فقط می‌توانند برای کاربران یعنی در قسمت User Configuration تنظیم شوند. چرا که فایل‌های ZAP از برنامه نصب کننده اختصاصی خود استفاده می‌کنند و نمی‌توانند از Elevated Privileges استفاده کنند. بنابراین در هنگام نصب اگر Administrative Permission نیاز باشد، تنها کاربرانی که دارای این مجوز هستند می‌توانند این فایل را نصب کنند. بنابراین باید Published شوند تا کاربری مراحل نصب را انجام دهد.
- **Advanced:** تنظیمات اضافی را در اختیار قرار می‌دهد. بسیاری از نکات از جمله Advanced را فعلا صرف نظر می‌کنیم.

توجه: به نسخه‌های ۳۲ بیتی و ۶۴ بیتی توجه کنید.



(در این مثال، ما Package را روی Computer نصب کردیم، لذا گزینه Published غیر فعال است.)

ساختن یک ZAP فایل: Zap فایل، یک فایل متنی است و بنابر این می‌تواند به راحتی با Notepad و یا هر ویرایشگر متن دیگری نوشته شود. در اینجا یک مثال برای ساخت Zap فایل ارائه می‌دهیم.

مثال: به آسانی کد زیر را در NotePad نوشته و تغییرات لازم را انجام دهید و سپس آن را با پسوند Zap ذخیره کنید. در این مثال Excel 2007 را نصب می‌کنیم. دقت کنید که فایل را با پسوند Zap.txt به اشتباه ذخیره نکنید.

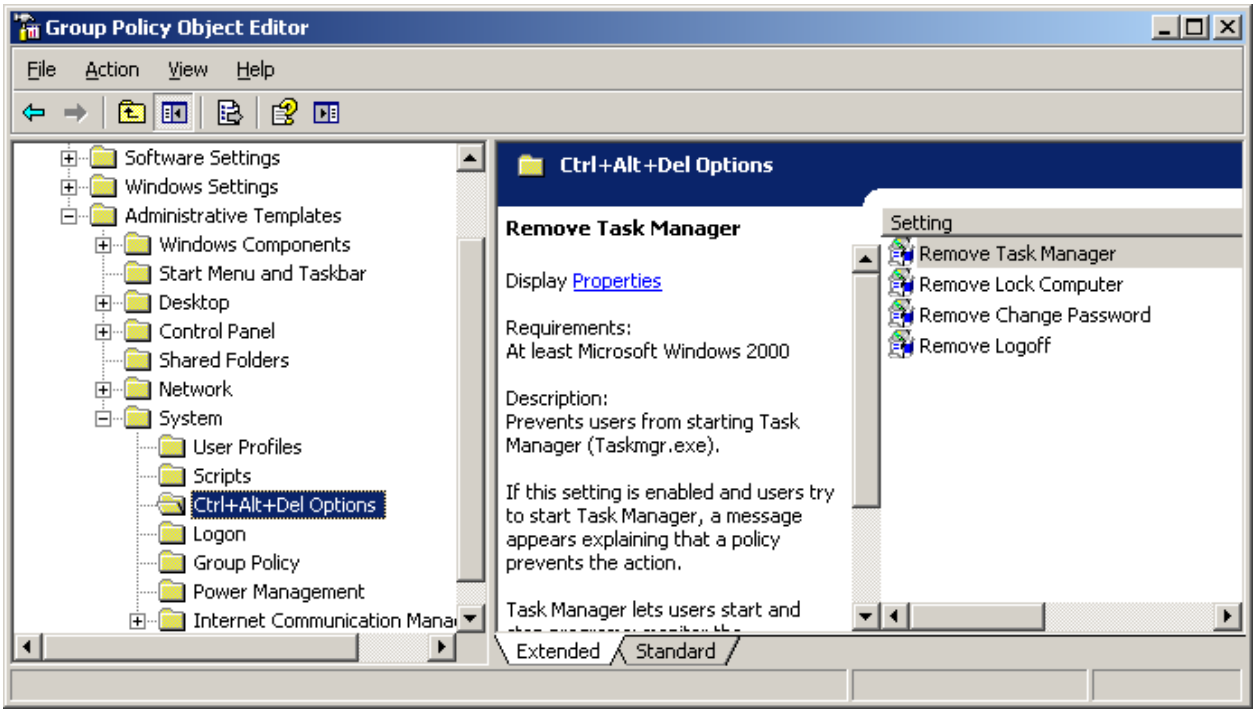
```
[Application]
FriendlyName = “Microsoft Excel 2007”
SetupCommand=“\\server5\share\Excel 2007\setup.exe”
```

۳۰-۴-۶- غیر فعال نمودن Ctrl + Alt + Delete

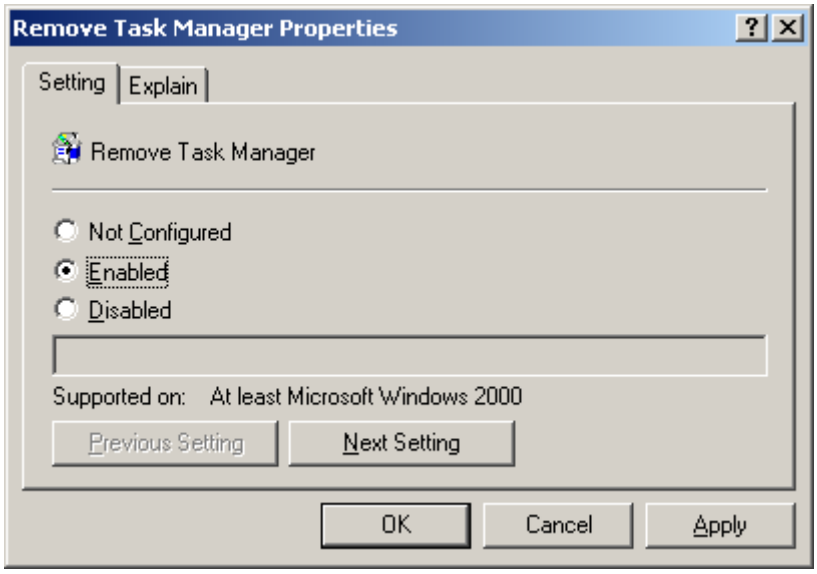
در بسیاری از موارد، نیاز داریم که امکان Ctrl + Alt + Delete را از کاربر بگیریم. بدین منظور ابتدا وارد Group Policy Object Editor شده و سپس به مسیر زیر بروید:

User Configuration ➔ Administrative Templates ➔ System ➔ Ctrl + Alt + Delete Options

سپس از صفحه سمت راست، گزینه Remove Task Manager را انتخاب کنید.



سپس در صفحه باز شده، گزینه Enabled را انتخاب نموده و سپس OK کنید.



بدین ترتیب کاربرانی که این سیاست روی آن‌ها اعمال می‌شود، هنگام فشردن کلیدهای Ctrl + Alt + Delete قسمت Task Manager آن‌ها غیر فعال خواهد بود.



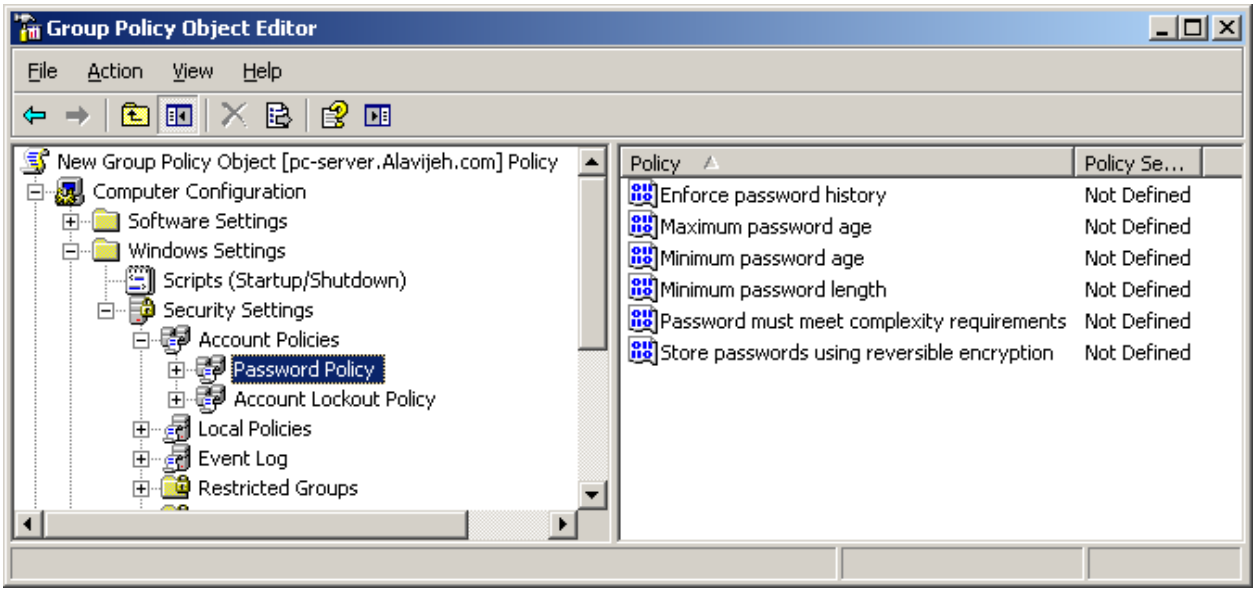
۳۰-۴-۷- امنیت رمز عبور کاربران

به عنوان آخرین مبحث آموزشی Group Policy، به بحث سیستم‌های امنیتی رمز عبور در Group Policy می‌پردازیم.

بدین منظور ابتدا وارد Group Policy Object Editor شده و سپس به مسیر زیر بروید:

Computer Configuration➔Windows Settings➔Account Policies➔Password Policy

در سمت راست صفحه، تعدادی از سیاست‌ها را مشاهده می‌کنید که در ادامه به توضیح آن خواهیم پرداخت:



– **Enforce Password History:** توسط این قسمت می‌توان به سیستم گفت که رمزهای عبور کاربر را (حتی رمزهای قبلی کاربر که اکنون تغییر یافته است) همیشه نگهداری کند، حال هنگام تغییر رمز عبور کاربر، سیستم به وی اجازه نمی‌دهد که از n رمز عبور قبلی خود استفاده کند. در مثال زیر ما تعیین کرده‌ایم که کاربر نتواند رمزی مانند ۳ رمز قبلی خود وارد کند.



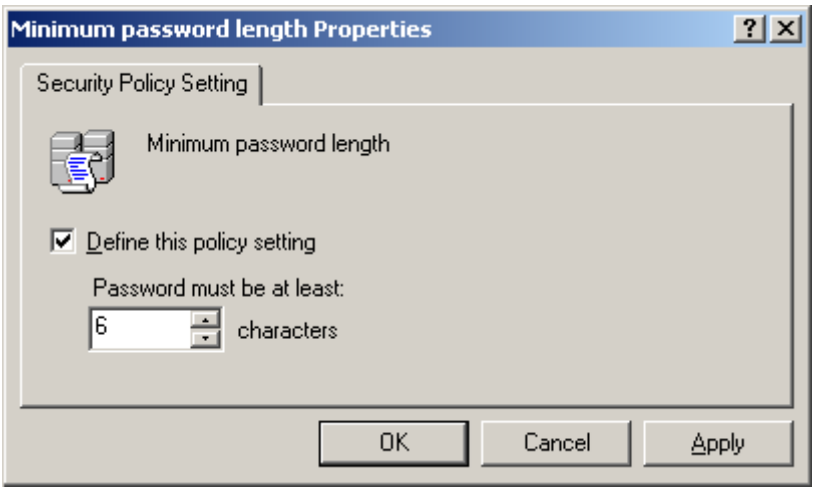
– **Maximum Password Age:** در این قسمت حداکثر طول عمر یک رمز عبور تعیین می‌شود و بعد از آن، رمز عبور Expire شده و کاربر بایستی رمز عبور خود را تغییر دهد. به طور پیش فرض این مقدار برابر با ۴۲ است. در اینجا ما مقدار را برابر ۳۰ در نظر گرفته‌ایم.



- **Minimum Password Age:** این قسمت حداقل طول عمر رمز عبور را تعیین می‌کند! یعنی اگر کاربری رمز عبور خود را تغییر دهد، تا n روز بعد، قادر به تغییر دادن رمز عبور خود نخواهد بود.



- **Minimum Password Length:** این قسمت، حداقل طول رمز عبور را تعیین می‌کند؛ مثلاً طول رمز عبور نمی‌تواند از ۶ حرف کمتر باشد.



- **Password Must Meet Complexity Requirements:** این قسمت تعیین می‌کند که نوع رمز عبور کاربر بایستی ساده یا پیچیده باشد. رمزی مانند ۱۲۳۴۵۶، یک رمز ساده و رمزی مانند abc@abc123، یک رمز پیچیده به حساب می‌آید. در این صفحه اگر گزینه Enabled را انتخاب کنید، سیستم کاربر را مجبور می‌کند که از رمزهای پیچیده استفاده کند. در ویندوز سرور ۲۰۰۳، این گزینه به صورت پیش فرض **غیر فعال** و در ویندوز سرور ۲۰۰۸، این گزینه به صورت پیش فرض **فعال** است.



Store Passwords Using Reversible Encryption – این قسمت تعیین می‌کند که سیستم رمزهای عبور را به گونه‌ای ذخیره کند که قابل بازیابی باشد. در ویندوز سرور رمزهای عبور به صورت کد شده ذخیره می‌شوند. اگر این گزینه را فعال کنید، سیستم رمزهای عبور را به گونه‌ای ذخیره می‌کند که با داشتن رمز عبور به مقدار کد شده آن و با داشتن مقدار کد شده، می‌توان به رمز عبور اصلی دسترسی داشت. اما اگر این گزینه غیرفعال کنید، فقط با داشتن رمز عبور می‌توان به مقدار کد شده آن دسترسی داشت؛ اما اگر مقدار کد شده را داشته باشیم، نمی‌توان به رمز عبور اصلی دسترسی یافت.



فصل ۳۱

کنترل از راه دور

۳۱-۱- مقدمه

تا قبل از به وجود آمدن شبکه‌های کامپیوتری، کاربران برای کارکردن با هر سیستمی، مجبور بودند که به صورت فیزیکی در محل حاضر شده و پشت سیستم مورد نظر بنشینند و با آن کار کنند. اما با به وجود آمدن شبکه‌های کامپیوتری، این محدودیت برطرف شد و کاربران این قابلیت را پیدا نمودند که از راه دور به یک سیستم متصل شده و با آن کار کنند؛ درست مانند اینکه به طور فیزیکی پشت آن سیستم نشسته‌اند. یکی از ابزارهایی که اجازه این کار را به ما می‌دهد، نرم‌افزار Remote Desktop Connection است. این نرم‌افزار به صورت رایگان به همراه ویندوز عرضه شده است. در ادامه این فصل به معرفی این نرم‌افزار می‌پردازیم. اما استفاده از Remote Desktop Connection یک محدودیت بزرگ دارد. و آن اینکه همزمان فقط یک کاربر می‌تواند با سیستم کار کند. بدین معنا که اگر کاربری با یک سیستم در حال کارکردن باشد و کاربری بخواهد از راه دور به سیستم متصل شود، کاربر جاری از سیستم خارج شده و Log out خواهد شد. مشکل دیگری که وجود دارد، مشکل عدم مدیریت کاربر متصل شده است. برای حل این مشکل، ویندوز سرور ابزار جدیدی به نام Terminal Server را معرفی نمود.

در بالا گفتیم که در ویندوز، برای اتصال به سیستم راه دور دو مشکل عمده وجود دارد: ۱- وجود همزمان فقط یک کاربر ۲- عدم مدیریت کاربران وارد شده. برای حل این مشکل، ویندوز سرور ابزار جدیدی به نام Terminal Server را معرفی نمود. بدین معنا که این ابزار این قابلیت را می‌دهد که در یک لحظه، تعداد نا محدودی کاربر به یک سیستم Login کنند. تمام این کاربران می‌توانند با یک نام کاربری یا با نام‌های کاربری متفاوت وارد سیستم شوند و هیچ کدام از کاربران نیاز به Log out به هنگام ورود کاربر جدید ندارند. همچنین تاثیرات تغییرات دیگر کاربران به سرعت نمایان می‌شود. یعنی فرض کنید دو کاربر با نام کاربری Reza وارد سیستم شده باشند؛ اگر هر دو در صفحه دسکتاپ باشند، اگر یکی از کاربران فایلی را روی صفحه دسکتاپ ایجاد کند، کاربر دوم به محض ایجاد فایل، آن را مشاهده نموده و قابلیت استفاده از آن را پیدا می‌کند.

به علاوه توسط Terminal Server این قابلیت وجود دارد که بتوان کاربرانی که به سرور Login کرده‌اند را مشاهده و آن‌ها را مدیریت نمود.

در ادامه، ابتدا به آموزش Remote Desktop Connection پرداخته و سپس به معرفی Terminal Server می‌پردازیم.

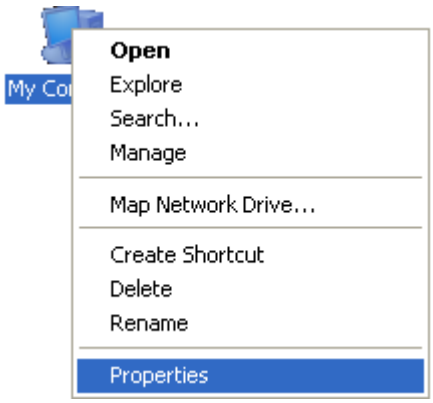
برای کنترل کردن سیستم‌ها از راه دور، ابزارهای دیگری نیز وجود دارد. یکی از آن‌ها Remote Assistance است. این ابزار بیشتر به عنوان ابزاری جهت حل مشکلات سیستم‌های راه دور شناسایی می‌شود که البته این کار به نیاز به کنترل کامپیوتر راه دور دارد. این ابزار و ابزارهای Remote Desktop و Terminal Server، محدودیت بزرگی دارند و آن اینکه برای اتصال به سیستم‌های موجود در شبکه اینترنت، کامپیوتر راه دور بایستی آدرس IP از نوع Valid داشته باشد؛ یعنی آدرسی که در کل دنیای اینترنت قابل شناسایی باشد. برای حل این مشکل نیز ابزار Team Viewer معرفی شد که البته ابزاری مستقل از محصولات مایکروسافت می‌باشد. البته این نرم‌افزار مشکل بزرگی نیز دارد و آن اینکه بر عکس سه نرم‌افزار فوق، قابلیت کار در یک شبکه محلی را ندارد.

در این فصل به آموزش این چهار ابزار خواهیم پرداخت.

Remote Desktop Connection -۲-۳۱

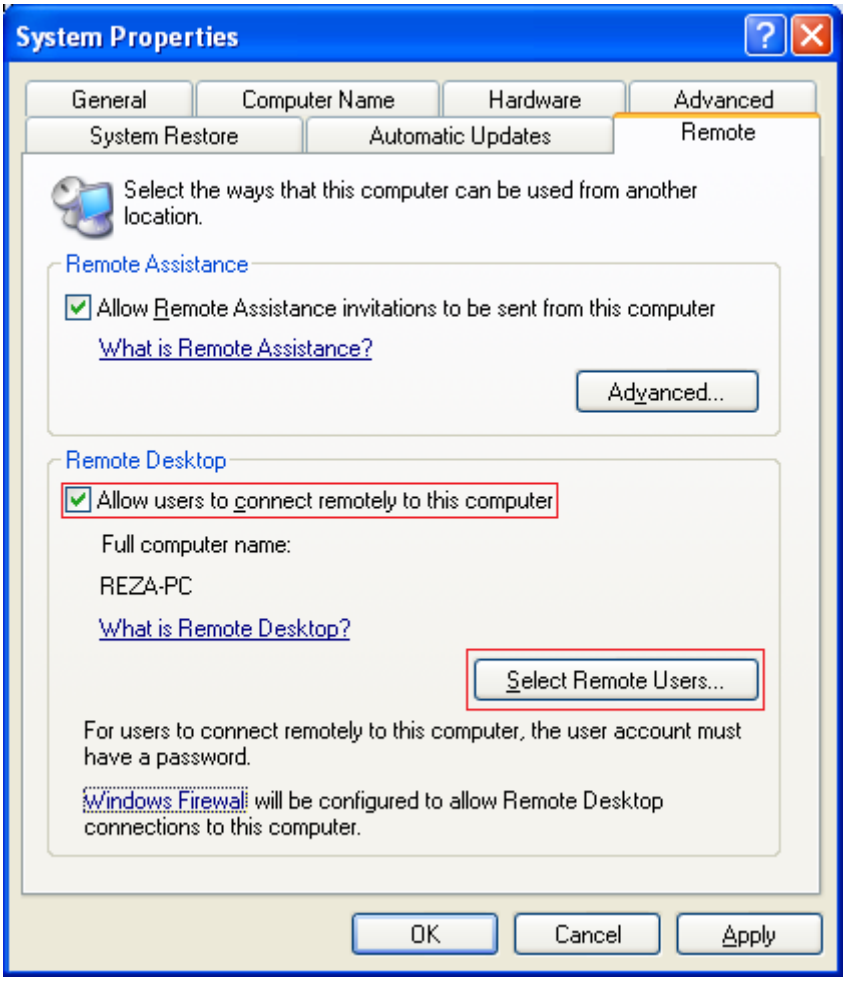
۳۱-۲-۱- آماده سازی کامپیوتر راه دور

فرض کنید که قصد دارید از راه دور به سیستمی متصل شوید که روی آن ویندوز XP نصب است. این سیستم می‌تواند در یک شبکه محلی باشد یا در شبکه اینترنت که البته اگر در دنیای اینترنت باشد، این سیستم بایستی آدرس IP از نوع Valid داشته باشد. در این صورت می‌توانید از Remote Desktop Connection استفاده نمایید (در مورد محدودیت‌های این روش در بالا صحبت کردیم). بدین منظور ابتدا بایستی تنظیماتی را در ویندوز XP انجام دهید. این تنظیمات را بایستی روی کامپیوتری انجام دهیم که می‌خواهیم از راه دور به آن متصل شویم. برای شروع، روی My Computer راست کلیک کرده و گزینه Properties را انتخاب نمایید.

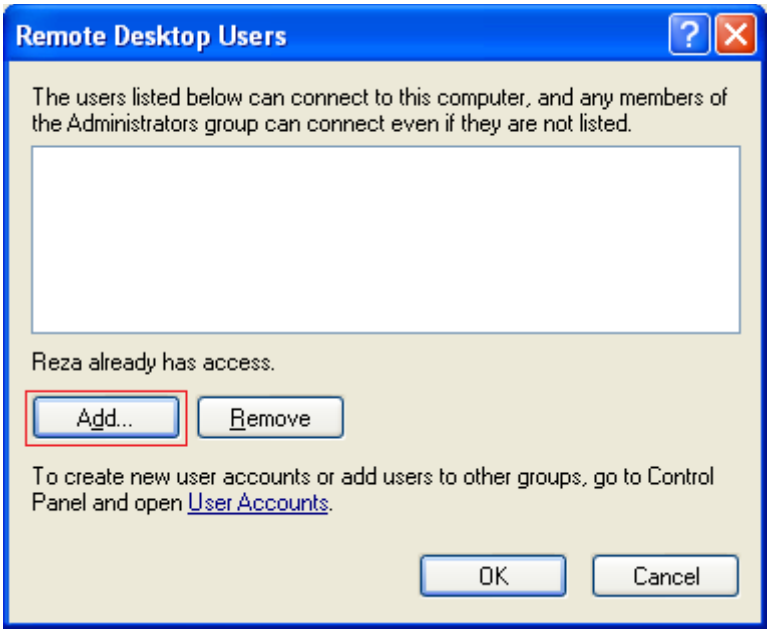


سپس در صفحه باز شده، وارد سربرگ Remote شوید. اولین کاری که باید انجام دهید، فعال کردن سرویس Remote Desktop Connection روی ویندوز است. بدین منظور، در قسمت Remote Desktop تیک گزینه Allow user to connect remotely to this computer را فعال کنید. سپس بایستی کاربرانی را مشخص کنید که اجازه Remote کردن

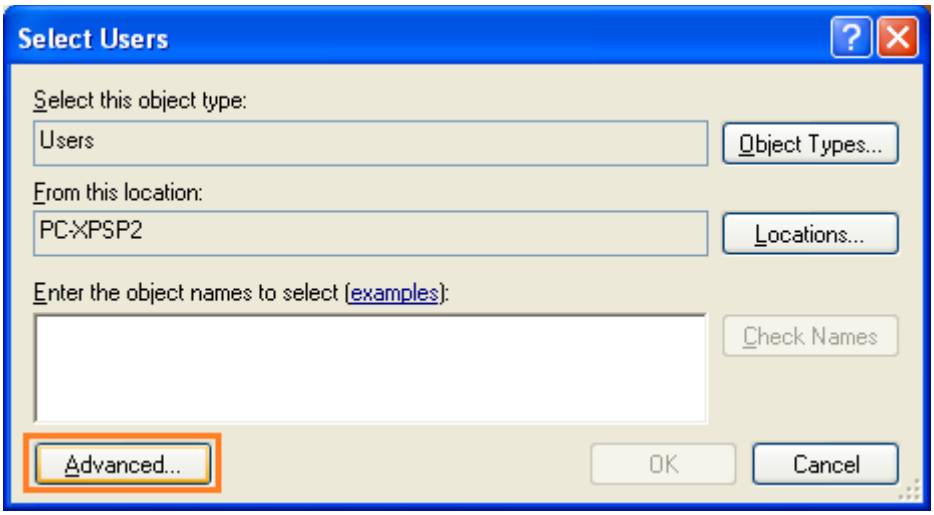
را دارند. این بدان معنا است که زمانی که کسی بخواهید از راه دور به سیستم ما وصل شود، بایستی یکی از این نام‌های کاربری و رمز عبور آن را وارد نماید. به صورت پیش فرض در ویندوز XP، فقط کاربرانی اجازه ورود به سیستم به صورت Remote را دارند که عضوی از گروه Remote Desktop باشند. یعنی کاربری که تعریف کردهاید را باید عضوی از (Member of) گروه Remote Desktop کنیم. برای انجام این کار، در همین صفحه روی دکمه Select Remote Users کلیک کنید.



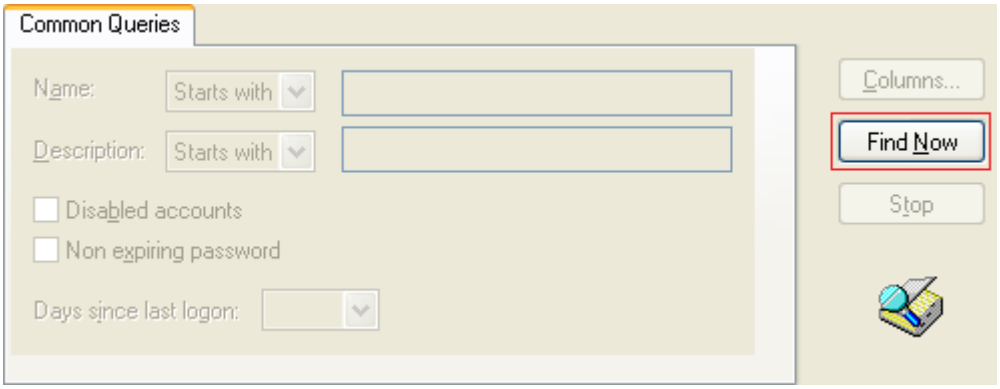
در صفحه باز شده، برای افزودن کاربر به گروه Remote Desktop، روی دکمه Add کلیک نمایید.



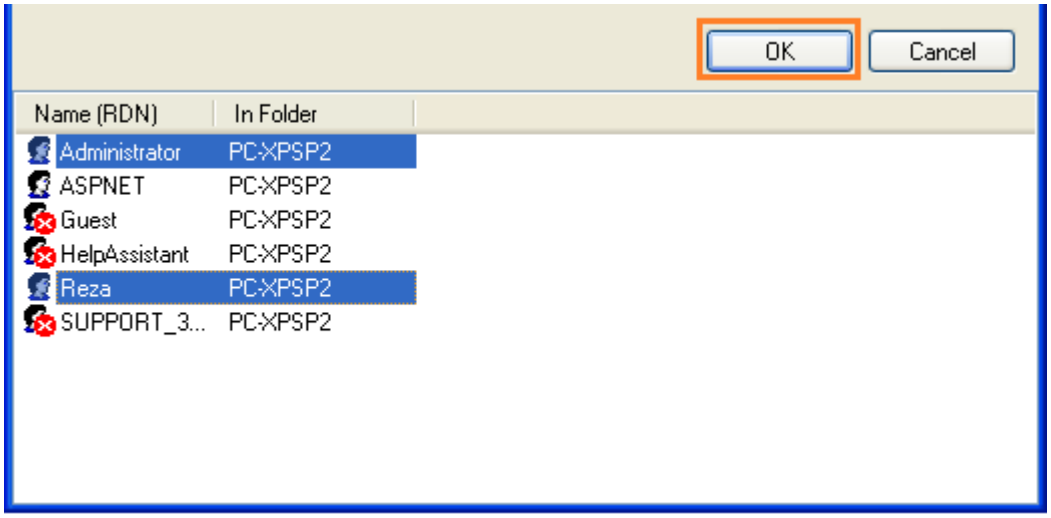
در این صفحه، دو راه برای انتخاب کاربران خود دارید. راه اول وارد کردن نام کاربر به صورت دقیق در جعبه متن پایین و سپس کلیک روی دکمه Check Names برای بررسی صحت نام وارد شده می‌باشد. راه دوم، انتخاب کاربر به صورت Visual (بصری) است. بدین منظور روی دکمه Advanced کلیک کنید.



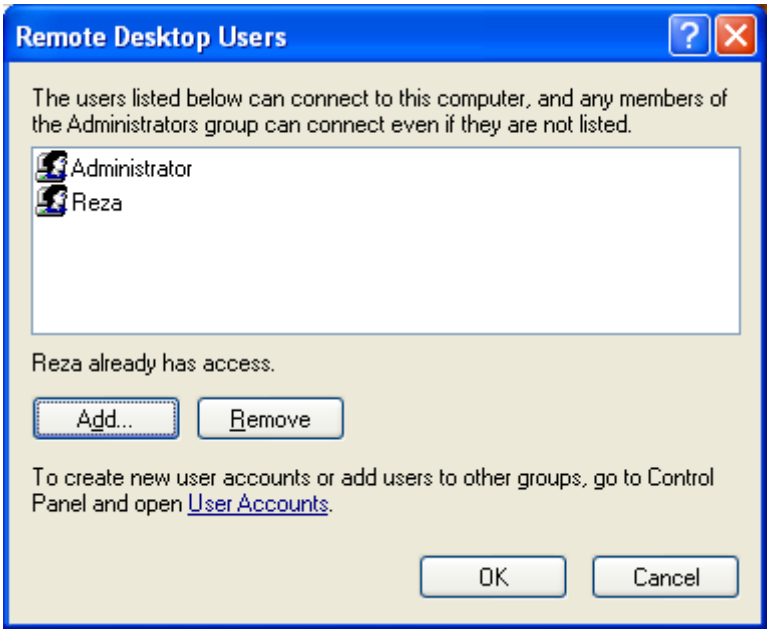
در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست کاربران و گروه‌ها ظاهر شود.



سپس کاربر یا کاربران مورد نظر که قصد دارید قابلیت Remote را داشته باشند، انتخاب کرده و سپس روی دکمه OK کلیک کنید.



در این صفحه لیست کاربران اضافه شده را مشاهده می‌نمایید. در نهایت روی دکمه OK کلیک کنید.

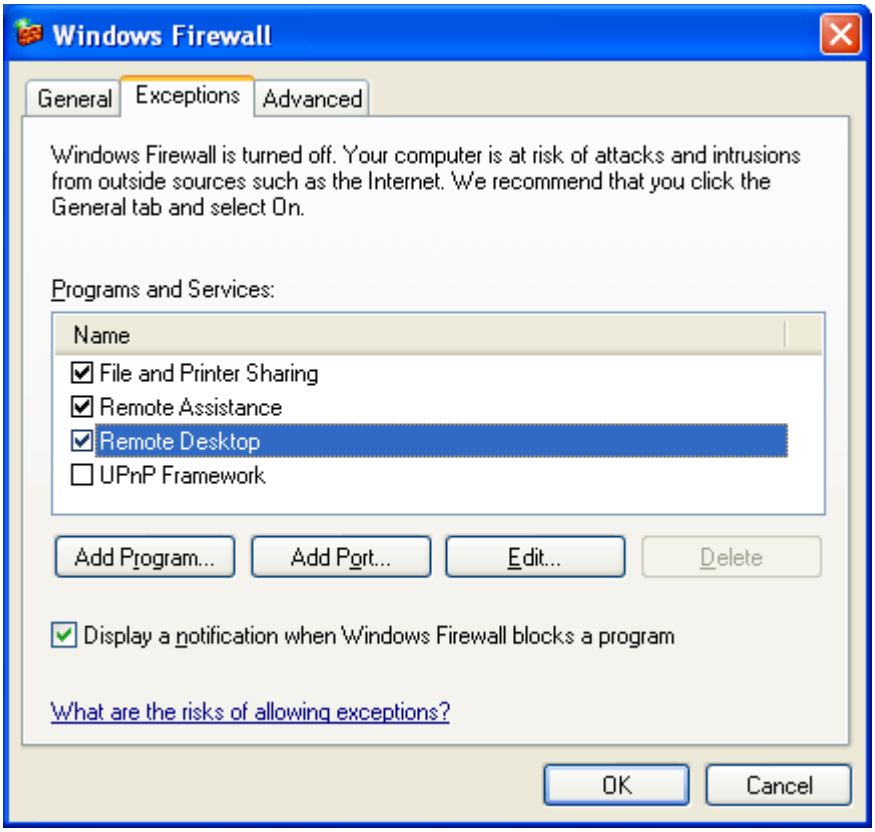


در مرحله بعد بایستی به Firewall بگویید که اجازه دسترسی به صورت Remote را بدهد (Firewall یک ابزار امنیتی در ویندوز است). بدین منظور وارد Control Panel شده و سپس برنامه Windows Firewall را باز نمایید.



سپس در صفحه باز شده، وارد سربرگ Exceptions شده و سپس گزینه Remote Desktop را فعال نمایید. در نهایت روی دکمه OK کلیک کنید.

البته توجه فرمایید که اگر Firewall غیر فعال باشد، نیازی به انجام این کار نیست.



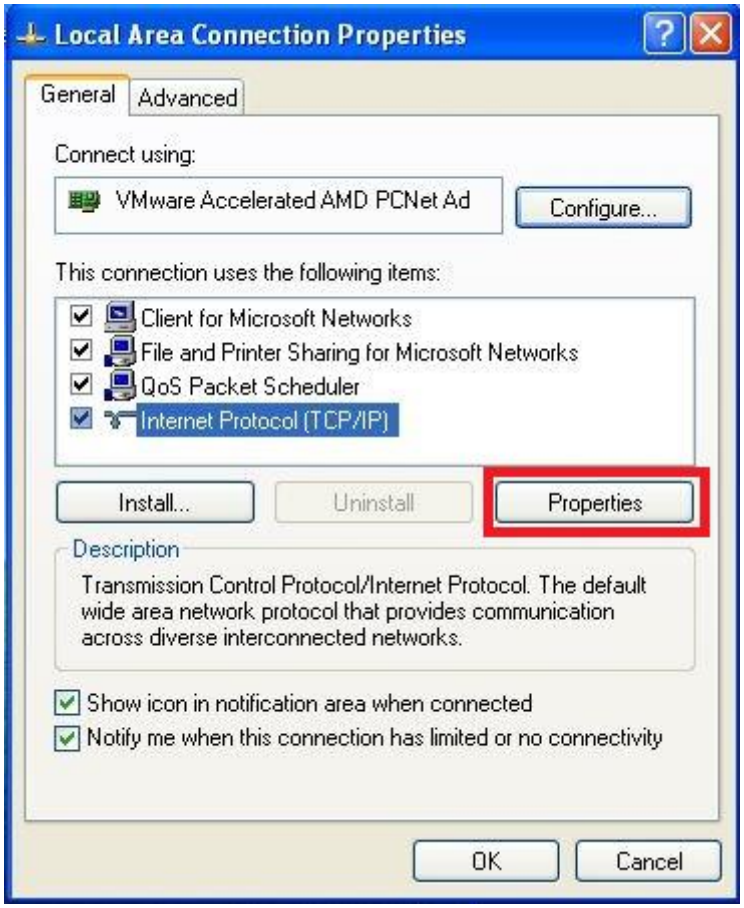
در مرحله آخر، بایستی آدرس IP کامپیوتر را تعیین نمایید. بدین دلیل که کامپیوترها برای اتصال راه دور از آدرس IP استفاده می‌کنند. البته برای اتصال، امکان استفاده از نام کامپیوتر نیز وجود دارد. برای انجام تنظیمات IP، وارد مسیر زیر شوید:

Control Panel ➔ Network Connections

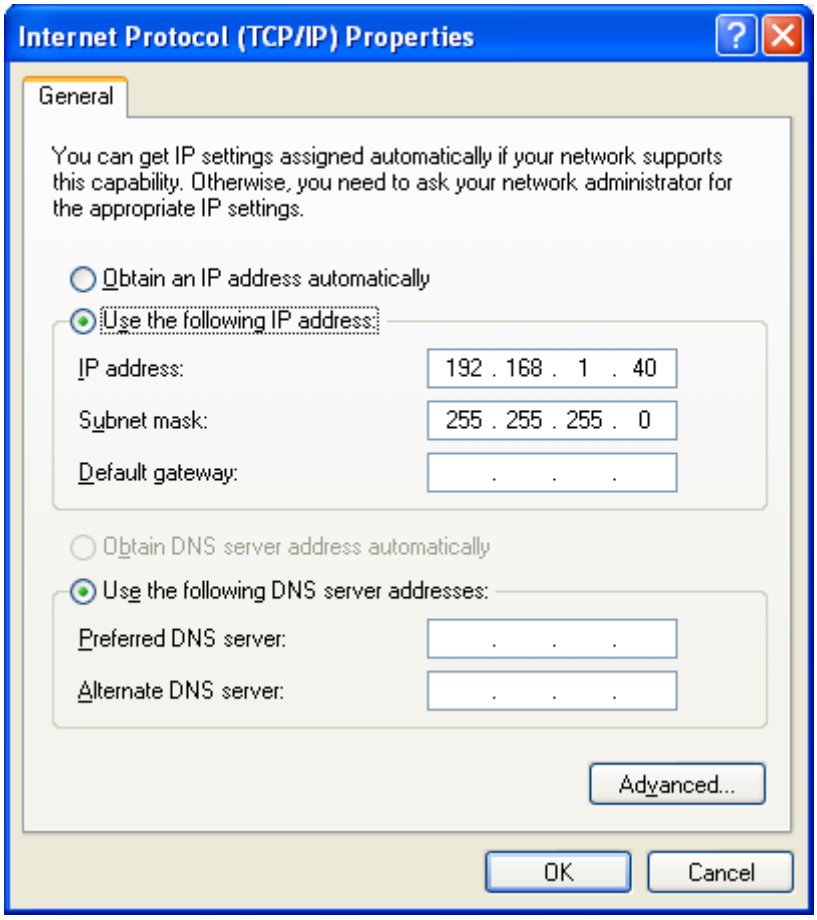
روی Local Area Network راست کلیک کرده و Properties را انتخاب نمایید.



در صفحه باز شده، گزینه Internet Protocol (TCP/IP) را انتخاب کرده و سپس روی دکمه Properties کلیک نمایید.



در صفحه باز شده، مانند شکل، آدرس IP را به صورت دستی تنظیم کنید. البته نیازی به تخصیص آدرس به صورت دستی نیست. تنها چیزی که نیاز داریم، دانستن آدرس IP یا نام کامپیوتر جهت اتصال راه دور است. در نهایت روی OK کلیک کنید.

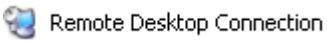


تا این مرحله، سیستم ما قابلیت پذیرش اتصال Remote را پیدا کرده است. فقط کافیست از سیستم‌های دیگر به آن متصل شویم.

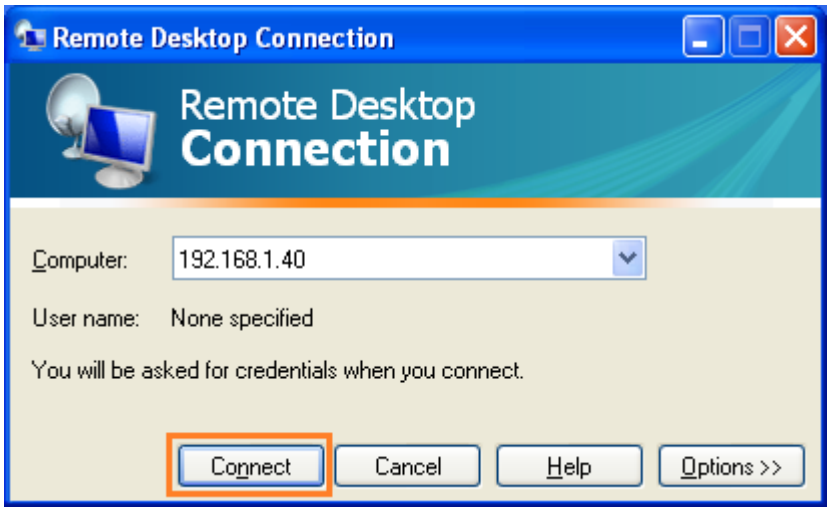
۳۱-۲-۲- اتصال به کامپیوتر راه دور

در این مرحله قصد داریم که توسط این سیستم به سیستم راه دور (سیستمی که آن را در مرحله قبل تنظیم نمودیم) متصل شویم. برای این کار، ابتدا نرم‌افزار Remote Desktop Connection را اجرا نمایید. محل این نرم‌افزار به صورت زیر است:

Start ➔ Accessories ➔ Communications ➔ Remote Desktop Connection

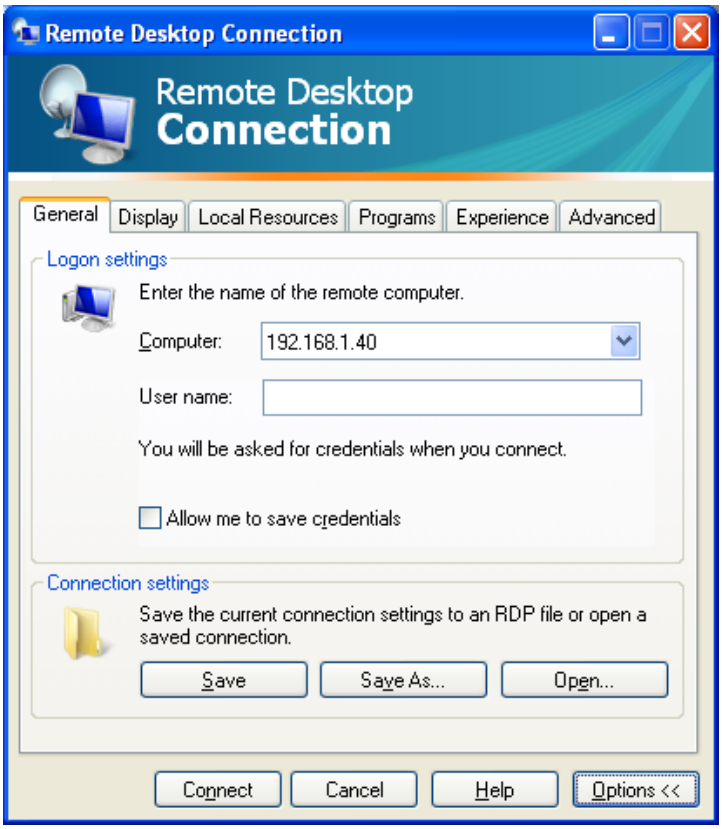


پس از اجرای نرم‌افزار Remote Desktop Connection، صفحه‌ای مانند شکل زیر نمایان می‌شود. در این صفحه ابتدا آدرس IP یا نام کامپیوتر مقصد (Remote) را وارد نمایید. در نهایت برای اتصال، روی دکمه Connect کلیک کنید. البته قبل از اتصال، می‌توان تنظیماتی را نیز انجام داد. بدین منظور روی دکمه Options کلیک نمایید.



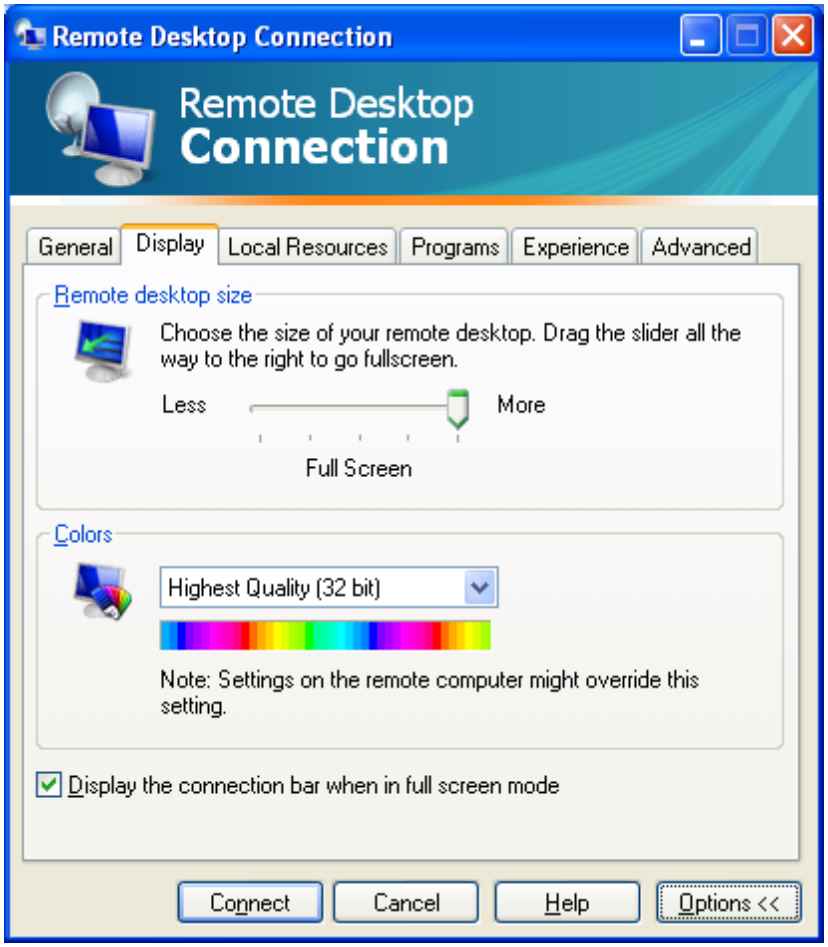
سربرگ General

در سربرگ General مربوط به تنظیمات، شما این قابلیت را دارید که نام کاربری خود جهت اتصال را وارد نمایید. البته توجه فرمایید که رمز عبور را فعلا نمی‌توانید وارد کنید. همچنین در این قسمت قابلیت ذخیره یا بازیابی تنظیمات وجود دارد.



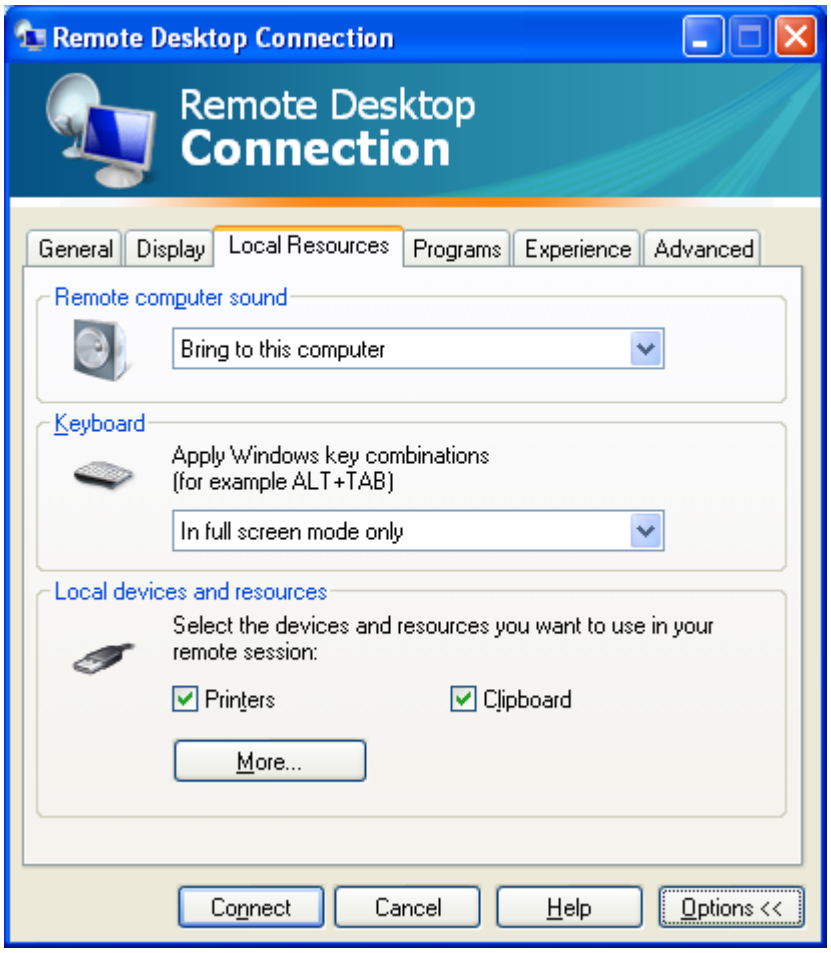
سربرگ Display

در این صفحه، قابلیت تنظیم وضوح تصویر نمایشی را دارید. این امر زمانی کاربرد دارد که سرعت اتصال شما کم باشد و بخواهد مقدار اطلاعات انتقالی هنگام نمایش صفحه کامپیوتر راه دور را کاهش دهید. مثلاً تنظیم کنید که سیستم رنگ ۱۶ بیتی شده؛ یا وضوح تصویر کم شود.



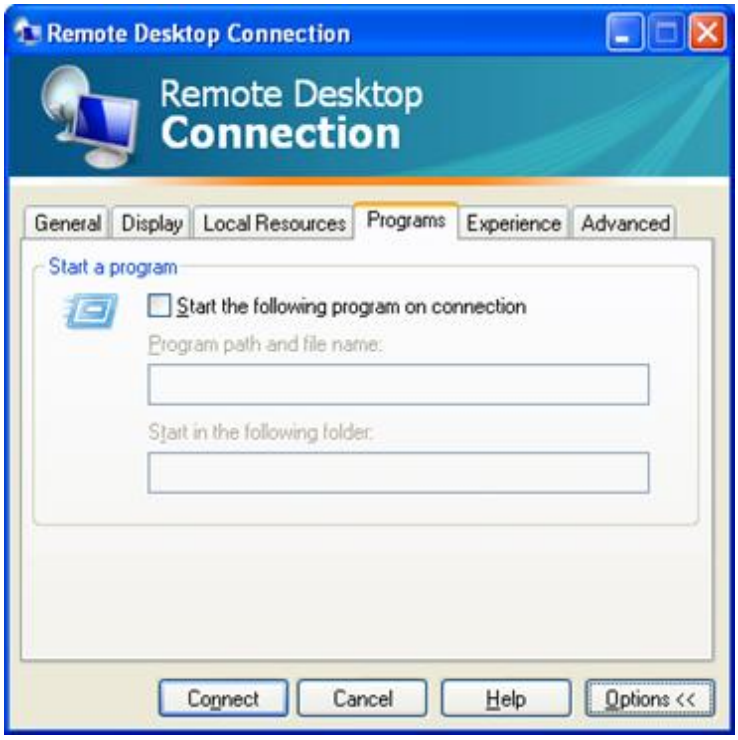
سربرگ Local Resource

در این سربرگ، می‌توانید تعیین کنید که قصد دارید از کدام یک از منابع کامپیوتر راه دور استفاده نمایید. مثلاً تنظیم کنید که صداهایی که روی کامپیوتر راه دور پخش می‌شوند را توسط Speaker خود بشنوید یا اینکه درایوهای Hard Disk کامپیوتر راه دور را در سیستم خود مشاهده نمایید.



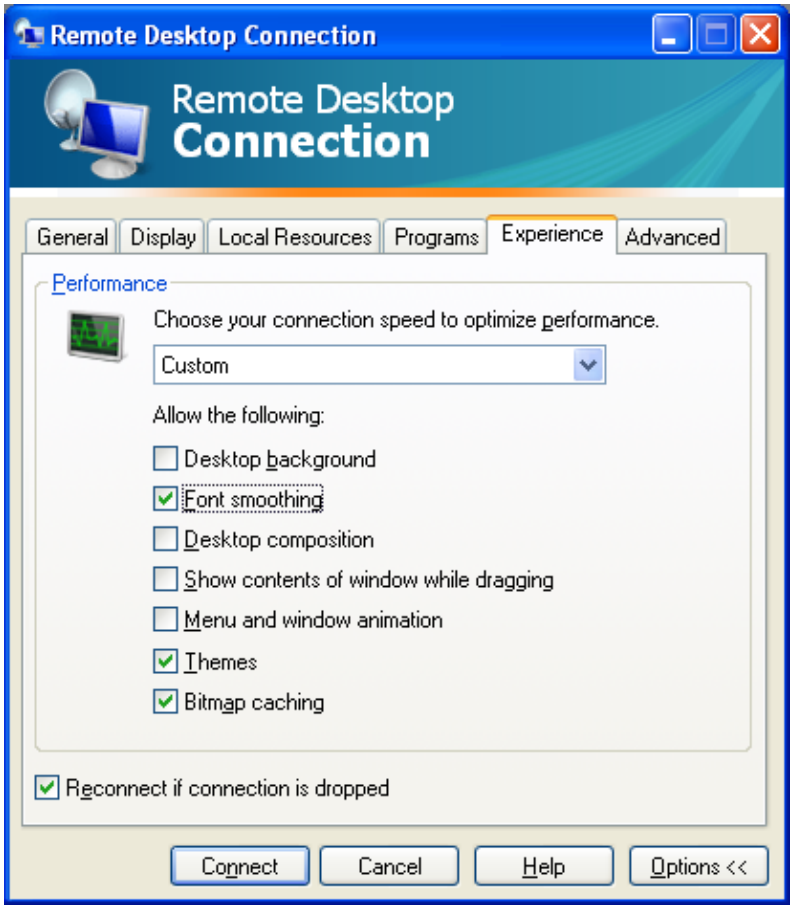
سربرگ Programs

در این قسمت می‌توانید تعیین کنید که در زمانی که به کامپیوتر راه دور متصل هستید، کدام برنامه اجرا شود. بدین منظور آدرس کامل برنامه و آدرس پوشه آن را وارد کنید. مثلاً برای اجرای برنامه موجود در مسیر C:\Program\Calc.exe، در جعبه متن بالایی مقدار C:\Program\Calc.exe و در جعبه متن پایینی مقدار C:\Program را وارد نمایید. منظور از جعبه متن پایینی، مقدار مسیر جاری برنامه هنگام اجرای آن است (این بحث در برنامه نویسی نمود پیدا می‌کند). فرض کنید که برنامه‌ای نوشتهاید و برنامه در حال اجرا می‌باشد؛ شما نیز در برنامه قطعه کدی نوشتهاید که مثلاً فایل A.txt را باز کند fopen("A.txt");". حال اگر مسیر جاری برنامه، همان محل وجود فایل exe باشد، فایل A.txt موجود در کنار فایل exe باز خواهد شد. اما اگر مسیر جاری برنامه را به C:\ تغییر دهیم، برنامه exe هر کجا که باشد، فایل موجود در C:\A.txt باز خواهد شد.



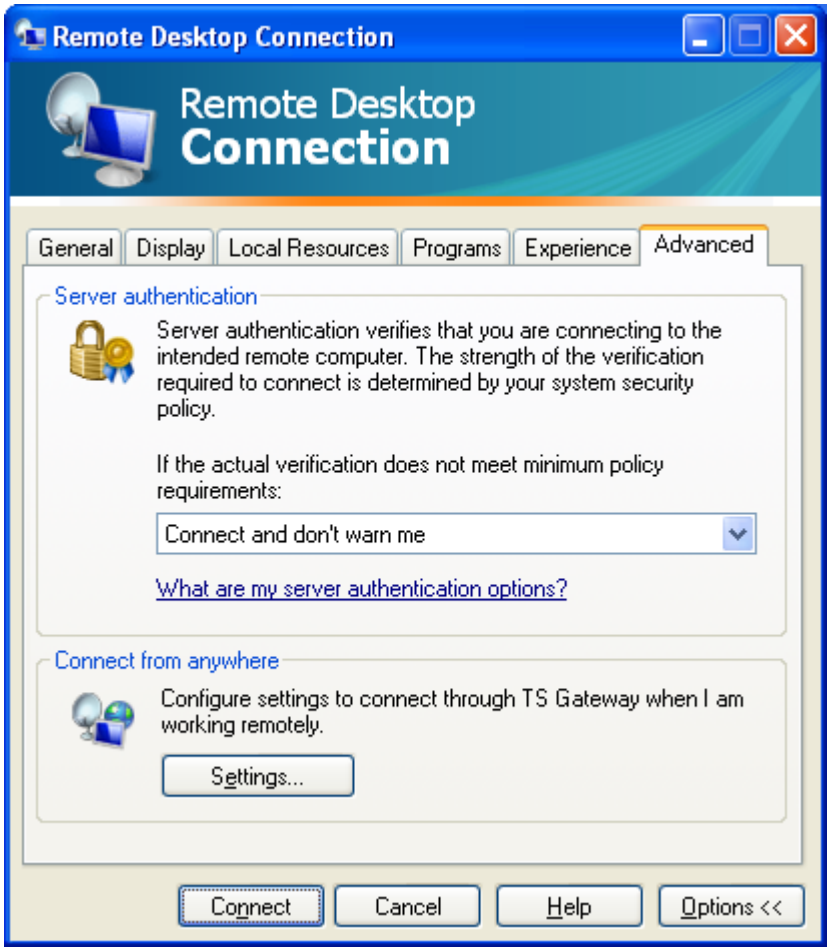
سربرگ Experience

در این قسمت می‌توانید تنظیماتی که مربوط به کارآیی (سرعت) اتصال است را وارد نمایید. مثلاً نمایش Background یا Theme کامپیوتر راه دور. اگر سرعت اتصال شما کم است. این قسمت را تنظیم نمایید.

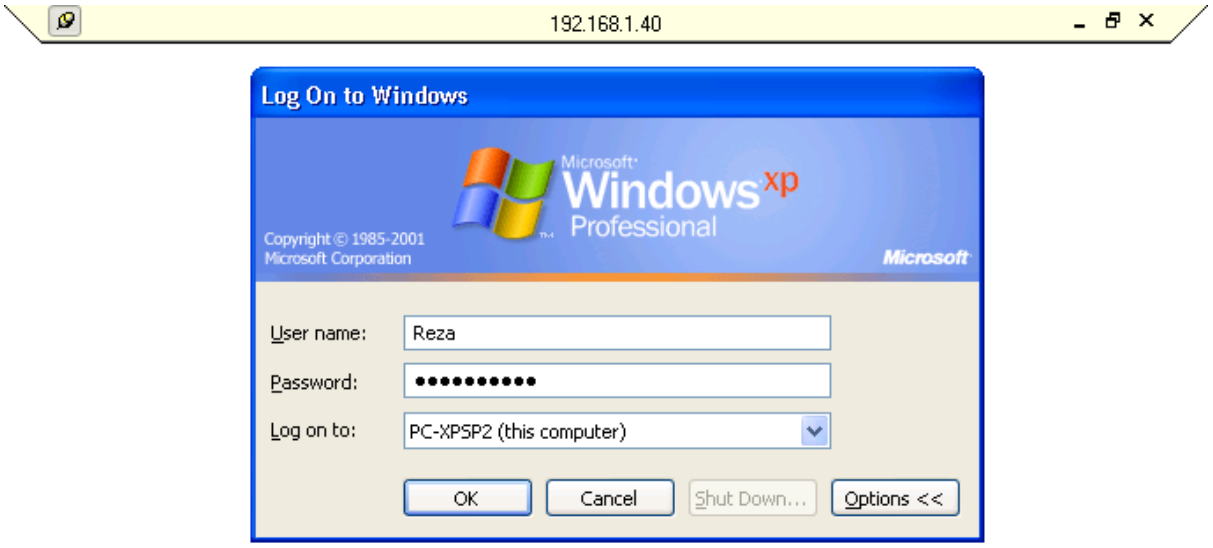


سربرگ Advanced

در این قسمت می‌توانید تنظیماتی همچون تنظیمات امنیتی را انجام دهید.



در نهایت پس از انجام تنظیمات، جهت اتصال به کامپیوتر راه دور، روی دکمه Connect کلیک کنید. اگر کامپیوتر مقصد درست پیکربندی شده باشد، صفحه Login به سیستم را مشاهده می‌کنید. جهت ورود به سیستم، در صفحه باز شده، نام کاربری و رمز عبور را وارد نمایید.

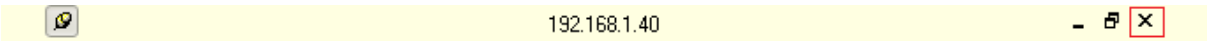


اگر نام کاربری و رمز عبور صحیح باشد، صفحه کامپیوتر مقصد را خواهید دید. گفتیم که یکی از معایب Remote Desktop Connection، این است که همزمان بیش از یک کاربر نمی‌تواند به یک سیستم Login کند. حال اگر به

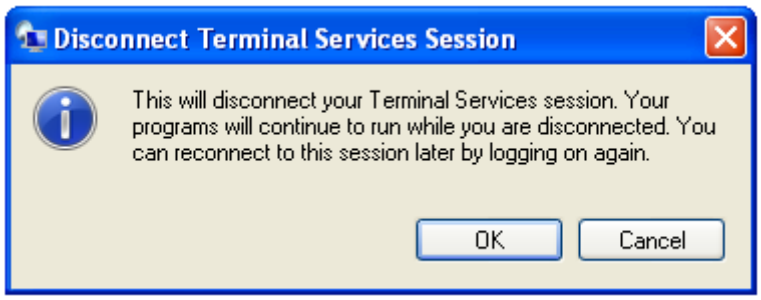
کامپیوتر راه دور سری بزنید، خواهید دید که کاربر آن Log out شده است. البته در عمل، کاربر Lock شده و اجازه کار ندارد. در صورت Unlock کردن، کاربر راه دور خارج خواهد شد.



برای قطع اتصال خود، روی دکمه Close که در بالای صفحه موجود است، کلیک نمایید.



قبل از بسته شدن، سیستم اخطار می‌دهد که با بستن صفحه Session شما قطع نشده و بعدا می‌توانید مجددا به سیستم Login کنید و کا خود را تا جایی که پیش رفته است؛ ادامه دهید.



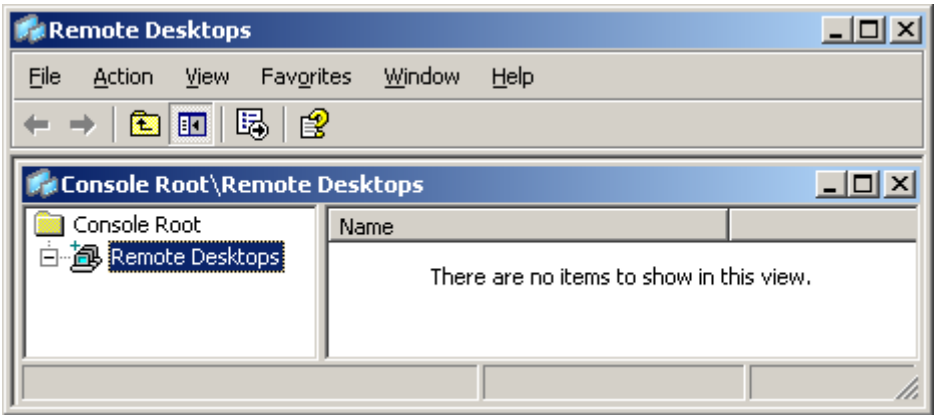
۳۱-۲-۳- Remote Desktop Connection در ویندوز سرور ۲۰۰۳

ویندوز سرور نیز مانند ویندوز XP، دارای ابزار Remote Desktop Connection جهت اتصال به سیستم‌های راه دور می‌باشد. اما در ویندوز سرور، ابزار قوی تری تحت عنوان Remote Desktops وجود دارد. توسط این ابزار می‌توان همزمان به چند سیستم راه دور دسترسی داشت و آن‌ها را کنترل نمود. مزیت دیگر این ابزار، این است که می‌توان با تنظیم User Name و Password برای یک اتصال برای بار اول، برای اتصال‌های بعدی دیگر User Name و Password وارد نکرد.

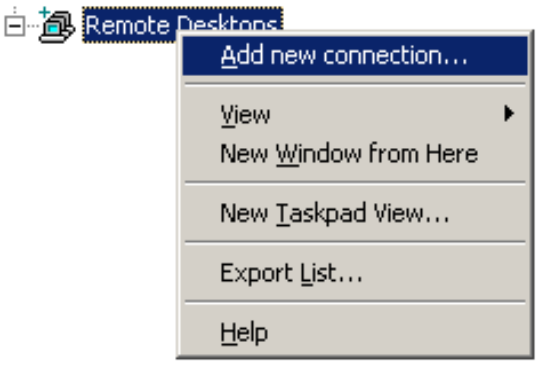
برای بازکردن این ابزار، از قسمت Administrative Tools ➔ Start، برنامه Remote Desktops را اجرا نمایید.



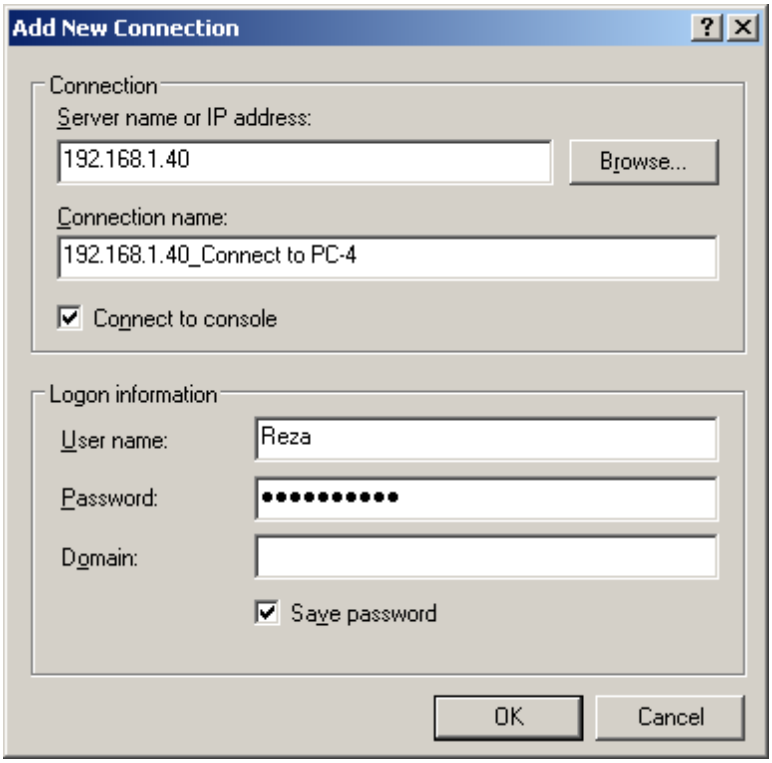
پس از باز شدن برنامه، صفحه‌ای مانند صفحه زیر را مشاهده خواهید کرد. قسمت سمت چپ، بیانگر اتصالات ساخته شده و قسمت سمت راست بیانگر صفحه کاری شما می‌باشد.



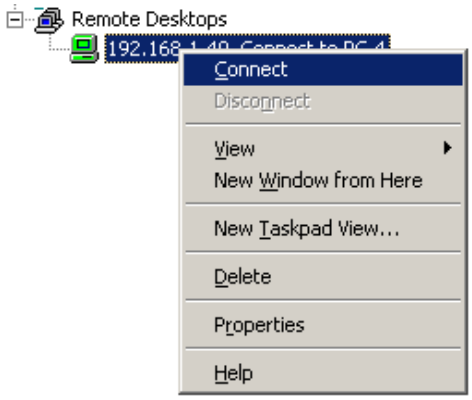
برای ساخت اتصال جدید، روی قسمت Remote Desktops راست کلیک کرده و Add new connection را انتخاب نمایید.



در صفحه باز شده، ابتدا آدرس IP یا نام کامپیوتر مقصد را وارد کنید. سپس یک نام برای Connection خود انتخاب نمایید. در نهایت نیز نام کاربری، رمز عبور و نام دامنه (در صورتی که نام کاربری وارد شده، مربوط به دامنه‌ای خاص بوده که کامپیوتر مقصد به آن متصل می‌باشد) را وارد کرده روی OK کلیک کنید. در صورتی که گزینه Save Password را فعال کرده باشید، برای اتصالات بعدی، نیازی به وارد کردن رمز عبور نخواهید داشت.



برای اتصال به کامپیوتر راه دور، روی Connection ساخته شده راست کلیک کرده و گزینه Connect را انتخاب نمایید.



پس از اتصال، صفحه کامپیوتر راه دور را در سمت راست مشاهده خواهید کرد.



البته توجه نمایید که اگر سیستم عامل کامپیوتر راه دور شما، ویندوز سرور نباشد، کاربر جاری آن از سیستم خارج (Log out) خواهد شد.



هنگام بستن برنامه Remote Desktops، سیستم از شما سوالی مبنی بر ذخیره اطلاعات اتصالات ساخته شده می‌پرسد. به سوال پرسیده شده، جواب مثبت بدهید تا اطلاعات شما ذخیره شود.

۳۱-۳- Terminal Server

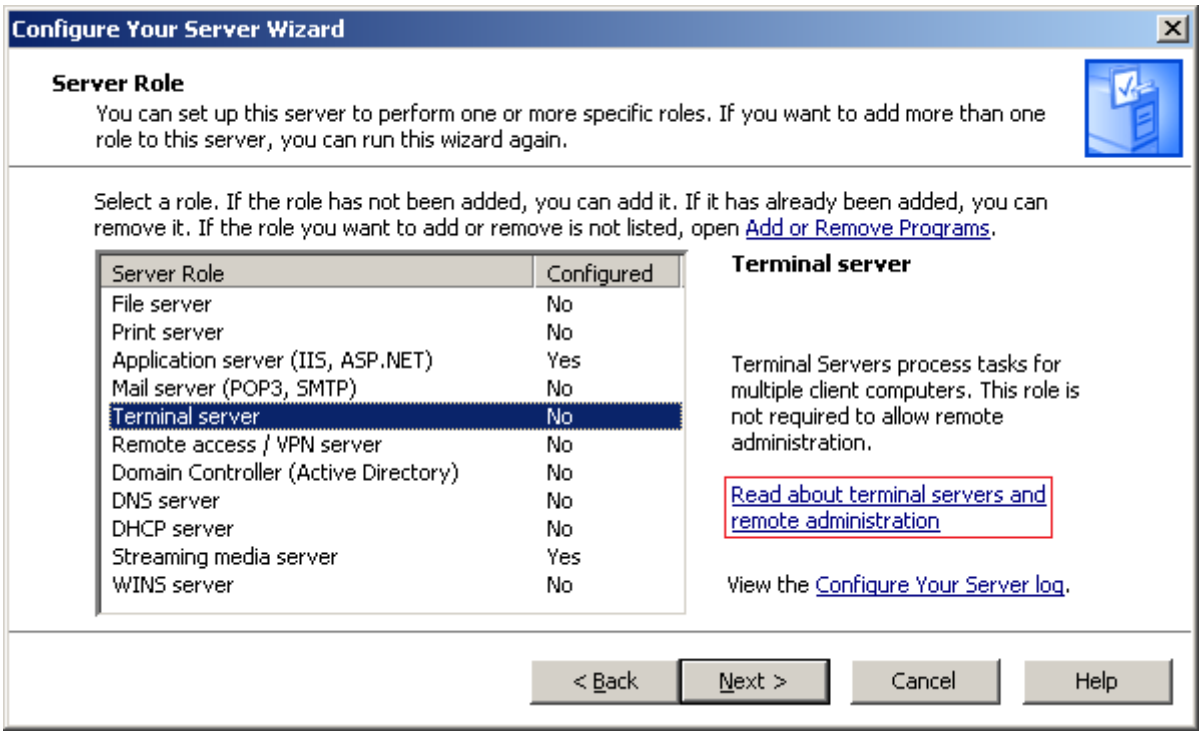
۳۱-۳-۱- راه اندازی Terminal Server در ویندوز سرور

در بخش‌های فوق با مشکلات Remote Desktop Connection آشنا شدید. برای حل این مشکلات، مایکروسافت Terminal Server را معرفی کرد. برای استفاده از این سرویس، بایستی ابتدا آن را روی ویندوز سرور نصب کنید. بدین منظور، مسیر زیر را اجرا کنید: Start ➔ Administrative Tools ➔ Configure Your Server Wizard. این بخش جهت افزودن نقش (Role) به سرور مورد استفاده قرار می گیرد.

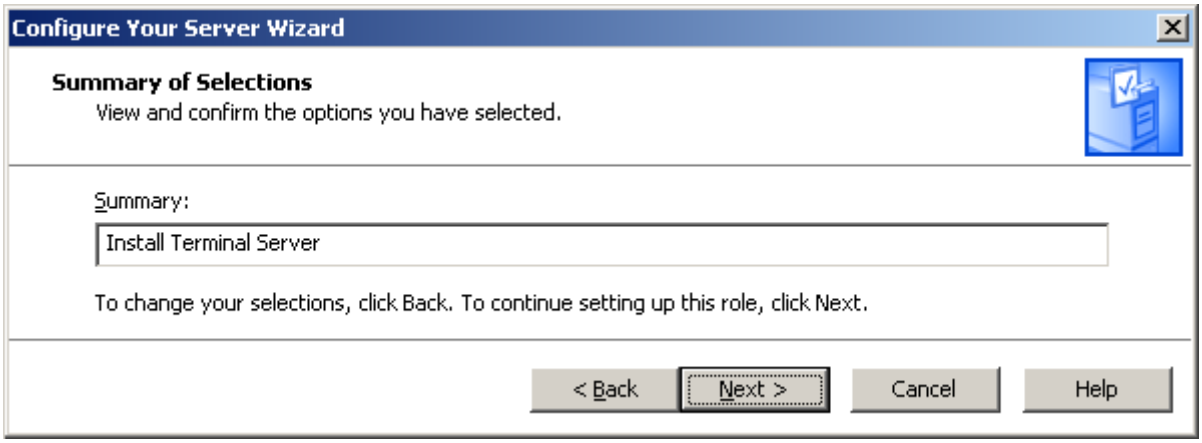


ابتدا صفحه خوش آمد گویی باز می‌شود. در این صفحه، دکمه Next را بزنید.

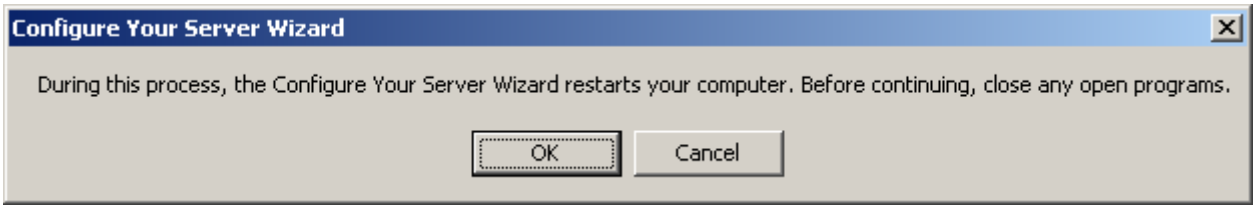
در صفحه باز شده، گزینه Terminal Server را انتخاب کنید، این بدان معناست که می‌خواهید نقش Terminal Server را به این کامپیوتر بدهید. جهت کسب اطلاعات بیشتر در مورد Terminal server روی گزینه Read about terminal servers and remote administration کلیک کنید. در نهایت روی دکمه Next کلیک کنید.



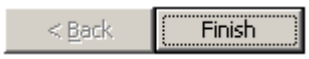
مجددا روی دکمه Next کلیک کنید.



در این صفحه، سیستم به شما پیغام می‌دهد که پس از نصب Terminal Server، سیستم شما Restart خواهد شد. لذا تمامی برنامه‌های باز شده را ببندید.



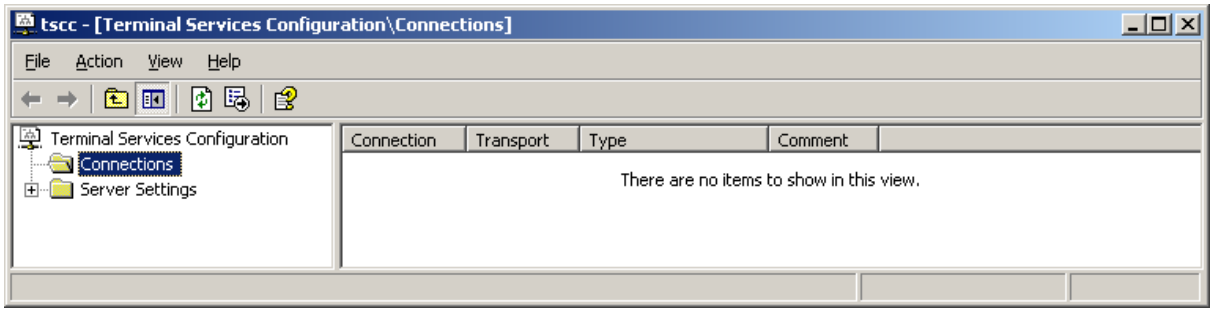
صبر کنید تا سیستم، Terminal Server را نصب کند. در صورتی که سیستم از شما سی دی ویندوز سرور را خواست، آن را در دستگاه قرار دهید. پس از پایان نصب، روی دکمه Finish کلیک نمایید.



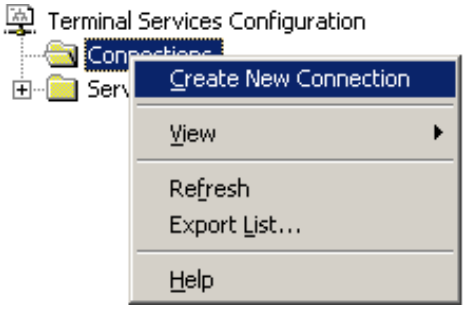
برای راه اندازی و پیکربندی Terminal Server، از مسیر Start ➔ Administrative Tools، برنامه Terminal Server Configuration را اجرا نمایید.



با اجرای برنامه Terminal Server Configuration، صفحه زیر نمایان می‌شود. در این صفحه می‌توانید اطلاعات مربوط به دریافت اتصالات راه دور را تنظیم نمایید.

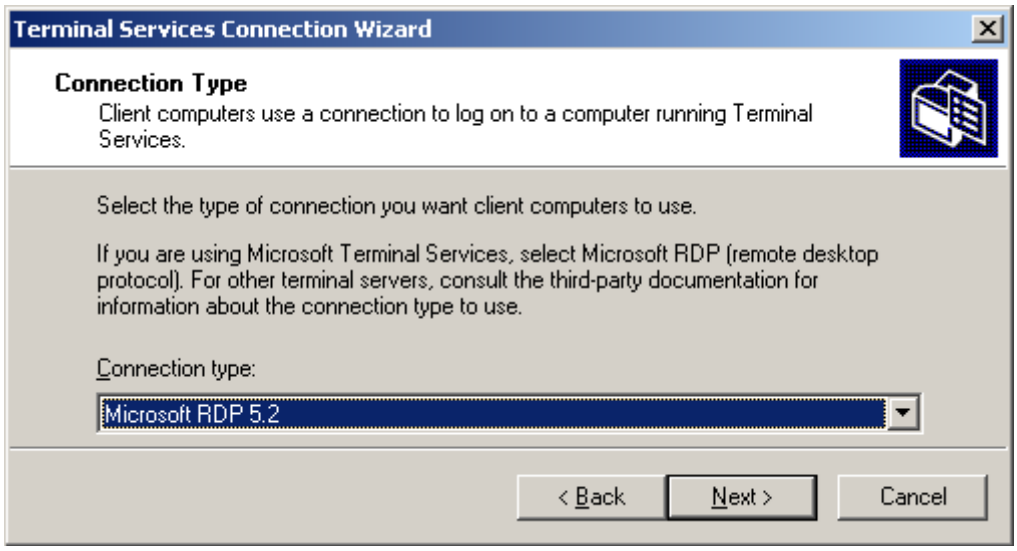


در ابتدا بایستی یک Connection جدید بسازید. این Connection مسئول پذیرش درخواست‌ها و اتصالات Remote خواهد بود. بدون این Connection، کاربران قادر به اتصال به ویندوز سرور نیستند. جهت ساخت Connection جدید، روی قسمت Connections راست کلیک کرده و سپس گزینه Create New Connection را انتخاب نمایید.



در صفحه خوش آمد گویی، روی دکمه Next کلیک کنید.

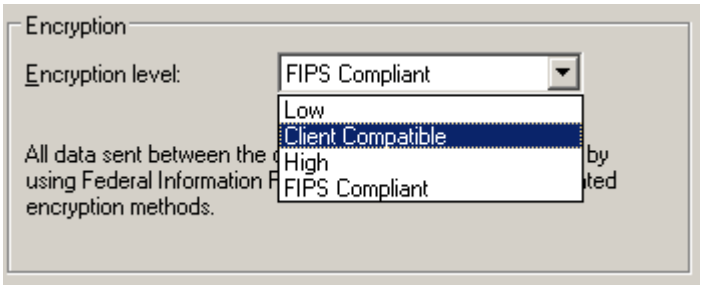
در صفحه بعد، نوع پروتکلی که برای اتصال راه دور استفاده می‌نمایید را انتخاب نمایید. به طور پیش فرض گزینه Microsoft RDP 5.2 انتخاب شده است. این گزینه پروتکل Remote Desktop Protocol است که توسط مایکروسافت عرضه شده است. لزوم این پروتکل، هماهنگی و توافق دستگاه‌ها روی اطلاعات ارسالی بین دو کامپیوتر است. سپس روی Next کلیک کنید.



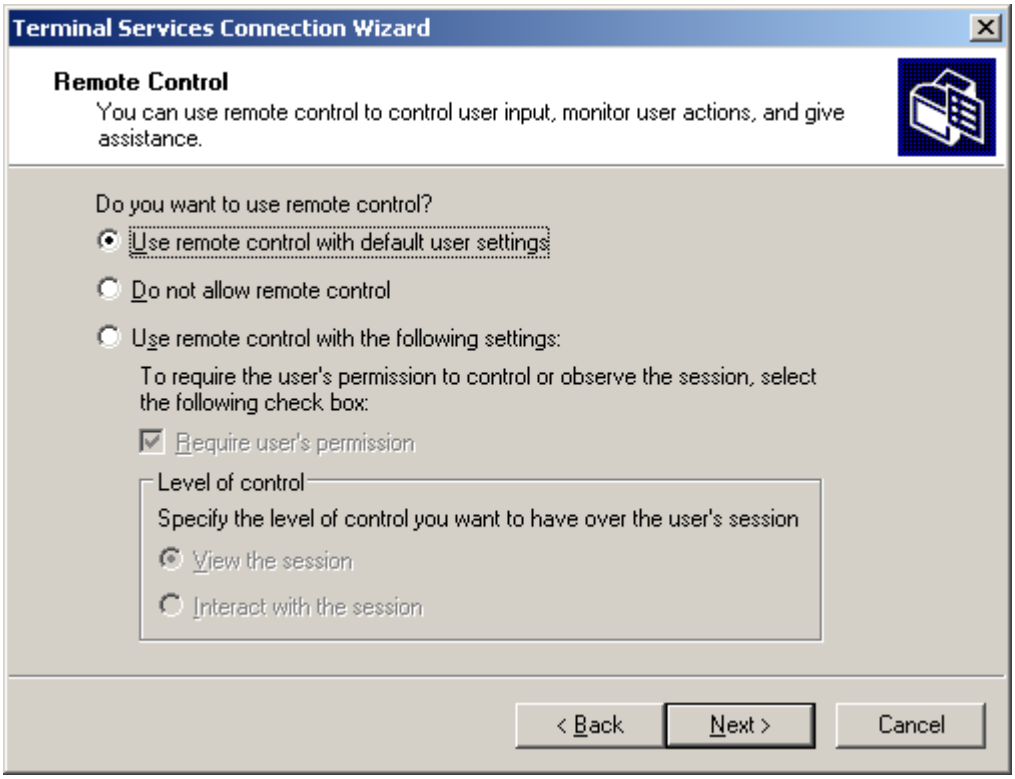
در مرحله بعد، مرحله و سطح کد گذاری (Encryption) را انتخاب کنید. در قسمت زیرین نیز گزینه Use standard Windows authentication را انتخاب نمایید تا احراز هویت کاربران ورودی توسط اعتبار سنجی ویندوز انجام شود.



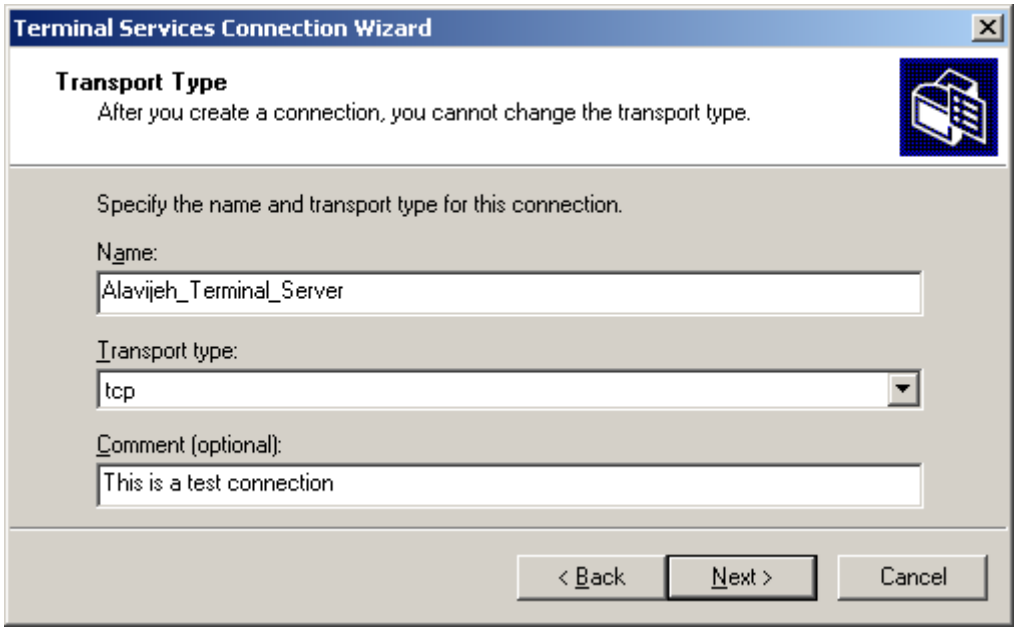
در این صفحه می‌توانید سطوح مختلفی از کد گذاری را انتخاب نمایید. همانطور که می‌دانید، هنگام کد گذاری اطلاعات یک کلید نیز برای آن تولید می‌شود، و عمل کد گشایی توسط این کلید انجام می‌شود. هرچه طول این کلید بیشتر باشد، امنیت کد گذاری بیشتر خواهد بود. اگر در این صفحه نوع Low را انتخاب کنید، طول کلید ۵۶ بیت و اگر نوع High را انتخاب کنید، طول کلید ۱۲۸ بیت خواهد بود. با انتخاب گزینه Client Compatible، طول کلید برابر با بیشترین طول قابل پشتیبانی توسط Client خواهد بود. توجه نمایید که هرچه سطح امنیت بالاتر باشد، سرعت پایین‌تر خواهد آمد. لذا بین امنیت و سرعت، بایستی تا حد امکان یک حد تعادل (Trade Off) قرار دهید.



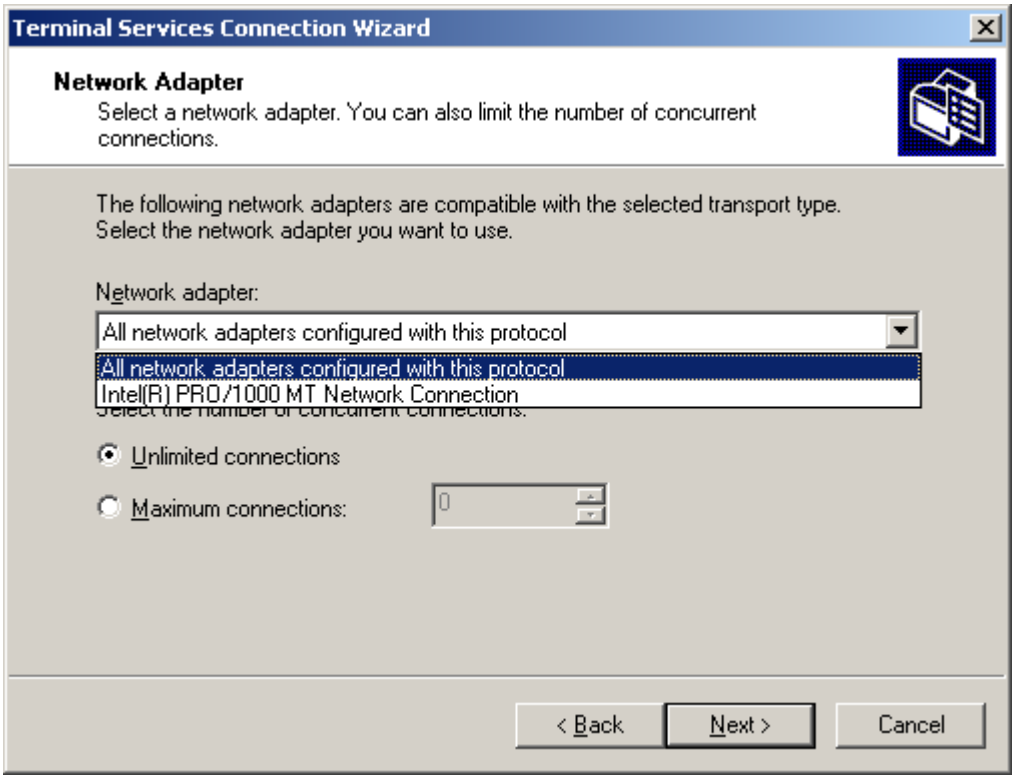
در این صفحه می‌توانید تنظیماتی را در مورد عدم پذیرش یا نحوه پذیرش Remote Control تعیین نمایید.



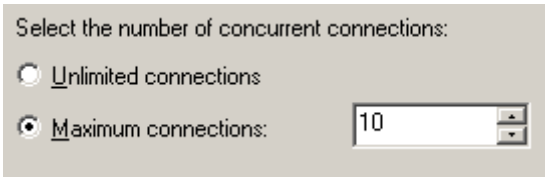
در صفحه بعد، یک نام و توصیف برای Connection خود انتخاب نمایید. همچنین می‌توانید نوع پروتکل انتقال را انتخاب نمایید. به صورت پیش فرض گزینه TCP فعال شود. به طور مختصر بدانید که پروتکل TCP یک پروتکل اتصال گرا و امن است. بدین معنا که با ارسال یک پیام، صبر می‌کند تا مطمئن شود که پیام حتما به دست مقصد می‌رسد. در مقابل TCP، پروتکل UDP قرار دارد. برعکس پروتکل TCP، این پروتکل امن نیست، یعنی تضمین نمی‌کند که پیام ارسالی حتما توسط مقصد دریافت شود؛ اما این پروتکل سرعت بالایی دارد. در نهایت روی Next کلیک کنید.



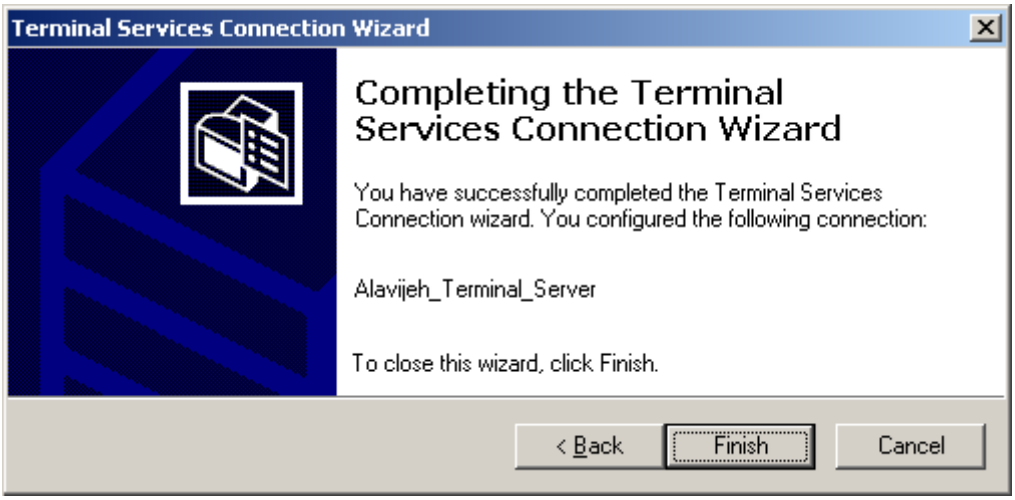
در این مرحله می‌توانید دو دسته تنظیمات را انجام دهید. دسته اول تعیین این موضوع است که کدام یک از تجهیزات شبکه شما (کارت شبکه، مودم و...)، مسئول رسیدگی به درخواست‌ها و اتصالات Remote می‌باشد؟ اگر گزینه اول، یعنی All network adapters configured with this protocol را انتخاب کنید، تمام تجهیزاتی که پروتکل تعیین شده در صفحه قبل را پشتیبانی می‌کنند، مسئول رسیدگی و مدیریت عملیات Remote خواهند بود.



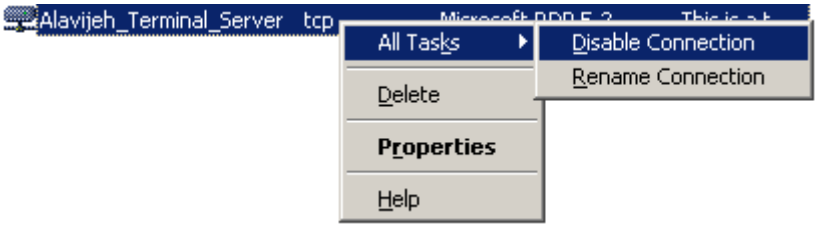
تنظیم بعدی که در این صفحه می‌توانید انجام دهید، این است که شما می‌توانید سیستم را محدود کنید که همزمان بیشتر از n کاربر، به سیستم متصل نشوند. تعیین این مقدار برای جلوگیری از شلوغی بیش از حد سرور هنگام اتصال همزمان سودمند است. در شکل زیر، ما این تعداد را به ۱۰ نفر محدود کرده‌ایم.



این صفحه نیز بیانگر اتمام ساخت Connection دریافت کننده اتصالات Remote است.

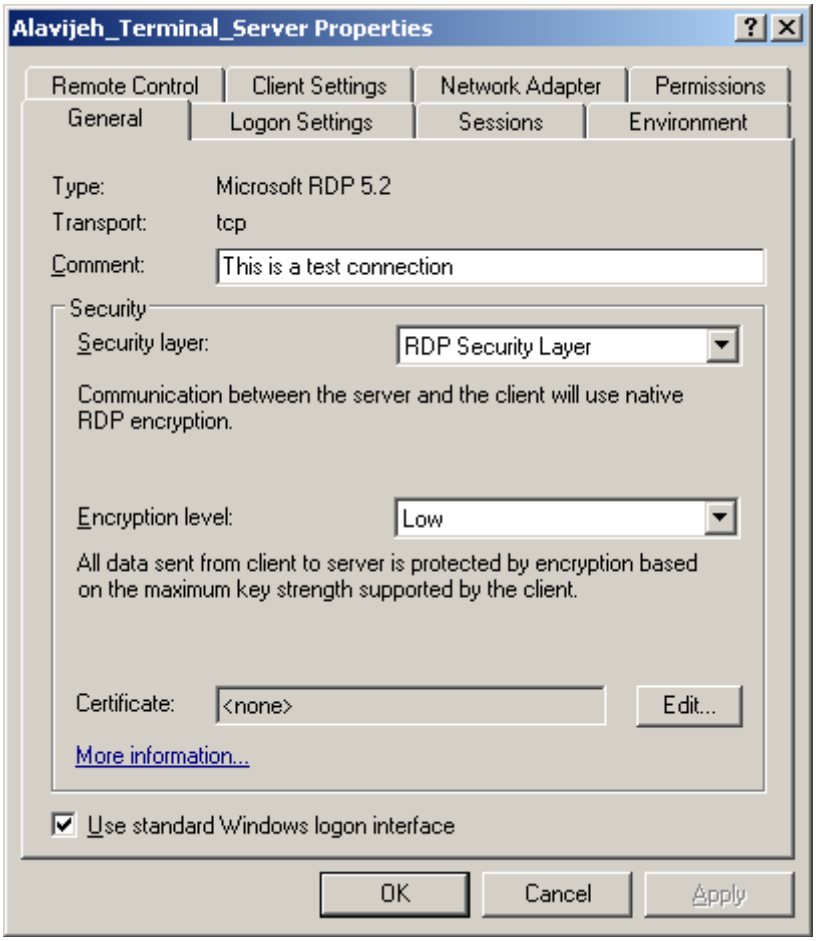


پس از ساخت Connection، ممکن است بخواهید آن را غیر فعال کنید، بدین منظور روی آن راست کلیک کرده و از قسمت All Tasks گزینه Disable Connection را انتخاب نمایید. همچنین جهت انجام تنظیمات، روی Connection ساخته شده راست کلیک کرده و گزینه Properties را انتخاب نمایید. در ادامه به معرفی قسمت‌های مختلف Properties می‌پردازیم.



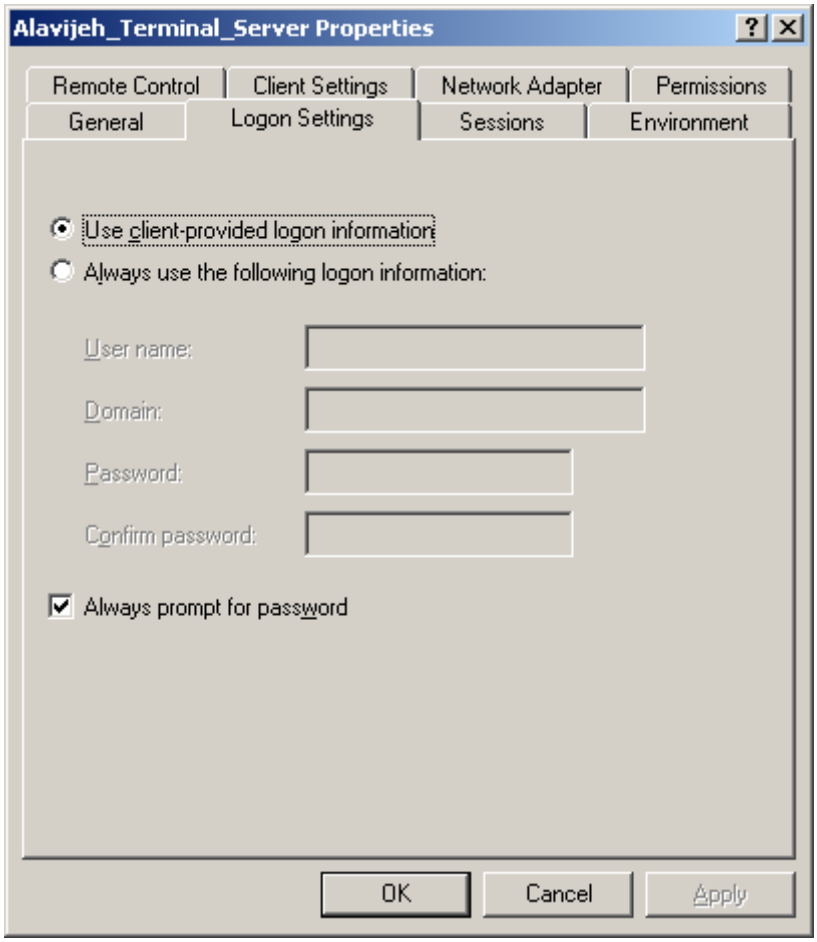
سربرگ General

در این قسمت می‌توانید تنظیمات اصلی نظیر لایه امنیتی، سطح Encryption، و نیز نوع احراز هویت را تعیین نمایید.



سربرگ Logon Settings

در این صفحه گزینه Use client provided logon information تعیین می‌کند که کاربر هنگام Login، می‌تواند هر User Name و Passwordی را وارد نماید و احراز هویت بر اساس User Name و Password وارد شده انجام می‌گیرد. اما اگر گزینه Always use the following logon information را فعال کرده و سپس مقداری را در User Name و Domain وارد نمایید، هنگام ورود کاربر، به صورت پیش فرض، همین مقادیر در صفحه Login به نمایش در خواهد آمد. همچنین اگر Always prompt for password را فعال کرده و رمزی را وارد نمایید، هنگام ورود کاربر از راه دور، به صورت خودکار همین نام کاربری و رمز عبور اعمال خواهد شد. حال اگر نام کاربری و رمز عبور آن صحیح باشد، کاربر به صورت خودکار و بدون نیاز به رمز عبور به سیستم وارد خواهد شد.



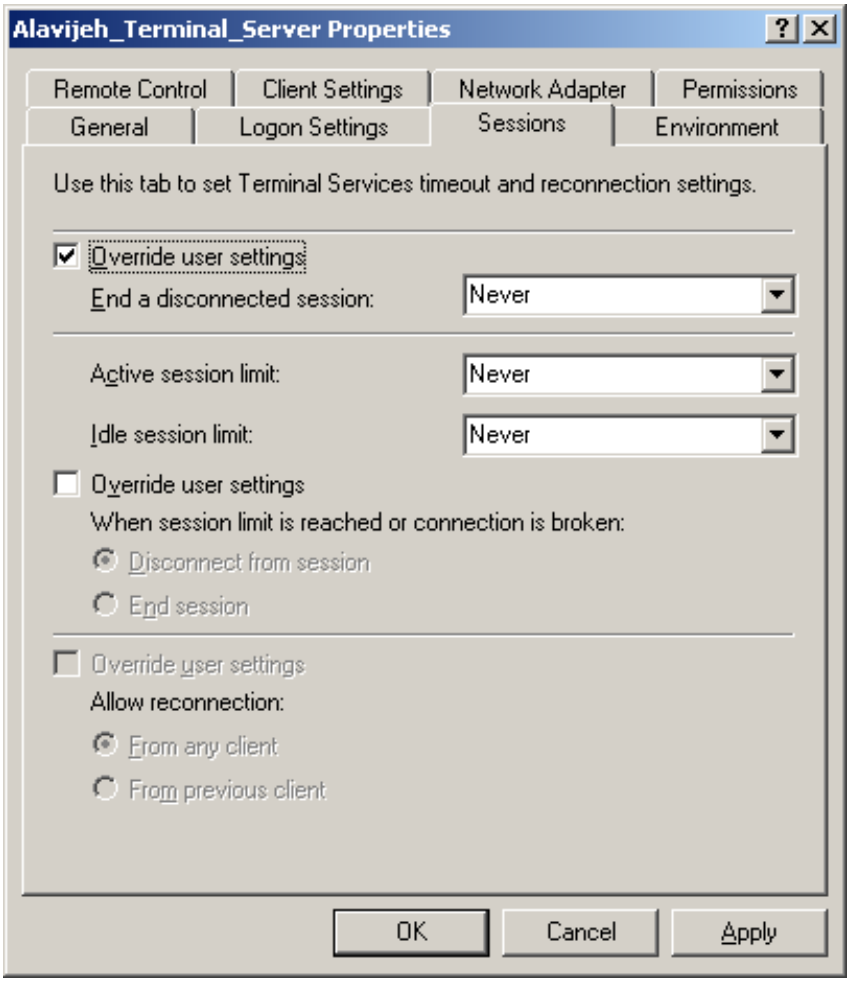
سربرگ Session

منظور از Session، اطلاعاتی در مورد جلسه ایجاد شده بین دو کامپیوتر است. در این صفحه می‌توانید اطلاعاتی را در مورد Session تنظیم نمایید. به ۳ مورد قابل تنظیم زیر توجه فرمایید:

۱. **End A Disconnected Session:** به طور پیش فرض، پس از قطع اتصال کلاینت به سرور، اطلاعات Session از بین نمی‌رود. به عنوان مثال، اگر کاربر به صورت Remote برنامه‌ای را اجرا کرده (فرض کنید برنامه رایت سی دی) و سپس از Remote خارج شود، در این صورت برنامه قطع نشده و به کار خود ادامه می‌دهد (به ادامه رایت می‌پردازد). و کاربر با Login بعدی، می‌تواند ادامه کار برنامه‌ها را ببیند. از طریق قسمت End a disconnected session می‌توان تنظیم کرد که چند دقیقه پس از Log out کردن کاربر راه دور، Session از بین برود.

۲. **Active SESSION LIMIT:** از طریق این بخش می‌توان تنظیم کرد که کاربر پس از ورود به صورت Remote، نهایتا تا چه زمانی می‌تواند داخل سیستم بماند. پس از آن به صورت خودکار، Log out خواهد شد.

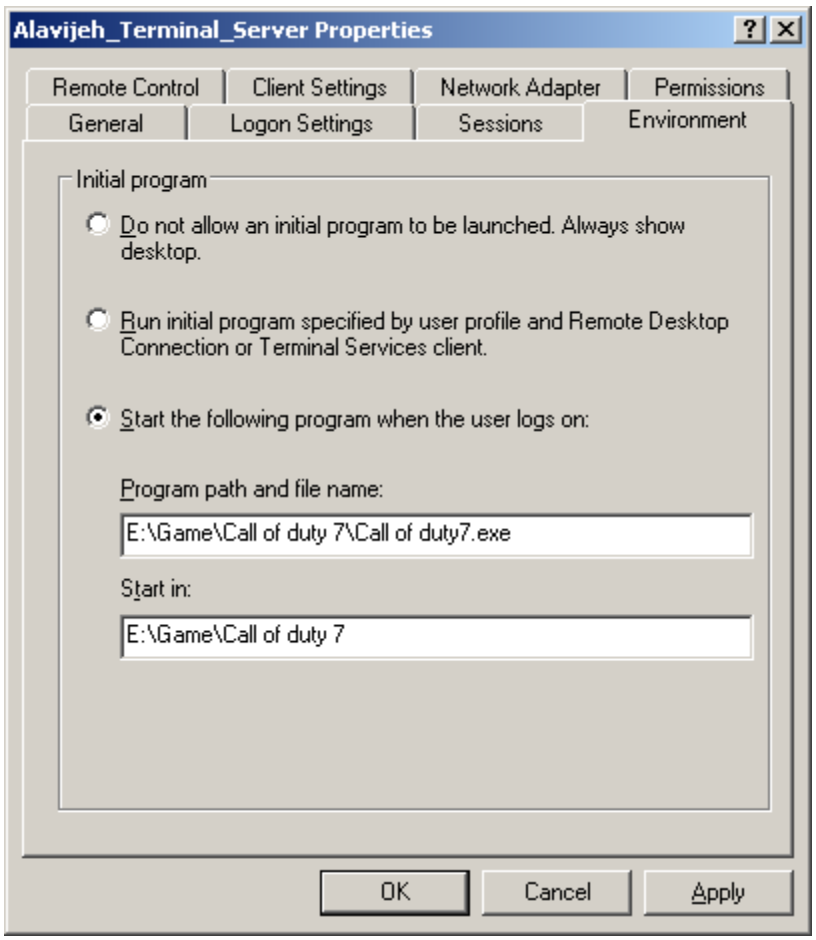
۳. **Idle Session Limit:** به کمک این قسمت می‌توان تنظیم کرد که کاربر تا چه زمانی می‌تواند بیکار باشد. منظور از بیکاری، عدم تکان دادن موس یا فشردن کلیدهای کیبرد است. با این تنظیم مشخص می‌کنیم که اگر کاربر تا زمان خاصی، از موس و کیبرد استفاده نکرد، به صورت خودکار Log out کند.



سربرگ Environment

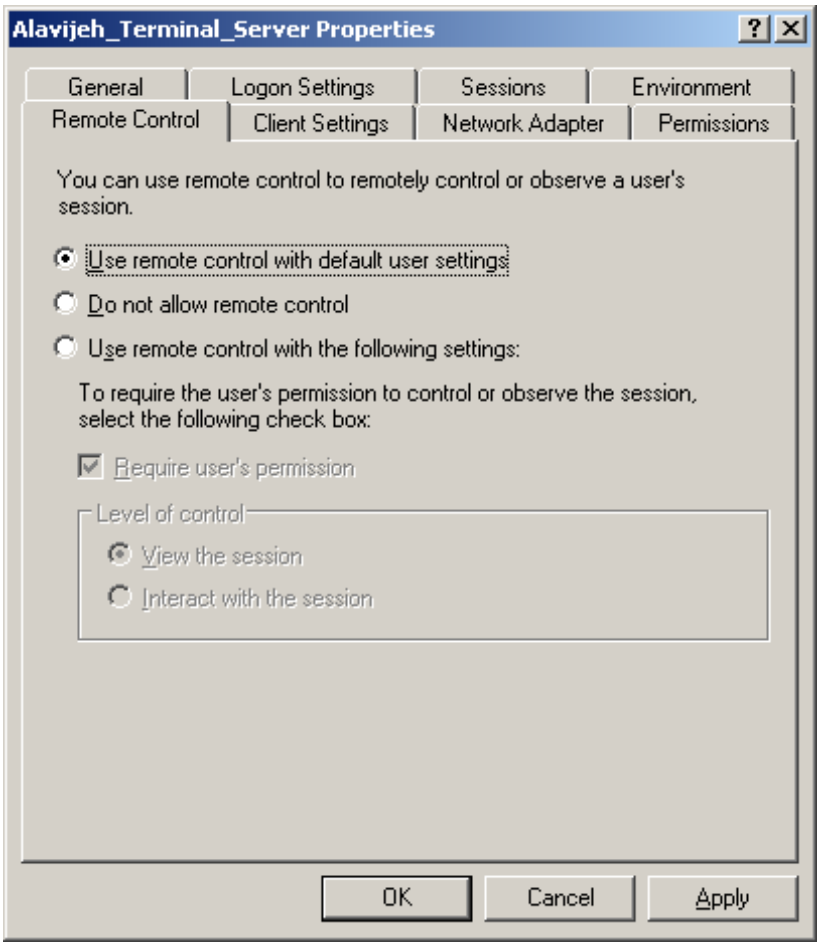
از طریق این قسمت می‌توان مشخص کرد که با Login کردن کاربر از راه دور، برنامه خاصی اجرا شود. قسمت‌های Program path and file name و Start in را به صورت زیر می‌توانید وارد نمایید (Start in همان Program path and file name ولی بدون نام فایل اجرایی است). لزوم وجود Start in را در بالاتر توضیح داده‌ایم.

توجه نمایید که با بستن برنامه، Session نیز بسته شده و کلاینت به صورت خودکار Log out خواهد شد.



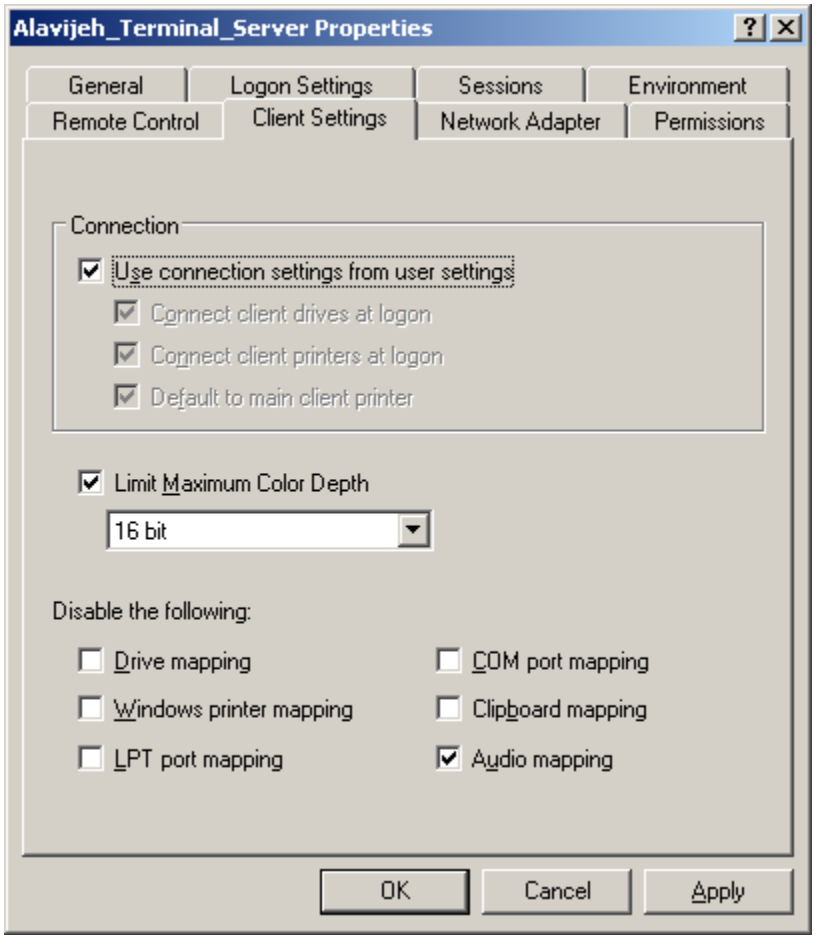
سربرگ Remote Control

در این صفحه نیز تنظیماتی را در مورد عدم پذیرش یا نحوه پذیرش Remote Control تعیین نمایید.



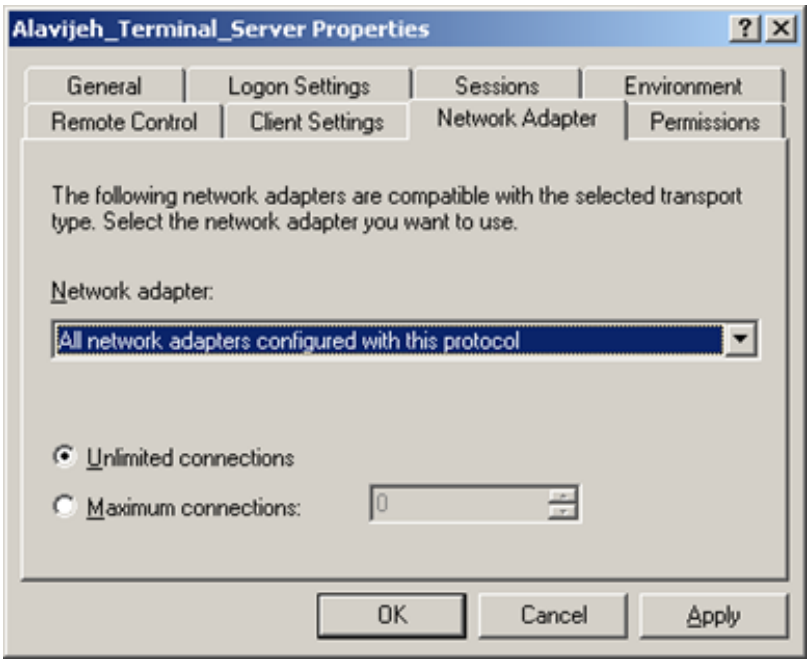
سربرگ Client Setting

در این صفحه می‌توان اطلاعات ارسال شده توسط Client به Server، مانند درایوها، چاپگر، وضوح تصویر و پورت‌های به کار گرفته شده توسط سخت‌افزارهای مختلف Client را فیلتر و انتخاب نمود.



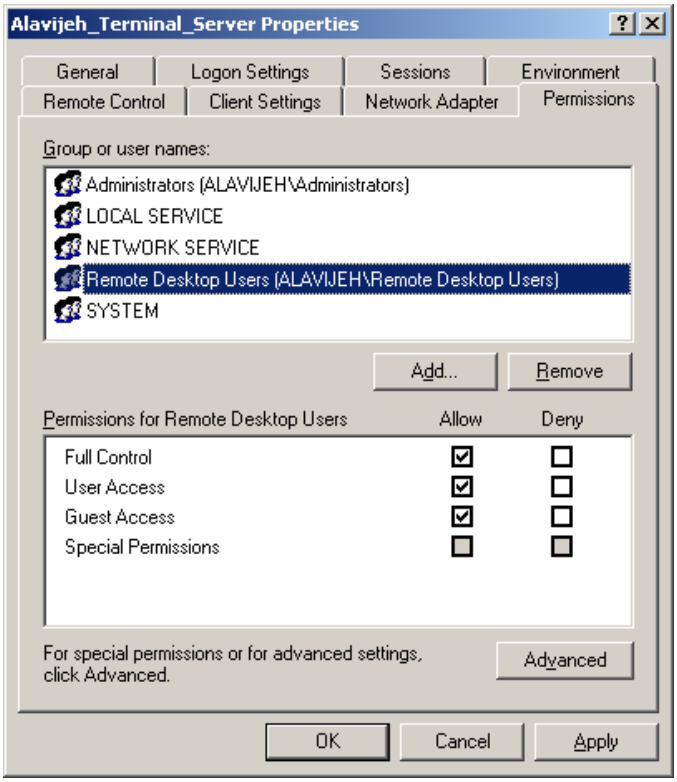
سربرگ Network Adapter

از طریق این صفحه می‌توان کارت شبکه دریافت کننده اطلاعات Remote، و نیز تعداد کاربرانی که به صورت همزمان قابلیت Login به سیستم را دارند را تعیین نمود.

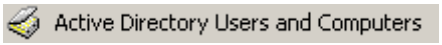


سربرگ Permissions

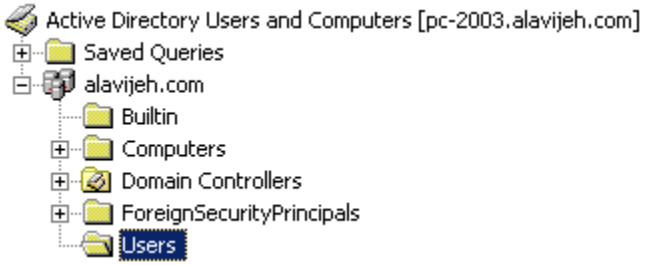
از طریق این صفحه می‌توانید مجوزهای لازم برای اتصال را تعیین نمایید.



تا این مرحله، شما تنظیمات لازم برای ساخت Connection را انجام دادهاید. این Connection وظیفه دریافت و مدیریت عملیات Remote را دارد. اما این مراحل کافی نیست. شما نیاز دارید کاربرانی را تعیین نمایید تا توسط آن‌ها به صورت Remote به سیستم Login کنید. **نکته** مهم این است که فقط کاربرانی حق ورود به صورت Login دارند که عضو دو گروه **Remote Desktop** و **Domain Admins** باشند. بنابراین بایستی کاربر مورد نظر را به گروه‌های فوق اضافه کنید. بدین منظور از مسیر Start، گزینه Administrative Tools ➔ Active Directory Users and Computers را انتخاب نمایید.



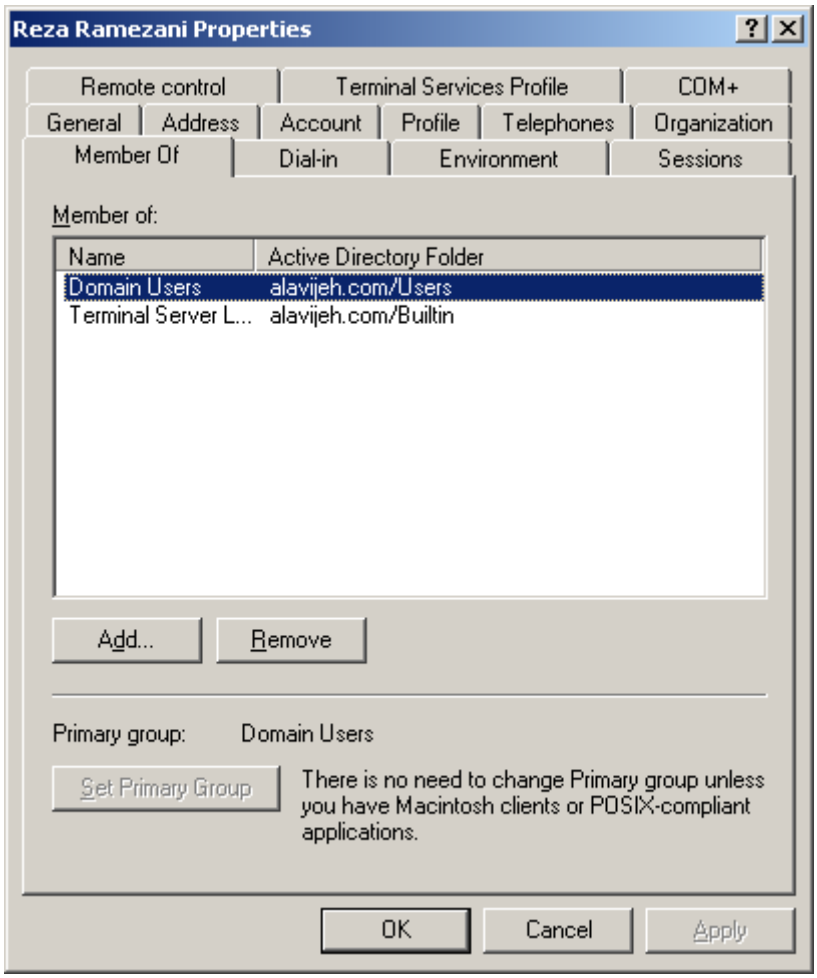
در این صفحه، روی قسمت Users کلیک کنید تا لیست کاربران و گروه‌های موجود را ببینید.



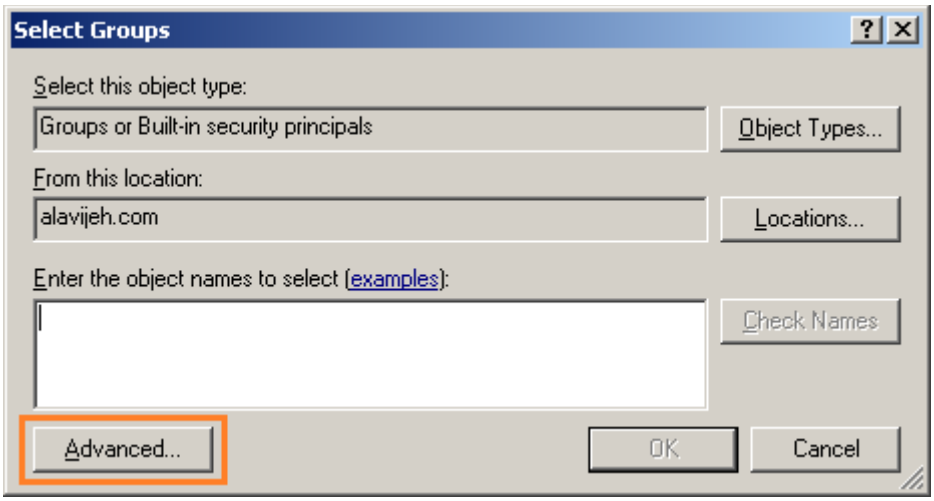
سپس روی کاربر مورد نظر راست کلیک کرده و گزینه Properties را انتخاب نمایید.



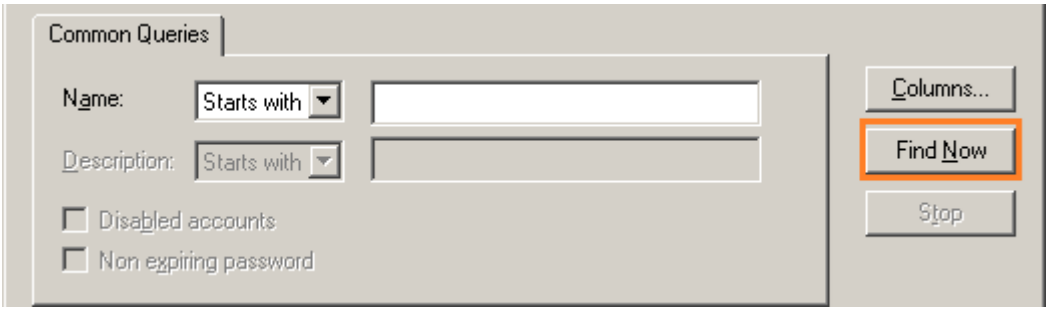
سپس در صفحه باز شده، وارد سربرگ Member of شوید. برای عضویت این کاربر در گروهی خاص، روی دکمه Add کلیک کنید.



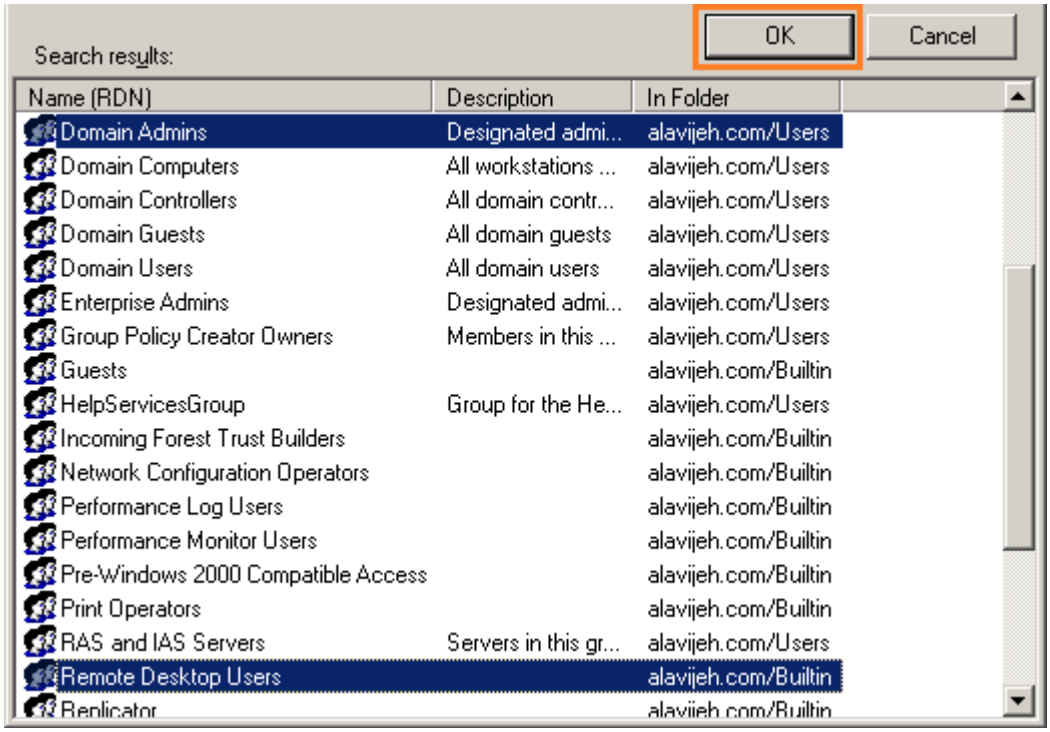
در صفحه باز شده، دو راه پیش رو دارید. راه اول وارد کردن متن Remote Desktop Users;Domain Admins و سپس کلیک روی دکمه Check Names است. راه دیگر انتخاب دو گروه فوق به صورت Visual (بصری) است. بدین منظور روی دکمه Advanced کلیک کنید.



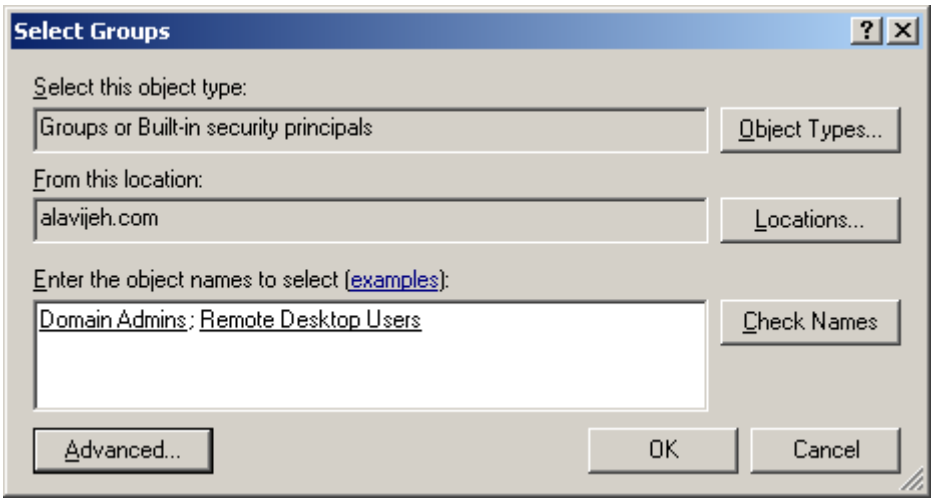
در صفحه باز شده، روی دکمه Find Now کلیک کنید تا لیست گروه‌های سیستم نمایان شود.



پس از نمایان شدن لیست گروه‌ها، دو گروه Remote Desktop Users و Domain Admins را انتخاب کرده و روی دکمه OK کلیک کنید.



در صفحه زیر، نام دو گروه انتخاب شده را مشاهده می‌کنید. روی دکمه OK کلیک کنید.



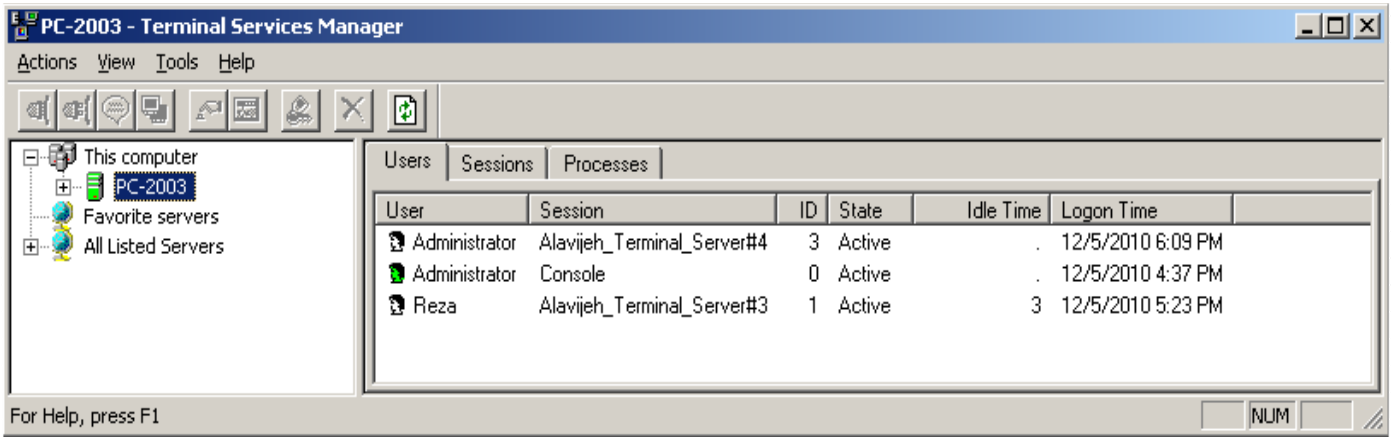
با انجام این امور می‌توانید، توسط کاربر انتخاب شده در فوق به صورت Remote به سیستم دسترسی یابید. برای این دسترسی از نرم‌افزار Remote Desktop استفاده نمایید.

۳۱-۳-۲- *Terminal Service Manager*

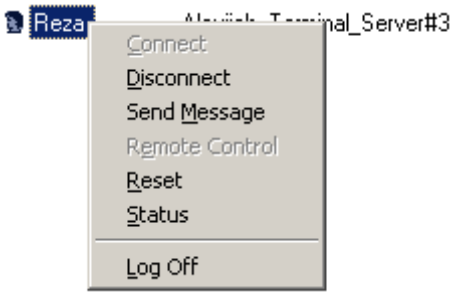
در معرفی Terminal Server گفتیم که یکی از مزایای Terminal Server، قابلیت مدیریت کاربران Login کرده به سیستم می‌باشد. یعنی در Server می‌توان کاربرانی را که به صورت Remote به Server وارد شده‌اند را مدیریت کرد. بدین منظور از ابزار Terminal Service Manager استفاده می‌کنیم. برای دسترسی به این ابزار، از مسیر Start ➔ Administrative Tools، گزینه Terminal Service Manager را انتخاب نمایید.



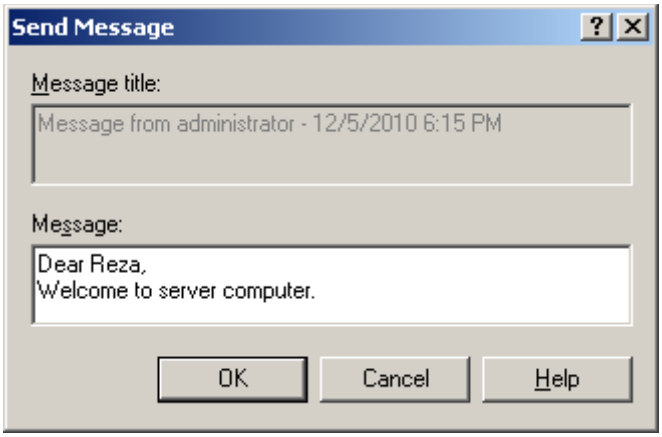
با انتخاب این برنامه، صفحه‌ای مانند زیر باز می‌شود. اگر از قسمت سمت چپ و بخش This Computer، نام Server را انتخاب کنید، مانند شکل زیر نام کاربران Login کرده را مشاهده خواهید کرد. در این شکل، ما توسط کاربر Administrator به صورت Local (محلی – ورود به سیستم به صورت مستقیم) و توسط کاربران Administrator و Reza به صورت Remote به سیستم Login کرده‌ایم. آن هایی که در قسمت Session، کلمه Console قرار گیرد، بیانگر کاربرانی می‌باشد که به صورت Local به سیستم وارد شده اند؛ اما بقیه بیانگر کاربرانی می‌باشد که به صورت Remote به سیستم وارد شده‌اند.



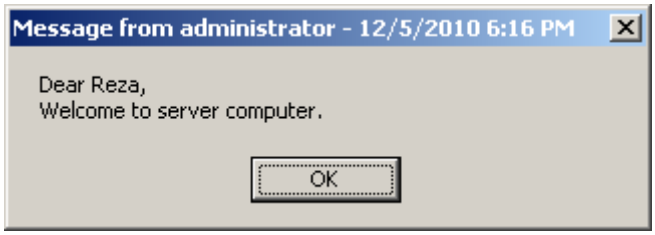
با راست کلیک روی نام کاربر، انواع عملیات قابل انجام را خواهید دید. این عملیات عبارتند از قطع ارتباط، ارسال پیغام به کاربر، Reset کردن ارتباط، مشاهده وضعیت کاربر و اخراج (Log Off) کاربر.



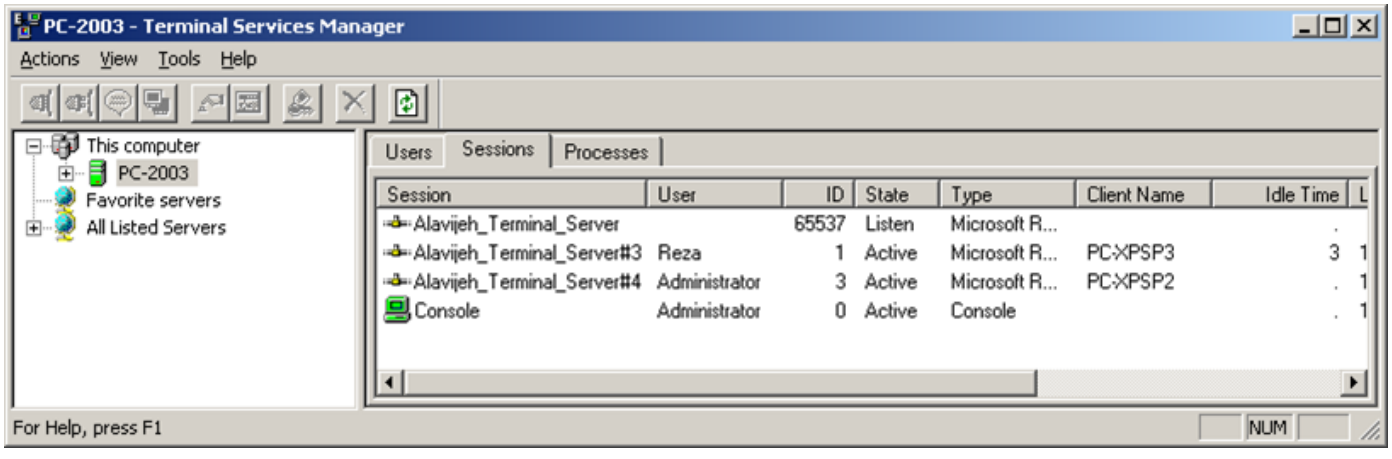
یکی از کاربردهای ارسال پیغام، هشدار دادن به کاربر و توجه دادن کاربر به این موضوع است که ما کارهای کاربر را مشاهده نموده و مراقب او هستیم. پس از راست کلیک کردن روی نام کاربر و انتخاب گزینه Send Message، صفحه زیر نمایان می‌شود. پس از وارد کردن پیغام، روی دکمه OK کلیک کنید.



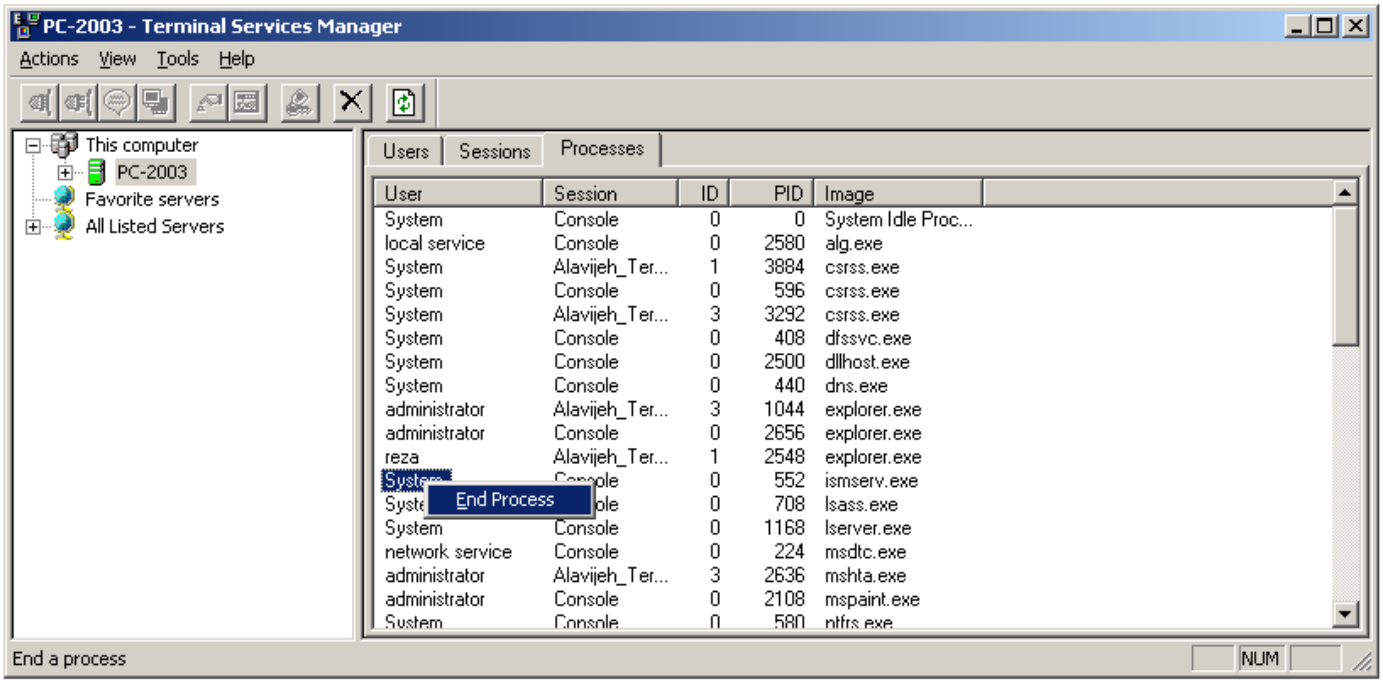
پس از این کار، کاربر راه دور، مانند شکل زیر پیام شما را مشاهده خواهد نمود.



اگر در همین صفحه، وارد سربرگ Session شوید، لیست Sessionهای (جلسه – نشست) ایجاد شده را مشاهده خواهید نمود.



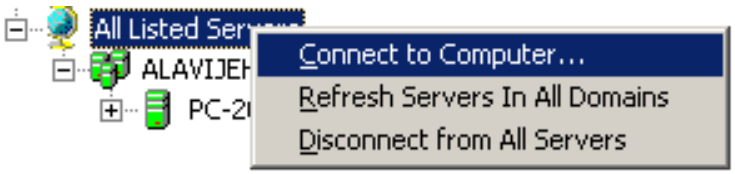
در همین صفحه، اگر وارد سربرگ Processes شوید، لیست تمام پردازش هایی که کاربران راه دور روی سیستم شما اجرا کرده‌اند را مشاهده خواهید نمود. ستون User بیانگر نام کاربری می‌باشد که این پردازش را اجرا کرده است. برای بستن یک پردازش، روی آن راست کلیک کرده و گزینه End Process را انتخاب نمایید.



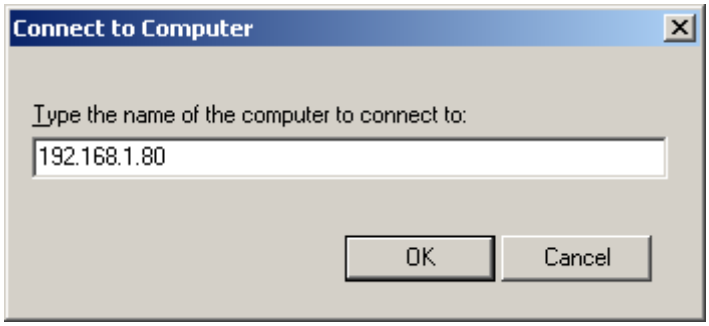
در قسمت سمت چپ، گزینه‌ای تحت عنوان All Listed Servers وجود دارد. در این قسمت لیست Serverهایی که دارای Terminal Server بوده و به آن متصل شده‌ایم را مشاهده خواهید نمود.



برای اتصال به Serverی دیگر که دارای Terminal Server می‌باشد، روی All Listed Servers راست کلیک کرده و گزینه Connect to Computer را انتخاب کنید.



در صفحه باز شده، نام یا آدرس IP کامپیوتر Server را وارد کرده و روی OK کلیک کنید. پس از اتصال قابلیت کنترل Server انتخاب شده را خواهید داشت.



۳۱-۴- Remote Assistance

قابلیت Remote Assistance، به معنای دستیار از راه دور، وسیله‌ای است که از آن برای کنترل و ایجاد تغییرات در یک رایانه دیگر به کار می‌رود. به طور کلی این قابلیت برای استفاده توسط اشخاصی است که قرار است رایانه هایشان را از طریق اینترنت به یکدیگر متصل کنند تا یکی به عنوان مددکار و دیگری به عنوان درخواست کننده عمل کنند. اما مددکار کیست؟ شخصی که با رایانه اش به عنوان یک متخصص یا تعمیرکار نرم‌افزار کامپیوتر، توسط درخواست کننده در قالب یک فرم به نام Invitation (دعوتنامه) فراخوانده می‌شود. متاسفانه این قابلیت فقط در ویندوز XP وجود دارد و لازمه استفاده از آن، موجود بودن ویندوز XP در هر دو رایانه است. به طور کلی در همه شرایط و در تمامی برنامه‌های Remoting، یک برنامه Client و یک برنامه Server وجود دارد. در این نوع برنامه‌ها کاربر درخواست کننده که گاهی Assist نامیده می‌شود با ایجاد و ارسال یک Invitation از طریق یک Email (که در واقع یک دعوتنامه به صورت فایل می‌باشد) برای رایانه مددکار ارسال می‌کند. کاربر مددکار با باز کردن Email و اجرای فایل Invitation (دعوتنامه) به صورت خودکار به سیستم درخواست کننده متصل خواهد شد.

۳۱-۴-۱- طریقه فعال سازی *Remote Assistance*

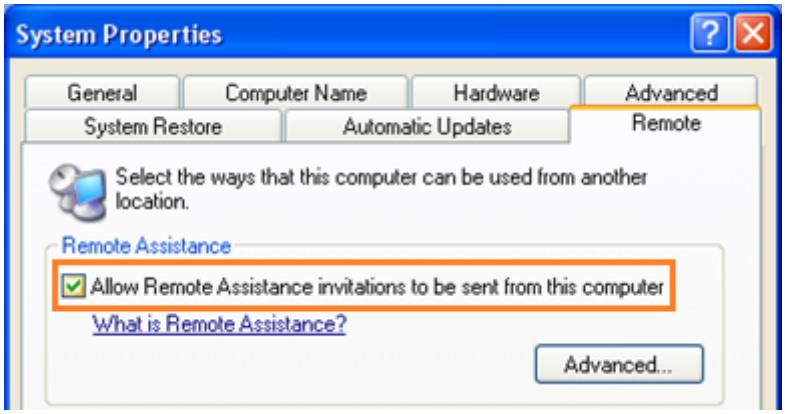
کاربری که Invitation تولید می‌کند قبل از استفاده از ابزار Remote Assistance و ایجاد فایل دعوتنامه می‌بایست در تنظیمات ویندوز این قابلیت را فعال نماید تا کاربر مددکار بدون هیچ مشکلی به آن سیستم وصل شده و به رفع عیوب بپردازد. برای دسترسی به تنظیمات فعال سازی Remote Assistance مسیرهای متفاوتی وجود دارد که در ابتدا نیاز به پنجره System Properties داریم.

۱. مسیرهای متفاوت آن شامل System ➔ Control Panel ➔ Start یا از طریق کلیک راست کردن روی My Computer و انتخاب Properties می‌باشد.

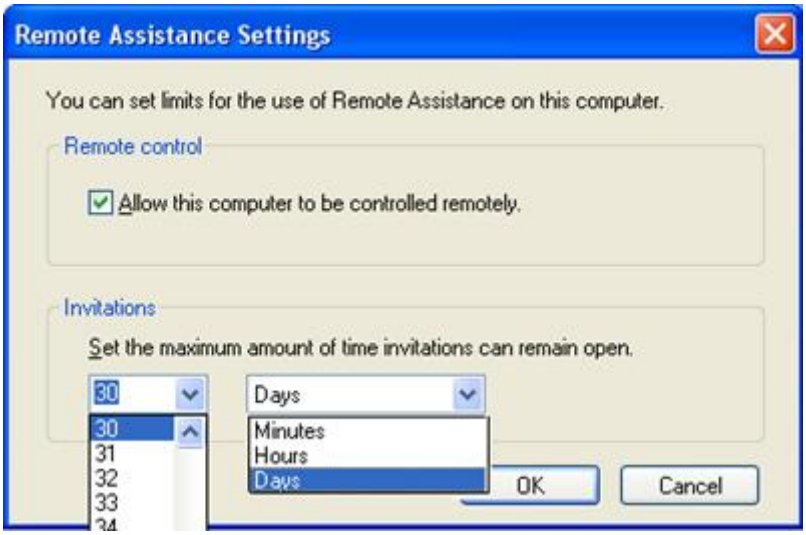


۲. در پنجره System Properties برگه Remote را انتخاب می‌کنیم. همانطور که مشاهده می‌کنید ابتدای برگه از ما درخواست شده که نوع ارتباط از موقعیت‌های دیگر را انتخاب کنیم. از فرم اول (Remote Assistance)، چک

باکس allow Remote Assistance Invitation to be sent from this computer را تیک دار می‌کنیم. در اینصورت از این پس اجازه استفاده از این قابلیت داده می‌شود که شامل ارسال دعوتنامه می‌شود:



۳. روی دکمه Advanced در همین پنجره کلیک کرده و در پنجره Remote Assistance Setting گزینه Allow this computer to be controlled Remotely. را تیک دار کنید. با این عمل به کامپیوتر مددکار اجازه می‌دهید که جهت رفع عیوب به سیستم شما متصل شود. هر دعوتنامه‌ای که برای رایانه مددکار می‌فرستید دارای اعتبار و میزان مدت زمان مشخص شده می‌باشد که این زمان همانطور که در شکل ملاحظه می‌کنید بر حسب تعداد ساعت، روز و ماه از فرم Invitation در همین پنجره قابل تنظیم می‌باشد:



۳۱-۴-۲- نکات مهم حین استفاده از Remote Assistance

۱. هنگام اتصال Firewall سیستم باید غیر فعال باشد تا هنگام اتصال از طریق پورت‌های سیستم عامل مشکلی در اتصال به وجود نیاید.

۲. کاربر مبتدی هنگامی که فرم Invitation را پر می‌کند می‌بایست به اینترنت متصل باشد.

۳. بعد از اتمام فرم و تولید فایل مربوطه مشخصات IP شما در این فایل ثبت می‌شود تا بعد از اجرای فایل توسط مددکار، وی امکان اتصال به رایانه درخواست کننده را داشته باشد.

۴. پس از تولید فایل دعوتنامه تا هنگام اتصال به مددکار، درخواست کننده نباید از اینترنت Disconnect شود؛ زیرا در صورت استفاده نکردن از IP ثابت، با هر بار اتصال به اینترنت و ISP مربوطه، سرویس DHCP (که وظیفه توزیع IP

را دارد) یک IP جدید تولید کرده که با مشخصات فایل ارسال شده برای مددکار متفاوت است و مددکار نمی‌تواند رایانه شما را از طریق فایلتان پیدا کند.

۵. در صورت استفاده از IP ثابت مانعی برای قطع اتصال اینترنت و اتصال مجدد وجود ندارد. بهترین کار این است که درخواست کننده و مددکار از طریق Online شدن و با نرم‌افزارهای Messenger بتوانند از متصل بودن یکدیگر به اینترنت مطلع شوند.

۳۱-۴-۳- روش ایجاد یک Invitation (دعوتنامه) توسط درخواست کننده

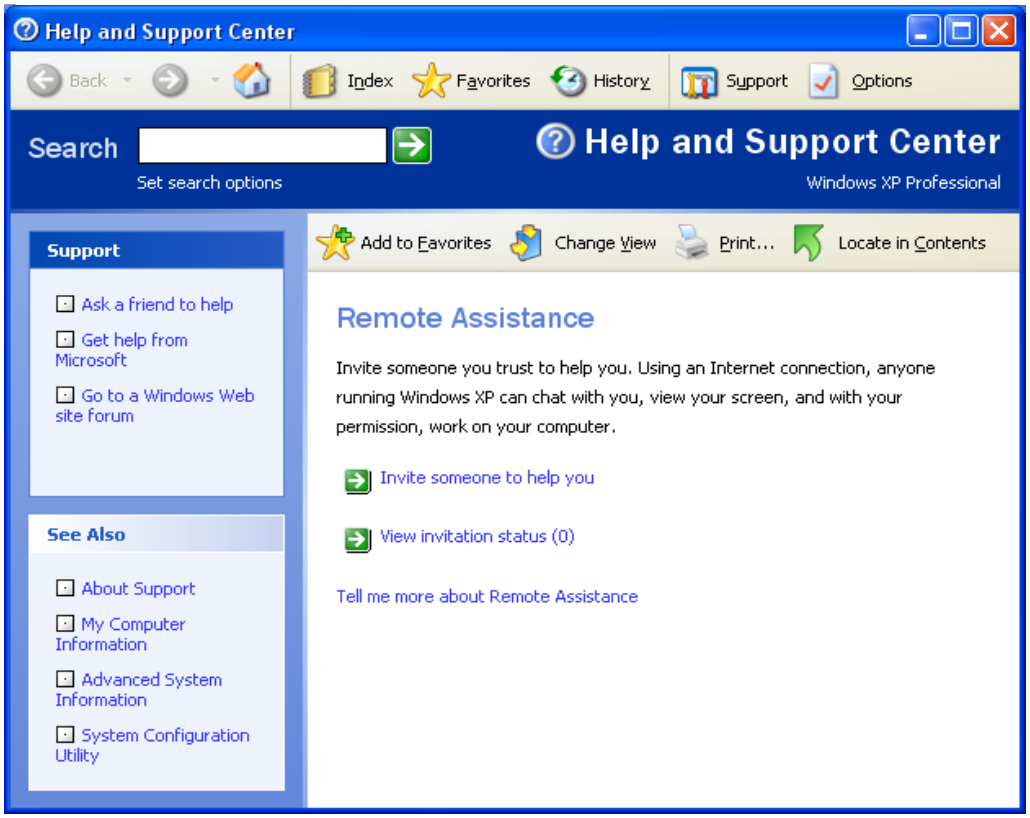
برای ایجاد یک دعوتنامه توسط درخواست کننده ابتدا باید از اتصال به اینترنت اطمینان حاصل کرد. سپس از دو روش می‌توان به Remote Assistance دسترسی داشت:

روش اول: Start ➔ All Programs ➔ Remote Assistance

روش دوم: فشردن دکمه F1 و وارد به پنجره Help اصلی ویندوز و در قسمت Ask for Assistance انتخاب گزینه اول:

Help Invite a friend to connect to your computer with Remote Assistance

پس از طی هر کدام از مسیرهای بالا پنجره Help مربوط به Remote Assistance ظاهر می‌شود:



در این صفحه اگر قبلاً دعوتنامه‌ای ایجاد نکرده باشید، روبروی گزینه View Invitation status مقدار صفر (۰) نمایش داده خواهد شد. برای ایجاد دعوتنامه در همین پنجره روی گزینه Invite someone to help you کلیک کنید.

۳۱-۴-۴- انواع روش ساخت دعوتنامه

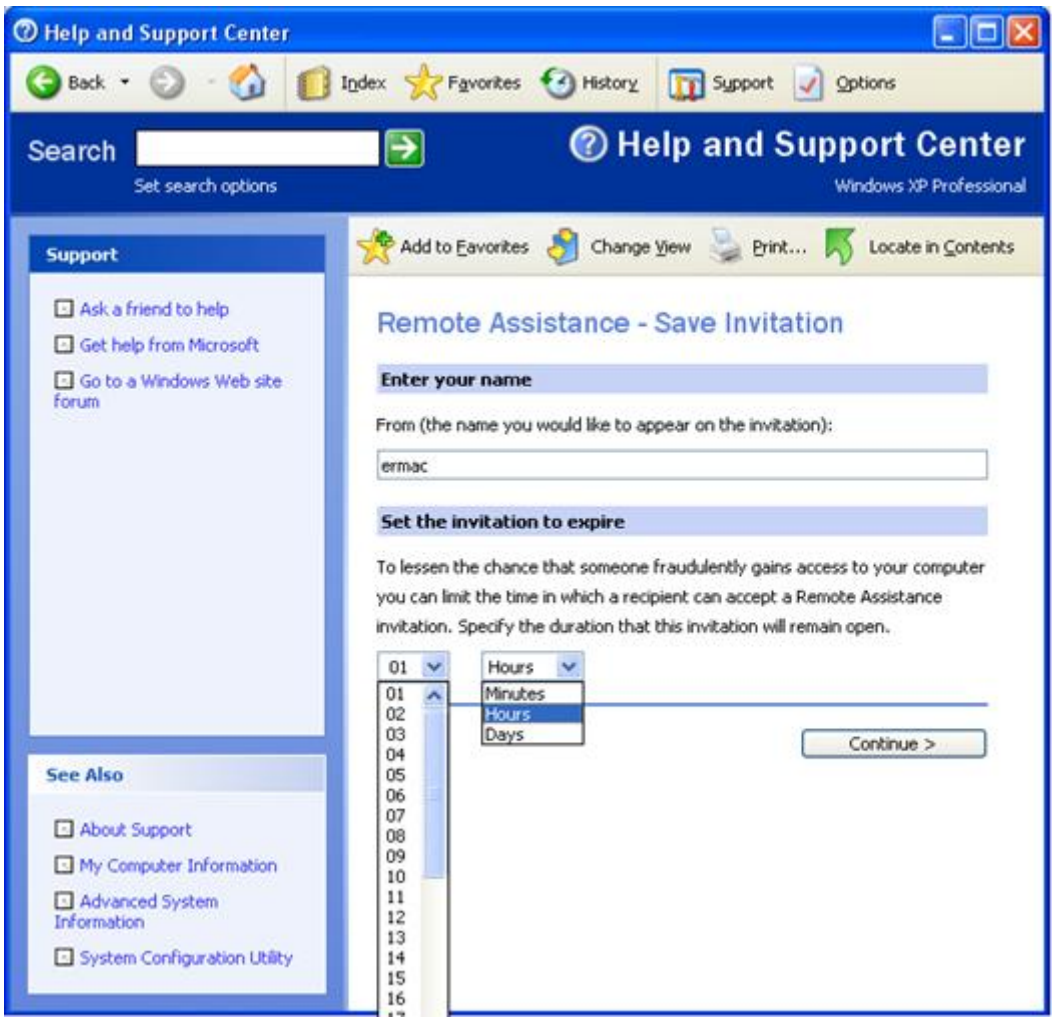
ساخت دعوتنامه در محیط Help با سه روش زیر امکانپذیر است:

۱. روش اول استفاده از Windows Messenger می‌باشد. کاربر درخواست کننده باید یک حساب در سایت Hotmail یا MSN داشته باشد و بعد از Sing In شدن و پر کردن فرم مربوط به دعوتنامه قابلیت ارسال آن را به شخص مددکار خواهد داشت.

۲. در روش دوم درخواست کننده از نرم‌افزار Outlook Express برای ارسال فرم دعوتنامه استفاده می‌کند که قبل از استفاده از آن می‌بایست تنظیمات کلی مبنی بر سرور SMTP مربوطه اعمال شود.

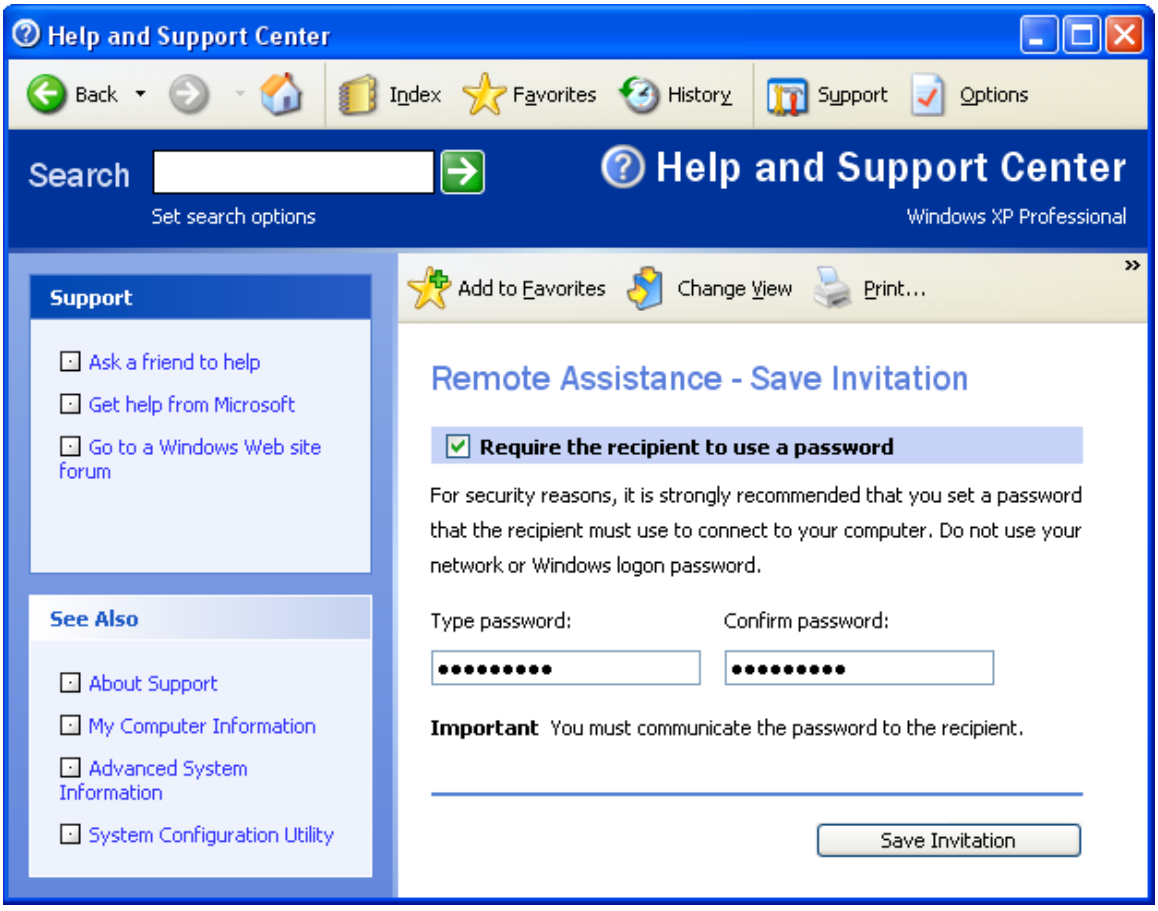
۳. روش سوم و بهترین روش استفاده از گزینه Save Invitation As A File (Advanced) می‌باشد که با استفاده از این روش، سیستم فایلی را با عنوان RAInvitation.msrcinccident و به حجم بسیار ناچیز (حدود ۱Kbyte) تولید می‌کند. کاربر درخواست کننده به راحتی به سیستم ایمیل خود مانند Yahoomail، Gmail و... وصل شده و این فایل را به یک نامه Attach کرده (روش اتصال یک فایل به متن یک ایمیل) و به آدرس ایمیل مددکار ارسال می‌کند. در دو روش اول و دوم، Windows Messenger و Outlook Express بطور خودکار یک ایمیل تولید می‌کنند و این فایل به آن Attach شده و ارسال می‌شود اما روش سوم به صورت دستی و Attach کردن آن به هر ایمیل به هر آدرسی امکانپذیر است.

پس از انتخاب روش سوم (روش پیشنهادی برای ادامه کار) و ایجاد فایل مذکور پنجره زیر ظاهر خواهد شد:

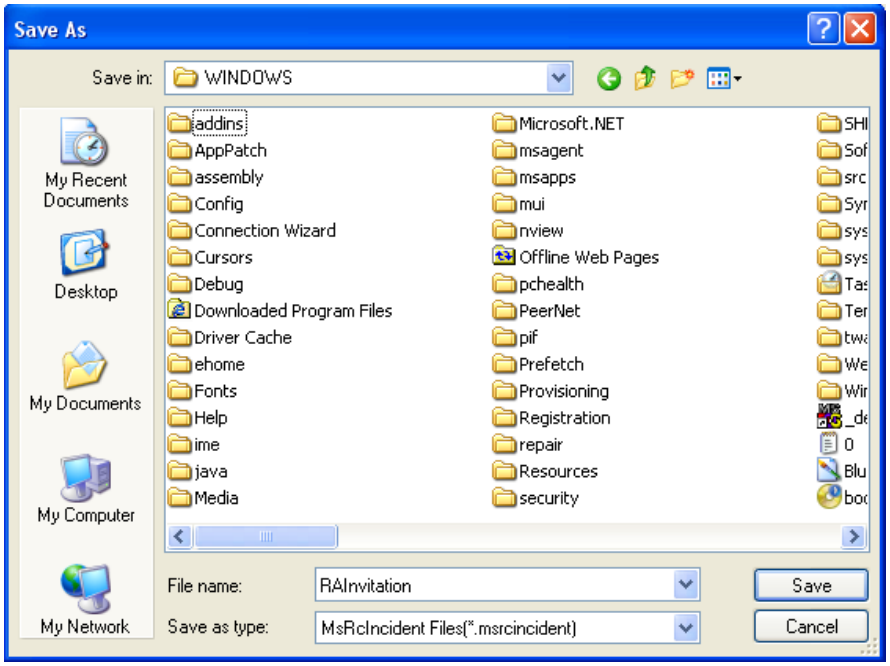


در این پنجره شما باید نام و مدت زمان اعتبار دعوتنامه خود را مشخص کنید. مدت زمان اعتبار دعوتنامه به صورت تعداد دقیقه، ساعت و روز تنظیم می‌شود. در واقع پس از به پایان رسیدن این مدت زمان ارتباط به طور خودکار قطع شده و اعتبار دعوتنامه از بین خواهد رفت. در این حالت مددکار برای برقراری ارتباط مجدد نیاز به یک دعوتنامه جدید از طرف درخواست کننده دارد.

با تکمیل پنجره بالا و انتخاب دکمه Continue، پنجره زیر ظاهر می‌شود:



در این پنجره کاربر درخواست کننده با انتخاب یک Password برای دسترسی و اتصال کاربر مددکار به فرم انتخاب می‌کند که البته این رمز باید از قبل در اختیار مددکار قرار گذاشته شده باشد. پس از انتخاب رمز و فشردن دکمه Save Invitation پنجره محاوره‌ای Save As ایجاد شده که از شما درخواست انتخاب یک مسیر مناسب برای ذخیره فعلی فایل RAInvitation را دارد:

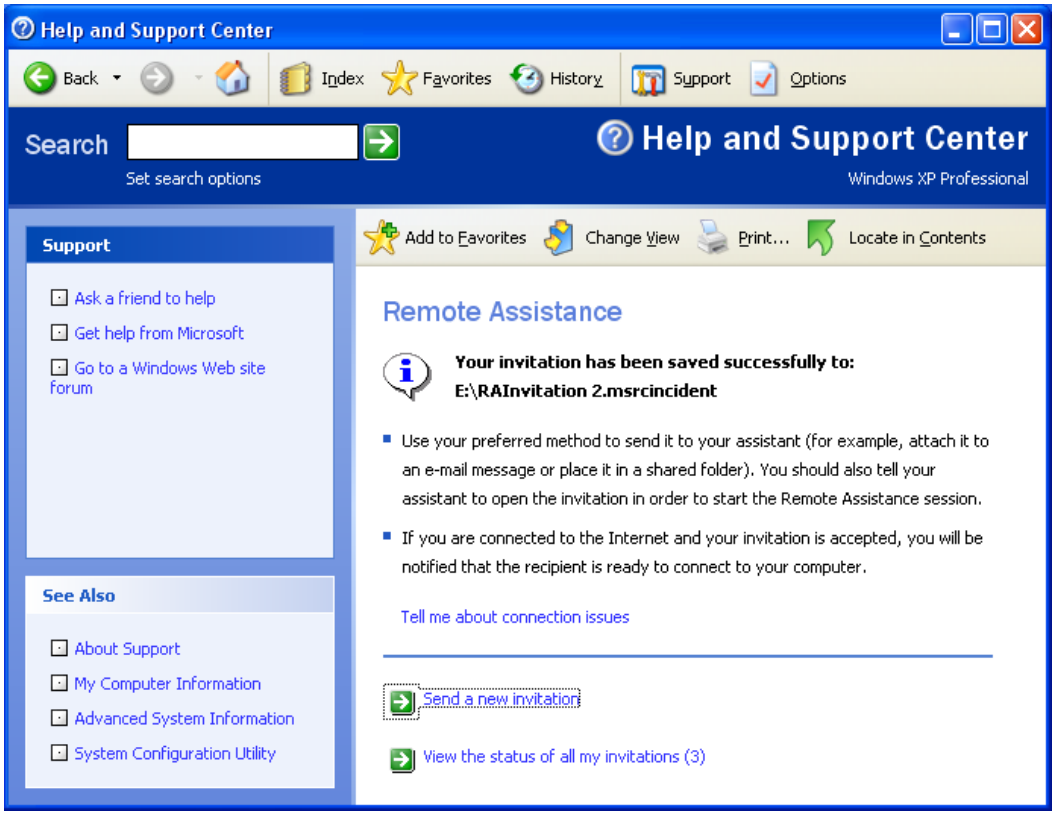


آیکون فایل ساخته شده و ذخیره شده به شکل زیر می‌باشد:

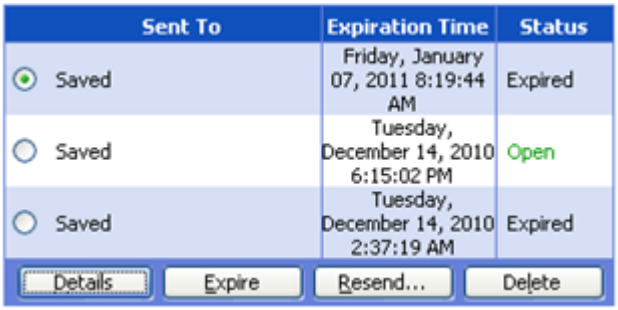


RAInvitation

پس از انتخاب مسیر مورد نظر برای ذخیره فایل دعوتنامه پنجره زیر ظاهر می‌شود که عدد مقابل گزینه view the status of all my Invitation (به عنوان مثال در اینجا ۳) نشان دهنده تعداد فایل‌های درخواست تولید شده است:

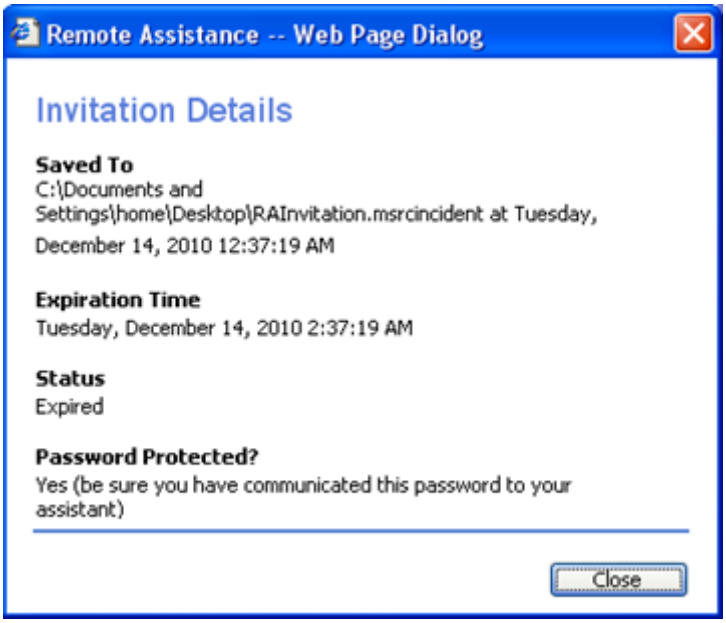


با انتخاب همین گزینه می‌توان تعداد و جزییات فایل‌های ساخته شده را در پنجره زیر مشاهده کرد:



در این پنجره تعداد سه فایل ساخته شده با روش سوم مشاهده می‌شود که با انتخاب هر کدام از فایل‌ها می‌توان آن‌ها را:

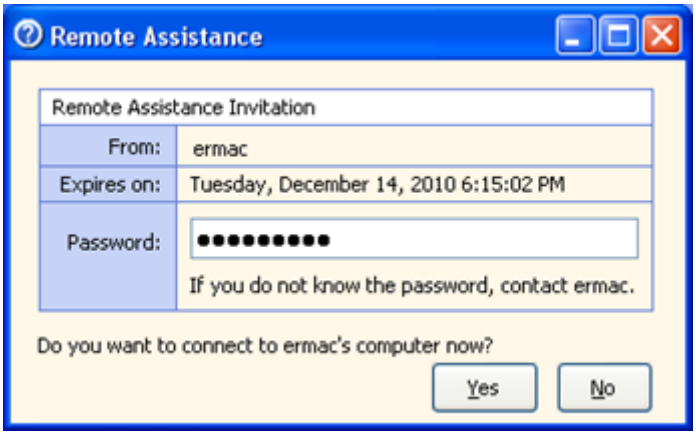
- با دکمه Delete آن را حذف نمود.
- با دکمه Resend... تعویض نام و رمز و مدت اعتبار برای ارسال مجدد فایل Expire شده، (Expired فایلی است که اعتبار آن تمام شده است)
- با دکمه Expire، آن را غیر معتبر نمود.
- و با استفاده از دکمه Details وضعیت فایل را در پنجره‌ای دیگر مشاهده کرد که شامل محل ذخیره سازی فایل، تاریخ به پایان رسیدن اعتبار، وضعیت در حال حاضر فایل و در نهایت یک تائیدیه Password که در یک پنجره درج می‌شود. پنجره زیر مربوط به Details فایل سوم می‌باشد:



پس از مشاهده فایل دعوتنامه، آماده ارسال با هر روشی (ایمیل– فلش و...) به مددکار می‌باشد.

۳۱-۴-۵- روش استفاده از فایل Invitation توسط مددکار

حال وظیفه مددکار پس دریافت دعوتنامه چیست؟ کاربر مددکار فایل RAInvitation را دریافت می‌کند. در ابتدا باید از Online بودن درخواست کننده مطلع شود که از طریق Windows Messenger می‌تواند این هماهنگی را با درخواست کننده ایجاد کند. پنجره زیر که همان Invitation (دعوتنامه) می‌باشد، شامل محل ورود Password درخواست کننده است که مددکار با فشردن yes متصل می‌شود.



۳۱-۴-۶- تفاوت‌های Remote Desktop و Remote Assistance

سوال مطرح شده درباره این دو قابلیت شبیه به هم ویندوز این است که چرا مایکروسافت هر دو قابلیت را در یک نرم‌افزار قدرتمند ارایه نکرده و تفاوتهای آن‌ها در چیست؟

اولین تفاوت در روش استفاده و ارتباط کاربر Client و کاربر Server می‌باشد. نرم‌افزار Remote Desktop یک ابزار ویرایش شده از نرم‌افزار Terminal Server در ویندوز ۲۰۰۳ می‌باشد. در این نرم‌افزار رایانه درخواست کننده که قسمت Server را در اختیار دارد می‌بایست از ویندوز نسخهXP یا ۲۰۰۳ استفاده کند ولی رایانه مددکار که به عنوان Client عمل می‌کند می‌تواند از هر سیستم عاملی استفاده کند. به عنوان مثال اگر مددکار از ویندوز ۹۸ استفاده کند، تنها با قرار دادن سی دی ویندوز XP در سی دی رام و نصب نرم‌افزار Set Up Remote Desktop Connection از گزینه Perform Additional Tasks می‌تواند از این ابزار جهت اتصال استفاده کند. اما نرم‌افزار Remote Assistance فقط در ویندوز XP وجود دارد و رایانه درخواست کننده و مددکار بالاجبار می‌بایست از این سیستم عامل استفاده کنند. برنامه Remote Assistance نیازی به ابزار Client ندارد و خودش به عنوان Server-Client عمل می‌کند، به این صورت که مددکار از یک درخواست در قالب XML استفاده می‌کند که با خاصیت XML نیازی به نصب نرم‌افزار اضافی مانند Remote Desktop Connection نمی‌باشد.

نکته دیگر Authentication یا تشخیص هویت کاربر در این سیستم‌ها می‌باشد. کاربران برای استفاده از Remote Desktop باید در ویندوز سیستمی که قرار است به آن متصل شوند، یک Account تعریف شده داشته دارند. این Account توسط Administrator (یا همان مدیر سیستم) به صورت دستی و با مجوزهای مشخص با یک کد کاربری و Password ثبت می‌شود که تشخیص هویت کاربر متصل شونده به سیستم از طریق سیستم تشخیص ویندوز صورت می‌گیرد. اما در Remote Assistance تشخیص هویت به گونه‌ای دیگر انجام می‌گیرد، در این اتصال کاربر مددکار، نیازی به داشتن Account در ویندوز ندارد. کاربر درخواست کننده که اقدام به تولید Invitation برای کاربر مددکار می‌کند در هنگام پر کردن فرم دعوتنامه یک Password تعیین می‌کند که این رمز خود به صورت رمز نگاری شده و با پسوند msrcincident ذخیره می‌شود. این فایل به هر روشی که به مددکار برسد برای اتصال به سیستم درخواست کننده حتما باید از کلمه عبور تعیین شده استفاده شود که در غیر اینصورت ارتباطی بر قرار نخواهد شد.

به هر حال، این دو نرم‌افزار محدودیت هایی نیز دارند. برای حل این محدودیت‌ها، در ادامه به معرفی نرم‌افزاری به نام Team Viewer خواهیم پرداخت. تنها عیب این نرم‌افزار، پولی بودن ما است که البته چقدر هم ما برای نرم‌افزارهایمان پول پرداخت می کنیم!!!!!

۳۱-۵- Team Viewer

۳۱-۵-۱- معرفی نرم‌افزار *Team Viewer*

نرم‌افزار Team Viewer که محصولی از شرکت GmbH می‌باشد، نرم‌افزاری است که به ما اجازه می‌دهد از طریق اینترنت و بدون نیاز به داشتن آدرس IP از نوع Valid، به یک سیستم راه دور وصل شد و آن را کنترل کرد. تنها لازمه این کار، نصب نرم‌افزار در هر دو سیستم است. منطق کار آن نیز بدون صورت است که ابتدا سیستم‌ها را به اینترنت وصل می‌نماییم. سپس نرم‌افزار Team Viewer را در هر دو سیستم اجرا می کنیم. این نرم‌افزار به صورت خودکار یک نام کاربری و یک رمز عبور تولید می کند. هر کدام از کامپیوترها با داشتن نام کاربری و رمز عبور تولید شده در کامپیوتر دیگر، قابلیت اتصال به آن را پیدا خواهد نمود.

ممکن است در مورد امنیت این اتصالات نیز برایتان سوال مطرح شود. در مورد بحث امنیت، به جز بحث‌های امنیتی در پیاده سازی، این سه گزینه قابل ارائه است:

۱) اتصال تنها در صورت باز بودن نرم‌افزار Team Viewer بر قرار می‌شود. لذا با بستن این نرم‌افزار، اتصال نیز قطع خواهد شد. همچنین اگر نرم‌افزار بسته باشد، قابلیت اتصال مجدد نیز وجود ندارد.

۲) نام کاربری که برای هر کامپیوتر تولید می‌شود، با هر بار باز شدن نرم‌افزار Team Viewer ثابت می‌ماند. اما با هر بار بازکردن این نرم‌افزار، رمز عبور تولیدی عوض خواهد شد و رمز عبور تولید شده قبلی از بین خواهد رفت و منقضی خواهد شد.

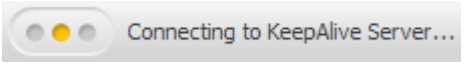
۳) هنگام کنترل سیستم راه دور، کاربر راه دور تمامی حرکات شما را می‌تواند ببیند. اگر به یاد داشته باشید این امکان در Remote Desktop Connection وجود نداشت.

مجددا یادآوری می کنم که مزیت بزرگ این نرم‌افزار این است که هیچ نیازی به داشتن آدرس IP از نوع Valid نداریم. نکته منفی این نرم‌افزار این است که در یک شبکه محلی قابل استفاده نیست.

۳۱-۵-۲- راه اندازی نرم‌افزار *Team Viewer* و کار با آن

در ادامه به سروری که قرار است سیستم راه دور را کنترل کند، سرور و به سیستمی که کنترل خواهد شد، Client می گوییم.

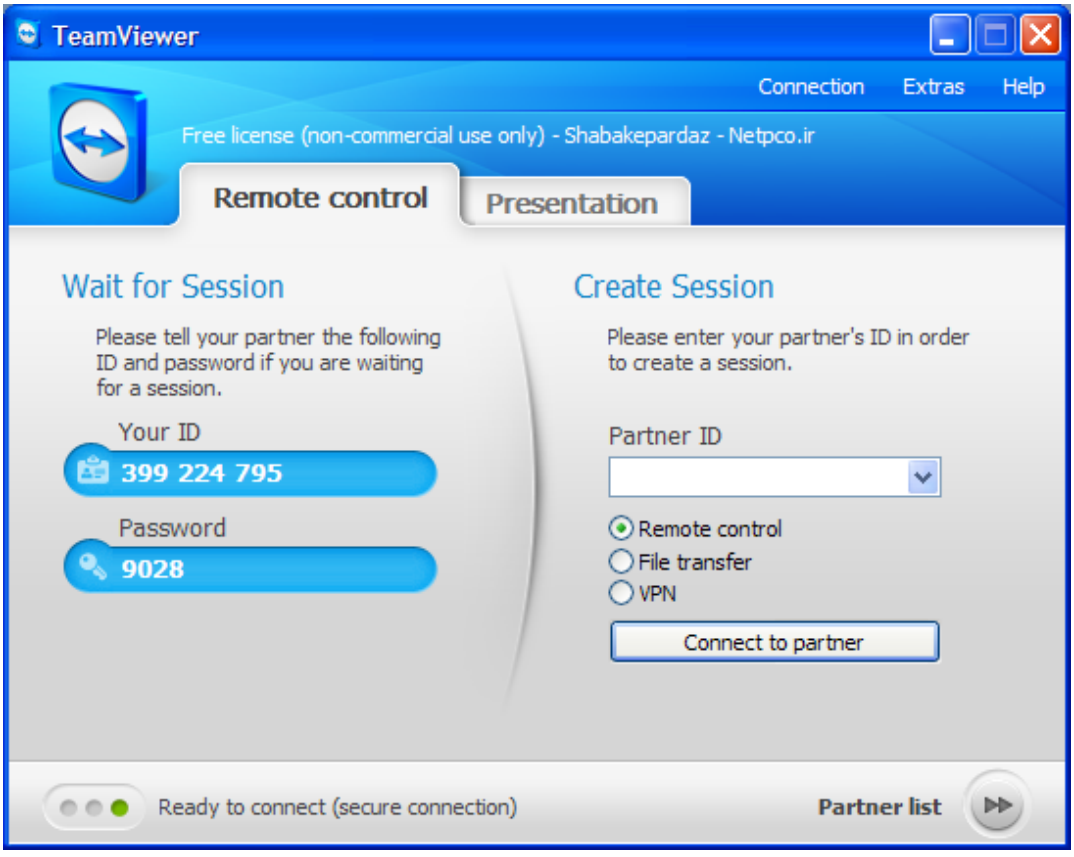
جهت کار با نرم‌افزار Team Viewer و اتصال به یک سیستم راه دور و کنترل آن، ابتدا هر دو سیستم را به اینترنت متصل نموده و سپس Team Viewer را باز نمایید. صبر نمایید تا هر دو سیستم جهت تولید نام کاربری و رمز عبور به سرور شرکت سازنده متصل شوند.



پس از اتصال، سیستم یک نام کاربری و یک رمز عبور تولید خواهد کرد. شکل زیر تصویر نام کاربری و رمز عبور تولید شده در سرور را نشان می‌دهد:



شکل زیر نیز تصویر نام کاربری و رمز عبور تولید شده در Client را نشان می‌دهد:



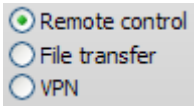
سپس نام کاربری تولید شده در Client را در قسمت Partner ID در سرور وارد نموده و روی دکمه Connect To Partner کلیک کنید.



صبر نمایید تا عمل اتصال به پایان برسد.



همانطور که از شکل بالا پیداست، سه راه جهت اتصال به یک سیستم راه دور وجود دارد:



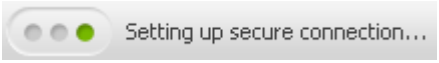
۱) Remote Control: قابلیت کنترل کامپیوتر راه دور را می‌دهد. دقیقا مانند اینکه پشت آن سیستم راه دور نشسته باشیم. البته این گزینه قابلیت File Transfer و VPN را نیز به صورت همزمان ما می‌دهد.

۲) File Transfer: صفحه‌ای باز شده و امکان انتقال فایل بین Client و Server را می‌دهد.

۳) VPN: اتصال به شبکه‌ای که کامپیوتر راه دور به آن شبکه متصل است. جهت یادگیری مفاهیم بیشتر در مورد VPN به فصل DialUP & VPN مراجعه نمایید.

ما گزینه Remote Control را انتخاب کردیم.

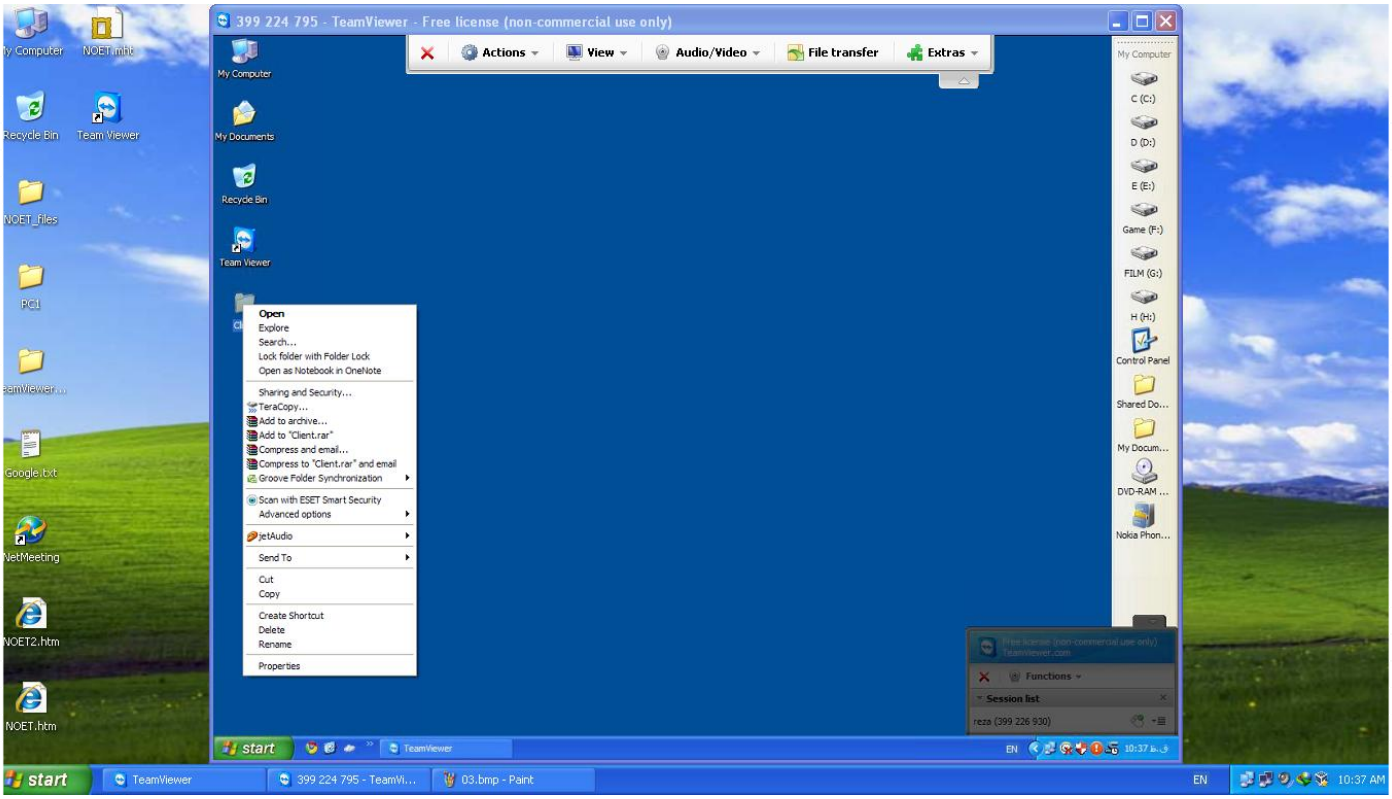
قبل از انجام اتصال، سرور سعی می‌کند که اتصال را به یک اتصال امن تبدیل کند.



پس از این تبدیل، سرور رمز عبور Client را از شما خواهد پرسید. کلمه عبوری که در Client تولید شده است را وارد نموده و روی Log On کلیک کنید. در اینجا من رمز عبور را ۹۰۲۸ وارد کردم.

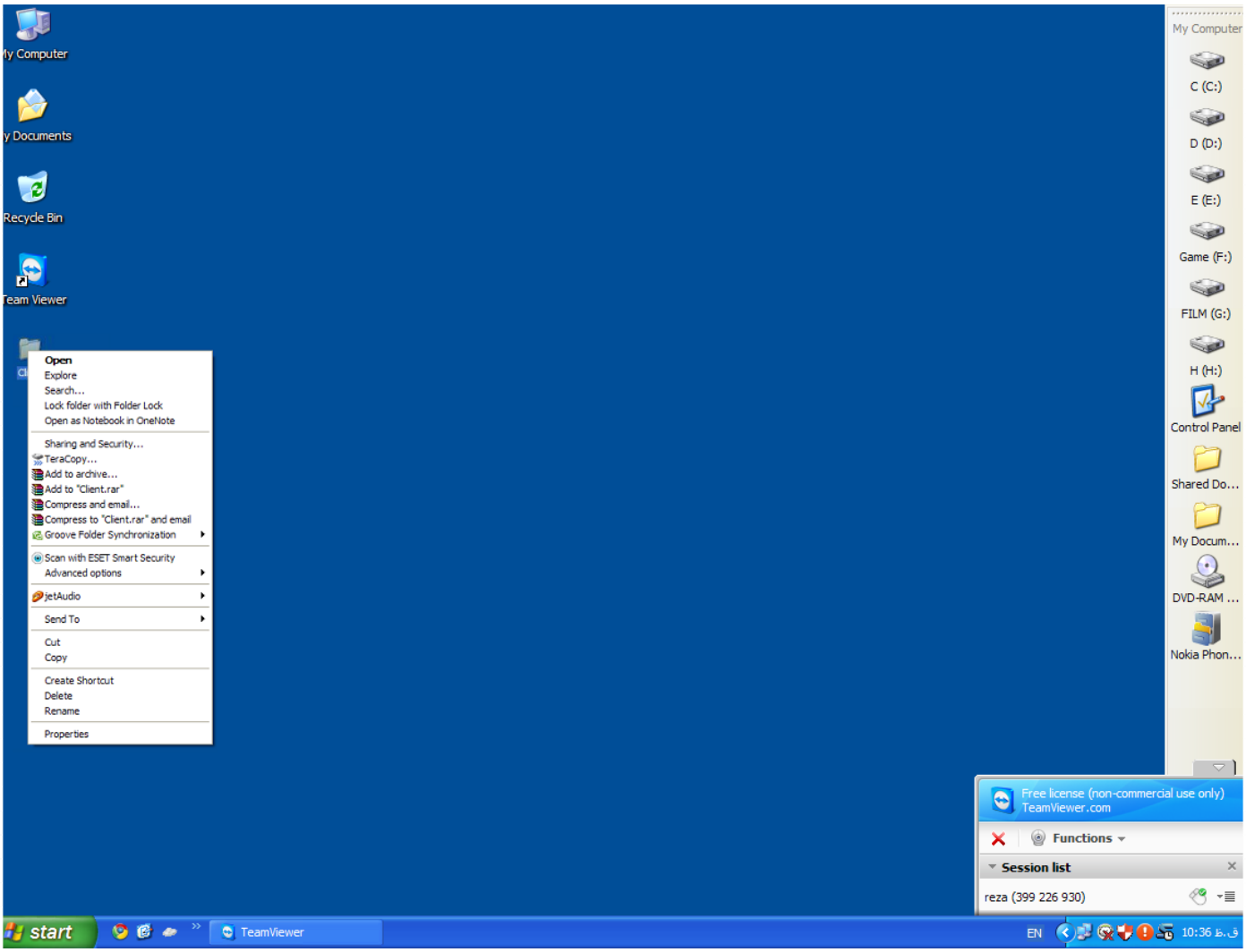


اگر رمز عبور صحیح باشد، اتصال بین Client و Server بر قرار شده و سرور خواهد توانست تا Client را کنترل کند. شکل زیر صفحه دسکتاپ سرور را نشان می‌دهد و صفحه باز شده در وسط نیز صفحه دسکتاپ Client را نشان می‌دهد. همانطور که پیداست، دقیقا مانند اینکه به صورت فیزیکی پشت کامپیوتر Client نشسته باشید، می‌تواند ان را کنترل کنید.



همانطور که در بالا نیز گفتیم، جهت امنیت بیشتر، کامپیوتر Client تمامی حرکات شما را می‌تواند ببیند. شکل زیر صفحه دسکتاپ Client را نشان می‌دهد که چگونه می‌تواند رفتارهای شما را مشاهده نماید.

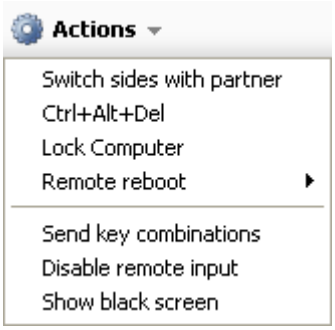
همانطور که در پایین صفحه و سمت راست مشاهده می‌نمایید، نرم‌افزار Team Viewer باز بوده و نشان می‌دهد که اکنون کاربری با نام کاربری Reza و شماره کاربری ۳۹۹۲۲۶۹۳۰ به شما متصل بوده و در حال کنترل شما می‌باشد. جهت بستن اتصال می‌توانید روی دکمه Close که قرمز رنگ است کلیک کنید.



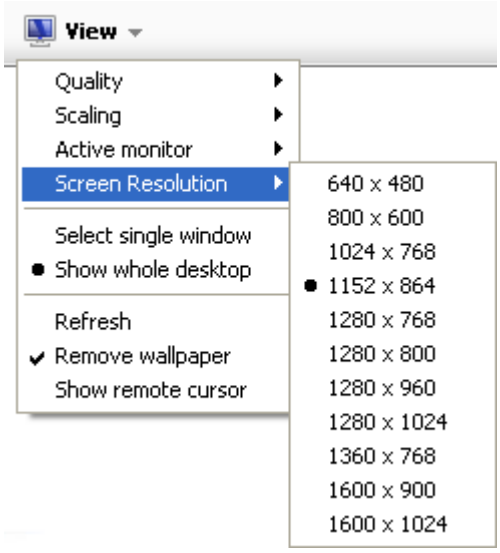
مجددا به سرور باز می‌گردیم. در بالای صفحه، تعدادی ابزار وجود دارد. جهت قطع اتصال، بر روی دکمه Close که در بالای صفحه قرار دارد، کلیک کنید.



منوی Actions نیز امکاناتی را در اختیار قرار می‌دهد. امکاناتی چون اجرای CtrlA+lt+Del در Client، قفل نمودن Client، راه اندازی مجدد و خاموش کرده Client، ارسال کلیدهای ترکیبی به Client و...



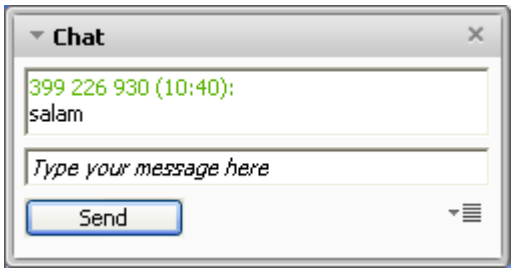
منوی View نیز امکاناتی را جهت نمایش بهتر صفحات به ما می‌دهد. امکاناتی چون کیفیت تصاویر ارسالی، نرخ نمونه برداری از صفحه، رزولوشن صفحه و....



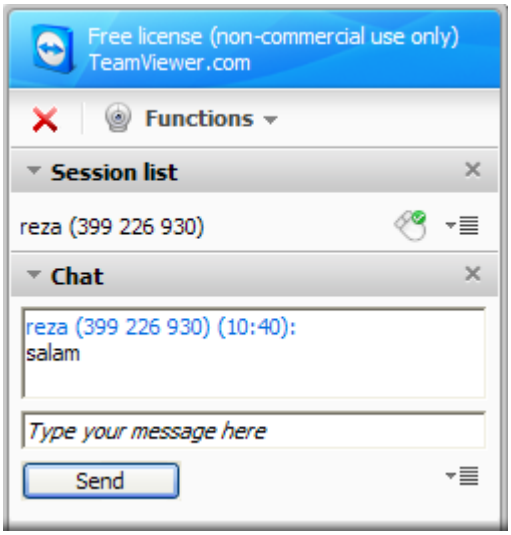
منوی Audio/Video نیز امکان برقراری ارتباط صوتی، تصویری و نوشتاری (Chat) را به ما می‌دهد.



مثلا با انتخاب گزینه چت می‌توان با Client چت نمود. من پیغام Salam را به Client فرستادم. شکل زیر، صفحه چت در سرور را نشان می‌دهد:



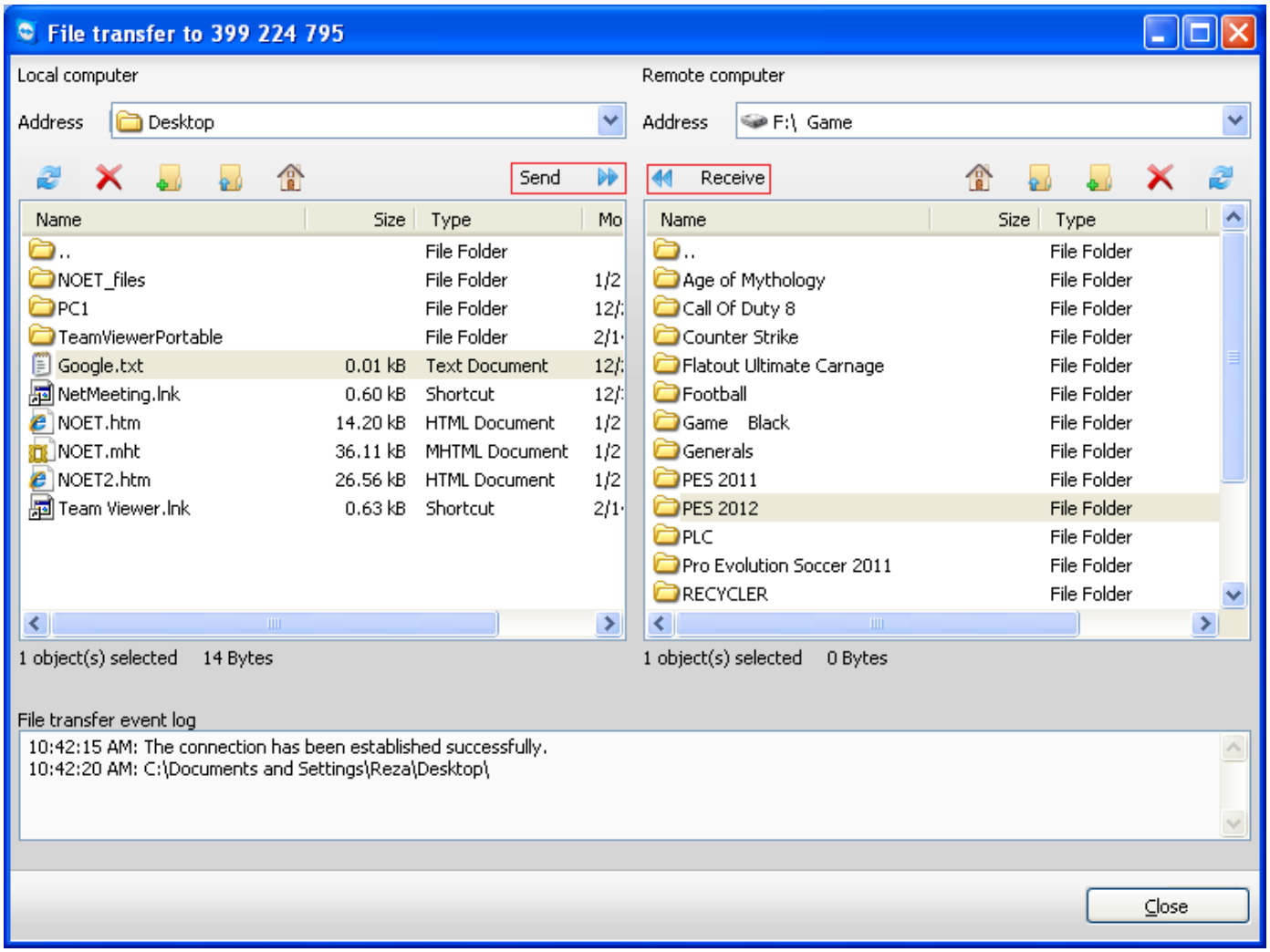
شکل زیر نیز صفحه چت در Client را نشان می‌دهد.



منوی بعدی نیز گزینه File Transfer است که امکان انتقال فایل بین Client و Server را به ما می‌دهد.

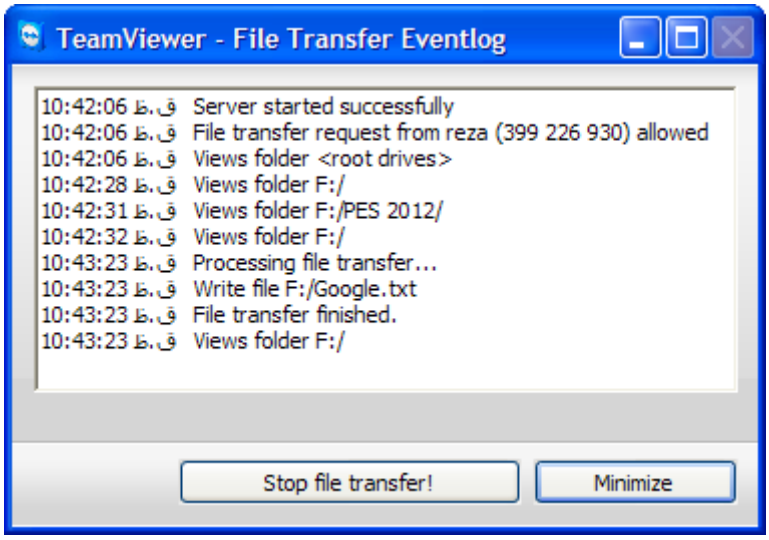


با انتخاب منوی File Transfer، صفحه زیر باز می‌شود. البته اگر هنگام اتصال به سیستم راه دور، به جای گزینه Remote Control، گزینه File Transfer را انتخاب می‌کردیم، مستقیم صفحه زیر را مشاهده می‌نمودیم.

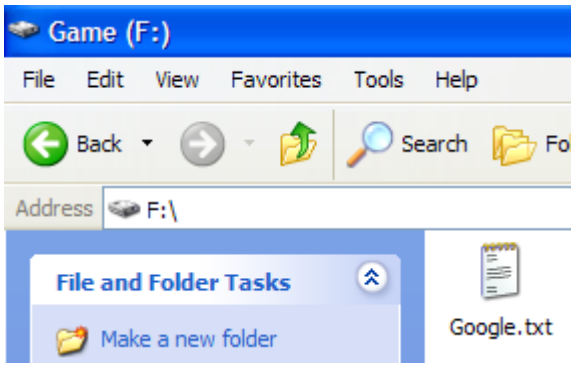


پنل سمت چپ، فایل‌های کامپیوتر سرور و پنل سمت راست، فایل‌های کامپیوتر Client را نشان می‌دهد. با انتخاب یک فایل از کامپیوتر سرور و کلیک روی دکمه Send، می‌توان آن فایل را به کامپیوتر سرور و محلی که پنل سمت راست به آن اشاره می‌کند ارسال نمود. همچنین با انتخاب یک فایل از Client و کلیک روی دکمه Receive، می‌توان آن فایل را از Client دریافت نموده و روی سرور کپی کرد.

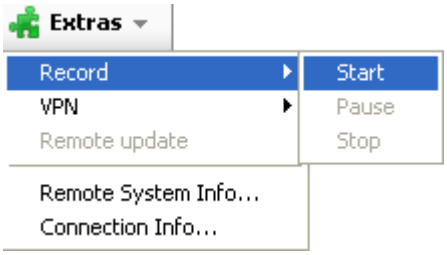
به عنوان مثال، من فایل Google.txt را توسط دکمه Send به درایو F:\ کامپیوتر Client کپی کردم. Client می‌تواند در همان لحظه تمامی حرکات سرور در کار با File Transfer را مشاهده کند. هنگام کار با File Transfer و کپی فایل به درایو F:\، اطلاعات زیر در کامپیوتر Client نمایش داده شده است:



همچنین می‌بینید که فایل با موفقیت به درایو F:\ در Client کپی شده است:

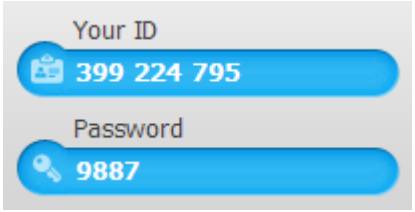


در نهایت منوی Extras نیز امکانات اضافه دیگری، همچون ضبط کارهای انجامی و نیز VPN را در اختیار قرار می‌دهد.



همانطور که دیدید، نرم‌افزار Team Viewer بسیار ساده و پر قدرت می‌باشد.

در انتها نرم‌افزار Team Viewer را در Client، یکبار بستم و مجددا اجرا نمودم. همانطور که مشاهده می‌کنید رمز عبور آن برای بار دوم عوض شد، اما نام کاربری تغییری نکرد:

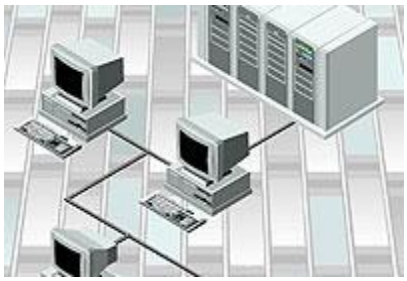


فصل ۳۲

اتصال از راه دور

(VPN , Dial UP)

۳۲-۱- چگونه از راه دور به شبکه خانگی خود متصل شویم؟



همانطور که تاکنون متوجه شدهاید، کامپیوترهای موجود در یک شبکه محلی، قابلیت تعامل با یکدیگر را دارند. بدین معنا که می‌توانند با یکدیگر ارتباط برقرار کرده و کاربران هر سیستم، از منابع دیگر سیستم‌ها استفاده نمایند. لازمه این کار این است که سیستم‌ها به صورت فیزیکی یا غیر فیزیکی (Wireless) به یکدیگر متصل شده باشند. اما آیا تاکنون به این فکر افتادهاید که سیستمی که کیلومترها از شما فاصله دارد، با اینکه اتصالی به شبکه شما ندارد، چگونه می‌تواند به شبکه شما متصل شده، جزئی از Workgroup شما به حساب آمده و از منابع سیستم شما استفاده کند؟ همچنین گاهی اوقات شما از یک PC دور هستید اما واقعاً نیاز دارید که به فایل‌ها و یا اسناد موجود بر روی آن دسترسی پیدا کنید. احتمالاً پس از انجام یک سفر متوجه شدهاید که فایل مهمی را جا گذاشتهاید. همچنین ممکن است یکی از اعضای خانواده نیاز به کمک شما برای انجام کاری روی PC منزل داشته باشد که اگر در منزل می‌بودید، این کار را در زمان ۳۰ ثانیه انجام می‌دادید.

در اینگونه شرایط، باید به سراغ فناوری دسترسی از راه دور بروید. به عبارت ساده تر، این فناوری شامل استفاده از یک کامپیوتر برای دسترسی به فایلهای ذخیره شده بر روی یک کامپیوتر دیگر و یا حتی کنترل آن می‌باشد. با ابزارهای مناسب و

کمی آگاهی می‌توانید از یک PC برای مشاهده و تعامل با دسکتاپ ویندوز یک PC دیگر در آن سوی جهان بهره گیری نمائید.

ما در این فصل به بررسی دو تکنیک مشهور دسترسی از راه دور خواهیم پرداخت، یکی VPN و دیگری Dial-UP.

نکته‌ای که بین هر دو روش اتصال وجود دارد، این است که برای برقراری ارتباط بین دو سیستم، نیاز به اتصال اینترنت دارید. منظور ما در اینجا یک اتصال اینترنت باند پهن است. در صورتیکه هنوز به یک اتصال Dial-up متکی هستید، ارتباط شما برای انجام اینگونه اقدامات بیش از حد کند خواهد بود.

توجه نمایید که برای برقراری ارتباط بین یک کامپیوتر با یک شبکه، حتما یکی از کامپیوترهای شبکه بایستی به اینترنت یا خط تلفن دسترسی داشته باشد. کامپیوتر راه دور، به همین کامپیوتر شبکه متصل خواهد شد.

به انجام این عمل، شبکه خصوصی مجازی می‌گویند. یک شبکه خصوصی مجازی (VPN,VPDN) بسط و توسعه یک شبکه محلی و خصوصی، به گونه‌ای است که اتصالات شبکه‌های اشتراکی یا عمومی مانند اینترنت را در بر می‌گیرد (یعنی کاربران شبکه‌های عمومی مانند اینترنت را قادر می‌سازد تا به شبکه خصوصی و محلی شما متصل شوند). یک شبکه خصوصی مجازی شما را قادر می‌کند اطلاعات را بین دو کامپیوتر در طول یک شبکه اشتراکی یا عمومی بفرستید، در حالتی که با خصوصیات یک اتصال خصوصی نقطه به نقطه یا به عبارتی نظیر به نظیر برابری بکند.

شبکه خصوصی مجازی (Virtual Private Network) و نیز شبکه خصوصی شماره گیری مجازی (Virtual Private Dialup Network) (در مورد این دو گزینه، بعدا بیشتر توضیح می‌دهیم) در اذهان، تصور یک مطلب پیچیده برای استفاده و پیاده کنندگان آن به وجود آورده است. اما این پیچیدگی، در مطالب بنیادین و مفهومی آن است نه در پیاده سازی.

این نکته را باید بدانید که پیاده سازی دارای روش خاصی نبوده و هر سخت‌افزار و نرم‌افزاری روش پیاده سازی خود را دارا است و نمی‌توان روش استانداردی را برای کلیه موارد بیان نمود. اما اصول کار همگی به یک روش است.

۳۲-۲- مفاهیم اولیه

مفهوم اصلی، چیزی جز برقراری یک کانال (Tunnel) ارتباطی خصوصی برای دسترسی کاربران راه دور به منابع شبکه نیست. در این کانال که بین دو نقطه برقرار می‌شود، ممکن است که از مسیرهای مختلفی عبور کند؛ اما کسی قادر به وارد شدن به این شبکه خصوصی شما نخواهد بود (مگر در صورت تایید اعتبار شدن کاربر). گرچه می‌توان از هر روشی برای اتصال استفاده نمود اما استفاده آن در خطوط Leased (خطوطی شخصی که توسط یک فرد اجاره شده باشد) کار غیر ضروری است. در ادامه به دلیل آن پی خواهید برد (منظور از Leased، مثلاً کابل کشی مستقیم بین دو کامپیوتر است).

در یک ارتباط، شبکه یا شبکه‌ها می‌توانند به کمک اینترنت به هم متصل شوند و از این طریق کاربران از راه دور، به راحتی به شبکه دسترسی پیدا کنند. اگر این روش (اتصال توسط اینترنت) را با روش خطوط اختصاصی فیزیکی (Leased) مقایسه کنیم، می‌بینید که ارائه یک ارتباط خصوصی از روی اینترنت به مراتب از هر روش دیگری ارزان‌تر تمام می‌شود.

از اصول دیگری که در یک شبکه در نظر گرفته شده بحث امنیت انتقال اطلاعات در این کانال مجازی می‌باشد. یک ارتباط می‌تواند بین یک ایستگاه کاری و یک شبکه محلی و یا بین دو شبکه محلی صورت گیرد. در بین هر دو نقطه یک تونل

ارتباطی برقرار می‌گردد و اطلاعات انتقال یافته در این کانال به صورت کد شده حرکت می‌کنند، بنابراین حتی در صورت دسترسی مزاحمان و هکرها به این شبکه خصوصی نمی‌توانند به اطلاعات رد و بدل شده در آن دسترسی پیدا کنند.

VPN -۳-۳۲

۳۲-۳-۱- شبکه VPN چیست؟

همزمان با عمومیت یافتن اینترنت، اغلب سازمان‌ها و موسسات ضرورت توسعه شبکه اختصاصی خود را به‌درستی احساس کردند. در ابتدا شبکه های اینترانت مطرح گردیدند.این نوع شبکه بصورت کاملا" اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده، قادر به ورود به شبکه و استفاده از منابع موجود می‌باشند. اخیراً، تعداد زیادی از موسسات و سازمان‌ها با توجه به مطرح شدن خواسته های جدید (کارمندان از راه دور، ادارات از راه دور)، اقدام به ایجاد شبکه های اختصاصی مجازیVPN (Virtual Private Network) نموده‌اند.

یک VPN، شبکه ای اختصاصی بوده که از یک شبکه عمومی (عموماً اینترنت)، برای ارتباط با سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می‌نماید. این نوع شبکه‌ها در عوض استفاده از خطوط واقعی نظیر خطوط Leased، از یک ارتباط مجازی به کمک اینترنت برای شبکه اختصاصی بمنظور ارتباط به سایت‌ها استفاده می‌کند.

۳۲-۳-۲- عناصر تشکیل دهنده یک VPN

دو نوع عمده شبکه های VPN وجود دارد:

- دستیابی از راه دور (Remote-Access): به این نوع از شبکه‌ها VPDN (Virtual private dial-up network)، نیز گفته می‌شود. در شبکه های فوق از مدل ارتباطی- User To-Lan (ارتباط کاربر به یک شبکه محلی) استفاده می‌گردد. سازمان‌هائی که از مدل فوق استفاده می‌نمایند، بدنبال ایجاد تسهیلات لازم برای ارتباط پرسنل (عموماً کاربران از راه دور و در هر مکانی می‌توانند حضور داشته باشند) به شبکه سازمان می‌باشند. سازمان‌هائی که تمایل به برپاسازی یک شبکه بزرگ " دستیابی از راه دور " می‌باشند، می‌بایست از امکانات یک مرکز ارائه دهنده خدمات اینترنت جهانی ESP (Enterprise service provider) استفاده نمایند. سرویس دهنده ESP، بمنظور نصب و پیکربندی VPN، یک NAS (Network access server) را پیکربندی و نرم‌افزاری را در اختیار کاربران از راه دور بمنظور ارتباط با سایت قرار خواهد داد. کاربران در ادامه با برقراری ارتباط قادر به دستیابی به NAS و استفاده از نرم‌افزار مربوطه به منظور دستیابی به شبکه سازمان خود خواهند بود.
- سایت به سایت (Site-to-Site): در مدل فوق یک سازمان با توجه به سیاست های موجود، قادر به اتصال چندین سایت ثابت از طریق یک شبکه عمومی نظیر اینترنت است. شبکه های VPN که از روش فوق استفاده می‌نمایند، دارای گونه های خاصی در این زمینه می‌باشند:
  - مبتنی بر اینترانت. در صورتیکه سازمانی دارای یک و یا بیش از یک محل (راه دور) بوده و تمایل به الحاق آن‌ها در یک شبکه اختصاصی باشد، می‌توان یک اینترانت VPN را بمنظور برقرای ارتباط هر یک از شبکه های محلی با یکدیگر ایجاد نمود.

- مبتنی بر اکسترانت. در مواردیکه سازمانی در تعامل اطلاعاتی بسیار نزدیک با سازمان دیگر باشد، می‌توان یک اکسترانت VPN را بمنظور ارتباط شبکه های محلی هر یک از سازمان‌ها ایجاد کرد. در چنین حالتی سازمان‌های متعدد قادر به فعالیت در یک محیط اشتراکی خواهند بود.

استفاده از VPN برای یک سازمان دارای مزایای متعددی نظیر: گسترش محدوه جغرافیائی ارتباطی، بهبود وضعیت امنیت، کاهش هزینه های عملیاتی در مقایسه با روش های سنتی WAN، کاهش زمان ارسال و حمل اطلاعات برای کاربران از راه دور، بهبود بهره وری، توپولوژی آسان و... است. در یکه شبکه VPN به عوامل متفاوتی نظیر: امنیت، اعتمادپذیری، مدیریت شبکه و سیاست‌ها نیاز خواهد بود.

۳۲-۳-۳- شبکه های LAN جزایر اطلاعاتی

فرض نمائید در جزیره ای در اقیانوسی بزرگ، زندگی می کنید.هزاران جزیره در اطراف جزیره شما وجود دارد. برخی از جزایر نزدیک و برخی دیگر دارای مسافت طولانی با جزیره شما می‌باشند. متداولترین روش بمنظور مسافرت به جزیره دیگر، استفاده از یک کشتی مسافربری است. مسافرت با کشتی مسافربری، بمنزله عدم وجود امنیت است. در این راستا هر کاری را که شما انجام دهید، توسط سایر مسافرین قابل مشاهده خواهد بود. فرض کنید هر یک از جزایر مورد نظر به مشابه یک شبکه محلی (LAN) و اقیانوس مانند اینترنت باشند. مسافرت با یک کشتی مسافربری مشابه برقراری ارتباط با یک سرویس دهنده وب و یا سایر دستگاههای موجود در اینترنت است. شما دارای هیچگونه کنترلی بر روی کابل‌ها و روترهای موجود در اینترنت نمی‌باشید. (مشابه عدم کنترل شما بعنوان مسافر کشتی مسافربری بر روی سایر مسافرین حاضر در کشتی). در صورتیکه تمایل به ارتباط بین دو شبکه اختصاصی از طریق منابع عمومی وجود داشته باشد، اولین مسئله ای که با چالش های جدی برخورد خواهد کرد، امنیت خواهد بود. فرض کنید، جزیره شما قصد ایجاد یک پل ارتباطی با جزیره مورد نظر را داشته باشد.مسیر ایجاد شده یک روش ایمن، ساده و مستقیم برای مسافرت ساکنین جزیره شما به جزیره دیگر را فراهم می‌آورد. همانطور که حدس زده اید، ایجاد و نگهداری یک پل ارتباطی بین دو جزیره مستلزم صرف هزینه های بالائی خواهد بود. (حتی اگر جزایر در مجاورت یکدیگر باشند). با توجه به ضرورت و حساسیت مربوط به داشتن یک مسیر ایمن و مطمئن، تصمیم به ایجاد پل ارتباطی بین دو جزیره گرفته شده است. در صورتیکه جزیره شما قصد ایجاد یک پل ارتباطی با جزیره دیگر را داشته باشد که در مسافت بسیار طولانی نسبت به جزیره شما واقع است، هزینه های مربوط بمراتب بیشتر خواهد بود. وضعیت فوق، نظیر استفاده از یک اختصاصی Leased است. ماهیت پل های ارتباطی (خطوط اختصاصی) از اقیانوس (اینترنت) متفاوت بوده و کماکن قادر به ارتباط جزایر(شبکه های LAN)خواهند بود. سازمان‌ها و موسسات متعددی از رویکرد فوق (استفاده از خطوط اختصاصی) استفاده می‌نمایند. مهمترین عامل در این زمینه وجود امنیت و اطمینان برای برقراری ارتباط هر یک سازمان‌های مورد نظر با یکدیگر است. در صورتیکه مسافت ادارات و یا شعب یک سازمان از یکدیگر بسیار دور باشد، هزینه مربوط به برقرای ارتباط نیز افزایشخواهد یافت. با توجه به موارد گفته شده، چه ضرورتی بمنظور استفاده از VPN وجود داشته و VPN تامین کننده، کدامیک از اهداف و خواسته های مورد نظر است؟ با توجه به مقایسه انجام شده در مثال فرضی، می‌توان گفت که با استفاده از VPN به هریک از ساکنین جزیره یک زیردریائی داده می‌شود. زیردریائی فوق دارای خصایص متفاوت نظیر:

- دارای سرعت بالا است.
- هدایت آن ساده است.
- قادر به استتار(مخفی نمودن) شما از سایر زیردریایی‌ها و کشتی‌ها است.
- قابل اعتماد است.
- پس از تامین اولین زیردریائی، افزودن امکانات جانبی و حتی یک زیردریائی دیگرمقرون به صرفه خواهد بود.

در مدل فوق، با وجود ترافیک در اقیانوس، هر یک از ساکنین دو جزیره قادر به تردد در طول مسیر در زمان دلخواه خود با رعایت مسایل ایمنی می‌باشند. مثال فوق دقیقا" بیانگر تحوه عملکرد VPN است. هر یک از کاربران از راه دور شبکه قادربه برقراری ارتباطی امن و مطمئن با استفاده از یک محیط انتقال عمومی (نظیر اینترنت) با شبکه محلی (LAN) موجود در سازمان خود خواهند بود. توسعه یک VPN (افزایش تعداد کاربران از راه دور و یا افزایش مکان های مورد نظر) به مراتب آسانتر از شبکه هائی است که از خطوط اختصاصی استفاده می‌نمایند. قابلیت توسعه فراگیر از مهمترین ویژگی های یک VPN نسبت به خطوط اختصاصی است.

۳۲-۳-۴- امنیت VPN

شبکه های VPN بمنظور تأمین امنیت (داده‌ها و ارتباطات) از روش های متعددی استفاده می‌نمایند:

- **فایروال:** فایروال یک دیواره مجازی بین شبکه اختصای یک سازمان و اینترنت ایجاد می‌نماید. با استفاده از فایروال می‌توان عملیات متفاوتی را در جهت اعمال سیاست های امنیتی یک سازمان انجام داد. ایجاد محدودیت در تعداد پورت‌ها فعال، ایجاد محدودیت در رابطه به پروتکل های خاص، ایجاد محدودیت در نوع بسته های اطلاعاتی و... نمونه هائی از عملیاتی است که می‌توان با استفاده از یک فایروال انجام داد.
- **رمزنگاری:** فرآیندی است که با استفاده از آن کامپیوتر مبداء اطلاعاتی رمزشده را برای کامپیوتر دیگر ارسال می‌نماید. سایر کامپیوترها ی مجاز قادر به رمزگشائی اطلاعات ارسالی خواهند بود. بدین ترتیب پس از ارسال اطلاعات توسط فرستنده، دریافت کنندگان، قبل از استفاده از اطلاعات می‌بایست اقدام به رمزگشائی اطلاعات ارسال شده نمایند. سیستم های رمزنگاری در کامپیوتر به دو گروه عمده تقسیم می گردد:

رمزنگاری کلید متقارن

رمزنگاری کلید عمومی

در رمز نگاری " کلید متقارن " هر یک از کامپیوترها دارای یک کلید (Secret کد) بوده که با استفاده از آن قادر به رمزنگاری یک بسته اطلاعاتی قبل از ارسال در شبکه برای کامپیوتر دیگر می‌باشند. در روش فوق می‌بایست در ابتدا نسبت به کامپیوترهائی که قصد برقراری و ارسال اطلاعات برای یکدیگر را دارند، آگاهی کامل وجود داشته باشد. هر یک از کامپیوترهای شرکت کننده در مبادله اطلاعاتی می‌بایست دارای کلید رمز مشابه بمنظور رمزگشائی اطلاعات باشند. بمنظور رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد. فرض کنید قصد ارسال یک پیام رمز شده برای یکی از دوستان خود را داشته باشید. بدین منظور از یک الگوریتم خاص برای رمزنگاری استفاده می‌شود.در الگوریتم فوق هر حرف به دوحرف بعد از خود تبدیل می‌گردد.(حرف A به حرف C، حرف B به حرف D) پس از رمزنمودن پیام و ارسال آن،

می‌بایست دریافت کننده پیام به این حقیقت واقف باشد که برای رمزگشائی پیام ارسال شده، هر حرف به دو حرق قبل از خود می‌باطست تبدیل گردد. در چنین حالتی می‌باطست به دوست امین خود، واقعیت فوق (کلید رمز) گفته شود. در صورتیکه پیام فوق توسط افراد دیگری دریافت گردد، بدلیل عدم آگاهی از کلید، آنان قادر به رمزگشائی و استفاده از پیام ارسال شده نخواهند بود. در رمزنگاری عمومی از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفا" برای کامپیوتر شما (ارسال کننده) قابل شناسائی و استفاده است. کلید عمومی توسط کامپیوتر شما در اختیار تمام کامپیوترهای دیگر که قصد ارتباط با آن را داشته باشند، گذاشته می‌شود. بمنظور رمزگشائی یک پیام رمز شده، یک کامپیوتر می‌بایست با استفاده از کلید عمومی (ارائه شده توسط کامپیوتر ارسال کننده)، کلید خصوصی مربوط به خود اقدام به رمزگشائی پیام ارسالی نماید. یکی از متداولترین ابزار "رمزنگاری کلید عمومی"، روشی با نام PGP (Pretty Good Privacy) است. با استفاده از روش فوق می‌توان اقدام به رمزنگاری اطلاعات دلخواه خود نمود.

- **پروتکل IPsec (Internet protocol security protocol):** یکی از امکانات موجود برای ایجاد امنیت در ارسال و دریافت اطلاعات می‌باشد. قابلیت روش فوق در مقایسه با الگوریتم های رمزنگاری بمراتب بیشتر است. پروتکل فوق دارای دو روش رمزنگاری است، Tunnel و Transport. در روش Tunnel، هدر و Payload رمز شده درحالیکه در روش Transport صرفاً payload رمز می‌گردد. پروتکل فوق قادر به رمزنگاری اطلاعات بین دستگاههای متفاوت است:

روتر به روتر
فایروال به روتر
کامپیوتر به روتر
کامپیوتر به سرویس دهنده

- **سرویس دهنده AAA:** سرویس دهندگان AAA (Authentication Authorization Accounting) ، بمنظور ایجاد امنیت بالا در محیط های VPN از نوع "دستیابی از راه دور " استفاده می‌گردند. زمانیکه کاربران با استفاده از خط تلفن به سیستم متصل می‌گردند، سرویس دهنده AAA درخواست آن‌ها را اخذ و عمایات زیر را انجام خواهد داد:
  - شما چه کسی هستید؟ (تایید Authentication)
  - شما مجاز به انجام چه کاری هستید؟ (مجوز Authorization)
  - چه کارهائی را انجام داده اید؟ (حسابداری Accounting)

۳۲-۳-۵- تکنولوژی های VPN

با توجه به نوع VPN ("دستیابی از راه دور" و یا "سایت به سایت")، بمنظور ایجاد شبکه از عناصر خاصی استفاده می‌گردد:

- نرم‌افزارهای مربوط به کاربران از راه دور
- سخت‌افزارهای اختصاصی نظیر یک " کانکتور " VPN و یا یک فایروال PIX
- سرویس دهنده اختصاصی VPN بمنظور سرویس های Dial-up
- سرویس دهنده NAS که توسط مرکز ارائه خدمات اینترنت بمنظور دستیابی به VPN از نوع "دستیابی از را دور" استفاده می‌شود.

شبکه VPN و مرکز مدیریت سیاست ها

با توجه به اینکه تاکنون یک استاندارد قابل قبول و عمومی بمنظور ایجاد ش VPN ایجاد نشده است، شرکت های متعدد هر یک اقدام به تولید محصولات اختصاصی خود نموده‌اند.

- **کانکتور VPN:** سخت‌افزار فوق توسط شرکت سیسکو طراحی و عرضه شده است. کانکتور فوق در مدل های متفاوت و قابلیت های گوناگون عرضه شده است. در برخی از نمونه های دستگاه فوق امکان فعالیت همزمان ۱۰۰ کاربر از راه دور و در برخی نمونه های دیگر تا ۱۰،۰۰۰ کاربر از راه دور قادر به اتصال به شبکه خواهند بود.

- **روتر مختص VPN:** روتر فوق توسط شرکت سیسکو ارائه شده است. این روتر دارای قابلیت های متعدد بمنظور استفاده در محیط های گوناگون است. در طراحی روتر فوق شبکه های VPN نیز مورد توجه قرار گرفته و امکانات مربوط در آن بگونه‌ای بهینه سازی شده‌اند.

- **فایروال PIX:** فایروال PIX (Private Internet eXchange) قابلیت هائی نظیر NAT، سرویس دهنده Proxy، فیلتر نمودن بسته ای اطلاعاتی، فایروال و VPN را در یک سخت‌افزار فراهم نموده است.

۳۲-۳-۶- تونل سازی (Tunneling)

اکثر شبکه های VPN بمنظور ایجاد یک شبکه اختصاصی با قابلیت دستیابی از طریق اینترنت از امکان "Tunneling " استفاده می‌نمایند. در روش فوق تمام بسته اطلاعاتی در یک بسته دیگر قرار گرفته و از طریق شبکه ارسال خواهد شد. پروتکل مربوط به بسته اطلاعاتی خارجی (پوسته) توسط شبکه و دو نقطه (ورود و خروج بسته اطلاعاتی) قابل فهم می‌باشد. دو نقطه فوق را "اینترفیس های تونل " می‌گویند. روش فوق مستلزم استفاده از سه پروتکل است: پروتکل حمل کننده. از پروتکل فوق شبکه حامل اطلاعات استفاده می‌نماید.

در پروتکل کپسوله سازی، از پروتکل هائی نظیر IPSec، L2F، PPTP، L2TP و GRE استفاده می‌گردد. در پروتکل مسافر نیز از پروتکل هائی نظیر IPX، IP و NetBeui بمنظور انتقال داده های اولیه استفاده می‌شود.

با استفاده از روش Tunneling می‌توان عملیات جالبی را انجام داد. مثلاً می‌توان از بسته ای اطلاعاتی که پروتکل اینترنت را حمایت نمی‌کند (نظیر NetBeui) درون یک بسته اطلاعاتی IP استفاده و آن را از طریق اینترنت ارسال نمود و یا می‌توان یک بسته اطلاعاتی را که از یک آدرس IP غیر قابل مسیردهی (اختصاصی) استفاده می‌نماید، درون یک بسته اطلاعاتی که از آدرس های معتبر IP استفاده می‌کند، مستقر و از طریق اینترنت ارسال نمود.

در شبکه های VPN از نوع " سایت به سایت "، GRE (generic routing encapsulation) بعنوان پروتکل کپسوله سازی استفاده می‌گردد. فرآیند فوق نحوه استقرار و بسته بندی " پروتکل مسافر" از طریق پروتکل " حمل کننده " برای انتقال را تبین می‌نماید. (پروتکل حمل کننده، عموما IP "است). فرآیند فوق شامل اطلاعاتی در رابطه با نوع بسته های اطلاعاتی برای کپسوله نمودن و اطلاعاتی در رابطه با ارتباط بین سرویس گیرنده و سرویس دهنده است. در برخی موارد از پروتکل IPSec در حالت Tunnel برای کپسوله سازی استفاده می‌گردد. پروتکل IPSec، قابل استفاده در دو نوع شبکه (VPN سایت به سایت و دستیابی از راه دور) است. اینترفیس های Tunnel می‌بایست دارای امکانات حمایتی از IPSec باشند.

در شبکه های VPN از نوع " دستیابی از راه دور "، Tunneling با استفاده از PPP انجام می گیرد. PPP بعنوان حمل کننده سایر پروتکل های IP در زمان برقراری ارتباط بین یک سیستم میزبان و یک سیستم ازه دور، مورد استفاده قرار می گیرد. هر یک از پروتکل های زیر با استفاده از ساختار اولیه PPP ایجاد و توسط شبکه های VPN از نوع "دستیابی از راه دور" استفاده می گردند:

- **L2F (Layer 2 Forwarding):** پروتکل فوق توسط سیسکو ایجاد شده است. در پروتکل فوق از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده‌اند، استفاده شد ه است.
- **PPTP (Point-to-Point Tunneling Protocol):** پروتکل فوق توسط کنسرسیومی متشکل از شرکت های متفاوت ایجاد شده است. این پروتکل امکان رمزنگاری ۴۰ بیتی و ۱۲۸ بیتی را دارا بوده و از مدل های تعیین اعتبار کاربر که توسط PPP حمایت شده‌اند، استفاده می‌نماید.
- **L2TP (Layer 2 Tunneling Protocol):** پروتکل فوق با همکاری چندین شرکت ایجاد شده است.پروتکل فوق از ویژگی های PPTP و L2F استفاده کرده است. پروتکل L2TP بصورت کامل IPSec را حمایت می کند. از پروتکل فوق بمنظور ایجاد تونل بین موارد زیر استفاده می گردد:
  - سرویس گیرنده و روتر
  - NAS و روتر
  - روتر و روتر

در واقع عملکرد Tunneling مشابه حمل یک کامپیوتر توسط یک کامیون است. فروشنده، پس از بسته بندی کامپیوتر (پروتکل مسافر) درون یک جعبه (پروتکل کپسوله سازی) آن را توسط یک کامیون (پروتکل حمل کننده) از انبار خود (اینترفیس ورودی تونل) برای متقاضی ارسال می‌دارد. کامیون (پروتکل حمل کننده) از طریق بزرگراه (اینترنت) مسیر خود را طی، تا به منزل شما (اینترفیس خروجی تونل) برسد. شما در منزل جعبه (پروتکل کپسول سازی) را باز و کامپیوتر (پروتکل مسافر) را از آن خارج می‌نمائید.

۳۲-۳-۷- پروتکل های درون تونل

Tunneling را می‌توان روی دو لایه از لایه های OSI پیاده کرد. PPTP و L2TP از لایه ۲ یعنی پیوند داده استفاده کرده و داده‌ها را در قالب Frame های پروتکل نقطه به نقطه (PPP) بسته بندی می‌کنند. در این حالت می‌توان از ویژگی های PPP همچون تعیین اعتبار کاربر، تخصیص آدرس پویا (مانند DHCP)، فشرده سازی داده‌ها یا رمز گذاری داده‌ها بهره برد.

با توجه به اهمیت ایمنی انتقال داده‌ها در VPN، دراین میان تعیین اعتبار کاربر نقش بسیار مهمی دارد. برای این کار معمولا" از CHAP استفاده می‌شود که مشخصات کاربر را در این حالت رمز گذاری شده جابه جا می‌کند. Call back هم دسترسی به سطح بعدی ایمنی را ممکن می‌سازد. در این روش پس از تعیین اعتبار موفقیت آمیز، ارتباط قطع می‌شود. سپس سرویس دهنده برای برقرار کردن ارتباط جهت انتقال داده‌ها شماره گیری می کند. هنگام انتقال داده‌ها، Packet های IPX، IP یا NetBEUI در قالب Frame های PPP بسته بندی شده و فرستاده می‌شوند. PPTP هم Frame های PPP را پیش از

ارسال روی شبکه بر پایه IP به سوی کامپیوتر مقصد، در قالب Packet های IP بسته بندی می‌کند. این پروتکل در سال ۱۹۹۶ از سوی شرکت هایی چون مایکرو سافت، 3com، Ascend و Robotics US پایه گذاری شد. محدودیت PPTP در کار تنها روی شبکه های IP باعث ظهور ایده ای در سال ۱۹۹۸ شد. L2TP روی X.25،Frame Relay یا ATM هم کار می‌کند. برتری L2TP در برابر PPTP این است که به طور مستقیم روی رسانه های گوناگون WAN قابل انتقال است.

VPN-Ipsec فقط برای اینترنت بوده و Ipsec برخلاف PPTP و L2TP روی لایه شبکه یعنی لایه سوم کار می‌کند. این پروتکل داده هایی که باید فرستاده شود را همراه با همه اطلاعات جانبی مانند گیرنده و پیغام های وضعیت رمز گذاری کرده و به آن یک IP Header معمولی اضافه کرده و به آن سوی تونل می‌فرستد.

کامپیوتری که در آن سو قرار دارد IP Header را جدا کرده، داده‌ها را رمز گشایی کرده و آن را به کامپیوتر مقصد می‌فرستد. Ipsec را می‌توان با دو شیوه Tunneling پیکر بندی کرد. در این شیوه انتخاب اختیاری تونل، سرویس گیرنده نخست یک ارتباط معمولی با اینترنت برقرار می‌کند و سپس از این مسیر برای ایجاد اتصال مجازی به کامپیوتر مقصد استفاده می‌کند. برای این منظور، باید روی کامپیوتر سرویس گیرنده پروتکل تونل نصب شده باشد. معمولا" کاربر اینترنت است که به اینترنت وصل می‌شود. اما کامپیوترهای درون LAN هم می‌توانند یک ارتباط VPN برقرا کنند. از آنجا که ارتباط IP از پیش موجود است تنها برقرار کردن ارتباط VPN کافی است. در شیوه تونل اجباری، سرویس گیرنده نباید تونل را ایجاد کند بلکه این کار از به عهده فراهم ساز سرویس (Service provider) است. سرویس گیرنده تنها باید به ISP وصل شود. تونل به طور خودکار از فراهم ساز تا ایستگاه مقصد وجود دارد. البته برای این کار باید همانگی های لازم با ISP انجام بگیرد.

۳۲-۳-۸- ویژگی های امنیتی در IPsec

Ipsec از طریق AH (Authentication Header) مطمئن می‌شود که Packet های دریافتی از سوی فرستنده واقعی (و نه از سوی یک نفوذ کننده که قصد رخنه دارد) رسیده و محتویات شان تغییر نکرده. AH اطلاعات مربوط به تعیین اعتبار و یک شماره توالی (Sequence Number) در خود دارد تا از حملات Replay جلوگیری کند. اما AH رمزگذاری نمی‌شود. رمز گذاری از طریق Security Header Encapsulation یا ESH انجام می‌گیرد. در این شیوه داده های اصلی رمز گذاری شده و VPN اطلاعاتی را از طریق ESH ارسال می‌کند.

ESH همچنین کارکرد هایی برای تعیین اعتبار و خطایابی دارد. به این ترتیب دیگر به AH نیازی نیست. برای رمز گذاری و تعیین اعتبار روش مشخص و ثابتی وجود ندارد اما با این همه، IETF برای حفظ سازگاری میان محصولات مختلف، الگوریتم های اجباری برای پیاده سازی Ipsec تدارک دیده. برای نمونه می‌توان به MD5،DES یا Secure Hash Algorithm اشاره کرد. مهمترین استانداردها و روش هایی که در Ipsec به کار می‌روند عبارتند از:

- **Diffie-Hellman:** برای مبادله کلیدها میان ایستگاه های دو سر ارتباط.
- **رمز گذاری Public Key:** برای ثبت و اطمینان از کلیدهای مبادله شده و همچنین اطمینان از هویت ایستگاه های سهیم در ارتباط.
- **الگوریتم های رمز گذاری:** مانند DES برای اطمینان از درستی داده های انتقالی.
- **الگوریتم های درهم ریزی:** (Hash) برای تعیین اعتبار تک تک Packetها.

• **امضاهای دیجیتال:** برای تعیین اعتبارهای دیجیتالی.

۳۲-۳-۹- Ipsec بدون تونل

Ipsec در مقایسه با دیگر روش‌ها یک برتری دیگر هم دارد و آن اینست که می‌تواند همچون یک پروتکل انتقال معمولی به کار برود.

در این حالت برخلاف حالت Tunneling همه IP packet رمز گذاری و دوباره بسته بندی نمی‌شود. بجای آن، تنها داده های اصلی رمزگذاری می‌شوند و Header همراه با آدرس های فرستنده و گیرنده باقی می‌ماند. این باعث می‌شود که داده های سرباز (Overhead) کمتری جابجا شوند و بخشی از پهنای باند آزاد شود. اما روشن است که در این وضعیت، خرابکاران می‌توانند به مبدا و مقصد داده‌ها پی ببرند. از آنجا که در مدل OSI داده‌ها از لایه ۳ به بالا رمز گذاری می‌شوند خرابکاران متوجه نمی‌شوند که این داده‌ها به ارتباط با سرویس دهنده Mail مربوط می‌شود یا به چیز دیگر.

جریان یک ارتباط Ipsec

بیش از آن که دو کامپیوتر بتوانند از طریق Ipsec داده‌ها را میان خود جابجا کنند باید یکسری کارها انجام شود.

• نخست باید ایمنی برقرار شود. برای این منظور، کامپیوترها برای یکدیگر مشخص می‌کنند که آیا رمز گذاری، تعیین اعتبار و تشخیصخطا یا هر سه آن‌ها باید انجام بگیرد یا نه.

• سپس الگوریتم را مشخص می‌کنند، مثلا" DEC برای رمزگذاری و MD5 برای خطایابی.

• در گام بعدی، کلیدها را میان خود مبادله می‌کنند.

Ipsec برای حفظ ایمنی ارتباط از SA) Security Association) استفاده می‌کند. SA چگونگی ارتباط میان دو یا چند ایستگاه و سرویس های ایمنی را مشخص می‌کند. SAها از سوی SIP (Security parameter Index) شناسایی می‌شوند. SPI از یک عدد تصادفی و آدرس مقصد تشکیل می‌شود. این به آن معنی است که همواره میان دو کامپیوتر دو SPI وجود دارد:

یکی برای ارتباط A و B و یکی برای ارتباط B به A. اگر یکی از کامپیوترها بخواهد در حالت محافظت شده داده‌ها را منتقل کند نخست شیوه رمز گذاری مورد توافق با کامپیوتر دیگر را بررسی کرده و آن شیوه را روی داده‌ها اعمال می‌کند. سپس SPI را در Header نوشته و Packet را به سوی مقصد می‌فرستد.

مدیریت کلیدهای رمز در Ipsec

اگر چه Ipsec فرض را بر این می‌گذارد که توافقی برای ایمنی داده‌ها وجود دارد اما خودش برای ایجاد این توافق نمی‌تواند کاری انجام بدهد.

Ipsec در این کار به IKE (Internet Key Exchange) تکیه می‌کند که کارکردی همچون IKMP (Key Management Protocol) دارد. برای ایجاد SA هر دو کامپیوتر باید نخست تعیین اعتبار شوند. در حال حاضر برای این کار از راه های زیر استفاده می‌شود:

• **Pre shared keys:** روی هر دو کامپیوتر یک کلید نصب می‌شود که IKE از روی آن یک عدد Hash ساخته و آن را به سوی کامپیوتر مقصد می‌فرستد. اگر هر دو کامپیوتر بتوانند این عدد را بسازند پس هر دو این کلید دارند و به این ترتیب تعیین هویت انجام می‌گیرد.

• **رمز گذاری Public Key:** هر کامپیوتر یک عدد تصادفی ساخته و پس از رمز گذاری آن با کلید عمومی کامپیوتر مقابل، آن را به کامپیوتر مقابل می‌فرستد.اگر کامپیوتر مقابل بتواند با کلید شخصی خود این عدد را رمز گشایی کرده و باز پس بفرستد برا ی ارتباط مجاز است. در حال حاضر تنها از روش RSA برای این کار پیشنهاد می‌شود.

• **امضاء دیجیتال:** در این شیوه، هر کامپیوتر یک رشته داده را علامت گذاری (امضاء) کرده و به کامپیوتر مقصد می‌فرستد. در حال حاضر برای این کار از روش های RSA و DSS (Digital Singature Standard) استفاده می‌شود. برای امنیت بخشیدن به تبادل داده‌ها باید هر دو سر ارتبا ط نخست بر سر یک یک کلید به توافق می‌رسند که برای تبادل داده‌ها به کار می‌رود. برا ی این منظور می‌توان همان کلید به دست آمده از طریق Diffie Hellman را به کاربرد که سریع‌تر است یا یک کلید دیگر ساخت که مطمئن‌تر است.

۳۲-۳-۱۰- پیش‌نیازها

برای اینکه دو کامپیوتر بر پایه ویندوز بتواند از طریق VPN به هم مرتبط شوند دست کم یکی از آن‌ها باید به ویندوز NT یا ۲۰۰۰ کار کند تا نقش سرویس دهنده VPN را به عهده بگیرد. ویندوز های ۹x یا Me تنها می‌توانند سرویس گیرنده VPN باشند. سرویس دهنده VPN باید یک IP ثابت داشته باشد. روشن است که هر دو کامپیوتر باید به اینترنت متصل باشند. فرقی نمی‌کند که این اتصال از طریق خط تلفن و مودم باشد یا شبکه محلی. IP در سرویس دهنده VPN باید مجاز (Valid) باشد تا سرویس گیرنده بتواند یک مستقیما آن را ببیند. در شبکه های محلی که اغلب از IP های شخصی (192.168.x.x) استفاده می‌شود VPN را باید روی شبکه ایجاد کرد تا ایمنی ارتباط بین میان کامپیوترها تامین شود.

۳۲-۳-۱۱- نصب سرویس دهنده VPN

روی کامپیوتر بر پایه ویندوز NT نخست باید در بخش تنظیمات شبکه، راه انداز Point to Point Tunneling را نصب کنید. هنگام این کار، شمار ارتباط های همزمان VPN پرسیده می‌شود. در سرویس دهنده های NT این عدد می‌تواند حداکثر ۲۵۶ باشد. در ایستگاه کاری NT، این عدد باید ۱ باشد چون این سیستم عامل تنها اجازه یک ارتباط RAS را می‌دهد. از آنجا که ارتباط VPN در قالب Remote Access برقرار می‌شود ویندوز NT به طور خودکار پنجره پیکر بندی RAS را باز می‌کند. اگر RAS هنوز نصب نشده باشد ویندوز NT آن را نصب می‌کند. هنگام پیکربندی باید VPN Adapter را به پورت های شماره گیری اضافه کنید. اگر می‌خواهید که چند ارتباط VPN داشته باشید باید این کار را برای هر یک از VPN Adapterها انجام دهید.

۳۲-۳-۱۲- پیکربندی سرویسدهنده RAS

اکنون باید VPN Adapter را به گونه ای پیکربندی کنید که ارتباطات به سمت درون (Incoming) اجازه بدهد. نخست باید پروتکل های مجاز برای این ارتباط را مشخص کنید. همچنین باید شیوه رمز گذاری را تعیین کرده و بگویید که

آیاسرویس دهنده تنها اجازه دسترسی به کامپیوترهای موجود در شبکه کامپیوتر ویندوز NT، در این وضیعت، سرویس دهنده VPN می‌تواند کار مسیر یابی را هم انجام دهد. برای بالاتر بردن ایمنی ارتباط، می‌توانید NetBEUI را فعال کرده و از طریق آن به کامپیوترهای دور اجازدسترسی به شبکه خود را بدهید. سرویس گیرنده، شبکه و سرویس های اینترنتی مربوط به سرویس دهنده VPN را نمی‌بینید. برای راه انداختن TCP/IP همراه با VPN چند تنظیم دیگر لازم است. اگر سرویس دهنده DHCP ندارید باید به طور دستی یک فضای آدرس IP (Adress Pool) را مشخص کنید. به خاطر داشته باشید که تنها باید از IP های شخصی (Private) استفاده کنید. این فضای آدرس باید دست کم ۲ آدرس داشته باشد،یکی برای سرویس دهنده VPN و دیگری برای سرویس گیرنده VPN. هر کار بر باید برای دسترسی به سرویس دهنده از طریق VPN مجوز داشته باشد. برای این منظور باید در User Manager در بخش Dialing اجازه دسترسی از دور را بدهید. به عنوان آخرین کار، Remote Access Server را اجرا کنید تا ارتباط VPN بتواند ایجاد شود.

۳۲-۳-۱۳- Transport در مقایسه با Tunnel

در حالت Transport دو میزبان به طور مستقیم روی اینترنت با هم گفتگو می‌کنند. در این حالت می‌توان IPsec را برای تعیین اعتبار و همچنین یکپارچگی و درستی داده‌ها به کار برد. به کمک IPsec نه تنها می‌توان از هویت طرف گفتگو مطمئن شدبلکه می‌توان نسبت به درستی و دست نخوردگی داده هاهم اطمینان حاصل کرد. به کمک عملکرد رمز گذاری می‌توان افزون بر آن خوانده شدن داده‌ها از سوی افراد غیر مجاز جلوگیری کرد.

اما از آنجا که در این شیوه، دو کامپیوتر به طور مستقیم داده‌ها را مبادله می‌کنند نمی‌توان مبدا و مقصد داده‌ها را پنهان کرد. از حالت Tunnel هنگامی که استفاده می‌شود که دست کم یکی از کامپیوترها به عنوان Security Gateway به کار برود. در این وضعیت حداقل یکی از کامپیوترهایی که در گفتگو شرکت می‌کند در پشت Gateway قراردارد و در نتیجه ناشناس می‌ماند. حتی اگر دو شبکه از از طریق Security Gateway های خود با هم داده مبادله کنند نمی‌توان از بیرون فهمید که دقیقا کدام کامپیوتر به تبادل داده مشغول است. در حالت Tunnel هم می‌توان از کارکردهای تعیین اعتبار،کنترل درستی داده‌ها و رمز گذاری بهره برد.

۳۲-۳-۱۴- Authentication Header

وظیفه Header IP Authentication آن است که داده های در حال انتقال بدون اجازه از سوی شخصسوم مورد دسترسی و تغییر قرار نگیرد. برای این منظور از روی Header مربوط به IP و داده های اصلی یک عدد Hash به دست آمده و به همراه فیلدهای کنترلی دیگر به انتهای Header اضافه می‌شود. گیرنده با آزمایش این عدد می‌تواند به دستکاری های احتمالی در Header یا داده های اصلی پی ببرد. Authentication Header هم در حالت Transport و هم در حالت Tunnel کاربرد دارد.

AH در حالت Transport میان Header مربوط به IP و داده های اصلی می‌نشیند. در مقابل، در حالت Tunneling،Gateway کل Paket را همراه با Header مربوط به داده‌ها در یک IP Packet بسته بندی می‌کند. در این

حالت، AH میان Header جدید و Packet اصلی قرار می‌گیرد. AH در هر دو حالت، اعتبار و سلامت داده‌ها را نشان می‌دهد اما دلیلی بر قابل اطمینان بودن آن‌ها نیست چون عملکرد رمز گذاری ندارد.

۳۲-۳-۱۵- *Encapsulated Security Payload*

Encapsulated Security Payload IP برای اطمینان از ایمنی داده‌ها به کار می‌رود. این پروتکل داده‌ها در قالب یک Header و یک Trailer رمز گذاری می‌کند. به طوری اختیاری می‌توان به انتهای Packet یک فیلد Auth ESP اضافه کرد که مانند AH اطلاعات لازم برای اطمینان از درستی داده‌ها رمز گذاری شده را در خود دارد. در حالت Transport Header مربوط به ESP و Trailer تنها داده های اصلی IP از پوشش می‌دهند و Header مربوط به Packet بدون محافظ باقی می‌ماند. اما در حالت Tunneling همه Packet ارسالی از سوی فرستنده، داده اصلی به شمار می‌رود و Security Gateway آن را در قالب یک Packet مربوط به IP به همراه آدرس های فرستنده و گیرنده رمز گذاری می‌کند. در نتیجه، ESP نه تنها اطمینان از داده‌ها بلکه اطمینان از ارتباط را هم تامین می‌کند. در هر دوحالت، ESP در ترکیب با AH ما را از درستی بهترین داده های Header مربوط به IP مطمئن می‌کند.

۳۲-۳-۱۶- *Association Security*

برای اینکه بتوان ESP/AH را به کار برد باید الگوریتم های مربوط به درهم ریزی (Hashing) تعیین اعتبار و رمز گذاری روی کامپیوترهای طرف گفتگو یکسان باشد. همچنین دو طرف گفتگو باید کلیدهای لازم و طول مدت اعتبار آن‌ها را بدانند. هر دو سر ارتباط IPsec هر بار هنگام برقرار کردن ارتباط به این پارامترهای نیاز دارند. SA یا Security Association به عنوان یک شبه استاندارد در این بخش پذیرفته شده. برای بالا بردن امنیت، از طریق SA می‌توان کلیدها را تا زمانی که ارتباط برقرار است عوض کرد. این کار را می‌توان در فاصله های زمانی مشخص یا پس از انتقال حجم مشخصی از داده‌ها انجام داد.

۳۲-۳-۱۷- *Internet Key Exchang*

پروتکل Internet Key Exchang یا IKE (RFC 2409) روند کار روی IPsec SA را تعریف می‌کند. این روش را Security Association and Key Internet Management Protocol یا ISAKMP نیز می‌نامند. این پروتکل مشکل ایجاد ارتباط میان دو کامپیوتر را که هیچ چیز از هم نمی‌دانند و هیچ کلیدی ندارند حل می‌کند. در نخستین مرحله IKE (IKE Phase 1) که به آن حالت اصلی(Main Mode) هم گفته می‌شود، دو طرف گفتگو نخست بر سر پیکر بندی ممکن برای SA و الگوریتم های لازم برای درهم ریزی (Hashing)، تعیین اعتبار و رمزگذاری به توافق می‌رسند. آغاز کننده (Initiator) ارتباط به طرف مقابل(یا همان Responder) چند گزینه را پیشنهاد می‌کند. Responder هم مناسب ترین گزینه را انتخاب کرده و سپس هر دو طرف گفتگو، از طریق الگوریتم Diffie-Hellman یک کلید رمز (Secret Key) می‌سازند که پایه همه رمز گذاری های بعدی است. به این ترتیب صلاحیت طرف مقابل برای برقراری ارتباط تایید می‌شود. اکنون مرحله دوم IKE (IKE Phase 2) آغاز می‌گردد که حالت سریع (Ouick Mode) هم نامیده می‌شود. ا ین مرحله SA مربوط به IPsec را از روی پارامترهای مورد توافق برای ESP و AH می‌سازد.

۳۲-۳-۱۸- گواهینامه x.506

همانطور که پیش از این گفتیم بهترین راه برای تبادل Public Keyها x.509 Certificate (RFC شماره ۲۴۹۵) است. یک چنین گواهینامه ای یک Public Key برای دارنده خود ایجاد می‌کند. این گواهینامه، داده هایی مربوط به الگوریتم به کار رفته برای امضاء ایجاد کننده، دارنده و مدت اعتبار در خود دارد که در این میان، Public Key مربوط به دارنده از بقیه مهمتر است. CA هم گواهینامه را با یک عدد ساخته شده از روی داده‌ها که با Public Key خودش ترکیب شده امضاء می‌کند.

برای بررسی اعتبار یک گواهینامه موجود، گیرنده باید این امضاء را با Public Key مربوط به CA رمز گشایی کرده و سپس با عدد نخست مقایسه کند. نقطه ضعف این روش در طول مدت اعتبار گواهینامه و امکان دستکاری و افزایش آن است. اما استفاده از این گواهینامه‌ها در ارتباط های VPN مشکل چندانی به همراه ندارد چون مدیر شبکه Security Gateway و همه ارتباط‌ها را زیر نظر دارد.

۳۲-۴- راه‌های اتصال یک کاربر به یک شبکه راه دور

دو روش برای اتصال یک کاربر به یک شبکه راه دور وجود دارد

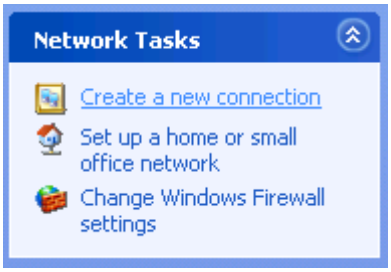
۱. استفاده از خطوط تلفن (VPDN): در این روش، کامپیوتر مبدا، کامپیوتر مقصد را به کمک خط تلفن شماره گیری می‌کند. در صورتی که کامپیوتر مقصد، کامپیوتر مبدا را بپذیرد، کامپیوتر مبدا جزئی از شبکه کامپیوتر مقصد به شمار خواهد آمد. عیب این روش، هزینه بالای تلفن برای اتصالات غیر شهری است. مزیت این روش این است که نیازی به دانستن آدرس IP کامپیوتر مقصد نداریم.

۲. اتصال از طریق اینترنت (VPN): در این روش، کامپیوتر مبدا ابتدا به اینترنت متصل شده (مثلاً توسط ADSL)، سپس با آدرس IP کامپیوتر مقصد ارتباط برقرار می‌کند. در صورتی که کامپیوتر مقصد، کامپیوتر مبدا را بپذیرد، کامپیوتر مبدا جزئی از شبکه کامپیوتر مقصد به شمار خواهد آمد. مزیت این روش نسبت به روش قبل، این است که فاصله کامپیوترها، هیچ تاثیری بر هزینه نخواهد داشت. اما عیب آن این است که کامپیوتر مقصد باید دارای یک آدرس IP به صورت Valid باشد.

در ادامه به آموزش‌های عملی انجام این کار می‌پردازیم.

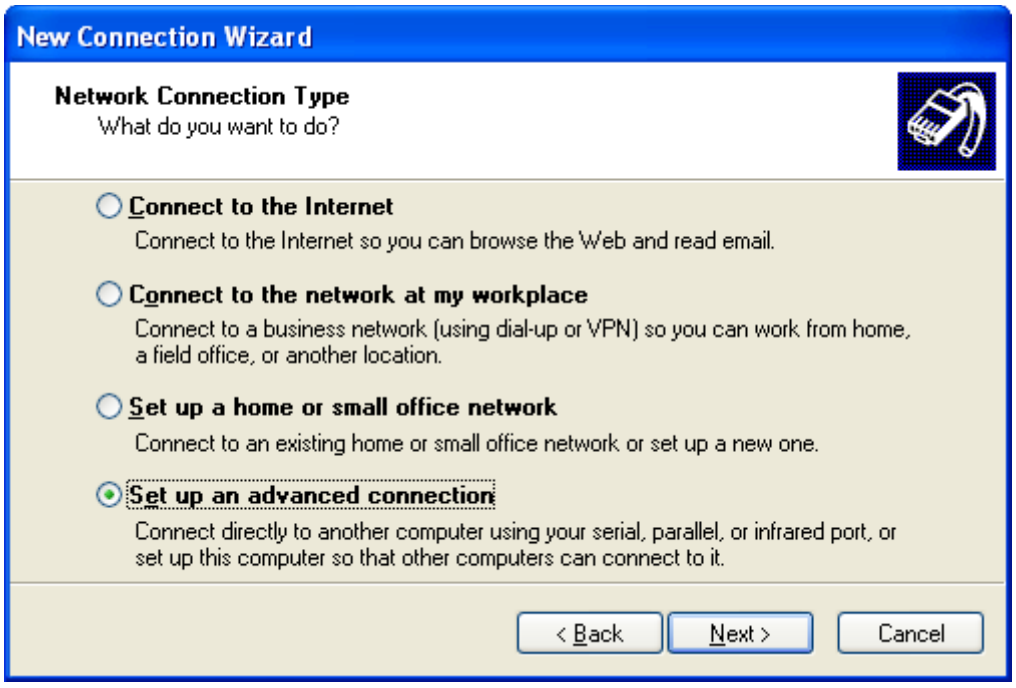
۳۲-۵- آماده سازی ویندوز XP جهت دریافت و پذیرش درخواستها

برای این آماده سازی، ابتدا وارد Control Panel ➔ Network Connection شده و سپس گزینه Create a new connection را انتخاب نمایید.



ابتدا صفحه خوش آمد گویی باز می‌شود. در این صفحه، روی Next کلیک نمایید.

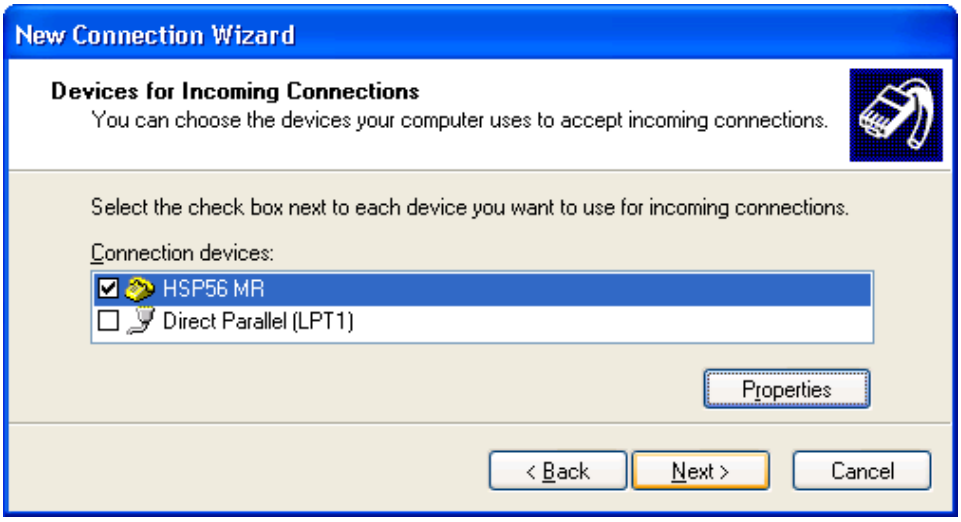
سپس در صفحه باز شده، گزینه Set up an advanced connection را انتخاب نمایید. این گزینه برای ساخت Connection به منظور ارتباط مستقیم بین کامپیوترها است.



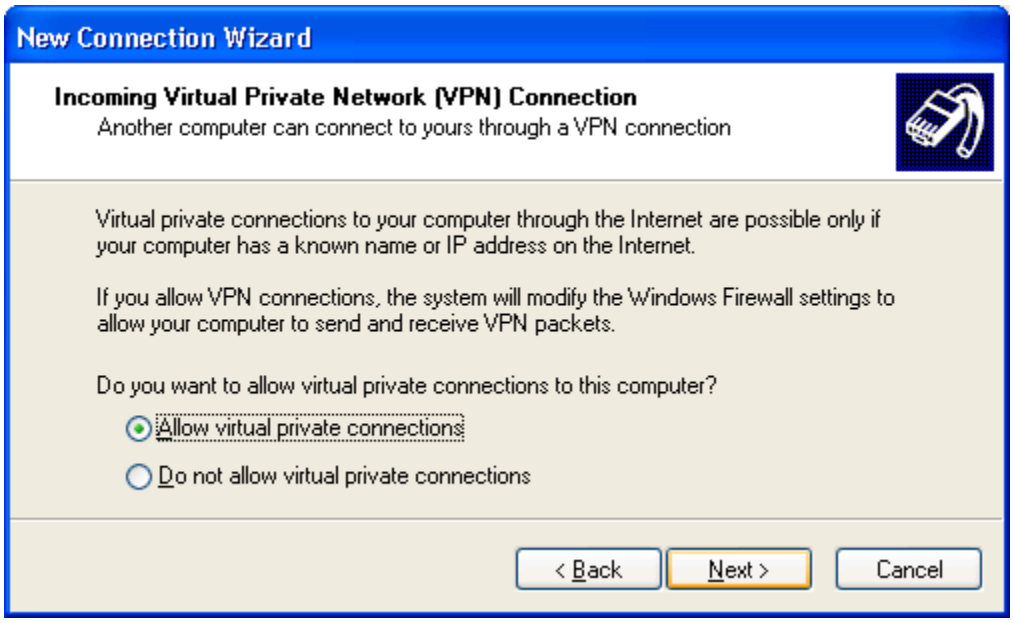
در صفحه بعد، گزینه Accept incoming connections را انتخاب نمایید. این بدان معناست که سیستم درخواست‌های اتصال را بپذیرد.



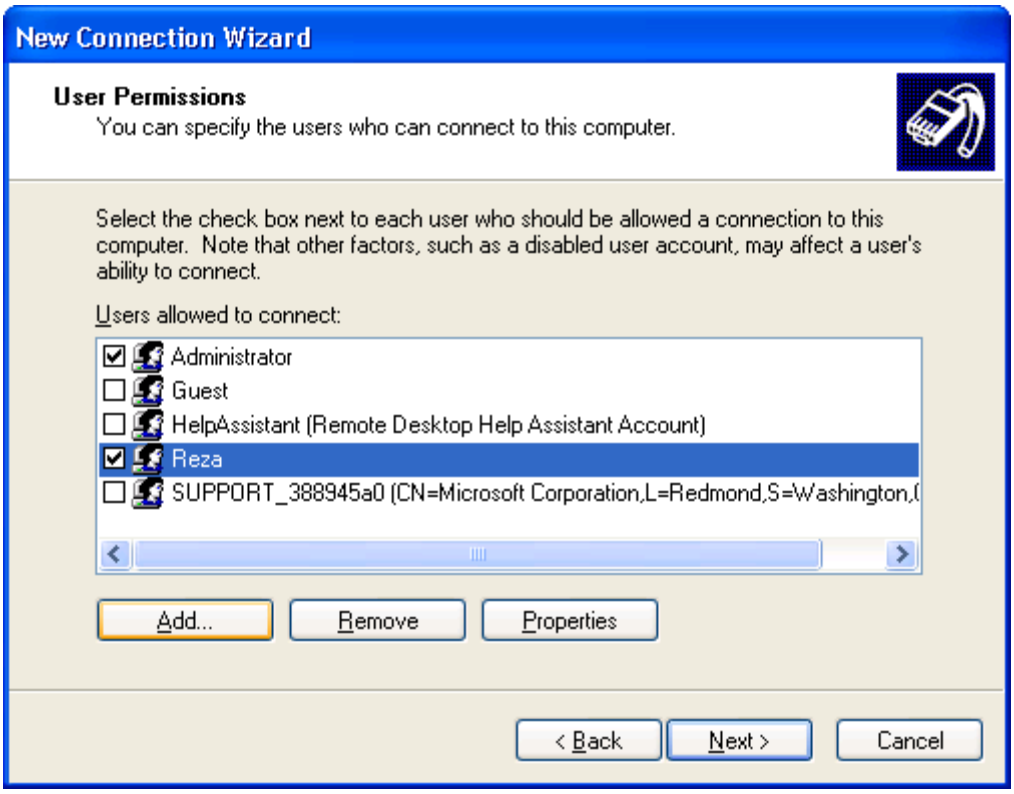
در صفحه بعد، وسیله ارتباطی خود را انتخاب نمایید. در این شکل، مودم Dial Up را انتخاب کرده‌ایم.



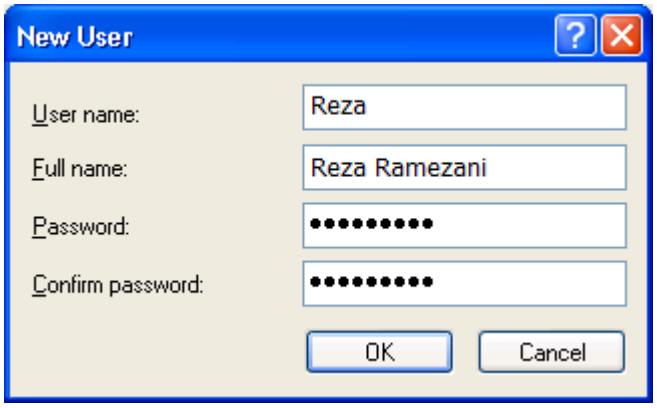
با این کار سیستم شما توسط شماره گیری (VPDN) قابل دسترس خواهد بود. اگر می‌خواهید که سیستم شما توسط VPN نیز قابل دسترسی باشد، گزینه Allow virtual private connections را انتخاب نمایید.



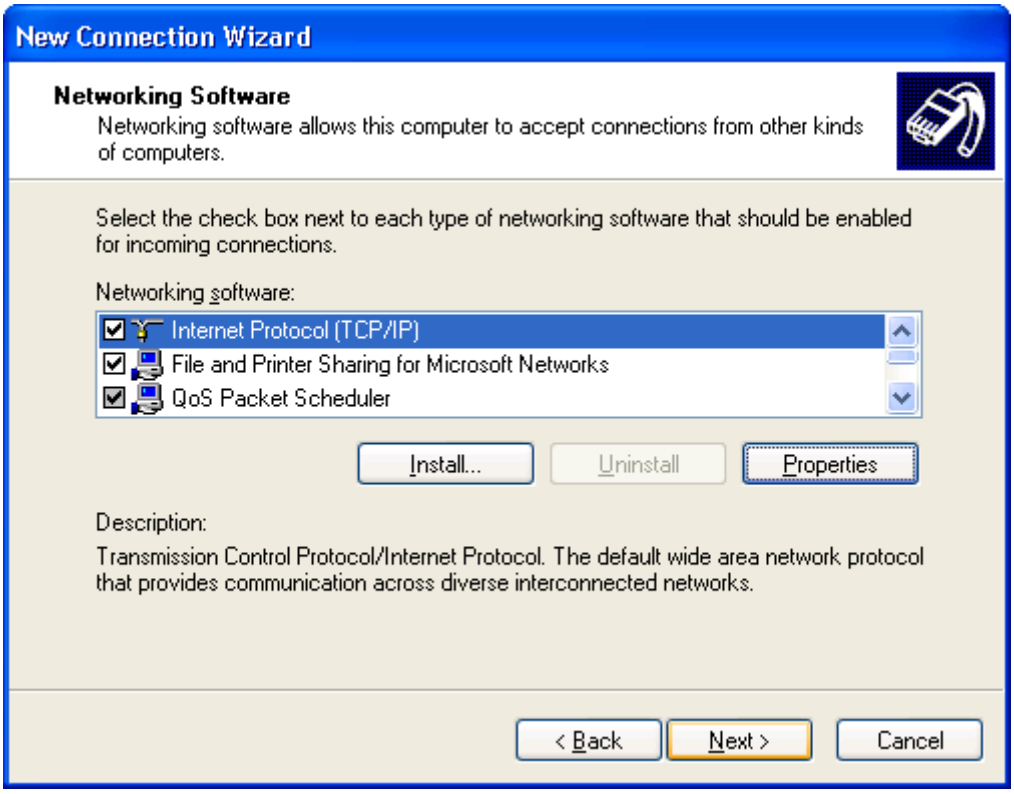
در صفحه بعد، کاربر یا کاربرانی که مجاز به ورود راه دور و استفاده از منابع هستند را انتخاب کنید. در این صورت، هنگام اتصال، بایستی یکی از این نام‌های کاربری و رمز عبور وی را وارد نمایید.



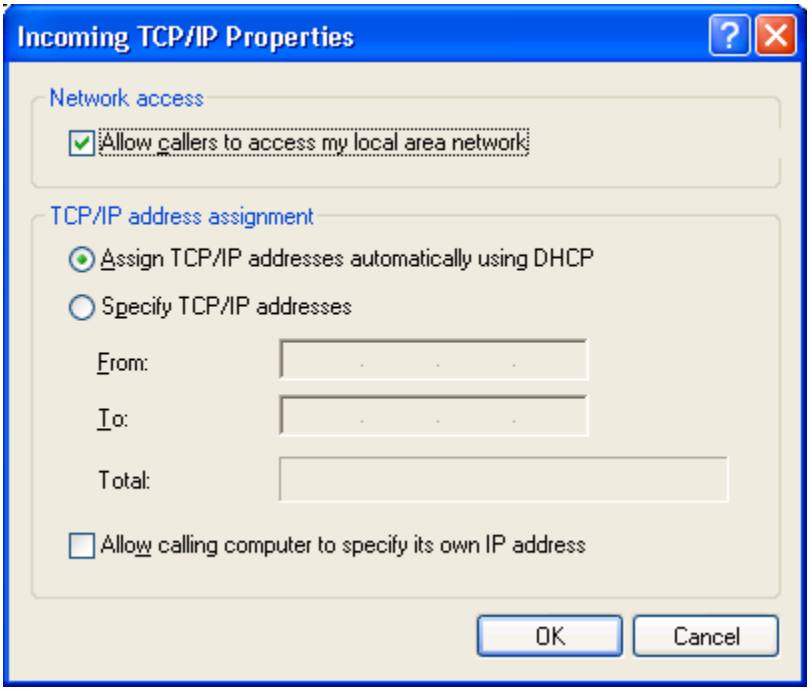
در صفحه قبل، اگر می‌خواهید، کاربر جدیدی را وارد نمایید، روی دکمه Add کلیک کنید. در صفحه باز شده، اطلاعات کاربر را وارد نمایید. در نهایت OK کرده و Next را بزنید.



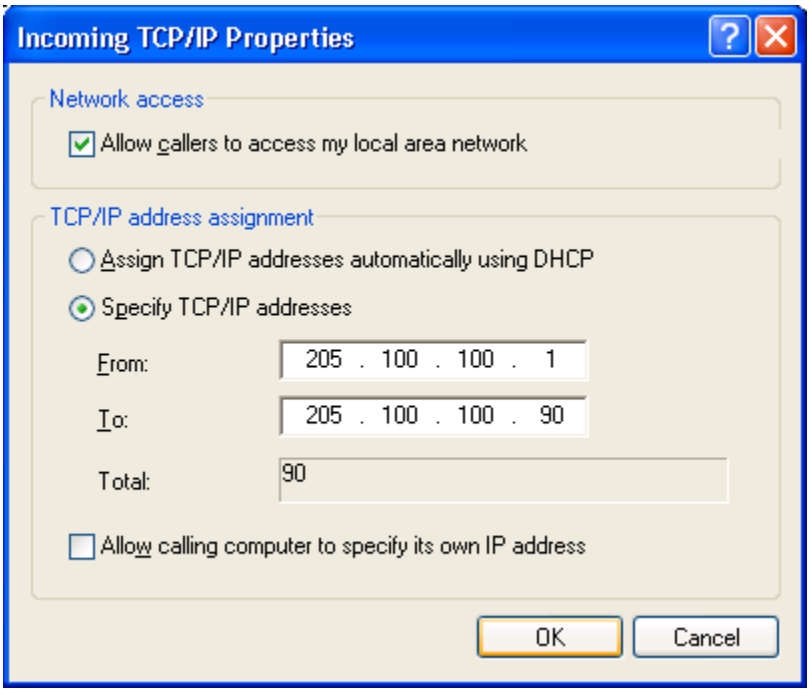
در صفحه بعد می‌توانید تنظیمات پروتکل خود را انتخاب نمایید. معروف ترین تنظیمات، تنظیم آدرس IP است. بدین معنی که شما بایستی به کاربری که به سیستم شما متصل می‌شود، یک آدرس IP اختصاص دهید. این آدرس IP باید در محدوده آدرس IP شبکه شما باشد، تا کاربر راه دور بتواند به شبکه شما متصل شود. برای تنظیم آدرس IP، گزینه Internet Protocol را انتخاب کرده و روی Properties کلیک کنید.



در صفحه باز شده، دو ره برای تخصص آدرس IP به کامپیوتر راه دور دارید. راه اول، تخصیص آدرس IP به صورت خودکار و توسط پروتکل DHCP است. با این کار، سیستم از محدوده آدرس IP شما، یک آدرس را انتخاب کرده و به Client تخصیص می‌دهد. بدین منظور گزینه Assign TCP/IP addresses automatically using DHCP را انتخاب کنید.



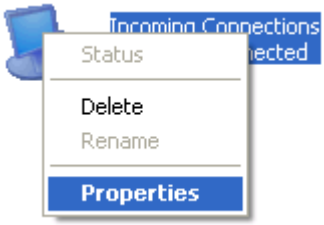
اما اگر قصد دارید که محدوده آدرس IP را خودتان تعیین کنید، بدین منظور گزینه Specify TCP/IP addresses را انتخاب کنید. سپس در قسمت From، آدرس شروع محدوده و در قسمت To، آدرس پایان محدوده IPهای قابل تخصیص را وارد نمایید. توجه نمایید که محدوده وارد شده، بایستی در محدوده آدرس شبکه شما باشد.



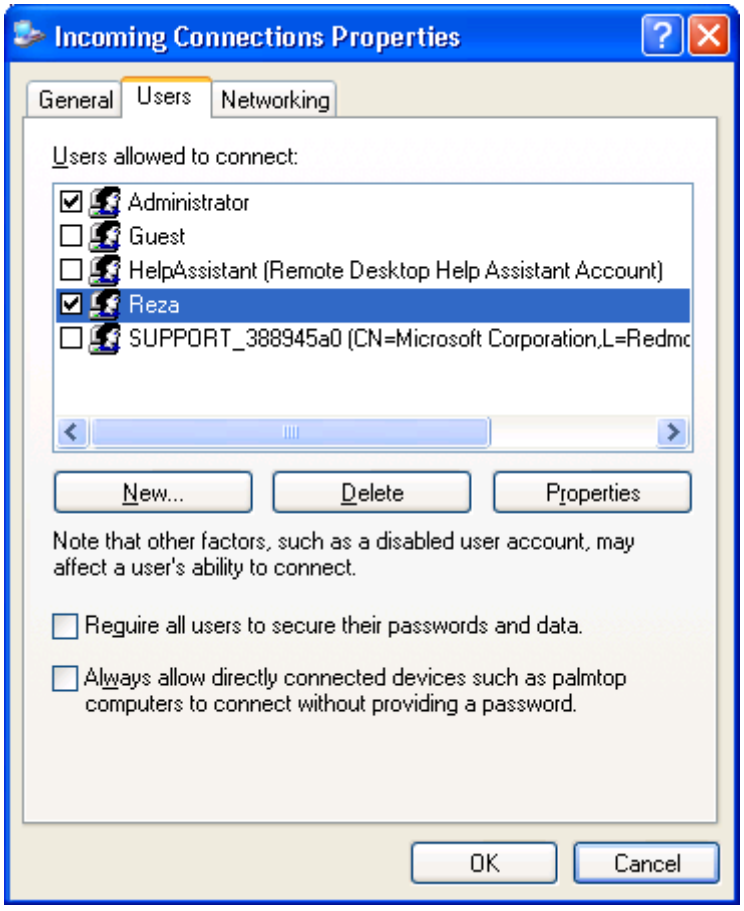
در نهایت روی دکمه Finish کلیک نمایید.



با انجام این کار، در Control Panel ➔ Network Connections، یک آیکون به نام Incoming Connections ساخته می‌شود. برای انجام تنظیمات، روی آن راست کلیک کرده و گزینه Properties را انتخاب نمایید.

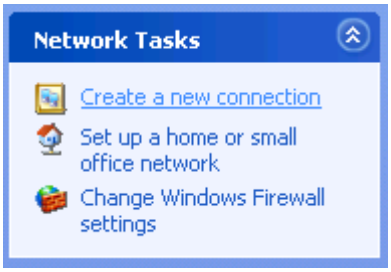


مثلاً با ورود به سربرگ Users، توانایی تعیین کاربرانی که قابلیت اتصال از راه دور را دارند، را پیدا می‌کنید.



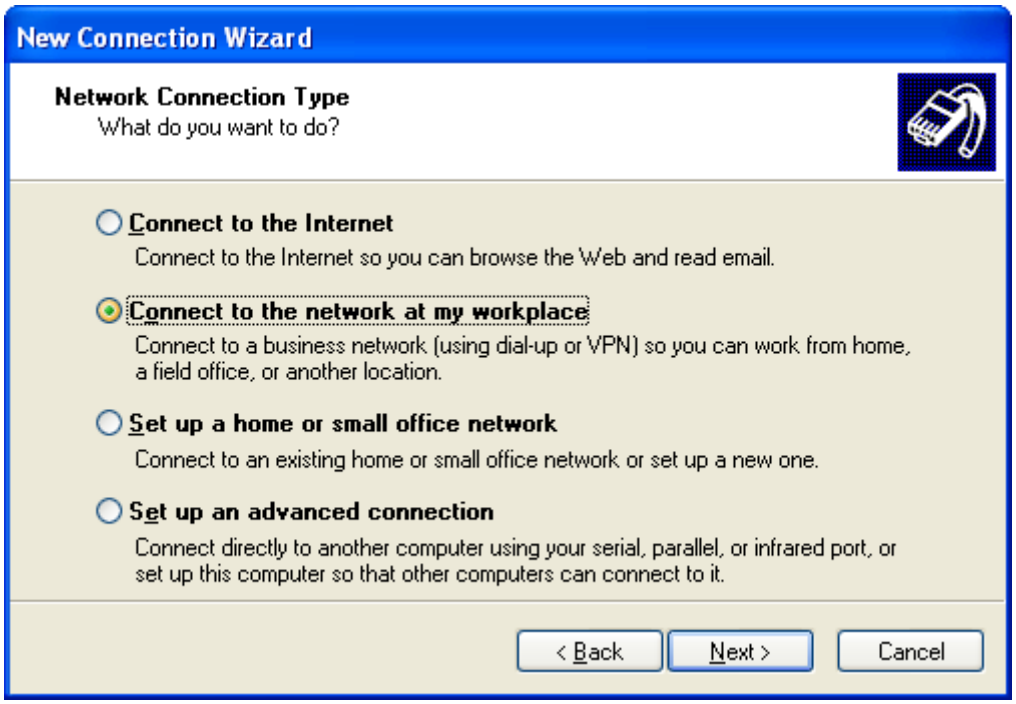
۳۲-۶- اتصال به کامپیوتر راه دور توسط Dial-UP یا VPDN

برای انجام این کار، در کامپیوتر مبدا ابتدا بایستی یک Connection بسازید. بدین منظور، وارد Control Panel ➔ Network Connections شده و روی قسمت Create a new connection کلیک کنید.



در صفحه خوش آمد گویی، روی دکمه Next کلیک کنید.

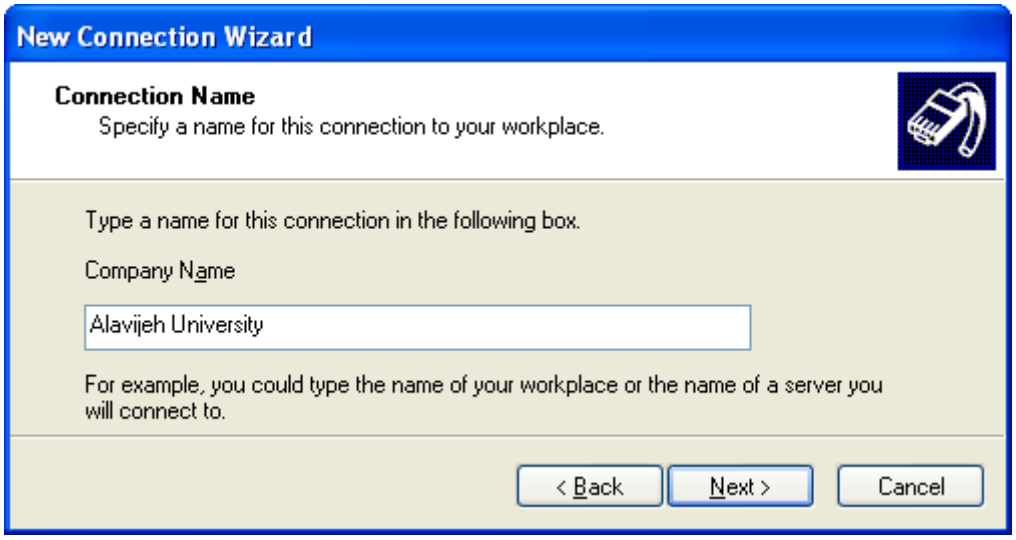
سپس گزینه Connect to the network at my workplace را انتخاب کرده و سپس Next را بزنید.



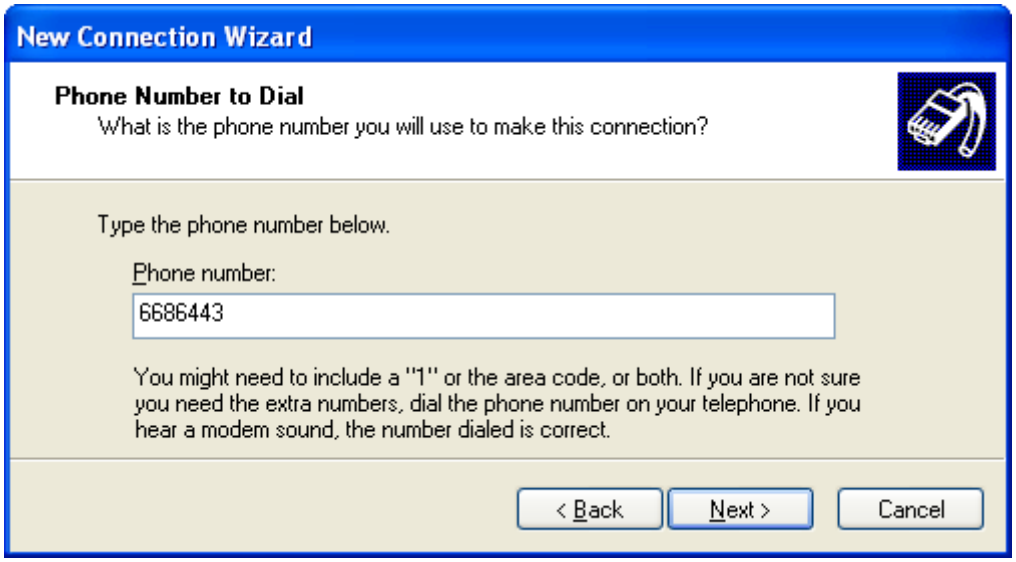
در این صفحه دو گزینه وجود دارد. گزینه اول برای VPDN و گزینه دوم برای VPN است. گزینه دوم را بعدا توضیح می‌دهید. در این قسمت گزینه Dial up connection را انتخاب کرده و Next را بزنید.



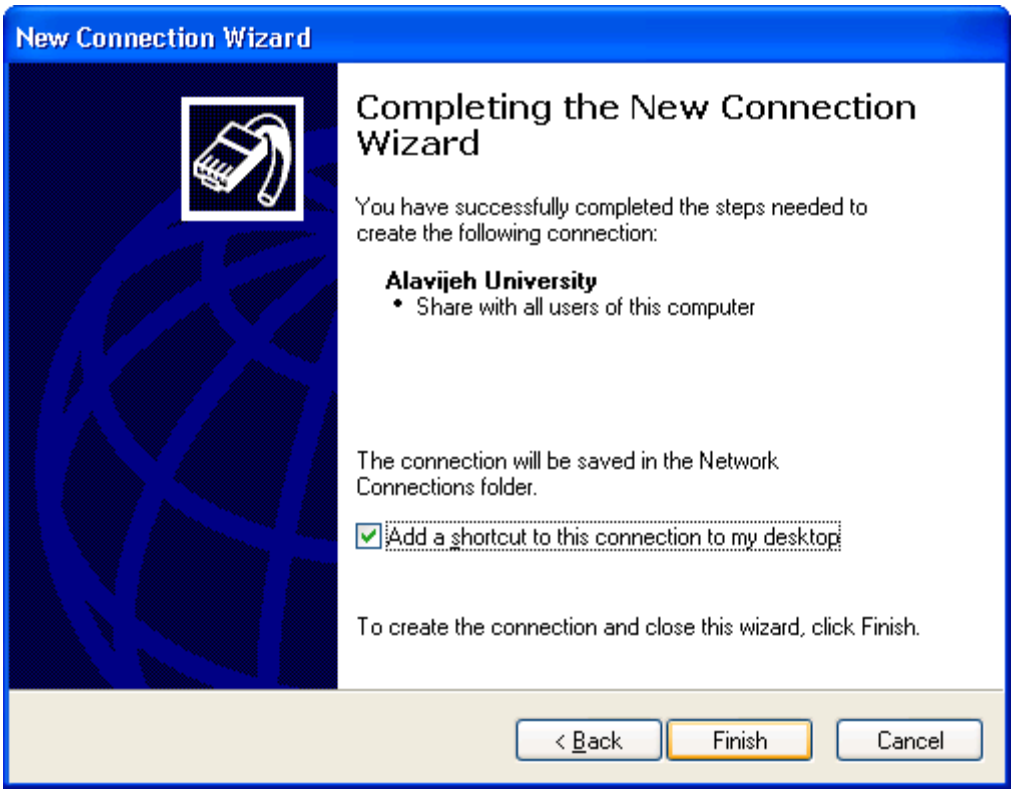
در صفحه بعد، نامی برای اتصال خود انتخاب کنید.



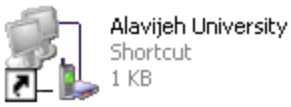
در صفحه بعد، شماره تلفن کامپیوتری که می‌خواهید به آن شماره گیری کنید را وارد نمایید. کامپیوتر مقصد بایستی توسط یک مودم Dial up به خط تلفن متصل باشد. توجه نمایید که اگر مقصد تماس درون شهری است، فقط شماره مقصد (مثلاً ۶۶۸۶۴۴۳)، اگر بین شهری است، علاوه بر شماره تلفن، کد شهر نیز نیاز است (مثلاً ۰۳۱۱۶۶۸۶۴۴۳). و اگر مقصد بین دو کشور جدا است، هم کد کشور، هم کد شهر و هم شماره تلفن مقصد مورد نیاز است (مثلاً ۹۸۳۱۱۶۶۸۶۴۴۳+ یا ۰۰۹۸۳۱۱۶۶۸۶۴۴۳).



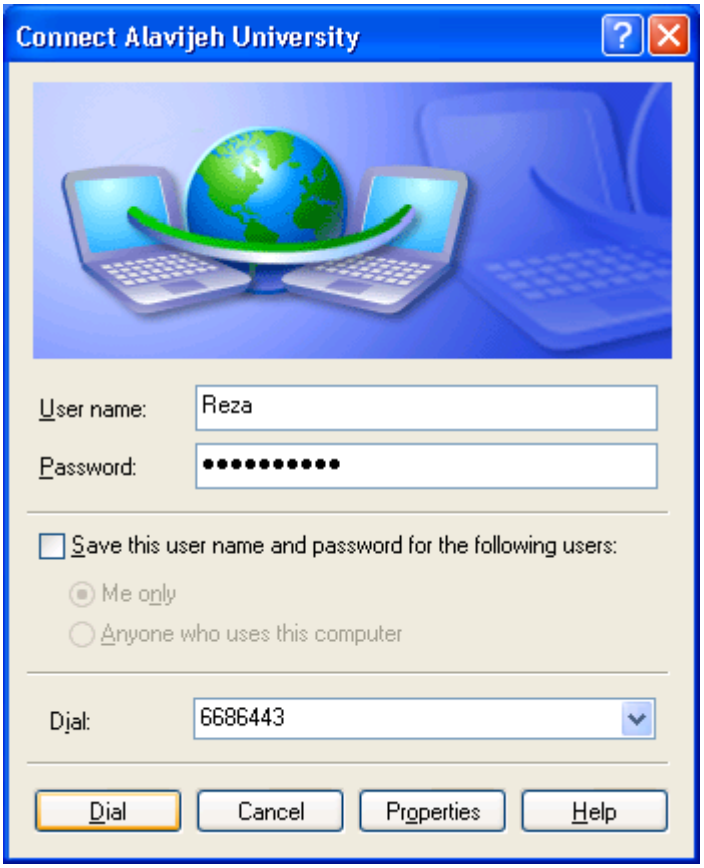
در نهایت گزینه Add a shortcut to this connection to my desktop را انتخاب کرده و روی Finish کلیک کنید.



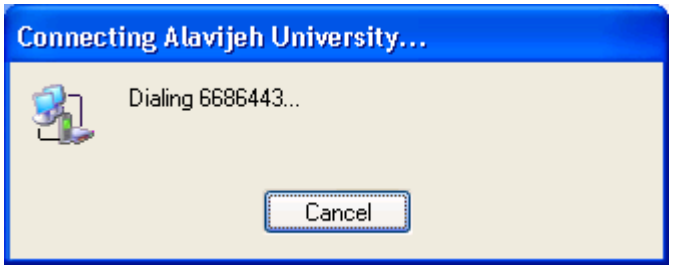
با این کار، یک آیکون در Network Connections و صفحه دسکتاپ شما ساخته می‌شود. برای اتصال آن را باز نمایید.



در صفحه باز شده، در قسمت User Name، نام کاربری و در قسمت Password، رمز عبور خود را وارد نمایید. توجه نمایید که جهت احراز هویت، این نام کاربری و رمز عبور، بایستی در کامپیوتر مقصد ثبت شده باشد. در نهایت در قسمت Dial شماره مقصد را وارد کرده (به طور پیش فرض این قسمت پر است)، و روی دکمه Dial کلیک نمایید.



با این کار سیستم شروع به شماره گیری می‌کند. در صورت تایید کامپیوتر مقصد، به آن متصل خواهید شد.



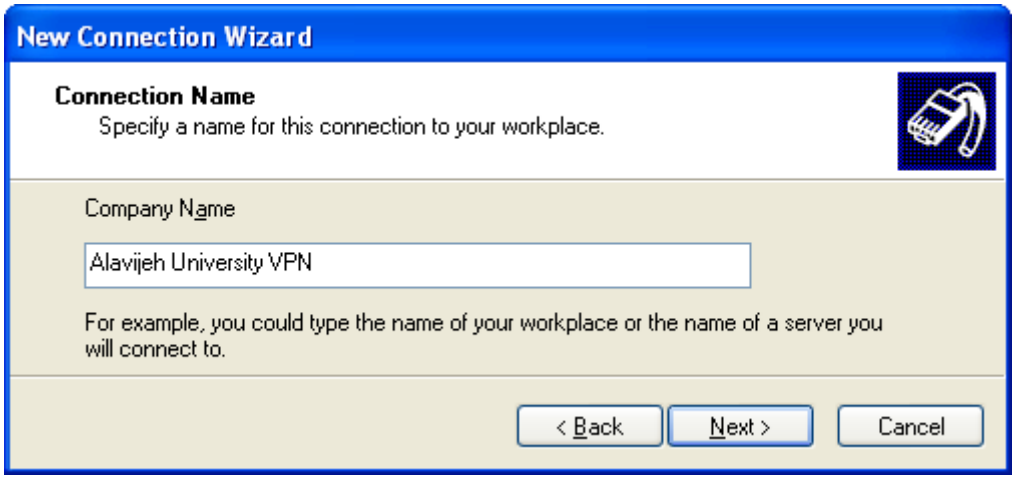
حال می‌توانید با اعضای شبکه ارتباط برقرار کنید (مثلاً توسط نرم‌افزار Netmeeting)، یا به کمک Remote Desktop می‌توانید یکی از کامپیوترها را کنترل نمایید.

۳۲-۷- اتصال به کامپیوتر راه دور توسط VPN

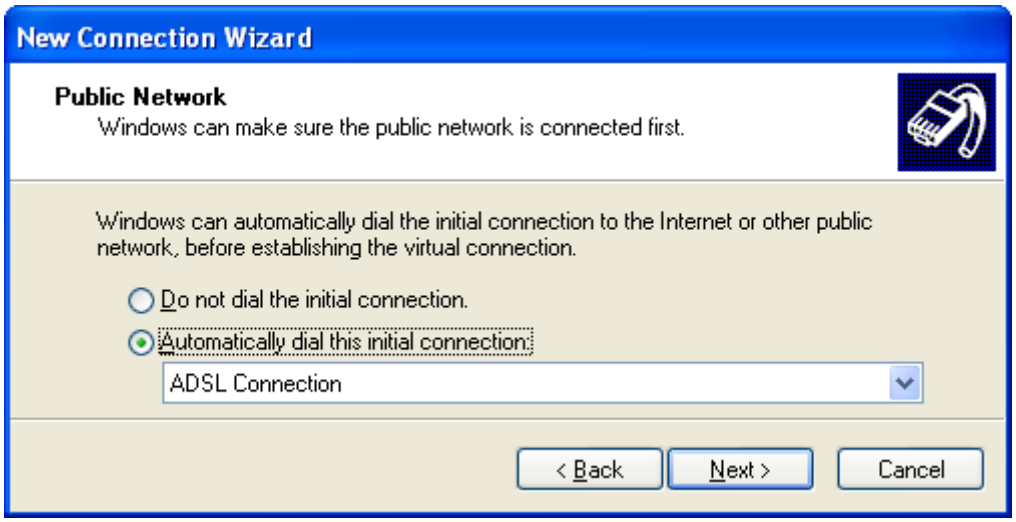
در قسمت‌های قبل گفتیم که اتصال توسط VPDN به علت هزینه‌های تلفن، مقرون به صرفه نیست. لذا از روش دیگری به نام VPN استفاده می‌کنیم. بدین منظور، در قسمت قبل هنگام ساخت Connection، به صفحه‌ای مانند زیر برخورد کردیم. این بار گزینه Virtual Private Network Connections را انتخاب کرده و روی Next کلیک کنید.



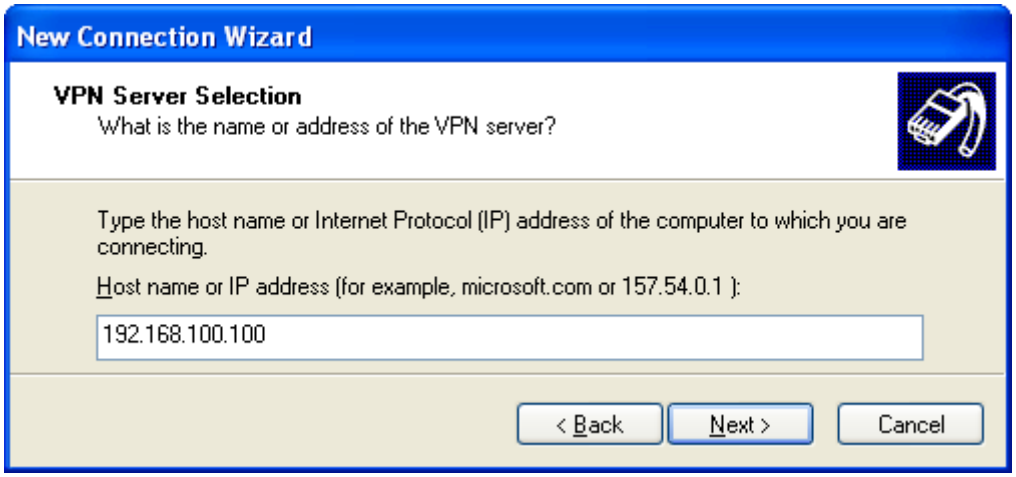
در صفحه بعد، یک نام برای Connection خود وارد نمایید.



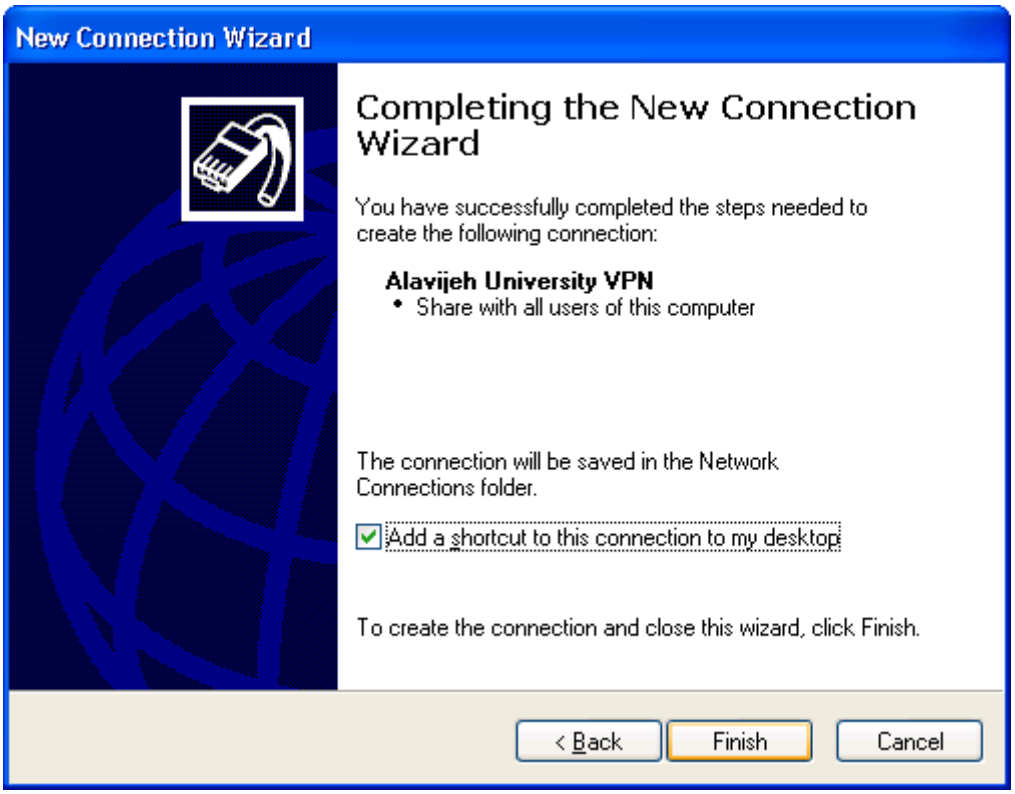
لازمه استفاده از VPN این است که سیستم مبدا و مقصد هر دو به اینترنت متصل باشند. در این صفحه مشخص می‌نمایید که هنگام استفاده از VPN، اگر سیستم شما به اینترنت متصل نبود، توسط کدام Connection به اینترنت وصل می‌شوید؟ مزیت این قسمت این است که می‌تواند یک اتصال ADSL را انتخاب نمایید.



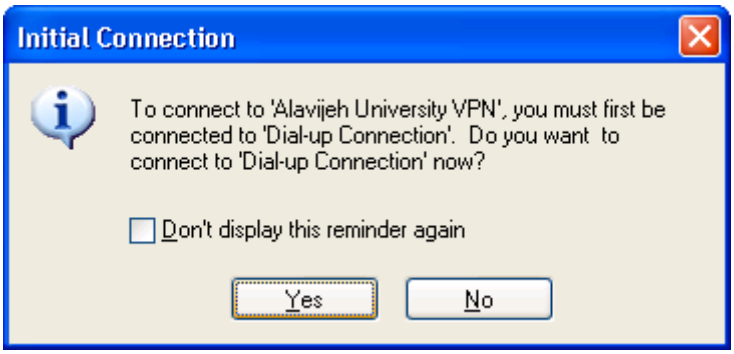
در صفحه بعد، آدرس IP کامپیوتر مقصد را وارد نمایید. همانطور که گفتیم، اتصال با VPN به کمک آدرس IP است. توجه نمایید که اگر کامپیوتر مقصد Static IP ندارد و هر بار هنگام اتصال به اینترنت، آدرس IP آن عوض می‌شود، شما نیز بایستی هر بار تنظیمات IP مربوط به Connection خود را تغییر دهید. در مورد تنظیمات جلوتر بحث می‌کنیم.



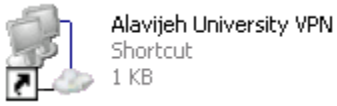
در نهایت گزینه Add a shortcut to this connection to my desktop را انتخاب کرده و روی Finish کلیک کنید.



پس از ساخت Connection، سیستم به شما پیغام می‌دهد که برای استفاده از VPN، بایستی ابتدا به اینترنت متصل شوید و از شما می‌پرسد که آیا می‌خواهد با Connectionی که مشخص کردهاید به اینترنت متصل شود؟ فعلا No را انتخاب کنید.



پس از پایان ساخت، یک آیکون در Network Connections و صفحه دسکتاپ شما ساخته می‌شود. برای اتصال آن را باز نمایید.



در صفحه باز شده، در قسمت User Name، نام کاربری و در قسمت Password، رمز عبور خود را وارد نمایید. توجه نمایید که جهت احراز هویت، این نام کاربری و رمز عبور، بایستی در کامپیوتر مقصد ثبت شده باشد. در نهایت برای اتصال روی دکمه Connect کلیک نمایید. همچنین اگر می‌خواهید تنظیماتی را انجام دهید، روی دکمه Properties کلیک نمایید.

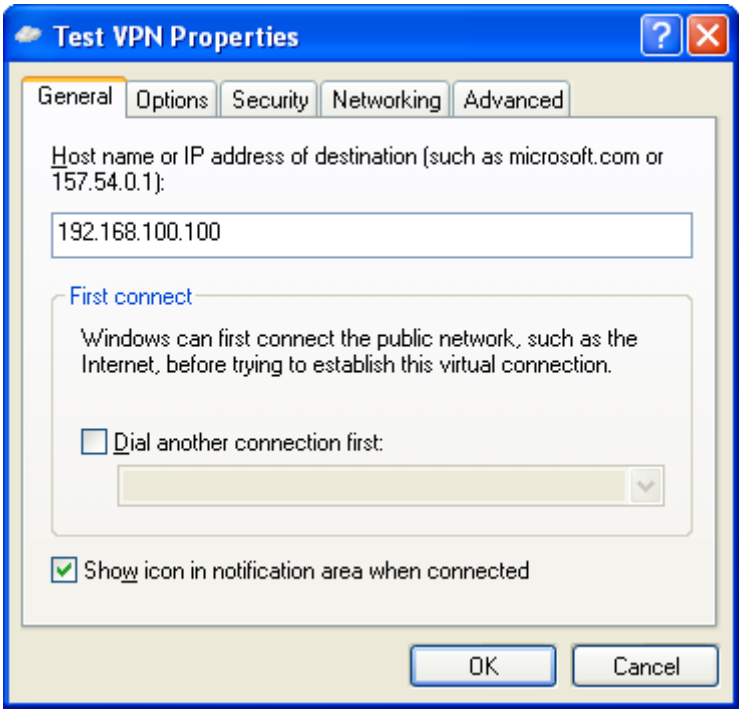


سربرگ General

همانطور که در شکل زیر ملاحظه می‌کنید، این قسمت نیاز به تنظیمات و تغییرات چندانی ندارد. اگر می‌خواهید نام و یا آدرس IP سروری که می‌خواهید به آن وصل شوید را تغییر دهید، در اولین کادر می‌توانید تغییرات را وارد نمایید. توجه نمایید که ما آدرس IP مورد نظر را قبلاً وارد کرده بودیم.

همچنین در همین صفحه و در قسمت First Connection می‌توانید تنظیم کنید که کدام یک از خطوط ISP را برای برقراری اتصال اینترنتی به VPN سرور می‌خواهید استفاده نمایید. این گزینه را نیز قبلاً تنظیم نموده‌ایم.

توجه: اگر بخواهید به VPN سرور داخل شبکه متصل شوید نیازی به تعریف این گزینه نیست. در انتها نیز گزینه‌ای مربوط به فعال یا غیر فعال کردن نمایش آیکون آداپتور شبکه در System Tray (بعد از برقراری اتصال به شبکه) می‌باشد.



سربرگ Options

همانطور که در شکل زیر مشاهده می‌نمایید، در این قسمت عملیاتی که در هنگامی برقراری اتصال انجام می‌شود، را می‌توان تنظیم نمود. برخی از این تنظیمات در قالب سوال‌های زیر نشان داده شده است.

- آیا سیستم وضعیت اتصال را به شما نشان دهد یا خیر؟
- نام کاربری، کلمه عبور و نام Domain را درخواست کند یا خیر؟

و با گزینه هایی که در قسمت Redialing Options وجود دارد، عکس العمل سیستم در مقابل عدم دریافت پاسخ از طرف سرور، را می‌توانید تنظیم نمایید:

- در صورت عدم دریافت پاسخ از سرور، چند بار سعی برای اتصال صورت گیرد؟
- تنظیم فاصله زمانی بین هر سعی با سعی دیگر
- اگر اتصال ناخواسته قطع شد، آیا مجددا برقرار شود یا خیر؟

در حالت عادی نیازی به تغییر در این برگه نیست.



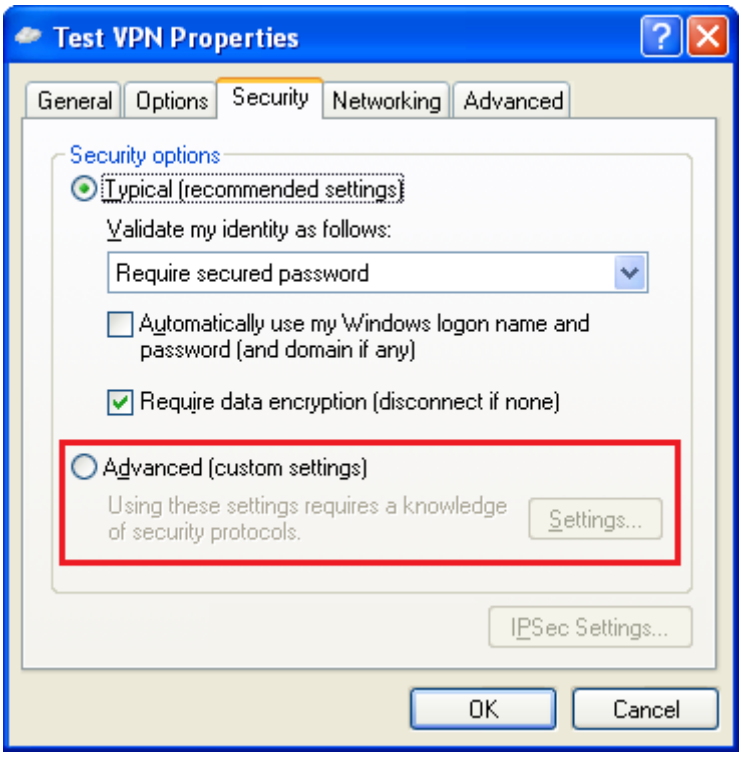
سربرگ Security

همانطور که در شکل زیر می‌بینید، در این قسمت می‌توانید امنیت اتصال خود را تنظیم کنید. اگر طبق دستور العمل‌های داده شده در VPN Server تنظیمات را انجام داده باشید نیازی به تغییر در اینجا احساس نمی‌شود، مگر اینکه بخواهید امنیت بیشتری را در نظر بگیرید. برای انجام این کار گزینه Advanced را انتخاب نموده و سایر تنظیمات را برحسب نیاز انجام دهید. (توضیحات تک تک گزینه‌های آن خارج ار بحث این جزوه می‌باشد).

توجه: این گزینه زیر را **فعال نکنید**:

Automatically use my Windows logon name and password

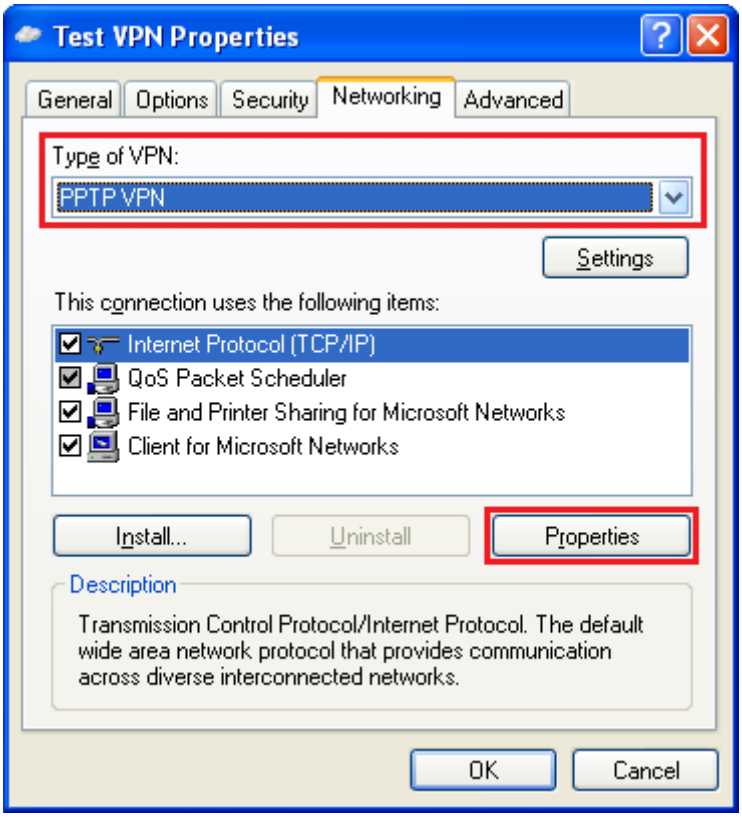
اگر این گزینه در کامپیوتر فعال باشد و این کاربر به قصد استراحت، برای مدت کوتاهی کامپیوتر را رها کرده باشد، هر کسی می‌تواند از طریق این کامپیوتر به شبکه (VPN Server) وصل شود. زیرا با فعال کردن این گزینه عملاً نیاز به تایپ نام کاربری و کلمه عبور برای ورود به سرور را از بین برده‌اید.



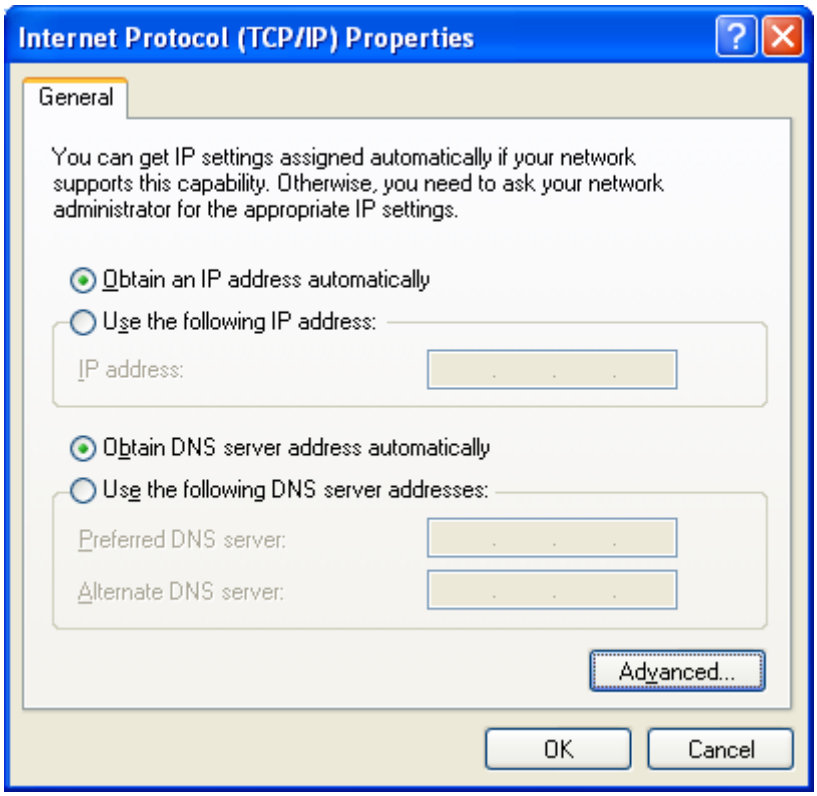
سربرگ Networking

در این قسمت تنظیمات مختلفی می‌توان انجام داد. همانگونه که در شکل زیر می‌بینید، اولین تنظیم مربوط به نوع اتصال VPN شما می‌باشد. به صورت پیش فرض Automatic انتخاب شده است که هر دو حالت PPTP VPN و L2TP VPN را به ترتیب بررسی می‌نماید.

PPTP برای کاربردهای عمومی و غیر حرفه‌ای مناسب‌تر می‌باشد. پروتکل L2TP که به وسیله شرکت CISCO ارائه شده است به لحاظ امنیتی بسیار قدرتمندتر است. پروتکل دیگری به نام IPSec پایه ریزی شده است که پیچیدگی‌های خاصی دارد. ما در اینجا از پروتکل PPTP استفاده می‌کنیم که تنظیمات راحت تری دارد. PPTP مخفف Point-To-Point Tunneling Protocol است.



یکی دیگر از تنظیمات، تعیین این است آیا می‌خواهید برای اتصال به شبکه VPN از Default Gateway استفاده شود یا نه؟ برای این کار می‌توانید، با توجه به شکل فوق، پس از انتخاب Internet Protocol (TCP/IP) دکمه Properties را بزنید. در صفحه باز شده، روی Advanced کلیک کنید.



در این صفحه، گزینه Use default Gateway on remote network به صورت پیش فرض تیک خورده و فعال است. ممکن است که برایتان این سوال پیش بیاید که چه زمانی این گزینه فعال و چه زمانی غیر فعال کنیم؟

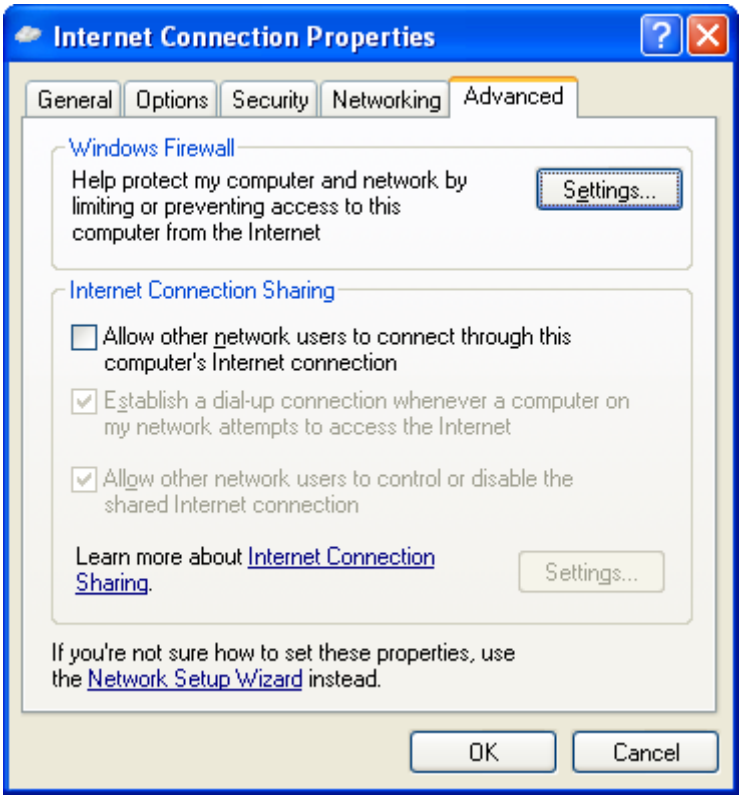
بعضی از کاربران در خانه، و یا بعضی‌ها در کافی نت‌ها و یا هتل و غیره... و از راه اینترنت به VPN وصل می‌شوند. اینگونه افراد برای اتصال به شبکه VPN، در واقع از راه دور (Remote) به VPN Server وصل می‌شوند. بنابرین با فعال کردن این گزینه یک مسیری برای آن‌ها ایجاد کرده‌اید که بتوانند بدون مشکل وصل شوند.

توجه: برای کاربران داخلی (کاربران داخل شبکه) که از یک محدوده خاصی از IP آدرس استفاده می‌کنند، گزینه "Use default Gateway on remote network" را غیر فعال کنید.



سربرگ Advanced

در اتصال معمولی و ساده به شبکه VPN، این قسمت نیاز به تنظیمات خاصی ندارد. در این صفحه امکان انجام تنظیمات امنیتی و به اشتراک گذاری اتصالات اینترنت وجود دارد.

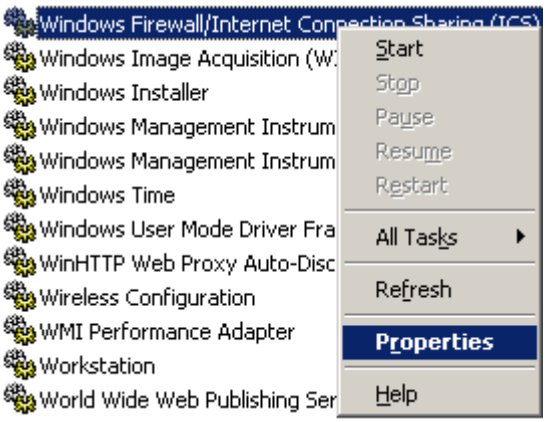


بعد از انجام تنظیمات لازم، نوبت به برقراری ارتباط می‌رسد. دکمه Connect در پنجره اصلی را بزنید. چنانچه تنظیمات VPN Server و VPN Client را به درستی انجام داده باشید. اتصال با موفقیت انجام می‌شود و آیکونی مشابه آیکون اتصال به اینترنت در System Tray ظاهر می‌شود. که می‌توانید خصوصیات اتصال خود را با زدن دکمه Properties مشاهده کنید. با این اتصال مانند آن است که خود در سرور قرار گرفته باشید. و از امکانات آن استفاده نمایید.

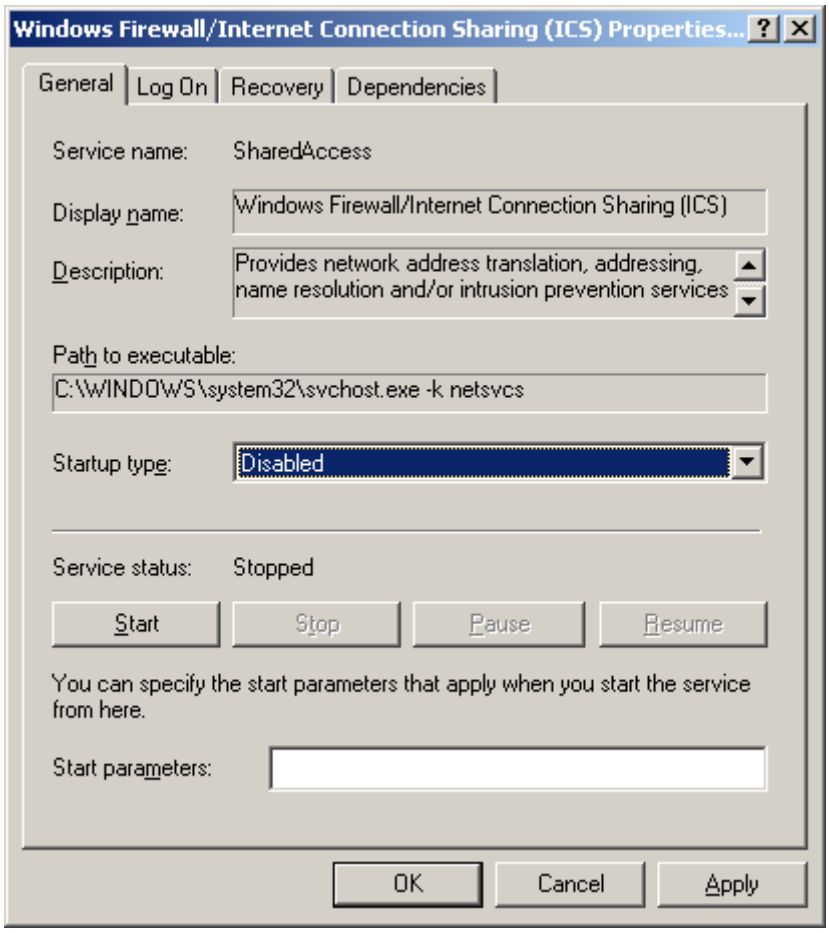
۳۲-۸- نصب VPN Server روی ویندوز سرور

۳۲-۸-۱- غیر فعال کردن سرویس Firewall و ICS

برای راه اندازی VPN Server، ابتدا بایستی سرویس Windows Firewall/Internet Connection Sharing را غیر فعال کنید. بدین منظور ابتدا وارد Control Panel ➔ Administrative Tools ➔ Services شده، روی سرویس مذکور راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



سپس در قسمت Startup type، گزینه Disabled را انتخاب کنید. همچنین با کلیک روی دکمه Stop، سرویس مذکور را غیر فعال نمایید. در نهایت روی OK کلیک کنید.



۳۲-۸-۲- نصب VPN Server

برای اعطای نقش Remote Access/VPN Server به ویندوز سرور ۲۰۰۳ یا به عبارت دیگر برای نصب و راه اندازی VPN Server باید ویزارد Configure Your Server Wizard را از مسیر زیر احضار کنیم:

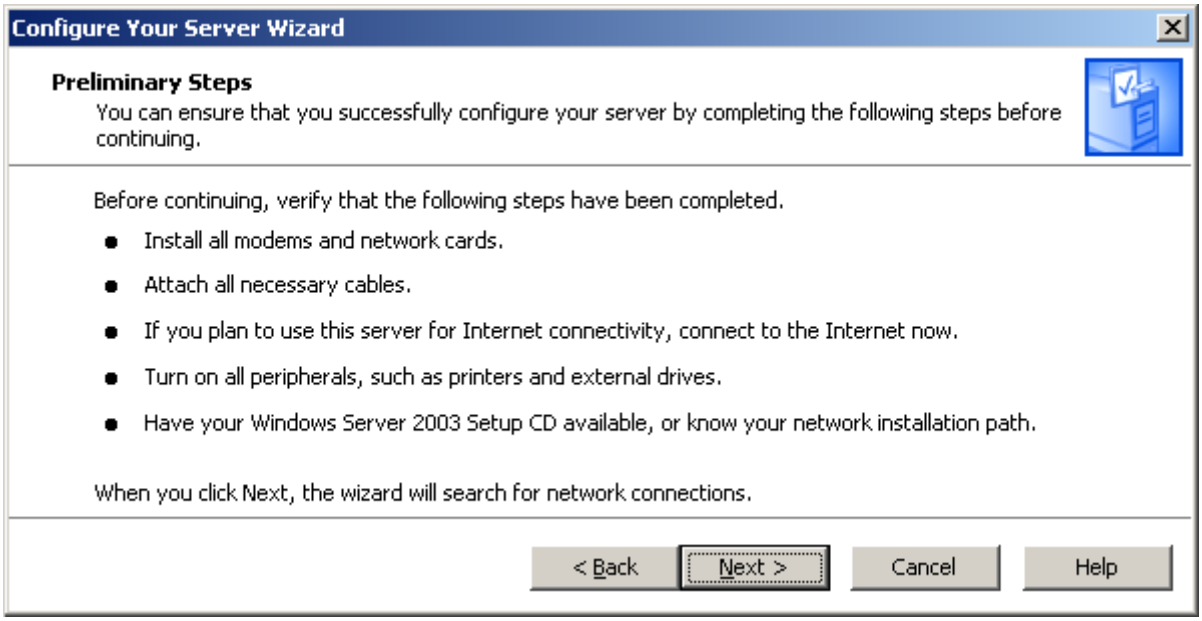
Start ➔ Administrative Tools ➔ Configure Your Server Wizard

اولین پنجره‌ای که ظاهر می‌شود، اطلاعات اولیه‌ای در مورد این ویزارد را نشان می‌دهد.

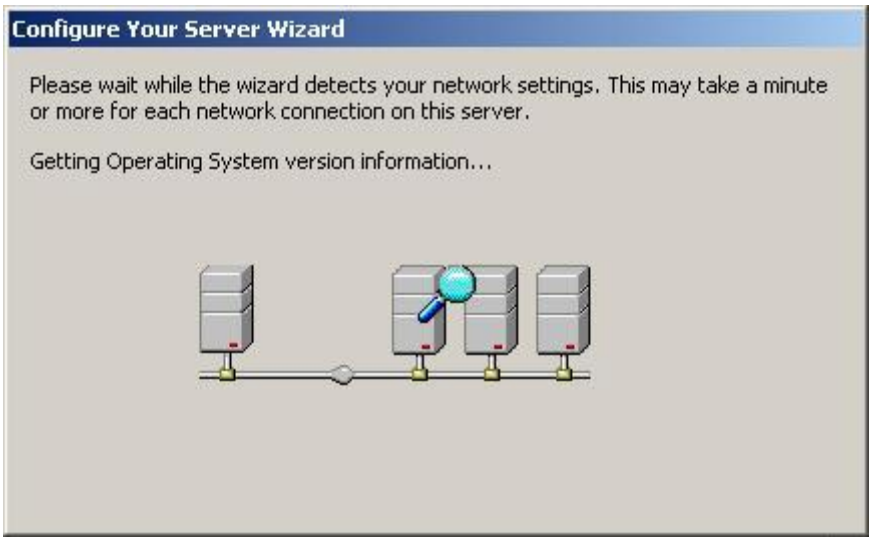
پنجره Preliminary Steps مواردی که لازم است قبل از شروع ویزارد انجام دهید را باز گو می‌کند مثلاً:

- اطمینان از نصب مودم‌ها و کارت‌های شبکه
- اگر ویزارد را برای اتصال به اینترنت می‌خواهید، از اتصال خود به اینترنت اطمینان حاصل کنید.
- و یا اینکه CD نصب ویندوز را آماده داشته باشید و غیره....

در این صفحه، روی دکمه Next کلیک کنید.



این صفحه نیز به صورت خودکار بسته خواهد شد.



پنجره Server Role سومین پنجره‌ای است که ظاهر می‌شود. همانطور که در شکل زیر مشاهده می‌کنید، لیستی از نقش هایی که روی سیستم می‌توانید اعمال کنید نشان داده شده است که در ستون مقابل هر کدام، وضعیت آن Role را از لحاظ اینکه این نقش اعطا شده است یا نه نشان داده شده است. برای اعطای نقش Remote Access / VPN به ویندوز، این مورد را از لیست انتخاب کرده و دکمه Next را بزنید.

Server Role	Configured
File server	Yes
Print server	No
Application server (IIS, ASP.NET)	Yes
Mail server (POP3, SMTP)	Yes
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	Yes
DNS server	Yes
DHCP server	No
Streaming media server	No
WINS server	No

پنجره بعدی ویزارد، توضیح مختصری درباره این نقش میدهد. پس از مطالعه آن دکمه Next را بزنید.

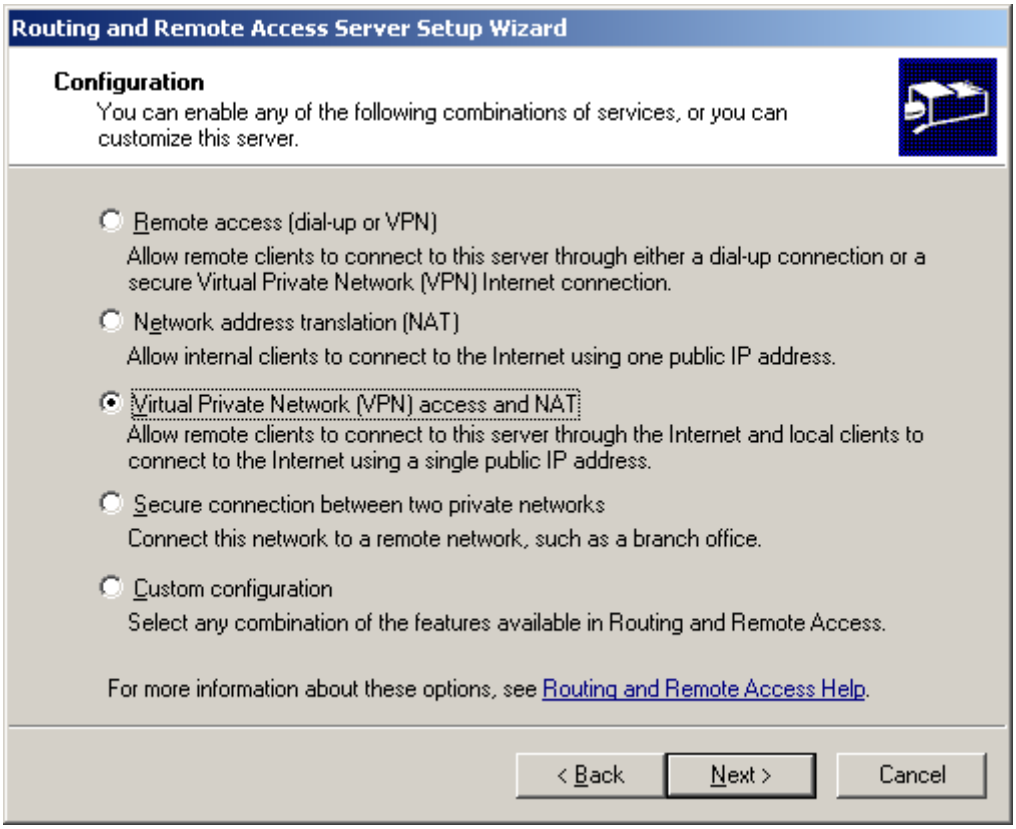
ویزاردی با نام Routing and Remote Access Wizard ظاهر می‌شود (ویزارد RRAS) که در ادامه به آن اشاره می‌شود.

۳۲-۸-۳- تنظیمات Routing and Remote Access (ویزارد RRAS)

مانند تمام ویزاردها، اولین پنجره این ویزارد، توضیح و نکات مختصری راجع به آن می‌باشد که ما با مطالعه آن و زدن دکمه Next از آن می‌گذریم.



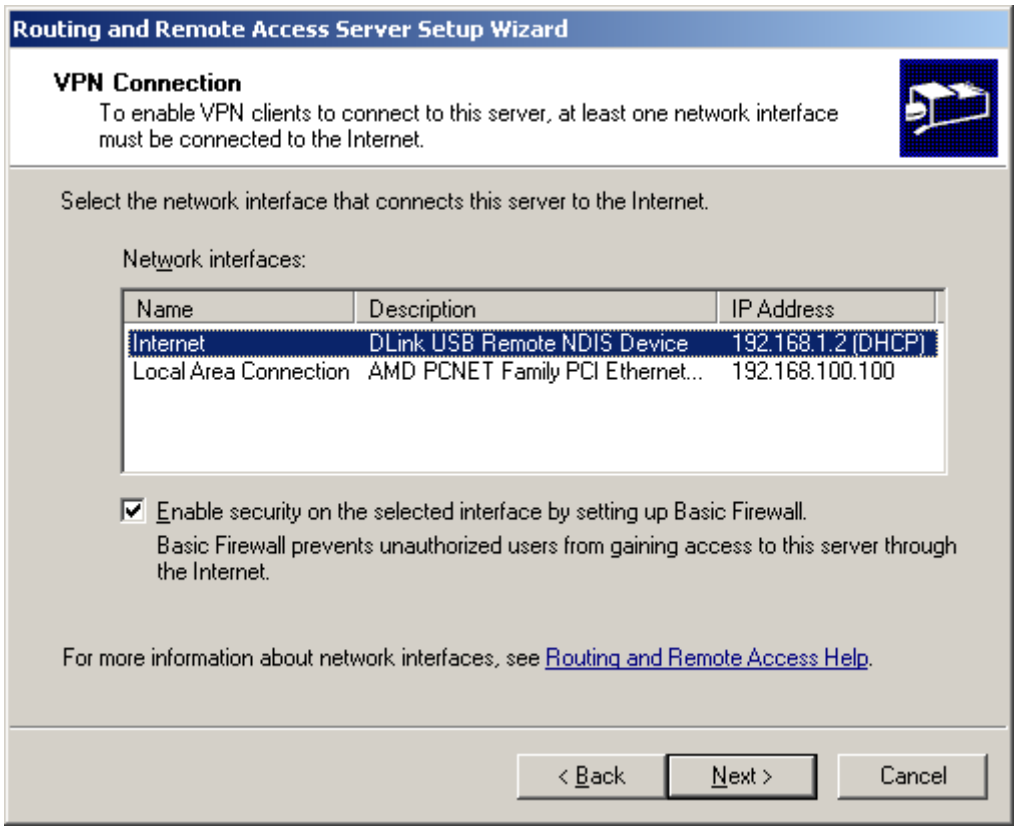
در پنجره بعدی یعنی پنجره Configuration، گزینه‌های مختلفی وجود دارد که با توجه به نوع اتصال از راه دور (Remote Access Connection) یکی از گزینه‌ها را انتخاب می‌کنیم. و چون قصد ما در اینجا راه اندازی VPN بر اساس PPTP می‌باشد ما گزینه Virtual Private Network VPN and NAT را انتخاب کرده و Next می‌زنیم.



توجه نمایید که برای راه اندازی VPN Server، حداقل به دو کارت شبکه نیاز دارید. یکی برای اتصال به اینترنت و دیگری برای اتصال به شبکه محلی. در غیر اینصورت، قادر به نصب VPN Server نخواهید بود.

مطابق شکل زیر و در پنجره VPN Connection **باید آداپتور یا Deviceی که با آن به اینترنت وصل می‌شوید را تعیین کنید.** نکته‌ای که در اینجا قابل توجه می‌باشد این است که برای برقراری امنیت بیشتر و در واقع برای کنترل دقیق تر، بهتر است که کارت شبکه مستقلی را برای VPN Server در نظر بگیرید. که در اینجا ما کارتی غیر از کارت شبکه‌ای که برای اتصال کاربران محلی انتخاب می کنیم.

گزینه Enable security on the selected interface by setting up Basic Firewall را تیک بزنید. این گزینه به عنوان یک Firewall نرم‌افزاری فعال شده و سرور شما از نفوذ خرابکاران و حملات مخرب آن‌ها از راه اینترنت در امان نگه می‌دارد. هر چند، نصب فایروال‌های پیشرفته و مستقل و یا یک فایروال سخت‌افزاری برای شبکه‌های محرمانه ضروری می‌باشد (و این بستگی به درجه اهمیت شبکه و اطلاعات موجود در آن دارد).



مطابق شکل زیر، باید تنظیم نمایید که از کدام کارت شبکه برای کاربران محلی شبکه استفاده می‌کنید. اگر دو کارت شبکه بیشتر نداشته باشید، شکل زیر را مشاهده نخواهید نمود؛ زیرا یک کارت شبکه برای اینترنت و دیگری برای سرویس دهی به کاربران VPN استفاده می‌شود.



همانطور که یک کاربر محلی برای برقراری اتصال با سرور و سایر کلاینت‌های موجود در شبکه نیاز به داشتن یک IP Address در همان محدوده دارد (یعنی باید قسمت Net ID آدرس‌های IP آن‌ها یکسان باشد)، VPN Clientها نیز در هنگام برقراری اتصال به VPN Server، نیاز به یک IP Address دارند که بتوانند به منابع مجاز در سرور دسترسی داشته باشند. در اینجا شما به عنوان مدیر شبکه با انتخاب یک روش از دو راه موجود، نحوه واگذاری آدرس IP به کلاینت‌های VPN را تعریف می‌کنید.

۱. با نصب و تعریف DHCP که در فصول قبل توضیح داده شد و اعمال تنظیمات لازم، سرور خود را به عنوان DHCP Server تعریف می‌کنید، به طوری که کاربران در هنگام برقراری اتصال به سرور شما از محدوده IP هایی که در سرور تعریف کرده‌اید، یکی را به خود اختصاص می‌دهند. با انتخاب گزینه Automatically روند واگذاری IP آدرس از روی تنظیمات DHCP Server انجام می‌گیرد.

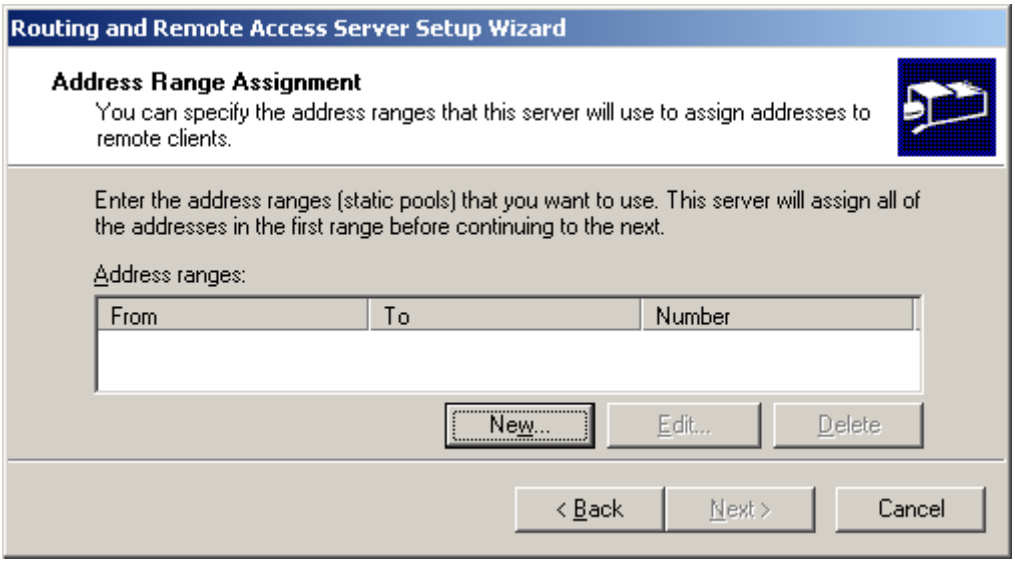
۲. تعیین محدوده خاصی از IP آدرس هایی که به کاربران واگذار شود.

ما در اینجا گزینه دوم را انتخاب می‌کنیم. به این دلیل که می‌خواهیم با استفاده از محدوده خاصی از IP آدرس‌ها که انتخاب می‌کنیم، کاربران شبکه محلی که به سرور وصل می‌شوند را از کاربرانی که از اینترنت (VPN Client) وصل می‌شوند تشخیص دهیم.



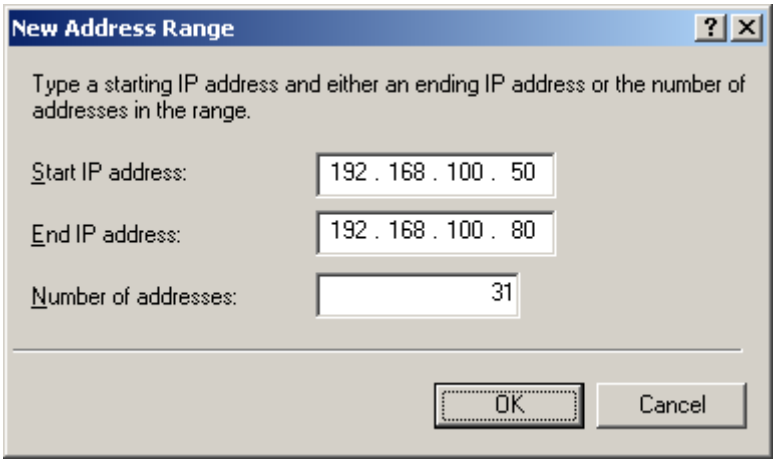
پس از انتخاب گزینه دوم (یعنی From a specified range of addresses)، دقیقا تعریف می‌کنید که چه آدرس IPهایی را به VPN Server اختصاص می‌دهید که سرور به Clientها واگذار نماید.

برای اینکار دکمه New در پنجره Address Range Assignment را بزنید.



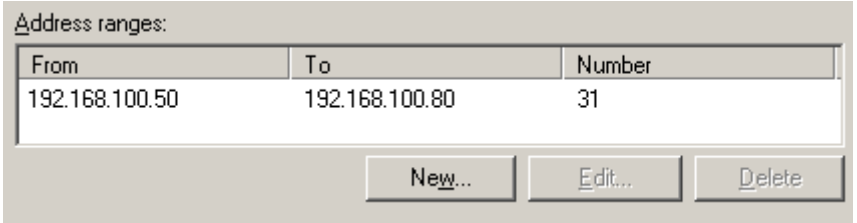
در پنجره باز شده، محدوده اولین و آخرین آدرس IP را تعیین کنید. بدین ترتیب، کاربران پس از اتصال به سرور به کمک VPN، یکی از آدرس‌های موجود در این محدوده را دریافت می‌کنند.

فیلد Number of addresses به صورت اتوماتیک با توجه به محدوده انتخابی شما تعیین می‌شود. می‌توانید فقط اولین آدرس IP را بنویسید و تعداد آدرس IPها را مشخص کنید؛ ویزارد محاسبات را انجام داده و آدرس IP پایانی را خودش وارد می‌کند. دکمه OK را بزنید تا تنظیمات شما ثبت شود.

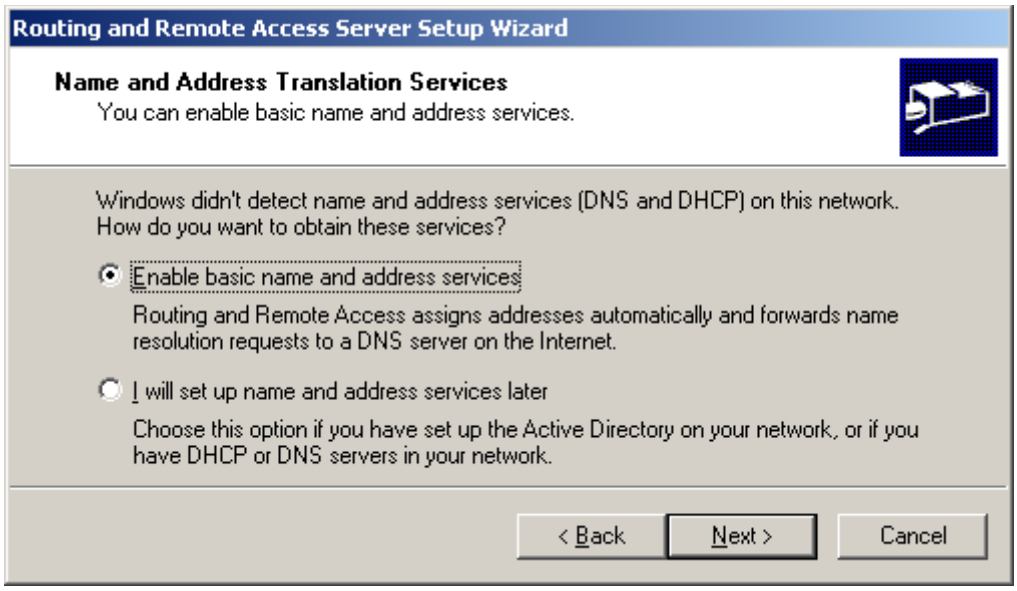


نکته مهم: دقت فرمایید که محدوده آدرس وارد شده، تداخلی با آدرس کامپیوتر هایی که اکنون به صورت محلی با کامپیوتر سرور شبکه هستند، نداشته باشد.

بدین ترتیب، محدوده وارد شده به لیست محدودههای آدرس IP اضافه می‌شود.



در مرحله بعدی، سیستم بررسی می‌نماید تا ببیند که آیا DNS Server و DHCP Server در شبکه شما وجود دارد یا خیر؟ اگر وجود نداشته باشد، صفحه زیر نشان داده می‌شود. با انتخاب گزینه اول، می‌توان این سرویس‌ها را نصب نمود. با انتخاب گزینه دوم، به سرور می‌گوییم که این تنظیمات را بعدا به صورت دستی انجام خواهیم داد.



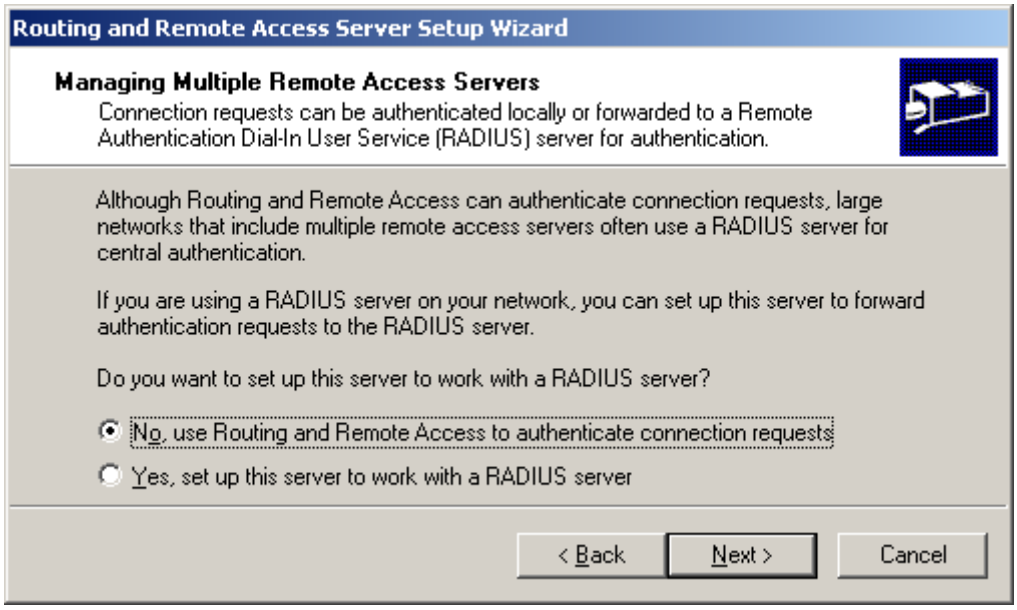
در پنجره بعدی، آدرس شبکه مجازی که به وجود خواهد آمد را مشاهده خواهید نمود.



در پنجره بعدی اطلاعات اعتبار سنجی را مشاهده خواهید نمود. اعتبار سنجی (Authentication) یا بازرسی کاربران VPNای که به سرور شما وصل می‌شوند بسیار مهم است. برای این اعتبار سنجی و برقراری امنیت دو گزینه را می‌توانید انتخاب نمایید:

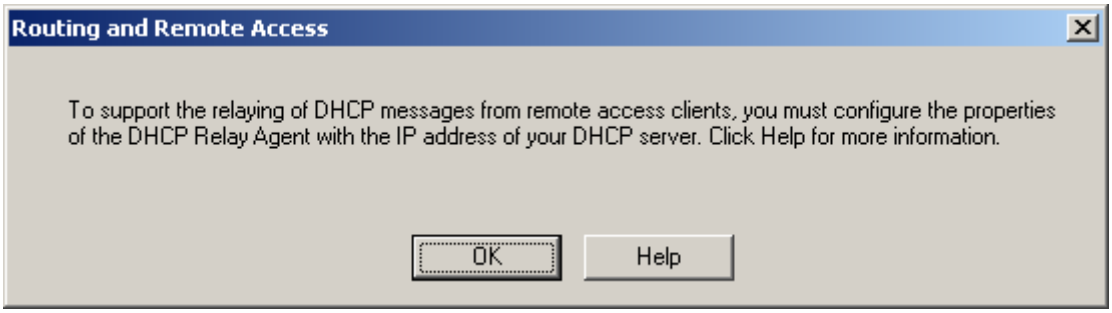
۱. اگر در شبکه سرویس دهنده RADIUS داشته باشید، می‌توانید تنظیم کنید که VPN سرور شما، برای اعتبار سنجی کاربران خود از RADIUS استفاده کند. بدین معنی که اگر یک RADIUS سرور مرکزی در شبکه تان داشته باشید، اعتبار سنجی تمام کاربران شبکه برای بررسی به این سرور فرستاده تا برای ورود به Server VPN، تایید صلاحیت و یا رد صلاحیت شوند. با این روش کاربران در بین تمام سرورهای VPN به اشتراک گذاشته شده و نیازی به تعریف کاربران در تمامی سرورها نمی‌باشد.
۲. اما گزینه دوم، تمام تقاضاها برای اتصال به VPN Server، از طریق خود سرور و تنظیماتی که در آن نظر گرفته است، مورد بررسی قرار گیرند.

که مطابق شکل زیر، ما اولین گزینه را انتخاب کرده و دکمه Next را می‌زنیم.

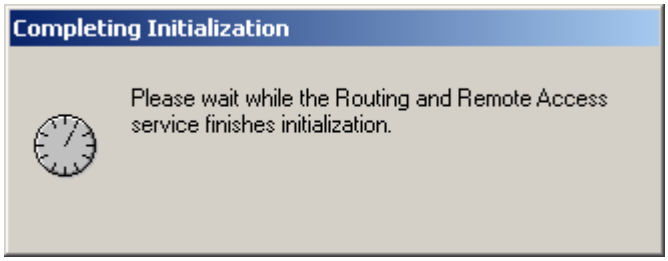


در انتها ممکن است که پنجره‌ای ظاهر گردد که فقط کافی است دکمه OK را بزنید.

سپس پیامی در مورد پیکربندی DHCP Relay Agent می‌بینید. روی OK کلیک کنید. در مورد DHCP Relay Agent بعدا بیشتر صحبت خواهیم کرد.



صبر نمایید تا سیستم عملیات نصب را به اتمام برساند. این کار ممکن است تا چند دقیقه به طول بیانجامد.

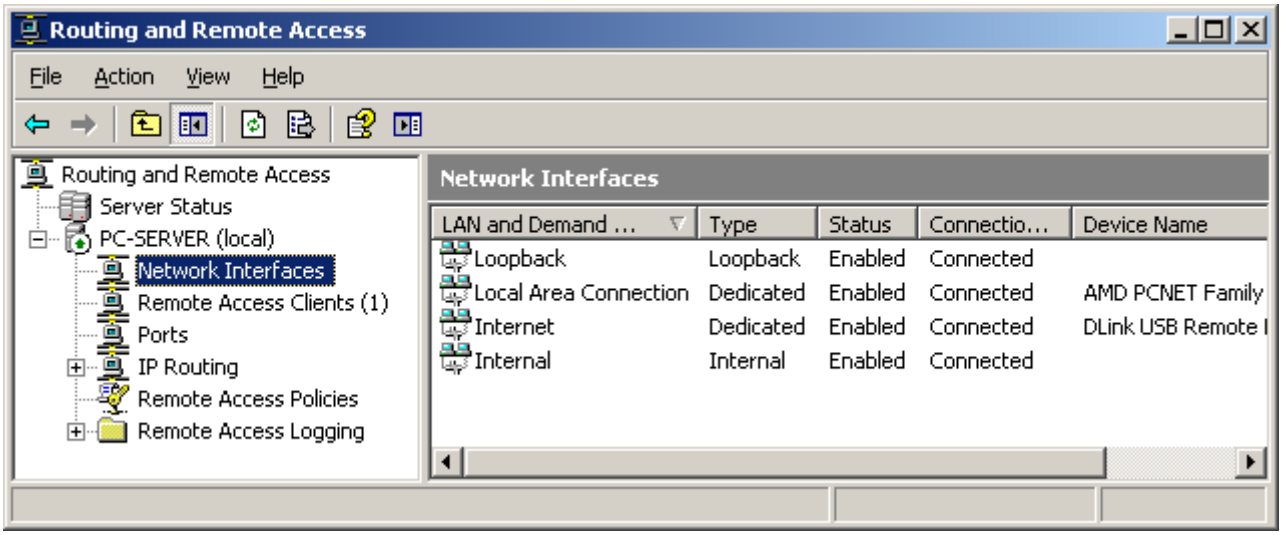


تا این مرحله تنظیمات مربوط به ویزارد نصب RRAS به پایان رسیده و نقش Remote Access / VPN Server به ویندوز ۲۰۰۳ اعطا شده است. اما برای دیدن نتیجه کار پنجره Routing and Remote Access را از مسیر زیر باز کنید.

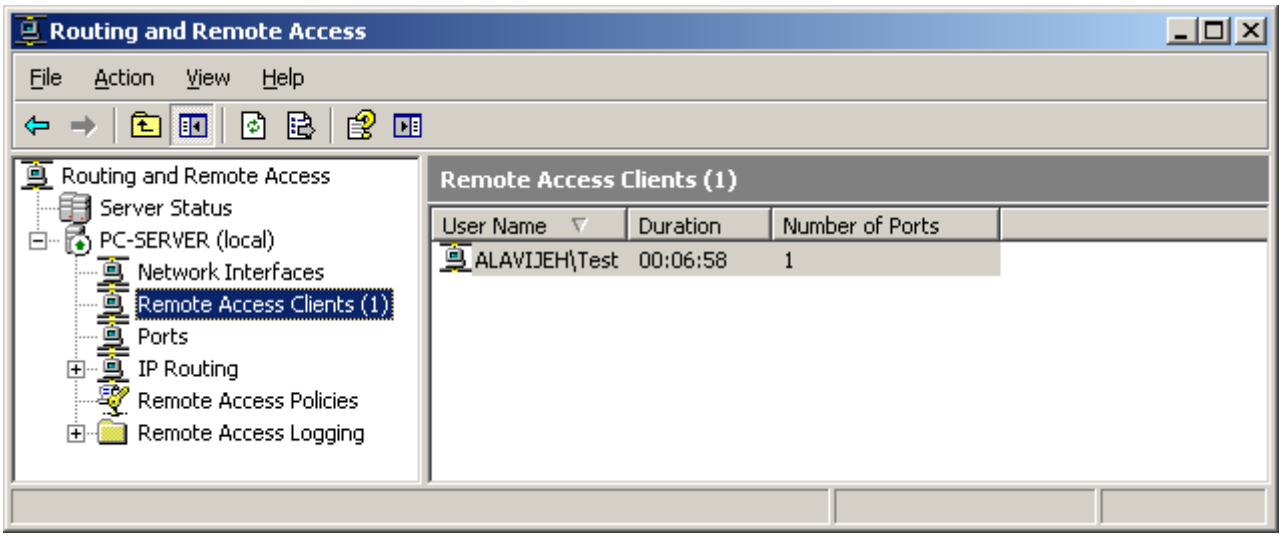
Start ➔ Administrative Tools ➔ Routing and Remote Access



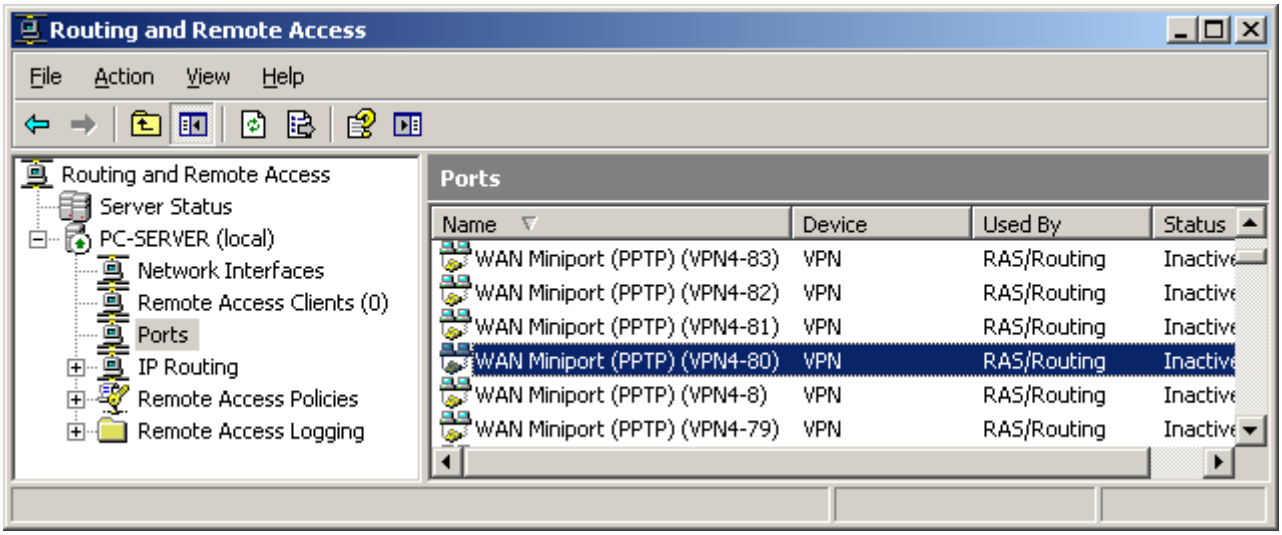
با این کار، صفحه تنظیمات Routing and Remote Access باز می‌شود؛ که همانطور که از شکل پیداست، این صفحه دارای چندین قسمت می‌باشد. قسمت Network Interface بیانگر واسط‌های شبکه‌ای می‌باشد که در حال حاضر روی سیستم وجود دارند.



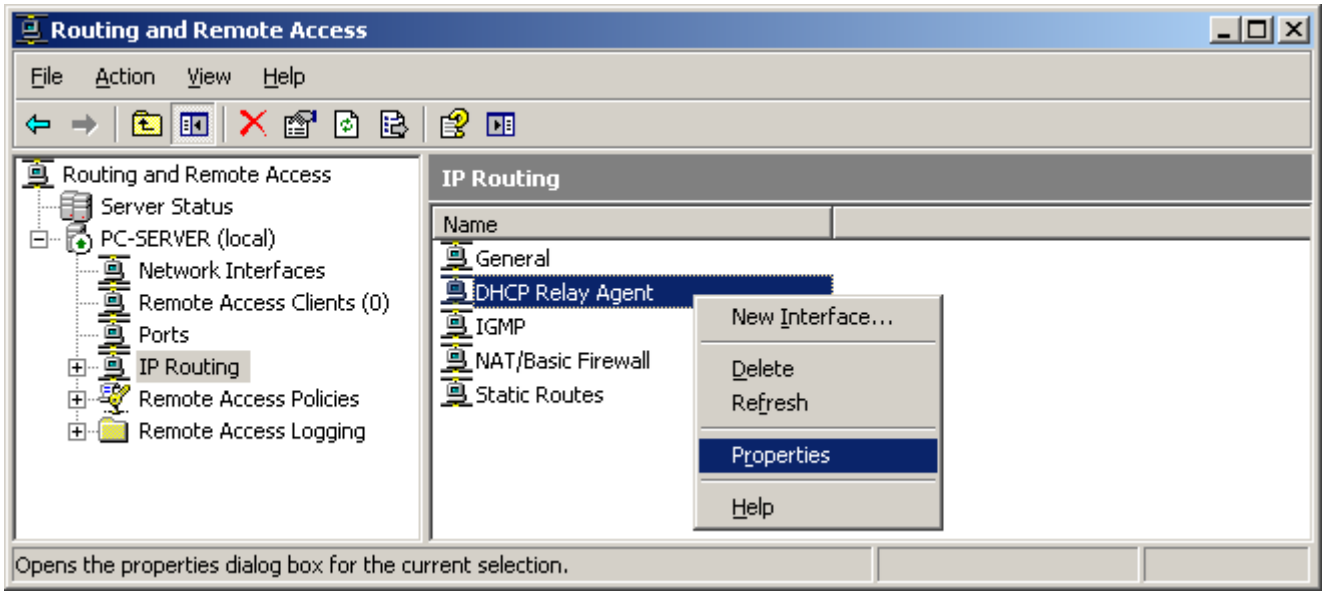
قسمت Remote Access Clients نیز بیانگر کاربرانی می‌باشد که در حال حاضر از راه دور به سرور (شبکه مجازی) متصل شده‌اند. از طریق این صفحه می‌توان ارتباط این کاربران را قطع نمود



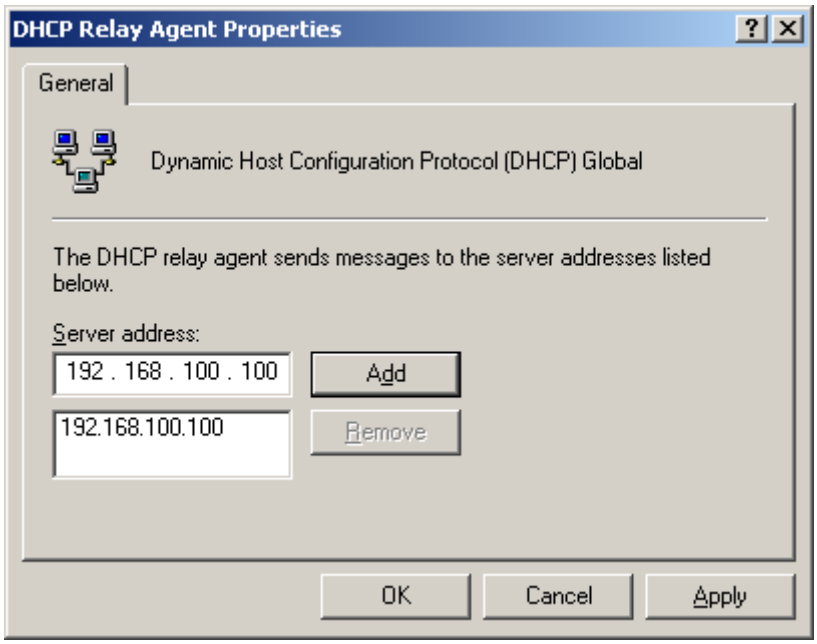
در صفحه بعد می‌توانید پورت‌های قابل استفاده توسط VPN Server را مشاهده نمایید.



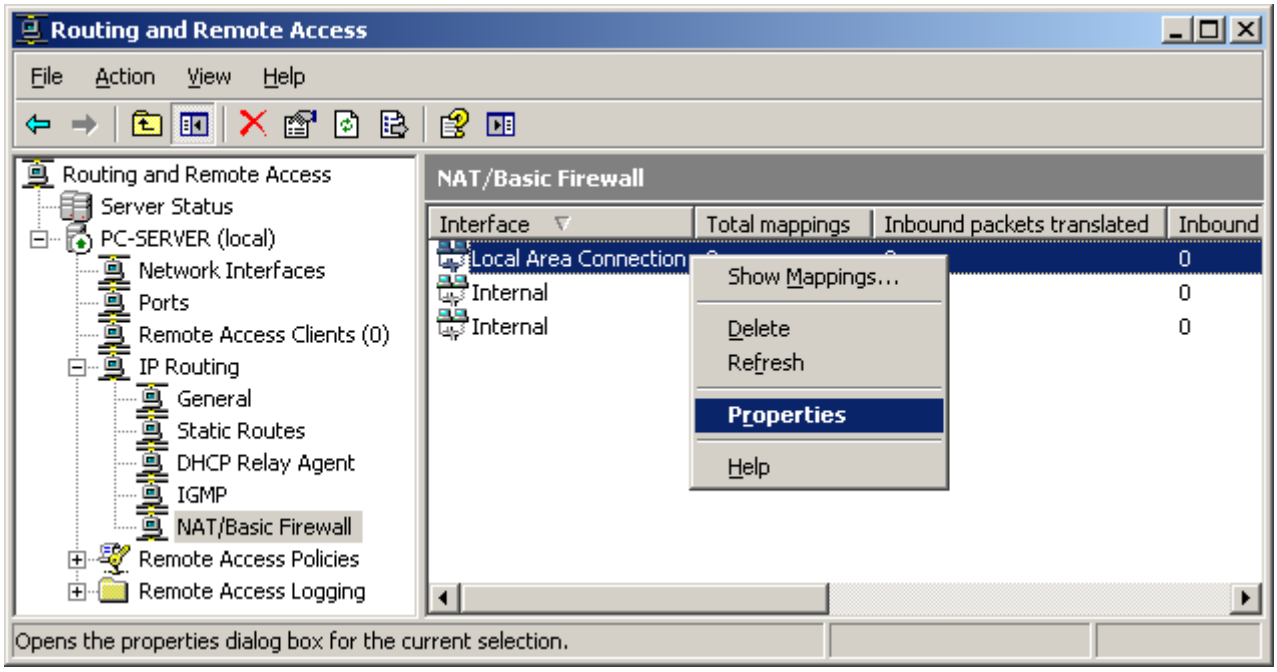
شاید مهمترین قسمت تنظیمات Routing and Remote Access، بخش DHCP Relay Agent باشد. بدین منظور از قسمت IP Routing، روی DHCP Relay Agent راست کلیک نموده و گزینه Properties را انتخاب نمایید.



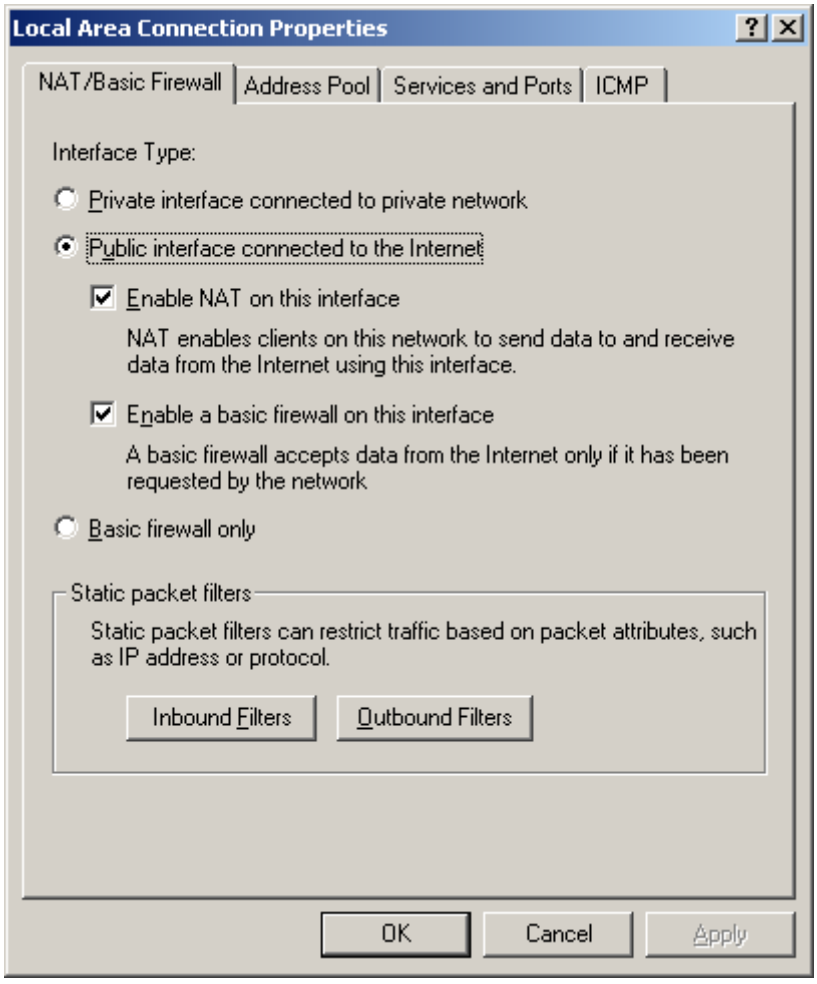
سپس این صفحه، آدرس IP کامپیوتر DHCP Server را به لیست اضافه نمایید. با این کار، سرور شما به عنوان DHCP Relay Agent شناخته می‌شود و می‌تواند آدرس IP را با پروتکل DHCP دریافت نماید.



قسمت بعدی که نیاز به معرفی دارد، بخش NAT/Basic Firewall می‌باشد. از این بخش برای تعیین نقش هر یک از کارت‌های شبکه و پروتکل‌های آن، استفاده می‌شود. بدین منظور در قسمت IP Routing، ابتدا NAT/Basic Firewall را انتخاب نموده و سپس یکی از کارت‌های شبکه خود را انتخاب نمایید. سپس روی کارت شبکه انتخاب شده، کلیک راست کرده و سپس گزینه Properties را انتخاب نمایید.



سپس در صفحه باز شده، وارد سربرگ NAT/Basic Firewall شود. در این سربرگ، می‌توان نقش کارت شبکه انتخاب شده را تعیین نمود.



این نقش‌ها به صورت زیر می‌باشد:

- **Private Interface connected to private network**: با این گزینه، تعیین می‌کنید که این کارت شبکه، یک کارت شبکه معمولی (عدم اتصال به اینترنت) می‌باشد که از آن برای اتصال به شبکه خصوصی استفاده می‌شود.
- **Public interface connected to internet**: با این گزینه تعیین می‌کنید که این کارت شبکه، کارت شبکه متصل به اینترنت می‌باشد؛ یعنی از طریق این کارت می‌توان به اینترنت دسترسی داشت. انتخاب گزینه Enable NAT on this device، باعث می‌شود که این کارت شبکه نقش NAT Server را نیز بازی کند و در نتیجه کاربرانی که به کمک VPN به سرور متصل می‌شوند، بتوانند به اینترنت نیز دسترسی داشته باشند. انتخاب گزینه Enable a basic firewall on this device نیز باعث می‌شود که این کارت شبکه، علاوه بر اتصال به اینترنت، نقش دیوار آتشین را نیز بازی کند.
- **Basic firewall only**: از این کارت شبکه، تنها به عنوان یک دیوار آتشین استفاده می‌شود.

۳۲-۹- تنظیمات کاربران جهت اتصال راه دور به VPN

در ویندوز ۲۰۰۳ بطور پیش فرض، به کاربران اجازه دسترسی به سرور از راه VPN داده نشده است. شما باید به صورت تک به تک، برای هر یک از کاربرانی که می‌خواهید از راه اینترنت به سرور شما وصل شوند این اجازه را بدهید. برای این کار مراحل زیر را انجام دهید:

اگر در سرور، Domain Controller تعریف کرده باشید (نصب و راه اندازی کامل Domain Controller در فصول پیش، به طور مفصل توضیح داده شده است)، پنجره Active Directory Users and Computers را از مسیر زیر باز کنید.

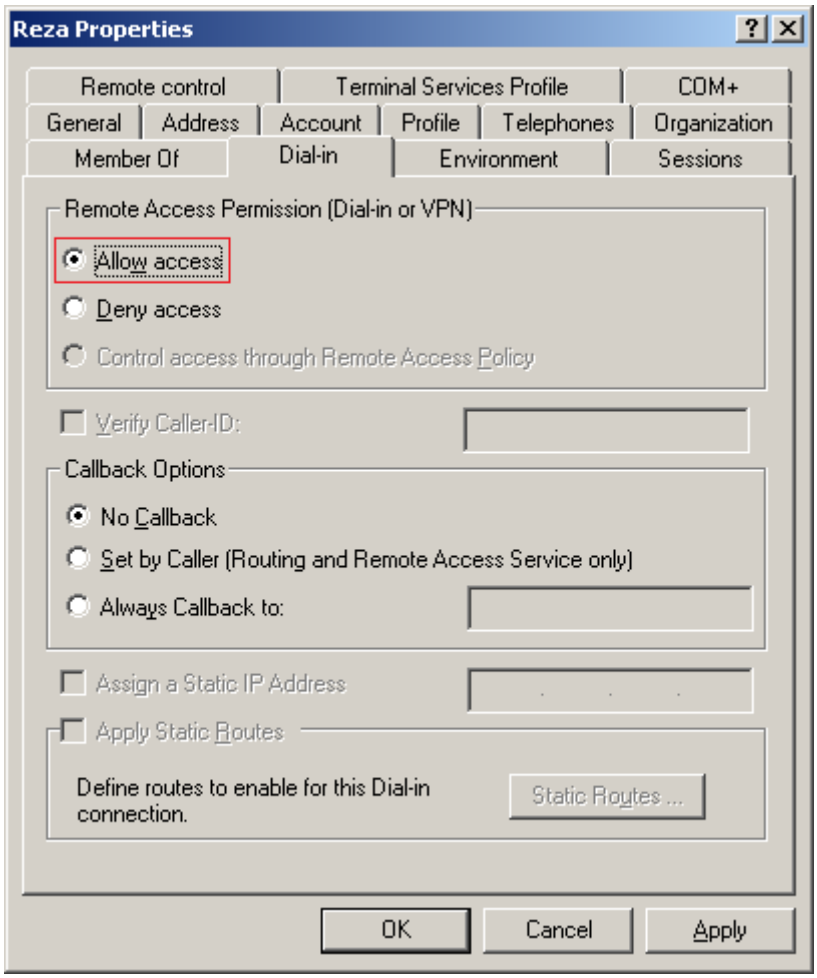
Start ➔ Administrative Tools ➔ Active Directory Users and Computers

در غیر اینصورت و اگر سرور شما در هیچ Domainای تعریف نشده باشد (و سرور به صورت Standalone باشد)، پنجره Computer Management را از مسیر زیر:

Start ➔ Administrative Tools ➔ Computer Management

باز کنید و صفحه Properties مربوط به کاربری که می‌خواهید اجازه اتصال به VPN سرور خود را به آن بدهید، را باز کنید و مطابق شکل زیر به قسمت Dial-In بروید و گزینه "Allow access" را انتخاب نمایید.

از طریق این صفحه می‌توانید تنظیمات امنیتی بیشتری را نیز اعمال نمایید. مثلاً از طریق قسمت Callback Option می‌توان تنظیم کرد که پس از اتصال Client به سرور، سرور اتصال را قطع نموده و خود را به کامپیوتری خاص متصل نماید؛ اگر کاربر از همان کامپیوتر خاص به سرور متصل شده باشد، قابلیت کار با سرور را پیدا خواهد نمود. یعنی با این کار، کاربر را موظف می‌کنیم که از کامپیوتری خاص به سرور متصل شود. بدین منظور در قسمت Always Callback To، شما تماس کامپیوتر Client را وارد نمایید. این شماره می‌تواند شماره تلفن خطی باشد که کاربر به کمک آن به اینترنت متصل شده است.



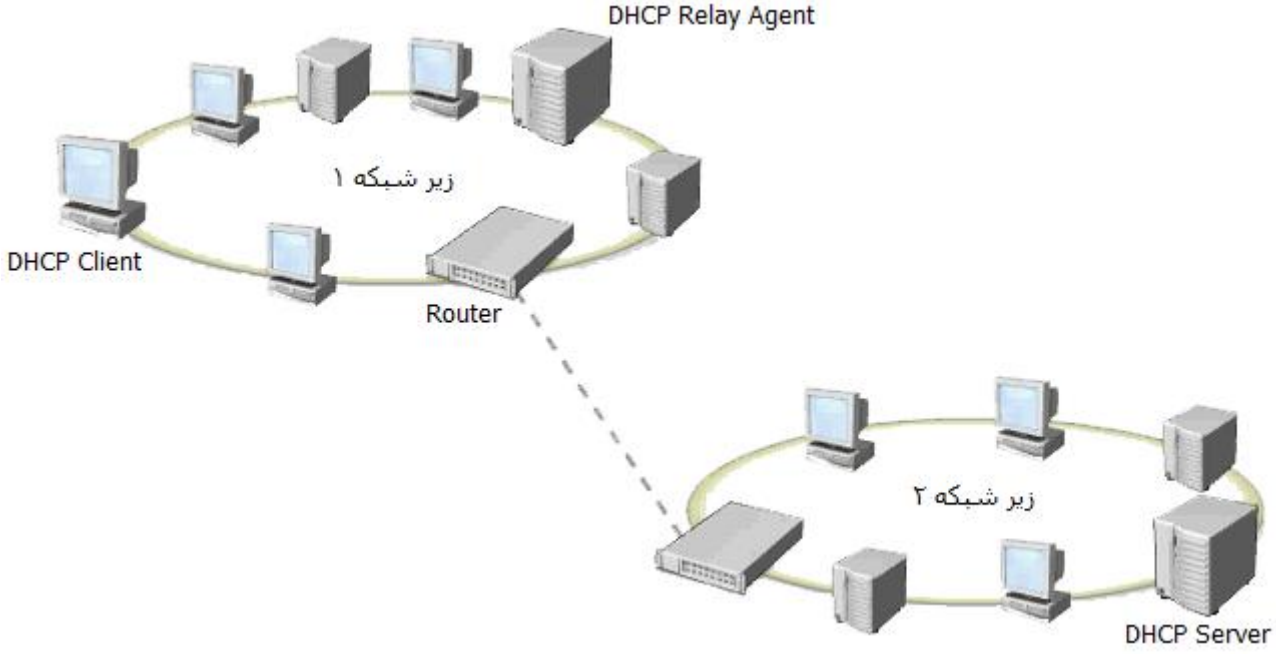
به خاطر بسپارید که پیاده سازی VPN بار زیادی را روی پردازنده سرور می‌گذارد و هر چقدر تعداد ارتباطات VPN بیشتر باشد بار زیادتری بر روی سرور خواهد گذاشت. می‌توانید از یک وسیله سخت‌افزاری مجزا مانند روتر جهت پیاده سازی VPN کمک بگیرد.

حال برای اتصال به VPN Server، بایستی در دیگر کامپیوترها یک اتصال بسازید که نحوه ساخت آن را در همین فصل توضیح داده‌ایم.

۳۲-۱۰- معرفی DHCP Relay Agent و نحوه نصب آن

اگر بخواهیم DHCP Relay Agent را مختصرا توضیح دهیم، باید بگوییم که درخواست دریافت آدرس IP توسط Client، به صورت **Broadcast** به تمامی کامپیوترهای شبکه ارسال می‌شود. در VPN ما با اینترنت سر و کار داریم و در مسیر اینترنت تعداد زیادی روتر وجود دارد. روترها، بر عکس سوییچ‌ها، قابلیت ارسال بسته‌های Broadcast را ندارند. لذا در VPN Server که از اینترنت استفاده می‌کند، قابلیت سرویس دهی DHCP Server وجود ندارد. لذا ما از یک DHCP Relay Agent استفاده می‌کنیم تا کار سرویس دهی DHCP Server را انجام دهد. این سرور بسته‌های Broadcast را به یک بسته خاص تبدیل نموده و آن را به DHCP Server تحویل می‌دهد. بعد از به دست آوردن آدرس IP از DHCP Server، آن را به Client تحویل می‌دهد. Client از جزئیات این کار مطلع نمی‌شود.

شکل زیر مفهوم DHCP Relay Agent را بهتر نشان می‌دهد. DHCP Relay Agent زمانی کاربرد دارد که دو زیر شبکه داشته باشیم و این دو زیر شبکه، به کمک مسیر یاب (Router) به یکدیگر متصل شده باشند. مشکل زمانی پیش می‌آید که یک کامپیوتر موجود در یکی از زیر شبکه‌ها درخواست آدرس IP کند، اما DHCP Server در زیر شبکه‌ای دیگر باشد. پیغام درخواست آدرس IP به صورت Broadcast به همه ارسال می‌شود، اما روترها قابلیت عبور بسته‌های Broadcast را ندارند (مگر اینکه برای این کار پیکربندی شده باشند)؛ لذا درخواست آدرس IP به زیر شبکه دیگر که DHCP Server در آن قرار دارد ارسال نمی‌شود. برای حل این مشکل، بایستی از DHCP Relay Agent استفاده نمود. بدین صورت که DHCP Relay Agent در زیر شبکه‌ای قرار می‌گیرد که Client (درخواست کننده) در آن قرار دارد. به هنگام درخواست آدرس IP توسط Client و به صورت Broadcast، چون DHCP Relay Agent آدرس DHCP Server را دارد، DHCP Relay Agent این پیام را به صورت Unicast به روتر می‌دهد و روتر نیز آن را به DHCP Server می‌دهد. DHCP Relay Agent پس از دریافت پاسخ از DHCP Server، آدرس دریافت شده را به Client تحویل می‌دهد.



در ادامه به چگونگی پیاده سازی DHCP Relay Agent می‌پردازیم.

برای پیاده سازی DHCP Relay Agent، دو راه داریم:

۱. از روترهای فیزیکی و سخت‌افزاری استفاده کرده و گزینه‌ی Relay DHCP Packets را روی آن فعال می‌کنیم.

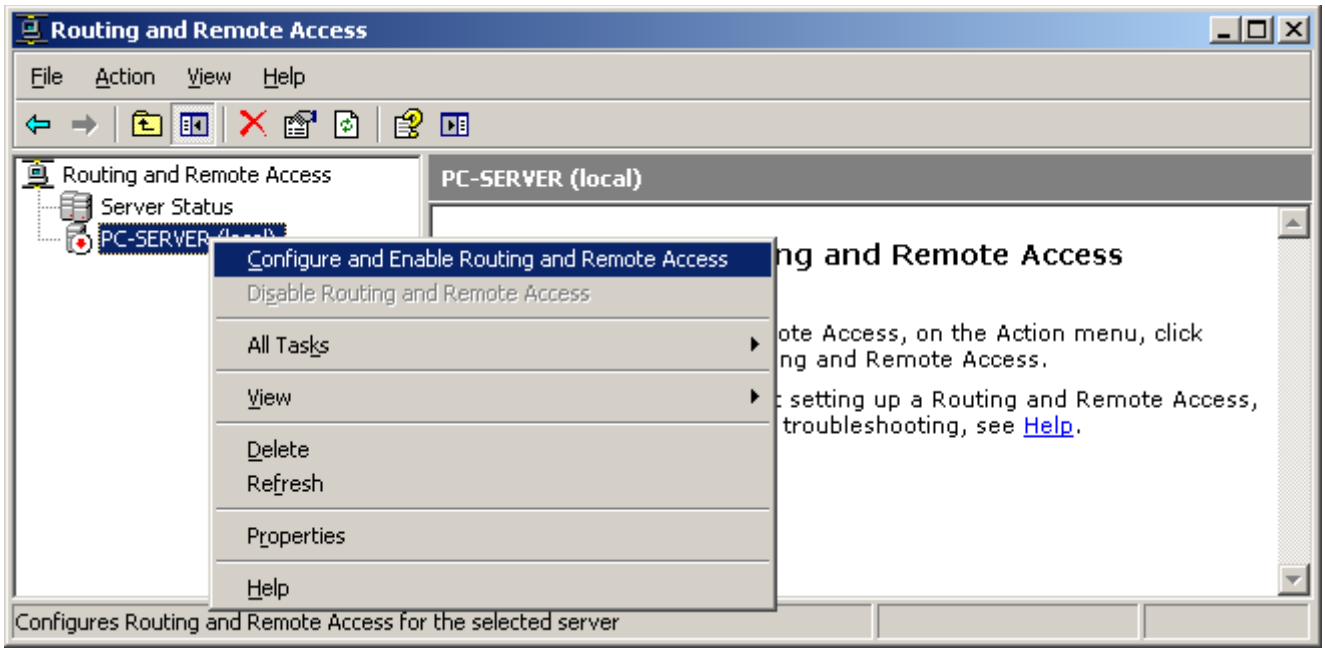
۲. از Windows Server 2003 به عنوان روتر نرم‌افزاری استفاده می‌نماییم.

ما در اینجا گزینه دوم را انتخاب خواهیم کرد. بدین منظور در ویندوز سرور برنامه Routing and Remote Access را از مسیر زیر باز کنید.

Start ➔ Administrative Tools ➔ Routing and Remote Access

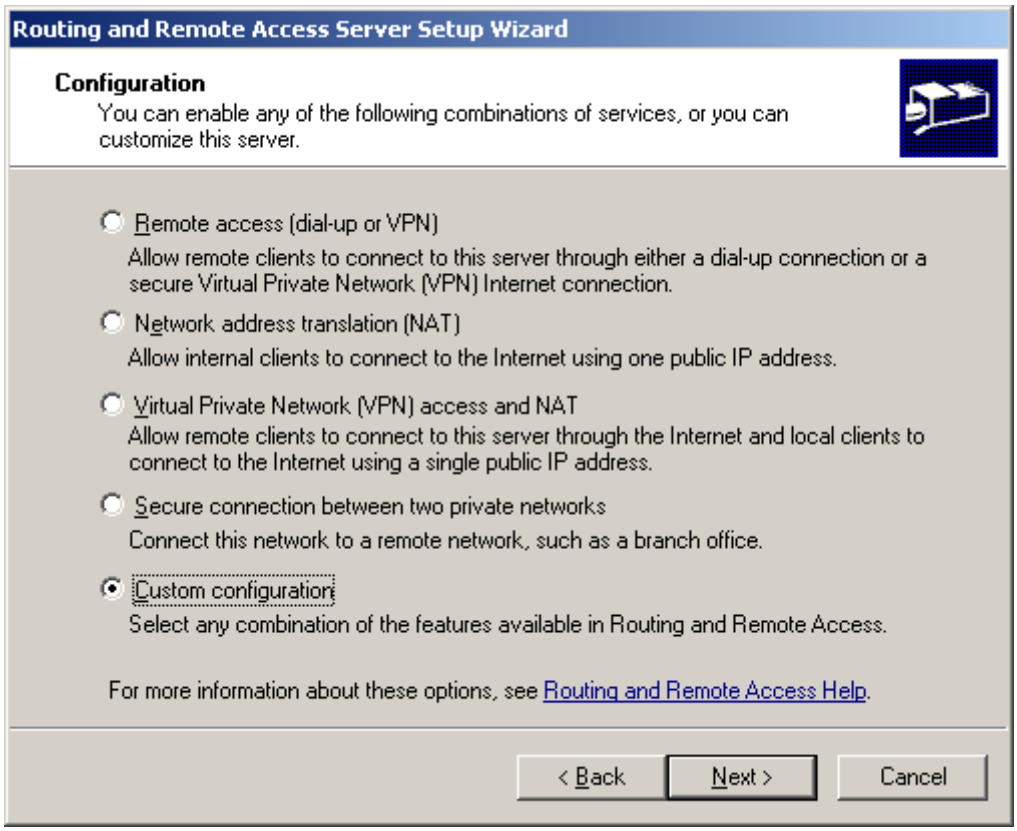


در صفحه باز شده، بر روی سرور، راست کلیک نموده و گزینه Configure and Enable Routing & Remote Access را انتخاب نمایید. توجه نمایید که سرور بایستی غیر فعال باشد. اگر سرور فعال بود، در منوی باز شده، گزینه Disable Routing and Remote Access را انتخاب نمایید.

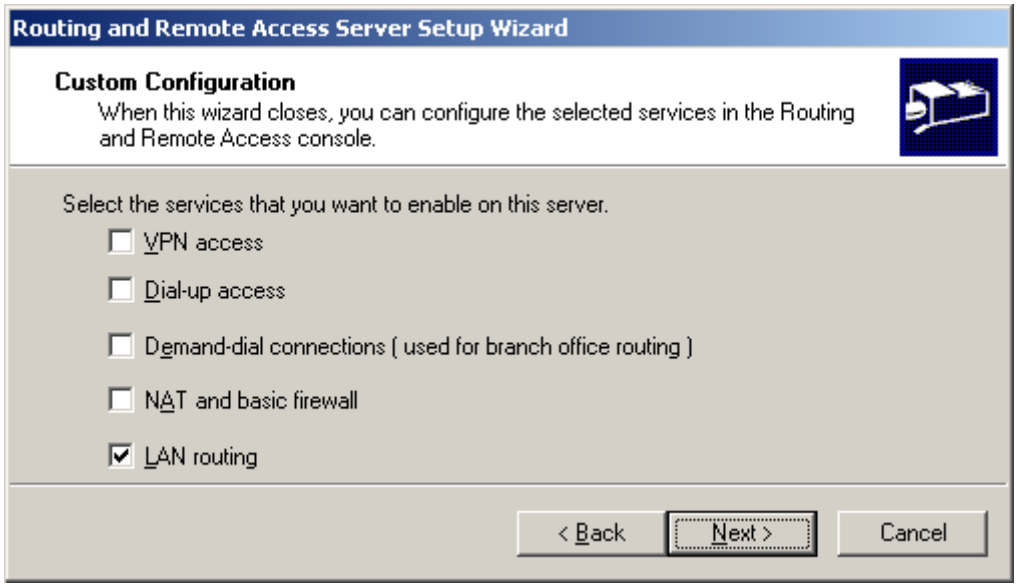


صفحه باز شده، به غیر از راهی برای پیاده سازی DHCP Relay Agent، شامل راه هایی برای تبدیل کامپیوتر به یک RAS Server (که می‌تواند VPN و یا Dial-Up Based باشد) و غیره (مثل پیاده سازی NAT) هم می‌باشد که فعلا مربوط به بحث ما نمی‌شود.

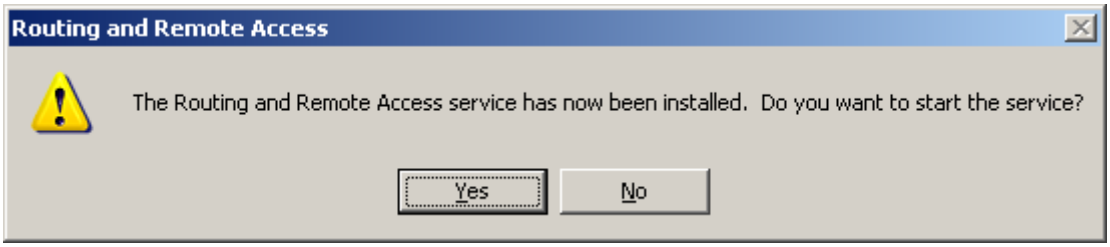
در صفحه باز شده، گزینه Custom Configuration را انتخاب نموده و روی Next کلیک کنید:



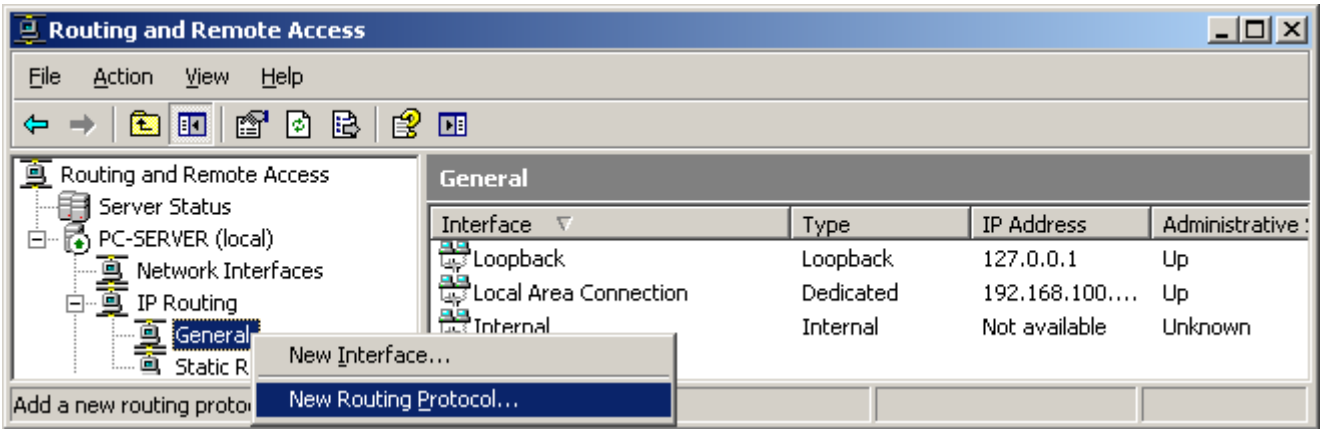
حالا ما می‌توانیم این کامپیوتر را به صورت دستی تبدیل به روتر کنیم. در اینجا ما می‌خواهیم که این کامپیوتر فقط بتواند بسته‌های Subnetهای مختلف رو به مقصدشان هدایت کند و به همین دلیل گزینه‌ی LAN Routing رو انتخاب کرده و روی Next کلیک نمایید.



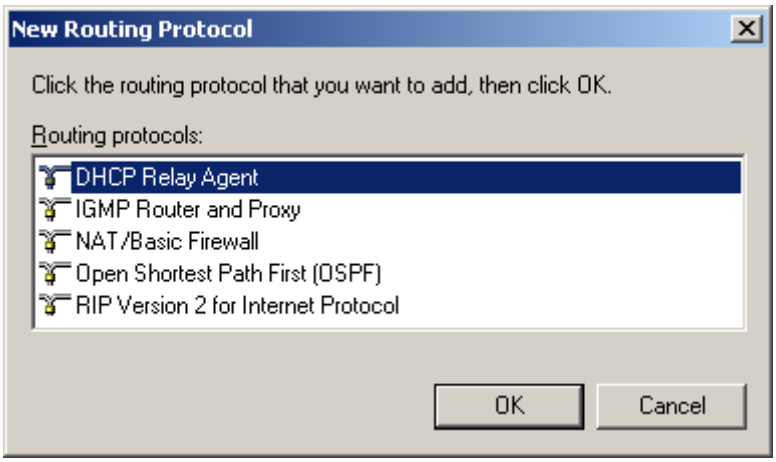
تا اینجا کار نصب تمام می‌شود. سیستم از شما سوال می‌پرسد که آیا سرویس Routing and Remote Access فعال شود یا خیر؟ گزینه Yes را انتخاب نمایید.



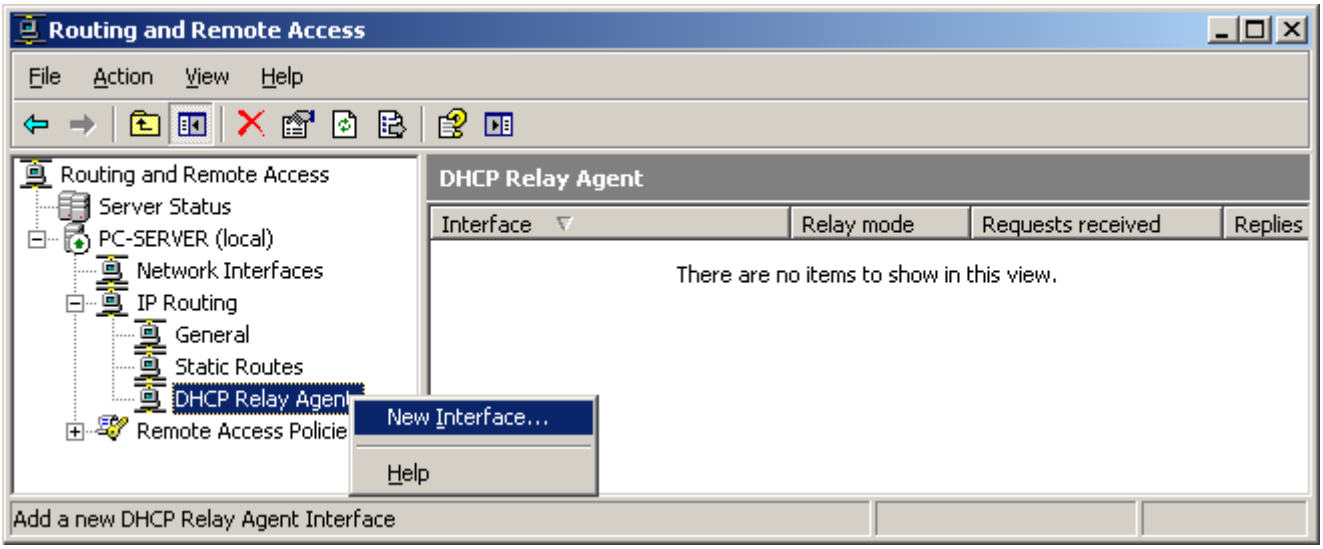
مجددا به صفحه اصلی باز می‌گردیم. در اینجا ما می‌خواهیم که یک پروتکل مسیر یابی جدید به پروتکلهای فعلی سیستم اضافه کنیم تا بتواند بسته‌های درخواست DHCP رو هدایت کند. لذا از قسمت IP Routing، روی گزینه General راست کلیک نموده و گزینه New Routing Protocol را انتخاب نمایید.



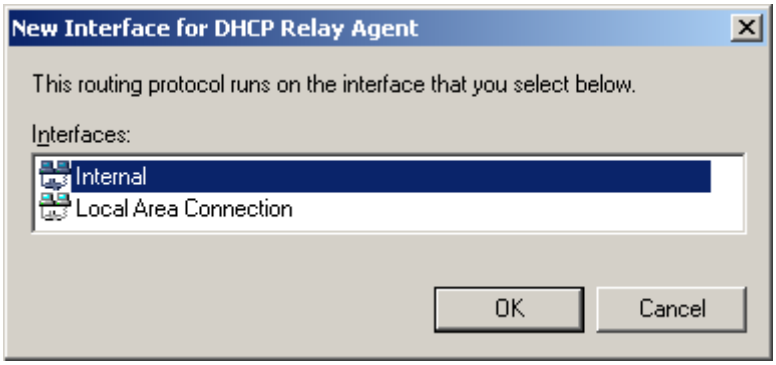
در صفحه باز شده، گزینه DHCP Relay Agent را انتخاب نمایید تا این سرویس روی سیستم شما نصب شود. سپس روی OK کلیک کنید.



وقتی که به صفحه اصلی برگردید، متوجه می‌شوید که در زیر مجموعه‌های IP Routing، یک قسمت جدید به نام DHCP Relay Agent اضافه شده است. حالا روی آن راست کلیک کرده و گزینه‌ی New Interface رو انتخاب نمایید. در اینجا می‌خواهیم به این سیستم بگوییم که پاکت‌های اطلاعاتی که از کدام کارت شبکه دریافت می‌کند را Relay کند.

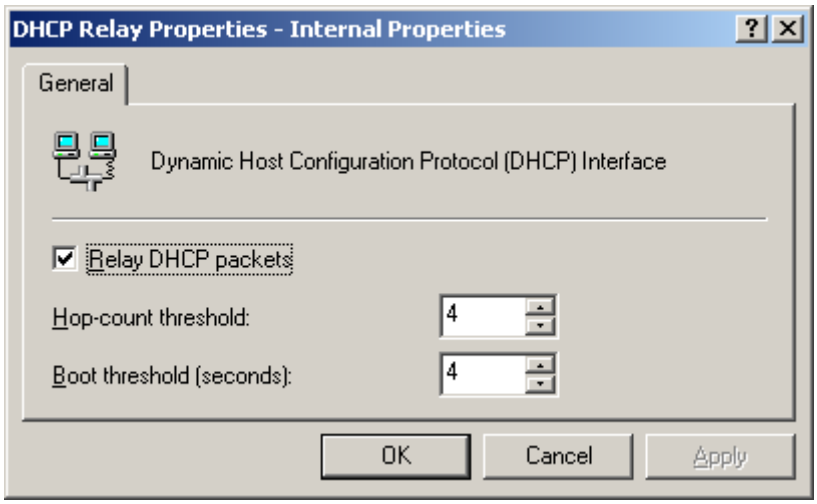


حالا باید کارت شبکه‌ای که Subnetهای مختلف به آن وصل می‌شوند را انتخاب کنید. این کارت شبکه، همان کارت شبکه‌ای است که کامپیوتر دروازه (Gateway) Subnetها چه با Switch و چه با Hub به آن وصل می‌شوند. پس یک دفعه یک کارت شبکه‌ای که اصلا به جایی وصل نیست را انتخاب نکنید! مثلاً در این تصویر من دو تا کارت شبکه دارم که کارت شبکه با نام Internal را انتخاب کرده ام.

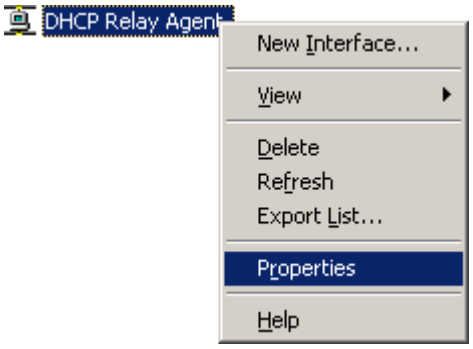


سپس صفحه زیر باز می‌شود. در این صفحه، سه گزینه می‌بینید. گزینه Relay DHCP Packet به معنای فعال بودن سرویس Relay است. آن را انتخاب نمایید.

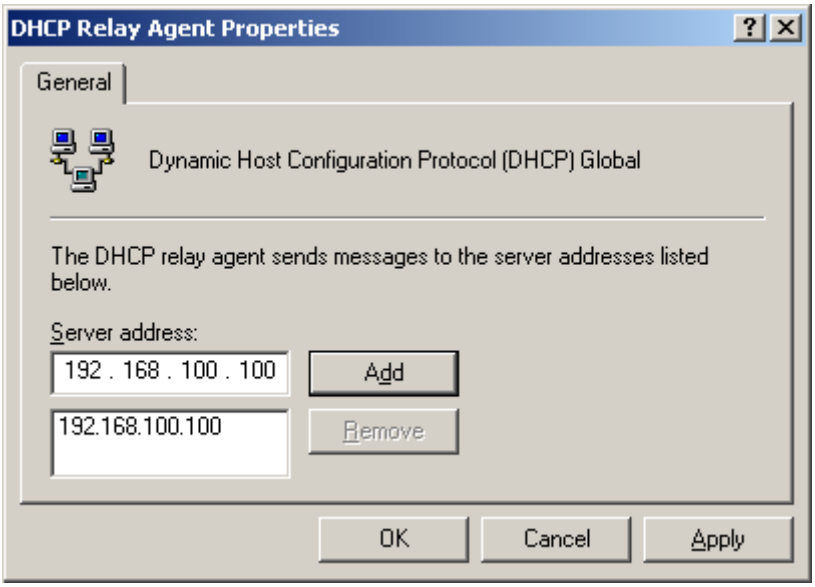
گزینه Hop-Count Threshold، معین می‌کند که Relay Agent باید بسته‌ها را تا چند تا روتر مسیر دهی کند و اگر مثلاً از ۴ تا بیشتر بشود، مسیر دهی و ارسال درخواست آدرس IP را دیگر ادامه نمی‌دهد. گزینه بعدی هم Boot Threshold نام دارد که تعداد ثانیه هایی است که Relay Agent، با در نظر گرفتن احتمال اینکه ممکن است یک DHCP Server درون زیر شبکه بوده باشد، صبر کرده و پیام درخواست IP را نمی‌فرستد. اگر این ثانیه‌ها تمام شود، Relay Agent، اقدام به فرستادن پیام می‌کند.



تا اینجا کار تنظیمات ما انجام شد. تنها کاری که باقی می‌ماند، این است که به DHCP Relay Agent بگوییم که DHCP Server در کدام زیر شبکه (Subnet) قرار دارد. لذا روی گزینه DHCP Relay Agent راست کلیک نموده و گزینه Properties را انتخاب نمایید.



در صفحه باز شده، آدرس سروری که سرویس DHCP روی آن نصب است را اضافه نمایید.



توجه: ممکن است تا اینجا سر در گم شده باشید که چرا این تنظیمات را روی سرور انجام دادیم؟ جواب این است که ما این کارها را روی سرور اصلی انجام ندادیم، بلکه این تنظیمات را روی کامپیوتری انجام دادیم که نقش DHCP Relay Agent را بازی می‌کند و این نقش فقط در ویندوز سرور وجود دارد. کامپیوتری که نقش DHCP Relay Agent را بازی می‌کند، متفاوت از سرور اصلی و DHCP Server می‌باشد. یعنی بایستی در یک زیر شبکه که DHCP Server ندارد، یک کامپیوتر مجزا که روی آن ویندوز سرور نصب است را قرار داده و نقش DHCP Relay Agent را به آن بدهیم.

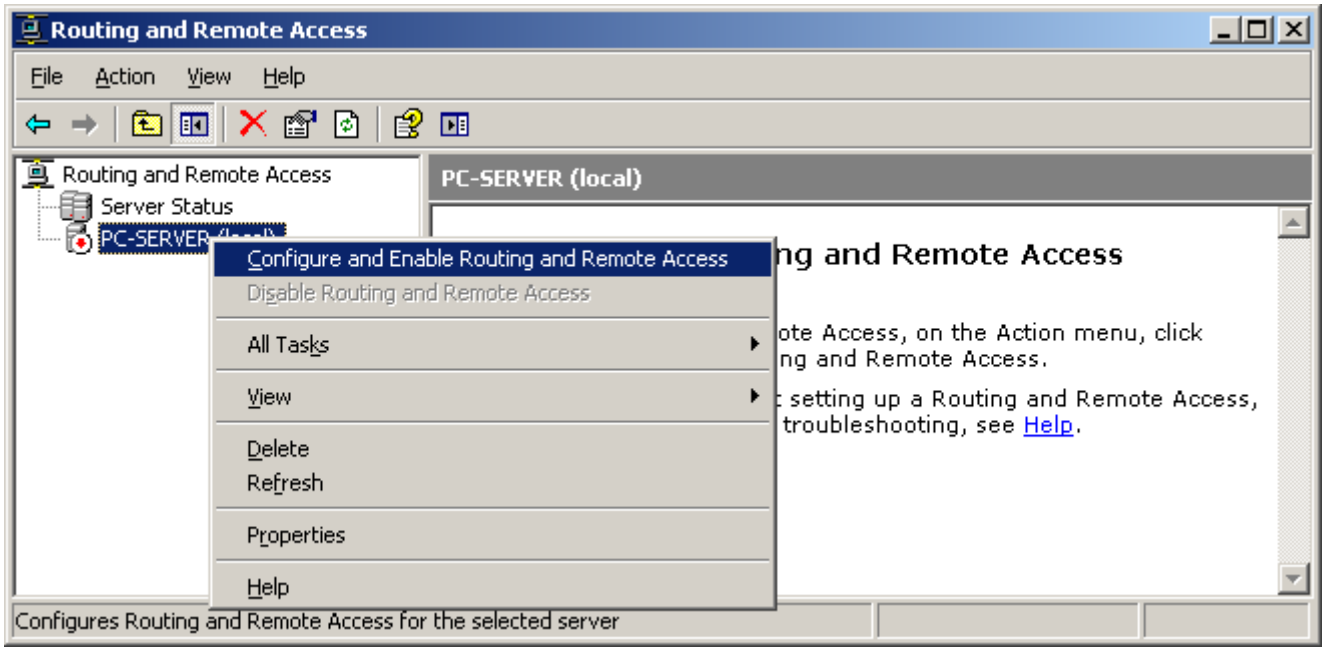
۳۲-۱۱- نصب VPN Server با داشتن یک کارت شبکه

در قسمت قبلی، نحوه نصب VPN Server روی ویندوز سرور ۲۰۰۳ را آموزش دادیم. در ابتدای بحث گفتیم که برای نصب VPN Server، بایستی حداقل دو کارت شبکه داشته باشیم؛ یکی برای اتصال به اینترنت و دیگری برای سرویس دهی به کاربران راه دور. اما اگر یک کارت شبکه بیشتر نداشتیم و بخواهیم از همین تک کارت شبکه، هم برای اتصال به اینترنت و هم برای سرویس دهی به کاربران استفاده کنیم چطور؟ آیا راه حلی وجود دارد؟ جواب مثبت است. بدین منظور، بایستی سرور را دستی پیکربندی نماییم. برای این کار، ابتدا سرویس Windows Firewall/Internet Connection Sharing (ICS) را غیر فعال نمایید که آن را در بخش قبل توضیح دادیم. سپس پنجره Routing and Remote Access را از مسیر زیر باز کنید.

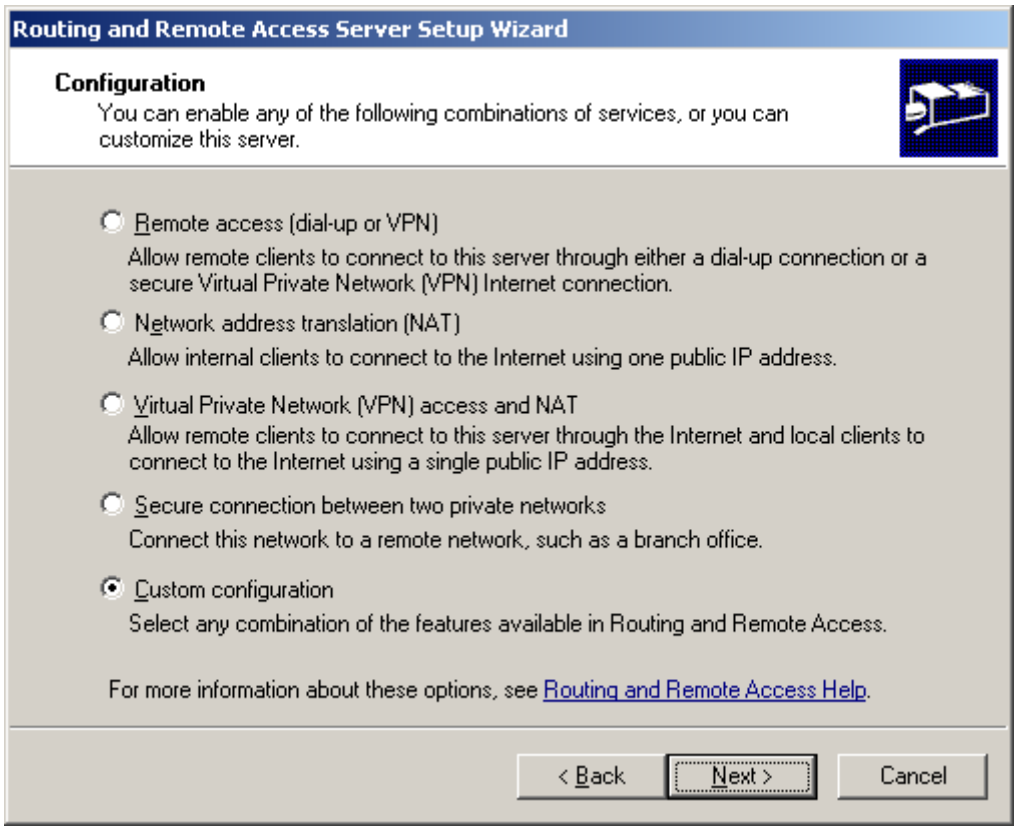
Start ➔ Administrative Tools ➔ Routing and Remote Access



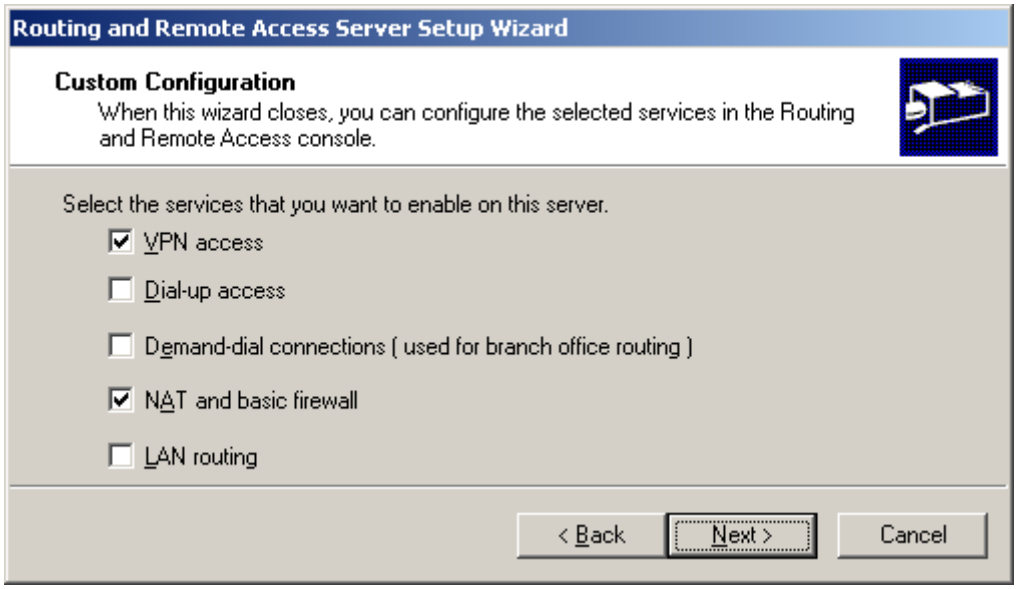
با این کار، صفحه تنظیمات Routing and Remote Access نمایان می‌شود. برای شروع کار و نصب VPN Server روی ویندوز سرور با یک کارت شبکه، روی نام سرور راست کلیک نموده و گزینه Configure and Enable Routing and Remote Access را انتخاب نمایید.



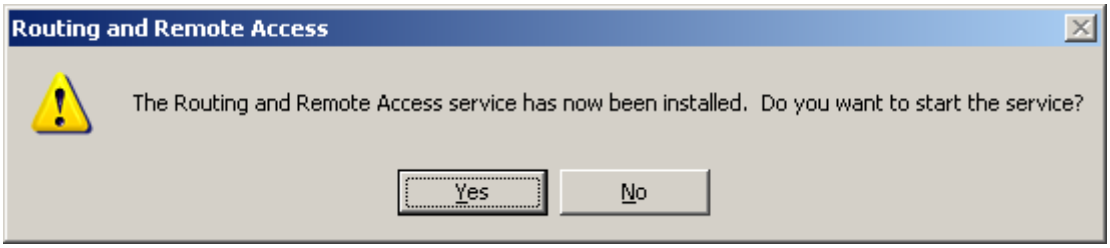
در صفحه باز شده، گزینه Custom Configuration را انتخاب نموده و روی Next کلیک کنید.



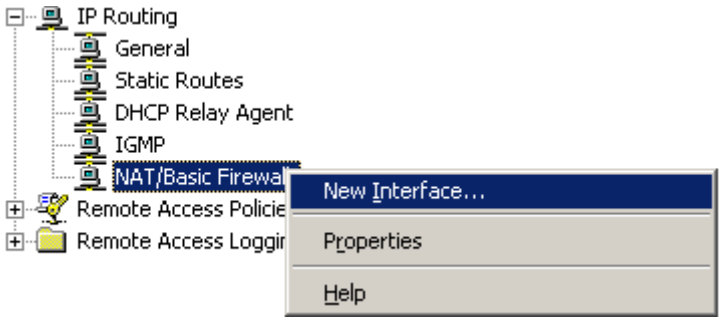
در صفحه بعدی، دو گزینه VPN Access و NAT and Basic Firewall را انتخاب نمایید تا هر دو سرویس روی سیستم شما نصب شود. سپس Next را بزنید. در نهایت نیز روی Finish کلیک کنید تا عملیات نصب به پایان برسد.



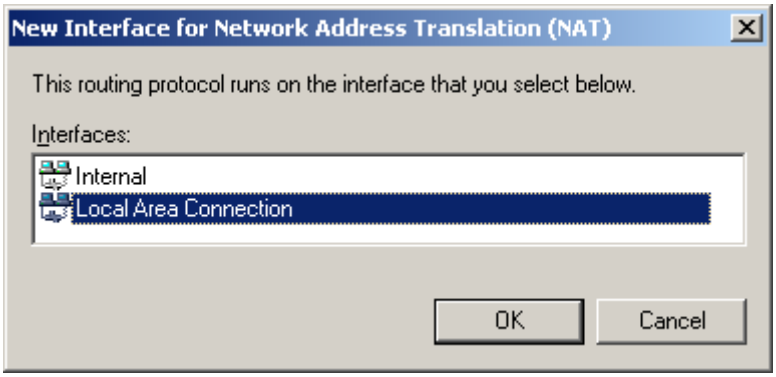
تا اینجا کار نصب تمام می‌شود. سیستم از شما سوال می‌پرسد که آیا سرویس Routing and Remote Access فعال شود یا خیر؟ گزینه Yes را انتخاب نمایید.



مجددا به صفحه اصلی باز می‌گردیم. پس از راه اندازی سرویس، از قسمت IP Routing، روی گزینه NAT/Basic Firewall راست کلیک نموده و گزینه New Interface را انتخاب کنید تا یک کارت شبکه را برای سرویس دهی انتخاب نمایید.



در صفحه باز شده، کارت شبکه‌ای که قرار است VPN روی آن اعمال شود را انتخاب نمایید. می‌خواهیم تنظیمات Firewall این کارت شبکه را تغییر دهیم.

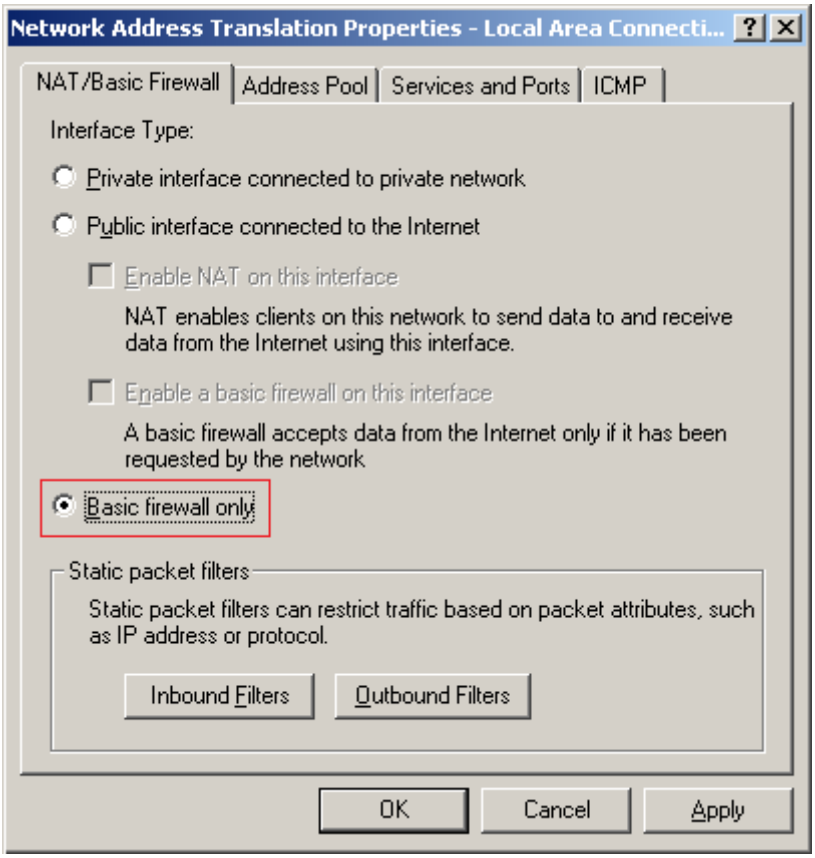


با کلیک روی دکمه OK، صفحه تنظیمات زیر باز می‌شود. در سربرگ NAT/Basic Firewall، گزینه Basic firewall only را انتخاب نمایید تا سرور به عنوان یک Firewall ساده عمل کند.

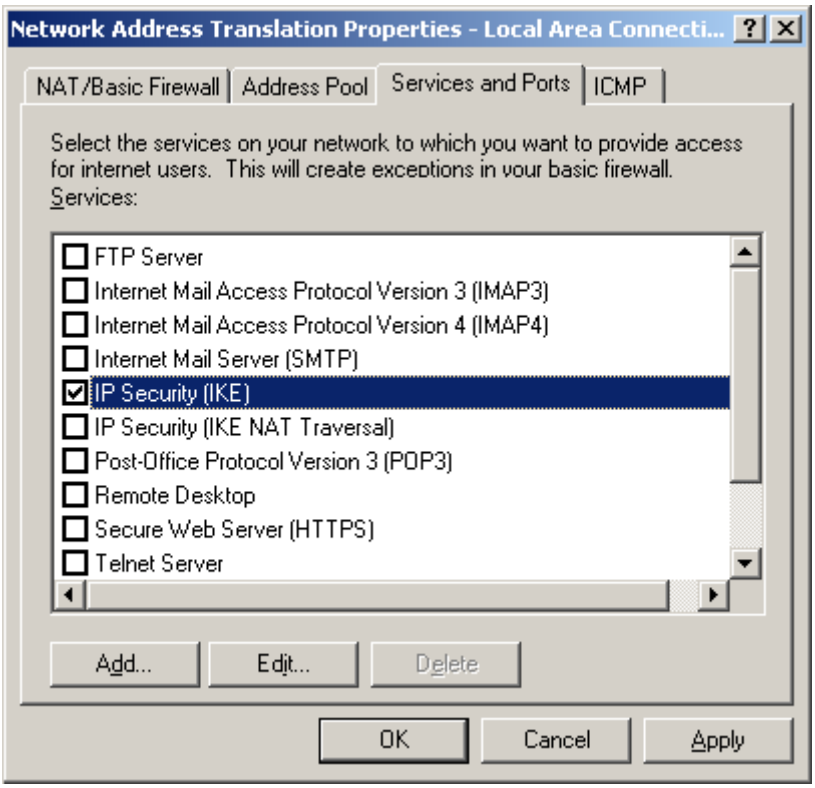
در شکل زیر، گزینه Private interface connected to private network، می‌گوید که این کارت شبکه، یک کابل شبکه می‌باشد که برای اتصال به شبکه خصوصی از آن استفاده می‌شود.

گزینه Public interface connected to the internet، بیان می‌کند که از این کارت شبکه برای اتصال به اینترنت استفاده می‌شود. اگر این گزینه را انتخاب نموده و سپس گزینه Enable NAT on this interface را انتخاب نمایید، کاربرانی که با VPN، به این سرور متصل می‌شوند، قابلیت دسترسی به اینترنت را نیز خواهند داشت. گزینه Enable a basic firewall on this interface نیز باعث می‌شود که این کارت شبکه، علاوه بر اتصال به اینترنت، نقش دیوار آتشین را نیز داشته باشد.

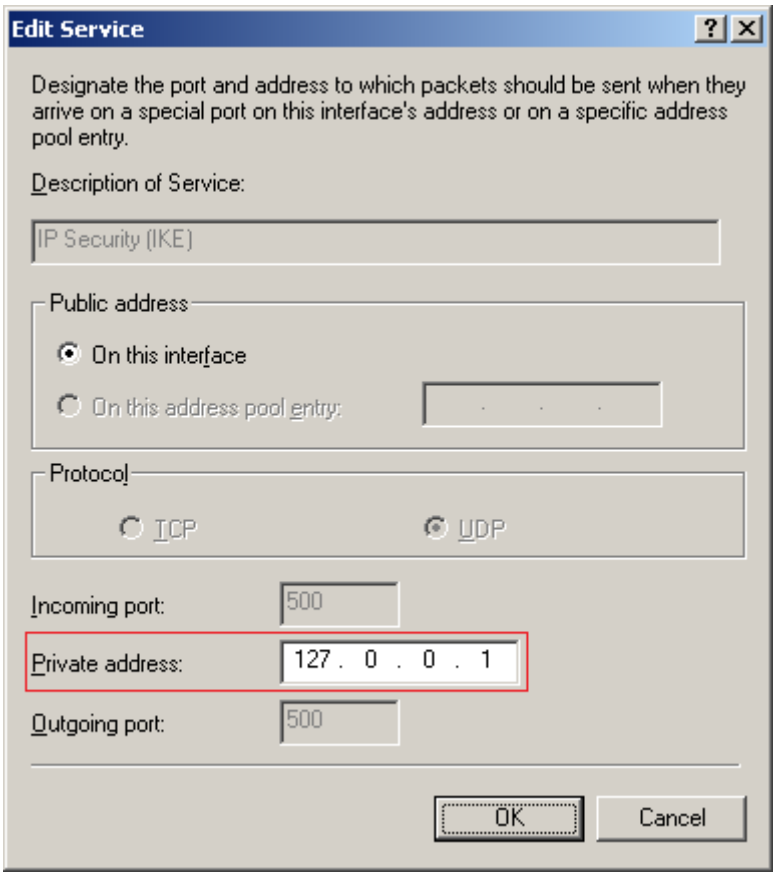
گزینه Basic firewall only نیز، تنها نقش یک دیوار آتشین را به این کارت شبکه می‌دهد.



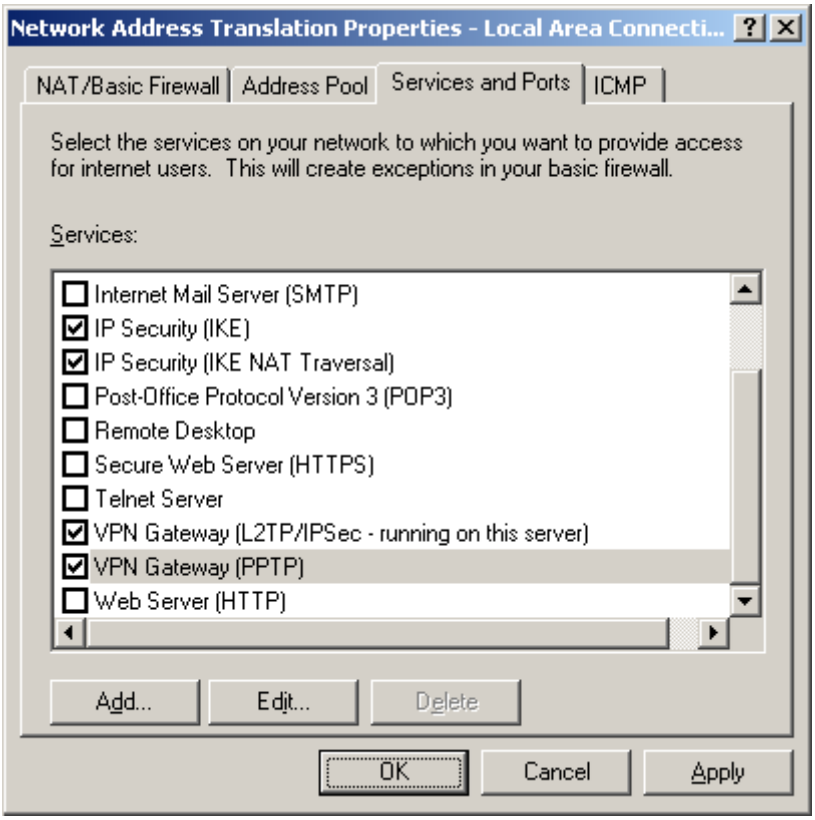
سپس وارد سربرگ Services and Ports شوید. ابتدا گزینه IP Security (IKE) را انتخاب نمایید.



به محض انتخاب این گزینه، صفحه زیر باز می‌شود. در این صفحه بایستی تنظیم نمایید که NAT پس از دریافت ترافیک (اطلاعات) از Firewall، آن‌ها را بایستی به کجا مسیر دهی کند؟ شما تنظیم نمایید که این ترافیک‌ها را به سرور محلی مسیر دهی کند. لذا در قسمت آدرس IP، آدرس محل خود، یعنی 127.0.0.1 را وارد نمایید. صفحه زیر، به ازاء انتخاب گزینه‌های دیگر نیز باز می‌شود. برای آن‌ها نیز همین آدرس IP را وارد نمایید.

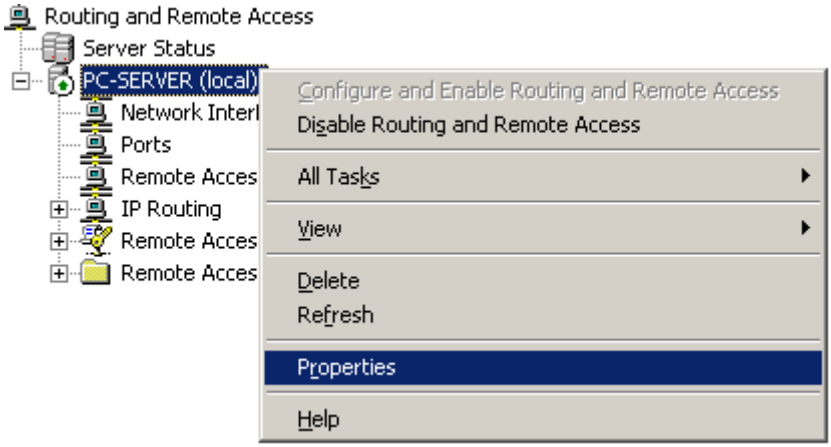


پس از تایید، گزینه‌های IP Security (IKE NAT Traversal)، VPN Gateway (L2TP/IPSec) و VPN Gateway (PPTP)را انتخاب نمایید. آدرس 127.0.0.1 را نیز برای آن‌ها ثبت نمایید.

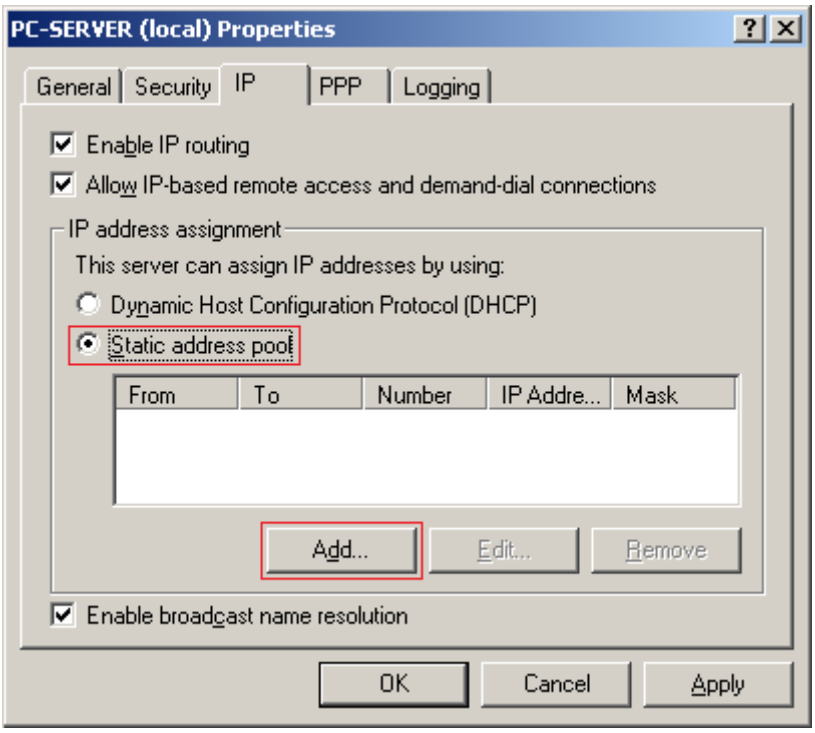


حال نوبت به تنظیم محدوده آدرس IP می‌شود.

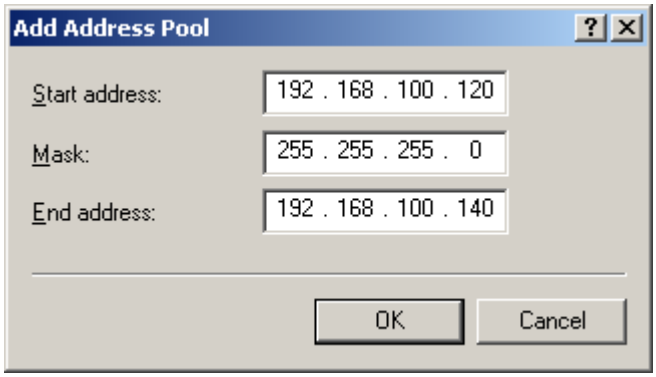
روی نام سرور راست کلیک نموده و Properties را انتخاب نمایید.



سپس وارد سربرگ IP شوید. در اینجا می‌خواهیم محدوده آدرس قابل تخصیص به Clientها را تعیین نماییم. لذا ابتدا گزینه Static address pool را انتخاب نمایید. سپس برای افزودن محدوده جدید، روی Add کلیک نمایید.

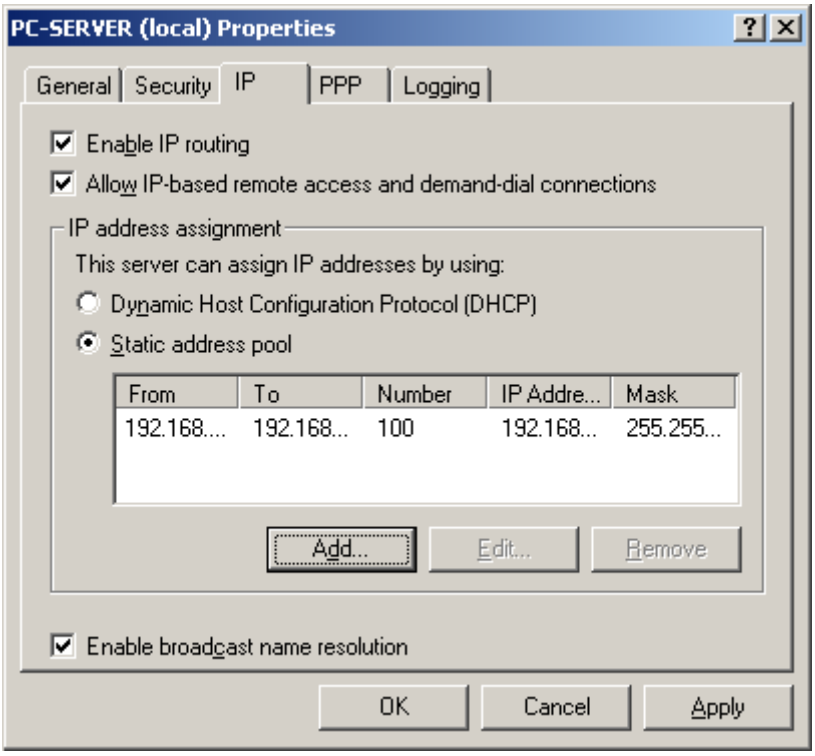


در صفحه باز شده، محدوده جدید را وارد نمایید. در این شکل ابتدا آدرس شروع، سپس Subnet Mask شبکه و سپس آدرس پایان را وارد نمایید. این تصویر با تصویری که قبلاً در مورد محدوده آدرس IP مشاهده نمودید، اندکی متفاوت است.



نکته مهم: دقت فرمایید که محدوده آدرس وارد شده، تداخلی با آدرس کامپیوتر هایی که اکنون به صورت محلی با کامپیوتر سرور شبکه هستند، نداشته باشد.

با این کار، محدوده آدرس وارد شده، به محدوده آدرس‌های موجود اضافه می‌شود. در نهایت روی دکمه OK کلیک نمایید.



تا اینجا، VPN Server ما، به درستی نصب شده است. فقط تنظیمات کاربران می‌ماند که مشخص نماییم که کدام کاربر، حق دسترسی به شبکه VPN را از راه دور دارد؟ که بایستی وارد قسمت Active Directory Users & Groups شویم.

نحوه تنظیمات کاربران برای اتصال به VPN را در همین فصل توضیح داده‌ایم.

۳۲-۱۲- ده نکته درباره رفع ایرادهای اتصالات VPN

منبع: http://www.freedanload.com/10-tips-VPN

۱- دسترسی کاربران به فایل سرورها امکان‌پذیر نیست.

اگر کاربران از طریق آدرس IP امکان دسترسی به فایل سرور را داشته باشند، اما با استفاده از نام سرور نتوانند با سرور ارتباط برقرار کنند، محتمل‌ترین دلیل، وجود ایراد در Name Resolution یا تشخیص نام است. تشخیص نام می‌تواند در نام هاست NetBIOS یا DNS مشکل ایجاد کند.

اگر سیستم‌عامل کلاینت به NetBIOS وابسته باشد، کلاینت‌های VPN می‌توانند از طریق سرور VPN آدرس سرور WINS را تعیین کنند، اما اگر سیستم‌عامل کلاینت ترجیحاً از DNS استفاده می‌کند، کلاینت‌های VPN از طریق یک سرور DNS داخلی به نام سرور شبکه داخلی دسترسی پیدا می‌کنند.

هنگام استفاده از DNS برای تخصیص نام‌های شبکه داخلی از توانایی کلاینت‌ها برای تعیین صحیح نام دامین‌های دارای مجوز شبکه سازمانی اطمینان حاصل کنید. این مشکل اغلب زمانی به‌وجود می‌آید که کامپیوترهای خارج از دامین برای دسترسی و استفاده از نام سرورهای موجود در شبکه داخلی، که پشت VPN قرار دارند، به استفاده از DNS اقدام می‌کنند.

۲ - کاربران نمی‌توانند به هیچ منبعی روی شبکه سازمانی دسترسی پیدا کنند.

در بعضی مواقع کاربران می‌توانند به سرور VPN راه دور متصل شوند، اما نمی‌توانند به هیچ‌کدام از منابع موجود روی شبکه سازمانی دسترسی پیدا کنند. در چنین مواردی کاربران نمی‌توانند نام هاست را شناسایی کرده و حتی قادر نیستند به منابع موجود در شبکه سازمانی Ping کنند.

رایج‌ترین دلیل وقوع این مشکل این است که کاربران به شبکه‌ای متصل هستند که ID شبکه آن با شبکه سازمانی مستقر در پشت سرور VPN یکسان است. به‌عنوان مثال، کاربر به شبکه پرسرعت یک هتل متصل شده و به این ترتیب ID شبکه پس از تخصیص آدرس IP اختصاصی به‌صورت ۱۰.۰.۰.۰/۲۴ اختصاص یافته است.

حال چنان‌چه شبکه سازمانی نیز روی همین ID شبکه ۱۰.۰.۰.۰/۲۴تعریف شده باشد، آن‌گاه کاربر قادر به اتصال به شبکه سازمانی خود نخواهد بود، زیرا ماشین کلاینت VPN آدرس مقصد را به‌صورت شبکه‌ای محلی می‌بیند و اتصال شبکه راه دور را از طریق رابط VPN ارسال نمی‌کند.

دلیل عمده دیگر برای عدم موفقیت در اتصال این است که کلاینت‌های VPN اجازه دسترسی به منابع موجود روی شبکه سازمانی را به‌دلیل قوانین تعیین شده از جانب فایروال نمی‌یابند. راه‌حل این مشکل پیکربندی فایروال به‌گونه‌ای است که اجازه دسترسی به منابع شبکه‌ای را به کلاینت‌های VPN بدهد.

۳ – کاربران نمی‌توانند از پشت ابزارهای NAT به سرور VPN متصل شوند.

اغلب روترهای NAT و فایروال‌ها به اصطلاح از پشت ابزارهای NAT از پروتکل PPTP VPN پشتیبانی می‌کنند. هرچند برخی از فروشندگان طراز اول تجهیزات شبکه‌ای، ویرایشگر NAT را در پروتکل PPTP VPN خود تعبیه نمی‌کنند. اگر کاربری در پشت چنین ابزاری واقع شده باشد، ارتباط VPN برای اتصال از طریق PPTP با شکست مواجه خواهد شد. البته، ممکن است با دیگر پروتکل‌های VPN کار کند.

همه ابزارهای NAT و فایروال‌ها در کار با پروتکل‌های VPN مبنی بر IPSec از IPSec پشتیبانی می‌کنند. این پروتکل‌های VPN شامل پیاده‌سازی‌های اختصاصی مد تونل IPSec و L2TP/IPSec سازگار با RFC خواهند بود. همچنین این دسته از پروتکل‌های VPN می‌توانند با استفاده از (Encapsulating) ارتباطات IPSec و در هدر UDP از پیمایش NAT یا (NAT Traversa) پشتیبانی کنند.

چنان‌چه سرور و کلاینت VPN شما از پیمایش NAT پشتیبانی کرده و کلاینت تمایل دارد از L2TP/IPSec برای اتصال به سرور سازگار با NAT استفاده کند، رایج‌ترین دلیل برای این مشکل این است که کلاینت از سیستم‌عامل Windows XP SP2 استفاده می‌کند.

سرویس پک ۲ پیمایش NAT Traversal را روی کلاینت‌های L2TP/IPSec به‌اصطلاح می‌شکند. شما می‌توانید این مشکل را از طریق ویرایش رجیستری روی کلاینت VPN آن‌گونه که در آدرس زیر توضیح داده شده حل کنید.

http://support.microsoft.com/default.aspx?scid=kb;en-us;885407

۴ – کاربران از سرعت پایین شکایت دارند.

سرعت کم یکی از مشکلاتی است که برطرف کردن آن بسیار دشوار است. دلایل زیادی برای کاهش کارایی ارتباط VPN وجود دارد و نکته مهم آن هم این است که کاربران بتوانند توضیح دهند دقیقاً در زمان انجام چه کاری با افت کارایی و کاهش در سرعت روبه‌رو می‌شوند.

یکی از عمده‌ترین موارد هنگام کاهش کارایی ارتباط VPN زمانی است که کلاینت در پشت شبکه DSL قرار گرفته و از پروتکل PPPoE استفاده می‌کند. چنین ارتباطات شبکه‌ای معمولاً موجب بروز مشکلات مرتبط با MTU شده که می‌توانند بر هر دو عامل اتصال و کارایی تأثیرگذار باشند. برای اطلاعات بیشتر درخصوص موارد مرتبط با MTU در کلاینت‌های ویندوزی به آدرس زیر مراجعه کنید.

http://support.microsoft.com/default.aspx?scid=kb;en-us;283165

۵ – کاربران از طریق PPTP متصل می‌شوند، اما امکان اتصال از طریق L2TP/IPSec وجود ندارد.

PPTP پروتکل ساده‌ای برای پیکربندی و تنظیم روی سرور و کلاینت VPN است. فقط کافی است که کاربر از نرم‌افزار کلاینت توکار VPN که به‌همراه تمام نسخه‌های سیستم‌عامل ویندوز ارائه می‌شود استفاده کرده و نام کاربری و کلمه عبور معتبر اکانتی را که مجوز دسترسی از راه دور را دارد، در اختیار داشته باشد.

اگر کامپوننت سرور VPN براساس مسیریابی ویندوز و Remote Access Service باشد، به‌سادگی تنظیم شده و پس از اجرای یک راهنمای پیکربندی کوتاه به‌طور خودکار اجرا خواهد شد. L2TP/IPSec قدری پیچیده‌تر است. اعتبار کاربر و ماشین وی باید توسط سرور VPN تأیید شوند.

تأیید اعتبار ماشین می‌تواند از طریق یک کلید مشترک (Pre-shared Key) یا ماشین ثبت‌شده صورت گیرد. اگر از کلید مشترک استفاده می‌کنید (که معمولاً به دلایل امنیتی توصیه نمی‌شود)، بررسی کنید که آیا کلاینت VPN برای استفاده از همان کلید مشترک پیکربندی شده یا خیر؟ اگر از روش ثبت ماشین استفاده می‌کنید نیز مطمئن شوید که کلاینت VPN مجوز مربوطه را دارد یا خیر؟

۶ – اتصال VPN سایت‌به‌سایت برقرار می‌شود، اما هیچ ترافیکی بین گیت‌وی‌های VPN جابه‌جا نمی‌شود.

هنگامی که یک ارتباط VPN سایت‌به‌سایت بین سرورهای RRAS ویندوزی ایجاد می‌کنید، این امکان وجود دارد که اتصال VPN درظاهر برقرار نشان داده شود، اما ترافیکی میان شبکه‌های متصل‌شده رد و بدل نشود. اشکال در شناسایی نام سرورها ایجاد شده وهاست‌ها حتی قادر به پینگ کردن به شبکه راه دور نیز نیستند.

عمده‌ترین دلیل برای بروز این مشکل این است که هر دو طرف اتصال سایت به سایت روی یک ID شبکه یکسان هستند. راه‌حل آن نیز تغییر الگوی آدرس‌دهی IP روی یک یا هر دو شبکه بوده تا به‌این ترتیب، تمام شبکه‌های متصل‌شده به‌صورت سایت به سایت روی IDهای شبکه متفاوتی قرار داشته باشند.

۷ – کاربران نمی‌توانند از پشت فایروال به ارتباط در مُد تونل IPSec اقدام کنند.

به‌طور معمول سرور VPN و کلاینت‌ها به‌طور صحیح پیکربندی می‌شوند تا بتوانند از مُد تونل IPSec یا ارتباط L2tp/IP Sec NAT-T برای ارتباط با یک سرور VPN استفاده کنند و در نتیجه ارتباط با شکست مواجه می‌شود. در برخی مواقع این اتفاق را بعد از برقراری اتصال موفق اولین کلاینت مشاهده می‌کنید، اما کلاینت‌های بعدی که در پشت همان ابزار NAT قرار دارند، با شکست در ارتباط روبه‌رو می‌شوند.

دلیل بروز این مشکل این است که تمام سرورهای IPSec NAT-T VPN با RFC سازگار نیستند. سازگاری با RFC نیازمند این است که سرور مقصد NAT-T VPN از تماس‌های IKE روی پورت منبع UDP 500 پشتیبانی کرده تا آن‌هابتوانند ارتباطات چندگانه را از چندین کلاینت در پشت یک گیت‌وی VPN واحد مالتی‌پلکس کنند.

حل این مشکل از طریق تماس با فروشنده سرور VPN و حصول اطمینان از این‌که پیاده‌سازی IPSec NAT-T VPN با RFC سازگاری دارد یا خیر، امکان‌پذیر خواهد بود. اگر این‌گونه نبود، از فروشنده درباره وجود Firmware برای به‌روز رسانی سؤال کنید.

۸ – کاربران نمی‌توانند به برخی از IDهای شبکه سازمانی دسترسی پیدا کنند.

برخی از اوقات کاربران مواردی را گزارش می‌کنند که در آن ذکر شده، می‌توانند بعد از برقراری ارتباط VPN به برخی از سرورها دسترسی پیدا کنند، اما بقیه سرورها قابل دسترسی نیستند. آنان وقتی ارتباط خود را آزمایش می‌کنند، مشاهده می‌کنند که نمی‌توانند با استفاده از نام یا آدرس IP به سرور مورد نظر خود پینگ کنند.

دلیل عمده برای این مشکل این است که سرور VPN ورودی‌های جدول روزمره را برای تمام IDهای شبکه‌هایی که کاربر نمی‌تواند به آنان متصل شود، در اختیار ندارد. کاربران فقط قادر به اتصال به سرورهایی هستند که روی زیرشبکه سرور VPN باشند، اما از طریق سرور VPN قادر به ارتباط با IDهای شبکه راه‌دور نیستند.

راه‌حل این مشکل پرکردن جدول مسیریابی روی سرورVPN به‌گونه‌ای است که آدرس گیت‌وی تمام IDهای شبکه‌هایی را که VPN باید به آنان متصل شود، در آن وجود داشته باشد.

۹ – کاربران هنگام اتصال به سرور VPN قادر به اتصال به اینترنت نیستند.

در برخی مواقع کاربران نمی‌توانند پس از این‌که اتصال VPN برقرار شد، به اینترنت متصل شوند. در این‌حالت همزمان با قطع ارتباط VPN کاربران در اتصال به اینترنت مشکلی نخواهند داشت. این مشکل زمانی مشاهده می‌شود که نرم‌افزار کلاینت VPN برای استفاده از سرور VPN به عنوان گیت‌وی پیش‌فرض خود پیکربندی شده‌باشد. این تنظیم، تنظیم پیش‌فرض نرم‌افزار کلاینت VPN مایکروسافت است.

از آنجا که همه هاست‌ها دور از محل کلاینت VPN مستقر هستند، ارتباطات اینترنت به‌سمت سرور VPN مسیردهی خواهند شد. اگر سرور VPN به‌گونه‌ای پیکربندی نشده باشد که ارتباط با اینترنت را از طریق کلاینت‌های VPN میسر سازد، هرگونه تلاشی برای اتصال به اینترنت با شکست روبه‌رو خواهد شد.

راه‌حل این مشکل پیکربندی سرور VPN به‌گونه‌ای است تا به کلاینت‌ها اجازه دسترسی به اینترنت را بدهد. سرور RRAS ویندوز و بسیاری از فایروال‌ها از چنین پیکربندی پشتیبانی می‌کنند. در برابر اصرار برای غیرفعال کردن تنظیمات پیکربندی کلاینت VPN جهت استفاده سرور VPN از گیت‌وی پیش‌فرض خود مقاومت کنید. زیرا این کار ویژگی Split Tunneling را که یکی از تهدیدات شناخته‌شده و خطرناک امنیتی محسوب می‌شود، فعال خواهد کرد.

۱۰ – چندین کاربر با استفاده از یک مجوز اعتبار PPP به سرور VPN متصل می‌شوند.

یکی از خطراتی که تمام سازمان‌هایی را که اقدام به پیاده‌سازی امکانات دسترسی راه‌دور به سرور VPN می‌کنند، تهدید می‌کند، این‌است که کاربران اطلاعات مربوط به نام کاربری و کلمه عبور را با یکدیگر به اشتراک می‌گذارند. در بسیاری از

پیاده‌سازی‌های سرور VPN شما قادر خواهید بود نه‌تنها پیش از برقراری ارتباط VPN نسبت به بررسی اعتبار و مجوز کاربر اقدام کنید، بلکه اگر آن کاربر به دسترسی به شبکه از طریق VPN مجاز نبود، درخواست لغو ارتباط به سرور صادر شود.

اگر کاربران به استفاده اشتراکی از مجوزها اقدام کنند، این عمل وضعیتی را ایجاد خواهد کرد تا کاربران غیرمجاز بتوانند با استفاده از مجوز کاربران مجاز به شبکه متصل شوند. یک راه‌حل برای این مشکل استفاده از الگوهای اضافی بررسی اعتبار است.

به‌عنوان مثال، شما می‌توانید مجوز کلاینت کاربر را نیز بررسی کنید. به‌این ترتیب، هیچ کاربر دیگری نمی‌تواند با مجوز یک کاربر مجاز وارد شبکه شود. انتخاب دیگر استفاده از کارت‌های هوشمند، ابزارهای بیومتریک و دیگر روش‌های دو فاکتوری تعیین هویت است.

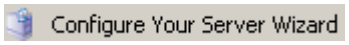
فصل ۳۳

Mail Server

۳۳-۱- نصب Mail Server

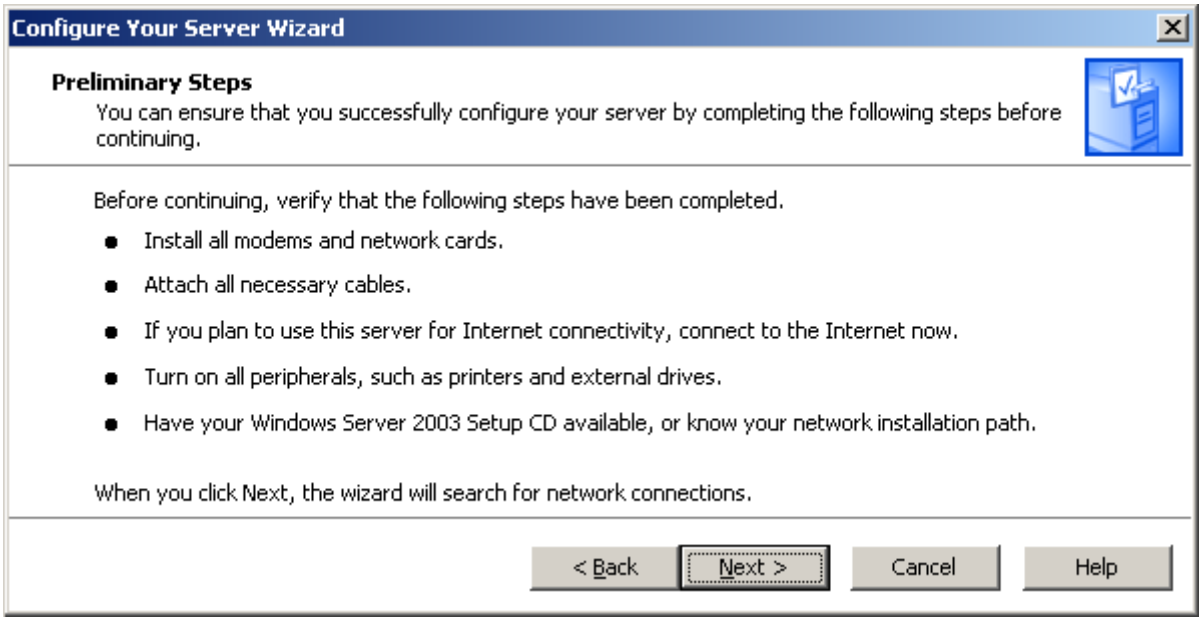
Mail Server، این امکان را به ما می‌دهد که برای کاربران شبکه خود ایمیل بسازیم و محل و آدرس این ایمیل‌ها، سرور خودمان باشد. با اینکار، نیاز به داشتن ایمیل‌های عمومی مانند Gmail و Yahoo از بین می‌رود. به علاوه اگر Mail Server ما دارای آدرس IP از نوع Valid باشد، امکان استفاده از این ایمیل‌ها در اینترنت نیز وجود خواهد داشت. IPهای Valid را بایستی از مخابرات خریداری نمود.

برای نصب Mail Server بر روی ویندوز سرور ۲۰۰۳، مسیر زیر را اجرا کنید: Start ➔ Administrative Tools ➔ Configure Your Server Wizard. این بخش جهت افزودن نقش (Role) به سرور مورد استفاده قرار می‌گیرد.

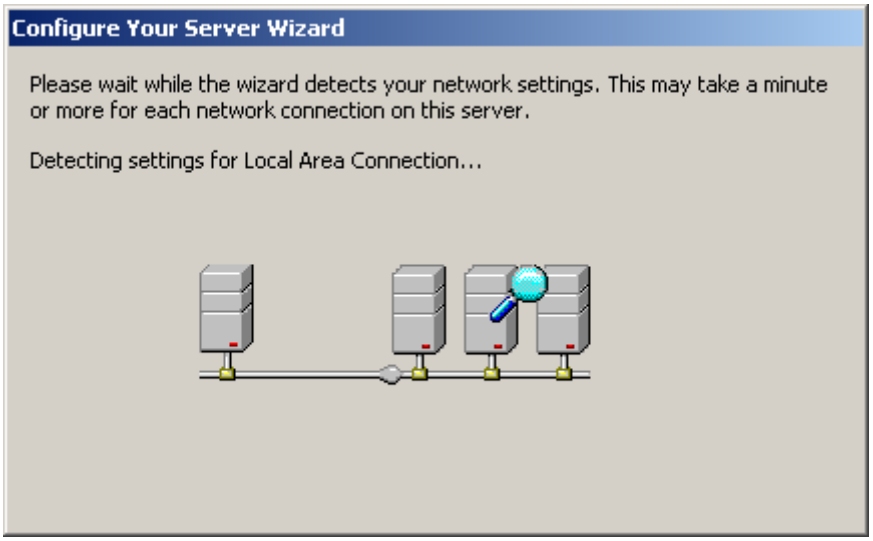


ابتدا صفحه خوش آمد گویی باز می‌شود. در این صفحه، دکمه Next را بزنید.

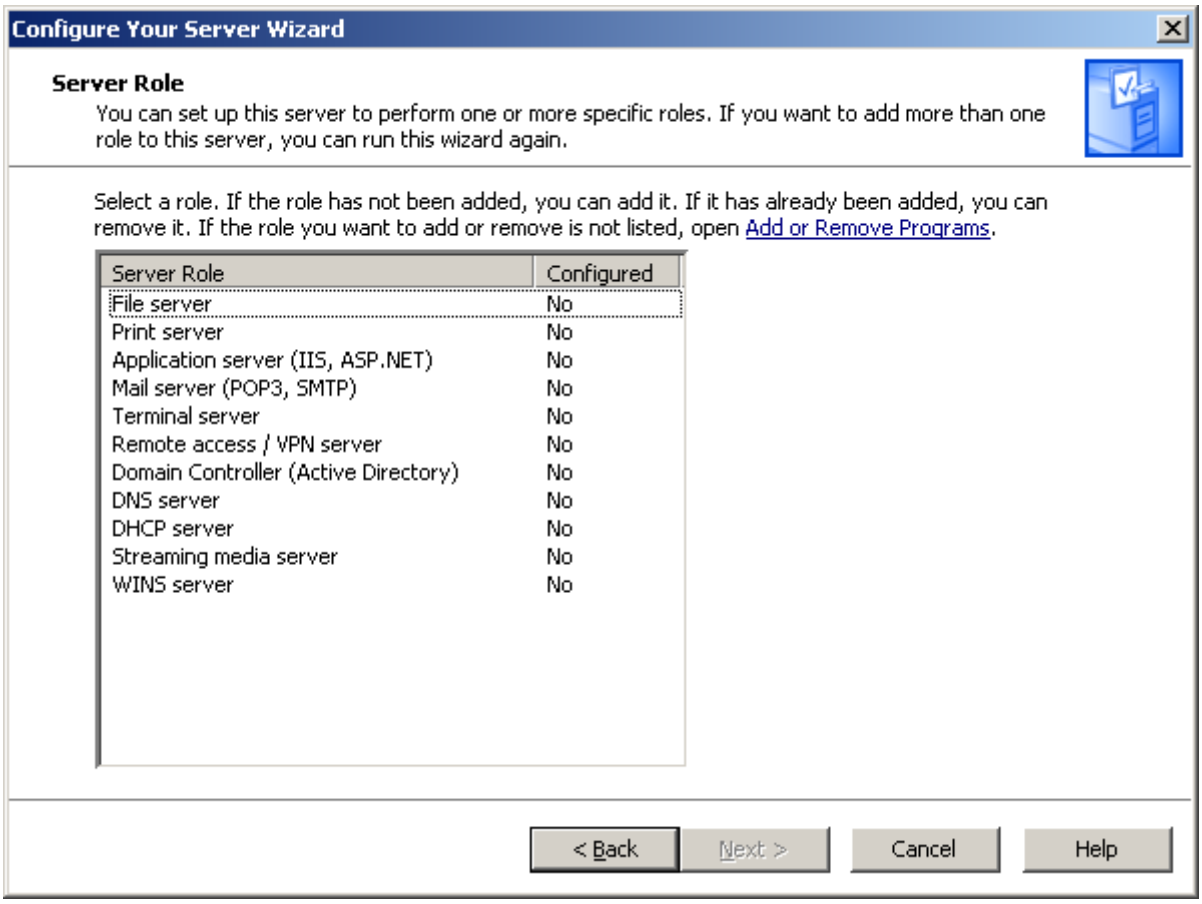
با این کار صفحه زیر ظاهر می‌شود که باید بر روی دکمه Next کلیک کنید.



پس از کلیک بر روی Next، صفحه زیر ظاهر می‌شود:



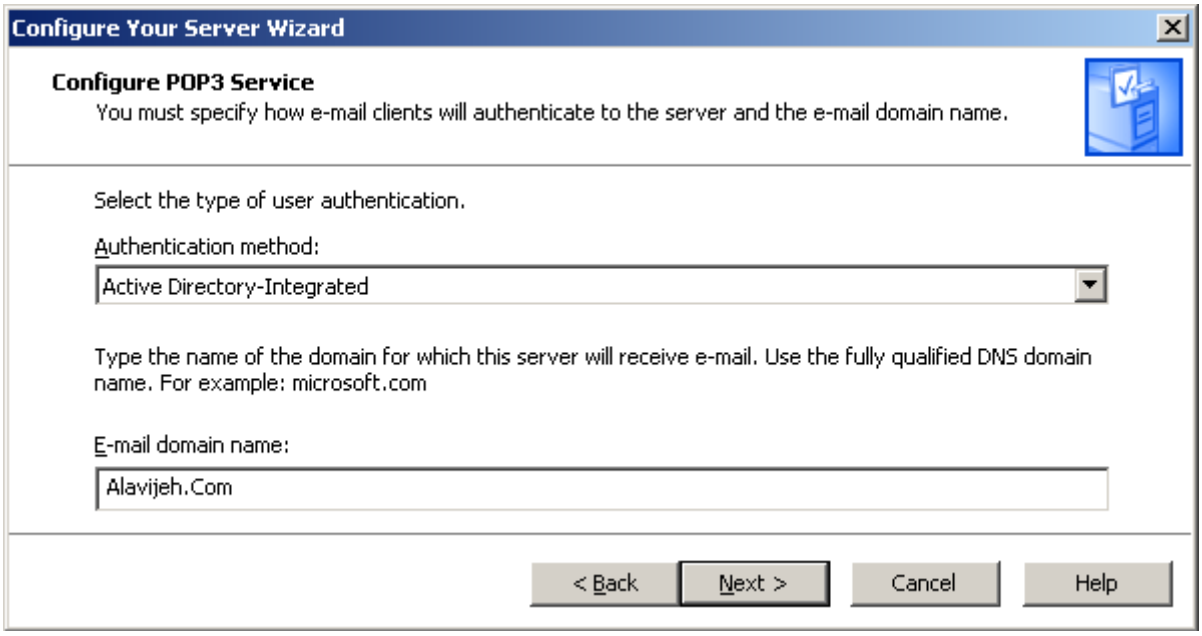
و سپس به صورت اتوماتیک صفحه زیر نمایان خواهد شد:



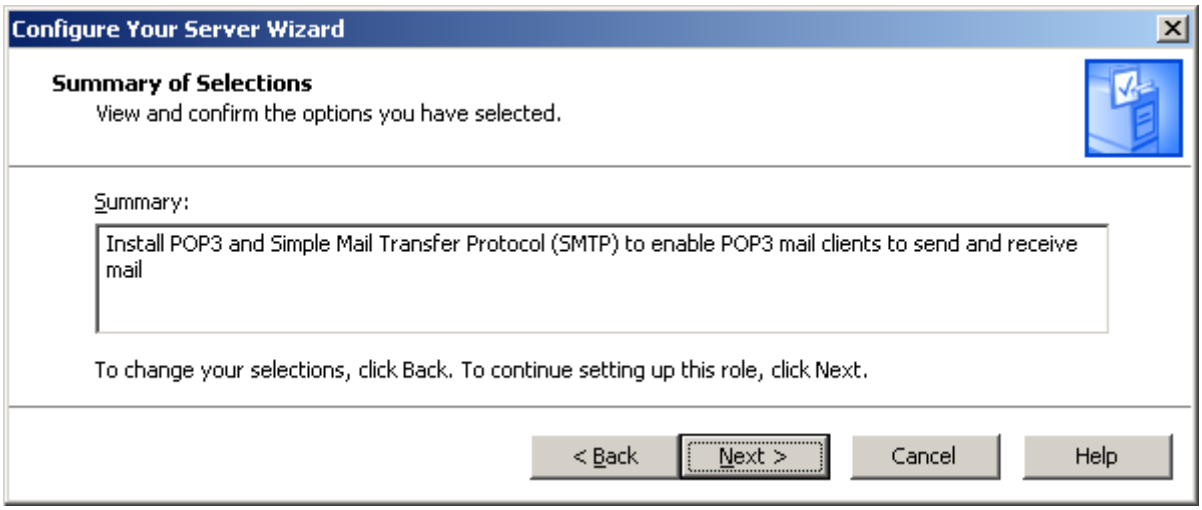
در این صفحه بر روی Mail Server (POP3 , SMTP) کلیک کرده و بر روی دکمه Next کلیک نمایید تا این نقش به نقش‌های سرور اضافه شود.



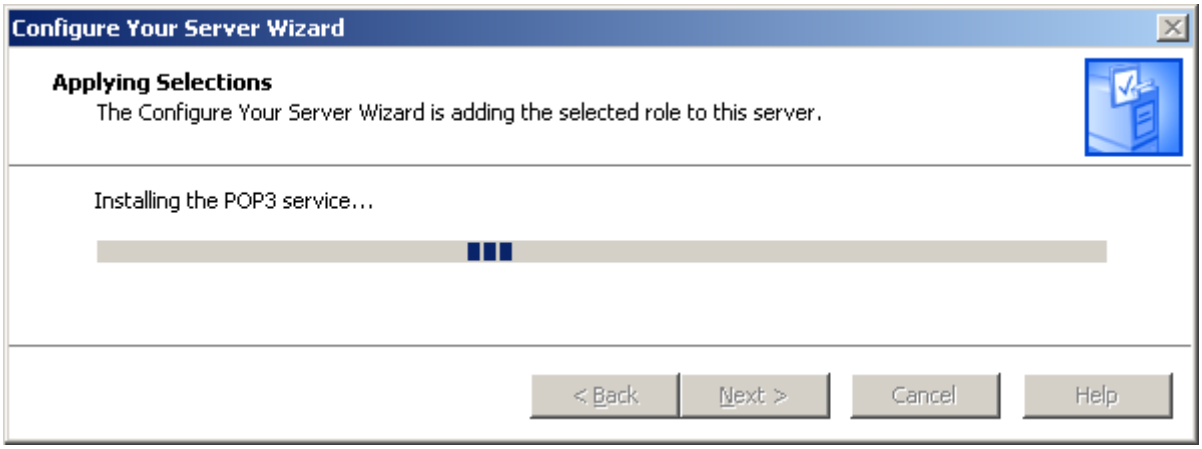
در مرحله بعدی نام Host مورد نظر خود را وارد کرده و سپس بر روی Next کلیک می‌کنیم. بهتر است نام Host را همان نام دامنه خود وارد نمایید. سپس روی Next کلیک کنید.



در این صفحه بر روی Next کلیک کنید.



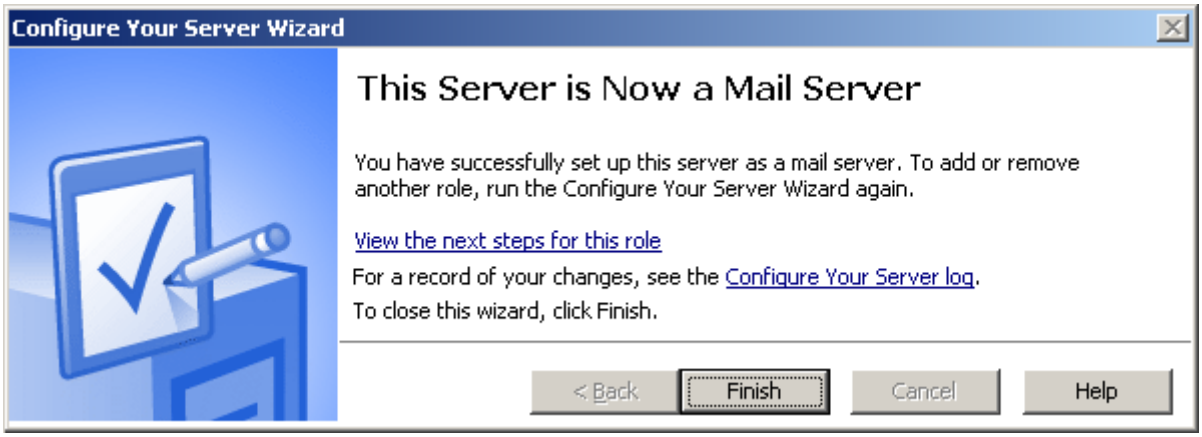
پس از کلیک بر روی دکمه Next، صفحه زیر ظاهر می‌شود:



پس از این مرحله نصب آغاز می‌شود و معمولاً نیاز به CD ویندوز سرور ۲۰۰۳ می‌باشد.



پس از پایان عملیات نصب صفحه اتمام نصب مشاهده می‌گردد که نشان می‌دهد Mail Server با موفقیت نصب شده است.

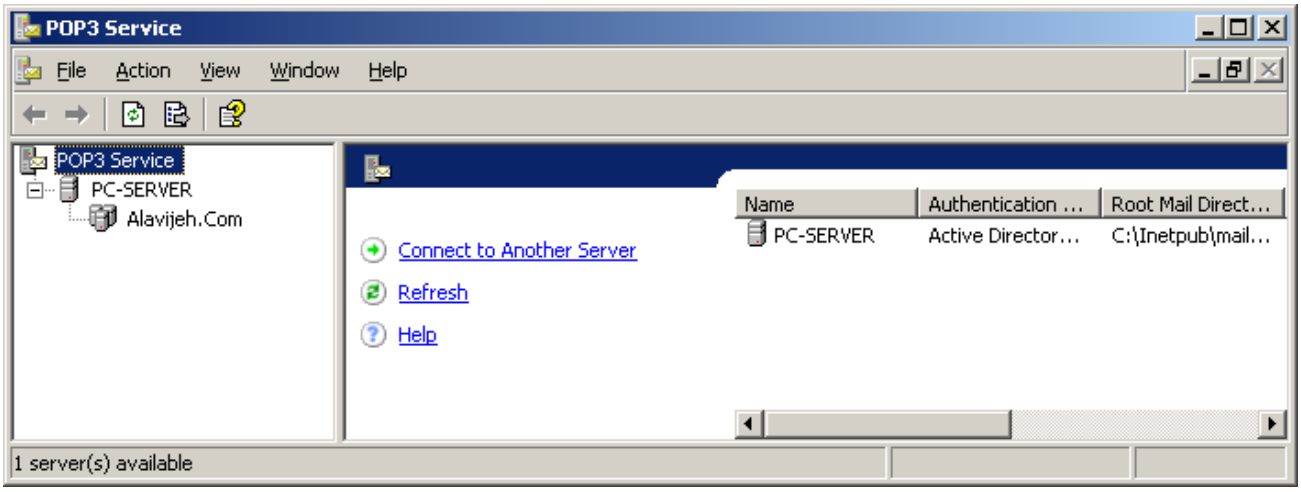


۳۳-۲- اجرای Mail Server

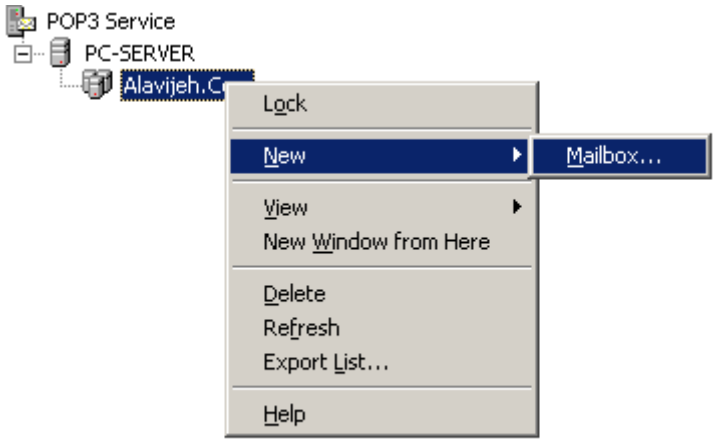
برای اجرا مانند شکل زیر از مسیر Administrative Tools ➔ Start، بر روی POP3 Service کلیک کنید تا برنامه سرویس ایمیل اجرا گردد.



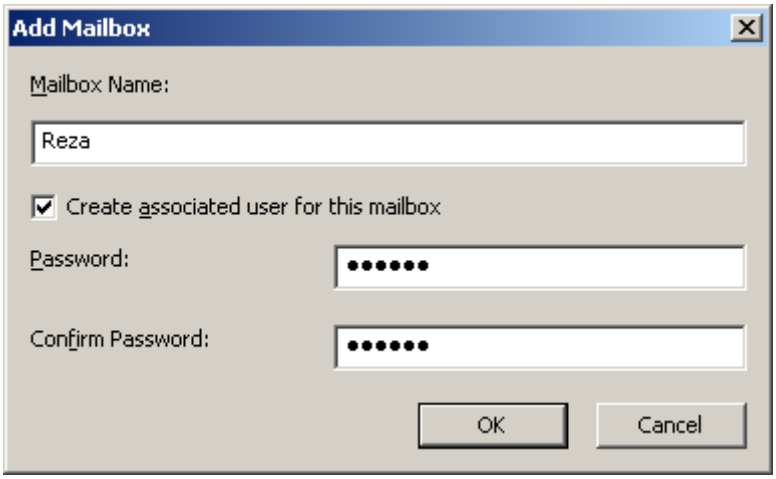
پس از اجرای Mail Server، صفحه زیر ظاهر می‌شود که نام Server و نام Host مورد نظر در آن قابل مشاهده می‌باشد.



برای ایجاد یک ایمیل جدید بر روی Host کلیک راست کرده و سپس بر روی MailBox ➔ New کلیک کنید.



سپس صفحه‌ای ظاهر می‌شود که در آن باید نام ایمیل و کلمه عبور را وارد نمائید.

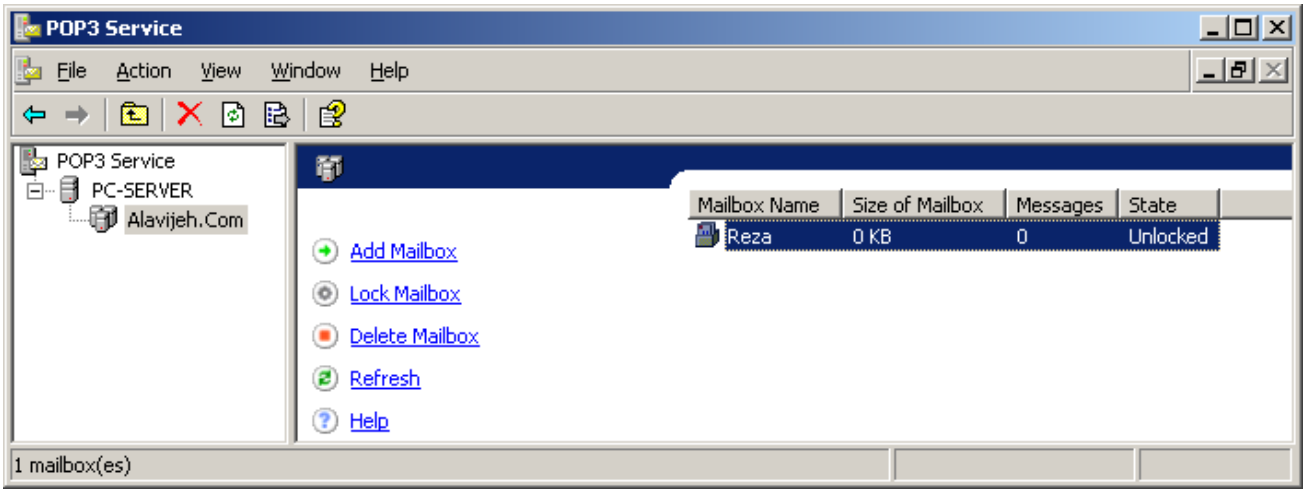


پس از کلیک بر روی OK، ایمیل جدید، مانند شکل زیر ظاهر می‌شود که شما می‌توانید تعداد ایمیل‌های بی شماری بر روی Hostهای مختلف ایجاد نمائید.



همانند شکل فوق پس از کلیک بر روی OK، پیغامی ظاهر می‌شود که اطلاعات مربوط به Account ایمیل ایجاد شده را نشان می‌دهد

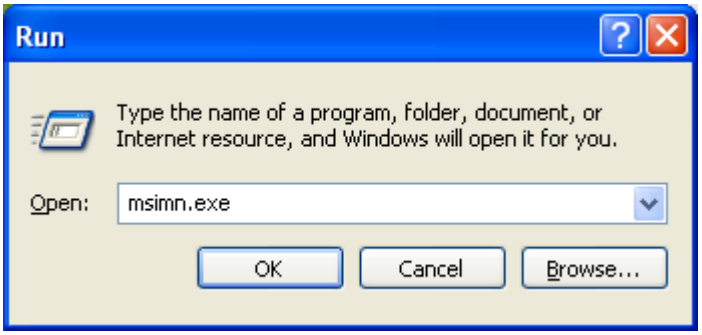
در این بخش شما می‌توانید ایمیل باکس ایجاد شده را نیز مدیریت نمائید. البته این بخش شامل یک سری دستورات و امکانات عمومی می‌باشد.



تا این مرحله Mail Server نصب شده است. حال نیاز به برنامه‌ای داریم که بتوانیم ایمیل ارسال و دریافت نماییم. برای این از نرم‌افزار Outlook Express استفاده می‌کنیم.

۳۳-۳- ارسال و دریافت ایمیل با استفاده از Outlook Express

برای اجرا و پیکربندی نرم‌افزار Outlook Express، در قسمت Run، دستور msimn.exe را نوشته و آن را اجرا کنید.

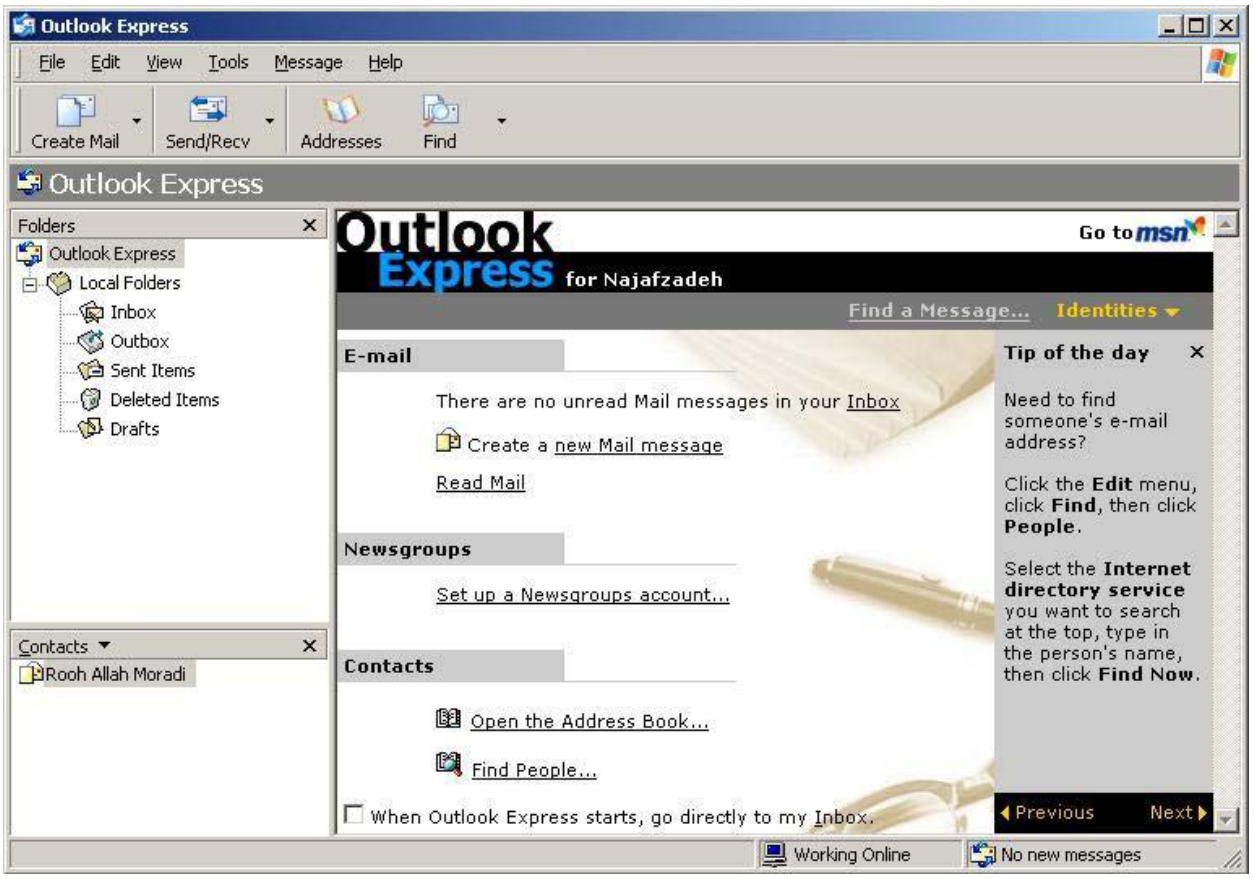


البته امکان باز کردن این نرم‌افزار به صورت مستقیم و از نوار Start وجود دارد.

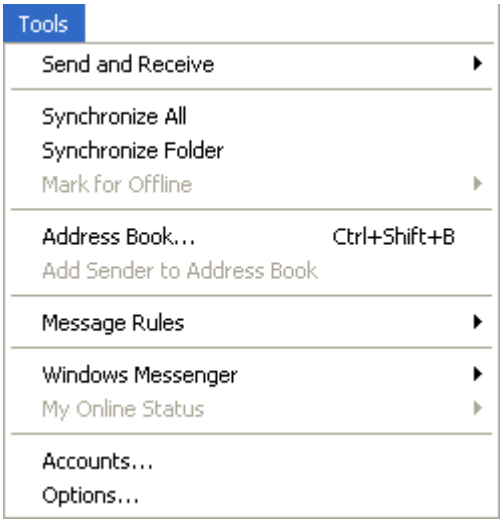
با این کار، نرم‌افزار Outlook Express اجرا می‌شود. در ابتدا سیستم اطلاعاتی مانند نام یا ایمیل شما را می‌پرسد. در صورت تمایل آن‌ها را وارد نمایید. در غیر اینصورت روی Cancel کلیک کنید. البته توصیه من نیز این است که حتما روی Cancel کلیک کنید. زیرا عملیات را در ادامه توضیح می‌دهیم.



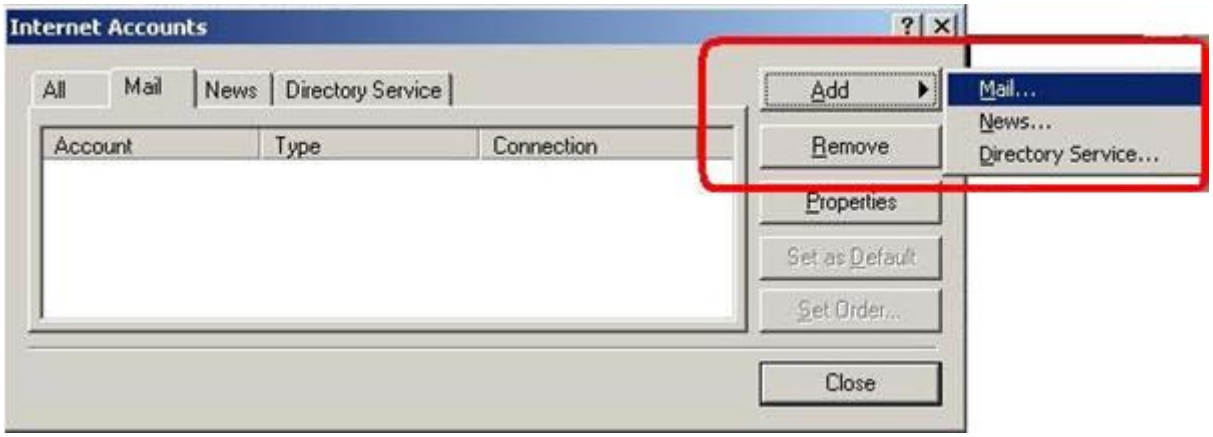
سپس شکل زیر ظاهر می‌شود:



ابتدا باید یک حساب ایجاد شده را معرفی نماییم. لذا از منوی Tools گزینه Accounts را انتخاب کنید.



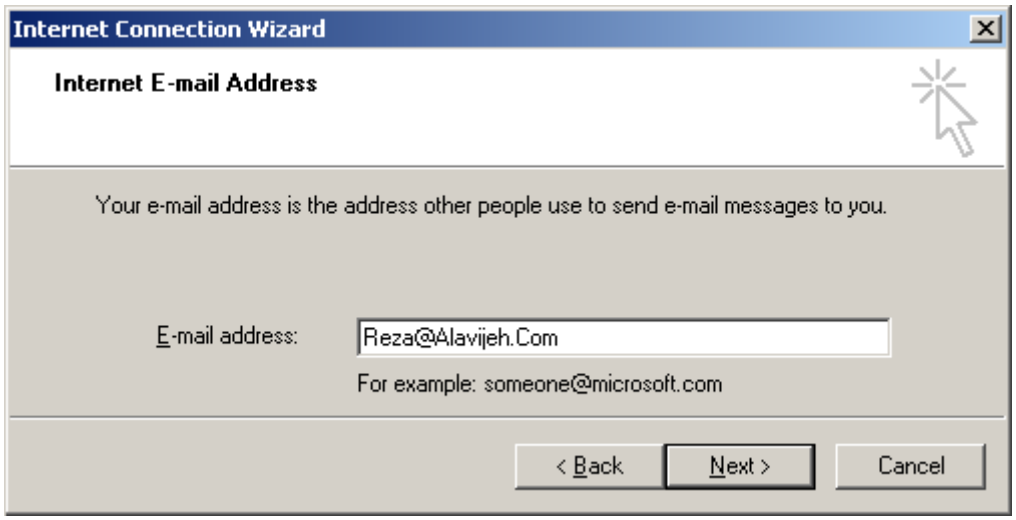
سپس صفحه زیر ظاهر می‌شود که باید در آن در سربرگ Mail، گزینه Mail ➔ Add را انتخاب نمایید.



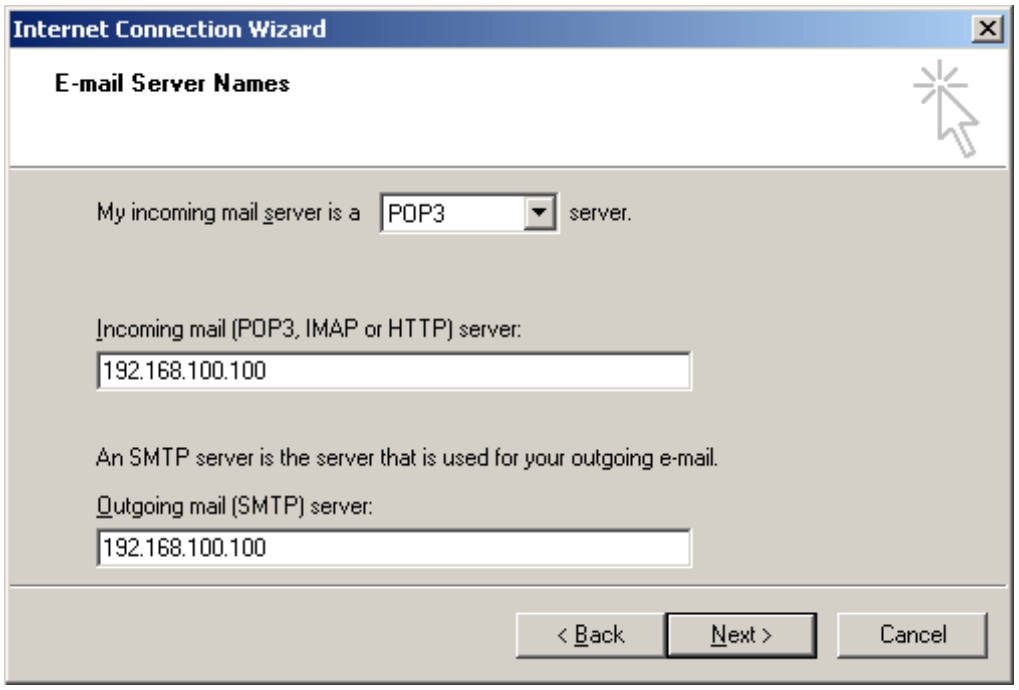
در مرحله بعد، نامی که به جای آدرس ایمیل (مثلاً نام صاحب ایمیل) نمایان خواهد شد را وارد نمایید.



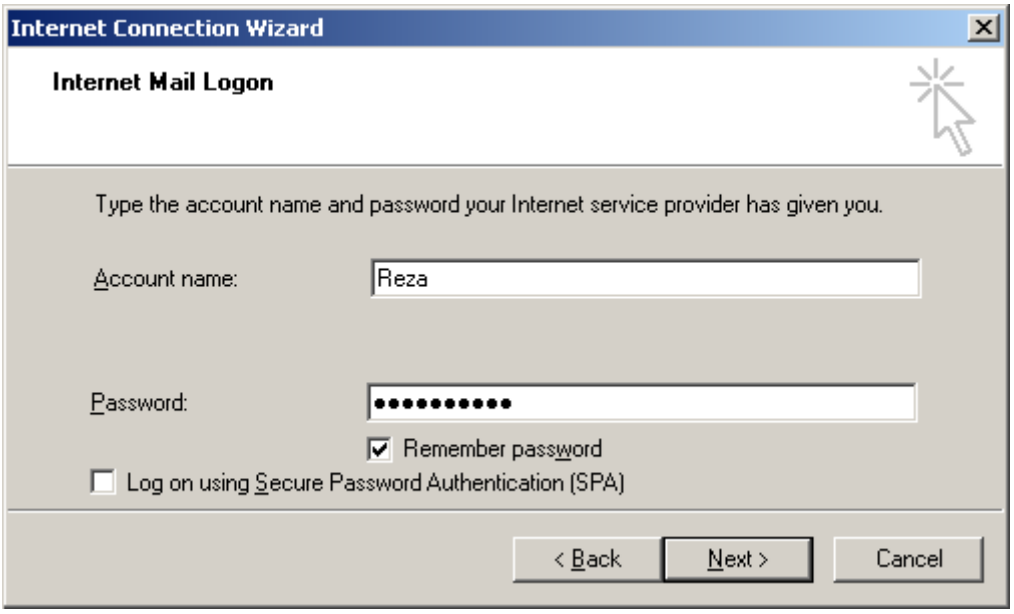
در مرحله بعدی آدرس ایمیل را به صورت کامل وارد کنید.



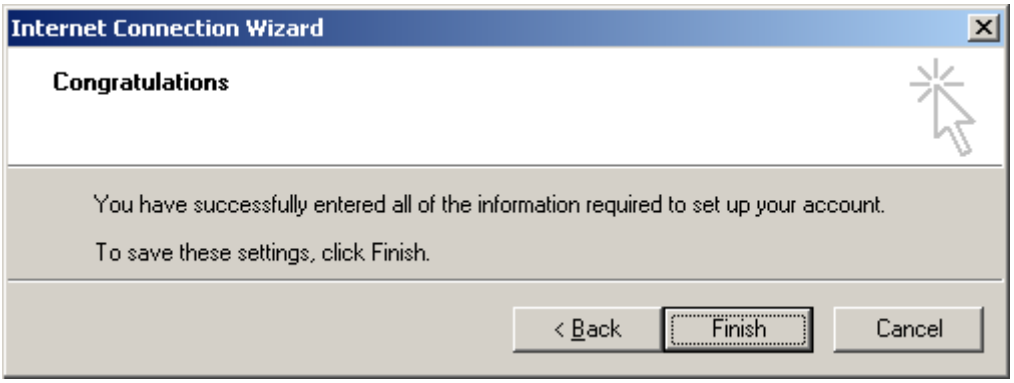
در مرحله بعدی باید تنظیمات SMTP و POP3 را انجام دهید. می‌توانید از آدرس IP یا نام سرور مورد نظر استفاده نمایید.



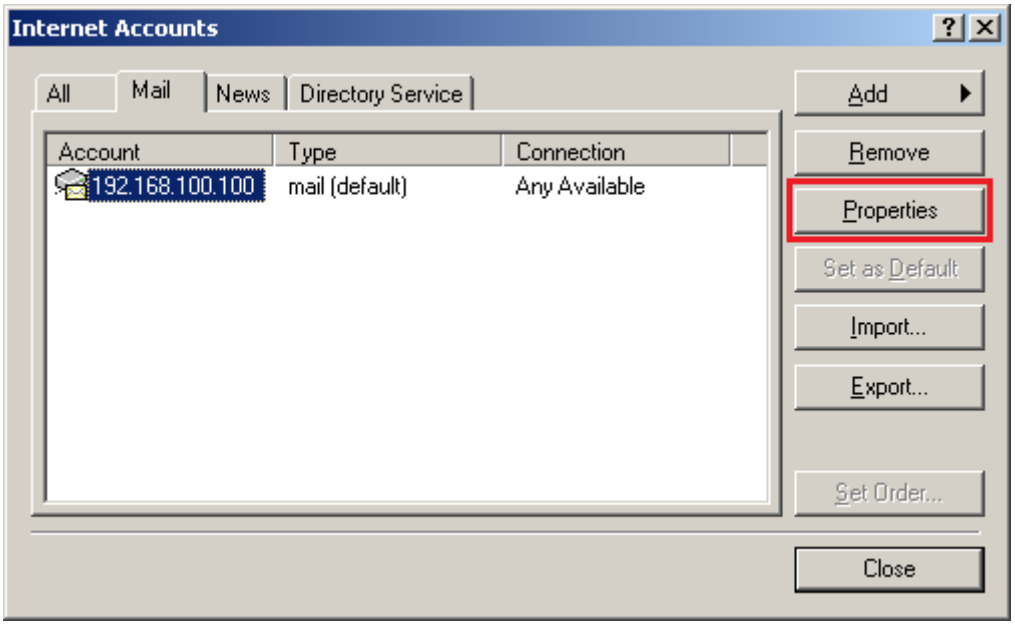
در مرحله بعدی، نام کاربری و کلمه عبور را وارد نمایید. توجه نمایید که نام کاربری ما در حقیقت آدرس کامل ایمیل می‌باشد.



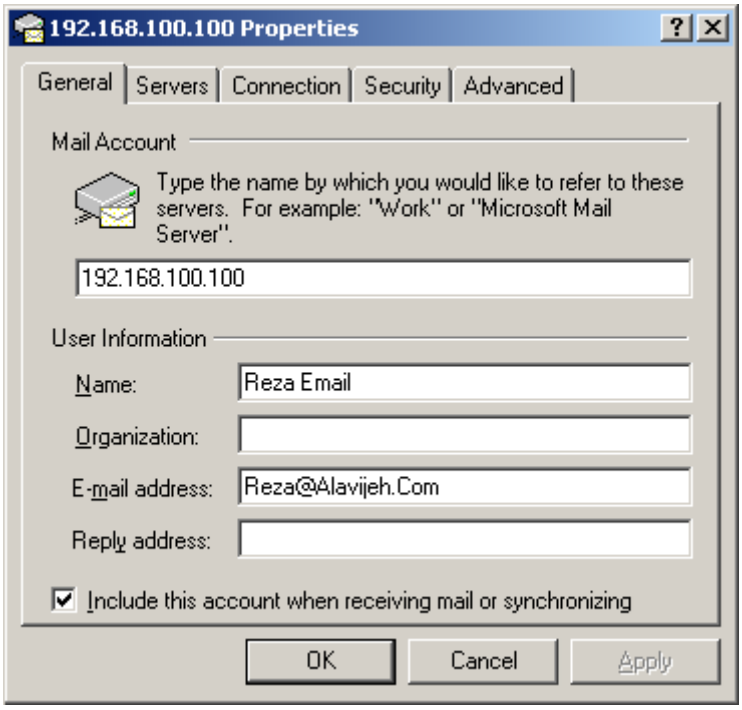
پس از این مرحله بر روی Finish کلیک کنید.



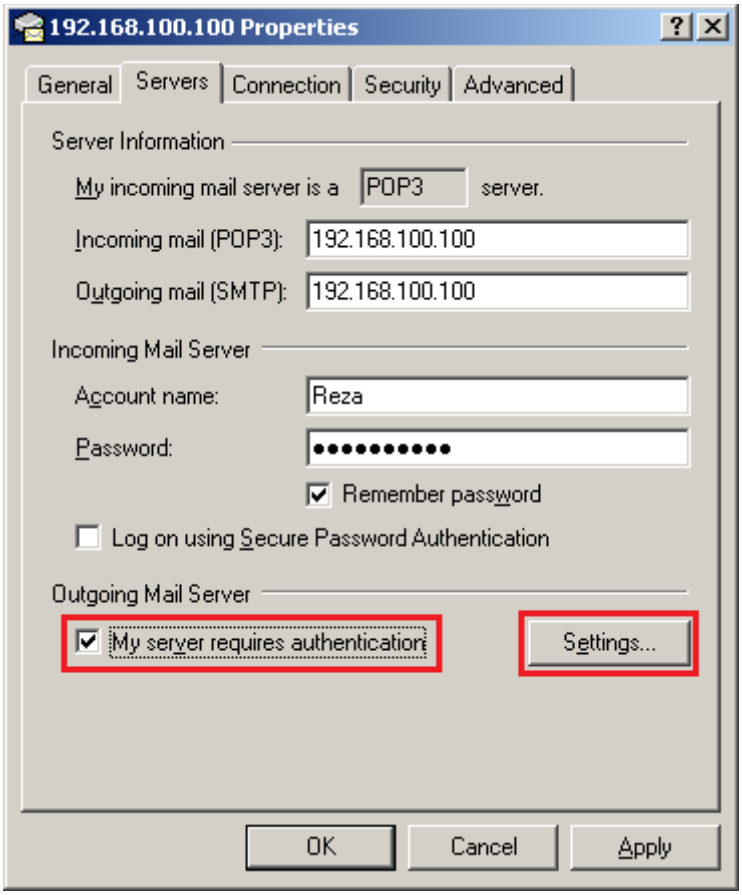
سپس مجددا به بخش Account وارد شده، بر روی آدرس ایمیل ساخته شده در بخش Mail کلیک نموده و در بخش سمت راست صفحه بر روی Properties کلیک می کنیم.



صفحه‌ای ظاهر می‌شود که در آن بر روی Servers کلیک می‌نماییم و تنظیمات دیگری را نیز انجام می‌دهیم.



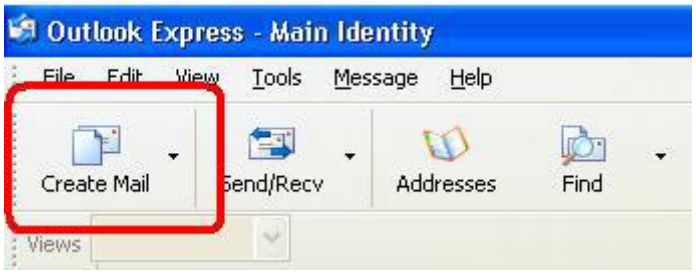
در ابتدا تیک مربوط به بخش My Server Requires authentication را زده و سپس بر روی دکمه Setting کلیک کنید.



سپس صفحه زیر ظاهر شده که باید نام کاربری و کلمه عبور را یک بار دیگر وارد نموده و سپس تیک گزینه Logon using Secure Password Authentication را می‌زنیم. توجه نمایید که در این بخش هم نام کاربری و هم نام دامنه (یعنی Alavijeh.Com) را وارد نمایید. سپس بر روی کلید OK کلیک کرده و از این بخش نیز خارج می‌شویم.

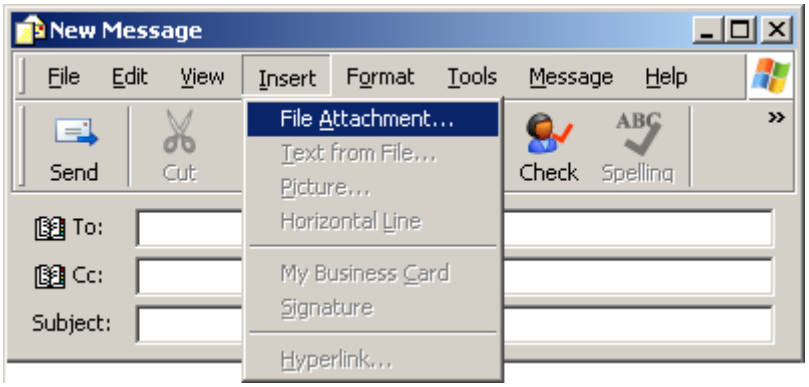


جهت ارسال ایمیل در Outlook Express، بر روی Create Mail کلیک کنید.

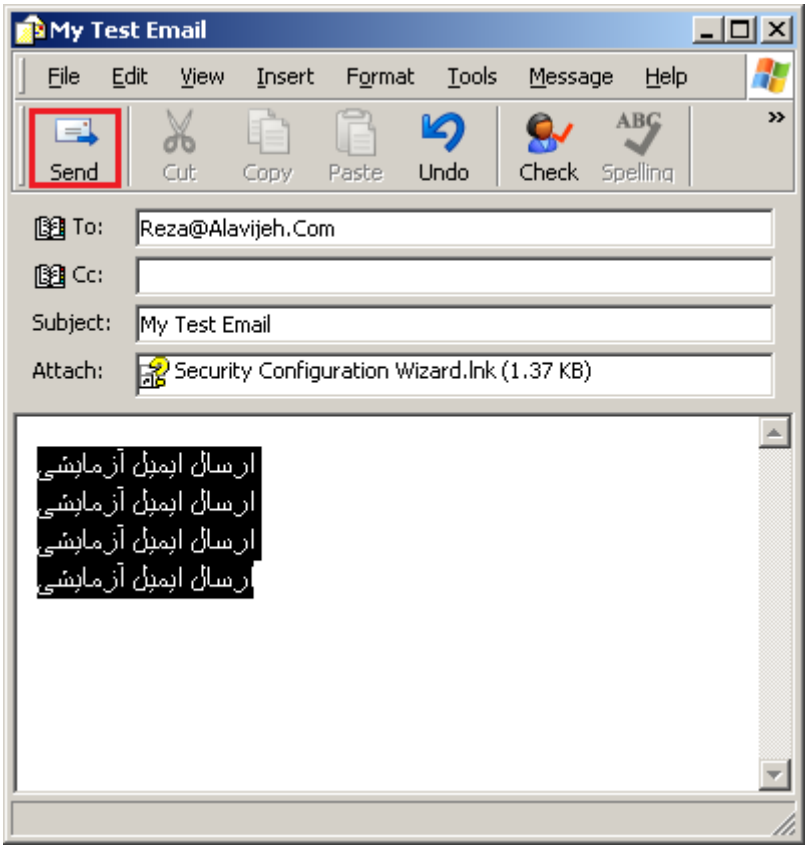


پس از این مرحله یک ایمیل خالی به شکل زیر ظاهر می‌شود که باید ایمیل گیرنده را و ارد نمود.

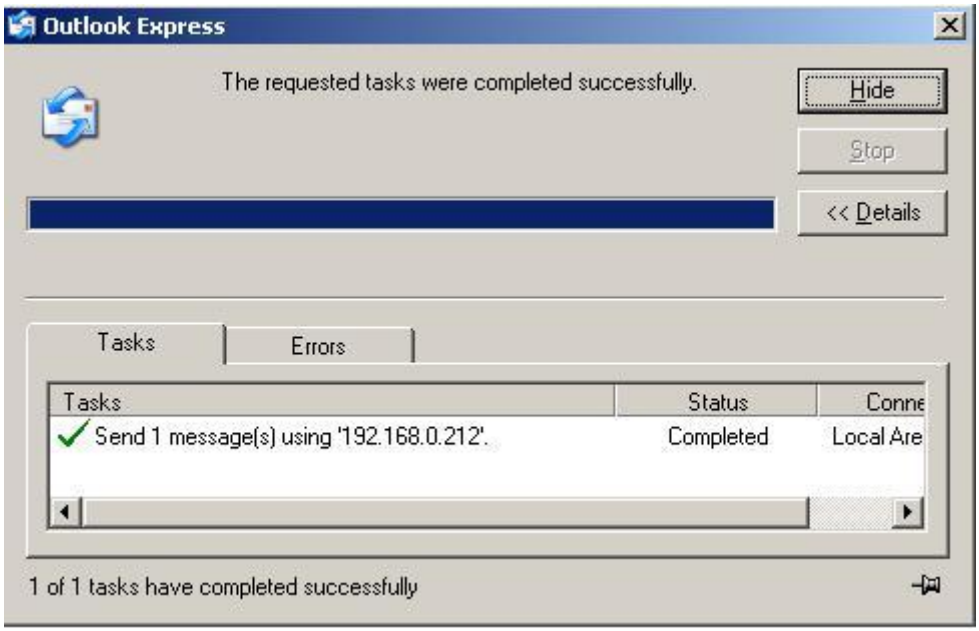
جهت ضمیمه نمودن فایلی خاص، از منوی Insert، گزینه File Attachment را انتخاب نمایید.



پس از وارد کردن اطلاعات مورد نیاز (ایمیل گیرنده، عنوان ایمیل، متن ایمیل، فایل‌های ضمیمه و...) بر روی Send کلیک کنید. در قسمت To، ایمیل گیرنده اصلی نامه و در قسمت Cc، ایمیل افرادی را وارد نمایید که یک رونوشت از ایمیل اصلی را دریافت می‌کنند. اعضای قسمت To متوجه می‌شوند که ایمیل برای چه کسانی در قسمت Cc ارسال شده است.



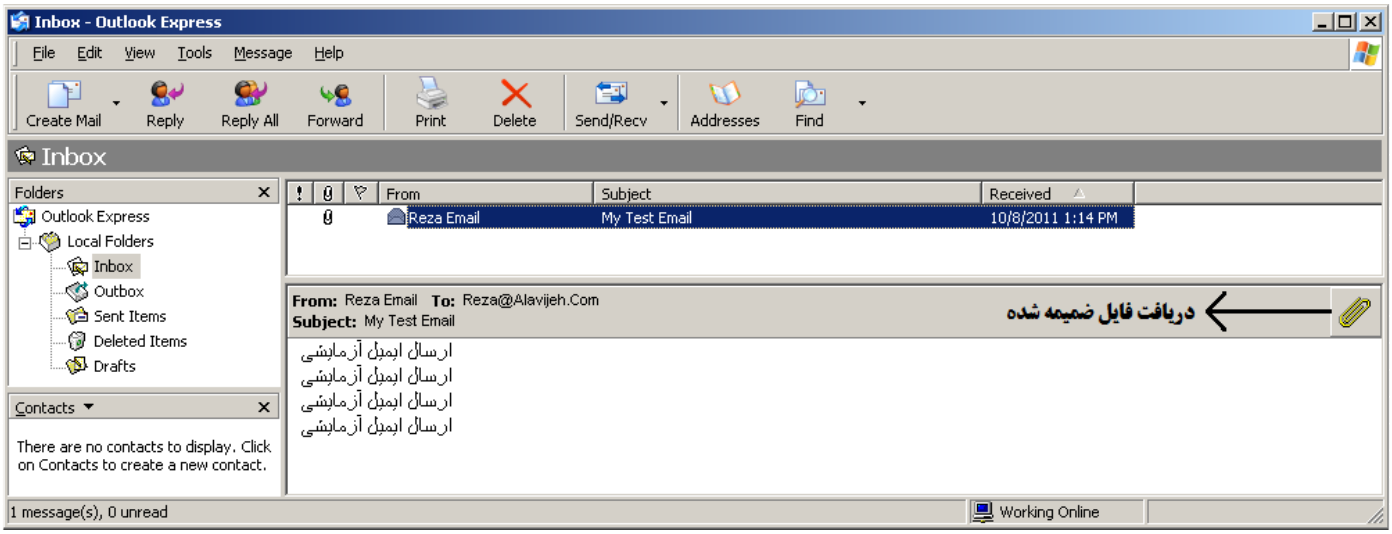
پس از ارسال شکل زیر در صورتی که ایمیل با موفقیت ارسال شود شکل زیر ظاهر می‌شود:



برای دریافت ایمیل نیز کافیست بر روی Send/Receive کلیک نمایید.



در صورتی که تنظیمات درست انجام شده باشد و ایمیلی در Inbox ما موجود باشد، توسط Outlook Express به صورت خودکار، به سیستم خودمان واکشی می‌شود.



۳۳-۴- نرم‌افزار مدیریت ایمیل MDaemon Mail Server

۳۳-۴-۱- *MDaemon Mail Server چیست؟*

تا اینجا یاد گرفتیم که چگونه یک Mail Server ایجاد نموده، سپس یک ایمیل داخل آن تعریف کرده و در نهایت توسط نرم‌افزار Outlook Express، از این ایمیل تعریف شده استفاده نماییم. این کار، کار خوبی است؛ اما نقص‌های زیادی دارد. مثلا چگونه می‌توانیم مانند جیمیل یا یاهو، به کاربران امکان دسترسی به ایمیل‌ها از طریق مرورگرهای وب و بدون درگیر کردن کاربر به مفاهیمی چون Incoming/Outcoming Mail Server را بدهیم؟

در این بخش به آموزش نرم‌افزاری به نام MDaemon Mail Server می‌پردازیم که امکانات زیادی را در اختیار ما قرار می‌دهد. برخی از این امکانات عبارتند از:

- دارای Antivirus جهت حفاظت از فرآیند انتقال اطلاعات
- مدیریت لیست و ایمیل‌های گروهی
- مدیریت مخاطبان
- دسترسی از راه دور و از طریق مرورگرهای وب به ایمیل
- مدیریت ایمیل‌های Spam، و ایجاد لیست‌های سیاه (Back List)
- یکپارچگی با Active Directory و استفاده از کاربران تعریف شده در سیستم
- کار با پروتکل‌های SMTP، POP3 و IMAP
- قابلیت مدیریت دفترچه تلفن و دفترچه آدرس
- پشتیبانی از ایمیل‌های مستعار (انتقال ایمیل دریافتی به صورت خودکار به ایمیلی دیگر) و...

۳۳-۴-۲- نصب MDaemon Mail Server

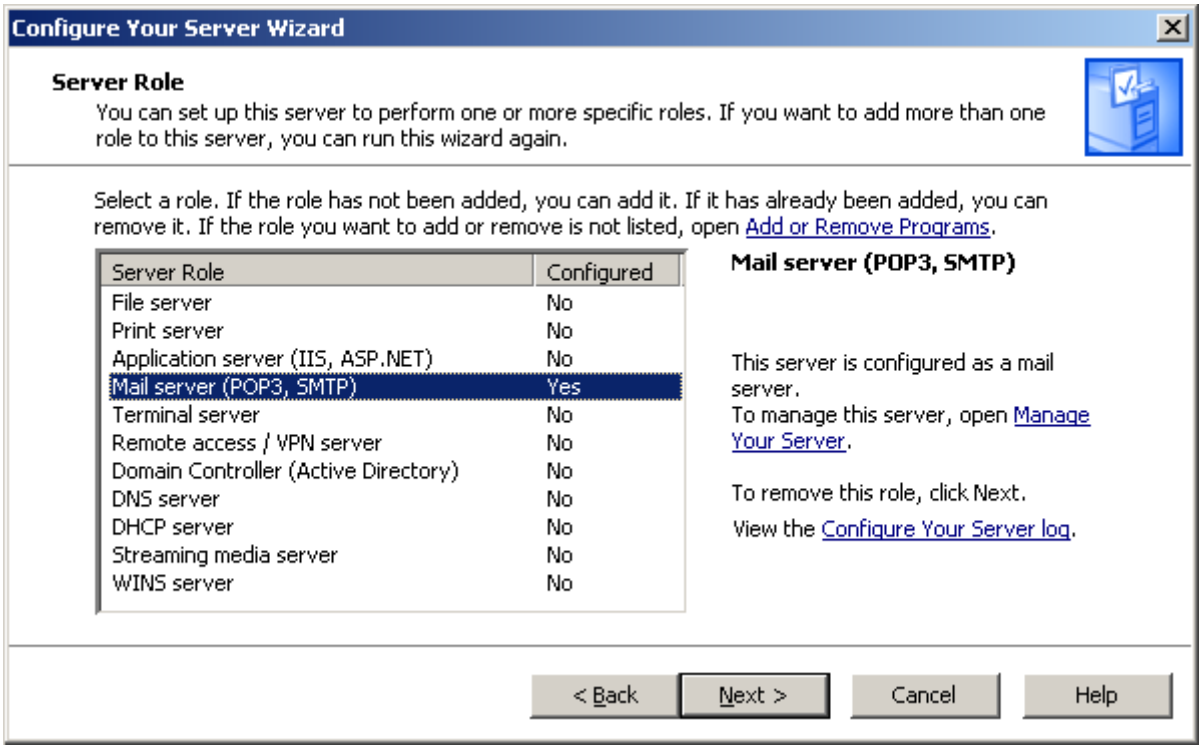
در این قسمت به آموزش نصب نرم‌افزار MDaemon Mail Server می‌پردازیم. نسخه‌ای که به آموزش آن خواهیم پرداخت، نسخه ۱۱ از نرم‌افزار MDaemon Mail Server است که حجمی حدود ۵۴ مگابایت دارد.

توجه: هنگام نصب MDaemon Mail Server، حتما بایستی به اینترنت متصل باشید.

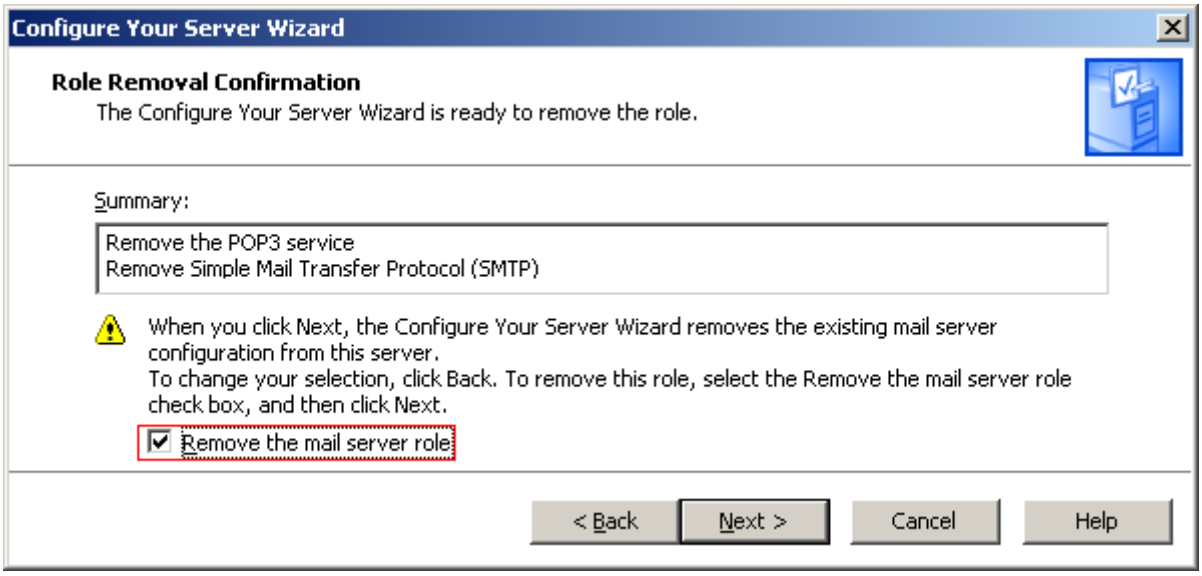
نکته مهم دیگر این است که حتما قبل از نصب MDaemon Mail Server، نقش Mail Server را از روی ویندوز سرور ۲۰۰۳ (چیزی که در بالا آموزش دادیم) حذف نمایید. توجه نمایید که MDaemon Mail Server روی اکثر سیستم عامل‌ها جواب می‌دهد و مستقل از سرویس Mail Server که روی ویندوز سرور ۲۰۰۳ نصب نمودیم عمل می‌کند. حتی جالب اینجاست که اگر نقش Mail Server روی ویندوز سرور ۲۰۰۳ نصب باشد، برخی از سرویس‌های MDaemon Mail Server اجرا نخواهد شد. جهت حذف نقش Mail Server از روی ویندوز سرور ۲۰۰۳، وارد Start ➔ Administrative Tools ➔ Configure Your Server Wizard شود.



در صفحه باز شده، چند بار Next بزنید تا صفحه مدیریت نقش‌های ویندوز سرور ۲۰۰۳ باز شود. در این صفحه مجددا گزینه Mail Server (POP3, SMTP) را انتخاب نمایید. اگر توجه نمایید، جلوی این گزینه کلمه Yes قرار دارد. این بدان معنا است که این سرویس در حال حاضر نصب بوده و اگر آن را انتخاب کرده و به مرحله بعد برویم، یعنی می‌خواهیم آن را حذف نماییم. روی Next کلیک کنید.



در صفحه بعد، گزینه Remember the mail server role را تیک بزنید. این بدان معناست که می‌خواهید این نقش را حذف نمایید. با کلیک روی Next، این نقش حذف خواهد شد.



حال نوبت به نصب نرم‌افزار MDaemon Mail Server می‌شود. فایل Setup آن را اجرا نمایید.



پس از عبور از صفحات خوش آمدگویی، بایستی مسیر نصب نرم‌افزار را تعیین نمایید.



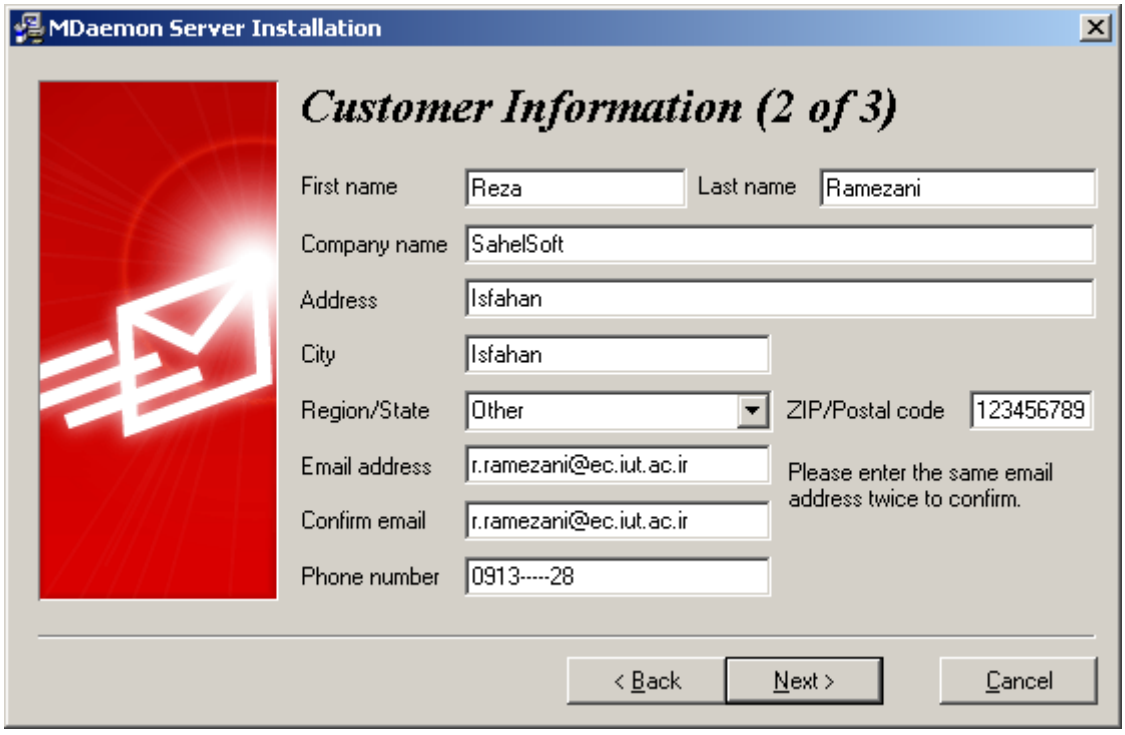
در صفحه بعد، شماره سریال نرم‌افزار را وارد نمایید. البته شما نیز مانند من سعی در خرید شماره سریال نمایید و از کرک‌های موجود استفاده نکنید که کار خیلی زشتیه! از این کار زشتا هیچوقت نکنید. بعله!



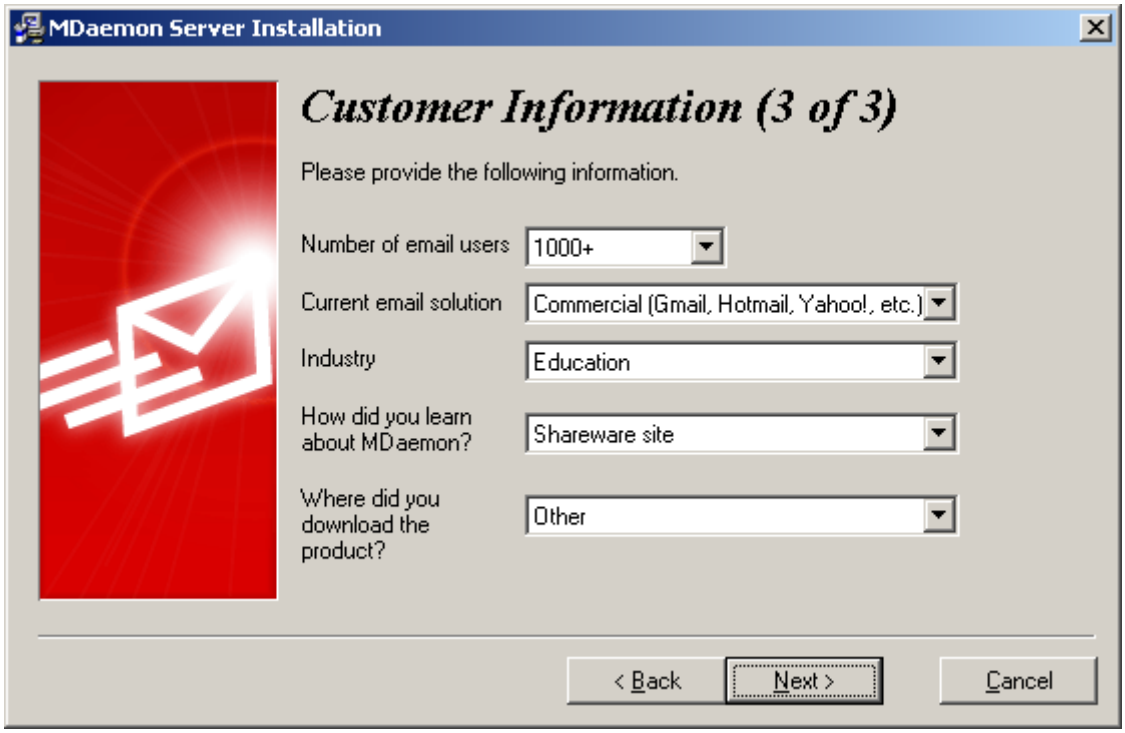
در صفحه بعدی، کشور خود را انتخاب نمایید.



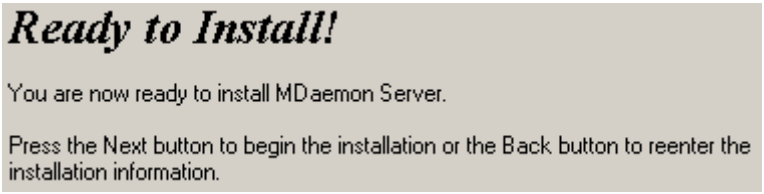
سپس اطلاعات شخصی خود را جهت ثبت در سایت شرکت سازنده وارد نمایید.



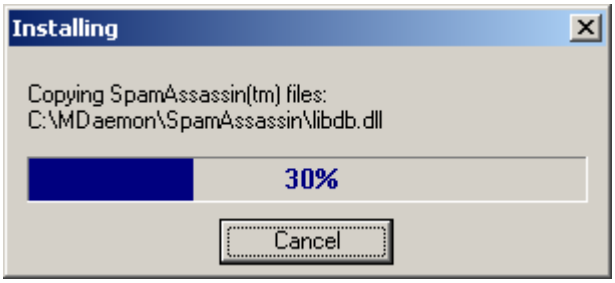
در نهایت به برخی از سوالات جانبی پاسخ دهید.



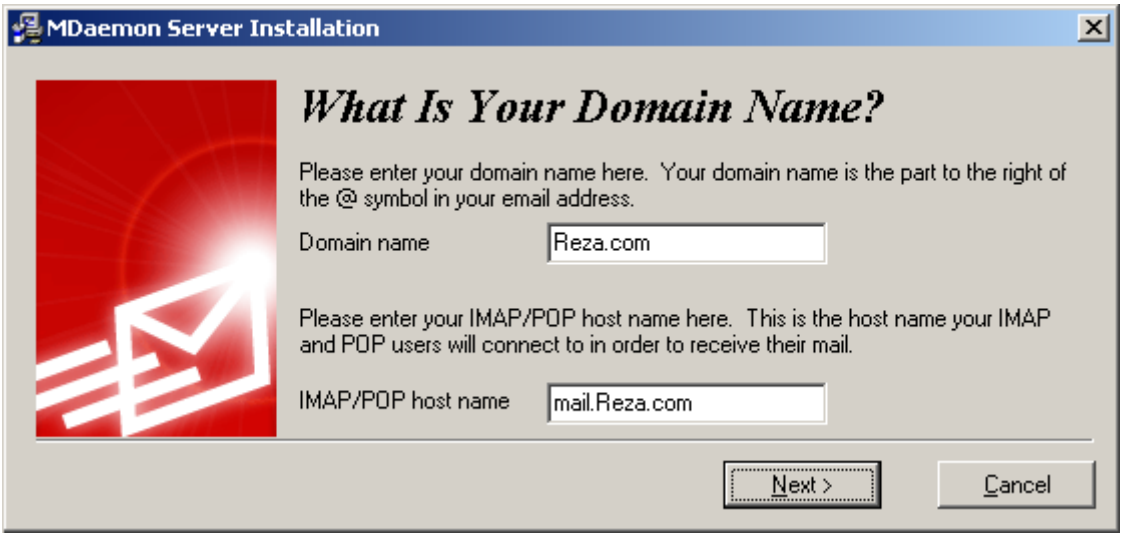
سوالاتی که در بالا پرسیده شد، عبارتند از: تعداد کاربران نرم‌افزار، سرویس ایمیلی که در حال حاضر از آن استفاده می‌کردیم، نوع استفاده از نرم‌افزار، چگونگی آشنایی با نرم‌افزار و چگونگی دانلود آن. با کلیک روی Next، نرم‌افزار، پس از اتصال به سایت سازنده، نرم‌افزار به اطلاع شما می‌رساند که آماده نصب است.



روی Install کلیک نمایید و صبر کنید تا نصب نرم‌افزار به پایان برسد.



پس از نصب، صفحه پیکربندی اولیه باز می‌شود. در این صفحه و در قسمت Domain Name، نرم‌افزار از شما می‌خواهد نام دامنه خود را وارد نمایید. نام دامنه همان نامی است که در انتهای آدرس ایمیل قرار می‌گیرد. مثلا Gmail.Com یا Yahoo.Com. در قسمت پایین نیز نام هاست نگهدارنده ایمیل‌ها را وارد نمایید که استاندارد آن کلمه mail قبل از نام دامنه است. بهتر است نام دامنه وارد شده، با نام سرور که از طریق اینترنت می‌توان به آن دسترسی داشت، یکی باشد.



در صفحه بعد، اولین ایمیل خود را بسازید که این ایمیل معمولا به عنوان ایمیل مدیریت شناخته می‌شود. ابتدا نام و نام خانوادگی خود، سپس آدرس ایمیل (بدون @ و نام دامنه) و در نهایت رمز عبور خود را وارد نمایید. توجه نمایید که رمز عبور بایستی شامل حروف کوچک و بزرگ و نیز عدد بوده و بین ۶ تا ۱۵ حرف طول داشته باشد. البته چگونگی تغییر سیاست رمز عبور را بعدا توضیح می‌دهیم. با کلیک روی Next اولین ایمیل شما ساخته خواهد شد.



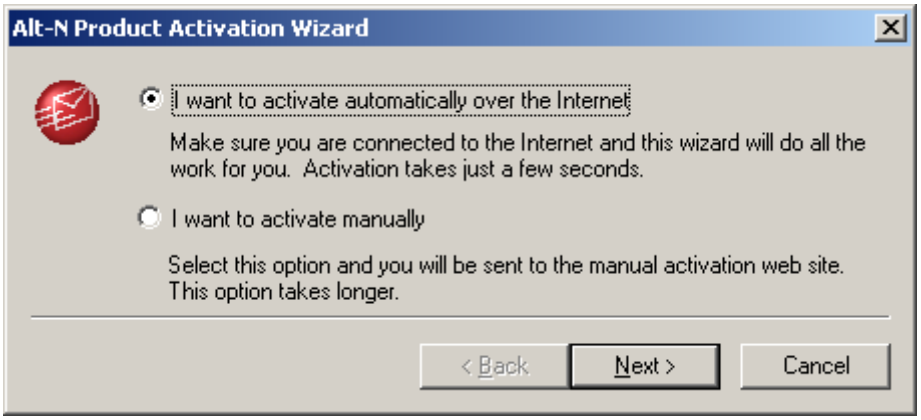
در صفحه بعد، تعیین نمایید که با هر بار روشن شدن کامپیوتر و بالا آمدن ویندوز، نرم‌افزار و سرویس MDaemon Mail Server به صورت خودکار اجرا گردد.



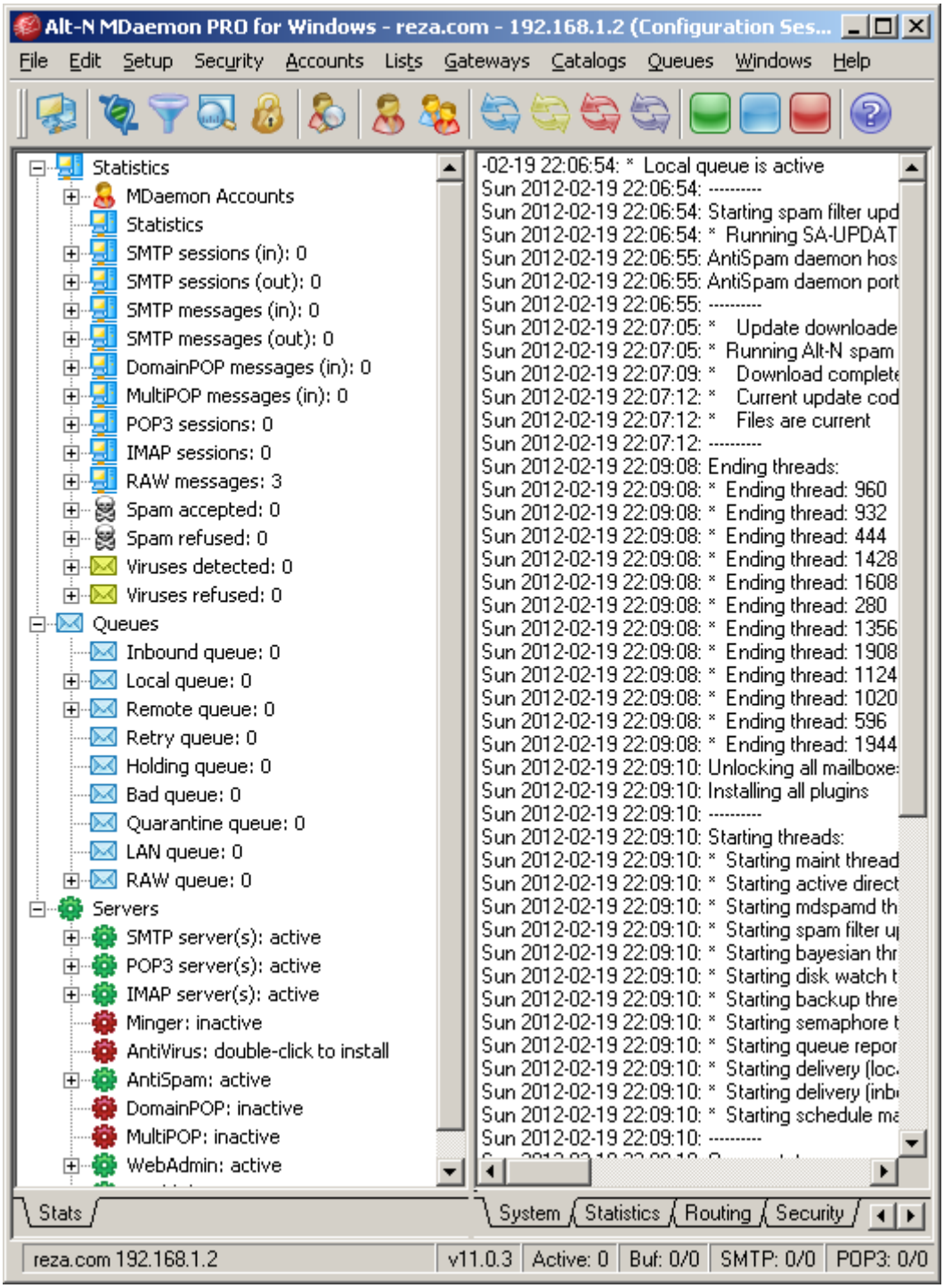
در صفحه بعد، با تیک زدن گزینه Start MDaemon، می‌گویید که نرم‌افزار اجرا گردد.



صفحه بعد، بایستی روش فعال سازی نرم‌افزار را تعیین نمایید. روش اول، فعال سازی از طریق اینترنت و دومی روش فعال سازی دستی است. روش اول بسیار ساده‌تر می‌باشد و اگر کد فعال سازی که هنگام نصب وارد نمودهاید، معتبر باشد، فرآیند فعال سازی به صورت خودکار انجام می‌گیرد. ما گزینه اول را انتخاب می‌کنیم. روی Next کلیک کنید تا فرآیند فعال سازی از طریق اینترنت انجام شود.

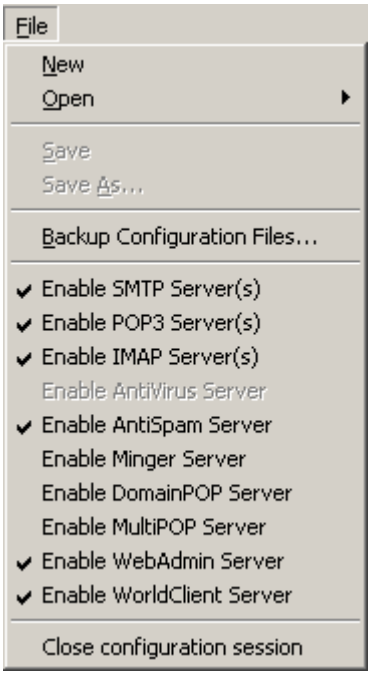


در نهایت نرم‌افزار باز شده و صفحه اول آن را مشاهده می‌نمایید. در بالا، منوهای نرم‌افزار را می‌بینید. در سمت راست، خلاصه‌ای از عملیاتی که انجام می‌شود را خواهید دید و در سمت چپ نیز می‌توانید وضعیت خود نرم‌افزار و برخی از سرویس‌های آن را مشاهده نمایید.

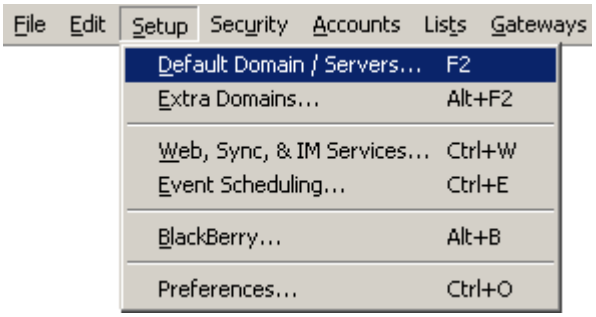


۳۳-۴-۳- پیکربندی نرم‌افزار *MDaemon Mail Server*

در ادامه به آموزش پیکربندی نرم‌افزار MDaemon Mail Server خواهیم پرداخت. ابتدا منوی File را باز نمایید. از طریق این منو می‌توانید وضعیت سرویس‌های نرم‌افزار را مشاهده نمایید. سرویس هایی که کنار آن‌ها تیک قرار دارد، به معنای فعال بودن آن‌ها است. برای فعال کردن هر سرویس، روی آن کلیک کنید. اگر سرویس Mail Server را از ویندوز سرور حذف نکرده باشید، سرویس‌های SMTP و POP3 در MDaemon Mail Server فعال نخواهند شد. دلیل نیز به خاطر شماره پورت مورد استفاده می‌باشد.



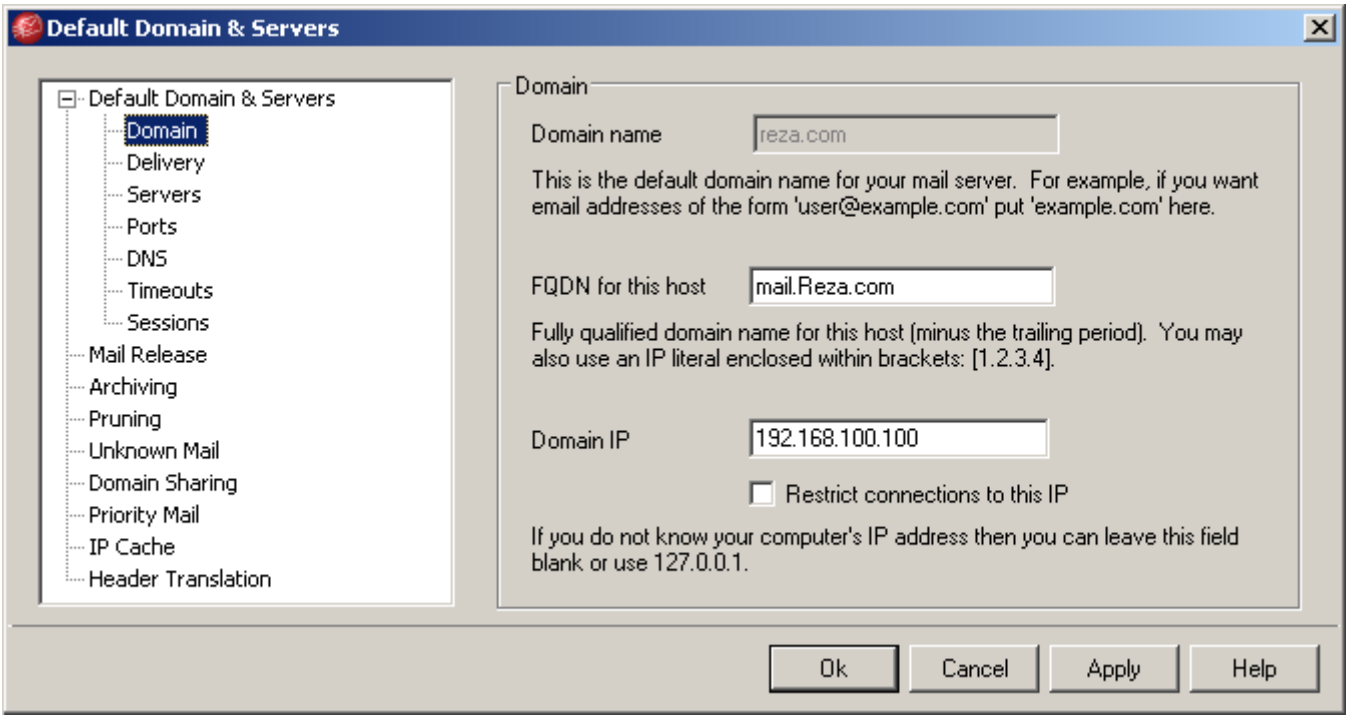
منوی پر اهمیت بعدی، منوی Setup می‌باشد که جهت انجام بسیاری از تنظیمات از آن استفاده خواهیم نمود. گزینه اول این منو، Default Domain / Servers می‌باشد که برای تنظیم اطلاعات سرور مورد استفاده می‌باشد. روی آن کلیک کنید.



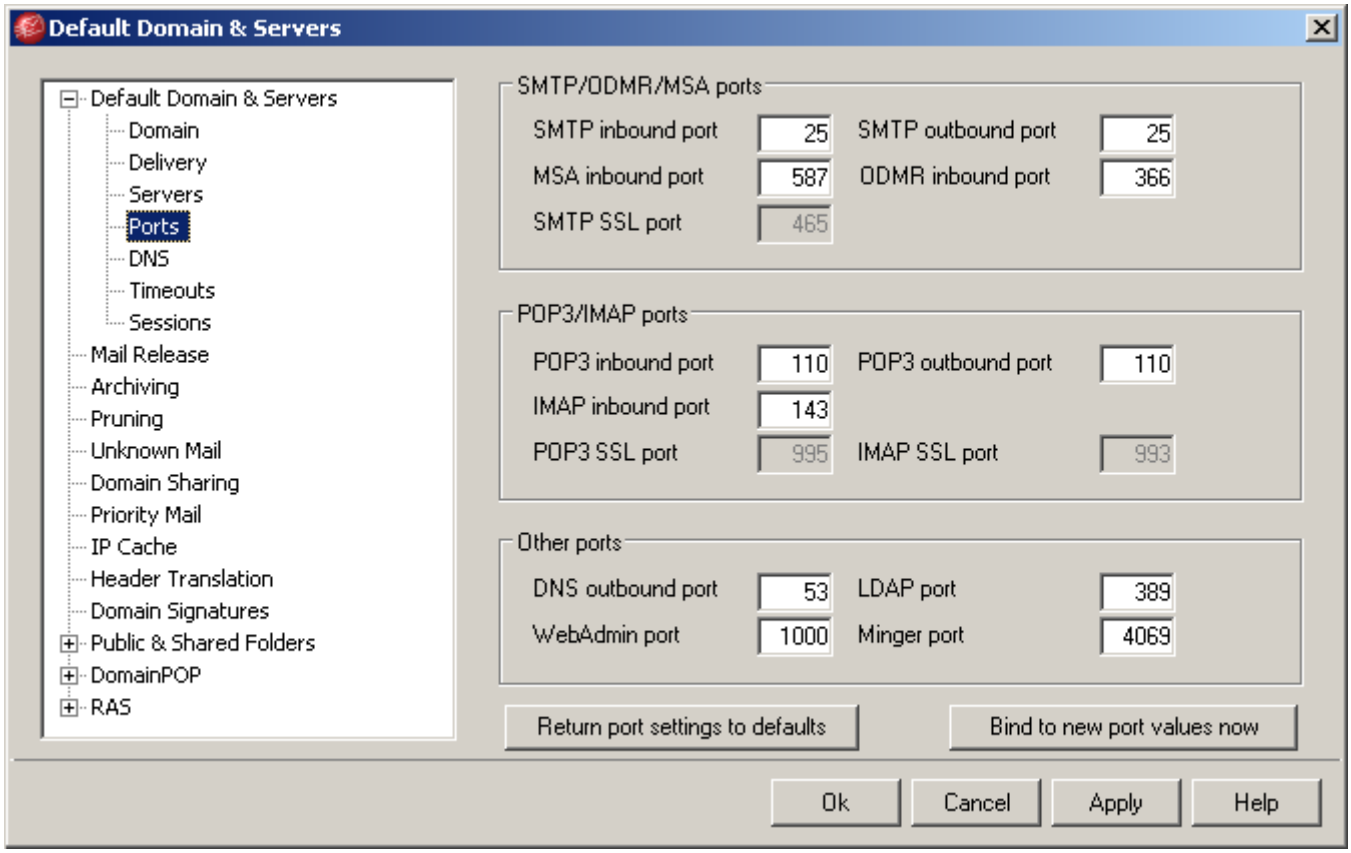
در این صفحه، در سمت چپ انواع تنظیمات قابل اعمال را مشاهده می‌نمایید. با انتخاب هر کدام از این گزینه‌ها، می‌توانید تنظیمات مربوط به آن را در صفحه سمت راست انجام دهید. در ادامه برخی از این تنظیمات را توضیح می‌دهیم. مثلا در شکل زیر، قسمت Domain را انتخاب کرده‌ایم. در سمت راست می‌توانید نام Domain را مشاهده نمایید.

گزینه قابل تنظیم بعدی، FQDN یا نام هاست نگهدارنده ایمیل در دامنه است. جهت آشنایی با FQDN به فصل DNS Server مراجعه نمایید.

گزینه قابل تنظیم بعدی، آدرس IP کامپیوتر نگهدارنده ایمیل‌ها است. این کامپیوتر همان کامپیوتری است که نرم‌افزار MDaemon Mail Server روی آن نصب شده است. از طریق این آدرس IP می‌توان از طریق مرورگرهای وب، ایمیل‌ها را مشاهده نمود.

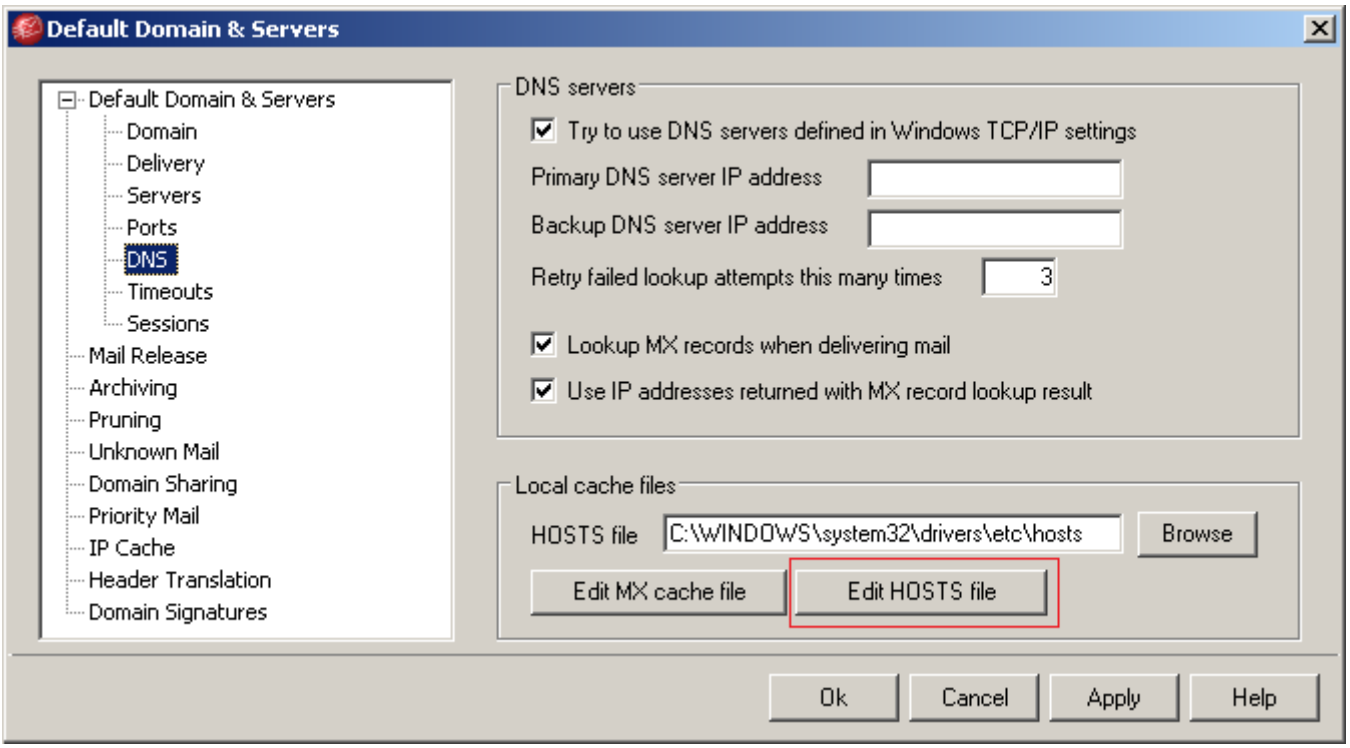


قسمت قابل تنظیم بعدی، قسمت Ports است که جهت تعیین هر کدام از پورت هایی است که سرویس‌های مختلف نرم‌افزار MDaemon Mail Server از آن‌ها استفاده می‌کند. با پورت‌ها در درس مهندسی اینترنت بیشتر آشنا خواهید شد، ولی اگر بخواهید به طور مختصر بدانید، هر نرم‌افزار هنگام کار با شبکه یا اینترنت، بایستی از یک پورت خاص استفاده نماید. حدود ۶۵۵۳۵ عدد پورت وجود دارد.

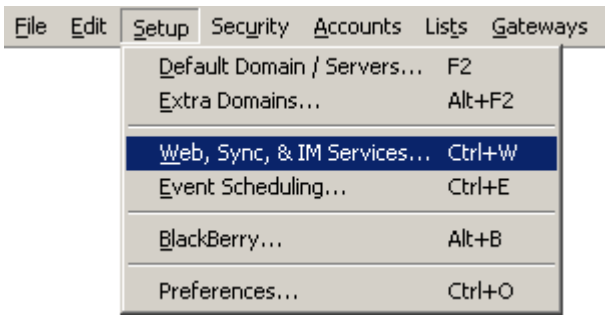


قسمت قابل تنظیم بعدی، DNS است که جهت تعیین DNS Server مورد استفاده قرار می‌گیرد. در مورد DNS در فصل‌های مختلف و هنگام تنظیم آدرس IP صحبت کرده‌ایم.

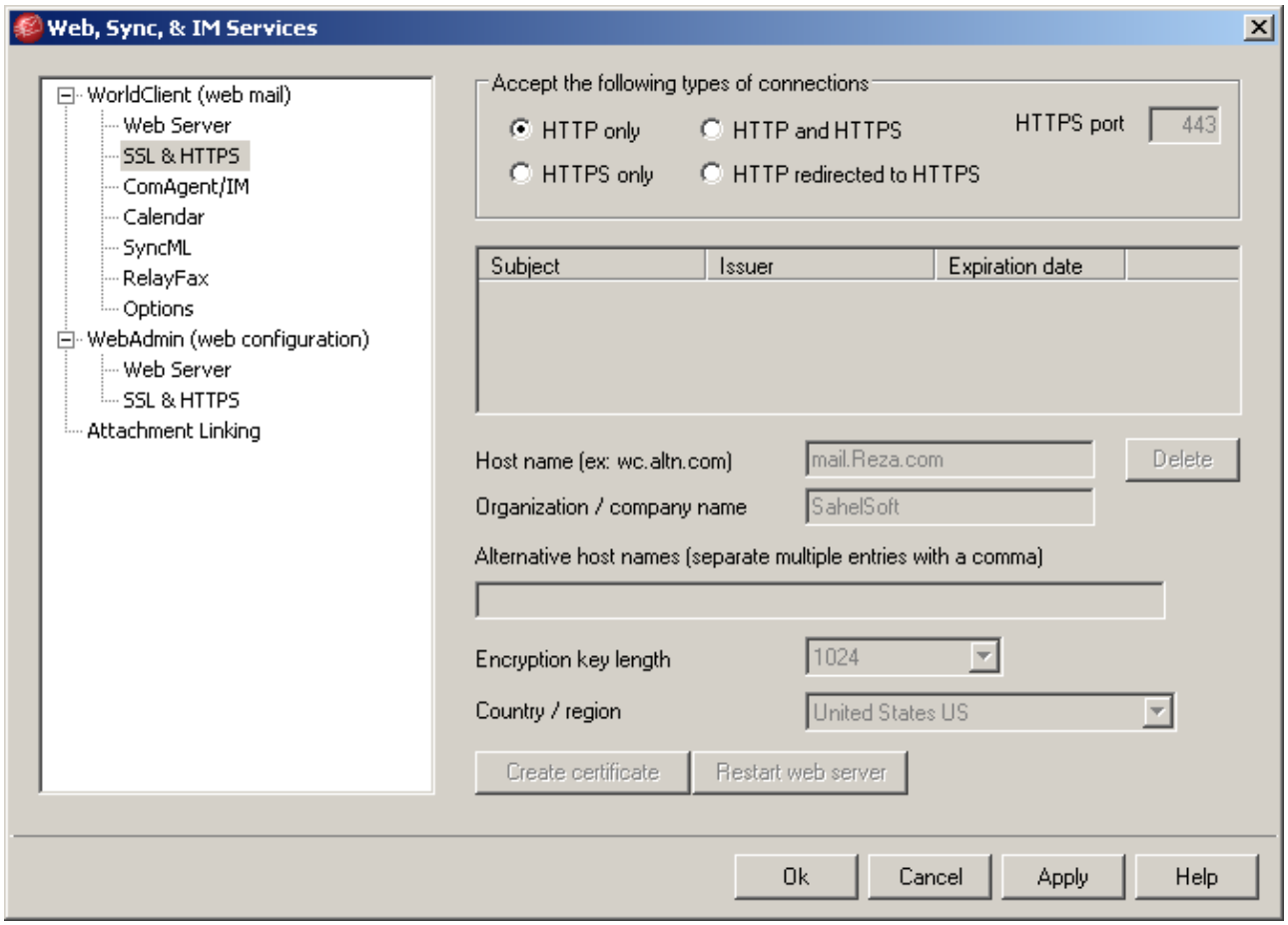
در فصل DNS Server، صحبت کردیم که اگر DNS Server وجود نداشته باشد، از یک فایل متنی به نام hosts استفاده می‌شود. جهت ویرایش این فایل، روی دکمه Edit HOSTS file کلیک کنید.



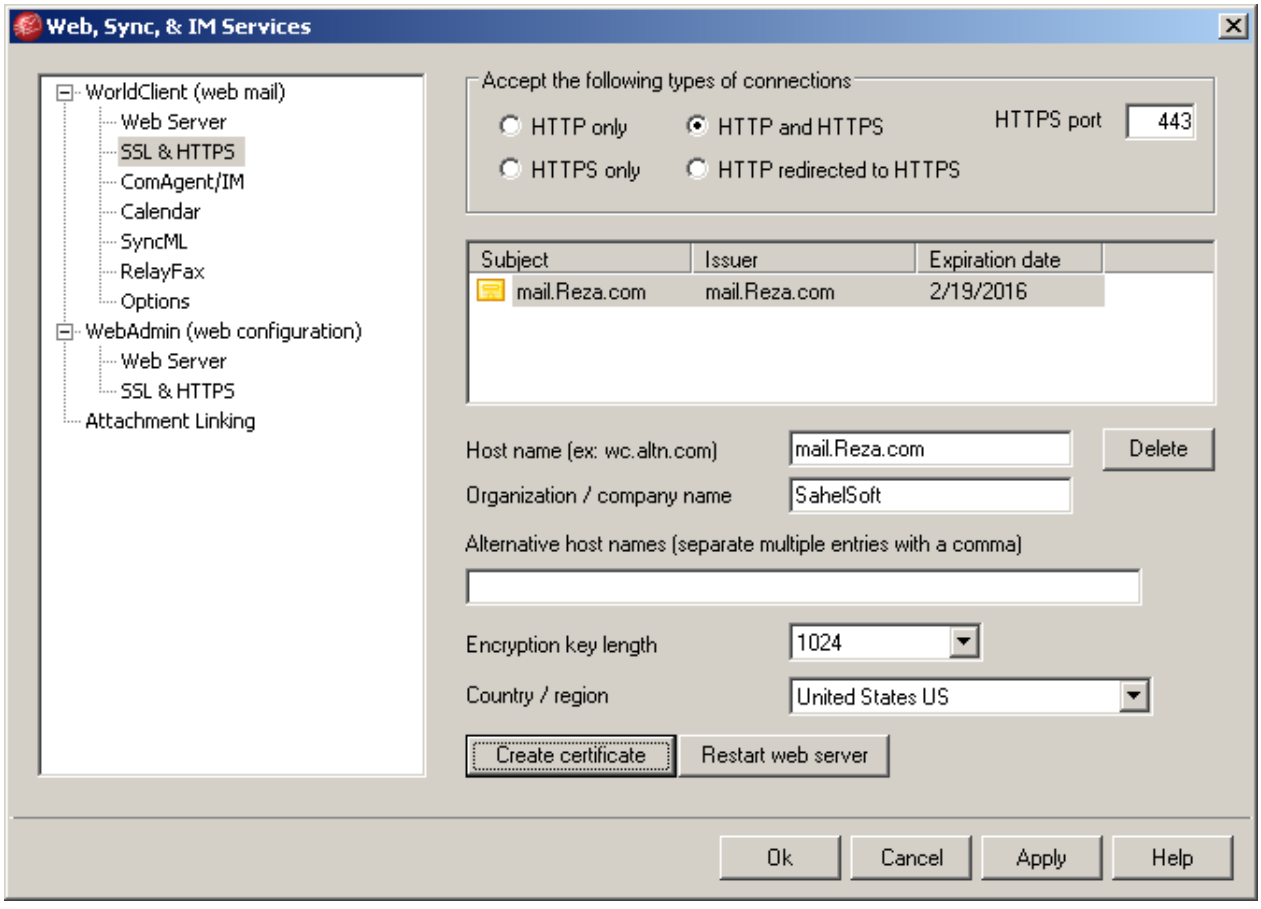
گزینه بعدی از منوی Setup، گزینه Web, Sync, & IM Service است که جهت تنظیمات وب و پروتکل‌های آن می‌باشد.



پس از انتخاب گزینه Web, Sync, & IM Service، صفحه زیر باز می‌شود. ابتدا وارد قسمت SSL & HTTPS شوید. از طریق این قسمت می‌توانید نوع پروتکل مورد استفاده در وب را تعیین نمایید. قابلیت استفاده از هر دو نوع پروتکل HTTP و HTTPS وجود دارد. همانطور که می‌دانید، HTTPS یک پروتکل امن است. به صورت پیش فرض، گزینه HTTP Only فعال است؛ بدین معنا که نرم‌افزار MDaemon Mail Server از پروتکل HTTP جهت کار با ایمیل از طریق وب استفاده می‌کند. این نرم‌افزار سرویس‌های خود را با پروتکل HTTP و با پورت شماره ۳۰۰۰ ارائه می‌کند.

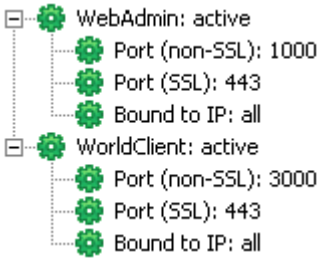


جهت استفاده از پروتکل HTTPS، گزینه HTTP and HTTPS را انتخاب کنید.



همانطور که در شکل بالا پیداست، پروتکل HTTPS از پورت شماره ۴۴۳ استفاده می‌کند. نکته مهم دیگر این است که پروتکل HTTPS به یک Certificate (گواهینامه – سند) جهت انجام کارهای امنیتی خود نیاز دارد. حال که شما پروتکل HTTPS را انتخاب نمودهاید، جهت ایجاد یک Certificate، روی دکمه Create Certificate کلیک کنید تا به لیست Certificate اضافه شود.

پس از تعیین پروتکل‌های وب، وارد صفحه اول نرم‌افزار شوید. بایستی در پایین و سمت چپ، شکلی مانند زیر ببینید. این شکل پروتکل‌های نصب شده که در وب قابل استفاده است را به همراه پورت‌های آن‌ها نشان می‌دهد.



۳۳-۴-۴- مدیریت حساب‌ها در MDaemon Mail Server

در این قسمت به آموزشی مختصری درباره چگونگی مدیریت حساب‌ها (ایمیل ها) در نرم‌افزار MDaemon Mail Server می‌پردازیم. مدیریت حساب‌ها از طریق منوی Accounts انجام می‌گیرد.

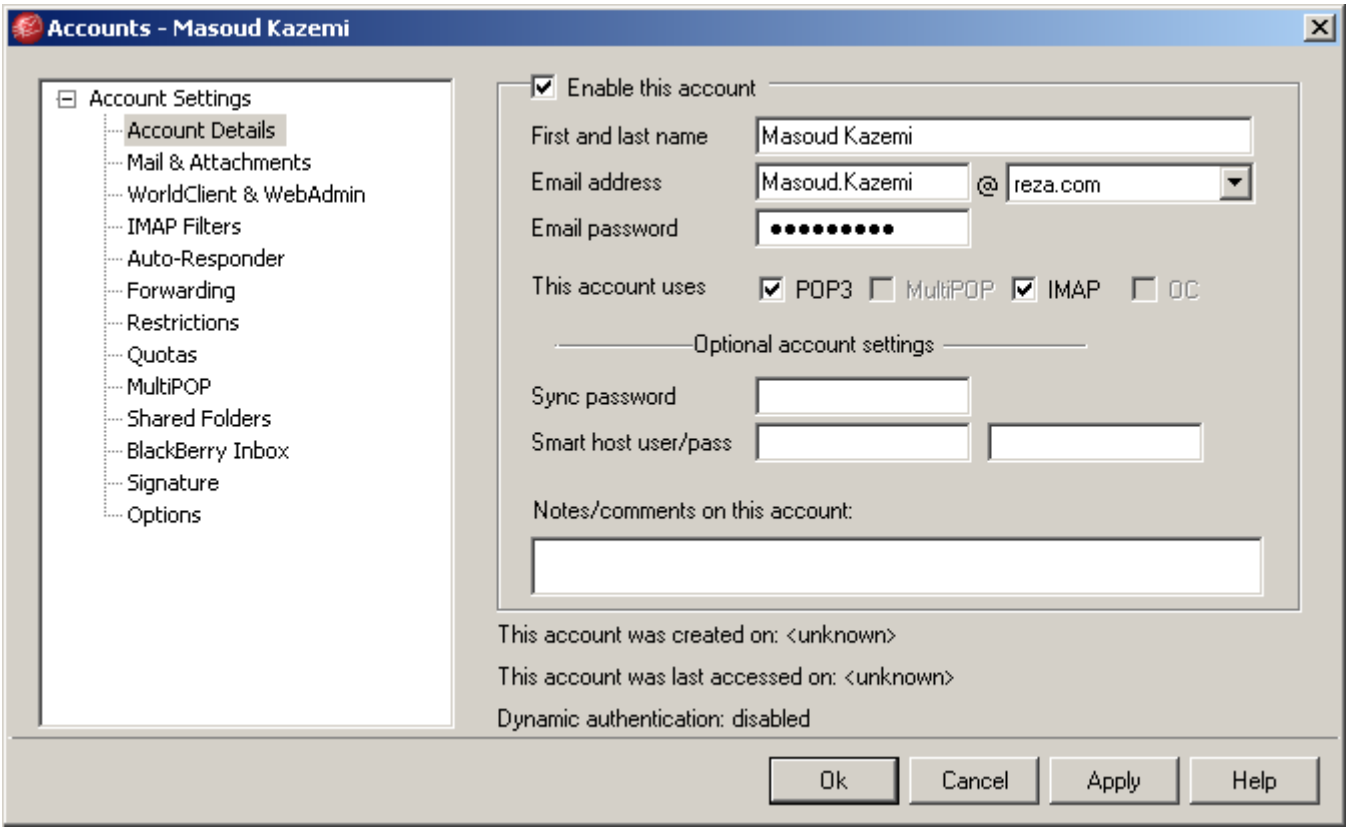
جهت ایجاد یک حساب جدید، از این منو، گزینه New Account را انتخاب نمایید.



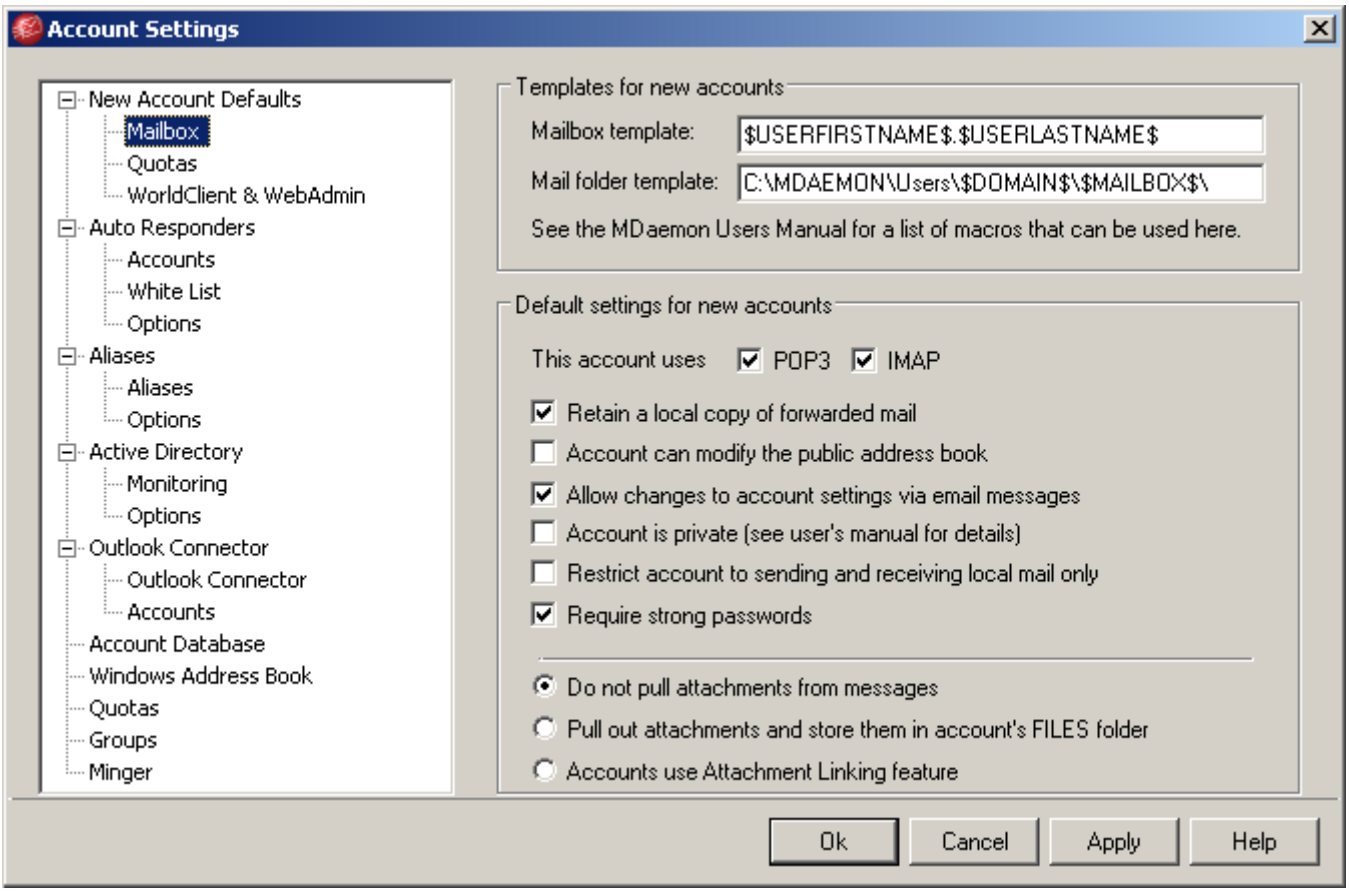
سپس اطلاعات ایمیل را وارد نمایید. بدین منظور ابتدا نام و نام خانوادگی صاحب ایمیل و سپس آدرس ایمیل را (بدون @ و نام دامنه) وارد نمایید. سپس رمز عبور ایمیل را وارد کنید. همانطور که قبلا نیز گفتم، به صورت پیش فرض، رمز عبور بایستی شامل حروف کوچک و بزرگ و عدد و نیز با طولی بین ۶ تا ۱۵ باشد. در این مثال، من رمز عبور را abc@ABC123 وارد نمودم.

در پایان نیز می‌توانید یک توضیحی در مورد ایمیل ساخته شده وارد نمایید.

در نهایت روی OK کلیک کنید.



بقیه کارهای مدیریتی حساب‌ها نیز از طریق همین منو انجام می‌گیرد. مثلا برای تنظیمات ایمیل‌ها، قسمت Account Settings را از منوی Accounts انتخاب کنید. مثلا از طریق صفحه فوق می‌توان پروتکل ایمیل را تنظیم نمود. همچنین اگر تیک گزینه Require strong passwords را بردارید، یعنی نیاز به استفاده از رمزهای عبور پیچیده برای حساب‌ها نمی‌باشد.



۳۳-۴-۵- استفاده از MDaemon Mail Server تحت وب

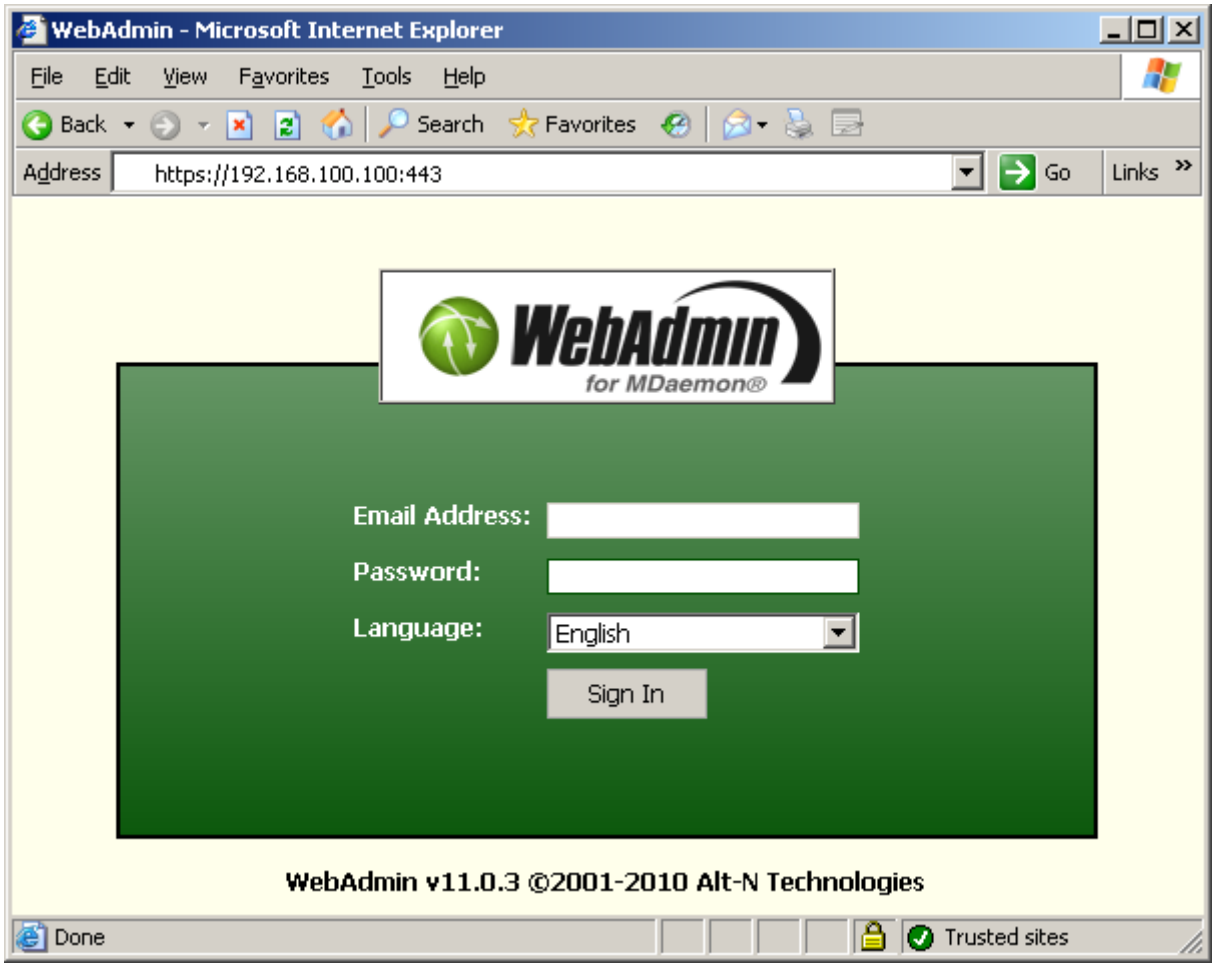
اگر قسمت تنظیمات WebClient را به درستی تنظیم کرده باشید، امکان استفاده از MDaemon Mail Server به صورت تحت وب و با مرورگرهای اینترنتی وجود خواهد داشت. بدین در مرورگر ابتدا پروتکل مورد استفاده وب، سپس آدرس IP سرور و سپس پورت مورد استفاده را وارد نمایید. در مثال زیر از پروتکل Http و از شماره پورت ۳۰۰۰ استفاده نموده‌ایم. آدرس IP سرور نیز ۱۹۲.۱۶۸.۱۰۰.۱۰۰ می‌باشد.

قسمت بالا برای ورود آدرس ایمیل و رمز عبور آن و قسمت پایین برای تعیین Style مورد نظر هنگام مشاهده ایمیل استفاده می‌شود.

پس از ورود اطلاعات، روی دکمه Sign In کلیک کنید.



اگر نیز قصد دارید از پروتکل HTTPS استفاده نمایید، به جای شماره پورت ۳۰۰۰، بایستی از شماره پورت ۴۴۳ استفاده نمایید.

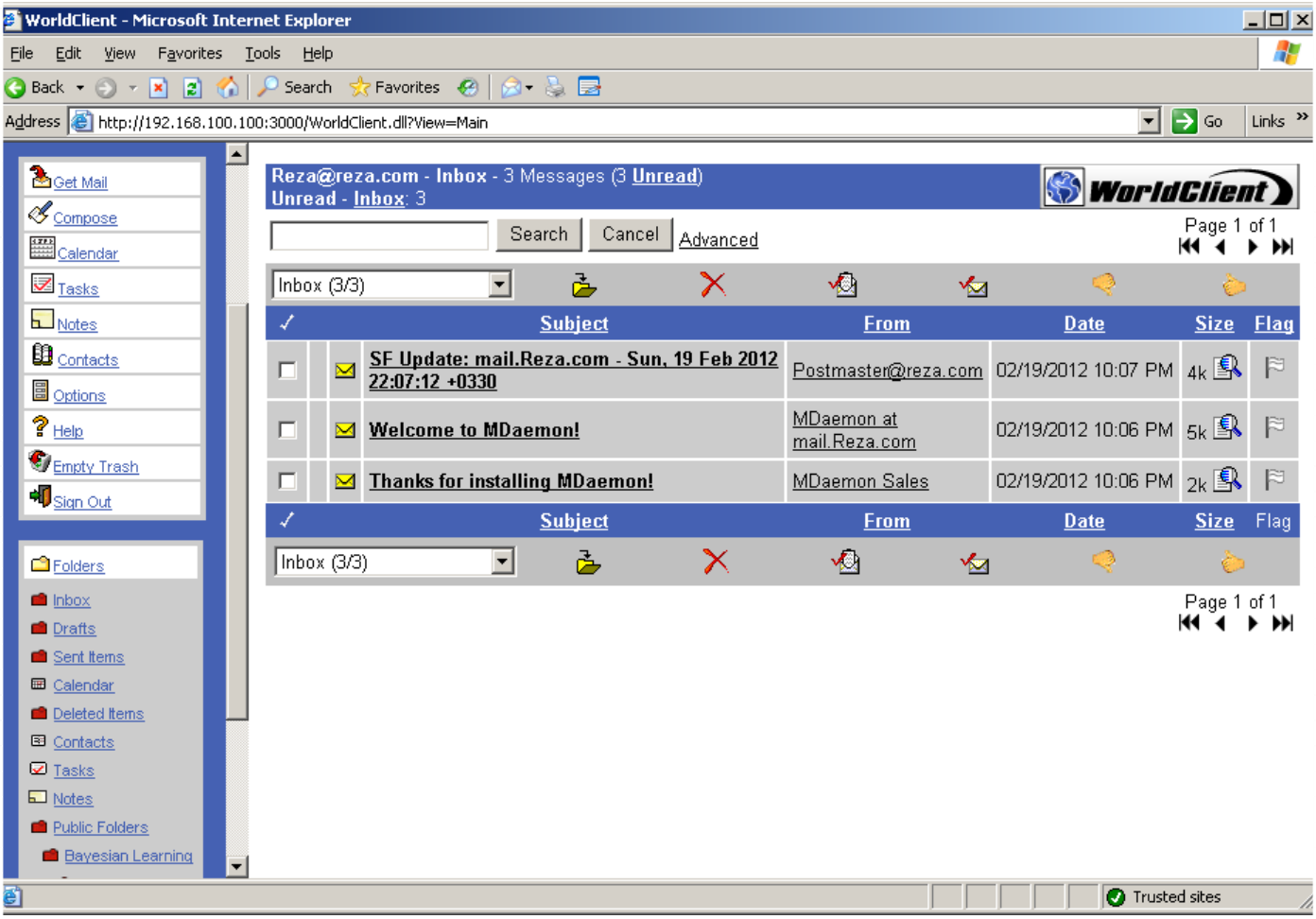


همچنین می‌توان به جای آدرس IP، نام سرور را وارد نمود. توجه نمایید که نام سرور با نام دامنه متفاوت است. در مثال ما نام دامنه Reza.Com و نام سرور PC-Server است.



پس از ورود، می‌توانید محیط کاری ایمیل خود را با توجه به Style انتخاب شده مشاهده نمایید.

مسلما صفحات کاری ایمیل برای شما بسیار آشناست و نیاز به توضیح ندارد. مثلا برای ارسال ایمیل، روی دکمه Compose کلیک کنید.



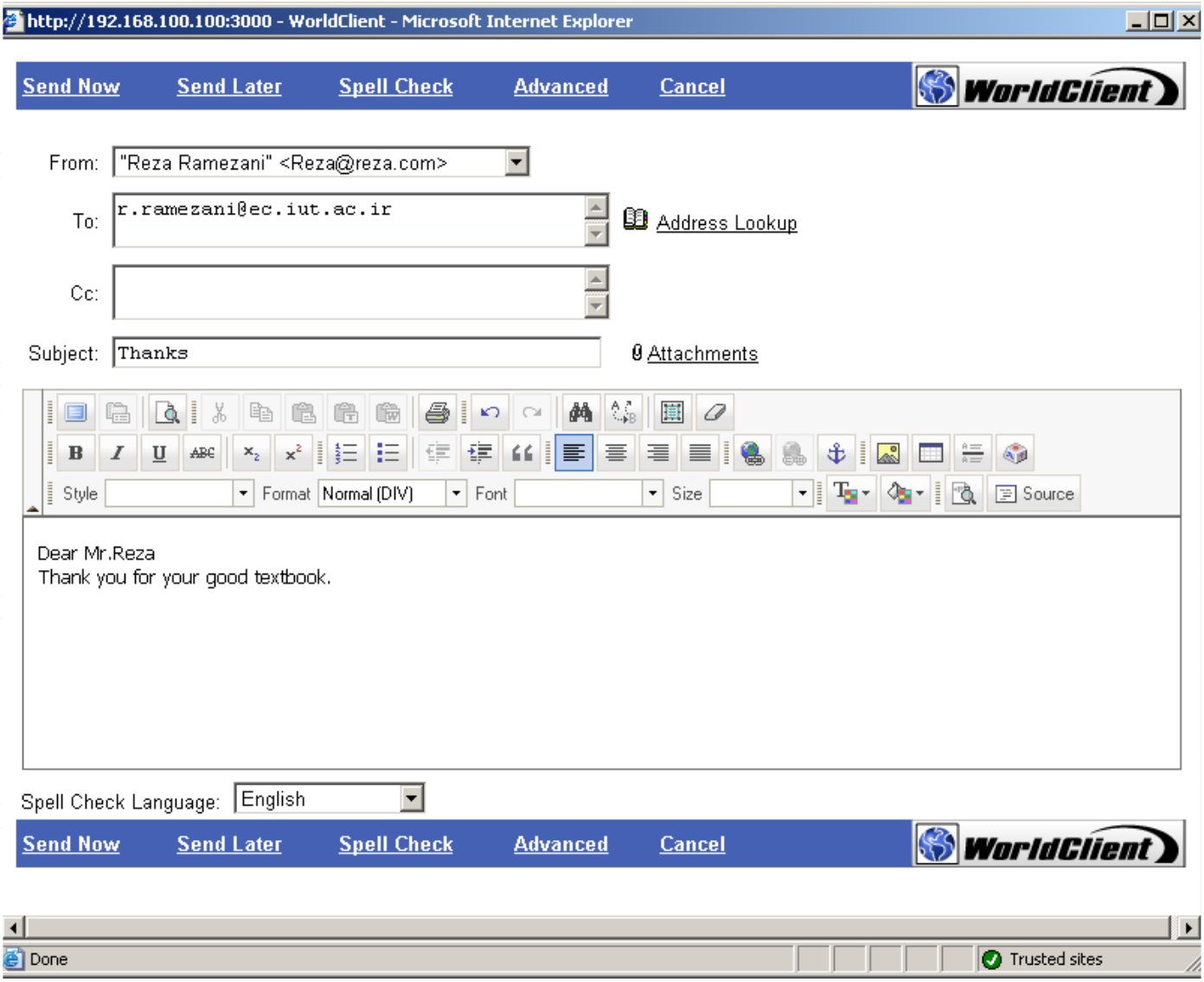
هنگام ارسال ایمیل، بایستی اطلاعاتی را در مورد ایمیل ارسالی و تحویل گیرنده / تحویل گیرندگان ایمیل وارد نمایید.

برخی از این اطلاعات عبارتند از:

- To: آدرس ایمیل گیرنده. اگر می‌خواهید ایمیل به چندین نفر ارسال شود، ایمیل‌ها را با ; از یکدیگر جدا کنید.
- CC: یک رو نوشت از ایمیل به شخصی که در CC مشخص نموده‌ایم نیز ارسال می‌شود و افراد حاضر در بخش To از این موضوع مطلع می‌شوند.
- BCC: یک رو نوشت از ایمیل به شخصی که در BCC مشخص نموده‌ایم نیز ارسال می‌شود اما افراد حاضر در بخش To و CC از این موضوع مطلع می‌شوند.
- Subject: موضوع ایمیل
- Attachment: فایل‌های ضمیمه شده
- Body: متن اصلی ایمیل

توجه: سرویس‌های ایمیل مختلف، امکانات مختلفی را ارئه می‌دهند.

در نهایت روی دکمه Send Now کلیک کنید.



توجه نمایید که این نرم‌افزار امکانات بسیار زیادی دارد. اما فکر می‌کنم این مطلب آموزش مختصر، نقطه مناسبی برای شروع باشد.

فصل ۳۴

FTP Server



به عنوان یک کاربر خانگی، ممکن است بارها برایتان پیش آمده باشد که بخواهید تعدادی از فایل‌های خود را در مدت زمانی نامحدود در دسترس دیگران قرار دهید؛ اما به دلایلی نمی‌خواهید که پوشه Share شده‌ای در سیستم تان وجود داشته باشد و یا شاید یک مدیر سیستم هستید که دفاتر متعددی در نقاط مختلف یک شهر یا یک کشور دارید و استفاده از فایل‌های مشترکی برای همه دفاتر الزامی به نظر می‌رسد اما حجم و محدودیت‌های شبکه امکان ارسال آن‌ها را با پست الکترونیکی فراهم نمی‌کند؛ اصلاً شما می‌خواهید این دسته از فایل‌ها همیشه در یک جای ثابت برای دریافت در دسترس باشند و دائم مجبور نباشید برای تک تک دفاتر آن‌ها را ارسال کنید. یک راه حل ساده، سریع و قدیمی برای این کار راه اندازی یک FTP Sever است. شما می‌توانید بر روی ویندوز XP Professional خانگی خود یا یکی از سرورهای محل کار به سادگی و در عرض چند دقیقه یک سرویس انتقال فایل راه اندازی کنید. پروتکل FTP یا File Transfer Protocol یکی از پروتکل‌های لایه کاربرد (Application) در معماری TCP/IP است که مسئولیت انتقال فایل‌ها را تحت شبکه بر عهده می‌گیرد، برنامه سرویس دهنده FTP از **پورت TCP شماره ۲۰ یا ۲۱** استفاده می‌کند که با استفاده از پروتکل TCP اقدام به انتقال فایل بین سیستم‌های مبتنی بر ویندوز و یک سرویس دهنده FTP ویندوزی می‌کند. با اینکه برخی از توانائی‌های این سرویس توسط سرویس وب (www) نیز ارائه می‌شود اما هنوز استفاده از سرویس FTP رواج دارد. به طور کلی به علت مسایل امنیتی سعی می‌شود که امکان ارسال فایل توسط همه کاربران غیر ممکن گردد و تنها عده خاصی با داشتن نام کاربری و رمز عبور قادر به ارسال فایل بر روی FTP Server باشند.

یک FTP Server می‌تواند سرویس دهنده‌ای بسیار کارآمد باشد، در عین اینکه عدم نظارت و کنترل آن ممکن است نقطه ضعفی برای سیستم به شمارایند.

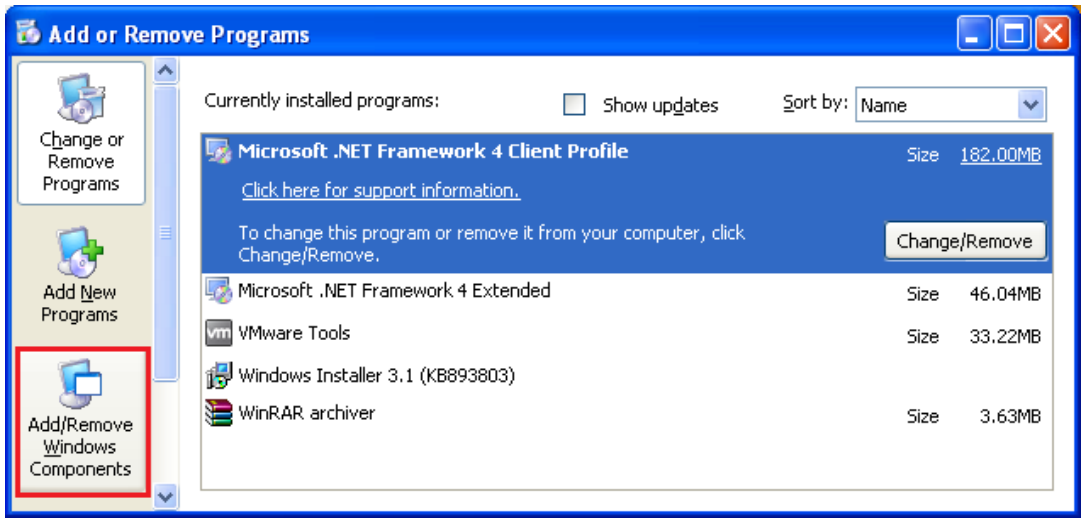
FTP با شماره پورت ۲۱، یک پروتکل قدیمی است و کاربرد آن به زمانی بر می‌گردد که استفاده از پورت ۸۰ (WEB) نیز چندان فراگیر نشده بود. زمانی می‌توان از یک کامپیوتر (با سیستم عامل XP، 2000 یا سرور ۲۰۰۳) خدمات FTP دریافت نمود که این سرویس روی آن سیستم عامل فعال شده باشد یعنی یک FTP Server روی سرور مورد نظر در حال کار باشد. بعد از برقراری ارتباط با FTP Server در حقیقت شما به یک FTP Client تبدیل می‌شوید.

بوسیله این پروتکل می‌توان فایل‌ها را در سرویس دهنده Upload نیز کرد اما برای قرار دادن فایل در طرف سرویس دهنده بایستی هر کاربر یک FTP Account داشته باشد که توسط ارائه دهنده سرویس در اختیار کاربر یا همان FTP Client قرار گرفته و به وسیله آن با توجه به حق دسترسی تعیین شده می‌توان به ایجاد، اضافه، حذف و یا تغییر فایل‌های موجود در سرویس دهنده از طریق یک دستگاه دیگر بپردازد. برای Upload کردن می‌توان از برنامه هایی مانند Cute FTP، Flash FXP، WS FTP و... استفاده نمود. اما در این فصل و جزوه آموزشی، قصد داریم از طریق راه اندازی FTP Server این کار را آموزش دهیم.

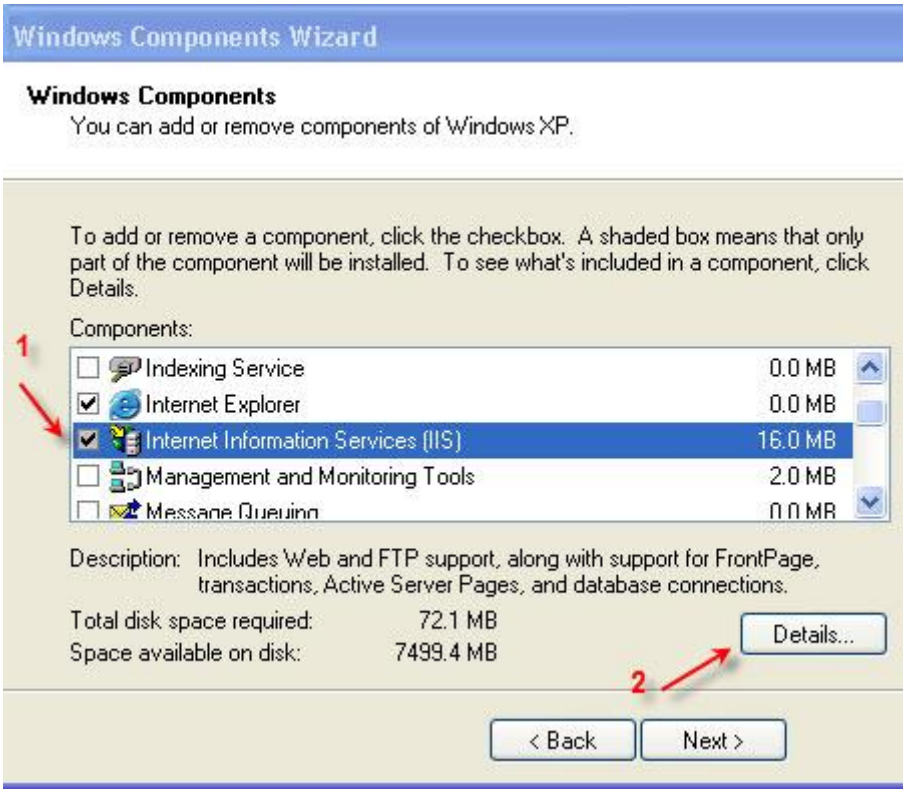
۳۴-۱- راه اندازی FTP Server

سرویس FTP یکی از سرویس‌های ارائه شده به همراه IIS (Internet Information Services) است که به طور پیش فرض در تمام سیستم عامل‌ها غیرفعال است پس بایستی آن را نصب و فعال کرد. برای این منظور در ویندوز XP مراحل زیر را طی کنید:

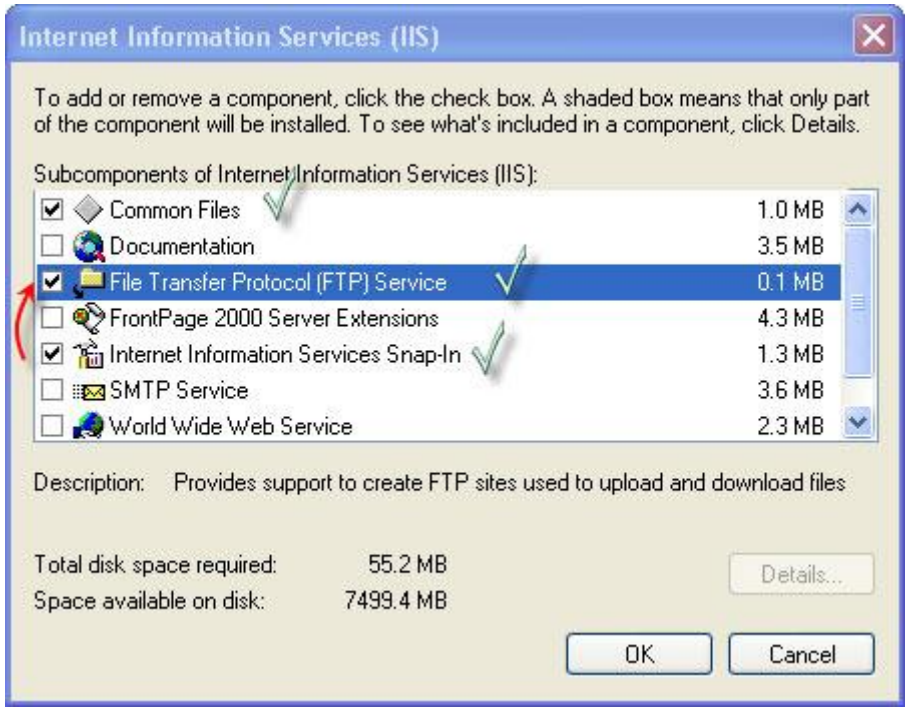
۱. Control Panel را باز و Add or Remove Program را انتخاب نمایید. در پنجره باز شده از قسمت سمت چپ، بر روی آیکون Add/Remove Windows ... را کلیک کنید.



۲. پس از چند لحظه انتظار پنجره مربوطه ظاهر می‌شود. در لیست Component، مانند شکل زیر در مربع کنار IIS تیک بزنید، بدون اینکه با زدن Next به مرحله بعد بروید، دکمه Details را انتخاب کنید.



۳. IIS شامل چندین سرویس است که یکی از آن‌ها FTP است و چون هدف ما تنها نصب FTP است پس در پنجره Details، در ابتدا تیک کنار همه گزینه‌ها را برداشته و فقط گزینه File Transfer Protocol (FTP) Service را انتخاب کنید، که طبق شکل زیر به همراه آن، دو سرویس دیگر نیز فعال می‌شود. تغییری در این تنظیمات ندهید؛ OK را بزنید و با بازگشت به صفحه قبل Next را انتخاب کنید.

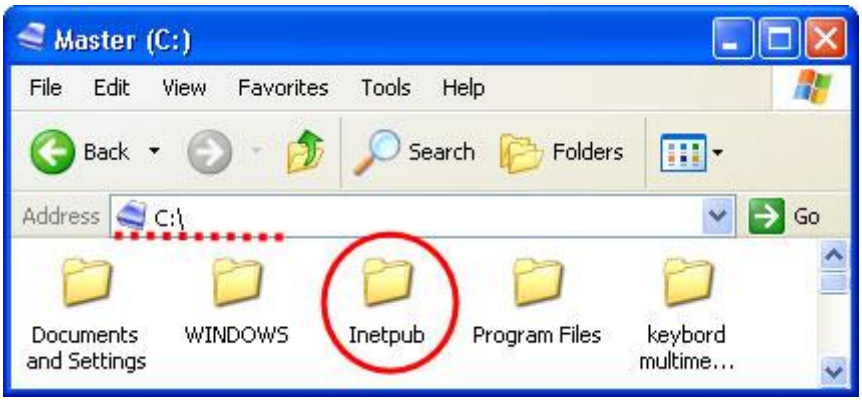


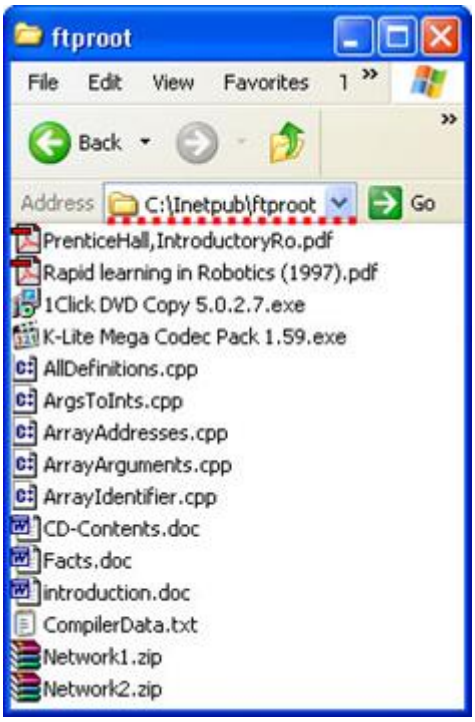
۴. در اینجا نصب سرویس شروع می‌شود. در اواسط روند نصب، از شما درخواست CD ویندوز می‌شود. پس از قراردادن CD و نصب فایل‌های مورد نیاز، سرویس FTP بر روی کامپیوتر فعال می‌گردد.

۳۴-۲- قراردادن فایل‌ها بر روی FTP Server

با طی شدن مراحل بالا اکنون سیستم به یک FTP Server تبدیل شده است. برای قراردادن فایل‌های مورد نظرتان، پوشه خاصی در نظر گرفته شده است که هر چیزی که در این پوشه قرار گیرد، سرویس دهنده آن را در لیست فایل‌ها و پوشه‌های FTP Server قرار می‌دهد.

همانطور که در دو شکل زیر مشاهده می‌کنید، به محض نصب FTP Server یک پوشه در درایو C کامپیوتر ایجاد می‌شود که Inetpub نام دارد. درون این پوشه نیز دو پوشه دیگر به نام‌های ftproot و AdminScripts قرار دارد، پوشه مورد بحث ما که محل قرارگیری فایل‌های FTP Server است ftproot است. حالا همه چیز آماده قرارگیری فایل‌ها است. فایل هایتان را در این مکان قرار دهید، هم اکنون شما یک FTP Server آماده استفاده دارید.





۳۴-۳- اتصال به FTP Server

مسلما یک FTP Client ابتدا باید به FTP Server متصل گردد تا بتواند از خدمات آن استفاده کند در یک شبکه داخلی این امر با تایپ یکی از دو نوع آدرس زیر در نوار آدرس IE یا هر Web Browser دیگری مثل Mozilla میسر

می‌شود و کاربران شبکه با داشتن IP Address یا نام کامپیوتر سرویس دهنده FTP، می‌توانند لیست فایل‌های موجود در آن را مشاهده و سپس نسبت به دریافت اقدام کنند.

ftp://FTP Server **Computer Name** یا ftp://FTP Server **IP address**

اما کاربرانی وجود دارند که می‌خواهند از این سرویس توسط نوع دیگری از ارتباط استفاده کنند بدین معنی که هدف آن‌ها از راه اندازی این سرویس در دسترس قرار دادن فایل هایی برای افراد خاصی است که با اجازه آن‌ها قادر به اتصال به سیستم باشند. نحوه ساختن این نوع ارتباط بدون نیاز به اینترنت و توسط مودم صورت می‌گیرد که به طور کامل در فصول قبل توضیح داده شده است؛ لذا از تکرار آن خودداری می‌کنیم.

طبق شکل زیر، ما لیستی از فایل‌ها را در پوشه ftproot قرار دادیم. فرض کنید آدرس IP ما، برابر با ۱۶۹.۲۵۴.۱۹۵.۱۵۷ باشد.

FTP Client مورد نظر مانند شکل زیر، این آدرس IP را در نوار آدرس مرورگر Mozilla وارد و سپس همان لیست را که در شکل فوق وجود داشت به صورت لینک‌های قابل Download می‌بیند. به همین راحتی!! کار ما تمام شد. از این به بعد شما تنها به ویرایش لیست تان می‌پردازید و دیگر لازم نیست پوشه‌ای را Share کنید و یا فایل‌ها را با درد سر Email کنید.

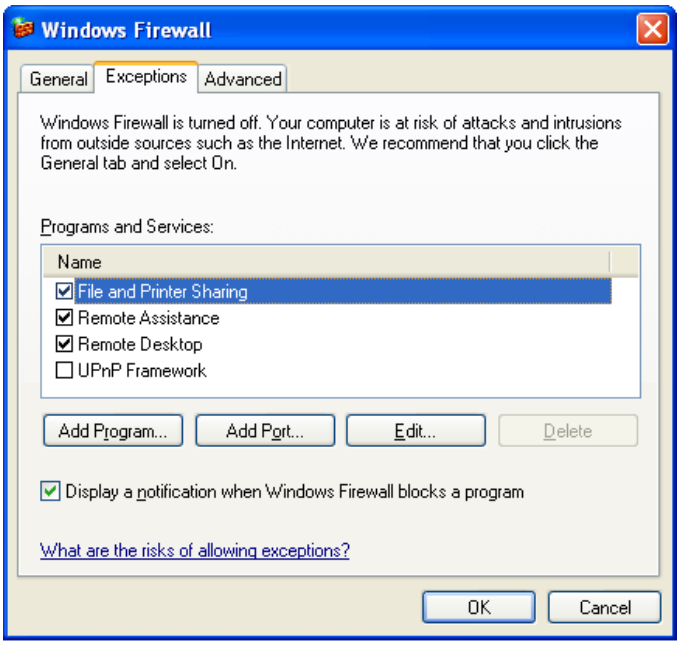


سرعت بالاتر و نظم موجود در این سرویس از مزایای آن به شمار می‌رود. نکته قابل توجه دیگر اینکه، با وجود یک نرم‌افزار مدیریت Download مثل IDM یا DAP می‌توان فایل‌های حجیم را هم با سرعت بالاتری منتقل کرد.

با هر نوع Connection که به سرور متصل شده باشید چه از طریق شبکه داخلی یا اینترنت و یا روشی که ما به شما ارائه کردیم امکانات FTP در اختیار شماست.

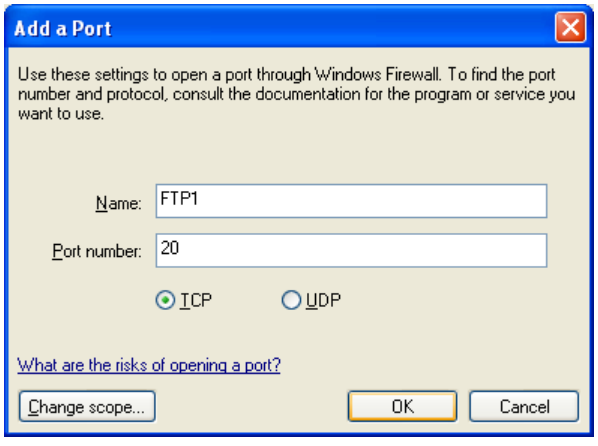
۳۴-۴- تنظیم Firewall

این مسأله را فراموش نکنید که در صورتیکه فایروال سیستم شما فعال باشد نمی‌توان به سرویس دهنده FTP شما متصل شد، پس بایستی آن را غیرفعال کنید. البته می‌توان این مشکل را با غیر فعال نکردن Firewall نیز حل کرد. راه حل این است که پورت‌های ۲۰ و ۲۱ را به Firewall خود معرفی کنید (همان دو پورتی که FTP Server برای خواندن و نوشتن از آن استفاده می‌کند). بدین منظور، ابتدا وارد Control Panel ➔ Windows Firewall شده و سپس وارد سربرگ Exceptions شوید.

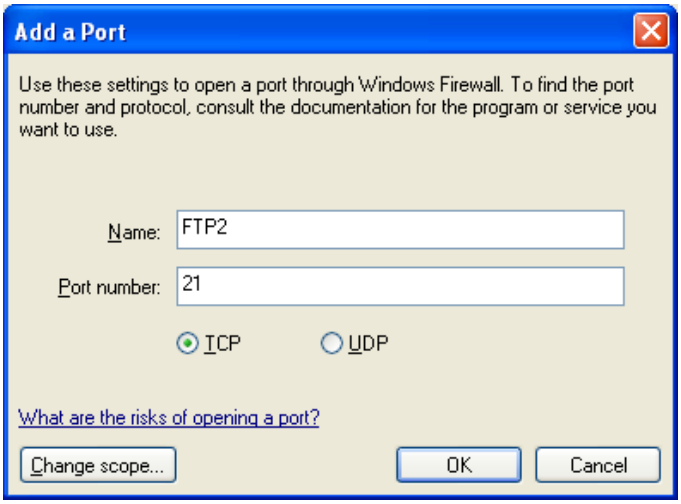


سپس روی دکمه Add Port کلیک کنید.

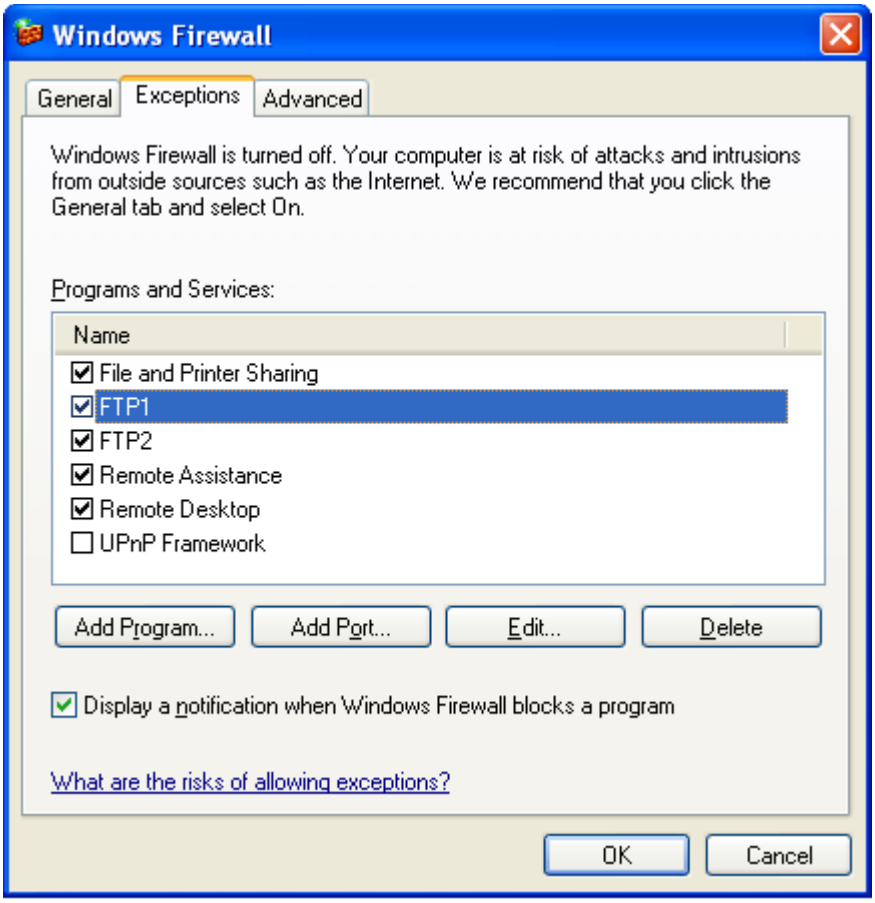
سپس در صفحه باز شده، پورت ۲۰ را با نام FTP1 اضافه کنید.



مجددا روی Add Port کلیک کنید. اینبار پورت ۲۱ را با نام FTP2 اضافه کنید.



با OK کردن، این دو پورت، به مجموعه پورت‌های ویندوز که Firewall جلوی آن‌ها را نمی‌گیرد، اضافه خواهد شد.



جهت استفاده از FTPهای فراهم شده، توصیه می‌کنم از نرم‌افزارهای CuteFTP یا FileZilla استفاده نمایید.

فصل ۳۵

Microsoft Management Console یا MMC

۳۵-۱- مفهوم Microsoft Management Console

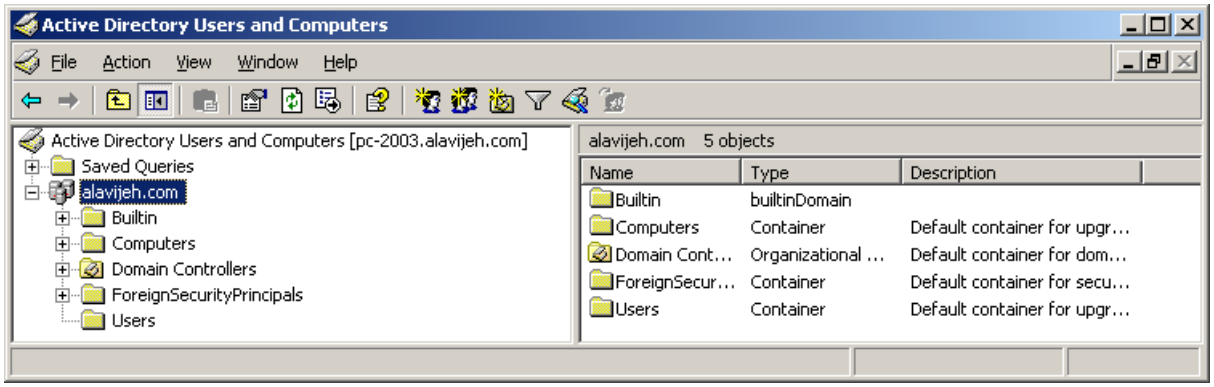
شاید برای شما هم اتفاق افتاده باشد که مجبور شده باشید کارهایی متعدد و تکراری را هر روز با کامپیوتر انجام دهید. در این وضعیت ما ۳ حالت را بررسی می‌کنیم. اولا برای شما خوشایند خواهد بود که به سرعت به نرم‌افزارهای مربوط به این کارها به سرعت دسترسی پیدا کنید. ثانیا اگر طراحی نرم‌افزارها به گونه‌ای باشد که ظاهری شبیه یکدیگر داشته و همگی از یک استاندارد طراحی پیروی کنند، این امر باعث خواهد شد که با دیگر نرم‌افزارها بتوانید به سادگی کار کنید. به عنوان مثال وقتی در ویندوز، با دو بار کلیک روی یک پوشه می‌توانید آن را باز کنید، انجام این کار در لینوکس نیز برای شما راحت خواهد بود. اما اگر تاکنون فقط با سیستم عامل Dos کار کرده باشید و بخواهید مستقیماً به سراغ محیط گرافیکی لینوکس بروید، احتمالا دچار مشکل خواهید شد. ثالثا، ممکن است شما به عنوان مدیر شبکه، نیاز داشته باشید که هر روز **قسمت‌های مدیریتی** برخی یا تمام کامپیوترهای موجود در شبکه را کنترل نمایید. برای این کار مجبورید که شخصا پشت هر کامپیوتر بروید و آن قسمت مدیریتی را بررسی نمایید. اما چقدر خوب می‌شود که بتوان از راه دور، قسمت‌های مدیریتی تمام سیستم‌ها را کنترل نمود. ممکن است بگویید که می‌توان این مشکل آخر را با نرم‌افزار Remote Desktop حل کرد. اما این روش دو عیب دارد: اول اینکه Remote Desktop تمام اطلاعات کامپیوتر راه دور را به کامپیوتر شما می‌آورد؛ لذا ترافیک شبکه بسیار بالا می‌رود؛ درحالی که ما به تمام قسمت‌های کامپیوتر راه دور نیازی نداریم و تنها به **قسمت‌های مدیریتی** آن نیاز

داریم. عیب دوم اینکه برای کار با Remote Desktop نیاز به نام کاربری و رمز عبور کامپیوتر راه دور داریم؛ و این امر نیز خود مشکلی بزرگ است.

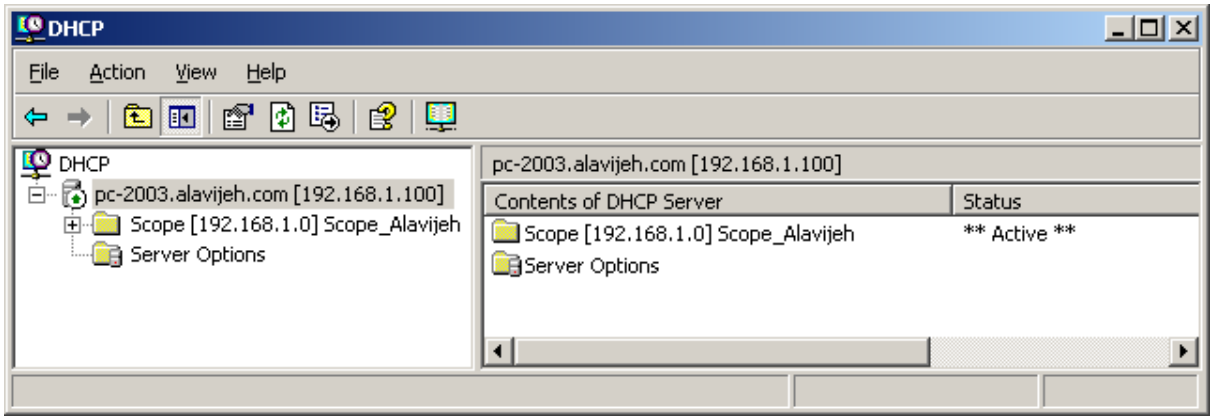
توجه نمایید که در این بخش هدف ما، اتصال به **قسمت‌های مدیریتی** کامپیوتر است نه فایل‌ها و پوشه‌های کامپیوتر. منظور از قسمت‌های مدیریتی، بخش هایی چون AD Users & Computers، DHCP، DNS، Computer Management و... است.

برای حل این مشکلات، مایکروسافت تکنیکی را تحت عنوان Microsoft Management Console یا به اختصار MMC را معرفی کرده است. MMC برای حل این مشکلات، اقدامات زیر را انجام می‌دهد: اولا می‌توان چندین قسمت مدیریتی را در کنار یکدیگر قرار داد و به راحتی در یک لحظه به همه آن‌ها دسترسی داشت. ثانیا، مایکروسافت شکل یکسانی را برای تمامی **قسمت‌های مدیریتی** طراحی کرده است. لذا کار کردن با آن‌ها راحت است. ثالثا توسط MMC این قابلیت وجود دارد که بتوان به کامپیوترهای راه دور بدون نیاز به نام کاربری و رمز عبور متصل شد و **قسمت‌های مدیریتی** را تغییر داد. برای اینکه، بهتر متوجه بحث فوق شوید، به تصاویر زیر دقت نمایید:

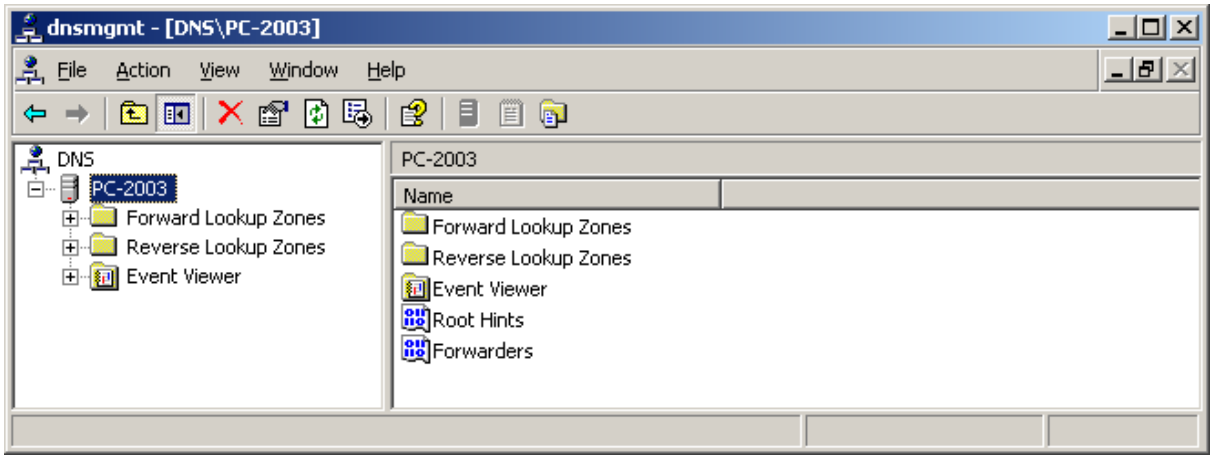
شکل زیر، کنسول مدیریتی Active Directory Users and Computers را نشان می‌دهد:



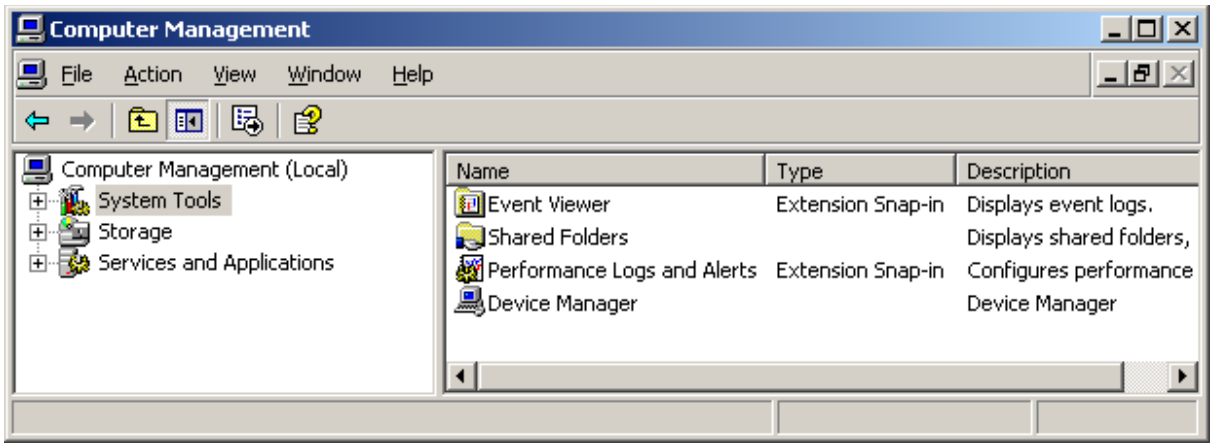
شکل زیر، کنسول مدیریتی DHCP را نشان می‌دهد:



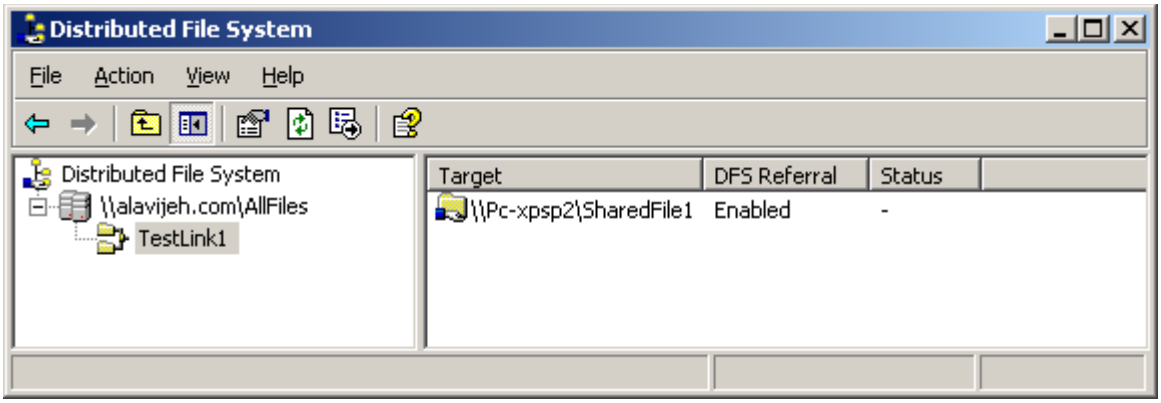
شکل زیر، کنسول مدیریتی DNS را نشان می‌دهد:



شکل زیر، کنسول مدیریتی Computer Management را نشان می‌دهد:



شکل زیر، کنسول مدیریتی Distributed File System را نشان می‌دهد:

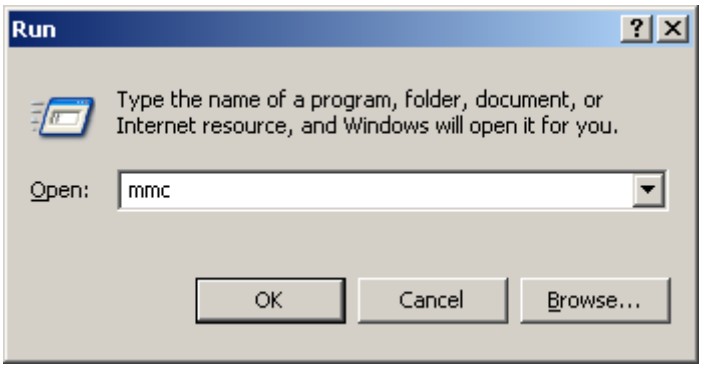


اگر دقیقا به شکل‌های فوق دقت کرده باشید، متوجه خواهید شد که ساختار و ظاهر طراحی آن‌ها به یک شکل است. بدین صورت که در سمت چپ یک ساختار سلسله مراتبی و درختی از عناصر طراحی و مدیریتی وجود دارد. با انتخاب هر کدام، زیر مجموعه‌های آن در سمت راست نمایان شده و می‌توان آن‌ها را تغییر داد. مایکروسافت تلاش نموده است که تمام کنسول‌های مدیریتی آن از این روش طراحی استفاده کنند؛ لذا با این عمل، مشکل دومی که در بالا مطرح کردیم حل می‌شود. حال نوبت به مشکل اول و سوم می‌شود.

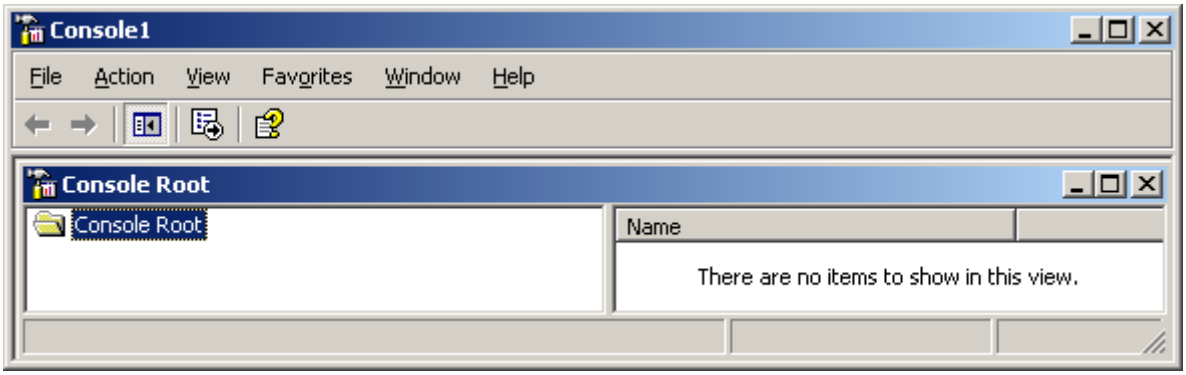
۳۵-۲- کار با MMC

برای حل اولین مشکل، مایکروسافت این راه حل را در نظر گرفته است: می‌توان یک Console جدید تعریف نمود و سپس تمامی کنسول‌های مدیریتی مورد نظر را به آن اضافه نمود. حال با باز کردن این Console، تمامی کنسول‌های مدیریتی خود را به صورت مجتمع و یکجا مشاهده خواهید نمود.

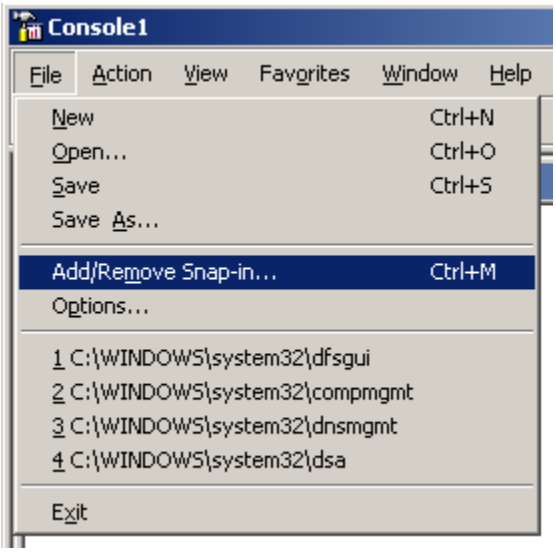
برای ساخت یک Console جدید، ابتدا وارد Run شده و سپس دستور mmc را وارد نمایید.



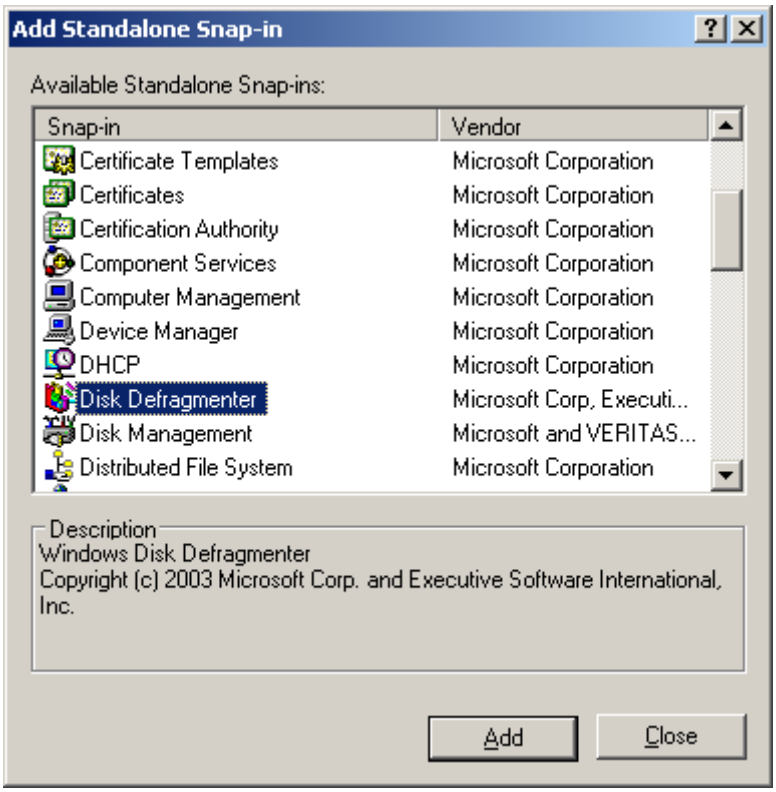
با این کار، یک Console جدید باز می‌شود.



حال نوبت به اضافه کردن کنسول‌های مدیریتی خود به این Console می‌شود (مانند DHCP و DNS). بدین منظور از منوی File، گزینه Add/Remove Snap-in را انتخاب کنید.

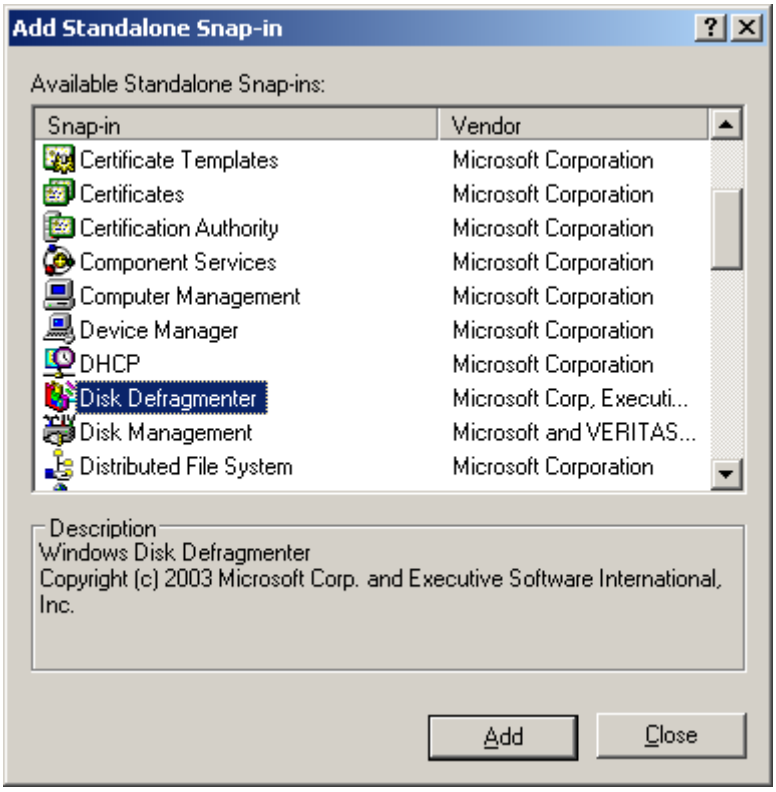


سپس در صفحه باز شده، کنسول‌های مدیریتی خود را انتخاب کرده و روی دکمه Add کلیک کنید.

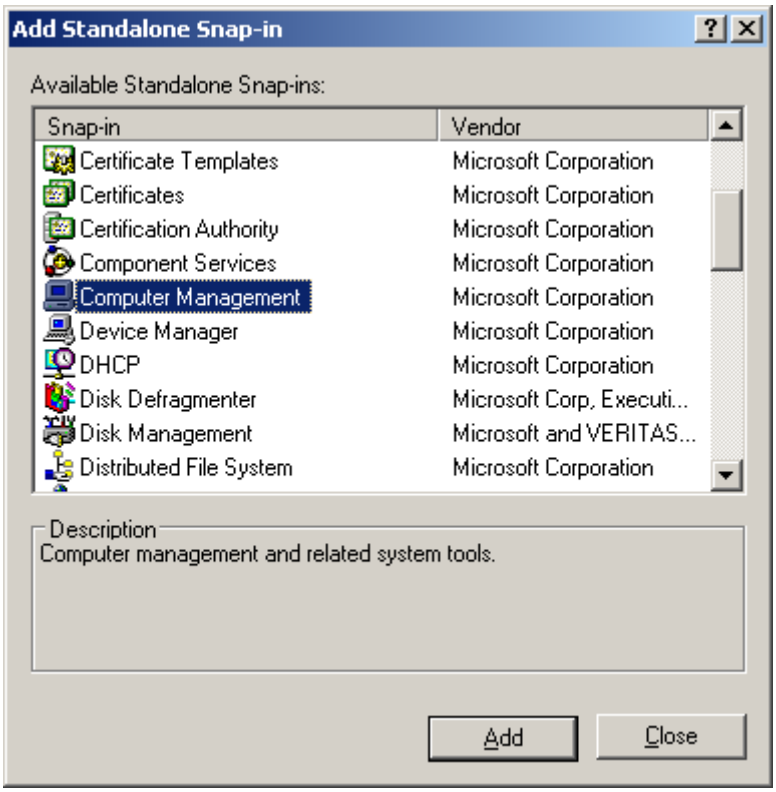


تا اینجا، ما برای مشکل اول و دوم راه حلی پیدا کرده‌ایم. اما مشکل سوم، یعنی کنسول‌های مدیریتی کامپیوترهای راه دور هنوز به قوت خود باقی است. برای حل این مشکل نیز از این روش استفاده می‌شود: هنگام انتخاب کرده یک کنسول مدیریتی، سیستم از ما سوال می‌پرسد که آیا می‌خواهید این کنسول مدیریتی، تنظیمات همین کامپیوتر را نشان دهد یا اینکه اطلاعات یک کامپیوتر راه دور را به نمایش در آورد؟ با انتخاب یک کامپیوتر راه دور، مشکل سوم نیز برطرف می‌شود. توجه نمایید که برای کنترل مدیریتی یک کامپیوتر راه دور، نیازی به نام کاربری و رمز عبور نیست. البته توجه داشته باشید که نمی‌توان به همه کنسول‌های مدیریتی راه دور دسترسی داشت و هنگام انتخاب آن‌های که قابلیت مدیریت از راه دور ندارند، سیستم از ما سوال نمی‌پرسد که آیا می‌خواهید این کنسول مدیریتی محلی باشد یا راه دور؟ و خودش آن را به صورت محلی انتخاب می‌کند.

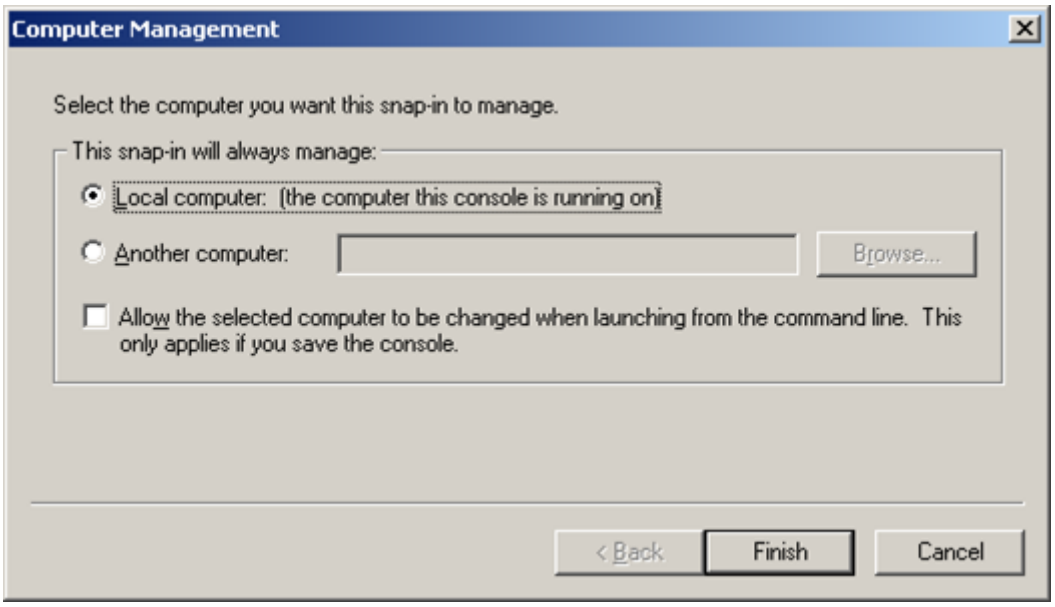
فرض کنید که می‌خواهیم کنسول مدیریتی Disk Defragment را اضافه کنیم؛ بدین منظور آن را انتخاب کرده و روی Add کلیک کنید. کنسول مدیریتی Disk Defragment، فقط قابلیت مدیریت به صورت محلی را دارد. لذا سیستم از ما سوالی در مورد محلی یا راه دور بودن آن نمی‌پرسد.



حال فرض کنید که می‌خواهیم کنسول مدیریتی Computer Management را اضافه کنیم. این کنسول مدیریتی قابلیت اتصال به صورت محلی و راه دور را دارد. لذا هنگام Add کردن آن، سیستم سوالی در مورد محلی یا راه دور بودن آن خواهد پرسید.



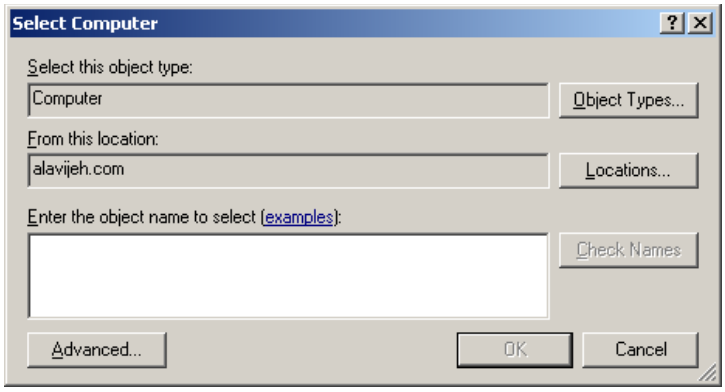
اگر می‌خواهید که این کنسول مدیریتی، فقط کامپیوتر خود شما را کنترل کند، گزینه Local computer را انتخاب کرده و سپس روی Finish کلیک کنید.



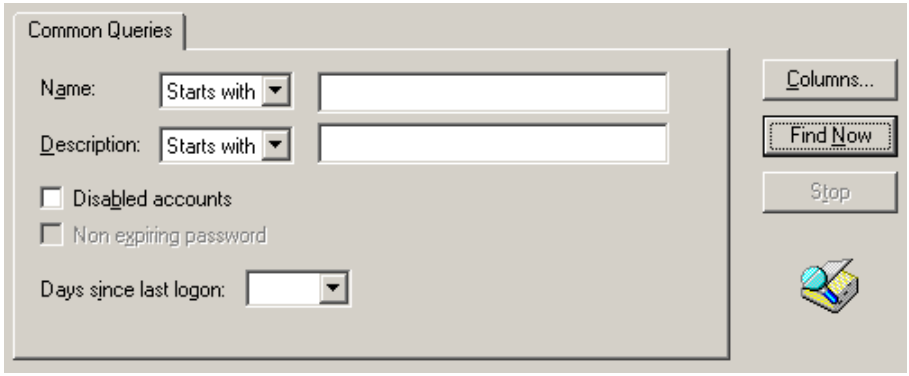
اما اگر می‌خواهید به کنسول مدیریتی کامپیوتر راه دور متصل شوید، گزینه Another computer را انتخاب کنید. حال دو راه پیش رو دارید. اول اینکه آدرس کامپیوتر را به صورت متنی در جعبه متن زیر وارد نمایید. دوم اینکه کامپیوتر راه دور را به صورت Visual انتخاب کنید. بدین منظور روی دکمه Browse کلیک کنید.



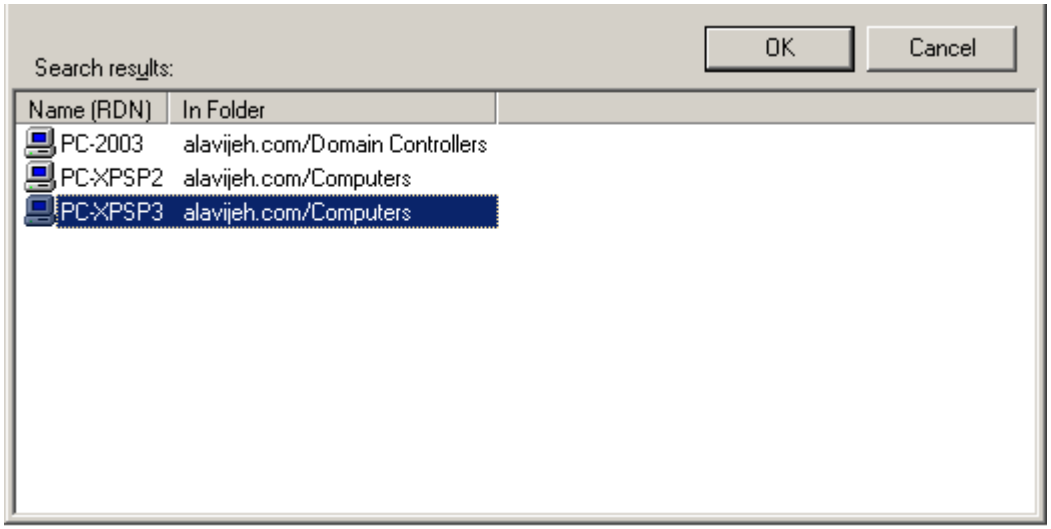
در صفحه باز شده، روی دکمه Advanced کلیک کنید.



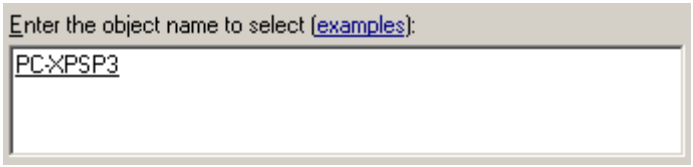
سپس در صفحه باز شده، برای پیدا کردن کامپیوترهای موجود در شبکه، روی دکمه Find Now کلیک کنید.



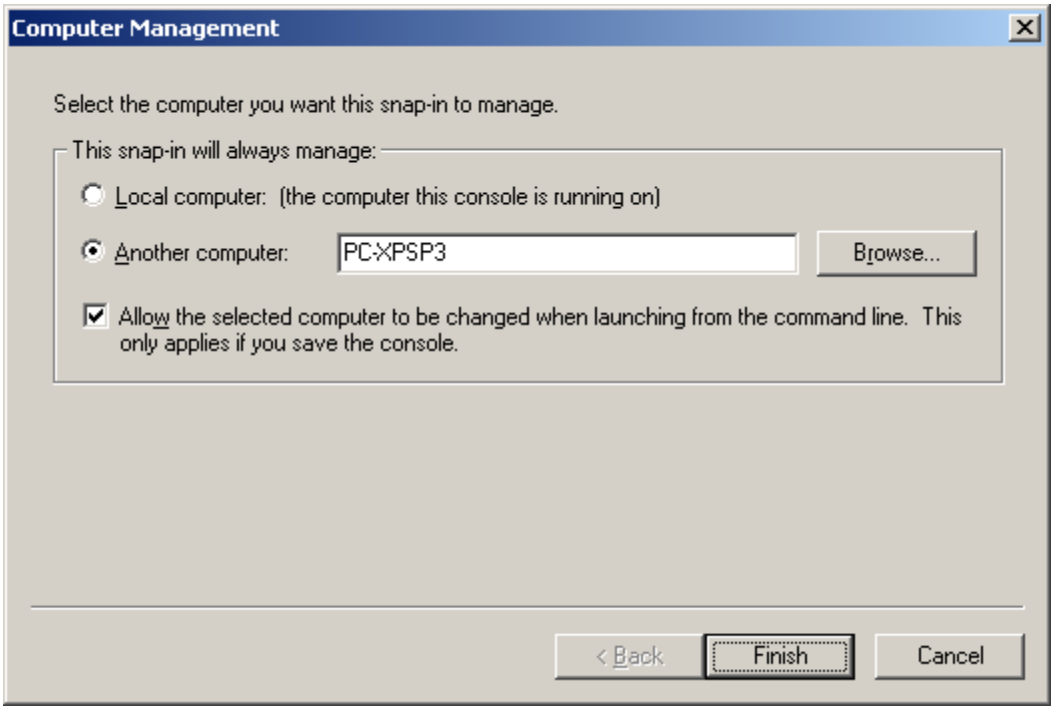
سپس کامپیوتر راه دور مورد نظر را انتخاب کرده و روی OK کلیک کنید.



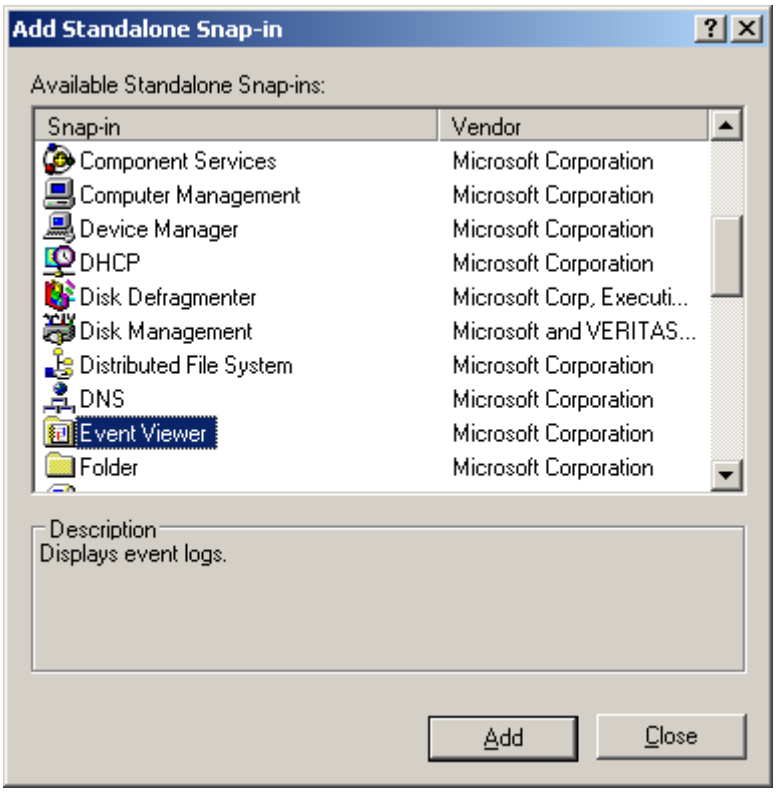
با این کار بایستی نام کامل (FQDN) کامپیوتر راه دور را مشاهده نمایید.



با انتخاب کامپیوتر راه دور، بایستی شکلی مانند زیر نمایان شود. حال روی Finish کلیک کنید.



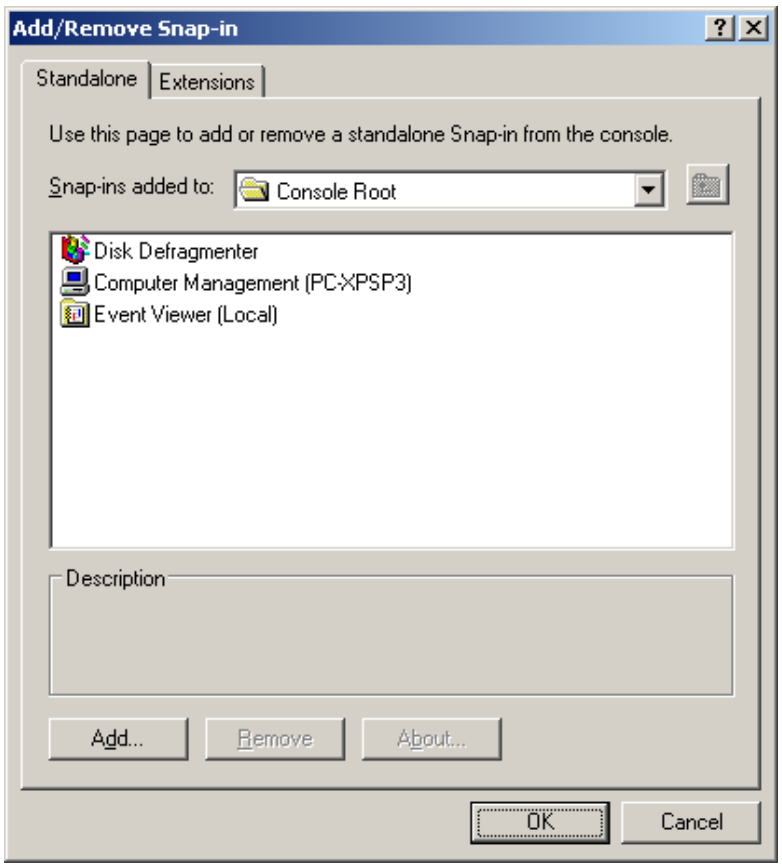
به عنوان کنسول مدیریتی آخر، فرض کنید که قصد داریم کنسول Event Viewer کامپیوتر خود را (نه کامپیوتر راه دور را) به کنسول‌های خود اضافه کنیم. بدین منظور، پس از انتخاب Event Viewer، روی دکمه Add کلیک کنید.



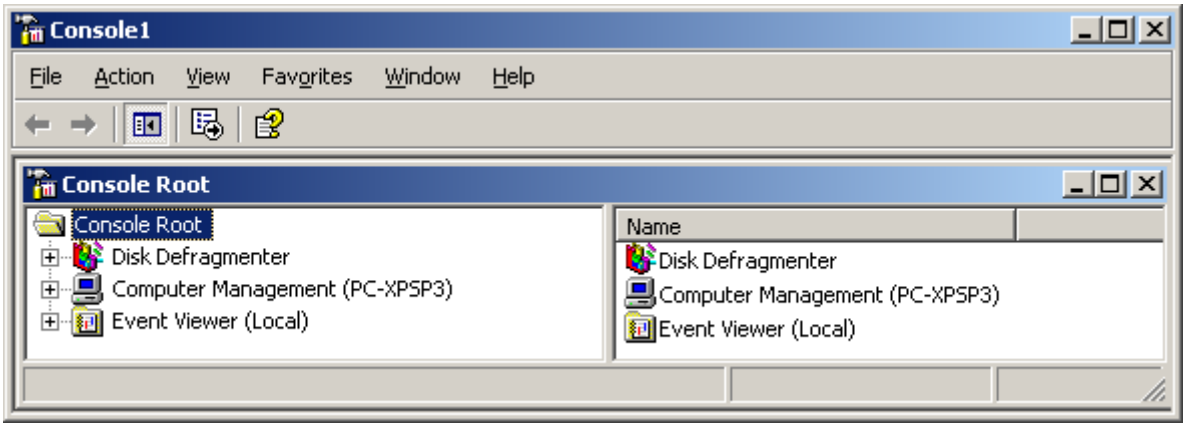
سپس در صفحه باز شده، گزینه Local computer را انتخاب کرده و روی Finish کلیک کنید.



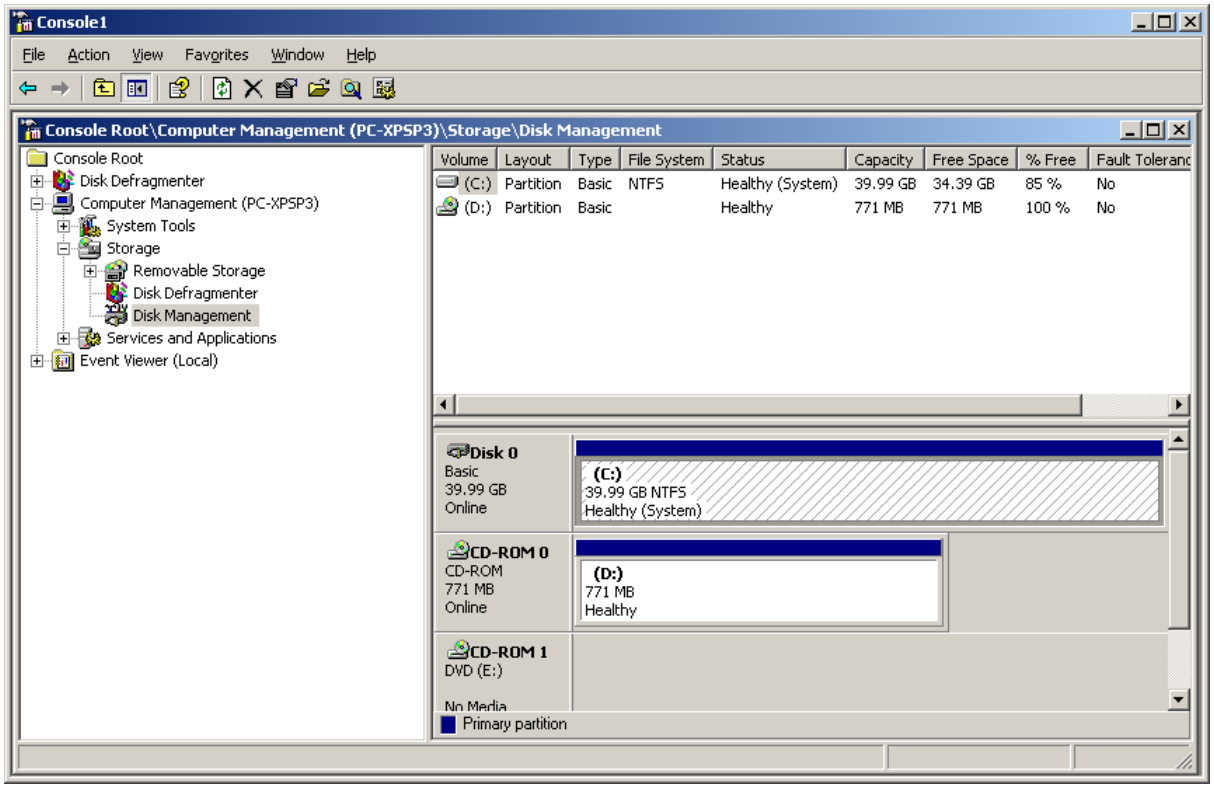
در نهایت روی Close کلیک کنید. بدین ترتیب هر ۳ کنسول مدیریتی انتخاب شده را مشاهده خواهید نمود.



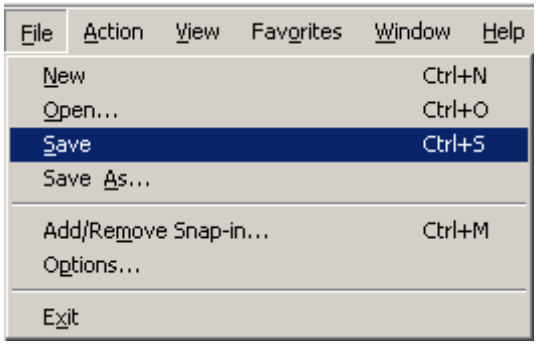
در نهایت روی OK کلیک کنید. بدین ترتیب هر ۳ کنسول مدیریتی شما، در یک کنسول واحد به نمایش در خواهد آمد.



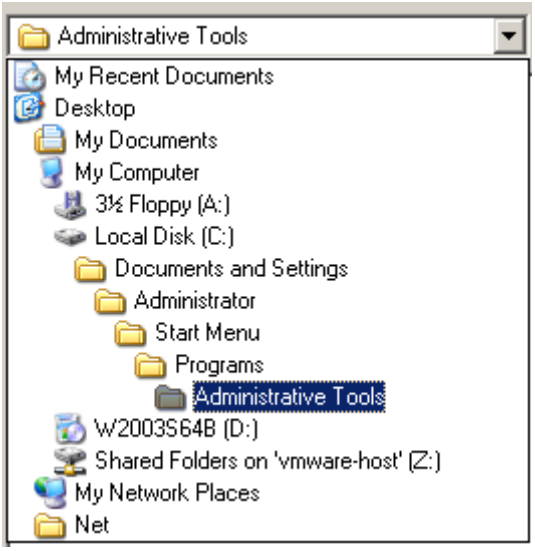
حال برای مدیریت هر کدام از کنسول‌ها، تنها کافیست آن را انتخاب نمایید. در این مثال، ما کنسول مدیریتی Computer Management که به صورت راه دور است را تنظیم خواهیم نمود تا بدین وسیله متوجه شوید که برای تنظیم یک کنسول مدیریتی راه دور نیازی به نام کاربری و رمز عبور نمی‌باشد.



حال بایستی این کنسول مدیریتی ساخته شده جدید را ذخیره نمایید تا دیگر نیازی به انجام موارد فوق نداشته باشید. بدین منظور از منوی File گزینه Save را انتخاب نمایید.



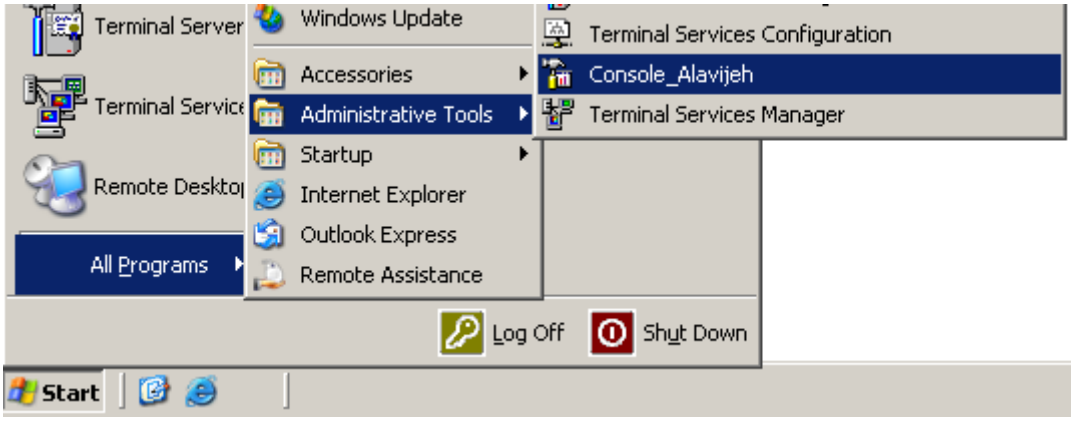
سپس آن را در همان مسیر پیش فرض، یعنی در پوشه Administrative Tools ذخیره کنید. به شکل زیر دقت نمایید.



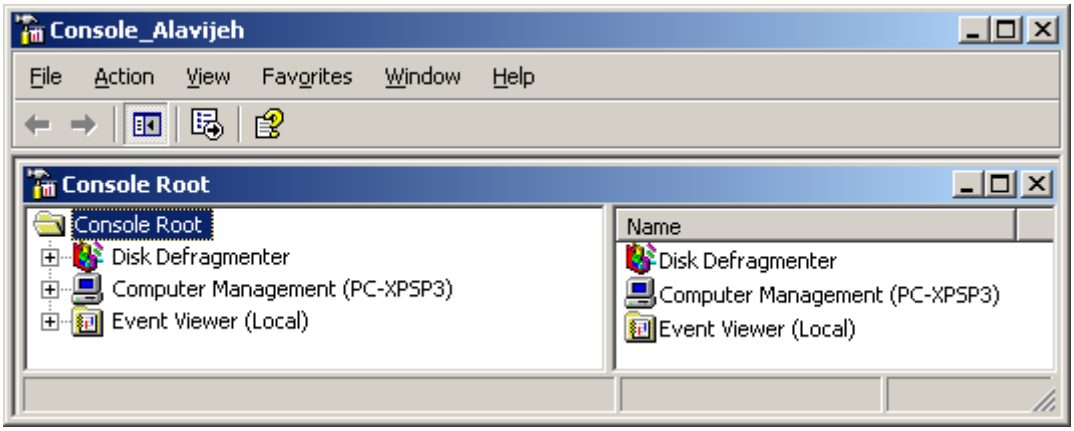
سپس نامی نیز برای این کنسول جدید وارد نمایید.



حال برای دسترسی به این کنسول مدیریتی می‌توانید به مسیر Start ➔ All Programs ➔ Administrative Tools رفته و کنسول ساخته شده را باز نمایید. توجه فرمایید که این مسیر با مسیر Start ➔ Administrative Tools که تاکنون کارهای مدیریتی خود را از آن انتخاب می‌کردیم، متفاوت است.



با بازکردن کنسول مدیریتی ساخته شده، کنسول‌های خود را به صورت مجتمع مشاهده خواهید نمود.



فصل ۳۶

Distributed File System یا DFS

۳۶-۱- متمرکز کردن اطلاعات Share شده

در فصل ۹، شما با راه اندازی شبکه‌های Workgroup و همچنین به اشتراک گذاری فایل‌ها و پوشه‌ها آشنا شدید. موضوعی که اکنون مطرح می‌شود این است که فرض کنید هر کدام از کامپیوترها نرم‌افزار خاصی را برای استفاده دیگران به اشتراک گذاشته‌اند. حال شما به یک نرم‌افزار نیاز پیدا می‌کنید؛ و فرض می‌کنیم که این نرم‌افزار در شبکه به اشتراک گذاشته شده باشد. تنها راه دسترسی به آن این است، که به تمام کامپیوترهای شبکه، تک تک Login کرده، و در فایل‌های اشتراک گذاشته شده آن‌ها، به جستجوی برنامه مورد نظر بپردازیم. علاوه بر این مشکل، مشکل دیگری نیز وجود دارد که ما بایستی به ازاء تک تک کامپیوترها، یک نام کاربری و رمز عبور ثبت شده در آن کامپیوتر را داشته باشیم. برای حل این مشکلات مایکروسافت Distributed File System یا به اختصار DFS را معرفی کرد.

۳۶-۲- Distributed File System چیست؟

همانگونه که اطلاع دارید، File System مکانیزمی برای نگهداری **اطلاعات و مشخصات** فایل‌های موجود در یک سیستم می‌باشد. هر سیستم یک File System مخصوص خود را دارد و لذا به آن Local File System می‌گویند. در مقابل Local File System، Distributed File System قرار دارد. یعنی اینکه یک کامپیوتر این قابلیت را پیدا می‌کند که **اطلاعات و مشخصات** فایل‌های موجود بر روی دیگر کامپیوترها را نگهداری می‌کند. حال برگردیم به بحث قبلی. در بالا ما دو مشکل: جستجوی تمامی کامپیوترهای شبکه و نیز نیاز به دانستن رمزهای عبور هر کامپیوتر را مطرح کردیم و گفتیم که برای حل آن Distributed File System یا به اختصار DFS عرضه شد. روند کار برای حل این مشکل بدین صورت است که هر کامپیوتری که قصد به اشتراک گذاری فایلی را داشته باشد، آن را به یک کامپیوتر خاص معرفی می‌کند (فایل را

در آن کپی نمی‌کند، بلکه فقط یک Link به آن فایل می‌دهد). این کامپیوتر خاص بهتر است کنترل‌کننده دامنه باشد (DC). لذا **لینک** تمامی فایل‌های Share شده، در یک نقطه متمرکز می‌گردند. حال اگر فردی به یک فایل نیاز پیدا کرد، با نام کاربری و رمز عبور خود که در سرور ذخیره شده است، به سرور متصل شده و فایل مورد نظر را در آن جستجو می‌کند؛ و این یعنی نیاز به **یک** نام کاربری و رمز عبور و نیاز به **یکبار** جستجو.

۳۶-۲-۱- مراحل انجام کار DFS

۱. یک سرور را تبدیل به DFS Root Server کرده و روی آن یک پوشه Root درست می‌کنیم.
۲. هر پوشه Share شده‌ی مهمی که داخل ساختار شبکه هست را پیدا کرده و آدرس آن پوشه را به DFS Server مان اضافه می‌کنیم.
۳. حالا هر کاربری که می‌خواهد از فایلهای Share شده‌ی پخش شده در شبکه ما استفاده کند، می‌رود سراغ DFS Server که خودش یک پوشه Root دارد که داخل این پوشه، Shortcut فایل‌های اضافه شده توسط کاربران، قرار گرفته است.
۴. با کلیک بر روی پوشه مورد نظر، کاربر به سمت کامپیوتری که پوشه مورد نظر روی آن قرار دارد، ارجاع داده می‌شود.

پس مشخص شد که کار اصلی DFS این است که: یک لیست بزرگ از فایل هایی که کاربران ممکن است به آن‌ها نیاز داشته باشند را از روی شبکه جمع کرده و توی یک پوشه نگهداری می‌کند تا کاربران به جای اینکه مجبور شوند هر کامپیوتر را برای وجود پوشه Shareشده خاص جستجو کنند، بتوانند با یک بار وصل شدن به پوشه ریشه، کل محتوای Share شده‌ی شبکه را ببینند.

۳۶-۲-۲- انواع DFS

DFS به دو نوع اصلی تقسیم می‌شود:

۱. Stand-Alone DFS Root

در این حالت، ما Active Directory نداریم و بر روی یک سیستم عامل سرور اقدام به اجرا کردن سرویس DFS می‌کنیم. در این حالت، فایل‌های مورد نظر ما Replicate نمی‌شوند و اگر DFS Server مان Down شود، کاربران قادر به دسترسی به پوشه‌های Shareشده نخواهند بود. در ضمن برای Fault Tolerance هم مجبوریم که از ساختارهای Clustering خود سیستم عامل استفاده کنیم.

۲. Domain DFS Root

در این یکی حالت، ما DFS را روی یک ساختار Domain Model نصب می‌کنیم، Replication بین Rootهای مختلف به کمک ساختاری به نام FRS انجام شده و Fault Tolerance هم توسط FRS یا File Replication Service صورت می‌گیرد.

در حالت اول اگه سرور Down شود، کاربران قادر به دسترسی به پوشه‌های Shareشده نخواهند بود. برای اینکه این اتفاق نیفتد، می‌توانید اقدام به استفاده از قابلیت Network Load Balancing ویندوز برای کلاستر کردن سیستم هایتان

کنید و سپس روی چندین سرور یک Root Folder یکسان تعریف نمایید که همگی به مکان‌های معینی اشاره می‌کنند. در این حالت، اگر سروری Down شود، کاربران به سرور بعدی هدایت شده و چون Root Folder سرورها یکسان است، پس کاربران متوجه تغییری نخواهند شد. اما یکی از مشکلات این حالت این است که اگر تغییری در یکی از Root Folderهای یکی از سرورها بدهیم، باید سریع برویم سراغ سرورهای دیگر عضو کلاستر و آن‌ها را نیز تغییر بدهیم.

در حالت دوم، یک سرور عضو Active Directory، مسئول کنترل Root Folderها می‌شود. اگر بخواهید اقدام به Fault Tolerance کنید، نیازی به Clustering ویندوز نیست، چرا که ساختاری به نام File Replication Service خودش اقدام به Replicate کردن فایل‌های هر سرور با دیگر سرورهای DFS کرده و بدین ترتیب اگر چندین سرور DFS داشته باشید، اطلاعات این‌ها هر چند دقیقه با هم Replicate شده و هر تغییری که اولی کرده باشد، در بقیه نیز اعمال می‌کند.

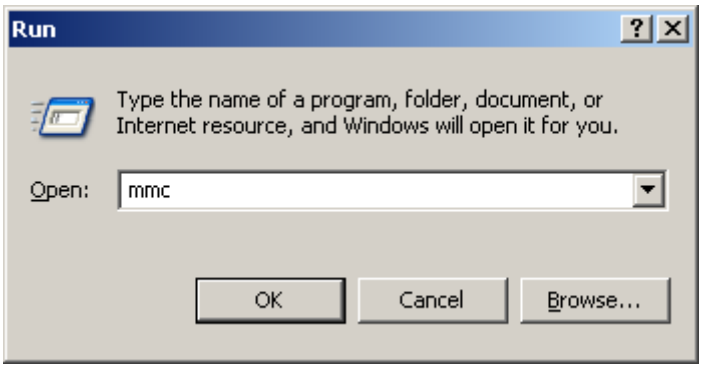
ما در ادامه، حالت دوم را توضیح می‌دهیم.

۳۶-۳- Distributed File System در ویندوز سرور

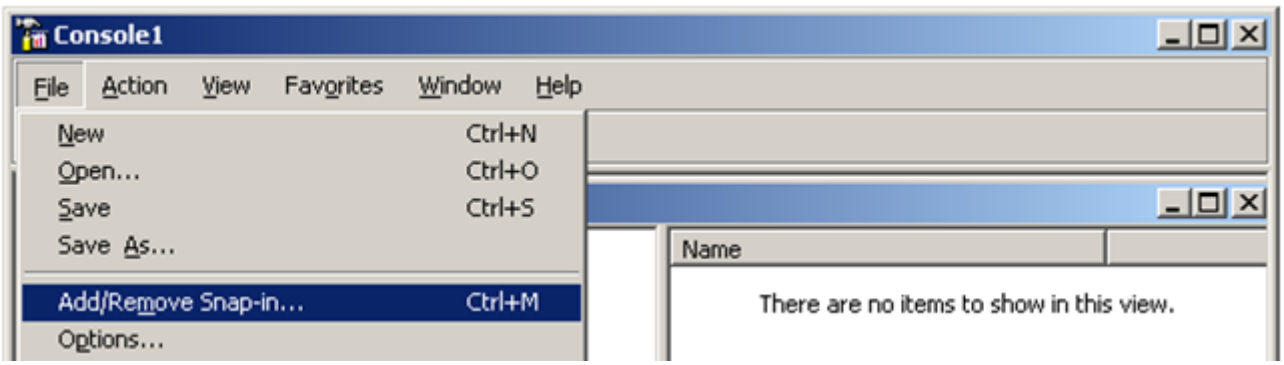
اینک به آموزش راه اندازی DFS می‌پردازیم. اول از همه یادتان باشد که هم پورت ۴۴۵ باید برای DFS باز باشد و هم اینکه DFS یک سرویس به نام Distributed File System دارد که بایستی آن را فعال نمایید. سپس محیط Distributed File System را باز نمایید. بدین منظور از مسیر Administrative Tools ➔ Start گزینه Distributed File System را انتخاب نمایید:



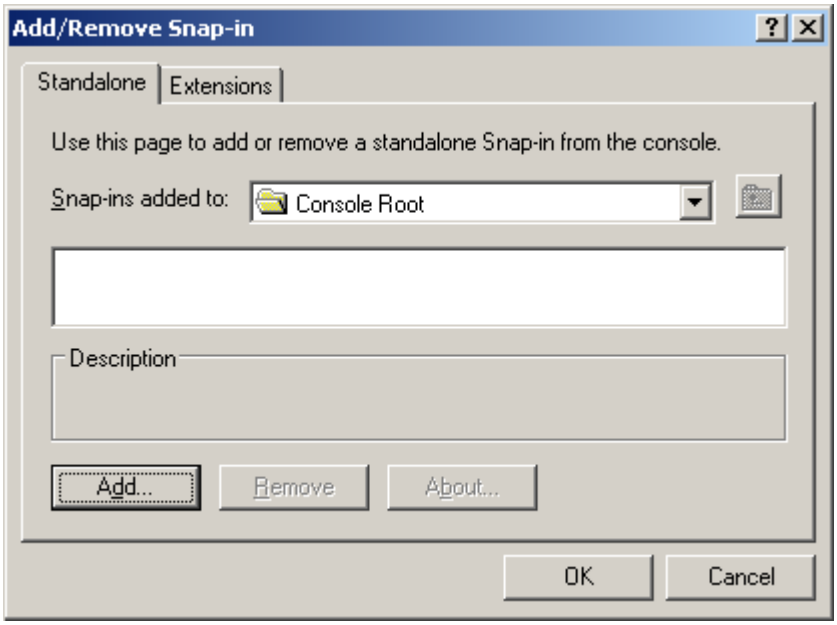
اگر Distributed File System را در این مسیر نیافتید، ابتدا وارد Run شده و عبارت mmc را وارد نمایید تا کنسول مدیریتی مایکروسافت نمایان شود.



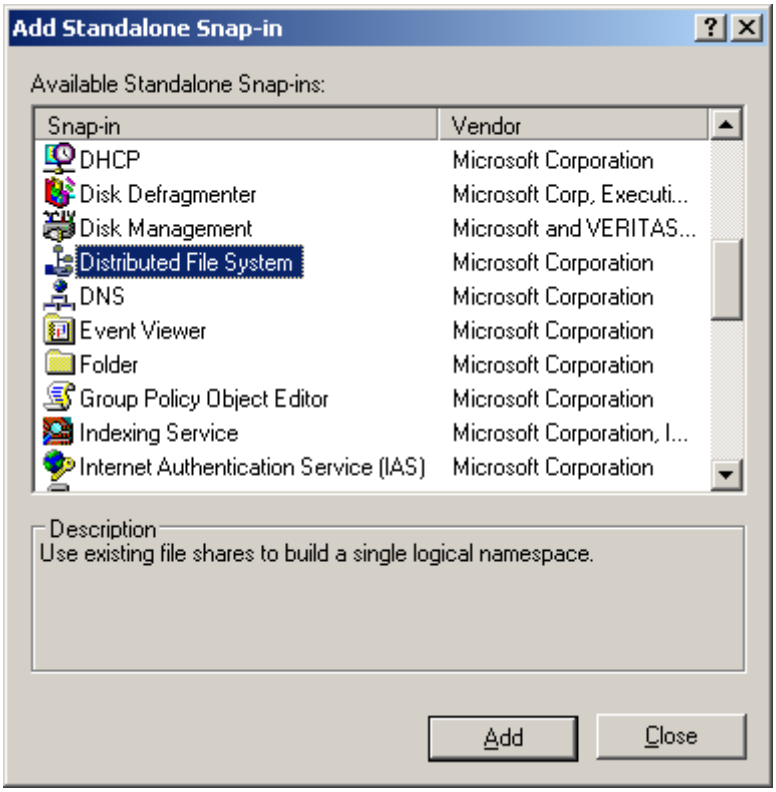
با این کار، صفحه mmc را مشاهده می‌نمایید. در مورد mmc، فصل گذشته صحبت کردیم. حال نوبت به بازکردن کنسول DFS می‌شود. برای این کار، از منوی File گزینه Add/Remove Snap-in را انتخاب کنید.



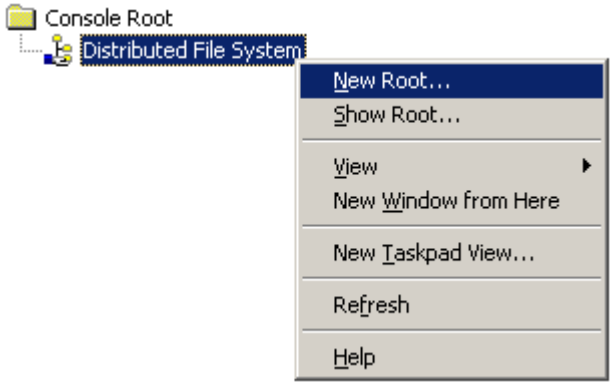
حال نوبت به انتخاب کنسول DFS می‌شود. لذا در صفحه باز شده، روی دکمه Add کلیک کنید.



حال در این صفحه، Distributed File System را انتخاب کرده و روی Add کلیک کنید.

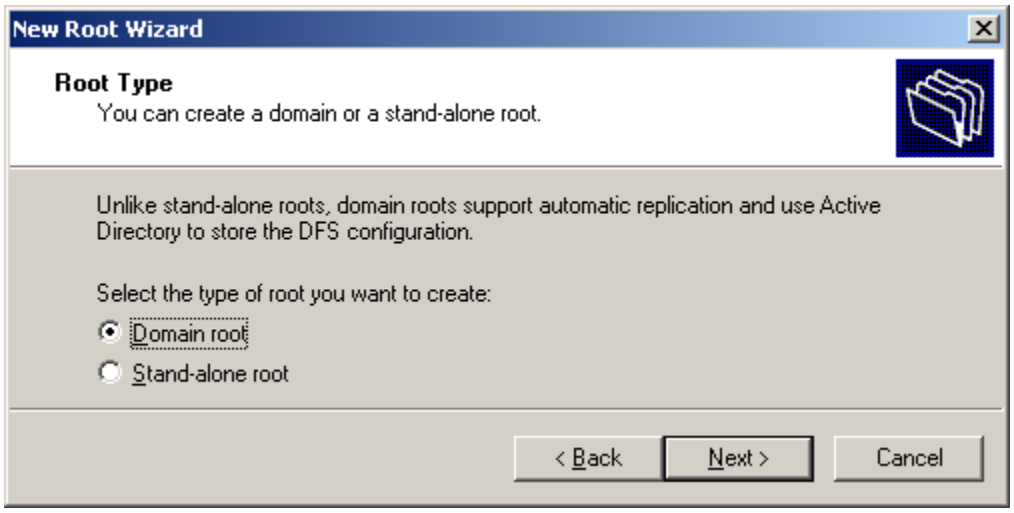


در مرحله بعد، شما بایستی بر روی سرور فضایی را برای ذخیره **اطلاعات و مشخصات** مربوط به فایل‌های Share شده تعیین نمایید. توجه نمایید که فایل‌ها از روی Client بر روی Server کپی نمی‌شوند؛ بلکه در سرور، فقط Linkی به آن فایل‌ها می‌دهیم. بدین منظور بر روی Distributed File System راست کلیک کرده و سپس گزینه New Root را انتخاب کنید. در اینجا Root اشاره به نقطه شروعی (یک آدرس) دارد که برای دسترسی به فایل‌ها و پوشه‌های Share شده از آن استفاده می‌کنیم. مثلاً ریشه (Root) درایو C:\، محلی آغازین برای دسترسی به فایل‌ها و پوشه‌های موجود در این درایو است.

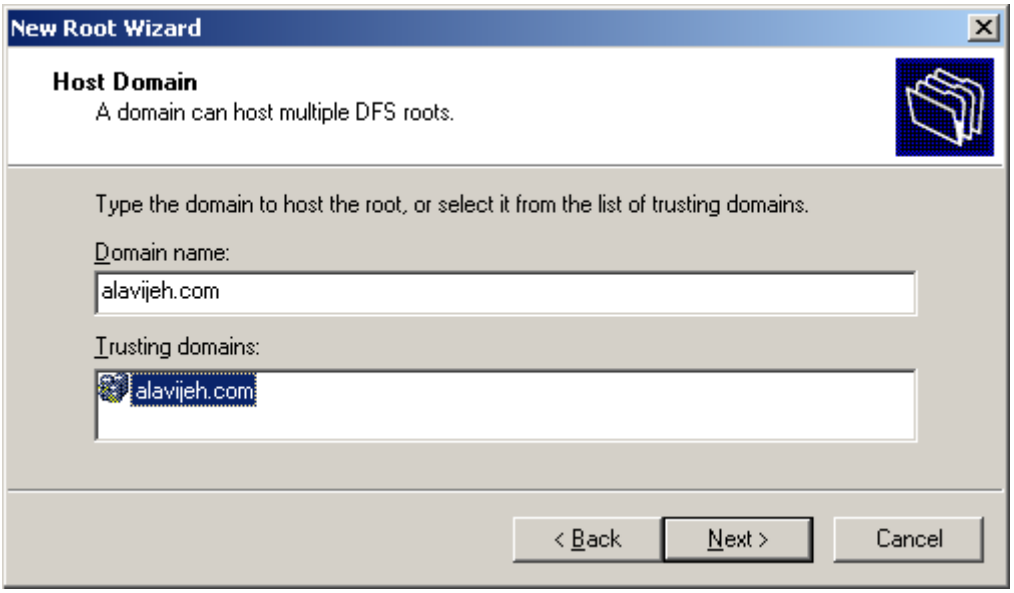


در صفحه خوش آمدگویی، Next را بزنید.

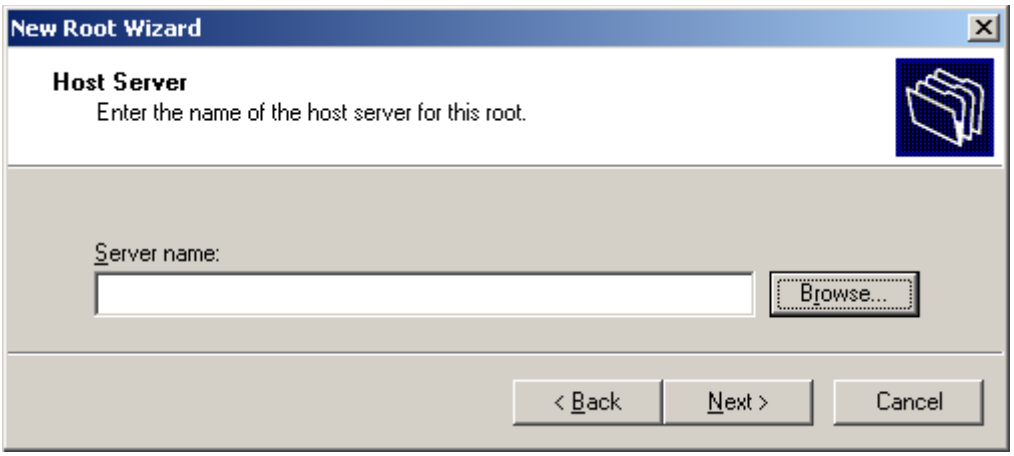
در مرحله بعد تعیین نمایید که کامپیوتری که می‌خواهد این فضا را نگهداری کند (فضای متمرکز برای اشاره به فایل‌های Share شده)، آیا در یک Domain قرار دارد یا اینکه یک کامپیوتر مستقل (Stand-alone) است؟ از آنجایی که ما Domain را راه اندازی کرده و کامپیوتر ما در Domain قرار دارد، لذا ما گزینه Domain root را انتخاب می‌کنیم.



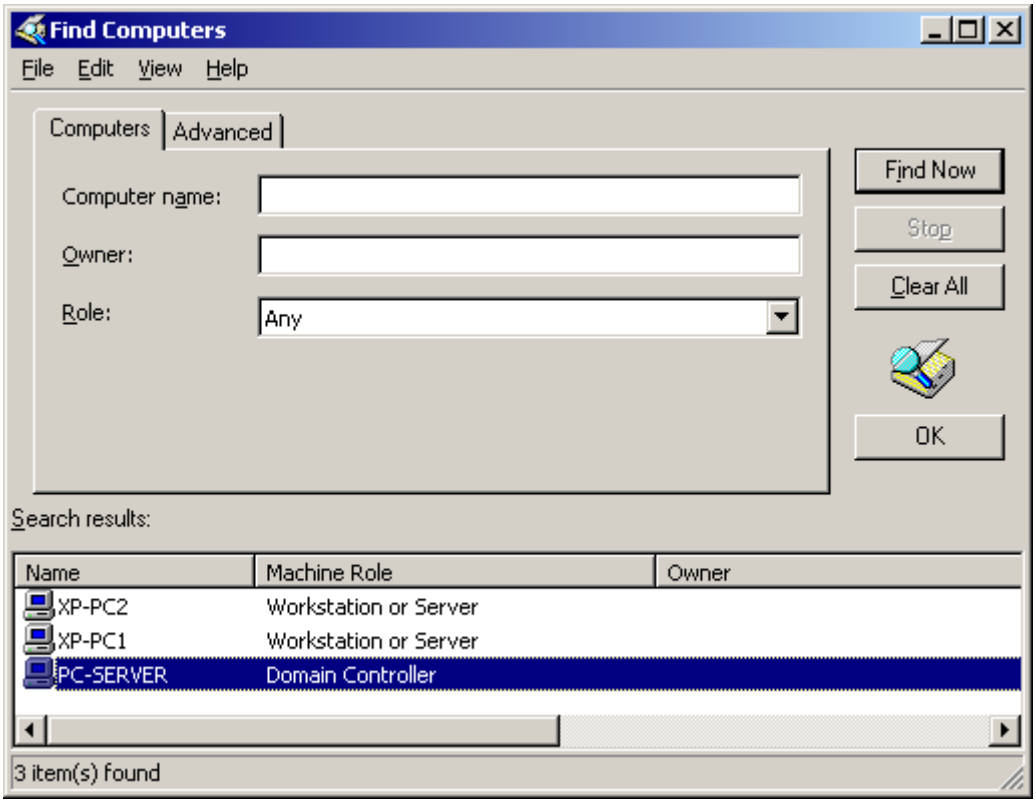
در این صفحه دامنه‌ای که کامپیوتر در آن قرار دارد را انتخاب نمایید. توجه نمایید که این دامنه می‌تواند یک دامنه Trust (مورد اعتماد) باشد.



در مرحله بعد کامپیوتری که فضا را نگهداری خواهد کرد تعیین نمایید. توجه نمایید که این کامپیوتر می‌تواند سرور نباشد. ولی حتما بایستی جزء دامنه باشد. در اصل، این همان سروری می‌باشد که اقدام به ذخیره‌ی اطلاعات Root Folder می‌کند. برای انتخاب کامپیوتر، روی Browse کلیک کنید.



در صفحه باز شده، کامپیوتر مورد نظر را انتخاب کرده و روی OK کلیک کنید.

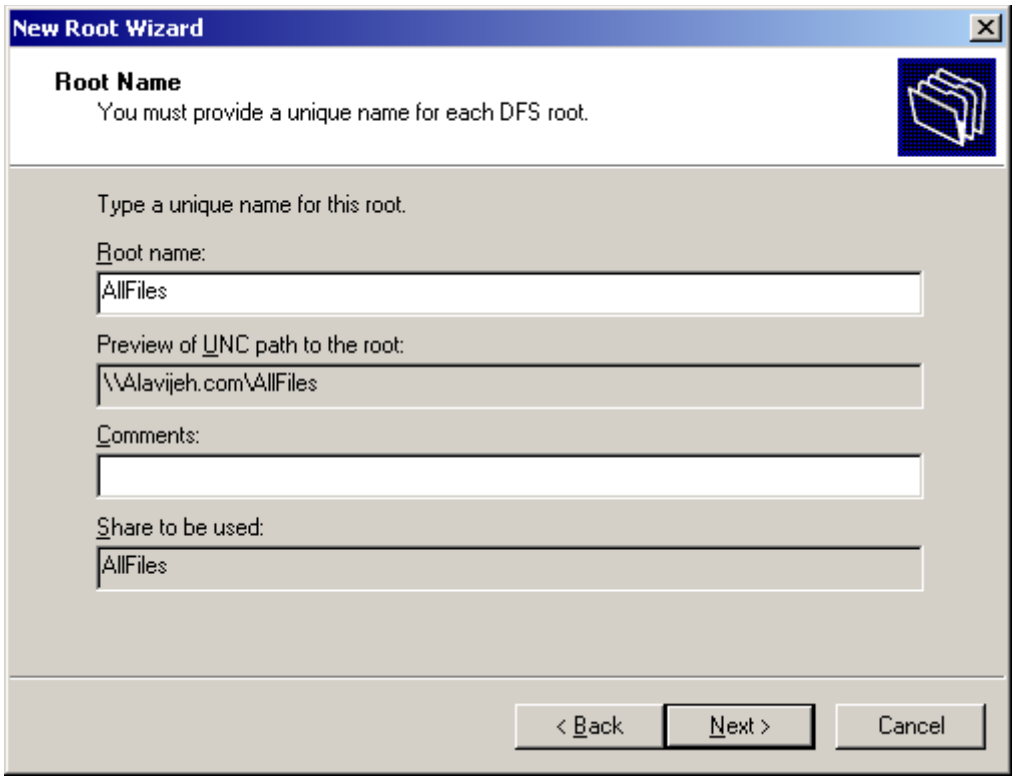


از آنجایی که این کامپیوتر در دامنه قرار دارد، پس از انتخاب آن، نام کامل آن (FQDN) نمایان می‌شود. یادآوری: FQDN، همان نام کامپیوتر به همراه نام دامنه آن می‌باشد.



در مرحله بعد، نام یک پوشه Share شده در کامپیوتری که Rootها را نگهداری می‌کند وارد نمایید. کاربرد این نام، این است که کاربران پس از Login به سرور، با ورود به پوشه‌ای به همین اسم، می‌توانند فایل‌های Share شده در شبکه (که به سرور معرفی شده اند) را مشاهده نمایند. در این مثال ما نام را AllFiles در نظر گرفته‌ایم. این بدان معنا است که در سرور

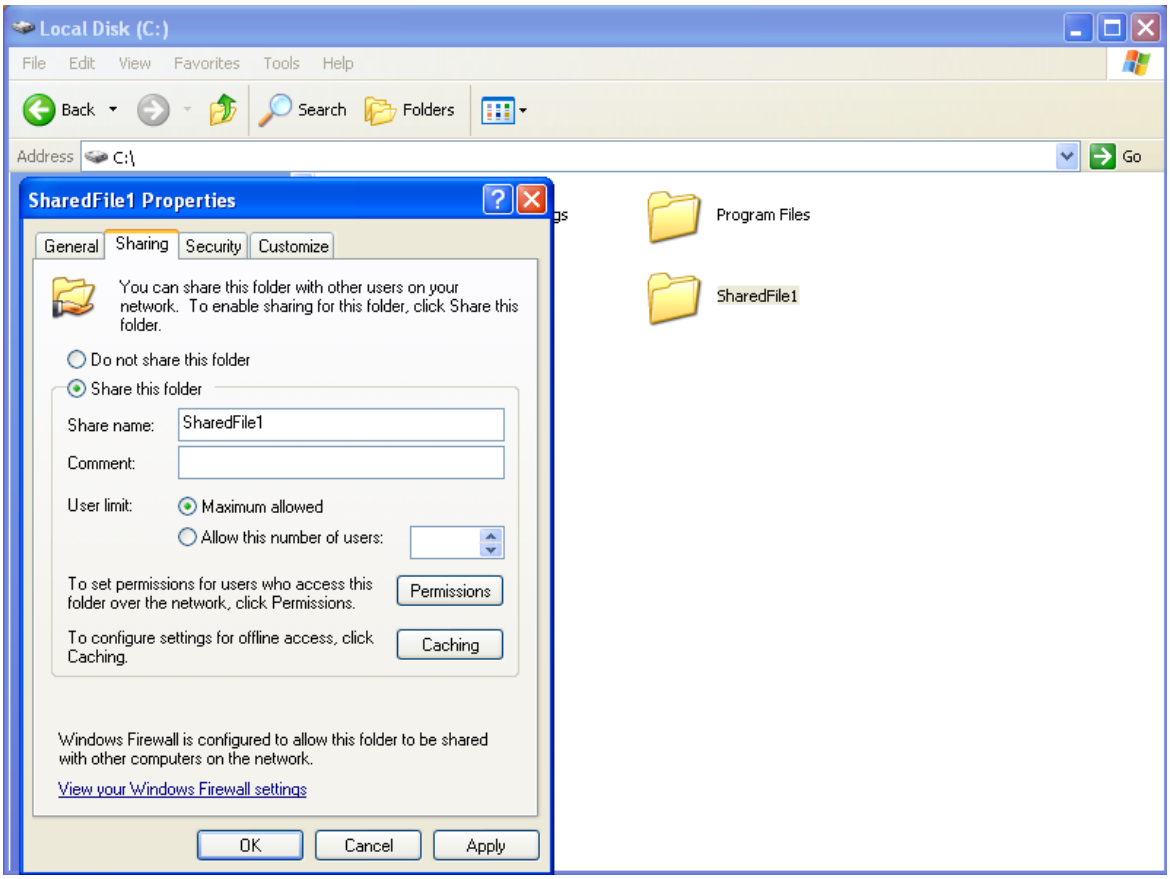
Root DFS، پوشه‌ای به نام AllFiles، به اشتراک گذاشته شده است. لذا کاربران برای مشاهده فایل‌های Share شده بایستی به مسیر \\alavijeh.com\AllFiles مراجعه نمایند. تا این لحظه بایستی متوجه شده باشید که می‌توان **اطلاعات و مشخصات** فایل‌های Share شده را در هر کامپیوتری ذخیره نمود، اما دسترسی به آن‌ها، تنها به کمک اتصال به سرور (DC) انجام می‌گیرد. باز هم تاکید می‌کنم که **در این صفحه، نام یکی از پوشه‌های Share شده را وارد نمایید**. اطلاعات Shortcutها در این پوشه ذخیره خواهد شد.



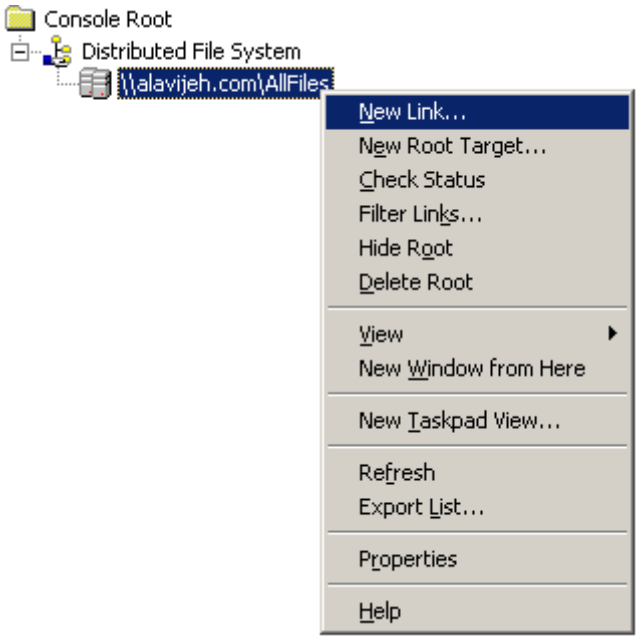
در نهایت، روی Finish کلیک کنید.

۳۶-۴- ایجاد Link به یک پوشه Share شده

حال بایستی در Client فایلی را Share کنید. در این مثال ما پوشه C:\SharedFile1 را در Client به اشتراک گذاشته‌ایم.

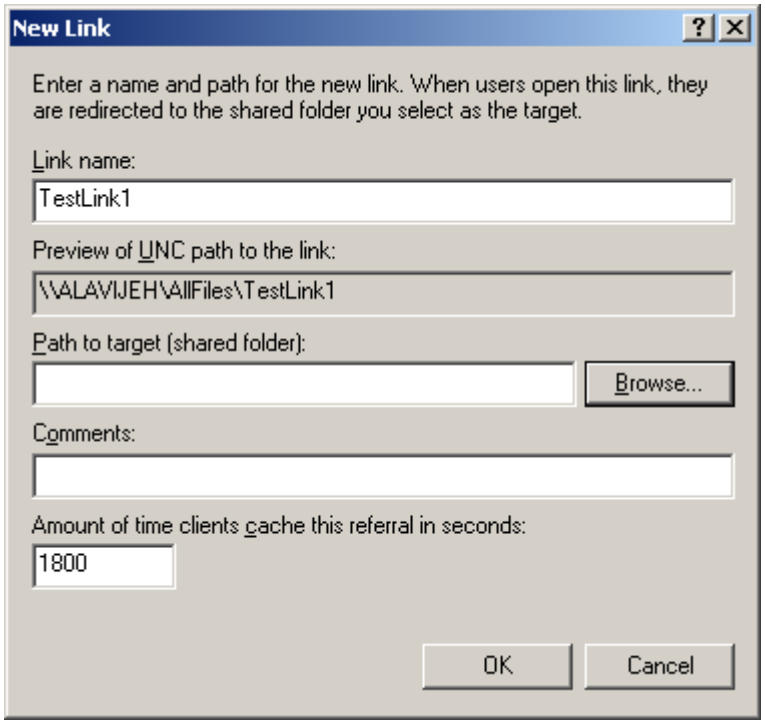


حال مجددا به سرور بر گردید. در این مرحله، برای اینکه این پوشه توسط دیگر کامپیوترها قابل مشاهده باشد، بایستی یک Link به آن پوشه ایجاد کنیم. بدین منظور روی Root ساخته شده در سرور راست کلیک کرده و گزینه New Link را انتخاب کنید.

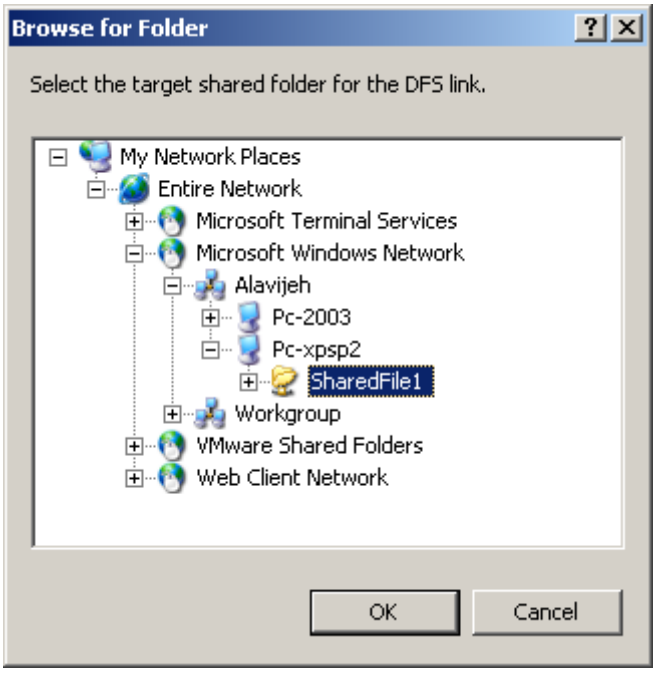


در صفحه باز شده، در قسمت Link Name، یک نام دلخواه برای Link ایجاد شده وارد نمایید به طوری که معرف محتویات آن باشد. سپس در قسمت Path to target، مسیر فایل Share شده را وارد نمایید. بدین منظور روی دکمه

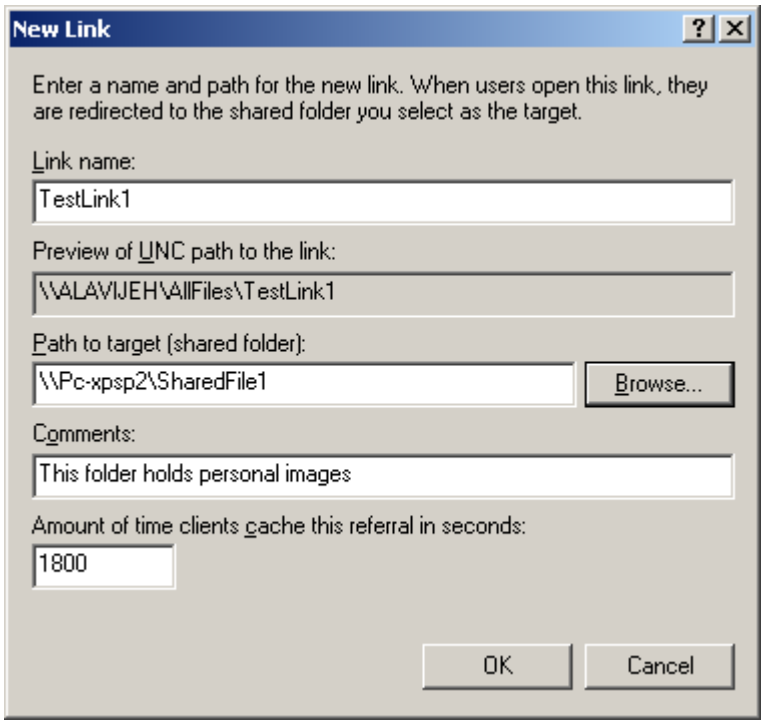
Browse کلیک نمایید. توجه نمایید که مقدار موجود در جعبه متن Preview of UNC path to the link، مسیری را نشان می‌دهد که کاربران برای دسترسی به محتویات این پوشه Share شده بایستی طی نمایند.



در صفحه باز شده، ابتدا کامپیوتر مورد نظر و سپس پوشه Share شده آن را انتخاب نمایید. توجه نمایید که اطلاعات کامپیوترهای یک شبکه، در قسمت Microsoft Windows Network قرار دارد. به شکل توجه فرمایید.

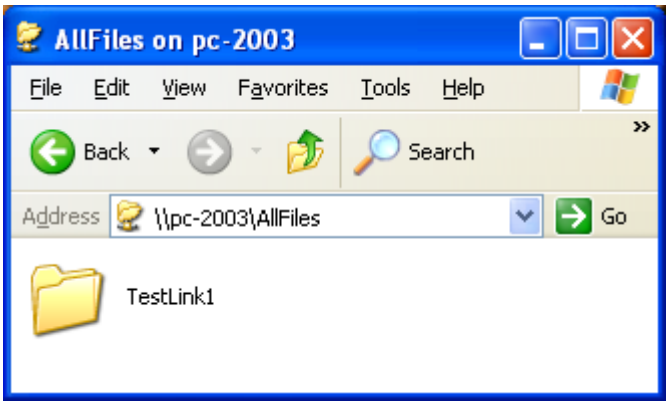


پس از انتخاب پوشه Share شده، شکلی مانند زیر را مشاهده می‌کنید. روی OK کلیک نمایید.



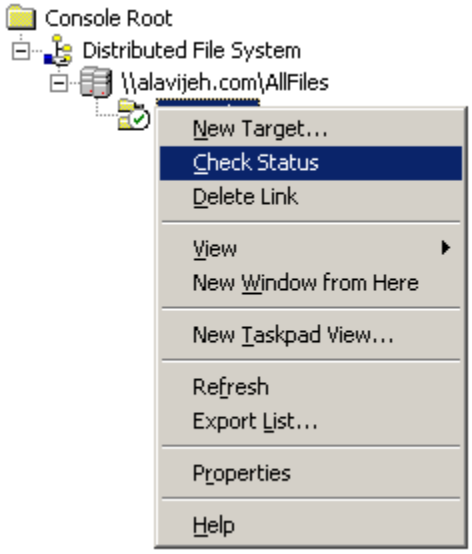
۳۶-۵- دسترسی به پوشه‌های Share شده

حال نوبت به استفاده از پوشه‌های Share شده می‌شود. بدین منظور مسیر Root ایجاد شده را در نوار آدرس یا در Run وارد نمایید. با این کار پوشه‌های Share شده و معرفی شده به سرور را مشاهده خواهید نمود.



برای تاکید می‌گویم که این صفحه، تمام پوشه‌های Share شده در شبکه را نشان نمی‌دهد. بلکه آن هایی را نشان می‌دهد که هم Share شده باشند و هم به سرور معرفی شده باشند (در سرور Linkی به آن‌ها ایجاد شده باشد).

همچنین در هر لحظه می‌توانید وضعیت یک Link را بررسی نمایید. بدین منظور روی Link ساخته شده راست کلیک کرده و گزینه Check Status را انتخاب نمایید.



اگر کامپیوتری که این پوشه را Share کرده است، خاموش بوده یا در دسترس نباشد، روی آن Link، یک علامت × قرمز رنگ مشاهده خواهد شد. بدین معنا که دیگر کامپیوترها به این Link دسترسی نخواهند داشت.

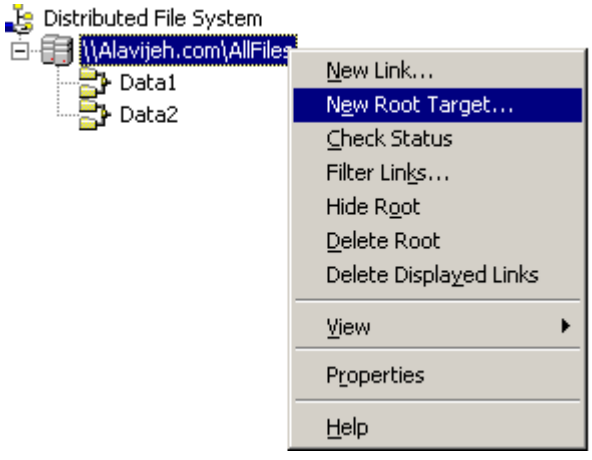


۳۶-۶- Replication در DFS

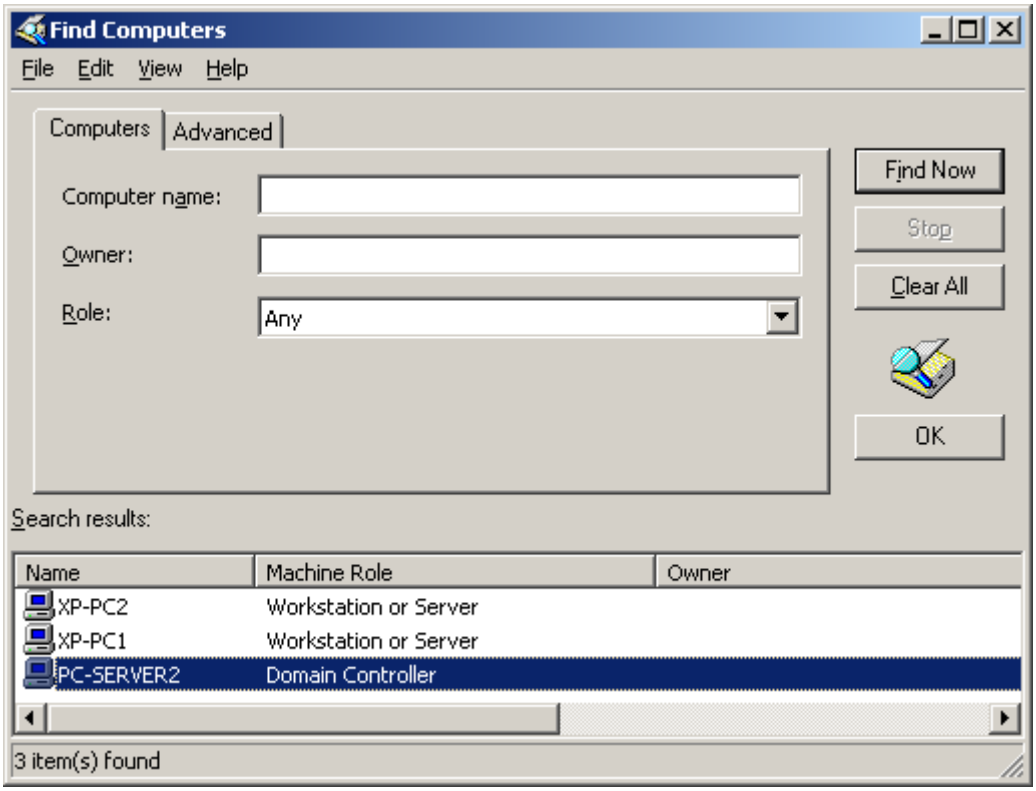
تنها بحثی که از DFS باقی می‌ماند، بحث FRS و Replication است. منظور از FRS و Replication، همان عملیات تکثیر Shortcut پوشه‌های Share شده در چندین سرور می‌باشد، به طوری که با خراب شدن یک سرور DFS، سرور دیگر بتواند عملیات سرویس دهی را انجام دهد. (Fault Tolerance)

بدین منظور مراحل زیر را طی نمایید:

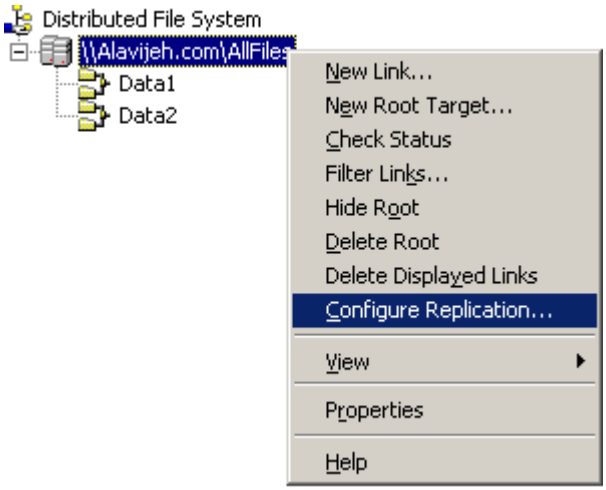
برای ایجاد Fault Tolerance، باید اطلاعات این سرور به پوشه‌ای عین Root Folder بر روی سروری دیگر منتقل شود. این سرور دوم، بایستی دقیقا مانند همین سرور، قابلیت DFS را داشته باشد؛ یعنی یک ویندوز سرور که همچنین بایستی دارای یک پوشه Share شده، همنام با پوشه Share شده سرور DFS اصلی که به عنوان Root DFS استفاده می‌شود، باشد. برای شروع، بر روی نام سرور راست کلیک کرده و گزینه New Root Target را انتخاب نمایید.



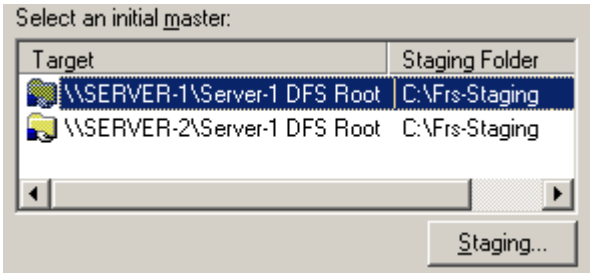
در صفحه باز شده، یکی دیگر از سرورهای موجود در Domain را انتخاب نمایید. همانطور که در بالا نیز ذکر شد، این سرور بایستی دارای سرویس Distributed File System بوده و نیز دارای یک پوشه Share شده، همنام با پوشه Share شده سرور DFS اصلی که به عنوان Root DFS استفاده شد، باشد. لذا در صفحه باز شده، روی Browse کلیک کرده و سپس سرور مورد نظر را انتخاب نمایید.



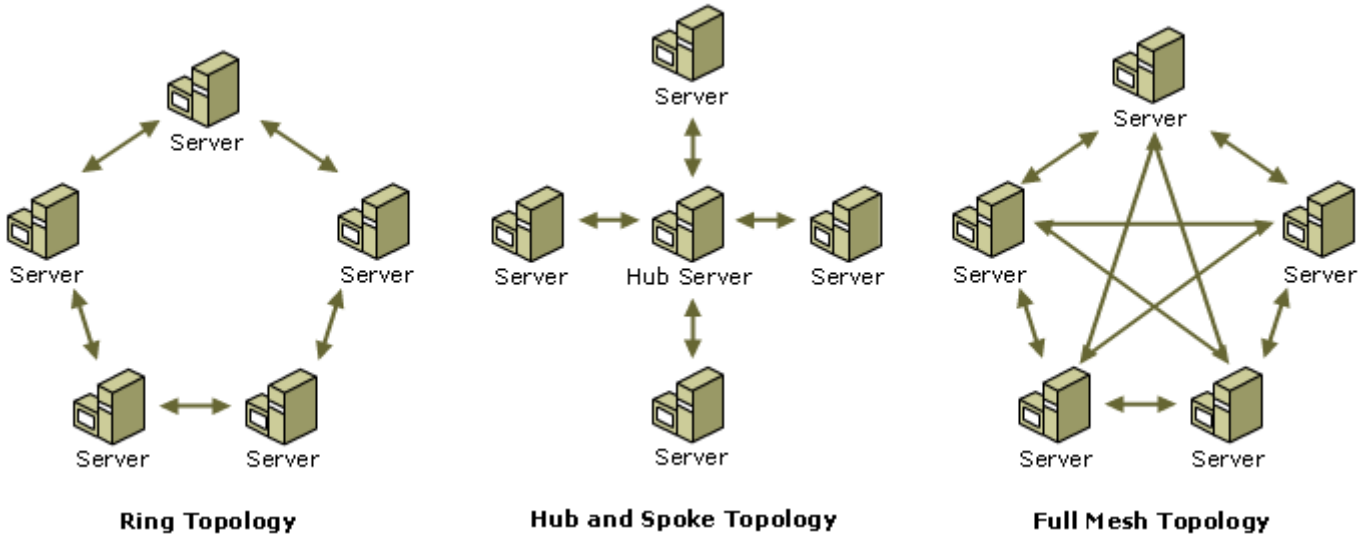
الان ما دو تا سرور داریم که به عنوان DFS Server عمل می‌کنند. تنها کاری که باید انجام شود، این است که بین این سرورها Replication راه بیندازیم. برای اینکار دوباره روی نام سرور راست کلیک کرده و سپس گزینه Configure Replication را انتخاب نمایید.



برای اینکه Replication بتواند صورت بگیرد، سیستم پوشه‌ای به نام Staging Folder به وجود می‌آورد تا فایل‌ها را به صورت موقت در آن نگه دارد. این پوشه را در این صفحه مشخص کنید:



در مرحله‌ی بعد هم باید اقدام به انتخاب توپولوژی Replication اطلاعات در بین سرورها کنید که پیشنهاد می‌کنم از نوع Ring باشد. برای اغلب شبکه‌ها این توپولوژی بهتر از بقیه جواب می‌دهد. تصویر زیر تفاوت توپولوژی‌های مختلف Replication را بهتر نشان می‌دهد.



فصل ۳۷

Streaming Media Server

۳۷-۱- Streaming Media Server چیست؟

چند سالی است که صدا و سیمای جمهوری اسلامی ایران، اقدام به آرشیو نمودن فیلم‌های پخش شده از تلویزیون نموده و کاربران را نیز قادر ساخته است که بتوانند از طریق اینترنت به این آرشیو دسترسی پیدا نموده و فیلم‌های ضبط شده را مشاهده نمایند. نکته قابل توجه این است که کاربران اقدام به دانلود فیلم‌ها و سپس مشاده آن‌ها نمی‌کنند؛ بلکه بایستی فیلم‌ها را به صورت مستقیم و توسط نرم‌افزارهای پخش صوت و تصویر مانند Windows Media Player و یا نرم‌افزارهای مرورگر وب مانند Internet Explorer مشاهده نمایند. تا کنون فکر کرده‌اید که این کار چگونه انجام می‌گیرد؟

همچنین این سناریو را در نظر بگیرید که در یک شبکه محلی بخواهید که در ساعاتی خاص فیلم خاصی را پخش کنید و تمام کاربران نیز (در صورت تمایل) با یک نرخ و سرعت یکسان، فقط همین فیلم را مشاهده نمایند. چیزی مانند ویدئو کنفرانس. یا اینکه مانند صدا و سیما، یک تعدادی فیلم را تدارک دیده باشید و بخواهید کاربران بتوانند با انتخاب نام یک فیلم، شروع به دیدن فیلم به صورت مستقیم کنند، اما باز هم قابلیت دانلود فیلم را نداشته باشند.

انجام این کارها در ویندوز سرور توسط امکانی به نام Streaming Media Server امکان پذیر است. Streaming Media Server نیز نقشی است که می‌توان این نقش را به ویندوز سرور داد و بدین ترتیب می‌توان از امکانات بیان شده در فوق استفاده نمود. این فصل به آموزش این مطالب خواهد پرداخت.

نکته دیگری که حائز امنیت است، این که راه اندازی Streaming Media Server از لحاظ باری که روی شبکه و روی سرور اعمال می‌کند، بسیار پر هزینه است؛ لذا اکیدا توصیه می‌کنم که برای Streaming Media Server از یک سرور مجزا استفاده نمایید.

همانطور که در بالا نیز ذکر شد، دو روش برای پخش صوت و تصویر وجود دارد. یکی این است که ما یک قطعه تصویری را پخش کنیم و دیگر کاربران فقط بتوانند قطعه تصویری در حال پخش را مشاهده نمایند. این روش در ویندوز سرور Broadcast نام دارد. وقتی پخش قطعه تصویری به پایان رسید، کاربران قطعه تصویری دیگری که اصطلاحا **Announce یا آگهی** نام دارد. روش دوم نیز تدارک دیدن تعدادی قطعه تصویری است و کاربران هر کدام از قطعات تصویری را که بخواهند می‌توانند مشاهده نمایند. این روش در ویندوز سرور On-Demand نام دارد.

۳۷-۲- نصب Streaming Media Server

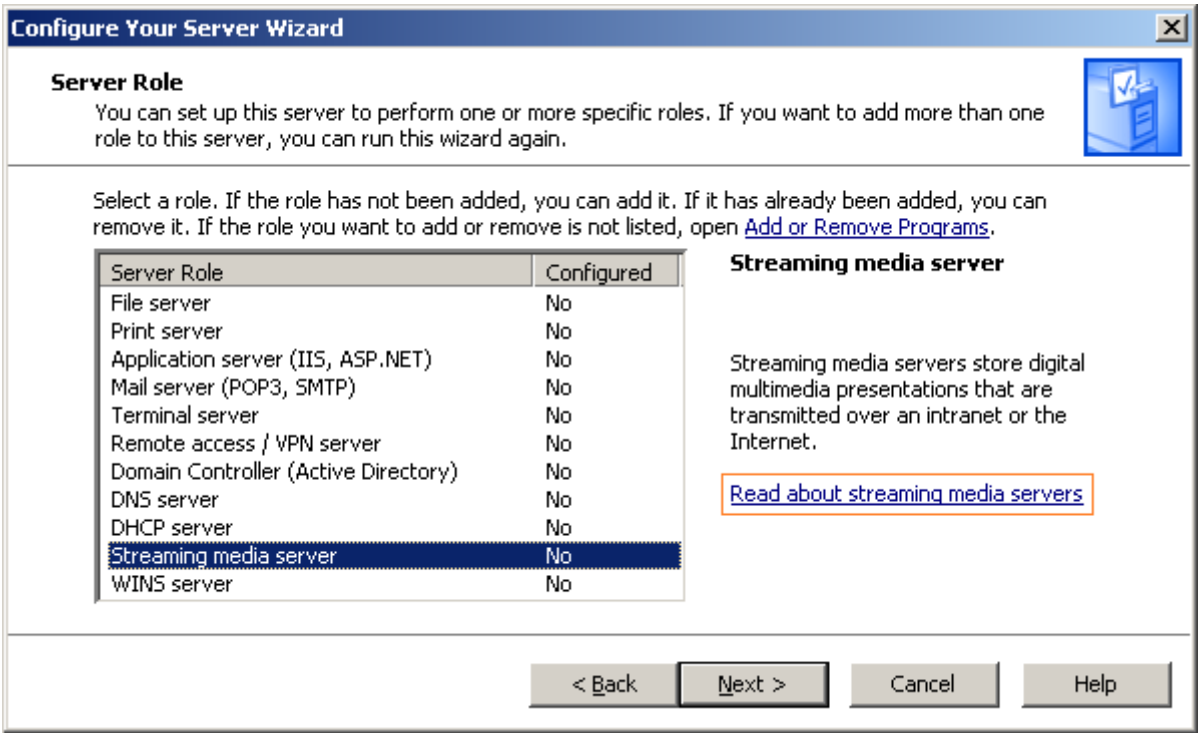
همانطور که قبلا گفته شد، Streaming Media Server یک نقش است که می‌توان این نقش را به ویندوز سرور داد. لذا جهت افزودن این نقش ابتدا از مسیر Start ➔ Administrative Tools برنامه Configure Your Server Wizard را اجرا کنید:



در صفحه باز شده دو بار Next را بزنید:

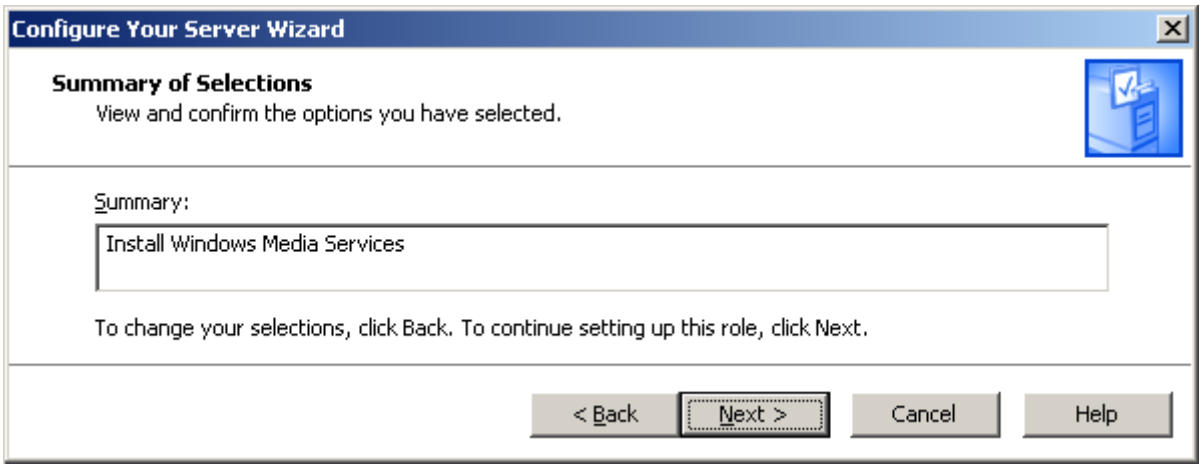


سپس در صفحه باز شده گزینه Streaming media server را انتخاب نمایید تا این نقش را به نقش‌های سرور اضافه کنید. سپس روی Next کلیک کنید.

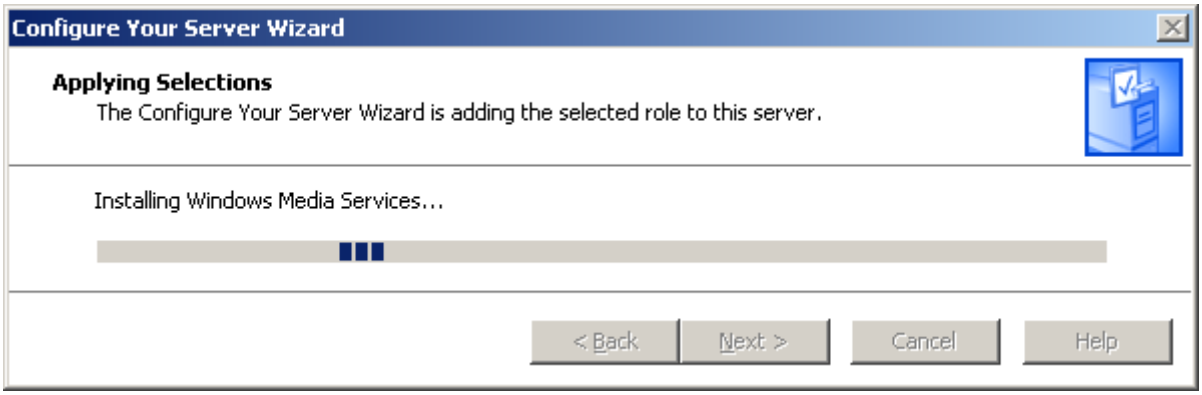


اگر می‌خواهید در مورد Streaming Media Server اطلاعات بیشتری کسب کنید، در صفحه بالا روی Read about streaming media servers کلیک کنید.

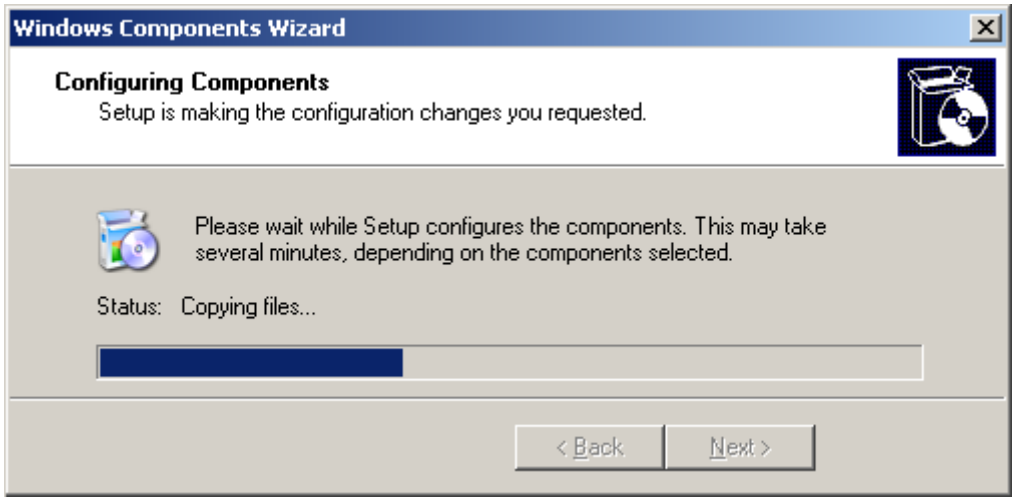
در صفحه بعد، سیستم به شما خواهد گفت که چه نقش هایی را جهت نصب انتخاب کرده‌اید. مجددا روی Next کلیک کنید.



صبر نمایید تا فرآیند نصب به پایان برسد.



اگر سیستم سی دی ویندوز سرور را از شما خواست، آن را درون CD-ROM قرار داده و مجددا صبر نمایید تا فرآیند نصب به پایان برسد.



سپس در صفحه زیر، سیستم به اطلاع شما می‌رساند که فرآیند نصب به پایان رسیده است. جهت خروج، روی دکمه Finish کلیک نمایید.



۳۷-۳- اجرای Streaming Media Server

تا اینجا عملیات نصب به پایان رسید.

جهت اجرای Streaming Media Server، از مسیر Administrative Tools ➔ Start، گزینه Windows Media Service را انتخاب نمایید.



صفحه اولیه که باز می‌شود، به صورت زیر است. در این صفحه، قسمتی به نام Getting Started دارد که شامل آموزش هایی در مورد Streaming Media Server می‌باشد.

در صورت لزوم، گزینه‌های مورد نظر را جهت آموزش بیشتر انتخاب نمایید.



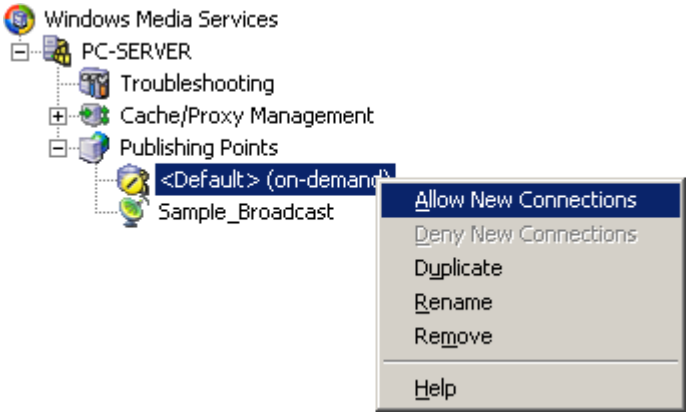
جهت شروع کار، از سمت چپ، سرور را انتخاب نمایید.



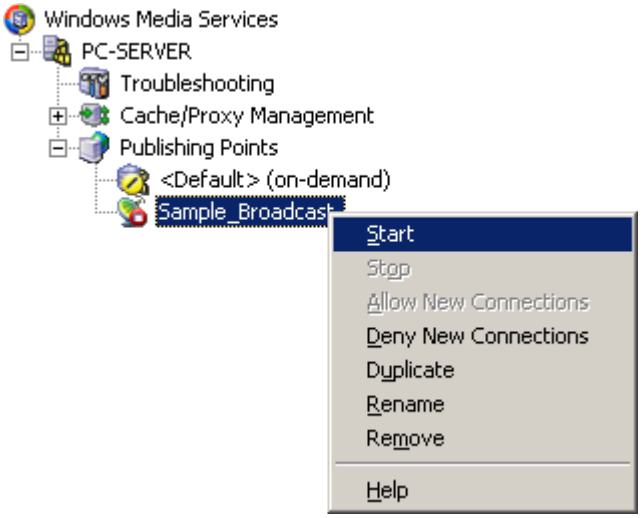
همانطور که در شکل بالا پیداست، قسمت Publishing Points، در بردارنده قسمت‌های مختلفی است که قطعه‌های صوتی/تصویری را نگهداری نموده و هر قسمت می‌تواند به صورت مجزا اقدام به سرویس دهی نماید. در زیر Publishing Points، دو قسمت وجود دارد. اولی <Default> (on-demand) است که کاربران می‌توانند هر کدام از قطعات تصویری این بخش را به دلخواه مشاهده نمایند. قسمت دوم نیز Simple_Broadcast است که کاربران تنها می‌توانند قطعه تصویری را مشاهده نمایند که در حال حاضر در سرور در حال پخش شدن است. روی قسمت اول، یک علامت زرد رنگ و روی قسمت دوم نیز یک علامت قرمز رنگ قرار دارد. این بدین معنا است که این سرویس‌ها هنوز اجرا نشده‌اند.

یک قاعده کلی که وجود دارد، این است که در بخش Publishing Points، گزینه هایی که به شکل هستند، به صورت On-Demand و گزینه هایی که به شکل هستند، به صورت Broadcast عمل می‌کنند.

جهت فعال سازی <Default> (on-demand) روی آن راست کلیک نموده و گزینه Allow New Connections را انتخاب کنید.



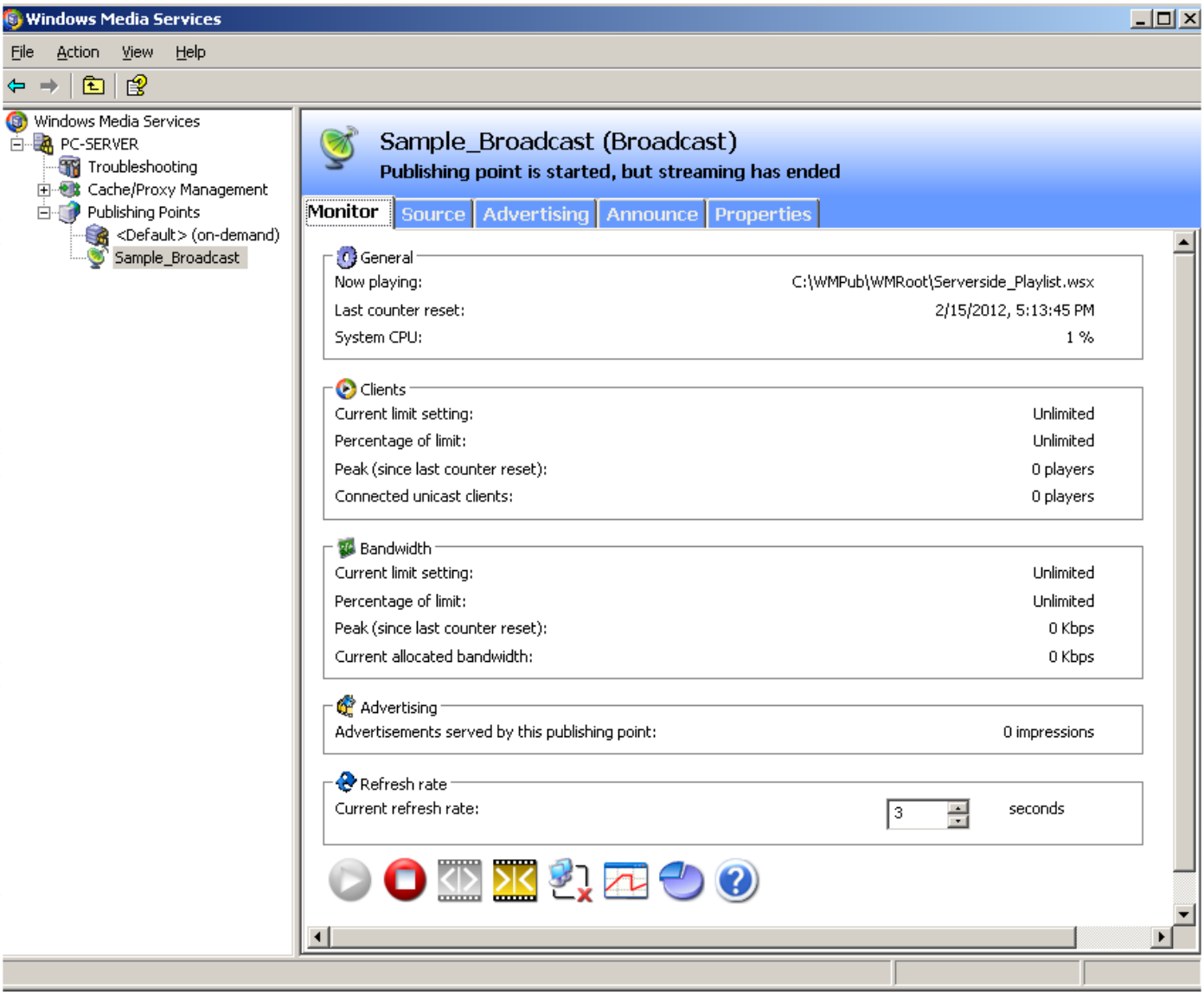
جهت فعال سازی Simple_Broadcast نیز روی آن راست کلیک نموده و گزینه Start را انتخاب کنید.



۳۷-۴- روش Broadcast

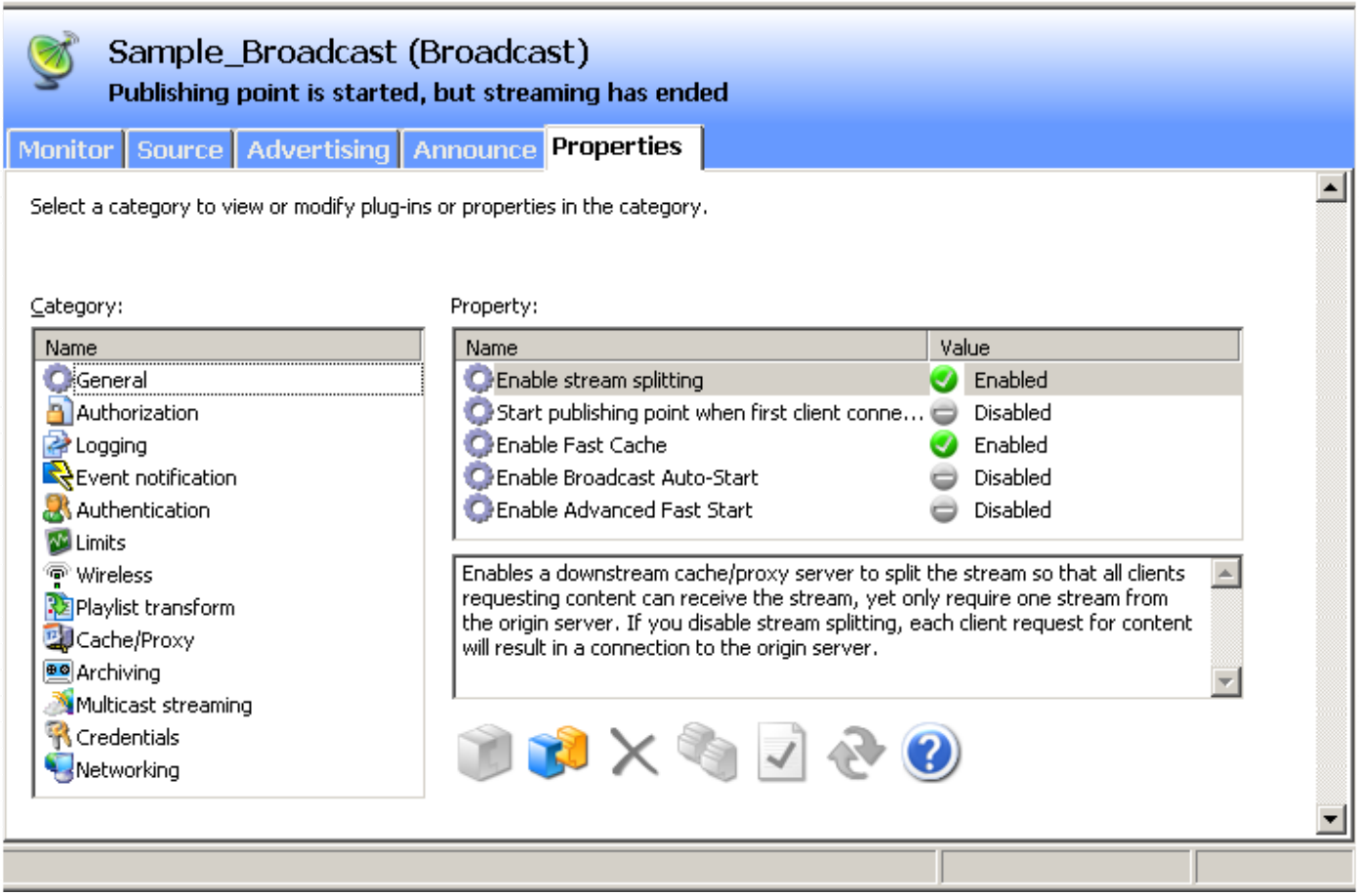
۳۷-۴-۱- راه اندازی سرور

در ابتدا به آموزش قسمت Broadcast می‌پردازیم. ابتدا از لیست، گزینه Simple_Broadcast را انتخاب نمایید. در صفحه باز شده، در سمت راست، چندین سربرگ وجود دارد که اولی Monitor نام دارد و یک سری اطلاعات آماری و وضعیتی در مورد سرور می‌دهد. مثلا از طریق این صفحه می‌توانید بفهمید که اکنون چند کاربر در حال مشاهده فیلم هستند و اینکه میزان بار روی سرور چقدر است.

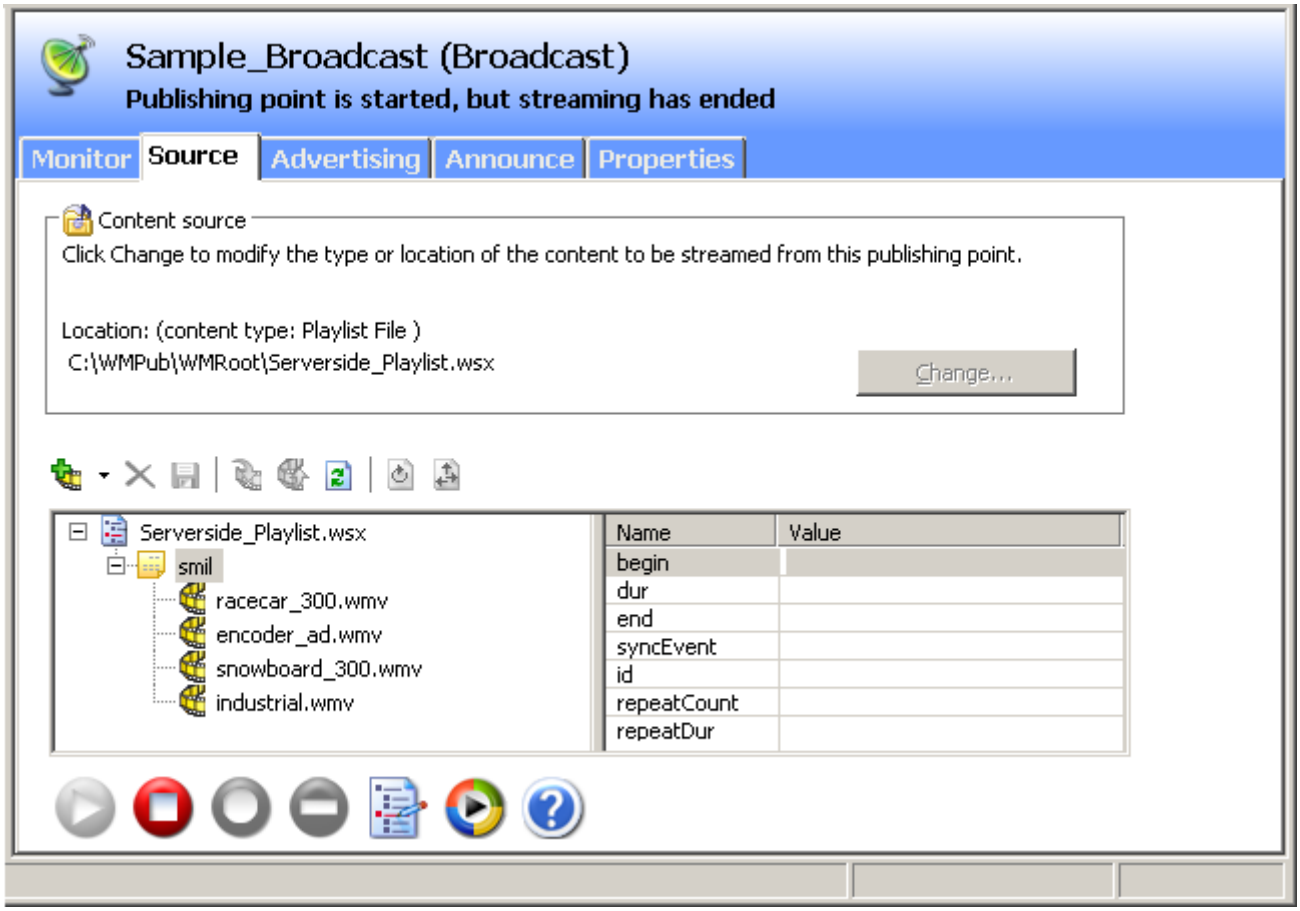


سربرگ آخر نیز سربرگ Properties است که امکان انجام تنظیماتی همچون Caching و Splitting، احراز هویت، Log گیری از رفتار کاربران، اطلاع رسانی، محدودیت‌های دسترسی، تنظیمات Network، تنظیمات شبکه بی‌سیم را به ما می‌دهد.

وارد جزئیات این تنظیمات نخواهیم شد، اما با انتخاب هر تنظیم و مشاهده توضیحات آن، به کاربرد آن پی خواهید برد.



مهمترین سربرگ، سربرگ Source است. از طریق این سربرگ، می‌توانید چندین قطعه تصویری را انتخاب نمایید تا پشت سر هم پخش شوند و کاربران نیز به صورت مستقیم فقط آن‌ها را مشاهده نمایند. در شکل مشخص است که چهار قطعه تصویری جهت پخش انتخاب شده است.



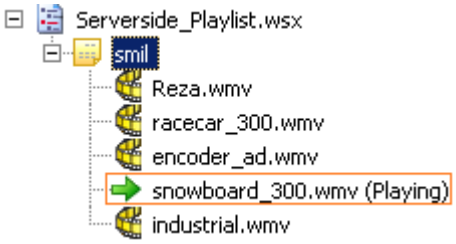
همانطور که در شکل بالا پیداست، اکنون هیچ قطعه تصویری در حال پخش نیست. دلیل نیز این است که قطعات تصویری انتخاب شده، از زمان Start نمودن سرویس، شروع به پخش کرده و به ترتیب پخش می‌شوند. پس از پخش آخرین قطعه، کاربر دیگر به نمایش قطعات تصویری نخواهد بود، مگر اینکه سرویس را مجددا Start کنیم. بدین منظور در همین صفحه روی دکمه Stop the publishing point کلیک کنید.



سپس روی دکمه Start publishing point کلیک کنید تا سرویس شروع به کار کند.



همانطور که از شکل زیر پیداست، اکنون یکی از قطعات تصویری که پشت آن فلش سبز رنگ وجود دارد، در حال پخش می‌باشد که کاربران قادر به مشاهده آن خواهند بود.



نکته: اگر هیچ قطعه تصویری در حال پخش نباشد، کاربران Announce یا آگهی را مشاهده خواهند نمود. این فایل هنگام تعریف کردن Broadcast جدید قابل تعیین خواهد بود.

۳۷-۴-۲- پخش قطعات صوتی/تصویری در Server

حال اگر می‌خواهید قطعات تصویری را تست کنید، روی دکمه Test Stream کلیک نمایید. این تست روی خود سرور انجام می گیرد.



ابتدا ممکن است که پیغام خطای زیر را مشاهده نمایید.

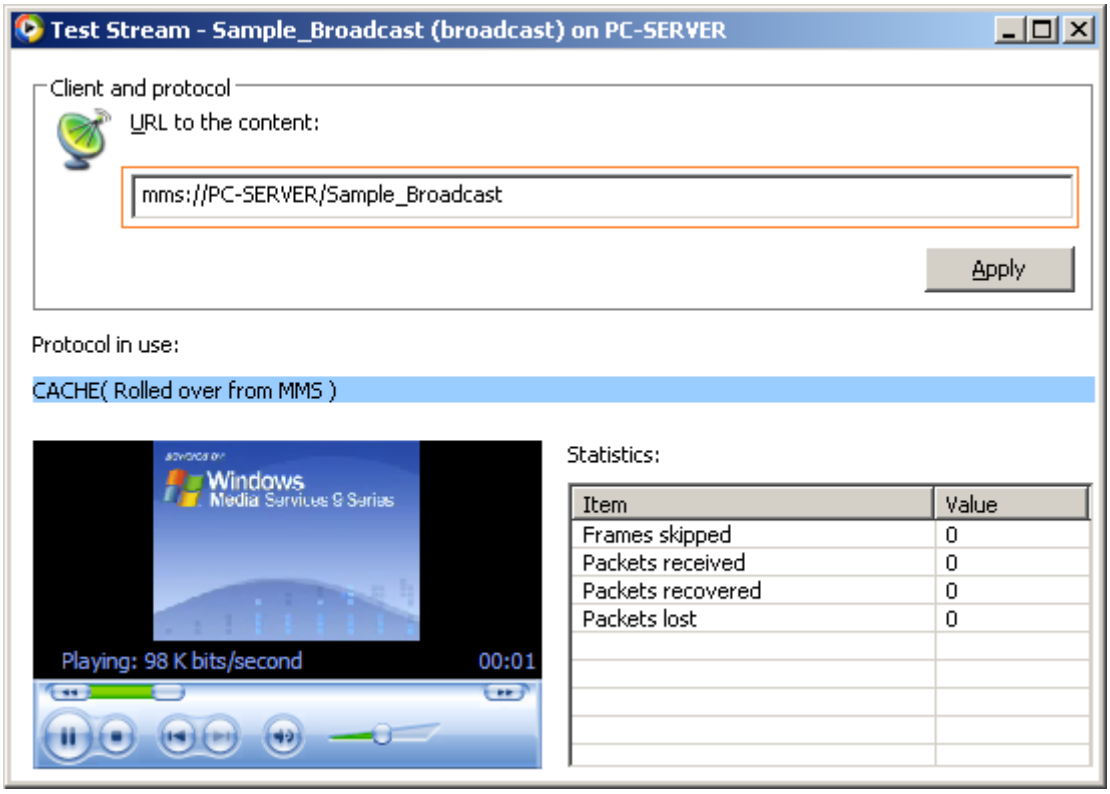


علت این خطا این است که ما داریم قطعات تصویری را روی خود سرور تست می کنیم. پس از OK کردن تصویر فوق، صفحه زیر باز می‌شود.

مهمترین قسمت این صفحه، آدرس سرور جهت مشاهده قطعات تصویری است. قسمت اول آدرس با mms:// شروع می‌شود. این بدان معناست که از پروتکل mms جهت مشاهده فیلم‌ها استفاده می‌شود.

قسمت بعدی آدرس، اسم سرور یعنی PC-SERVER می‌باشد. می‌توان از آدرس IP نیز استفاده کرد.

قسمت آخر آدرس نیز نام Publishing Point است. همانطور که از این آدرس پیداست، ما نام فایلی را جهت پخش وارد نکرده‌ایم. بلکه در حالت Broadcast، همیشه فایلی پخش خواهد شد که در سرور در حال اجراست. اما اگر می‌خواهید، فایل خاصی را خودتان جهت پخش انتخاب کنید، بایستی از روش On-Demand استفاده نمایید.



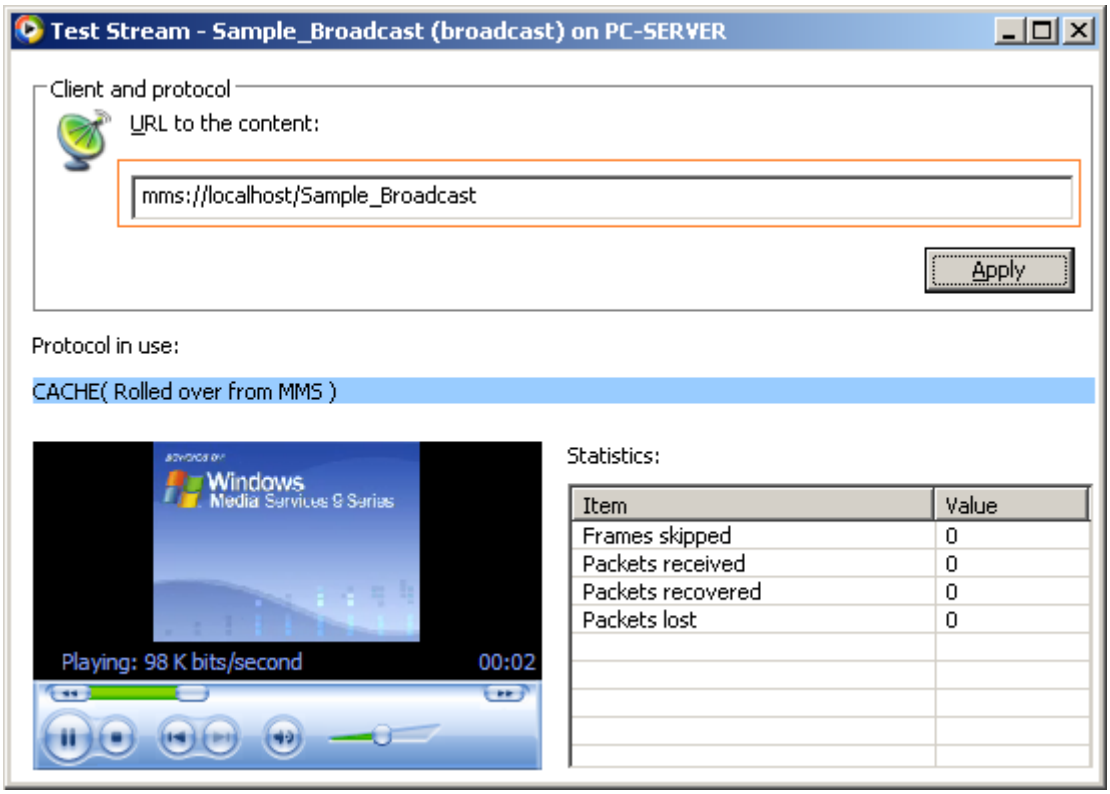
اگر پیغام خطای دو شکل بالاتر را دریافت نمودهاید و در حال حاظر نیز فیلمی را مشاهده نمی‌کند، مشکل از نام سرور است. برای حل مشکل، در قسمت آدرس سرور، نام سرور را انتخاب نموده



و به جای آن کلمه localhost را وارد نمایید. کلمه localhost در هر کامپیوتری، اشاره به همان کامپیوتر داشته و معادل IP با آدرس ۱۲۷.۰.۰.۱ می‌باشد. البته کلمه localhost باعث می‌شود که دسترسی از داخل انجام شده و دیگر پیغام خطای فوق را مشاهده ننمایید.

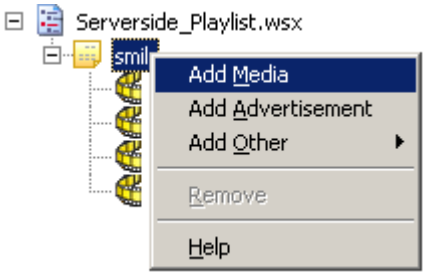


پس از تغییر آدرس IP، بر روی دکمه Apply کلیک کنید.



۳۷-۴-۳- افزودن قطعه صوتی/تصویری جدید

در صورت لزوم، این امکان وجود دارد که قطعات صوتی/تصویری جدید را به لیست پخش یا حتی Codecهایی جهت افزودن پشتیبانی از پخش فرمت‌های صوتی/تصویری جدید، به نرم‌افزار اضافه نمود. بدین منظور وارد سربرگ Source شوید. سپس روی قسمت smil راست کلیک نموده و سپس گزینه Add Media را انتخاب کنید.



صفحه باز شده نشان می‌دهد که قابلیت افزودن موارد زیر وجود دارد:

۱) فایل صوتی یا تصویری

۲) Codec جهت پخش فایل‌های جدید

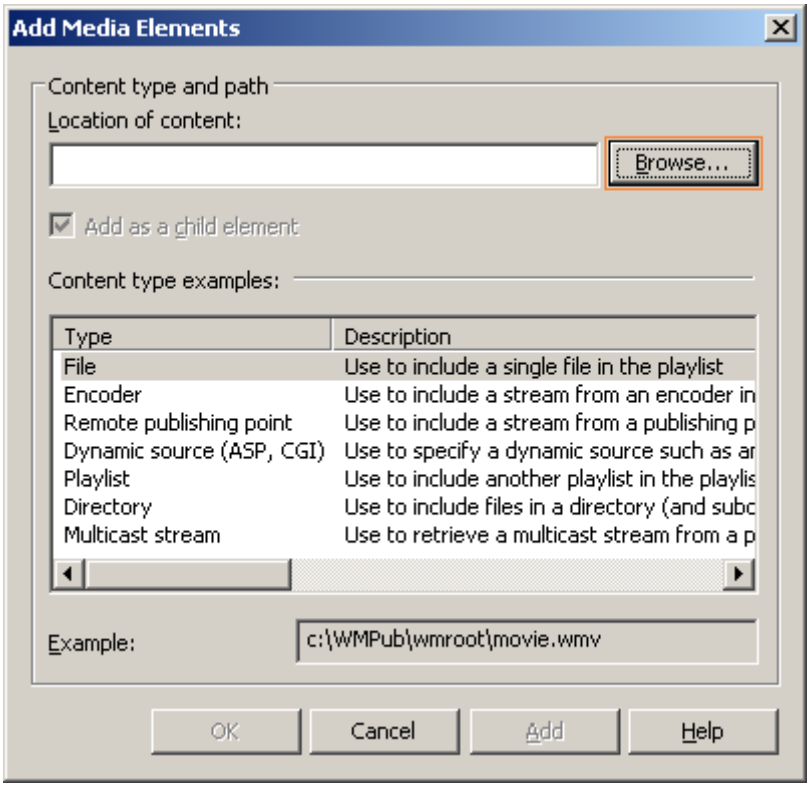
۳) Publishing Pointهایی که روی کامپیوترهای دیگر وجود دارد.

۴) صفحات پویای ASP.Net یا CGI

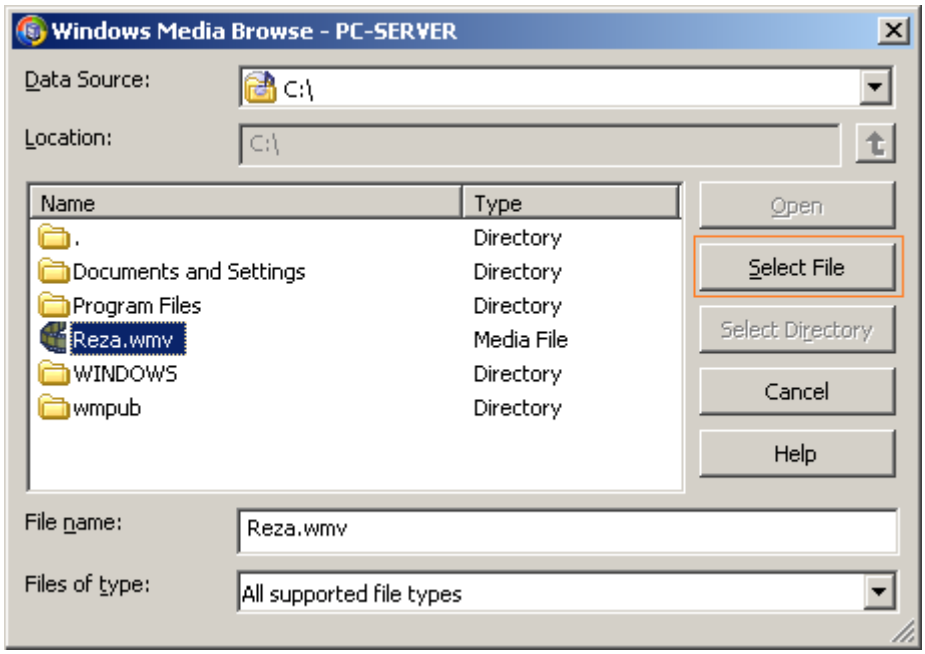
۵) Playlist یا همان لیست هایی که شامل نام فایل‌های صوتی/تصویری جهت پخش می‌باشد.

۶) پوشه‌ای که دارای چندین فایل صوتی/تصویری باشد.

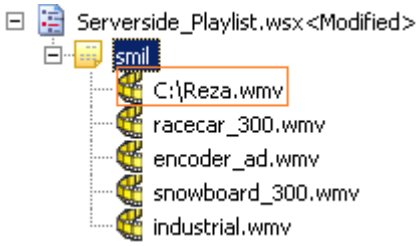
جهت افزودن هر کدام از موارد فوق، روی دکمه Browse کلیک کنید.



در صفحه باز شده، فایلی را انتخاب نمایید. در این شکل من فایل Reza.wmv که درایو C:\ قرار دارد را انتخاب کرده ام. سپس روی Select File کلیک کنید. اما اگر قصد انتخاب پوشه دارید، پس از انتخاب پوشه مورد نظر، روی دکمه Select Directory کلیک کنید. البته نمی‌توان هر فایلی را انتخاب کرد.



پس از تایید، مشاهده خواهید نمود که فایل انتخابی به لیست پخش اضافه خواهد شد.



۳۷-۴-۴- پخش قطعات صوتی/تصویری در Client

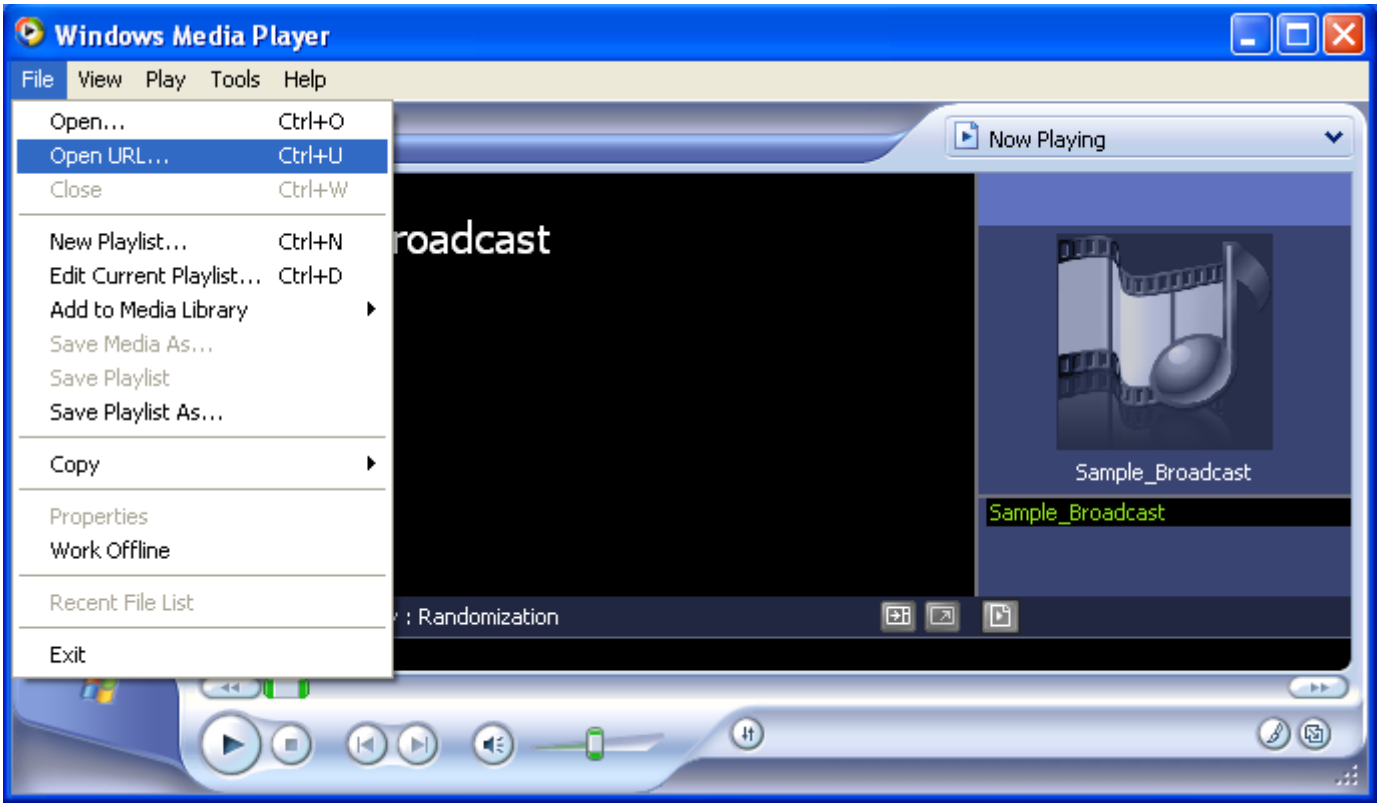
جهت پخش قطعات تصویری در Client، به نرم‌افزار هایی نیاز دارید که پخش فیلم از راه دور و با پروتکل mms را پشتیبانی نمایند. همچنین امکان پخش فیلم از طریق مرورگرهای وب نیز وجود دارد.

قبل از پخش قطعات صوتی/تصویری در Client، ابتدا پخش آن‌ها در سرور را Start کنید.

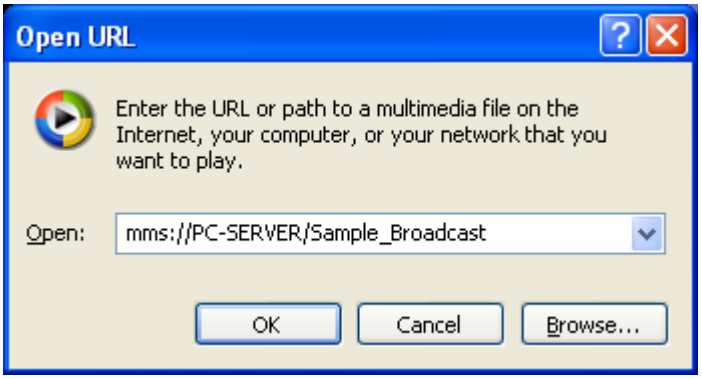
جهت پخش قطعات صوتی/تصویری در Client، ما از نرم‌افزار Windows Media Player که بصورت پیش فرض در ویندوز وجود دارد، استفاده خواهیم کرد. برای شروع این نرم‌افزار را باز نمایید.



در صفحه اول نرم‌افزار، از منوی File، گزینه Open URL… را انتخاب نمایید.



سپس در صفحه باز شده، ابتدا پروتکل مورد استفاده (mms)، سپس نام سرور (PC-Server) و در نهایت نیز نام نقطه انتشار (Sample_Broadcast) را وارد نمایید. در نهایت روی OK کلیک کنید.



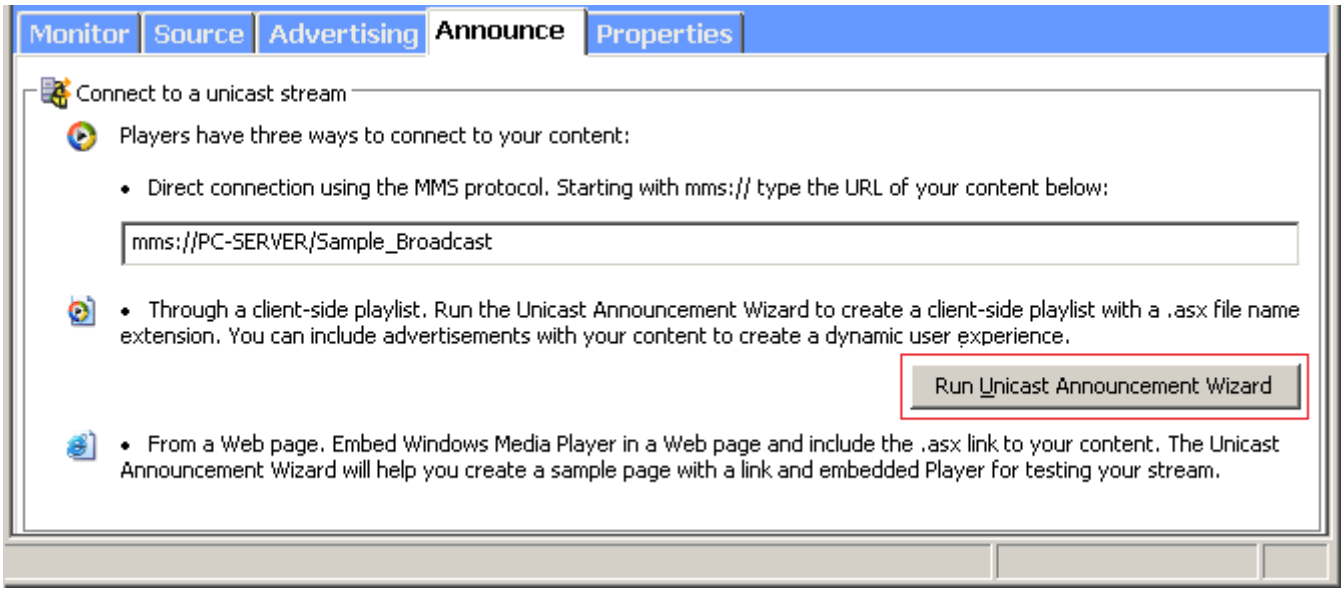
می بینیم که Client اقدام به پخش قطعه تصویری خواهد نمود. کیفیت پخش به کیفیت اولیه قطعه تصویری، نرخ انتقال، نرخ Refresh و میزان ترافیک شبکه بستگی دارد.



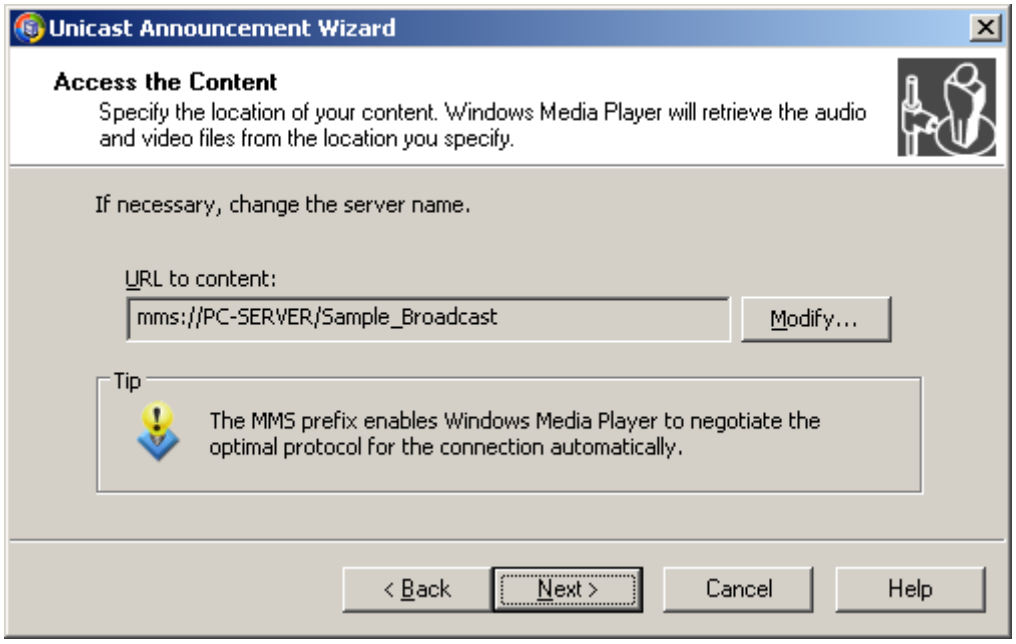
۳۷-۴-۵- پخش قطعات صوتی/تصویری از طریق مرورگر

گفتیم که امکان پخش قطعات صوتی/تصویری از طریق مرورگرهای وب، مانند IE وجود دارد. این کار بیشتر برای پخش از شبکه اینترنت کاربرد دارد.

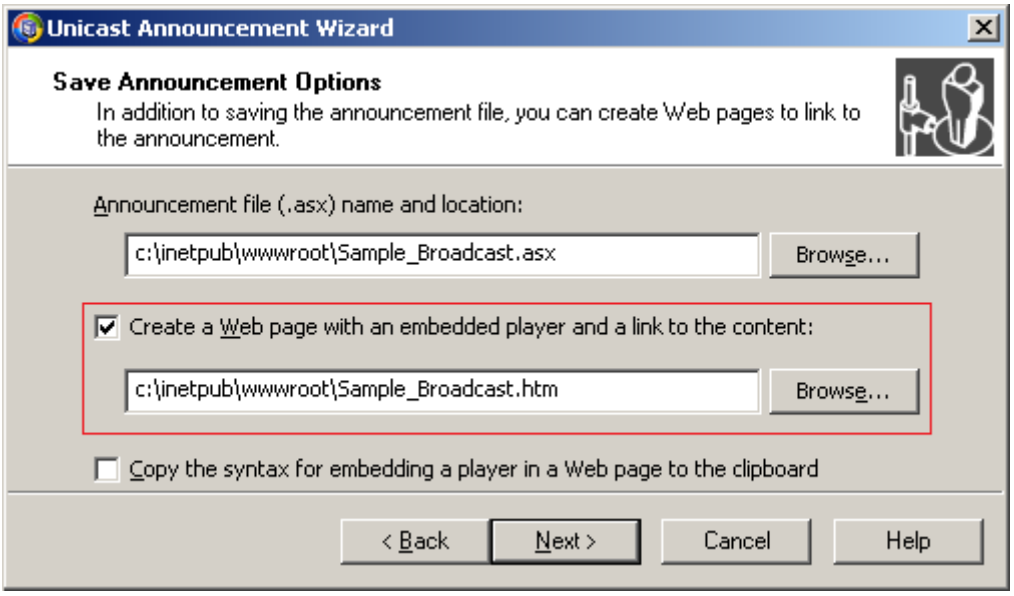
توصیه: قبل از ادامه کار، اگر می‌خواهید که Clientها بتوانند از امکان مشاهده قطعات صوتی/تصویری از طریق مرورگر استفاده کنند، حتما IIS را روی سرور نصب کنید. جهت آموزش این کار به فصل ۳۱ و قسمت نصب IIS روی سرور (۳۱-۲)، مراجعه فرمایید. برای پخش قطعات صوتی/تصویری از طریق مرورگر، وارد سربرگ Announce شده و روی Run Unicast Announcement Wizard کلیک کنید.



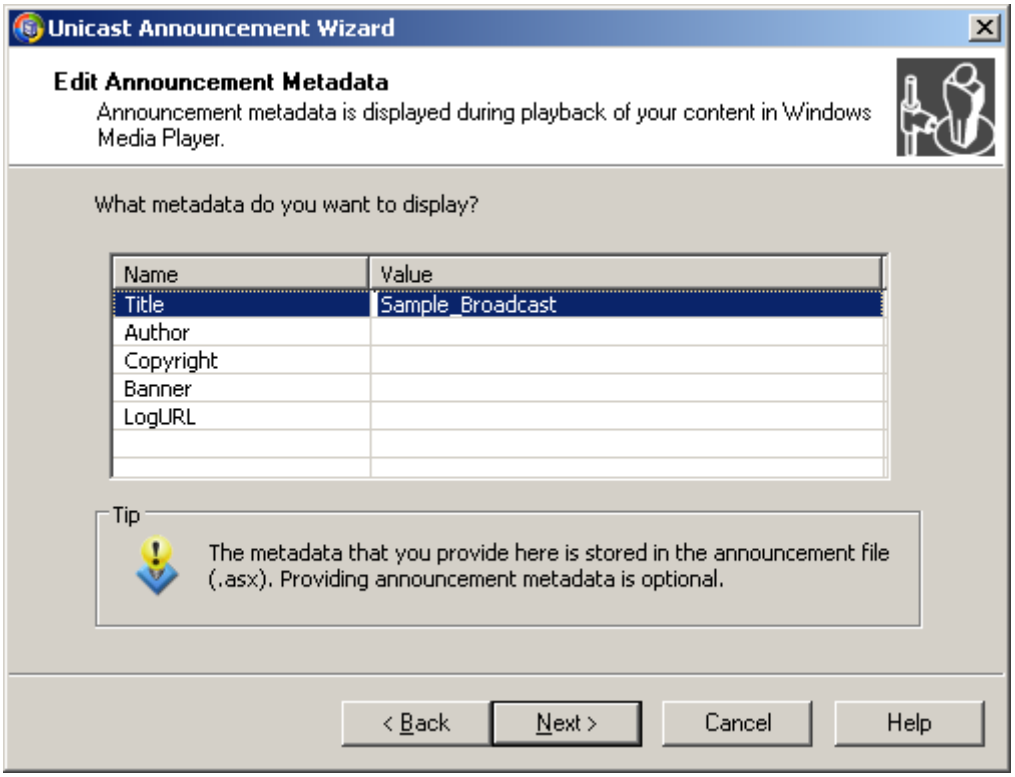
در صفحه باز شده، سیستم به شما می‌گوید که Clientها دسترسی به محتوا، بایستی چه آدرسی را وارد کنند. جهت تغییر آدرس روی دکمه Modify کلیک کنید. اما توصیه می‌کنم که این آدرس را عوض نکنید. برای رفتن به صفحه بعد، روی Next کلیک نمایید.



در صفحه بعد گزینه Create as Web page... را تیک بزنید. با این کار یک صفحه Web با پسوند htm ایجاد می‌شود که کاربران با باز کردن آن قادر به مشاهده قطعات صوتی/تصویری خواهند بود. گزینه اول یعنی Announcement file نیز یک فایل با پسوند.asx ایجاد می‌کند که حاوی اطلاعات در مورد فایل Announce یا آگهی خواهد بود. این فایل زمانی برای کاربر پخش می‌شود که هیچ فایل در حال حاضر بر روی سرور در حال پخش نباشد.



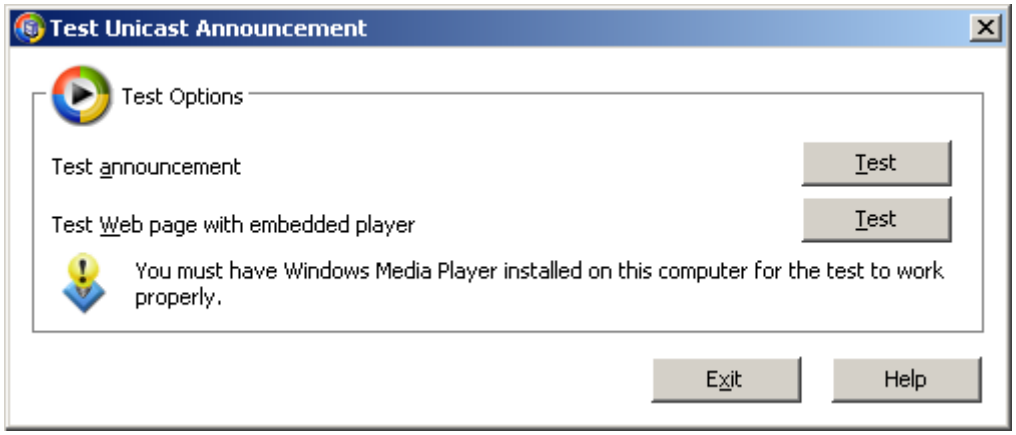
در صفحه بعد می‌توانید تعدادی Metadata در مورد فایل‌های صوتی/تصویری وارد نمایید. اطلاعاتی از قبیل عنوان، مولف، حق کپی، بنر و.... این اطلاعات در پخش کنندهها در Client قابل مشاهده خواهند بود. برای رفتن به صفحه بعد، بر روی Next کلیک کنید.



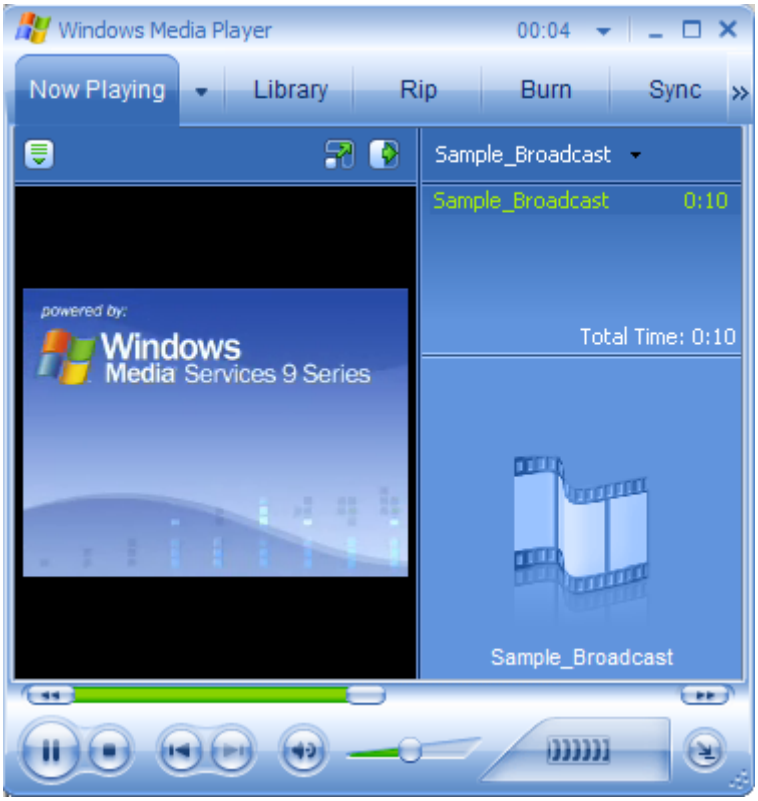
در نهایت، کار به اتمام رسیده و خلاصه‌ای از کار را می‌توانید مشاهده نمایید. جهت تست کارهای انجام شده، گزینه Test files when this wizard finished را تیک زده و روی Finish کلیک کنید.



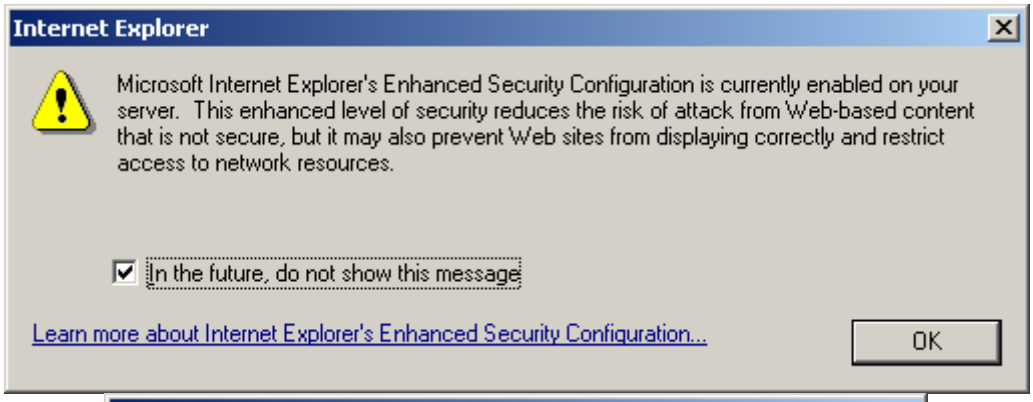
با این کار صفحه زیر باز می‌شود:

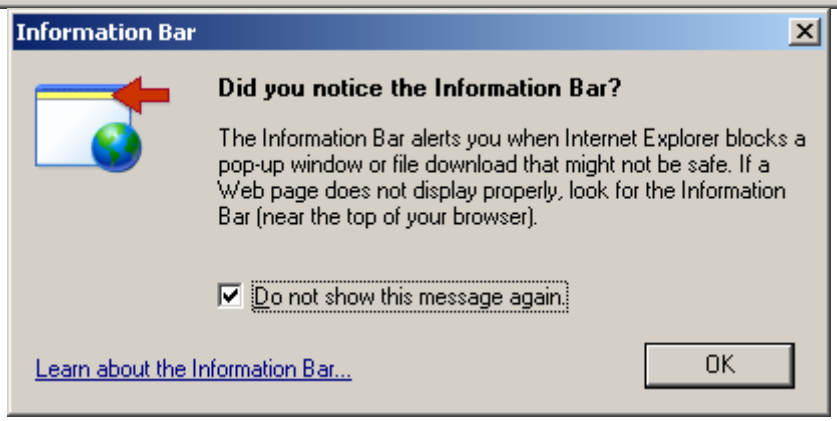


اگر روی دکمه Test که مقابل Test announcement قرار دارد کلیک کنید، Windows Media Player باز شده و یک قطعه تصویری مشاهده خواهد نمود.



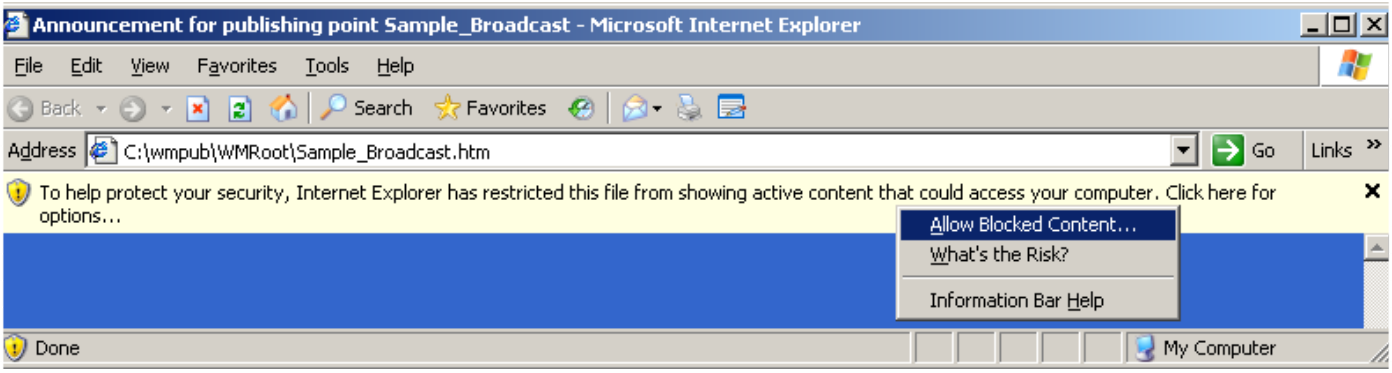
اما اگر روی دکمه Test که مقابل Test web page... قرار دارد کلیک کنید، مرورگر IE جهت نمایش یک قطعه تصویری باز می‌شود. در ابتدا پیغام‌های زیر را مشاهده خواهید نمود. مانند زیر عمل کنید:



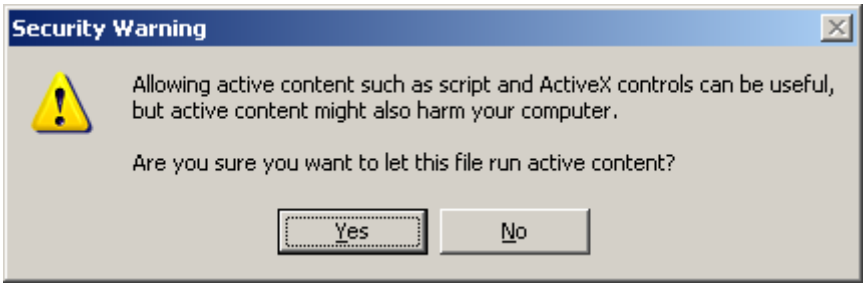


سپس باید به IE بگویید که اجازه پخش را به Windows media player ActiveX بدهد.

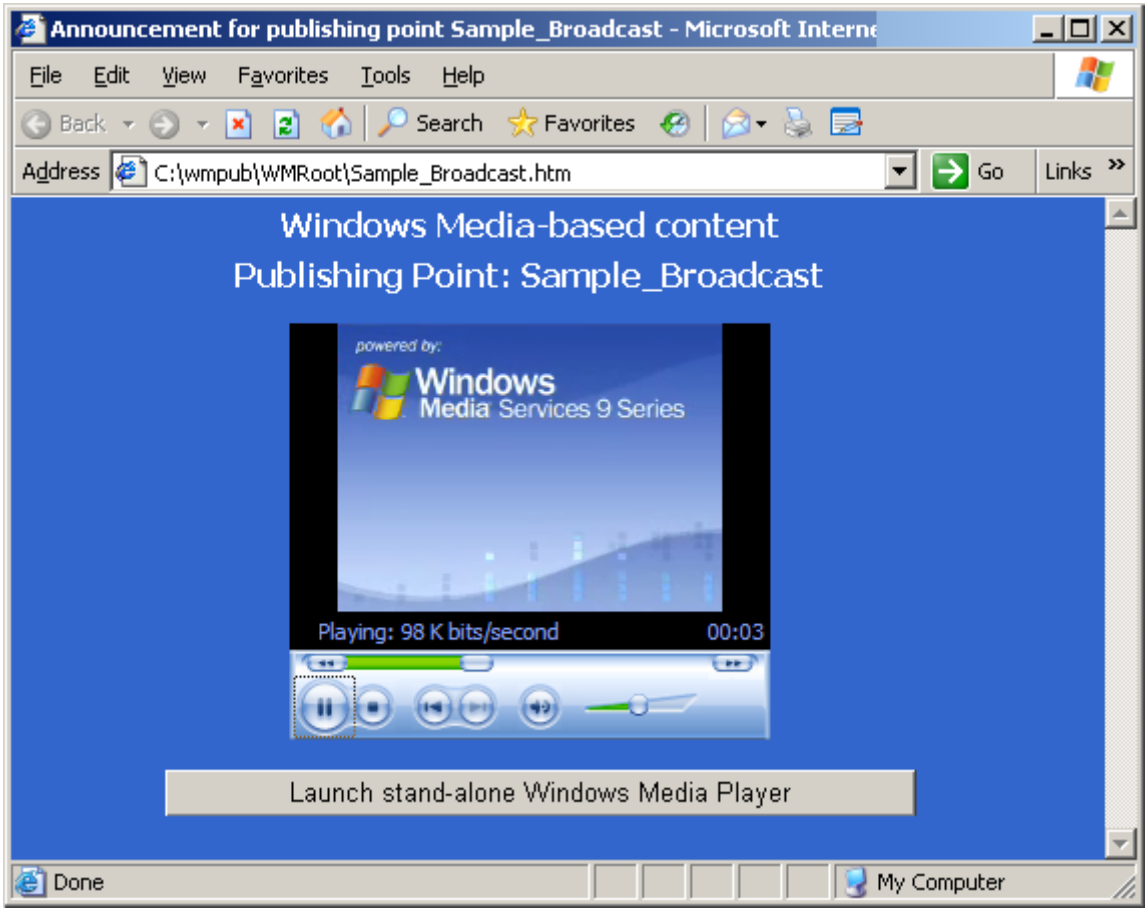
لذا بر روی نوار زرد رنگ بالای صفحه کلیک نموده و گزینه Allow Blocked Content را انتخاب نمایید.



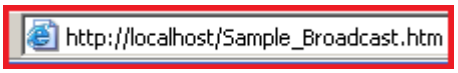
سیستم از شما سوالی خواهد پرسید، Yes را انتخاب کنید.



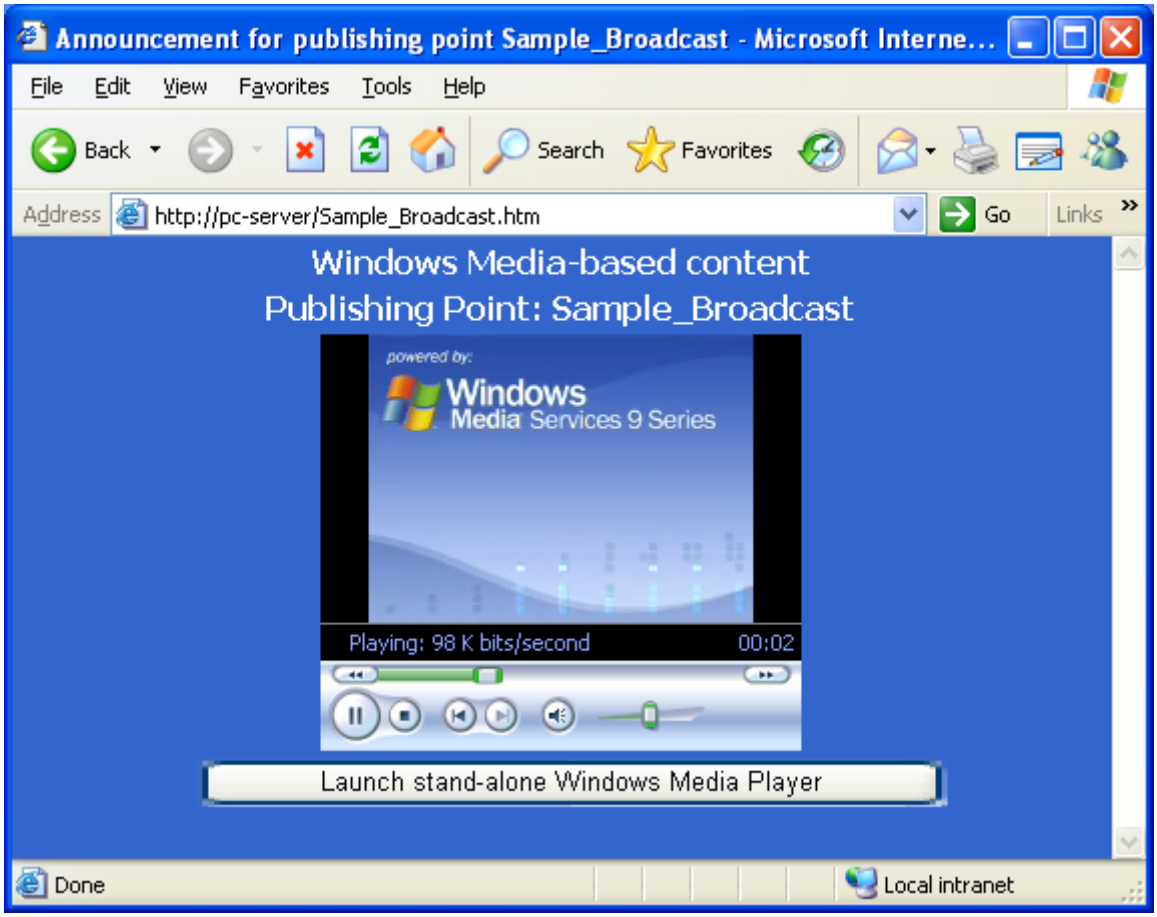
با اینکار خواهید دید که مرورگر، قطعه تصویری را پخش می کند.



اگر فایل را پخش نکرد، همانطور که قبلا نیز ذکر شد، قسمت آدرس را عوض کرده و به جای مقدار PC-SERVER، مقدار localhost را وارد نموده و سپس Enter را فشار دهید.



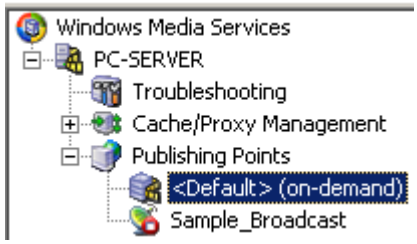
برای پخش قطعه تصویری در Client نیز وارد نرم‌افزار IE در Client شده و در قسمت آدرس، ابتدا نام پروتکل، سپس نام سرور و سپس نام Publishing Point را وارد نمایید. مانند شکل زیر:



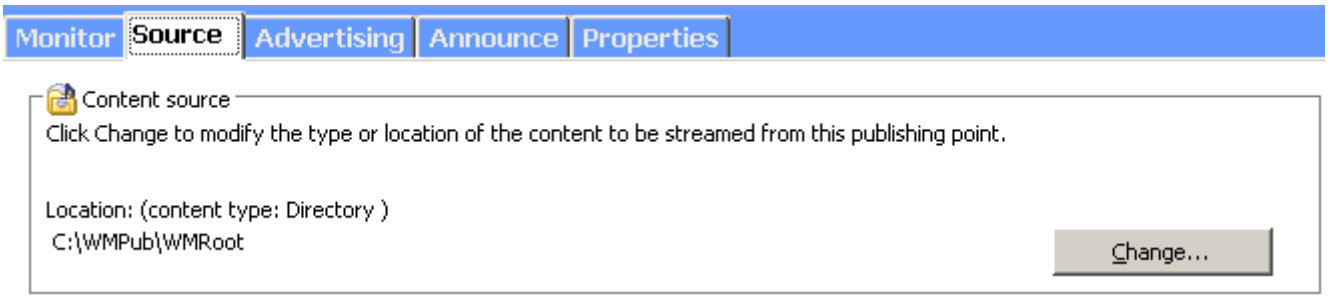
با کلیک روی دکمه Launch stand-alone Windows Media Player، نرم‌افزار Windows Media Player جهت پخش همین فایل باز خواهد شد.

۳۷-۵- روش On-Demand

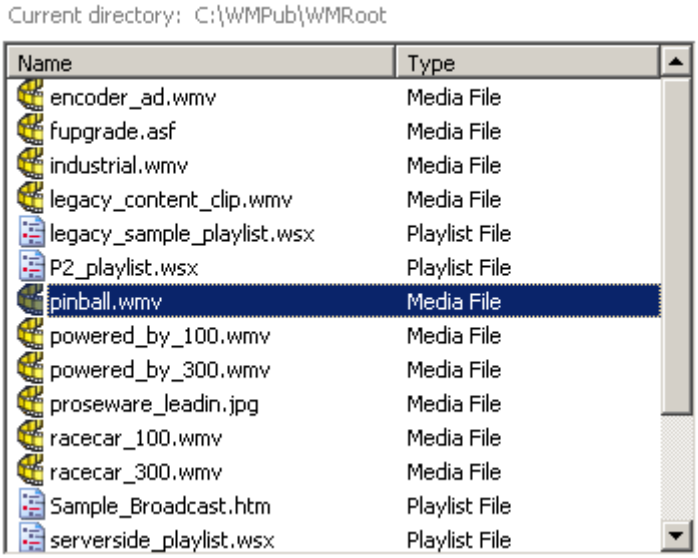
روش On-Demand شباهت‌های زیادی با روش Broadcast دارد. تنها تفاوت در این است، که کاربر در صورت نیاز، می‌تواند نام فایلی خاص را جهت پخش انتخاب نماید و اگر فایلی را انتخاب نکند، فایل Announce یا آگهی پخش خواهد شد. بدین منظور در صفحه اصلی نرم‌افزار Windows Media Service گزینه (On-Demand) <Default> را انتخاب کنید.



سپس وارد سربرگ Source شوید. قسمت Content Source، محل فایل‌های صوتی/تصویری در آن Publishing Point را نشان می‌دهد. اگر می‌خواهید این مسیر را عوض کنید، روی دکمه Change کلیک کنید. تصویر زیر نشان می‌دهد، که فایل‌های موجود در مسیر C:\WPub\WMRoot قرار دارند.



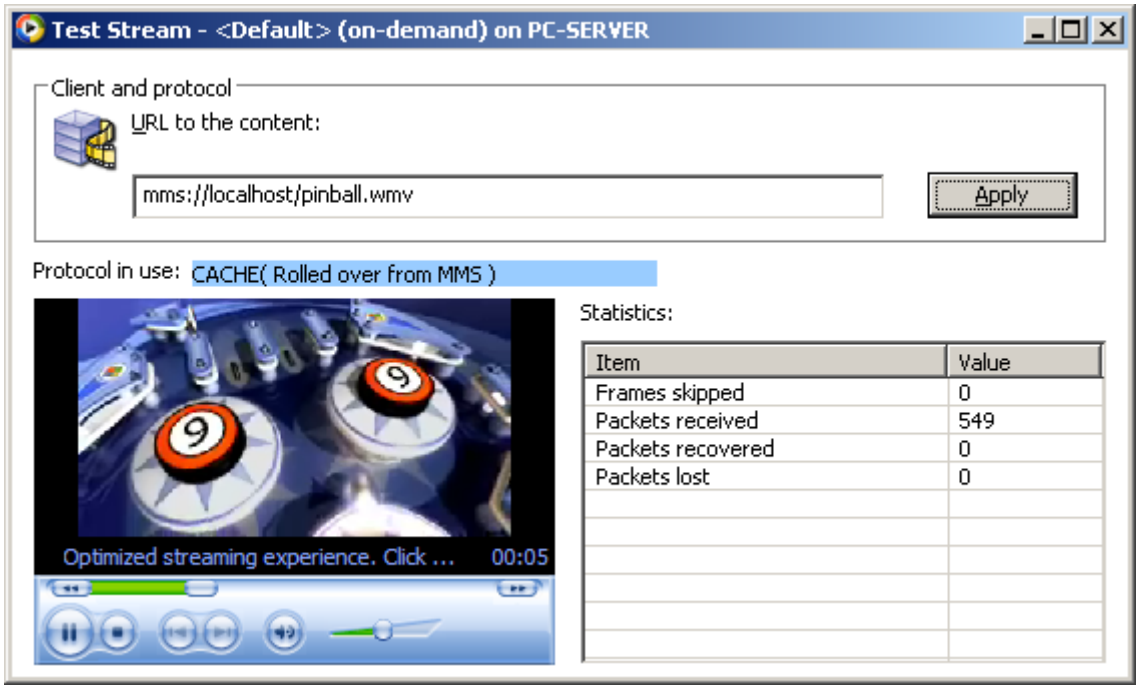
قسمت پایین همین سربرگ، لیستی از فایل‌های موجود در پوشه‌ای که در قسمت بالا مشخص کردیم را نشان می‌دهد.



اگر می‌خواهید کاری که تا کنون انجام داده‌اید را تست کنید، روی دکمه زیر کلیک کنید:

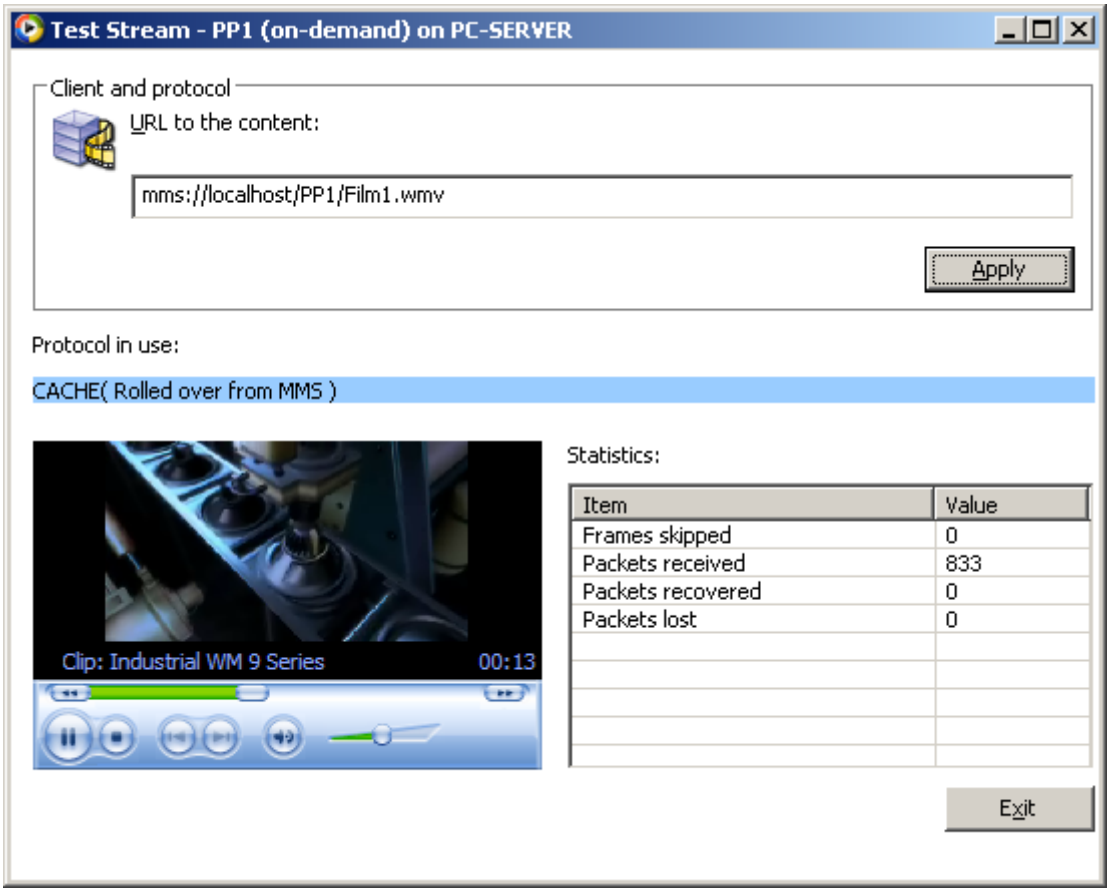


با این کار، صفحه پخش باز می‌شود. همانطور که می‌بینید، من آدرس PC-SERVER را به localhost تغییر داده ام.



همانطور که در شکل فوق می‌بینید، ما ابتدا نام پروتکل (mms)، سپس نام سرور (localhost) و سپس نام فایل را (pinball.wmv) وارد کرده‌ایم. در این آدرس‌دهی، خبری از نام Publishing Point نیست، دلیل نیز این است که ما در قسمت پیش فرض ((On-Demand) <Default>) هستیم و نیازی به آدرس Publishing Point نیست. اما اگر یک Publishing Point جدید ساختیم، بایستی نام آن را نیز وارد نماییم. مثلا در شکل زیر، ما یک Publishing Point جدید با نام PP1 ساخته‌ایم که از آنجایی که PP1، یک Publishing Point پیش فرض نیست، بایستی نام آن در آدرس بیاید.

در تصویر زیر مشخص است که فایل Film1.wmv در حال پخش می‌باشد.



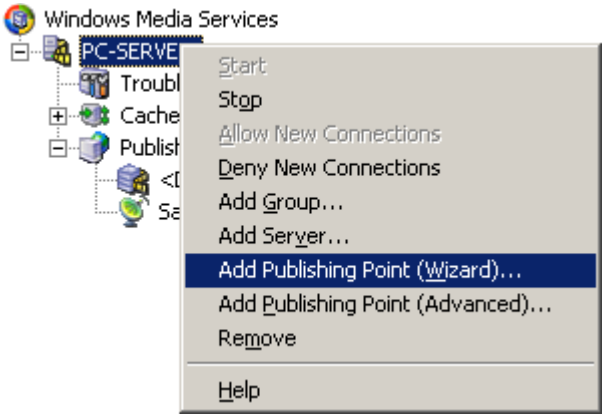
Clientها نیز جهت پخش این فیلم بایستی آدرس mms://PC-Server/PP1/wmv را وارد نمایند.

نکته: سایر کارها و تنظیمات روش On-Demand، شبیه روش Broadcast است که قبلا در مورد آن صحبت شده است. لذا مجددا از ذکر آن‌ها خودداری می‌کنیم.

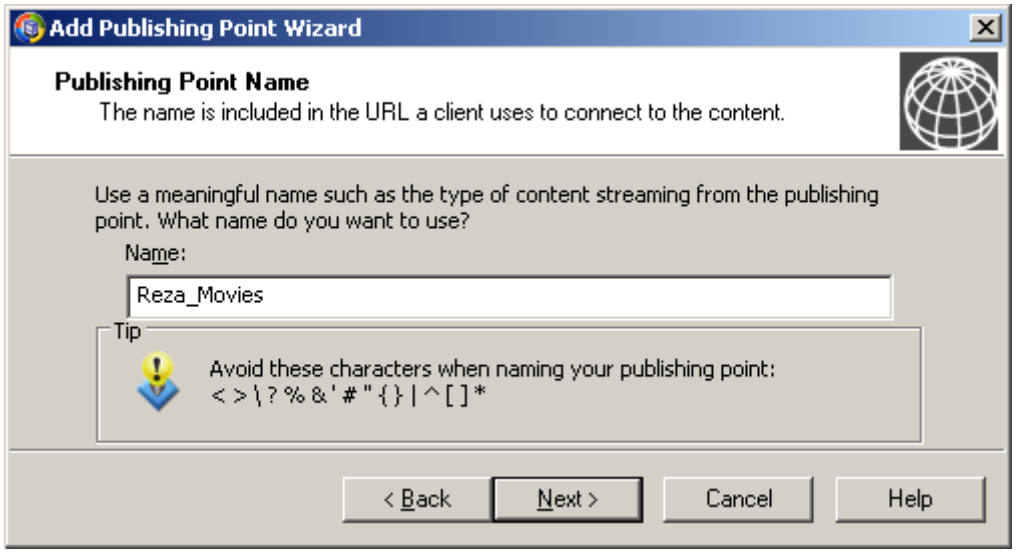
۳۷-۶- ایجاد Publishing Point جدید

فکر می‌کنم تا کنون مفهوم Publishing Point یا نقطه انتشار را متوجه شده باشد. Publishing Point یک نقطه مرکزی است که می‌توان با اتصال به آن، قطعات صوتی و تصویری درون آن را مشاهده نمود. Publishing Point به دو نوع کلی Broadcast و On-Demand تقسیم می‌شود که تفاوت این دو را در بالا ذکر نموده ام.

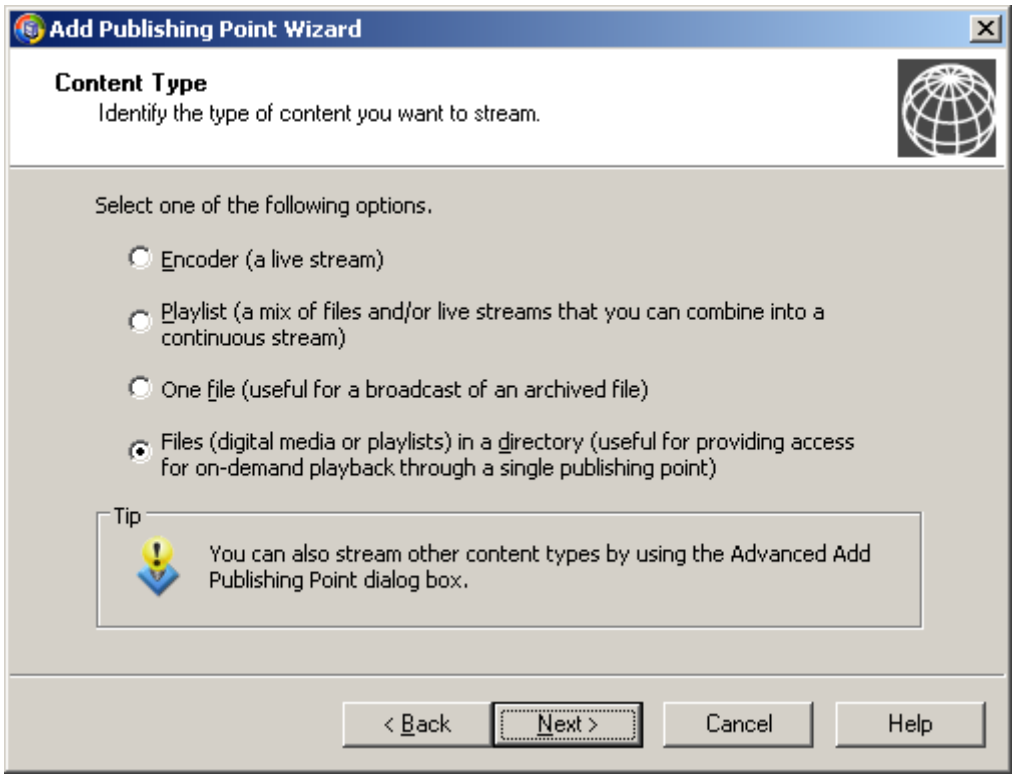
جهت ساخت Publishing Point جدید، ابتدا روی نام سرور راست کلیک نموده و سپس گزینه Add Publishing Point (Wizard) را انتخاب نمایید.



در صفحه باز شده و در قسمت Name، یک نام برای Publishing Point انتخاب نمایید.



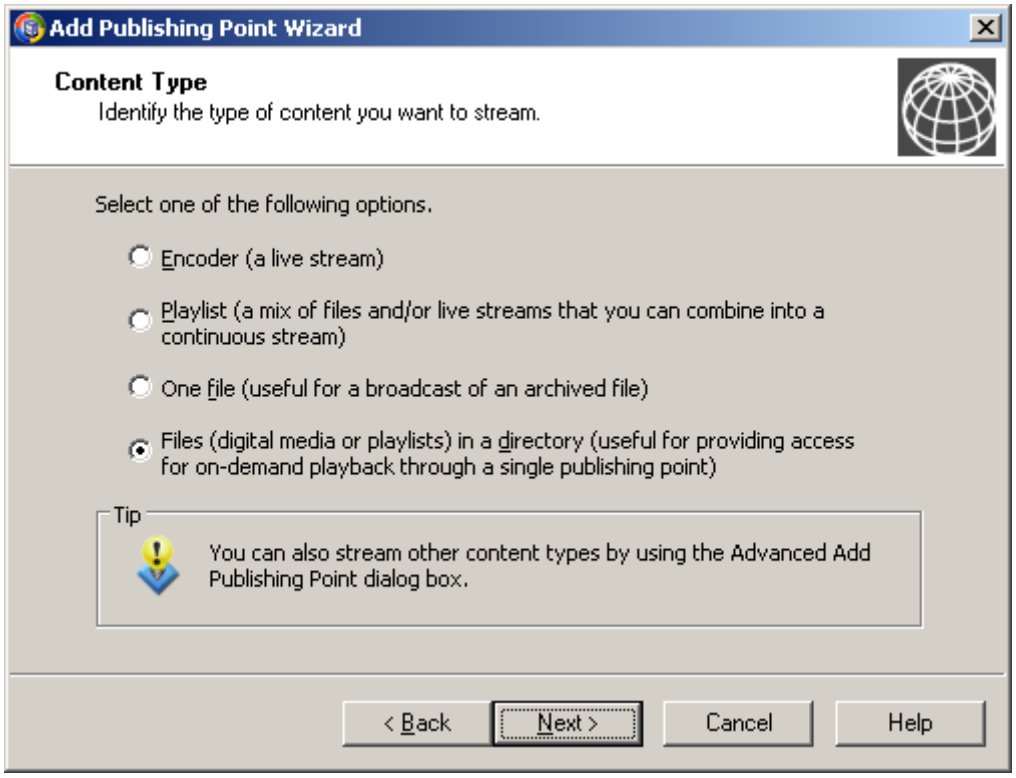
سپس در صفحه بعد نوع Publishing Point را انتخاب نمایید.



این انواع به صورت زیر است:

- **گزینه ۱**، Encoder (a live stream): این گزینه که مربوط به بحث ما نمی‌شود، سروری را جهت انجام عملیات Encoding تعیین می‌کند. منظور از Encoding، همان Codec است.
- **گزینه ۲**، Playlist: یک لیست پخش ایجاد نموده و قطعات صوتی/تصویری این لیست به ترتیب پخش می‌شود. در این روش، ما تنها یک Playlist با پسوند.wsx انتخاب می‌کنیم. فیلم‌های یک Playlist ممکن است در مکآن‌های مختلفی از کامپیوتر قرار داشته باشند و مجتمع نباشند.
- **گزینه ۳**، One file: از طریق این گزینه تنها می‌توان یک فایل را جهت انتشار انتخاب نمود. در این گزینه، چیزی به نام Playlist معنی ندارد.
- **گزینه ۴**، ...Files: همان چیزی است که تا کنون انجام می‌دادیم. در این روش، یک پوشه تعیین می‌شود و سپس قطعات صوتی/تصویری داخل آن، جهت پخش انتخاب می‌گردند.

لذا گزینه ۴ را انتخاب کرده و روی Next کلیک کنید.



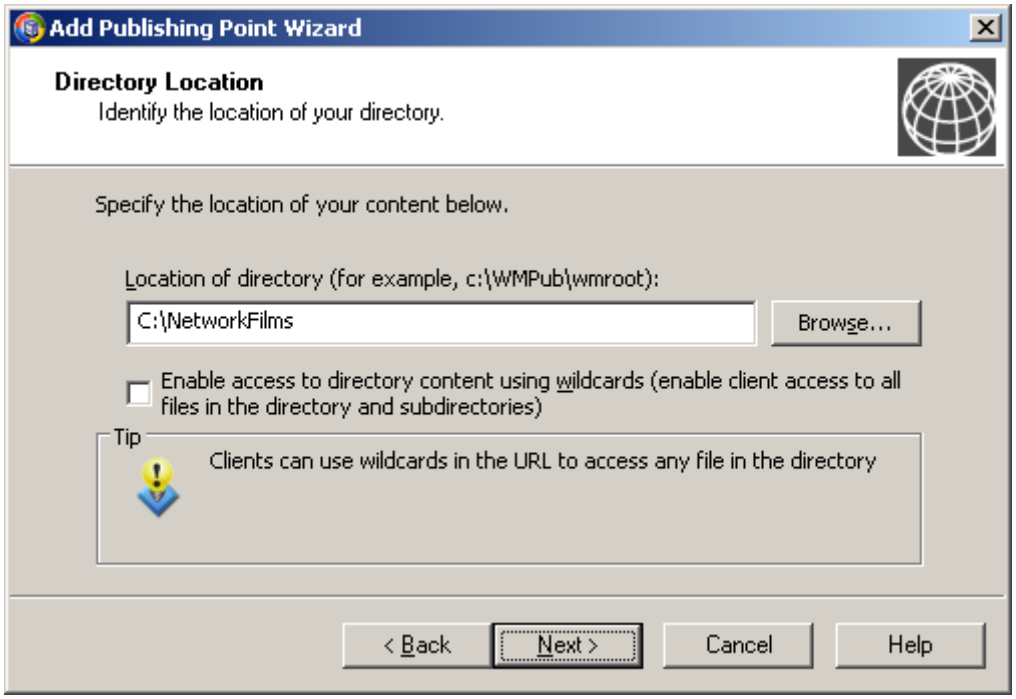
در صفحه بعد نحوه انتشار را انتخاب نمایید. نحوه انتشار می‌تواند به صورت Broadcast یا به صورت On-Demand باشد که تفاوت این دو را قبلا توضیح داده‌ایم.

گزینه On-Demand را انتخاب نموده و روی Next کلیک کنید.

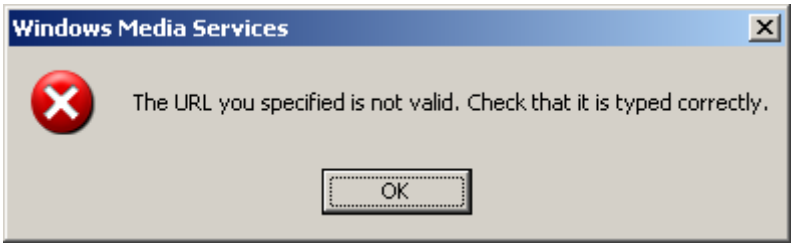
با این کار می‌گویید که کاربران از بین قطعات صوتی/تصویری موجود، هر کدام که نیاز دارند را انتخاب نموده و مشاهده نمایند.



در صفحه بعد، پوشه‌ای را انتخاب کنید، که می‌خواهید فایل‌های داخل آن پخش شود.

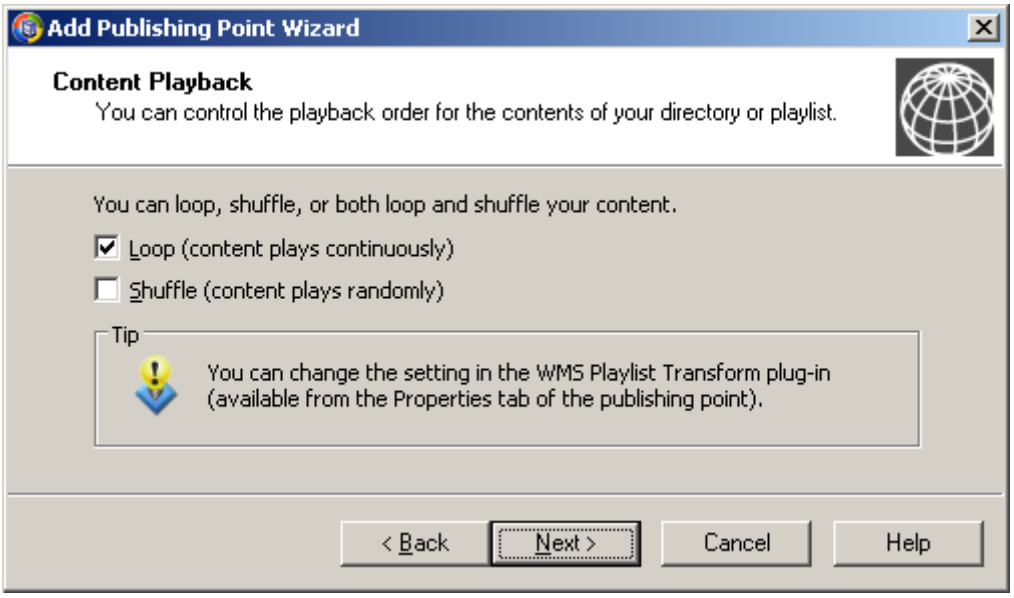


دقت فرمایید که پوشه از قبل وجود داشته باشد، زیرا در غیر اینصورت خطای زیر را مشاهده خواهید نمود:

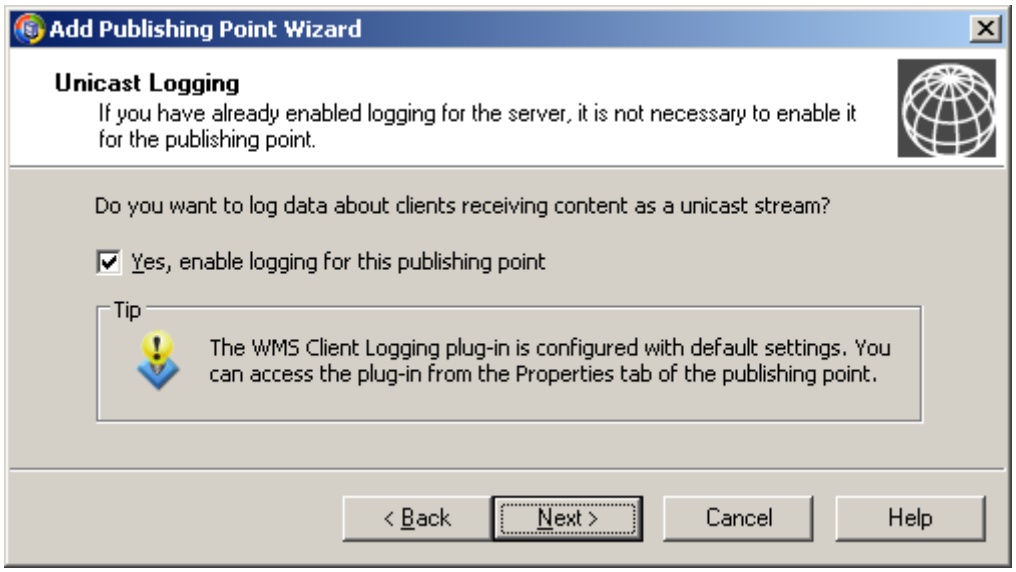


در صفحه بعد دو گزینه وجود دارد. گزینه اول، یعنی Loop می‌گوید که پس از اتمام یک قطعه صوتی/تصویری، مجددا همان قطعه پخش شود. گزینه Shuffle نیز می‌گوید که قطعات صوتی/تصویری، به ترتیبی که در لیست هستند، پخش نشوند؛ بلکه به صورت تصادفی پخش شوند.

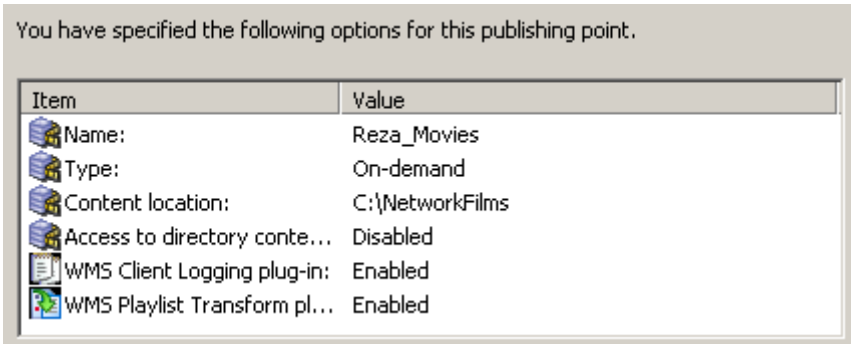
گزینه دلخواه را انتخاب نموده و روی Next کلیک کنید.



در صفحه بعد، اگر تیک گزینه Yes... را بزنید، به سیستم می‌گویید که رفتار کاربر را Logگیری کرده تا رفتارهای وی، در زمان مورد نیاز باشد قابل پیگیری باشد.

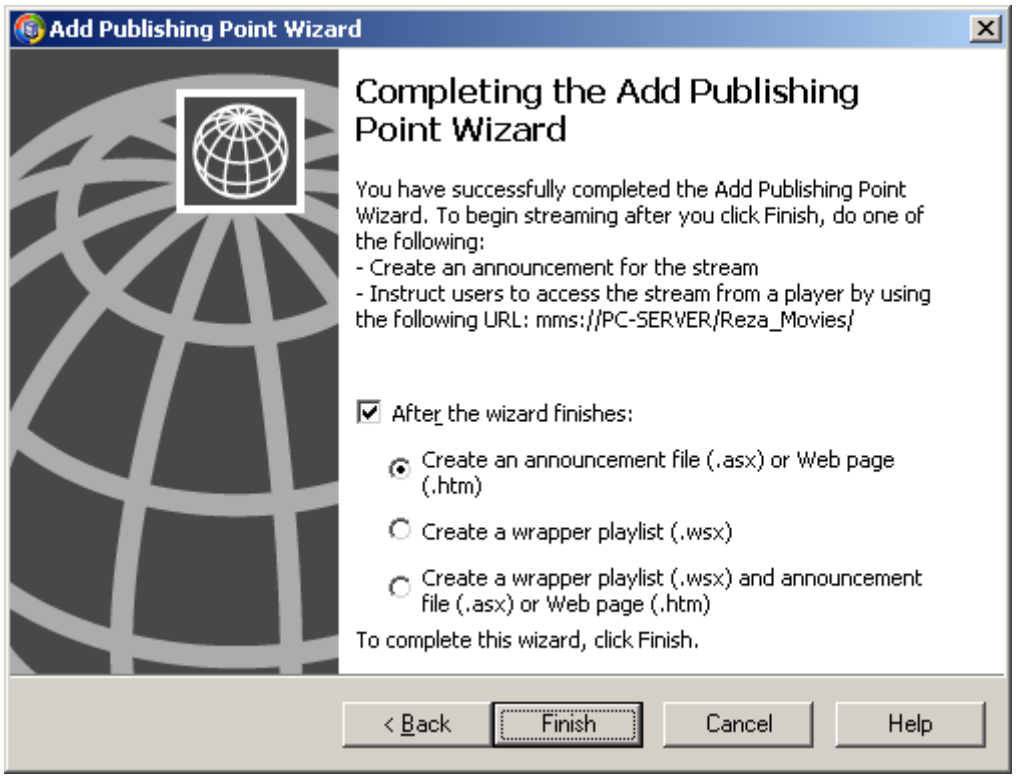


در صفحه بعد، خلاصه‌ای از کارهای انجامی را مشاهده خواهید نمود. روی Next کلیک کنید.



در پایان، صفحه پایان نصب را مشاهده خواهید نمود. در این صفحه اگر گزینه After the wizard finishes را انتخاب کنید، ۳ گزینه فعال می‌شود که معانی زیر را دارند:

- **گزینه ۱**، (.asx و.htm): با این انتخاب این گزینه، می‌توانید پس از نصب یک فایل Announce یا آگهی و یک صفحه وب جهت دسترسی به فایل‌های صوتی/تصویری ایجاد کنید.
- **گزینه ۲**، (.wsx): با این انتخاب این گزینه، می‌توانید پس از نصب یک فایل Playlist جهت نگهداری نام فایل‌های قابل پخش ایجاد کنید.
- **گزینه ۳**، (.wsx و.htm): با این انتخاب این گزینه، می‌توانید پس از نصب یک فایل Playlist و یک صفحه وب جهت دسترسی به فایل‌های صوتی/تصویری ایجاد کنید.



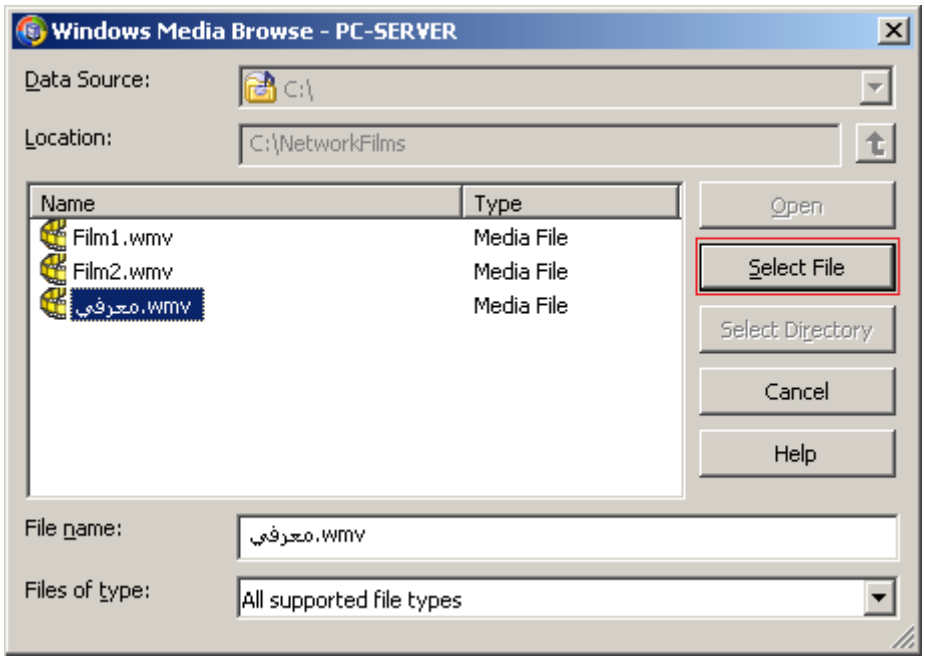
اگر گزینه ۱ را انتخاب کنید، با کلیک روی دکمه Finish، صفحه ساخت فایل آگهی و فایل صفحه وب باز می‌شود. روی Next کلیک کنید.



در مرحله بعد، بایستی فایلی را به عنوان فایل آگهی انتخاب کنید. لذا روی دکمه Browse کلیک کنید.



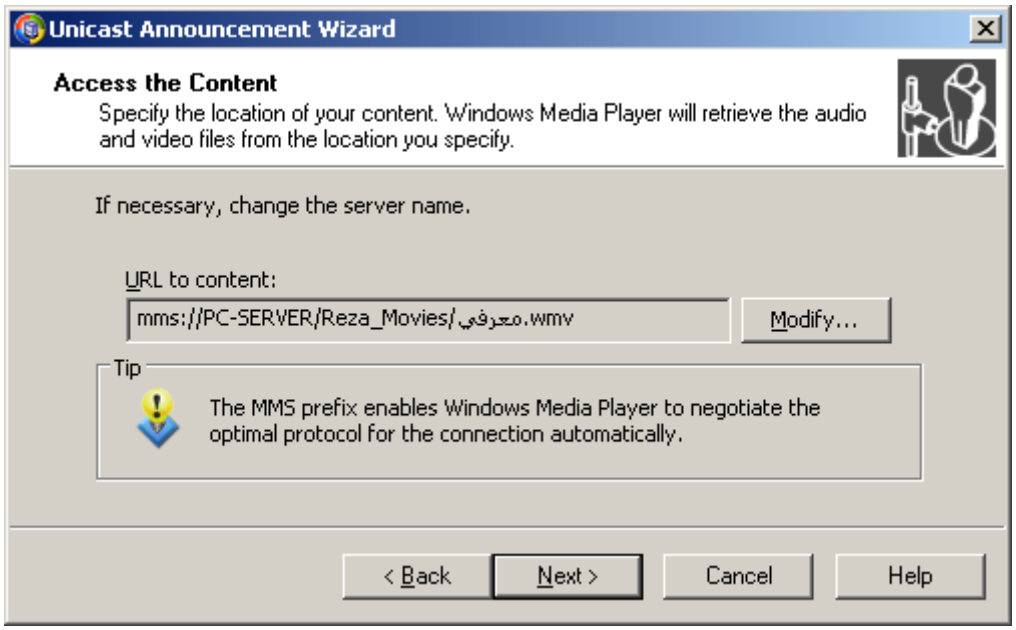
در صفحه باز شده، یک فایل مناسب جهت آگهی انتخاب نموده و سپس روی Select File کلیک کنید.



سپس نام و مسیر فایل خود را مشاهده خواهید نمود. روی Next کلیک کنید.

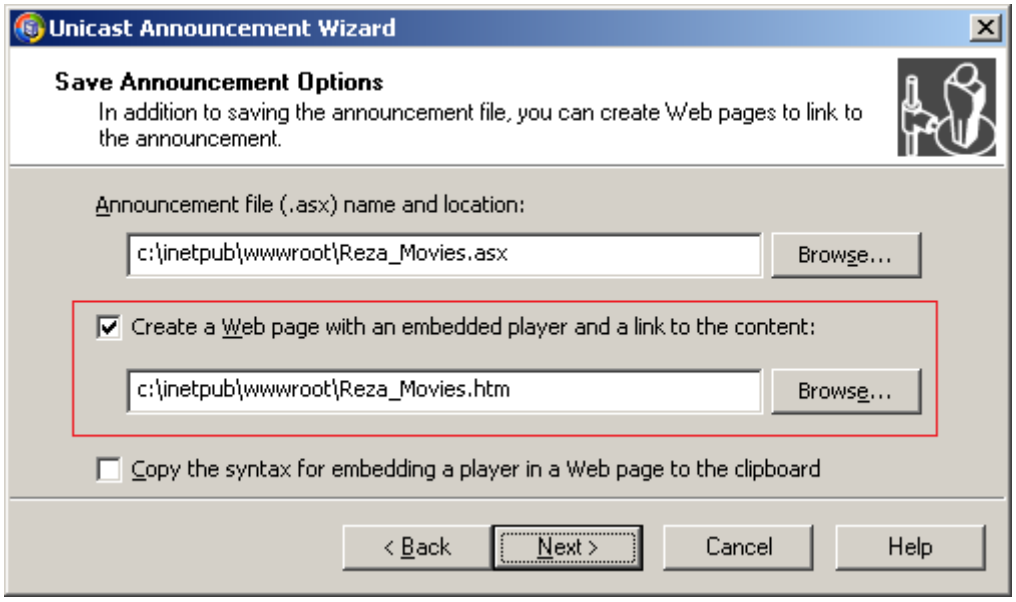


در صفحه بعد، مسیری که از طریق آن، Clientها می‌توانند فایل آگهی را ببینند مشاهده می‌نمایید. با کلیک روی دکمه Modify می‌توانیدای مسیر را عوض کنید. اما توصیه می‌کنم که این کار را انجام ندهید. روی Next کلیک کنید.

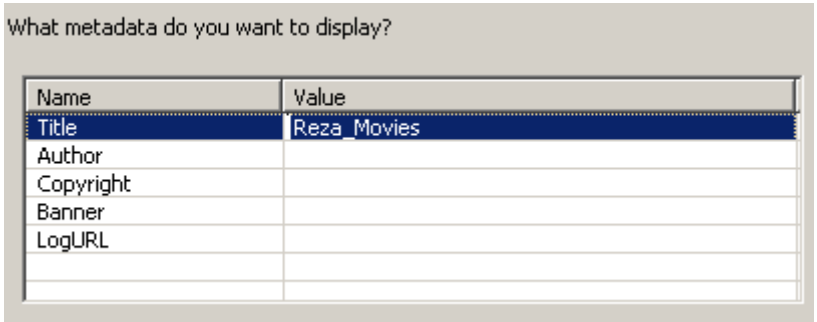


در صفحه بعدی، گزینه اول، مسیر فایل Announce که پسوند.asx دارد را نشان می‌دهد.

سپس گزینه دوم را فعال نمایید. این گزینه محل ذخیره فایل صفحه وب جهت دسترسی Clientها را مشخص می‌کنند. اگر می‌خواهید Clientها بتوانند از راه دور و از طریق مرورگر دسترسی یابند، این فایل بایستی در مسیر C:\inetpub\wwwroot\ ذخیره گردد. در نهایت روی Next کلیک کنید.



سپس می‌توانید Metadataهایی را همچون عنوان، مولف، حق نشر و... را تعیین نمایید.



در نهایت، صفحه اتمام کار را می‌بینید. اگر تیک گزینه Test files when this wizard finishes را بزنید، پس از پایان نصب، صفحه تست کارهای انجام شده باز خواهد شد. روی Finish کلیک کنید.

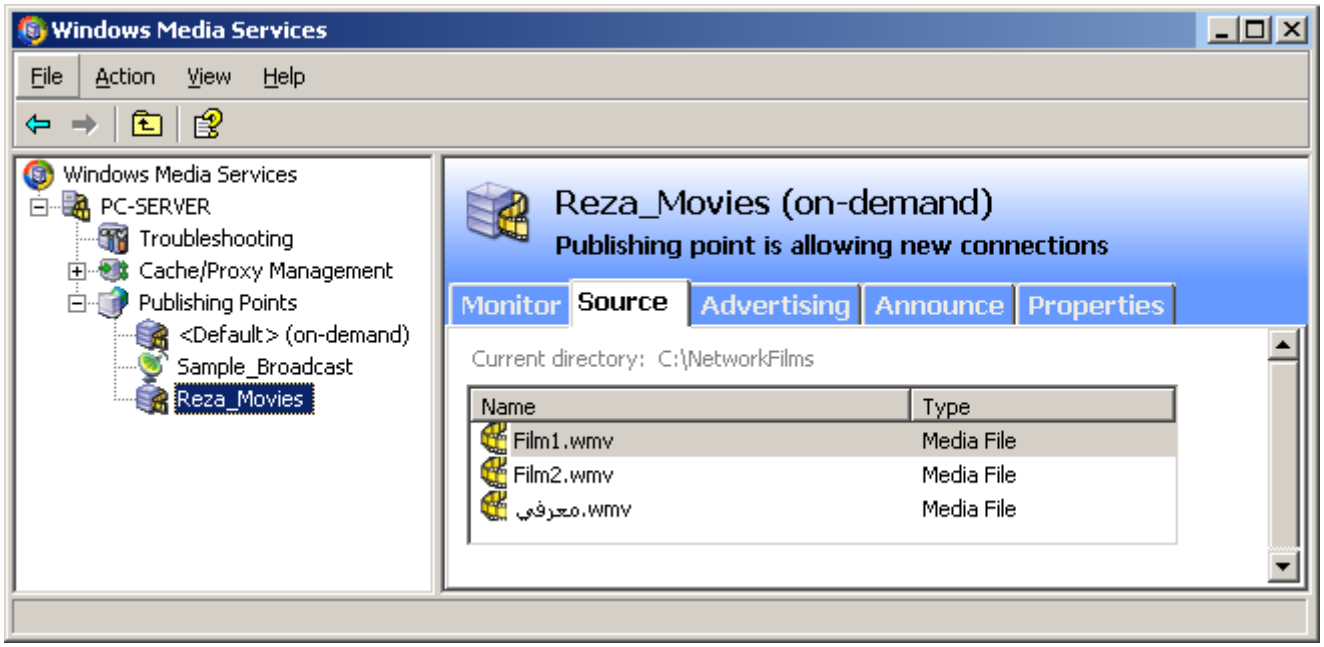
در مورد صفحه تست، قبلا صحبت کرده‌ایم. فقط جهت یادآوری مجدد بیان می‌کنم که صفحه تست، پخش فایل‌های صوتی/تصویری را توسط Windows Media Player و Internet Explorer مورد بررسی قرار می‌دهد.



جهت استفاده از این Publishing Point، در Client آدرس زیر را وارد نمایید:

mms://PC-SERVER/Reza_Movies/نام فایل

سپس Publishing Point ساخته شده که Reza_Movies نام دارد را انتخاب کرده و وارد سربرگ Source شوید. بدین ترتیب فایل‌های قابل پخش را مشاهده خواهید نمود.



Client جهت مشاهده این فایل‌ها، بایستی یکی از آدرس‌های زیر را در Windows Media Player خود وارد نماید:

mms://PC-SERVER/Reza_Movies/Film1.wmv
mms://PC-SERVER/Reza_Movies/Film2.wmv
mms://PC-SERVER/Reza_Movies/معرفی.wmv

فصل ۳۸

نصب و راه اندازی سرور سایت (IIS)

۳۸-۱- معرفی IIS

مسلما تا کنون در ویندوز برنامه‌های اجرایی با پسوند exe را اجرا کرده‌اید. اجرای این نوع برنامه‌ها به سادگی و با رو بار کلیک کردن روی آن‌ها انجام می‌گیرد. اما آیا تاکنون به این فکر افتاده‌اید که چگونه می‌توان وب سایت‌های تولید شده با تکنولوژی ASP.Net را بدون کمک Microsoft Visual Studio اجرا کرد؟ ویندوز، سرویسی به نام "سرویس اطلاعاتی اینترنت" یا به اختصار IIS (Internet Information Service) دارد که سرویس هایی جهت انجام امور ارتباطی برای شما فراهم می‌کند که از جمله آن‌ها، امکان راه اندازی وب سایت است.

برخی سرویس‌های IIS عبارتند از:

۱. **HTTP (Hyper Text Transfer Protocol):** توسط این سرویس می‌توانید وب سایت‌های خود را اجرا کرده و آن‌ها را مشاهده نمایید.
۲. **FTP (File Transfer Protocol):** این سرویس، خدمات انتقال فایل را ارائه می‌کند.
۳. **SMTP (Simple Mail Transfer Protocol):** این سرویس، خدمات ارسال ایمیل را ارائه می‌کند.
۴. **NNTP (Network News Transfer Protocol):** این سرویس خدمت ایجاد گروه‌های خبری و شرکت کاربران در مباحث گفتگویی را فراهم می‌کند.

در این فصل فقط به معرفی پروتکل HTTP و تنظیمات آن می‌پردازیم.

۳۸-۲- نصب IIS

جهت نصب IIS، دو روش وجود دارد که شخصا روش اول را بیشتر ترجیح می‌دهم. البته روش دوم امکانات بیشتری را در اختیار قرار می‌دهد.

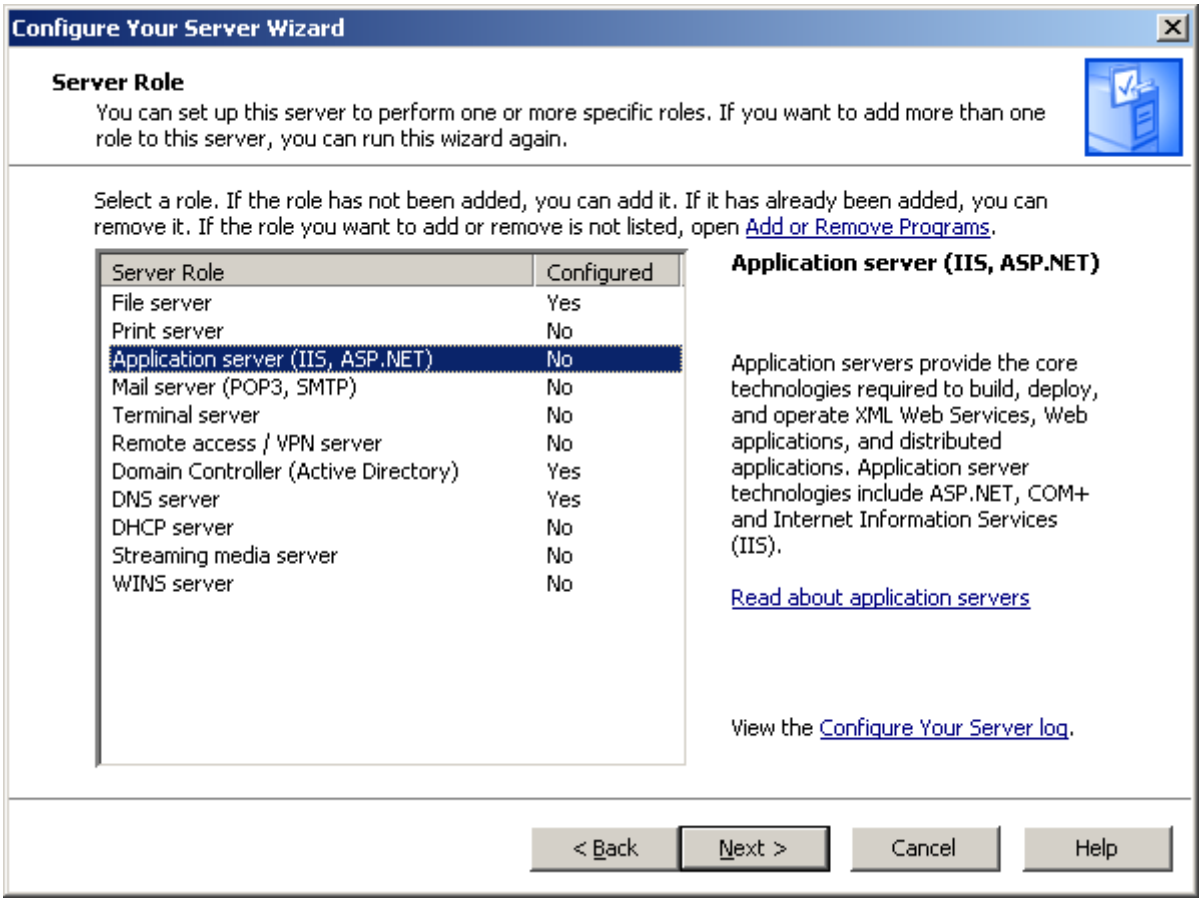
روش اول: بدین منظور ابتدا از مسیر Start ➔ Administrative Tools برنامه Configure Your Server Wizard را اجرا کنید:



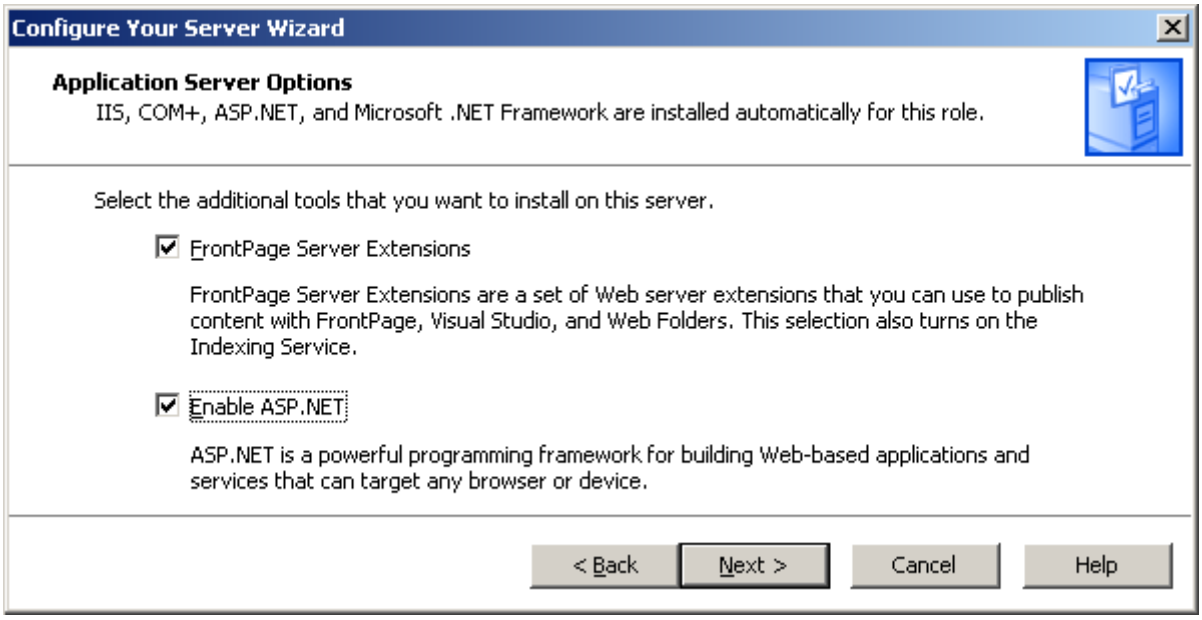
در صفحه باز شده دو بار Next را بزنید:



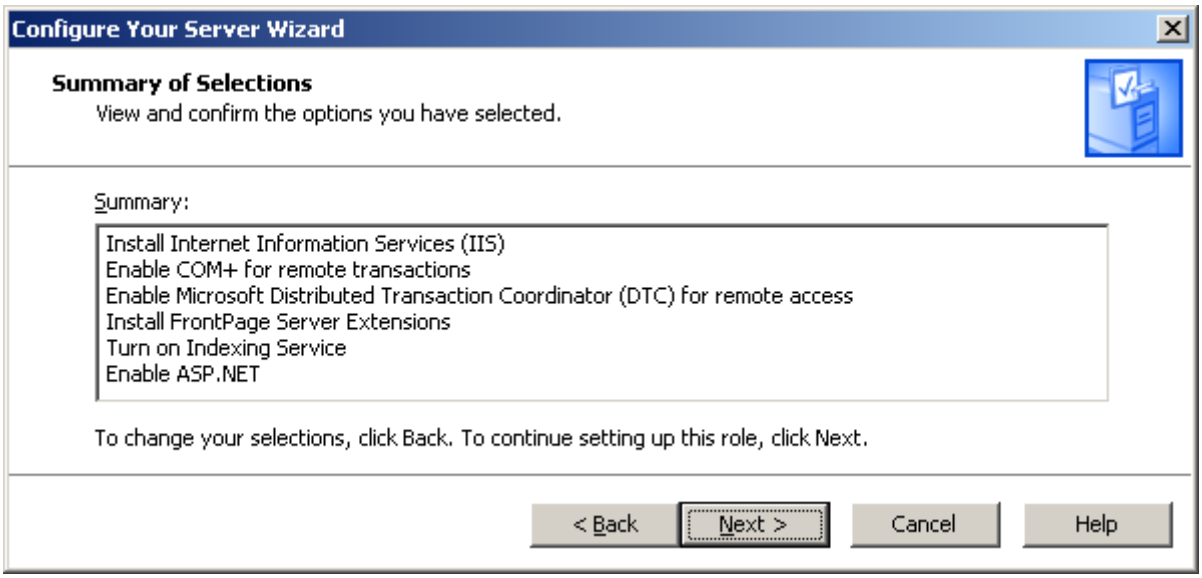
سپس در صفحه باز شده گزینه Application Server را انتخاب نمایید تا این نقش را به نقش‌های سرور اضافه کنید. سپس روی Next کلیک کنید.



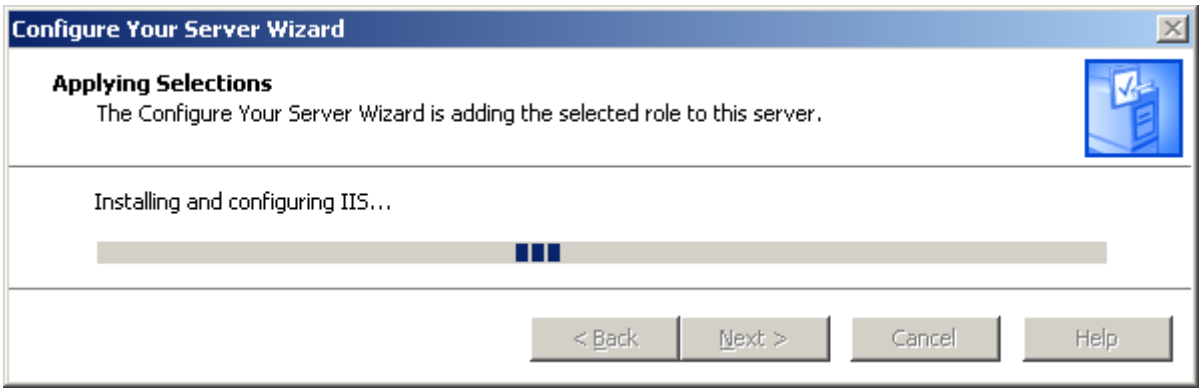
در صفحه بعد، هر دو گزینه FrontPage Server Extensions و Enable ASP.Net را فعال کرده و سپس روی دکمه Next کلیک کنید. دلیل فعال نمودن این دو گزینه این است که سرور بتواند افزونه‌های FrontPage و فایل‌های ASP.Net را به عنوان صفحات وب ترجمه نموده و اجرا نماید.



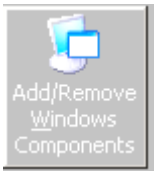
در پایان می‌توانید خلاصه‌ای از موارد قابل نصب را مشاهده کنید. جهت نصب روی Next کلیک کنید.



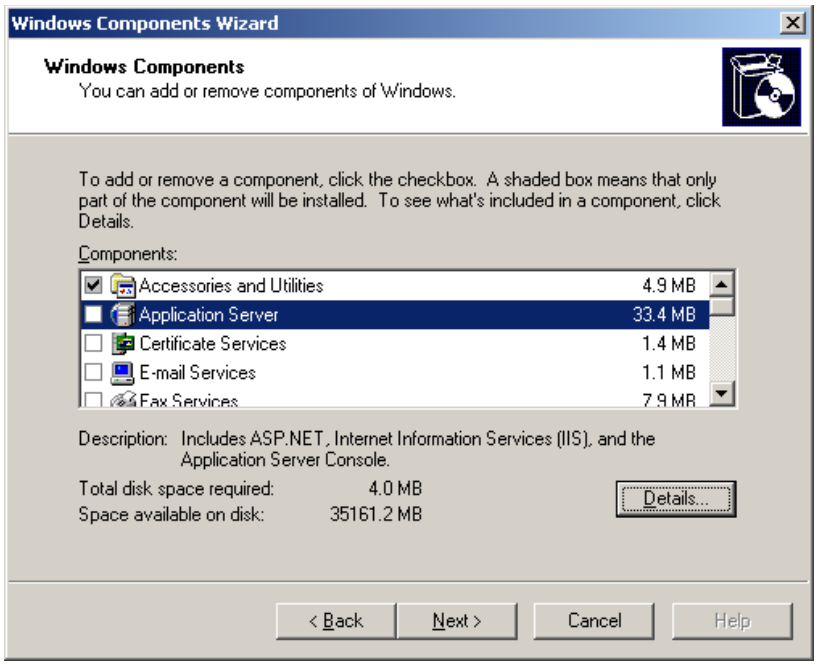
صبر نمایید تا عملیات نصب به پایان برسد. در نهایت روی Finish کلیک کنید.



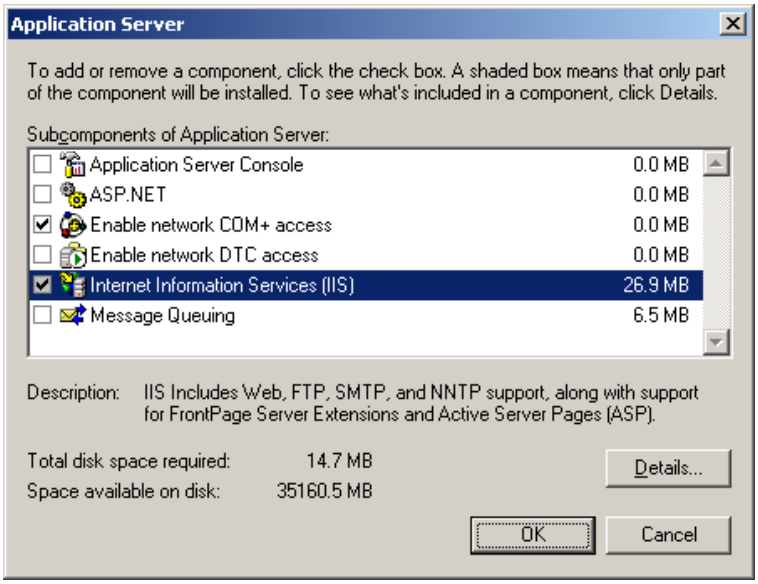
روش دوم: ابتدا وارد Control Panel ➔ Add/Remove Programs شده و سپس روی دکمه Add/Remove Windows Components کلیک کنید تا عناصر ویندوز را مشاهده نمایید.



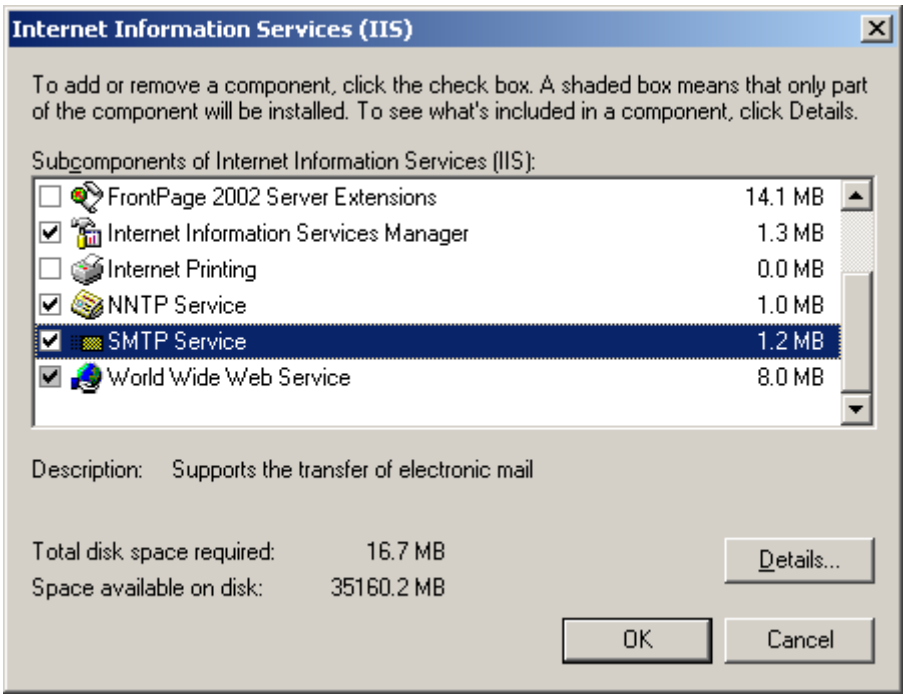
سپس در صفحه باز شده (مانند شکل زیر) گزینه Application Server را انتخاب کرده (توجه: تیک آن را فعال نکنید) و سپس روی دکمه Details کلیک کنید تا امکانات Application Server را مشاهده نمایید.



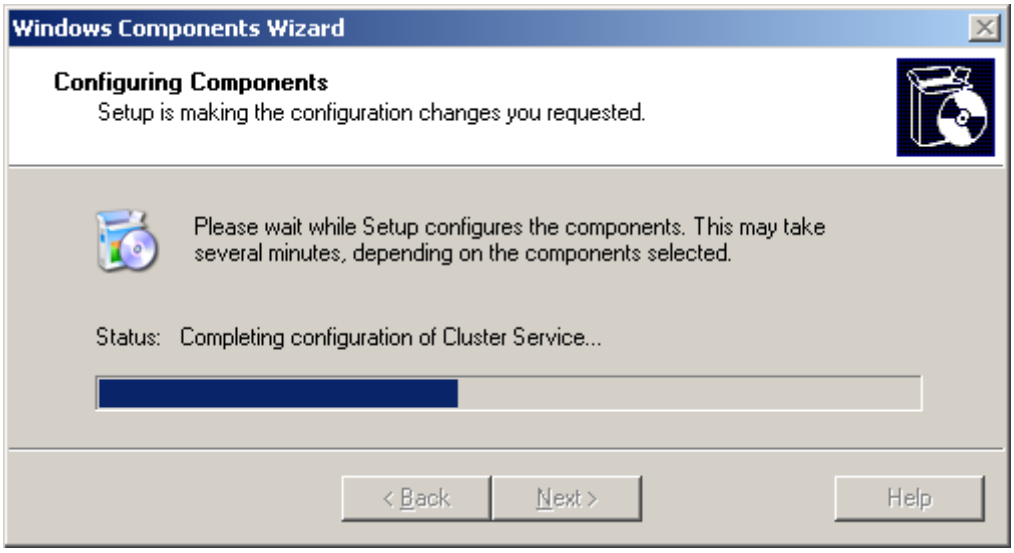
مجددا در صفحه باز شده تیک گزینه Internet Information Services (IIS) را فعال کرده و سپس روی دکمه Details کلیک کنید تا امکانات IIS را مشاهده کرده و آن‌ها را برای نصب انتخاب کنید.



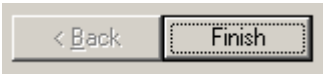
در صفحه باز شده، سرویس‌های مورد نظر را برای نصب انتخاب کنید. سعی کنید که هر ۴ سرویس معرفی شده در فوق (HTTP، FTP، SMTP و NNTP) را انتخاب و نصب نمایید. سپس روی OK کلیک کنید تا عملیات نصب شروع شود.



صبر نمایید تا عملیات نصب اتمام یابد. احتمالا در هنگام نصب به CD ویندوز نیاز خواهید داشت.



پس از نصب، روی دکمه Finish کلیک کنید تا عملیات نصب خاتمه یابد.

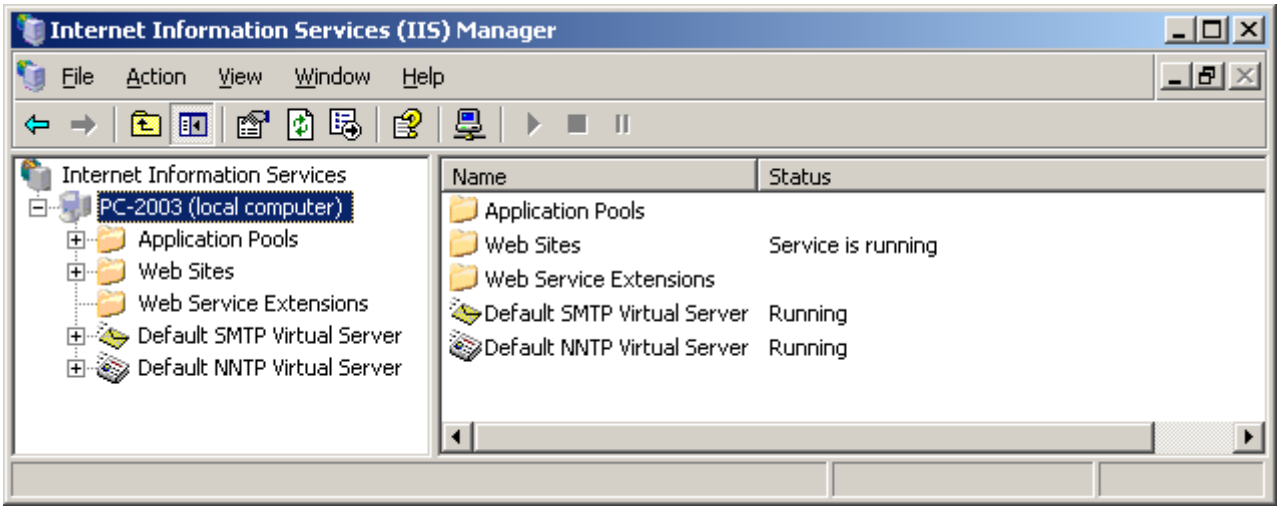


۳۸-۳- اجرا و پیکربندی IIS

جهت اجرای IIS، از مسیر Administrative Tools ➔ Start، گزینه Internet Information Service (IIS) Manager را انتخاب نمایید.

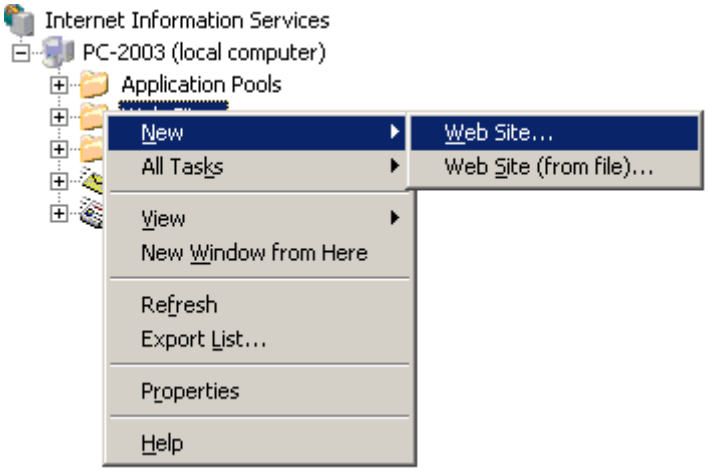


پس از اجرا، صفحه اصلی IIS را مشاهده می‌بینید که در سمت چپ، ابتدا نام سرور و سپس سرویس‌های نصب شده را مشاهده خواهید نمود. بخش Web Sites جهت راه اندازی وب سایت می‌باشد.



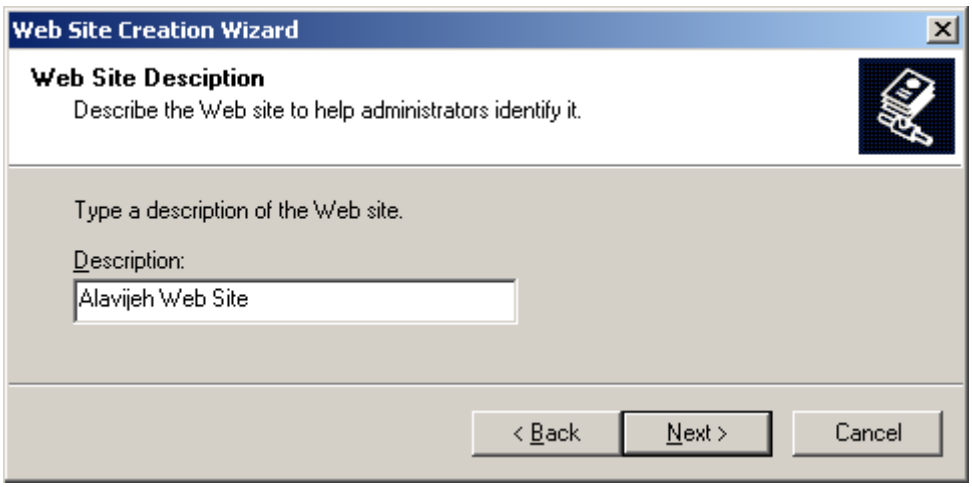
۳۸-۳-۱- تعریف Web Site جدید

جهت ایجاد وب سایت جدید، بر روی بخش Web Sites راست کلیک کرده و سپس گزینه New ➔ Web Site را انتخاب کنید.

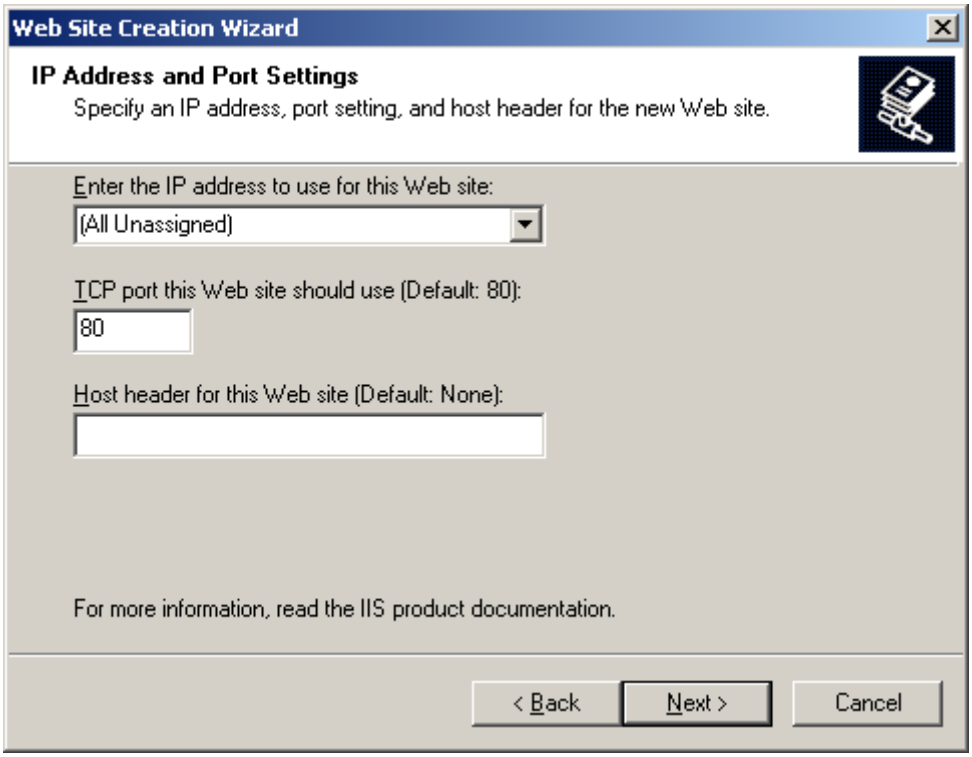


در صفحه خوش آمد گویی، Next را بزنید.

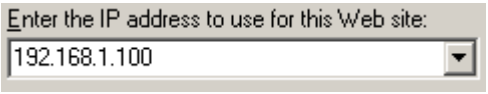
در صفحه بعد، یک **توصیف** (نه نام واقعی) برای وب سایت خود وارد نمایید. این توصیف برای راحتی شما در شناسایی وب سایت‌های موجود است.



در صفحه بعد، دو تنظیم مهم را باید انجام دهید. یکی آدرس IP است که برای این وب سایت استفاده می‌شود و به صورت پیش فرض این مقدار برابر All Unassigned است. یعنی با هر آدرس IP که روی سرور تنظیم شده باشد، می‌توان به وب سایت دسترسی داشت. و تنظیم دیگر، تنظیم پورت مورد استفاده وب سایت است. توجه نمایید که مقدار پورت‌ها به ازاء وب سایت‌های ایجاد شده، نباید با هم برابر باشد (توضیح در جلوتر).

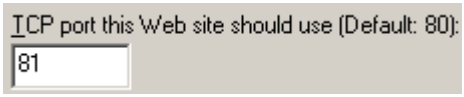


برای تنظیم اول، ما به جای گزینه All Unassigned، از آدرس IP تخصیص داده شده به سرور استفاده می‌کنیم.

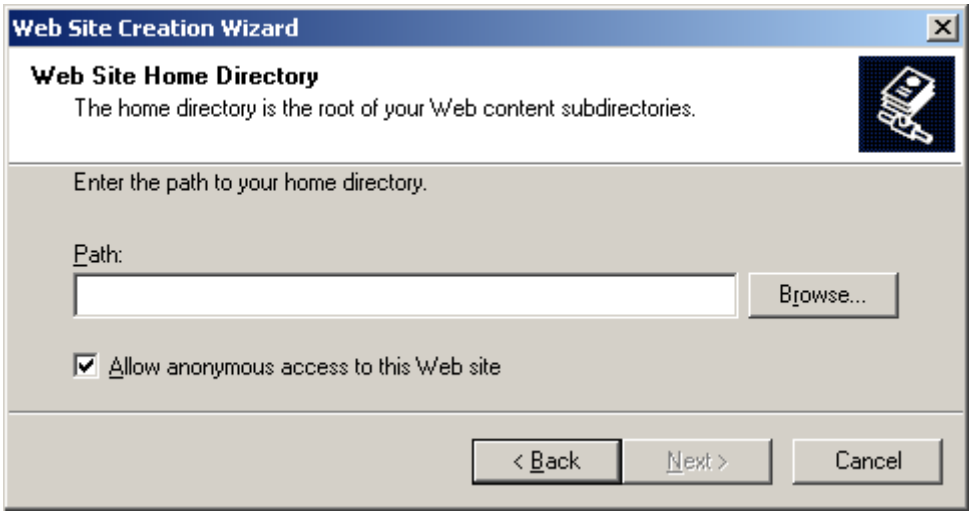


کاربرد تنظیم IP این می‌باشد که می‌توان روی سیستم چندین کارت شبکه نصب نمود تا هر سایت از طریق یکی از این کارت شبکه‌ها به ارائه سرویس بپردازد. همچنین این امکان وجود دارد که چندین سایت از یک کارت شبکه استفاده نمایند.

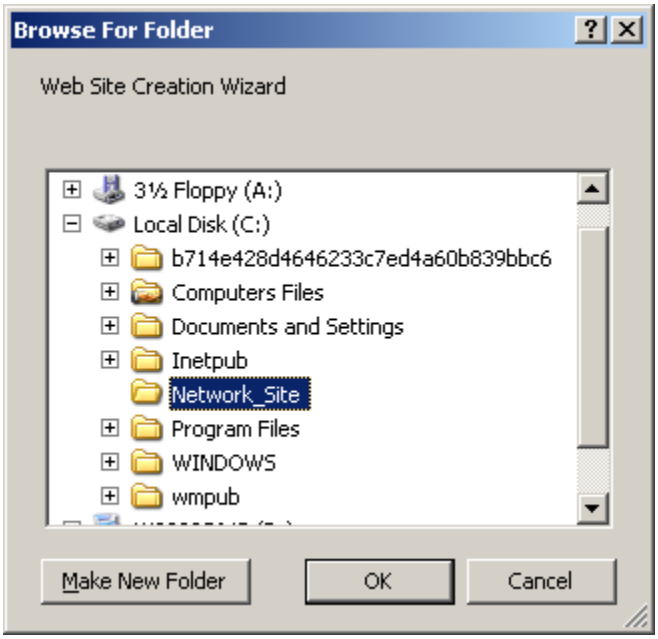
در تنظیم پورت نیز باید توجه داشته باشیم که اگر چند وب سایت تعریف می‌کنیم، آدرس پورت آن‌ها نباید با هم برابر باشد. مقدار پورت به صورت پیش فرض ۸۰ است. لذا ما مقدار پورت را ۸۱ یا چیز دیگری تعیین می‌کنیم. سپس روی دکمه Next کلیک کنید.



در صفحه بعد، مسیری فیزیکی در هارد را تعیین نمایید که فایل‌های سایت در آن قرار می‌گیرد. بدین منظور روی دکمه Browse کلیک کنید.



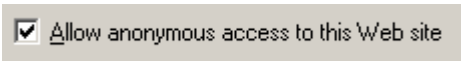
در پنجره باز شده، آدرس فیزیکی خود را انتخاب نمایید. در اینجا، ما مسیر C:\Network_Site را انتخاب نموده‌ایم.



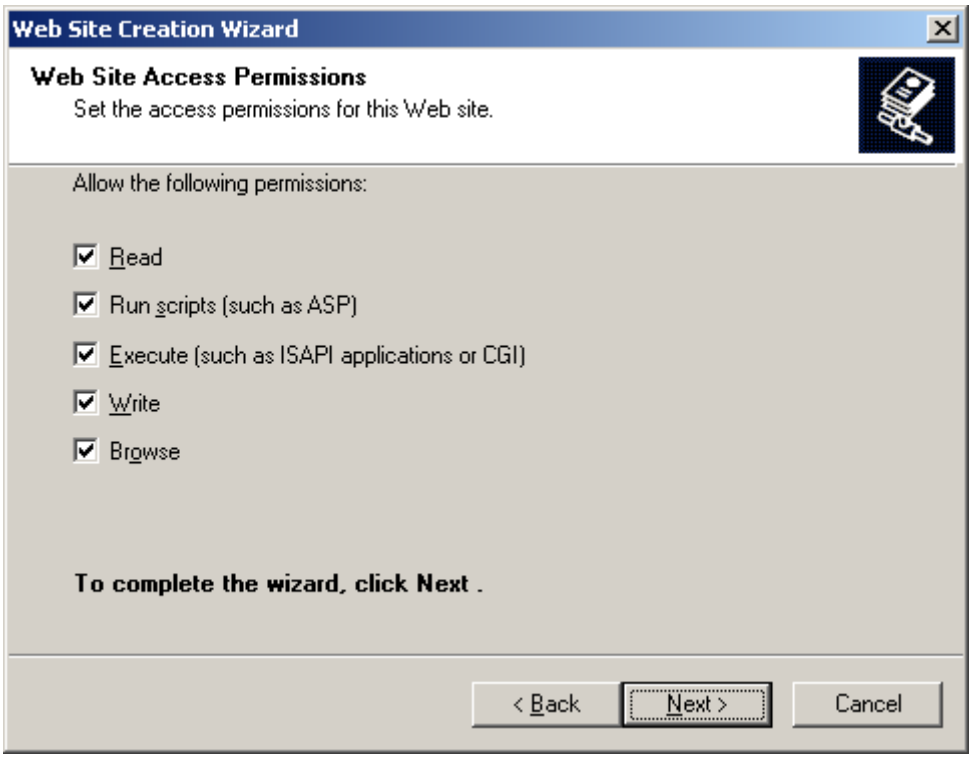
پس از OK کردن، آدرس مسیر فیزیکی را مشاهده خواهید نمود.



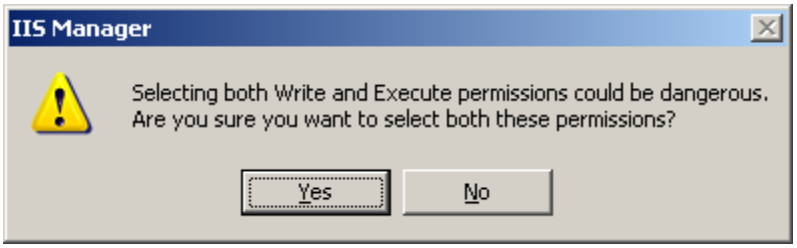
نکته: حتما در این صفحه گزینه Allow anonymous access to this Web site را فعال کنید تا کاربران از دیگر کامپیوترها بتوانند به وب سایت شما دسترسی یابند. سپس روی Next کلیک کنید.



در این صفحه، سطوح دسترسی سایت خود را تعیین نمایید. مثلاً می‌توان گفت که این سایت قابلیت ۱- خواندن اطلاعات ۲- اجرای Script (مثل دستورات ASP 3)- اجرای برنامه‌ها ۴- تغییر اطلاعات و ۵- عمل Browse را داشته باشد. پس از انتخاب Permissionها، روی Next کلیک کنید.



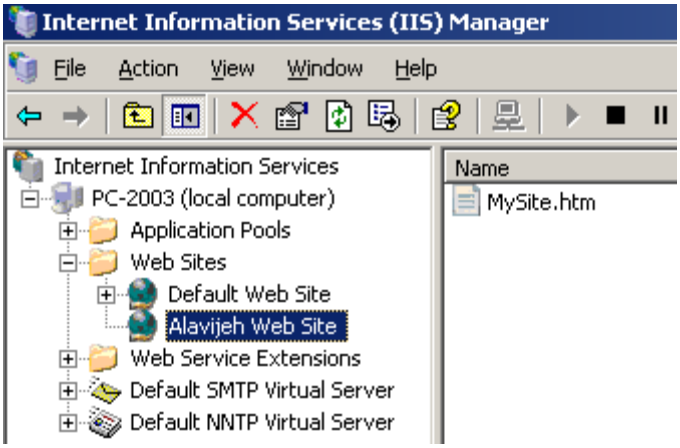
سیستم سوالی در مورد Permissionها و خطر آن‌ها می‌پرسد، روی Next کلیک کنید.



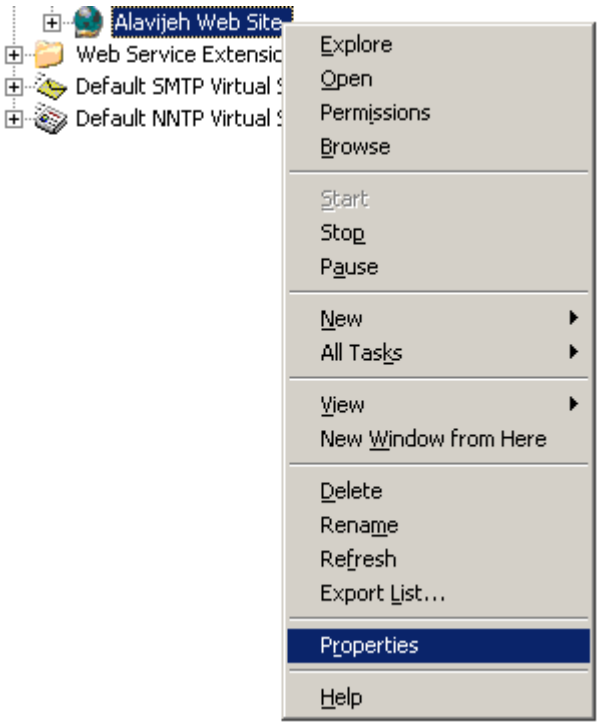
در نهایت روی Finish کلیک کنید تا عملیات ایجاد سایت اتمام یابد.

۳۸-۳-۲- تنظیم وب سایت

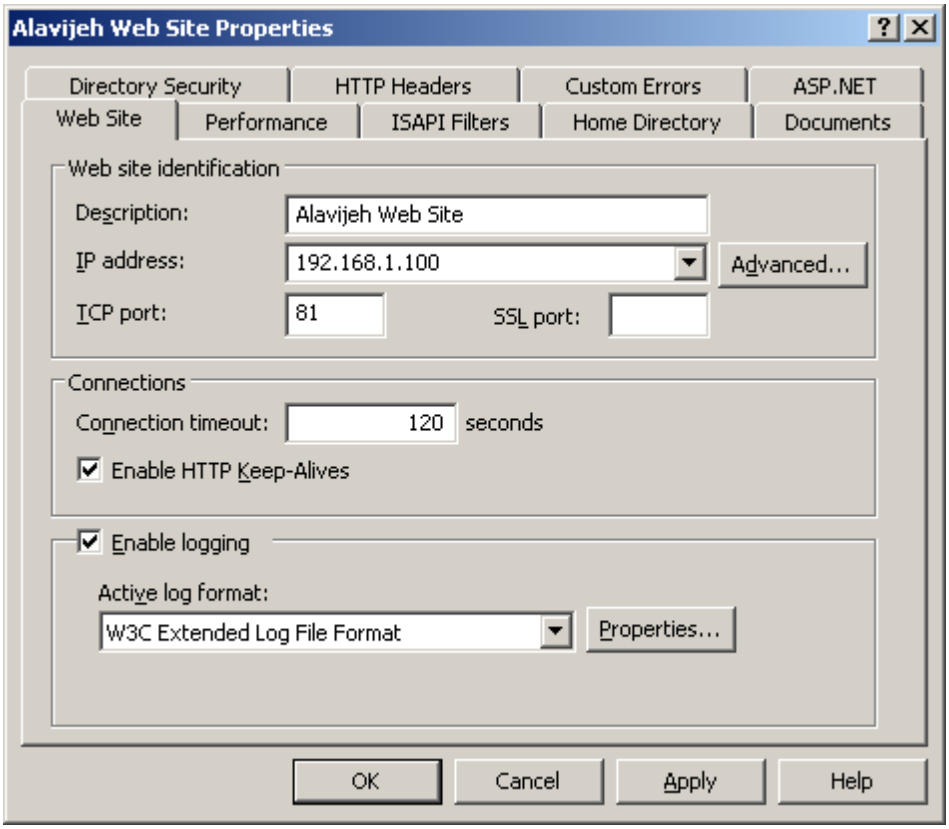
پس از ایجاد وب سایت، فایل‌های وب سایت خود را در مسیر فیزیکی تعیین شده کپی نمایید. سپس در پنجره IIS، در بخش Web Sites، وب سایت مورد نظر را انتخاب نمایید تا فایل‌های آن را در سمت راست ببینید.



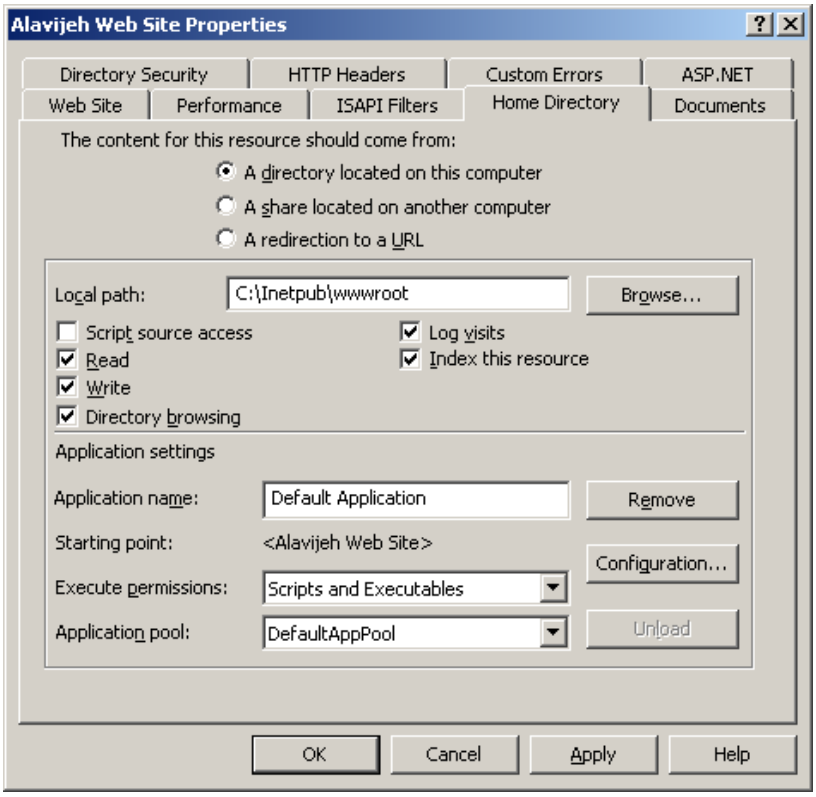
حال قبل از اجرا، نوبت به تنظیمات وب سایت می‌شود. بدین منظور، روی نام وب سایت راست کلیک کرده و سپس گزینه Properties را انتخاب نمایید.



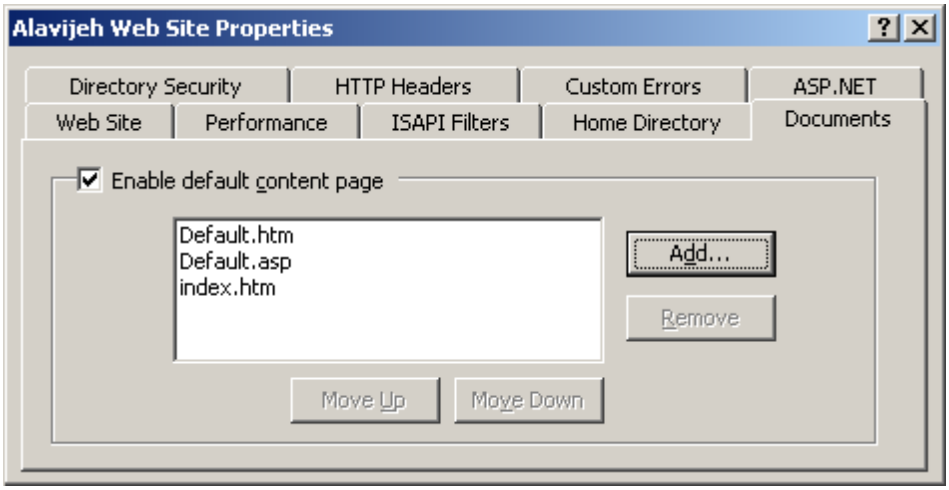
در پنجره خصوصیات وب سایت، وارد سربرگ Web Site شوید. در این قسمت می‌توانید تنظیمات اولیه مانند توصیف وب سایت، آدرس IP که برای وب سایت استفاده می‌شود، پورت مورد استفاده برای وب سایت (توجه نمایید که برای سایت هایی که تعریف می‌کنید، این آدرس پورت نباید تکراری باشد)، پورت مورد استفاده برای SSL (استفاده از وب سایت در حالت امن) و مقدار Connection Timeout (مدت زمانی که یک اتصال در صورت جواب ندادن باید از بین برود) را تعیین نمایید.



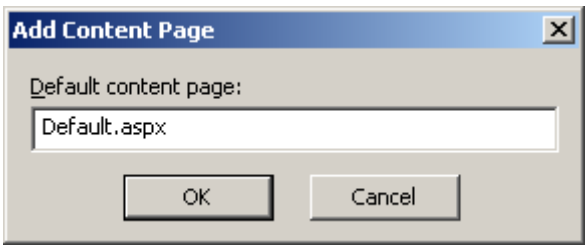
در سربرگ Home Directory می‌توانید تنظیماتی مانند مسیر فیزیکی فایل‌های وب سایت و نیز سطوح دسترسی وب سایت را تعیین نمایید.



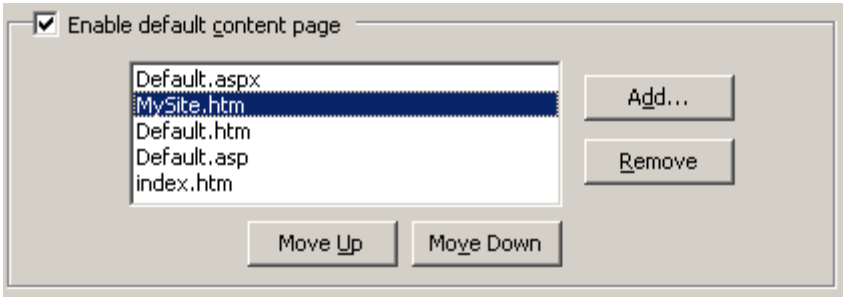
سربرگ Documents، نام فایل‌های پیش فرضی را مشخص می‌کند که سیستم هنگام بازکردن وب سایت، در صورتی که نام فایلی را وارد نکرده باشیم، به دنبال این فایل‌ها می‌گردد تا آن‌ها را اجرا کند. در مثال زیر، فرض کنید این تنظیمات را روی وب سایت Google.Com تنظیم کرده‌ایم. حال پس از وارد کردن آدرس http://www.google.com، سیستم ابتدا دنبال فایل Default.htm می‌گردد، اگر آن را یافت، آن را اجرا خواهد کرد، و گرنه دنبال فایل Default.asp می‌گردد تا آن را اجرا کند. اگر آن را یافت، آن را اجرا خواهد نمود و گرنه دنبال فایل index.htm می‌گردد. اگر سیستم نتواند این فایل را نیز بیابد، یا وب سایت را در حالت FTP نشان می‌دهد یا اینکه خطای دسترسی می‌دهد.



برای افزودن یک فایل پیش فرض جدید، روی دکمه Add کلیک کرده و سپس نام فایل را وارد نمایید.

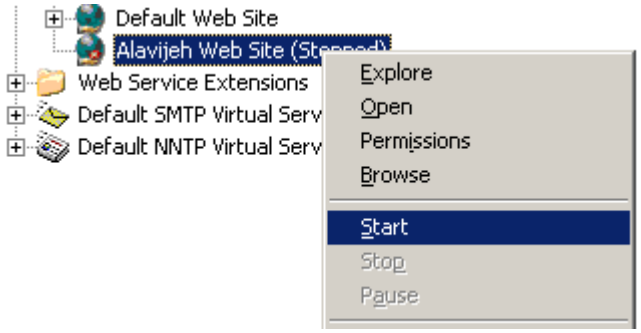


توسط دکمه‌های Move UP و Move Down نیز می‌توانید اولویت فایل‌های پیش فرض برای جستجو و اجرا را تغییر دهید. سپس OK کنید تا پنجره تنظیمات بسته شود.

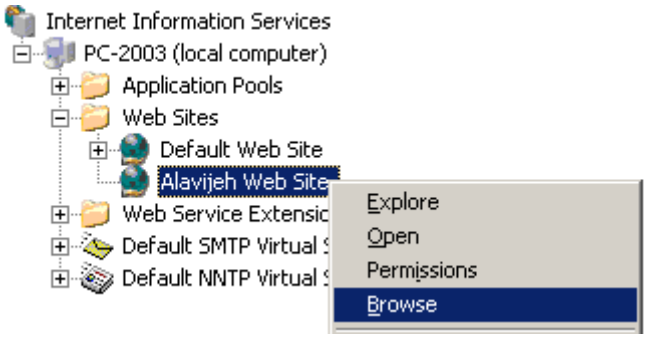


۳۸-۳-۳- اجرای وب سایت

حال برای اجرای وب سایت، ابتدا باید سرویس وب سایت را فعال نمایید. بدین منظور روی نام وب سایت راست کلیک کرده و سپس گزینه Start را انتخاب نمایید.



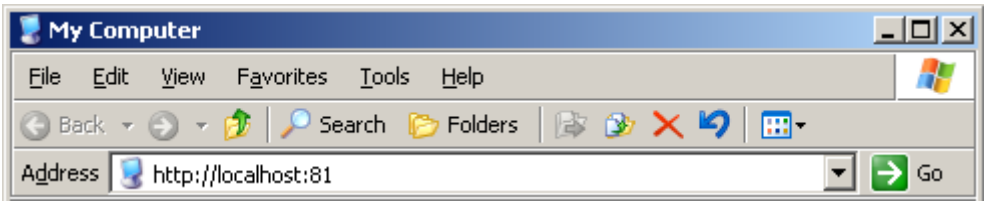
حال برای اجرای وب سایت، روی نام وب سایت راست کلیک کرده و گزینه Browse را انتخاب نمایید.



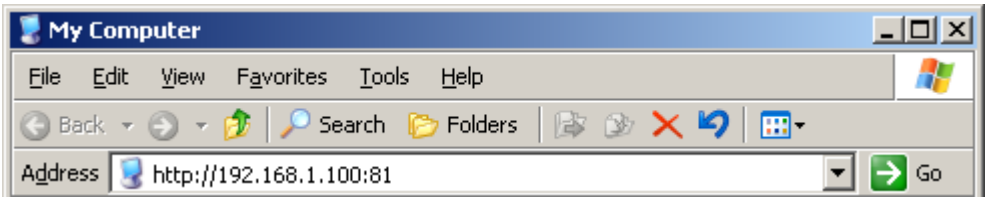
با اینکار، وب سایت اجرا شده را در صفحه IIS مشاهده خواهید نمود.



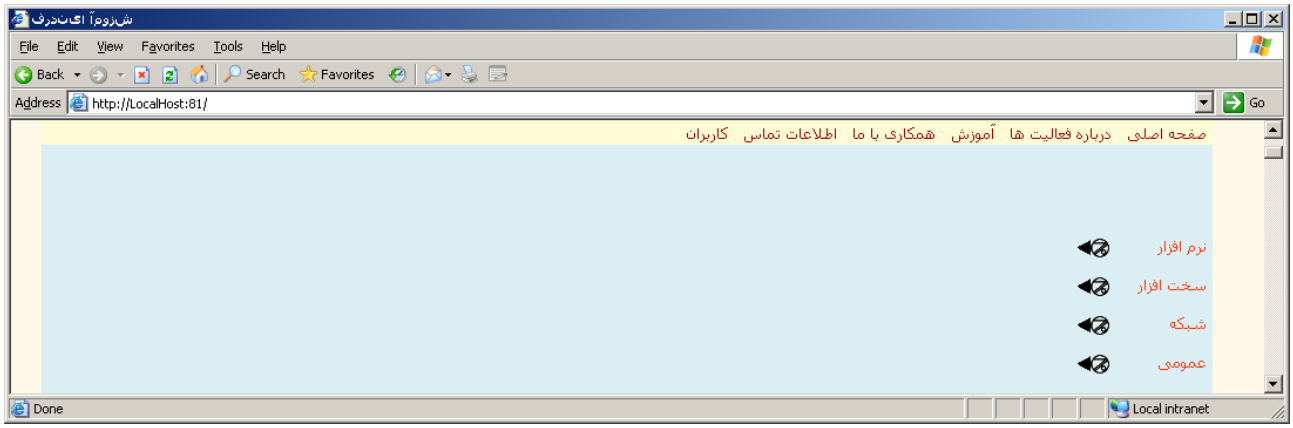
البته راه دیگری نیز برای اجرای وب سایت وجود دارد. اگر در سیستم خودتان بخواهید وب سایت را اجرا کنید، ابتدا وارد My Computer یا IE شده و سپس آدرس http://LocalHost را به همراه دو نقطه (:) و سپس شماره پورت وب سایت وارد نمایید. مانند شکل زیر:



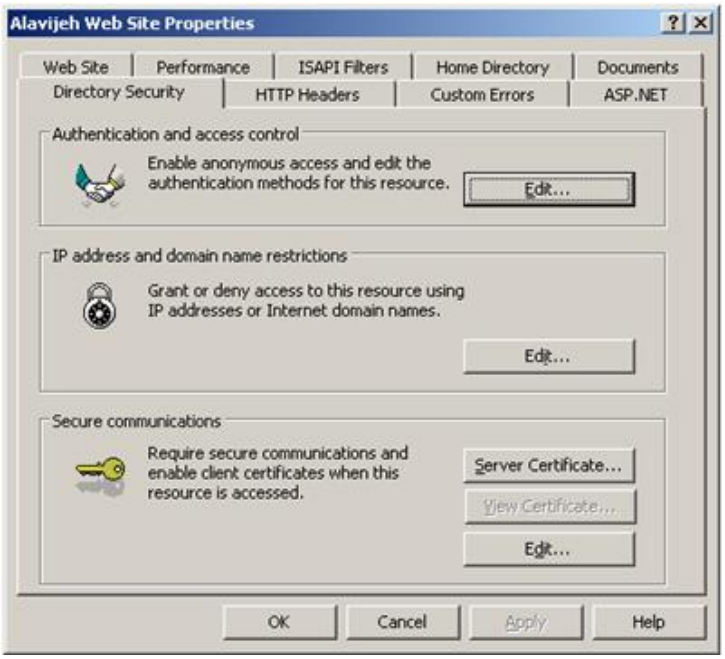
اما اگر بخواهید وب سایت را از سیستمی دیگر اجرا کنید، اینبار به جای LocalHost، آدرس IP مربوط به وب سایت را وارد نمایید.



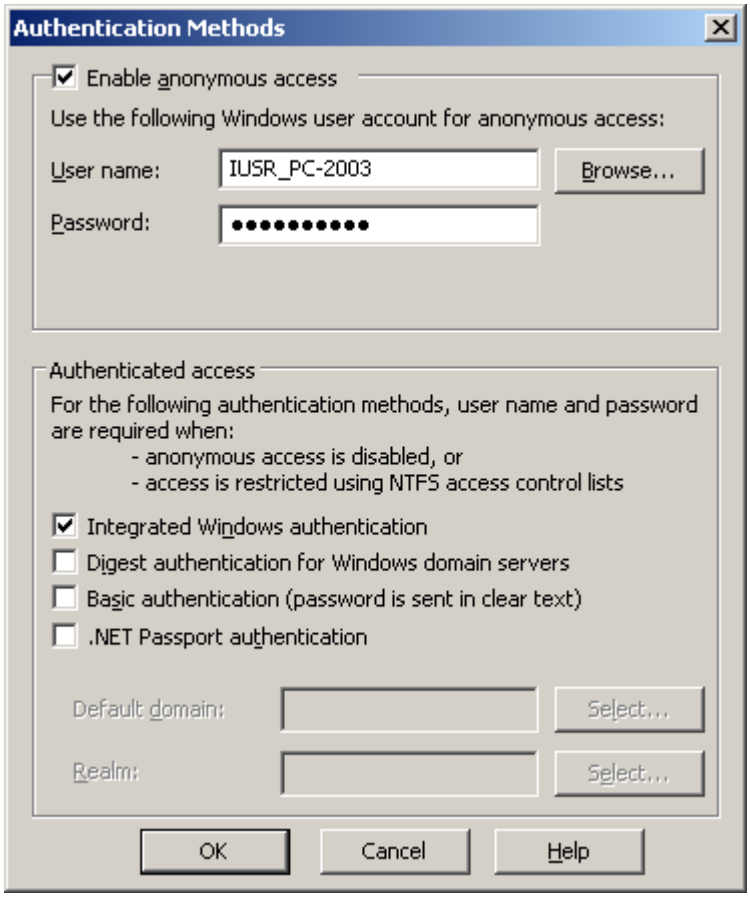
بدین ترتیب وب سایت شما اجرا خواهد شد.



مجددا وارد تنظیمات وب سایت شده و سپس سربرگ Directory Security را انتخاب نمایید. این بخش مربوط به تنظیمات امنیتی می‌باشد. در این صفحه در قسمت Authentication and access control روی دکمه Edit کلیک کنید تا وارد صفحه تنظیمات دسترسی شوید.



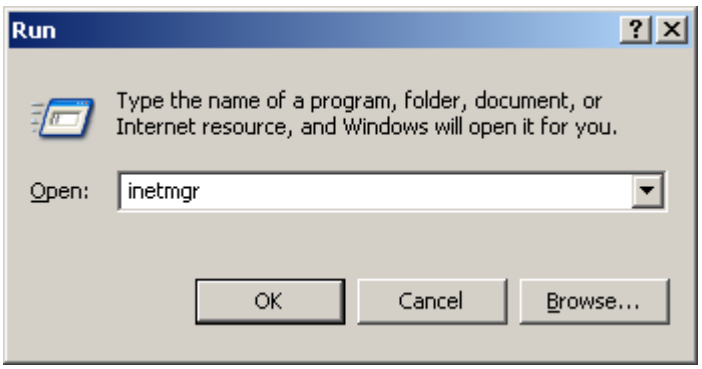
در این صفحه گزینه Enable anonymous access فعال بوده و یک نام کاربری و رمز عبور پیش فرض نیز وجود دارد. این بدان معنا است که کاربران می‌توانند از راه دور و بدون هیچ Username و Passwordی به وب سایت شما متصل شوند. برای غیر فعال کردن این امکان، تیک گزینه Enable anonymous access را بردارید.



۳۸-۴- اجرای وب سایت‌های ASP.Net

IIS به صورت پیش فرض قابلیت اجرای وب سایت‌های ASP.Net را نداشته و فقط می‌تواند وب سایت‌های HTML را اجرا کند. اگر می‌خواهید وب سایتی که با تکنولوژی ASP.Net نوشته شده است را روی IIS اجرا کنید، مراحل زیر را دنبال نمایید:

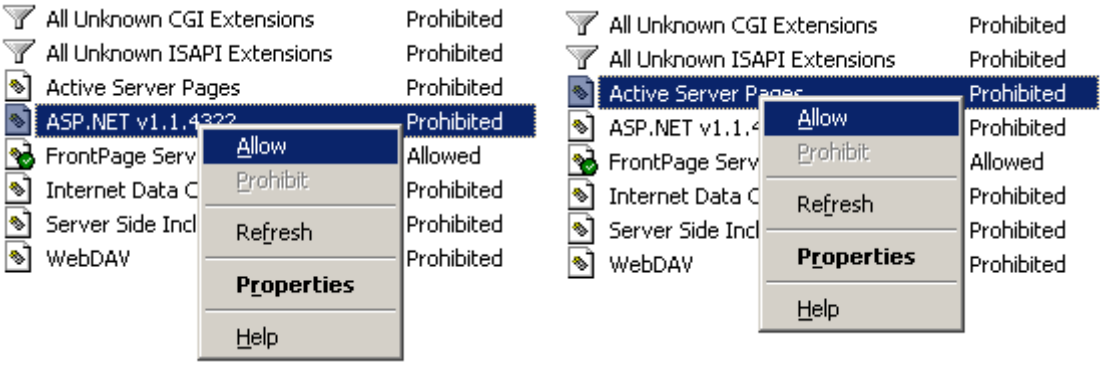
جهت فعال نمودن ASP.Net ابتدا وارد محیط IIS شوید. بدین منظور در Run تایپ کنید: inetmgr



سپس در صفحه باز شده، قسمت Local Computer را بسط داده و سپس Web Service Extensions را انتخاب نمایید.

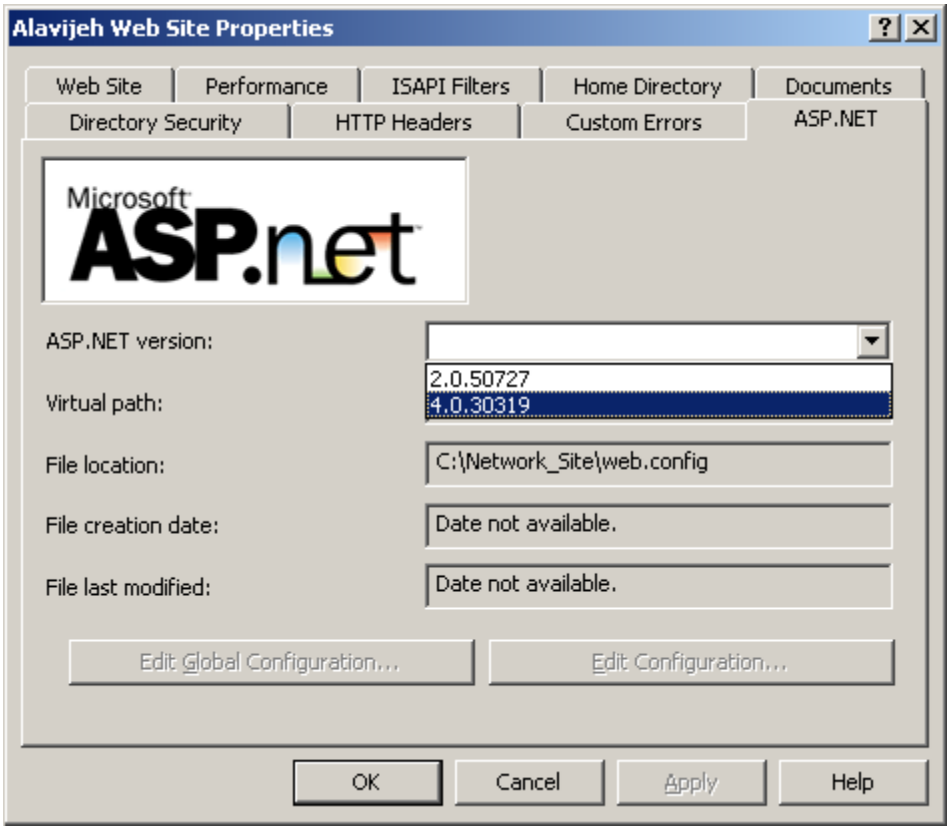


سپس روی گزینه ASP.Net راست کلیک نموده و سپس گزینه Allow را انتخاب نمایید:

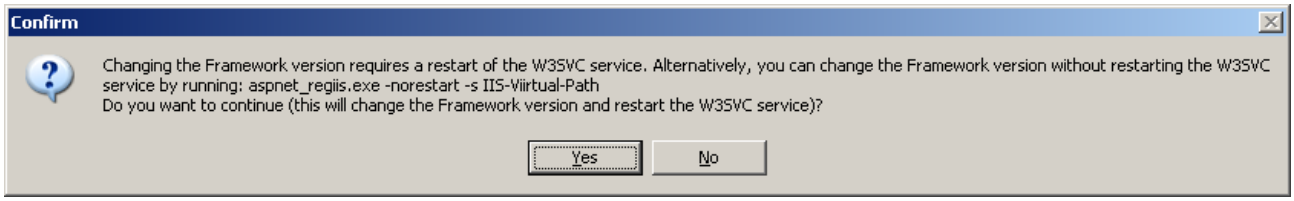


البته اگر نسخه‌های جدیدتر Framework را نصب کرده باشید، بایستی بتوانید ASP.Netهای متناظر را نیز ببینید. سپس آن‌ها را نیز فعال نمایید.

اگر این کار جواب نداد، یک Framework متناسب با وب سایت خود نصب نمایید. یعنی Framework 1.1 برای Visual Studio 2003، Framework 2.0 برای Visual Studio 2005، Framework 3.5 برای Visual Studio 2008 و Framework 4.0 برای Visual Studio 2010. پس از نصب Framework مناسب، وارد تنظیمات وب سایت شده و سپس سربرگ ASP.Net را انتخاب نمایید. سپس در این قسمت، در بخش ASP.Net version، نسخه ASP.Net خود را انتخاب نمایید.



پس از OK کردن، سیستم سوالی از شما می‌پرسد که دکمه Yes را انتخاب کنید.

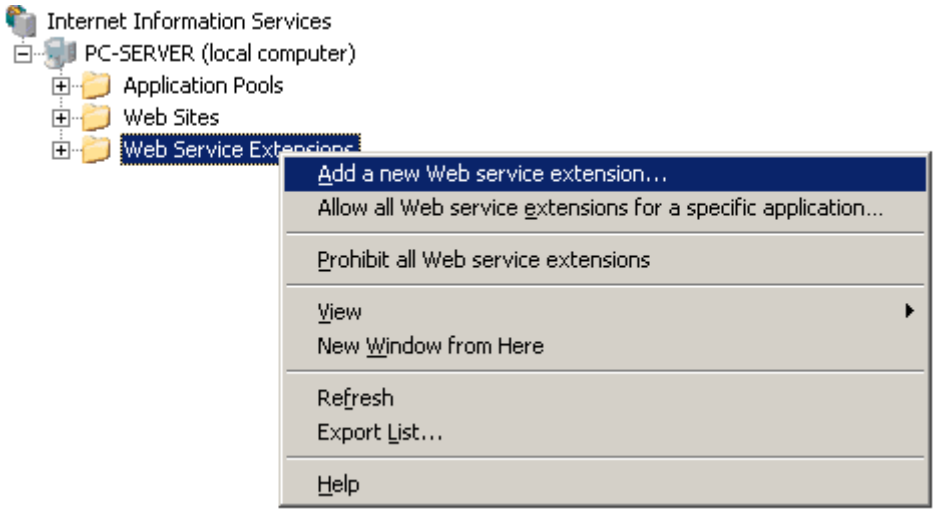


اما اگر بازهم نتوانستید وب سایت ASP.Net خود را اجرا کنید، بایستی یکی از دستورات پیکربندی Visual Studio را اجرا نمایید. ما مثال خود را در Visual Studio 2010 می‌زنیم. بدین منظور ابتدا وارد Start ➔ Microsoft Visual Studio 2010 ➔ Visual Studio Tools ➔ Visual Studio Command Prompt (2010) شوید. سپس در Visual Studio Command Prompt باز شده، دستور aspnet_regiis –i را اجرا نمایید تا ASP.Net شما روی IIS پیکربندی شود.

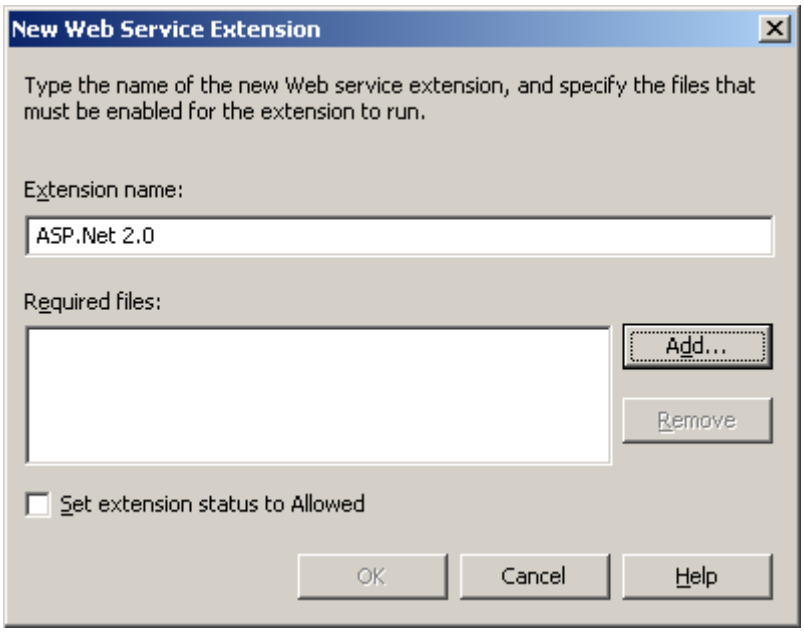


اگر بازهم جواب نداد، ممکن است که مشکل از این باشد که نسخه قدیمی Framework را روی نسخه جدید Framework نصب کرده‌ایم. برای حل این مشکل، مثلاً برای اجرای ASP.Net 2.0، ابتدا وارد IIS شده و سپس Web Service Extensions را انتخاب کنید. اگر گزینه ASP.Net 2.0 را ندیدید، مشکل نصب Framework قدیمی روی

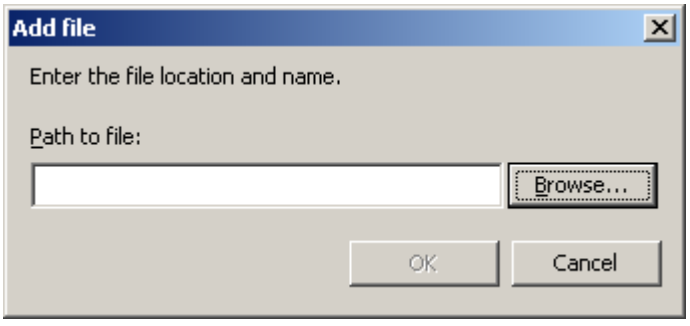
Framework جدید است. لذا برای حل مشکل، روی Web Service Extensions راست کلیک نموده و گزینه Add a new Web service extension را انتخاب نمایید:



سپس نام ASP.Net 2.0 را وارد نموده و روی دکمه Add کلیک کنید:

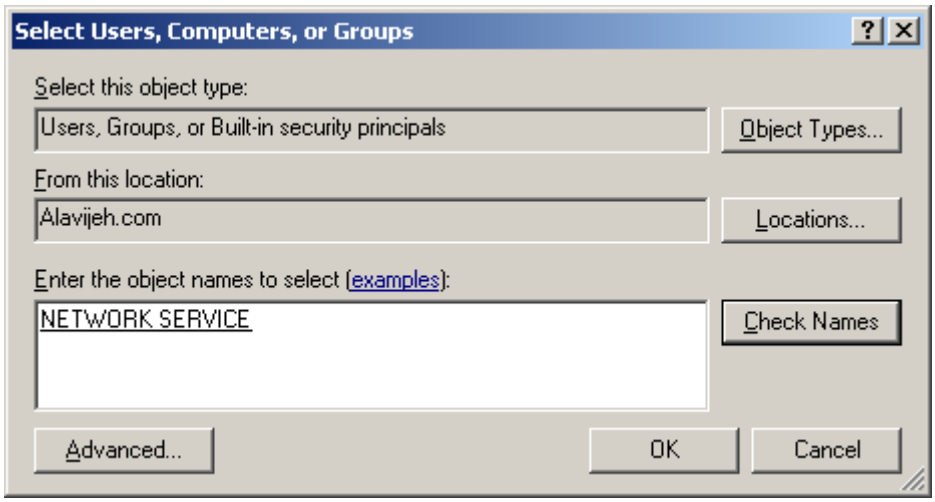


سپس روی دکمه Browse کلیک کنید:

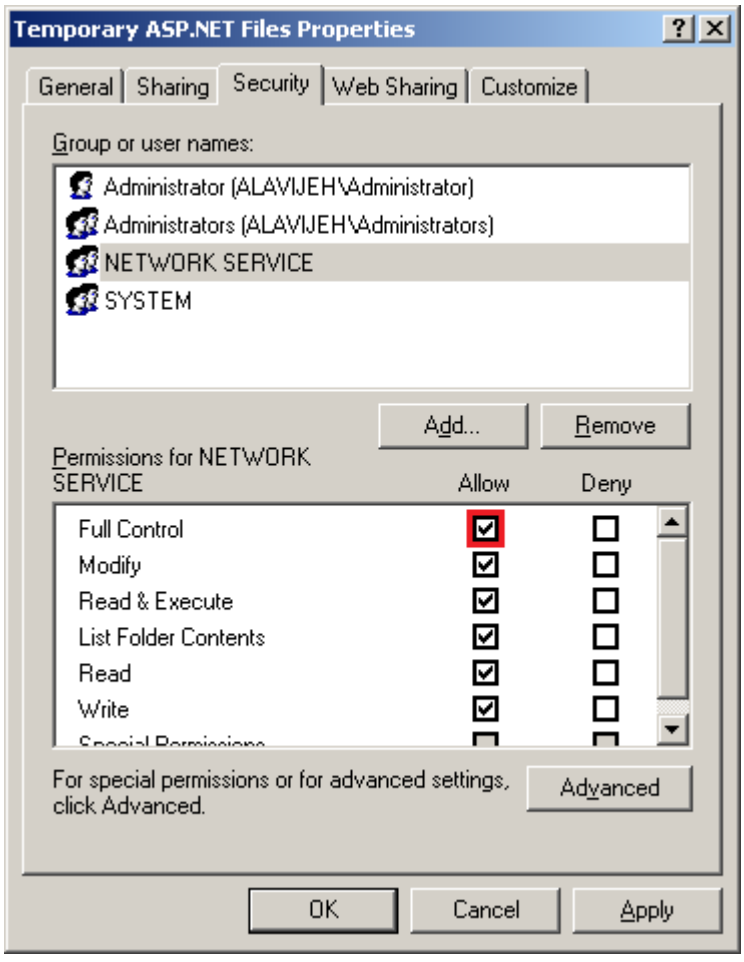


فایل aspnet_isapi.dll را از مسیر C:\Windows\Microsoft.NET\Framework\v2.0.50727 انتخاب نموده و OK کنید. در نهایت مطمئن شوید که وضعیت آن Allow است.

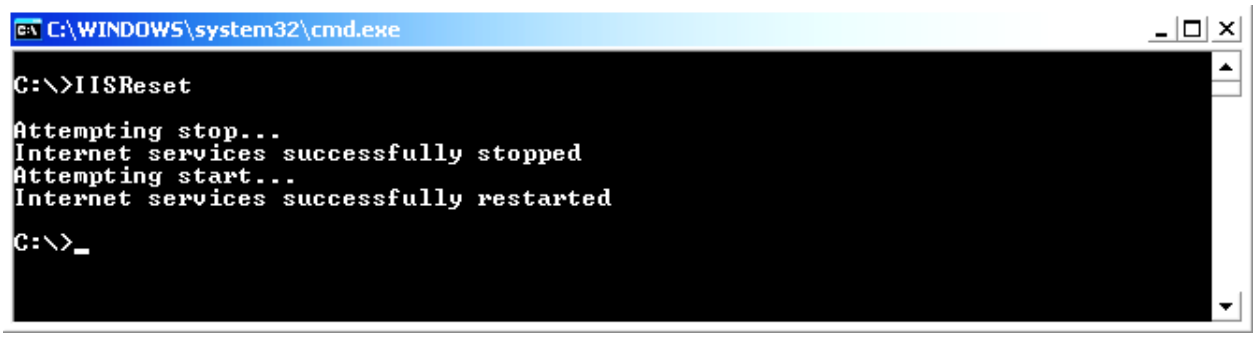
سپس بایستی مطمئن شویم که تمامی کاربران دسترسی کامل به فایل‌های ASP.Net دارند. لذا پوشه C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files را پیدا نموده، روی آن راست کلیک کرده و گزینه Sharing & Security را انتخاب نمایید. سپس وارد سربرگ Security شوید. اگر گزینه Network Service در گزینه‌ها وجود ندارد، روی Add کلیک نموده، سپس تایپ نمایید Network Service و پس از کلیک روی Check Names، روی دکمه OK کلیک کنید.



سپس در قسمت گزینه‌های دسترسی، گزینه Full Control را روی Allow تنظیم نموده و سپس روی OK کلیک کنید.



در نهایت برای اعمال تغییرات، IIS را راه اندازی مجدد نمایید. بدین منظور در Command Prompt دستور IISRESET را تایپ نمایید.



اگر باز هم جواب نداد، یعنی قسمت نیست که ASP.Net روی ویندوز سرور ۲۰۰۳ اجرا شود. لذا از اصل و قانون "**عامو ولش کن**" شیرازی‌ها استفاده می‌کنیم که این قانون بر هر درد بی درمان دواست!

فصل ۳۹

مجازی‌سازی با VMware vSphere 5



منبع: سید محمد جواد اسماعیلی؛ " مجازی‌سازی با VMware vSphere 5 "

رضا رمضانی – ramezani.cs@gmail.com - http://ramezani-cs.blogfa.com

۳۹-۱- مقدمه

موضوع اصلی این فصل *مجازی‌سازی سرور* است که vSphere به عنوان یک نمونه از تکنولوژی‌های موجود مورد بررسی قرار گرفته است.

سیستم‌های *مجازی‌سازی سرور* به طور کلی از دو قسمت اصلی تشکیل می‌شوند: یکی بخش فوق‌ناظر که بر روی سخت‌افزار قرار گرفته (البته در فوق‌ناظر نوع۲ این بخش بر روی سیستم‌عامل ماشین میزبان قرار می‌گیرد) و ماشین‌های مجازی بر روی آن اجرا می‌شوند و مسئولیت اجرا ماشین‌های مجازی و تقسیم منابع بین آن‌ها را برعهده دارد؛ و دیگری بخش مدیریت که به کمک آن می‌توان سرورهای فیزیکی و ماشین‌های اجرا شده بر روی آن‌ها را مدیریت کرد.

در حال حاضر شرکتهای بسیاری به حیطه سیستمهای *مجازی‌سازی سرور* وارد شده‌اند. در بخش فوق ناظر، مایکروسافت Hyper-v را معرفی می‌کند؛ VMWare که از پیشتازان مجازی‌سازی است ESX و ESXi را ارائه کرده است؛ اوراکل نیز Oracle VM Server را بعنوان فوق‌ناظر معرفی می‌کند؛ و در نهایت Xen که یک فوق ناظر متن باز است توسط سیتریکس ارائه شده است. البته Xen بعنوان یک کامپوننت همراه با اکثر توزیع‌های لینوکس ارائه می‌شود. ضمنا، توزیع Red Hat لینوکس، KVM را نیز بعنوان یک فوق‌ناظر ارائه کرده است. در بخش مدیریت نیز هر یک از این شرکتها ابزارهای برای مدیریت فوق ناظرهای خود ارائه می‌دهند. از جمله اوراکل که Oracle VM Manager را ارائه می‌کند؛ و یا vCenter Serve که ابزاریست برای مدیریت مجموعه vSphere. مضاف بر این شرکتهای ثالثی نیز برای مدیریت این پلتفرم‌ها ابزارهایی ارائه داده‌اند.

این فصل مشتمل بر ۶ بخش بوده که در ادامه توضیحات مختصری راجع با هر یک از بخش‌ها ارائه می‌شود:

بخش اول: همین سطوریست که در حال حاضر از نظر می‌گذرانید؛ وشاید گزاردن نام بخش بر آن اندکی گران باشد.

بخش دوم: شرح کاملیست از تکنولوژی‌های مجازی سازی در ردههای مختلف که *مجازی سازی سرور* به عنوان زیرشاخه‌ای از مجازی‌سازی در این بخش به تفصیل بررسی می‌شود. توصیه می‌شود بجهت رفع ابهام و تسلط بیشتر بر مفاهیم، این بخش را مطالعه کنید.

بخش سوم: در این بخش مجموعه vSphere بعنوان یک تکنولوژی قدرتمند در زمینه *مجازی‌سازی سرور* معرفی شده و تمامی مولفه‌ها و ابزارهای موجود در آن بطور مشروح مورد بررسی قرار می‌گیرد.

بخش چهارم: در این بخش فرایند نصب اجزا مختلف vSphere و نیازمندیهای سخت‌افزاری و نرم‌افزاری برای نصب هر یک از این اجزا بطور کامل بررسی می‌شود.

بخش پنجم: از آنجایی که سیستم‌های ذخیره‌سازی اهمیت بالایی در *مجازی‌سازی سرور* دارند؛ واینکه بسیاری از قابلیت‌های مجموعه vSphere -که شرح آن‌ها در ادامه خواهد آمد- فقط و فقط در سایه ذخیره سازهای share شده قابل استفاده خواهند بود. بنابراین در این بخش شرح مختصری از سیستم‌های ذخیره‌سازی بیان می‌شود؛ و در همین بخش توسط Openfiler یک سیستم iSCSI برای استفاده در vSphere راه‌اندازی خواهیم کرد.

بخش ششم: در این بخش نحوه مدیریت دیتا سنتر مجازی سازه شده را به کمک vCenter Server، را بررسی خواهیم کرد.

۳۹-۲- مجازی سازی

در بخش قبل اشاره مختصری به مجازی‌سازی داشتیم و تا حد کمی با آن آشنا شدیم. دراین بخش با ارائه یک تعریف کلی و همچنین یک مدل مرجع، مجازی سازی را به طور مبخش بررسی می کنیم.

مجازی‌سازی روشی برای دور نگه داشتن کاربردها[1] و مولفه‌های[2] زیرین آن‌ها از سخت‌افزاری که آن‌ها را اجرا و پشتیبانی می‌کند و همچنین تکنولوژی است که یک دید منطقی و مجازی از منابع موجود ارائه می‌کند. این دید مجازی ممکن است تفاوت بسیار زیادی با دید فیزیکی واقعی داشته باشد.

برای مجازی سازی می‌توان اهداف زیر را برشمرد:

- سطح بالاتری از کارایی[3]
- مقیاس پذیری[4]
- توانایی دسترسی مستمر[5]
- قابلیت اطمینان بالاتر
- مدیریت آسان تر
- امنیت بیشتر

قبل از ادامه بحث ذکر یک نکته ضروری بنظر می‌رسد و آن اینکه در این فصل و بسیاری از کتب با موضوع مجازی‌سازی اصطلاحات زیادی دیده می‌شود که هرکدام تعریف‌های متفاوتی از این اصطلاحات ارائه می‌دهند؛ وبه نظر می‌رسد دلیل این امر تعاریف متفاوتی هستند که شرکت‌های مختلف با توجه به محصولات خود از تکنولوژی‌ها ارائه می‌دهند. بیشتر مطالب و تعریف‌ها و اصطلاحات موجود در این فصل بر گرفته از کتاب virtualization managers guide فصل Dan Kusnetzky از انتشارات OREILLY است که بنظر می‌تواند مرجع مناسبی باشد.

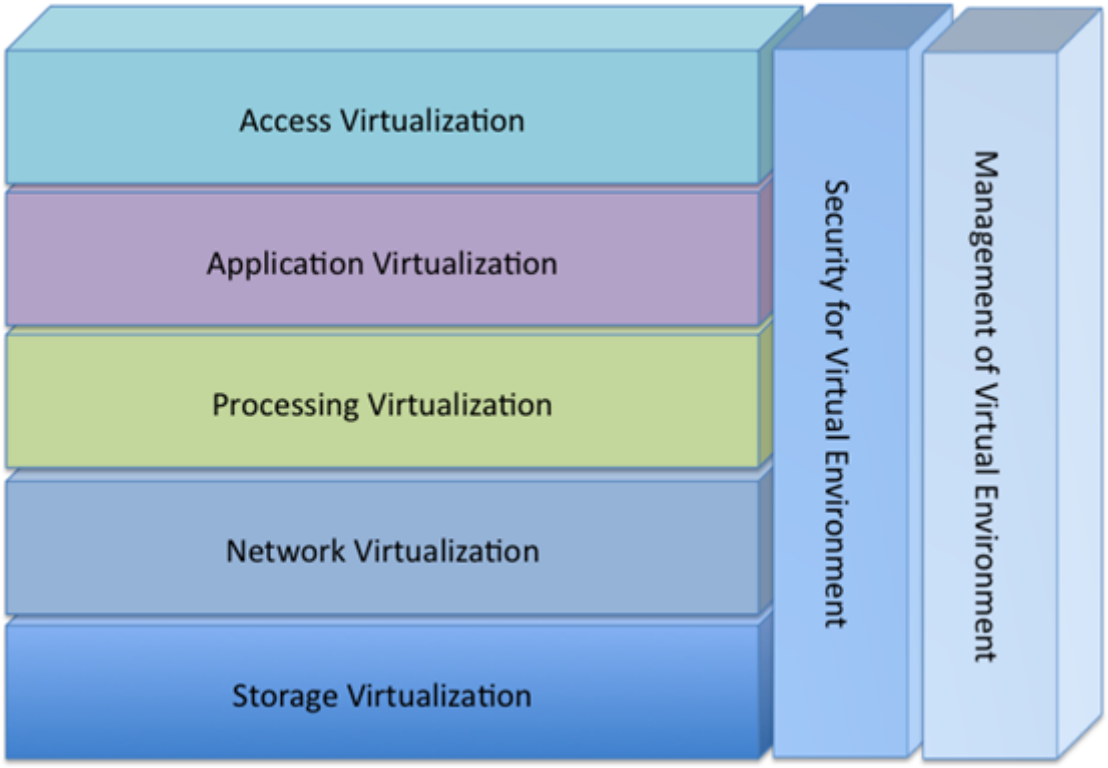
این را گفتم تا اگر در کتب مختلف با تعاریفی متفاوت و حتی تقسیم بندی‌های مختلف از تکنولوژی‌های متفاوت مجازی‌سازی مواجه شدید، دچار سردرگمی و ابهام نشوید.

۳۹-۲-۱- مدل مجازی‌سازی

اغلب اوقات با ارائه یک مدل مرجع، می‌توان فهم یک مسئله و یا یک تکنولوژی را آسان کرد. شکل ۲-۱ یک مدل معروف از مجازی‌سازی را ارائه می‌کند. البته باید توجه داشت که معمولا مدل‌های مرجع، باگذشت زمان و تغییر تکنولوژی‌ها بایستی روزآمد شوند تا اعتبار خود را حفظ کند و همچنان بعنوان یک مدل مرجع باقی بمانند.

---

[1] applications
[2] components
[3] performance
[4] scalability
[5] High Availability



شکل ۲-۱. لایه‌های مجازی سازی

۳۹-۲-۲- لایه‌های مجازی‌سازی

هر یک از لایه‌ها بخشی از یک سیستم کامپیوتری را مجازی‌سازی می‌کند که در ادامه هر یک ازآن‌ها توضیح داده شده است.

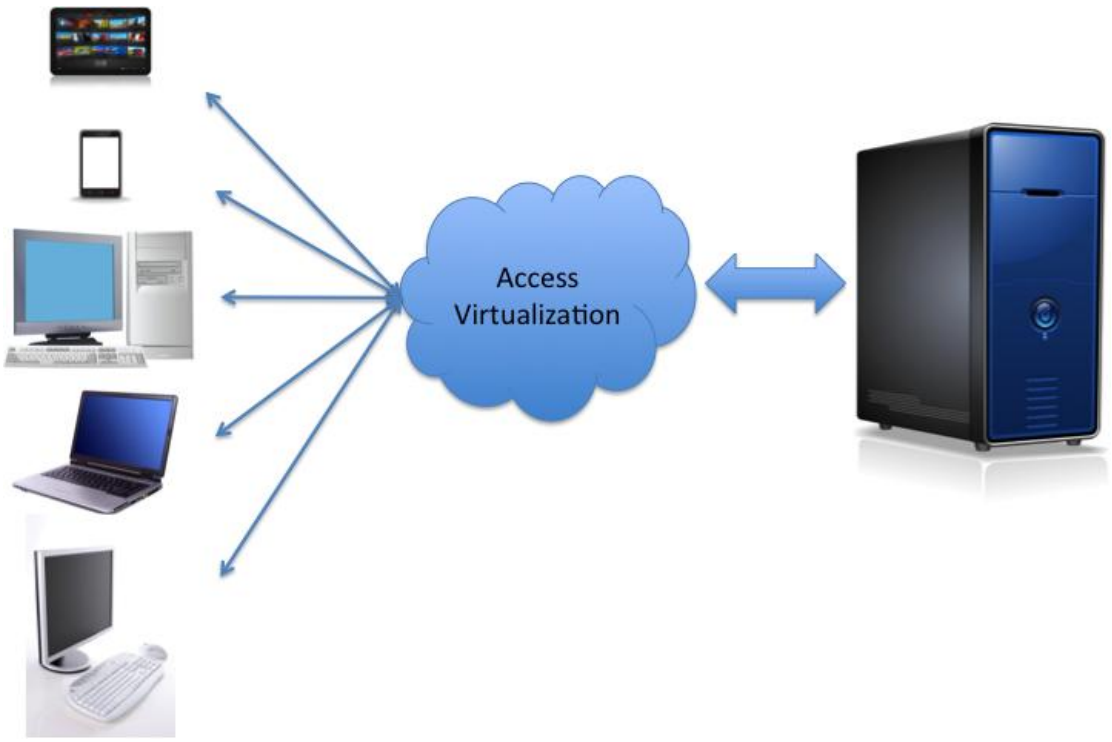
۲-۲-۱ مجازی‌سازی دست‌یابی[6]

تکنولوژی نرم‌افزاری و سخت‌افزاری که این امکان را ایجاد می‌کند که ابزار[7] به هر کاربردی دست پیدا کنند، بدون اینکه هریک (ابزار و کاربرد) اطلاعات زیادی در مورد دیگری داشته باشد. کاربرد ابزاری را می‌بیند که با آن کار می‌کند و ابزار نیز کاربرد را. در بعضی موارد جهت افزایش کارایی، سخت‌افزارهای خاص در دو طرف شبکه نصب می‌شوند.

شکل ۲-۲ این مدل از مجازی‌سازی را نشان می‌دهد.

در این تکنولوژی همانطور که در سطوح بالاتر اشاره شد، داده‌ها و پردازش در طرف سرور است، اما ورودی و خروجی کاربردها وبرنامه‌ها توسط کلاینت و در طرف دیگر اتفاق می‌افتد و یا به بیان دیگر مجازی سازی دسترسی این امکانرا فراهم می‌آورد که کلاینتی که در طرف دیگر شبکه قرار دارد، رابط کاربری کاربردی که در سرور در حال اجرا است مشاهده نماید؛ و کاربرد ورودی‌های ماوس و صفحه‌کلید و دیگر ورودی‌ها را از کابر سمت کلاینت دریافت کند. نکته مهم دیگری که در این تکنولوژی وجود دارد این است که ممکن است کاربرد در حال اجرا در سرور که از طریق کلانیت قابل دسترسی است، یک برنامه لینوکسی باشد ولی کلاینت مثلا دارای سیستم‌های ویندوز باشد. یعنی هیچ نیازی نیست سیستم‌عامل و حتی پلتفرم سخت‌افزاری سرور و کلاینت هیچ شباهتی به یکدیگر داشته باشند.

[6] Access Virtualization
[7] Device



شکل ۲-۲. مجازی‌سازی دستیابی

شکل ۲-۳ این مفاهیم را به تصویرکشیده است. احتمالا شما هم متوجه شده‌اید که این تکنولوژی، همانطور که در بخش اول هم توضیح داده‌شد، نرم‌افزار به عنوان سرویس یا همان saas در سیستم‌های پردازش ابری است.

البته چون اسم پردازش ابری آمد نباید فکر کنیم که این یک تکنولوژی جدید است چرا که سابقه این تکنولوژی به سال ۱۹۸۰ و حتی قبل از آن بازمی‌گردد؛ زمانی که مجازی سازی دسترسی توسط سازندگان main frame یعنی IBM، Burroughs (که در حال حاضر جزئی از Unisys است) RCA و دیگران ارائه می‌شد. بدین‌صورت که مجموعه‌ای از پایانه‌ها[8] به کاربردهای در حال اجرا بر روی سرورهای دیتاسنتر[9] دسترسی داشتند.

در حال حاضر شرکت‌های زیاد در این زمینه مشغول به فعالیت هستند که البته ما در ادامه مهمترین آن را نام می‌بریم.

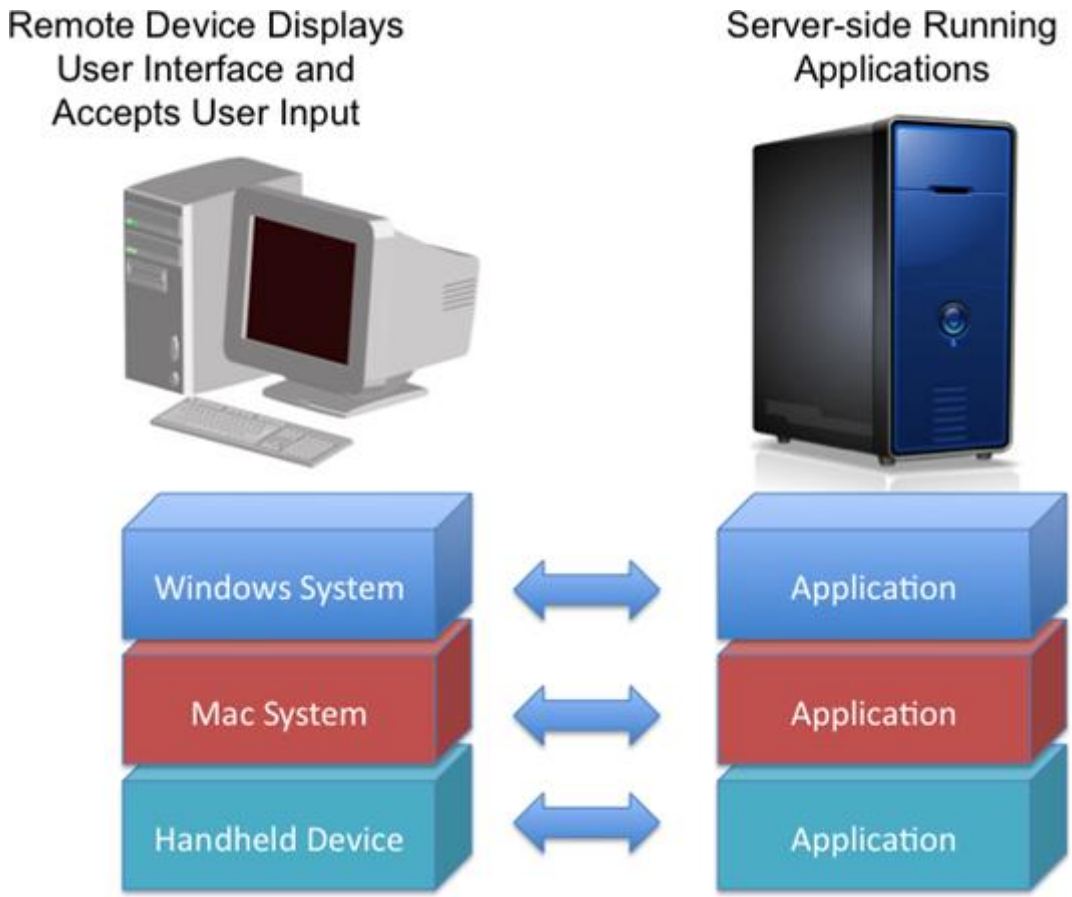
سیتریکس (Citrix): سیتریکس یکی از پیشروترین شرکت‌ها در این زمینه است. محصولات اولیه این شرکت که main frame نامیده می‌شد اجاره می‌داد تعدادی کلاینت با سیستم‌های متفاوت به کاربردهای ویندوزی و سولاریس (یونیکس) که در حال اجرا بر روی سرور بودند دسترسی داشته باشند. بعدها این سیستم به meta frame تغییر نام داد. این سیستم امروزه با نام XenApp شناخته می‌شود.

مایکروسافت: این شرکت نیز مجازی سازی دست یابی را با افزودن ابزارهایی در ویندوز ۹۵ و سرور NT شروع کرد. تکنولوژی مایکروسافت، Microsoft Terminal Service نامیده می‌شود.

HP، IBM ، اوراکل (Sun سابق) و دیگر پشتیبانان یونیکس: x–windows در دانشگاه MIT بعنوان بخشی از یونیکس استاندارد شد. x-windows که محصول همکاری چند شرکت بزرگ حامی یونیکس ازجمله IBM، HP، DEC (که در

[8] Terminals
[9] Data Center

حال حاضر جزئی از HP است) و چند شرکت بزرگ دیگر بود، یکی از مهمترین ابزارهای مجازی سازی دسترسی از سال ۱۹۸۰ به بعد می‌باشد.



شکل ۲-۳. مجازی‌سازی دست‌یابی. اجرا سمت سرور، دسترسی سمت کلاینت

ردهت، سوزه و دیگر توزیع‌های لینوکس: از زمانی که x- windows به طور تجاری عرضه شد توزیع‌های لینوکس هم شروع به سازگاری و ارائه آن به عنوان مولفه‌های[۱۰] خود کردند؛ به طوری که تمام سرویس هایی که x-windows در یونیکس پشتیبانی می‌شود، در محیط‌های لینوکس هم ارائه می‌شود.

۲-۲-۲ مجازی سازی کاربرد[۱۱]

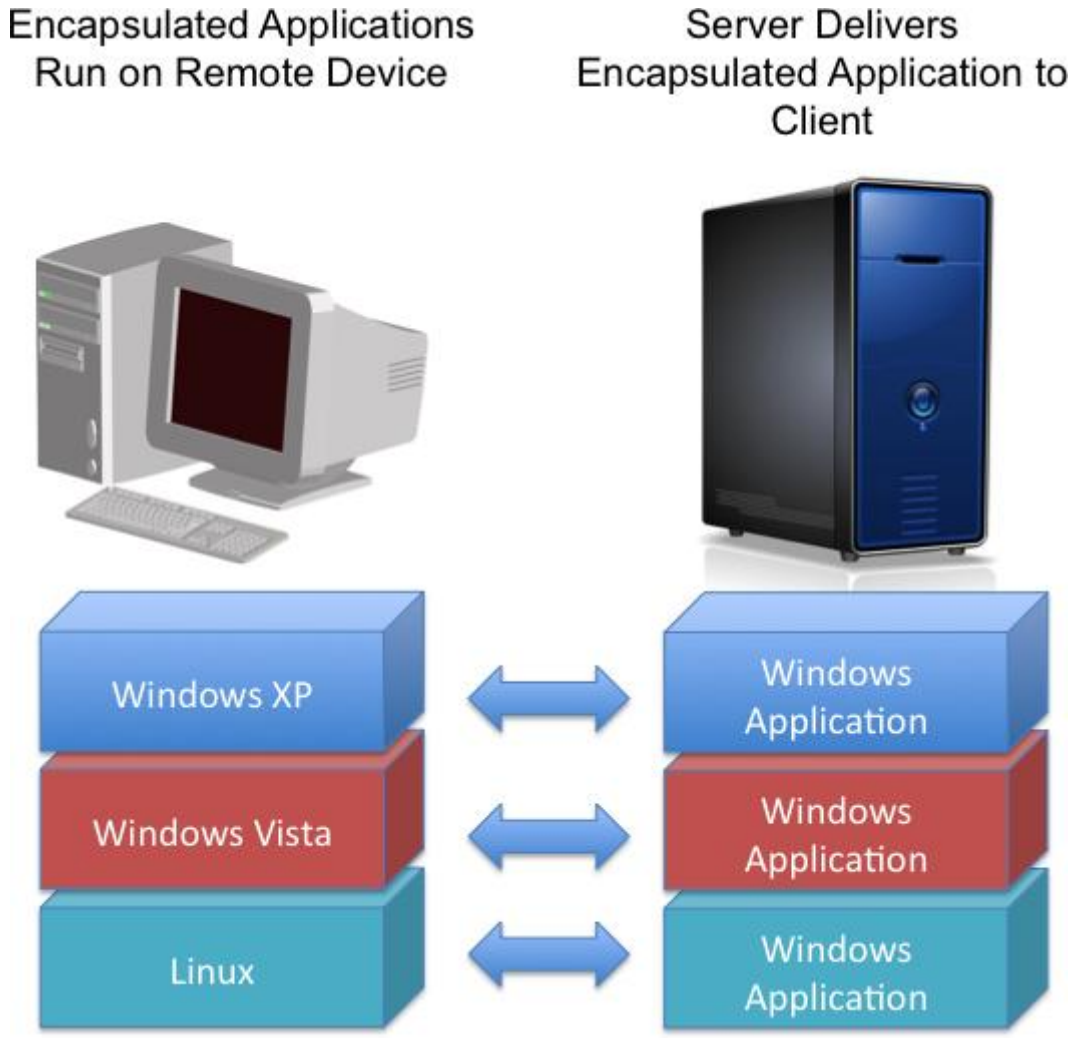
تکنولوژی نرم‌افزاری که به کاربردها اجازه می‌دهد بر روی سیستم‌عامل‌های متفاوت و حتی بر روی سکوهای[۱۲] سخت‌افزاری متفاوت اجرا شوند؛ و این یعنی کاربرد طوری فصل شده که بر روی یک فریم‌ورک اجرا شود. موارد پیشرفته این تکنولوژی، این قابلیت را ایجاد می‌کند که در صورت از کار افتادن[۱۳] یا به اصطلاح فیل شدن یک کاربرد، آن کاربرد دوباره اجرا شده و یا یک نسخه جایگزین[۱۴] اجرا شود؛ و یا اینکه برای دستیابی سطح بالایی از مقیاس پذیری[۱۵]، یک توازن بار

[10] Componenets
[11] Application Virtualization
[12] Platform
[13] fail
[14] instance
[15] scalability

کاری[16] بین چند نمونه از یک کاربرد ایجاد کرد. این قابلیت‌ها درحالی عملیاتی و قابل اجرا است که حتی در بسیاری از موارد نیازی به معماری دوباره و دوباره نویسی کاربرد نیز نخواهد بود.

همچنین این تکنولوژی بر روی سیستم‌عامل اجرا می‌شود تا کاربرد موردنظر کپسوله شده و یا بر روی یک محیط ساختگی اجرا شود.

مجازی‌سازی کاربرد، دارای دو حالت سمت سرور[17] و سمت کاربر[18] میباشد که این موضوع در شکل ۲-۴ به تصویر کشیده است.



شکل ۲-٤. مجازی‌سازی کاربرد

حال هریک از دو حالت را مورد بررسی قرار می‌دهیم:

مجازی سازی کاربرد سمت کاربر: این تکنولوژی یک محیط محافظت شده بوجود می‌آورد که اجازه می‌دهد تا کاربرد بتواند از دیگر کاربردهای در حال اجرا در محیط وحتی از سیستم عامل هم ایزوله شود؛ و این بعضی بسیاری از نرم‌افزارهایی که قبلا نمی‌توانستند در کنار یکدیگر و بر روی یک سیستم اجرا شوند از این به بعد می‌توانند در کنار یکدیگر استفاده شوند. همچنین بسیاری از نرم‌افزارها که برای نسخه‌های قبلی یک سیستم‌عامل فصل شده‌اند می‌توانند بر روی نسخه‌های جدیدتر

[16] Load Balancing
[17] Server-side
[18] Client-Side

سیستم‌عامل اجرا شوند. و مورد دوم زمانی مفید خواهد بود که سازمان برای بالا بردن کارایی و استفاده از تکنولوژی جدیدتر قصد ارتقا سیستم عامل را داشته باشد ولی به جهت نبود نسخه‌های سازگار با نسخه جدید سیستم عامل، این کار مقدور نباشد.

مجازی‌سازی کاربرد سمت سرور: در این حالت، علاوه بر داشتن مزایا حالت سمت کاربر می‌توان ازآن برای اجرای چند نمونه از یک نرم‌افزار برای ارائه به چند کاربر بهره برد. مثلا می‌توان به طور همزمان بر روی یک سرور۱۰ نمونه از office word ۲۰۰۷ را اجرا کرده و از طریق ترمینال به ۱۰ کاربر سرویس داد. و یا اینکه در هنگام درخواست یک نسخه از یک کاربرد چند نمونه از آن به روی چند ماشین مختلف اجرا شود تا در صورت از کار افتادن یکی، از دیگری استفاده شود.

در حال حاضر بسیاری از شرکت‌ها سیستم‌های مجازی‌سازی کاربرد را ارائه می‌دهد که از آن جمله می‌توان به موارد زیر اشاره کرد.

سیتریک که در همه زمینه‌های مجازی‌سازی فعال است در این زمینه نیز یکی از پیشتازین است. XenApp این شرکت یک محصول مجازی‌سازی کاربرد سمت کاربر است.

مایکروسافت از سال ۲۰۰۶ با Softricity به این عرصه وارد شد که بعدها آن را بهSoftGrid تغییرنام داد. در حال حاضر تکنولوژی مایکروسافت را با نام Microsoft Application Virtualization یا App-V شناخته می‌شود. App-V هم مجازی‌سازی سمت کاربر و هم مجازی‌سازی سمت سرور را ارائه می‌دهد.

VMware نیز در سال ۲۰۰۸، Thin App را ارئه کرد که یک تکنولوژی مجازی‌سازی کاربرد سمت کاربر است.

AppZero virtualization هم این امکان را به سازمان‌ها می‌دهد تا بتوانند نرم‌افزارهایشان را در داخل یک محیط مجازی که VAA نامیده می‌شود کپسوله نمایند.

۲-۲-۳ مجازی‌سازی پردازش[19]

تکنولوژی نرم‌افزاری و سخت‌افزار که این امکان را می‌دهد تا پیکربندی سخت‌افزار فیزیکی از دید سرویس‌های سیستم‌عامل و کاربرد مخفی بماند. این تکنولوژی اجازه می‌دهد تا چند سیستم بتوانند یک سیستم دیده شوند ویا برعکس؛ یک سیستم بتواند از دید خارجی چندین سیستم دیده‌شود. از مزایایی این نوع مجازی سازی می‌توان به افزایش کارایی، دسترسی به سطح بالایی از گسترش پذیری، قابلیت اعتماد بالاتر[20]، دسترسی همیشگی[21]، دستیابی به سرعت بیشتر در پردازش، همچنین ایجاد محیط‌های متفاوت بر روی یک سیستم فیزیکی منفرد، اشاره کرد.

مجازی سازی پردازش دارای پنج فرم مختلف است:

- ناظر پردازش موازی[22]
- ناظر مدیریت بار کاری[23]
- ناظر قابلیت دسترسی بالا/ بازگشت از خطا/ بازیابی سیستم[24]
- نرم‌افزار ماشینی مجازی[25]

---

[19] Process Virtualization
[20] Reliability
[21] High Availability
[22] parallel processing monitors
[23] workload management monitors
[24] high availability/fail over/disaster recovery monitors

- مجازی‌سازی سیستم‌عامل و بخش بندی

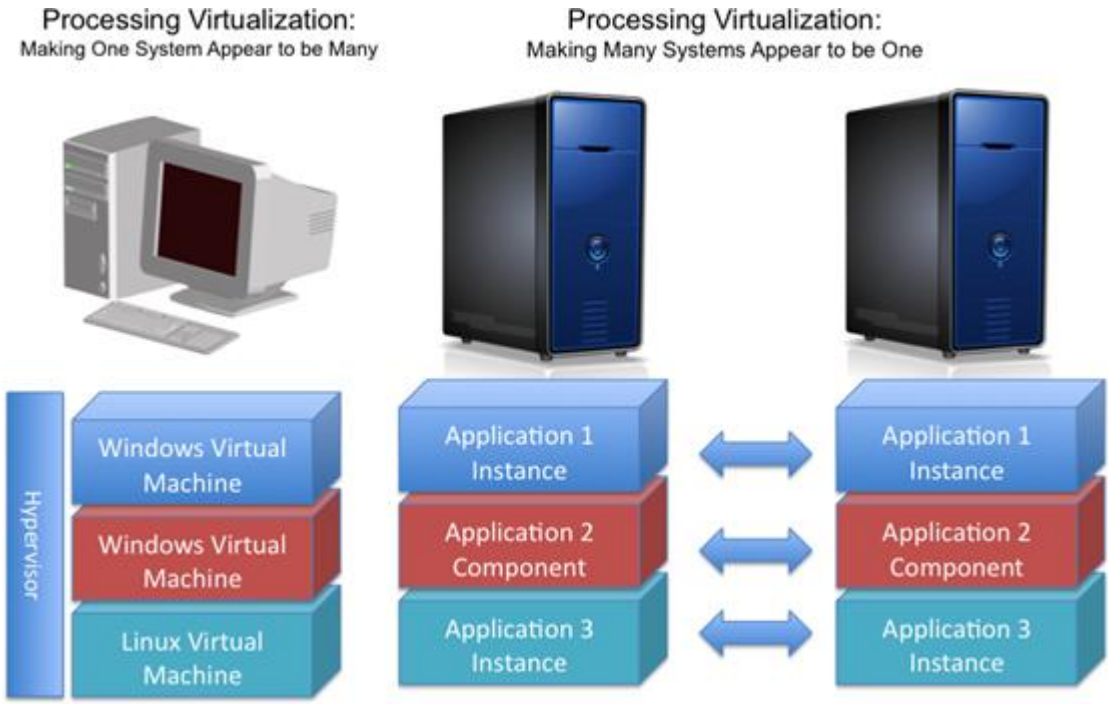
پردازش‌موازی، مدیریت بار کاری و پیکربندی با قابلیت دسترسی بالا را معمولا با نام خوشه‌بندی[۲۶] یا کلاستر می‌شناسند؛ اگر چه هر یک سرویس‌های متفاوتی ارائه می‌دهد.

مجازی سازی پردازش یکی از این سه کار را انجام می‌دهد:

۱. کپسوله کردن سیستم عامل بطوری که تعداد زیادی ماشین مجازی می‌توانند برروی یک سیستم اجرا شوند
۲. متصل کردن چند سیستم برای اینکه یک کاربرد و یا داده بین آن‌ها توزیع شده تا بتوان به کمک پردازش‌موازی کارایی را بالا برد
۳. متصل کردن کردن چند سیستم تا در صورتی خرابی یکی از آن‌ها سیستم متوقف نشده و به کمک بقیه ماشین‌های متصل به مجموعه، به کار خود ادامه دهد.

۲-۲-۳-۱ یک سیستم بجای چند سیستم وچند سیستم بجای یک سیستم.

همانطور که در شکل ۲-۵ نشان داده شده است، تفاوت زیادی بین اینکه یک سیستم از دید خارجی چند سیستم دیده شود یا چند سیستم از دیده برون یک سیستم دیده شوند وجود دارد. در ادامه هریک از این دو حالت را بررسی می‌کنیم.



شکل ۲-۵. مجازی‌سازی پردازش

۲-۲-۳-۱-۱ پیکربندی یک سیستم بطوری که از دید خارجی چند سیستم دیده شود

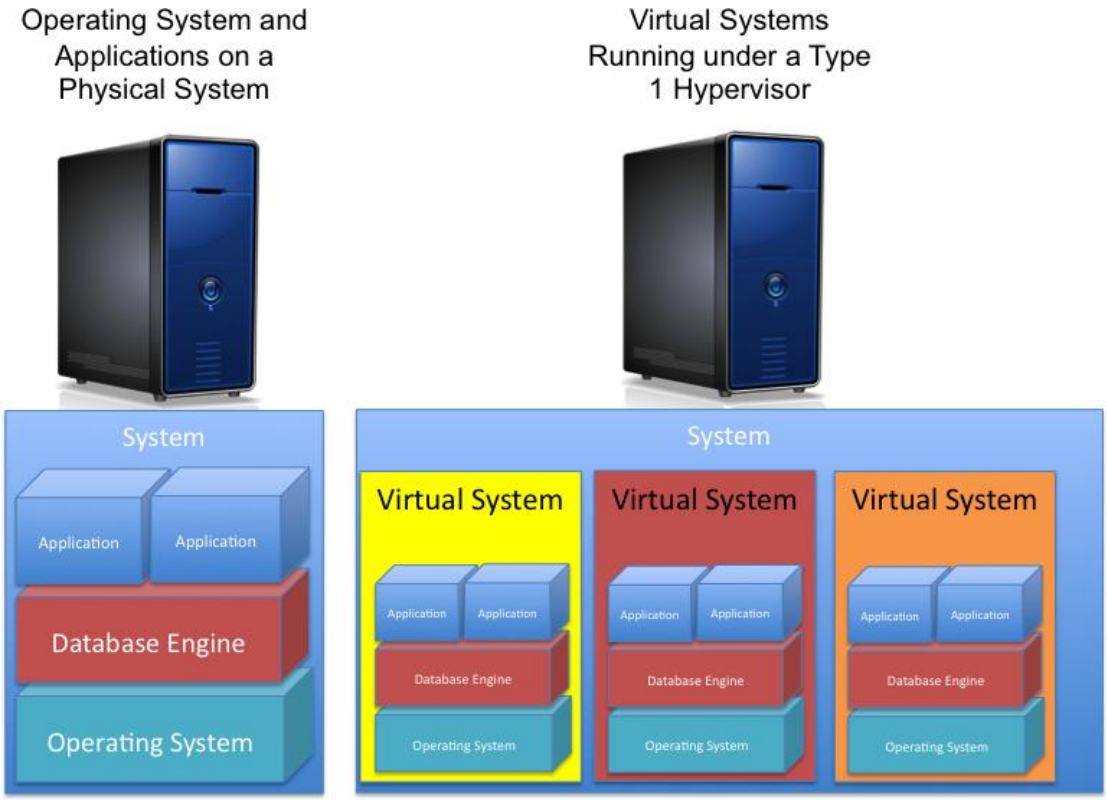
نرم‌افزار ماشین مجازی کل پشته نرم‌افزار را که سیستم را می‌سازد در داخل فایل ماشین‌مجازی کپسوله می‌کند.

فوق ناظر[۲۷] می‌تواند یک یا چند ماشین‌مجازی را بر روی یک ماشین فیزیکی اجراکند.

شکل ۲-۶ این موضوع را به تصویر می‌کشد.

---

[25] virtual machine software
[26] cluster
[27] Hypervisor



شکل ۲-٦. سرور مجازی در برابر سرور فیزیکی

دو نوع فوق ناظر وجود دارد:

فوق‌ناظر نوع۱[۲۸] که بر روی سیستم فیزیکی اجرا می‌شود و فوق‌ناظر نوع۲[۲۹]که ماشین‌های مجازی میهمان را به عنوان یک پروسس در سیستم‌عامل نصب‌شده بر روی سخت‌افزار اجرا می‌کند؛ که البته هر کدام از این پروسس‌ها کنترل کامل سیستم خود رادارد، که تنها بخشی از منابع سیستم فیزیکی اصلی را در اختیار دارد.

مجازی سازی سیستم‌عامل و بخش بندی این امکان را فراهم می‌کنند تا تعدد زیادی کاربرد تحت یک سیستم‌عامل و به‌طور کاملا ایزوله شده و هریک در محیط محافظت‌شده خود اجرا شوند. هر یک از این کاربردها بر روی سیستم خود اجرا شده و منابع خود را مدیریت می‌کند.

فوق ناظر

فوق ناظر پلتفرم مجازی سازی است که این امکان را به شما می‌دهد تا بتوانید چندین سیستم عامل را بر روی یک سیستم فیزیکی واحد که آن را میزبان[۳۰] می‌خوانند اجرا کنید. عملکرد اصلی فوق ناظر این است که برای هر یک از ماشین‌های مجازی یک محیط ایزوله شده محیا کند و همچنین ارتباط بین سیستم عامل‌های اجرا شده بر روی ماشین‌های‌مجازی و ارتباط آن‌ها با ماشین میزبان را مدیریت نماید.

اصطلاح فوق ناظر به سال ۱۹۷۲ بر می‌گردد؛ هنگامی که IBM برای کنترل مینفریم، system/ 370 را برای پشتیبانی از مجازی‌سازی بروزرسانی کرد.

---

[28] Type one Hypervisor
[29] Type two Hypervisor
[30] Host

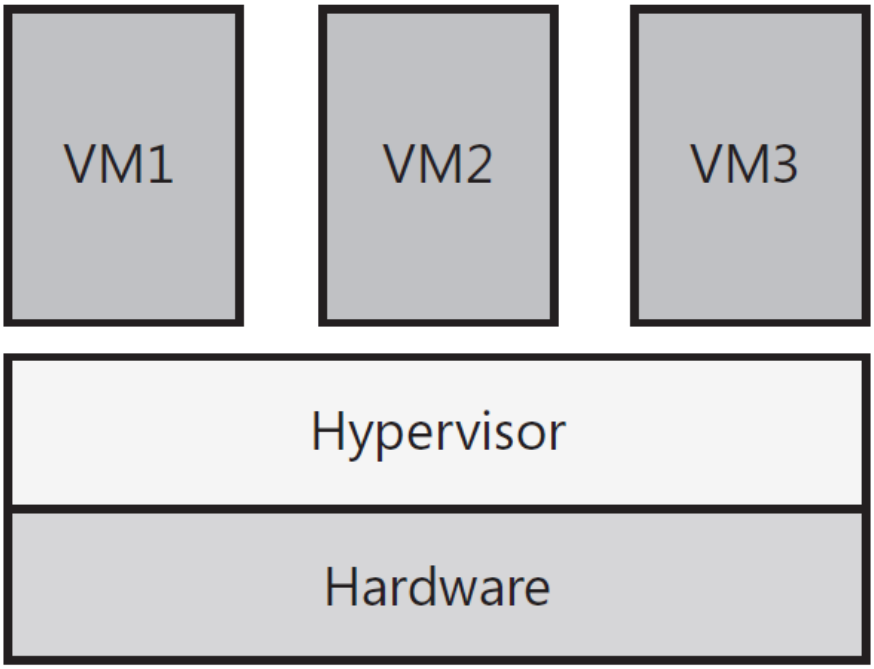
فوق ناظر را به دو طریق می‌توان دسته بندی کرد:

اول از نظر اجرا بر روی سخت‌افزار که به دو دسته نوع ۱[۳۱] و نوع ۲[۳۲] طبقه بندی می‌شود.

دوم از نظر طراحی که به دو گروه یکپارچه[۳۳] و ریزهسته[۳۴] دسته بندی می‌شوند.

فوق ناظر نوع ۱

فوق ناظر نوع ۱ بر روی سخت‌افزار اجرا شده و عملکرد آن شبیه برنامه کنترل است. سیستم عامل‌های میهمان[۳۵] هم بر روی ماشین‌های مجازی که بر روی لایه فوق‌ناظر قرار دارند اجرا می‌شوند. شکل ۱-۲ این موضوع را به تصویر کشیده است.



شکل ۲-۷. فوق‌ناظر نوع۱

از آنجایی که فوق ناظر نوع ۱ مستقیما بر روی سخت‌افزار اجرا می‌شوند، معمولا دارای کارایی و بهروری بهتر، دسترسی بالاتر و امنیت بیشتری نسبت دیگر فوق ناظرها دارند. بعضی از محصولات مجازی سازی نوع یک عبارتند از

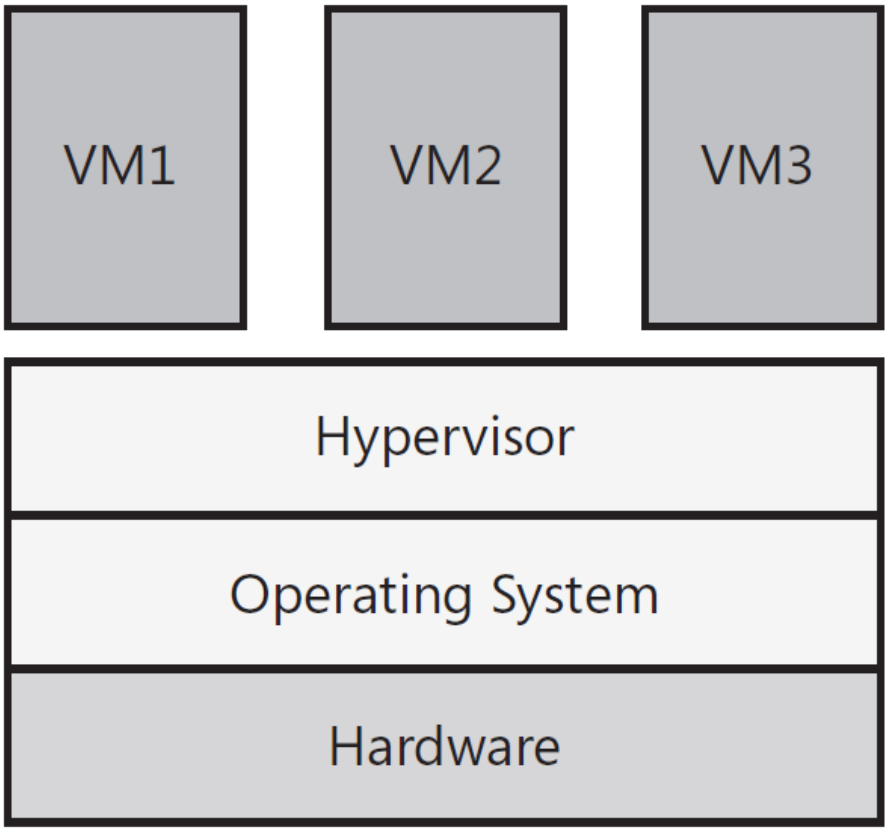
Microsoft Hyper-V
Citrix Xen Server
VMware ESX Server

فوق ناظر نوع ۲

فوق ناظر نوع ۲ بر روی سیستم عامل نصب شده بر روی کامپیوتر میزبان، اجرا می‌شود. سیستم عامل‌های میهمان هم بر روی ماشین‌های مجازی ساخته شده برروی فوق ناظر نصب و اجرا می‌شوند که این مسئله در شکل ۲-۸ نشان داده شده است.

---

[31] Type 1
[32] Type 2
[33] Monolithic
[34] Microkernel
[35] Guest OS



شکل ۲–۸ فوق‌ناظر نوع۲

با مقایسه‌ای بین دو شکل ۲–۷ و ۲–۸ متوجه خواهید شدکه در فوق ناظر نوع ۲ یک لایه اضافی بین سیستم عامل‌های میهمان و سخت‌افزار وجود دارد که این لایه بار اضافی را به سیستم تحمیل می‌کند که باعث افت کارایی این سیستم به نسبت سیستم‌های دارای فوق ناظر نوع۱ می‌شود. این مسئله (افت کارایی در فوق ناظر نوع۲) باعث ایجاد محدودیت بر تعداد ماشین‌های میهمان بر روی فوق ناظر نوع۲ می‌شود.

چند نمونه از فوق ناظرهای نوع ۲ به قرار زیر هستند.

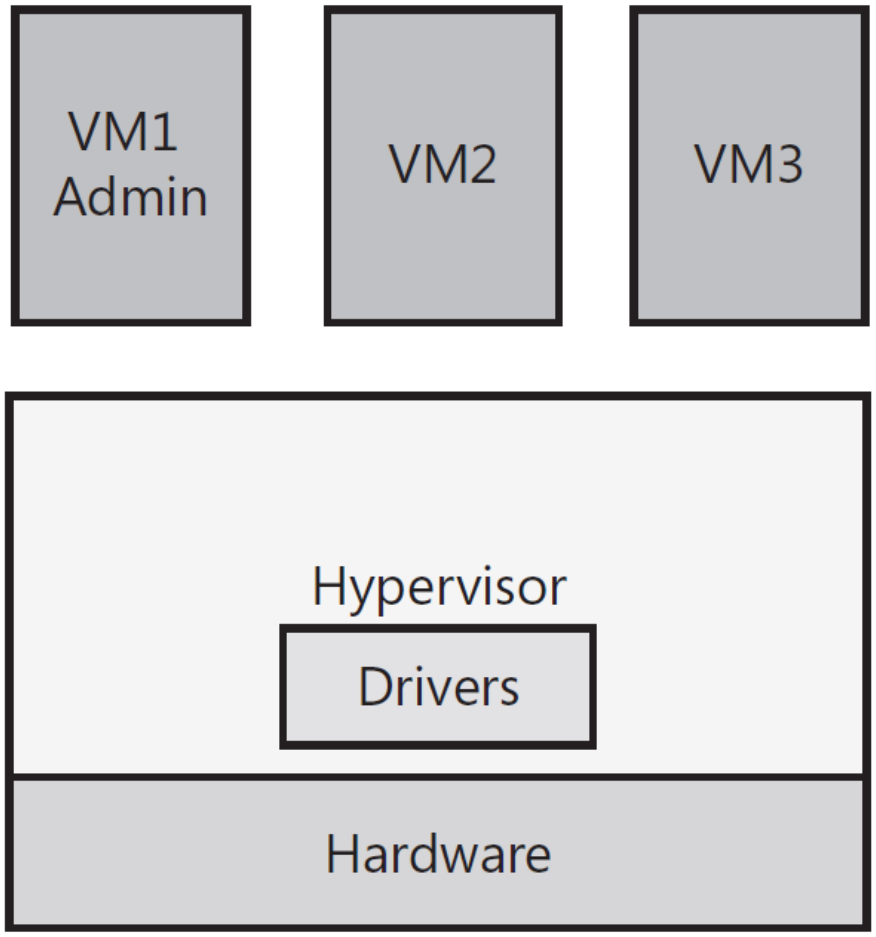
Microsoft virtual server
VMware server
Oracle virtual box

سیستم مجازی‌سازی رومیزی[۳۶] مایکروسافت موسوم به virtual pc نیز از معماری فوق‌ناظر نوع۲ استفاده می‌کند.

فوق ناظر یکپارچه

طراحی فوق ناظر یکپارچه طوری است که شامل راه‌اندازهای[۳۷] سخت‌افزاری اصطلاحا hyperviso–aware بوده و این راه‌اندازها توسط فوق‌ناظر مدیریت می‌شوند. شکل ۲–۹ این موضوع را به تصویر می‌کشد.

[36] Desktop
[37] Driver



شکل ۲-۹. فوق ناظر یکپارچه

این طراحی مزایا و معایبی دارد که از آن جمله اینکه این نوع از فوق‌ناظرها نیازی به قسمت کنترل‌کننده و یا سیستم عامل والد[۳۸] ندارد چرا که سیستم‌عامل‌های میهمان مستقیما و از طریق راه‌اندازهای hyperviso–aware موجود در فوق‌ناظر با سخت‌افزار در ارتباط هستند. و این یکی از مزیت‌های این نوع معماری است. از طرف دیگر این مسئله که راه اندازهای سخت‌افزاری بایستی برای این فوق ناظرها توسعه داده شوند مشکل بزرگی خواهند بود.

چرا که انواع مختلفی از سخت‌افزارها از سازندگان مختلف وجود دارد. نتیجه اینکه سازندگان این نوع از فوق ناظرها بایستی ارتباط بسیار نزدیکی با سازندگان سخت‌افزار داشته باشند تا نسخه Hypervisor-aware راه‌اندازهای سخت‌افزارها را تهیه کنند. و این یعنی اینکه سازندگان این نوع از پلتفرم‌ها بسیار وابسته به تولیدکنندگان سخت‌افزار هستند. همچنین این مسئله باعث می‌شود تا این نوع فوق‌ناظرها دارای محدودیت بیشتری برای پشتیبانی از سخت‌افزارها مختلف می‌باشند. فوق‌ناظر VMware ESX از این معماری بهره می‌برد.

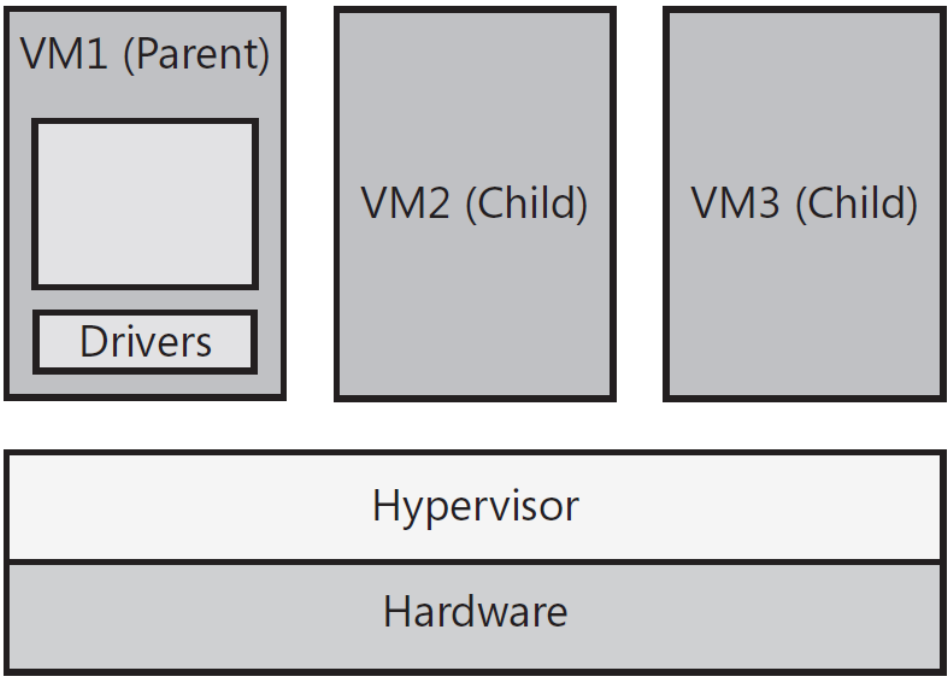
فوق ناظر ریز هسته

فوق‌ناظرهای ریزهسته نیازی به راه‌اندازهای سخت‌افزاری Hypervisor-aware ندارند؛ چرا که دارای سیستم عاملی هستند که شبیه به بخش ریشه یا والد عمل می‌کند. بخش والد محیط اجرایی که راه اندازهای سخت‌افزاری برای ارتباط با

[38] Parent

سخت‌افزارهای کامپیوتر میزبان لازم دارند رافراهم می‌کند. اصطلاح "بخش[۳۹]" را می‌توانید معادل با مفهوم ماشین مجازی به کار برید.

در پلتفرم‌های با فوق‌ناظر ریز هستند، بایستی راه اندازهای سخت‌افزاری بر روی سیستم‌عامل که در حال اجرا بر روی بخش والد است نصب شده و نیازی به نصب این راه‌اندازها بر روی تک تک سیستم‌عامل‌های میهمان نیست؛ چرا که هر گاه سیستم‌عامل‌های میهمان نیازی به ارتباط با سخت‌افزارهای کامپیوتر میزبان داشته باشند از طریق بخش والد بسادگی انجام می‌دهند. به عبارت دیگر در طراحی ریزهستند، سیستم عامل میهمان دسترسی مستقیمی ندارند بلکه از طریق بخش والد با سخت‌افزار ارتباط برقرار می‌کنند. شکل ۲-۱۰ طراحی ریز هسته را نمایش می‌دهد.



شکل ۲-۱۰. فوق‌ناظر ریزهسته

از آنجایی که معماری ریز هسته نیازی به راه اندازی سخت‌افزاری Hypervisor-aware ندارد، تعداد بسیار بیشتری از سخت‌افزارها را می‌تواند بکار گیرد. و البته ایراد این معماری هم این است که نیاز به بخش والد دارد.

فوق ناظر Microsoft Hyper-V از معماری ریز هستند استفاده می‌کند که از ویندوز سرور۲۰۰۸ بعنوان بخش والد بهره می‌برد.

۲-۲-۳-۱-۲ پیکربندی چندسیستم بطوری که از دید خارجی یک سیستم دیده شوند

ناظر پردازش موازی این امکان را در اختیار قرار می‌دهد تا چند سیستم یک کاربرد را اجرا کند (هر سیستم بخشی از کاربرد مورد نظر اجرا می‌کند) تا بتوان زمان پردازش را کم کرد. بدین ترتیب کاربرد به چندین بخش تقسیم می‌شود و به هر سیستم یک بخشی از آن داده می‌شود. هر گاه سیستم مد نظر بخش محول شده را پردازش کند، ناظر پردازش موازی، بخش دیگری را برای پردازش در اختیار آن سیستم قرار می‌دهد.

[39] Partition

ناظرمدیریت بار کاری (گاهی آن را ناظر تنظیم بار[40] هم می‌خوانند) این امکان را ایجاد می‌کند تا چند نسخه از یک کاربرد بطور همزمان به روی تعداد زیادی سیستم اجرا شوند. هر گاه درخواستی برای آن کاربرد وجود داشت ناظر مدیریت بار کاری درخواست را به سیستمی که بار کاری پائین‌تری دارد ارجاع می‌دهد.

ناظر دسترسی‌مستمر/ بازگشت از خطا/ بازیابی سیستم/هم شرایطی را ایجاد می‌کند تا افرادی که از سرویس‌های پردازشی استفاده می‌کند از خرابی در کاربرد، سیستم، مولفه‌های سیستم محافظت شوند. ناظر خرابی را شناسایی کرده و کاربرد را دوباره بر روی یک سیستم سالم اجرا می‌کند.

در حال حاضر تعداد زیادی شرکت بزرگ پشتیبان این تکنولوژی هستند و به روش‌های مختلف آن را ارائه می‌دهند. سیتریکس که در اکثر زمینه‌های مجازسازی وارد شده است، xen sourse را ارائه داده است. در بخشی فوق‌ناظر هم xen server را معرفی کرد. همچنین این شرکت نرم‌افزارهایی را هم برای مدیریت بار کاری ارائه کرده است.

مایکروسافت هم که در همه زمینه‌های کامپیوتری وارد شده است در سال ۲۰۰۳ Connectix را بکارگرفت محصول شرکت بعدها به hyper-V تغییر نام داد و البته در طول چند سال بسیار پیشرفت کرد. مایکروسافت همچنین در زمینه‌های پردازش‌موازی، مدیریت بار کاری، بازگشت از خطا، بازیابی سیستم نیز سیستم‌ها و نرم‌افزارهایی را ارائه داده است.

VMware هم که از پیشتازین سیستم‌های مجازی‌سازی است ESX را به عنوان یک فوق‌ناظر ارائه کرد.

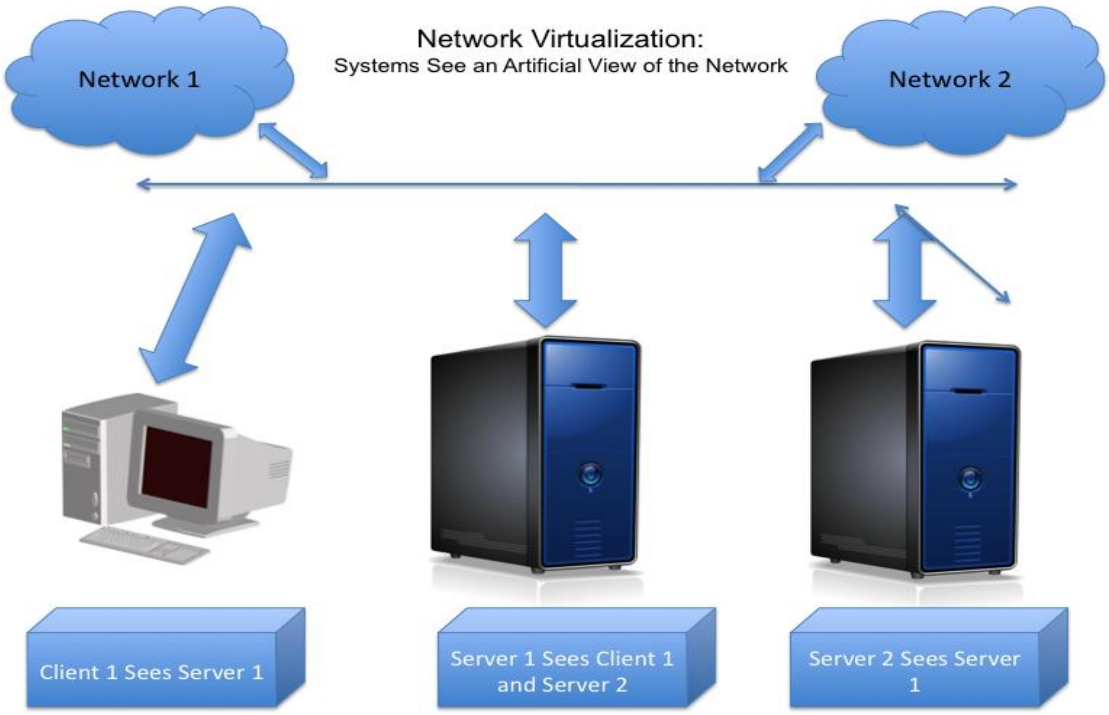
این شرکت همچنین سیستم انتقال[41] ماشین‌های مجازی بین سرورها را توسعه داد. VMware محصولاتی قدرتمندی را هم در رابطه با دسترسی‌مستمر، بازگشت از خطا و بازیابی‌سیستم معرفی کرده است.

۲-۲-۴ مجازی سازی شبکه[42]

تکنولوژی نرم‌افزاری و سخت‌افزاری که این امکان را ایجاد می‌کند تا دیدی از شبکه ایجاد کرد که با واقعیت و دید فیزیکی متفاوت باشد. مثلا به یک کامپیوتر شخصی اجازه داده شود تا تنها، سیستم‌هایی را ببیند که به او اجازه داده شده است؛ و یا مثلا کاری کرد تا چندین لینک در داخل شبکه یک لینک دیده شوند که مزیت آن بالا بردن کارایی و افزایش اطمینان در شبکه است.

مجازی سازی شبکه اشاره دارد به ابزاری که این امکان را می‌دهد تا بتوان دیدی ساختگی و مصنوعی از شبکه ایجاد کرد. و یا به عبارت می‌توان شبکه فیزیکی را از دید کامپیوتر و سرورها مخفی کرد. این مسئله در شکل ۲-۱۱ نشان داده شده است.

[40] load balancing monitors
[41] Migration
[42] Network Virtualization



شکل ۲-۱۱. مجازی‌سازی شبکه

احتمالا شما هم متوجه شده‌اید، تقریبا تمام مواردی که تحت عنوان مجازی سازی شبکه شناخته می‌شوند همان سرویس‌ها و امکانات رایج شبکه است. مثلا سرویس NAT، V-LAN یا همون LAN مجازی و یا لیست‌های دست‌یابی[۴۳] در مسیر یاب‌ها و سوئیچ‌های لایه سه؛ و بسیاری دیگر از تکنولوژی‌های شبکه از این دست هستند.

از کاربردهای تکنولوژی مجازی سازی شبکه می‌توان به بالا بردن کارایی شبکه، بهبود قابلیت دسترسی و افزایش امنیت شبکه اشاره کرد. از آنجایی که مجازی‌سازی شبکه ارتباط چندانی با موضوع این فصل ندارد، به جهت جلوگیری از اطناب، از توضیح بیشتر در این زمینه خودداری کرده و با معرفی چند شرکت برتر فعال در این زمینه به مطالب این بخش خاتمه می‌دهیم.

شرکت سیسکو که یکی از بزرگترین شرکت‌های فعال در زمینه تجهیزات شبکه است تعداد زیادی سرور شبکه که در مجازی سازی شبکه عمل می‌کنند ارایه کرده است.

شرکت HP هم توابع[۴۴] مجازی سازی را بعنوان بخشی از سیستم‌عامل سرور چندمنظوره خود ارائه می‌دهد.

شرکت IBM هم که یکی از قدیمی ترین شرکت‌های کامپیوتری است نیز مانند HP مجازی سازی را بعنوان بخشی از سیستم عامل سرور چند منظوره خود عرضه کرده است.

شرکت Junper Systems نیز تعداد زیادی سرورهای شبکه که کار مجازی‌سازی شبکه انجام می‌دهند ارائه می‌کند.

۲-۲-۵ مجازی‌سازی سیستم‌های ذخیره‌سازی داده[۴۵]

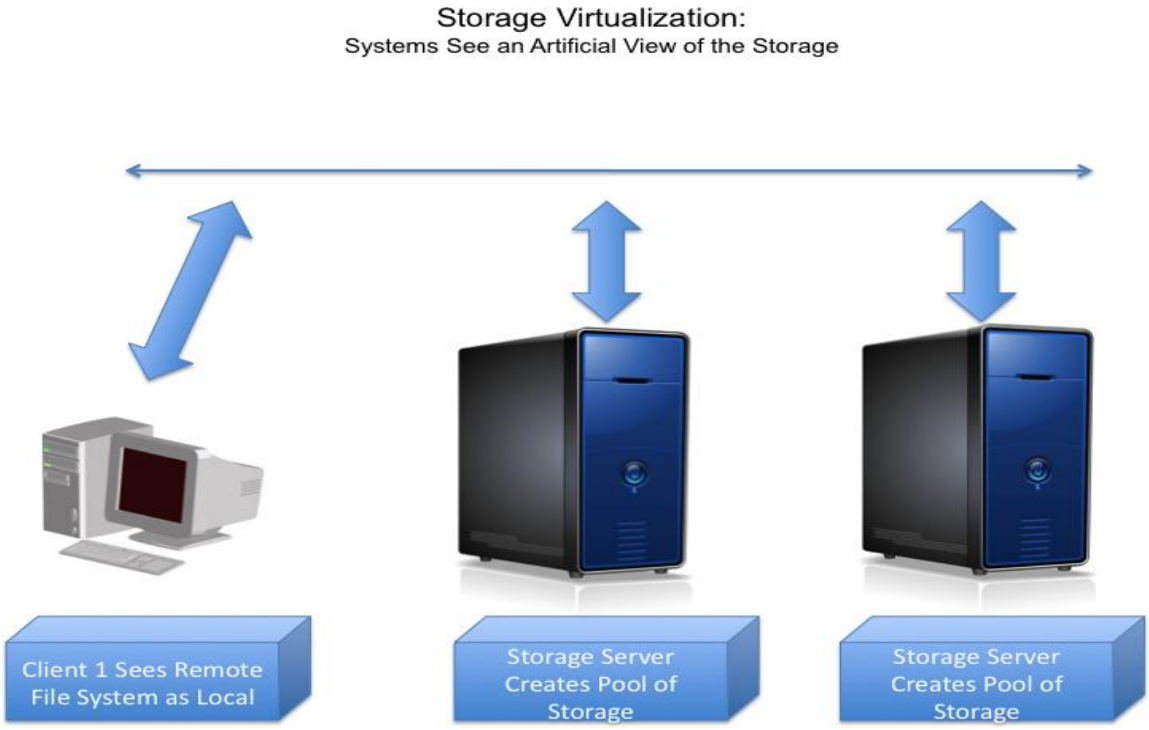
تکنولوژی نرم‌افزاری و سخت‌افزاری که باعث می‌شود تا جزئیات ذخیره‌سازی از قبیل محل ذخیره‌سازی و یا تکنولوژی بکار رفته در سیستم ذخیره‌سازی داده‌ها از کاربردها مخفی بماند. این تکنولوژی اجازه می‌دهد تا تعداد زیادی سیستم یک واحد ذخیره‌سازی را بین خود اصطلاحا share کنند بدون اینکه هر یک از دیگران اطلاعاتی داشته باشد.

[43] Access Lists
[44] Functions
[45] Storage Virtualization

این تکنولوژی همچنین اجازه میدهد تا از یک بسته در حال اجرا اصطلاحاsnapshot گرفته شود تا بتوان از این سیستم یک نسخه پشتیبان[۴۶] تهیه کرد بدون اینکه برای کاربردهای و تراکنشهای در حال اجرا مشکل و مراقب ایجاد شود.

مجازی سازی سیستم ذخیره‌سازی اغلب توسط سرورهای ذخیره‌سازی[۴۷] پشتیبانی می‌شود. کلاینت‌ها و سرورها نیازی ندارند بدانند فایل‌هایی که در حال پردازش آن‌ها هستند در کجا ذخیره شده‌اند. همچنین نیازی هم ندارند تا بدانند چه نوع از ذخیره‌سازها، داده‌ها و کاربردها را ذخیره کرده‌اند. مثلا دستگاه‌های ذخیره‌سازی می‌توانند دیسک سخت باشند یا SSD و یا هر تکنولوژی دیگر.

همانطور که در شکل ۲-۱۲ نشان داده شده است، مجازی‌سازی ذخیره‌سازی یک دید مصنوعی از شبکه ذخیره‌سازی ایجاد می‌کند که جزئیات شبکه فیزیکی را از کلاینت‌ها و سرورها مخفی می‌کند.



شکل ۲-۱۲. مجازی‌سازی در سیستم‌های ذخیره‌سازی

این سیستم توابع زیر را فراهم می‌کند:

- ایجاد سیستم فایل توزیع شده[۴۸]

سیستم ذخیره‌سازی راه دور طوری ساخته شده که از دید کلاینت به نظر برسد وسیله ذخیره‌ساز مستقیما به کامپیوتر متصل است.

- ایجاد درایوهای با اندازه غیرواقعی و دلخواه

در این سیستم می‌توان چندین ابزار ذخیره‌سازی را به یکدیگر متصل کرده تا از دید خارجی طوری به نظر برسد که یک واحد ذخیره‌سازی است.

- ایجاد آرایه‌های از ابزارهای ذخیره سازی

---

[46] Back Up
[47] Storage Server
[48] Distributed

داده‌ها و کاربردها می‌توانند بر روی چندین واحد ذخیره‌سازی توزیع شوند تا بدین‌طریق کارایی سیستم افزایش پیدا کنند. این سیستم همچنین می÷تواند قابلیت اطمینان سیستم را هم افزایش دهد؛ بدین صورت که یک داده واحد بر روی چندین واحد ذخیره‌سازی و یا سرور ذخیره‌سازی قرار می‌گیرد. اگر یکی از واحدها خراب شود داده‌ها از واحد دیگر قابل بازیابی است.

- امکان مدیریت بیشتر بر فضای ذخیره‌سازی

ابزارهای ذخیره‌سازی می‌توانند به چند فایل‌سیستم بخش‌بندی شوند تا بتوان از ابزارهای ذخیره‌سازی بهتر استفاده کرد.

- ایجاد سازوکاری برای Share کردن یک ابزار ذخیره سازی بین چند سیستم ناسازگار

مینفریم‌ها، لینوکس، یونیکس، ویندوز و دیگر سیستم عامل‌ها هر یک از مکانیسم متفاوتی برای ذخیره‌سازی و بازیابی داده‌ها وکاربردها استفاده می‌کنند. مجازی سازی ذخیره‌سازی این امکان رو فراهم می‌کند تا همه این سیستم‌عامل‌ها یک واحد ذخیره‌سازی و فایل‌های آن را بین خود share کنند.

سرورهای ذخیره‌سازی تعداد زیادی دستگاه ذخیره‌سازی را مدیریت می‌کنند و این سیستم اجازه می‌دهد تعداد زیادی سیستم همه منظوره[۴۹] به یک ذخیره‌ساز دسترسی داشته باشند. سیستم عامل سرور ذخیره‌سازی، اطلاعاتی دارد که می‌داند کدام سرور همه منظوره، به کدام واحد ذخیره‌سازی و کدام فایل‌سیستم اجازه دسترسی دارد. اگر این سرور ذخیره‌سازی، از طریق یک شبکه ذخیره داده خاص‌منظوره به یک سیستم همه‌منظوره متصل باشد، این پیکربندی را شبکه ناحیه ذخیره‌سازی[۵۰] و یا به اختصارSAN می‌گویند. ابزارذخیره‌سازی که از طریق شبکه دستیابی می‌شود را ذخیره‌ساز ضمیمه به شبکه[۵۱] و یا به اختصار NAS می‌گویند؛ خواه در یک شبکه SAN باشد، خواه یک شبکه LAN که توسط یک سیستم همه منظوره استفاده می‌شود.

اگر چه شرکت‌های زیادی در زمینه مجازی‌سازی ذخیره‌سازی فعال هستند، در زیر چند مورد از مهمترین بازیگران این عرصه را ذکر می‌کنم.

EMC کار خود را با ساخت دستگاه‌های ذخیره‌سازی مینفریم‌ها و کامپیوترهای شخصی آغاز کرد ولی با گذشت زمان شرکت به بازار سرورهای ذخیره‌سازی داده هم وارد شد و در حال حاضر انواع سیستم‌های را تولید می‌کند.

Hitachi انواع ابزارهای ذخیره‌سازی و سرورهای ذخیره‌سازی را برای مینفریم‌ها، سیستم‌های متوسط[۵۲] و سیستم‌های صنعتی استاندارد تولید می‌کنند.

HP سرورهای ذخیره‌سازی خودرا برای پشتیبانی از سیستم‌های متوسط و سیستم‌های صنعتی خود ارایه می‌کند.

IBM انواع مینفریم‌ها، سیستم‌های متوسط و صنعتی استاندارد خود را راهی بازارکرده. شرکت همچنین سرورهای ذخیره سازی که تمام نیازهای سیستم‌های خود را تامین می‌کند نیز تولید می‌نماید.

۲-۲-۶ امنیت در سیستم‌های مجازی‌سازی

تکنولوژی نرم‌افزاری که دسترسی به اجزای مختلف در محیط مجازی سازی را کنترل کرده و از دسترسی غیرمجاز و خرابکارانه جلوگیری می‌کند.

---

[49] Multi-Purpose
[50] Storage Area Network
[51] Network Attached Storage
52 midrange systems

امنیت محیط مجازی اشاره به ابزاری دارد که برای کنترل دستیابی به لایه‌های مختلف تکنولوژی مجازی لازم است. نظر به اینکه امنیت، موضوع این فصل نیست از توضیح بیشتر راجع به امنیت خودداری می‌کنیم.

۲-۲-۷ مدیریت محیط مجازی

تکنولوژی نرم‌افزاری که این امکان رو فراهم می‌آورد که چندین سیستم مجازی را مانند یک سیستم کامپیوتری منفرد مدیریت کرد.

مدیریت محیط مجازی اشاره به ابزاری دارد که به کمک آن می‌توان محیط مجازی را ایجاد، مشاهده و آنالیز، کنترل خودکار و بهینه‌سازی کرد. هر چه محیط مجازی پیچیده‌تر شود اهمیت این بخش نیز بیشتر می‌شود.

سیستم مدیریت محیط مجازی بایستی توابع و عملکردهای زیر را داشته باشد:

- ایجاد محیط مجازی ومولفه‌های آن
- نظارت بر محیط مجازی
- کنترل محیط مجازی و مولفه‌ها آن
- آنالیز وقایع ثبت شده جهت یافتن مشکلات پیکربندی، کارایی و عملکردی
- بهینه‌سازی استفاده از محیط مجازی و مولفه‌ها آن
- خود کارسازی استفاده از محیط مجازی ومولفه‌های آن

شرکت‌های زیادی در زمینه مدیریت سیستم‌های مجازی سازی فعال هستند که از آن جمله می‌توان به موارد زیر اشاره کرد:

شرکت CA که در این زمینه یکی از قدیمی ترین‌ها است.

شرکت HP که محصولات خود را در این زمینه سالهای زیادی است که ارائه کرده.

IBM Tivoli هم سابقه طولانی در زمینه نرم‌افزارهای مدیریت مجازی‌سازی دارد.

و البته مایکروسافت و VMware هم محصولاتی برای مدیریت سیستم‌های مجازی‌سازی خود ارائه کرده‌اند.

۳۹-۲-۳- چند اصطلاح – چند اشتباه

بسیاری اوقات یک تکنولوژی با موارد استفادههای موردی از آن تکنولوژی اشتباه گرفته می‌شود. مثلا در بحث مجازی سازی وقتی در مورد تکنولوژی ماشین‌مجازی که یکی از موارد پنج‌گانه مجازی‌سازی پردازش بحث می‌شود، بسیاری افراد (حتی متخصصین) با مجازی‌سازی سرور[۵۳] و مجازی‌سازی دسکتاپ[۵۴] اشتباه می‌گیرند. در این بخش سعی می‌کنیم چند واژه معمول در بحث مجازی‌سازی را تعریف کرده و مواد اشتباه را برطرف کنیم.

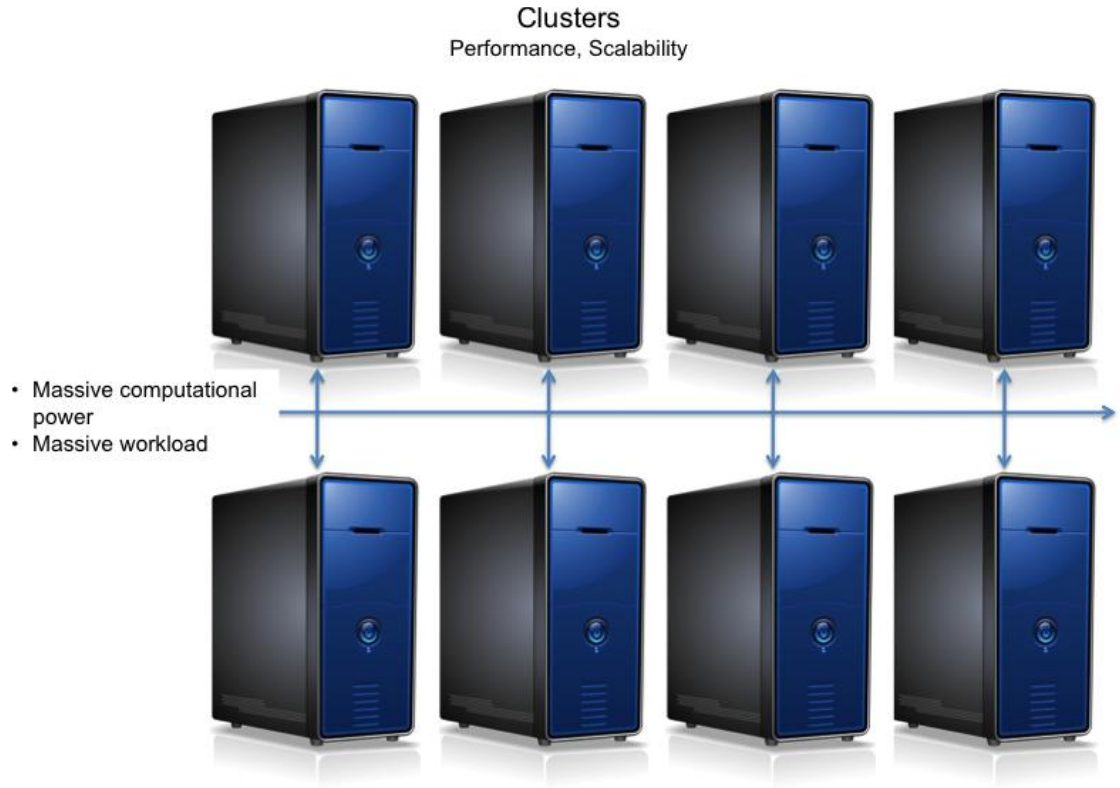
۲-۳-۱ کلاستر[۵۵]

تکنولوژی متفاوتی وجود دارند که از قدرت پردازش چندسیستم تحت مدیریت یک سیستم بهره می‌گیرند. اگر چه تکنولوژی‌های همه آن‌ها به عنوان کلاستر شناخته می‌شوند. در ادامه یک تعریف جامع از کلاسته ارائه می‌دهیم.

---

[53] Server Virtualization0
[54] Desktop Virtualizatin
[55] Cluster

یک کلاستر، مجموعه‌ای از کامپیوترهای جدا از هم است (معمولاً یکسان یا مشابه به لحاظ معماری سخت‌افزاری و ظرفیت محاسباتی) که از طریق شبکه اتصالی بسیار پرسرعت به یکدیگر متصل شده‌اند. شکل ۲-۱۳ تصویری از یک کلاستر به دست می‌دهد.



شکل ۲-۱۳. کلاستر

عملکرد یک کلاستر را می‌توان بسیار مشابه با یک مالتی‌پروسسور دانست با این تفاوت که یک کلاستر مزایای زیادی در مقایسه با ابررایانه‌های سنتی (مالتی‌پروسسورهایی که تا اواخر ۱۹۹۰ ساخته می‌شدند) دارد. هزینه تهیه یک کلاستر بسیار کمتر از یک ابر رایانه سنتی با توان پردازشی مشابه است.

ابررایانه‌های سنتی، معمولاً معماری غیرمتغیر[۵۶] و Hard-Wired داشتند، بنابراین معمولاً مقیاسپذیر نبودند، در صورتی که افزودن به توان محاسباتی یک کلاستر ساده‌تر است. با توجه به رشد قدرت پردازنده‌ها و پیدایش شبکه‌های کامپیوتری سریع، اکثر ابررایانه‌های امروزی از معماری کلاستر استفاده می‌کنند و ابر رایانه‌های سنتی، از نظر نسبت کارایی به قیمت، قابل مقایسه با ابررایانه‌های مدرن امروزی نیستند.

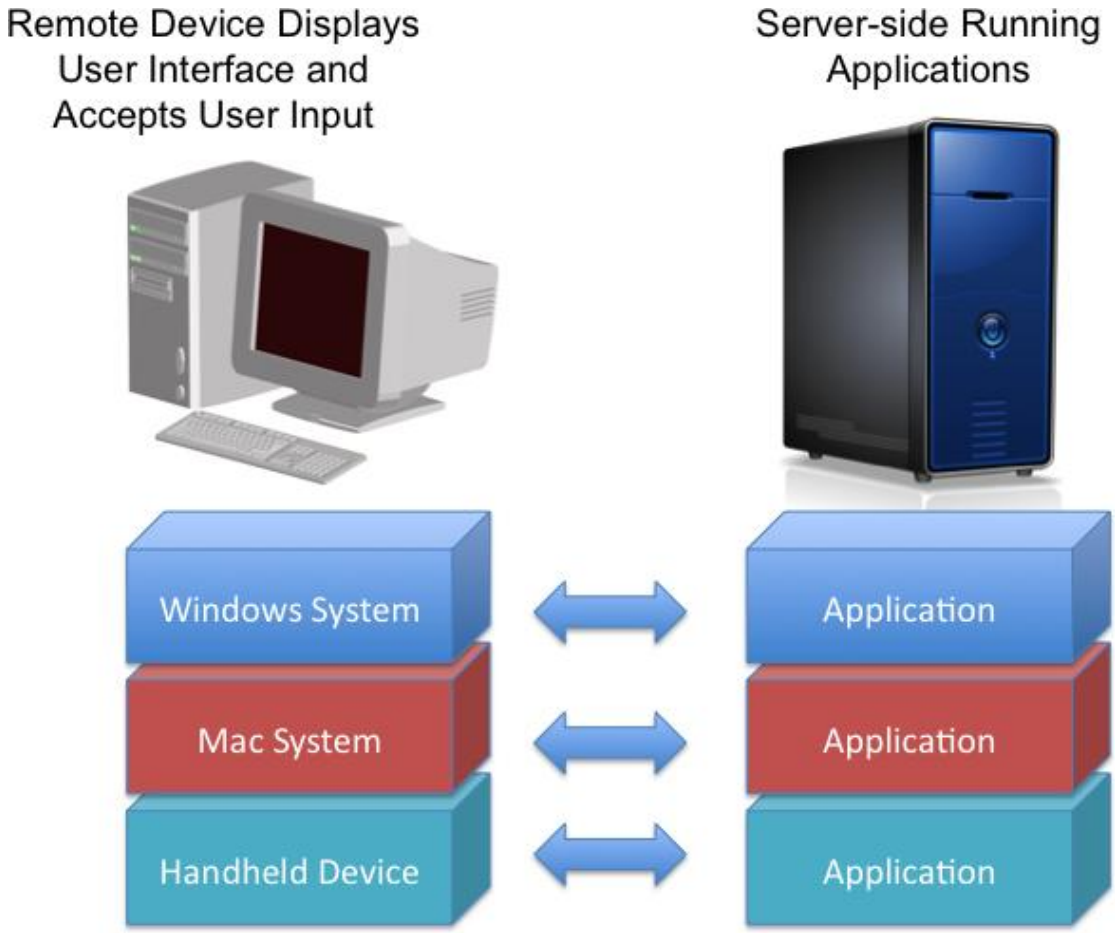
۲-۳-۲ مجازی سازی دسکتاپ

مجازی سازی دسکتاپ، استفاده از چندین تکنولوژی مجازی سازی به طور جداگانه ویا با هم می‌باشد که در ادامه به چند مورد از آن اشاره می‌کنیم.

هر گاه مجازی سازی دسکتاپ در مورد دسترسی از راه دور به یک سیستم فیزیکی یا مجازی مدنظر باشد، تکنولوژی مورد استفاده مجازی سازی دسترسی خواهد بود. در این حالت تصویر رابط‌کاربری[۵۷] کاربرد از طریق شبکه منتقل شده و به

[56] Fixed
[57] User Interface

کاربر مقصد می‌رسد. داده‌های ورودی کاربر هم به همین طریق از طریق شبکه به کاربرد در حال اجرا در کامپیوتر مبداء منتقل می‌شود. این موضوع در شکل ۲-۱۴ نشان داده شده است. شرکت‌های مثل مایکروسافت، VMware و سیتریکس، نرم‌افزارهای سمت‌کلاینت برای لوح رایانه‌ها[58]، تلفن‌های هوشمند، لب تاپ‌ها و PCها ارائه کرده‌اند که این امکان را به کاربران می‌دهند تا به برنامه‌های کاربردی که در هر جای از شبکه در حال اجرا است دسترسی داشته باشند.



شکل ۲-۱٤. مجازی‌سازی دسکتاپ از طریق مجازی‌سازی دسترسی

گاهی اوقات اصطلاح مجازی‌سازی دسکتاپ در مورد کپسوله کردن کاربرد به کمک تکنولوژی مجازی‌سازی کاربرد و ارسال آن را به کلاینت موردنظر جهت اجرا به کار می‌رود؛ که البته بایستی سیستم‌عامل مناسب بر روی کلاینت نصب شده‌باشد. مثلا برای کاربردهای ویندوزی بایستی سیستم‌عامل نصب شده بر روی کلاینت نسخه مناسبی از ویندوز باشد. شکل ۲-۱۵ را مشاهده کنید.

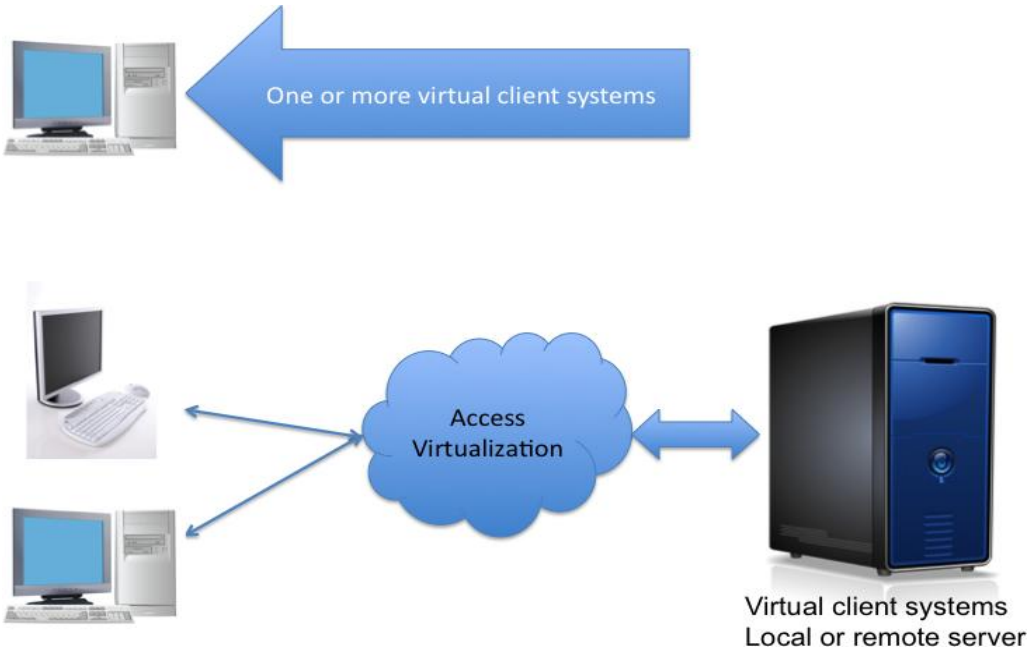
[58] Tablets

Desktop Virtualization
Application Streaming



شکل ۲-۱۵. مجازی‌سازی دسکتاپ از طریق مجازی‌سازی کاربرد

در مواقعی هم مجازی‌سازی دسکتاپ در مورد کپسوله کردن کل پشته کاربرد که در حال اجرا بر روی کلاینت است بکارمی‌رود. در این حالت قابلیت جابه‌جایی سیستم کلاینت مجازی کپسوله شده بسیار بالا خواهد بود. تصویر ۲-۱۶ این موضوع را نشان می‌دهد.



شکل ۲-۱۶. مجازی‌سازی دسکتاپ از طریق مجازی‌سازی پردازش

در زیر حالت مختلف مورد اخیر آورده شده است:

- یک یا چند سیستم کلاینت مجازی بر روی یک کلاینت فیزیکی منفرد می‌توانند اجرا شوند. در این حالت این امکان فراهم می‌شود تا برنامه‌های ناهمگون و ناسازگار بتوانند در کنار هم بطور همزمان اجرا شوند.

- سیستم کلاینت مجازی می‌تواند بر روی سرور تیغه‌ای[۵۹] محلی ویا نصب شده در داخل مرکزداده[۶۰] سازمان، اجرا شود. رابط کاربری هم می‌تواند از طریق شبکه بر روی یک PC معمولی، لب تاپ، لوح‌رایانه و یا یک thin client به کمک تکنولوژی مجازی سازی دسترسی، قابل دستیابی باشد.

از اونجایی که شرکت‌ها برای همه این موارد یک تعریف بکار می‌برند، مجازی سازی دسکتاب می‌تواند کمی گیج کننده باشد.

۳-۳-۲ مجازی سازی سرور

مجازی سازی سرور همان استفاده از تکنولوژی ماشین مجازی و یا مجازی سازی سیستم‌عامل و بخش‌بندی[۶۱] برای راه‌اندازی چندین سرور مجازی با بار کاری مجزا بر روی یک سرور فیزیکی است. شکل ۷-۹ را ببینید. اگر تکنولوژی مجازی‌سازی سیستم‌عامل و بخش‌بندی برای این کار استفاده شود تمام بار کاری بایستی توسط یک سیستم عامل منفرد انجام شود؛ و اگر تکنولوژی ماشین‌مجازی استفاده شود، هر ماشین مجازی یک سیستم‌عامل را اجرا می‌کند. این سیستم‌عامل‌ها می‌توانند نسخه‌های مختلف یک سیستم عامل باشند و یا حتی سیستم‌عامل‌های مختلف از شرکت‌های مختلف مثل ویندوز، لینوکس، یونیکس و.... این تکنولوژی باعث افزایش بهره‌وری سیستم (کاهش اوقات بیکاری سیستم) می‌شود.

۳۹-۳- معرفی مجموعه VMware vSphere 5

vSphere 5 نسل پنجم از تکنولوژی مجازی‌سازی شرکت VMware است که قبلا با نام VMware Infrastructure عرضه می‌شد. این مجموعه عظیم کاملترین ابزار برای راه اندازی سیستم مجازی سازی سرور با پشتیبانی از انواع سیستم‌عامل‌های میهمان و همچنین پشتیبانی از انواع تکنولوژی‌های پردازشی و ذخیره‌سازی می‌باشد. vSphere از اجزای مختلف برای اهداف مختلف استفاده می‌کنند که طی این بخش این اجزا را معرفی کرده ودر بخش‌ها آتی نحوه راه‌اندازی، پیکربندی و کارکرد بعضی از این قسمت‌هارا خواهیم گفت.

مجموعه WMware vSphere از مولفه‌ها و کاربردهای زیر تشکیل شده است:

- VMware ESXi
- VMware vCenter Server
- vSphere Update Manager
- VMware vSphere Client and vSphere Web Client
- VMware vShield Zones
- VMware vCenter Orchestrator
- vSphere Virtual Symmetric Multi-Processing
- vSphere vMotion and Storage vMotion
- vSphere Distributed Resource Scheduler
- vSphere Storage DRS
- Storage I/O Control and Network I/O Control
- Profile-Driven Storage
- vSphere High Availability

[59] blade server
[60] Data center
[61] Partitioning

- vSphere Fault Tolerance
- vSphere Storage APIs for Data Protection and VMware Data Recovery

البته این مجموعه، تمام اجزای تکنولوژی مجازی‌سازی VMware را پوشش نمی‌دهد؛ بلکه بسیاری از ابزارهای شرکت WMware که در زمینه مجازی‌سازی و پردازش ابری ارائه شده‌اند بطور جداگانه و خارج از این مجموعه فروخته می‌شوند که برخی از آن‌ها عبارتند از:

- VMware vCloud Director
- VMware vCloud Request Manager
- VMware vCenter AppSpeed
- VMware vCenterSite Recovery Manager

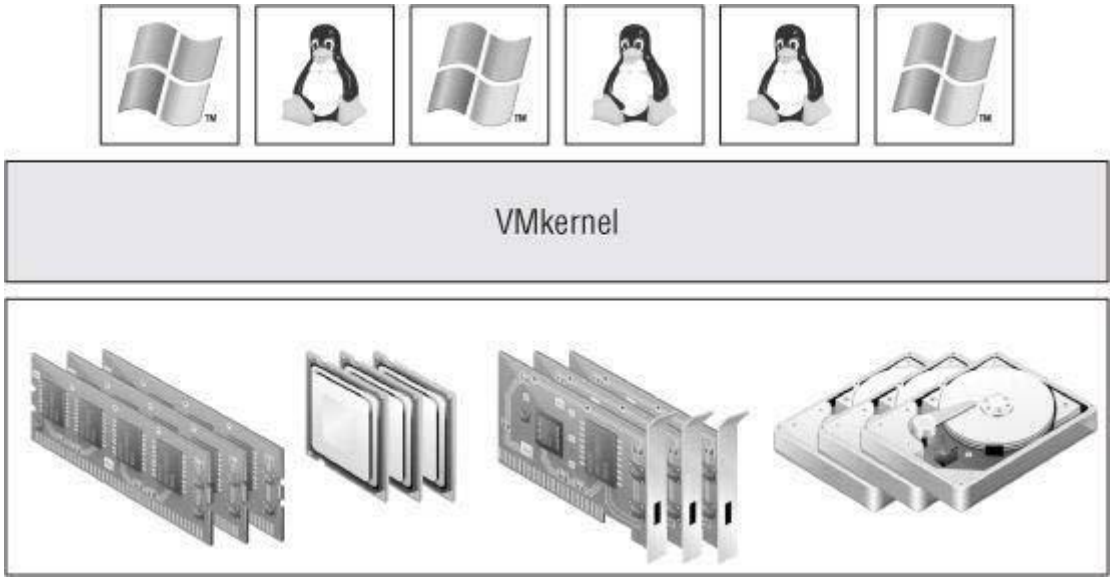
حال هر یک از اجزای مجموعه vSphere را توضیح می‌دهیم.

۳۹-۱-۳- *VMware ESXi*

هسته مجموعه vSphere را فوق‌ناظر آن تشکیل می‌دهد. ESXi لایه فوق ناظر مجموعه vSphere است. البته در نسخه‌های قبلی vSphere هم ESX و هم ESXi به عنوان فوق‌ناظر استفاده می‌شد ولی در نسخه ۵ فقط ESXi ارائه می‌شود.

هر چند هر دو فوق ناظر دارای موتور مجازی‌سازی یکسان و ویژگی‌های برابر هستند؛ در نسخه ESX یک کنسول سرویسی پایه لینوکسی نیز وجود دارد که هر یک از کاربران به آن دسترسی مستقیم داشتند.

علیرغم حذف کنسول از ESXi این فوق ناظر تمام قابلیت‌ها و ویژگی‌های ESX را پشتیبانی می‌کند. و دلیل این امر هم این است که مبنای مجازی سازی در ESXi را vmkernel تشکیل می‌دهد که در داخل کنسول سرویس قرار ندارد. وظیفه vmkernelمدیریت دسترسی ماشین‌های مجازی به سخت‌افزار به کمک زمان‌بندی CPU، مدیریت حافظه و مدیریت پردازش داده سوئیچ‌های مجازی می‌باشد. شکل ۳-۱ ساختار VMware ESXi را نشان می‌دهد.



شکل ۳-۱ . ساختار ESXi

ESXi دارای قدرت بالایی در ارائه منابع به ماشین‌های مجازی می‌باشد در جدول ۳-۱ به برخی از این ویژگی‌ها اشاره شده است.

جدول ۳-۱. قابلیت‌های ESXi

COMPONENT	VMWARE ESXI 5 MAXIMUM
Number of virtual CPUs per host	2048
Number of cores per host	160
Number of logical CPUs (hyperthreading enabled)	160
Number of virtual CPUs per core	25
Amount of RAM per host	2 TB

۳۹-۳-۲- *VMware vCenter Server*

vCenter Server مانند Active Directory ابزاریست برای مدیریت متمرکز تمام ماشین‌های ESXi وتمامی متعلقات و ماشین‌های مجازی ساخته شده بر روی آن‌ها. همچنین برای کمک به توسعه‌پذیری محیط vCenter Serverیک پایگاه داده back-end برای نگهداری اطلاعات مربوط به میزبآن‌ها و ماشین‌های مجازی بکار می‌گیرد، که این بانک اطلاعاتی می‌تواند Microsof SQL و یا Oracle باشد. در نسخه‌های قبلی vSphere، vCenter Server , فقط می‌توانست بر روی ویندوز اجرا شودولی در نسخه ۵ یک appliance[۶۲] پایه لینوکس همراه با مجموعه ارائه شده است.

البته بدون استفاده از vCenter Server هم می‌توان سرورهای ESXi را بصورت منفرد مدیریت کرد ولی برای استفاده از قابلیتهای بسیار ارزشمند مجموعه مجازی سازی VMware نظیر، vMotion، زمان‌بند منابع توزیع شده[۶۳]، قابلیت دسترسی مستمر[۶۴]، سیستم تحمل خطا[۶۵] و بسیاری از قابلیت‌های دیگر که در بخش‌های بعدی همگی آن‌ها توضیح داده خواهند شد، استفاده از vCenter لازم است.

۳۹-۳-۳- *vSphere Update Manager*

update manager پلاگینی[۶۶] است برای vCenter Server که به کمک آن می‌توان سرورهای ESXi و ماشین‌های مجازی انتخاب شده را با آخرین بروزها[۶۷] و وصله[۶۸] کرد. Update Manager توابع زیر را فراهم می‌آورد:

---

[۶۲] appliance درواقع ماشین‌های مجازی پیش ساخته‌ای هستند که به راحتی می‌توان به عنوان یک ماشین مجازی بر روی سرورهای ESXi اجرا کرد.

[63] Distributed Resource Scheduler

[64] High Availability

[65] Fault Tolerance

[66] Plug-in

[67] Up dates

[68] Patch

- بررسی و تشخیص سیستم‌هایی که نیاز به بروز شدن دارند.
- نصب خودکار بروزها
- یکپارچگی کامل با دیگر قابلیت‌های vSphere مثل سیستم زمان‌بند منابع توزیع شده

۳۹-۳-۴- *vSphere Client and vSphere web Client*

vCenter Server یک چارچوب مدیریتی متمرکز برای مدیریت میزبآن‌های ESXi ایجاد می‌کند ولی امکان دسترسی به خود vCenter Server از طریق vSphere Client خواهد بود؛ یعنی تمام دسترسی‌ها، پیکربندی‌ها و... از طریق vSphere Client انجام می‌شود. البته سیستمی که vCenter Server بر روی آن نصب شده است نیز خود می‌تواند میزبان vSpher Client نیز باشد. همانطور که قبلا نیز گفته شد بدون اتصال vSphere Cilent به vCenter Server و فقط با اتصال به ESXi به طور منفرد و به کمک vSphere Client می‌توان ESXiها را مدیریت کرد. شکل ۱ را نگاه کنید.

vSphere web Client یک سیستم مدیریت ESXiها را از طریق وب بروزر[۶۹] و البته تنها از طریق vCenter Server ایجاد می‌کند. البته تمام ویژگی‌های مجموعه مجازی‌سازی شرکت VMware از طریق vSphere web Client در دسترس نخواهد بود.

۳۹-۳-۵- *VMware vShield Zones*

یک دیوار آتش[۷۰] مجازی است که به کمک آن می‌توان ترافیک شبکه در داخل سوئیچ‌های شبکه مجازی را مشاهده و مدیریت کرد.

همچنین می‌توان به کمک آن سیاست‌های امنیتی خاصی را بر روی گروهی از ماشین‌های مجازی اعمال کرد که حتی در صورت انتقال یک ماشین مجازی به میزبان دیگر از طریق DRS و vMotion این سیاست‌ها حفظ شوند.

۳۹-۳-۶- *VMware vCenter Orchestrator*

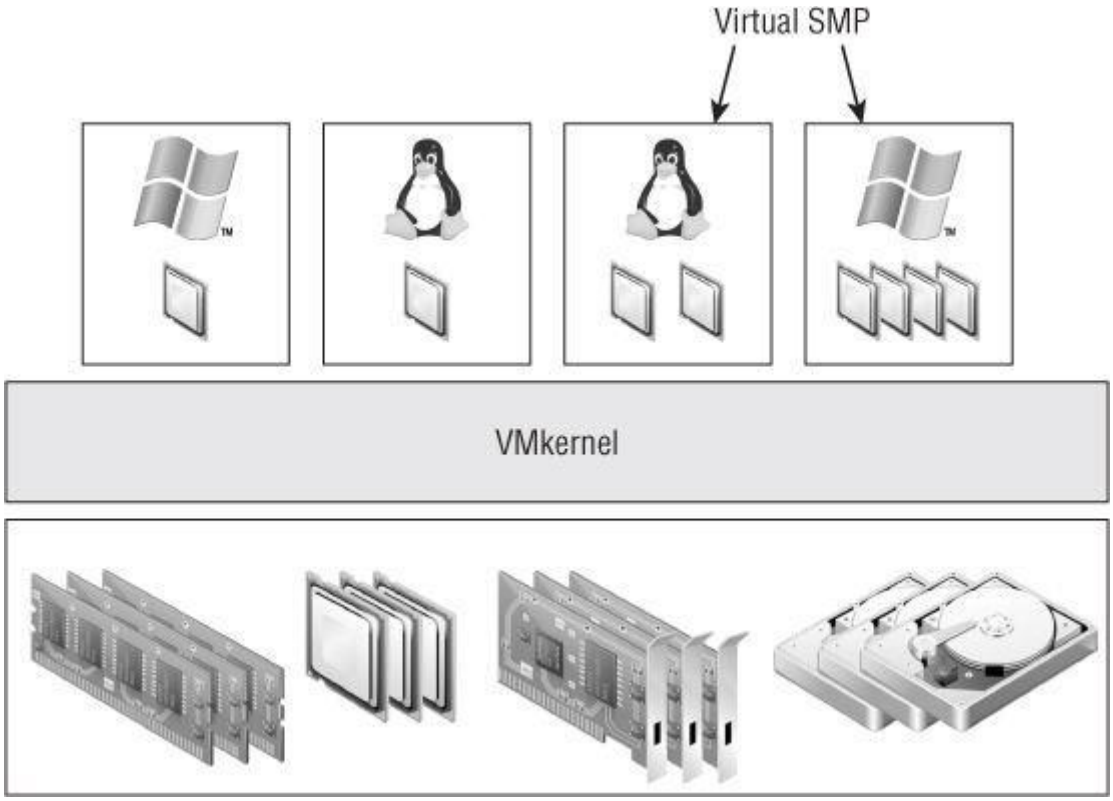
vCenter Orchestrator یک موتور خودکار ساز جریان کاری است که با vCenter Server به طور اتوماتیک نصب می‌شود. به کمک این ابزار می‌توان بسیاری از اعمال vCenter Server را بصورت خودکار درآورد که این کارها می‌توانند ساده و یا بسیار پیچیده باشند.

۳۹-۳-۷- *چند پردازشی متقارن مجازی*[۷۱]

این تکنولوژی به مدیران شبکه این امکان را می‌دهد تا بتوانند ماشین‌هایی مجازی با چند پردازنده مجازی ایجاد کنند. شکل ۳-۲ تفاوت بین چندپردازنده‌ای در میزبآن‌های ESXi وچندپردازنده مجازی را نشان می‌دهد.

---

[69] Web Browser
[70] Fire wall
[71] Virtual Symmetric Multi-Processing



شکل ۳-۲. چند پردازشی متقارن مجازی

بدین طریق کاربردهایی که برای اجرا شدن نیاز به چندپردازنده دارند می‌توانند در این ماشین‌های مجازی اجرا شوند. در vSphere 5 این قابلیت با اضافه شدن امکان ایجاد پردازنده‌های مجازی یاچند هستنه مجازی توسعه داده شده است.

۳۹-۳-۸- *vSphere vMotion and vSphere Storage vMotion*

vMotion که live migration نیز خوانده می‌شود ویژگی در ESXi و vCenter Server است که اجازه می‌دهد ماشین‌های مجازی در حال اجرا از یک میزبان فیزیکی به میزبان دیگر منتقل شوند بدون حتی لحظه‌ای خاموش شدن ماشین مجازی و قطع شدن اتصال ماشین مجازی به شبکه.

vMotion محتویات در حال اجرا(حافظه اصلی) را از یک سیستم به سیستم دیگر منتقل می‌کند اما محتویات سیستم ذخیره سازی دست ناخورده در جای خود باقی می‌مانند. Storage vMotion امکانی است برای انتقال محتویات دیسک مجازی یک سیستم مجازی خاموش ویا در حال اجرا از یک واحد ذخیره‌سازی به یک واحد ذخیره‌سازی دیگر بدون جابه جایی ماشین پردازش. یعنی محل اجرای ماشین مجازی تغییر نمی‌کند، و این در حالی اتفاق می‌افتد که ماشین مجازی روشن بوده و طی زمان انتقال واحد ذخیره‌سازی خللی در کار آن ایجاد نمی‌شود.

۳۹-۳-۹- سیستم زمانبند منابع توزیع شده[۷۲]

vMotion یک عمل دستی[۷۳] است یعنی مدیر سیستم باید بطور دستی عمل vMotin را انجام دهد. اگربخواهیم با توجه به نیاز مثلا برای تنظیم بار میزبآن‌های ESXi عمل vMotion بطور خودکار انجام شود، اینجاست که پای زمان‌بند منابع توزیع شده و یا به اختصار DRS وسط می‌آید.

[72] Distributed Resource Scheduler

قبل از ادامه بحث در حد چند خط در مورد کلاستر در vSphere توضیح دهیم.

در بخش قبلی با مفهوم کلاستر آشنا شدید نیازی به تکرار دوباره نیست. در مجموعه vSphere، کلاستر، مجموعه‌ای از میزبآن‌های ESXi است که منابع خود را در یک استخر منابع[۷۴] به اشتراک می‌گذارند. به عبارت دیگر کلاستر ESXi، یک تجمیع ضمنی توان پردازشی و حجم حافظه‌های تمام میزبآن‌های عضو کلاستر است.

حال برمی‌گردیم به موضوع DRS. اهداف و وظایف DRS در دو بند خلاصه می‌شود:

- در هنگام شروع(روشن شدن ماشین مجازی)، DRS سعی می‌کند ماشین‌های مجازی را در میزبانی اجرا کند که دارای بار پردازشی کمتری باشد.
- هنگامی که ماشین مجازی در حال اجرا است، DRS مدام (هر ۵ دقیقه یکبار) در حال جستجو و اندازه‌گیری است تا ماشین‌های مجازی را به میزبانی انتقال دهد که برای منابع مورد نیازشان، کمترین رقابت وجود داشته باشد.

مورد اول که معمولا Intelligent Placement نیز خوانده می‌شود اشاره به این مفهوم دارد که در هنگام روشن‌شدن ماشین مجازی که در داخل یک کلاستر قرار دارد، ماشین مجازی برای اجرا به میزبانی منتقل می‌شود که از لحاظ منابع آزاد موجود بهترین باشد. بند دوم هم این موضوع را بیان می‌کندکه حتی وقتی ماشین‌های مجازی روشن هم هستند، DRS دائما سعی می‌کند بهترین میزبان ESXi را از نظر منابع آزار موجود که داخل همان کلاستر قرار دارد، برای انتقال ماشین مجازی انتخاب کند.

مثل وقتی در هنگام روشن بودن چندین ماشین مجازی عضو کلاستر اگر یک یا چند تا از ماشین‌های مجازی بار پردازش بالایی را به سیستم تحمیل کنند، DRS به طور خودکار یک یا چند تا از آن‌ها را به ESXiهای عضو همان کلاستر که منابع پردازشی آزاد بیشتری دارند منتقل می‌کند.

۳۹-۳-۱۰- vSphere Storage DRS

همانطور که DRS بار پردازش بر روی ESXiها را تنظیم می‌کند، Storage DRS با جا بجایی ماشین‌های مجازی بار ترافیکی بر روی سرورهای ذخیره سازی را متعادل می‌کند. البته مانند DRS، Storage DRS هم در داخل یک کلاستر عمل می‌کند. همانگونه که DRS از تکنولوژی vMotion برای متعادل کرد-ن سیستم استفاده می‌کند. Storage DRS هم از Storage vMotion بهره می‌گیرد.

۳۹-۳-۱۱- سیستم کنترل ورودی خروجی شبکه و کنترل ورودی خروجی سیستم‌های ذخیره سازی

vSphere کنترل بسیار زیادی بر روی تخصیص منابع پردازشی همچنین حافظه‌های اصلی به ماشین‌های مجازی دارد. قابلیتی مشابه نیز در اختصاص دادن ترافیک ورودی – خروجی شبکه و سیستم‌های ذخیره‌سازی به ماشین‌های مجازی وجود دارد.

---

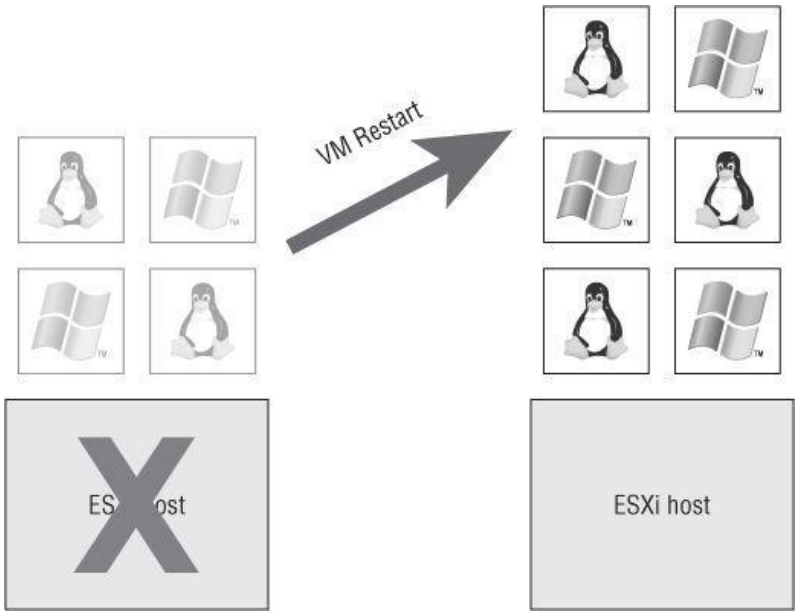
[73] Manual
[74] Resource Pool

سیستم کنترل ورودی-خروجی ذخیره‌سازها این امکان را به مدیران می‌دهد تا به هر یک از ماشین‌های مجازی یک اولویت در دسترسی به منابع ذخیره‌سازی اختصاص دهدند تا در صورت رقابت بین ماشین‌های مجازی در دسترسی به ذخیره‌سازها، این اولویت‌ها اعمال شوند. این قابلیت در vSphere5 فقط در ذخیره سازهایی با سیستم فایل VMFS , NFS وجود دارد.

سیستم کنترل ورودی-خروجی شبکه هم قابلیتی مشابه است؛ ولی در دسترسی به کارت‌های شبکه فیزیکی. این سیستم به مدیران شبکه این امکان را می‌دهد تا با اختصاص دادن اولویتی به ماشین‌های مجازی دسترسی آن‌ها به ترافیک و پهنای باند را مدیریت کنند.

۳۹-۳-۱۲- قابلیت دسترسی مستمر[۷۵] (HA)

نگرانی که ممکن است پیش بیاید این است که اگر چندین سرور بر روی یک سرور فیزیکی اجرا شوند در صورت خراب شدن سرور فیزیکی تمام سرورهای مجازی ازکار خواهد افتاد. دسترسی مستمر پاسخی به این مشکل است. عملکرد این تکنولوژی بدین‌صورت است که ابتدا دو یا چند سرور فیزیکی در قالب یک کلاستر قرار می‌گیرند. ماشین‌های مجازی بر روی سرورهای فیزیکی کلاستر توزیع می‌شوند. اگر یکی از سرورها خراب شود، ماشین‌های مجازی روی آن سرور به سرورهای دیگر عضو آن کلاستر منتقل می‌شوند. در این بین ماشین‌های مجازی اجرا شده به روی سرور خراب شده قبل از انتقال ریست می‌شوند. تمام این اعمال بطور کاملا اتوماتیک انجام می‌شوند. شکل ۳-۳ این مسئله را به تصویر کشیده است.



شکل ۳-۳. قابلیت دسترسی مستمر. در حین انتقال، ماشین‌های مجازی ریست می‌شوند

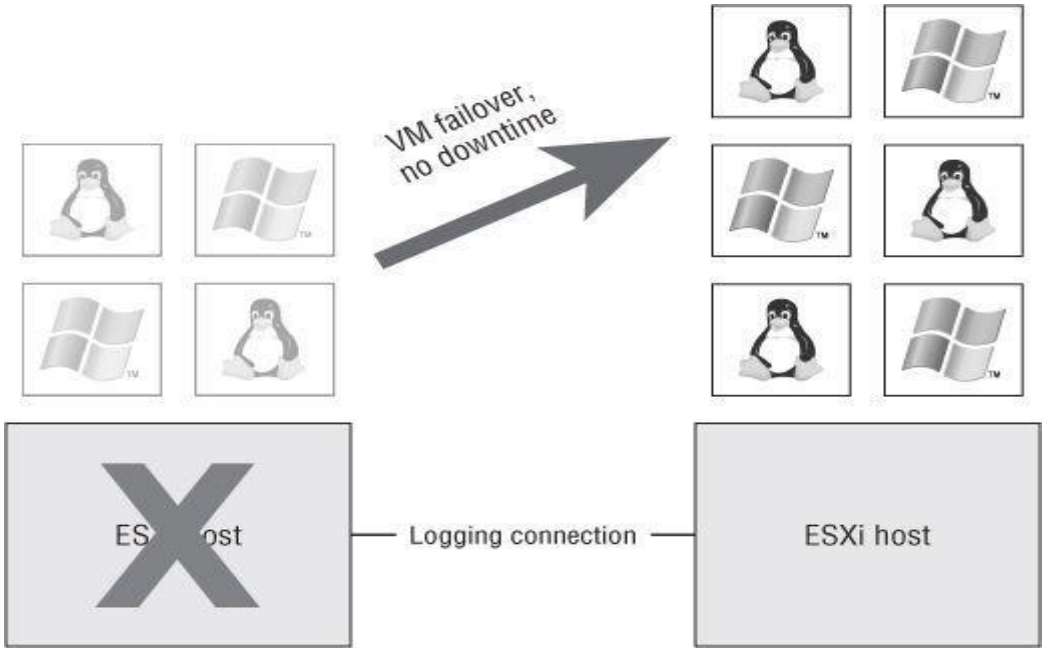
۳۹-۳-۱۳- سیستم تحمل‌پذیر خطا[۷۶] (FT)

اگر در یک کلاستر که HA در آن فعال است یکی از سرورهای فیزیکی به هر دلیلی از کار بیفتد ماشین‌های مجازی آن، قبل از انتقال به سرور فیزیکی دوم ریست شده و برای مدت کوتاهی که ممکن است تا ۳ دقیقه طول بکشد خارج از سرویس

[75] High Availability
[76] Fault Tolerance

خواهند بود و قاعدتا تمام داده‌های ذخیره نشده داخل حافظه رم نیز ازبین خواهد رفت. FT تکنولوژی است که حتی این مسئله را نیز حل کرده است. عملکرد این تکنولوژی بدین‌صورت است که در کلاسترهایی که FT فعال است یک کپی از ماشین‌های مجازی در حال اجرا، بر روی یک سرور دومی نیز اجرا می‌شود. هرگاه یک سرور فیزیکی خاموش شود، ماشین‌های مجازی که آینه‌وار بر روی سرور دوم اجرا می‌شدند، بلافاصله بدون کوچکترین وقفه‌ای جایگزین می‌شوند؛ و کاربر نهایی متوجه این موضوع نخواهد شد.

بعد از جایگزینی یک کپی از ماشین مجازی بر روی سرور سوم ایجاد خواهد شد. تمامی این اعمال بطور اتوماتیک توسط vSphere انجام می‌شود. شکل ۳-۴ این موضوع را به تصویر کشیده است.



شکل ۳-٤. سیستم تحمل خطا. در حین انتقال ماشین‌های مجازی بدون وقفه به کار خود ادامه خواهند داد

اگرهر دو سرور اصلی و سرور آینه‌ای خراب شوند ماشین مجازی، ریستارت شده و یک کپی از آن بر روی یک سرور در دسترس، دوباره اجرا خواهد شد.

۳۹-۳-۱۴- *vSphere Storage API for data protection and VMware data recovery*

یک قسمت مهم از هر شبکه‌ای -نه فقط یک زیر ساختار مجازی‌شده- استراتژی پشتیبان‌گیری است. بدین منظور VMware vSphere دومولفه کلیدی دراختیار قرار می‌دهد: یکی vSphere Storage APIs for Data Protection و یابه اختصار VADP و دیگری VMware Data Recovery یا VDR. VADPیک API است که امکانات لازم برای سیستم‌های پشتیبان‌گیری را فراهم می‌کند.

این API از انواع سیستم‌های پشتیبان‌گیری از جمله پشتیبان‌گیری سطح فایل[۷۷]، پشتیبان‌گیری افزایشی[۷۸]، پشتیبان گیری تفاضلی[۷۹]، پشتیبان گیری ایمج گیری کامل[۸۰] و...

[77] File level
[78] incremental
[79] differential

VADP مانند یک فریم‌ورک کار می‌کند که امکان پشتیبان‌گیری را فراهم می‌کند. در واقع شما تنها به وسیله VADP نمی‌توانید از محیط مجازی خود نسخه پشتیبان تهیه کنید. بلکه شما به یک کاربرد که از قابلیت VADP پشتیبانی می‌کند نیاز خواهید داشت.

تعداد زیادی کاربرد که می‌تواند با VADP کار کند وجود دارد که VMware بدین منظور نرم‌افزار پشتیبان‌گیری خود را با نام VMware Data Recovery(VDR) را ارائه کرده است که برای محیط‌های مجازی کوچک تهیه شده است.

۳۹-۳-۱۵- مقایسه *Xenserver , Hyper–V , VMware*

شاید مقایسه بین سیستم‌های مجازی سازی کار درستی نباشد؛ چرا که سیستم‌های مختلف در روش و اهداف متفاوت هستند. ولی در اینجا ما برای دادن یک دید کلی و درک بهتر موضوع یک مقایسه ارائه می‌کنیم. برای ارائه یک مقایسه بهتر ما فقط پلتفرم‌های مجازی سازی نوع یک را بررسی می‌کنیم.

نکته اول در مقایسه این پلتفرم های‌مجازی سازی این است که: هم Microsoft Hyper-V و هم Citrix Xenserver تمام عملیات ورودی خروجی خود را از طریق پارتیشن والد انجام می‌دهد. یعنی همان dom0. این روش امکان سازگاری بیشتری با سخت‌افزار را فراهم می‌کند. در پارتیشن والد یک سیستم‌عامل همه‌منظوره قرار می‌گیرد که تمام عملیات ورودی خروجی ماشین‌های مجازی را انجام می‌دهد. نسخه‌های قبلی Hyper-V از Server 2003 و نسخه جدیدتر این فوق ناظر از Server 2008 R2 بدین منظور استفاده می‌کند. در مورد Xenserver هم کار به همین شکل است با این تفاوت که در پارتیشن والد یک سیستم‌عامل همه منظوره لینوکسی قرار دارد.

اما در ESXi مدیریت ورودی–خروجی بطور کامل توسط فوق‌ناظر انجام می‌شود. این موضوع باعث کاهش سربار و بالا رفتن بهره‌وری می‌شود؛ و از طرف دیگر مجموعه سخت‌افزارهایی که پشتیبانی می‌شود بالطبع کمتر خواهدبود.

این موضوع تحت عنوان دسته بندی فوق ناظر به (فوق ناظر یکپارچه و ریز هستند) در بخش دوم مورد بررسی قرار گرفته است. نکته دوم اینکه هر یک از پلتفرم‌های مجازی سازی مزایا معایت و کاربردهای خود را دارند.

مثلا برای دیتاسنترهای بزرگ vSphere مناسب‌تر است ولی برای دیتاسنترهای کوچکتر شاید Microsoft hyper-V , Citrix Xenserver مناسبتر باشد. و یا مثلا شما بعنوان مدیر IT سازمان نیازی به DRS , FT و یا Storage vMotion ندارید مناسب‌تر است تا از Xenserver یا Hyper-V استفاده کنید.

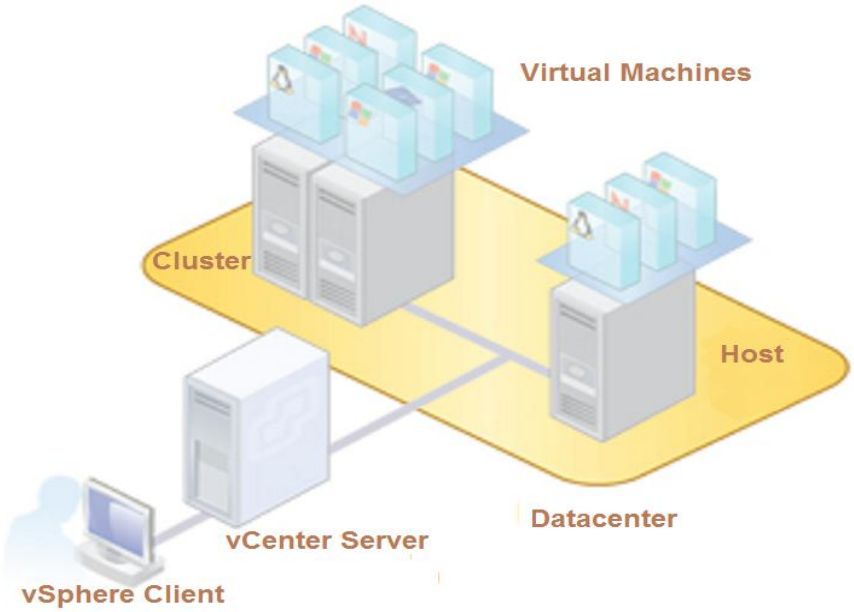
۳۹-۴- نصب و راه اندازی مجموعه WMware vSphere 5

ساختار کلی مجموعه vSphere و مولفه‌های اساسی تشکیل دهنده آن و ساختار کلی این مجموعه در شکل ۴-۱ قابل مشاهده است.

همانطور که در بخش قبل نیز اشاره شد بر روی میزبآن‌ها (سرورهای فیزیکی)، ESXi نصب می‌شود. یک سرور تحت عنوان vCenter Server نقش مدیریت مجموعه را بر عهده دارد. ابزارهای مدیریتی که توسط vCenter Server ارائه می‌شود، توسط vSphere cilent در دسترس خواهدبود. البته توسط vSphere Client و حتی بدون کمک vCenter

[80] full-image

Serverو مستقیما می‌توان به ESXiها متصل شد و هر یک از آن‌ها را بطور مجزا مدیریت و برنامه‌ریزی کرد. کاملا واضح است که در این صورت بسیاری از ابزارهای مدیریتی در دسترس نخواهد بود.



شکل ٤-١. ساختار کلی مجموعه vSphere

۳۹-۴-۱- نصب راه اندازی و پیکر بندی ESXi

با توجه به توضیحات ارائه شده اولین مرحله در راه اندازی این مجموعه نصب ESXi خواهد بود. یک نکته مهم که قبل از شروع نصب ESXiها بایستی به آن اشاره کنیم این است که: همانطور که در بخش قبل نیز به آن اشاره شد فوق ناظر ESXi از نوع یکپارچه بوده که بایستی راه اندازهای سخت‌افزارهایی که با آن‌ها کار می‌کند رادر خود داشته باشد. بنابراین ESXi بر روی هر سخت‌افزاری نمی‌تواند نصب و اجرا شود. البته این مسئله نگرانی عمده‌ای نیست، چرا که اکثر سرورها با قطعات داخلی آن‌ها توسط ESXiها پشتیبانی می‌شوند. پس لازم‌است قبل از خرید سرورها و سخت‌افزارهای مورد نیاز، سری به سایت VMware بزنید تا لیست قطعات و سخت‌افزارهای سازگار با ESXi را مشاهده کنید.

۴-۱-۱ نصب ESXi

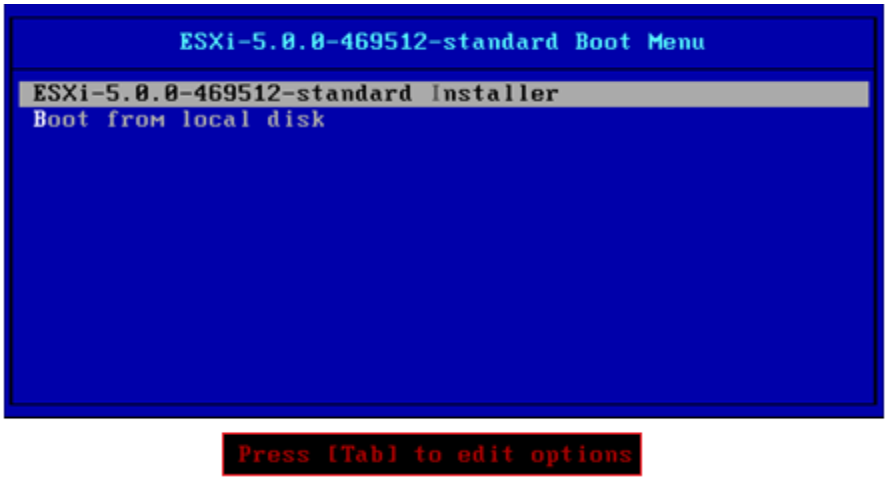
ESXi به سه طریق قابل نصب است:

Interactive Installation یا نصب تعاملی، Unattended Installtien یا نصب خودکار و مورد آخر که در واقع بارگذاری ESXi داخل رم سیستم فیزیکی در قالب یک imag بوده و نصب در کار نیست و این روش را Stateless Provisioning می‌نامند.

در این فصل به جهت اختصار ما فقط روش اول، یعنی نصب تعاملی را بررسی خواهیم کرد.

برای نصب ESXi ابتدا CD حاوی فایل نصب را در داخل سرور قرار دهید. سیستم را روشن نموده و boot سیستم را CD-ROM قرار دهید و از طریق CD-ROM، بوت شوید.

اولین موردی که با آن مواجه خواهید شد. تصویری شبیه به شکل ۴-۲ خواهد بود. برای ادامه گزینه اول را انتخاب کرده و اینتر را بفشارید.



شکل ٤-۲. صفحه شروع نصب ESXi

پس از مدتی با صفحه خوش‌آمدگویی مواجه خواهد شد. با زدن اینتر ادامه دهید.

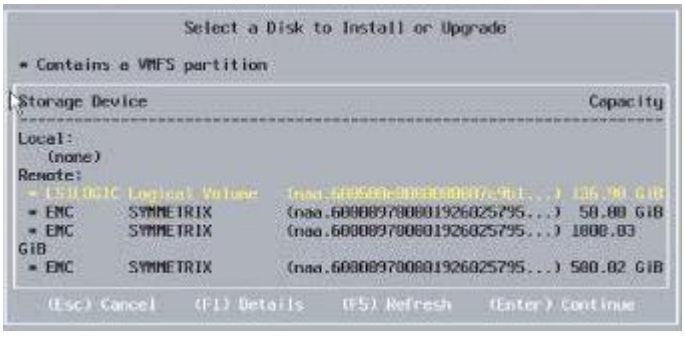
سپس به موافقت‌نامه خواهید رسید که برای تائید و ادامه F11 را بزنید.

در ادامه هارددیسک‌های در دسترس برای انتخاب نمایش داده خواهند شد. اگر تنها دیسک محلی داخل سیستم موجود باشد تصویری شبیه شکل ۴-۳ و اگر علاوه بر دیسک‌های محلی دیسک‌های ریموت در دسترس باشد، تصویری شبیه به شکل ۴-۴ نمایش داده خواهدشد.



شکل ٤-۳. انتخاب دیسک برای نصب ESXi

پس از انتخاب دیسک مورد نظر برای نصب ESXi، با زدن Enter به مرحله بعد بروید.



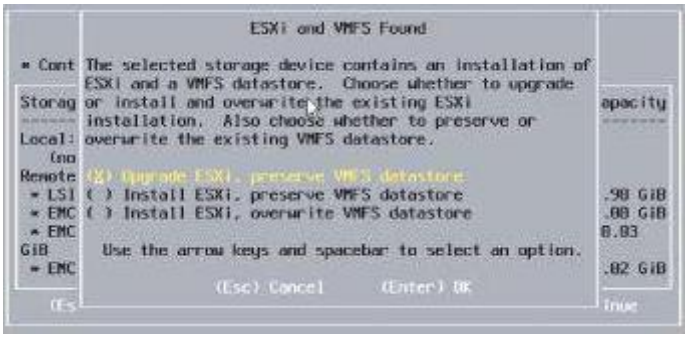
شکل ٤-٤. انتخاب دیسک برای نصب ESXi

در مرحله بعد اگر بر روی دیسک انتخاب شده از قبل ESXi نصب بوده باشد، همانطور که در شکل ۴-۵ نشان داده شده است، سه امکان در اختیار شما قرار خواهد گرفت:

اول Upgrade ESXi , preserve VMFS datastore که نسخه موجود را به ESXi5 ارتقا می‌دهد و ماشین‌های مجازی قبلی که بر روی دیسک قرار دارند حفظ خواهند شد.

دوم Install ESXi , preserve VMFS datastore که نسخه قبلی را پاک کرده و نسخه جدید را جایگزین آن می‌کندولی ماشین‌های مجازی کماکان باقی خواهند ماند.

سوم Install ESXi , overwrite VMFS dalastore که کلیه اطلاعات موجود بر دیسک وحتی فایلهای مربوط به ماشین‌های مجازی را پاک خواهد کرد و ESXi را نصب می‌کند.



شکل ٤-٥. انتخاب نحوه تخصیص دیسک سخت برای نصب ESXi

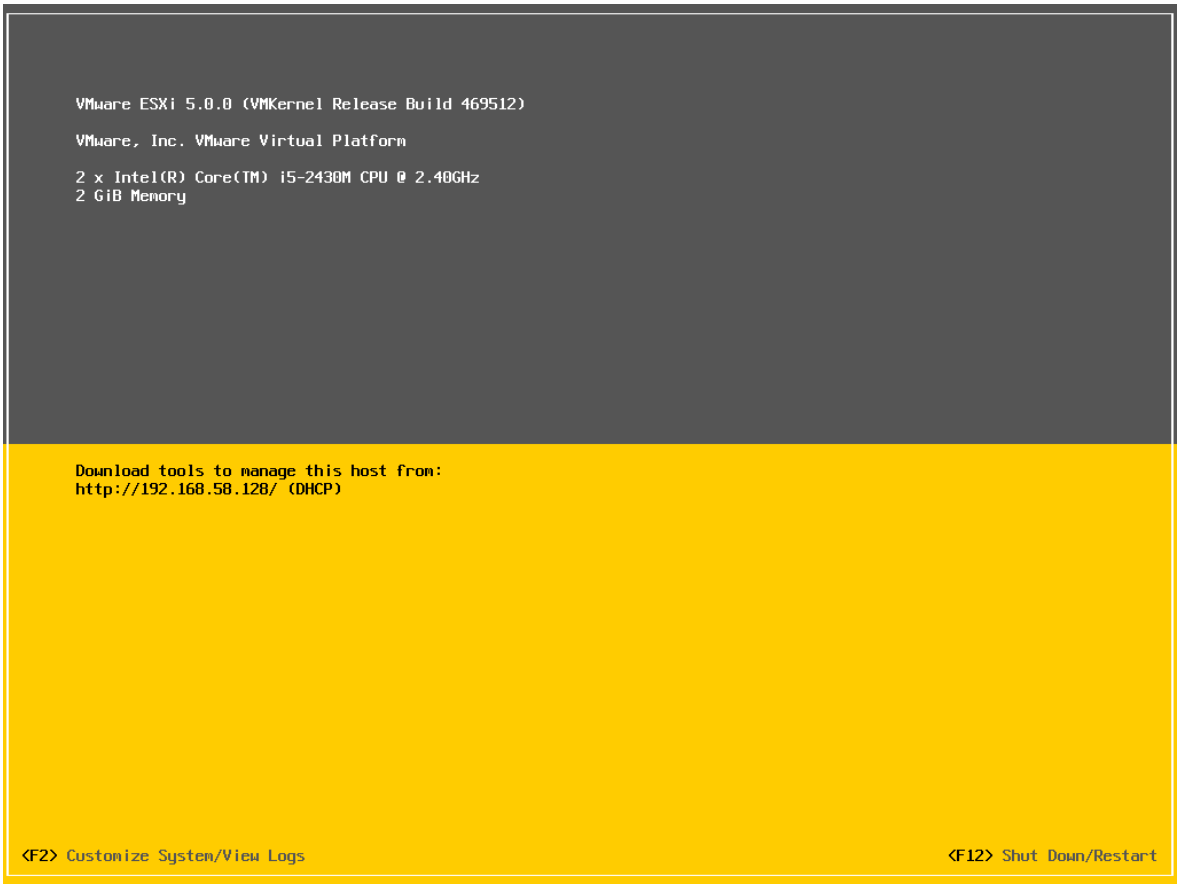
حال مورد مناسب را انتخاب کرده و Enter را بفشارید تا به مرحله بعد بروید.

زبان کیبرد را انتخاب کرده Enter را بزنید.

در این‌مرحله هم پسورد دلخواه و البته با طول حداقل ۷ کاراکتر وارد کرده و با زدن اینتر از این مرحله خارج شوید در انتها با زدن اینتر سیستم را ویستارت نمائید.

۴-۱-۲ پیکر بندی اولیه ESXi

پس از نصب ESXi با صفحه‌ای مشابه شکل ۴-۶ مواجه خواهید شد. با زدن کلید F2 وارد تنظیمات اولیه و اساسی ESXi server می‌شوید. ابتدا جهت ورود نام کاربری و پسورد سیستم را وارد کنید.در اینجا می‌توانید با کاربر root و پسوردی که در هنگام نصب وارد کردید به سیستم login کنید.



شکل ٤-٦. اولین تصویر ESXi پس از نصب

در بخش Configure Password می‌توانید رمز ورود خود را تغییر دهید.

در بخش Configure Management Network می‌توانید تنظیمات شبکه سیستم از جمله انتخاب Ip، تنظیم Dns و... را انجام داد.

در بخش Test Management Network می‌توانید به کمک سرویس Ping از اتصالات بین سیستم‌های متصل به شبکه اطمینان حاصل کنید.

با استفاده از Restor Network Setting می‌توان تنظیمات شبکه را به حالت اولیه پس از نصب درآورد.

زبان صفحه کلید را می‌توان در بخش Configure Keyboard تغییر داد.

دربخش Trouble Shooting می‌توانید تنظیمات مربوط به عیب یابی، از جمله فعال وغیر فعال کردن واسط فرمان و... را انجام دهید.

در بخش Viewsystem Logs می‌توانید اتفاقات[۸۱] ثبت شده[۸۲] سیستم را مشاهده کنید.

و در نهایت توسط Reset System Configuration می‌توانید تنظیمات کل Esxi را به حالت اولیه پس از نصب بازگردانید.

همچنین بوسیله کلید F12 می‌توانید سیستم را ریستارت و یا خاموش کنید.

[81] event
[82] logged

۳۹-۴-۲- راه اندازی vCenter Server

همانطور که قبلا هم اشاره شد برای استفاده از ESXiها و راه اندازی ماشین مجازی بر روی آن‌ها و همچنین بهره‌برداری از تمامی امکانات vSphere بایستی آن‌ها را تحت مدیریت vCenter Server درآورد. در این قسمت vCenter Server را نصب خواهیم کرد؛ و پیکر بندی آن را به بخش‌ها اتی موکول می‌کنیم. و البته قبل از نصب کمی در مورد آن توضیحاتی ارائه خواهیم داد.

۴-۲-۱ ساختار و سرویس‌های vCenter Server

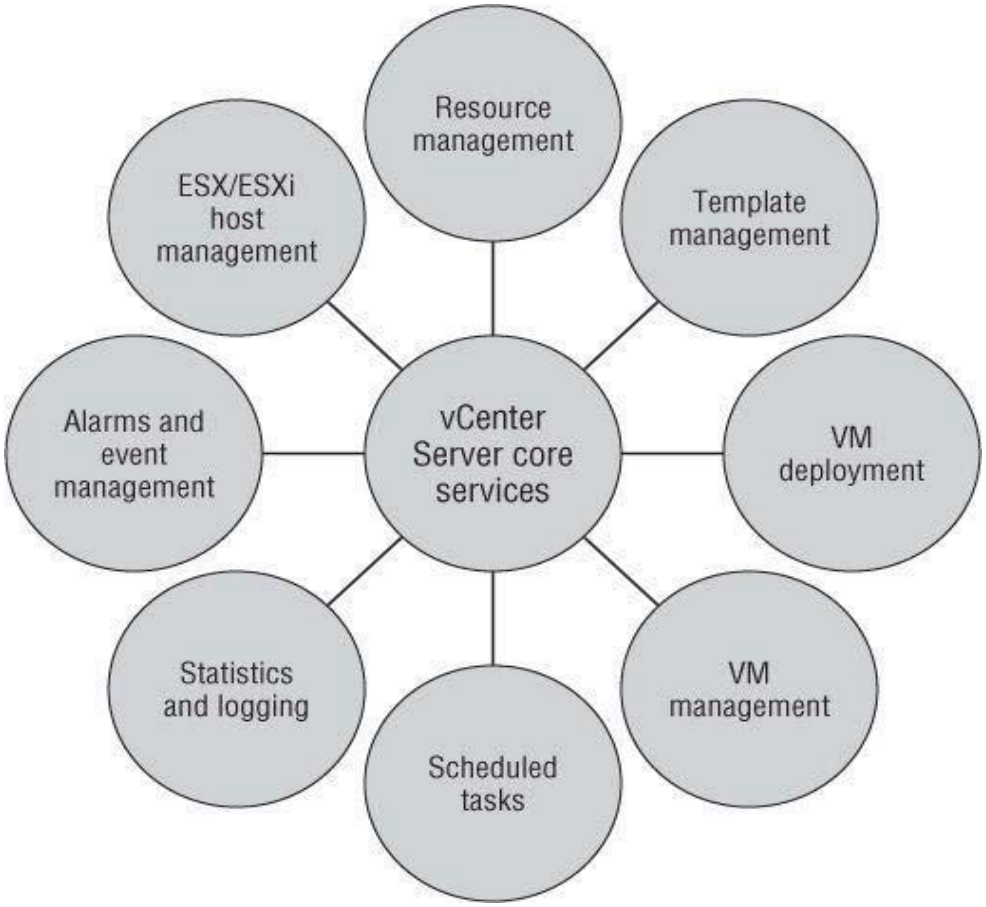
همانطورکه قبلا هم گفته شد vCenter Serverرا یک کاربرد تحت ویندوز بوده که وظیفه مدیریت میزبآن‌ها ESXi وماشین‌های مجازی ساخته شده بر روی آن‌ها را بر عهده دارد. البته یکapplianceپایه لینوکسی (Suse-linux) همراه مجموعهvSphere ارائه می‌شود که محدودیت‌هایی نسبت به vCenter Server ویندوزی دارد.

به طور کلی وظایف اصلی vCenter Serverرا می‌توان اینگونه خلاصه کرد.

- مدیریت منابع میزبآن‌های ESXi و ماشین‌های مجازی
- مدیریت قالب‌های آماده[۸۳]
- توسعه و آماده سازی ماشین‌های مجازی[۸۴]
- مدیریت ماشین‌های مجازی
- زمانبندی وظایف[۸۵]
- آمارگیری[۸۶] و ثبت وقایع[۸۷]
- آلارم‌ها و مدیریت رویدادها
- مدیریت میزبآن‌های ESXi

موارد بالا بصورت نموداری در شکل ۴-۷ نشان داده شده‌اند.

[83] templates
[84] VM Deployment
[85] Task scheduler
[86] Statistics
[87] Logging



شکل ٤-۷. سرویس‌های vCenter Server

یک سرویس مهم که در شکل بالا به آن اشاره نشد مدیریت متمرکز حساب‌های کاربردی است.

برای درک اهمیت این سرویس به مثال زیر توجه کنید.

فرض کنید صدها میزبان ESXi تحت مدیریت یک vCenter داشته باشید. اگر چندین مدیر قصد مدیریت این مجموعه را داشته وهر یک حساب کاربری خود داشته باشند، لازم است بطورجداگانه به هر یک از این میزبآن‌های ESXi وارد شده و یک کاربر جدید ایجاد کنید؛ و یا مثلا برای تغییر کلمه عبور هرکاربر بایستی این سناریو تکرار شود.

ولی vCenter Server این مشکل را حل کرده بدین ترتیب که کافی است تنها یکبار میزبآن‌های ESXi را عضو vCenter کرده و در سرور ویندوزی vCenter Server کاربرها و گروهای لازم را ایجاد کرده و هر مدیر به کمک vSphere Client با نام کاربری خود در vCenter Server، به سیستم وارد شده و وظایف خود را انجام دهد. اگر از applianee لینوکسی بعنوان vCenter Server استفاده شود وظیفه تصدیق هویت به عهده سیستم اکتیو دایرکتوری که vCenter Server عضو آن است خواهد بود.

علاوه بر سرویس‌های گفته شده vCenter Server یک API در اختیار برنامه‌نویسان قرار می‌دهد تا شرکت‌های ثالث هم بتوانند برای vCenter Server برنامه‌نویسی کنند، و این کمک بسیار بزرگی برای توسعه سیستم‌های مجازی‌سازی خواهد بود.

همچنین vCenter Server دارای یک حالت link-mode است که برای محیط‌های بزرگتر در نظر گرفته شده است بطوریکه چندین سرور vCenter می‌توانند تحت مدیریت یک Active Directory کنترل یک دیتا سنتر را بر عهده بگیرند.

۴-۲-۲ نیازمندی‌های نرم‌افزاری و سخت‌افزاری vCenter Server

قبل از هر چیز لازم است بدانیم چه مواردی برای نصب vCenter Server نیاز است. مثلا بر روی چه پلتفرم سخت‌افزاری اجرا می‌شود، بر روی چه ورژن هایی از ویندوز قابل نصب است، از چه بانک اطلاعاتی استفاده می‌کند و.... پاسخ این سوالات بسته به محیط عملیاتی و اندازه دیتاسنتر متفاوت خواهد بود.

حداقل سخت‌افزار لازم برای vCenter Server به قرار زیر است:

- دو پردازنده ۶۴ بیت و یا یک پردازنده دو هسته‌ای ۶۴ بیتی با فرکانس کاری ۲ گیگاهرنز
- ۳ گیگا بایت رم
- ۳ گیگا بایت فضای خالی بر روی هارد دیسک
- یک کارت شبکه اترنت (بهتر است گیگابیت باشد)

برای سیستم عامل هم یکی از موارد زیر لازم است:

ویندوز سرور ۲۰۰۳، ویندوز سرور 2003 R2 ویندوز سرور ۲۰۰۸ و ویندوز سرور 2008 R2. لازم به ذکر است که vCenter Server فقط بر روی سیستم عامل‌های ۶۴ بیتی اجرا می‌شود.

موارد گفته شده در بالا، حداقل را در نظر گرفته است. قاعدتا برای دیتاسنترهای بزرگتر سیستم قوی‌تری لازم خواهد بود. همچنین موارد بالا با این پیش فرض در نظر گرفته شده‌اند که بانک اطلاعاتی بر روی سرور دیگری راه اندازی شده است؛ اگر چه با تهیه کردن یک سرور قوی‌تر می‌توان vCenter Server و بانک اطلاعاتی را در کنار هم و بر روی یک سرور نصب کرد. البته این کار اصلا توصیه نمی‌شود چرا که در صورت خرابی سرور، دو نقطه از شبکه ما دچار مشکل خواهد شد یکی سرور vCenter و دیگری سرور بانک اطلاعاتی.

بانک اطلاعاتی در اینجا وظیفه نگهداری اطلاعات میزبآن‌های ESXi و ماشین‌های مجازی از جمله اطلاعات پیکربندی، مجوزها، آمارها و دیگر اطلاعات را بر عهده دارد.

اگر بخواهیم سرور vCenter و بانک اطلاعاتی یکی باشد یعنی هر دو بر روی یک سرور اجرا شوند، حداقل سخت‌افزار لازم به قرار زیر خواهد بود:

یک پردازنده دو هسته و ۴ گیگابایت رم برای یک مجموعه با ۵۰ میزبان ESXi و ۵۰۰ ماشین مجازی. اگر دیناسنتر شما دارای ۳۰۰ میزبان ESXi و ۳۰۰۰ ماشین مجازی است،ای با ۴ هسته پردازنده و مقدار ۸ گیگابایت رم لازم خواهد بود. برای یک دیناسنتر با ۱۰۰۰ میزبان ESXi و ۱۰۰۰۰ ماشین مجازی ۸ هسته پردازنده نیاز است. مقدار حداقل رم مورد نیاز هم برابر با ۱۶ گیگابایت خواهد بود. میزان فضای آزاد بر روی دیسک نیز متناسب با تعداد میزبآن‌های ESXi و ماشین‌های مجازی افزایش خواهد یافت.

از آنجایی که بانک اطلاعاتی اهمیت فوق العاده‌ای برای vCenter Server دارد، تنهااز بانک‌های اطلاعاتی اینترپرایز پشتیبانی می‌کند. در حال حاضر بانک‌های اطلاعاتی زیر می‌توانند برای vCenter Server استفاده شوند:

- IBM DB2 9.5 (fix pack 5 required; fix pack 7 recommended)

- IBM DB2 9.7 (fix pack 2 required; fix pack 3a recommended)
- Microsoft SQL Server 2008 R2 Express (bundled with vCenter Server)
- Microsoft SQL Server 2005 (32-bit or 64-bit; SP3 is required, and SP4 is recommended)
- Microsoft SQL Server 2008 (32-bit or 64-bit; SP1 is required, and SP2 is recommended)
- Microsoft SQL Server 2008 R2
- Oracle 10g R2 (10.2.0.4 required)
- Oracle 11g R1 (11.1.0.7 required)
- Oracle 11g R2 (11.2.0.1 with patch 5 required)

توجه داشته باشید که ممکن است بانک‌های اطلاعاتی ذکر شده توسط مولفه‌های دیگر vSphere نظیر vSpher Update Manager پشتیبانی نشوند که برای اطلاعات بیشتر در این موضوع می‌توانید به سایت VMware مراجعه نمائید.

یک نکته مهم که در استفاده از بانک‌های اطلاعاتی حائز اهمیت است این است که نوع بانک اطلاعاتی می‌تواند در تعداد میزبآن‌های ESXi و ماشین‌های مجازی محدودیت ایجاد کند چرا که شرکت VMware استفاده از SQL server 2008 Express را برای دینا سنترهای با ۵ میزبان ESXi و ۵۰ ماشین مجازی و بیشتر اصلا توصیه نمی‌کند.

بنابراین پس ازتهیه مایحتاج سخت‌افزاری دومین مسئله راه اندازی بانک اطلاعاتی است.

۴-۲-۳ آماد سازی بانک اطلاعاتی

همانطور که گفته شد لازم است قبل از نصب vCenter Server بانک اطلاعاتی را آماده‌سازی کنیم.

اگر دیتاسنتر شما کوچک بوده بطوری که تعداد میزبان ESXi کمتر از ۵ و ماشین‌های مجازی کمتر از ۵۰ بوده و همچنین نیازی به استفاده از بانک اطلاعاتی که بر روی سروری غیر از سرور vCenter وجود دارد ندارید می‌توانید از این بخش عبور کنید. اما توصیه می‌شود حداقل برای افزایش آگاهی خود در مورد چگونگی کار با بانک اطلاعاتی ریموت این قسمت را مطالعه نمائید.

قدم اول ایجاد پایگاه داده، یا همان بانک اطلاعاتی است. به سروری که بانک اطلاعاتی را بر روی آن نصب کرده‌اید login کنید. از مسیر

start > All programs > Microsoft SQL Server 2008 R2 > SQL Server management st

به SQL وارد شوید. بعد از login کردن به بخشی مدیریت پایگاه وارد خواهید شد.

ابتدا لازم است تا برای اتصال به بانک اطلاعاتی یک نام کاربری ایجاد شود. گر چه کاربر sa به طور پیش‌فرض وجود دارد. بدین منظور: سمت چپ صفحه، در بخش object explorer بر روی علامت بعلاوه کنار security کلیک کنید.

حال بر روی بعلاوه کنارlogins نیز کلیک نمائید. بر روی logins کلیک راست کرده، ابتدا new و بعد ...login را انتخاب کنید. در قسمت login name نامی برای کاربر جدید انتخاب کنید.SQLserver authentication را انتخاب کرده و پسوردی نیز برای کاربر جدید انتخاب کنید.تیک گزینه enforce password policy را بردارید. سمت چپ، بالای همین صفحه بر روی server roles کلیک کنید. گزینه‌های sysadmin , public را تیک بزنید.با زدن ok صفحه رابببندید.

در بخش object explorer برروی Databases کلیک راست کرده new Databases را برگزینید. در تکست‌باکس Databases name یک نام برای پایگاه‌داده خود انتخاب کنید. owner آن را به کاربری اختصاص دهیدکه قصد دارید بوسیله آن به بانک اطلاعاتی متصل شوید. با زدن ok صفحه رابببندید.

حال از برنامه مدیریت پایگاه داده خارج شوید.

قبل از ادامه مطمئن شوید سرویس SQLagent در حالت اجرا باشد. بدین‌منظور پس از وارد شدن به سرور پایگاه‌داده، از مسیر start ➔ administrative tools ➔ services، به بخش سرویس‌ها وارد شوید و SQL Server agent را اجرا کرده ودرحالت Automatic قرار دهید.

به سرور vCenter Server وارد شوید. برای اتصال به پایگاه داده لازم است یک ODBC DSN ایجاد کنید. بدین منظور از مسیر:

start ➔ administrative tools ➔ Datasource

به ODBC Datasource Administrator وارد شوید. در سربرگ System DSN بر روی Add کلیک کنید. پس از انتخاب درایور SQL Server native client بر روی finish کلیک کنید.

اگر native client وجود ندارد بایستی قبل از ادامه کار آن رانصب کنید. native client رامی‌توانید از سایت مایکروسافت دانلود کنید و یا داخل DVD حاوی SQL آن را بیابید. اگر نتوانستید بطورمجزا آن را داخل DVD بیابید، نصب SQL را آغاز کنید ولی هنگام انتخاب مولفه‌ها، تنها client tools connectivity را انتخاب کنید. البته بعد از پایان نصب می‌توانید تمام مولفه‌های مربوط به SQL بجز native client را ازطریق programs and features حذف کنید.

همچنین قبل از ادامه کار، دیوار آتش سروری که SQL در آن اجرا می‌شود را نیز خاموش کنید. بعد از نصب native client فرایند ایجاد ODBC DSN را دوباره تکرار کنید.

بعد از انتخاب SQL Server native client و زدن دکمه finish صفحه جدیدی باز می‌شود. در این صفحه در قسمت name نامی دلخواه برای این DSN وارد نمائید. در بخش server نام و یا IP سرور بانک اطلاعاتی را وارد کنید. توجه داشته باشید اگر سرور DNS ندارید تنها IP می‌توان وارد کرد. با زدن next به صفحه بعد بروید. with SQL Server Authentication را انتخاب کنید و نام کاربری که در مرحله قبل در بخش مدیریت SQL ایجاد کردید را به همراه رمز عبور آن را وارد کنید. برای اطمینان از اتصال تیک گزینه پایین صفحه را بزنید، سپس برروی next کلیک نمائید.

تیک گزینه change the default databases را بزنید وبانک اطلاعاتی که در بخش مدیریت SQL ایجاد کردید را انتخاب کنید. Next را بزنید صفحه جدید را بدون تغییر رها کنید. پس از زدن finish می‌توانید با زدن test Datasource از صحت کارکردDSN مطمئن شوید.

ODBCDSN ساخته شد. می‌توانیم نصب vCenter Server را آغاز کنیم.

۴-۲-۴ نصب vCenter Server

بدین منظور:

۱. ابتدا رسانه حاوی فایل نصب vCenter را داخل درایو قرار دهید پس از اجرا شدن اتوران با تصویری مشابه به شکل ۴-۸ مواجه خواهید شد.



شکل ٤-۸ اتوران رسانه حاوی vCenter Server

۲. از سمت چپ، بالای اتوران vCenter Serverرا انتخاب و پس از آن بر روی install کلیک کنید.
۳. پس از انتخاب زبان مورد نظر بر روی ok کلیک نمائید.
۴. بر روی next کلیک نمائید.
۵. بار دیگر بر روی next کلیک نمائید.
۶. پس از انتخاب گزینه agree که به معنای قبول موافقت نامه است، بر روی next کلیک نمائید.
۷. در این صفحه نیز پس از پر کردن موارد خواسته شده، بر روی next کلیک نمائید.
۸. در این صفحه بایستی بانک اطلاعاتی خود راانتخاب نمائید. همانطورکه قبلا اشاره شد در صورت کوچک بودن دیتاسنتر شما و یا نداشتن سرور بانک اطلاعاتی، با انتخاب گزینه اول یک نسخه SQL Server 2008 express که در داخل رسانه vCenter قرار دارد را نصب نمائید که در این‌صورت شما نیاز به هیچ‌گونه تنظیماتی برای بانک اطلاعاتی خود ندارید. در غیر این صورت گزینه دوم را انتخاب کنید و از لیست موجود DSN که در بخش قبلی ساختید را انتخاب نمائید.

نام سرور راوارد کنید. اگر سیستم عضو دامنه است نام کامل به‌همراه نام دامنه را وارد کنید. مثلا اگر نام سرور server1 و نام دامنه mydomain.com است؛ در این قسمت serverl.mydomain.com را وارد کنید.

۹. اگر گزینه دوم را انتخاب کرده باشید، یعنی بانک اطلاعاتی جداگانه، در این صورت پس از زدن next از شما نام کاربری و رمز ورودی که در SQL ایجاد کردیم خواسته خواهد شد. البته اگر از domain controller استفاده کرده باشید می‌توانید windows authentication نیز استفاده کنید.

تیک گزینه use system account را بزنید و یا نام کاربری از سیستم یا دامنه را وارد کنید که می‌خواهید برای ورود به vCenter از آن استفاده کنید. در غیر این صورت، یعنی انتخاب گزینه نصب SQL server 2008 express این مرحله نمایان نخواهد شد.

۱۰. در این مرحله مسیری که vCenter در آن نصب می‌شود را انتخاب کنید و بر روی next کلیک نمائید.
۱۱. در این قسمت هم گزینه اول را انتخاب کرده و برروی next کلیک نمائید. در مورد گزینه دوم در ادامه صحبت خواهیم کرد.
۱۲. در اینجا شماره پورت هایی که vCenter نیاز دارد مشاهده می‌کنید. توصیه می‌شود هیچ یک از شماره‌ها را تغییر ندهید. اما اگر ناچار به تغییر این شماره پورت‌ها شدید، مثلا پورت‌ها قبلا توسط برنامه‌های دیگر انتقال شده‌اند، شماره پورت‌های جدید را حتما یادداشت کرده و به پیغام هایی که برنامه‌ی نصب، می‌دهد توجه کنید.
۱۳. در صفحه بعد هم امکانی برای تغییر پورت هایی UDP , TCP مورد نیاز وجود دارد که پیشنهاد می‌شود آن‌ها را نیز بدون تغییر رها کرده و بر روی next کلیک نمائید.
۱۴. در این مرحله می‌توانید اندازه دیتا سنتر و محیط عملیاتی خود را انتخاب کنید. بر روی next کلیک نمائید.
۱۵. install را زده و پس از انجام نصب بر روی finish کلیک نمائید.

در اینجا نصب vCenter Server نیز به پایان رسید.

۴-۲-۵ نصب vCenter Server در حالت linked mode

چنانچه دیتاسنتر شما بسیار بزرگ باشد[۸۸] که یک vCenter Server برای مدیریت آن کافی نباشد و یا محدودیت‌های دیگر مثل محدودیت‌های جغرافیایی مانع از مدیریت دیتا سنتر توسط فقط یک vCenter می‌شود، لازم است چندین vCenter داشته باشیم.

در vSphere امکانی وجود دارد که بتوان چندین vCenter Server را با ورود به یکی از آن‌ها مدیریت کرد که این امکان را linked-mode می‌نامند. برای نصب vCenter در این مورد مراحل نصب vCenter را تا مرحله ۱۰ مانند حالت عادی ادامه دهید ولی در مرحله ۱۱ گزینه دوم یعنی linked-mode را انتخاب کنید.

در این حالت در مرحله بعد نام سرور vCenter Server که قبلا نصب و راه‌اندازی شده است را وارد کنید. مراحل بعدی نیز مانند حالت نصب ساده خواهد بود. یعنی مراحل ۱۲ و به بعد. البته یک vCenter Server که به‌صورت Single نصب شده است را نیز می‌توان پس از نصب، به عضویت یک linked-mode group درآورد. این کار بوسیه ابزار vCenter Server linked mode configuration که با vCenter Server نصب می‌شود، امکان پذیر خواهد بود.

برای نصب vCenter درحالت linked-mode توجه به نکات زیر ضروری است.

- تمامی vCenter Serverهای عضو یک دامنه باشند؛ و یا اگر عضو دامنه‌های مختلف هستند، بین دامنه‌ها بایستی two- way trust relationship برقرار باشد.
- سرویس DNS بایستی فعال بوده و نام سرورها با نام DNSشان مطابق باشد.

[۸۸] یک vCenter Server می‌تواند تا ۱۰۰۰ میزبان ESXi و یا ۱۰۰۰۰ ماشین مجازی را تحت مدیریت خود داشته باشد

- سروری که vCenter است نمی‌تواند همزمان Domain Controller و یا Terminal Server باشد.
- vCenter Server5 را نمی‌توان با نسخه‌های قبلی vCenter درحالت linked-mode قرار داد
- هر یک از vCenterها بایستی بانک اطلاعاتی خود را به‌طور مجزا داشته باشد (الزاما نه سرورهای جداگانه)

در ضمن هر یک از vCenter بطور جداگانه مدیریت می‌شوند یعنی مثلا نمی‌توان عمل vMotion را بین دو سرور که عضو vCenter مختلف هستند انجام داد.

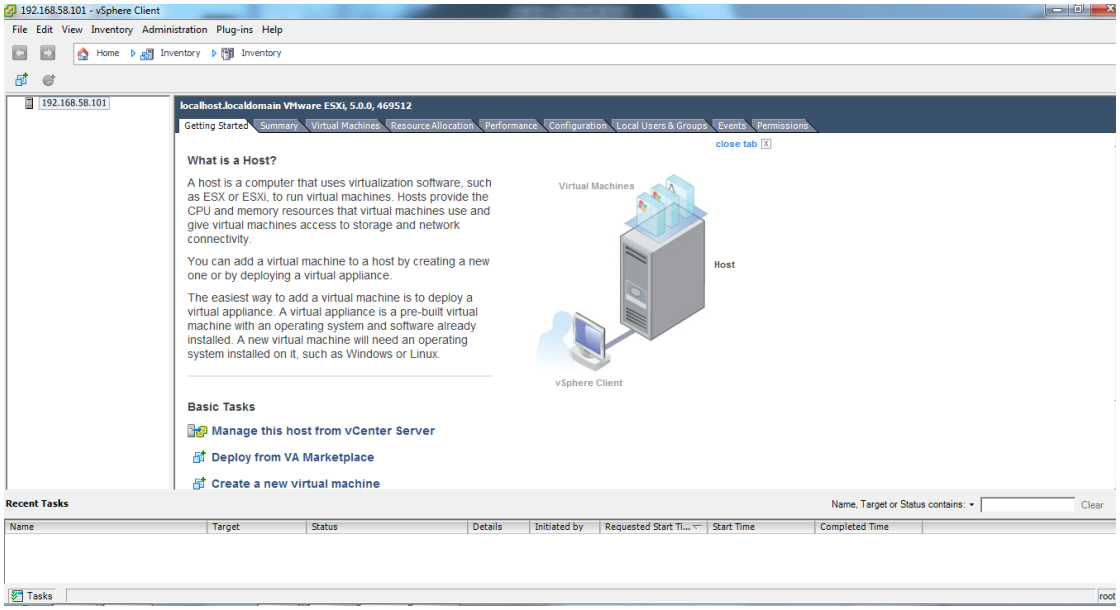
۳۹-۴-۳- نصب vSphere Client برای ورود به vCenter Server

برای ورود به بخش مدیریت vCenter Server به دو طریق می‌توان عمل کرد. یکی استفاده از vSphere Client و دیگری vSphere web client که اولی یک کاربرد ویندوزی است و دیگری یک کاربرد تحت وب که ما از vSphere Client استفاده می کنیم.

vSphere Client , Web Client در داخل رسانه حاوی vCenter Server نیز وجود دارد. به دلیل سادگی نصب vSphere Client، از توضیح دادن آن خودداری می کنیم.

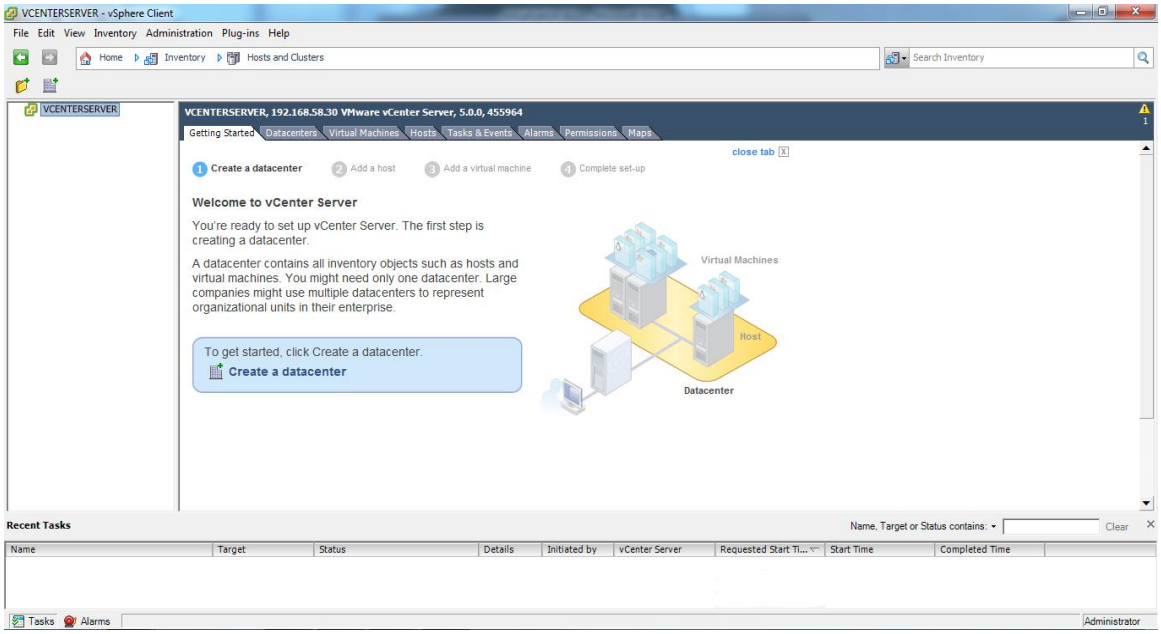
vSphere Client می‌تواند بر روی سرور vCenter نصب شود و یا بر روی یک سیستم دیگر. نیاز به سخت‌افزار خاصی هم ندارد و بر روی تمامی نسخه‌های ویندوز XP و به بعد قابل نصب می‌باشد.

پس ازنصب vSphere Client، آن را اجرا کنید. در قسمت IP Address/name نام و یا آدرس IP سرور vCenter Server را وارد کنید و در قسمت password , username نام کاربری که حق دسترسی به vCenter را دارد و کلمه عبور آن را وارد کنید. اگر با کاربری که حق دسترسی به vCenter را دارد به سیستم login کرده باشید(مثل زمانی که vSphere Client بر روی سرور vCenter نصب شده است) با زدن تیک Use Windows Authentication نیازی به وارد کردن نام کاربری و کلمه عبور نیز نخواهد بود. پس از ورود به سیستم برای اولین بار، اگر به ESXi، login کرده باشید شکل ۴-۹ و اگر به vCenter Server، login کرده باشید شکل 10-4 را مشاهده خواهید کرد.



شکل ٤-۹. اتصال به ESXi به‌کمک vSphere Client

در بخش‌های بعد نحوه کاربا vCenter Server و استفاده از توانایی‌های آن را خواهیم آموخت.



شکل ٤-١٠. اتصال به vCenter Server به‌کمک vSphere Client

۳۹-۴-۴- نصب *vSphere Web Client*

گر چه vSphere Client تمام قابلیت vCenter را در دسترس قرار می‌دهد و کاملتر و قوی‌تر از web client است، اما گاهی ممکن است مدیر سایت در محلی باشد که دسترسی به vSphere web client نداشته باشد.

در این وضعیت می‌تواند به کمک یک browser مثل IE و یا فایرفاکس که مجهز به adobe flash player و با استفاده از یک اتصال اینترنت به vSphere web client متصل شده و سیستم مجازی را از راه دور مدیریت کند. بدین منظور ابتدا نرم‌افزار vSphere web client را نصب می‌کنیم. می‌توان این نرم‌افزار رابر روی سرور vCenter نیز نصب کرد. این برنامه در رسانه حاوی vCenter قرار دارد و فرایند نصب آن نیز بسیار ساده است که در اینجا در مورد آن صحبت نمی‌کنیم.

پس از نصب web client لازم است تا vCenter را در web client ثبت کنید. بدین منظور به سیستمی که vSphere web client بر روی آن نصب است login کرده پس از اجرای browser (IE و یا فایر فاکس) آدرس سرور vSphere web client را وارد کنید(یعنی همین سرور)

آدرس بصورت زیر خواهد بود

مثلاگرآدرس IP سرور vSphere web client، 192.168.10.10 است این آدرس بصورت زیر خواهد بود:

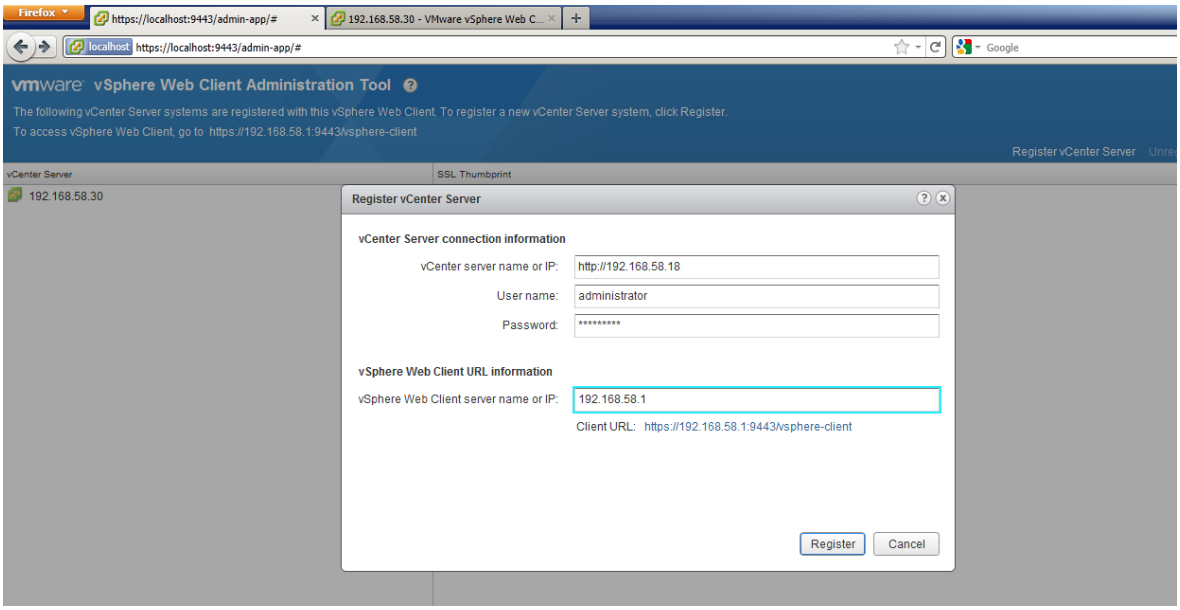
https://192.160.10.10:9443/admin-app

پس از لود شدن صفحه از سمت راست بالای صفحه register vCenter Server را کلیک کنید.

در پنجره باز شده که بصورت شکل ۴-۱۱ است اطلاعات خواسته شده را بصورت زیر وارد کنید.

در کادر اول IP سرورvCenter را همانطور که در شکل نشان داده شده وارد کنید.

در کادرهای دوم و سوم نام کاربری ورمز عبوری که حق دسترسی به بخش مدیریت vCenter را دارند وارد کنید.در کادر انتهایی هم نام سروری که vSphere web client بر روی آن نصب است را وارد کنید و دکمه register را بزنید.



شکل ٤-۱۱. افزودن سرورهای vCenter به vSphere web Cliebt برای مدیریت

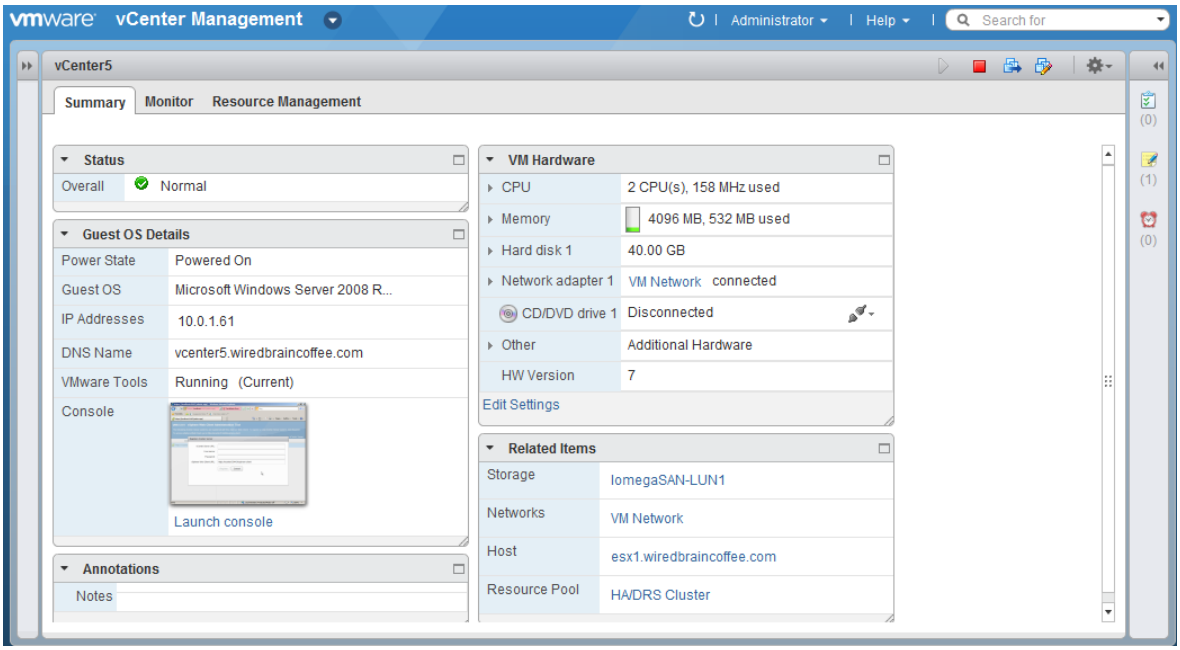
پس ازثبت vCenterها از هر سیستمی و تنها به کمک یک browser می‌توانید به سرور webclient توسط آدرس به صورت زیر به بخش مدیریت webclient وارد شوید.

https://webclient-ipaddress/vSphere-client

مثلا اگر ip سرور web client 192.168.58.1 است آدرس بصورت زیر خواهد بود.

https://192.168.58.1/vSphere-client

پس ازلود شدن در پایین سمت چپ صفحه با انتخاب vCenter و وارد کردن نام کاربری و رمز عبور آن به بخش مدیریت آن وارد شوید. پس از login، باصفحه‌ای مشابه شکل۴-۱۲ مواجه خواهید شد.



شکل ٤-۱۲. بخش مدیریت در vSphere web Client

vSphere web client محدودیت‌هایی هم نسبت به vSphere Client دارد که از آن جمله می‌توان به موارد زیر اشاره کرد:

- در web client برای اضافه کردن vCenterها برای مدیریت باید به سیستمی که web client بر روی آن نصب شده login کرد.
- در web client نمی‌توان cluster ایجاد کرد.
- در web client نمی‌توان میزبان‌های ESXi را اضافه کرد.
- و بسیاری از موارد دیگر که با وارد شدن به web client آن‌ها را خواهید دید.

۳۹-۵- دستگاه‌های ذخیره‌سازی داده

سیستم‌های ذخیره‌سازی یکی از مهمترین بخش‌های هر سیستم کامپیوتری است. در این بین سیستم‌های ذخیره سازی اشتراکی به دلیل بالا بردن کارایی و دسترسی از اهمیت ویژه‌ای برخوردارند.

به دلیل وابستگی بسیاری از قابلیت‌های اساسی vSphere به دستگاه‌های ذخیره‌سازی اشتراکی این سیستمها یکی از حیاتی‌ترین اجزای پلتفرم مجازی سازی VMware است.

در ادامه این بخش ابتدا در مورد انواع سیستم‌های ذخیره‌سازی صحبت می‌کنیم. پس از آن یک ISCSI را به کمک سیستم‌عامل openfiler شبیه‌سازی کرده ودر انتها این ISCSI SAN را در پلتفرم مجازی‌سازی بکار خواهیم گرفت.

۳۹-۵-۱- انواع سیستم‌های ذخیره‌سازی

ذخیره سازها را ازنظر نوع اتصال به سرور می‌توان به دو دسته تقسیم کرد:

نوع اول ذخیره‌سازها با اتصال مستقیم به سرور و نوع دوم سیستم‌های ذخیره‌سازی اشتراکی یا همان Shared Storageها هستند که در ادامه هریک را بررسی خواهیم کرد.

۵-۱-۱ ذخیره‌سازها با اتصال مستقیم به سرور

این نوع ذخیره‌سازها، همان دیسک‌های محلی هستند که اختصارا به آن‌ها DAS[۸۹] گفته می‌شود. این نوع ذخیره‌سازی‌ها همانطور که بارها نیز به آن اشاره شد، به جهت عدم پشتیبانی از سیستم‌های پیشرفته vSphere در این مجموعه کاربرد کمی دارند. البته این نوع ذخیره‌سازی مزایایی نیز دارند که از جمله آن می‌توان به موارد زیر اشاره کرد.

- نصب و راه اندازی آسان
- ارزانی (نیاز به سخت‌افزار و نرم‌افزار اضافی ندارد، چرا که تمامی بار پشتیبانی و مدیریت آن به عهده سخت‌افزار و سیستم‌عامل سرور خواهد بود.)
- عدم نیاز به اتصالات شبکه اضافی

[89] Direct Attached Storage

۵-۱-۱ سیستم‌های ذخیره‌سازی اشتراکی

نوع دوم سیستم‌های ذخیره‌سازی اشتراکی یا همان Shared Storageها هستند که انواع و اقسام زیادی دارند که هر یک در سطوح مختلف از تکنولوژی‌های متفاوتی استفاده می‌کند. ذخیره‌سازهای اشتراکی به دو دسته اصلی NAS و SAN تقسیم می‌شوند که در ادامه توضیح مختصری در مورد هر یک ارائه خواهیم کرد.

۵-۱-۱-۱ ذخیره‌سازهای SAN[۹۰]

همان طور که از نام آن نیز فهمیده می‌شود، SAN یک شبکه است؛ شبکه‌ای جهت انتقال اطلاعات بین سرورها و زیرشبکه ذخیره‌سازی. از نظر سیستم‌عامل SAN همانند DAS خواهد بود. فضای موجود در SAN بصورت بلوک‌های منطقی به نام LUN (همانند پارتیشن‌های یک دیسک محلی) در اختیار سرور قرار می‌گیرد. سیستم عامل با این LUN همانند یک پارتیشن محلی برخورد کرده و فایل سیستم مورد نظر خود را بر روی آن اعمال می‌کند. البته برای اینکه چندین سرور بتواند به یک LUN دسترسی داشته باشند بایستی با فایل‌سیستم‌های خاصی فرمت شوند.

مثلا ویندوز Server 2008 R2 برای این منظور از فایل سیستم CSV استفاده می‌کند.

برای اتصال SAN به سرور عمدتا ازدو تکنولوژی FC , ISCSI استفاده می‌شود. FC یا تکنولوژی فیبرنوری پیچیده‌تر و پرهزینه‌تر است و البته سرعت بسیار بالایی نیز دارد. همچنین این تکنولوژی نیاز به سوئیچ‌های فیبرنوری نیز دارد که هزینه نسبتا بالایی را به سیستم تحمیل می‌کنند. از مزیت‌های دیگر این تکنولوژی بجز سرعت بالای آن فاصله بسیار بالایی است که پشتیبانی می‌شود (تا ۱۰ کیلومتر)

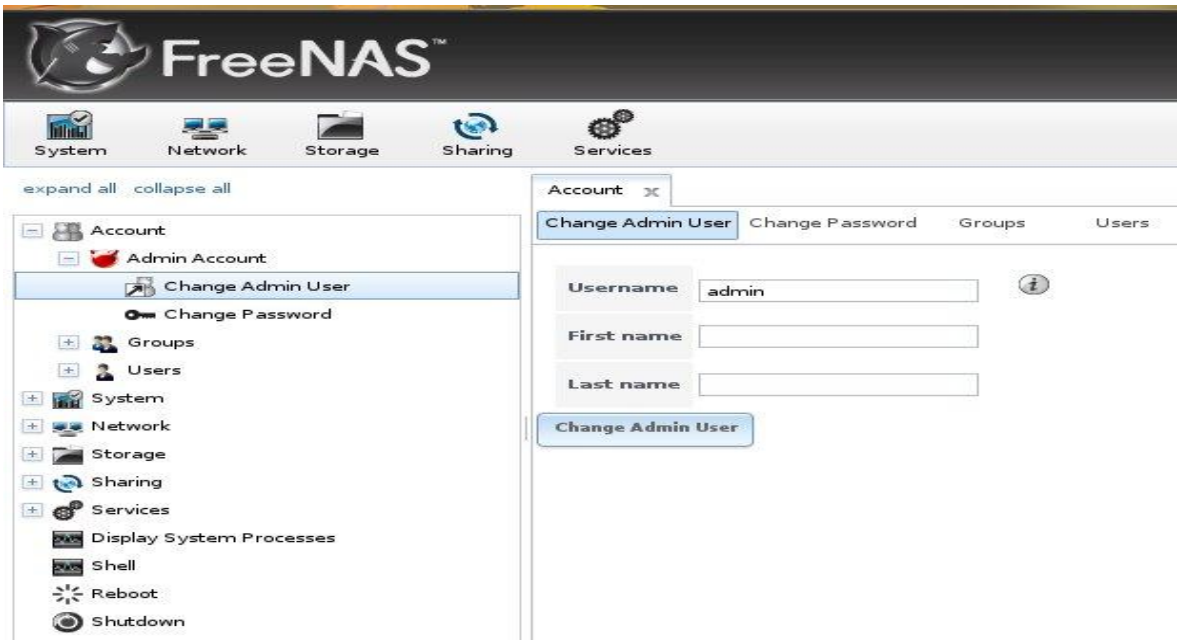
ISCSI، استاندارد انتقال بلاک‌های SCSI در شبکه اترنت با استفاده از TCP/IP است. وظیفه اتصال سرور با ذخیره‌سازهای ISCSI بر عهده ISCSI Initiator است که به عنوان یک نرم‌افزار در سرور اجرا می‌شود. همانطور که گفته شد ISCS برای انتقال داده از TCP/IP استفاده می‌کند؛ بنابراین، این شبکه می‌تواند در بستر اینترنت فعالیت کند و این یعنی پشتیبانی از فاصله نامحدود. البته از نظر سرعت نسبت به FC محدودتر است.

۵-۱-۱-۲ ذخیره سازهای NAS[۹۱]

NASها در واقع سرورهایی با سیستم‌عامل مخصوص ارائه سرویس فایل هستند. یعنی یک سرور ارزان قیمت که دارای تعداد زیادی هارد دیسک SATA و یا SCSI و یک یا چند کارات اترنت باشد را می‌توان در نقش سرور NAS بکار گرفت. بدین ترتیب دیگر سرورهای قدرتمند و گران‌قیمت همه‌منظوره درگیر سرویس فایل نمی‌شوند. همانطور که گفته شد، برای اتصال ذخیره‌سازهای NAS به شبکه می‌توان از کارت شبکه اترنت 100,10 , GIG , 10G استفاده کرد. سرورهای ذخیره‌سازی NAS برای انتقال داده از TCP/IP استفاده می‌کند. بعلاوه به کمک سرور NAS می‌توان بطور همزمان به سرورهای ویندوزی و لینوکسی سرویس داد و با استفاده از چند اینترفیس (مجازی یا حقیقی) به چند شبکه متصل شده و به سرورهای متصل به آن‌ها سرویس داد. مشهورترین سیستم عامل NAS در حال حاضر FreeNAS می‌باشد که رابط کاربری آن که از اتصال به نرم‌افزار web-base آن که از طریق فایرفاکس حاصل شده است در شکل ۵-۱ قابل مشاهده است. البته سیستم عامل‌های دیگری چون Nexenta و NASLite نیز بدین منظور ارائه شده‌اند.

---

[90] Storage Area Network
[91] Network Attached Storage



شکل ۵-۱. صفحه مدیریت freeNAS

۳۹-۵-۲- راه اندازی یک *ISCSI SAN*

در این بخش قصد داریم به کمک سیستم عامل open filer یک ISCSI SAN نرم‌افزاری را راه‌اندازی کرده تا آن را به میزبان‌های ESXi متصل کنیم.

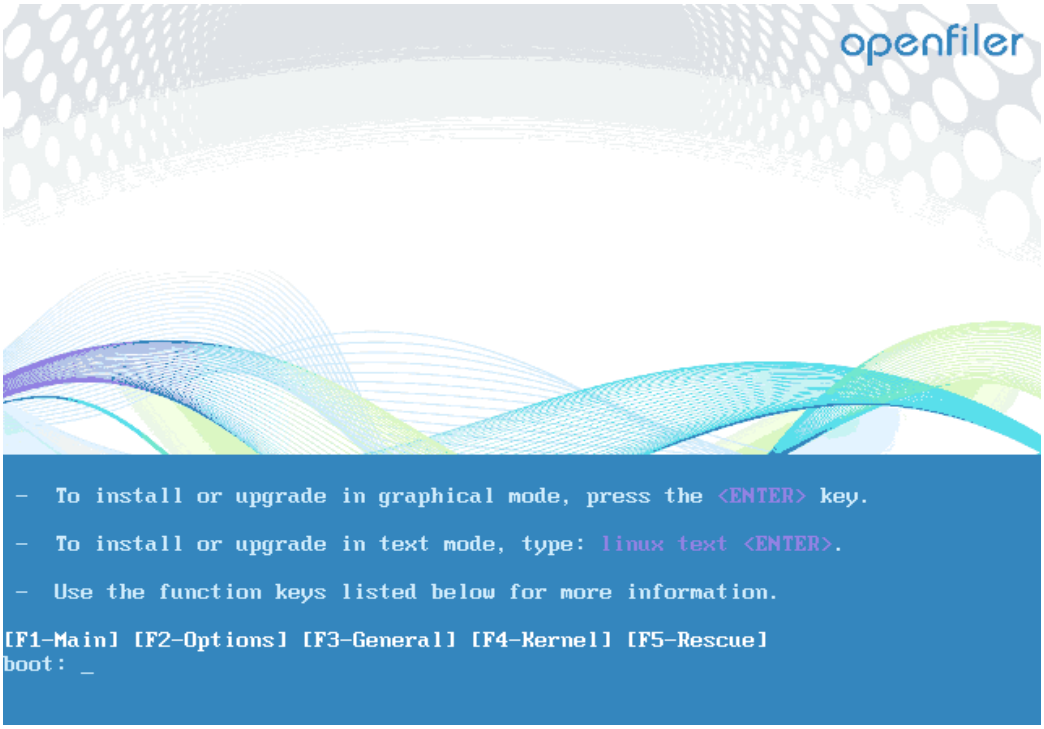
بدین منظور ابتدا لازم است تا این سیستم عامل را نصب کنیم.

۵-۲-۱ نصب Open Filer

قبل از شروع نصب توجه داشته باشید که این سیستم‌عامل را می‌توانید بصورت مجازی‌سازی شده بر روی یکی از میزبان‌های ESXi نصب کنید. یعنی بدون اینکه نیازی به سخت‌افزار اضافی داشته باشید یکی از ماشین‌های مجازی اجرا شده بر روی یکی از میزبان‌هایESXi را بعنوان ذخیره‌ساز SAN استفاده کنید.

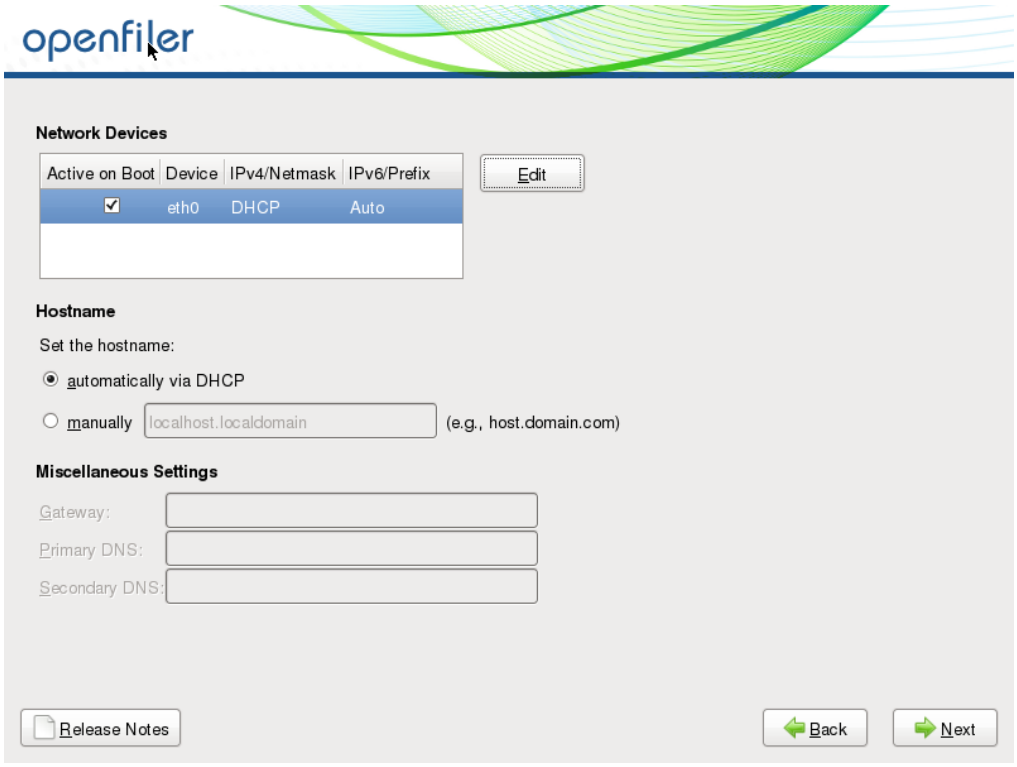
اگرچنین قصدی دارید و یا اینکه قصد شبیه سازی به کمک WMvare workstation را دارید هنگام انتخاب سیستم‌عامل لینوکسی cent os را انتخاب نمائید. حال فرایند نصب را آغاز می‌کنیم.

پس از بوت کردن سیستم از طریق CD حاوی سیستم عامل open filer تصویری مشابه با شکل ۵-۲ را مشاهده خواهید کرد. برای نصب در حالت گرافیکی اینتر را بفشارید.



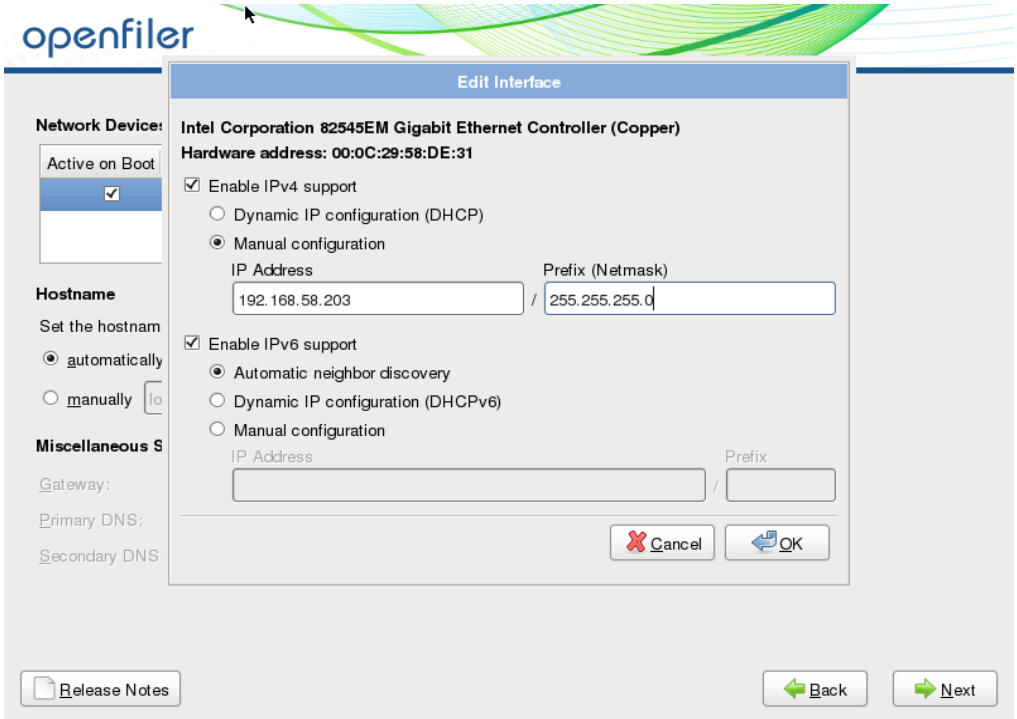
شکل ۵-۲. نصب open filer

پس از لود کامل دکمه next را کلیک کنید. در ادامه با انتخاب زبان صفحه‌کلید، next را بزنید پس ازلود کامل دکمه next راکلیک کنید. در ادامه با انتخاب زبان صفحه‌کلید next را بزنید احتمالا با زدن next با پیغامی با این مضمون برخورد خواهید کرد که اطلاعات موجود در هارددیسک شما به طورکامل از بین خواهد رفت. اگر اطلاعات مهمی ندارید؛ با انتخاب yes فرایند نصب را ادامه دهید. در صفحه بعد می‌توانید پیکربندی لازم هارددیسک را برای نصب انتخاب کنید که می‌توانید بدون هیچ تغییری در گزینه‌های پیش فرض با زدن next به مرحله بعد بروید. در ادامه با صفحه مربوط به تنظیمات شبکه مواجه خواهید شد که مشابه شکل ۵-۳ خواهد بود در اینجا می‌توانید با کلیک بر روی Edit، به اینترفیس‌ها IP استانیک اختصاص دهید. مشابه شکل ۵-٤.



شکل ۵-۳. تنظیمات شبکه open filer

با کلیک بر روی next به صفحه انتخاب منطقه زمانی وارد می‌شوید که پس از انتخاب شهر مورد نظر با کلیک بر روی next به صفحه بعد خواهید رفت.



شکل ۵-٤. اختصاص IP به کارت شبکه در open filer

در اینجا نیز رمز عبور کاربر ریشه یا همان root را وارد کرده و next را بفشارید. حال با زدن next فرایند نصب شروع خواهد شد که ممکن است چندین دقیقه به طول انجامد. در پایان فرایند نصب، با کلیک بر روی reboot سیستم را ریستارت نمائید.

پس از ریستارت شدن ولود کامل openfiler با تصویری شبیه به شکل 5-5 مواجه خواهید شد.

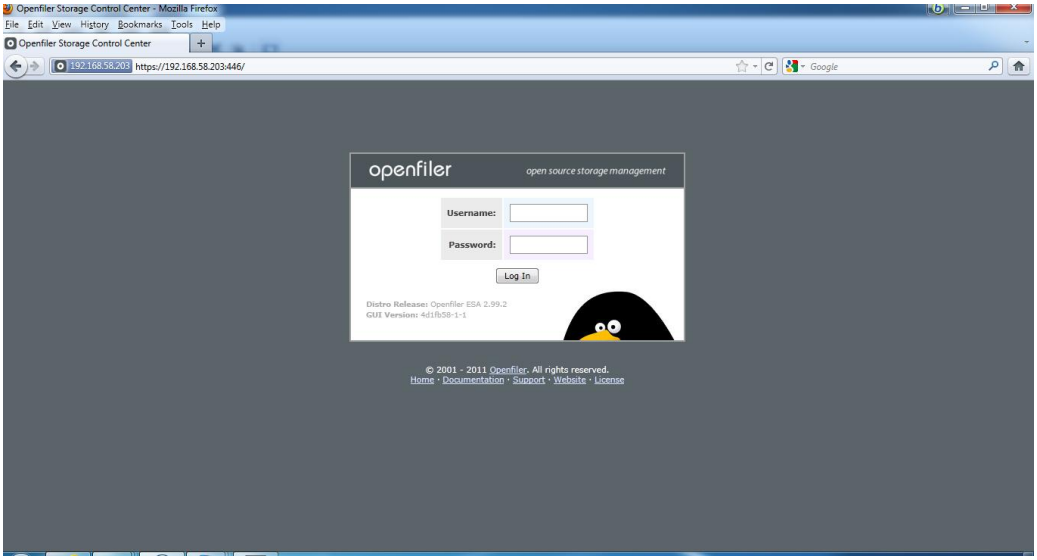


شکل ۵-۵. open filer پس از نصب

در اینجا نصب open filer به پایان رسید. حال می‌توانید به کمک یک web broswser (بهتر است از firefox استفاده کنید) و یک سیستم دومی به open filer متصل شده و آن را مدیریت کنید.

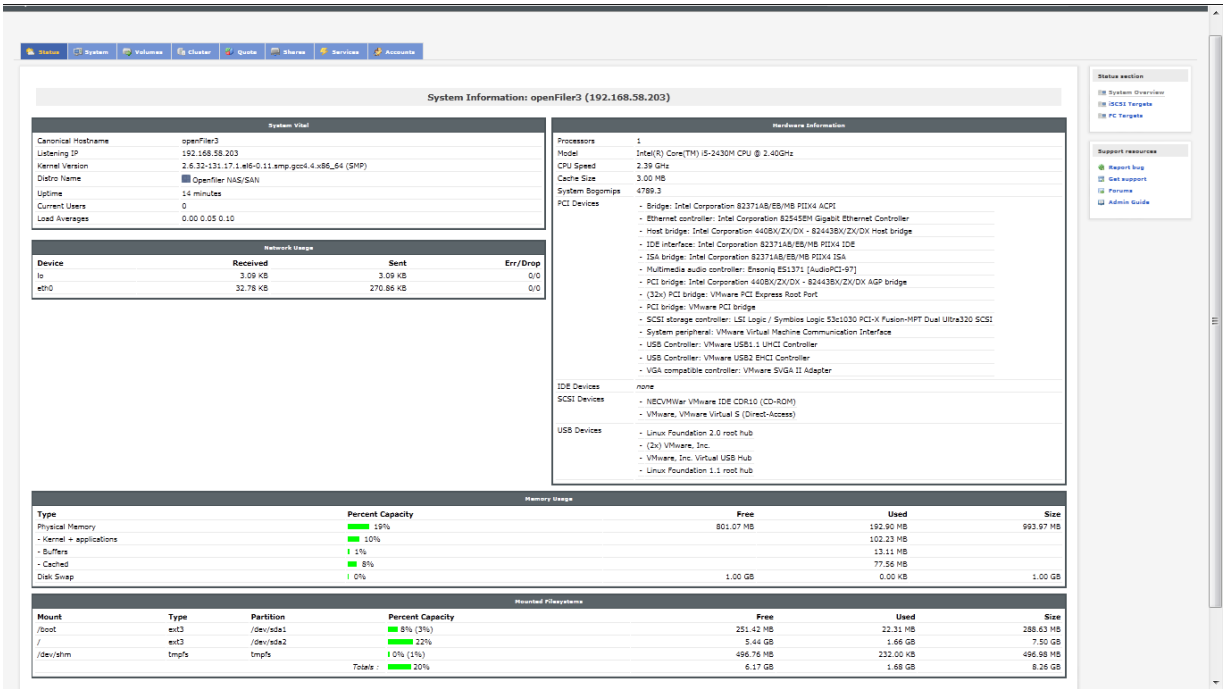
۵-۲-۲ مدیریت Open Filer

برای مدیریت open filer، پس از اجرای web browser، آدرس ip سیستم open filer را با پورت ۴۴۶ و پروتکل https در نوارآدرس وارد کرده و اینتر را بفشارید. یعنی به شکل https://IP:446 پس از لود شدن صفحه که مشابه شکل۵-۶ است با نام کاربری "openfiler" و رمز عبور "password" به سیستم login کنید.



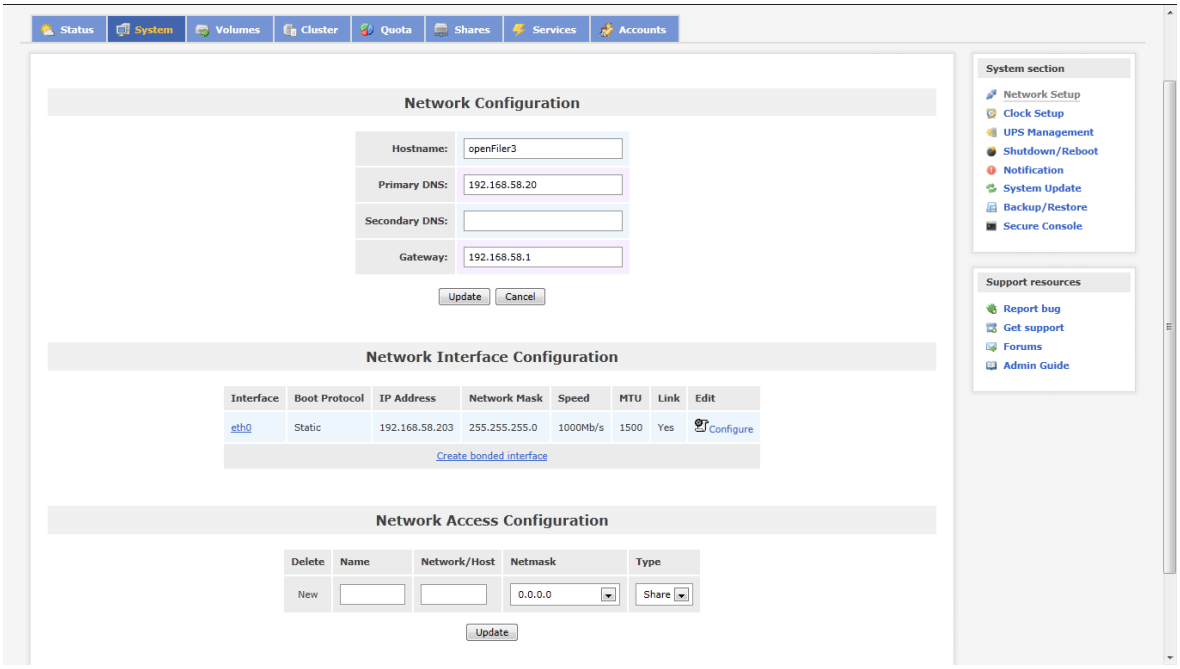
شکل ۵-۶. صفحه login در open filer

درابتدا اولین صفحه‌ای که می‌بینید مشابه شکل ۵-۷ خواهد بود که همان صفحه status است و حاوی اطلاعاتی در مورد سخت‌افزار سیستم می‌باشد.



شکل ۵–۷. صفحه مدیریت open filer

با ورود به مرکز مدیریت متوجه خواهید شد که مرکز مدیریت، دارای سربرگ‌های[۹۲] مختلف بوده و هر کدام از سربرگ‌ها در سمت راست خود ابزارهایی را در دسترس قرار می‌دهند. مثلا در سربرگ system که در شکل ۵–۸ قابل مشاهده است، با کلیک بر روی هر یک از ابزارها در سمت راست صفحه می‌توانید تنظیماتی از قبیل تنظیم زمان، تنظیمات مربوط به شبکه پشتیبان‌گیری، بروز[۹۳] کردن سیستم و... را انجام دهید. باکلیک بر روی سربرگ‌های دیگر به تنظیمات دیگر نیز دسترسی خواهید داشت که مادر اینجا به بعضی از آن‌ها اشاره خواهیم کرد.

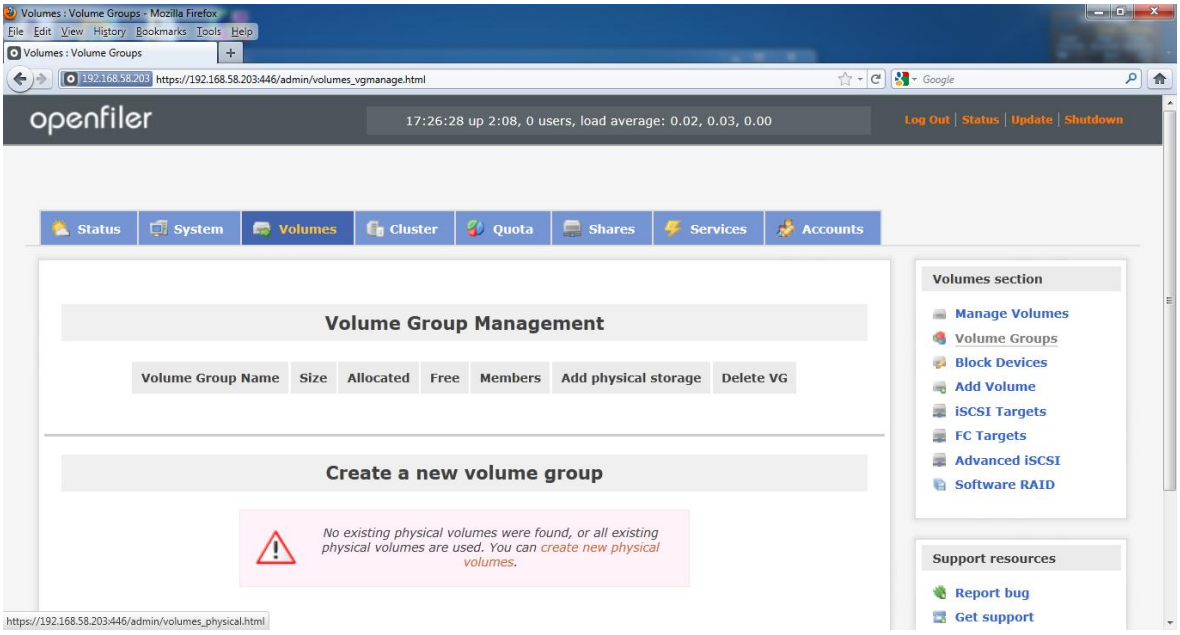


شکل ۵–۸. سربرگ system در صفحه مدیریت open filer

[92] tabs
[93] Update

هدف ما از استفاده open filer، راه اندازی یک SAN storage است. بدین منظور لازم است یک فرایند چند مرحله‌ای صورت پذیرد؛ که ما در ادامه تمام این مراحل را گام به گام طی خواهیم کرد.

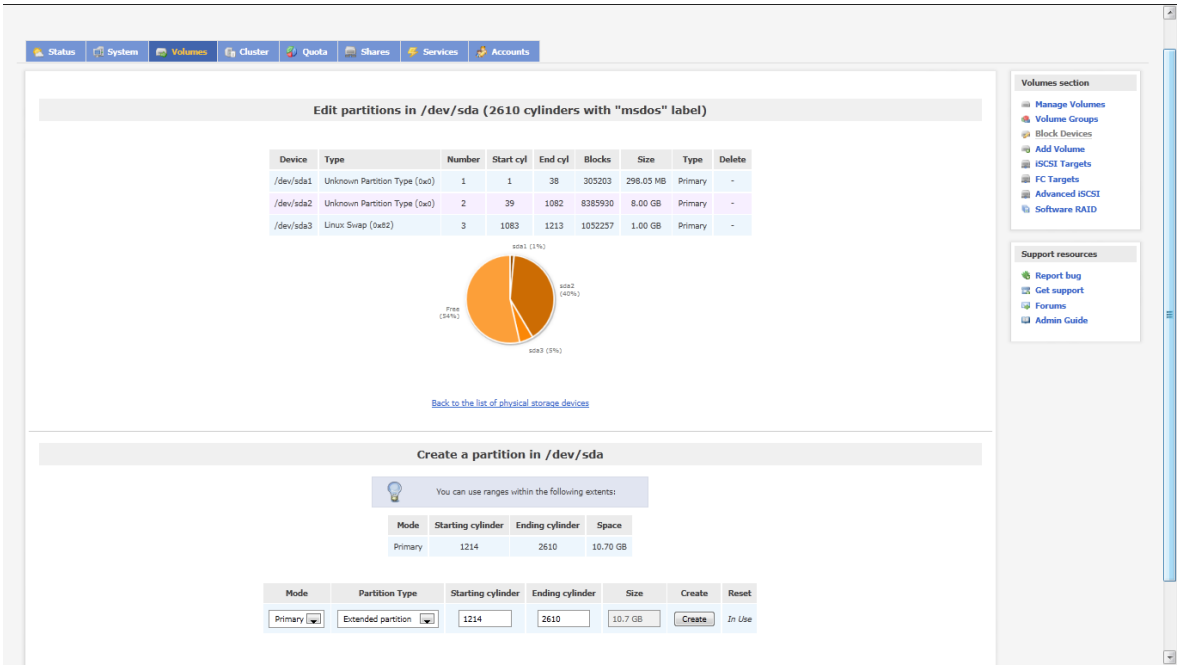
۱. ابتدا لازم است بر روی دیسک‌های متصل به سیستم پارتیشن‌هایی ساخته شود برای این کار بر روی سربرگ volumes کلیک کنید. تصویری مشابه شکل ۵-۹ را مشاهده خواهید کرد. (البته اگر از قبل پارتیشن نساخته باشید)



شکل ۵-۹. ساخت پارتیشن بر روی دیسک

۲. برای ایجاد پارتیشن جدید بر روی لینک create new physical volumes کلیک نمائید. پس ازآن هارد دیسک‌های متصل به سیستم را مشاهده خواهید کرد.

۳. بر روی دیسک مورد نظر برای ساخت پارتیشن کلیک نمائید. تصویری مشابه به شکل ۵-۱۰ را خواهید دید.



شکل ۵-۱۰. تنظیم ویژگی‌های پارتیشن

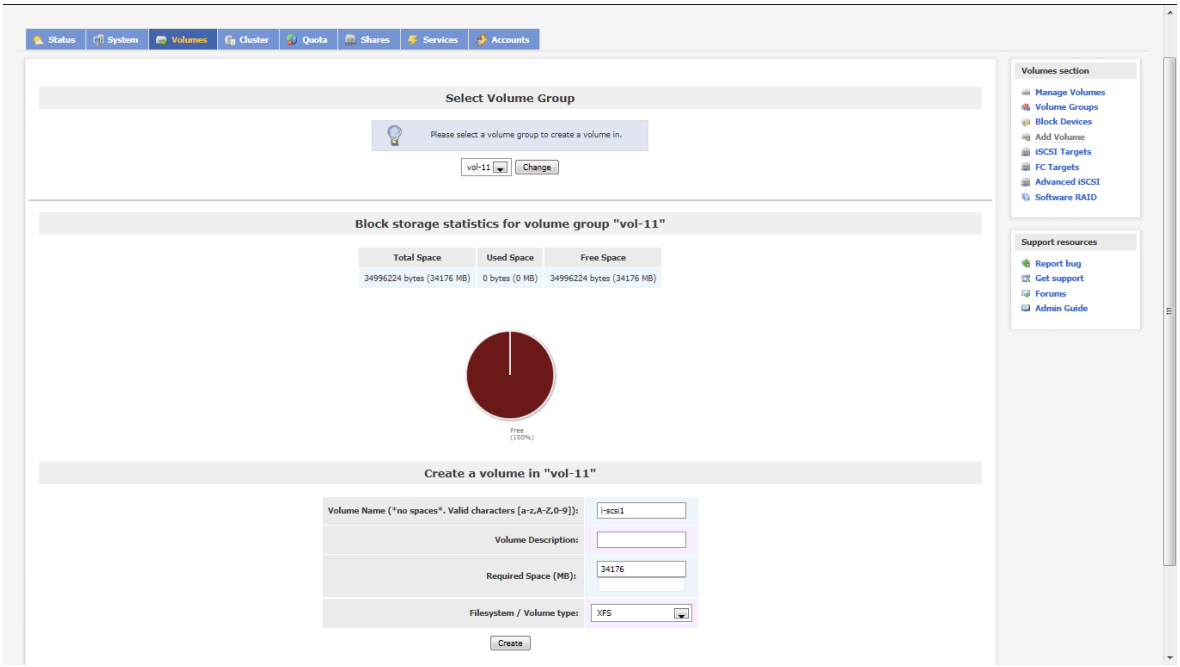
۴. در پائین صفحه آپشن‌های مربوط به پارتیشن جدید قابل تنظیم است. Mode را primary و type را physical volume انتخاب کنید. پس از وارد کردن سیلندر شرع و پایان بر روی create کلیک کنید تا پارتیشن مورد نظر ساخته شود. اگرپارتیشن مورد نظر ساخته نشد، تعدادی از سیلندرها را نادیده بگیرید(با افزایش شماره سیلندر شروع و کاهش شماره سیلندر انتها).

البته توجه داشته باشید که یک هارد دیسک نمی‌تواند بیش از چهار پارتیشن primary داشته باشد. اگر به بیش از ۴ پارتیشن نیاز دارید باید حداکثر سه پارتیشن primary و یک پارتیشن primary- extended ایجاد کنید و پس از آن ما بقی پارتیشن‌ها را در logical mode ساخته و زیر مجموعه پارتیشن primary- extended قرار دهید. از آنجایی که کمتر نیاز به این مورد پیدا می‌شود از توضیح بیشتر در رابطه با آن خودداری می کنیم و ذکر این نکته هم صرفا جهت اطلاع بود.

۵. در مرحله بعد لازم است تا یک volume group ایجادشود. برای این منظور از همین سربرگ volumes، از سمت راست صفحه بر روی volume group کلیک نمائید. در صفحه‌ای که باز می‌شود نامی برای volume group وارد کنید و پارتیشن‌هایی که قصد دارید تا زیر مجموعه این volume group قرار دهید را با پر کردن چک باکس کنارشان انتخاب کنید. مجموع فضای پارتیشن‌های انتخاب شده، حجم volume group را تشکیل می‌دهد.

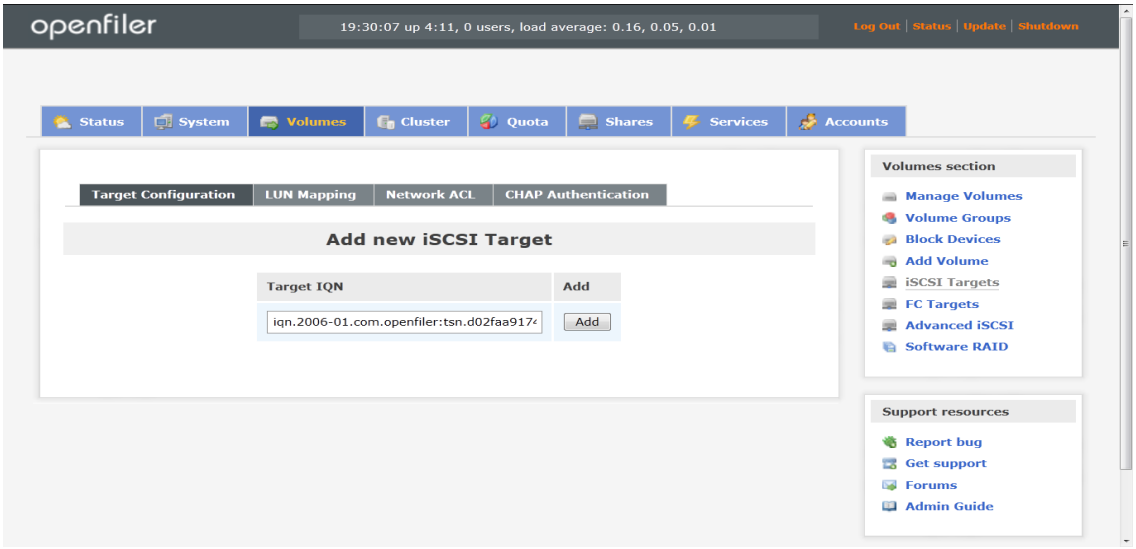
۶. حال لازم است volumeی را ساخته و فایل‌سیستمی را به آن اختصاص دهیم. بدین‌منظور بر روی سربرگ shares کلیک کرده و در صفحه لود شده بر روی لینک create new filesystem volume کلیک نمائید و یا اینکه مستقیما از سربرگ volume ، از سمت راست بر روی add volume کلیک کنید.

۷. در صفحه باز شده که شبیه به شکل ۵-۱۱ خواهد بود، در قسمت name نامی دلخواه را برای volume جدید وارد نمائید، پس از وارد کردن توضیحات و حجم مورد نیاز، block را بعنوان file system برگزینید. توجه داشته باشید که این volumeها همان LUN یا واحدهای منطقی SAN Storageها هستند.



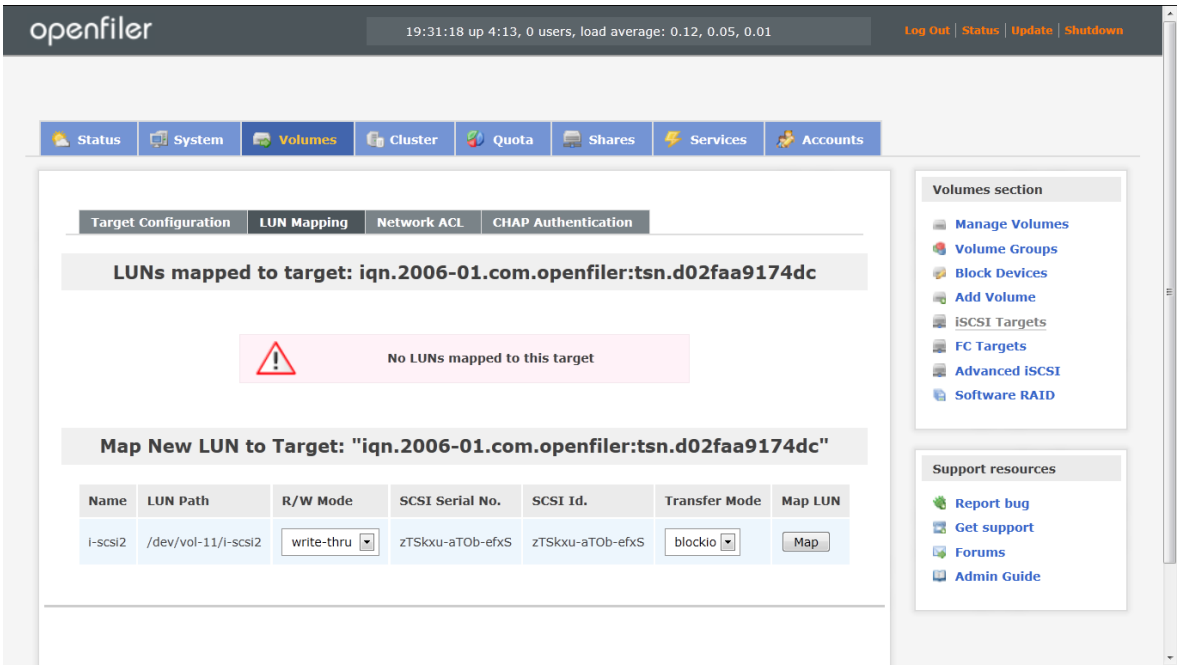
شکل ۵-۱۱. ساخت Volume Group

۸. برای استفاده از این volumeها در سرورهای ESXi و یا هر سرور و سیستم دیگر می‌بایست یک iqn به هر یک از آن‌ها اختصاص داد.برای اینکار از سربرگ volume از سمت راست صفحه بر روی ISCSI target کلیک نمائید. صفحه‌ای مشابه شکل ۵-۱۲ را مشاهده خواهید کرد. البته بایستی قبل از این کار سرویس ISCSI targetفعال باشد که برای فعال سازی آن به سر برگ services رفته و سرویس مذکور فعال و اجرا کنید.



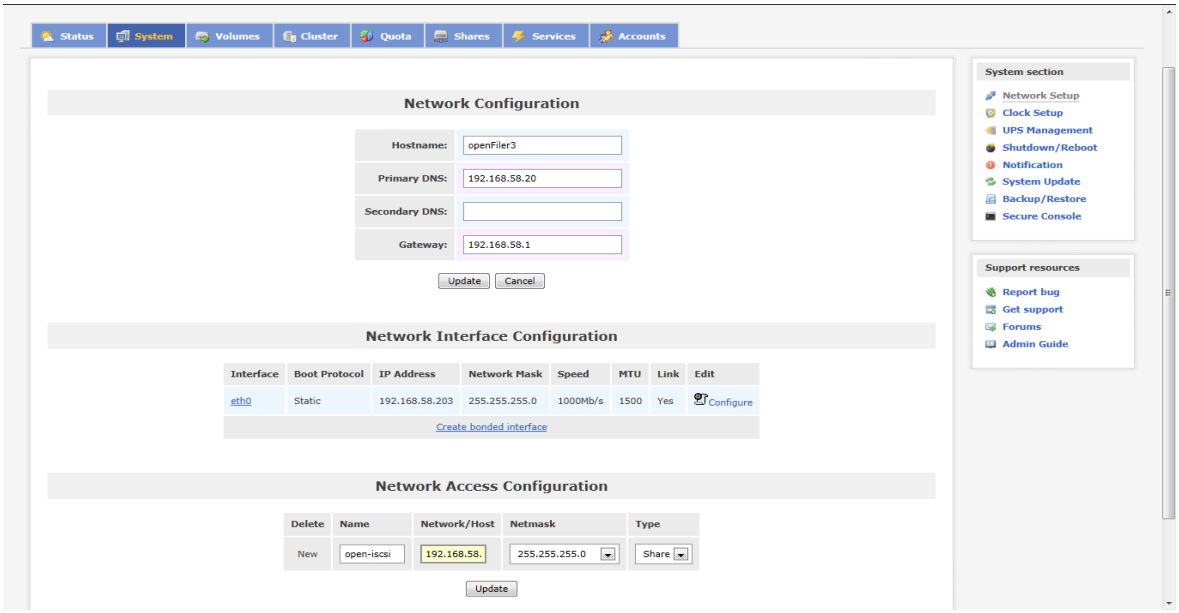
شکل ۵-۱۲ . ساخت iqn

۹. برای ایجاد یک iqn بر روی add کلیک کنید. پس از ایجاد iqn باید آن را به volumeها یا همان LUNها، map نمائید. برای این کار به سربرگ LUN mapping در همین صفحه رفته و iqn ساخته شده را به volume مورد نظر map نمائید. مطابق شکل ۵-۱۳. اگر volumeهای دیگر نیز دارید به سربرگ target configuration بازگشته و پس از ایجاد iqn، آن را به volume مورد نظر map کنید.



شکل ۵-۱۳. map کردن volumeها به iqn

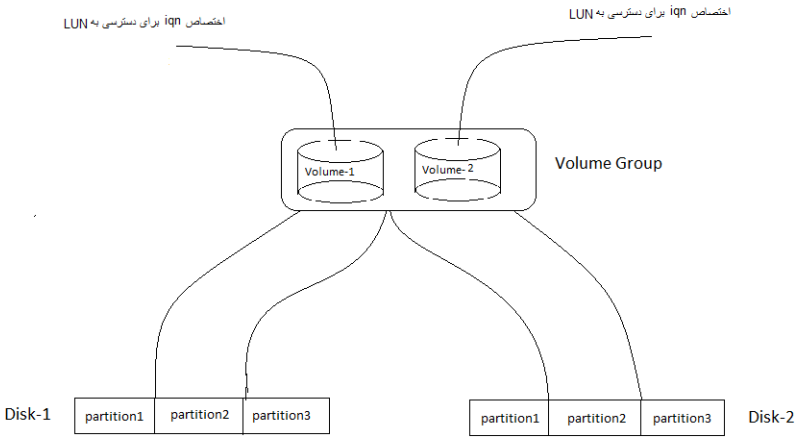
۱۰. قبل از ادامه بایستی امکان دسترسی سرورهای شبکه به volumeها را فراهم کرد. برای این کار به سر برگ system رفته و در پائین صفحه مطابق شکل ۵-۱۴ آدرس شبکه و ماسک آن راوارد کنید.



شکل ۵-۱۴. تنظیم دسترسی شبکه به volumeها

۱۱. در آخرین مرحله بایستی امکان دسترسی به سرورهای شبکه در مرحله قبل فراهم شد را فعال نمائید. برای این کار به سر برگ volume بازگشته و پس از کلیک بر روی ISCSI target به network ACL رفته و امکان access را allow کرده و بر روی update کلیک نمائید. لازم به ذکر است که می‌توانید از همین صفحه در قسمت chap authentication، از پروتکل رمز گذاری chap نیز استفاده نمائید.

شکل ۵-۱۵ تصویری از این فرایند ۱۱ مرحله‌ای بدست می‌دهد.



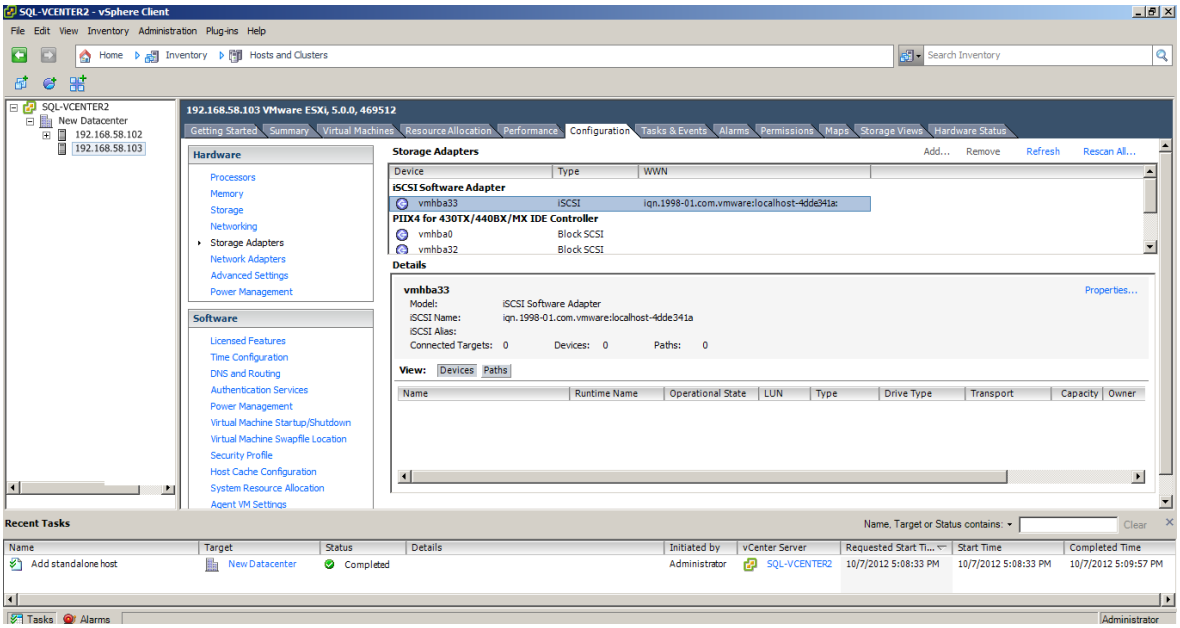
شکل ۵-۱۵. نحوه ساخته شدن یک ذخیره‌ساز ISCSI به‌کمک open filer

کار مادر open filer تمام است. در ادامه بایستی ESXi را برای استفاده از این ISCSI، پیکربندی نمائیم.

برای اتصال ISCSI به میزبان‌های ESXi بدین صورت عمل می‌کنیم:

۱. ابتدا vCenter Server وارد شوید (login نمائید). نحوه ورود به vCenter Server در بخش‌های گذشته گفته شده است.

۲. بر روی میزبان ESXi مورد نظر کلیک کنید (برای اطلاع از نحوه اضافه کردن میزبآن‌های ESXi به سرور vCenter به بخش ششم مراجعه فرمائید) وپس ازآن به سربرگ configuration بروید واز سمت چپ صفحه بر روی storage adapters کلیک نمائید. شکل ۵-۱۶ این موضوع را نشان می‌دهد.



شکل ۵-۱۶. پیکربندی ESXi برای استفاده از ذخیره‌سازهای ISCSI

۳. می‌بایست قبل از هرکاری یک آداپتور ISCSI بسازید. بدین‌منظوردر بالای صفحه سمت راست بر روی Add کلیک کرده و در پیغام نمایش داده شده بر روی ok کلیک نمائید.

۴. پس از ساخت آداپتور، بر روی آن راست کلیک کرده، properties را برگزینید.

۵. از سربرگ dynamic discovery بر روی Add کلیک کرده آدرس IP سرورopen filer را وارد نموده و شماره پورت را بدون تغییر رها کنید. اگردر موقع ساخت iqn در open filer، chap را فعال کرده‌اید در این جا نیز قسمت مربوط به chap را تنظیم کنید و با زدن ok صفحه Add را بسته و پس ازآن با کلیک بر روی close خارج شوید. بعد از بسته شدن صفحه، از شما در مورد scan دوباره آداپتور سوال خواهد شد که بر روی yes کلیک نمائید.

پس از چندثانیه LUNهای موجود در open filer درپائین صفحه نمایش داده خواهد شد.

۶. در ادامه می‌بایست برای استفاده از این ذخیره‌سازه آن‌ها را باسیستم‌فایل VMFS فرمت کرد. برای این کار از سمت چپ صفحه بر روی storage کلیک نمائید واز بالای صفحه، سمت راست، بر روی Add storage کلیک کنید.

۷. در ویزارد اجرا شده پس از انتخابDisk /LUN بر روی next کلیک نمائید.

۸. در این مرحله LUN مورد نظر را انتخاب کرده و بر روی next کلیک نمائید.

۹.در اینجا سیستم فایل مناسب را انتخاب کرده و next را بزنید. بهتر است VMFS-5 را انتخاب کنید. البته اگر از نسخه ESXi بجز نسخه ۵ استفاده می‌کنید از این سیستم فایل پشتیبانی نخواهد شد و بایتسی vmfs-3 را انتخاب نمائید.

۱۰. پس از کلیک بر روی next و next و وارد کردن نام برای datastor بر روی next کلیک کنید.

۱۱. در ادامه حجم دلخواه را انتخاب کرده بر روی next کلیک نمائید و در انتها finish را بزنید.

با بسته شدن صفحه ویزارد پس ازچند ثانیه data store به لیست اضافه خواهد شد. توجه داشته باشید که نیازی نیست که این فرایند برای هر یک از میزبآن‌های ESXi تکرار شود؛ بلکه با افزودن یکdata store به یک سرور ESXi همه سرورهای عضو کلاستر، به آن data store دسترسی خواهند داشت.

در اینجا این بخش به پایان می‌رسد. البته دنیای ذخیره‌سازها، دنیای بسیار وسیعی است که خود به‌تنهایی نیاز به یک کتاب جداگانه دارد.

۳۹-۶- راه اندازی و مدیریت سیستم مجازی سازی

همه چیز برای شروع آماده است تمام توضیحات پیشنیاز در بخش‌ها گذشته گفته شد. پس بدون هیچ مقدمه‌ای پس کار اصلی را آغاز می‌کنیم.

کار اصلی ما با میزبآن‌ها یا همان hostها و کلاسترها است بنابراین بر روی آیکون hosts and clusters کلیک نمائید و یا کلید ترکیبی ctrl+shift+h را بفشارید.

۳۹-۶-۱- ایجاد دیتاسنتر و اضافه کردن میزبآن‌های ESXi به vCenter

برای شروع یک دیتا سنتر ایجاد می‌کنیم. بدین منظور از سمت چپ صفحه بر روی نام سرور vCenter راست کلیک کرده و new data vCenter را انتخاب کرده و نامی برای آن وارد کنید.

در ادامه بایستی میزبآن‌های ESXi را به vCenter متصل نمائید. برای این کار مراحل زیر را انجام دهید.

۱.بر روی دیتا سنتر راست کلیک کرده و برروی Add Host کلیک نمائید. ویزاردی اجرا خواهد شد. شکل ۶-۱ این موضوع را نشان می‌دهد.

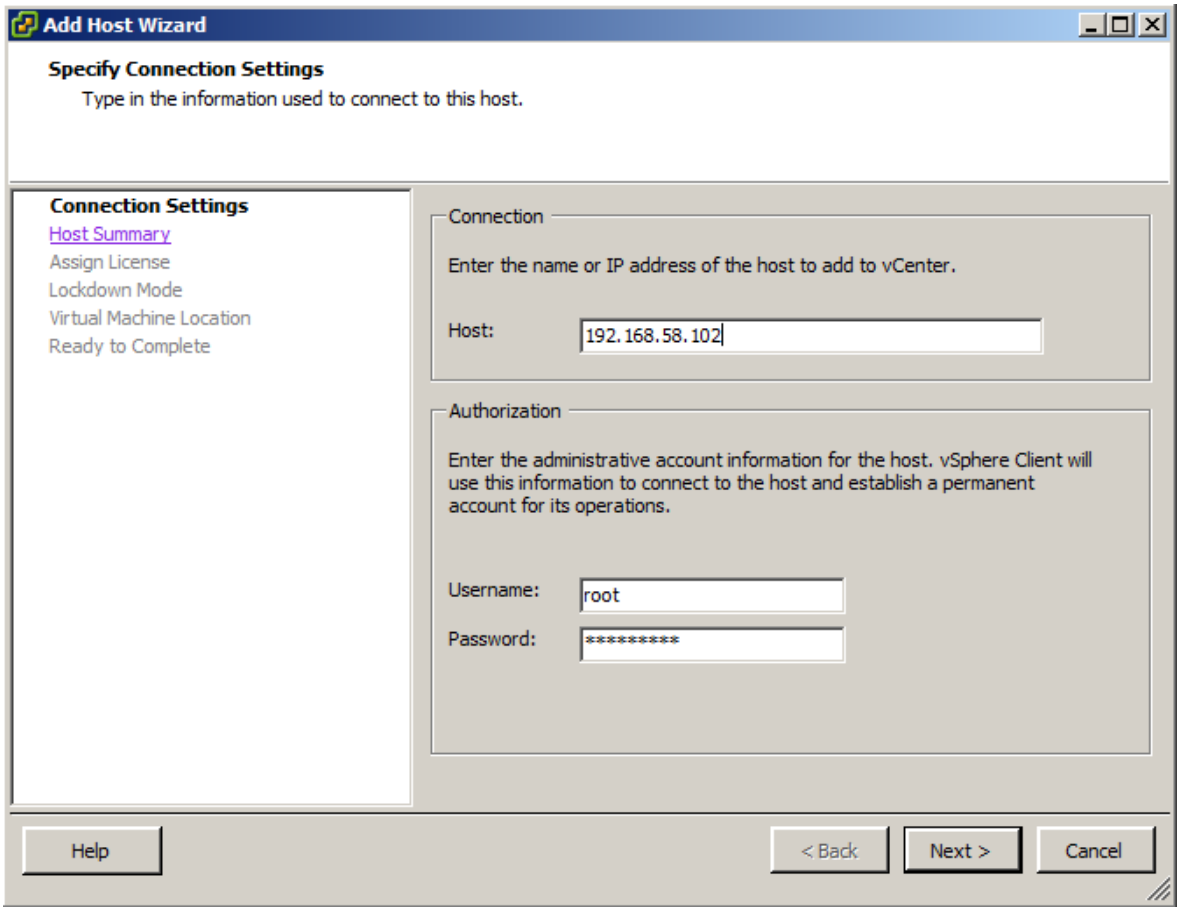
۲. در صفحه اول ویزارد اجرا شد در قسمت host نام سرور ESXi و یا آدرس IP آن را وارد کنید. در قسمت username نام کاربری root و در قسمت password، پسورد کاربر root را وارد نمائید بر روی next کلیک کنید.

۳. اطلاعاتی در مورد سرور نمایش داده خواهد شد. دوباره next رابزنید.

۴. در این مرحله می‌توانیدlicense key به سرور اختصاص دهید. و next را بزنید.

۵. در این قسمت می‌توانید با علامت زدن چک باکس enable lockdown mode امکان وارد شدن سرور ESXi به طور مستقیم (بدون استفاده از vCenter) از راه دور را غیر فعال نمائید. با زدن next به مرحله بعد بروید.

۶. در اینجا پس ازانتخاب دیناسنتر برای ماشین‌های مجازی بر روی next کلیک کنید، و پس از آن finish را کلیک کنید. پس از مدت کوتاهی میزبان اضافه شده در سمت چپ صفحه نمایش داده خواهد شد.



شکل ٦-۱. اضافه کردن میزبآن‌های ESXi به vCenter

۳۹-۶-۲- ساخت ماشین مجازی

دومین مسئله پس از اضافه کردن میزبآن‌ها، ایجاد و راه‌اندازی ماشین‌های مجازی است.برای این کار:

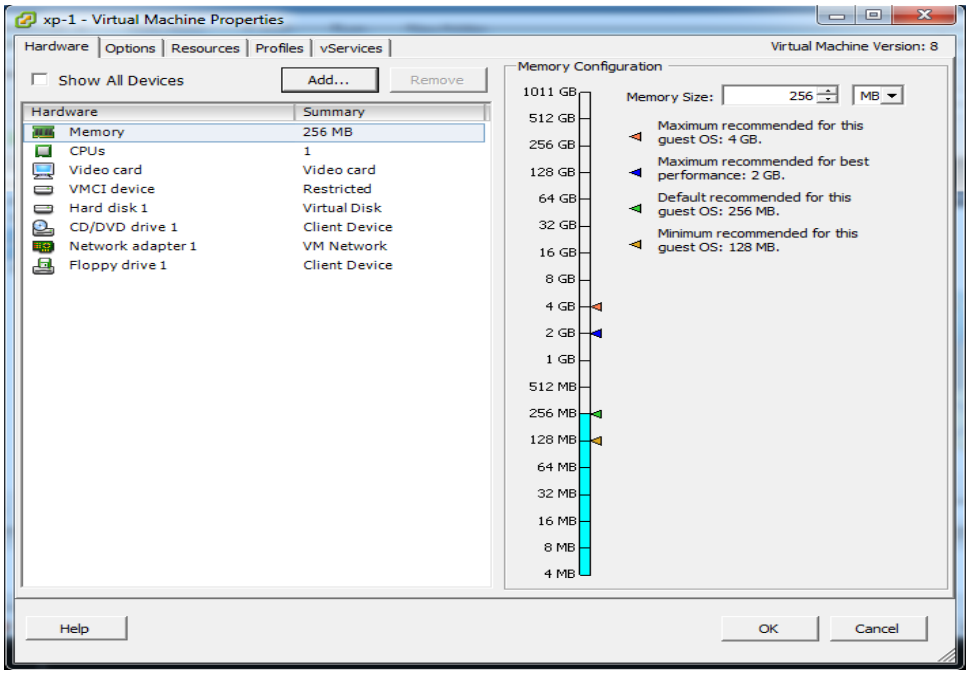
۱. بر روی کلاستر یا میزبان مورد نظر راست‌کلیک کرده، New Virtual Machine را انتخاب کنید.
۲. ویزاردی اجرا خواهد شد. در صفحه اول دو گزینه در دسترس خواهد بود. با انتخاب گزینه Typical سخت‌افزار مجازی پیش‌فرض به سیستم اختصاص خواهد یافت که البته پس از ساخت ماشین مجازی قابل تغییر خواهد بود. اما در گزینه Custom، اختصاص سخت‌افزار، در طی ویزارد صورت خواهد پذیرفت. Typical را انتخاب کرده Next را بزنید.
۳. پس از انتخاب دیتاسنتر برای عضویت ماشین مجازی و واردکردن نامی دلخواه برای ماشین مجازی Next را کلیک کنید.
۴. در این قسمت، ذخیره‌ساز موردنظر برای نگهداری ماشین مجازی را انتخاب کنید و Next را بزنید.
۵. در اینجا می‌توانید سیستم‌عامل مورد نظر برای ماشین مجازی را انتخاب کنید.
۶. در این جا کارت شبکه، نوع آن و شبکه/شبکه‌های متصل به آن را انتخاب کنید. Next را بزنید.
۷. در این مرحله فضای مورد نیاز برای اختصاص به ماشین مجازی(به عنوان دیسک سخت مجازی) را انتخاب کنید. برای اختصاص فضا به ماشین مجازی دو انتخاب وجود دارد. Thick Provision و Thin Provision. اگر اولی را

انتخاب کنید، کل فضای درخواست شده به محض ساخته شدن ماشین مجازی، به آن اختصاص خواهد یافت. یعنی کل فضای درخواست شده اشغال خواهد شد. اما در حالت دوم (Thin Provision) فضای درخواست شده فقط نشانگر محدودیت ماشین مجازی در استفاده از فضای دخیره‌سازی است. یعنی تا زمانی که ماشین مجازی از این فضا استفاده نکند (فایلی در آن قرار ندهد) فضایی اشغال نخواهد شد. پس از تکمیل این قسمت، بر روی Next کلیک کنید.

۸. در این قسمت خلاصه‌ای از مشخصات ماشین مجازی نمایش داده خواهد شد. در پایان بر روی Finish کلیک کنید تا ماشین مجازی ساخته شود.

۳۹-۶-۳- تخصیص منابع به ماشین‌های مجازی

در هنگام ایجاد و پس از ساخت ماشین‌های مجازی می‌توان منابع اختصاص داده شده به ماشین‌های مجازی، از جمله حافظه، پردازنده، کارت‌های شبکه، ذخیره‌سازها و.... را افزایش و کاهش داد؛ و یا حتی در هنگام روشن بودن ماشین مجازی هم می‌توان بعضی از آن‌ها را ویرایش کرد (افزایش یا کاهش داد). برای این کار برروی ماشین مجازی مورد نظر راست کلیک کرده Edit setting را برگزینید. همانطور که در شکل ۶-۲ نیز مشاهده می‌کنید دارای چندین سربرگ است که بترتیب آن‌ها را توضیح خواهیم داد.



شکل ۶-۲. تخصیص منابع به ماشین‌های مجازی

سربرگ اول که Hardware است و در آن می‌توانید منابع فیزیکی اختصاص داده شده به ماشین مجازی را تغییر تغییر دهید و یا حتی می‌توانید با کلیک برروی Add، سخت‌افزار مجازی دیگری به سیستم اضافه کنید (شکل ۶-۳). در عین اهمیت، کارکردن با این قسمت ساده بوده و نیاز به دانش زیادی ندارد بنابراین از توضیح بیشتر در این رابطه خودداری می‌کنیم.

در سربرگ Option ویژگی‌های فنی‌تری در دسترس خواهد بود که بیشتر مربوط به فوق ناظر است. از جمله این ویژگی‌ها می‌توان به موارد زیر اشاره کرد:

- تغییر نوع ماشین مجازی (ویندوز، لینوکس و.....)
- فعال و غیرفعال کردن VMware tools که برروی سیستم عامل ماشین مجازی نصب می‌شود و امکان مدیریت بهتر آن رافراهم می‌کند.
- تنظیمات مربوط به روشن و خاموش کردن ماشین مجازی
- فعال کردن ویزگی‌های سخت‌افزاری مربوط به مجازی سازی

سربرگ سوم: Resourse است که در آن می‌توانید محدودیت‌های ماشین‌های مجازی در دسترسی به منابع پردازش و حافظه را تنظیم نمائید. دراین سربرگ دو گزینه خیلی مهم وجود دارد یک CPU و دیگری Memory در هریک از این دو بخش سه قسمت را مشاهده می‌کنید:

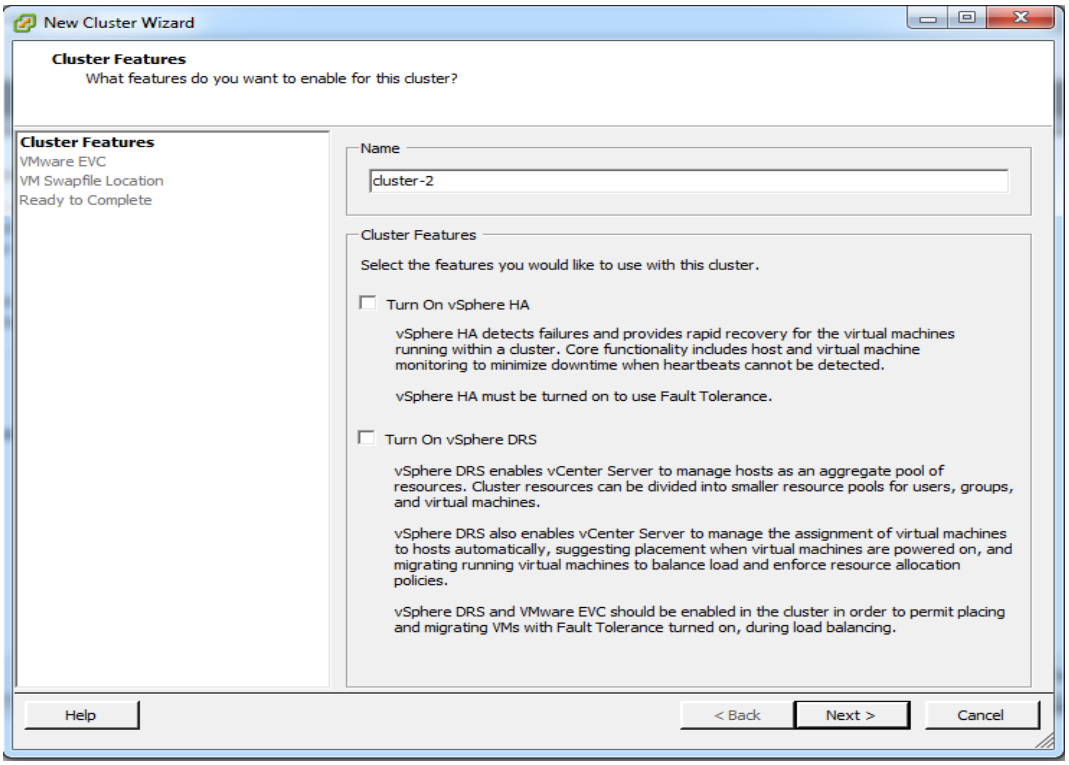
- Reservation: کاملا روشن است که منابع یک میزبان فیزیکی بین ماشین مجازی راه اندازی شده برروی آن تسهیم یا همان share می‌شود. مقدار موجود در Reservation مقداری است که به محض روشن شدن ماشین مجازی، به آن اختصاص می‌یابد اگر چه از آن استفاده نکند.
- Limit: این مقدار، حداکثر فضایی از حافظه یا فرکانس از پردازنده است که ماشین مجازی می‌تواند استفاده کند. البته با زدن تیک Unlimited ماشین مجازی امکان دسترسی به کل منابع) در صورت وجود (را خواهد داشت.
- Shares: همانطور که گفته شد منابع سرور فیزیکی بین ماشین‌های مجازی Share می‌شود و هر یک از ماشین‌های مجازی برای استفاده از منابع با دیگر ماشین‌ها رقابت می‌کند. Shares همان اولویت ماشین مجازی برای استفاده از منابع مشترک است؛ که می‌توان یکی از مقدارهای low، normal و high را به آن اختصاص داد.و یا با انتخاب Custom مقداری دلخواه به آن نسبت داد.

توجه داشته باشید که اگر ماشین مجازی نیاز بالایی به منابع دارد عدد بالاتری در share به آن اختصاص دهید؛ و دیگر اینکه مقداری که به limit اختصاص می‌دهید بهتر است ۵۰ درصد مقدارReservation باشد. مقدار Reservation هم در حدود ۵ تا ۱۰ درصد ظرفیت میزبان فیزیکی باشد.

۳۹-٦-٤- ساخت کلاستر و اضافه کردن میزبان‌های ESXi به آن

همانطور که قبلا هم گفته شد بسیاری از ویژگی‌ها و قابلیت‌های vSphere با وجود کلاستر، ممکن می‌شوند. برای ساخت کلاستر به طریق زیر عمل کنید:

۱- برروی دیتا سنتر مورد نظر راست کلیک کرده،new cluter را انتخاب کنید. شکل ٦-۳.



شکل ٦-۳. ساخت کلاستر

۲- در ویزارد اجرا شده، در کادر name، نامی برای آن انتخاب کنید، در همین قسمت می‌توانید ویژگی‌های مربوط به قابلیت دسترسی بالا یا همان HA و همچنین زمانبند منابع توزیع شد یا DRS را نیز با پرکردن چک باکس مربوط به هر کدام فعال کنید. البته فعلا این دوگزینه را انتخاب نکنید در ادامه هر دو این ویزگی‌ها را بطور مبخش بررسی خواهیم کرد. حال برروی next کلیک نمائید.

۳- در این قسمت می‌توانید با انتخاب شرکت سازنده و نوع پردازنده میزبآن‌های عضو کلاستر قابلیت EVC[۹۴] را فعال کنید. توجه داشته باشید که برای فعال سازی EVC، این قابلیت می‌بایست در پردازنده‌های میزبآن‌های عضو کلاستر وجود داشته باشد و در BIOS این میزبآن‌ها نیز این قابلیت که در پردازنده اینتل ان را با Intel-VT در پردازنده‌های AMD با نام AMD-Vشناخته می‌شوند، فعال باشد. دوباره next را بزنید.

٤- د راین قسمت می‌توانید محل ذخیره سازی swap مربوط به ماشین‌های مجازی عضو کلاستر را مشخص کنید بازدن next به مرحله بعد بروید.

٥- در این قسمت می‌توانید خلاصه‌ای از مشخصات کلاستر ایجاد شده را ببینید که با زدن Finish مرحله ساخت کلاستر به پایان می‌رسد.

برای اضافه کردن میزبآن‌های ESXi به کلاستر، می‌توانید برروی ان راست کلیک کرده و مراحل افزودن میزبان به کلاستر را همانند افزودن میزبان به دیتا سنتر را تکرار کنید. (افزودن میزبان به دیتا سنتز قبلا در همین بخش گفته شد)

همچنین اگر از قبل میزبآن‌هایی عضو دیتاسنتر هستند با عمل drag&drop می‌توانید میزبآن‌های ESXi را به عضویت کلاستر درآورید ویا بین دیتاسنترها و کلاسترهای مختلف جابه‌جا کنید. برای خارج کردن یک میزبان ESXi از کلاستر نیز

[94] Enhanced vMotion Compatability

می‌توانید پس از قراردادن میزبان در حالت maintenance mode (برای قراردادن میزبان در حالت maintenance mode، برروی میزبان موردنظر راست کلیک کرده Enter maintenance made را انتخاب می‌کنیم.

۳۹-٦-٥- فعال‌سازی ویژگی DRS در کلاستر

همانطور که قبلا نیز گفته شد DRS یا زمانبندی منابع توزیع شد، این امکان را فراهم می‌کند تا بار پردازشی و حافظه‌ای بین ماشین‌های عضو یک کلاستر توزیع شود واضح است که برای استفاده از این قابلیت می‌بایست ماشین‌های مجازی برروی ذخیره‌سازهای share شده (از جمله NAS،SAN) قرارداشته باشد. برای فعال سازی DRS برروی کلاستر مورد نظر راست کلیک کرده edit setting را انتخاب می‌کنیم.

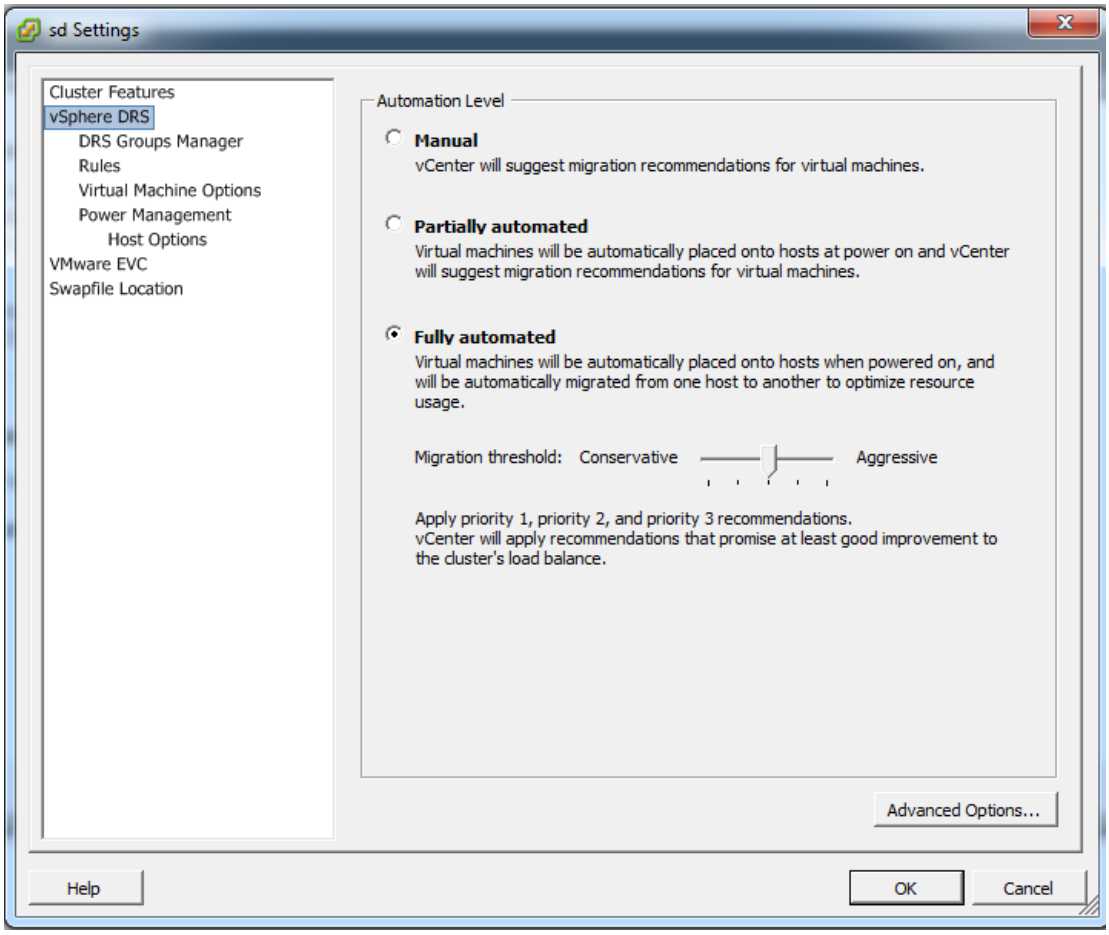
در صفحه باز شده، تیک گزینه turn on vSphere DRS را بزنید.

در سمت چپ صفحه تحت شاخه vSphere DRS می‌توانید ویژگی‌های مختلف مربوط به DRS را با کلیک برروی ویژگی مورد نظر تنظیم کنید.

در ادامه هر یک از این ویزگی هارا توضیح خواهیم داد.

٦-٥-١ Automation level

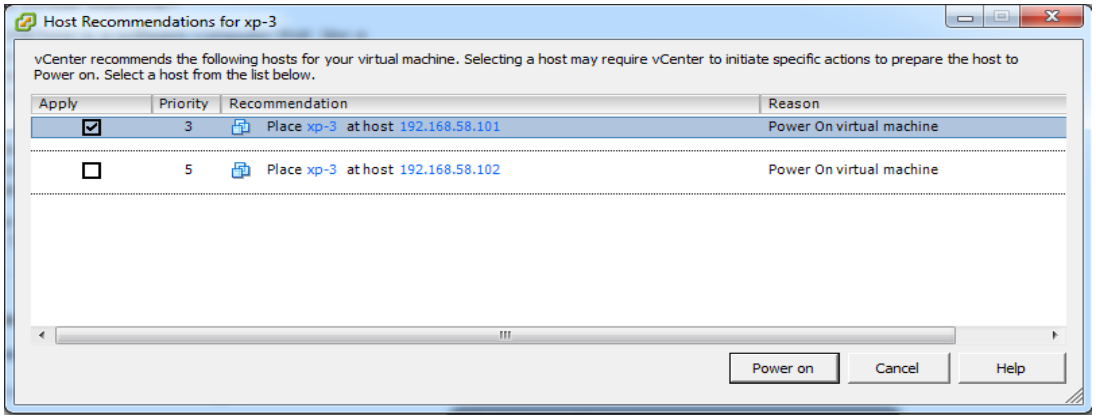
برای تعیین سطح اتوماسیون از همین صفحه (صفحه setting) از سمت چپ صفحه برروی vSphere DRS کلیک کنید همانطور که در شکل ۶-۴ مشاهده می‌کنید، سه سطح از اتوماسیون در دسترس خواهد بود.



شکل ٦-٤. تعیین سطح اتوماسیون در DRS

Manual:

در این حالت هنگام روشن شدن ماشین مجازی از کاربر در مورد محل اجرای ماشین مجازی سوال می‌شود. (یعنی ماشین مجازی برروی کدام سرور ESXi اجرا شود) شکل ٦-٥



شکل ٦-٥. روشن کردن ماشین مجازی در حالت manual DRS

Partially Automated

در این حالت هنگام روشن شدن، ماشین مجازی به طور اتوماتیک در مناسب ترین سرور اجرا می‌شو؛ ولی در صورتی که براثر بالارفتن بار پردازش یک سرور، نیاز به انتقال یک ماشین مجازی به سرور دیگر وجود داشته باشد سیستم DRS با پیغامی این موضوع را به کاربر اطلاع می‌دهد و از کاربر(مدیر) درباره انتقال ماشین مجازی سوال کرده و بهترین سرور را برای انجام این انتقال پیشنهاد خواهد کرد. تفاوت این حالت با حالت قبل فقط در هنگام روشن شدن ماشین مجازی است که، انتخاب سرور، در حالت اول بصورت دستی و در حالت دوم بصورت اتوماتیک انجام خواهد شد.

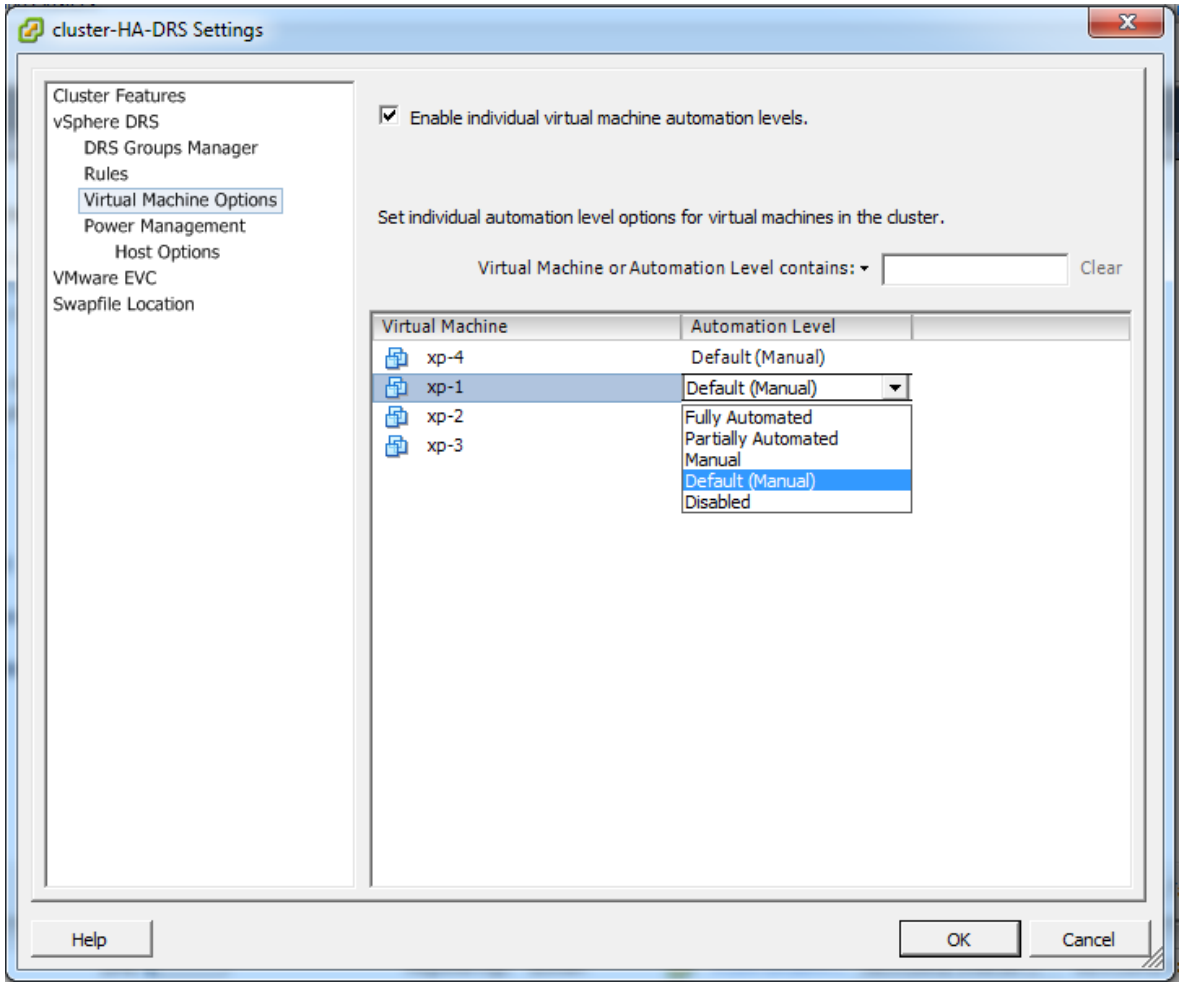
Fully Automated

در این حالت کلیه مراحل تنظیم بار پردازشی چه هنگام روشن شده ماشین مجازی چه در حین اجرا، کاملا بصورت خودکار انجام خواهد شد.

در همین قسمت، پائین صفحه یک نوار لغزان به نام Migration threshold وجود دارد که به کمک آن می‌توان سطح آستانه‌های برای انتقال ماشین مجازی به سرور دیگر را تعیین کرد. هر چه بسمت aggressire نزدیکتر باشد تعداد انتقال‌ها بیشتر خواهد بود.

تنظیمات گفته شده در بالا برروی کل ماشین‌های مجازی کلاستر اعمال می‌شود.

البته می‌توان بعضی از ماشین‌ها را مستثنی کرد و برای این کار برروی Virtual machine option کلیک کنید. مشابه شکل ٦-٦، تمام ماشین‌های عضو کلاستر را مشاهده خواهید کرد با کلیک برروی هر ماشین می‌توان سطحی از اتوماسیون را به هر کدام اختصاص داد. البته باید قبل از آن تیک گزینه Enable individual virtual machine automation را فعال کنید.



شکل ٦-٦. انتصاب سطح اتوماسیون در DRS به ماشن‌های مجازی

٦-٥-٢ گروه بندی ماشین‌های مجازی و میزبآن‌های ESXi

از دیگر قابلیت‌های دیگر DRS این است که می‌توان ماشین‌های مجازی و میزبآن‌های ESXi را دسته‌بندی کرده تا بتوان برروی آن‌ها سیاست‌های خاصی را اعمال کرد. برای ایجاد یک گروه ماشین مجازی: در صفحه Setting مربوط به کلاستر پس از فعال کردن DRS (با انتخاب گزینه Turn on vSphere DRS) برروی DRS group manager از سمت چپ صفحه کلیک کنید.

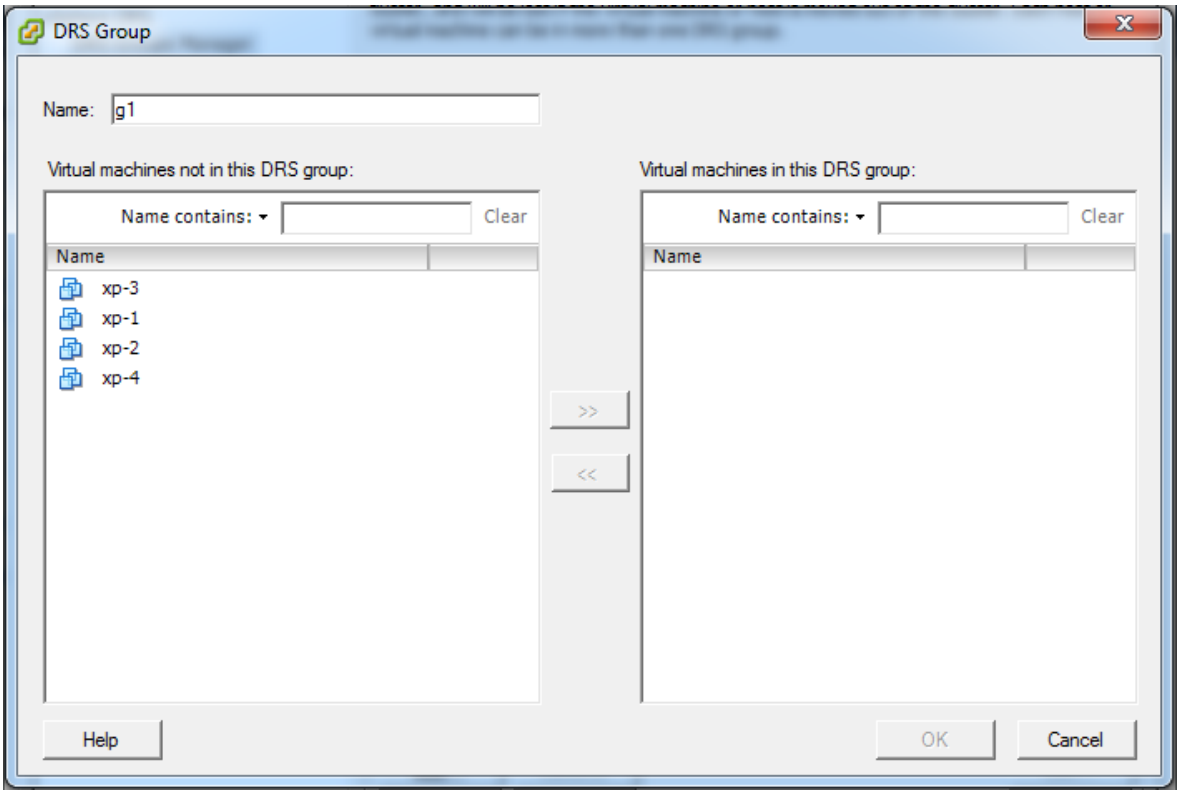
۲ برروی صفحه Add در قسمت Virtual machine DRS group کلیک کنید.

۳ در صفحه جدید باز شده در قسمت name نامی برای گروه انتخاب کنید. شکل ٦-٧

۴ برای افزودن ماشین‌های مجازی به گروه از سمت چپ صفحه بر روی ماشین‌های مجازی کلیک کنید.

۵ پس از انتخاب ماشین‌های مجازی برروی ok کلیک نمائید.

۶ برای ساخت گروه میزبآن‌های ESXi پس از کلیک بر روی Add در قسمت Hostprs group، مانند مراحل ایجاد گروه ماشین مجازی را انجام دهید.



شکل ٦-٧. گروه بندی ماشین‌های مجازی در DRS

٦-٥-٣ اعمال سیاستهای DRS در رابطه با اجرای ماشین‌های مجازی بر روی سرورهای ESXi

به کمک DRS می‌توان سیاست‌هایی بر روی ماشین‌های مجازی اعمال کرد تا هر یک فقط بتوانند بر روی سرورهایی خاصی اجرا شوند؛ و اعمال از این دست. بدین منظور می‌توانید رول‌هایی اضافه کنید. برای اضافه کردن رول از صفحه Setting مربوط به کلاستر، بر روی Add کلیک کنید.

سه نوع سیاست می‌توان بر روی ماشین‌ها و سرورها اعمال کرد.

Separate virtual machines

ماشین‌های مجازی عضو این رول هر یک بر روی سرورهای فیزیکی جداگانه اجرا خواهند شد. این حالت زمآن‌هایی استفاده می‌شوند که بخواهیم مثلا دو سرور که یک کار را انجام می‌دهند، بر روی دو میزبان فیزیکی اجرا شوند تا در صورتی که یکی از میزبآن‌های ESXi خراب و یا خاموش شد دیگری در دسترس باشد.

این حالت را Anti-Affinite Rules می‌نامند.

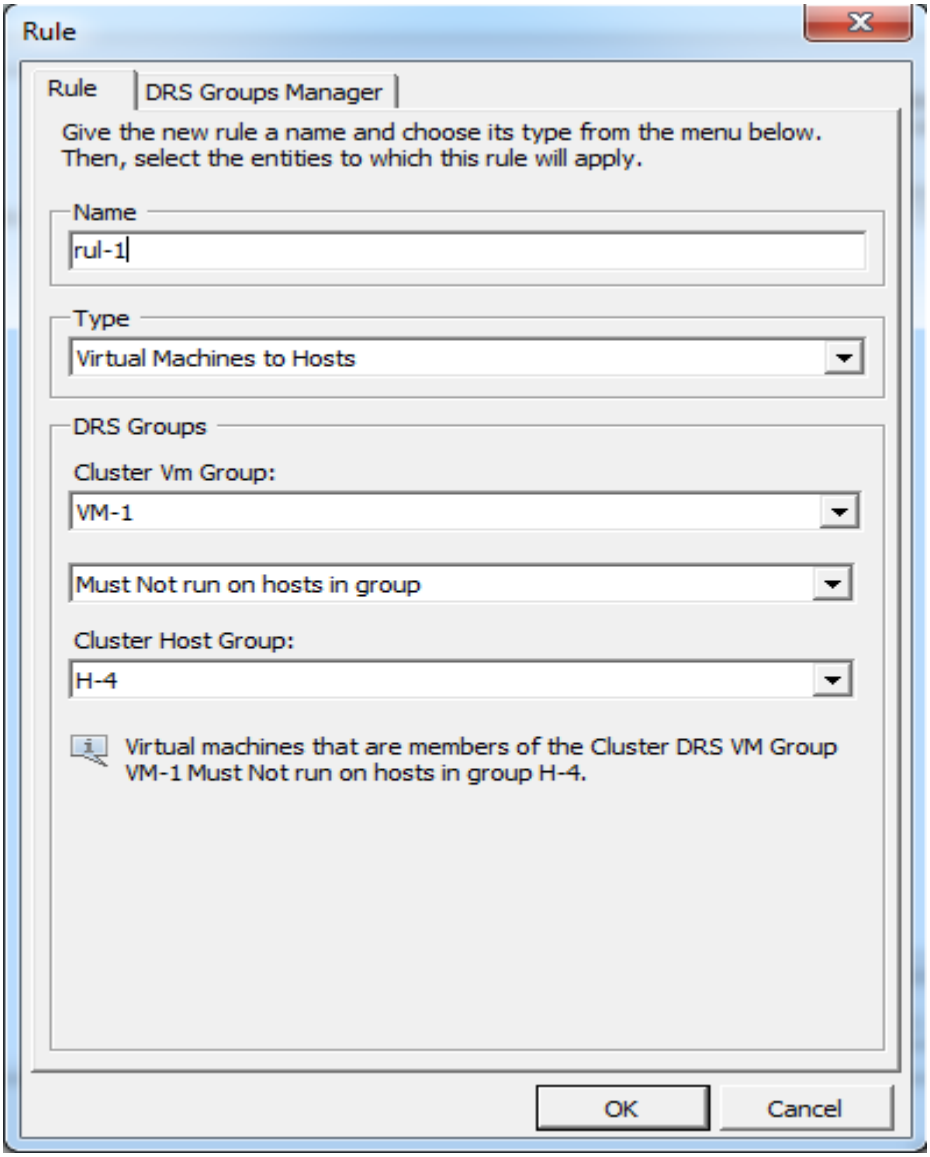
Keep virtual machin Togcther

ماشین‌های مجازی عضو این رول، همواره بر روی یک میزبان ESXi اجرا خواهند شد. این حالت نیز زمانی مفید خواهد بود که دو ماشین مجازی ارتباط بالایی داشته باشند مثلا یک سرور و سرور پایگاه داده مربوط به آن. در این حالت ترافیک سوئیچ‌های فیزیکی بسیار کم خواهد شد؛ چرا که دو یا چند ماشین مجازی پر ترافیک بر روی یک میزبان هستند.

Virtual machines to hostes

این سیاست شرایطی را ایجاد می‌کند تا ماشین‌های مجازی بر روی میزبآن‌ها خاصی اجرا شوند و یا بر روی بعضی از میزبآن‌ها اجرا نشوند. توجه داشته باشید که برای استفاده از این ویژگی می‌بایست از قبل ماشین‌های مجازی و میزبآن‌های مورد

نظر خود را در گروه‌هایی قرار داده باشید. در شکل ٦-٨ ماشین‌های مجازی عضو گروه VM-1 نمی‌توانند بر روی میزبآن‌های ESXi گروه H-4 اجرا شوند.



شکل ٦-٨ اعمال رول بر روی گروه‌های ماشین‌های مجازی و میزبآن‌ها

۳۹-٦-٦- مدیریت و تقسیم بندی منابع با Resource Pools

vSphere این امکان را فراهم کرده تا بتوان منابع پردازشی و حافظه‌ای یک کلاستر را به قسمت‌های مختلف تقسیم بندی کرده تا بتوان مدیریت بهتری بر روی منابع داشت. توجه داشته باشید برای ساخت یک Resource pool می‌بایست DRS را در کلاستری که قصد دارید Resource pools را در آن بسازید فعال نمائید.

ساخت Resource pools بر روی کلاستر مورد نظر راست کلیک کرده New Resource pool را انتخاب کنید.

تنظیمات مربوط به Resource pool شبیه به تنظیم و تخصیص منابع در ماشین‌های مجازی است که در قسمت 3-6 گفته شد.

۳۹-۶-۷- تکثیر ماشین‌های مجازی

فرایند ساخت ماشین مجازی و نصب سیستم‌عامل و برنامه‌های ضروری بر روی آن یک فرآیند زمانبر است که اگر در دیتاسنترهای بزرگ به این روش عمل شود،کار مدیریت غیر ممکن خواهد بود. یکی از امکاناتی که در vSphere برای حل این مسئله قرارداده شده، کپی کردن ماشین مجازی است. برای ساخت یک نمونه مشابه از یک ماشین مجازی فرایند زیر را انجام دهید:

۱.بر روی ماشین مجازی مورد نظر راست کلیک کرده Clone را انتخاب کنید.

۲. در کادر Name، نامی برای ماشین مجازی کپی شده انتخاب کنید. پس از انتخاب محل ماشین مجازی جدید در دیتاسنتر، بر روی Next کلیک نمائید

۳. در این قسمت نیز کلاستر و یا میزبان ESXi برای اجرای ماشین مجازی جدید انتخاب کرده ؛Next را کلیلک کنید.

٤. در مرحله قبل اگر کلاستر انتخاب کرده باشید در این قسمت می‌بایست میزبان ESXi مورد نظر برای اجرای ماشین مجازی جدید را انتخاب کنید؛ در غیر اینصورت این مرحله را مشاهده نخواهید کرد. برای ادامه Next را بزنید.

۵. دوباره اگر در مرحله‌ی ۳ کلاستر را برای اجرای ماشین مجازی جدید انتخاب کرده باشید و در آن کلاستر Resource pools ساخته شده باشد در این مرحله می‌توان Resource pool مورد نظر خود را انتخاب کنید. با کلیک بر روی Next به مرحله بعد بروید.

٦. در این قسمت می‌توان محل ذخیره‌سازی فایل‌های ماشین مجازی را از بین ذخیره‌سازهای موجود، انتخاب کنید. ضمناً می‌توانید از منوی کرکره‌ای بالای صفحه نحوه ذخیره سازی را نیز تغییر دهید.

۷. پس از دوبار کلیک بر روی Next و بعد از مشاهده خلاصه‌ای از مشخصات ماشین مجازی جدید با زدن Finish، فرایند کپی ماشین مجازی اجرا خواهد شد.

فصل ۴۰ نرم‌افزار ISA Server

۴۰-۱- مقدمه

نرم‌افزار ISA یا Internet Security and Acceleration توسط شرکت Microsoft برای Windows عرضه گردیده است. این نرم‌افزار که در حقیقت نسخه جدیدی از MSProxy است دارای قابلیت‌ها و توانایی‌های جالبی است. در این فصل به آموزش نسخه ۲۰۰۴ این نرم‌افزار خواهیم پرداخت.

نرم‌افزار ISA دارای دو قابلیت اصلی است.

۱- Cache

۲- Firewall

با استفاده از قابلیت Caching می‌توان Requestهای HTTP و FTP کاربران شبکه را Cache کرد تا در هنگام درخواستهای تکراری با صرفه جویی در زمان و پهنای باند بتوان به آن درخواستها از طریق اطلاعات Cache Server پاسخ گفت.

۴۰-۱-۱- *Cache*

بخش Caching خود، دارای قابلیتهای زیر است:

۱) Automatic & Scheduled Caching: در این قابلیت ISA بطور هوشمندانه در ساعات مشخصی (ساعاتی که ترافیک شبکه کم است) به سراغ سایتهایی که قبلا Cache شده‌اند اما زمان TTL آن‌ها تمام شده است و Expire شده‌اند رفته و بطور اتوماتیک آن‌ها را Update می‌کند. ISA این عمل را با اولویت سایتهای محبوب (سایت هایی که بیش از سایر سایت‌ها توسط کاربران درخواست شده اند) انجام می‌دهد. نتیجه این کار این است که سایتهای محبوب کاربران همواره بصورت Update شده در ISA برای تحویل به کاربران فراهم است. ضمن اینکه ما بصورت دستی نیز می‌توانیم ساعاتی را برای Update کردن سایتهای دلخواهمان تعیین کنیم.

۲) Reverse Caching: با استفاده از این قابلیت ISA می‌تواند اطلاعاتی را که بر روی Web Server داخلی شبکه قرار دارند را پس از آنکه یکبار در اختیار کاربران موجود در اینترنت قرار داد بر روی خود Cache نموده و در صورت تقاضای

مجدد بدون مراجعه به Web Server اطلاعات Cache شده را در اختیار کاربران Internet قرار دهد. این خاصیت موجب کاسته شده ترافیک بر روی Web Server می‌شود.

۳) Transparent Cache: یکی از قابلیتهای ISA این است که هم بصورت Proxy Base و هم بصورت Transparent قابلیت Cache کردن را دارد. در جلسات بعد در این مورد بیشتر صحبت خواهیم کرد.

۴) Distributed and Hierarchical Caching: می‌توان بجای یک ISA Cache از چند ISA Cache در شبکه استفاده کرد. سپس همه آن‌ها را بصورت یک Array درآورد. در این حالت تمام ISAها دست به دست هم داده و یک Cache یکپارچه را تشکیل می‌دهند. درصورتیکه Objectهای Cache شده از لحاظ فیزیکی بر روی این ISA Serverها توزیع شده است و هر کدام قسمتی از اطلاعات را Cache نموده‌اند. ضمنا" ما می‌توانیم از یک Root System نیز استفاده کنیم بگونه‌ای که یک یا چند ISA Server به اینترنت مستقیما" وصل بوده و Objectهای مورد نیاز خود را از طریق ISA Serverهای بالاتر تأمین نماید. در این حالت با استفاده از پروتکل CARP یا Cache Array Routing Protocol اطلاعات مورد نیاز Clientها از روی یک Array جمع آوری شده و در اختیار آن‌ها قرار می‌گیرد.

۴۰-۱-۲- Firewall

امروزه Firewallها در دو نوع سخت‌افزاری و نرم‌افزاری وجود دارند. مزیت عمده Firewallهای سخت‌افزاری در سرعت آن‌هاست. از نمونه‌های سخت‌افزاری می‌توان به Cisco PIX Firewall اشاره کرد که MicroSoft ادعا می‌کند تمامی قابلیتهای یک Firewall سخت‌افزاری در ISA گنجانده شده است و بدلیل قیمت بسیار کمتر برای استفاده اقتصادی‌تر است.

بطور کلی می‌توان گفت قابلیتهای نرم‌افزار ISA در زمینه Firewall عبارتند از:

۱- کنترل استفاده از اینترنت: در ISA می‌توان با استفاده از Policyها ترافیک ورودی و خروجی را بر مبنای سایتها ، Protocolها و محتویات Packetها Filter کرد.

۲- می‌توان Packetها را بر اساس لایه‌ها (از لایه Network تا Application) فیلتر نموده و حتی ترافیک‌های مربوط به DNS را کنترل کرد.

۳- ISA با استفاده از قابلیت Intrusion Detection می‌تواند جلوی نفوذ هکرها را بگیرد. بر روی ISA روشهای معروف Hack تعریف شده است و در صورتیکه فردی اقدام به استفاده از این روشها نماید ISA جلوی او را خواهد گرفت. به عنوان مثال ISA می‌تواند Scan شدن Portها را تشخیص داده و جلوی آنرا بگیرد.

۴۰-۱-۳- دیگر قابلیت‌ها

البته نرم‌افزار ISA دارای قابلیتهای دیگری نیز است که می‌توان آن‌ها را بصورت زیر خلاصه کرد:

۱- قابلیت اعمال Policyهای مختلف.

۲- امکان کنترل (Bandwidth Qos).

۳- امکان پشتیبانی از VPN.

۴- امکان Publish کردن WebServerهای داخلی شبکه. (پس از Publish کردن WebServerهای داخلی هرگاه یک کاربر از طریق Intenet بخواهد به WebServer ما دسترسی پیدا کند اطلاعات مورد نیاز او از طریق ISA در اختیارش قرار می‌گیرد. در نتیجه هیچکس از طریق Internet نمی‌تواند مستقیما" به WebServerهای ما دسترسی داشته باشد.)

۵- H.323 GateKeeper: ویژه برنامه هایی است که از IP تلفنی استفاده می‌نمایند. (مثل NetMeeting)

۶- Monitoring & Alerts.

نکته: ذکر این نکته لازم است که هر سیستم عاملی که HTTP (ver 1.1) را پشتیبانی کند می‌تواند به عنوان یک WebProxyClient عمل نماید. اگر بخواهیم از ISA به عنوان یک Firewall استفاده نماییم باید Clientها دارای Win95 به بعد باشند. Clientها می‌توانند به عنوان SecureNAT Client عمل کرده و از خیلی از قابلیتهای ISA بهره مند شوند.

۴۰-۱-۴- حالات نصب

ISA Server می‌تواند در دو حالت زیر نصب شود:

۱- Stand-Alone: در این حالت ISA Serverها مستقل از یکدیگر عمل کرده و به یکدیگر متصل نمی‌شوند.

مزایای این روش عبارت است از:

- هزینه کمترو تنظیمات کمتری نیاز دارد.
- تمام قابلیتهای Caching و Firewall را داراست.
- از هرنوع Connection حتی Dialup می‌تواند استفاده کند.

معایب این روش هم عبارت است از:

- دارای Enterprise Policy نیست. بنابراین اگر از چند Stand-alone استفاده کنیم باید هرکدام را جداگانه کنترل کنیم.
- Single Point of Failure: در حالت Stand alone همه چیز وابسته به ISA است و اگر ISA دچار مشکل گردد Internet قطع خواهد شد.

۲- Enterprise Array: پیاده سازی این روش فقط بر روی Active Directory امکان پذیر است. در این روش یک Array مرکب از چندین ISA Server تشکیل می‌شود که همگی بصورت منطقی از یک نقطه کنترل می‌گردند. ضمنا" هر کدام از اعضای Array قسمتی از اطلاعات را Cache می‌کنند. در صورت نیاز می‌توان Array را گسترش داد. نکته قابل توجه این است که یک Array فقط تحت یک Domain واحد قابل پیاده سازی است. یعنی اعضای یک Array باید همگی عضو یک Domain باشند.

مزایای این روش:

- امکان اعمال Enterprise Policy.
- امکان مدیریت متمرکز
- No Single Point of Failure: در این حالت اگر یک یا چند ISA Server دچار اختلال شود اختلالی در شبکه بوجود نمی‌آید.

معایب این روش:

- نیازمند ایجاد تغییراتی در توپولوژی شبکه است.
- از نظر هزینه نسبت به روش قبلی گرانتر است.
- در ابتدای کار نیاز به مطالعه ، تحقیق ، برنامه ریزی و صرف وقت بیشتری برای پیاده سازی دارد.

۴۰-۲- ISA Server

۴۰-۲-۱- *Internet Security & Acceleration Server*

این نرم‌افزار تمام بسته‌های رد وبدل شده از یک شبکه داخلی به یک شبکه خارجی وبه عکس را مورد بررسی قرار می‌دهد. این نرم‌افزار جهت ایجاد امنیت در شبکه مورد استفاده می‌شود ومانند یک فایروال عمل نماید.

کاربردهای این نرم‌افزار را به موارد زیر می‌توان دسته بندی نمود.

- ✓ استفاده از این نرم‌افزار به عنوان یک فایروال
- ✓ ایجاد ارتباطات امن Secure connection
- ✓ Virtual primary network که جهت امن کردن یک ارتباط مورد استفاده قرار می‌گیرد
- ✓ ارائه سرویس cashing در یک شبکه

عملیات فایروال

عملیات فایروال توسط ISA Server به سه روش صورت می‌گیرد

- Packet filitering
- Application layer filitering
- State Full filitering

عملیات ارتباطات امن به دو صورت انجام می‌گیرد

- VPN (Virtual Ptivate Network) جهت ایجاد ارتباط امن به خارج از شبکه
- WPR (Web Publishing Rule) برای ارتباط امن جهت دسترسی کاربران خارج از شبکه به منابع شبکه داخلی

۴۰-۳- نصب نرم‌افزار ISA Server

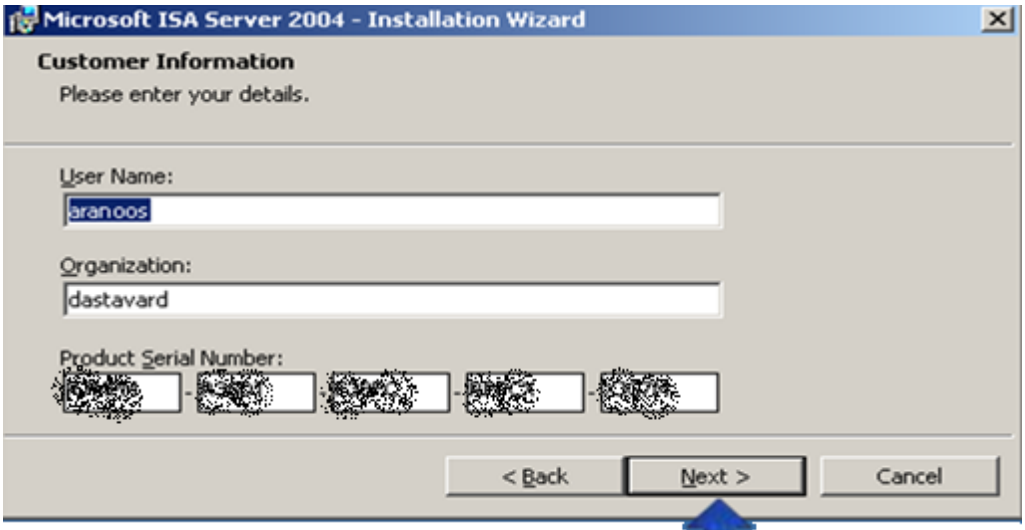
سخت‌افزار مورد نیاز عبارت است از یک کامپیوتر معمولی P4 که دوکارت شبکه بر روی آن نصب گردیده باشد.

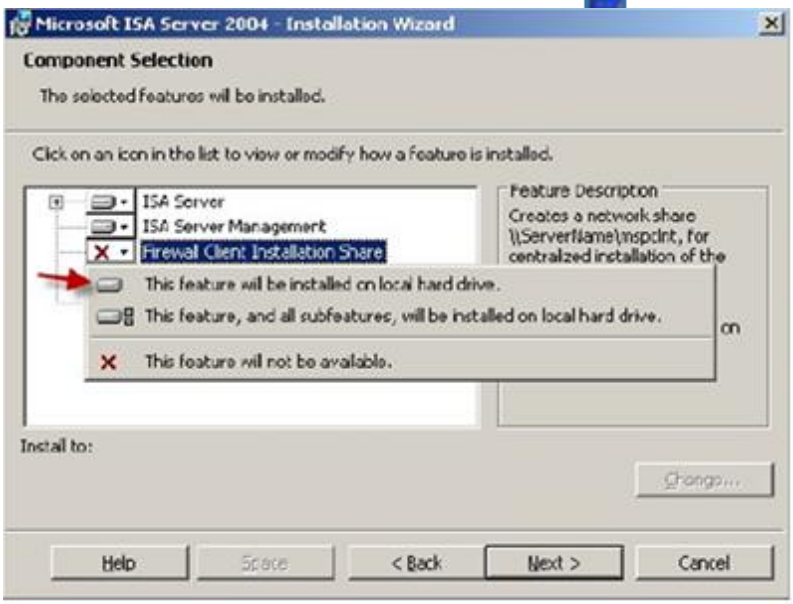
توجه: اگر ISA Server را به عنوان فایروال یا VPN Server مورد استفاده قرار دهیم حداقل به نصب دو کارت شبکه نیاز داریم؛ اما اگر ISA Server به عنوان Cash Server یا Proxy Server مورد استفاده قرار گیرد، نصب یک کارت شبکه نیز کافی می‌باشد.

توجه: قبل نصب ISA Server تمامی سرویس‌های لازم مثل DHCP Server، DNS Server و Active Domain Control باید نصب کرده باشید. بهتر است ISA Server را به صورت Stand Alone بر روی یک سیستم نصب کنید

۴۰-۳-۱- مراحل نصب ISA Server

پس از اجرای گزینه Setup صفحه نصب ظاهر می‌گردد. مراحل نصب را دنبال نمایید.



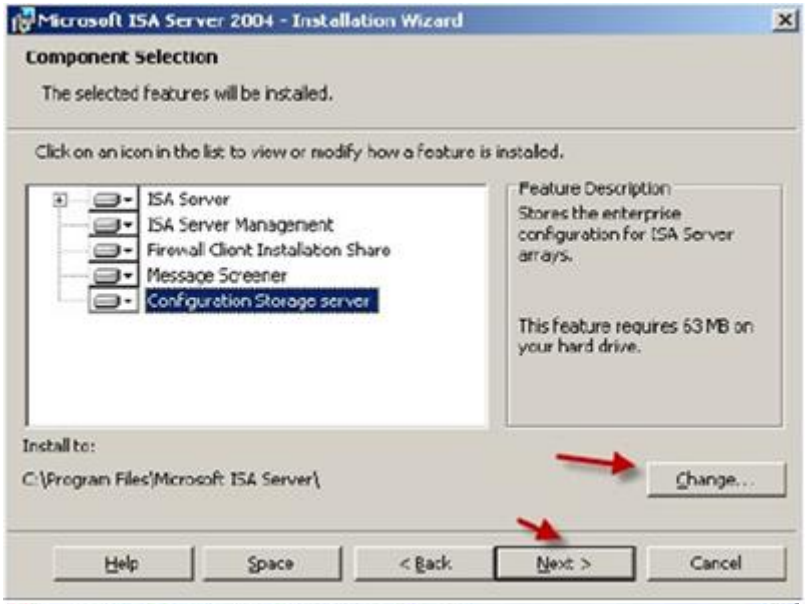


گزینه ISA Server یا در برخی نسخه‌ها Firewall ISA Server جهت کنترل ترافیک بین شبکه‌ها می‌باشد.

ISA Server Management جهت دسترسی به کنسول مدیریتی ایزا سرور می‌باشد.

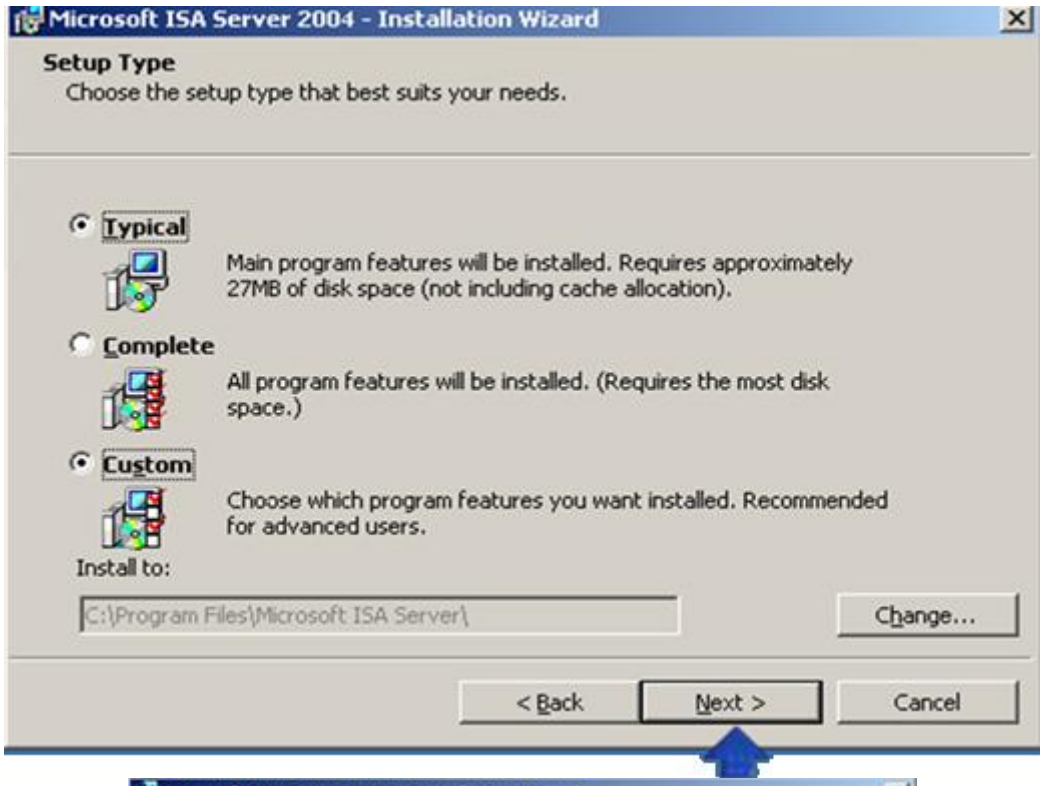
Firewall Client Installation Share یک فولدر Share شده به نام Msp Client بر روی سرور ایجاد کرده وکاربران می‌توانند از طریق ان نرم‌افزار Firewall Client را نصب کنند.

Message Screener جهت فیلتر کردن بسته‌های SMTP بکار می‌رود قبل از نصب این گزینه باید سرویس SMTP را نصب کرده باشید.



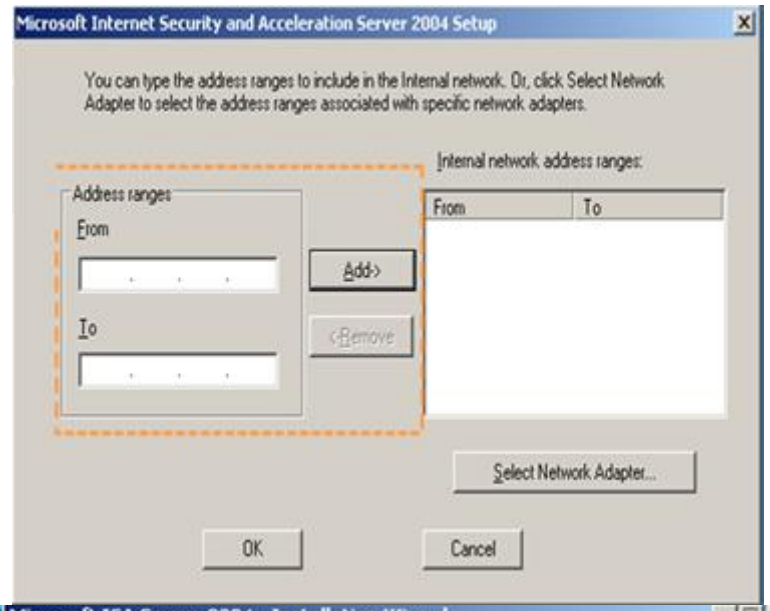


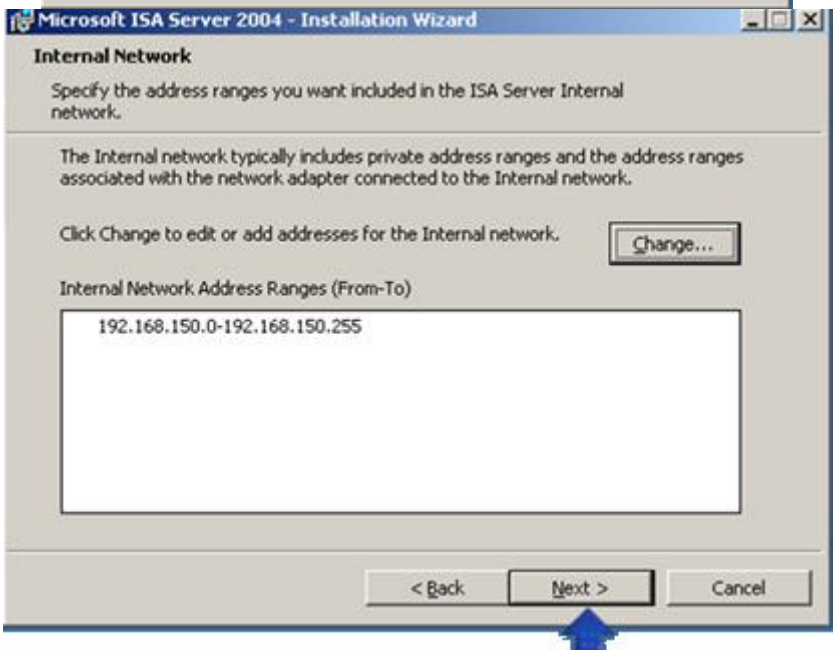
درصورتی که قبلا ISA Server را نصب کرده اید و بخواهید تنظیمات قبلی ISA Server را در این نصب اعمال کنید گزینه Change را کلیک نمایید و در در صفحه باز شده گزینه Create A Replicat of The Enterprice Configuriation را انتخاب کنید.





در این قسمت محدوه رنج آدرس شبکه داخلی را وارد می‌نماییم. این عمل جهت تشخیص شبکه داخلی از شبکه خارجی توسط ایزا سرور می‌باشد. همچنین می‌توان از گزینه Select Network Adapter نیز برای تایین آدرس شبکه داخلی استفاده نمود.





در این صفحه در صورت انتخاب گزینه روبرو اجازه اتصال به جدیدترین نسخه‌های Firewall داده می‌شود



در این قسمت بر روی گزینه Install کلیک کرده. عملیات نصب بطور کامل انجام شود.



۴۰-۴- تنظیمات ISA Server

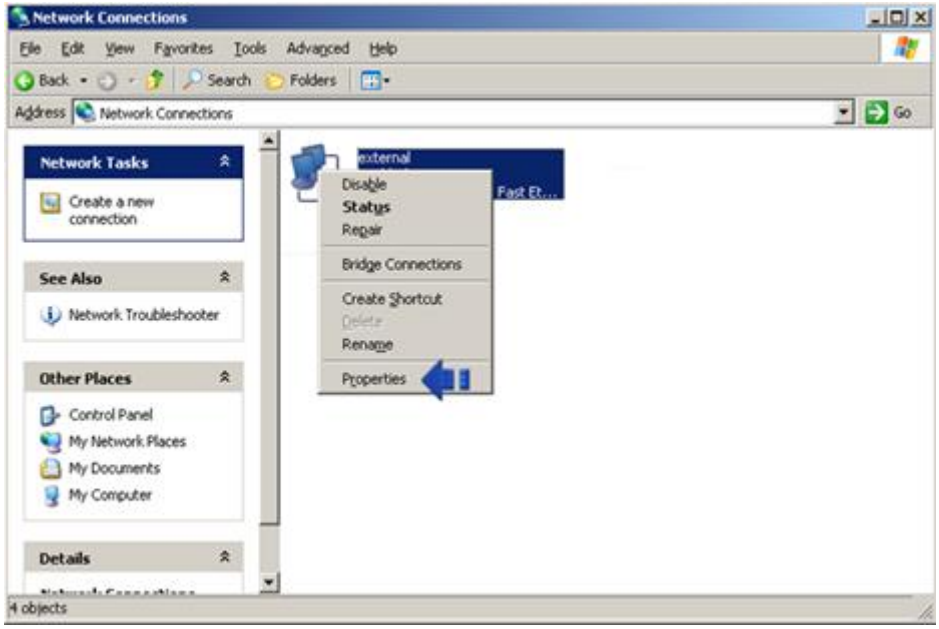
جهت ایجاد امکان برقراری ارتباط برخی برنامه‌ها با شبکه، بدین جهت باید برخی از ترافیک‌های مورد نیاز را مجوز دسترسی (Alow) داد. بعد از نصب ایزا سرو به طور پیش فرض تمام ارتباطات رسیده به ایزا سرور مسدود می‌شوند.

در مرحله بعد کلیه ترافیک‌های ناخواسته یا برنامه‌های ناخواسته را با استفاده Paket Filitering یا Aplication Filitering باید محدود نمود وفقط به برخی از برنامه‌های اجازه دسترسی داد. همچنین با تنظیم کردن Intojan Detection نرم‌افزار فایروال را تنظیم کرد

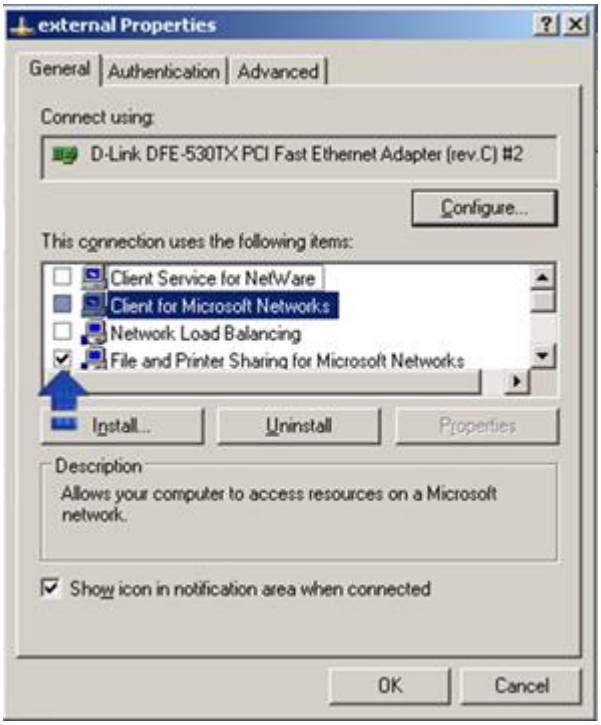
با استفاده از Firewall Policy Rule می‌توان تمامی ارتباطات داخل به خارج یا بعکس خارج به داخل را مدیریت نمود. از تنظیمات دیگر دادن مجوز دسترسی از طریق Administration Digniration Wizard می‌باشد.

۴۰-۴-۱- تنظیمات امنیت شبکه خارجی در نقل وانتقال داده

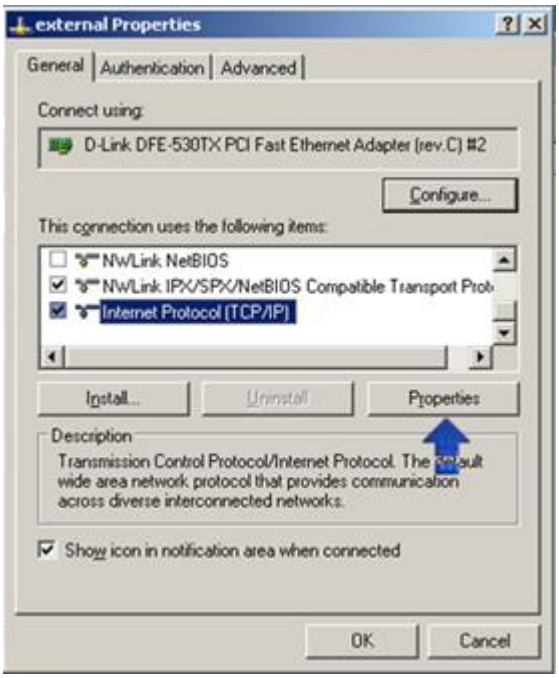
ابتدا در پانل کنترل (Control Panel) رفته و بر روی گزینه (Network Connection) کلیک کرده تا صفحه مورد نظر بازشود. بر روی ایکن شبکه راست کلید کرده وگزینه Properties را کلیک نمایید.



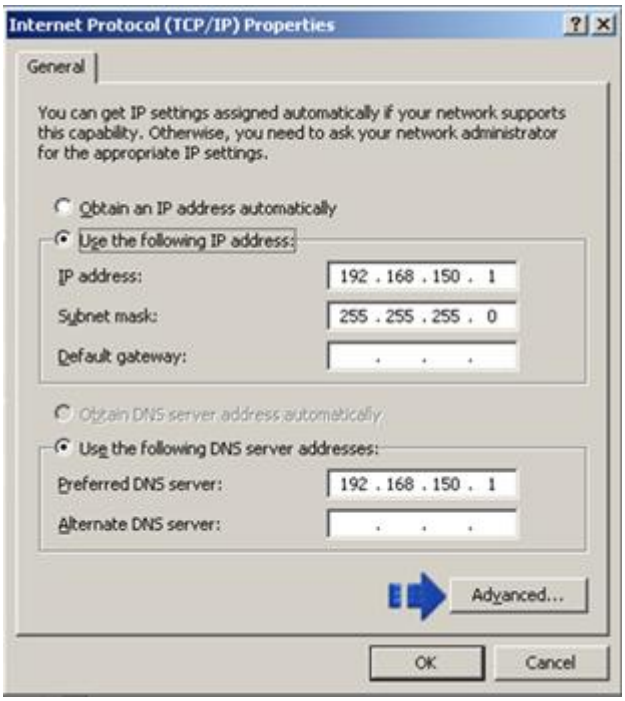
تیک گزینه‌های Client For Microsoft Network و File And Printer Sharing For Microsoft Network را بر میداریم.



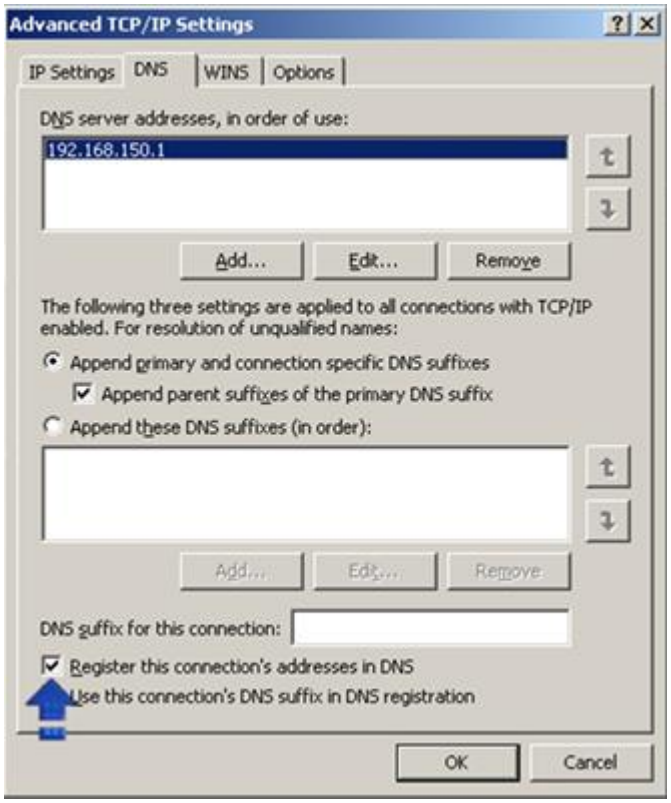
سپس بر روی گزینه TCP/IP (Internet Protocol) کلیک کرده وگزینه Properties را انتخاب می کنیم.



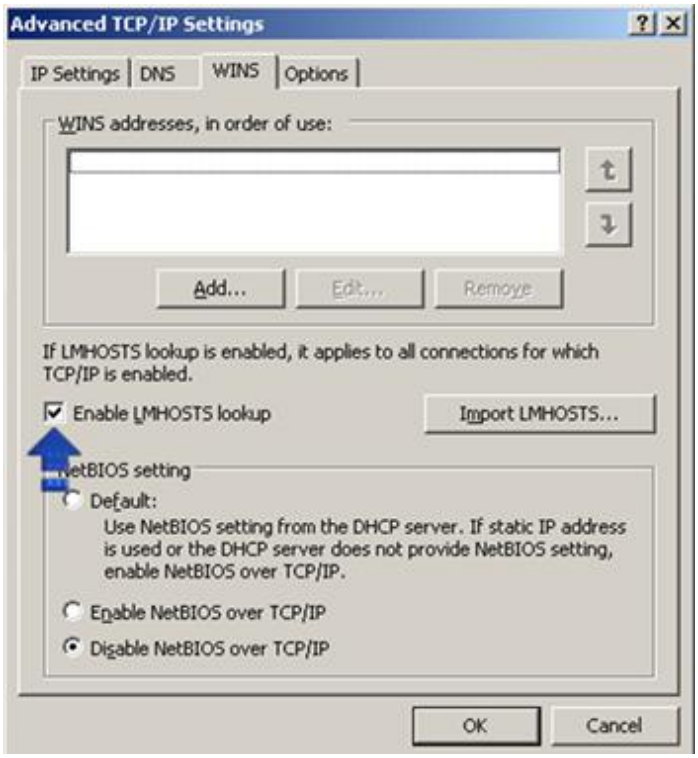
در صفحه باز شده گزینه Advanced را انتخاب می‌کنیم



در صفحه باز شده سربرگ DNS را انتخاب می‌کنیم. سپس تیک گزینه Register This Connection Addresses DNS برمیداریم.



در سربرگ Wins نیز تیک گزینه Enable LMHOST Lookup را برمیداریم. وسپس بر روی گزینه OK کلیک می کنیم



۴۰-۴-۲- تنظیمات ISA Server به عنوان یک Firewall

این تنظیمات به صورت سه روش صورت میگیرد:

- ✓ Intrusion Detection (تشخیص حمله)

- ✓ Packet Filitering
- ✓ State Full Filitering

بدین صورت که:

- ✓ Introjan Detection: تمام بسته‌های غیر استاندارد که بصورت نفوذگر هستند را تشخیص میدهد و با بررسی Inrojan Detection می‌توان امنیت شبکه را بالا برد.
- ✓ Packet Filitering: براساس شماره IP وشماره پورت بسته‌های دریافتی عمل می‌کند. و عمل فلیترینگ را در لایه IP انجام می‌دهد.
- ✓ State Full Filitering روشی قویتر نسبت به: Packet Filitering است بطوری که هدرهای بسته‌ها را نیز مورد بررسی قرار می‌دهد ودر صورت داشتن هدر نا استاندار ان بسته را به عنوان هدر حمله تشخیص می‌دهد.

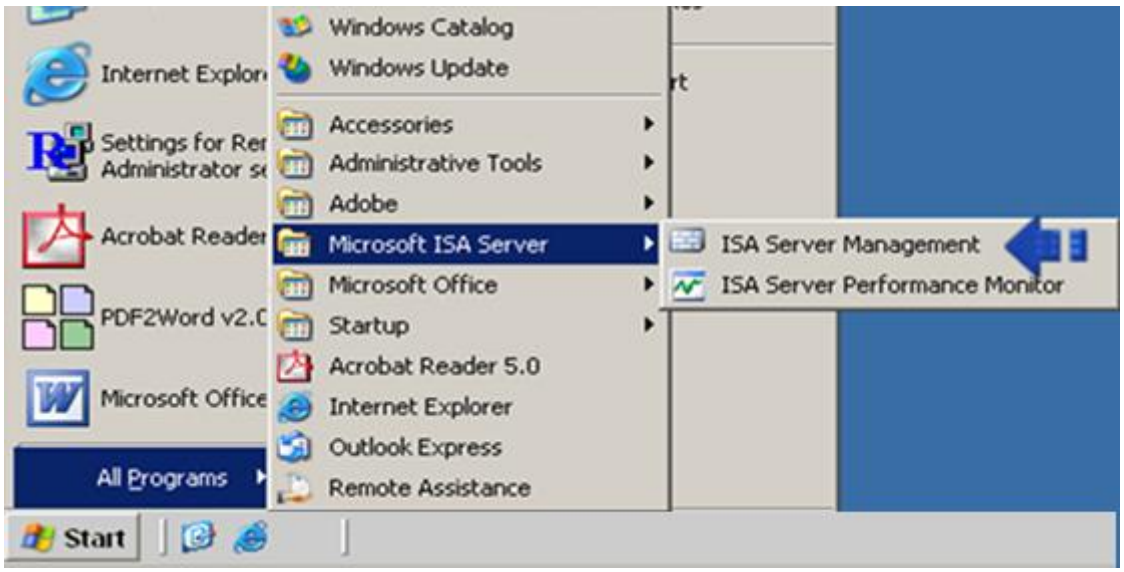
ISA Server می‌تواند به صورت Application Filitering عمل نماید و جلو حمله ویروس‌ها و کرم‌ها را که داری هدر غیر استاندارد هستند را بگیرد. ISA Server قابلیت Multi Networking را دارد ومی تواند ارتباطات بین چندین شبکه را مورد بررسی قرار دهد همچنین ISA Server می‌تواند شبکه را به صورت Local Host، Internal Network، External Network، VPN Remote Access و Current Time Clien در نظر بگیرد.

تنظیمات فایروال توسط ISA Server را می‌توان به صورت یک شبکه Perimeter در نظر گرفت که شبیه یک شبکه DMZ می‌باشد. شبکه‌های DMZ می‌تواند جدا از شبکه‌های خارجی (اینترنت) وشبکه‌های داخلی در نظر گرفته شود. این محل جایی است که سرورهای شبکه در]ن محل قرار گرفته‌اند و سیاستهای امنیتی خاصی در مورد آن‌ها باید در نظر گرفت.

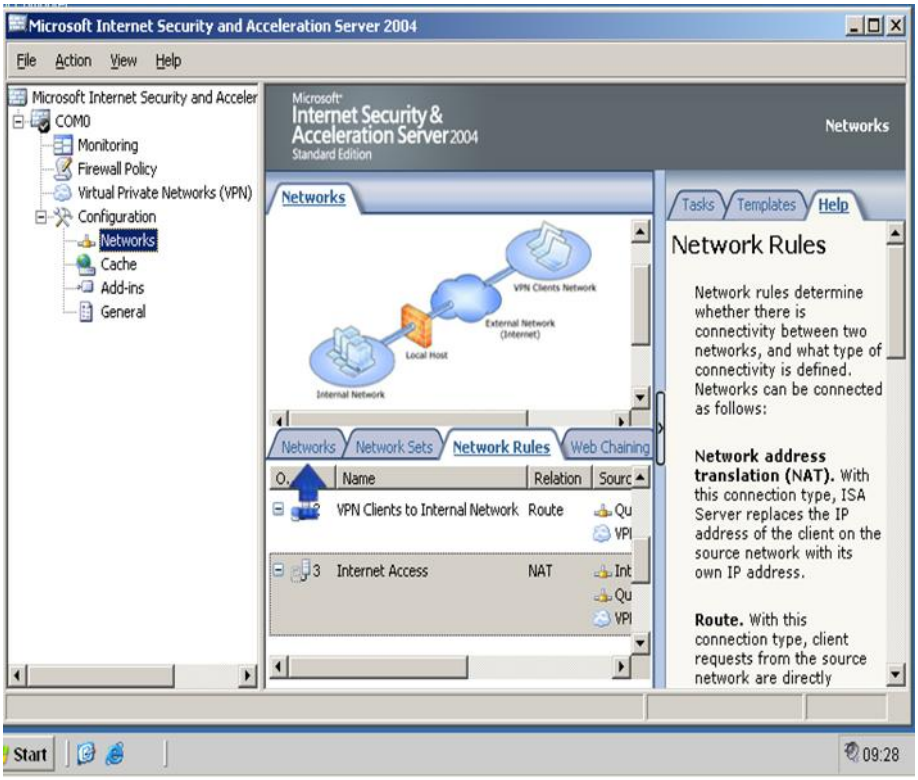
خمچنین ISA Server دارای Templateهای امنیتی از پیش طراحی شده می‌باشند که هر کدام دارای Access Listها وموارد مربوط به خود می‌باشد.

۴۰-۴-۳- نحوه تنظیم یک شبکه جدید بر روی ISA Server

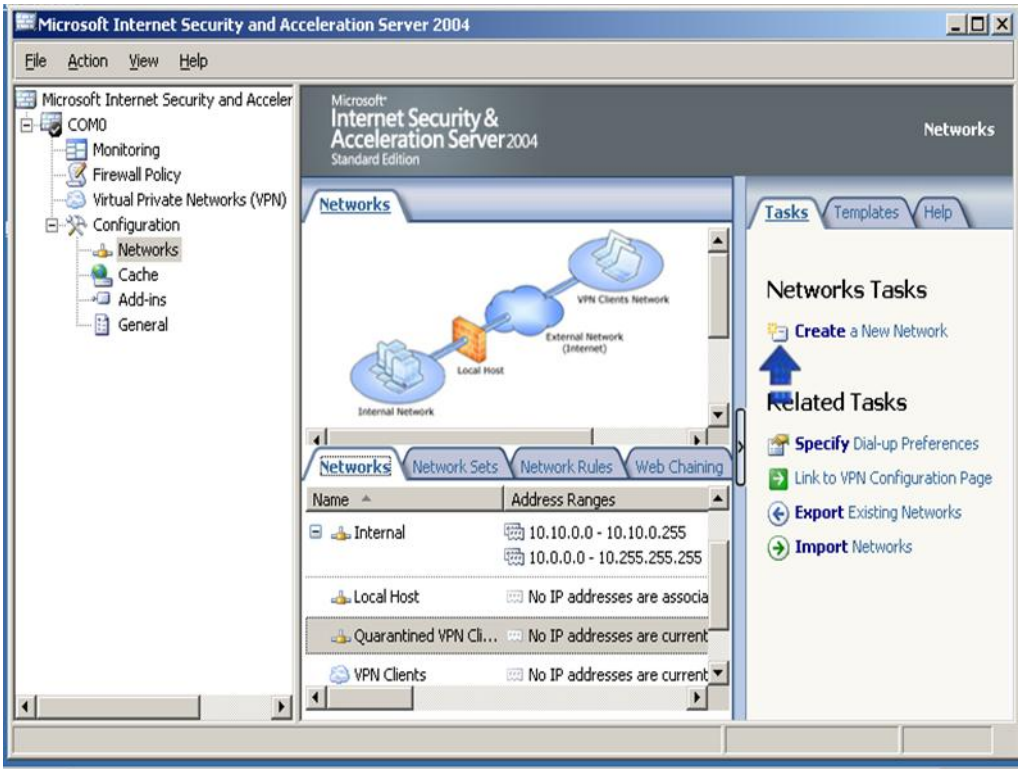
از منوی Start گزینه All Programs را انتخاب کنید. از منوی Microsoft ISA Server گزینه ISA Server Management را انتخاب کنید تا صفحه زیر باز شود.



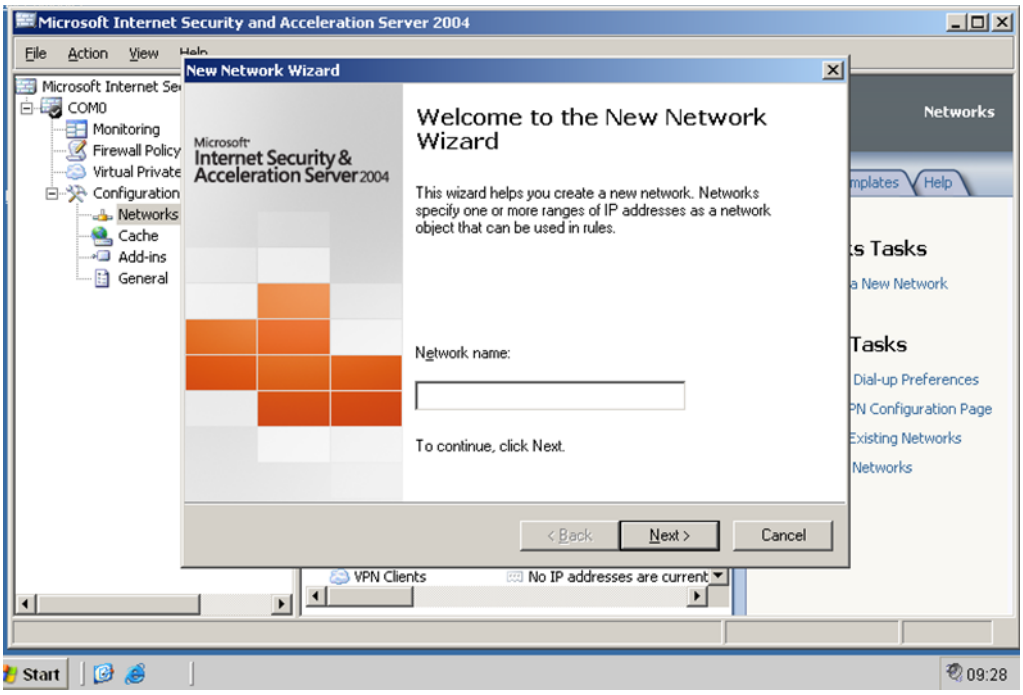
بر روی گزینه Configuration+ کلیک کنید. گزینه Network را انتخاب نموده و سپس در وسط صفحه گزینه Network را انتخاب نماید.



سپس بر روی Tasks در سمت راست پنجره کلیک کنید و گزینه Create a New Network را انتخاب نمایید.



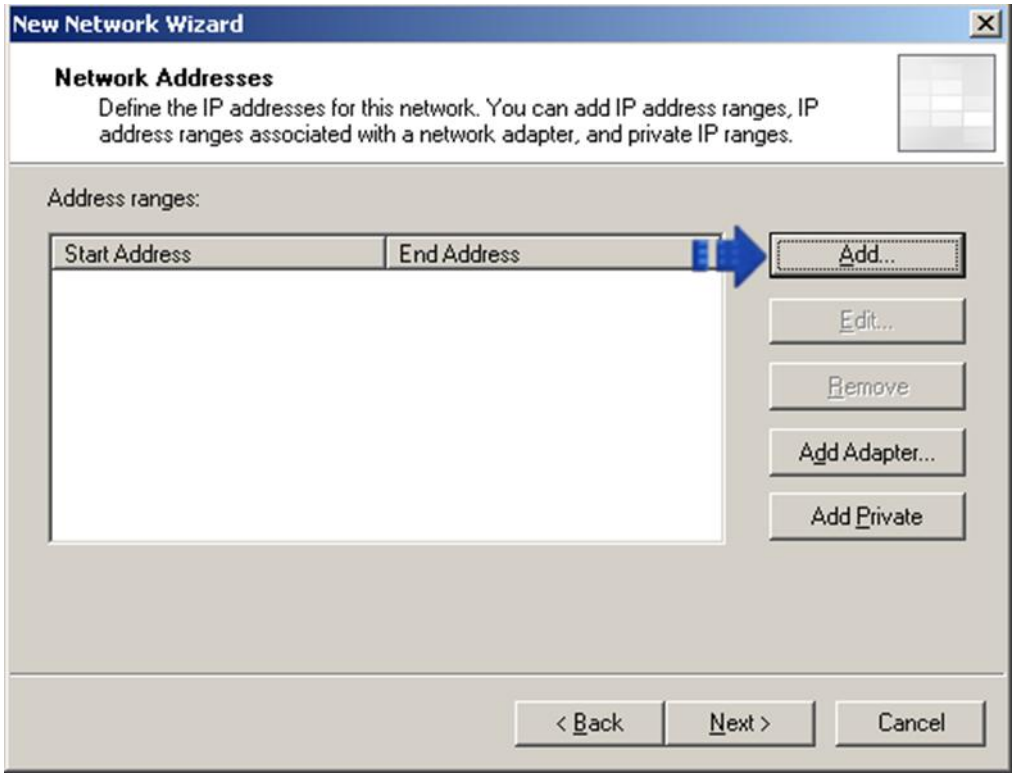
یک نام را وارد نمایید و رویگزینه Next در پنجره باز شده کلیک نمایید.

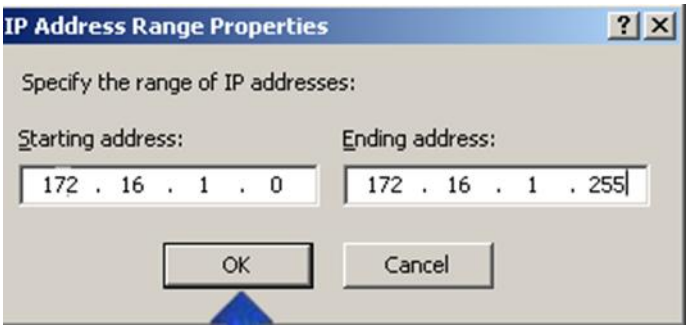


گزینه Perimeter Network را انتخاب کنید و بر روی گزینه Next کلیک نمایید.



سپس بر روی گزینه Add کلیک نمایید. محدوده IP را وارد نموده و بر روی گزینه OK کلیک کنید.



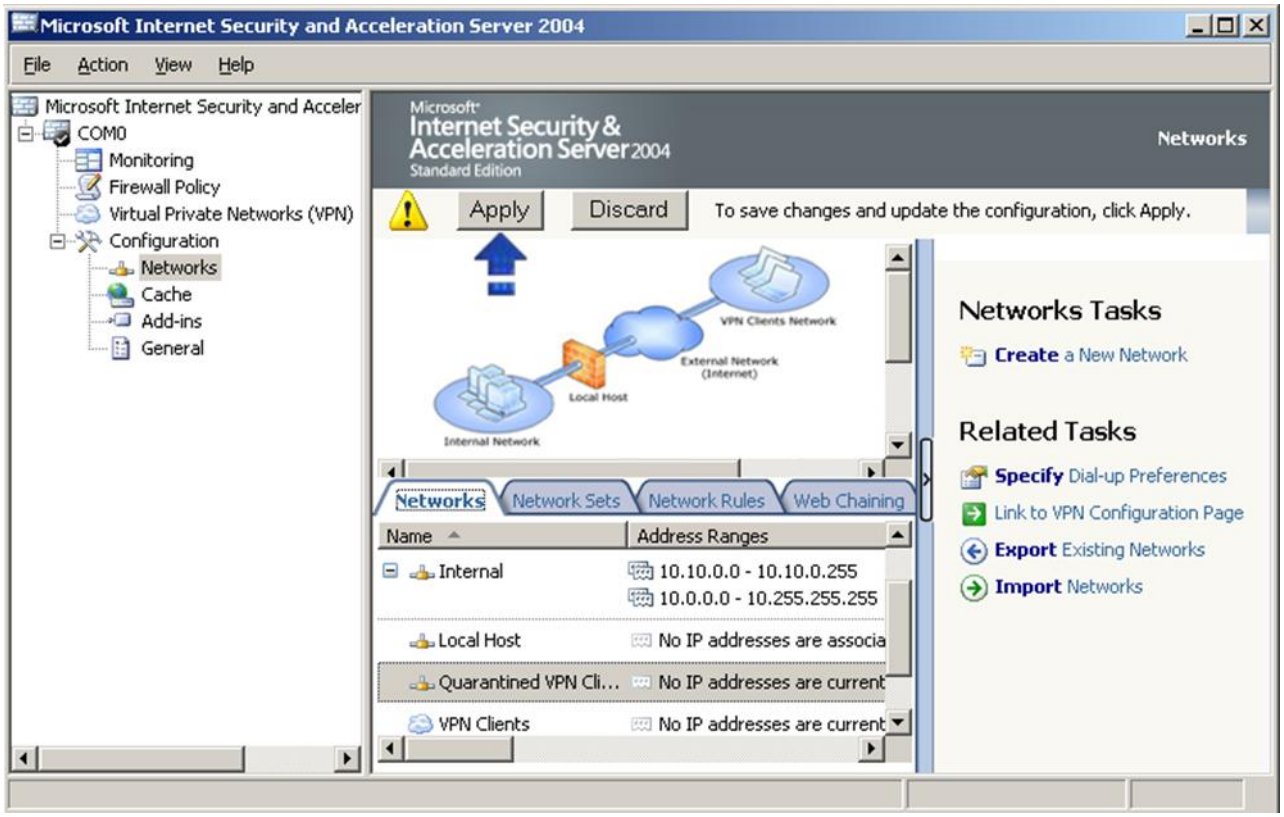


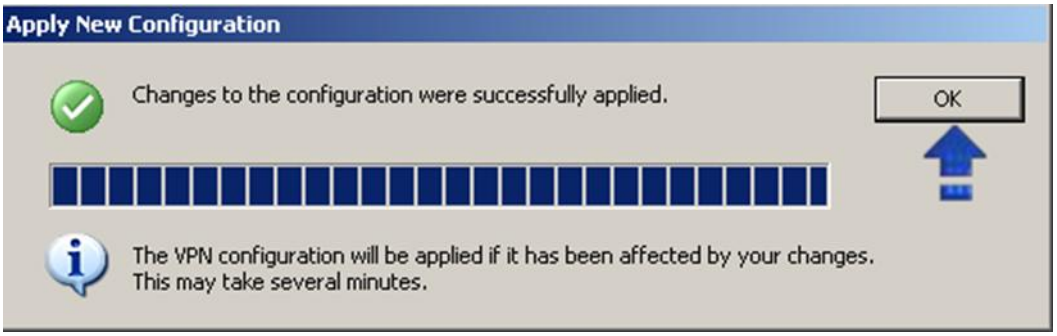
پس انتخاب گزینه Next پنجره مقابل ظاهر می‌گردد. بر روی گزینه Finish کلیک کنید



جهت اعمال تغییرات روی گزینه Apply کلیک نمایید تا تغییرات اعمال شود سپس بر روی دکمه OK کلیک کنید.

بدین صورت یک شبکه جدید بر روی ISA Server تعریف می‌گردد.



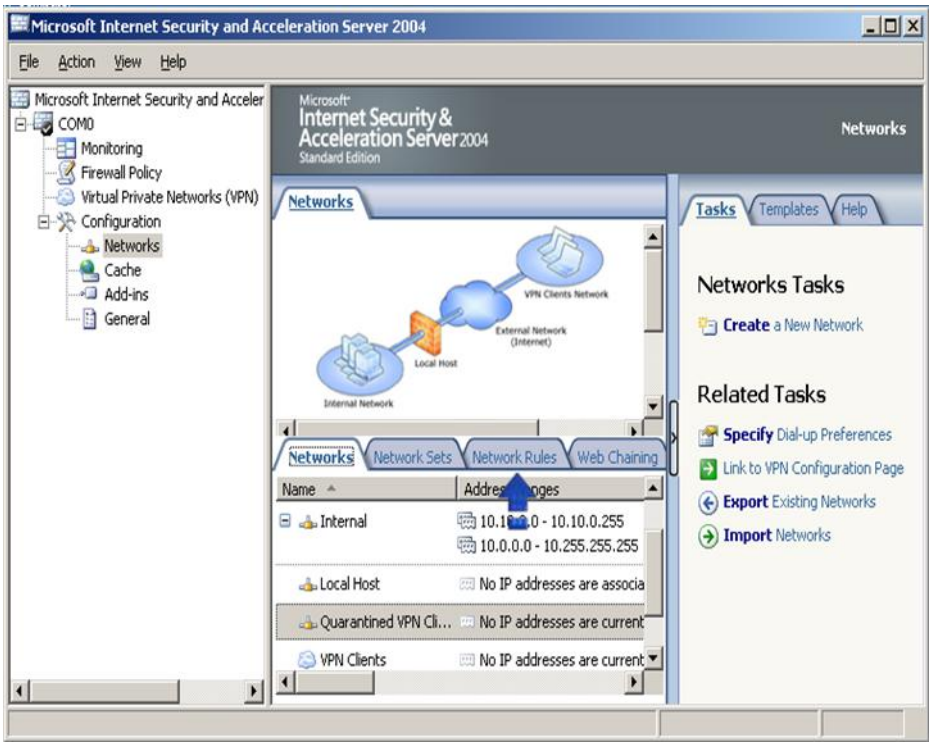


۴۰-۴-۴- تنظیمات Network Rule on ISA Server (جهت ارتباط یک شبکه Local وخارجی)

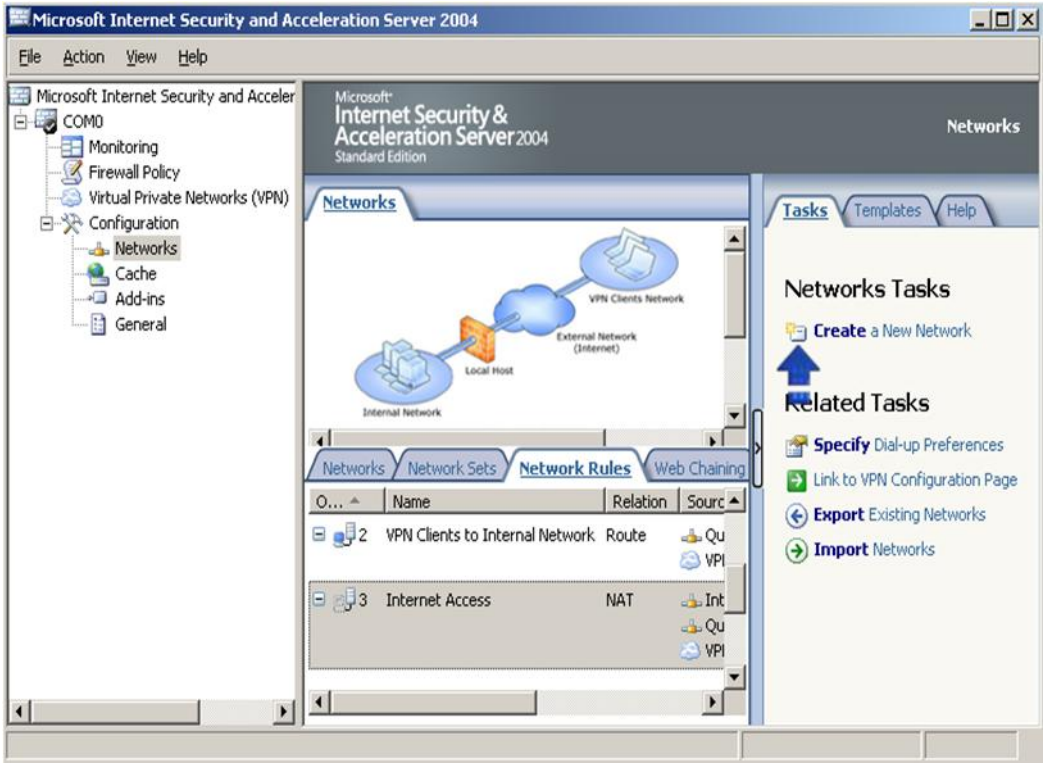
از منوی Start گزینه All Programs را انتخاب کنید. از منوی Microsoft ISA Server گزینه ISA Server Management را انتخاب کنید تا صفحه زیر باز شود.



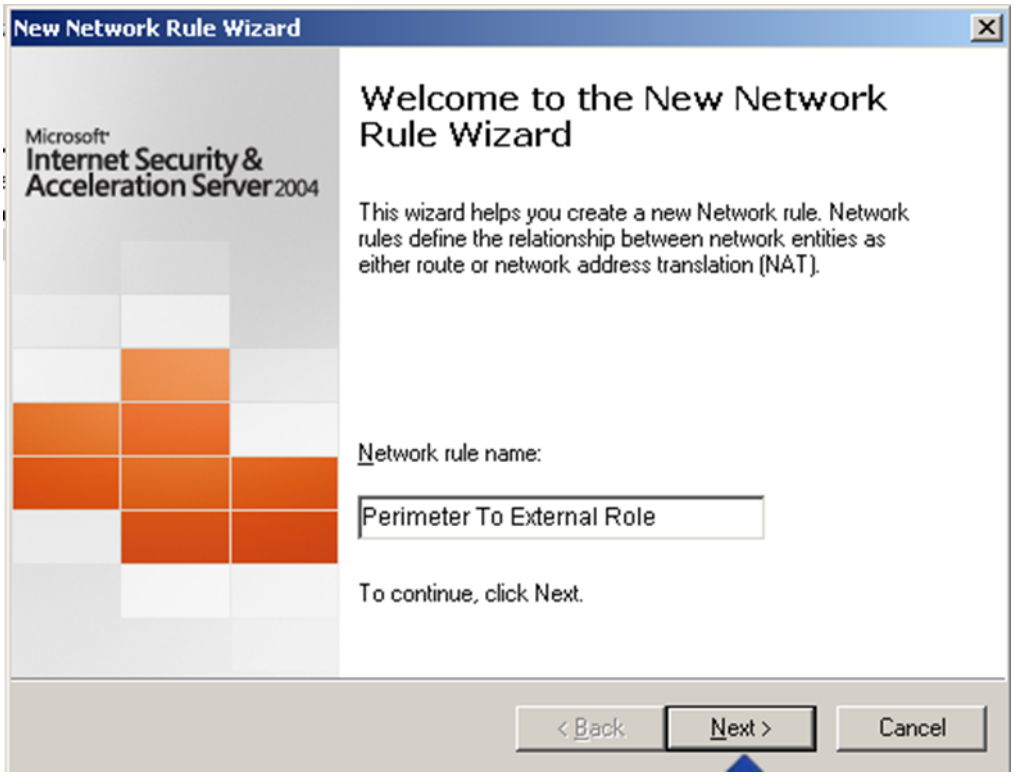
بر روی گزینه Configuration+ کلیک کنید. گزینه Network را انتخاب نموده و سپس در وسط صفحه گزینه Network Rules را انتخاب نماید.



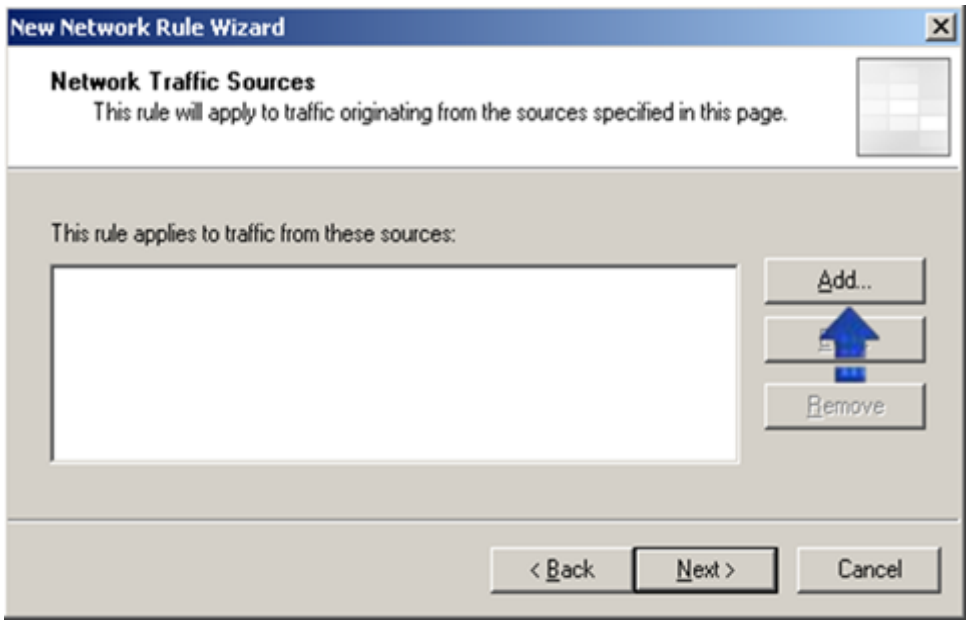
سپس بر روی Tasks در سمت راست پنجره کلیک کنید و گزینه Create a New Network را انتخاب نمایید.

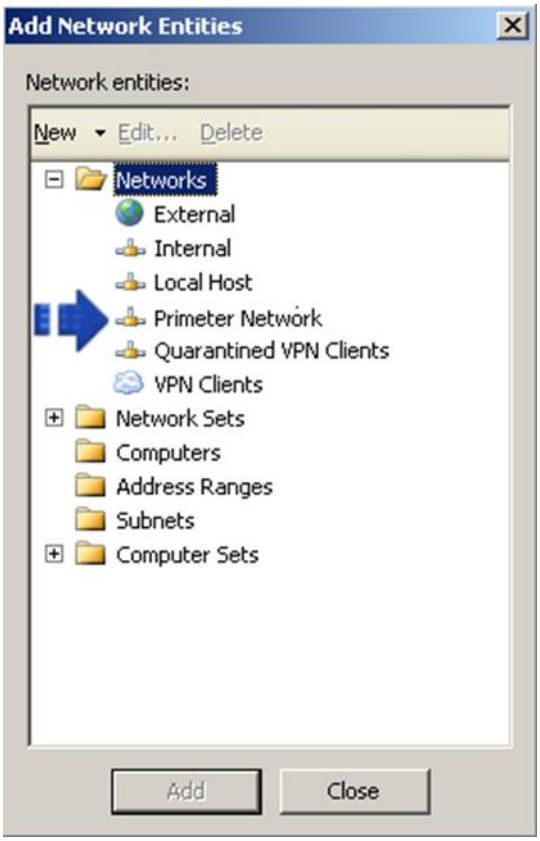


در پنجره باز شده یک نام وارد نمایید وگزینه Next را کلیک نمایید.

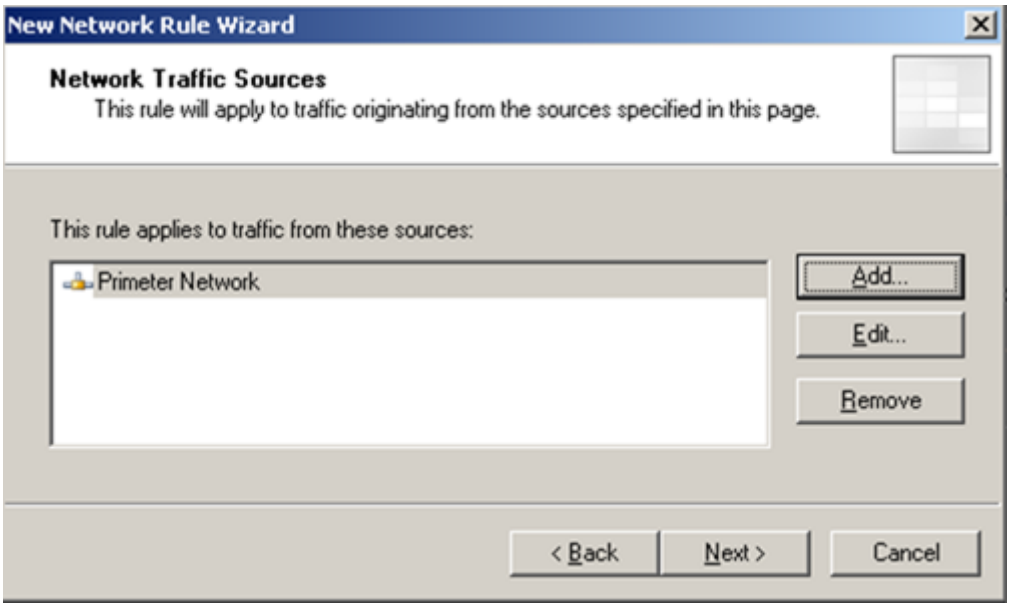


گزینه Add را انتخاب کرده سپس گزینه Primeter Network را انتخاب کنید. وسپس بر روی گزینه Add کلیک کنید.

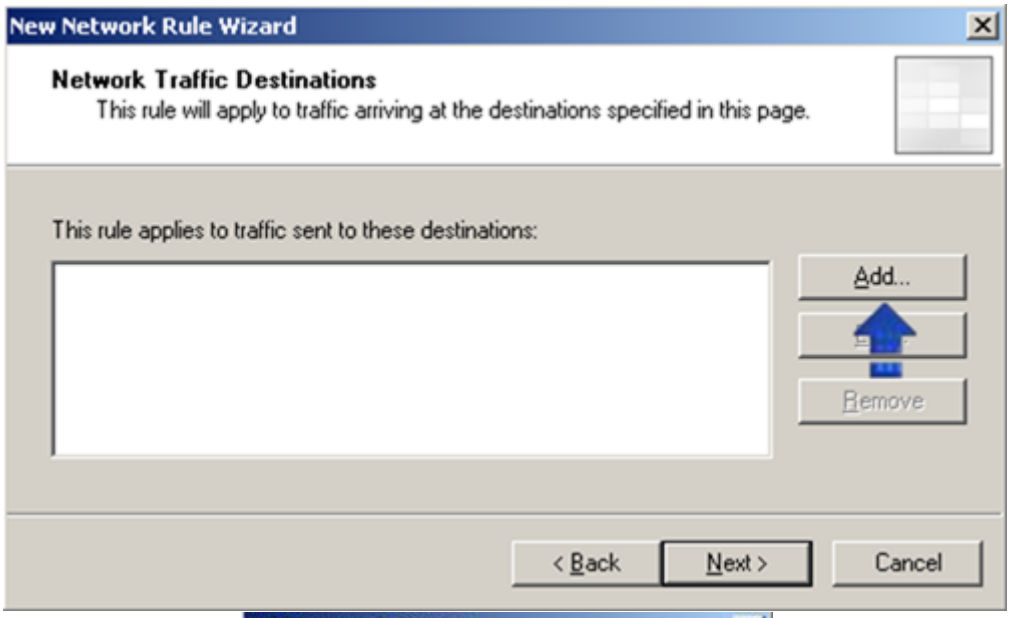


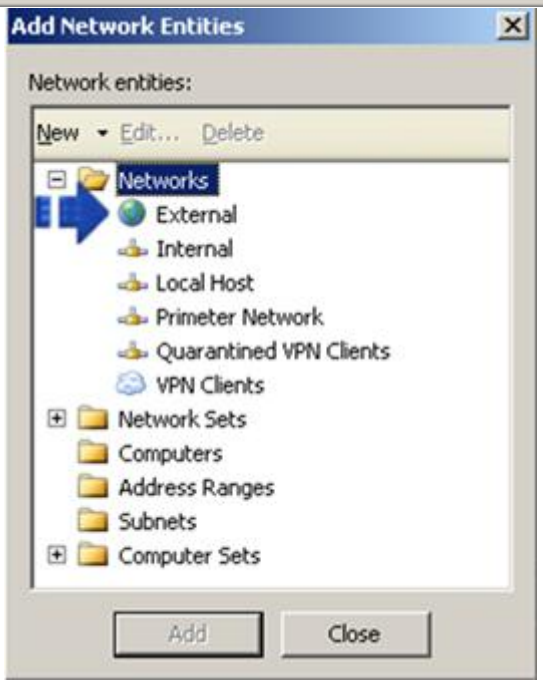


بر روی دکمه Next کلیک کنید.

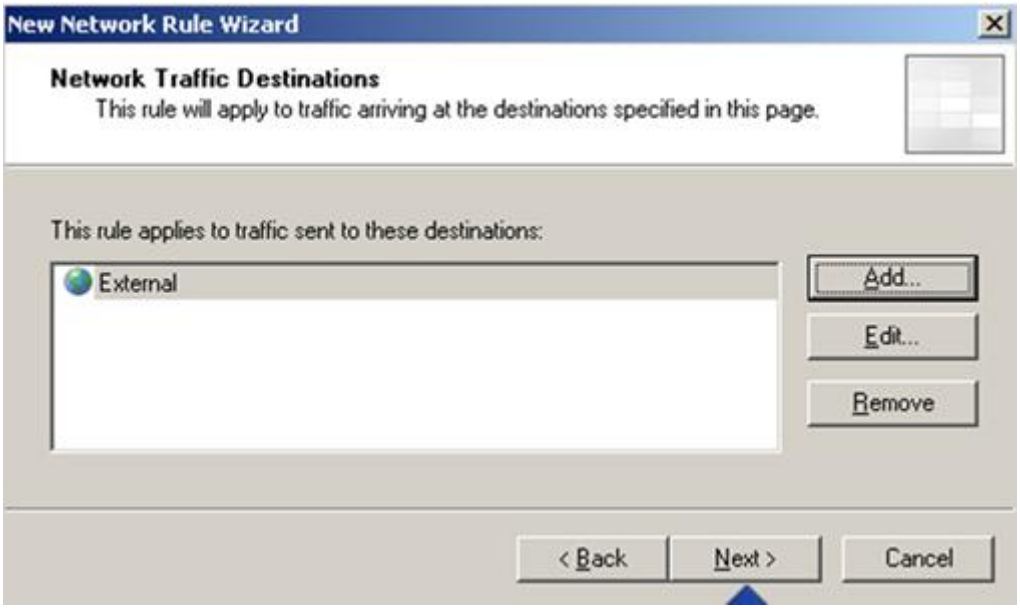


بر روی گزینه Add کلیک کنید. سپس از پنجره باز شده گزینه External را در قسمت Network روی گزینه Add انتخاب کرده وسپس روی Next کلیک کنید.





بر روی دکمه Next کلیک کنید.



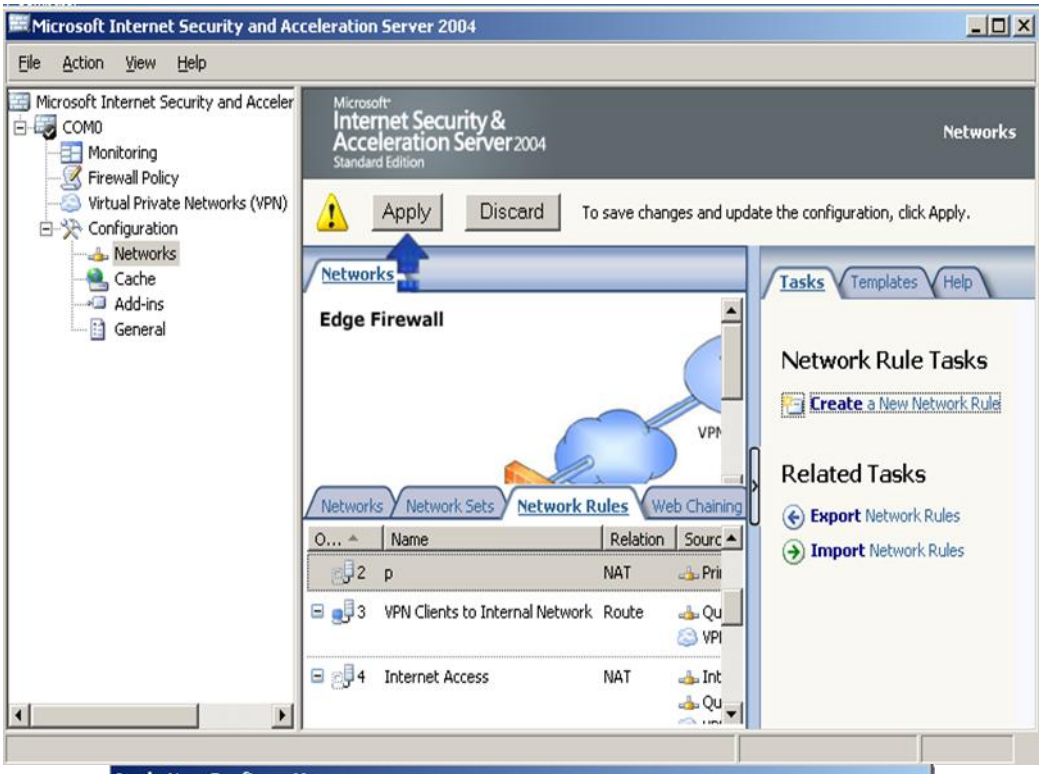
گزینه Network Address Translation (NAT) را انتخاب کرده و سپس بر روی Next کلیک کنید.



سپس با انتخاب گزینه Next پنجره مقابل ظاهر می‌گردد. بر روی گزینه Finish کلیک کنید



بر روی دکمه Applay کلیک کنید. سپس در صفحه ظاهرشده بر روی دکمه OK کلیک کنید.

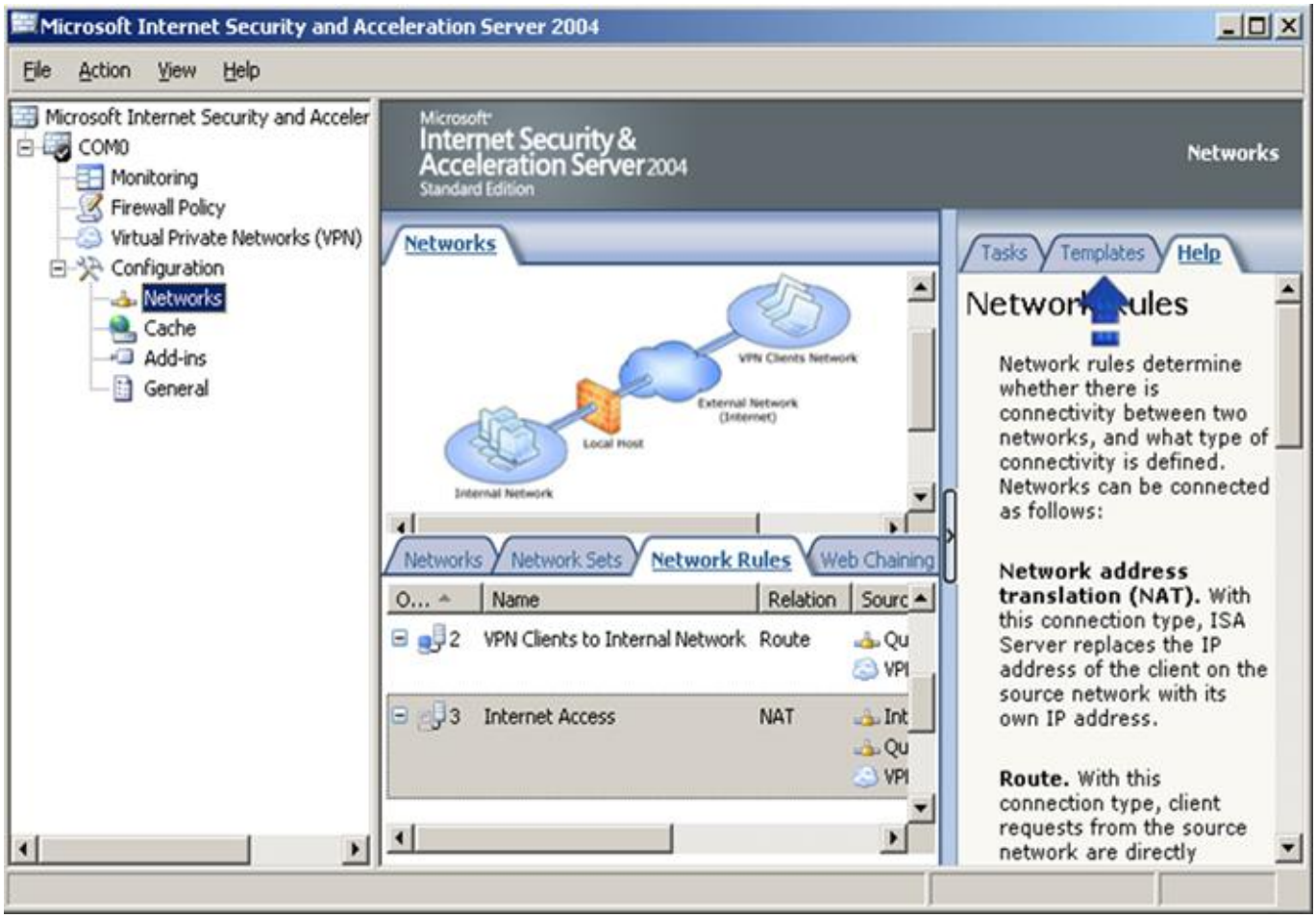


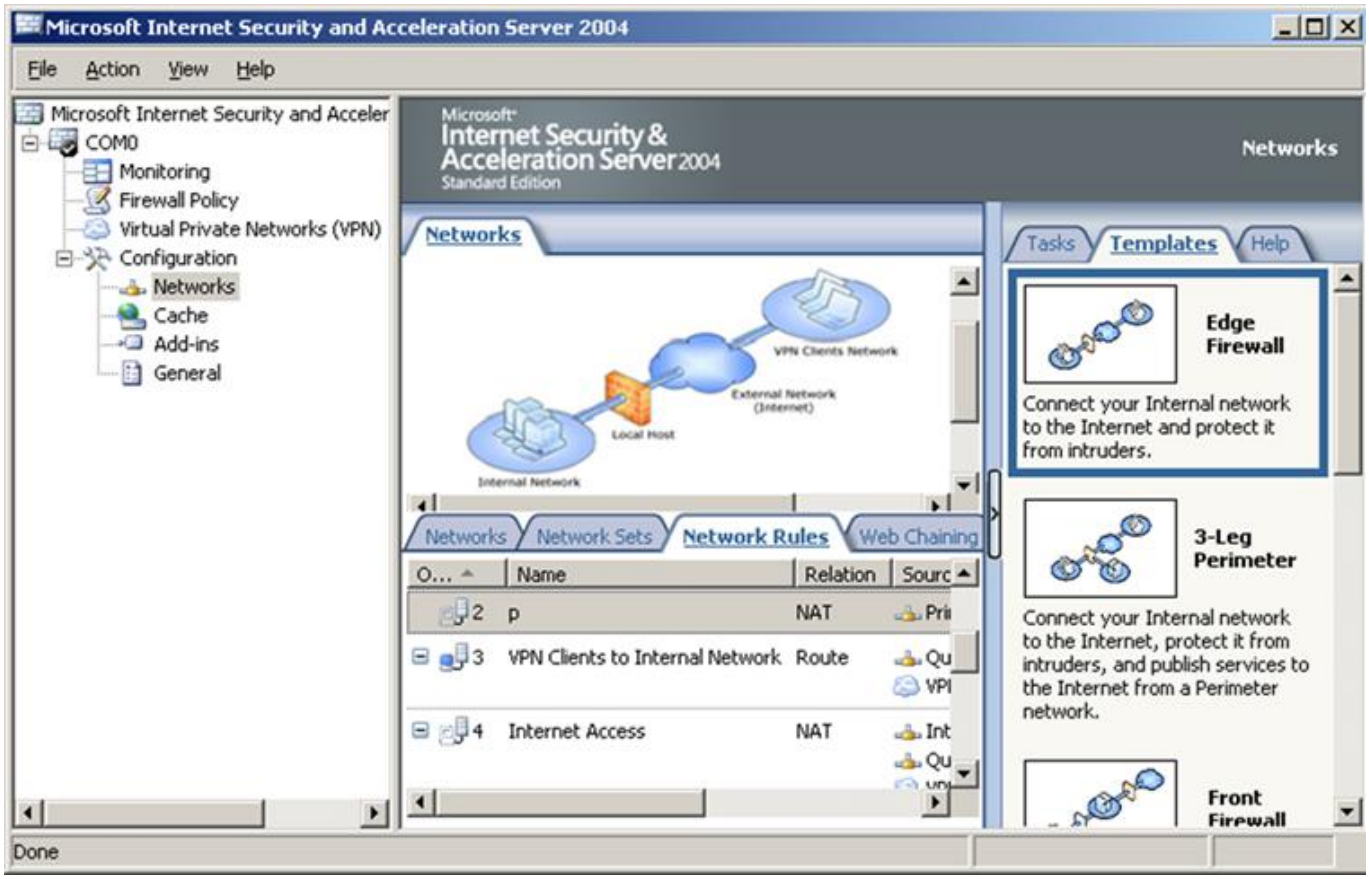
۴۰-۴-۵- تنظیمات Network Ruleon ISA Server (جهت ارتباط یک شبکه Local وخارجی)

از منوی Start گزینه All Programs را انتخاب کنید. از منوی Microsoft ISA Server گزینه ISA Server Management را انتخاب کنید تا صفحه زیر باز شود.

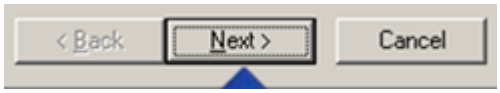


بر روی گزینه Configuration+ کلیک کنید. گزینه Network را انتخاب نموده و سپس در سمت ر است گزینه Tempelates را انتخاب نماید. بر روی گزینه Edge Firewall کلیک کنید.


Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Security and Acceler
COM0
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Networks
Networks
VPN Clients Network
External Network (Internet)
Local Host
Internal Network
Networks Network Sets Network Rules Web Chaining
O... Name Relation Sourc
2 VPN Clients to Internal Network Route
3 Internet Access NAT
Tasks Templates Help
Network Rules
Network rules determine whether there is connectivity between two networks, and what type of connectivity is defined. Networks can be connected as follows:
Network address translation (NAT). With this connection type, ISA Server replaces the IP address of the client on the source network with its own IP address.
Route. With this connection type, client requests from the source network are directly


Microsoft Internet Security and Acceleration Server 2004
File Action View Help
Microsoft Internet Security and Acceler
COM0
Monitoring
Firewall Policy
Virtual Private Networks (VPN)
Configuration
Networks
Cache
Add-ins
General
Microsoft Internet Security & Acceleration Server 2004
Standard Edition
Networks
Networks
VPN Clients Network
External Network (Internet)
Local Host
Internal Network
Networks Network Sets Network Rules Web Chaining
O... Name Relation Sourc
2 p NAT
3 VPN Clients to Internal Network Route
4 Internet Access NAT
Tasks Templates Help
Edge Firewall
Connect your Internal network to the Internet and protect it from intruders.
3-Leg Perimeter
Connect your Internal network to the Internet, protect it from intruders, and publish services to the Internet from a Perimeter network.
Front Firewall
Done

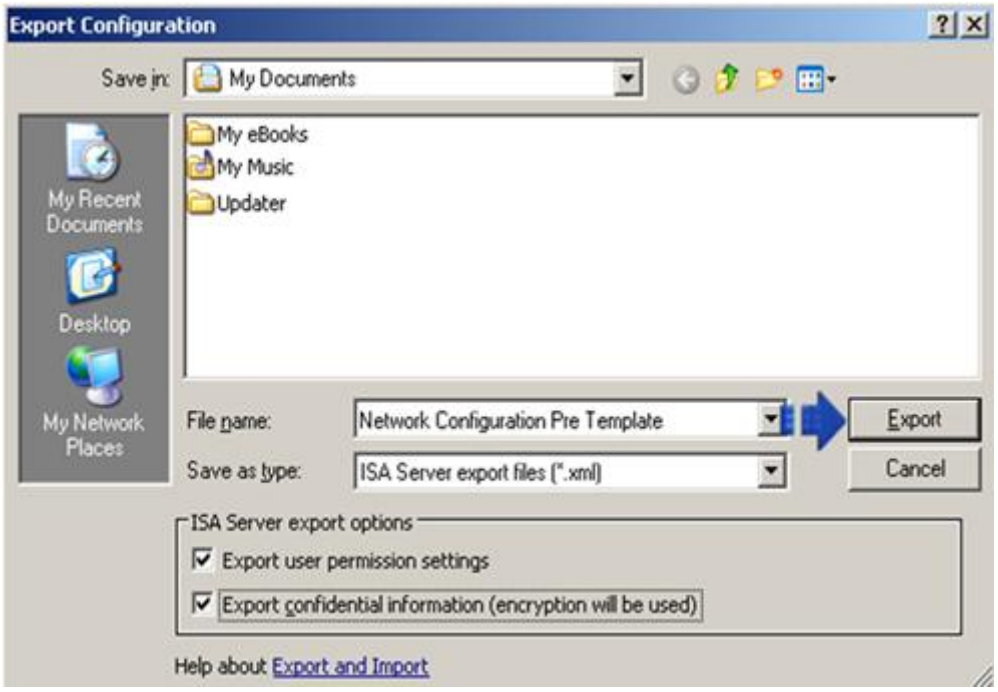
بر روی دکمه Next کلیک کنید.



بر روی Export کلیک کنید



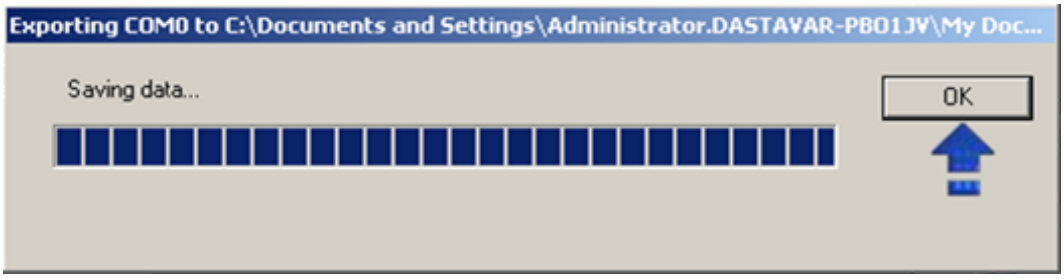
در پنجره باز شده در قسمت Filename یک نام وارد کنید و گزینه Export User Permission Settings و Export Confidential را تیک زده وبر روی گزینه Export کلیک کنید.



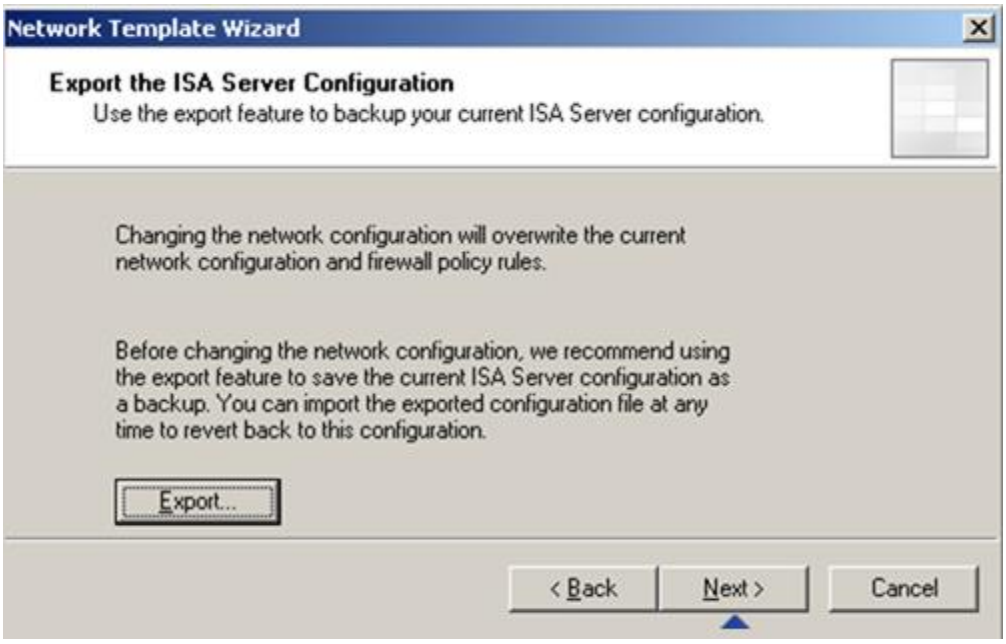
یک رمزعبور وارد نموده وبر روی دکمه OK کلیک کنید.



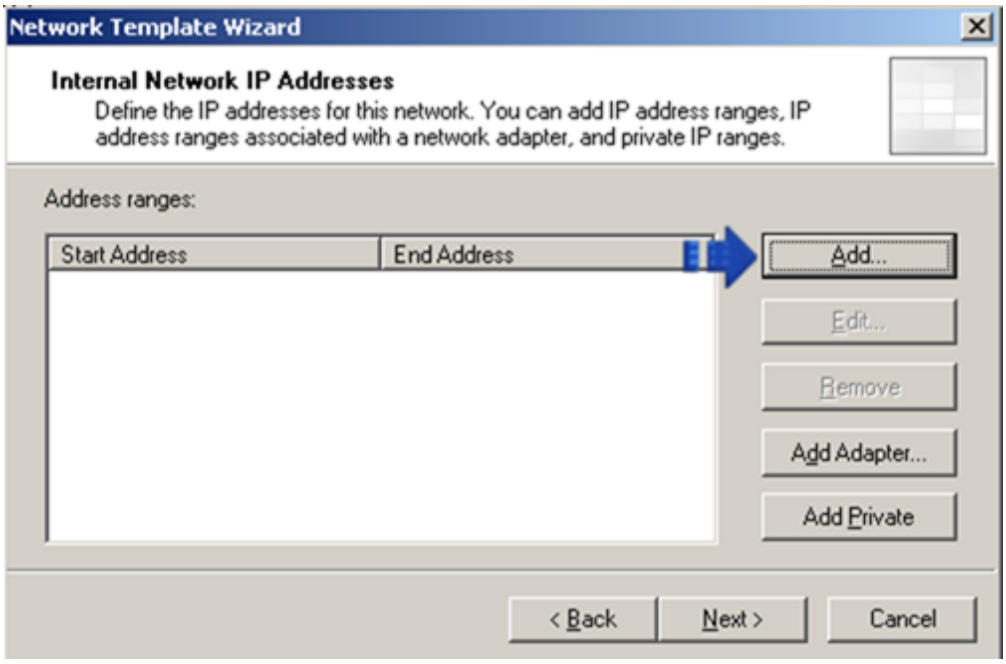
پس از اتمام عملیات Export بر روی OK کلیک کنید.

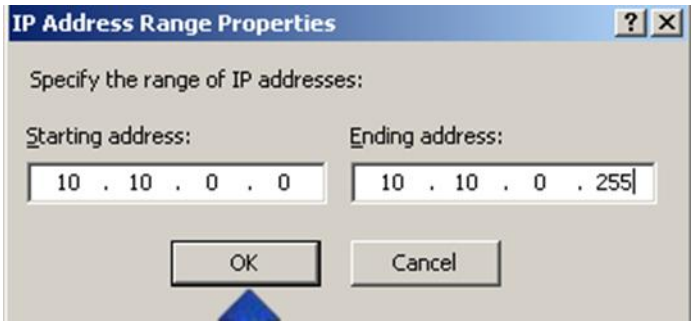


در ادامه بر روی دکمه Next کلیک کنید.

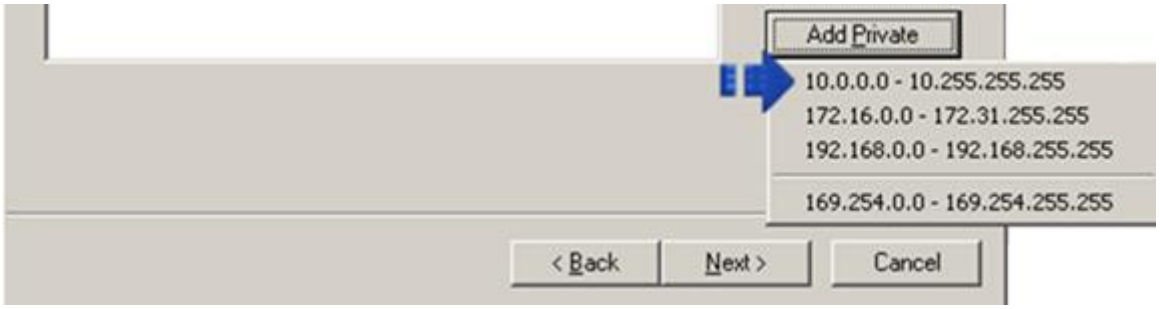


بر روی دکمه Add کلیک نمایید تا پنجره تعیین IP Address باز شود. محدوده آدرس را وارد کرده وگزینه OK را انتخاب کنید.

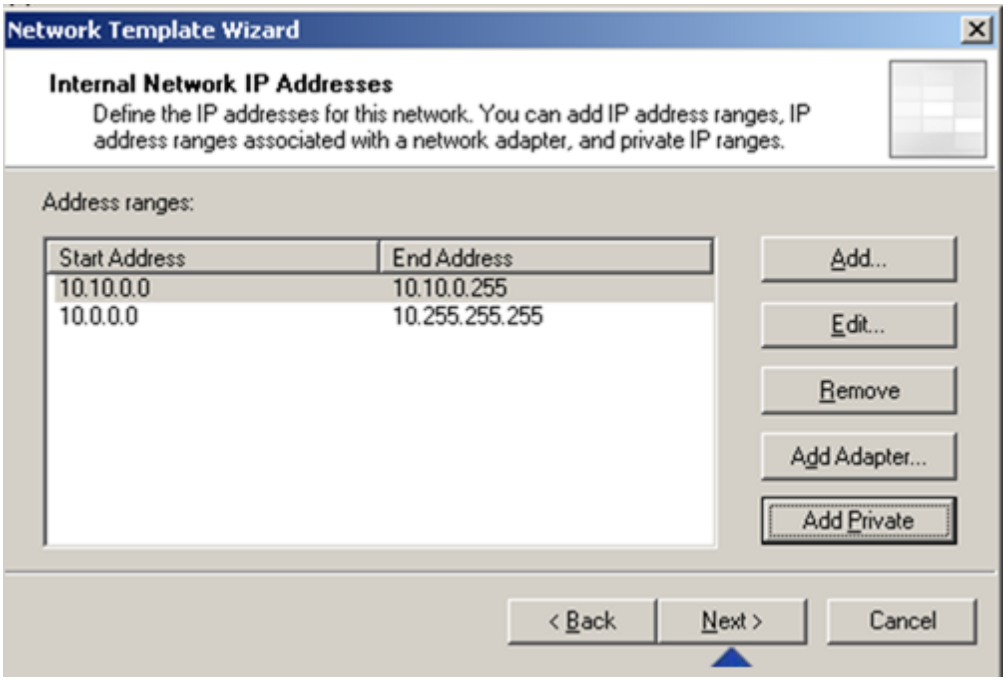




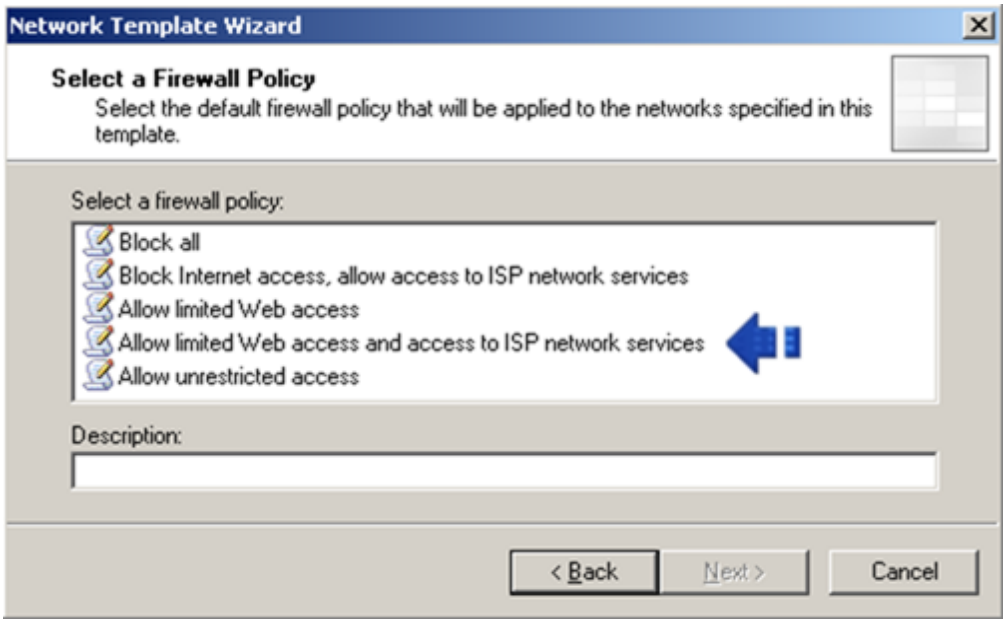
همچنین می‌توانید از محدوده آدرس خصوصی استفاده نمایید. همانطور که در فصل ۲ گفته شد، آدرس‌های خصوصی، آدرس هایی هستند که فقط در شبکه محلی کاربرد دارند و معادل آن‌ها در دنیای اینترنت وجود ندارد.



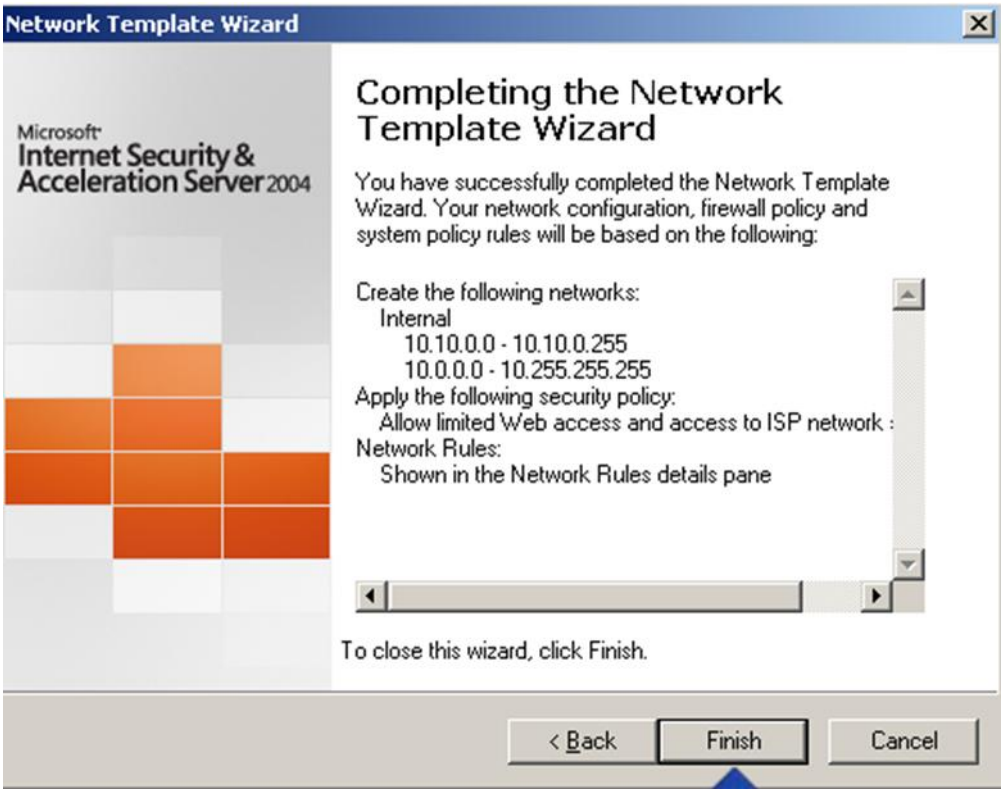
پس از اضافه کردن ادرس باید کنترل کنید که آدرس مورد نظر نیز موجود باشد. بر روی دکمه Next کلیک کنید.



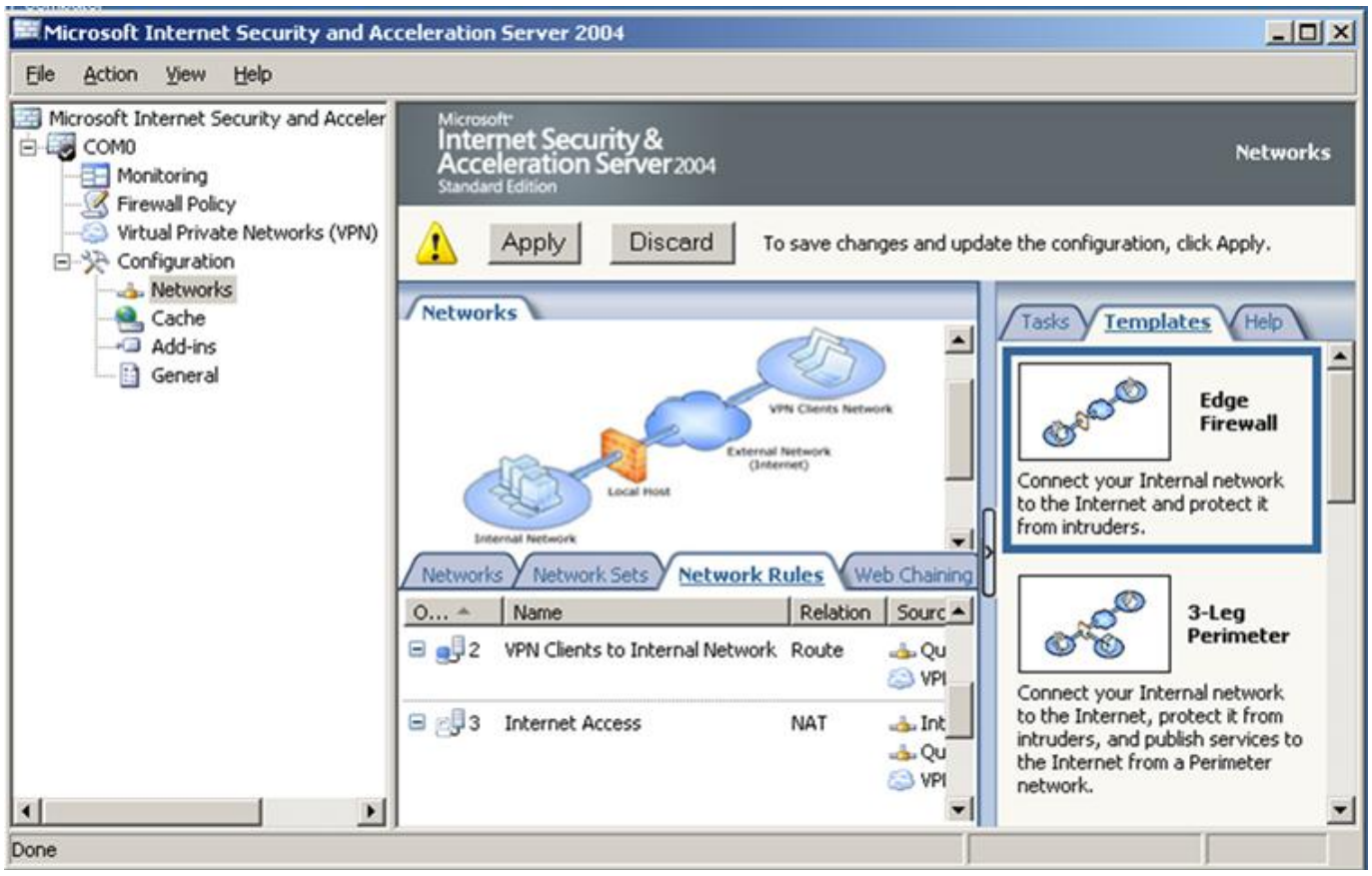
در این صفحه گزینه مورد نظر را انتخاب کنید وبر روی دکمه Next کلیک کنید.

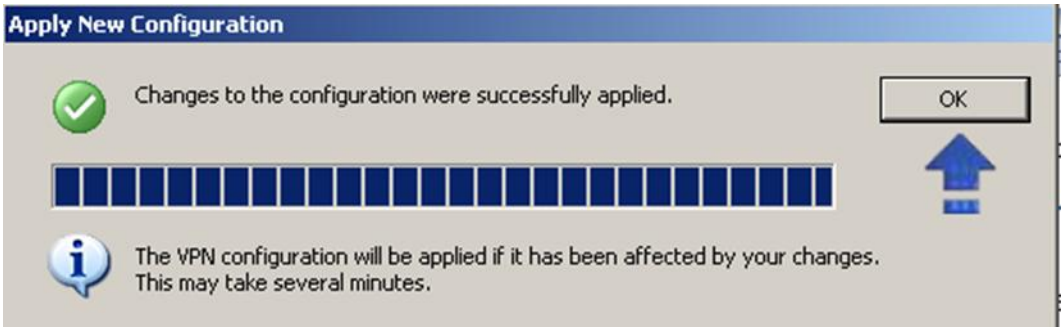


بر روی گزینه Finish کلیک کنید



در نهایت بر روی دکمه Applay کلیک کرده، سپس در صفحه ظاهرشده بر روی دکمه OK کلیک کنید.

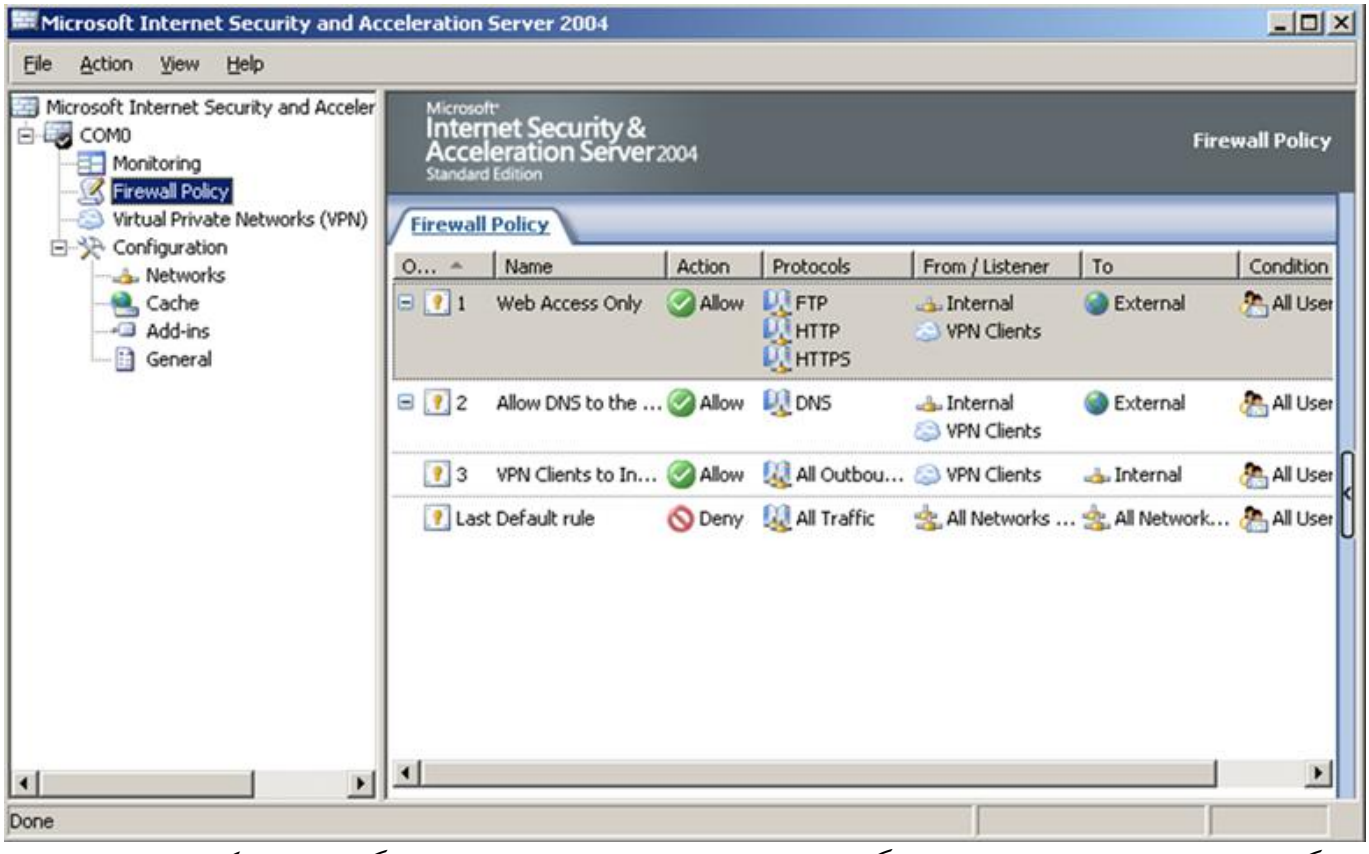




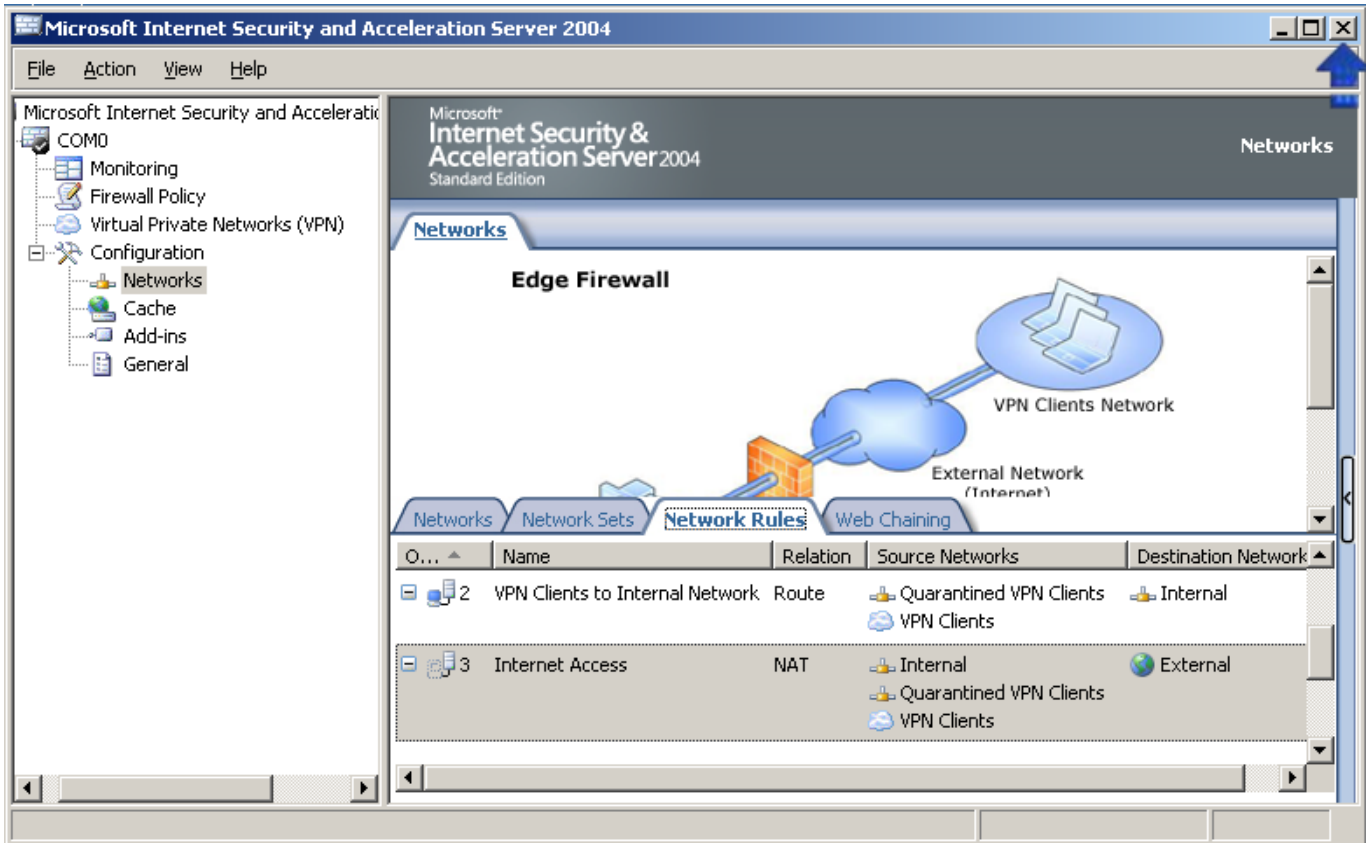
۴۰-۵- مشاهده روش‌های دستیابی به شبکه در ISA Server

با کلیک بر ISA Server Management در منوی All Programs ➔ Strart پنجره زیر باز می‌گردد. بر روی گزینه Firewall Policy کلیک کنید تا موارد زیر مشاهده شود.

این تنظیمات توسط Template هایی که ایجاد کرده‌ایم حاصل شده است. با دابل کلیک روی هر گزینه می‌توان مشخصات هر گزینه را دید به عنوان مثال گزینه اول اجازه دسترسی به HTTPs - HTTP - FTP را میدهد. گزینه دوم (DNS) اجازه دسترسی کلاینت‌های Internal و VPN را به یک شبکه خارجی می‌دهد.

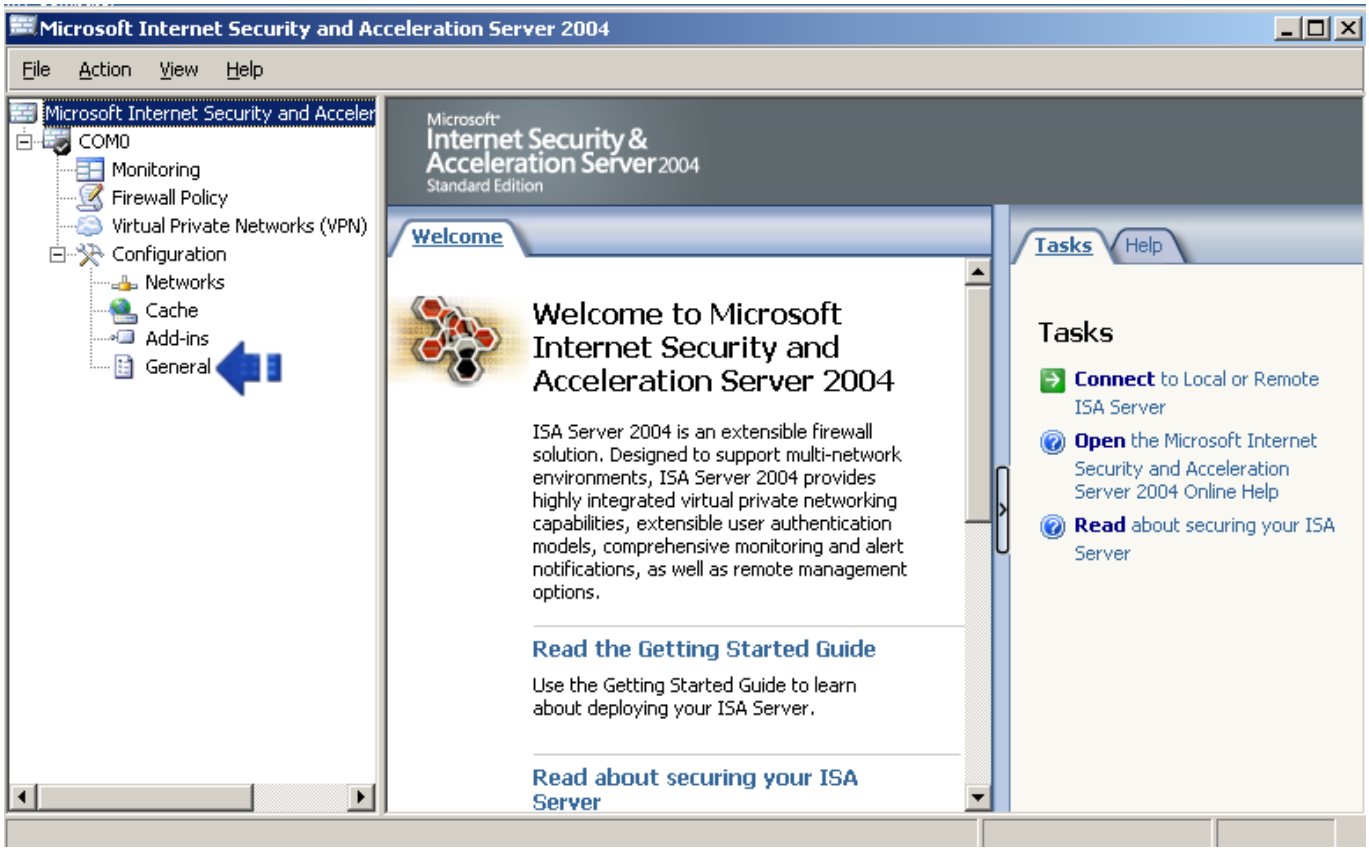


گزینه Internet Access از موارد دیگر قابل بررسی در Network می‌باشد. این گزینه نحوه یک ارتباط Nat میان internal و Quarantined VPN Client تعیین می‌کند

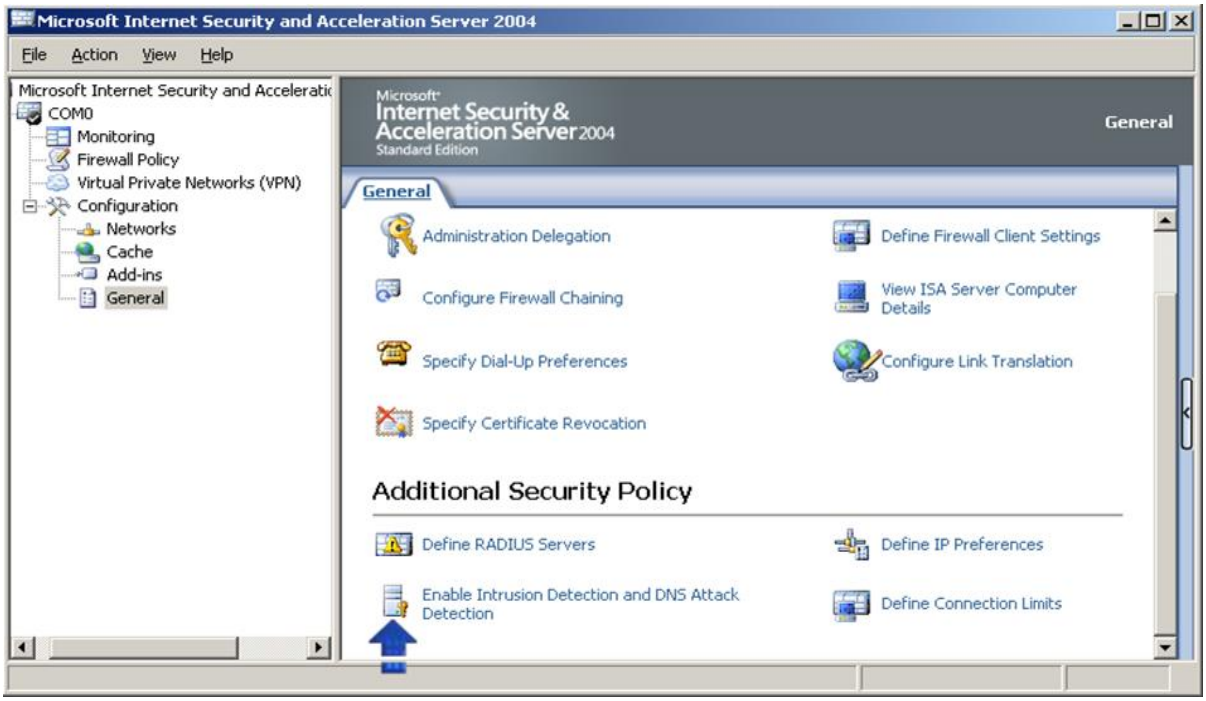


۴۰-۶- تشخیص نفوذ

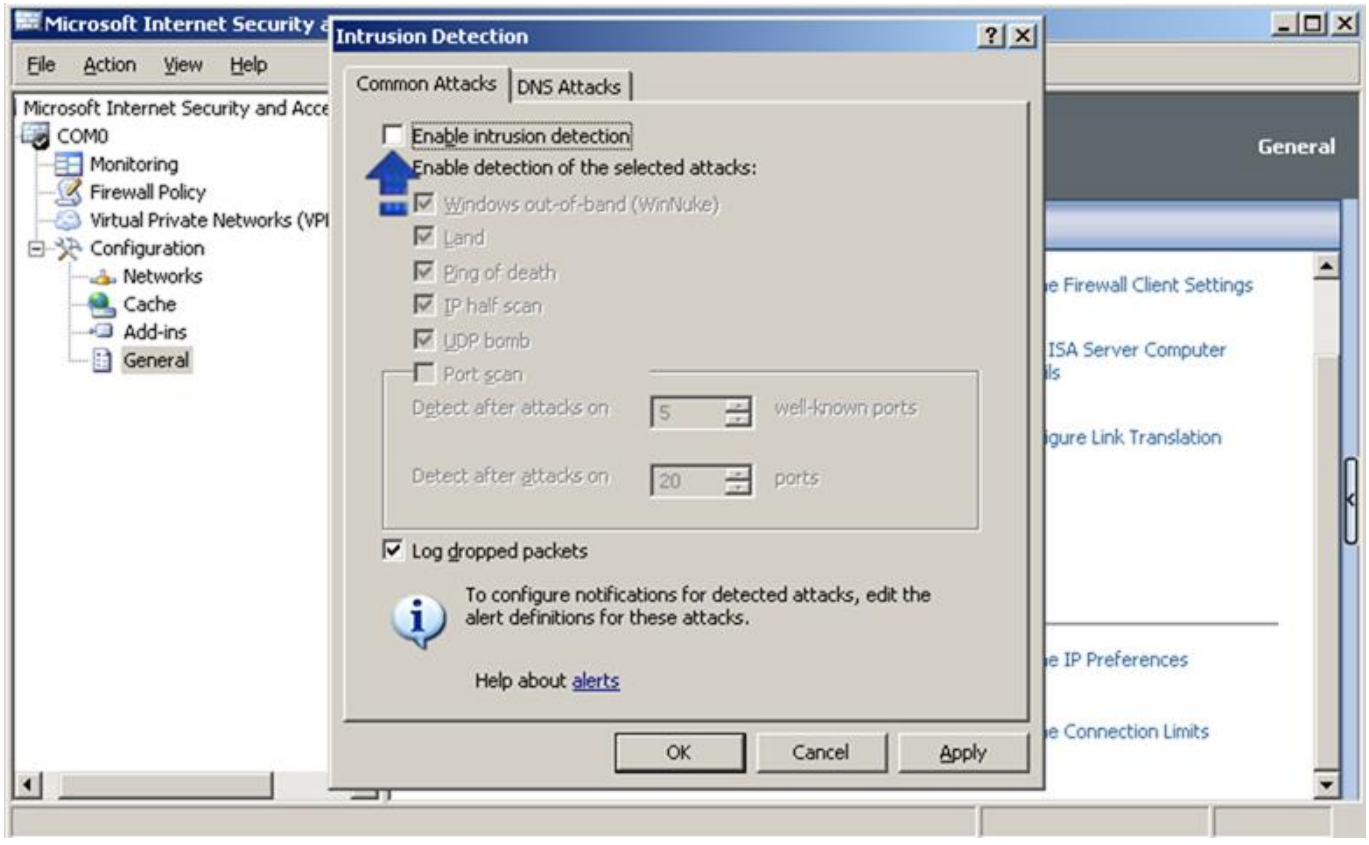
از منوی Start گزینه All Programs را انتخاب کنید. از منوی Microsoft ISA Server. گزینه ISA Server Management را انتخاب کنید تا صفحه زیر باز شود.



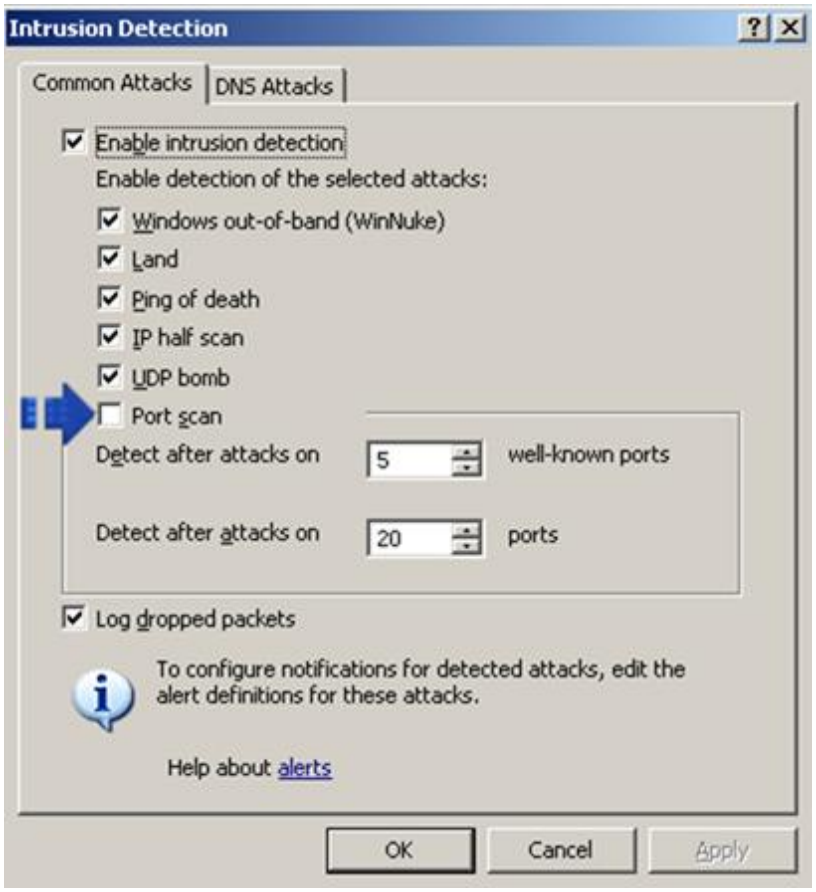
در صفحه بالا گزینه General را انتخاب نمایید.



بر روی گزینه Enable Intrusion Detection And DNS Attack Detection کلیک کنید.



گزینه Enable Intrusion Detection را کلیک کنید تا انتخاب شود. گزینه Port Scan را انتخاب کنید.گزینه دیگر نیز می‌توانند برای اعمال تغییرات مورد استفاده قرار گیرند. پس از انتخاب OK، روی گزینه Applay کلیک کنید تا تغییرات اعمال شود.



۴۰-۷- نحوه ایجاد سرویس‌های VPN با ISA Server

VPN ایجاد یک ارتباط امن بین کاربران شبکه و منابع داخلی یا خارجی شبکه؛ و یا برعکس ارتباط بین کاربران خارج از شبکه با منابع داخلی شبکه می‌باشد. به عنوان مثال ارائه سرویس اینترنت به کاربران درون شبکه با استفاده از VPN.

ISA Server به دو روش برای ایجاد VPN استفاده می‌کند.

- با استفاده از پروتکل PPTP (Point To Point)
- بااستفاده از پروتکل L2TP

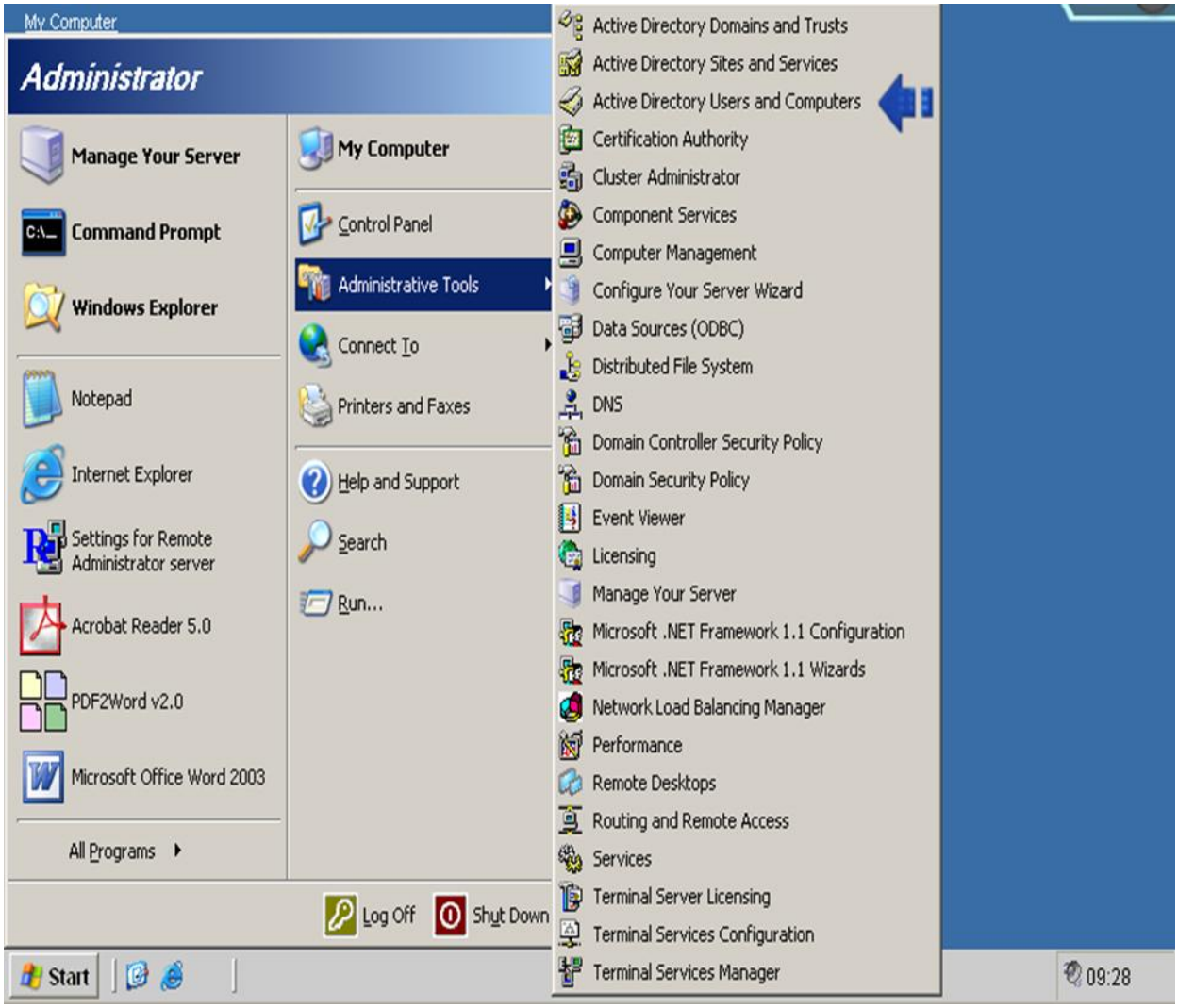
ISA Server دارای یک کامپونت به نام VPN Contol Current Time است که تنظیمات VPN کاربران را مورد بررسی قرار می‌دهد که در صورت درست نبودن تنظیمات یا غیر ستاندارد بودن VPN از ارتباط ان کلاینت با سرور جلوگیری می‌کند.

به طور پیش فرض VPN روی ISA Server فعال می‌باشد. زمانی که ISA Server را برای VPN تنظیم می‌کنیم ISA Server همانند DHCP، IPهایی را به کلاینت‌ها تخصیص می‌دهد که این محدوده آدرس در تنظیمات مشخص می‌شود. ISA Server با ارتباط Side By Side می‌تواند بین چند شبکه ارتباط VPN برقرار کنند. به عنوان مثال ارتباط VPN شعبه‌های یک شرکت با شعبه اصلی از طریق اینترنت.

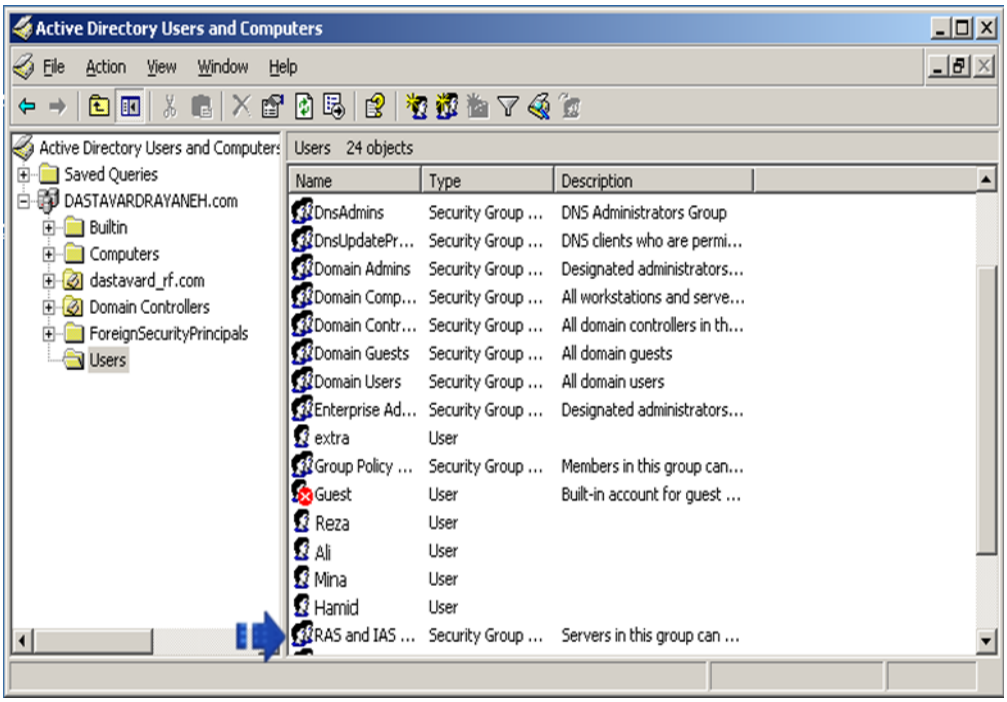
۴۰-۷-۱- تنظیمات VPN در ISA Server

از منوی Start گزینه Administrator Tools وسپس Active Directory User & Computer را انتخاب کنید.

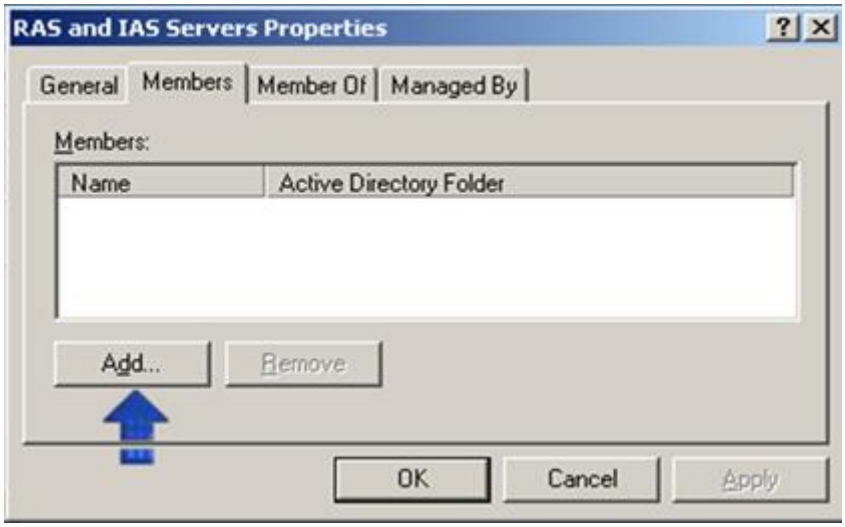
این گزینه تنها در ویندوز سرورهایی که روی آن‌ها Active Directory نصب شده باشد، موجود است.



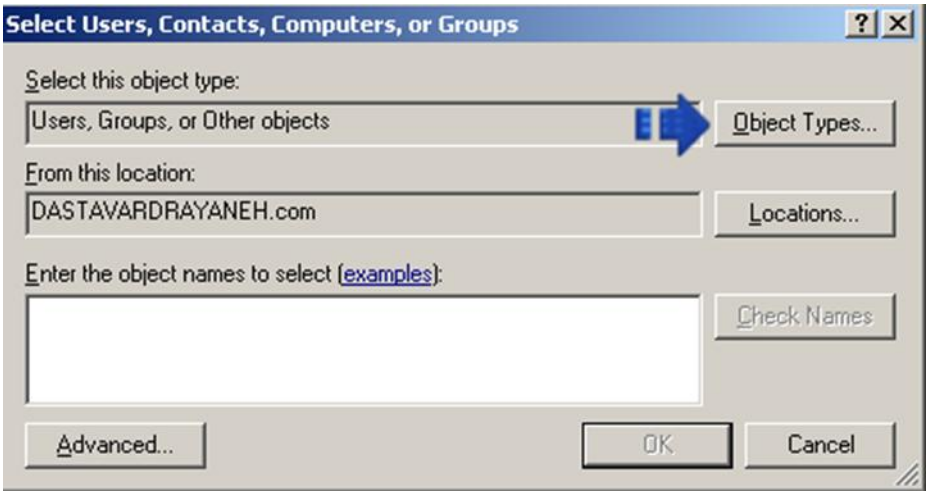
بر روی RAS and IAS Server دابل کلیک کنید



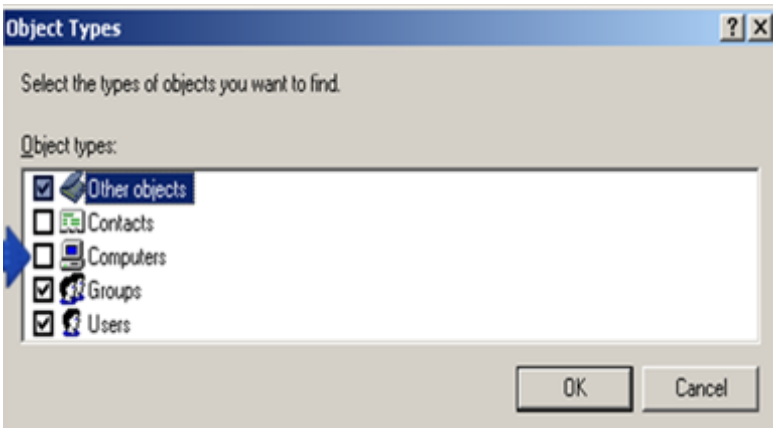
در پنجره باز شده Members Tab را انتخاب کرده وگزینه Add را کلیک کنید تا پنجره زیر باز شود.



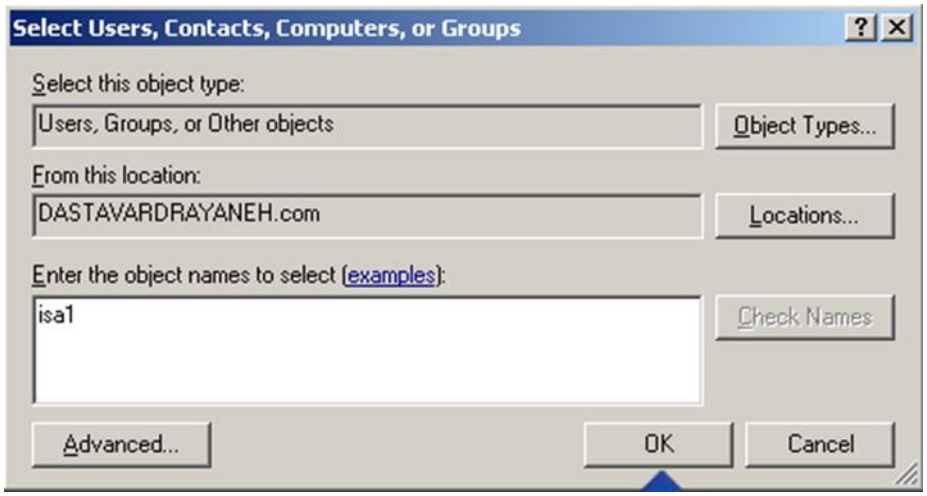
بر روی گزینه Object Type کلیک کنید.



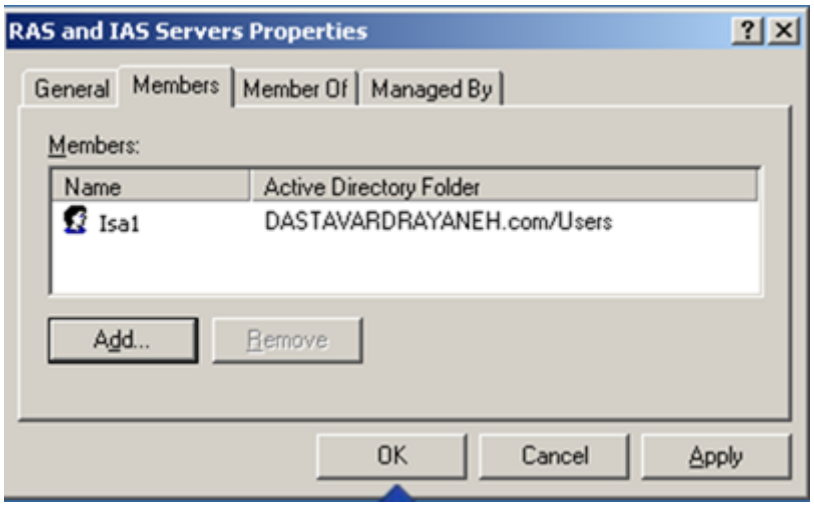
در کادر Object Type گزینه Computer را انتخاب نمایید. سپس بر روی OK کلیک کنید.



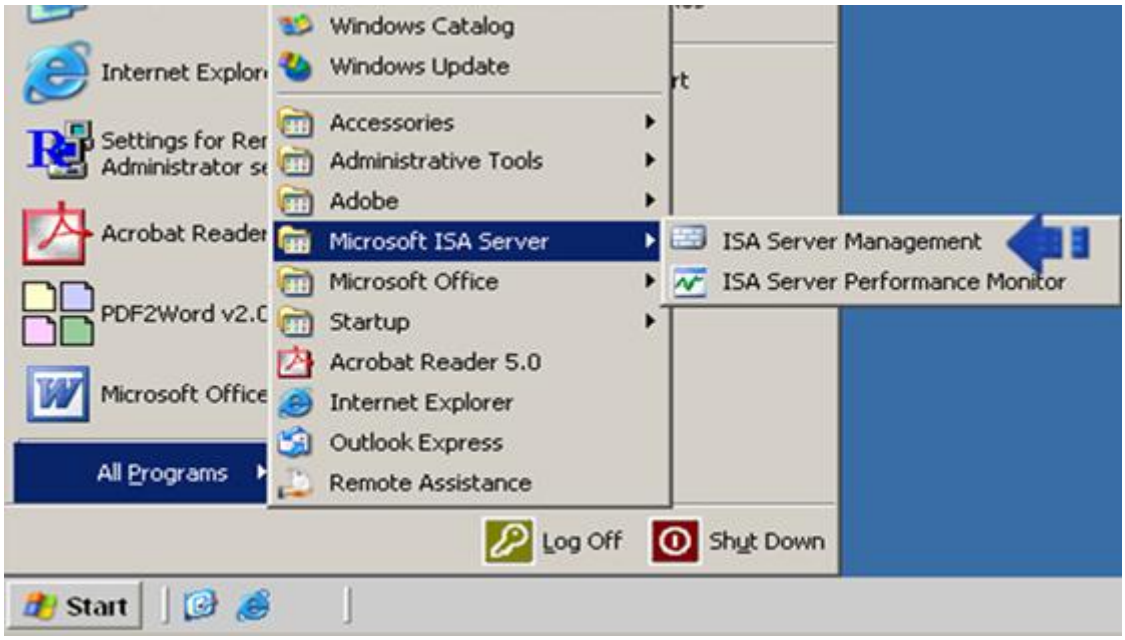
در کادر مقابل نام کامپیوتر مورد نظر را نوشته و بر روی OK کلیک کنید.



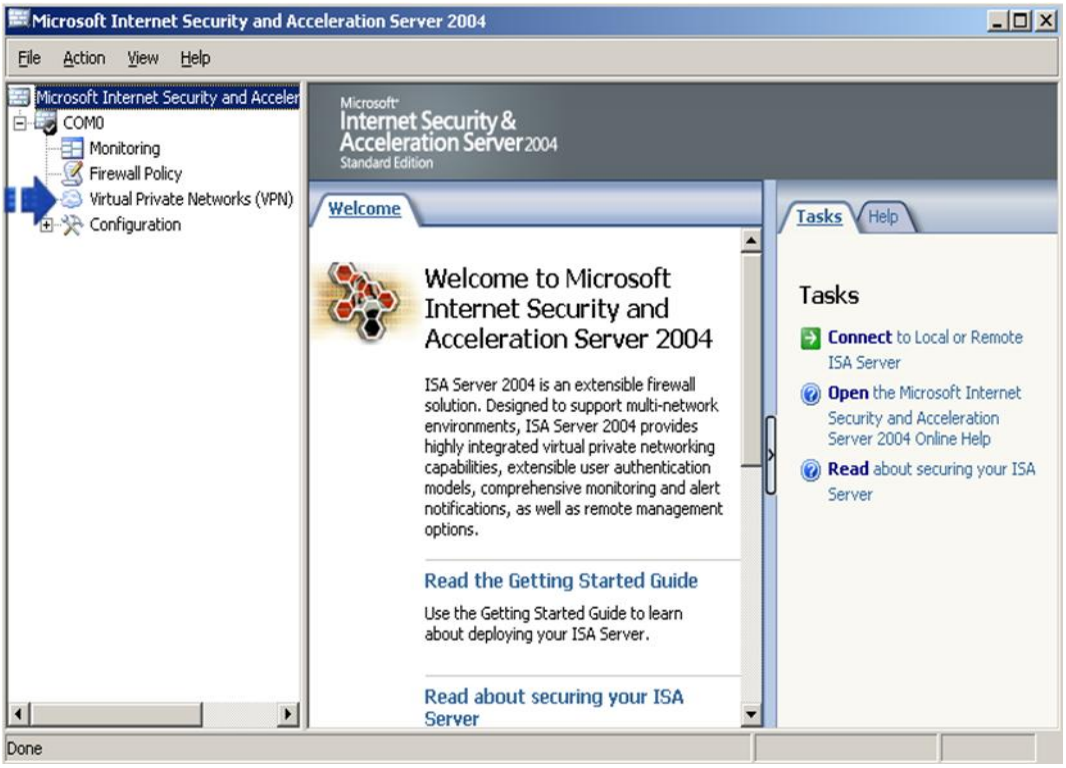
در کادر مقابل بر روی OK کلیک کنید تا پنجره بسته شود.



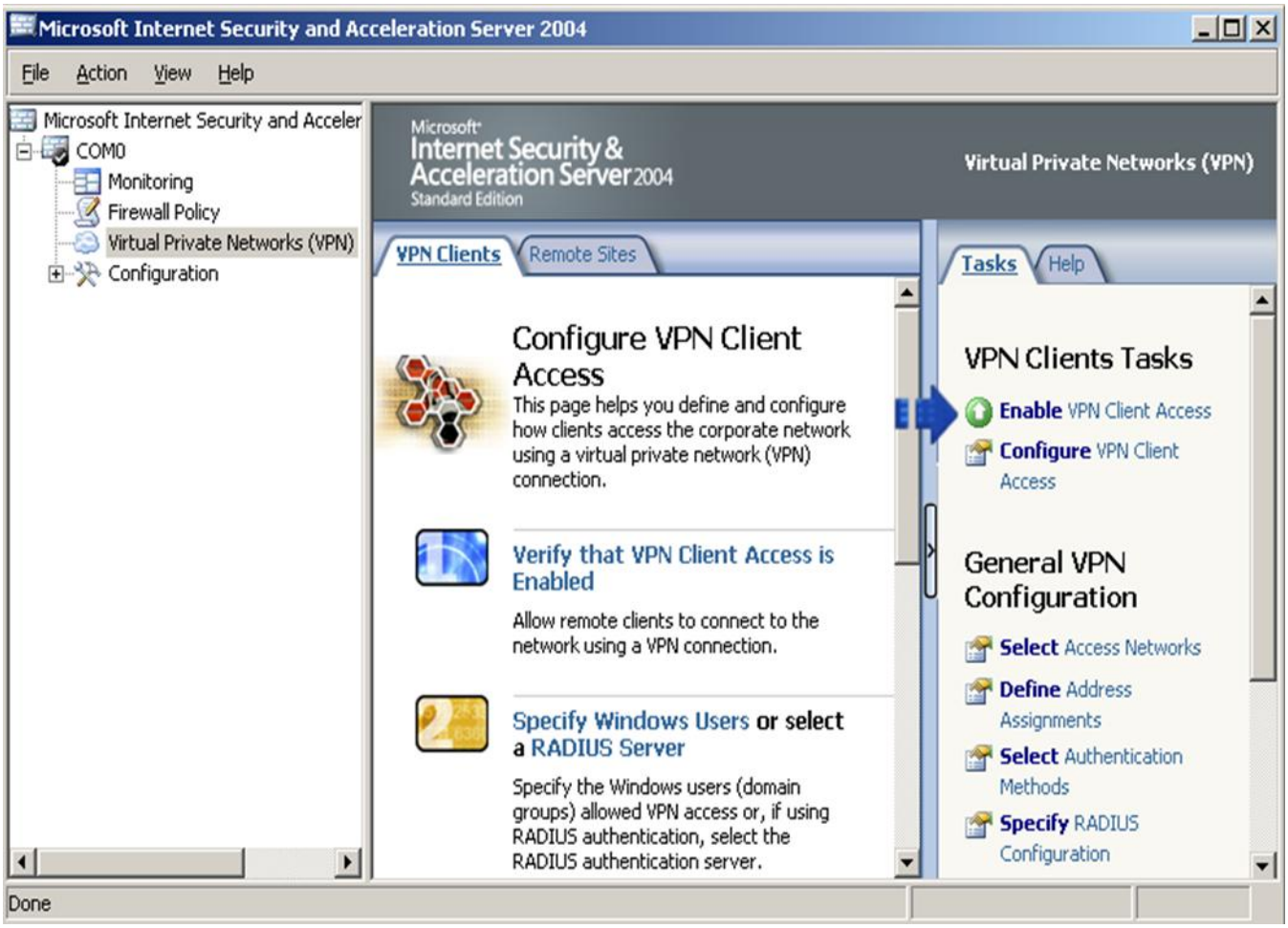
سپس از منوی Start گزینه All Programs را انتخاب کنید. از منوی Microsoft ISA Server گزینه ISA Server Management را انتخاب کنید تا صفحه زیر باز شود.



گزینه Virtual Private Network را انتخاب کنید.



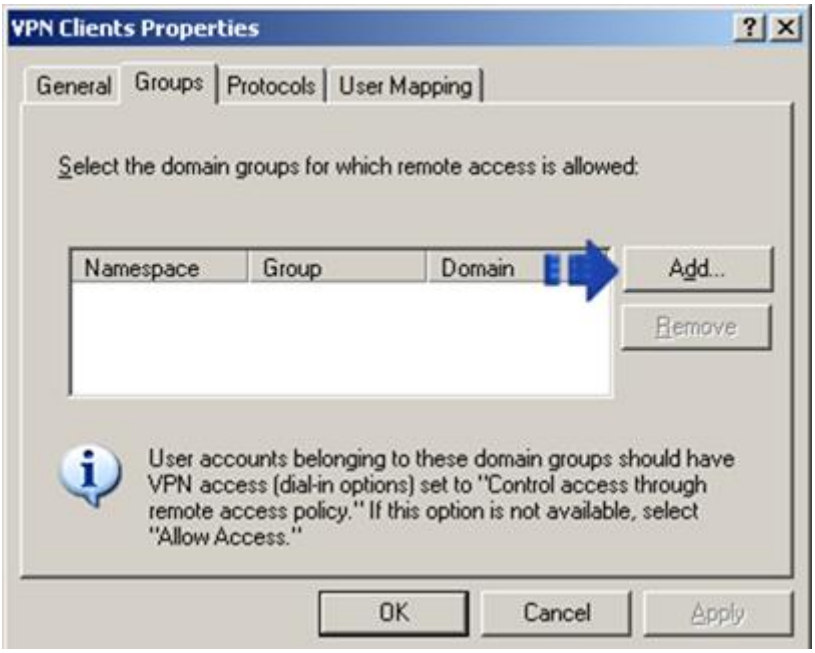
جهت فعال‌سازی VPN، گزینه Enable VPN Client Access را انتخاب کنید



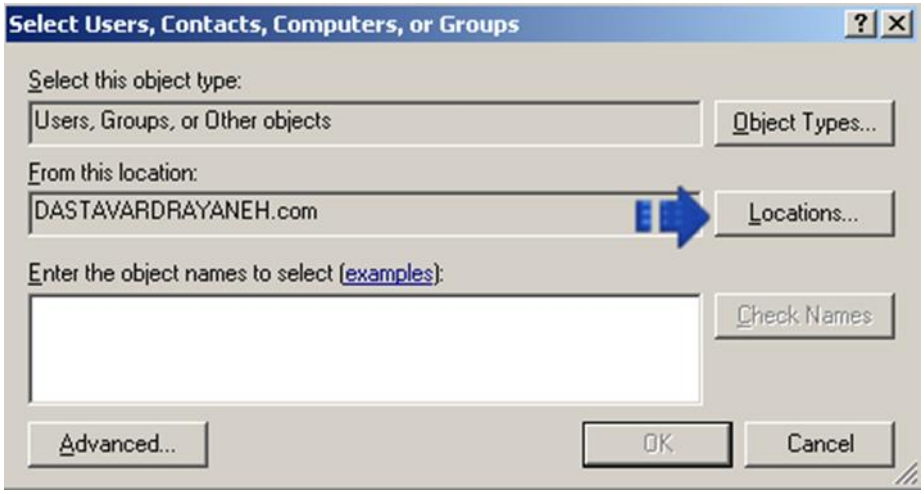
سپس جهت تنظیمات VPN بر روی گزینه Configure VPN Client کلیک کنید.



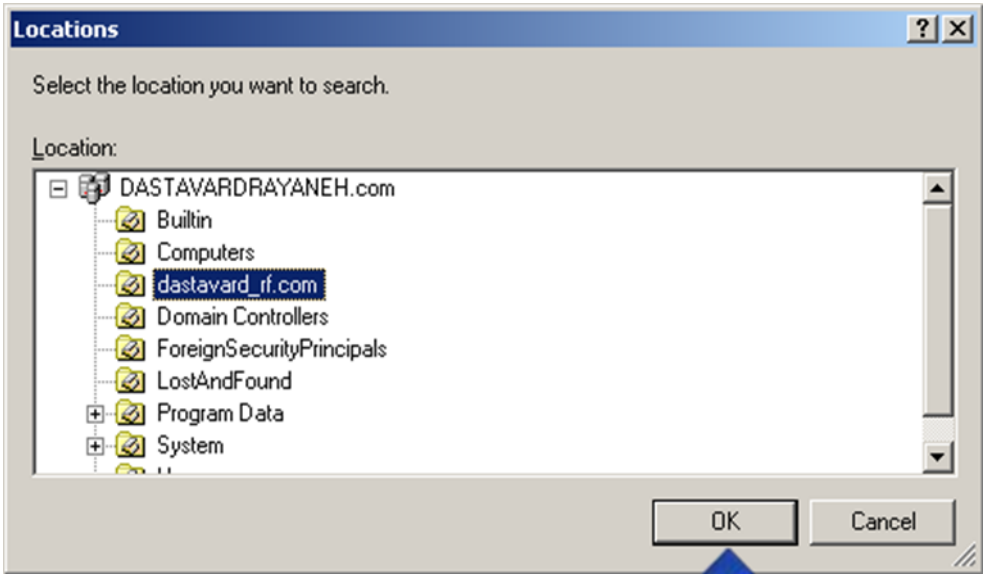
در سربرگ Groups بر روی گزینه Add کلیک کنید.



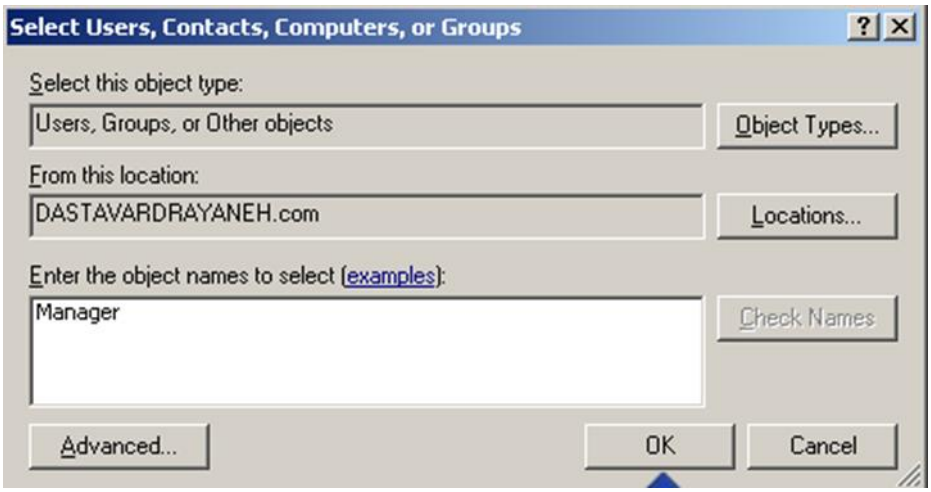
در کادر مقابل بر روی Location کلیک نمایید.



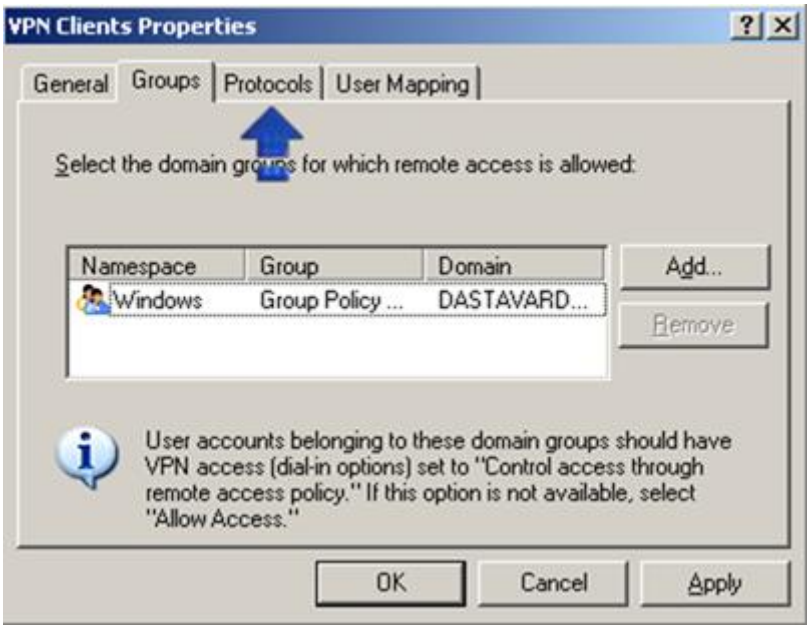
دامنه مورد نظر را انتخاب وبر روی گزینه OK کلیک کنید.



در کادر مقابل نام کاربر مورد نظر را بنویسید. سپس بر روی گزینه OK کلیک کنید



بعد از تعیین دامنه و گروه و کاربر بر روی سربرگ Protocols کلیک کنید.



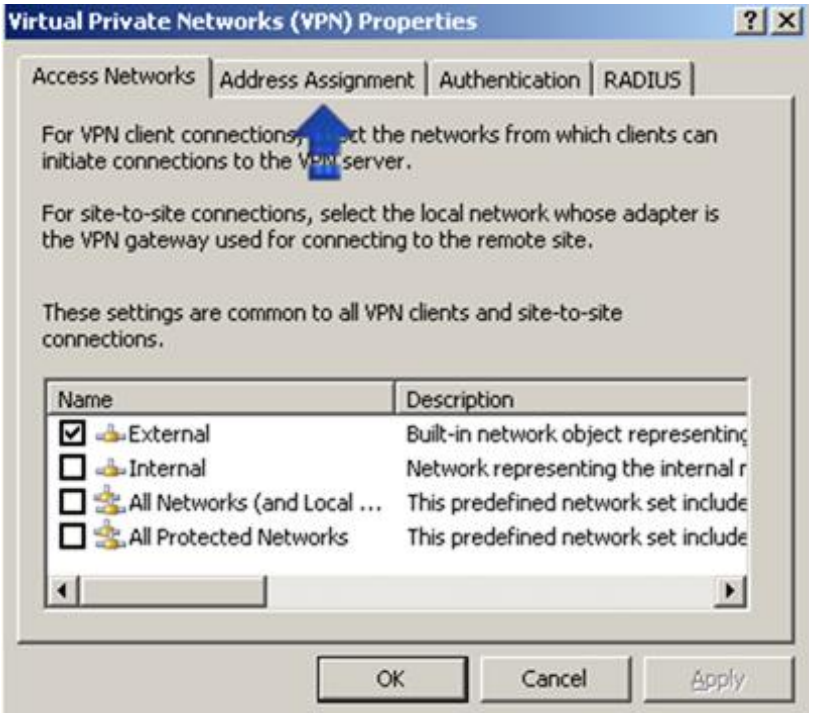
در کادر مقابل گزینه Enable PPTP باید تیک خورده باشد. سپس بر روی گزینه OK کلیک کنید.



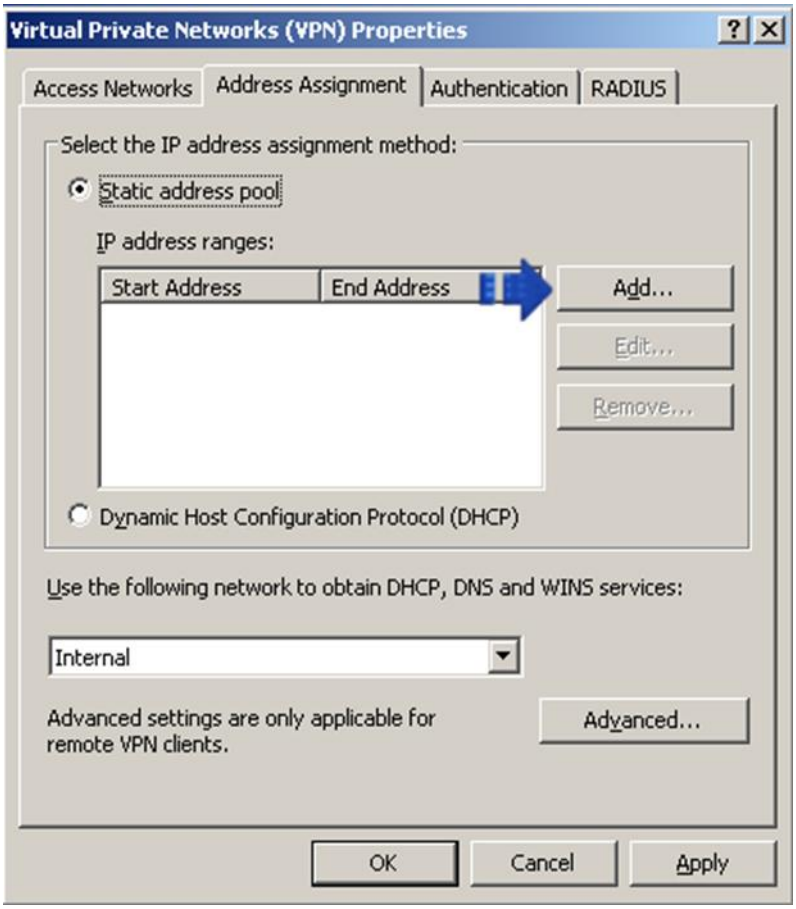
بر روی گزینه Virtual Private Network راست کلیک کنید وگزینه Peroperties را انتخاب نمایید.



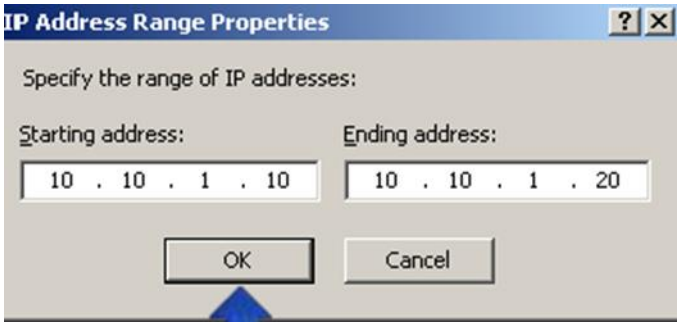
در این صفحه باید گزینه External برای ارتباطات خارجی تیک خورده باشد. سپس بر روی Address Assignment کلیک کنید تا آدرس‌های IP مد نظر جهت تخصیص به کاربران راه دور را تعیین نمایید.



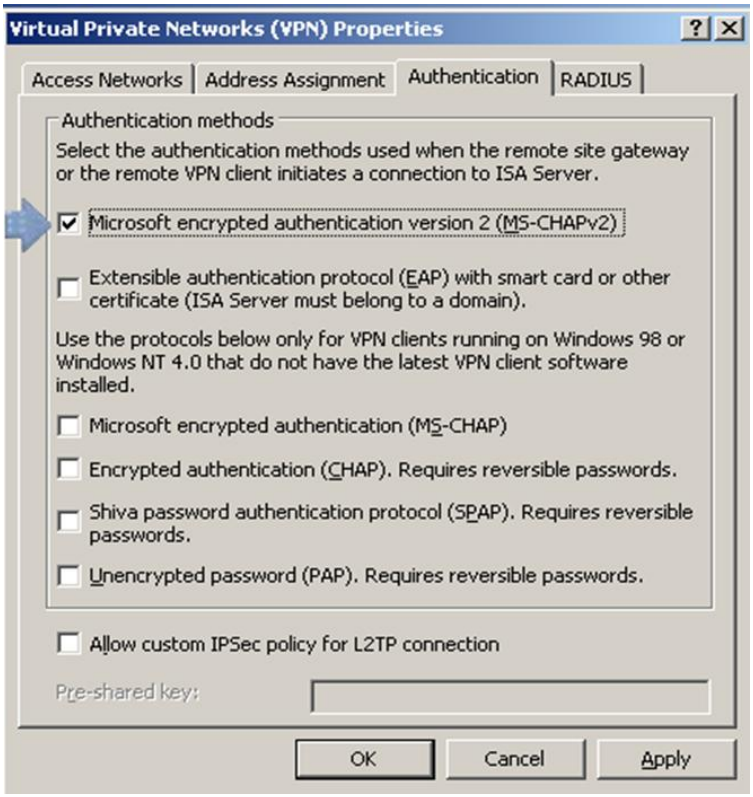
گزینه Static Address Pool را انتخاب کرده و بر روی گزینه Add کلیک نمایید.



در کادر باز شده محدوده آدرس VPN را مشخص نمایید. آدرس‌های تخصیصی به کاربران از این محدوده انتخاب می‌شود. سپس بر روی گزینه OK کلیک نمایید.



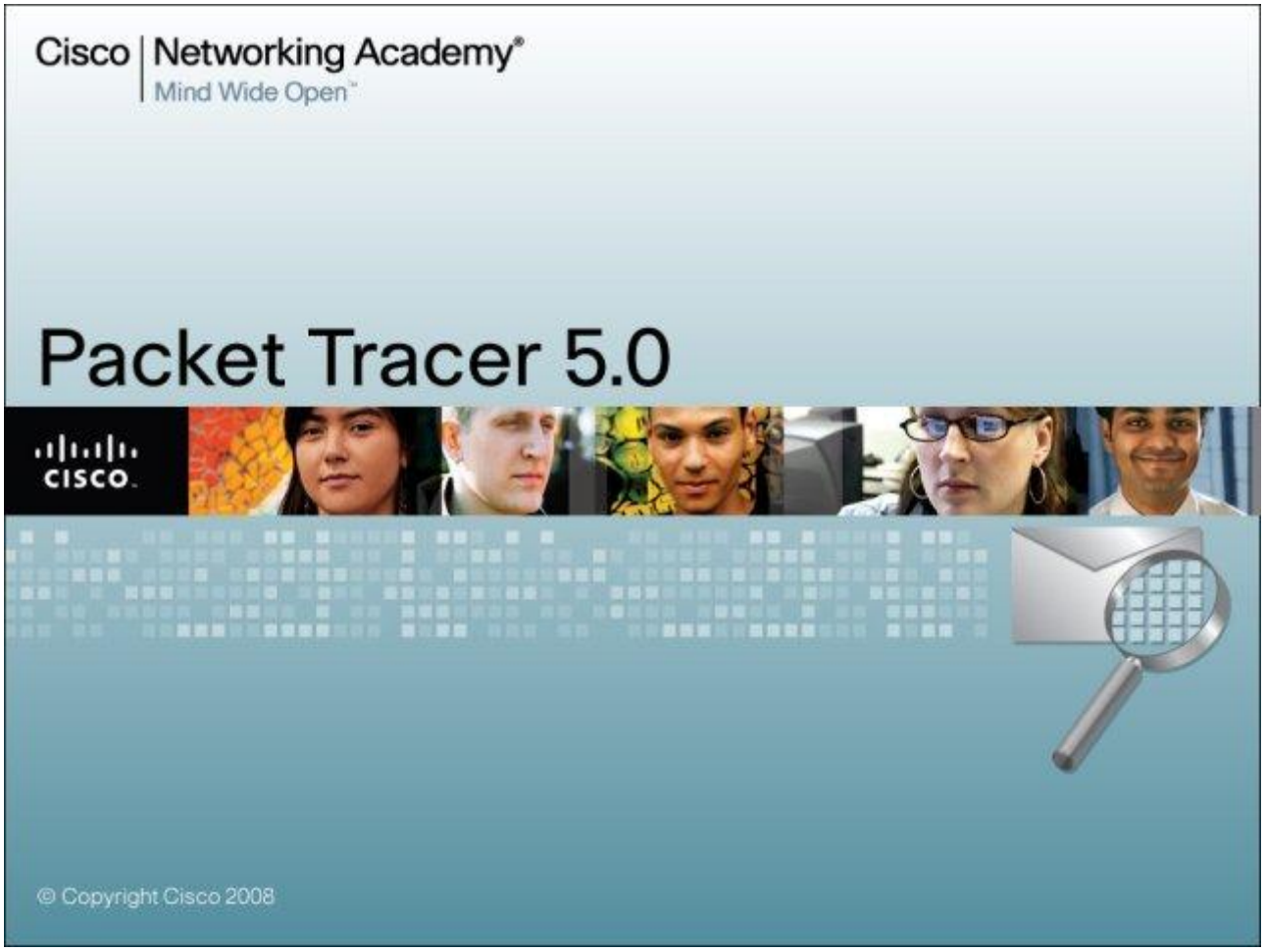
پس از تنظیمات آدرس، در سربرگ Authentication گزینه Microsoft Encrypted Authentication Version2 را تیک بزنید. سپس بر روی گزینه OK کلیک کنید تا پنجره بسته شود.



برای اعمال تغییرات بر روی Apply کلیک کنید.



فصل ۴۱ نرم‌افزار Packet Tracer



Packet Tracer یک محیط شبیه‌سازی برای کسانی است که قصد طراحی شبکه، توپولوژی، پیکربندی، بررسی مشکلات و... را دارند. کاربران می‌توانند براحتی ابزارهای مورد نظر خود را در محیط شبیه سازی وارد نموده و توپولوژی مورد نظر خود را ایجاد کنند. آنگاه پس از پیکر بندی شبکه ایجاد شده می‌توانند به بررسی تحلیل و بررسی و رفع مشکلات آن بپردازند.

در این فصل به آموزش نسخه ۵ این نرم افزار می‌پردازیم.

۴۱-۱- آشنایی با نرم افزار Packet Tracer

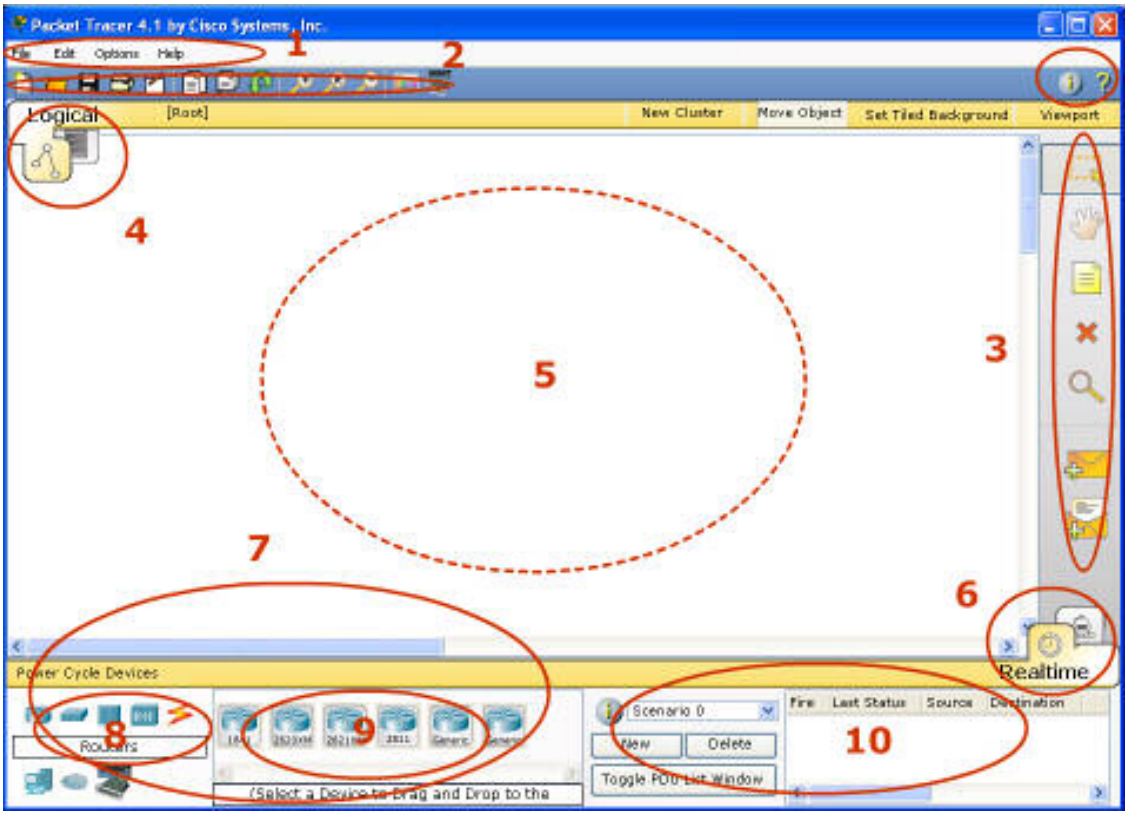
نرم افزار Packet Tracer یک محیط شبیه سازی جهت طراحی، پیاده سازی توپولوژی، پیکربندی، بررسی مشکلات و ... را در شبکه دارند. کاربران می توانند با استفاده از ابزارهای مورد نظر در محیط شبیه سازی، به راحتی توپولوژی دلخواه خود را ایجاد و پس از پیکربندی شبکه ایجاد شده، به بررسی، تحلیل و رفع مشکلات آن بپردازند.

انواع تکنولوژی ها و توپولوژی هایی که توسط این نرم افزار پشتیبانی می شود به همراه ویژگی های اصلی آن در جدول زیر آورده شده است:

فضای کار منطقی	ایجاد توپولوژی شبکه دستگاه ها: عمومی، واقعی و ماژولار، مسیریاب، سوئیچ، میزبان، هاب، پل، بی سیم، نقطه دسترسی، ارتباط بین دستگاه ها از طریق انواع مختلف رسانه های شبکه بندی
فضای کار فیزیکی	سلسله مراتب دستگاه ها، فضاهای سیم بندی، ساختمان ها، شهرها و نماهای بین شهری، استفاده از تصاویر گرافیکی ایجاد شده توسط کاربر
حالت Realtime	به روز رسانی پروتکل ها بصورت زنده حد متوسطی از پیکربندی های IOS CLI برای سوئیچ ها و مسیریاب ها
پروتکل ها	پروتکل های LAN : CSMA/CD*, Ethernet, DHCP سوئیچینگ : VLANs, 802.1q, trunking TCP/IP : ARP, IP, ICMP, UDP, TCP* مسیریابی: static, default, RIPv1, RIPv2, EIGRP, inter-VLAN routing NAT : static, dynamic, overload ACLs:standard, extended, named WAN : HDLC, PPP, Frame Relay* * نشان دهنده این است که شامل محدودیت های قابل ملاحظه ای هستند
حالت شبیه سازی (Simulation)	Packet animation Global event list (packet sniffer) OSI Model, Detailed PDU, and Device Table Views User-defined multiple packet scenarios
طراحی و به اشتراک گذاری	گزینه های متنوع ذخیره سازی فایل Activity Wizard برای فعالیت های تمرینی با تصحیح اتوماتیک Challenge Mode با امکان تصمیم گیری کاربران در مورد نحوه اجرای الگوریتم روی بسته ها ویژگی های متنوع برای توضیحات متنی و گرافیکی

شروع کار با Packet Tracer

پس از اجرای نرم افزار Packet Tracer 4.1، محیط زیر رابه طور پیش فرض مشاهده خواهید کرد:

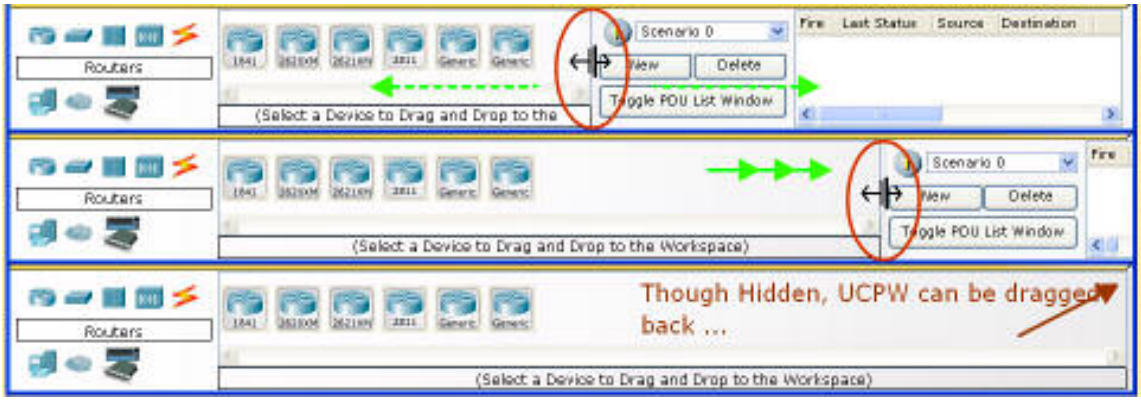


این واسط آغازین شامل ۱۰ جزء است. برای آگاهی از عملکرد هر جزء خاص، تنها کافیست نشانگر ماوس را بر روی آن حرکت داده تا توضیح مربوط به آن نمایش داده شود.

نوار منو	شامل منو های File ، Options و Help که دستورات رایجی نظیر Open، Save ، Print و Preferences در این منوها قرار گرفته اند.
نوار ابزار اصلی	شامل آیکن های میانبر برای دستورات منوی File و Edit و شامل دکمه هایی برای بزرگنمایی، پالت ترسیم، و مدیریت الگوها (Device Template Manager) است. در سمت راست آن دکمه Network Information قرار دارد که می توانید توضیحات دلخواه خود را در مورد شبکه جاری در آن وارد کنید.
نوار ابزارهای رایج	شامل دسترسی به ابزارهای رایج فضای کار: انتخاب، جابجایی لایه، درج توضیح، حذف، بررسی، افزودن PDU های ساده و افزودن PDU های پیچیده.
فضای فیزیکی/	می توان بین فضای فیزیکی و منطقی توسط این برگه ها سوئیچ نمود.

فضای منطقی و نوار پیمایش	همچنین این نوار امکان پیمایش در سطوح گره ها، ایجاد گروه جدید، جابجایی اشیاء، تنظیم پس زمینه و دیدن پورت ها را می دهد.
فضای کار	در این محدوده می توان شبکه خود را ایجاد و شبیه سازی ها و انواع اطلاعات و آمار مربوط به آن را مشاهده نمود.
نوار Realtime /Simulation	توسط برگه های این نوار می توان بین حالت های Realtime و شبیه سازی سوئیچ کرد. این نوار شامل دکمه Power Cycle Devices ، دکمه های Play Control و نیز Event List در حالت شبیه سازی می باشد.
جعبه اجزای شبکه	جعبه ای است که توسط آن می توان دستگاه ها و اتصالات را برای قرار دادن در فضای کار انتخاب نمود. این جعبه شامل کادر انتخاب نوع وسیله و کادر انتخاب یک وسیله خاص می باشد.
جعبه انتخاب نوع دستگاه	این جعبه شامل انواع دستگاه ها و اتصالات موجود در Packet Tracer 4.1 می باشد. کادر Device-Specific Selection بر اساس نوع وسیله مورد انتخاب تغییر می کند.
جعبه انتخاب یک دستگاه خاص	کادری است که توسط آن می توان دستگاه یا اتصال مورد نظر شبکه خود را انتخاب نمود.
پنجره بسته های ایجاد شده توسط کاربر	این پنجره بسته هایی که در سناریوهای شبیه سازی در شبکه قرار می گیرند را مدیریت می کند.

پنجره ها را توسط ماوس می توان به راحتی تغییر اندازه داده و همچنین با حرکت دادن آن به سمت راست پنهان نمود.



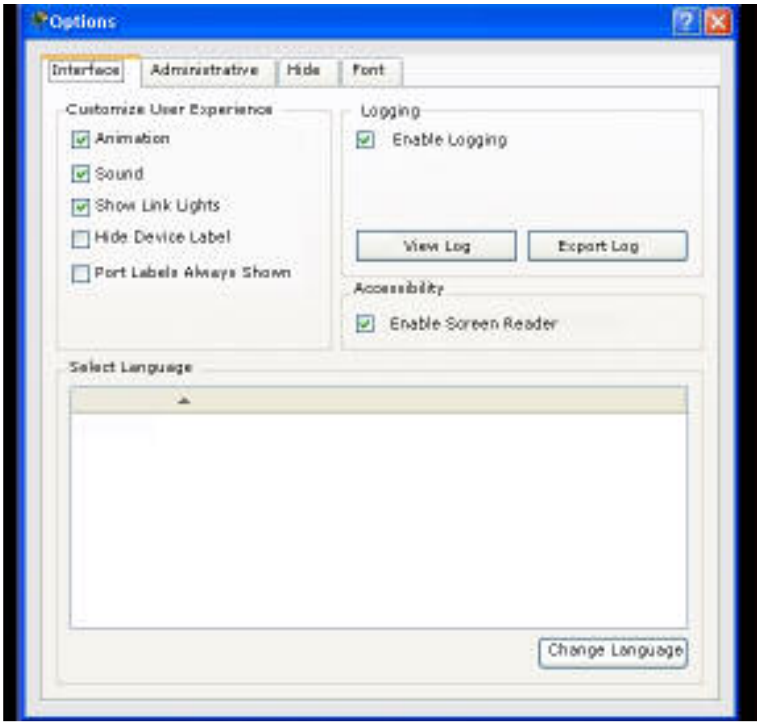
فضاهای کاری و حالت ها

نرم افزار Packet Tracer 4.1 شامل دو فضای کاری منطقی و فیزیکی، و دو حالت Realtime و شبیه سازی است. هر شبکه را می توان در نمای منطقی ایجاد کرده و در حالت real time، اجرای آن را مشاهده نمود. همچنین می توان برای اجرای سناریو های کنترل شده به حالت شبیه سازی سوئیچ نمود. برای تنظیم چیدمان فیزیکی وسایل، به حالت Physical Workspace می توان رفت. ذکر این نکته لازم است که امکان اجرای شبکه در حالت فیزیکی وجود ندشته و باید برای این منظور دوباره به فضای منطقی برگشت.

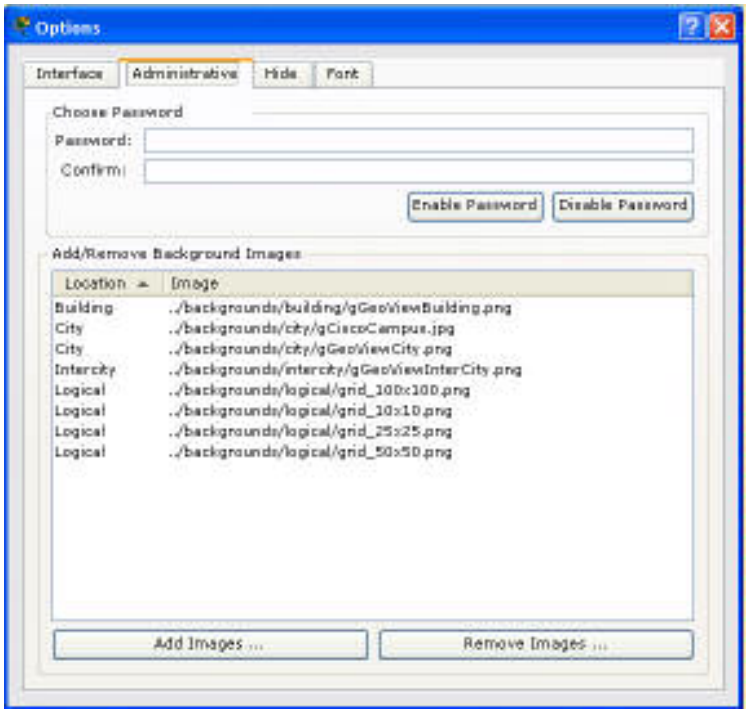
تنظیم علاقه مندی ها

نرم افزار Packet Tracer 4.1 را می توان به دلخواه تنظیم کرد. برای این کار از منوی Option دستور Preferences را اجرا، تا تنظیمات برنامه را مشاهده نمائید.

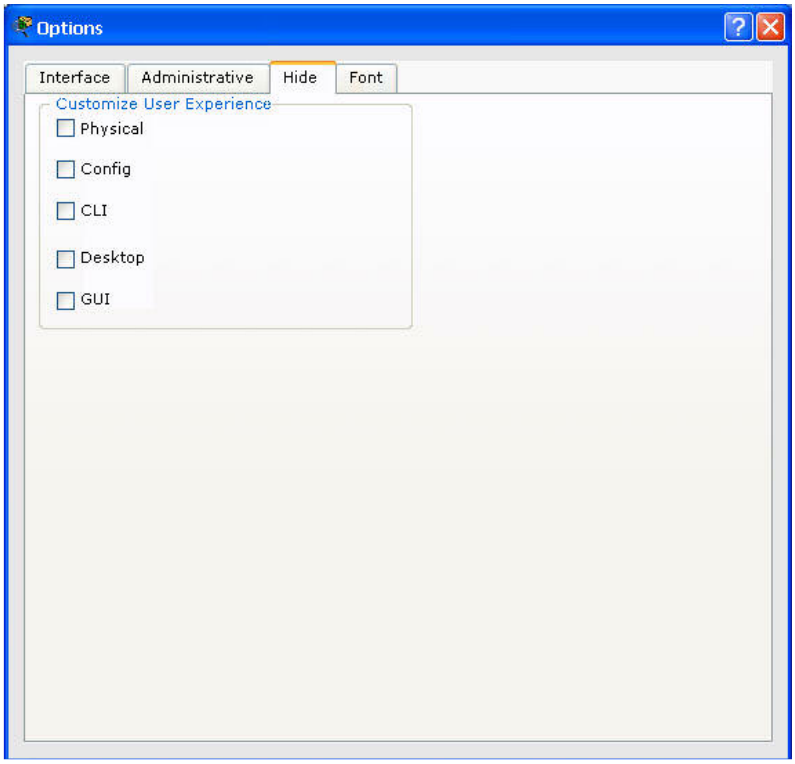
در برگه Interface می توان تنظیمات صدا، انیمیشن و چراغ های اتصال را انجام داده تا با عملکرد سیستم شما متناسب شود. همچنین می توانید برچسب های ابزارها یا پورت ها را نیز مخفی نموده و یا نمایش داد. ویژگی logging امکان ثبت همه دستورات IOS وارد شده را فراهم می کند. ویژگی Enable Screen Reader Support نیز همه عنوان ها و توضیحات پنجره در حال نمایش را می خواند. زبان برنامه را نیز از قسمت Language می توان تغییر داد.



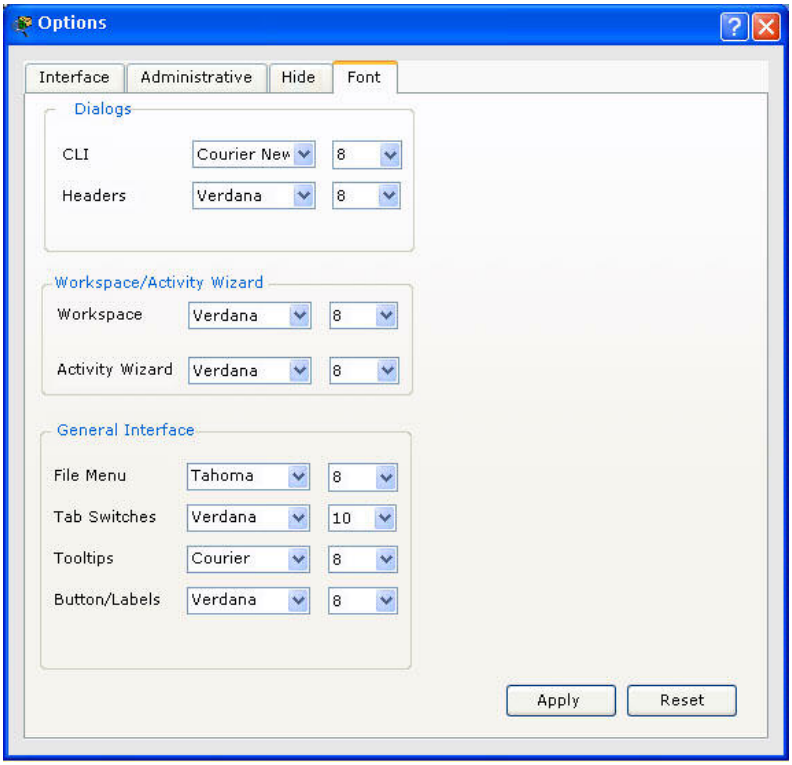
در برگه Administrative تصاویر زمینه ای که در برنامه فعال است را می توان مدیریت نمود. در این برگه امکان تعیین کلمه عبور برای جلوگیری از تغییرات ناخواسته نیز وجود دارد.



در برگه Hide هر یک از موارد مشخص شده را از پنجره برنامه یا کادرهای مختلف، می توان پنهان نمود.

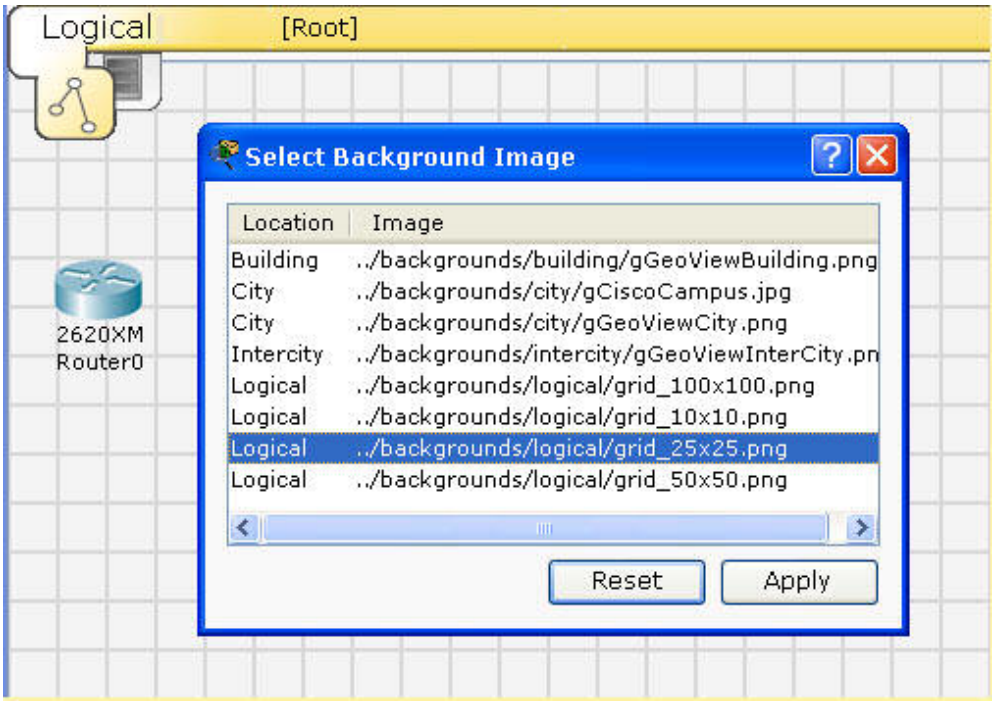


در برگه Font ، نوع و اندازه فونت کادرها و واسط های مختلف تعیین می گردد.



تنظیم پس زمینه

در این بخش می توان یک فضای کاری سفید را با تصویر پس زمینه دلخواه جایگزین نمود. تصویر پس زمینه فقط از تصاویر موجود در برگه Administrative قابل انتخاب است. با کلیک روی دکمه Set Tiled Background در نوار Logical Workspace می توان تصویر زمینه را تنظیم نمود. از لیست تصاویر باز شده تصویر مورد نظر را انتخاب و دکمه Apply را کلیک کنید. برای برگشت به حالت اولیه کافیست دکمه Reset را کلیک کنید.



برای استفاده از تصاویر زمینه دلخواه، می توان آنها را در پوشه background/logical قرار داده و سپس به لیست موجود در برگه Administrative اضافه نمود. توجه کنید که این تصاویر تاثیری در عملکرد شبکه ندارند. قالب پیشنهادی برای این تصاویر png یا bmp (برای ترسیمات یا متن) و jpg (برای تصاویر حقیقی) می باشد.

اصطلاحات مهم

- ICMP Ping: دستوری که شامل یک پیغام تقاضای echo از یک وسیله به وسیله دیگر و پاسخ آن می باشد.
- آدرس IP: همانگونه که قبلا گفته شد یک آدرس۳۲ بیتی است که به دستگاه ها برای شناسایی آنها در شبکه اختصاص داده شده است.

- اترنت: یکی از رایج ترین استانداردهای LAN برای سخت افزار، ارتباطات و کابل کشی می باشد.
- Fast Ethernet Interface: پورت اترنت با سرعت 100 Mbps است.
- مدل OSI: چهارچوب ۷ لایه ای برای بررسی پروتکل های شبکه و دستگاه ها است و شامل لایه های فیزیکی، پیوند داده، شبکه، انتقال، جلسه، ارائه، کاربرد می باشد.
- PDU: واحد داده پروتکل، یک گروه از داده متناسب با لایه در مدل OSI
- بسته: واحد داده در لایه سوم OSI که به صورت یک پاکت نامه در حالت Simulation نمایش داده می شود.
- جداول: شامل جداول مسیریابی، سوئیچینگ و ARP که شامل اطلاعات مرتبط با دستگاه و پروتکل های شبکه هستند.
- جدول ARP: جدول Address Resolution Protocol جفت آدرس IP و آدرس MAC کارت شبکه اترنت را ذخیره می کند.
- سناریو: یک توپولوژی با مجموعه ای از PUD ها که در شبکه قرار می دهید تا در زمان خاصی ارسال شوند. با استفاده از سناریو ها مختلف می توانید ترکیبات و حالت مختلف ارسال بسته ها را در یک توپولوژی یکسان بررسی کنید.

ایجاد اولین شبکه

ایجاد شبکه را با تنظیم تصویر زمینه به حالت مشبک از طریق دکمه Set Tiled Background شروع کنید

Generic PC را از End Devices انتخاب و آن را در فضای کاری قرار دهید.

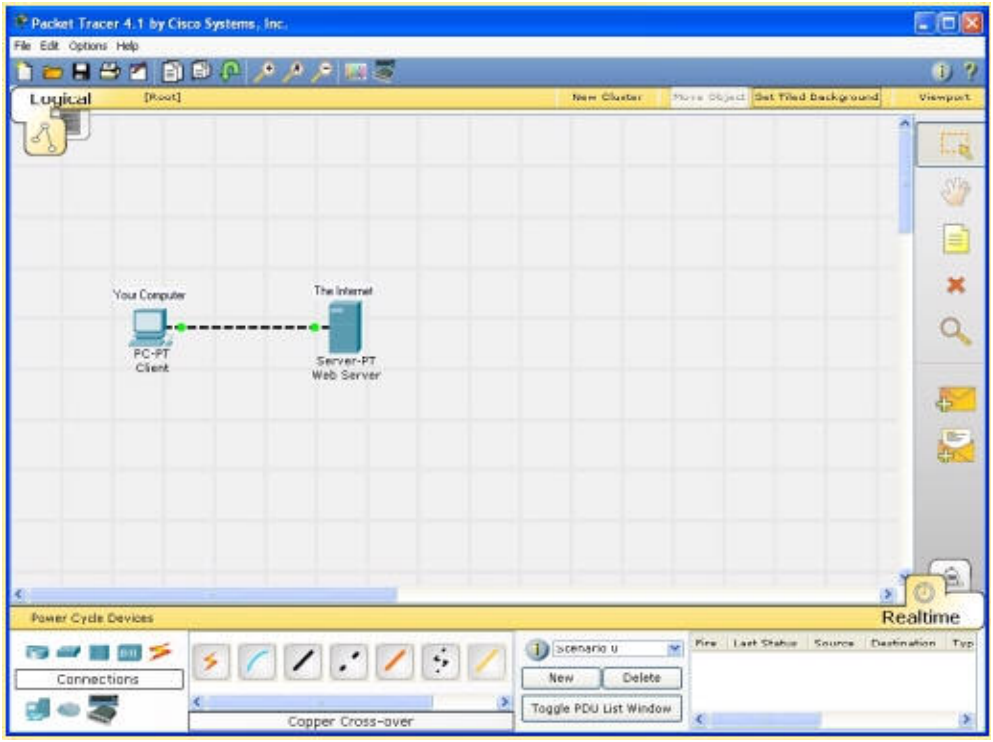
سه روش برای کسب اطلاعات بیشتر در مورد این وسیله وجود دارد. اول این که نشانگر ماوس را روی وسیله قرار داده تا اطلاعات پایه پیکربندی آن را مشاهده گردد. دوم این که با ابزار Select روی آن کلیک تا پنجره تنظیمات آن باز شود. سوم این که از ابزار Inspect استفاده کنید تا جداولی که این وسیله ایجاد می کند را مشاهده کنید. مثلا در مورد این وسیله، جدول ARP نمایش داده خواهد شد. همیشه به خاطر داشته باشید که پس از مشاهده جداول، برای این که فضای کاری شلوغ نشود، آنها را ببندید.

پنجره تنظیمات PC را باز کنید و با رفتن به برگه Config تنظیمات آن ، همچون نام آن را تغییر دهید. در قسمت Interface روی FastEthernet کلیک و آدرس IP را به صورت 192.168.1.1

تنظیم کنید. مطمئن شوید که وضعیت پورت On است. سایر ویژگی ها نظیر ماسک شبکه، آدرس MAC ، پهنای باند و duplex نیز در هر زمان در این قسمت قابل تغییر است.

رایانه دیگری را به فضای کار اضافه کنید. آدرس IP آن را 192.168.1.2 قرار داده و مطمئن شوید وضعیت پورت آن On است.

در قسمت Connections، کابل Copper Straight-through (خط مشکی) را انتخاب و اتصال بین این دو رایانه را برقرار کنید. خط قرمز نشان دهنده این است که اتصال کار نمی کند. حالا با استفاده از ابزار Delete این اتصال را حذف و از کابل Copper Crossover به جای آن برای برقرار ارتباط استفاده کنید. چراغ های سبز باید روشن شوند و اگر ماوس را روی هر یک از رایانه ها قرار دهید، می بایست وضعیت اتصال را به صورت up مشاهده کنید. شبکه شما باید شبیه تصویر باشد.



دستگاه ها را با درگ کردن جابجا کنید. با استفاده از دکمه i در گوشه بالا سمت راست نرم افزار، یک توضیح کلی ایجاد نمایید. سپس تعدادی برچسب متنی با استفاده از ابزار Place Note در Logical Workspace اضافه کنید.

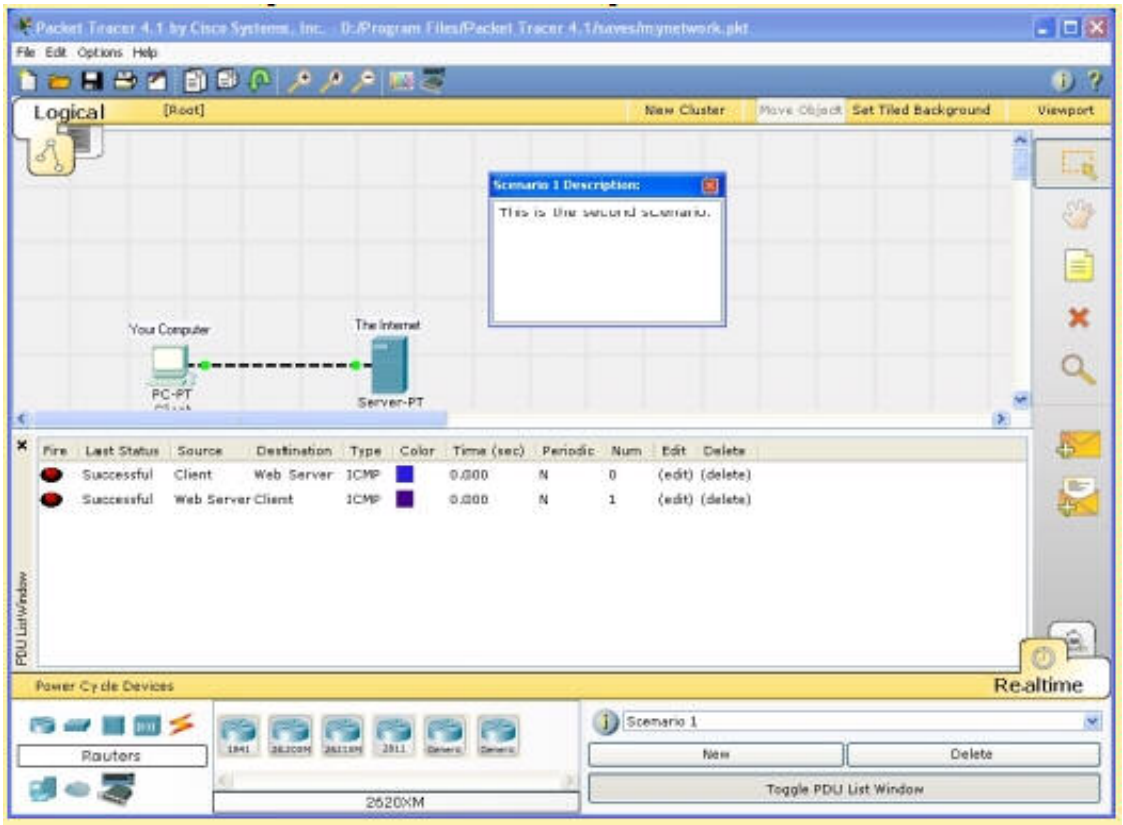
روی رایانه اول یک بار کلیک نموده و در حالی که وضعیت چراغ های اتصال را مشاهده می کنید، رایانه را خاموش و سپس روشن نمایید.

همین کار را برای رایانه دوم نیز انجام دهید. مشاهده می کنید که خاموش کردن رایانه سبب قرمز شدن چراغ اتصال می شود که به معنای down شدن اتصال است.

با استفاده از دستور Save as در منوی File می توان شبکه خود را ذخیره نمود.
به این ترتیب اولین شبکه با موفقیت ایجاد می گردد.

ارسال پیغام های ساده در حالت Real Time

کار خود را با باز کردن شبکه قبل ادامه دهید.
دقت کنید که در حالت Real Time قرار داشته باشید. با استفاده از ابزار Add Simple PDU یک بسته Ping ساده از یک رایانه به رایانه دیگر ایجاد کنید.
در پنجره User Created Packet پیمایش کنید تا حالت های مختلف این پیغام Ping را مشاهده کنید. از جمله، موردی که نشان می دهد Ping موفقیت آمیز بوده است[1].
به روش مشابه، روی دکمه toggle the PDU List Window کلیک، تا پنجره را بزرگتر مشاهده نمایید. می توان یک یا چند مورد از این پیغام ها را به عنوان یک سناریو ذخیره نمود.
روی New کلیک کرده تا سناریوی جدیدی ایجاد شود. سناریوی جدید در ابتدا خالی خواهد بود.
با استفاده از ابزار Simple PDU دو بسته جدید از هر رایانه به رایانه دیگر ایجاد کنید.

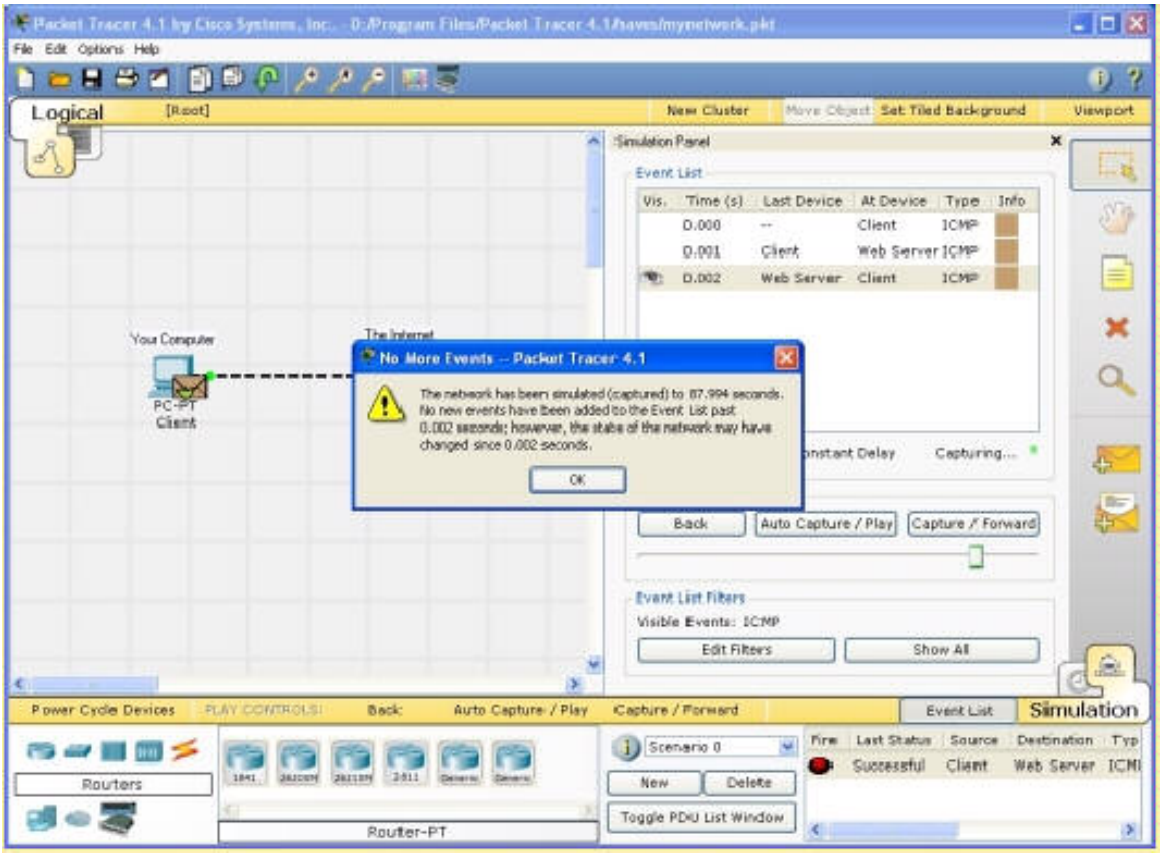


[1] - Successful

بین دو سناریو سوئیچ نمایید تا حالت های مختلف را مشاهده کنید.
سناریوی دوم را با استفاده از دکمه Delete حذف کنید.
حالا در Scenario 0 قرار دارید. اگر قصد حذف PDU را داشته باشید، باید در پنجره User Created Packet پیمایش کنید و دکمه Delete در آخرین ستون را کلیک کنید.
به این ترتیب شما با موفقیت توانستید در حالت Real Time بسته ارسال و آنها را مدیریت کنید.

ثبت رویداد ها و مشاهده انیمیشن در حالت شبیه سازی

کار را با باز کردن فایل قبلی ادامه دهید.
در حالت Real Time یک بسته ساده از رایانه اول به رایانه دوم ارسال کنید.
PDU را حذف نمایید.
به حالت Simulation سوئیچ کنید. در این حالت زمان حرکت نمی کند. بنابراین شما می توانید شبکه را در مراحل آرام تری اجرا و مشاهده نموده و مسیرهایی که بسته طی می کند را به همراه جزئیات آن ها مشاهده کنید.
در Event List Filters روی All/None کلیک نموده تا همه فیلدها غیرفعال شوند. سپس روی ICMP کلیک کنید تا تنها بسته های ICMP در انیمیشن قابل مشاهده باشند.
یک بسته PDU ساده از بسته اول به بسته دوم ایجاد کنید. دقت کنید که بسته جدید به لیست بسته های ایجاد شده توسط کاربر اضافه می شود. این بسته در اولین رویداد در لیست رویدادها ثبت می شود و یک آیکن پاکت نامه در فضای کاری نشان داده خواهد شد. آیکن چشم در سمت چپ Event List نشان دهنده این است که بسته در حال حاضر در حال نمایش است.
روی دکمه Capture/Forward یک بار کلیک کنید. به این ترتیب رویداد دوم که در شبکه اتفاق می افتد ثبت می شود. دقت کنید که پس از کلیک بر روی این دکمه، پاکت نامه در فضای کاری از یک وسیله به دیگری حرکت می کند (این پیغام ICMP echo است).
سرعت انیمیشن را با حرکت دادن لغزنده Play Speed به سمت راست افزایش دهید.
برای بار دوم روی Capture/Forward کلیک کنید. رویداد بعدی شبکه ثبت خواهد شد (پاسخ echo).
دوباره روی Capture/Forward کلیک کنید. در این حالت چون بسته دیگر وجود ندارد، کادر No More Events نمایش داده خواهد شد.

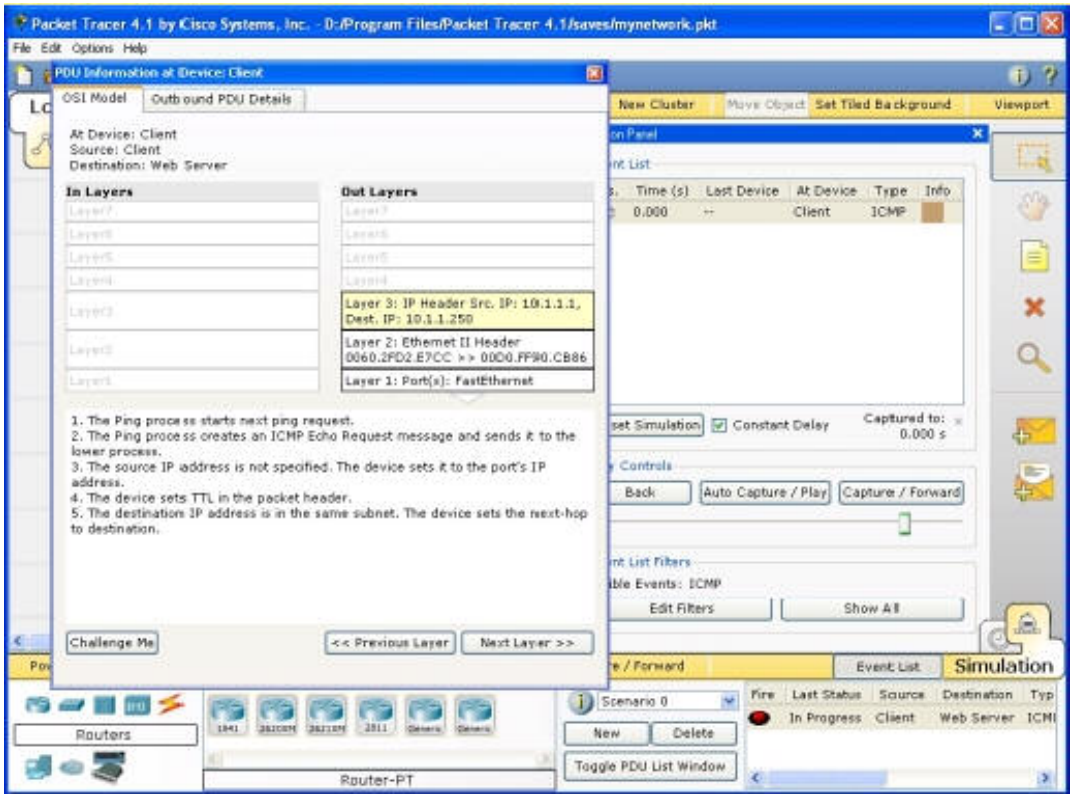


به این ترتیب با موفقیت رویداد ها را ثبت کرده و انیمیشن ها را در حالت شبیه سازی مشاهده نموده اید.

مشاهده داخل بسته ها در حالت شبیه سازی

فعالیت قبلی را ادامه دهید. روی Reset Simulation کلیک کنید. تمام Event List بجز بسته اصلی پاک خواهد شد.

روی پاکت نامه در فضای کاری کلیک کنید تا پنجره اطلاعات PDU نمایش داده شود. این پنجره شامل برگه OSI Model است که چگونگی پردازش بسته را در هر لایه OSI در وسیله فعلی نمایش می دهد. این پنجره را ببندید و دقت کنید که بسته در لیست رویدادها با آیکن چشم نمایش داده شده است. روی مربع رنگی در ستون Info این ردیف کلیک کنید. این کار معادل کلیک کردن مستقیم بر روی پاکت نامه است.



از دکمه های Next Layer و Previous Layer برای مشاهده جزئیات پردازش بسته در لایه های مختلف استفاده کنید. باید به این نکته توجه داشت که فقط Out Layers قابل مشاهده است.

روی برگه Outbound PDI Details کلیک کنید. این برگه دقیقا سرآمد PDU را نمایش می دهد.

پنجره PDU Information را ببندید. یک بار روی دکمه Capture/Forward کلیک کنید.

دوباره روی بسته در فضای کاری کلیک کنید تا پنجره باز شود. (دقت کنید که این بار اطلاعات In Layers و Out Layers با هم قابل مشاهده است)

روی برگه Inbound PDU Details کلیک کنید. در این حالت جزئیات درخواست echo ورودی نمایش داده شده است. اگر روی برگه Outbound PDU Details کلیک کنید، اطلاعات مشابهی نمایش داده خواهد شد، اما این بار شامل بسته پاسخ echo است.

دوباره روی Reset Simulation کلیک کنید. این بار روی Capture/Play کلیک کنید. ارسال پیغام echo و ارسال پاسخ echo به طور اتوماتیک ثبت می شود و در انتها پنجره No More Events نمایش داده می شود.

روی دکمه Back دوبار کلیک کنید تا هر بار انیمیشن یک مرحله به عقب برود. حالا روی دکمه Capture/Forward دوبار کلیک کنید تا بسته دوباره به جلو حرکت داده شود. به رویدادهایی که مشخص می گردند دقت کنید.

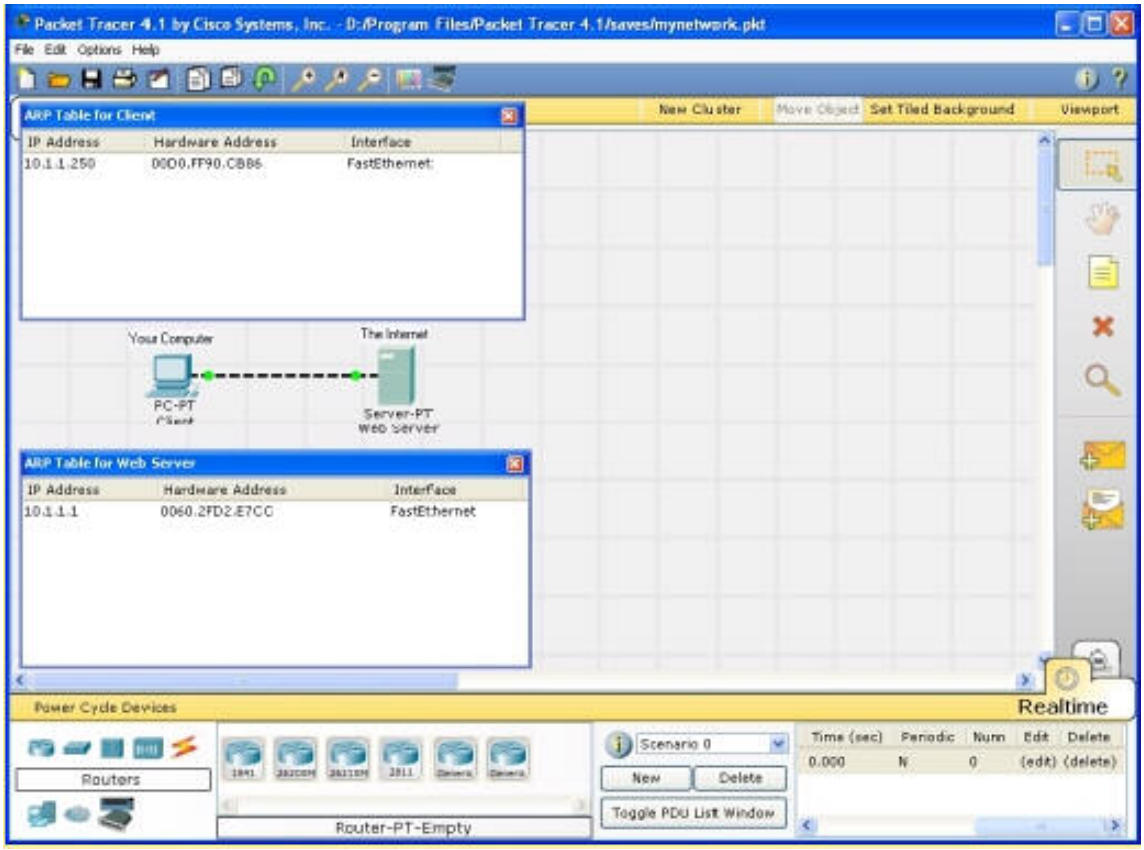
به این ترتیب شما با موفقیت توانستید داخل یک بسته را مشاهده کنید، منطقی را که دستگاه ها در زمان پردازش بکار میگیرند مشاهده و پخش انیمیشن را به دلخواه مدیریت نمایید.

مشاهده جدول دستگاه ها و تنظیم مجدد شبکه

کار را با بستن فضای کار فعلی و بازکردن فایل اصلی که قبلا ذخیره کرده اید شروع می کنیم.

با استفاده از ابزار Inspect، جدول ARP دو رایانه را مشاهده کنید. جداول ARP همیشه در نقطه یکسانی ظاهر می شوند. یکی از آنها را جابجا کنید تا هر دو قابل مشاهده شوند. برای دید بهتر می توانید آنها را تغییر اندازه دهید.

در حالت Real Time یک بسته PDU از یک رایانه به دیگری ارسال کنید. مشاهده می کنید که جداول ARP به طور خودکار پر می شوند.



PDU را حذف کنید. مشاهده می کنید که جدول ARP پاک نمی شود. به این دلیل که ورودی های ARP هم اکنون در رایانه ها ذخیره شده است و حذف PDU ها آنچه که در شبکه اتفاق افتاده است را reset نمی کند.

بر روی Power Cycle Devices کلیک کنید تا شبکهReset شود. به این ترتیب که تمام دستگاه ها خاموش و سپس روشن می شوند و اطلاعات موقت آنها و جداولی که یادگرفته اند پاک می شود.
به حالت Simulation بروید. در Event List Filters مطمئن شوید که ICMP و ARP فعال هستند.
بسته PDU دیگری ایجاد کنید.
با توجه به این که اخیرا شبکه reset شده است، جداول ARP خالی هستند. بنابراین لازم است قبل از ارسال بسته های Ping، بسته های تقاضای ARP ارسال شوند تا رایانه ها از وجود همدیگر مطلع شوند. روی Auto Capture/Play کلیک کنید تا انیمیشن را مشاهده کنید.
روی Reset Animation کلیک کنید. مشاهده می کنید که لیست رویدادها پاک می شوند (بجز PDU های ایجاد شده توسط کاربر) ، ولی جداول ARP هنوز پر هستند. روی Capture/Play کلیک کنید. در این زمان، با توجه به این که جداولARP قبلا پر هستند، دیگر بسته ARP ارسال نمی شود.
اگر شبکه را Reset کنید، بسته های ARP جدید به طور خودکار در لیست رویدادها ظاهر خواهند شد.
به این ترتیب شما توانسته اید جداول دستگاه ها را مشاهده کنید و نیز شبیه سازی و شبکه را reset کنید.

مرور مطالب

یک بار کلیک بر روی دکمه Delete کل یک سناریو با همه PDU های آن را حذف خواهد کرد.
دوبار کلیک بر روی Delete در آخرین ستون در پنجره PDU List بسته ها را حذف خواهد کرد.
دکمه Reset Simulation همه محتوای Even List ، بجز PDU های ایجاد شده توسط کاربران را حذف خواهد کرد و به شما امکان مشاهده مجدد انیمیشن را می دهد ولی جداول دستگاه ها را پاک نمی کند.
دکمه Reset Network همه دستگاه ها را خاموش، و دوباره روشن خواهد کرد. به این ترتیب جداول دستگاه ها و نیز تنظیماتی که ذخیره نشده است از بین خواهد رفت.
با ذخیره کردن فایل در فواصل معین، می توانید از حذف شدن تنظیمات و تغییراتی که در شبکه می خواهید نگه دارید جلوگیری کنید.
حال شما آماده هستید تا شبکه های مختلفی را در نرم افزار Packet Tracer 4.1 ایجاد و تحلیل کنید. ویژگی های بسیار دیگری وجود دارد که در ادامه شرح داد خواهد شد.

۴۱-۲- فضاهای کار فیزیکی و منطقی

نرم افزار Packet Tracer 4.1 شامل دو الگوی نمایشی برای شبکه است: فضای منطقی و فضای فیزیکی. فضای منطقی به شما امکان ایجاد توپولوژی منطقی شبکه را بدون در نظر گرفتن مقیاس فیزیکی و چیدمان آن می دهد. فضای فیزیکی به شما امکان چیدن دستگاه ها به صورت فیزیکی در شهرها، ساختمان ها و فضاهای سیم بندی را می دهد. مسافت ها و دیگر اندازه های فیزیکی در عملکرد شبکه و دیگر مشخصه های آن تاثیر خواهد گذاشت. در این نرم افزار شما باید ابتدا شبکه منطقی را ایجاد کنید و سپس آن را در فضای فیزیکی مرتب نمایید.

۴۱-۳- فضای کار منطقی

فضای کار منطقی جایی است که شما بیشتر زمان خود را برای ایجاد و پیکربندی شبکه در آن سپری می کنید. در ترکیب با حالت Realtime می توانید از این فضا برای تکمیل بسیاری از آزمایش های دوره CCNA استفاده کنید.

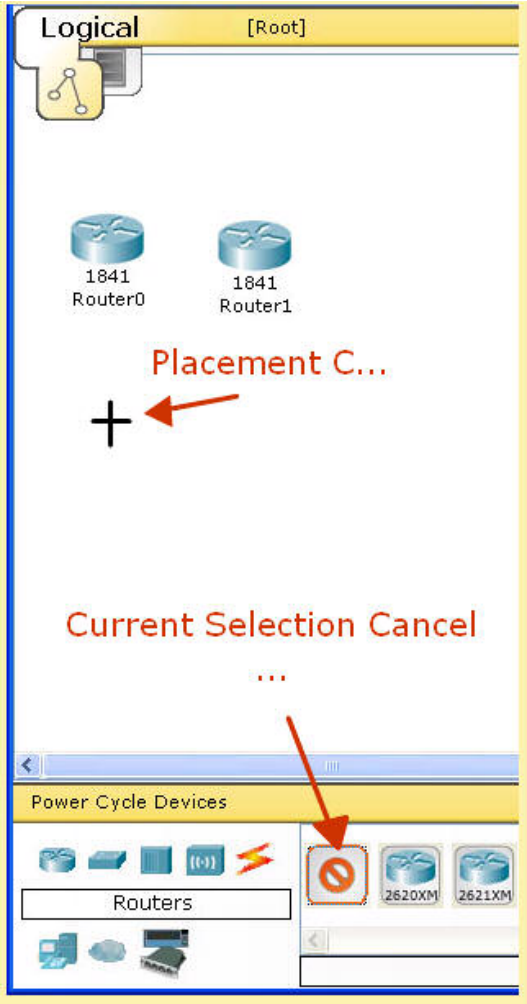
ابتدا شما باید دستگاه ها را ایجاد کنید. این کار با انتخاب دستگاه از کادر Network Component انجام می شود. سپس می توانید هر یک از موارد زیر را انجام دهید:

- افزودن ماژول جدید به دستگاه ها برای دستیابی به واسط های بیشتر (دقت کنید که قبل از افزودن ماژول باید دستگاه را با کلیک بر روی دکمه Power خاموش کنید)
- اتصال دستگاه ها به همدیگر با انتخاب کابل مناسب.
- پیکربندی های پارامترهای دستگاه ها (نظیر نام و آدرس IP) در کادرهای گرافیکی یا با استفاده از دستورات IOS سیسکو (در مورد مسیریاب ها و سوئیچ ها)
- ایجاد تنظیمات پیشرفته و مشاهده اطلاعات شبکه از واسط CLI مسیریاب یا سوئیچ

ایجاد دستگاه ها

برای قرار دادن یک دستگاه در فضای کار، ابتدا نوع دستگاه را از کادر Device-Type Selection انتخاب و سپس روی مدل مورد نظر از قسمت Device-Specific Selection کلیک کنید. در نهایت روی مکانی از فضای کار که می خواهید دستگاه را قرار دهید کلیک کنید. برای انصراف از انتخاب، روی آیکن Cancel همان دستگاه کلیک کنید. به روش دیگر شما می توانید ایجاد وسیله را با

کشیدن و انداختن آن به داخل فضای کار انجام دهید. همچنین اگر دستگاه ها را از کادر DeviceType Selection دراگ نمایید، مدل پیشفرض انتخاب خواهد شد.



برای ایجاد تعداد زیادی از یک وسیله یکسان، دکمه Ctrl را نگه داشته و روی دستگاه مورد نظر کلیک کنید و سپس دکمه Ctrl را رها کنید. به این ترتیب وسیله مورد نظر قفل خواهد شد و شما می توانید چندین بار در فضای کار کلیک نمایید تا کپی های زیادی از آن ایجاد شود. برای انصراف از عملیات روی آیکن Cancel کلیک کنید. برای تکثیر یک دستگاه می توانید دکمه Ctrl را نگه داشته و دستگاه مورد نظر را فضای کاری دراگ کنید یا این که از Copy و Paste استفاده کنید.

ایجاد دستگاه های سفارشی

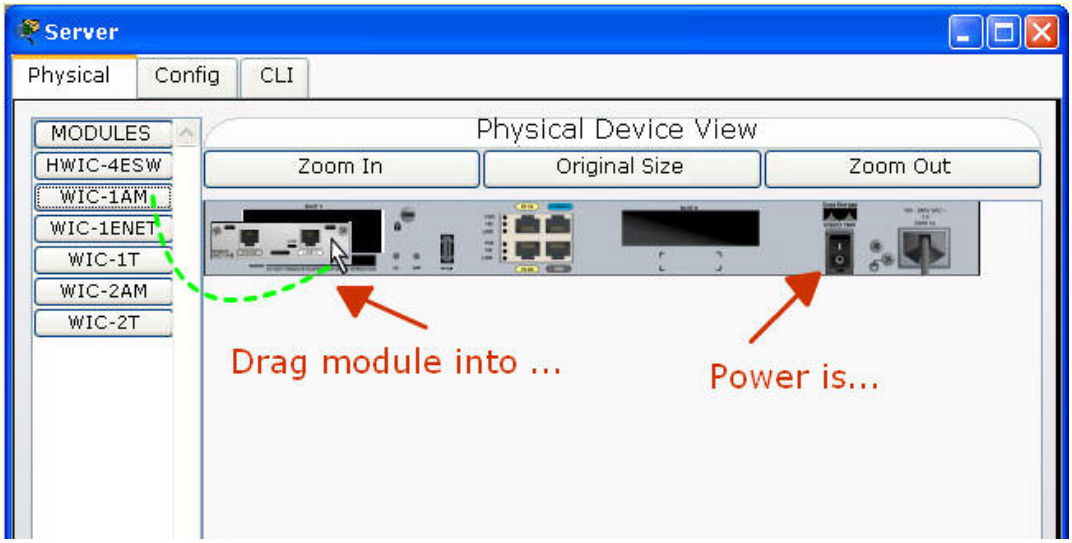
دستور Device Template Manager به شما امکان ذخیره کردن دستگاه ها را بعنوان الگوهایی فراهم می کند تا بعدا بتوانید از این الگوها برای ایجاد دستگاه های دلخواه خود استفاده کنید. مثلا فرض کنید که می خواهید الگویی از مسیریاب 2621XM با یک ماژول NM-2FE2W و دو ماژول WIC-2T ایجاد کنید. بنابراین ابتدا مدل مورد نظر را در فضای کار ایجاد کنید و ماژول ها دلخواه را به آن اضافه نمایید. سپس روی Custom Device Dialog در نوار منوی اصلی کلیک کنید. پس از انتخاب دکمه Select در کادر بازشده، روی وسیله مورد نظر کلیک کرده و سپس توضیحی را برای

آن اضافه کنید. در نهایت روی دکمه Add کلیک کنید و در کادری که باز می شود الگوی خود را در پوشه template در مسیر نصب برنامه ذخیره نمایید.

برای استفاده از این الگو در نمای منطقی روی آیکن Custom Made Device در کادر انتخاب نوع دستگاه کلیک کنید. به این ترتیب دستگاه های سفارشی شما ظاهر خواهد شد. حال می توانید همه الگوهای ایجاد شده را پیدا کنید و سپس آنها را به فضای کار اضافه کنید. برای حذف یک دستگاه سفارشی روی دکمه Custom Devices Dialog در نوار ابزار اصلی کلیک کرده و پس از انتخاب الگوی مورد نظر از قسمت Edit، دکمه Remove را کلیک کنید.

افزودن ماژول ها

اکثر دستگاه های Packet Tracer 4.1 محفظه های ماژولار دارند که شما می توانید ماژلها را در آنها قرار دهید. در فضای کار، روی یک دستگاه کلیک کنید تا پنجره پیکربندی های آن نمایش داده شود. به طور پیش فرض شما در برگه Physical خواهید بود. یک تصویر محاوره ای از وسیله نیز در سمت راست و لیستی از ماژول های سازگار با آن در سمت چپ قرار دارد. شما می توانید تصویر را با دکمه های Zoom in ، Original Size و Zoom out تغییر اندازه دهید. همچنین می توانید در لیست ماژول ها پیمایش کرده و توضیحات و اطلاعات آنها را در کادر پایین مطالعه کنید. وقتی ماژول مورد نظر را پیدا کردید آن را از لیست روی محفظه سازگار با آن در تصویر دراگ کنید. با دراگ مجدد یک ماژول به این لیست، امکان حذف آن نیز وجود دارد.

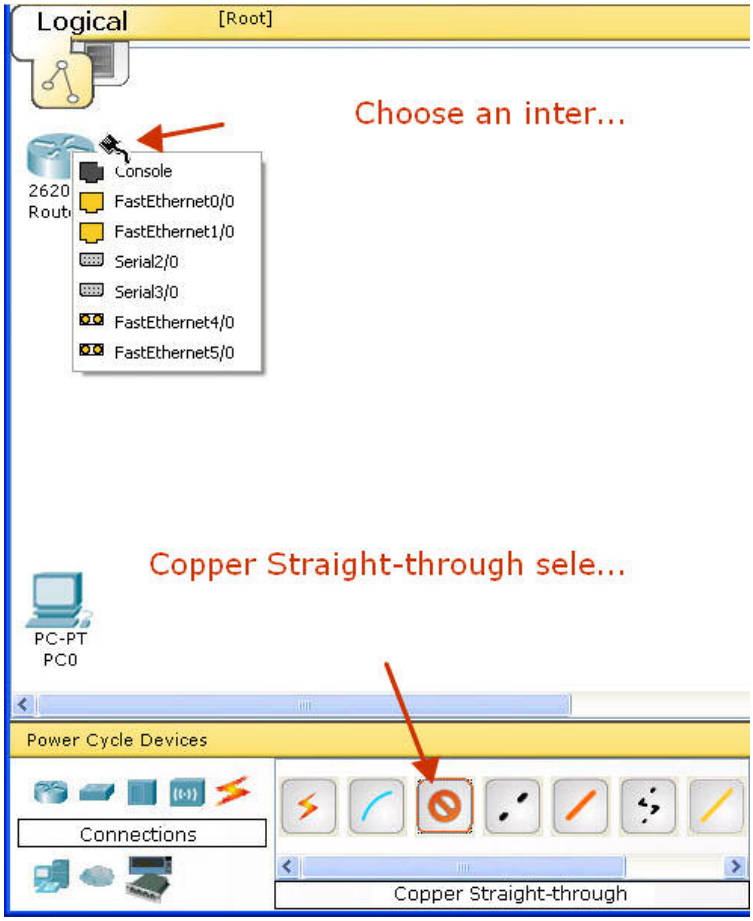


دقت کنید که قبل از افزودن یا حذف ماژول، باید دستگاه را خاموش کنید و پس از انجام کار مجددا آنرا روشن نمایید.

ایجاد اتصالات

برای ایجاد یک اتصال بین دو دستگاه، ابتدا روی آیکن Connections در کادر انتخاب نوع وسیله کلیک نمایید تا لیستی از انواع اتصالات موجود نمایش داده شود. سپس روی نوع کابل مورد نظر کلیک کنید. نشانگر ماوس به شکل اتصال تغییر خواهد کرد. روی اولین وسیله کلیک کرده و واسط مناسب با کابل را انتخاب کنید. روی دومین وسیله نیز کلیک کرده و به همین ترتیب عمل کنید. یک کابل بین دو دستگاه ایجاد خواهد شد و در انتهای آن چراغهایی وجود دارد که وضعیت اتصال را در دو طرف نمایش می دهد.

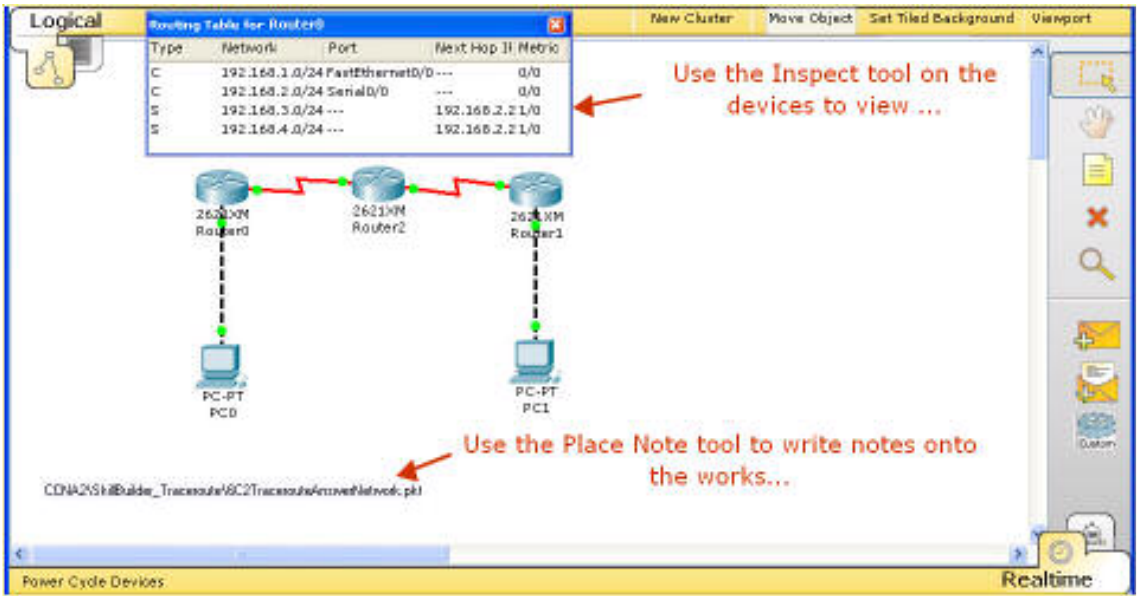
برای ایجاد سریع اتصالات مختلف از نوع یکسان، دکمه Ctrl را نگه دارید و روی اتصال مورد نظر کلیک کنید. سپس دکمه Ctrl را رها کنید تا بتوانید مکرراً از اتصال یکسان بین دستگاه ها استفاده نمایید. برای اتمام عملیات روی آیکن Cancel کلیک کنید.



ابزارهای ویرایش توپولوژی منطقی

شما می توانید از نوار ابزار اصلی ، نوار فضای کار Logical/Physical و نوار ابزار رایج برای ویرایش و نیز افزودن توضیحات به توپولوژی استفاده کنید.

ابزار	کاربرد
Copy	کپی آیتم های انتخاب شده
Paste	الصاق آیتم های کپی شده
Undo	برگرداندن عمل قبلی
Zoom In	بزرگ کردن تصویر
Zoom Reset	تنظیم بزرگ نمایی به حالت پیش فرض
Zoom Out	کوچک کردن فضای کار
Palette	ایجاد خط، مستطیل و بیضی
New Cluster	ایجاد گروه های جدید
Move Object	جابجا کردن اشیاء
Set Tiled Background	تنظیم تصویر پس زمینه
Viewport	مشاهده فضای کار در یک مقیاس کوچک
Select	انتخاب اشیاء
Move Layout	جابجا کردن محتوای فضای کار
Place Note	افزودن توضیح به فضای کار
Delete	حذف اشیاء از فضای کار
Inspect	مشاهده جداول دستگاه ها
Add Simple PDU	افزودن بسته های PDU ساده
Add Complex PDU	افزودن PDU های پیشرفته تر



پیکربندی دستگاه ها

برای استفاده از دستگاه ها، باید برخی تنظیمات پایه نظیر آدرس IP و ماسک شبکه را تنظیم کنید. پارامترهای پایه را می توانید از طریق واسط گرافیکی پیکربندی دستگاه انجام دهید. (روی برگه Config در پنجره پیکربندی دستگاه کلیک کنید). دستگاه های مختلف تنظیمات مختلفی دارند که بعدا شرح داده خواهد شد.

مسیریاب ها و سوئیچ ها Cisco IOS

برای مسیریاب ها و سوئیچ ها شما دسترسی محدودی به IOS های سیسکو دارید. در حالت Realtime می توانید از این نرم افزار برای ایجاد تنظیمات پیشرفته و نیز مشاهده اطلاعات مختلف شبکه استفاده کنید. مثلا دستوراتی نظیر Ping ، traceroute ، show interfaces، ip access-list و switchport access vlan که شرح بیشتری از دستورات بعدا ارائه خواهد شد.

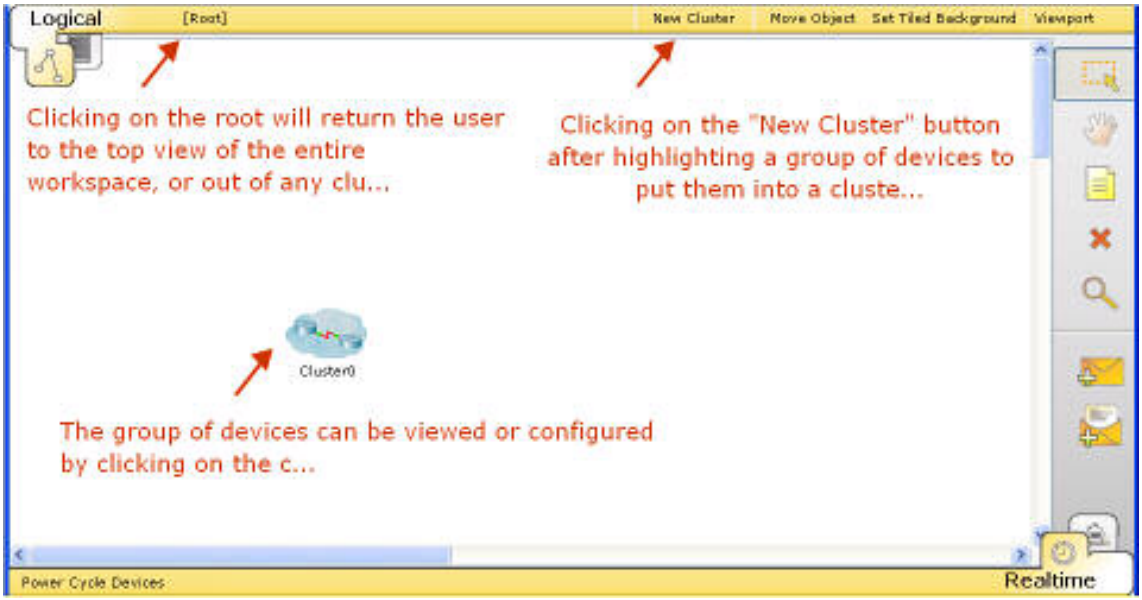
گروه بندی دستگاه ها (Clustering)

گروه بندی دستگاه ها به شما امکان ایجاد ظاهری بهتر از فضای کار با کاهش گروهی از دستگاه ها به یک تصویر را فراهم می کند. به طور پیش فرض همه دستگاه ها در نمای منطقی در سطح ریشه (Root) قرار می گیرند. شما می توانید تعدادی از موارد موجود در صفحه را که سبب آشفتگی فضا می شوند با ایجاد یک گروه جدید در سطح بعدی کاهش دهید. برای این کار دستگاه های مورد نظر را انتخاب کنید و روی New Cluster کلیک کنید. حال می توانید با کلیک بر روی گروه ایجاد

شده وارد آن شوید و نیز گروه های جدیدی داخل آن ایجاد کنید. همچنین می توان یک گروه را تغییر نام داد یا با کلیک بر روی سطح مورد نظر در نوار پیمایش، بین آنها سوئیچ کرد. دقت کنید که در فضای منطقی می توانید تا ۴ سطح گروه ایجاد کنید. برای خارج کردن دستگاه ها از گروه می توانید از ابزار Delete استفاده کنید.

وقتی یک گروه ایجاد شد، می توانید اتصالاتی را به دستگاه های داخل گروه ایجاد کنید. برای اینکار پس از انتخاب اتصال مور نظر روی گروه کلیک کنید تا لیستی از دستگاه های داخل آن را مشاهده کنید که به شما امکان انتخاب دستگاه را می دهد. پس از انتخاب دستگاه مورد نظر می توانید واسط مورد نظر را نیز انتخاب کنید.

همچنین علاوه بر ایجاد گروه، شما می توانید توسط دکمه Move Objet ، دستگاه ها و اشیاء را در بین آنها جابجا کنید. برای اینکار روی دکمه Move Object کلیک کنید و سپس شیء یا دستگاه مورد نظر را انتخاب کنید. منویی ظاهر خواهد که سلسله مراتب سطوح و گروه ها در آن نمایش داده شده است. با انتخاب مکان مورد نظر، شیء به آنجا منتقل خواهد شد.

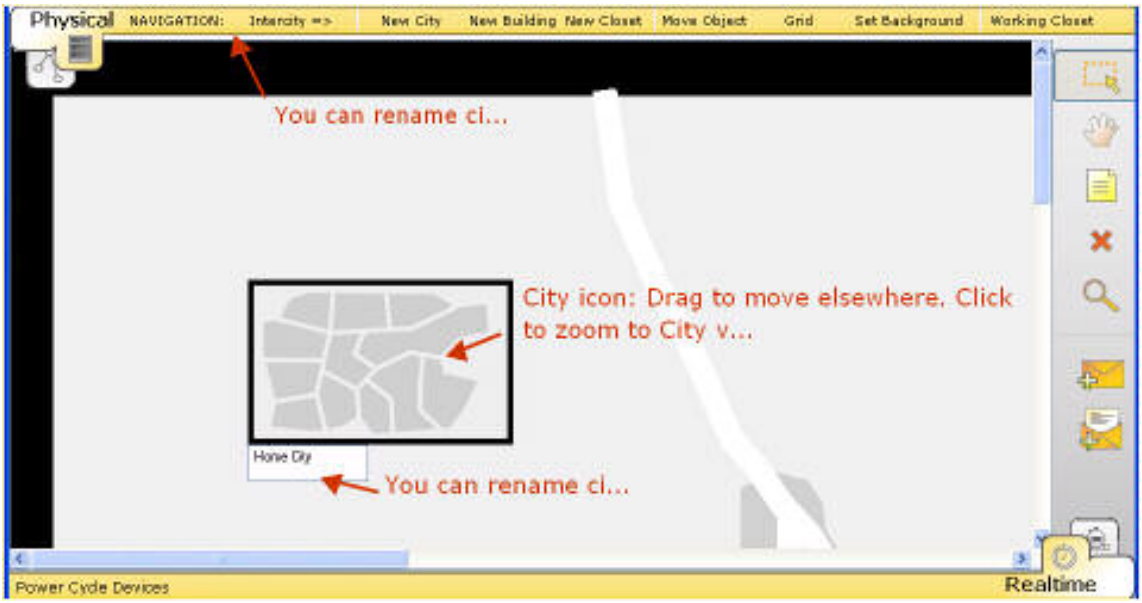


۴۱-۴- فضای کار فیزیکی

فضای کار فیزیکی، بعد فیزیکی توپولوژی شبکه شما را ارائه می دهد. این فضا به شما حسی از مقیاس و مکان و این که در محیط واقعی، شبکه شما چگونه خواهد بود را فراهم می کند.

فضای کار فیزیکی به ۴ لایه تقسیم شده است که مقیاس فیزیکی ۴ محیط را نشان می دهد: بین شهری[۱]، شهر، ساختمان و اتاق سیم بندی[۲]. بزرگترین فضا، بین شهری است که می تواند شامل چندین شهر باشد. هر شهر می تواند شامل ساختمان های متعدد و در نهایت هر ساختمان می تواند شامل اتاق های سیم بندی زیادی باشد. اتاق سیم بندی جایی است که شما واقعا دستگاه های ایجاد شده در فضای منطقی را مشاهده می کنید که در قفسه ها[۳] و روی میزها قرار داده شده اند.

وقتی که اولین بار وارد فضای کار فیزیکی می شود، در نمای Intercity قرار دارید.



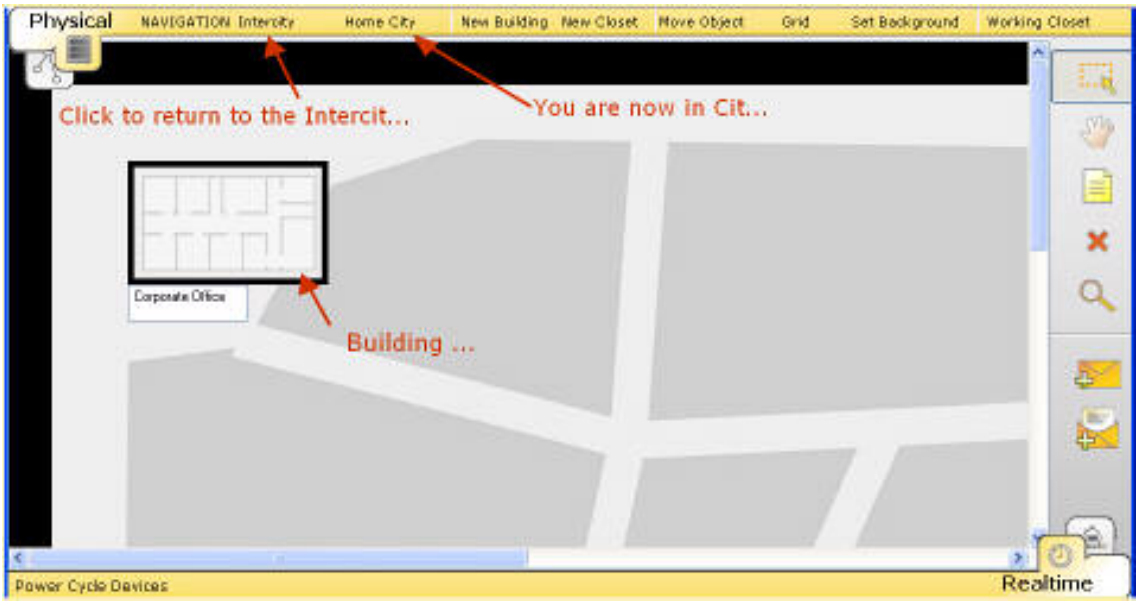
به طور پیش فرض، این فضا شامل یک شهر به نام Home City است. که می توان آن را در روی نقشه جابجا نمود. و نیز می توان به آسانی روی آن کلیک تا نقشه شهر نمایش داده شود.

---

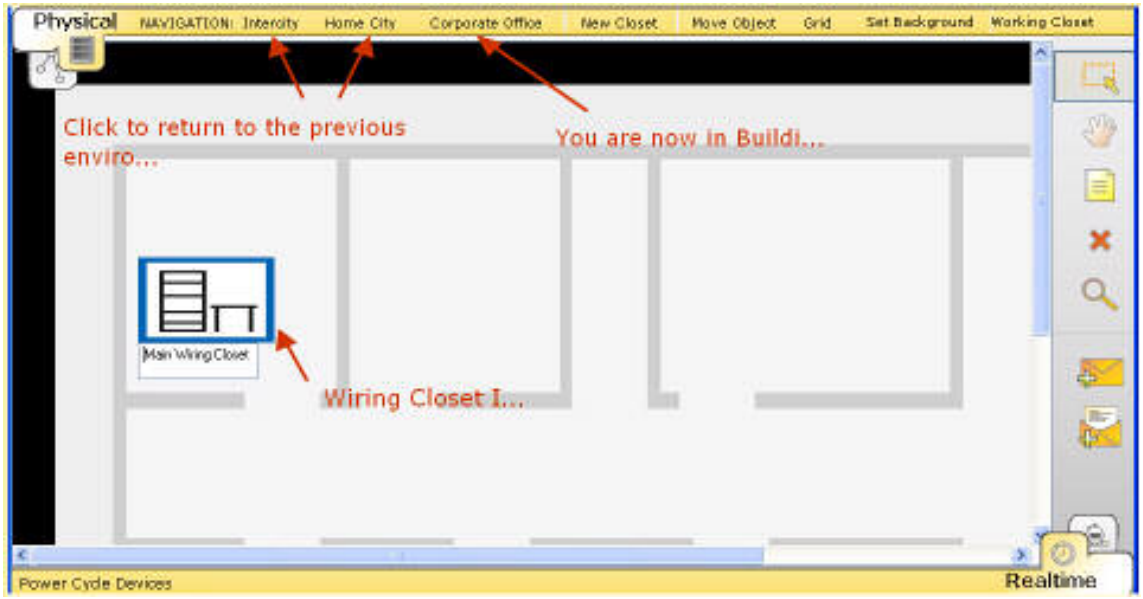
[1]- Intercity

[2]- wiring closet

[3]- Racks



شهر Home City شامل یک ساختمان پیش فرض به نام Corporate Office است. این ساختمان نیز می تواند در شهر جابجا شود. با کلیک برروی آیکن ساختمان، نمای داخلی ساختمان بزرگتر نمایش داده خواهد شد. همه ساختمان ها به یک طبقه محدود هستند. از نمای شهر شما می توانید با کلیک بر روی آیکن Intercity در نوار پیمایش، به محیط بین شهری برگردید.

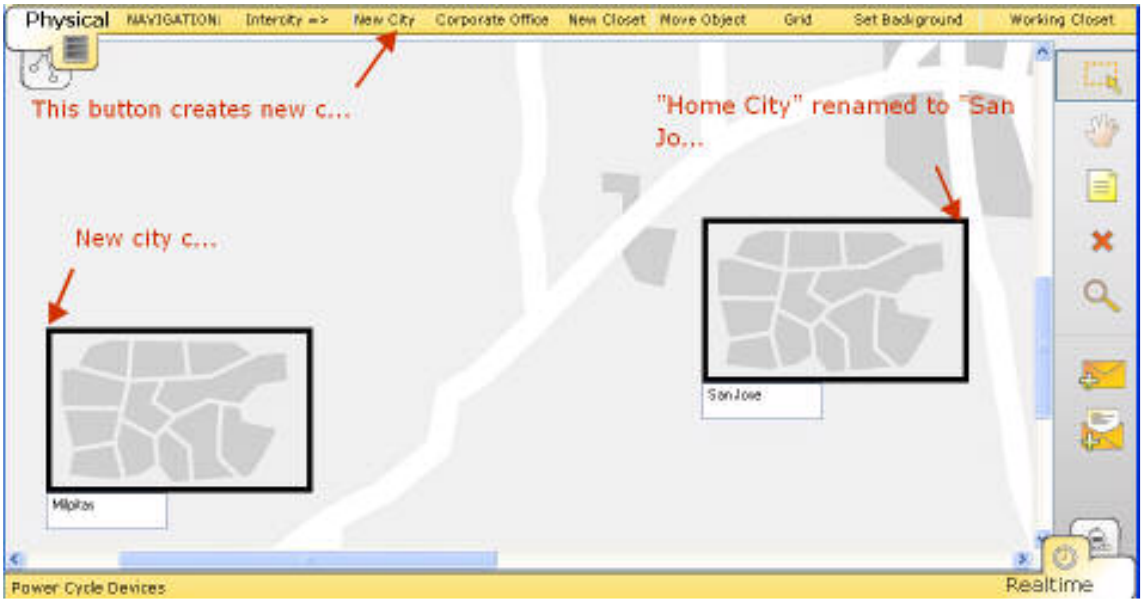


ساختمان Corporate Office شامل یک اتاق پیش فرض به نام Main wiring closet است. با کلیک بر روی آن می توانید محتوای اتاق را مشاهده نموده و سپس توسط نوار پیمایش به هر یک از محیط های قبلی برگردید.

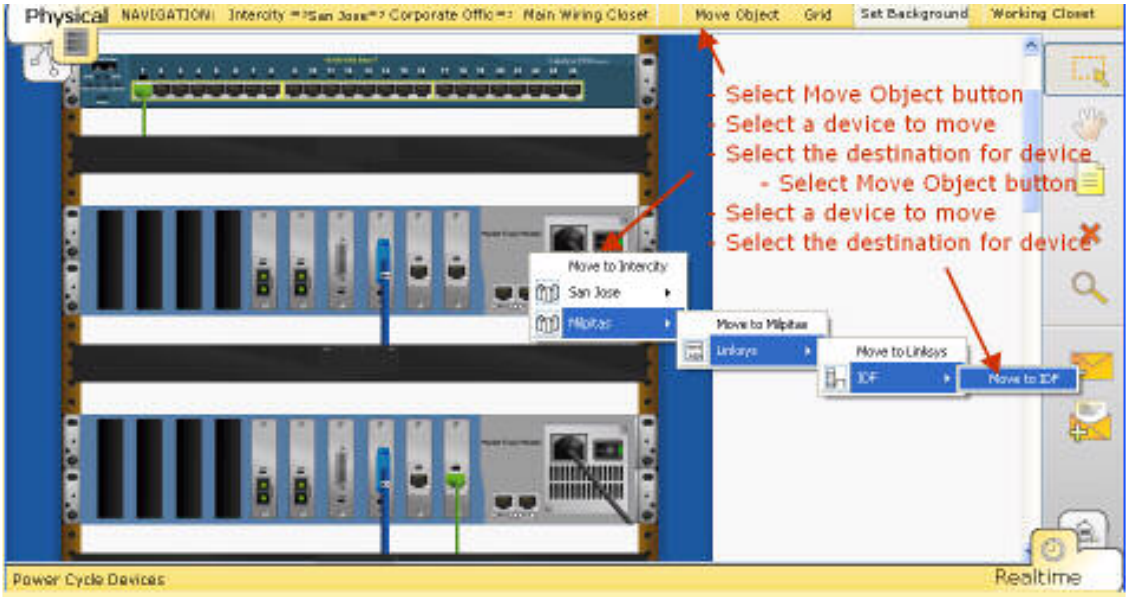
جابجا کردن اشیاء در فضای کار فیزیکی

فضای کار فیزیکی امکان جابجا کردن دستگاه ها به مکان های مختلف را به طراح می دهد. برای توسعه توپولوژی فیزیکی، ابتدا نیازمند ایجاد یک مکان جدید می باشیم. در محیط Intercity می توان توسط دکمه New City یک شهر جدید ایجاد کرد. همچنین امکان ایجاد ساختمان و اتاق سیم بندی نیز در این فضا توسط دکمه های New Building و New Closet وجود دارد. به طور مشابه می توان در محیط شهر، یک ساختمان جدید و در محیط ساختمان، یک اتاق جدید ایجاد کنید.

البته باید دقت کرد که هر شهر، ساختمان و یا اتاق جدیدی که ایجاد می شود، ابتدا در گوشه بالا سمت چپ ظاهر شود. برای جلوگیری از سردرگمی، باید آنها را فورا تغییر نام داده و مکان آنها را تعیین کنید.

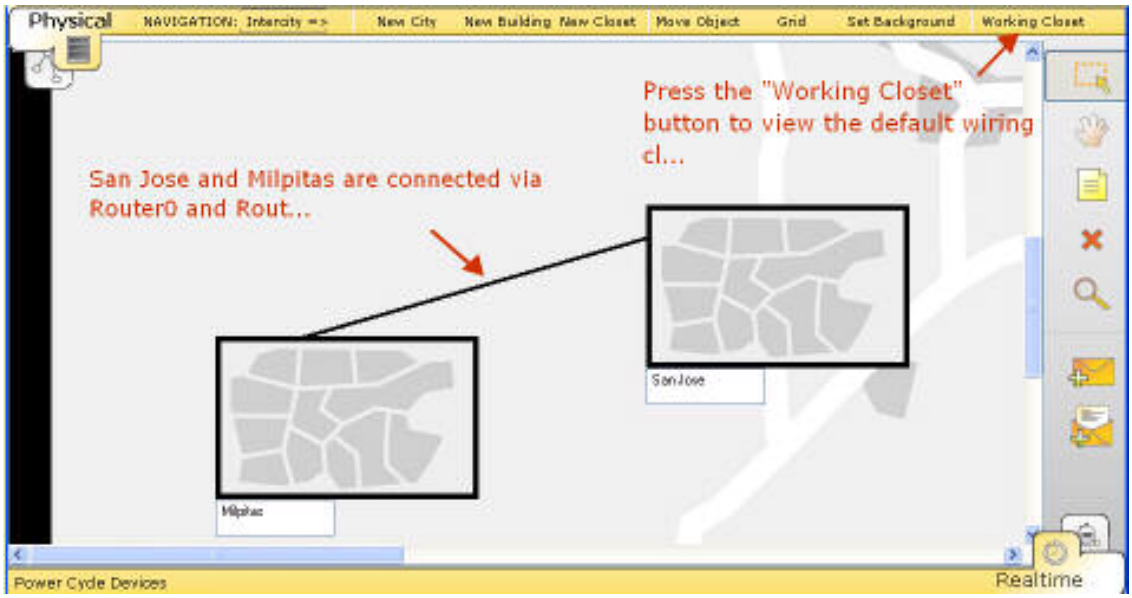


در این مثال، Home City پیش فرض به San Jose تغییر نام داده شده و شهر جدیدی به نام Milpitas نیز ایجاد شده است. داخل شهر San Jose ساختمانی به نام Cisco ایجاد شده است که اتاق سیم بندی به نام MDF دارد. به طور مشابه در داخل Milpitas ساختمان جدیدی به نام Linksys ایجاد شده است که اتاق سیمی بندی به نام IDF دارد. در ابتدا همه دستگاه ها در MDF قرار داده شده اند، از جمله دو مسیریاب به نام های Router0 و Router1 که از طریق پورت سریال به هم متصل شده اند.



برای مثال، برای انتقال Router1 به IDF، ابتدا باید به MDF رفته و روی دکمه Move object کلیک کنید. حال روی Router1 کلیک و سپس در ساختار سلسله مراتبی، IDF را پیدا کنید، آنگاه Move to IDF را انتخاب نمایید. در نمای Intercity خواهید دید که یک خط سیاه بین San Jose و Milpitas ایجاد شده است. این خط نشان دهنده اتصال ایجاد شده بین دستگاه های موجود در این دو شهر است که در این مثال یک اتصال سریال بین دو مسیریاب می باشد.

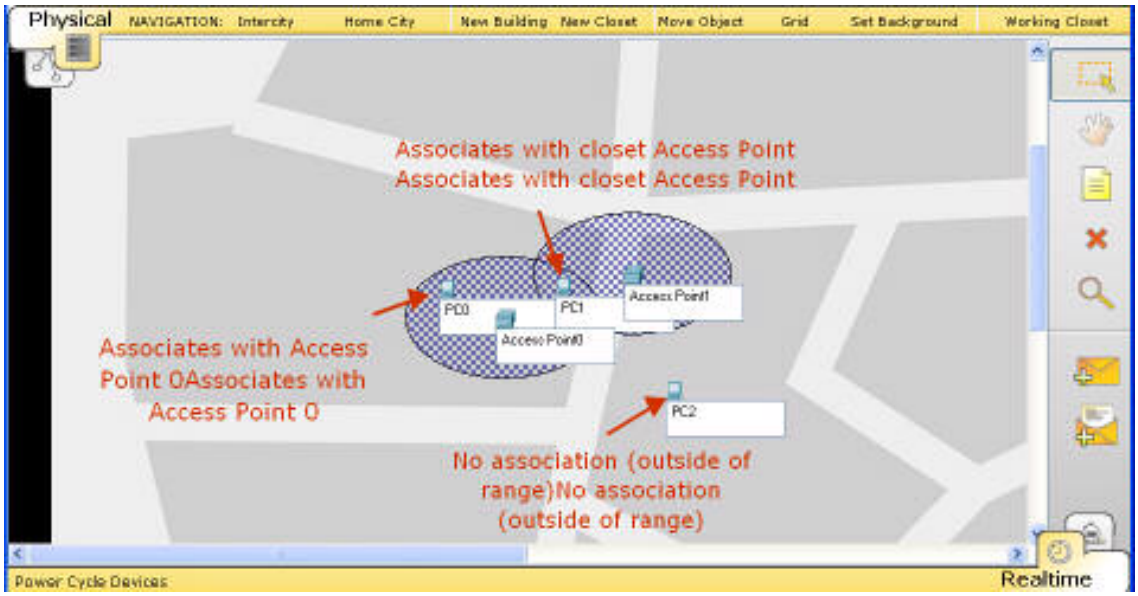
دقت کنید که با کلیک بر روی Working Closet در سمت راست نوار پیمایش می توان، به سرعت به اتاق سیم بندی پیش فرض برگشت.



علاوه بر جابجا کردن دستگاه ها توسط دکمه Move Object، می توان ساختمان ها و اتاق ها را نیز به همین روش جابجا نمود. به روشی دیگر، از دکمه Navigation نیز می توان برای جابجا کردن اشیاء استفاده کرد.

دستگاه های بی سیم در فضای کار فیزیکی

فضای کار فیزیکی برای دستگاه های بی سیم مشخصه بعد مسافت را نیز فراهم کرده است. نقاط دسترسی می توانند بین دستگاه های بیسیم که در محدوده معینی هستند اتصال برقرار کنند. این محدوده با شبکه خاکستری رنگ پیرامون نقطه دسترسی مشخص می شود. بر اساس ابعاد تصویر زمینه، این محدوده می تواند دایره یا بیضی باشد. اگر تصویر زمینه مربع باشد، شبکه دایره ای خواهد بود. اگر تصویر زمینه مستطیل باشد، شبکه با توجه به نسبت طول و عرض تصویر بیضی شکل خواهد شد.



در این مثال، سه رایانه با قابلیت بی سیم و دو نقطه دسترسی ایجاد شده اند که به منظور نمایش تاثیر مسافت، همه آنها از اتاق سیم بندی پیشفرض مستقیما در خیابانهای شهر قرار داده شده اند.

- PC0 در محدوده Access Point 0 قرار دارد بنابراین به آن مرتبط است.
- PC1 در محدوده هر دو نقطه دسترسی قرار دارد. به هر حال چون به Access Point1 نزدیکتر است، در ارتباط با آن است.
- PC2 در محدوده هیچ کدام نیست، بنابراین اتصالی برای آن وجود ندارد.

نکات مهم در فضای کار فیزیکی

استفاده از تصاویر زمینه دلخواه :

در فضای فیزیکی تعدادی تصویر زمینه برای نماهای مختلف قرار دارد که می توان زمینه هر یک از محیط ها را همانند فضای منطقی با تصاویر زمینه دلخواه خود جایگزین نمود. مثلا برای تغییر تصویر زمینه شهر مانند زیر عمل کنید:

- تصویر را در پوشه background/city قرار دهید
- تصویر را به قسمت Administrative اضافه کنید.
- در نمایش هر، دکمه background را کلیک کنید و تصویر را اعمال کنید.

توجه داشته باشید که ابعاد تصویر زمینه، در مقیاس نمایشی برخی اشیاء تاثیر می گذارد.

استفاده از Navigation :

با کلیک بر روی دکمه Navigation در نوار پیمایش، یک ساختار درختی از مکان ها نمایش داده خواهد شد. به راحتی می توان بین مکان ها پرش و یا اشیاء را بین آنها جابجا نمود.

استفاده از Grid :

با کلیک بر روی دکمه Grid می توانید یک صفحه مشبک دلخواه به نماهای مختلف بین شهری، شهر و ساختمان اعمال کنید. این ابزار به شما امکان تنظیم فاصله شبکه های هر سطح و نیز تعیین رنگ آنها را می دهد.

محدودیت های اتاق های سیم بندی :

هر اتاق سیم بندی می تواند حداکثر سه قفسه یا رک، سه میز، دو میز و یک قفسه یا دو قفسه و یک میز داشته باشد. دستگاه های نهایی روی میزها قرار گرفته و دیگر دستگاه ها در داخل قفسه ها قرار داده می شود. اگر توپولوژی منطقی بیش از ظرفیت یک اتاق دستگاه داشته باشد، اتاق دیگر به طور خودکار در همان ساختمان پیش فرض ایجاد خواهد شد و اتاق سیم بندی جدید به طور پیش فرض تنظیم خواهد شد.

حذف اشیاء :

توسط ابزار Delete می توان هر شهر، ساختمان و اتاق سیم بندی را حذف کرد. اما امکان حذف دستگاه ها در این فضا وجود ندارد. اگر یک اتاق سیم بندی را حذف گردد، دستگاه های موجود در آن به طور خودکار مستقیما در کف ساختمان قرار گرفته و اگر یک ساختمان حذف شود، دستگاه ها در خیابان های شهر قرار می گیرد.

۴۱-۵- حالت های عملکرد

حالت های عملکرد نرم افزار Packet Tracer 4.1 الگوی زمانی شبکه را نشان می دهد.
در حالت Realtime شبکه به صورت زنده کار می کند. شبکه به فعالیت های خود همچون یک شبکه واقعی فورا پاسخ می دهد. برای مثال، به محض ایجاد یک اتصال اترنت، چراغ های لینک برای اتصال ظاهر و وضعیت اتصال را نمایش می دهند. وقتی که یک دستور نظیر ping یا show در CLI تایپ می کنید، نتیجه یا پاسخ به صورت زنده تولید شده و می توان آن را مشاهده کرد. همه فعالیت های شبکه، مخصوصا جریان PDU ها در شبکه به صورت زنده اتفاق می افتد.
در حالت شبیه سازی (Simulation) کنترل مستقیم بر روی زمان داشته و می توان اجرای شبکه را قدم به قدم یا رویداد به رویداد با سرعتی دلخواه مشاهده نمود. می توانید سناریوهای مختلفی ایجاد کنید. ضمن این که هر کاری که انجام دهید تا زمانی که آن را play ننمائید اجرا نخواهد شد. پس از play شبیه سازی، نمایش گرافیکی حرکت بسته ها در بین دستگاه ها را می توان مشاهد کرد. شبیه سازی را متوقف، جلو و عقب برد تا اطلاعات مختلفی را از موضوعات خاص در زمان های خاص بدست آورد. به هر حال، دیگر موارد شبکه هنوز به صورت زنده کار می کنند. مثلا اگر پورتی خاموش گردد، چراغ آن فورا قرمز می شود.

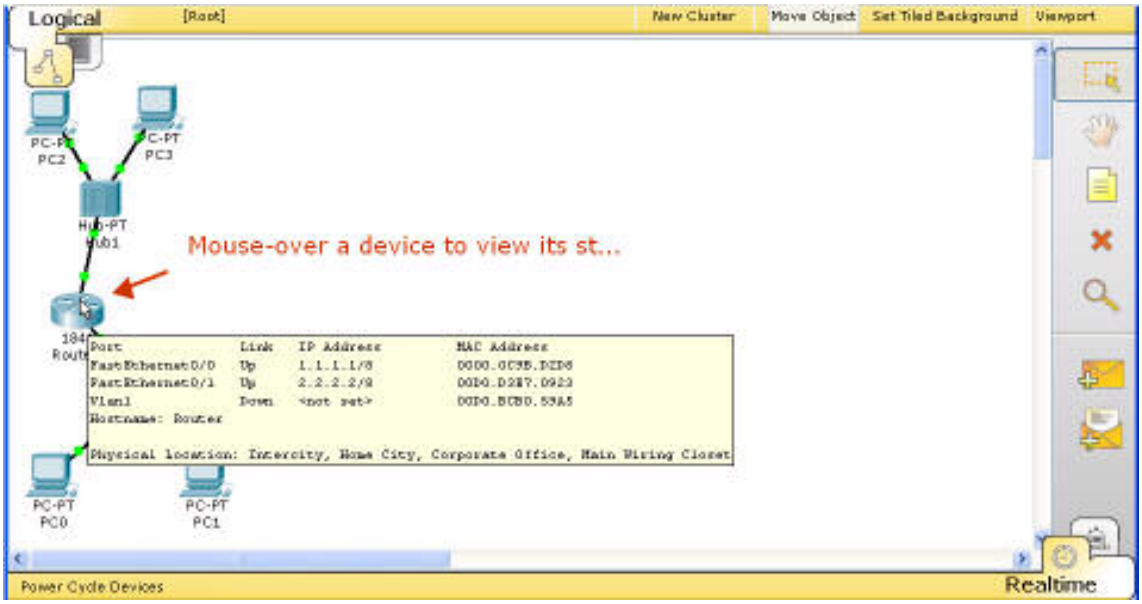
۴۱-۶- حالت Realtime

در حالت Realtime، شبکه همچون یک شبکه واقعی همیشه در حال اجراست چه روی شبکه کار کنید و چه کار نکنید. پیکربندی ها به صورت زنده اعمال و شبکه به صورت زنده پاسخ می دهد. آمار شبکه نیز به صورت زنده نشان داده می شوند. علاوه بر این که می توان از دستورات IOS سیسکو برای پیکربندی و خطایابی شبکه استفاده نمود، و نیز می توان از دکمه های Add Simple PDU و User Creaetd PDU List برای ارسال ping به صورت گرافیکی استفاده کرد.

کسب اطلاعات از دستگاه ها

در هنگامی که شبکه کار می کند، از ابزار Inspect می توان برای مشاهده جداول دستگاه ها در حال پر شدن و به روز رسانی استفاده نمود. مثلا برای مشاهده اطلاعات جدول ARP مسیریاب، روی ابزار Inspect کلیک، سپس روی مسیریاب کلیک تا لیست جداول موجود آن نمایش داده شود و سپس شما ARP Table را انتخاب کنید.

علاوه بر ابزار Inspect، برای مشاهده جزئیات یک دستگاه نظیر آدرس IP و آدرس فیزیکی همه پورت های آن، می توان ماوس را روی دستگاه قرار داد.



ارسال گرافیکی PDU ها

اگرچه حالت Simulation برای ارسال بسته ها ترجیح داده می شود، اما از دستورات PDU Simple Add و نیز User Created PDU List برای ping کردن یا ارسال دیگر بسته ها در این حالت می توان استفاده کرد. لذا شما آیکن PDU را که در شبکه حرکت کند مشاهده نخواهید کرد. کل مراحل به صورت زنده اتفاق افتاده و نتیجه را می توان در پنجره User Created Packet مشاهده نمود.

خاموش و روشن کردن دستگاه ها (Power Cycle Devices)

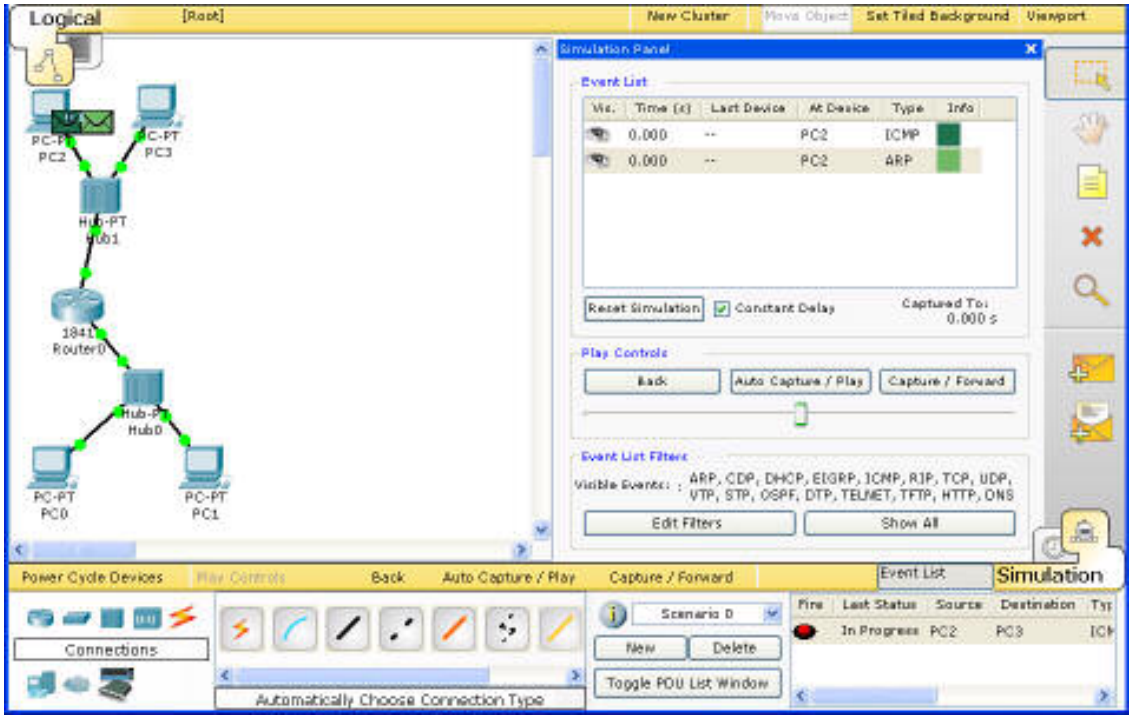
دکمه Power Cycle Devices در نوار ابزار Realtime امکان خاموش و روشن کردن همه دستگاه های شبکه را می دهد. در نتیجه فشار این دکمه سبب پاک شدن همه رویدادها در حال شبیه سازی نیز خواهد شد.

چنانچه توسط این دکمه شبکه را Reset کنید، همه پیکربندی های درحال اجرا در مسیریاب ها و سوئیچ ها را از دست خواهید داد. بنابراین قبل از فشار این دکمه، مطمئن شوید که دستور run start copy را در همه مسیریاب ها و سوئیچ ها اجرا کرده اید.

۴۱-۷- حالت شبیه سازی(Simulation)

در حالت شبیه سازی شما می توانید شبکه خود را با اجرای آهسته تر مشاهده کنید، مسیری را که بسته طی می کند را دیده و اطلاعات مورد نیاز را با جزئیات دریافت کنید.

وقتی به این حالت سوئیچ می کنید، کادر شبیه سازی[1] ظاهر خواهد شد که می توانید به صورت گرافیکی PDU ها را با استفاده از دکمه Add Simple Button برای ارسال بین دستگاه ها ایجاد کنید و سپس با کلیک بر روی دکمه Auto Capture/Play سناریوی شبیه سازی را اجرا کنید. پنجره Even List هر آنچه که در طی انتشار PDU در شبکه رخ می دهد را ثبت می کند. شما می توانید سرعت شبیه سازی را با لغزنده Play Speed کنترل و اگر نیاز به کنترل بیشتر شبیه سازی دارید می توانید از دکمه Capture/Forward برای شبیه سازی دستی استفاده کنید. توسط دکمه Back نیز می توانید به زمان های قبلی برگشته و رویدادهای قبل را مجددا مشاهده نمایید. ضمنا دکمه های Play Control علاوه بر این پنجره، در نوار Simulation bar نیز قرار دارند.



شما می توانید سناریو را توسط دکمه Reset Simulation پاک کنید و از اول اجرا کنید که با این کار هر آنچه در Event List ثبت شده است پاک خواهد شد. دقت کنید که در حین اجرای شبیه سازی، ممکن است بسته هایی را مشاهده کنید که خود شما آنها را ایجاد نکرده اید. علت این است

[1]- Simulation Panel

که برخی دستگاه ها می توانند خودشان در حین اجرای شبکه بسته هایی نظیر CDP ایجاد کنند. همچنین می توان نوع بسته هایی را که منتشر می شوند را در قسمت Type مشاهده نمود و برای مخفی کردن آنها باید از دکمه Edit Filter استفاده کرد. برای مشاهده همه انواع بسته ها کافیست بر روی دکمه Show All کلیک نمود.

Evnt List و روند زمانی رویداد

نرم افزار Packet Tracer 4.1 شبیه سازی را در مقیاس زمانی خطی انجام نمی دهد. زمان، بستگی به رویدادهایی دارد که اتفاق می افتد. یک رویداد می تواند در حالات مختلفی و برای هر نوع از PDU که تولید می شود، تعریف گردد. لیست رویدادها اطلاعات مربوط به همه نمونه ها را ثبت می کند. فیلدهای این پنجره به شرح زیر هستند:

- Visible: آیکن یک چشم در این فیلد به معنای این است که رویداد در زمان فعلی شبیه سازی اتفاق افتاده است. همه بسته هایی که در حال نمایش هستند، این آیکن را دارند.
- Time: زمان اتفاق افتادن رویداد را مشخص می کند.
- Last Device: مکان قبلی بسته را مشخص می کند.
- At Device: مکان فعلی بسته را مشخص می کند.
- Type: این فیلد بیانگر نوع بسته است (ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP, VTP, STP, OSPF, DTP, Telnet, TFTP, HTTP, DNS)
- Info: نمایش اطلاعات جزئی تر در مورد نوع بسته به تفکیک لایه های مدل OSI.

برخی رویداد ها بسیار رایج بوده و به طور متداول و برخی رویدادها کمتر اتفاق می افتد. در فضای کاری، رویدادهای شبکه پشت سرهم و با سرعت مشابه (که با لغزنده مشخص شده است) اتفاق می افتند، در حالی که واقعا ممکن است بر حسب میلی ثانیه یا حتی دقیقه فاصله داشته باشند. با مشاهده فیلد Time می توان زمان واقعی رخداد را مشاهده نمود. با فعال کردن گزینه Delay Constant زمان تاخیر 1 ms بین رویدادها لحاظ می شود. اما اگر این گزینه غیرفعال باشد، عوامل مختلفی نظیر تاخیر انتقال، تاخیر انتشار و ... در این تاخیر تاثیر خواهند داشت.
درصورتی که شما برخی از انواع PDU را فیلتر کنید، در لیست رویدادها نمایش داده نخواهند شد ولی هنوز در شبکه وجود داشته و فقط شما آنها را نمی بینید. این کار تنها باعث می شود که شبیه سازی سریعتر اجرا شود.

اجرای مجدد سناریو

وقتی که شبیه سازی مجددا اجرا شود، زمان شبیه سازی صفر شده و لیست رویدادها پاک خواهد شد. شبیه سازی را می توان به شکل های زیر از اول اجرا کرد:

- کلیک بر روی دکمه Reset Simulation
- کلیک بر دکمه Power Cycle Devices
- سوئیچ بر روی حالت Realtime
- تغییر شبکه (حذف،اضافه یا تغییر پیکربندی)
- وارد کردن یک دستور در تنظیمات حالت global یک دستگاه (در CLI)
- سوئیچ به یک سناریوی دیگر
- حذف PDU از لیست داده PDU ها

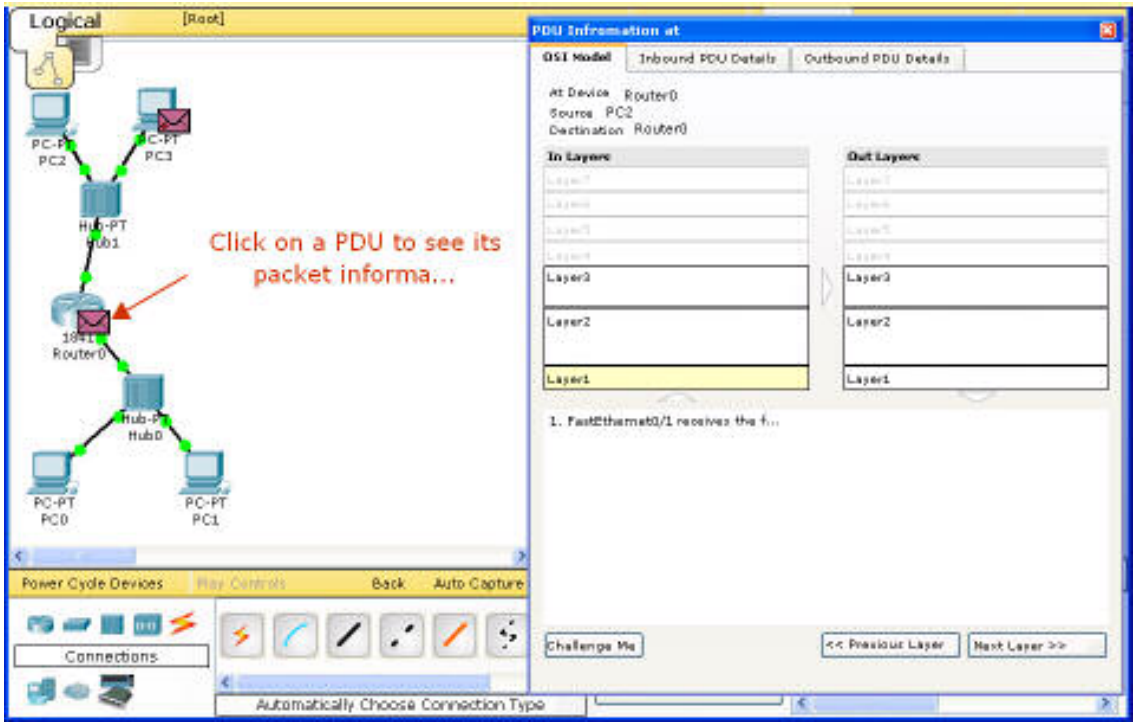
دقت کنید که اجرای مجدد شبیه سازی رویه های زمان بندی شده PDU فعلی را حذف نخواهد کرد، بلکه تنها رویداد های ثبت شده را حذف خواهد کرد. برای حذف PDUها باید به صورت دستی آنها را از پنجره مربوط به بسته های ایجاد شده کاربر حذف کنید.

ارسال PDU های ساده (Ping)

در نرم افزار Packet Tracer 4.1 دکمه Add Simple PDU یک روش ضروری، سریع و گرافیکی برای ping کردن است. می توانید ping هایی را بین دو دستگاه که حداقل یکی از واسط های آنها آدرس IP دارد ارسال کنید. برای ارسال Ping روی دکمه Add Simple Button کلیک کنید (نشانگر ماوس به آیکن پاکت نامه تغییر می کند). ابتدا روی دستگاه مبدا و سپس روی دستگاه مقصد کلیک کنید. ping تنها در صورتی کار می کند که پورت های دستگاه ها پیکربندی شده باشد. بعد از ایجاد درخواست، دستگاه مبدا یک بسته ICMP یا ARP (یا هر دو) در صف قرار خواهد داد و منتظر خواهد ماند تا دکمه Auto Capture/Play یا Capture/Forward را کلیک کنید. وقتی یکی از این دکمه ها را کلیک کنید، بسته شروع به حرکت خواهد کرد و شما روند ping را مشاهده خواهید کرد. شما می توانید انواع بسته های خاصی را توسط Event List Filters مخفی کنید تا از سردرگمی ایجاد شده توسط تعداد زیاد بسته ها در شبکه جلوگیری شود.

۴۱-۸- اطلاعات بسته در حالت شبیه سازی

در طول شبیه سازی، می توانید روی یک بسته کلیک نموده (در توپولوژی یا رویداد متناظر آن در لیست رویدادها) تا پنجره اطلاعات آن با جزئیات ظاهر شود. پنجره جزئیات شامل ۳ برگه است. OSMI Model ، Inbound PDU Details و Outbound ODU Details.



برگه OSI Model نشان می دهد که چگونه بسته در دستگاه جاری در هر یک از لایه های مدل OSI پردازش می شود. پردازش با توجه به جهت بسته، فرق خواهد داشت. لایه های ورودی (Layer In) نشان می دهند که چگونه یک بسته ورودی یا بافر شده پردازش می شود و لایه های خروجی (Out Layer) نشان می دهند که وقتی قرار است دستگاه بسته ای را از یکی از پورت های خود ارسال کند، چگونه پردازش را انجام می دهند.

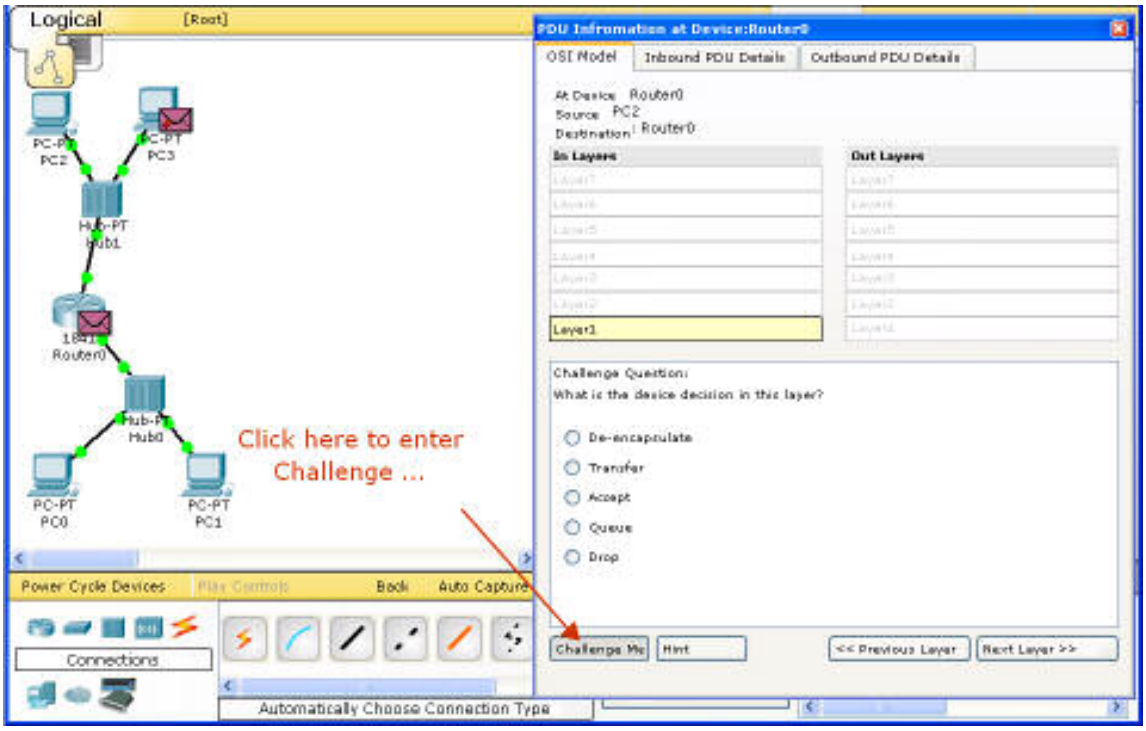
In Layer به معنای این است که از پایین به بالا خوانده می شود (از لایه ۱ تا ۷) و Out Layer از بالا به پایین خوانده می شود (لایه ۷ تا ۱). به این دلیل که لایه فیزیکی اولین لایه ای است که بسته های PDU ورودی با آن مواجه می شوند و آخرین لایه ای است که PDU های خروجی از آن رد خواهند شد تا از دستگاه خارج شوند.

برگه Inbound PDU Details تنها در صورتی وجود دارد که PDU مورد نظر توسط دستگاه دریافت شده باشد. اگر خود دستگاه تولید کننده بسته باشد، این برگه ظاهر نمی شود. این برگه نشان می دهد که دقیقا چه چیزی در سرآمد PDU وجود دارد. برگه Outbound PDU Details اطلاعات مشابهی برای بسته های خروجی دارد. این برگه نیز تنها در صورتی وجود دارد که PDU جهت ارسال وجود داشته باشد.

اکثر اوقات، یک دستگاه PDU ای را دریافت خواهد کرد و سپس بسته ای دیگر را ارسال خواهد کرد. در این حالات هر دو برگه وجود خواهند داشت.

۴۱-۹- حالت Challenge

شما می توانید از خودتان در مورد رویه های انجام شده در لایه های مختلف آزمون به عمل آورید. برای این منظور باید روی Challenge Me کلیک کنید. جزئیات لایه پنهان خواهد شد و اطلاعات پنجره با سئوال جایگزین خواهد شد و از شما سئوال می شود که دستگاه با PDU چه عملی انجام می شود. شما باید یک گزینه را انتخاب کنید. اگر پاسخ صحیح باشد، جزئیات آن لایه نمایش داده خواهد شد و سئوال مربوط به لایه بعدی پرسیده خواهد شد. برای کسب راهنمایی می توانید از Hint استفاده کنید.

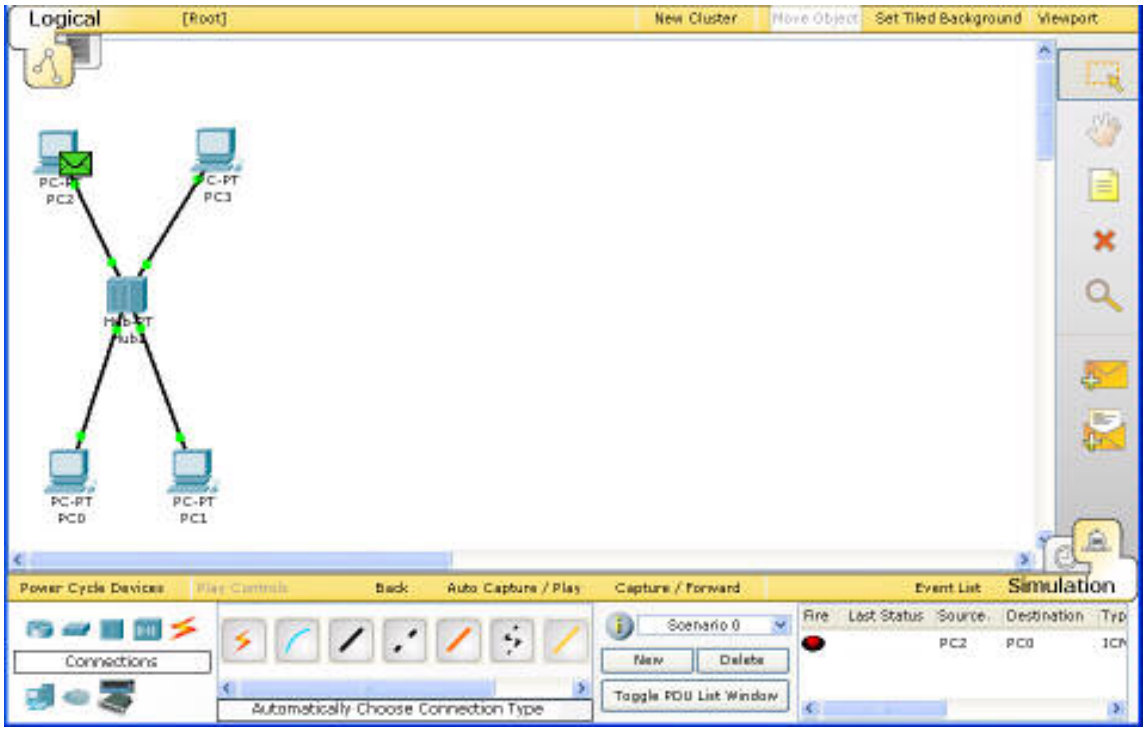


هر سئوال ممکن است شامل پاسخ های زیر باشد:

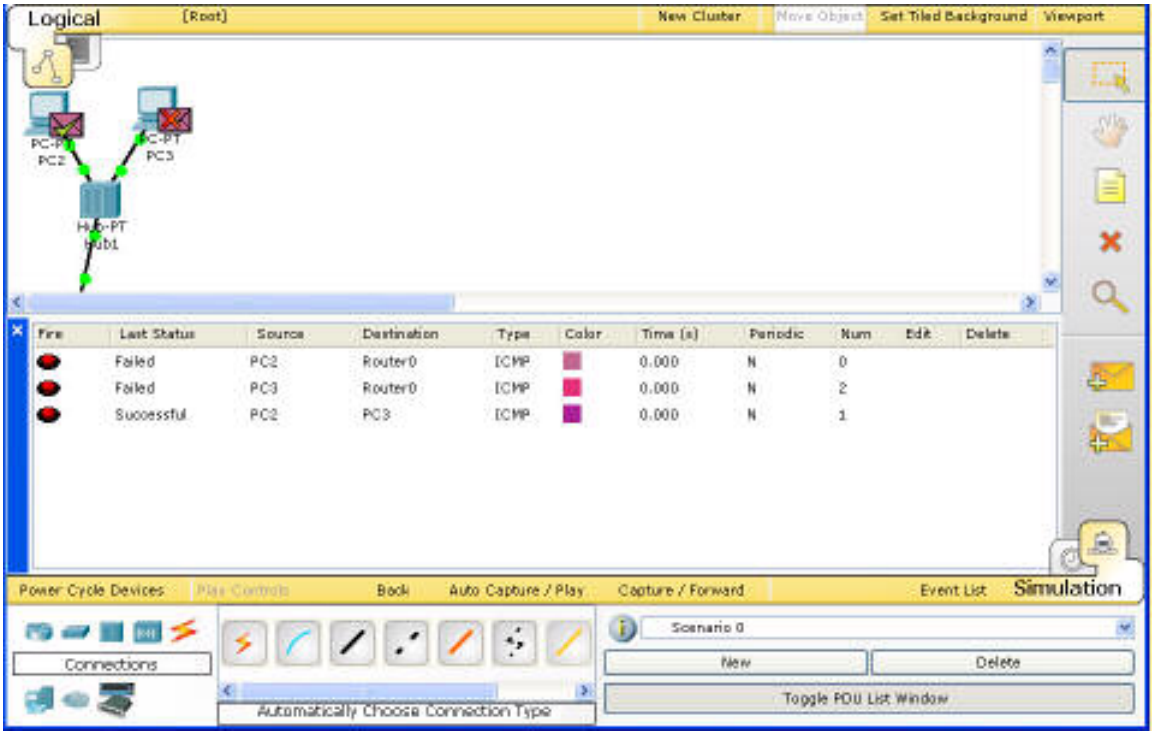
- Encapsulate: افزودن یک header یا یک header و trailer به PDU مربوط به این لایه برای ایجاد PDU ارسالی به لایه پایینتر
- De-encapsulate: حذف header یا header و trailer از PDU مربوط به این لایه و ایجاد PDU برای لایه بالاتر
- Transfer: انتقال PDU از قسمت inbound به قسمت outbound
- Accept: پذیرش بسته و پایان پردازش آن
- Queue: قرار دادن PDU در صف جهت پردازش یا ارسال در زمانی جلوتر
- Drop: حذف PDU
- Transmit: ارسال سیگنال به خارج از رسانه فیزیکی

۴۱-۱۰- مدیریت سناریو ها در حالت شبیه سازی

در نرم افزار Packet Tracer 4.1 می توانید حالت های شبکه بندی (سناریوهای) پیچیده ای را راه اندازی کرده و شبیه سازی کنید. این کار از طریق پنجره User Created Packet یا UCPW در گوشه پایین سمت راست برنامه انجام می شود. یک سناریو مجموعه ای از PDU ها است که شما آنها را در شبکه قرار می دهید تا در زمانی خاص ارسال شوند. وقتی که برای اولین بار به حالت شبیه سازی سوئیچ کنید، سناریوی پیش فرض Scenario 0 خواهد بود. شما می توانید نام آن را تغییر دهید و یا با کلیک بر روی آیکن Scenario Description که در کنار نام آن قرار دارد، توضیحاتی را برای آن ایجاد کنید. همچنین شما می توانید سناریوها را توسط دکمه های New و Delete ایجاد یا حذف کنید و بین سناریوهای مختلف سوئیچ کنید.



لیست PDU ها ایجاد شده توسط کاربر بخش مهمی در این پنجره است که همه PDU های ایجاد شده در سناریوی جاری را ثبت می کند. با کلیک بر روی Toggle PDU List Windows می توانید این لیست را در پنجره جداگانه خودش مشاهده کنید.



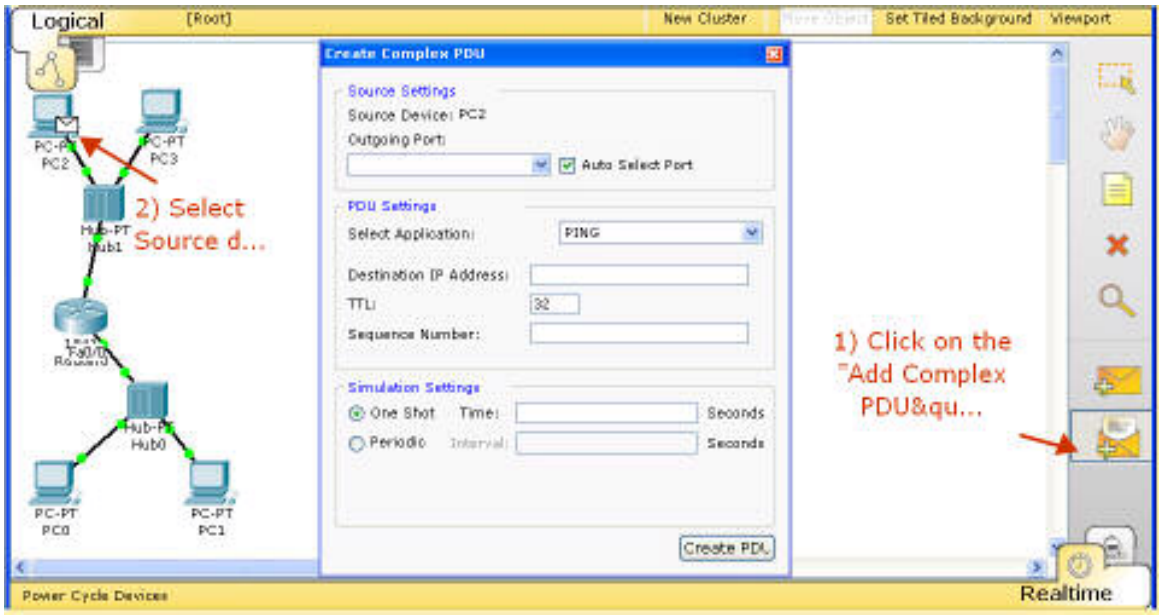
هر PDU در این لیست شامل فیلد های زیر است.

- Fire: با دابل کلیک بر روی این فیلد، بسته فورا در حالت realtime ارسال خواهد شد یا در حالت شبیه سازی در صف قرار خواهد گرفت و منتظر ارسال خواهد شد.
- Last Status: شامل آخرین وضعیت شناخته شده PDU می باشد (Successful ، Fail یا Progress)
- Source: شامل نام وسیله ای است که PDU را تولید کرده است
- Destination: نام وسیله ای است که PDU سرانجام باید به آنجا برسد
- Type: نام پروتکل PDU است
- Color: نمایش رنگ PDU است که با این رنگ در انیمیشن ظاهر خواهد شد.
- Time: زمانی از شبیه سازی که بسته باید در آن زمان ارسال شود
- Periodic: این فیلد نشان می دهد که آیا بسته باید به صورت متناوب ارسال شود(Y) یا خیر(N)
- Num: شماره اندیس عددی PDU
- Edit: با دابل کلیک بر روی این دکمه می توانید مشخصه های PDU را ویرایش کنید.
- Delete: با دابل کلیک بر روی این دکمه می توانید PDU را از لیست حذف کنید.

PDU های ایجاد شده توسط کاربر در ابتدا یک رنگ تصادفی می گیرند. شما می توانید با دابل کلیک بر روی مربع رنگی مربوط به آن، رنگش را تغییر دهید.

۴۱-۱۱- Complex PDU در حالت شبیه سازی

علاوه بر PDU های ساده که برای ping کردن استفاده می شوند، PDU های دلخواه دیگری را نیز می توان ارسال نمود. در نوار ابزار، پس از کلیک روی آیکن Add Complex PDU، دستگاه مبدا را انتخاب کنید. به این ترتیب کادر Create Complex PDU ظاهر می شود. در این کادر شماره پورت خروجی می توان را تعیین و یا نوع PDU را تغییر داد. بسته به برنامه ای که انتخاب می کنید ممکن است نیاز باشد تنظیمات مربوط به آدرس IP مقصد ، TTL (زمان حیات)، پورت مبدا ، پورت مقصد و شماره ترتیب را انجام دهید.



نرم افزار Packet Tracer 4.1 از بسته های PDU با پورت های مبدا و مقصد مطابق با پروتکل های زیر پشتیبانی می کند:

DNS, Finger, FTP, HTTP, HTTPS, IMAP, NetBIOS, Ping, POP3, SFTP, SMTP, SNMP, SSH, Telnet, TFTP, other

پارامترهای زمانبندی PDU نیز قابل تنظیم هستند. One Shot یعنی این که بسته تنها در زمان تعیین شده (بر حسب ثانیه) ارسال شود و Periodic یعنی بسته به صورت متناوب مطابق آنچه که تنظیم می شود (بر حسب ثانیه) ارسال شود.

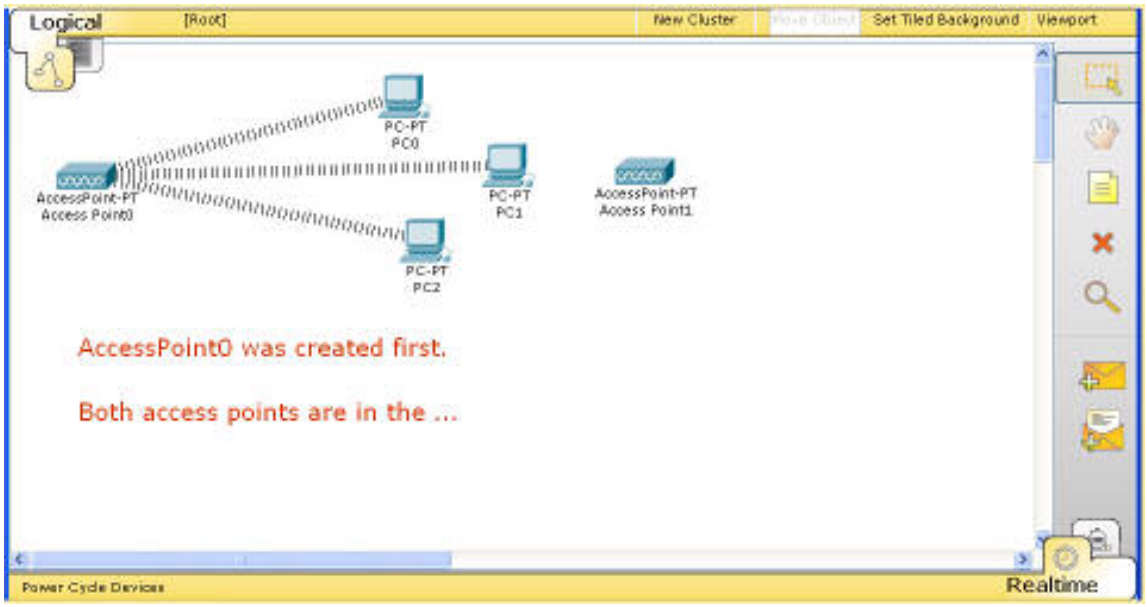
۴۱-۱۲- انواع اتصالات

نرم افزار Packet Tracer 4.1 از اتصالات مختلفی پشتیبانی می کند.

نوع کابل	شرح
 Console	اتصال کنسول بین رایانه ها مسیریاب ها یا سوئیچ ها برقرار می شود. برای ورود به بخش کنسول می بایست تنظیمات یکسانی در دو دستگاه برقرار شود. (parity ، stop bit و...)
 Copper Straight-through	کابل استاندارد اترنت برای اتصال بین دستگاه هایی که در لایه های مختلف قرار دارند. (مانند هاب به روتر، سوئیچ به رایانه، روتر به هاب و ...) و می تواند به پورت های زیر متصل شود. 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), 1000 Mbps Copper (Gigabit Ethernet)
 Copper Cross-over	کابل اترنت برای اتصال بین دستگاه هایی که در لایه های یکسان قرار دارند. (مانند هاب به هاب، رایانه به رایانه، رایانه به چاپگر و ...) و می تواند به پورت های زیر متصل شود. 10 Mbps Copper (Ethernet), 100 Mbps Copper (Fast Ethernet), 1000 Mbps Copper (Gigabit Ethernet).
 Fiber	برای اتصال بین پورت های فیبر نوری(100 Mbps or 1000 Mbps)
 Phone	اتصال خط تلفن می تواند بین دستگاه هایی که پورت مودم دارند برقرار شود. کاربرد استاندارد آن بین رایانه و ابر است.
 Coaxial	برای اتصال بین پورت های coaxial (نظیر مودم کابلی و ابر)
 Serial DCE and DTE	اتصال سریال معمولا یک اتصال WAN است و فقط می تواند بین پورت های سریال برقرار شود. برای استفاده از این اتصال باید clocking را در سمت DCE فعال کنید. سمت DCE با یک علامت ساعت در کنار پورت آن مشخص می شود.

اتصالات بیسیم

بین نقاط دسترسی و دستگاه های پایانی (نظیر رایانه، سرور، چاپگر) می توان اتصال بی سیم برقرار کرد؛ برای این کار باید ماژول فعلی دستگاه را برداشته و بجای آن ماژول بی سیم قرار داد. اگر دو یا چند نقطه دسترسی در یک اتاق سیم بندی قرار داشته باشد، مسافت دستگاه از نقاط دسترسی یکسان است، بنابراین اتصال با نقطه دسترسی که زودتر ایجاد شده است برقرار می شود.



وضعیت اتصال

وقتی که دو وسیله به هم متصل می شوند، معمولا چراغ هایی را در دو سمت اتصال مشاهده می گردد. البته برخی اتصالات این چراغ ها را ندارند.

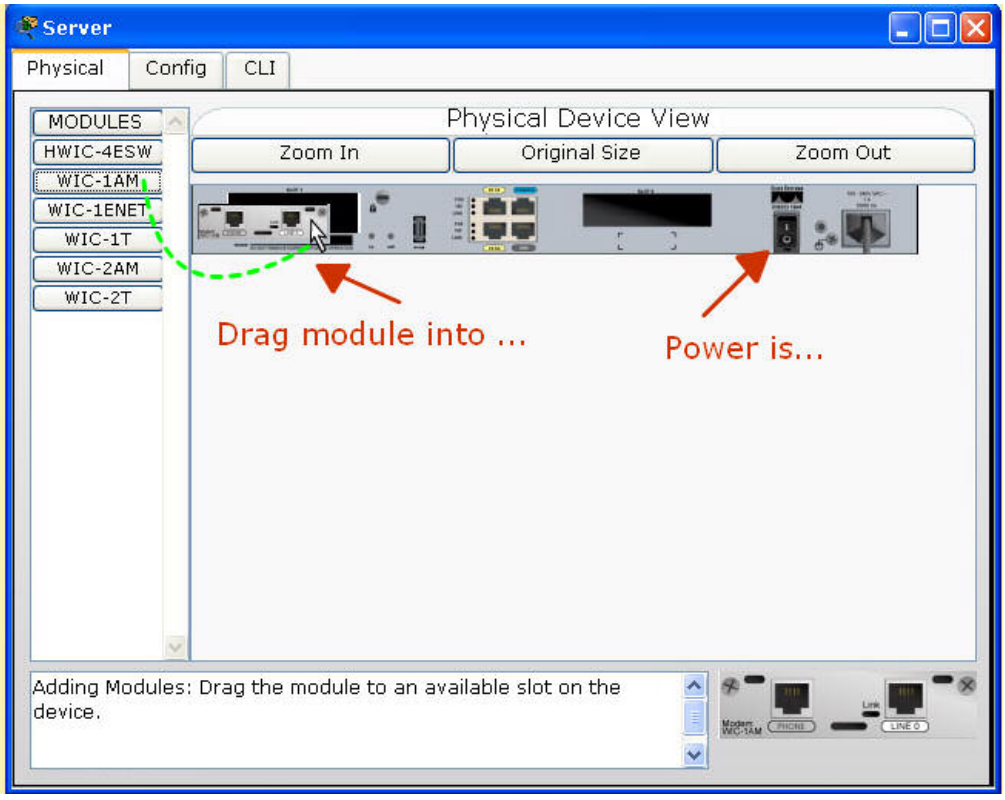
- سبز روشن: اتصال فیزیکی up است.
- سبز چشمک زن: اتصال فعال است.
- قرمز: اتصال down است. سیگنالی پیدا نمی شود.
- کهربایی: پورت در وضعیت بلاک است. (فقط برای سوئیچ ها ظاهر می شود)

۴۱-۱۳- دستگاه ها و ماژول ها

نرم افزار Packet Tracer 4.1 از انواع مختلف ماژول ها برای دستگاه های مختلف پشتیبانی می کند. برای حذف و اضافه کردن ماژول ها باید ابتدا دستگاه خاموش شود. همچنین وقتی که سوئیچ و یا روتر خاموش و سپس مجددا روشن می شود، فایل های پیکربندی startup آنها بارگزاری شده و چنانچه تنظیمات درحال اجرا (running) را ذخیره نکرده باشید، از دست خواهند رفت. بنابراین وقتی شبکه شما شامل سوئیچ و مسیریاب است عادت کنید که همیشه قبل از خاموش کردن دستگاه ها یا Reset کردن شبکه، تنظیمات در حال اجرا را ذخیره کنید.

لیست ماژول ها و پیکربندی های فیزیکی

وقتی روی یک دستگاه در فضای کار کلیک کنید، ابتدا با نمای فیزیکی دستگاه مواجه خواهید شد. یک تصویر محاوره ای از دستگاه در پانل اصلی نمایش و لیستی از ماژول های سازگار با آن در سمت چپ نمایش داده خواهد شد. با فشردن دکمه Power و افزودن ماژول (با درگ کردن ماژول بر روی قسمت مورد نظر) یا حذف یک ماژول (درگ کردن ماژول به بیرون) می توان با دستگاه تعامل داشت.



۴۱-۱۴- پیکربندی دستگاه ها

همانند شبکه های واقعی، شبکه هایی که با نرم افزار Packet Tracer 4.1 ایجاد می شوند نیز باید قبل از این که کارکنند، بدرستی پیکربندی شوند. برای دستگاه های ساده این کار به صورت وارد کردن چند فیلد ساده (نظیر آدرس IP و subnet mask) و یا انتخاب گزینه هایی در صفحه گرافیکی پیکربندی (در برگه config) می باشد. از طرف دیگر مسیریاب ها و سوئیچ ها دستگاه های پیشرفته ای هستند که تنظیمات پیچیده تری دارند. برخی از این تنظیمات می تواند در برگه config انجام شود، اما اکثر پیکربندی های پیشرفته باید توسط دستورات IOS سیسکو انجام شوند. این بخش برگه config را برای همه دستگاه ها شرح می دهد. همچنین لیست کامل دستورات IOS پشتیبانی شده مسیریاب و سوئیچ را مشاهده خواهید کرد.

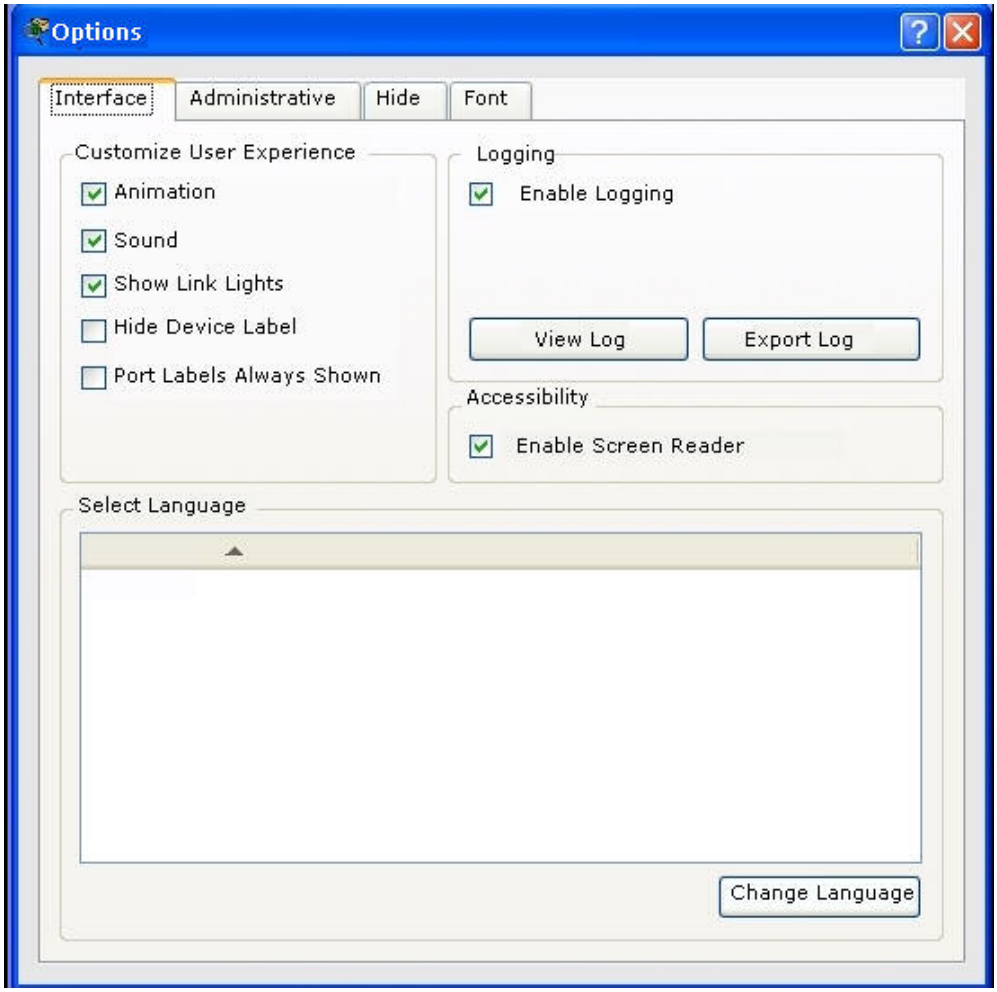
ترتیب Booting و بارگزاری تصویر IOS در مسیریاب ها و سوئیچها

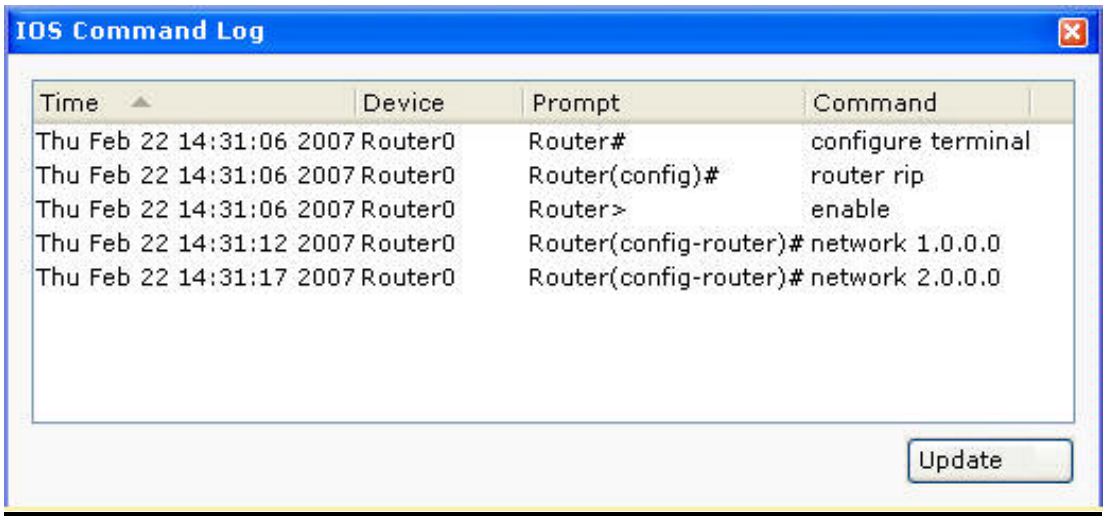
در حین راه اندازی مسیریاب یا سوئیچ ، روند راه اندازی در برگه CLI نمایش داده می شود، اگر فایل startup وجود داشته باشد بارگزاری خواهد شد و تصویر IOS ذخیره شده در حافظه فلش، برای اجرا در RAM بارگزاری می شود. در حالی که تصویر IOS بارگزاری می شود، نمی توان وارد برگه config شد یا دستوری را در برگه CLI وارد نمود. اگر تصویر موجود در حافظه فلش نامعتبر باشد یا فایل مربوط به آن معتبر نباشد، دستگاه در حالت ROM Monitor راه اندازی می گردد. در صورت فشار کلید های Ctrl+Break یا Ctrl+C (در ۶۹ ثانیه اول راه اندازی دستگاه) نیز می توان وارد این حالت شد. البته پس از گذشت ۱۰ ثانیه می توانید سریعتر به دستگاه دسترسی داشته باشید. حالت ROM Monitor یک محیط بسیار کوچک است که می توان فایل ها موجود در NVRAM و Flash را دستکاری کرد، تصاویر IOS را از طریق TFTP بارگزاری و نحوه راه اندازی دستگاه را انتخاب کنید.

وقتی مراحل راه اندازی و بارگزاری تصویر IOS کامل شد، حالت logout بار می شود. برای شروع کلید Enter را فشار دهید.

گزارشگیری دستورات IOS

اگر این ویژگی(Options>Preferences) فعال باشد همه دستورات IOS وارد شده را می توان ثبت کرد. با کلیک بر روی دکمه View پنجره گزارش دستورات باز خواهد شد.


Options
Interface
Administrative
Hide
Font
Customize User Experience
Animation
Sound
Show Link Lights
Hide Device Label
Port Labels Always Shown
Logging
Enable Logging
View Log
Export Log
Accessibility
Enable Screen Reader
Select Language
Change Language


IOS Command Log
Time
Device
Prompt
Command
Thu Feb 22 14:31:06 2007 Router0 Router# configure terminal
Thu Feb 22 14:31:06 2007 Router0 Router(config)# router rip
Thu Feb 22 14:31:06 2007 Router0 Router> enable
Thu Feb 22 14:31:12 2007 Router0 Router(config-router)# network 1.0.0.0
Thu Feb 22 14:31:17 2007 Router0 Router(config-router)# network 2.0.0.0
Update

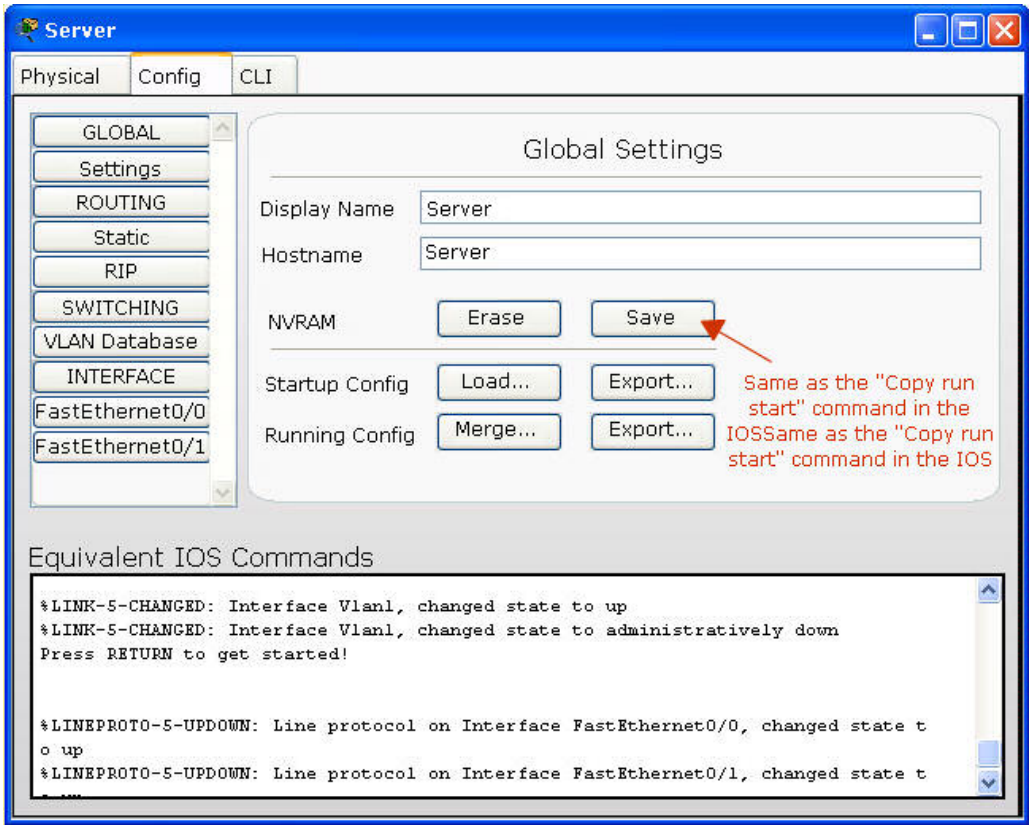
پیکربندی مسیریاب

در برگه Config امکان انجام ۴ سطح پیکربندی global ، routing ، switching و interface وجود دارد. برای انجام یک پیکربندی global، روی دکمه GLOBAL کلیک تا دکمه Settings نمایش داده شود. برای پیکربندی مسیریاب، دکمه ROUTING را کلیک و Static یا RIP را انتخاب کنید. برای پیکربندی سوئیچ، دکمه SWITCHING را کلیک تا Vlan Database نمایش داده شود. برای پیکربندی یک واسط، دکمه INTERFACE را کلیک تا لیست واسط ها نمایش داده شود.

کادر پایین پنجره پیکربندی ها در برگه Config ، دستورات IOS معادل اعمالی که انجام می دهید را نمایش می دهد.

تنظیمات Global:

در تنظیمات Global شما می توان نام مسیریاب (جهت نمایش در فضای کاری) و نام میزبان (جهت نمایش در IOS) را تعیین نمود. همچنین می توان فایل های پیکربندی مسیریاب را به شکل های مختلف دستکاری کرد:

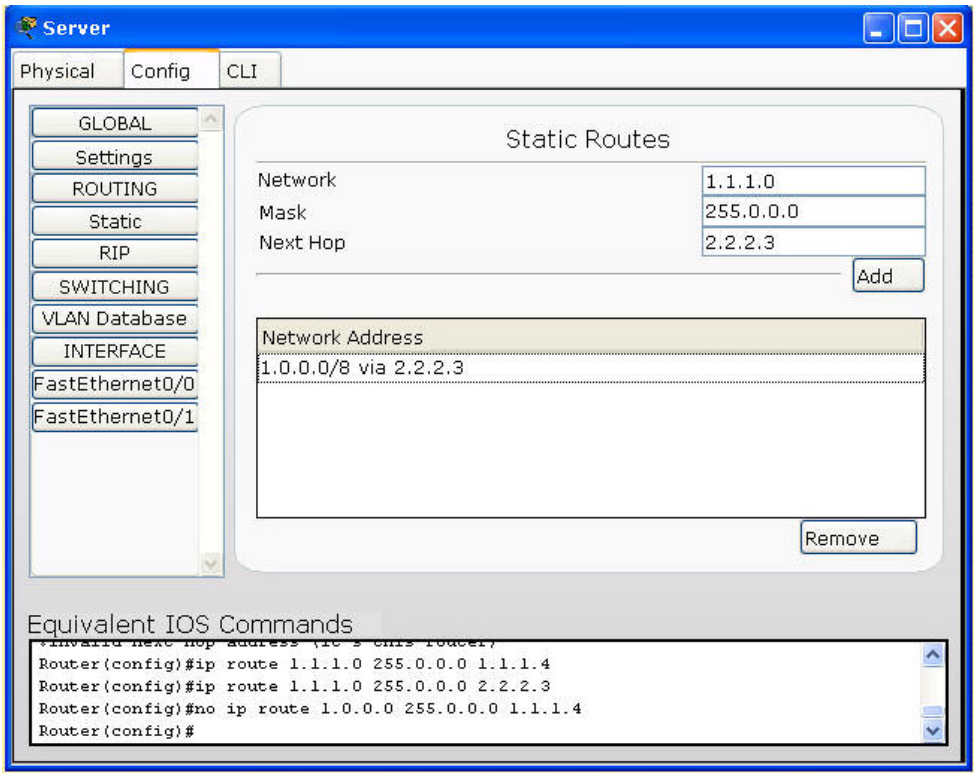


- حذف NVRAM (جایی که تنظیمات Startup ذخیره می شوند)
- ذخیره کردن تنظیمات در حال اجرای فعلی در NVRAM

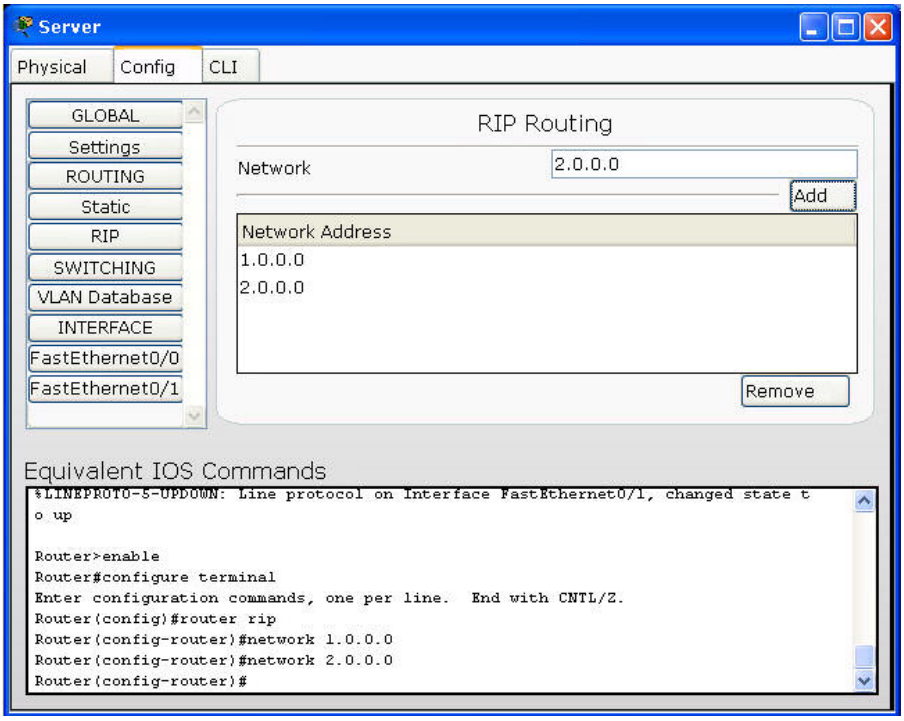
- استخراج تنظیمات startup و running دریک فایل متن
- بارگزاری یک فایل پیکربندی (با فرمت متنی)
- ادغام تنظیمات در حال اجرای فعلی با یک فایل پیکربندی دیگر

پیکربندی مسیریابی:

با انتخاب Static مسیریابی را می توان به روش استاتیک انجام داد. هر مسیر استاتیکی که اضافه می گردد نیازمند یک آدرس IP، ماسک زیرشبکه و آدرس گام بعدی می باشد. همچنین default gateway را نیز می توان تنظیم نمود.

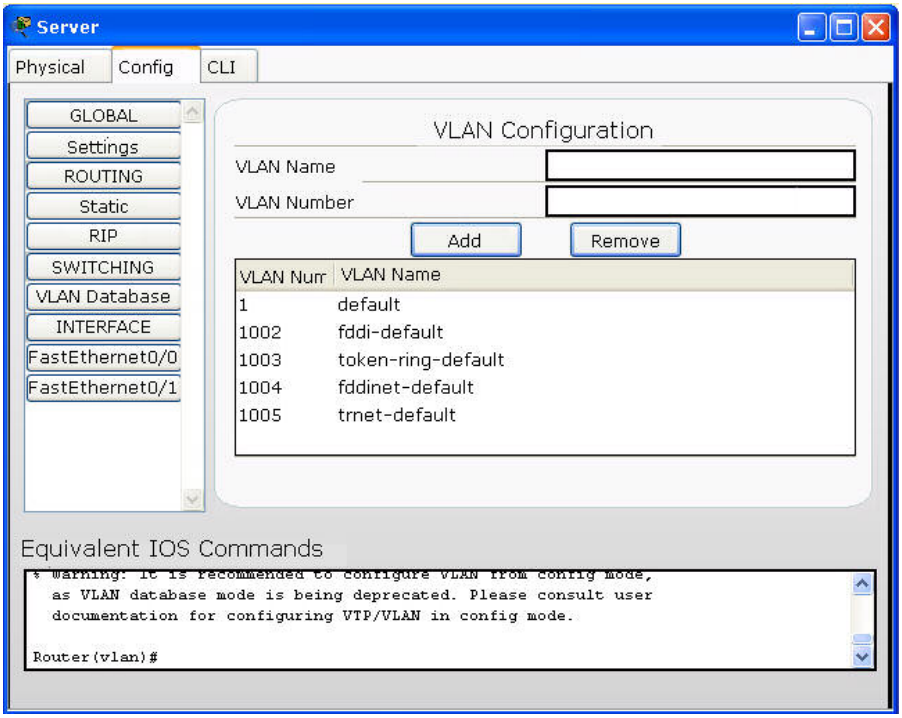


در شبکه های خاصی امکان فعال نمودنRIP نیز وجود دارد. آدرس هر شبکه را در فیلد Network وارد کنید و Add را کلیک تا RIP برای آن شبکه فعال شود. برای غیرفعال کردنRIP در یک شبکه می توانید از دکمه Remove استفاده نمود.



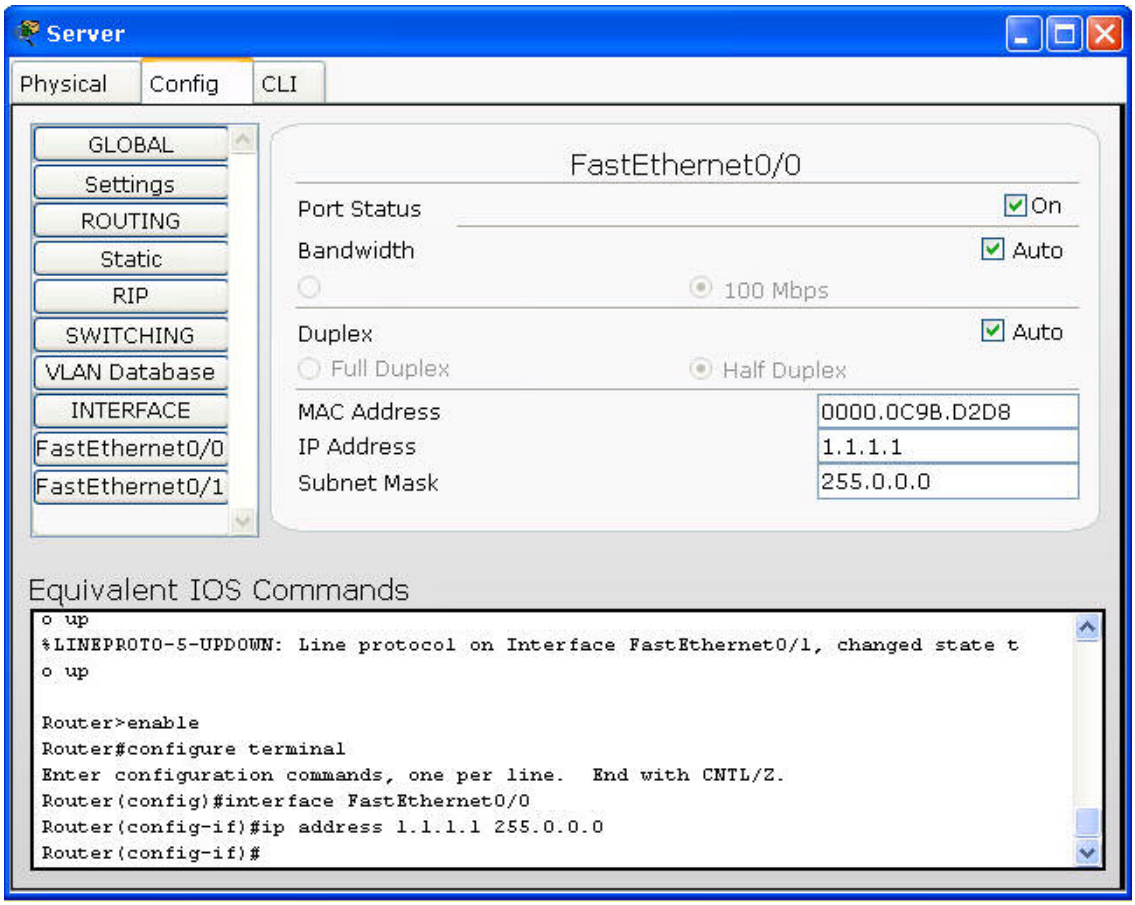
پیکربندی های پایگاه داده VLAN (فقط در مدل های 1481 و 2811):

VLAN مسیریاب ها در قسمت VLAN Database مدیریت می شود. هر VLAN را می توان با وارد کردن نام و شماره آن و فشار کلید Add تعریف نمود. همه VLAN های موجود، در لیست نمایش داده شده و می توان هر مورد را پس از انتخاب توسط Remove حذف کرد.



پیکربندی واسط:

یک مسیریاب انواع مختلفی از واسط ها از جمله سریال، مودم، اترنت مسی و اترنت فیبر را پشتیبانی می کند. هر نوع واسط گزینه های پیکربندی زیادی دارد. اما به طور کلی می توان وضعیت پورت، آدرس IP و ماسک زیرشبکه را تنظیم نمود. برای واسط های اترنت می توان آدرس فیزیکی ، پهنای باند و Duplex و برای پورت های سریال می توان Clock Rate را تنظیم نمود.



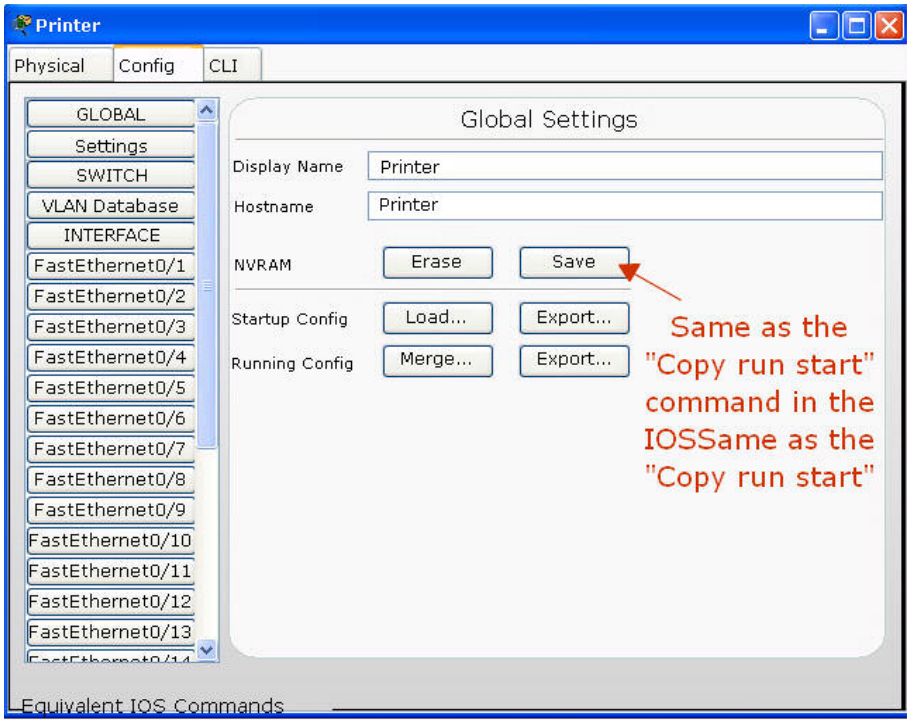
پیکربندی سوئیچ

برگه Config در سوئیچ سه سطح پیکربندیglobal ، switching، interface را دارد. سطح global همانند مسیریاب است. سطح سوئیچینگ جایی است که VLAN Database را می توان مدیریت کرد. سطح واسط هم امکان دسترسی به VLAN های سوئیچ را فراهم می آورد. کادر پایین پنجره پیکربندی در برگه Config، دستورات IOS معادل اعمالی که انجام می دهید را نمایش می دهد.

تنظیمات Global:

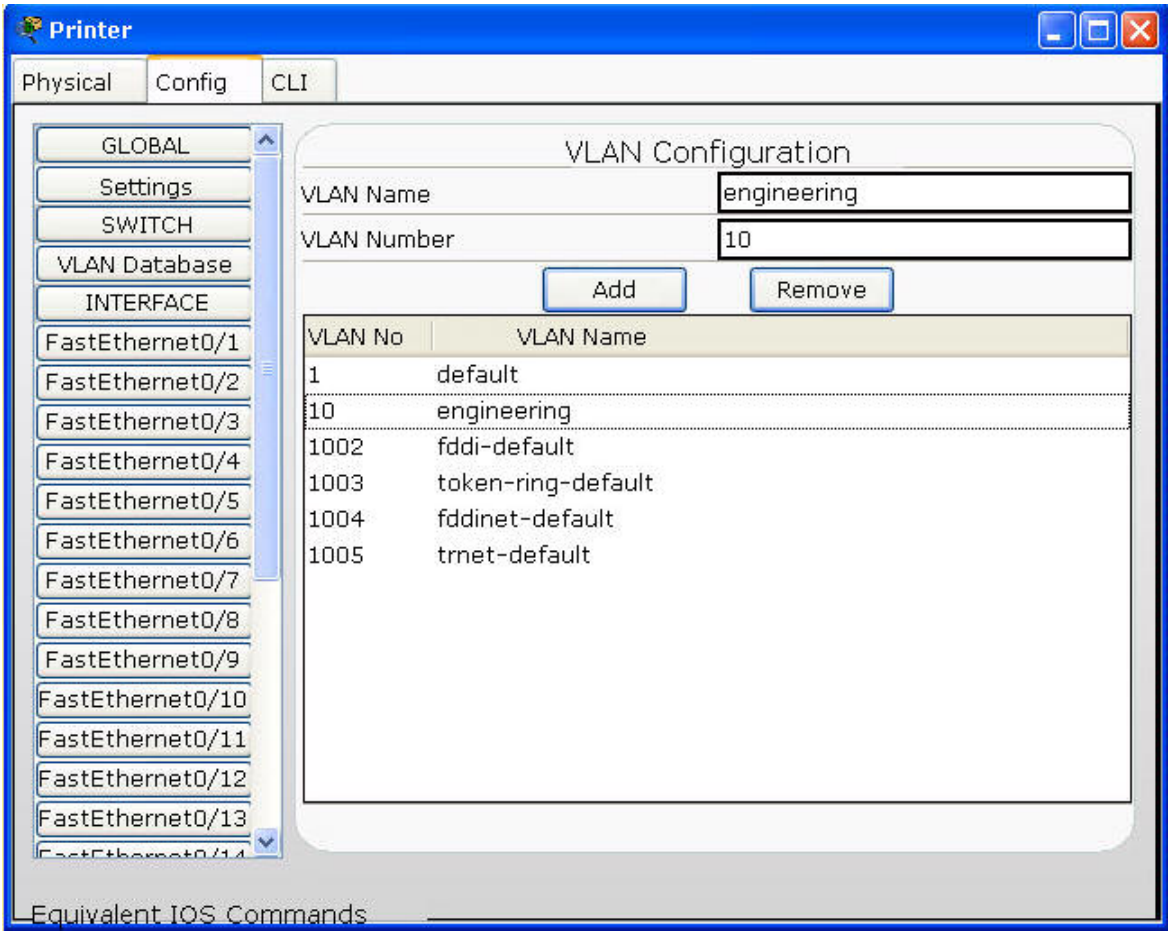
در تنظیمات Global می توان نام سوئیچ (جهت نمایش در فضای کاری) و نام میزبان (جهت نمایش در IOS) را تعیین نمود. همچنین می توانید فایل های پیکربندی سوئیچ را به شکل های مختلف دستکاری کرد:

- حذف NVRAM (جایی که تنظیمات Startup ذخیره می شوند)
- ذخیره کردن تنظیمات در حال اجرای فعلی در NVRAM
- استخراج تنظیمات startup و running دریک فایل متن
- بارگزاری یک فایل پیکربندی (با فرمت متنی)
- ادغام تنظیمات در حال اجرای فعلی با یک فایل پیکربندی دیگر



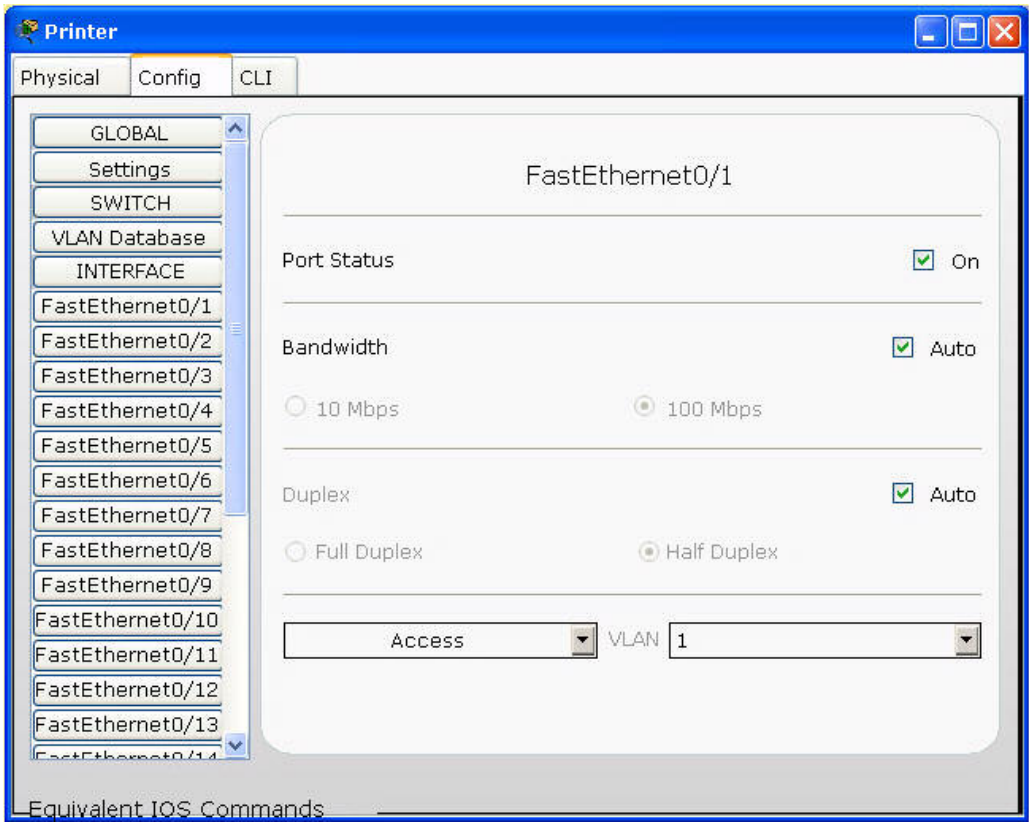
پیکربندی VLAN Database:

VLAN های سوئیچ را از قسمت VLAN Database می توان مدیریت نمود. تعریف هر VLAN با وارد کردن نام و شماره آن و فشار کلید Add انجام می گیرد. همه VLAN های موجود، در لیست نمایش داده شده و هر مورد را پس از انتخاب آن توسط Remove می توان حذف کرد.



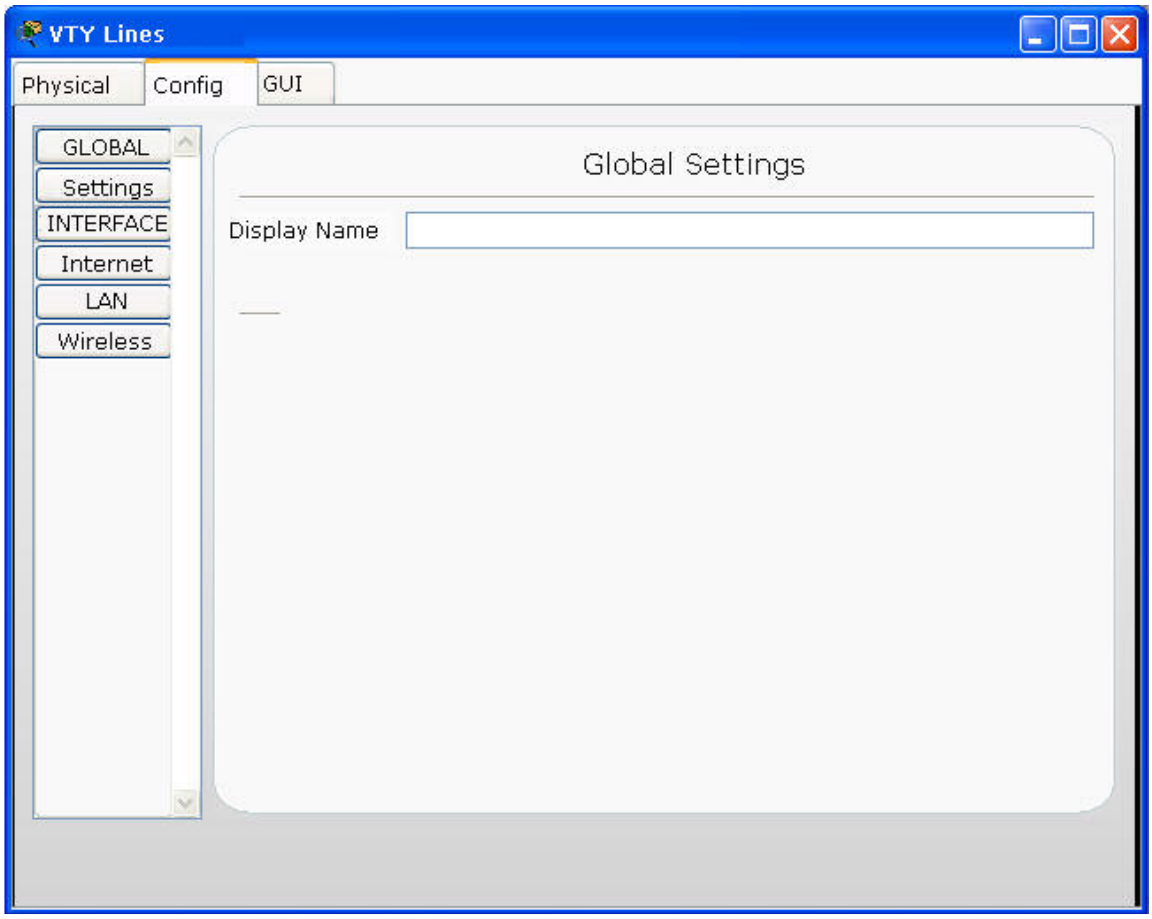
پیکربندی Interface:

سوئیچ ها فقط واسط های از نوع اترنت دارند. برای هر واسط می توان وضعیت پورت، پهنای باند و Duplex حالت VLAN را تنظیم کرد. به طور پیش فرض یک واسط دسترسی به VLAN1 دارد. با استفاده از منوی موجود در سمت راست صفحه می توان پورت آن را در VLAN دیگری قرار دهید. همچنین واسط را به یک پورت trunk تغییر داده و سپس VLAN هایی را که می توانند از این trunk عبور کنند را مشخص کنید.


Printer
Physical
Config
CLI
GLOBAL
Settings
SWITCH
VLAN Database
INTERFACE
FastEthernet0/1
FastEthernet0/2
FastEthernet0/3
FastEthernet0/4
FastEthernet0/5
FastEthernet0/6
FastEthernet0/7
FastEthernet0/8
FastEthernet0/9
FastEthernet0/10
FastEthernet0/11
FastEthernet0/12
FastEthernet0/13
FastEthernet0/1
Port Status
On
Bandwidth
Auto
10 Mbps
100 Mbps
Duplex
Auto
Full Duplex
Half Duplex
Access
VLAN
1
Equivalent IOS Commands

پیکربندی Linksys WRT300N

برگه Config دو سطح پیکربندی Global و interface را فراهم می آورد. برای پیکربندی در سطح global، دکمه GLOBAL را کلیک تا Settings نمایش داده شود. برای پیکربندی یک واسط، INTERFACE را کلیک تا لیست واسط ها نمایش داده شده، سپس واسط مورد نظر را انتخاب کنید.

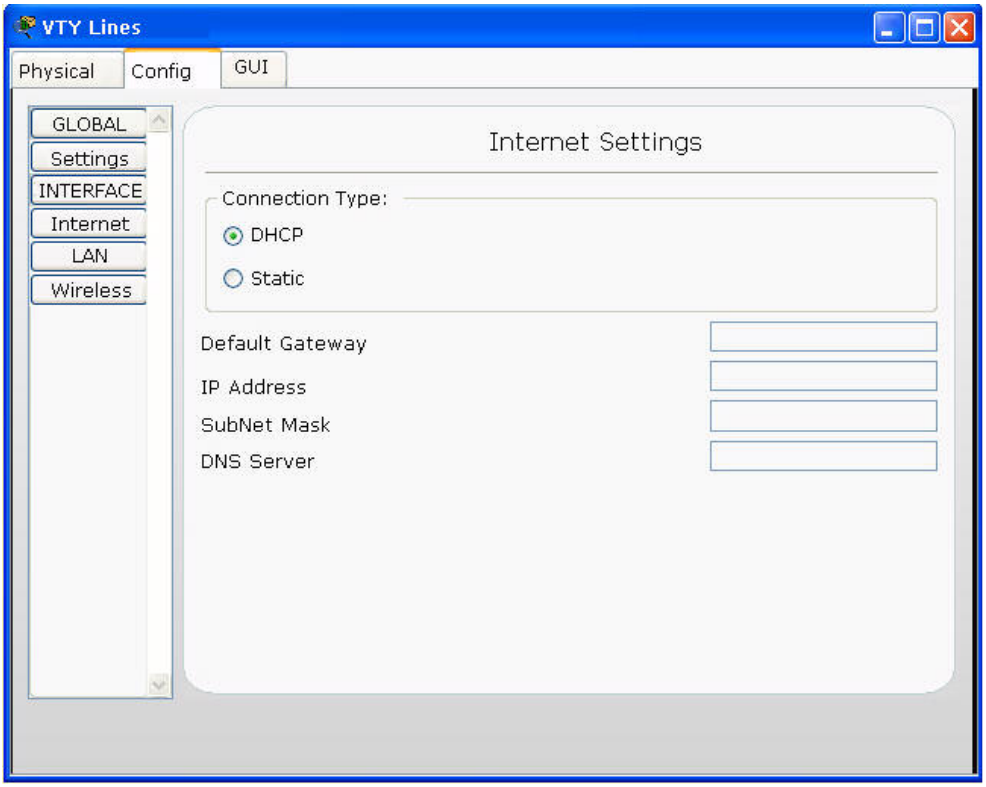


تنظیمات Global:

در تنظیمات Global می توان نام نمایش داده شده در صفحه را تغییر داد.

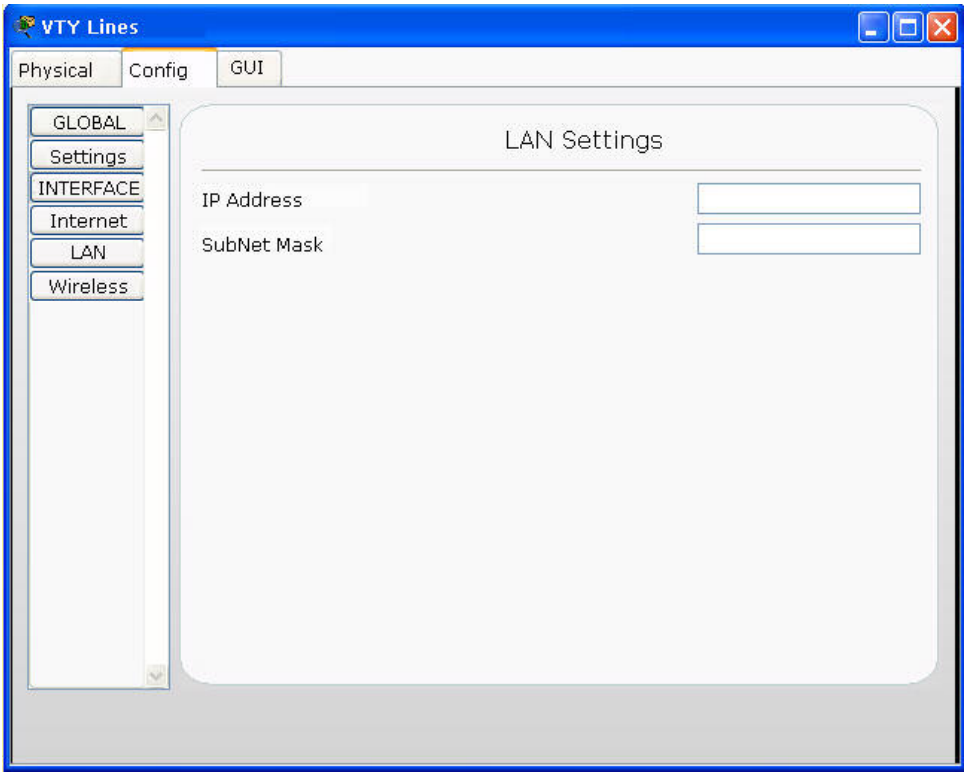
تنظیمات واسط اینترنت:

در تنظیمات Internet نوع اتصال و این که IP به صورت اتوماتیک از DHCP گرفته شود یا به طور دستی، می توان تنظیم نمود.



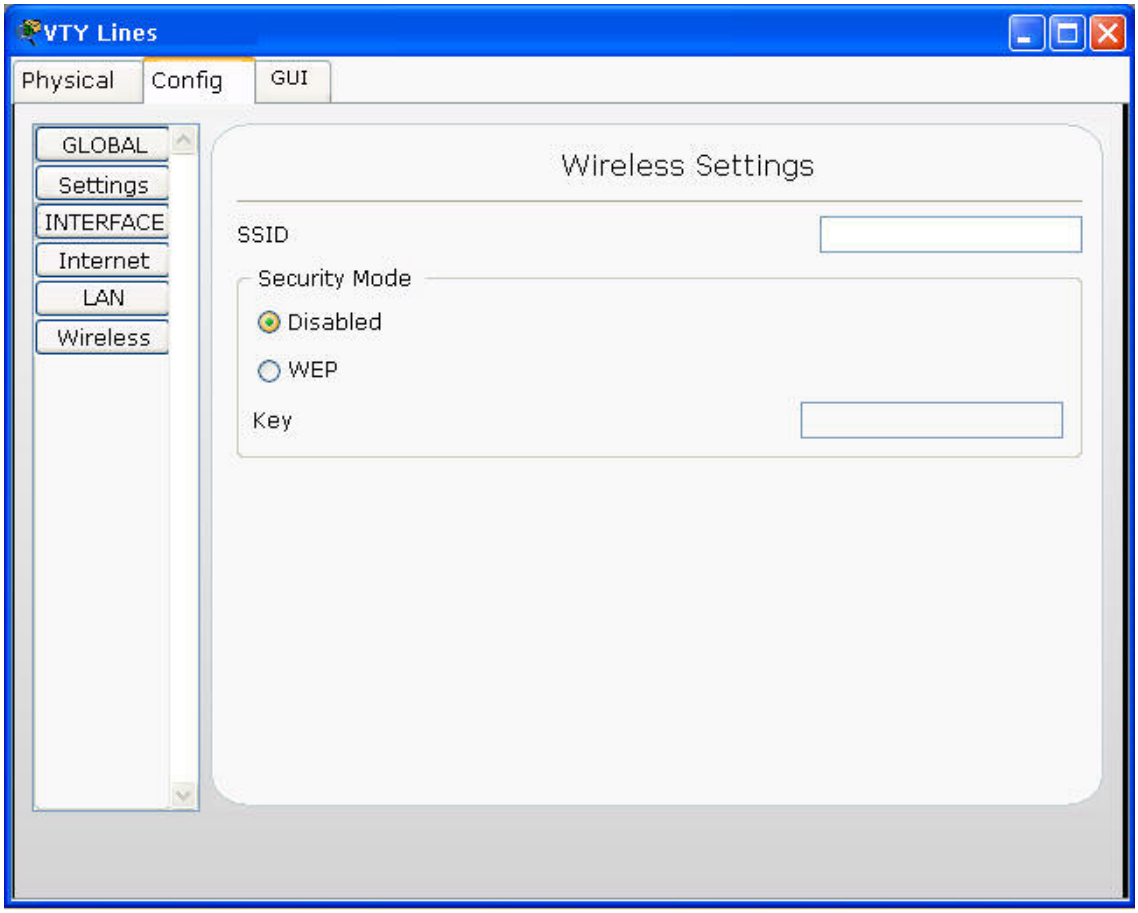
تنظیمات واسط LAN:

در تنظیمات LAN آدرس IP و ماسک زیر شبکه LAN تنظیم می گردد.



پیکربندی واسط Wireless:

در تنظیمات بیسیم، می توان SSID ، گزینه امنیتی WEP، و کلید احراز هویت را تنظیم نمود.

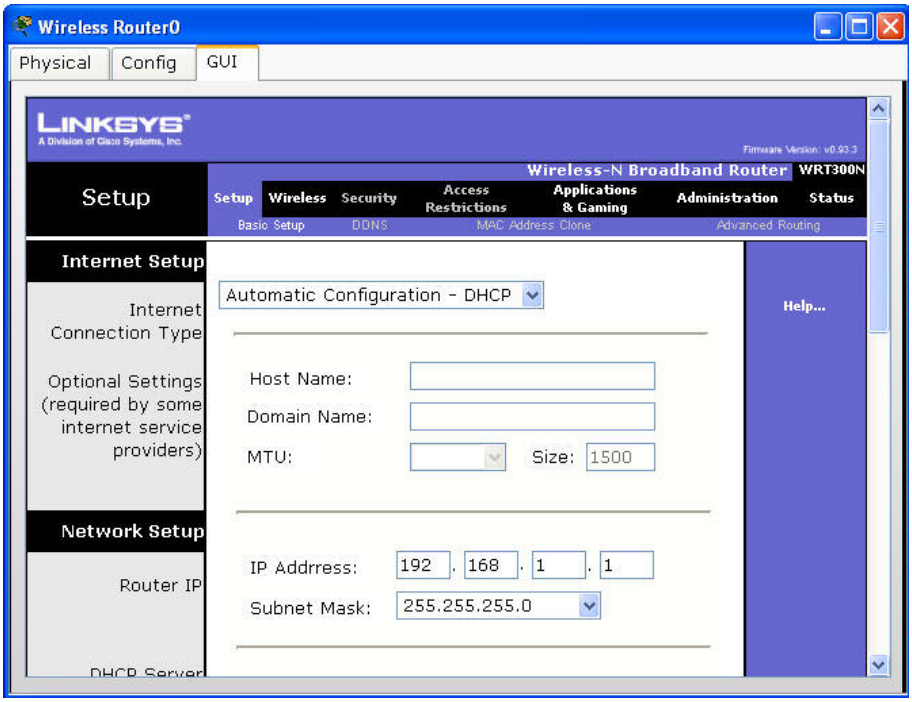


واسط گرافیکی Linksys WRT300N:

برگه GUI، پیکربندی ها و تنظیمات مشابه برگه Config و همچنین تعدادی ویژگی دیگر برای port forwarding و مدیریت دارد. برای اعمال تنظیمات می بایست بر روی دکمه Save Settings کلیک کنید.

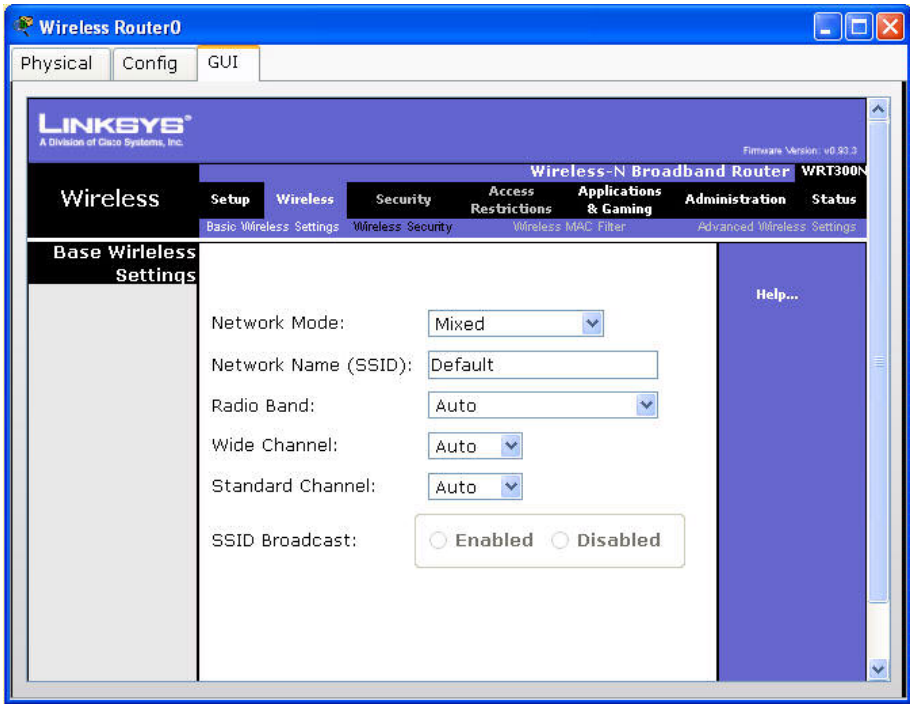
پیکربندی Setup:

در برگه Setup زیر برگه Basic Setup، می توان اتوماتیک یا استاتیک نوع اتصال اینترنت را مشخص نمود. تنظیمات آدرس IP و DHCP در قسمت Network Setup انجام می گیرد.



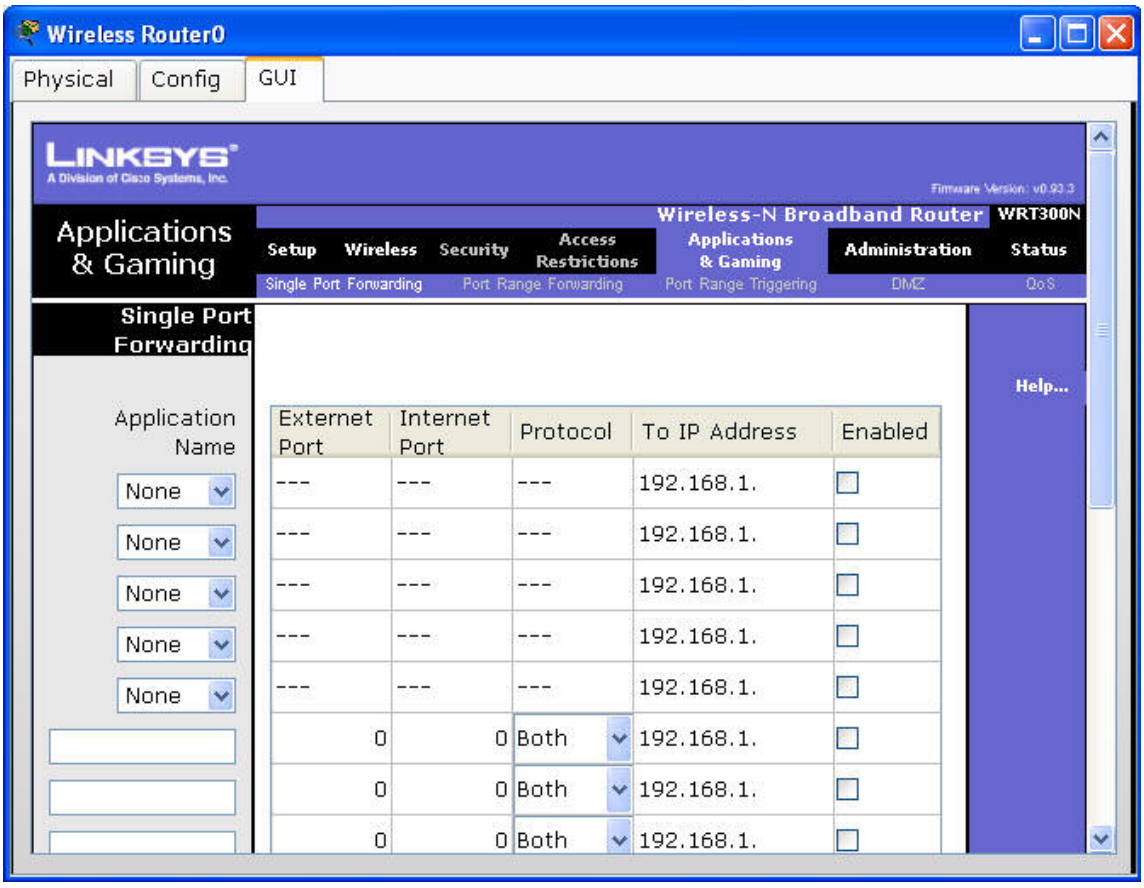
پیکربندی Wireless:

در برگه Wireless زیر برگه Basic Wireless Settings، تنها تنظیمی که قابل تغییر است Network Name (SSID) است. در زیر برگه Wireless Security حالت امنیتی را می توان غیرفعال یا آن را بر روی WEP تنظیم کرد. و یک کلید برای احراز هویت تعیین نمود.



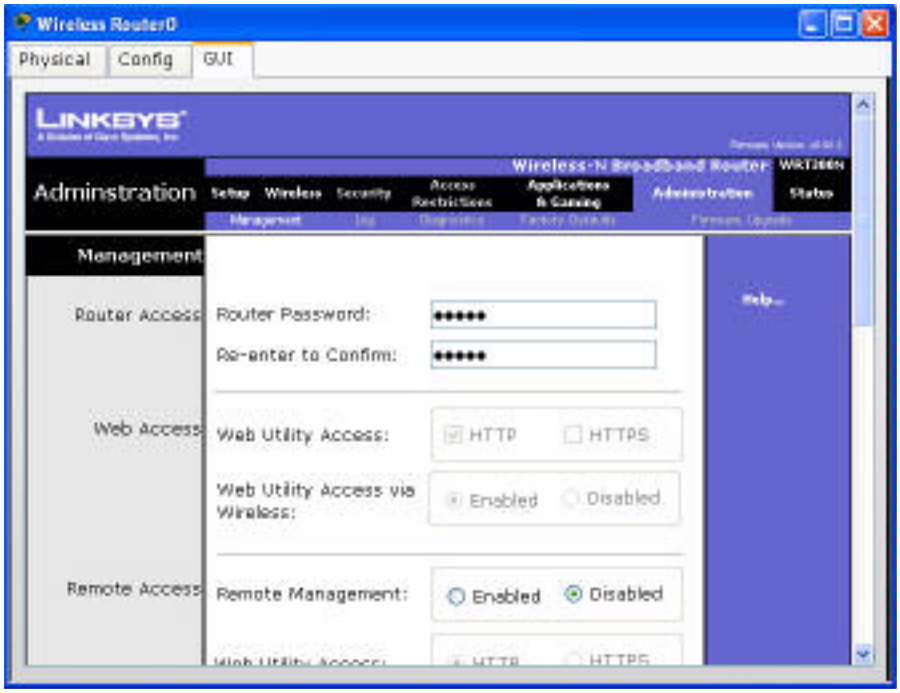
پیکربندی Application & Gaming:

در برگه Application&Gaming زیر برگه Single Port Forwarding می توان بسته ها را به آدرس IP دلخواه ارسال کرد. برای forward کردن یک بسته، برنامه مورد نظر را از قسمت Name Application انتخاب و آدرس IP را که قصد دارید بسته ها به آنجا ارسال شوند را در ستون To IP Address وارد کنید. سپس در ستون Enable آنرا فعال نمائید. برای ارسال به یک پورت دلخواه می بایست External Port و Internal Port را نیز تعیین کرد. External پورتی است که مسیریاب Linksys از سمت WAN به آن گوش می دهد. Internal پورتی است که بسته ها را به سرور محلی شما ارسال می کند.



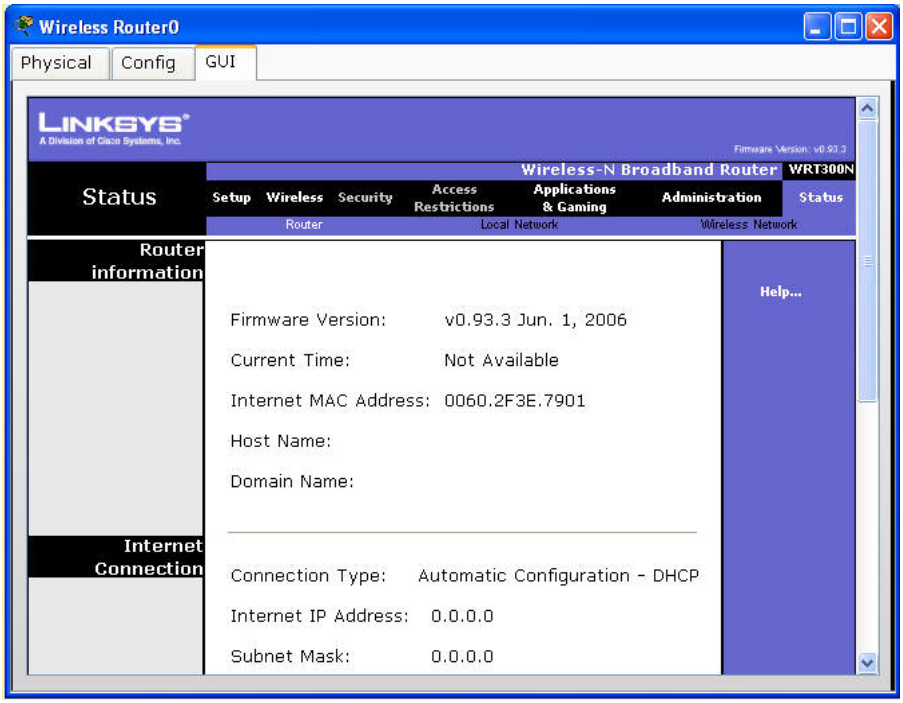
Administration Management:

در برگه Administration زیر برگه Management، می توان کلمه عبور پیش فرض را برای دسترسی به مسیریاب از طریق تنظیمات وب با استفاده مرورگر وب PC انجام داد. وManagement Remote را فعال نمود.



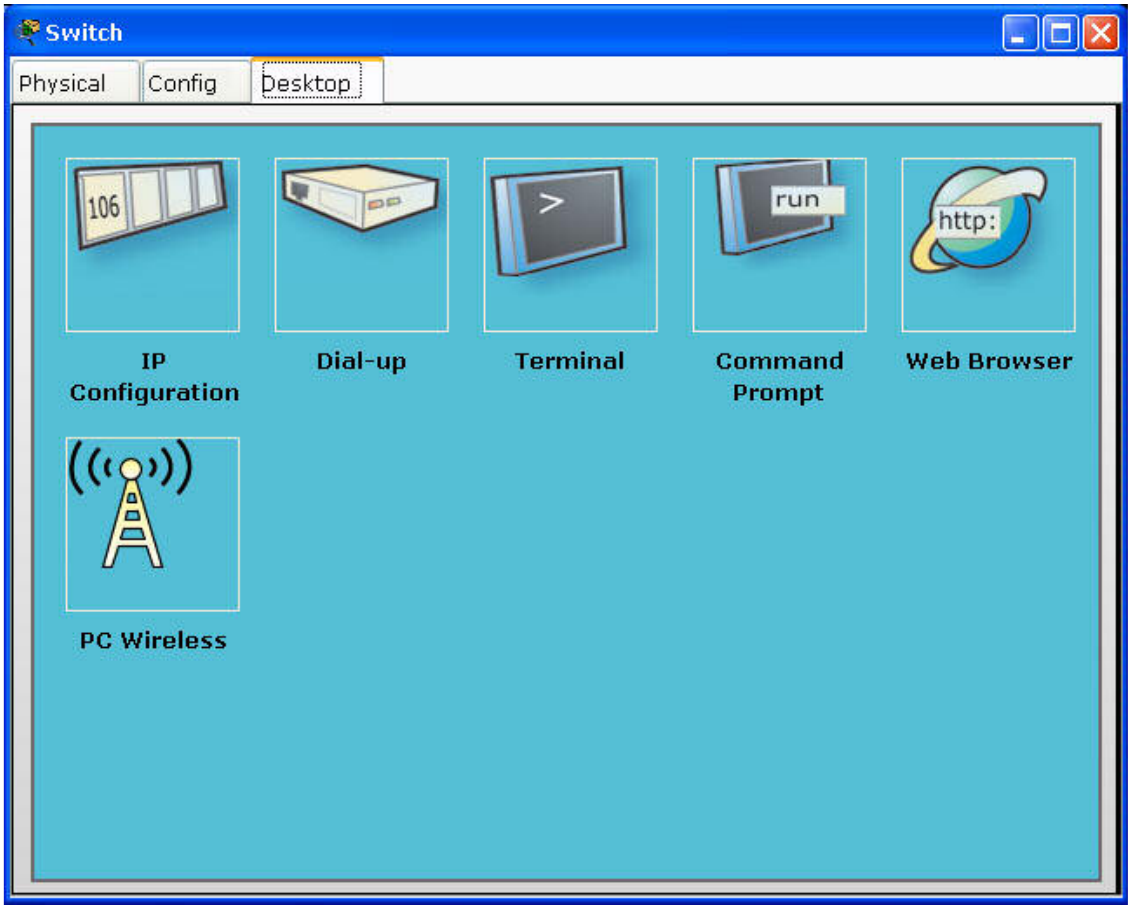
Status:

در برگه Status می توانید اطلاعات مختلف مربوط به مسیریاب، شبکه محلی و شبکه بی سیم را مشاهده کنید.



پیکربندی PC

در برگه Config شما می توانید تنظیمات Global و Interface را انجام دهید. علاوه براین برگه Desktop ابزارهایی را برای پیکربندی IP ، پیکربندی diul-up ، استفاده از پنجره terminal ، باز کردن واسط خط فرمان، بازکردن مرورگر وب و پیکربندی تنظیمات بی سیم Linksys فراهم می کند.



تنظیمات Global:

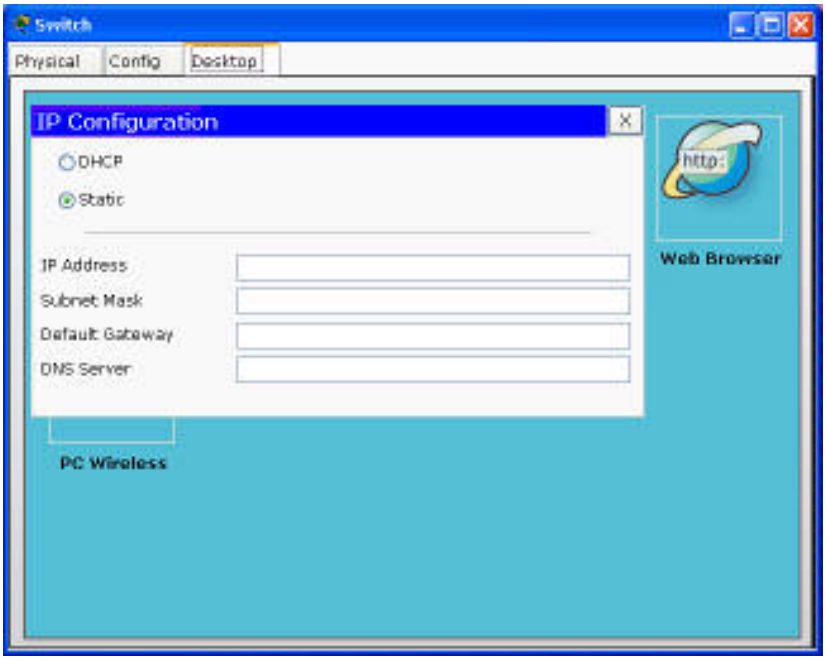
در تنظیمات global نام نمایش داده شده در صفحه، تنظیمات آدرس IP به صورت استاتیک یا پویا، و نیز Gateway و DNS Server را نیز می توان مشخص نمود.

پیکربندی Interface:

رایانه ها می توانند یک واسط اترنت (مسی یا فیبر)، مودم یا بی سیم را پشتیبانی کنند. وضعیت پورت، پهنای باند، Duplex و آدرس MAC ، آدرس IP و ماسک زیرشبکه را برای واسط می توان تنظیم کرد که البته با توجه به نوع واسط متغییر است.

ابزار IP Configuration:

در برگه Desktop روی آیکن IP Configuration کلیک نموده تا این ابزار باز شود. اگر PC به یک مسیریاب یا سرور DHCP متصل باشد، با استفاده از DHCP به طور خودکار IP می گیرد، در غیر اینصورت باید IP به صورت استاتیک تنظیم شود.

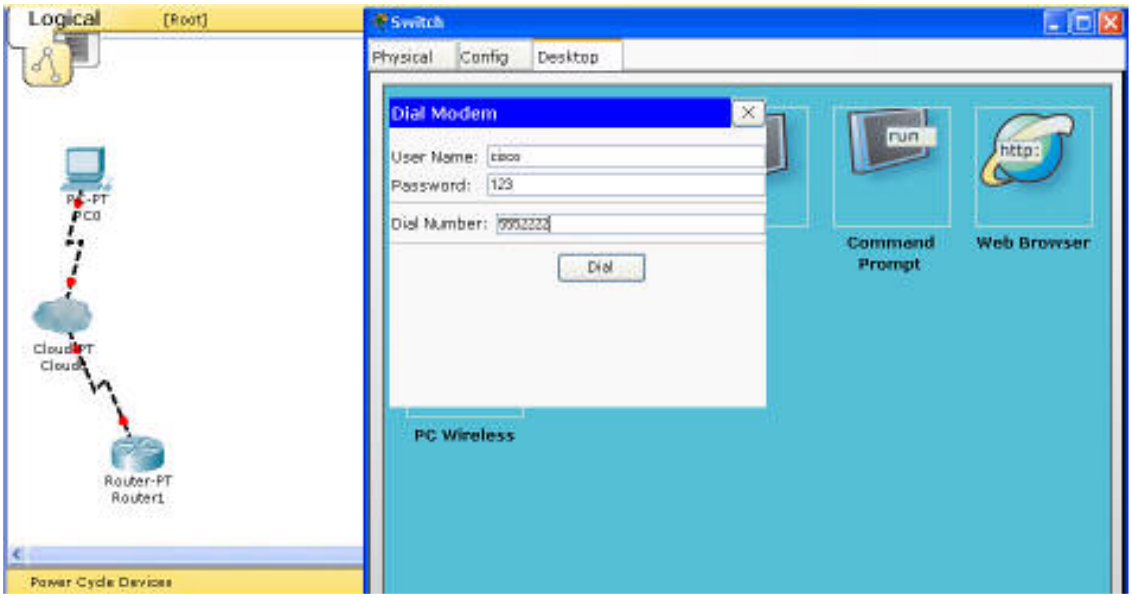


ابزار Modem Dial-Up:

در برگه Desktop، بر روی آیکن Dial-up کلیک کنید تا ابزار آن باز شود. اتصال مودم را می توان با اتصال PC به یک ابر که به روتر متصل است برقرار نمود. ابر مانند یک شرکت تلفن بین PC و مسیریاب عمل می کند. برای برقراری تماس باید شرایط مختلفی برقرار باشد.

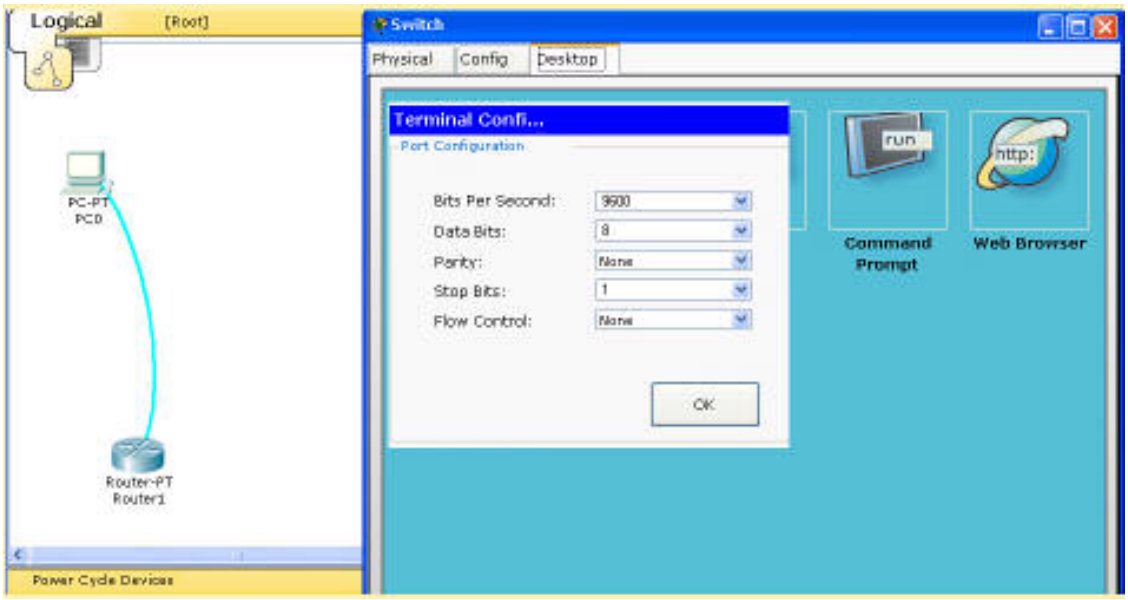
- مسیریاب یک مودم دارد و شما احراز هویت با نام کاربری را در مسیریاب راه اندازی کرده‌اید (با استفاده از دستور username WORD password LINE در حالت global IOS)
- پورت مودم ابر یک شماره تلفن معتبر دارد
- شما نام کاربری و کلمه عبور و شماره اتصال را وارد کرده اید.

اگر همه نیازمندی ها فراهم شده باشد، با کلیک بر روی دکمه Dial اتصال برقرار می شود. وضعیت خط به شما موفقیت اتصال را نشان می دهد و با استفاده از دکمه Disconnect می توان به اتصال خاتمه داد. برای Ping کردن بین PC و مسیریاب باید دقت نمود تا همه تنظیمات IP مربوطه به طور دستی انجام شود.



ابزار Terminal:

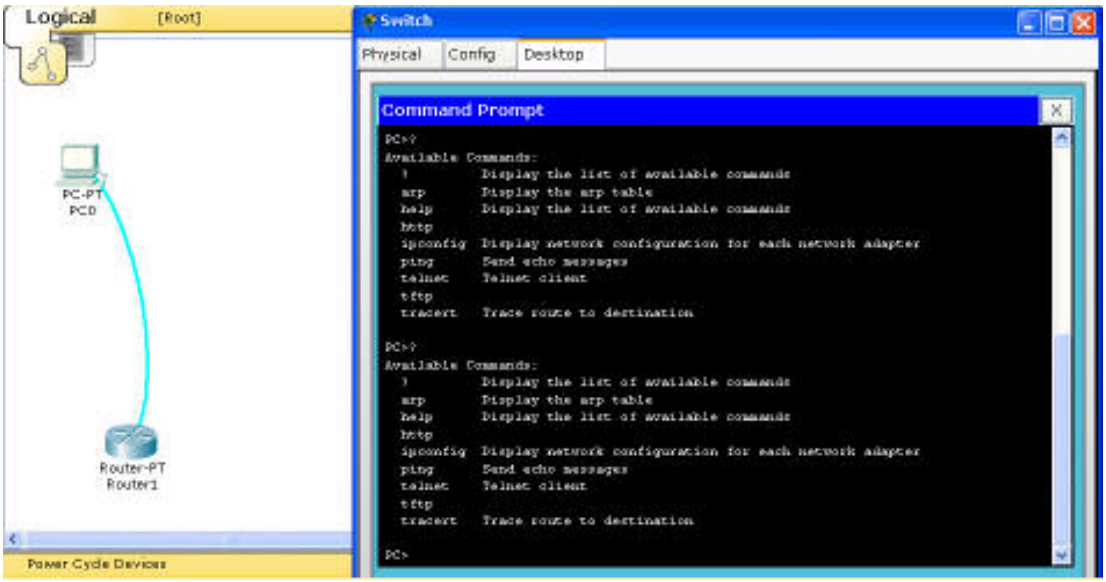
رایانه متصل به یک مسیریاب یا سوئیچ از طریق اتصال کنسول (پورت RS 232) از برنامه Terminal برای دسترسی به CLI دستگاه مورد نظر استفاده می کند. در برگه Desktop روی آیکن Terminal کلیک نموده تا این ابزار باز شود. پارامترهای مناسب را برای بخش کنسول تنظیم و سپس Ok را کلیک کنید تا پنجره Terminal با CLI دستگاه راه دور باز شود.



ابزار خط فرمان:

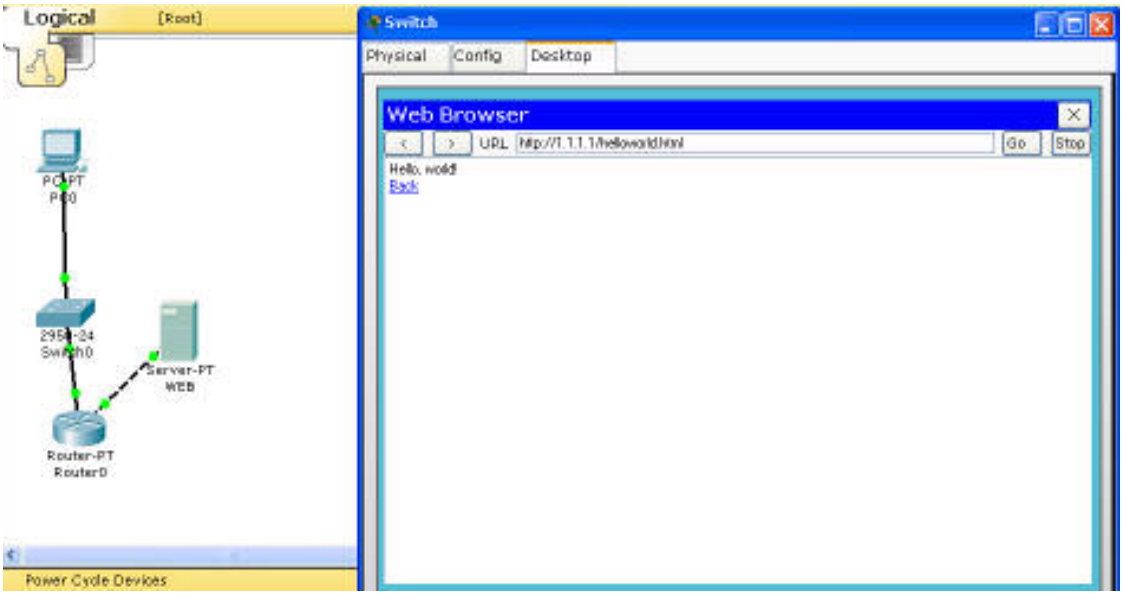
در برگه Desktop بر روی دکمه Command Prompt کلیک تا خط فرمان باز شود. در خط فرمان شما می دستورات زیر را صادر کنید:

- **?**
- **arp**
- **help**
- **ipconfig**
- **netstat**
- **ping**
- **telnet**
- **tracert**



ابزار مرورگر وب:

در برگه Desktop با کلیک روی دکمه Web Browser مرورگر وب را باز نمائید. مرورگر وب امکان دسترسی به پیکربندی های وب سرور Linksys را می دهد. اگر PC مستقیم یا غیرمستقیم به سرور با سرویس فعال HTTP متصل باشد، می توانید نام دامنه یا آدرس IP آن را برای دسترسی به وب سایت سرور وارد کنید. اگر رایانه به مسیریاب بی سیم Linksys WRT300N متصل باشد، می توانید آدرس IP مسیریاب را برای دسترسی به پیکربندی های وب آن وارد کنید. که در این حالت یک اعلان ورود نام کاربری و کلمه عبور ظاهر می شود (به طور پیش فرض هر دو admin است)



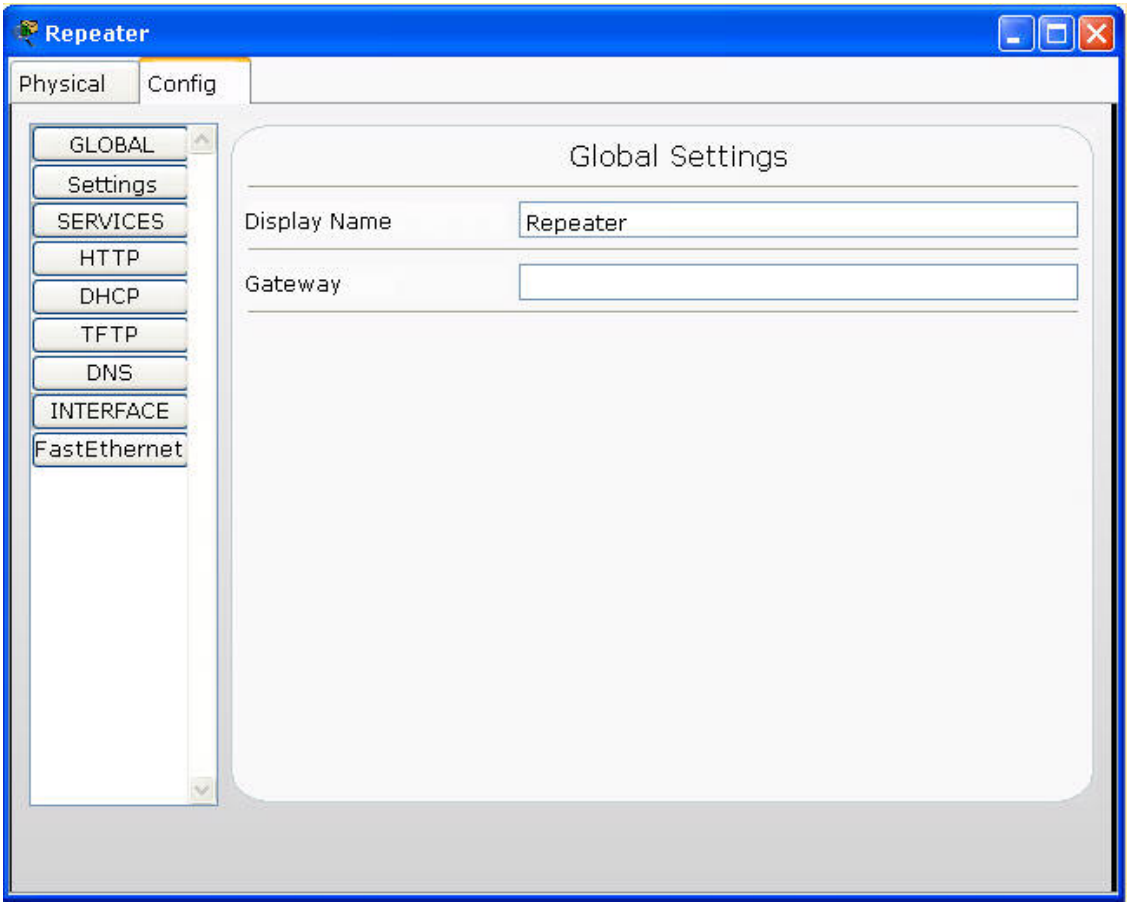
ابزار PC Wireless:

در برگه Desktop بر روی دکمه PC Wireless کلیک تا نرم افزار کلاینت بی سیم باز شود. برای دسترسی به این قسمت ماژول Linksys-WMP300N مورد نیاز است. در این قسمت می توان اطلاعات اتصال را مشاهده نمود. به هر شبکه بیسیم موجود در محدوده خود متصل شوید و پروفایل هایی را برای اتصال به مسیریاب های بی سیم ایجاد/ ویرایش/ حذف کنید.



پیکربندی سرورها

در برگه Config سه سطح پیکربندی global ، services و interface وجود دارد. برای پیکربندی در سطح global دکمه GLOBAL را کلیک کنید تا settings نمایش داده شود. برای پیکربندی سرویس ها بر روی دکمه SERVICES برای پیکربندی واسط ها بر روی دکمه INTERFACE کلیک کنید.

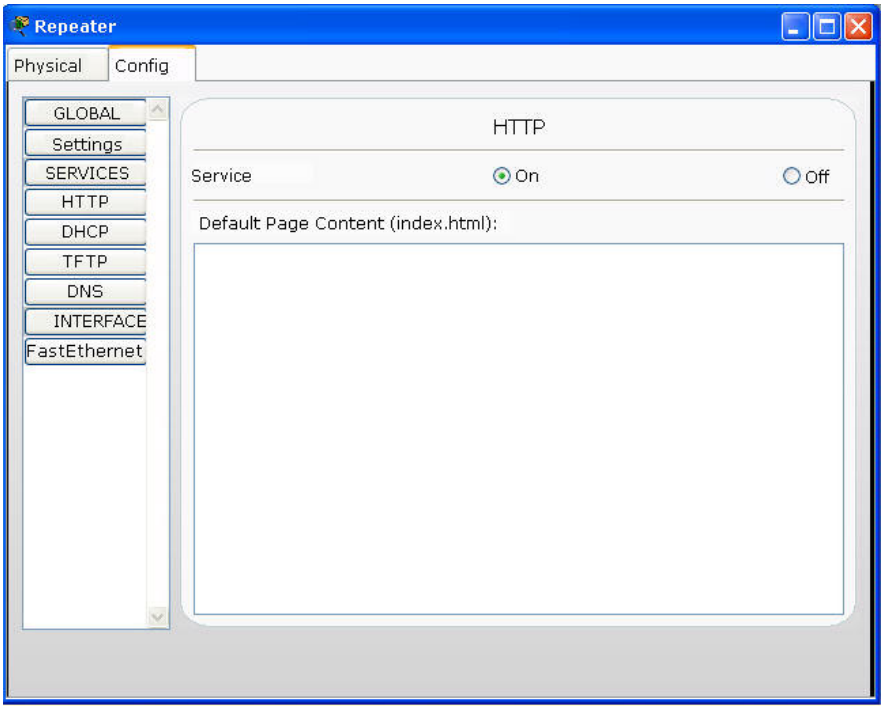


تنظیمات Global:

در تنظیمات global می توان نام و Gateway را تنظیم نمود.

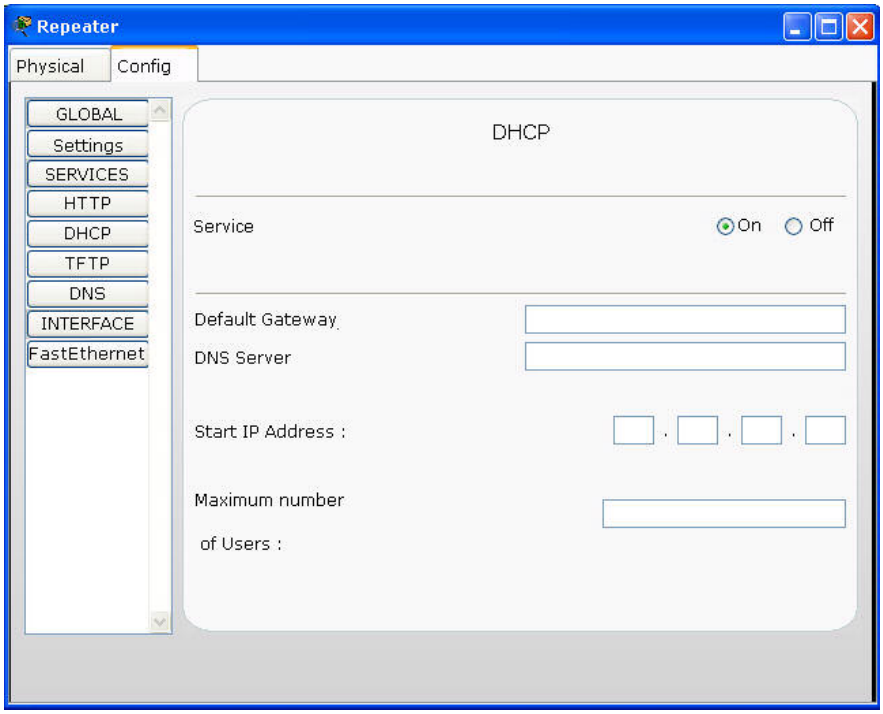
پیکربندی سرویس HTTP:

در قسمت سرویس HTTP می توان محتوای صفحه پیش فرض (index.html) را با استفاده از برخی تگ های HTML ویرایش کرد. وقتی رایانه ای به صفحه وب سرور با استفاده از مرورگر وب دسترسی پیدا کند، این صفحه به او نمایش داده خواهد شد.



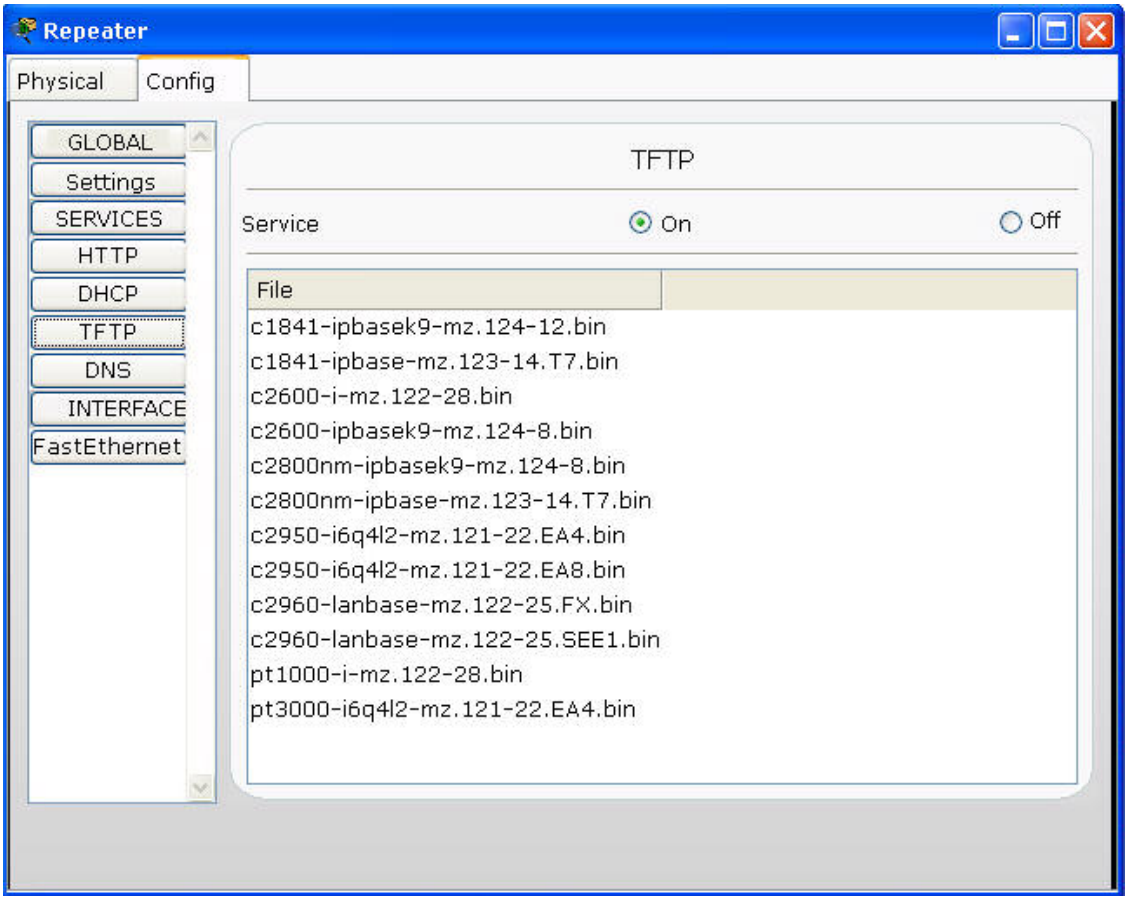
پیکربندی سرویس DHCP:

در برگه DHCP می توان تنظیمات سرور DHCP را انجام داد. پارامترهای Default Gateway ، DNS Servr، آدرس IP اولیه و حداکثر تعداد کاربران برای دریافت آدرس IP را می توانید ویرایش نمائید.



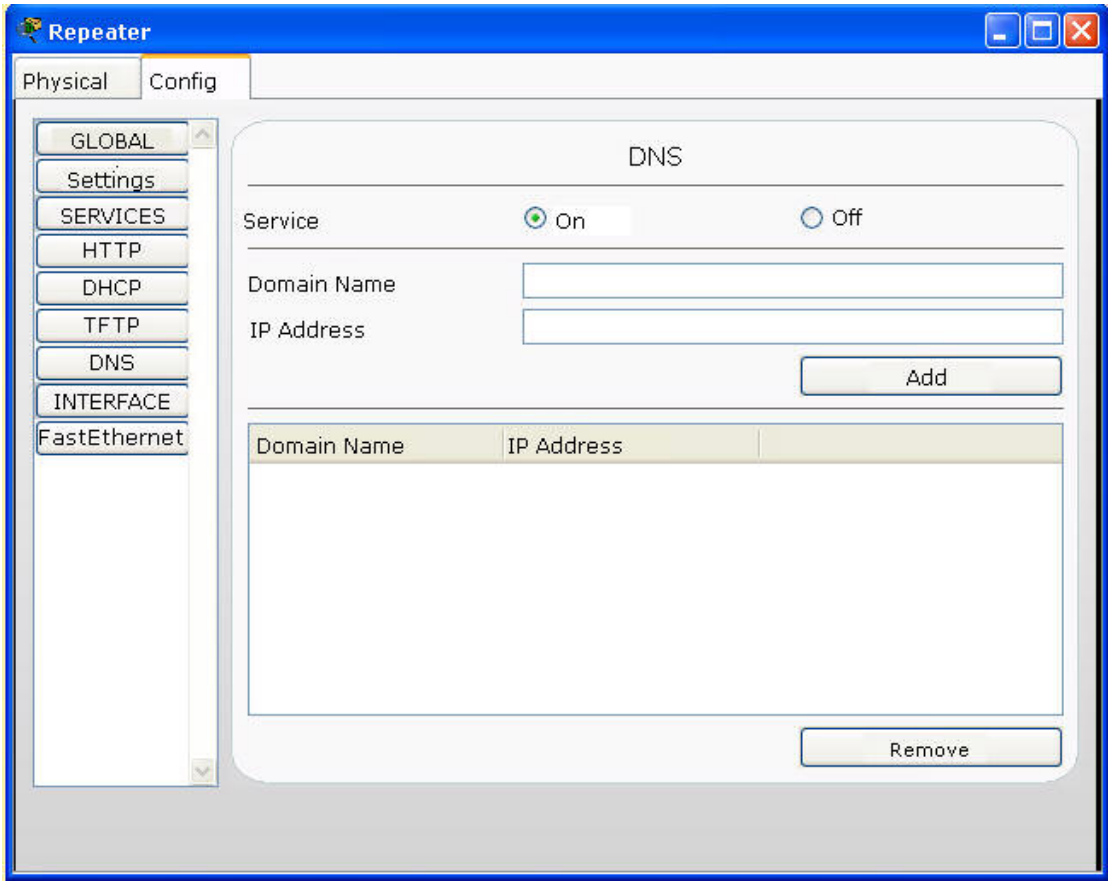
پیکربندی سرویس TFTP:

در سرویس TFTP پارامتری برای تنظیم وجود ندارد. سرویس TFTP شامل یک پایگاه داده ثابت از تصاویر IOS است که می تواند توسط فلش مسیریاب ها و سوئیچ ها مورد استفاده قرار بگیرد.



پیکربندی سرویس DNS:

در پیکربندی سرویس DNS می توان DNS سرور را برای ترجمه نام دامنه به آدرس IP راه اندازی کرد. برای این کار نام دامنه را در Domain Name و آدرس IP آن را در IP Address وارد و سپس دکمه Add را کلیک نمایید. برای حذف هر آیتم از DNS از دکمه Remove استفاده می شود.



پیکربندی واسط:

سرورها یک واسط اترنت (مسی و فیبر)، مودم یا بی سیم را پشتیبانی می کنند. بسته به نوع پورت وضعیت پورت، پهنای باند، Duplex، آدرس MAC، آدرس IP و ماسک زیر شبکه قابل تنظیم است.

پیکربندی ابر (cloud)

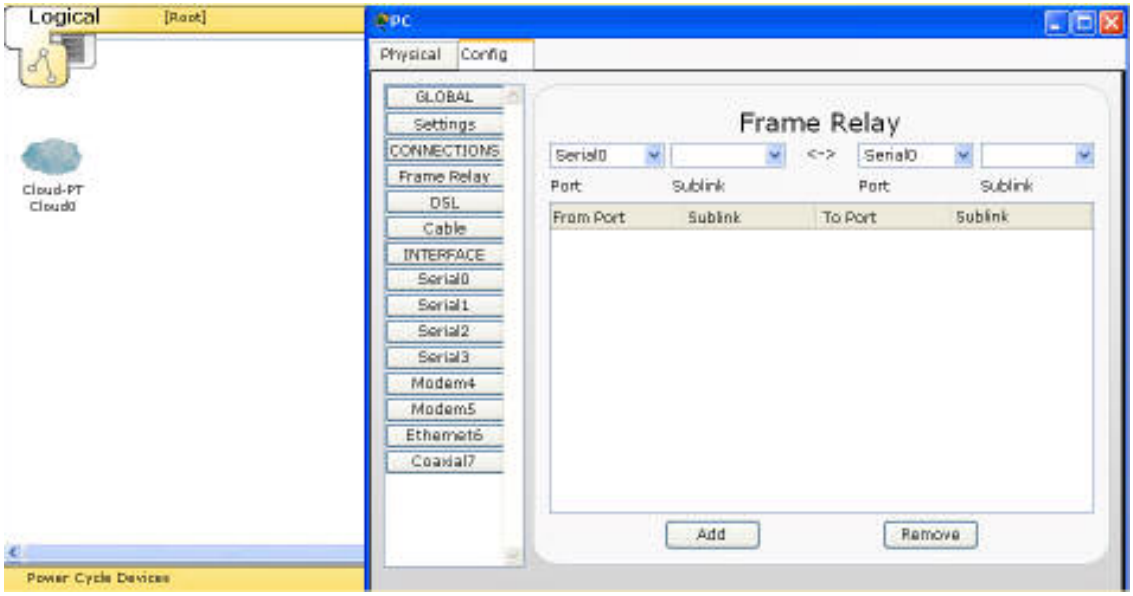
برگه Config سه سطح تنظیمات global، connections و interface را فراهم می کند که برای پیکربندی هر سطح باید بر روی دکمه های GLOBAL، CONNECTIONS یا INTERFACE کلیک کنید.

تنظیمات Global:

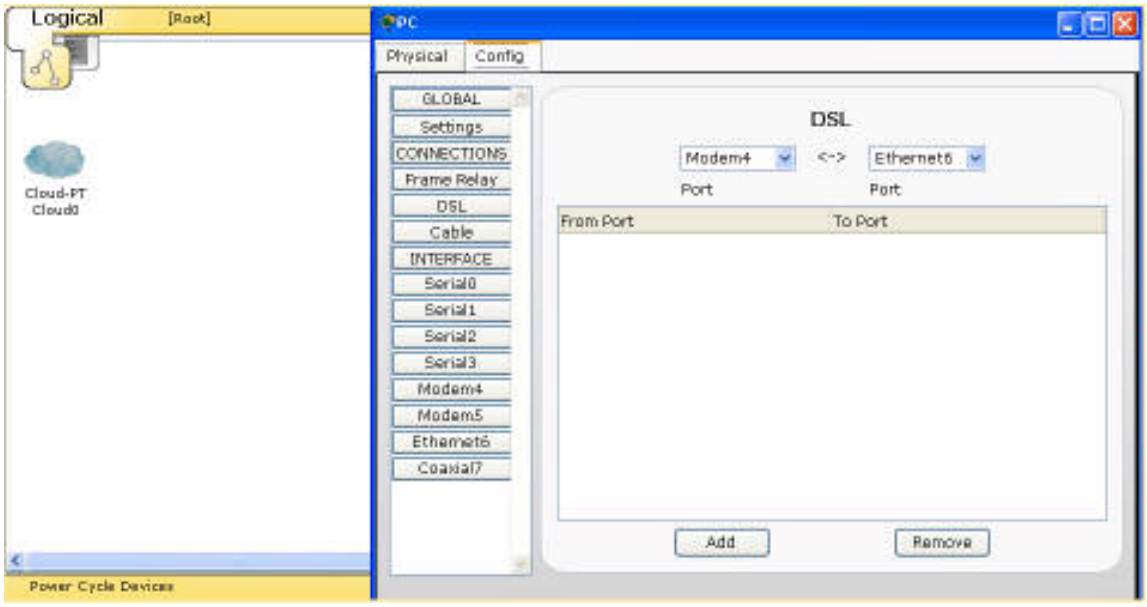
برای تغییر نام ابر استفاده می شود.

تنظیمات Connections:

در قسمت Frame Relay می توان اتصالات Frame Relay را برقرار کرد. برای اینکار ابتدا DLCI ها را در واسط های سریال پیکربندی نموده سپس از سمت چپ یکی از زیر لینک های یک پورت را انتخاب و از سمت راست یکی از زیرلینک های پورتی دیگر را انتخاب کنید. روی دکمه Add کلیک کنید تا یک اتصال بین دو زیرلینک برقرار شود.

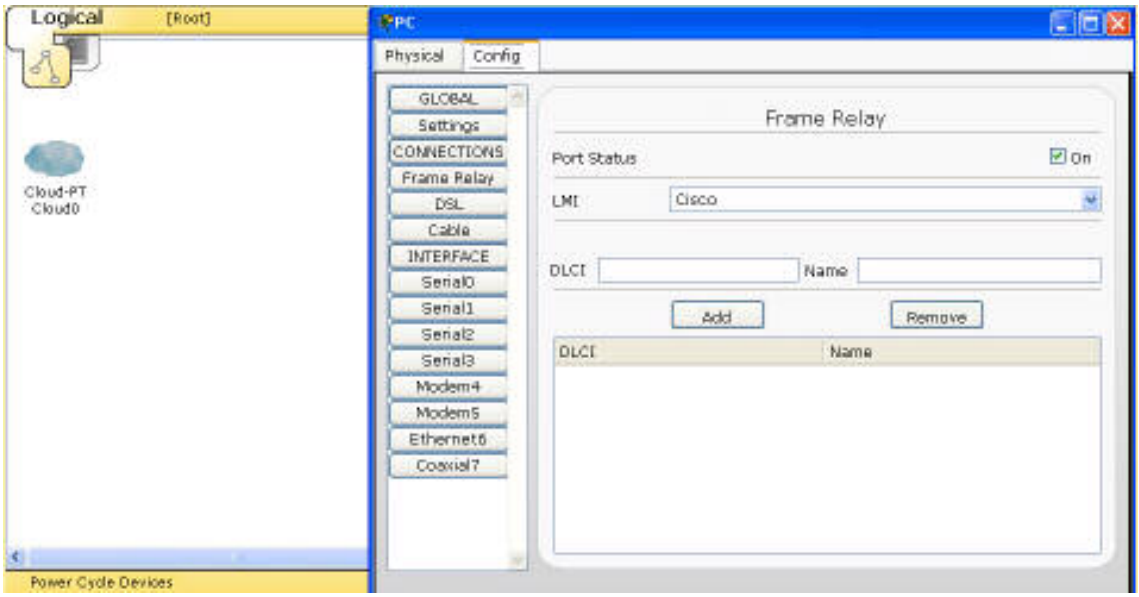


همچنین می توانید از قسمت DSL یا Cable برای برقراری اتصال بین پورت های مودم (برای DSL) یا پورت های کواکسیال (برای Cable) به پورت های اترنت استفاده کنید.



پیکربندی Interface:

ابر می تواند ۴ نوع واسط مودم، اترنت، کواکسیال و سریال را پشتیبانی کند. برای پورت مودم می توانید شماره تلفنی که دستگاه دیگر بتواند از آن استفاده کند را مشخص کنید. همچنین برای پورت اترنت می توان Provider Network را یا برای DSL یا برای Cable مشخص نمود. برای پورت coaxial تنظیمی وجود ندارد. ضمن این که برای پورت سریال می توان وضعیت پورت را مشخص، LMI را انتخاب و DLCI واسط را تنظیم نمود. برای افزودن یک DLCI یک نام و شماره منحصر به فرد وارد و دکمه Add را کلیک تا به لیست افزوده شود.



پیکربندی دستگاه های دیگر

تنظیمات پیکربندی برای سایر دستگاه ها نسبتا ساده است. نام آنها را می توان تغییر داده و یا تنظیمات پایه را برای هر واسط انجام داد.

پل ها

پل مثل سوئیچ دو پورت داشته و فاقد VLAN و trunk می باشد.

تکرار کننده

وسیله ای ساده با دو پورت است که سیگنال دریافت شده در یک پورت را از پورت دیگر مجددا ارسال می کند. تنظیمات پورت این وسیله قابل تغییر نیست.

هاب

مانند تکرار کننده دارای چند پورت است و سیگنال دریافتی را به همه پورت های دیگر ارسال می کند.

نقطه دسترسی

همچون تکرار کننده با یک پورت بی سیم و یک پورت اترنت است.

چاپگر

تنظیمات چاپگر همانند سرور است بجز این که فاقد سرویس های آن می باشد.

IP Phone

IP Phone گزینه قابل تنظیمی ندارد و توسط DHCP پیکربندی می شود.

DSL Modem

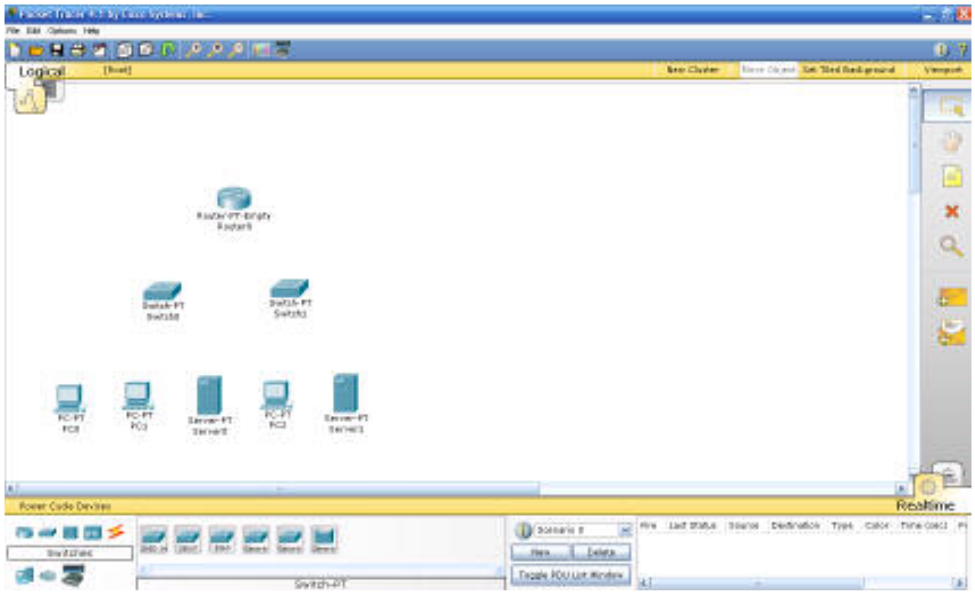
این مودم گزینه قابل تنظیمی ندارد.

Cable Modem

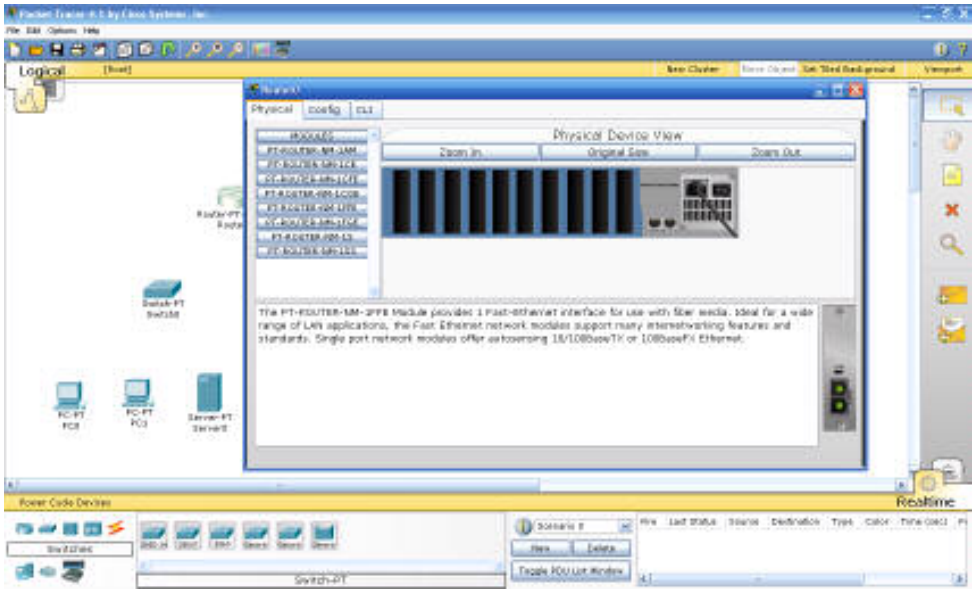
این مودم گزینه قابل تنظیمی ندارد.

۴۱-۱۵- مثال عملی) قسمت اول- ایجاد یک شبکه

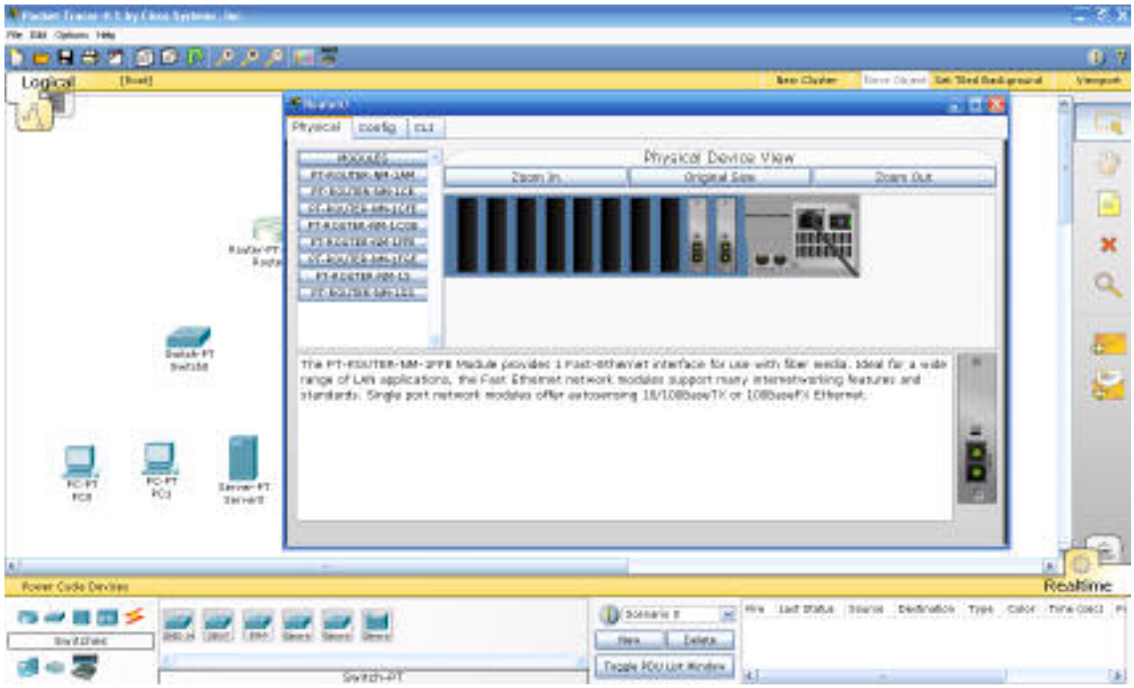
در این قسمت قصد داریم یک شبکه فرضی با امکانات و ویژگی های مختلف ایجاد کنیم. برای این منظور ابتدا دستگاه های مورد نیاز را وارد فضای کار کنید. این دستگاه ها شامل ۳ رایانه، ۲ سرور، ۲ سوئیچ و یک مسیریاب می باشند.



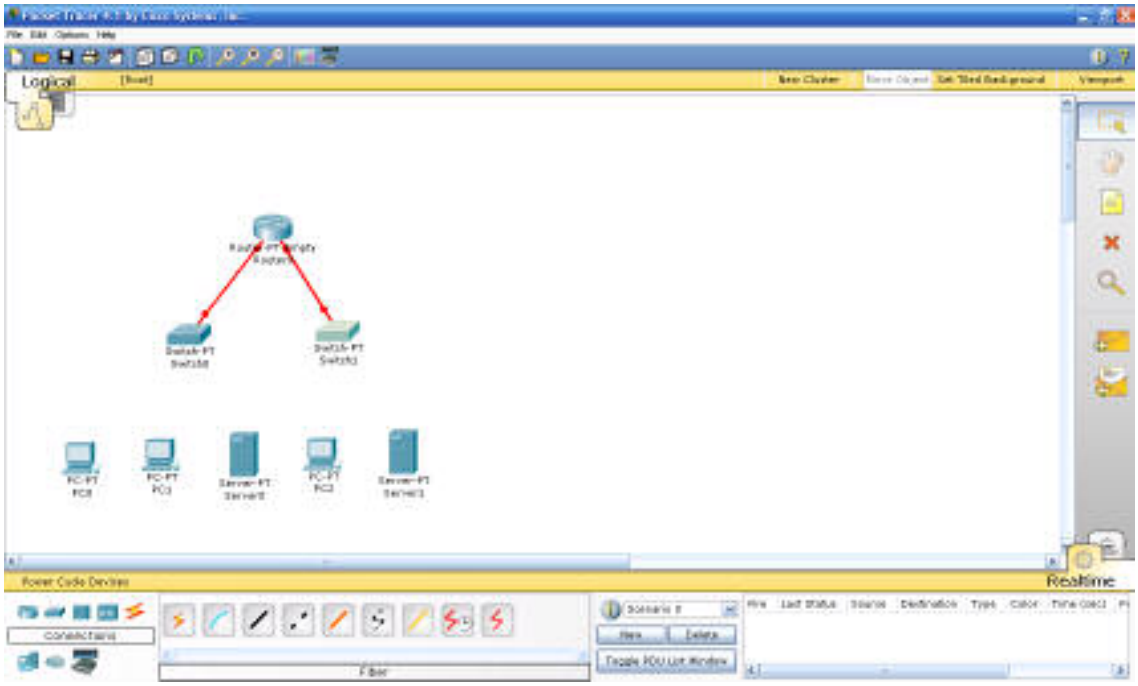
مسیریاب را از نوع Router-PT-Empty انتخاب کرده تا بتوان ماژول های مورد نیاز را به صورت دستی به آن اضافه نمود. بنابراین روی آن کلیک کرده تا صفحه تنظیمات آن باز شود. پس از خاموش کردن مسیریاب، ماژول PT-Router-NM-1FFE را از سمت چپ انتخاب کنید.



این ماژول را با درگ کردن در دو شیار از روتر قرار داده و سپس روتر را روشن کنید.

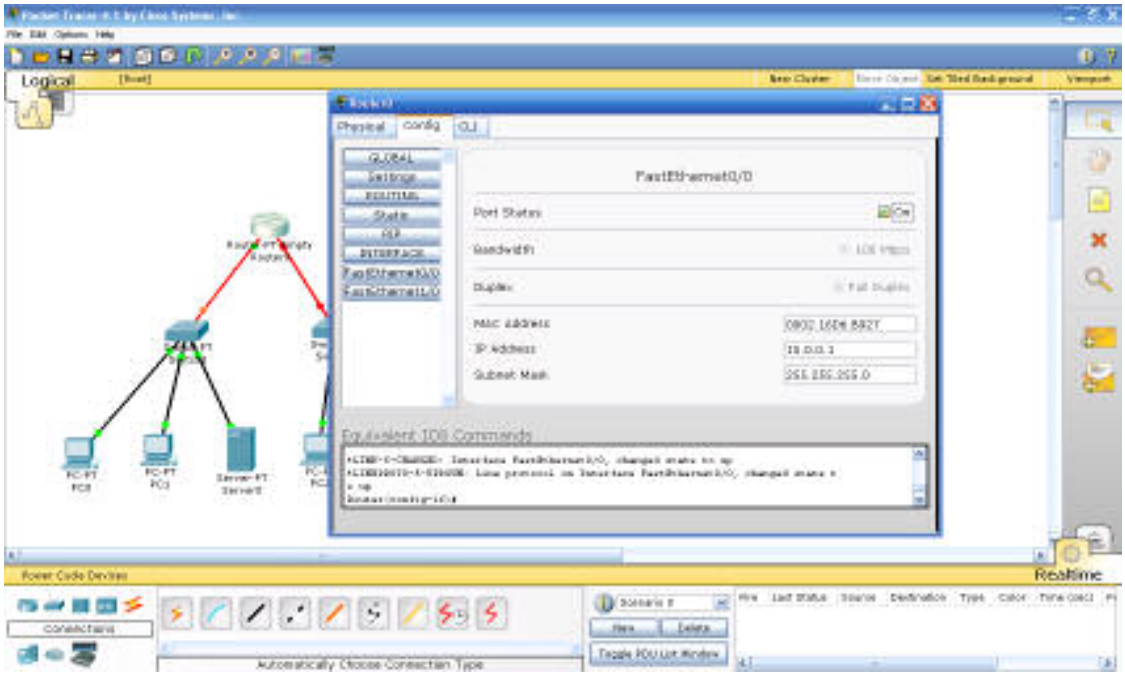


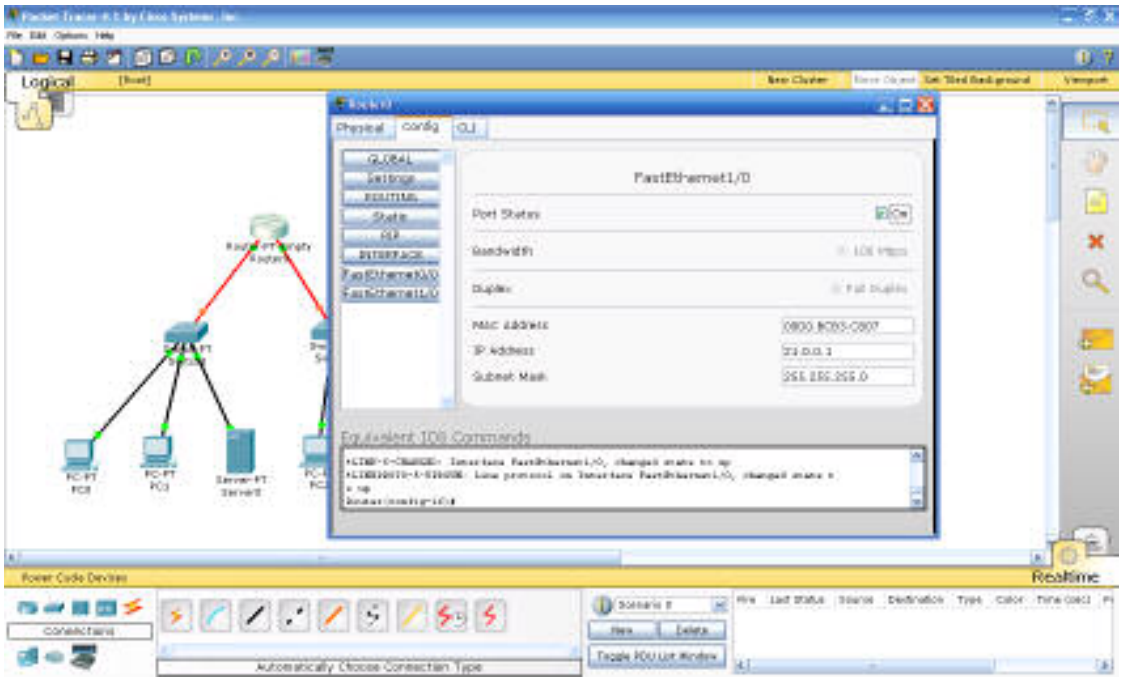
حال با استفاده از کابل فیبرنوری، اتصال بین مسیریاب و سوئیچ ها را برقرار نمایید.



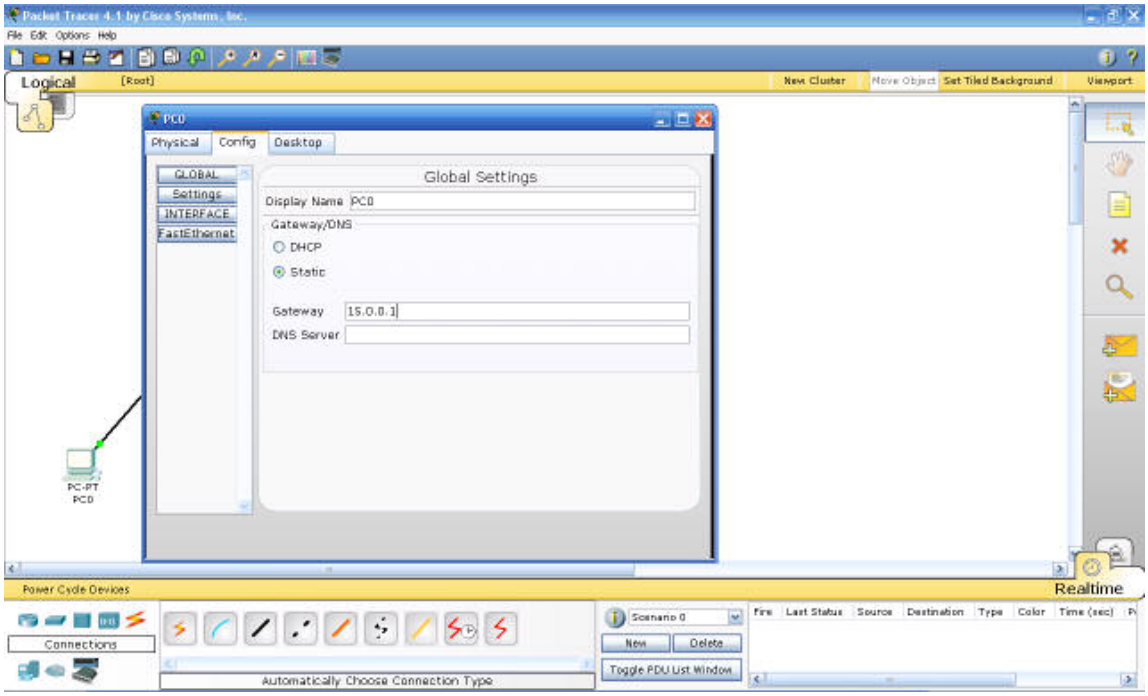
سپس با استفاده از آیکن اتصال اتوماتیک، اتصال سایر دستگاه ها را به سوئیچ مطابق شکل برقرار کنید. برای فعال کردن اتصال مسیریاب، می بایست واسط های آن را پیکربندی نمود. بنابراین روی

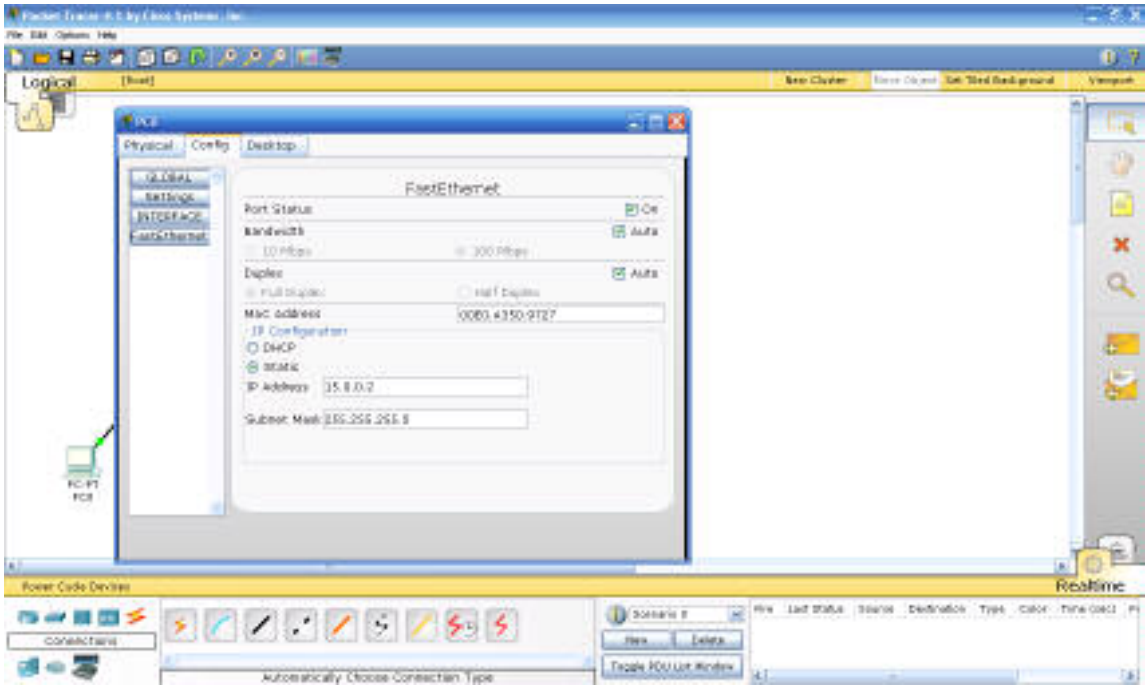
مسیریاب کلیک و در برگه config به ترتیب واسط های FastEthernet0/0 و FastEthernet1/0 را انتخاب کرده و تنظیمات را مطابق شکل انجام دهید.



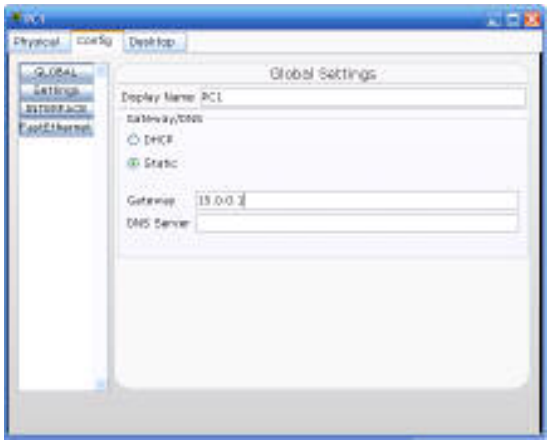


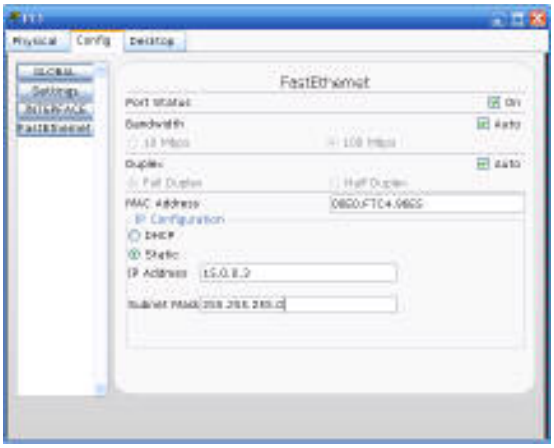
حال نوبت به پیکربندی سایر دستگاه ها می رسد. برای این دستگاه ها می بایست آدرس Gateway و IP و ماسک زیر شبکه مشخص شود. تنظیمات PC0 به صورت زیر می باشد.

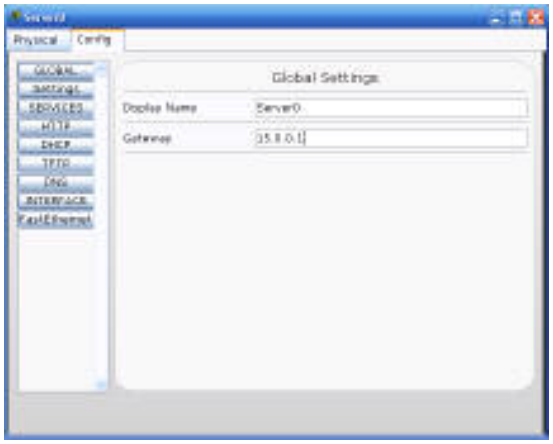


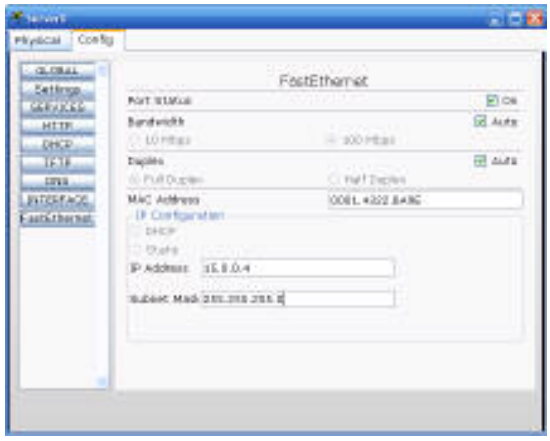


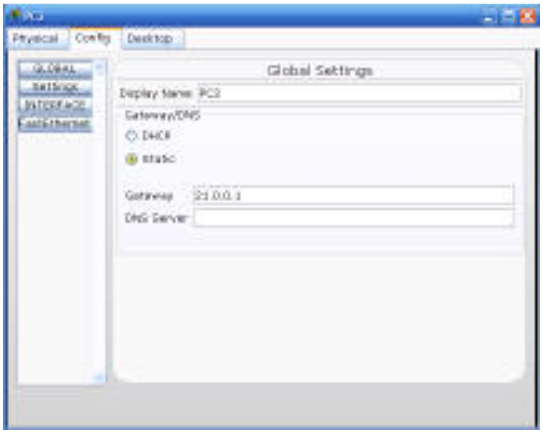
به همین ترتیب تنظیمات PC1 ، Server0 ، PC2 و Server1 به صورت زیر انجام می شود.

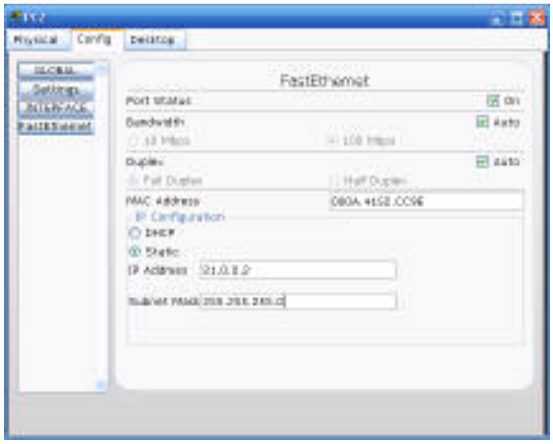


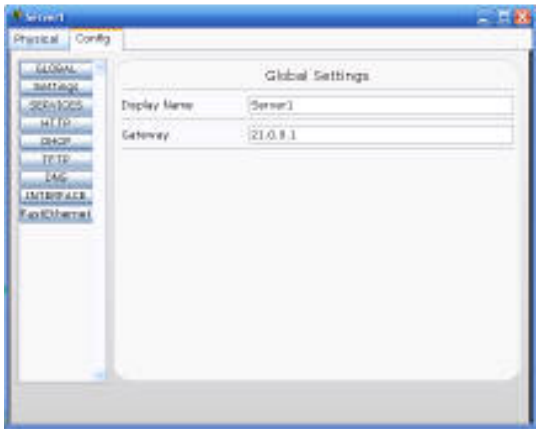


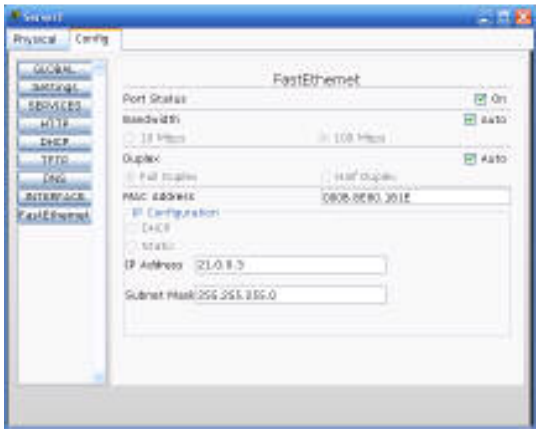




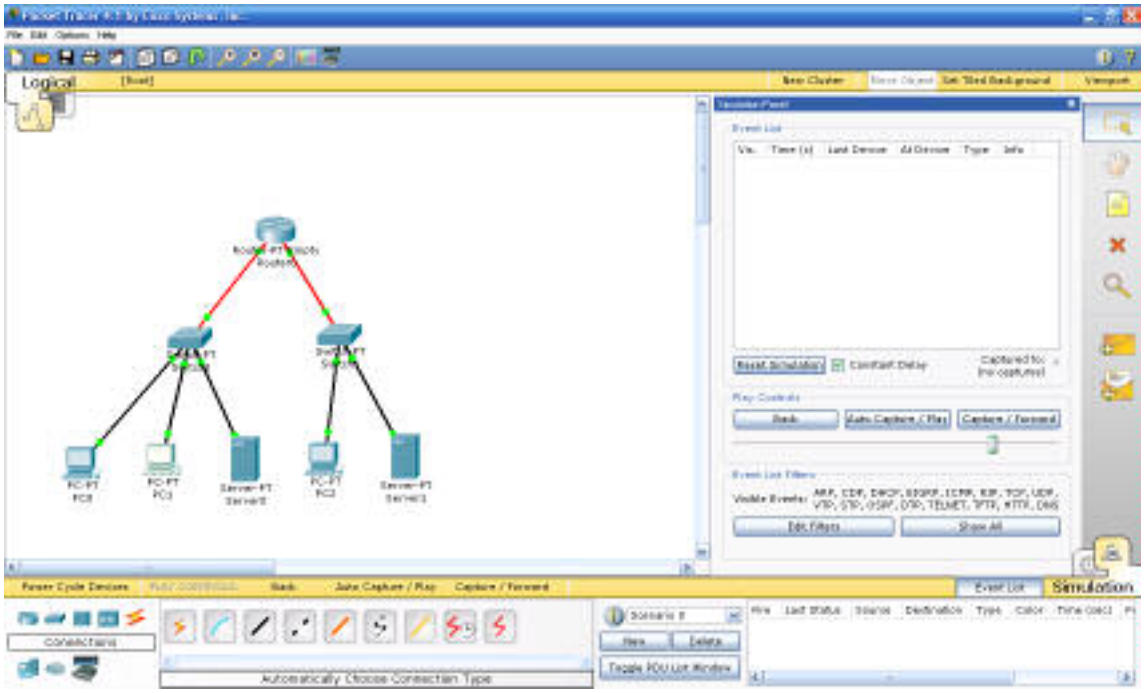




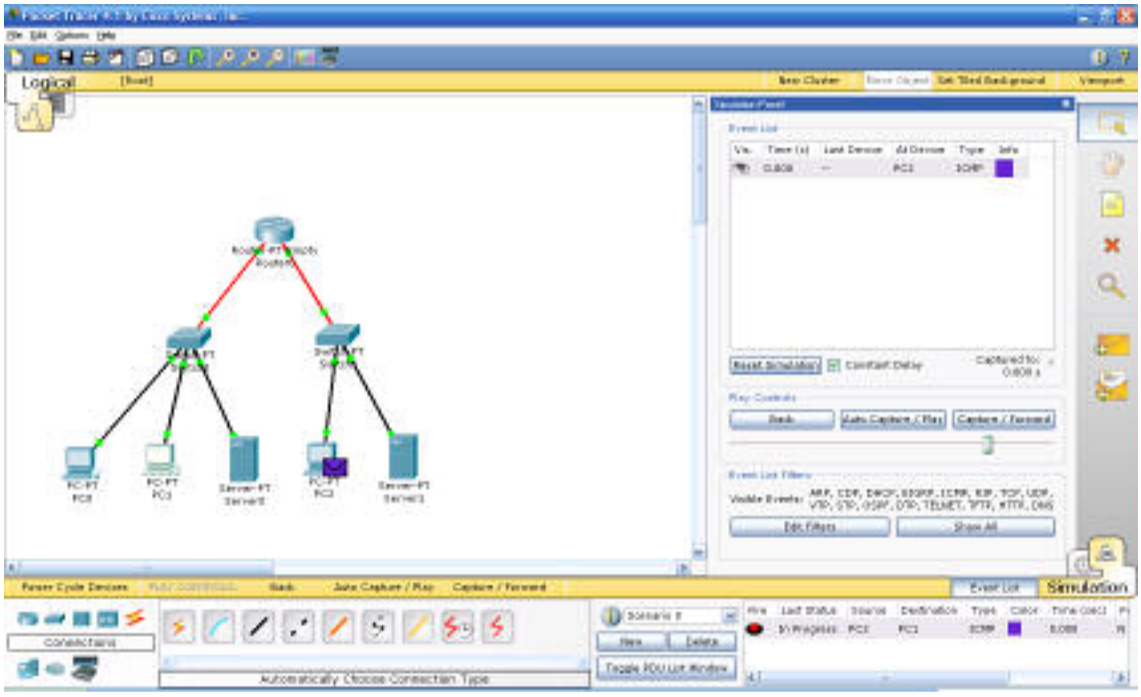




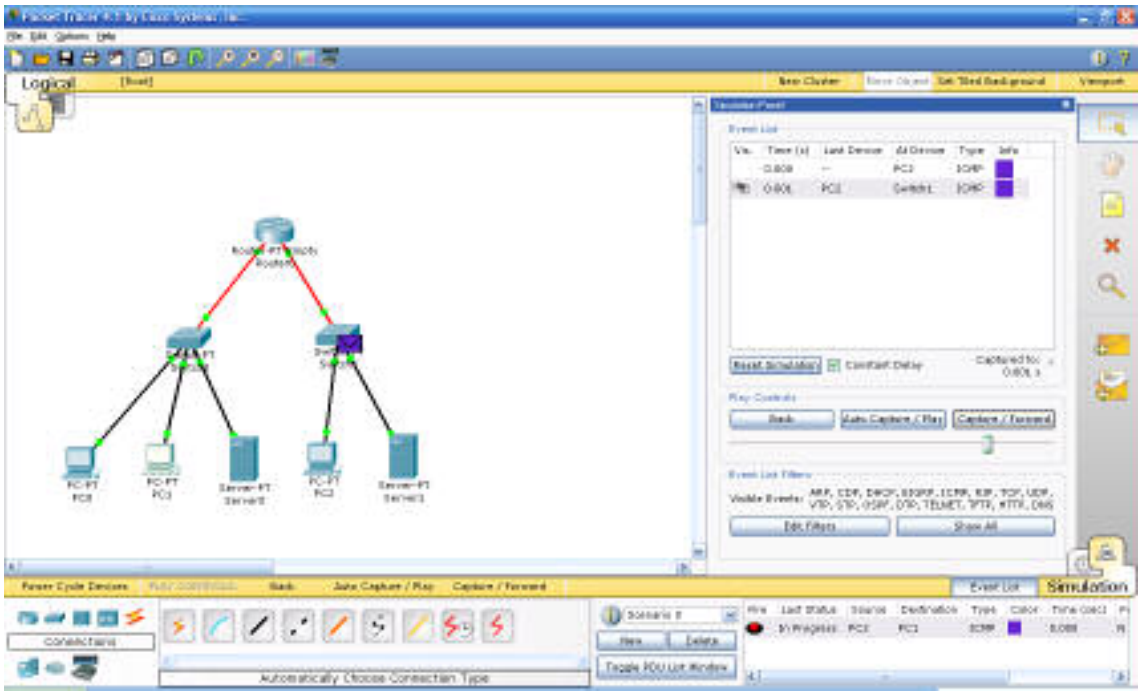
حال توپولوژی منطقی شبکه آماده است و می توانید در بخش شبیه سازی آن را تست کنید.



پس از ورودی به حالت simulation یک بسته از نوع Simple PDU از PC2 به PC1 ایجاد کنید.

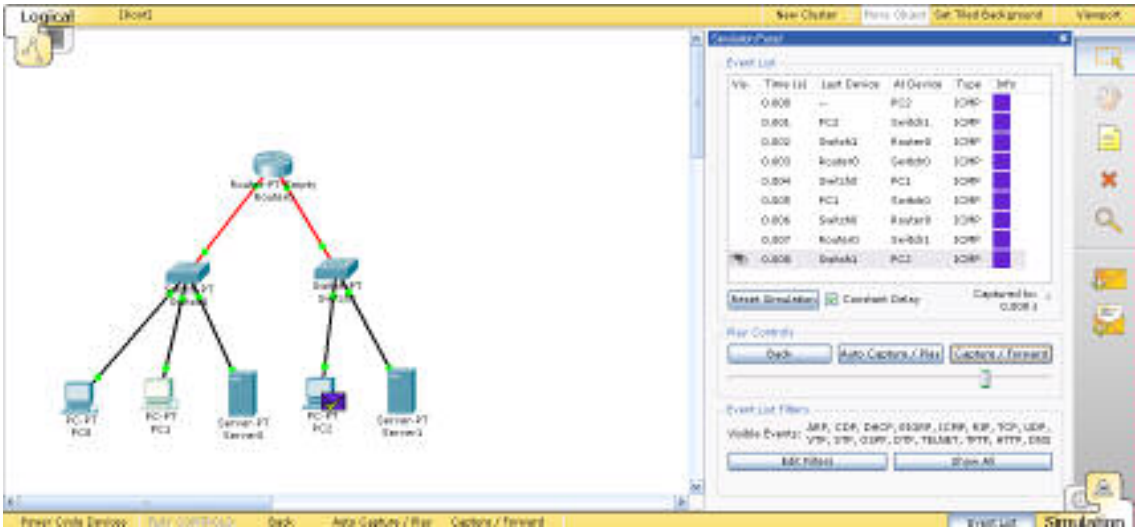


به طور منظم بر روی دکمه Capture/Forward کلیک و مراحلی را که بسته در شبکه طی می کند دنبال کنید.

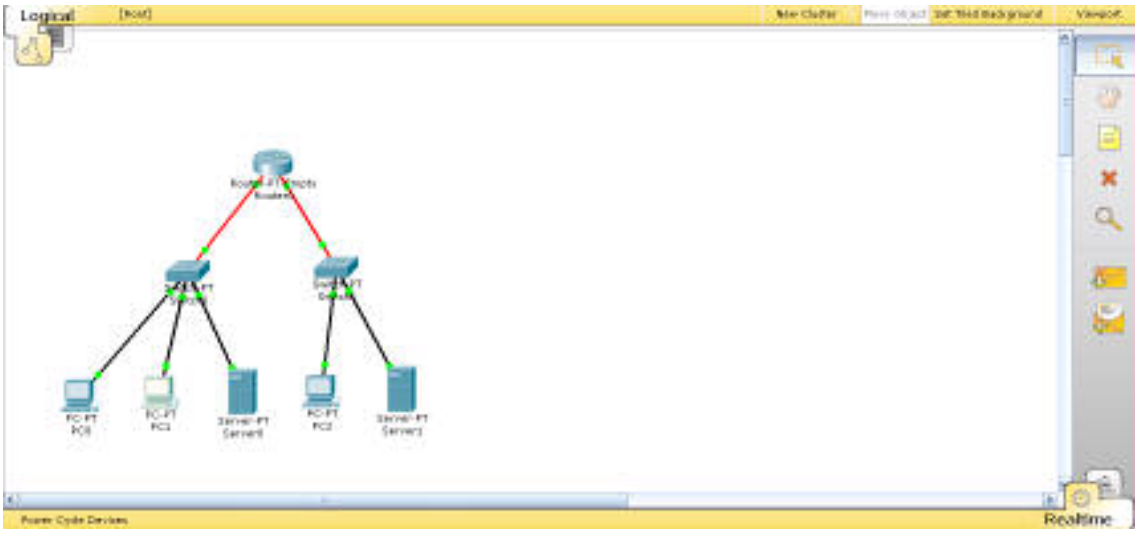



Logical
[Root]
Simulation
Logical
[Root]
Simulation
Logical
[Root]
New Cluster
Move Object
Set Tiled Background
Viewport
Simulation Panel
Event List
Vis.
Time (s)
Last Device
At Device
Type
Info
0.000
PC2
ICMP
0.001
PC2
Switch1
ICMP
0.002
Switch1
Router0
ICMP
0.003
Router0
Switch0
ICMP
0.004
Switch0
PC1
ICMP
Reset Simulation
Constant Delay
Captured to:
0.004 s
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters
Visible Events:
ARP, CDP, DHCP, EIGRP, ICMP, RIP, TCP, UDP, VTP, STP, OSPF, DTP, TELNET, TFTP, HTTP, DNS
Edit Filters
Show All
Router-PT-Empty
Router0
Switch0
Switch1
PC-PT
PC0
PC-PT
PC1
Server-PT
Server0
PC-PT
PC2
Server-PT
Server1
Power Cycle Devices
PLAY CONTROLS:
Back
Auto Capture / Play
Capture / Forward
Event List
Simulation


Logical
[Root]
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Back
Auto Capture / Play
Capture / Forward
Event List Filters
Edit Filters
Show All
Power Cycle Devices
Event List
Simulation

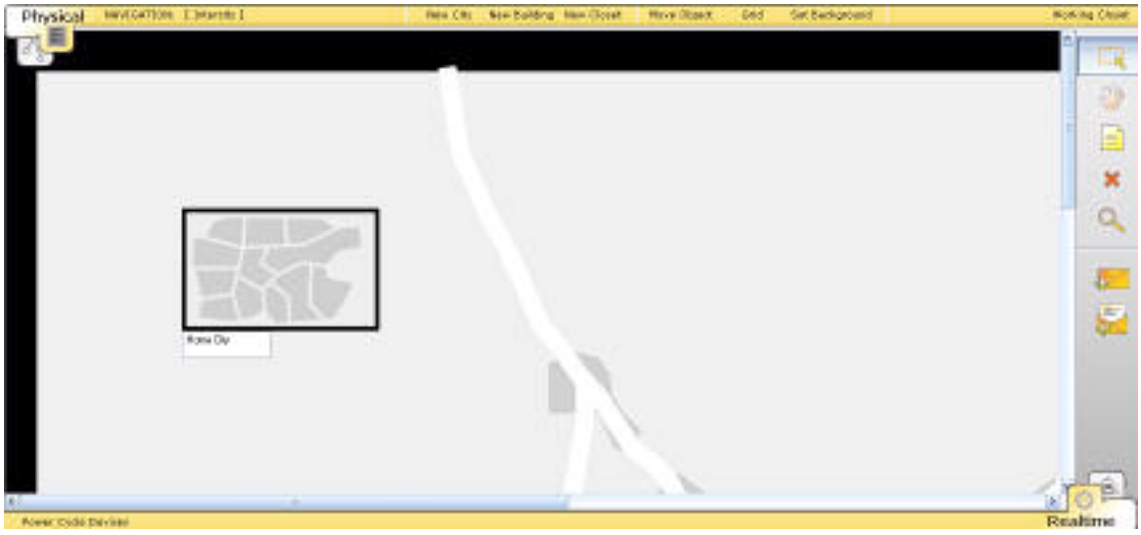


به این ترتیب مشاهده نمودید که یک بسته ICMP برای پینگ کردن PC1 از طریق PC2 ایجاد شد و عملیات با موفقیت به اتمام رسید. PDU ایجاد شده را حذف و مجدد به حالت Realtime بازگردید.

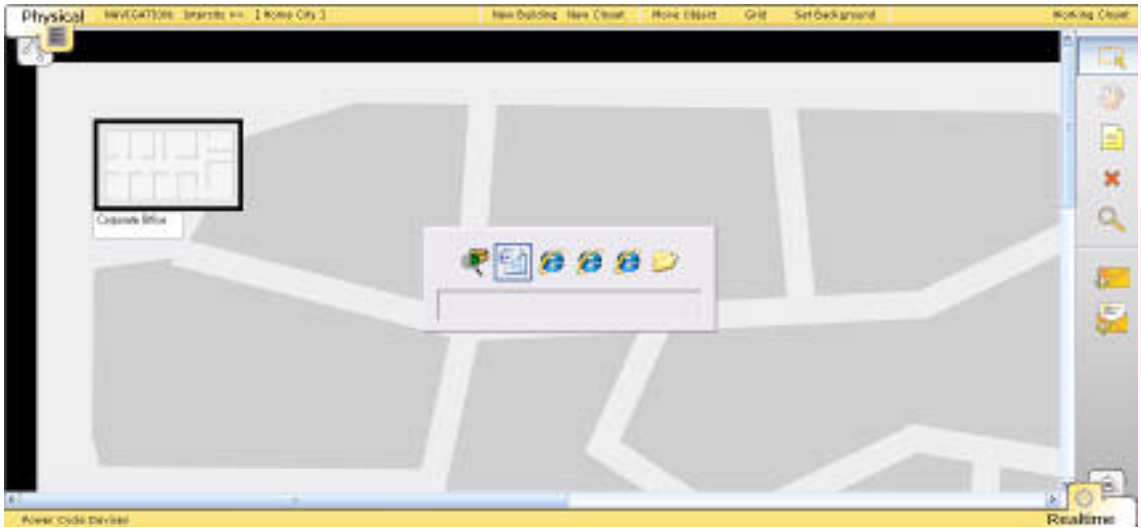


۴۱-۱۶- مثال عملی) قسمت دوم- توسعه توپولوژی شبکه

حال قصد داریم توپولوژی شبکه را از نظر فیزیکی بررسی کنیم. روی نمای Physical Workspace کلیک کنید.



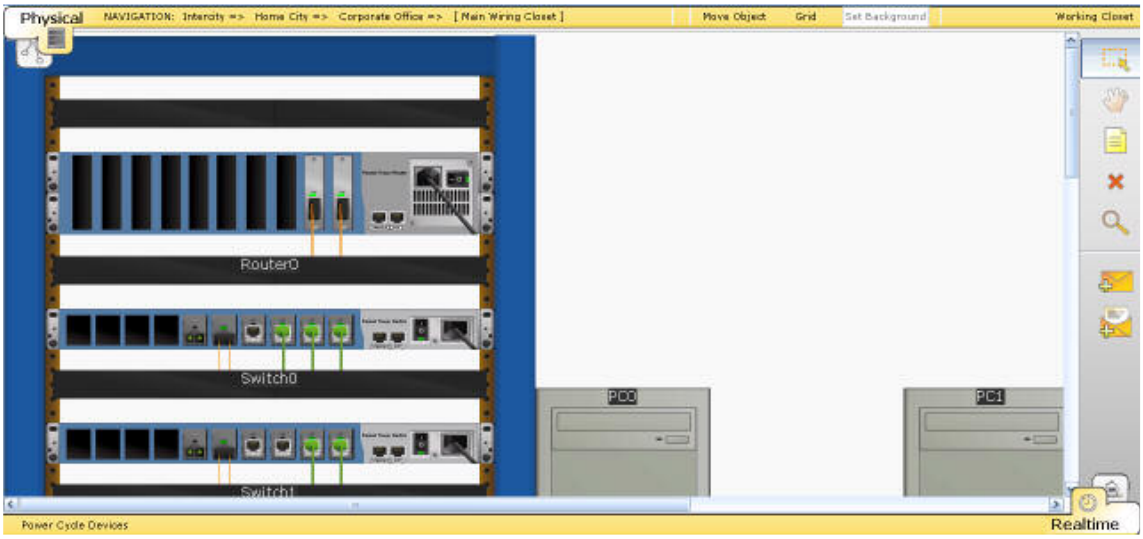
اکنون در ناحیه Intercity قرار دارید، روی Homecity کلیک کنید تا به داخل شهر بروید.



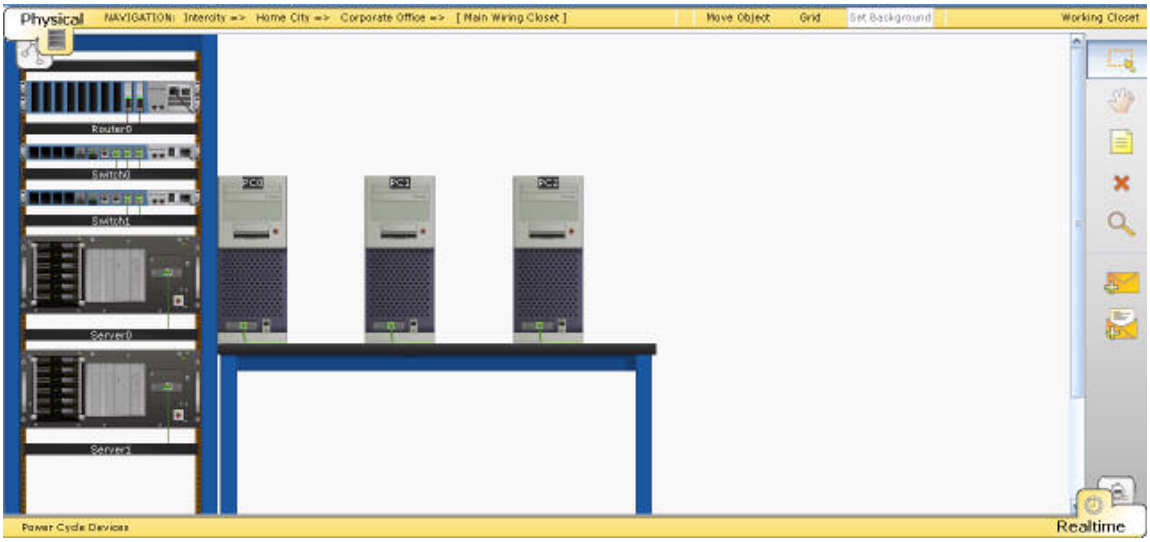
در Homecity ساختمان corporate Office قابل مشاهده است. بر روی آن کلیک کنید تا به داخل ساختمان قرار بگیرید.



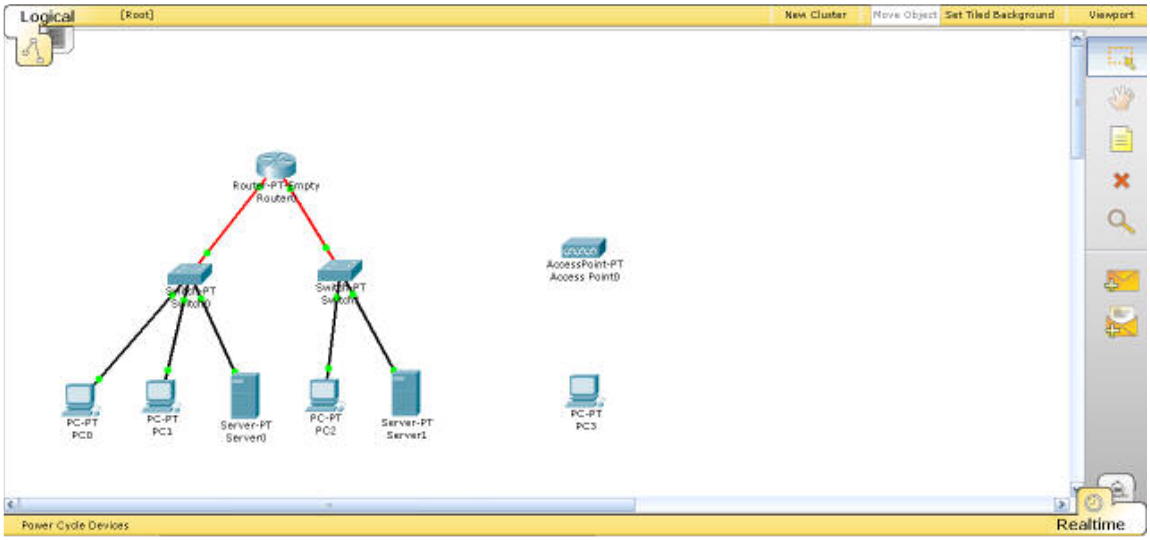
در حال حاضر در داخل ساختمان، اتاق Main Wiring Closet قابل مشاهده است که دستگاههای ما در داخل آن قرار دارد. برای مشاهده تجهیزات شبکه خود بر روی آن کلیک کنید.



برای این که تجهیزات را بهتر مشاهده کنید، با استفاده از ابزار بزرگ نمایی ، تصویر را کوچک کنید.



مشاهده می کنید که تجهیزات شبکه در داخل قفسه (rack) و دستگاه های رایانه روی میز قرار گرفته اند. حال قصد داریم یک ارتباط بی سیم برقرار کنیم. بدین منظور مجددا به نمای منطقی شبکه باز گردید. یک AccessPoint و یک رایانه جدید به شبکه اضافه نمایید.



برای ایجاد ارتباط بی سیم می بایست ماژول بیسیم را به رایانه خود اضافه کنید. بنابراین روی PC3 کلیک کنید تا پنجره تنظیمات آن باز شود. پس از خاموش کردن رایانه، ماژول فعلی آن را از قسمت پایین خارج ساخته و ماژول بی سیم را در جای آن قرار دهید. سپس مجددا رایانه را روشن کنید.



۱



۲

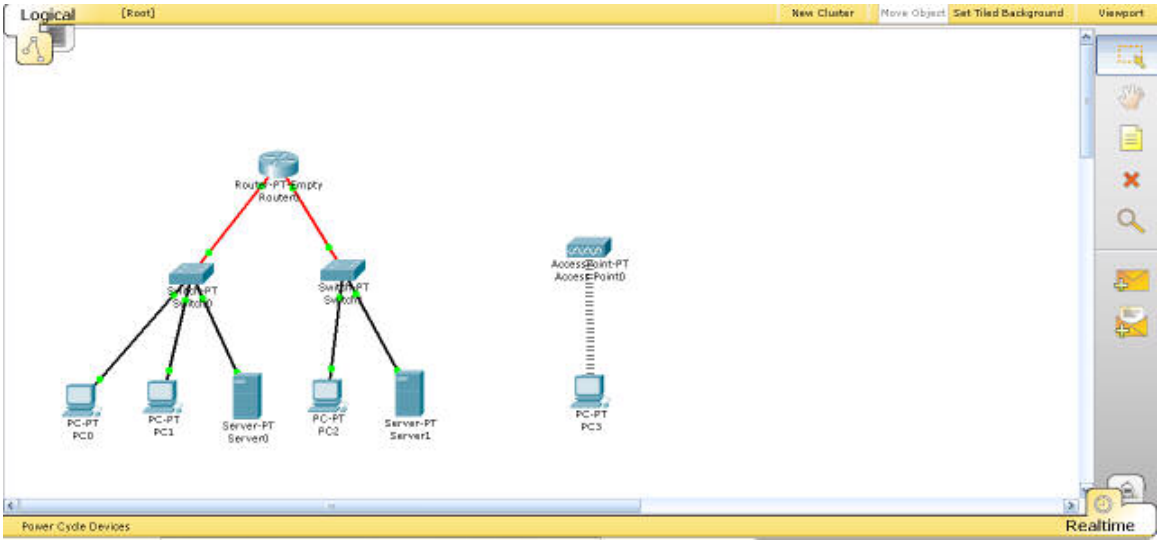


۳

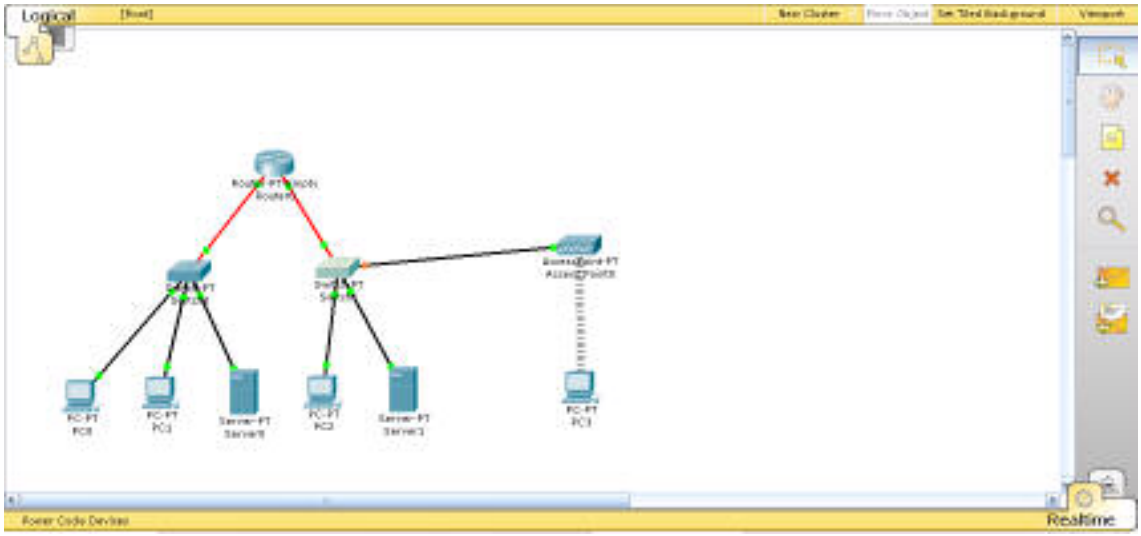


۴

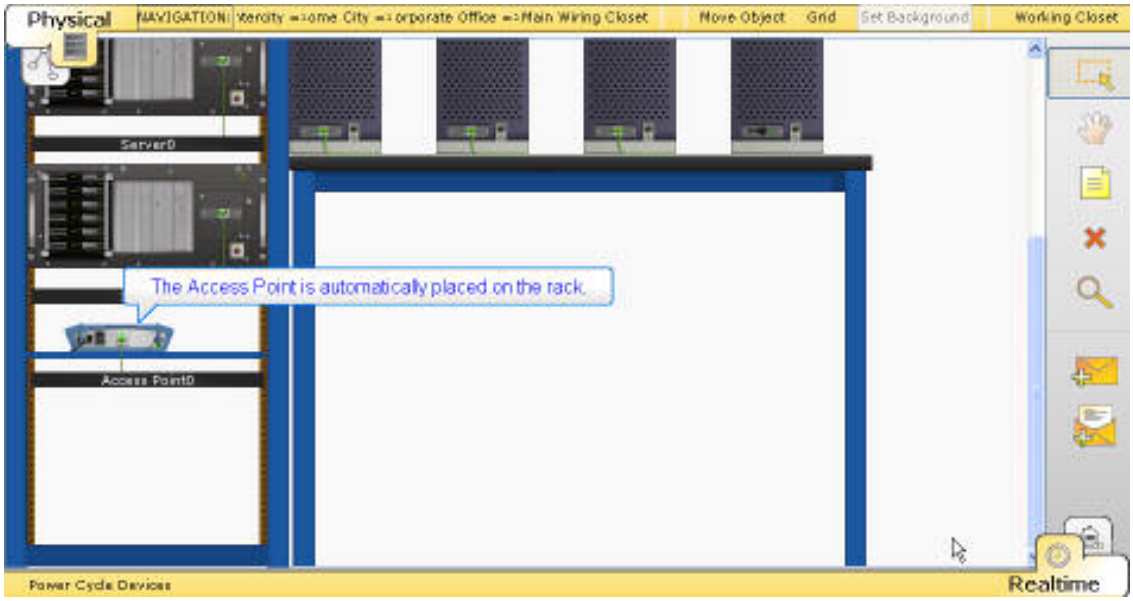
پس از بازگشت به صفحه اصلی مشاهده خواهید کرد که ارتباط بی سیم برقرار شده است.



برای اتصال این اجزای جدید به شبکه، با استفاده از کابل Copper Straight یک اتصال بین AccessPoint و سوئیچ مطابق شکل برقرار کنید.



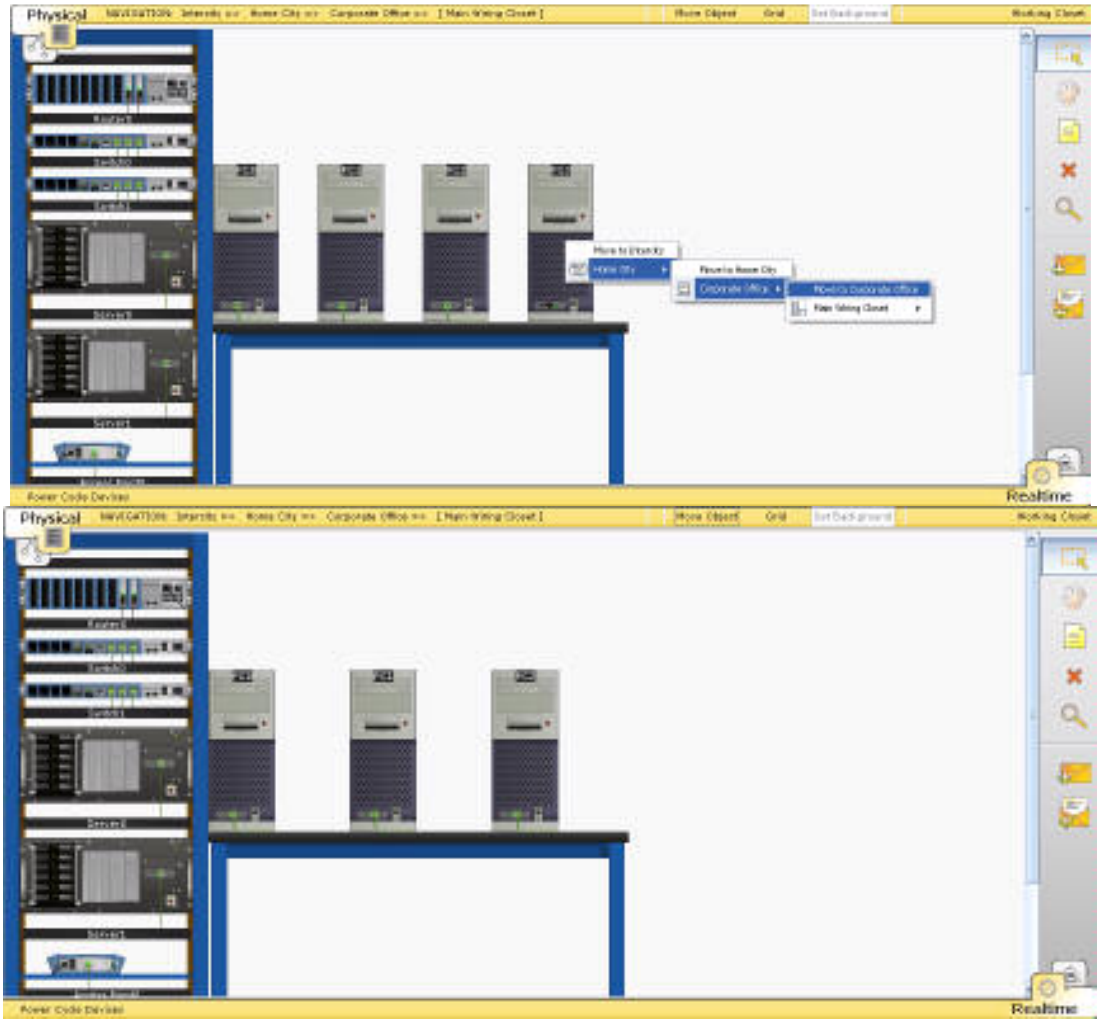
حال برای بررسی توپولوژی فیزیکی به نمای Physical بازگردید. مشاهده می کنید که Point Access به طور خودکار به قفسه افزوده شده است.



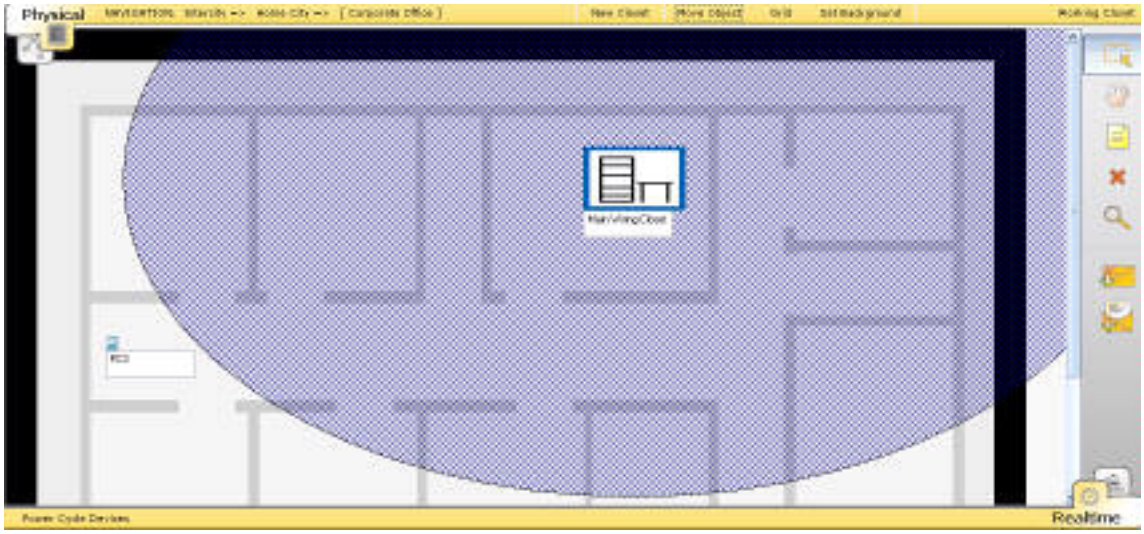
با کلیک برروی Corporate Office از قسمت نوار پیمایش، به فضای داخل ساختمان بروید. محدوده نمایش داده شده در محوطه ساختمان مربوط به Access Point و فضای تحت پوشش آن می باشد.



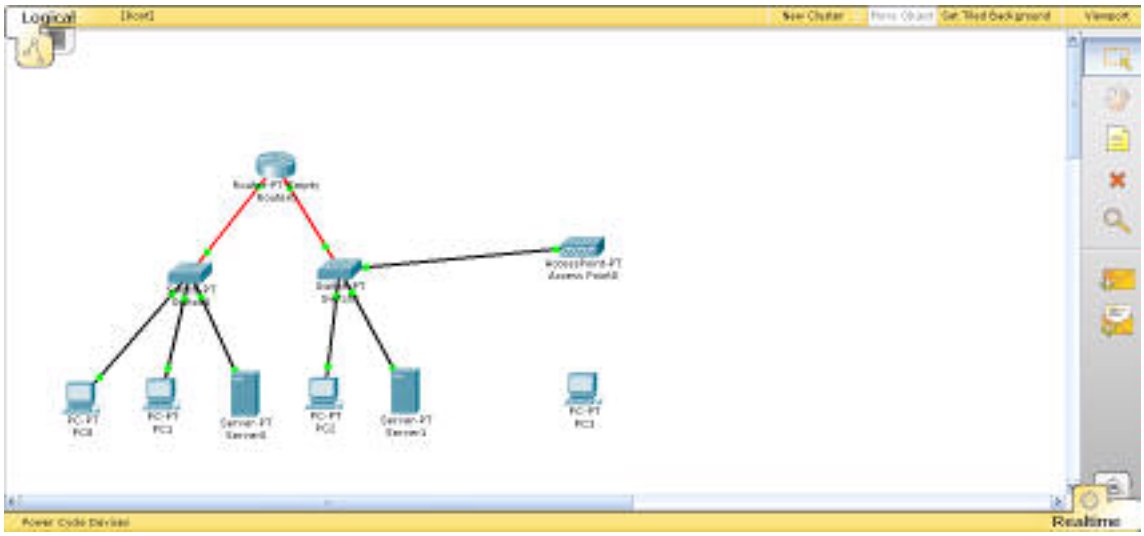
به داخل اتاق رفته و با استفاده از دکمه Move Object، رایانه PC3 را به داخل محوطه ساختمان منتقل کنید.



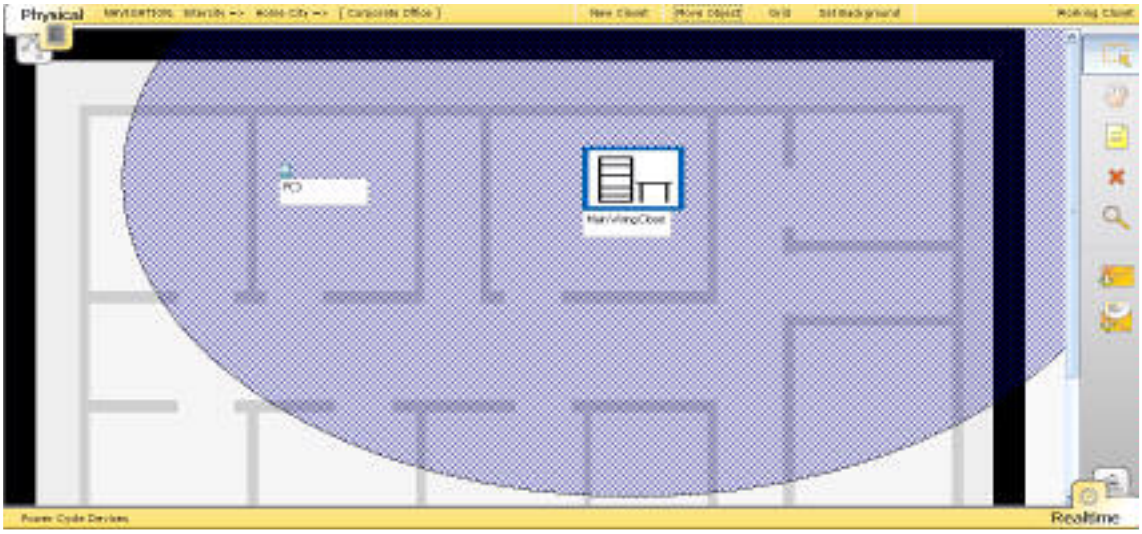
مجددا به محوطه ساختمان بروید و با جابجایی اتاق و PC3 آنها را به گونه ای قرار دهید که PC3 در محدوده خارج از پوشش AccessPoint قرار داده شود.

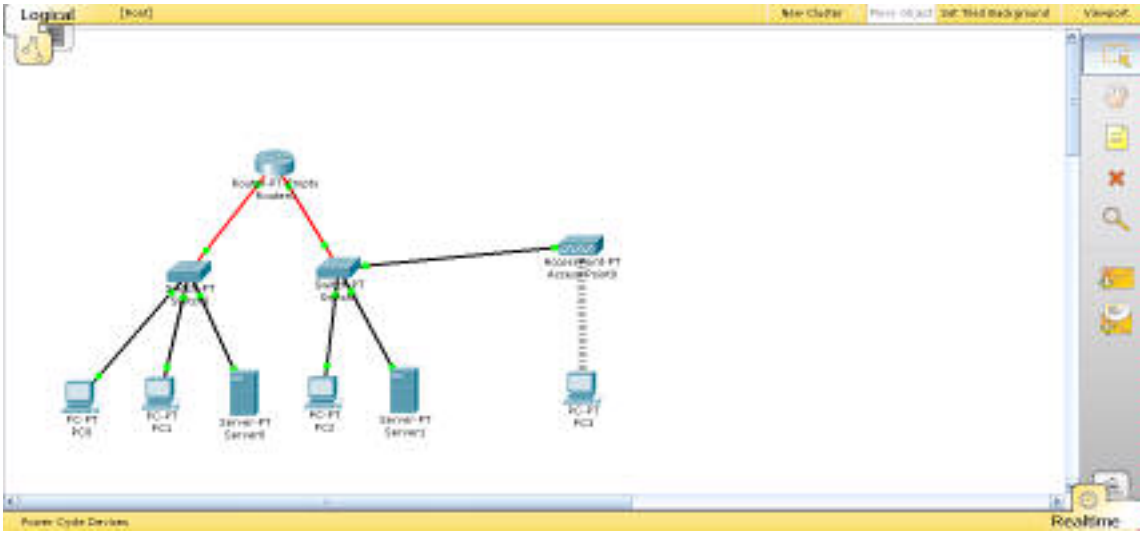


در این حالت اگر به فضای کار منطقی باز گردید مشاهده خواهید کرد که اتصال بین PC3 و AccessPoint قطع شده است.



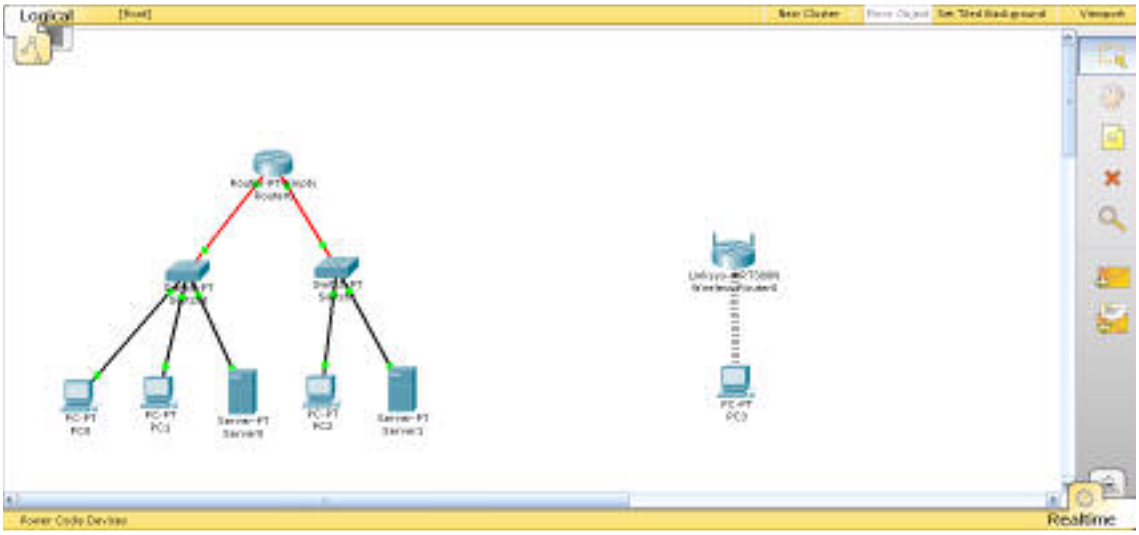
پس برای برقرار مجدد این اتصال می بایست در فضای فیزیکی ، رایانه را در محدوده تحت پوشش بیسیم قرار دهید.


Physical
Realtime

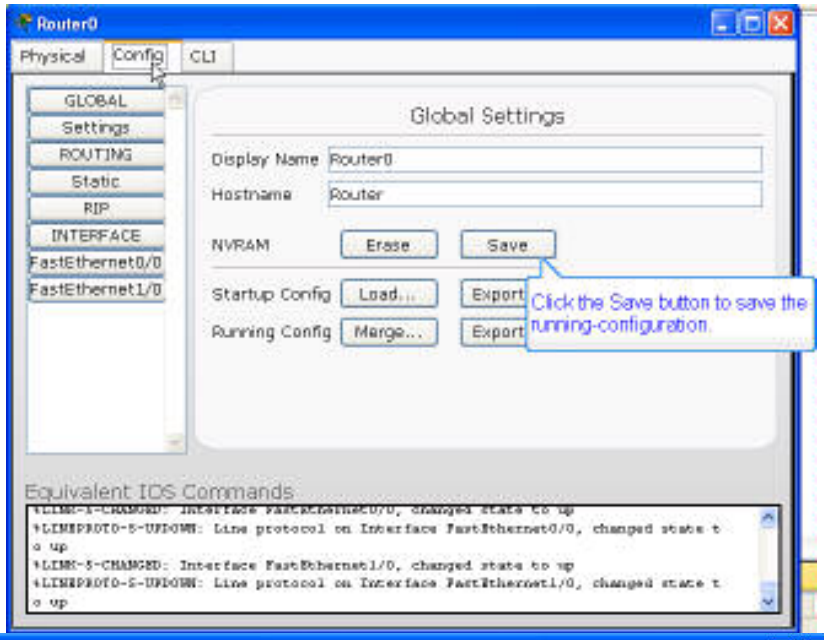

Logical
Realtime

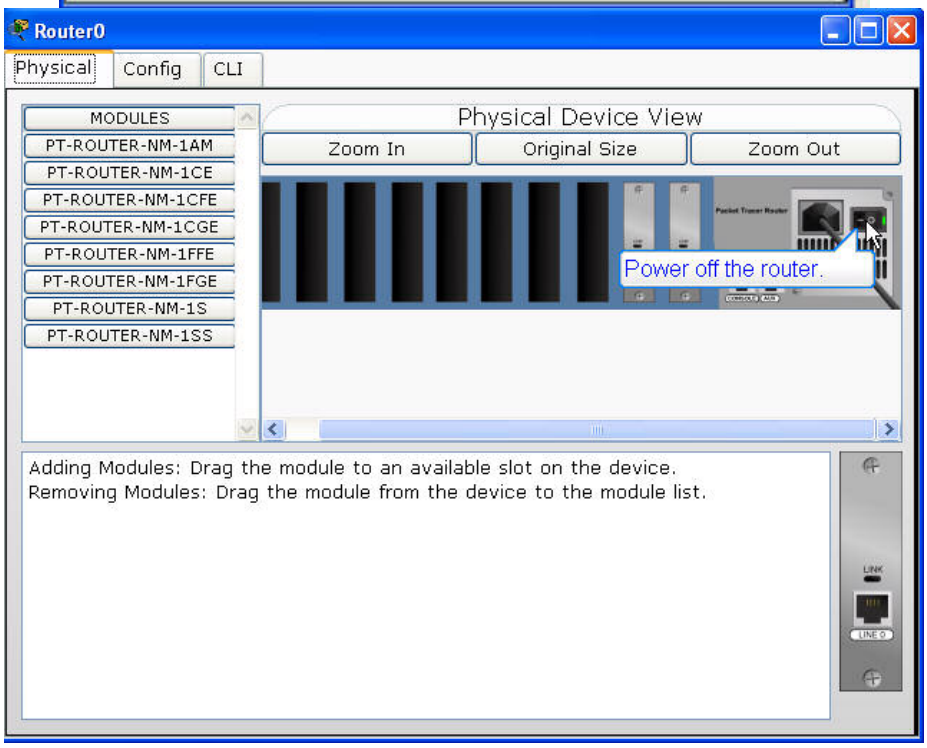
۴۱-۱۷- مثال عملی) قسمت سوم- شبیه سازی یک شبکه ISP و شبکه خانگی

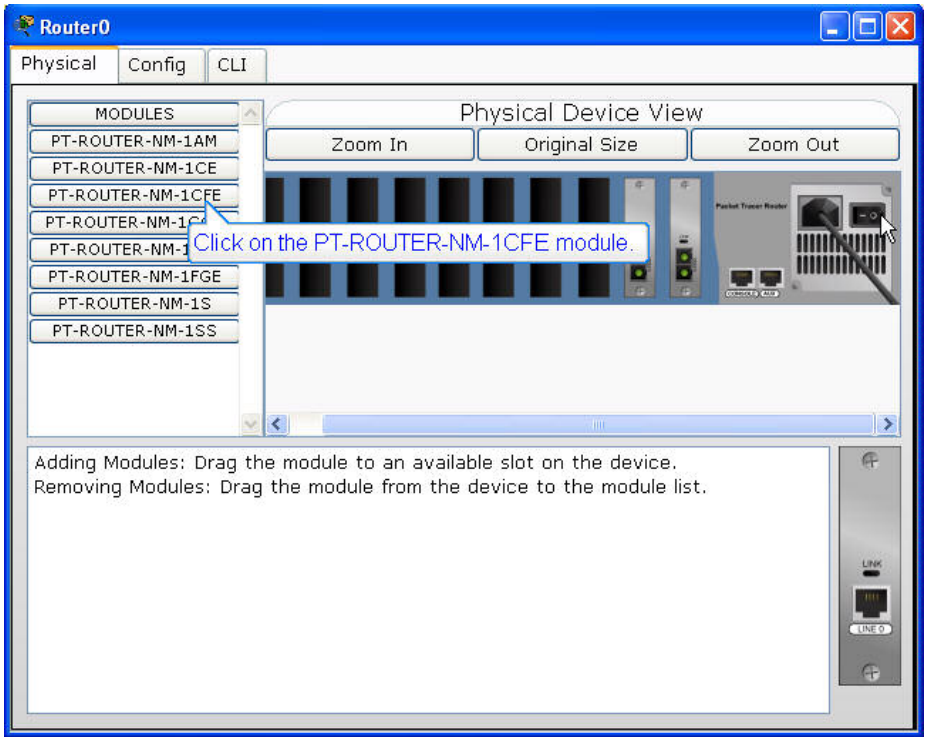
در ادامه این تمرین قصد راه اندازی یک شبکه خانگی بیسیم و اتصال آن به یک ISP با استفاده از ارتباط DSL را داریم. برای ادامه کار، AccessPoint موجود را شبکه فعلی را حذف نموده و یک AccessPoint از نوع Linksys-WRT300N بجای آن قرار دهید.



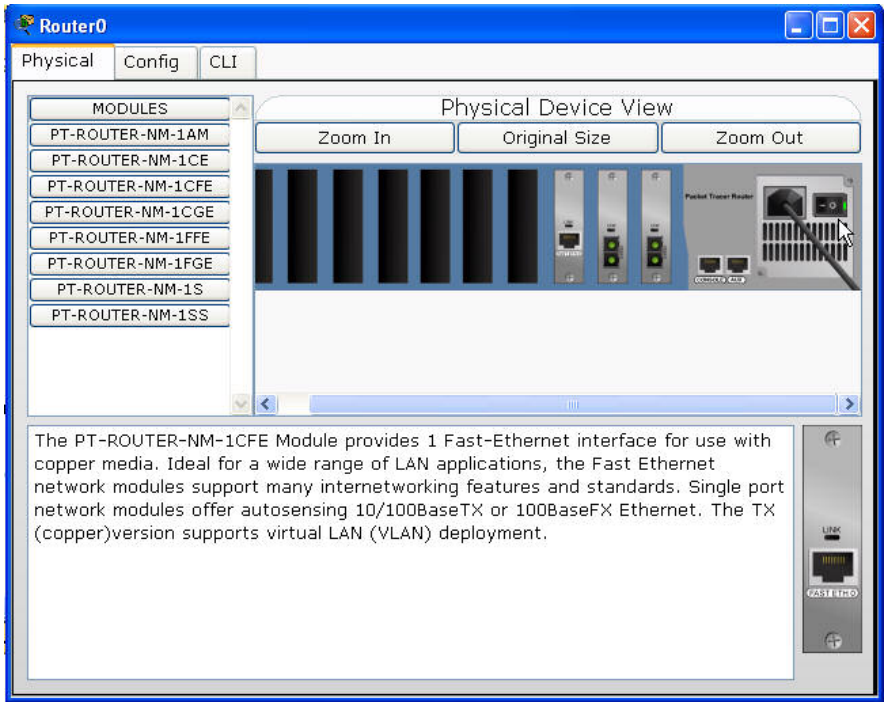
ابتدا باید برای افزودن قابلیت اتصال کاربران به ISP، به Router0 که متعلق به ISP است یک ماژول جدید اضافه کنیم. روی Router0 کلیک کنید. دقت کنید که برای اضافه نمودن ماژول جدید باید روتر خاموش شود، ولی با این کار کلیه تنظیمات آن از بین خواهد رفت. پس ابتدا تنظیمات را مطابق شکل ذخیره کنید. سپس ماژول جدید را اضافه کنید.

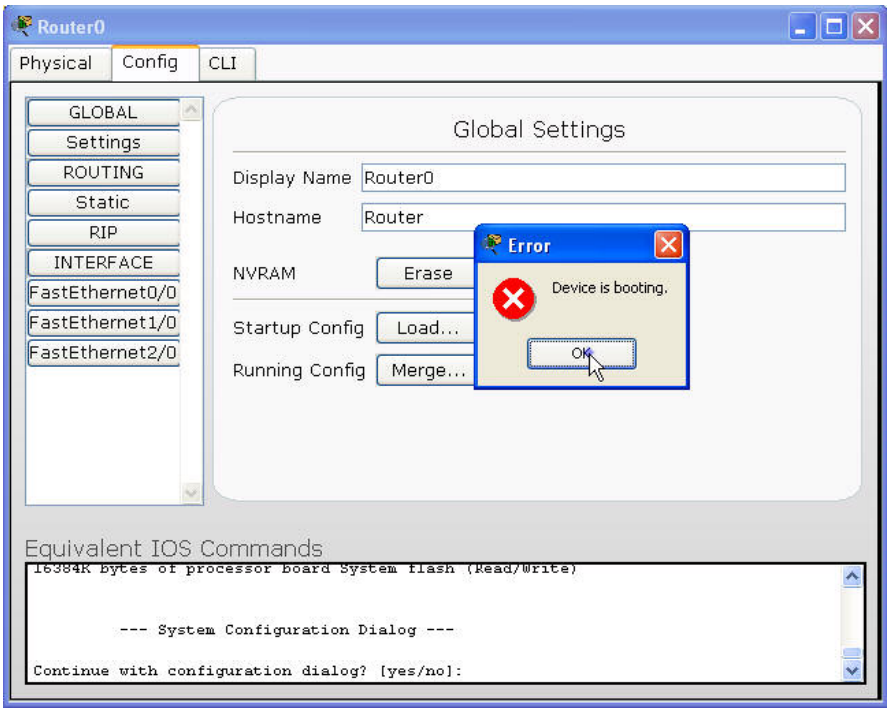

Router0
Physical
Config
CLI
GLOBAL
Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
Global Settings
Display Name
Router0
Hostname
Router
NVRAM
Erase
Save
Startup Config
Load...
Export
Running Config
Merge...
Export
Click the Save button to save the running-configuration.
Equivalent IOS Commands

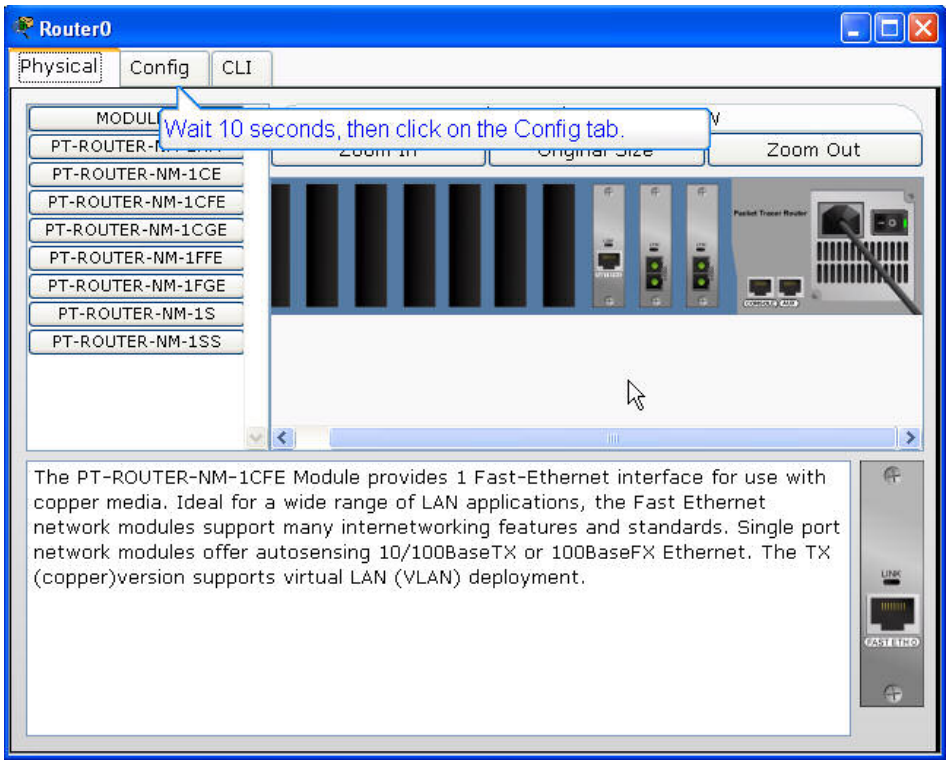

Router0
Physical
Config
CLI
MODULES
PT-ROUTER-NM-1AM
PT-ROUTER-NM-1CE
PT-ROUTER-NM-1CFE
PT-ROUTER-NM-1CGE
PT-ROUTER-NM-1FFE
PT-ROUTER-NM-1FGE
PT-ROUTER-NM-1S
PT-ROUTER-NM-1SS
Physical Device View
Zoom In
Original Size
Zoom Out
Power off the router.
Adding Modules: Drag the module to an available slot on the device.
Removing Modules: Drag the module from the device to the module list.



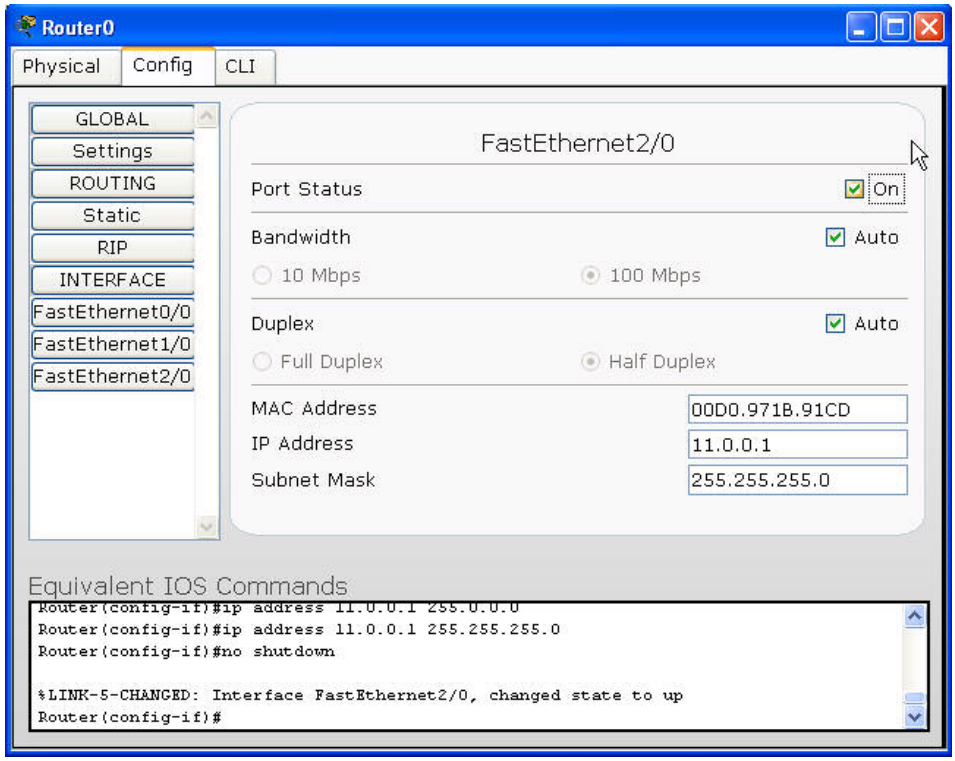
پس از روشن کردن مسیریاب، برای پیکربندی واسط جدید، بر روی برگه config کلیک کنید. یک پیغام خطا ظاهر می شود و اطلاع می دهد که مسیریاب در حال راه اندازی است (راه اندازی مسیریاب حدود ۱۰ ثانیه طول می کشد). بنابراین پس از ۱۰ ثانیه مجددا بر روی این برگه کلیک کنید.



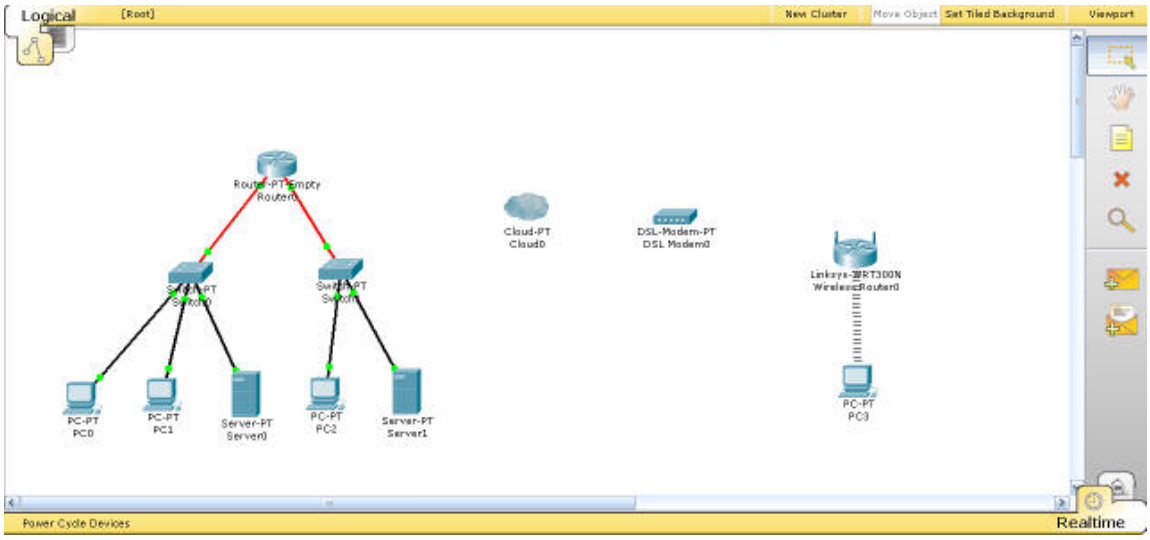

Router0
Physical
Config
CLI
GLOBAL
Settings
ROUTING
Static
RIP
INTERFACE
FastEthernet0/0
FastEthernet1/0
FastEthernet2/0
Global Settings
Display Name
Router0
Hostname
Router
NVRAM
Erase
Startup Config
Load...
Running Config
Merge...
Error
Device is booting.
OK
Equivalent IOS Commands
16384K bytes of processor board System flash (Read/Write)
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]:


Router0
Physical
Config
CLI
Wait 10 seconds, then click on the Config tab.
PT-ROUTER-NM-1CE
PT-ROUTER-NM-1CFE
PT-ROUTER-NM-1CGE
PT-ROUTER-NM-1FFE
PT-ROUTER-NM-1FGE
PT-ROUTER-NM-1S
PT-ROUTER-NM-1SS
Zoom Out
The PT-ROUTER-NM-1CFE Module provides 1 Fast-Ethernet interface for use with copper media. Ideal for a wide range of LAN applications, the Fast Ethernet network modules support many internetworking features and standards. Single port network modules offer autosensing 10/100BaseTX or 100BaseFX Ethernet. The TX (copper)version supports virtual LAN (VLAN) deployment.

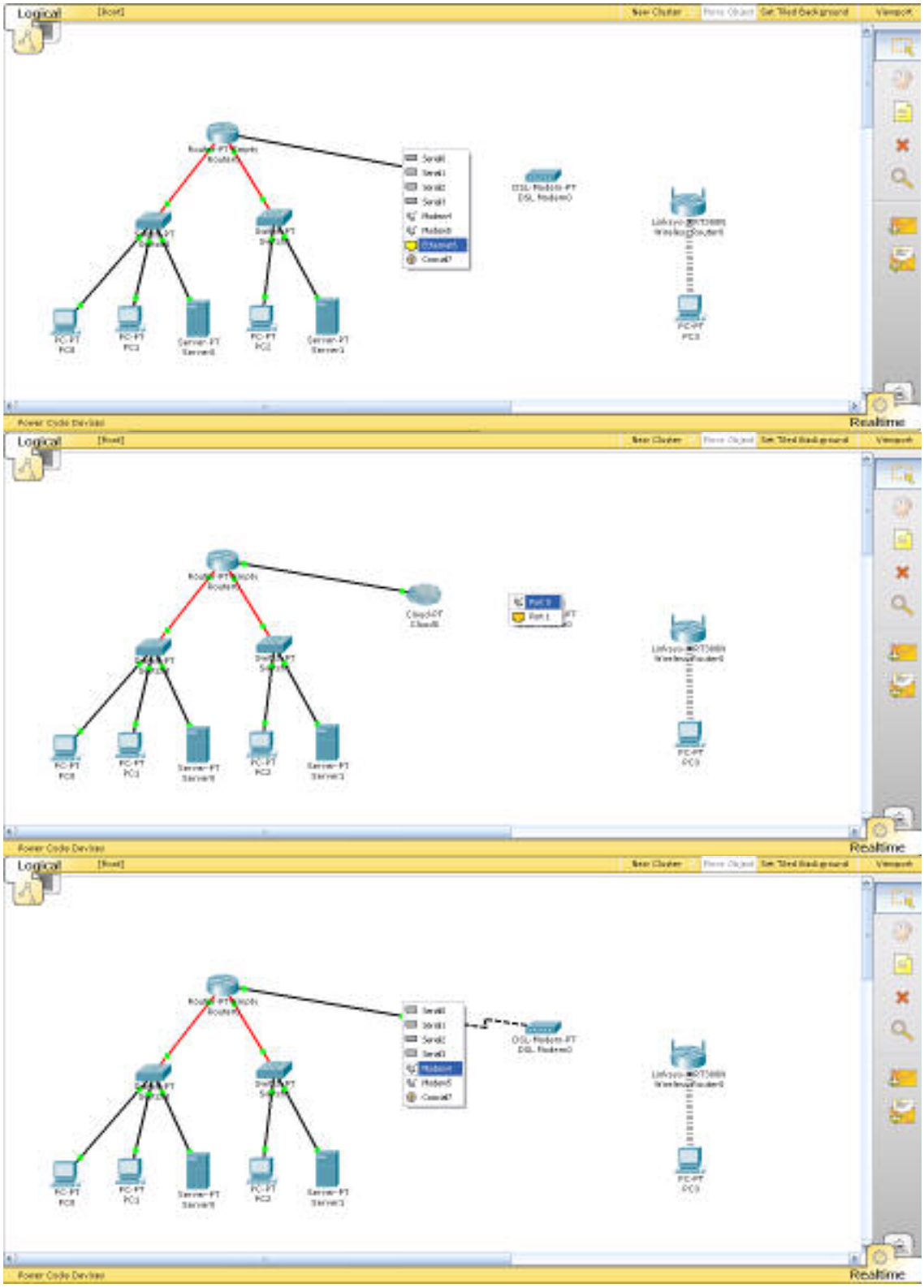
واسط جدیدی که اضافه شده است FastEthernet2-0 است. تنظیمات آن را مطابق شکل انجام دهید.



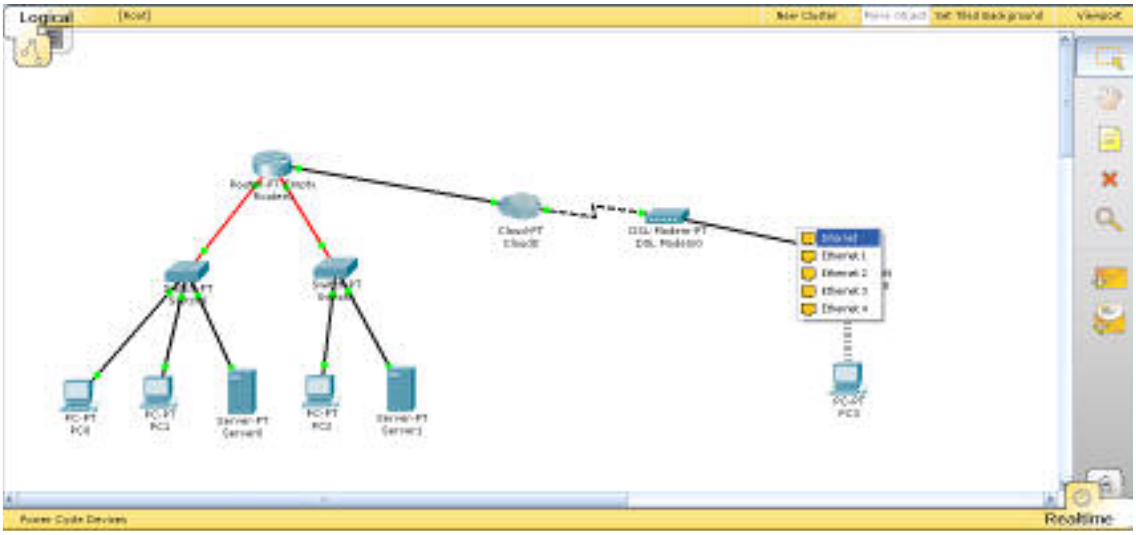
برای ایجاد ارتباط بین شبکه خانگی و ISP یک مودم DSL به محیط کار اضافه کنید. همچنین باید یک ابر (cloud) که نشانگر شبکه مخابراتی است نیز به فضای کار اضافه نمایید.



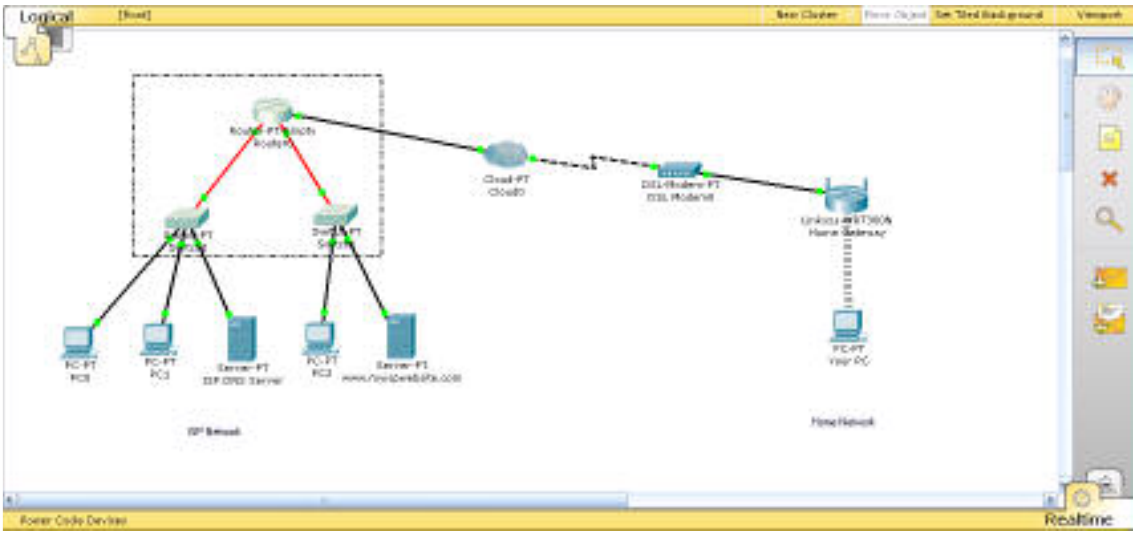
مطابق شکل، مسیریاب را به پورت Ethernet ابر متصل کنید و Port0 مودم را به پورت مودم ابر متصل کنید.

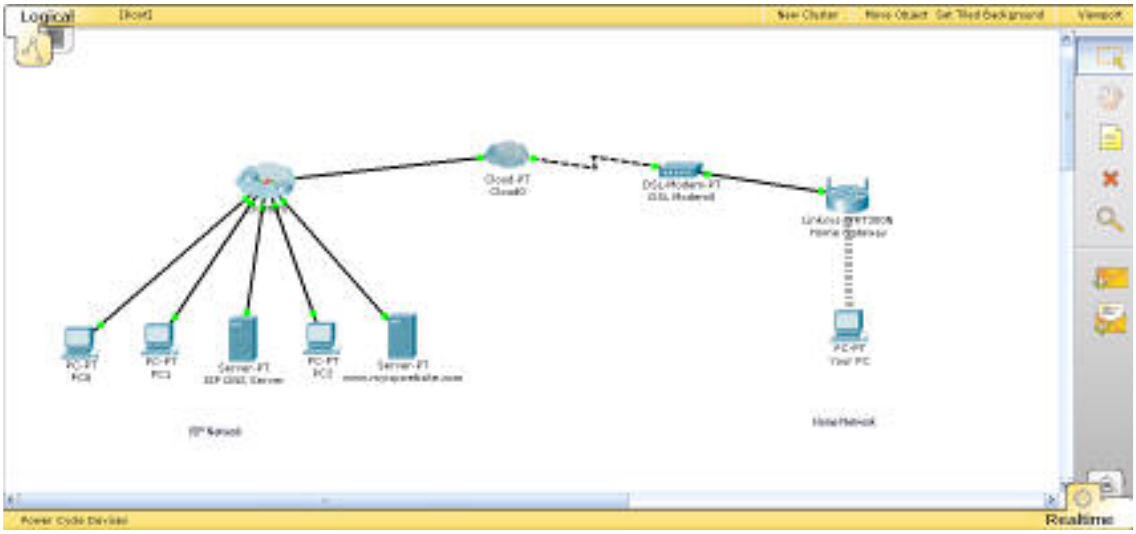


در ادامه می بایست مودم را به پورت اینترنت مسیریاب Linksys متصل کنید.

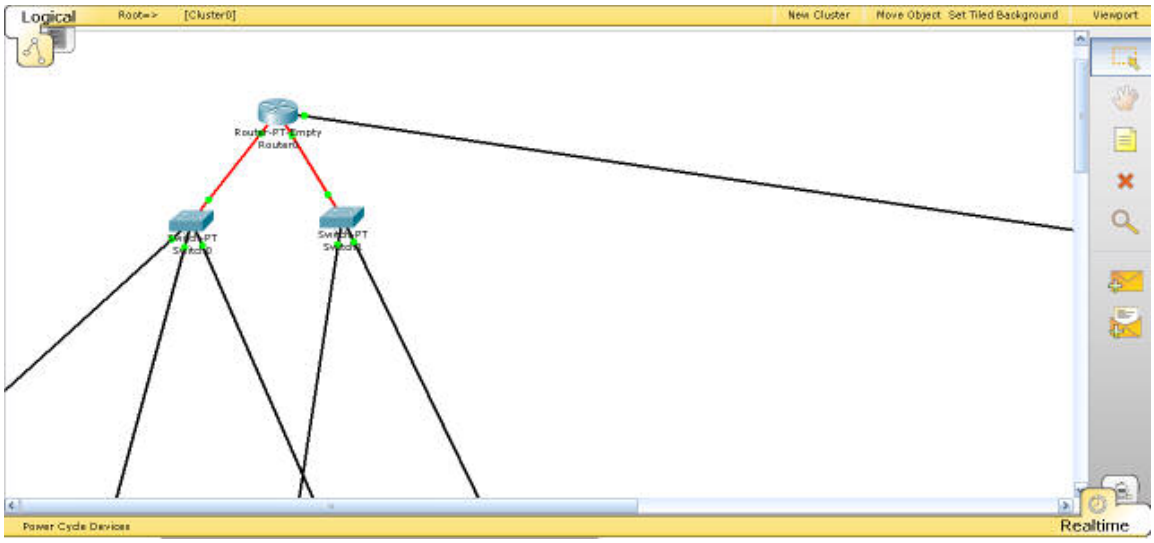


برای این که اجزای داخلی ISP پنهان شود و توپولوژی شبکه منظم تر گردد، مسیریاب و سوئیچ های شبکه را انتخاب نموده و بر روی دکمه New Cluster کلیک کنید.

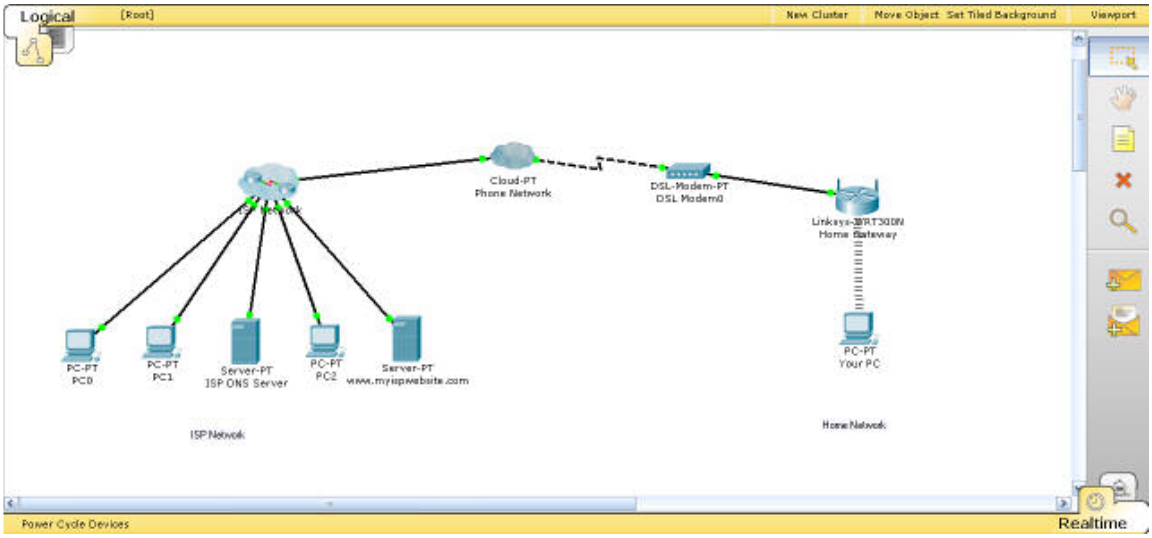




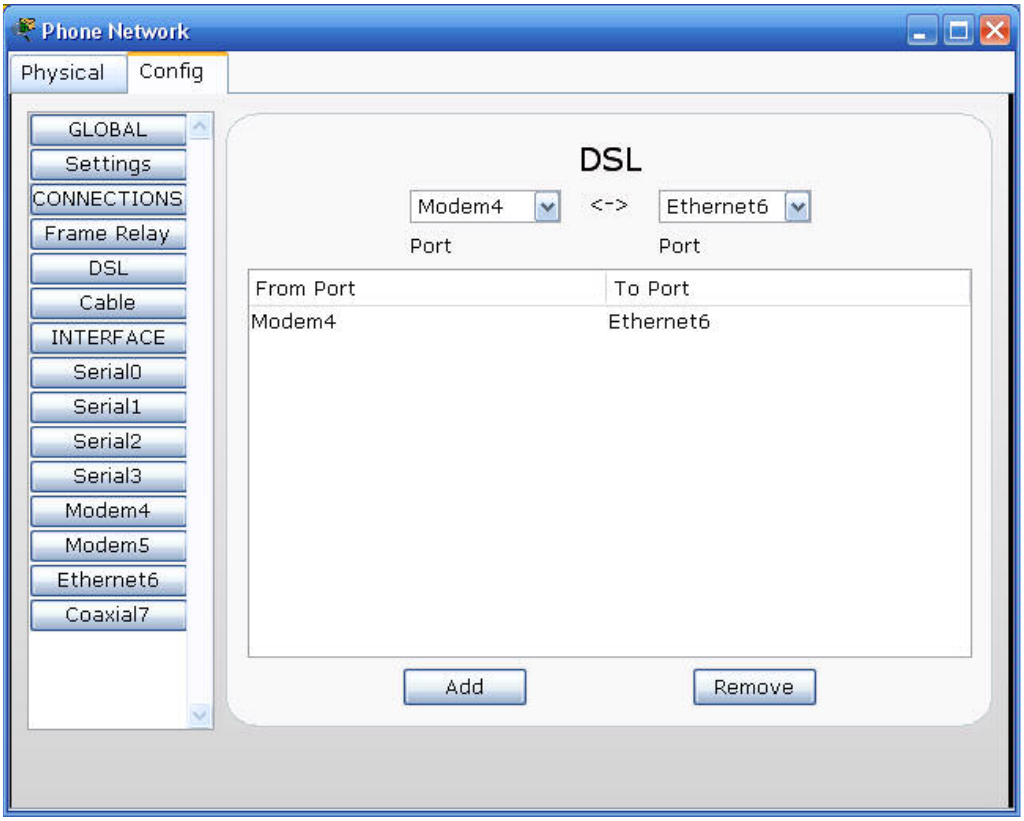
مشاهده می کنید که این اجزا در داخل یک گروه قرار می گیرند. در هر لحظه می توانید با یک کلیک وارد ISP شده و اجزای داخل آن را ویرایش کنید. برای خروج از ISP نیز می توان بر روی دکمه Root در قسمت نوار پیمایش کلیک نمود.



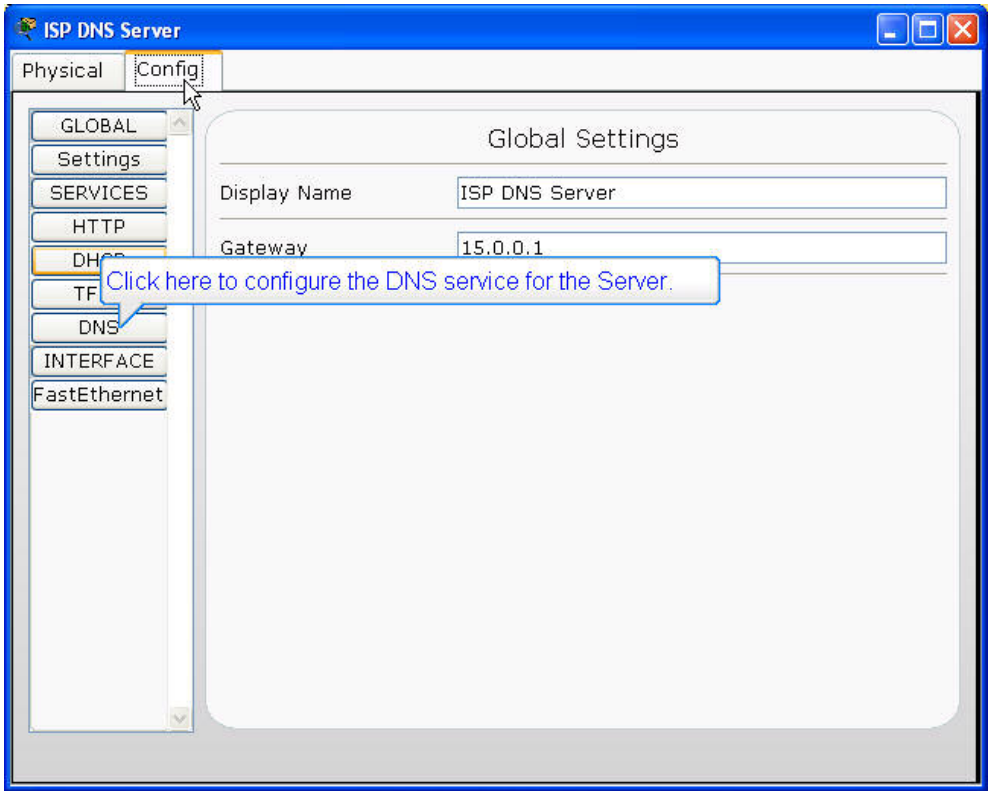
حال برای نظم بهتر شبکه، باید اجزای مختلف شبکه از جمله سرور وب، DNS سرور، نام رایانه شبکه خانگی و ابرهای شبکه مخابراتی و ISP را نام گذاری نمود.

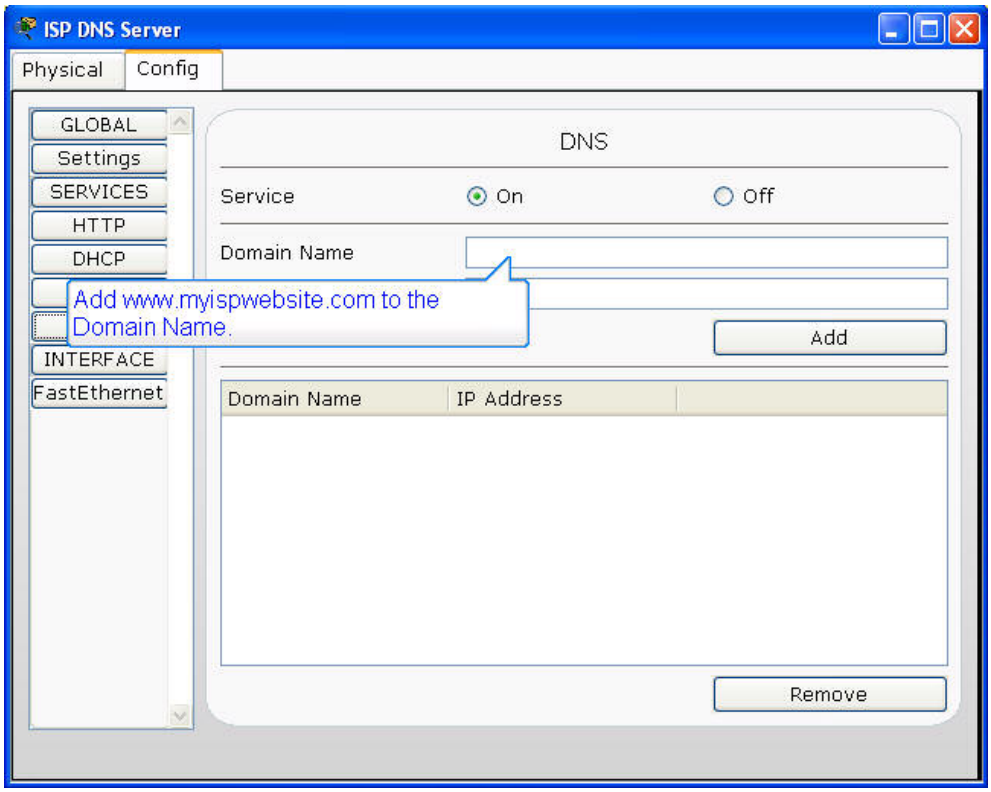


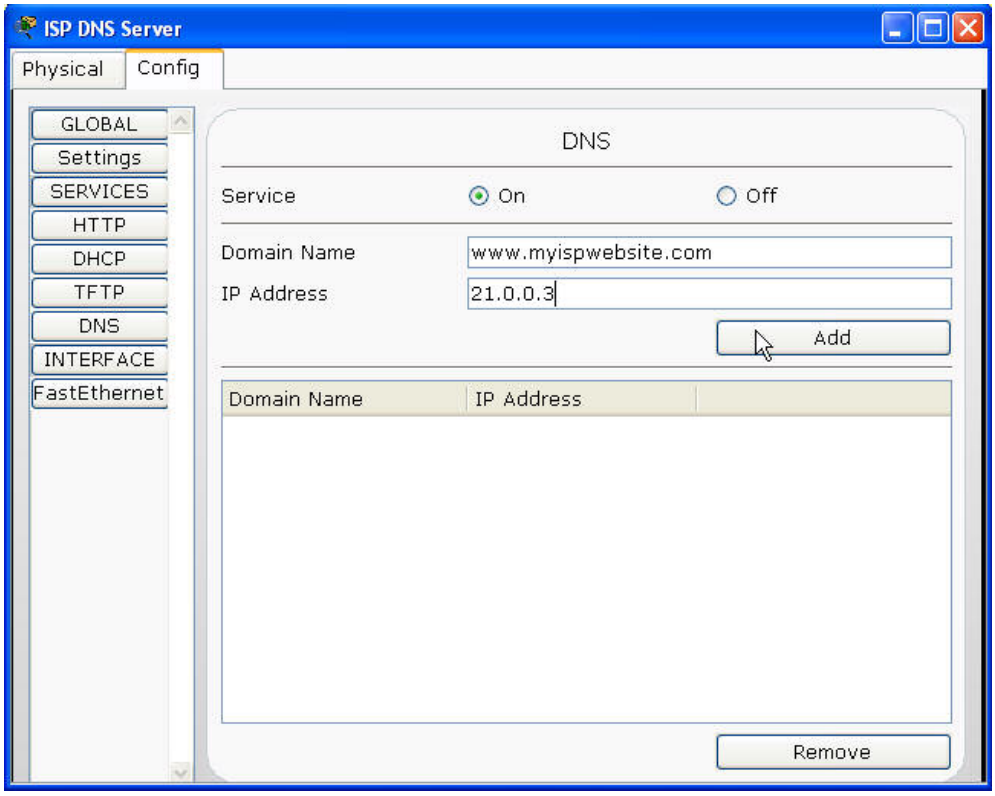
برای تنظیم ارتباط DSL وارد ابر شبکه مخابرات شده و در قسمت DSL پس از مشخص کردن ارتباط صحیح بر روی دکمه Add کلیک، تا ارتباط بین ISP و مودم DSL برقرار شود.

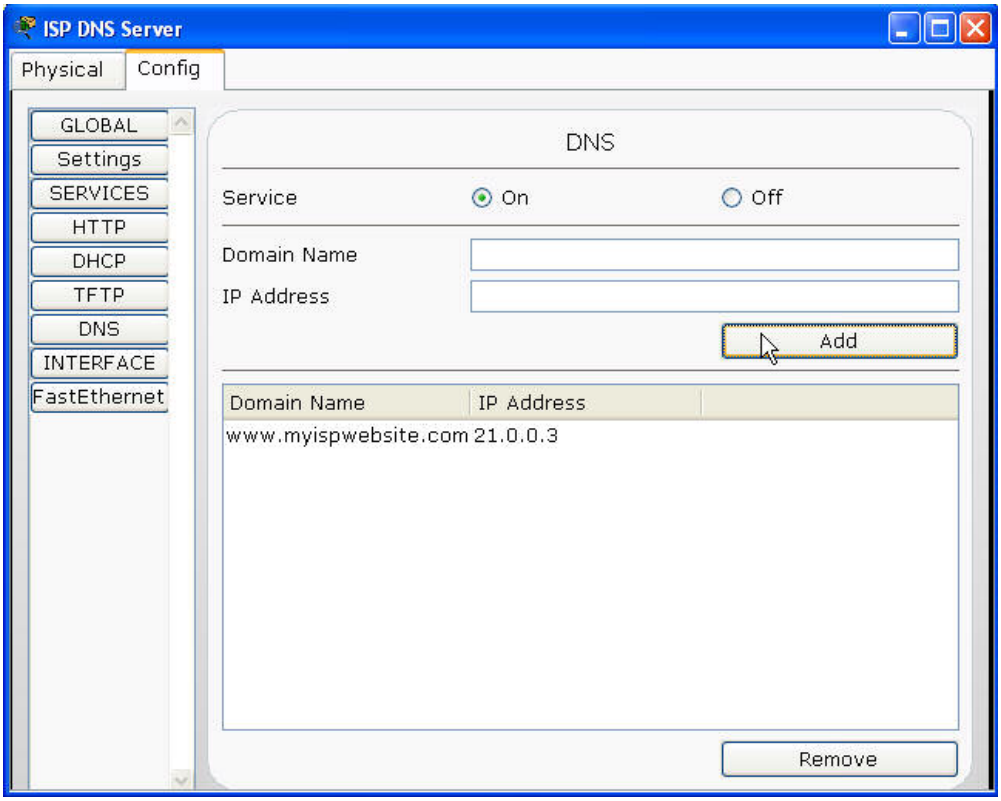


برای تنظیم DNS سرور، بر روی ISP DNS Server کلیک و تنظیمات DNS آن را مطابق شکل انجام دهید.


ISP DNS Server
Physical
Config
GLOBAL
Settings
SERVICES
HTTP
DHCP
TF
DNS
INTERFACE
FastEthernet
Global Settings
Display Name
ISP DNS Server
Gateway
15.0.0.1
Click here to configure the DNS service for the Server.

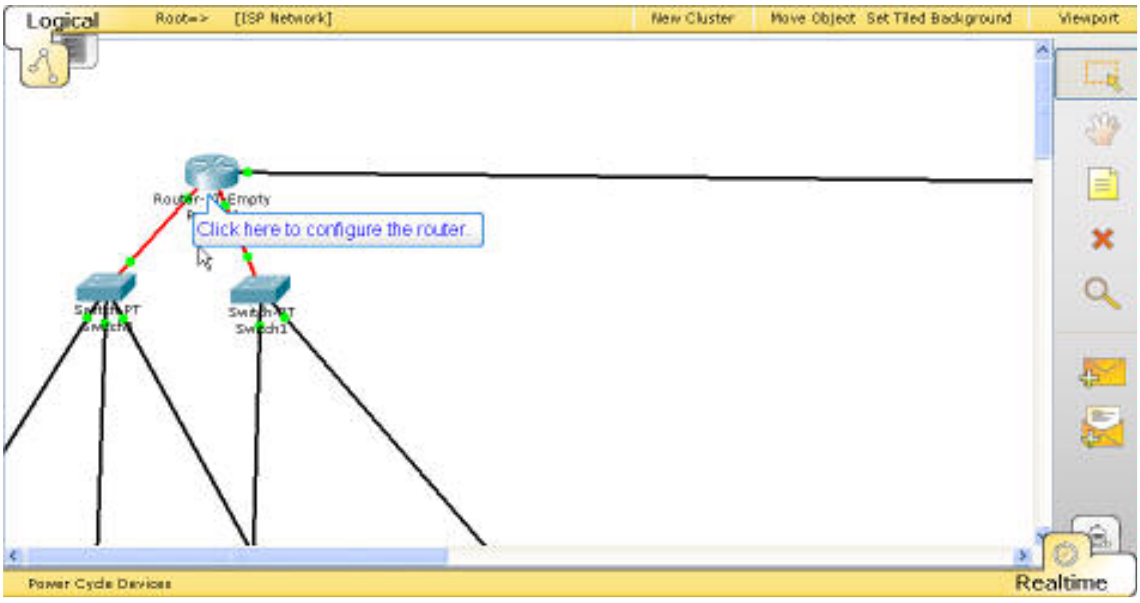

ISP DNS Server
Physical
Config
GLOBAL
Settings
SERVICES
HTTP
DHCP
INTERFACE
FastEthernet
DNS
Service
On
Off
Domain Name
Add www.myispwebsite.com to the Domain Name.
Add
Domain Name
IP Address
Remove

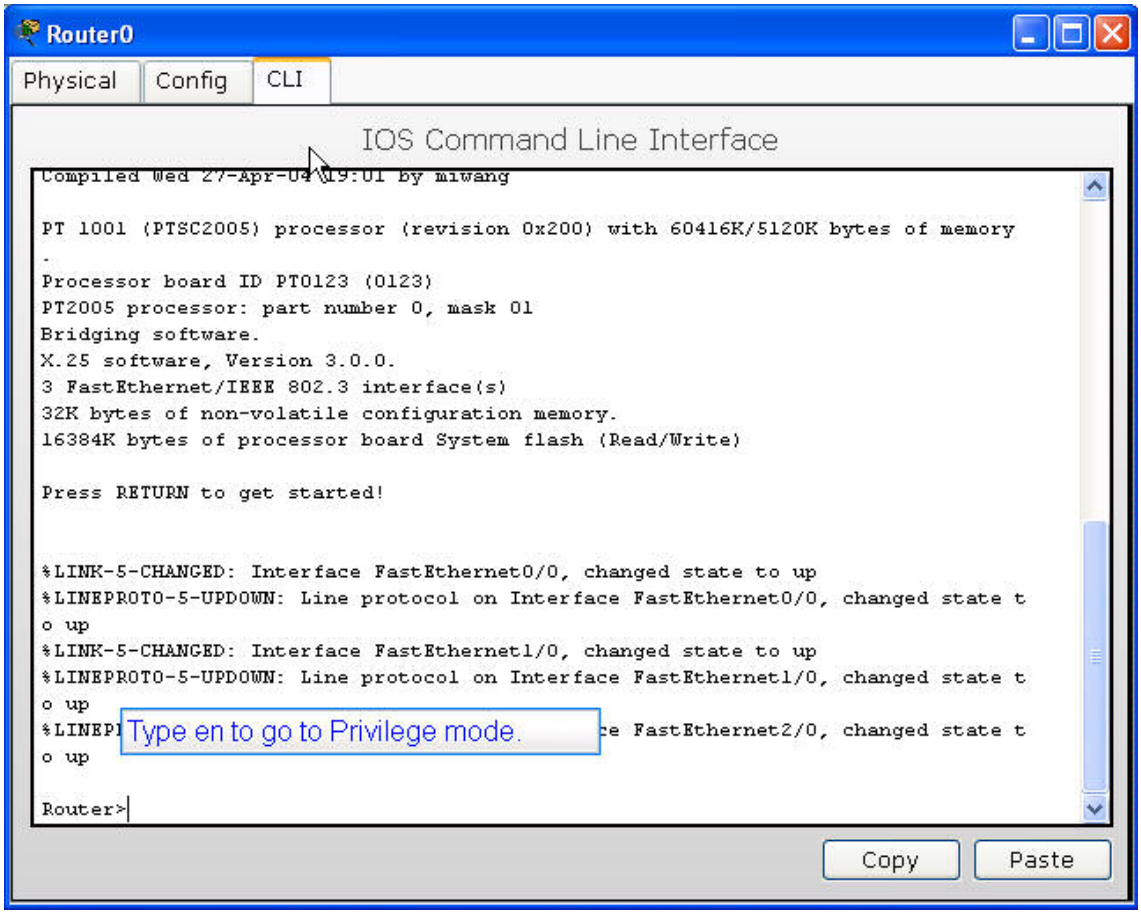

ISP DNS Server
Physical
Config
GLOBAL
Settings
SERVICES
HTTP
DHCP
TFTP
DNS
INTERFACE
FastEthernet
DNS
Service
On
Off
Domain Name
www.myispwebsite.com
IP Address
21.0.0.3
Add
Domain Name
IP Address
Remove

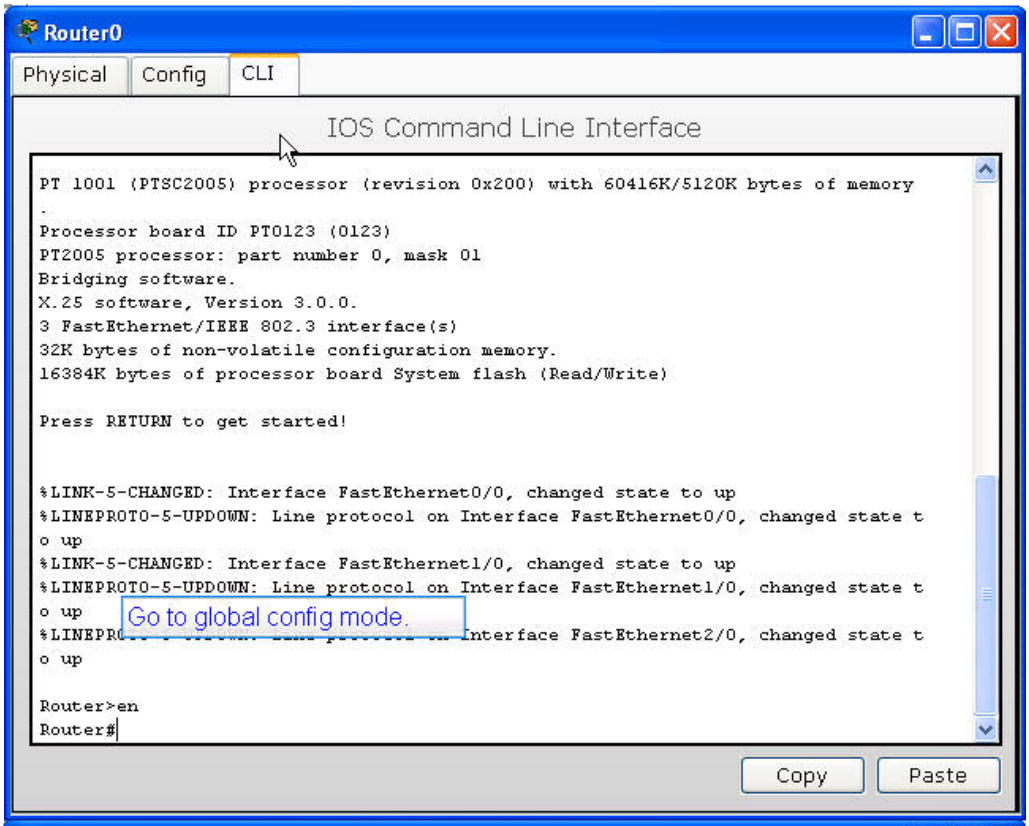

ISP DNS Server
Physical
Config
GLOBAL
Settings
SERVICES
HTTP
DHCP
TFTP
DNS
INTERFACE
FastEthernet
DNS
Service
On
Off
Domain Name
IP Address
Add
Domain Name
IP Address
www.myispwebsite.com 21.0.0.3
Remove

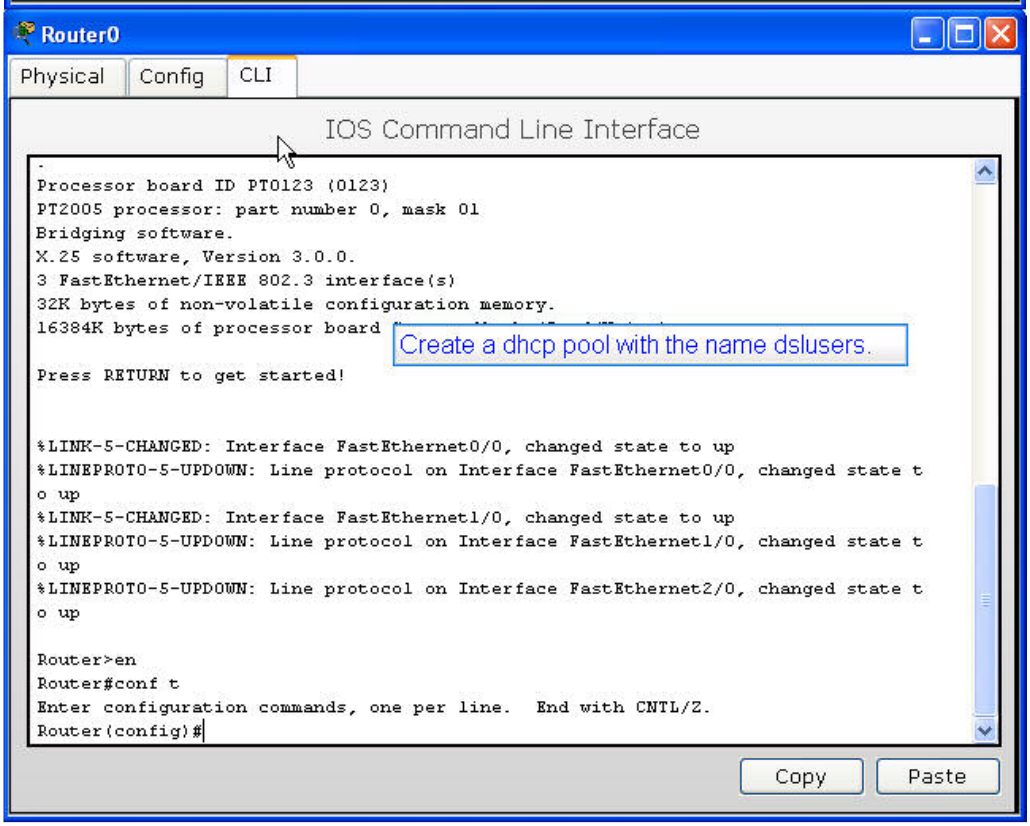
برای تنظیم مسیریاب، وارد ISP شده و بر روی مسیریاب کلیک کنید. تنظیمات را مطابق شکل در برگه CLI انجام دهید:

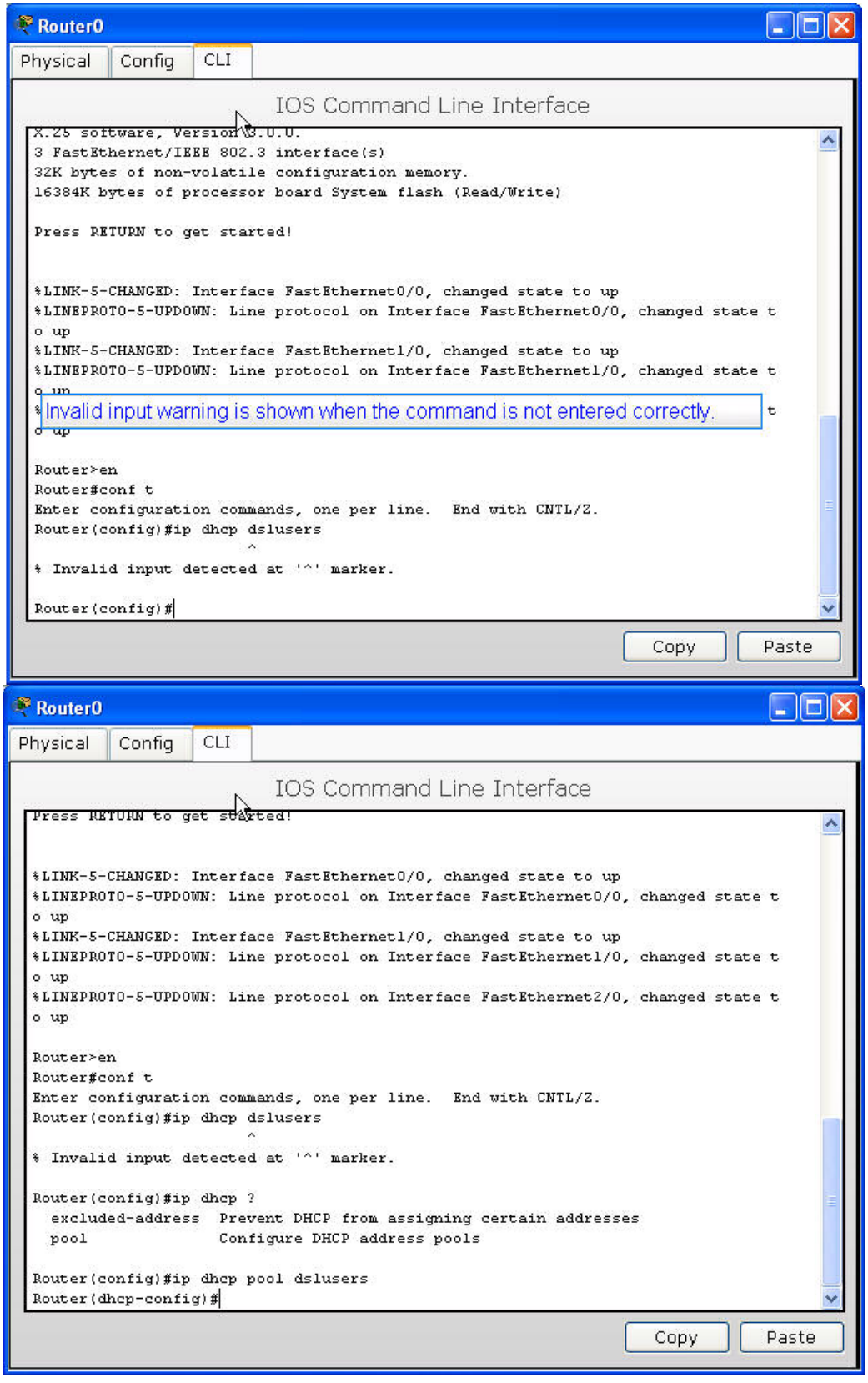
- ورودی به حالت Enable
- ورود به حالت Config
- ایجاد DHCP برای کاربران DSL
- تعیین سرور DNS برای کاربران DSL
- تعیین محدوده آدرس های DHCP
- تعیین gateway برای DHCP

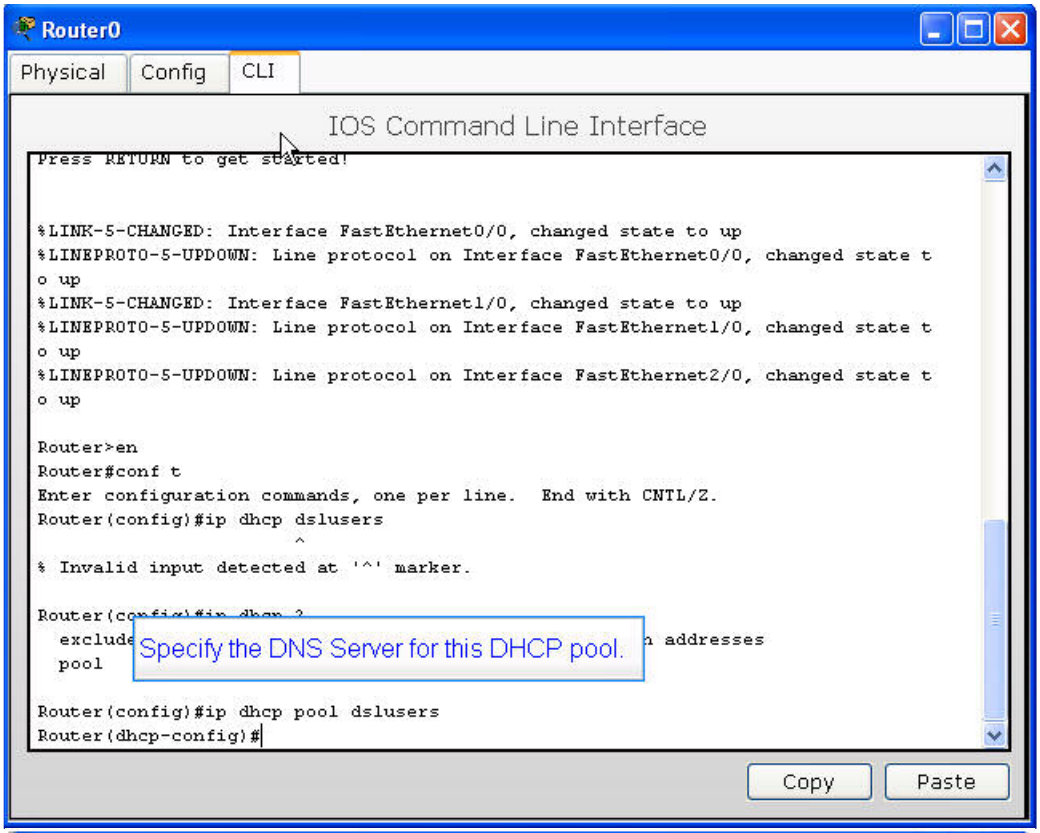


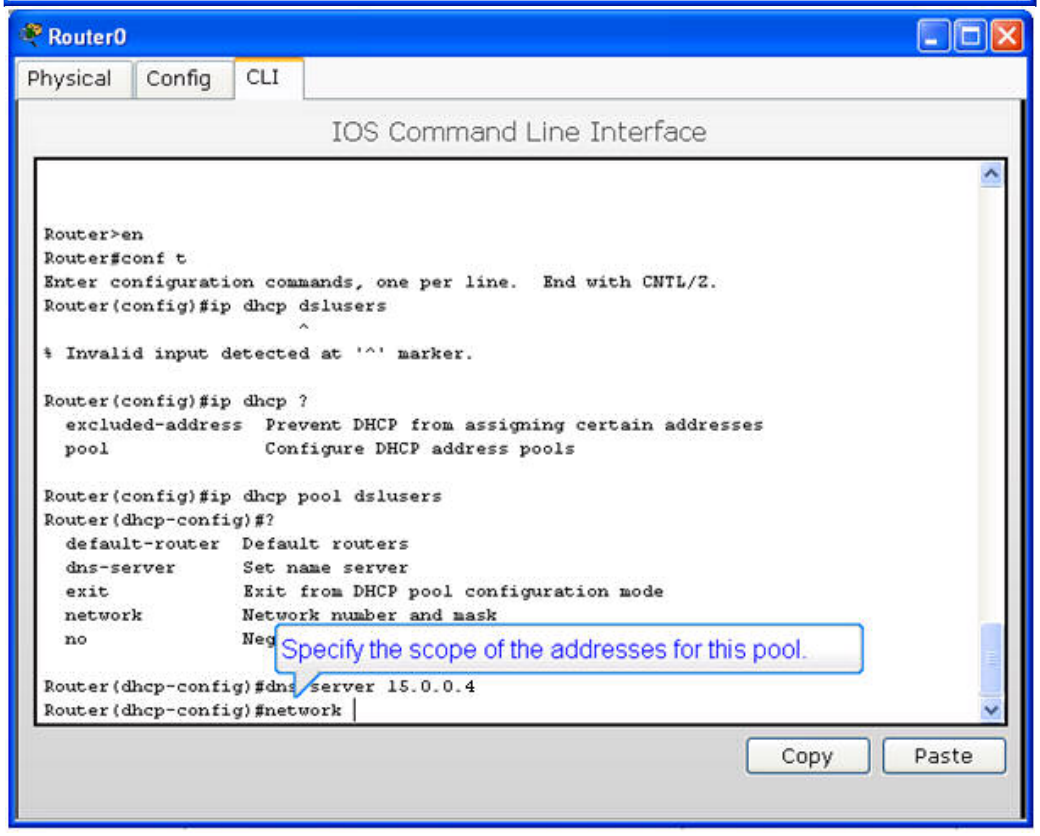

Router0
Physical
Config
CLI
IOS Command Line Interface
Compiled Wed 27-Apr-04 19:01 by miwang
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
3 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state t
o up
%LINEPI
Type en to go to Privilege mode.
ce FastEthernet2/0, changed state t
o up
Router>
Copy
Paste

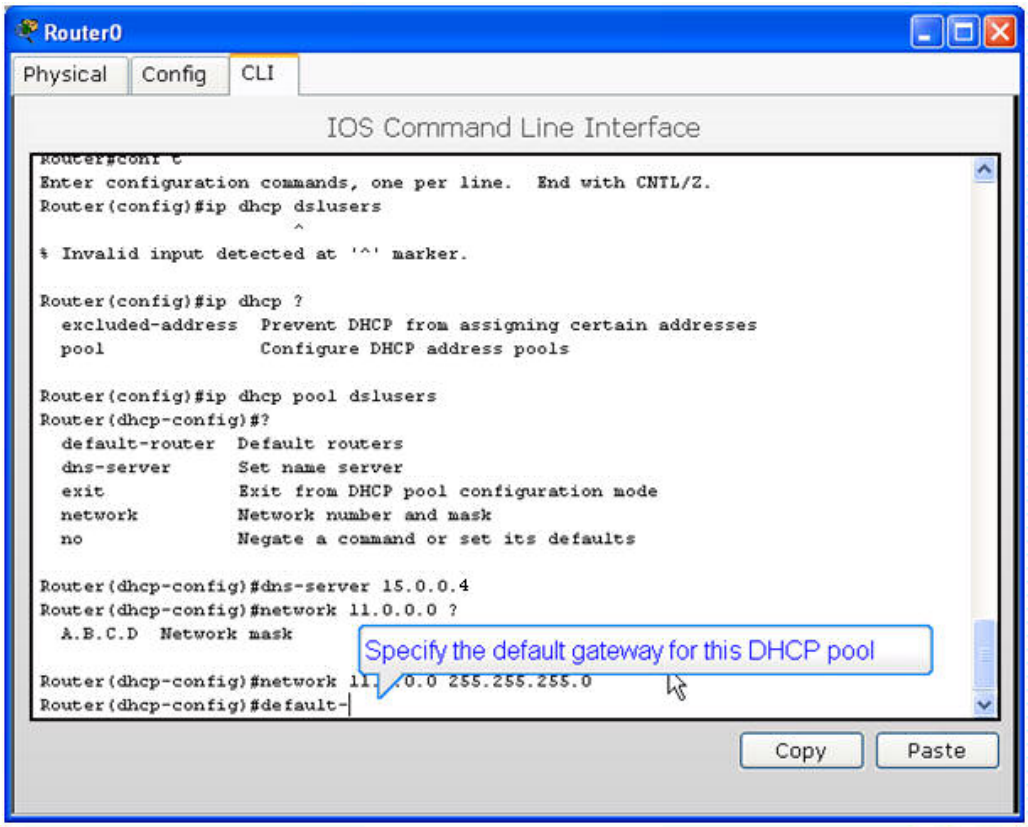

Router0
Physical
Config
CLI
IOS Command Line Interface
PT 1001 (PTSC2005) processor (revision 0x200) with 60416K/5120K bytes of memory
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
3 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state t
o up
Go to global config mode.
%LINEPR
nterface FastEthernet2/0, changed state t
o up
Router>en
Router#
Copy
Paste

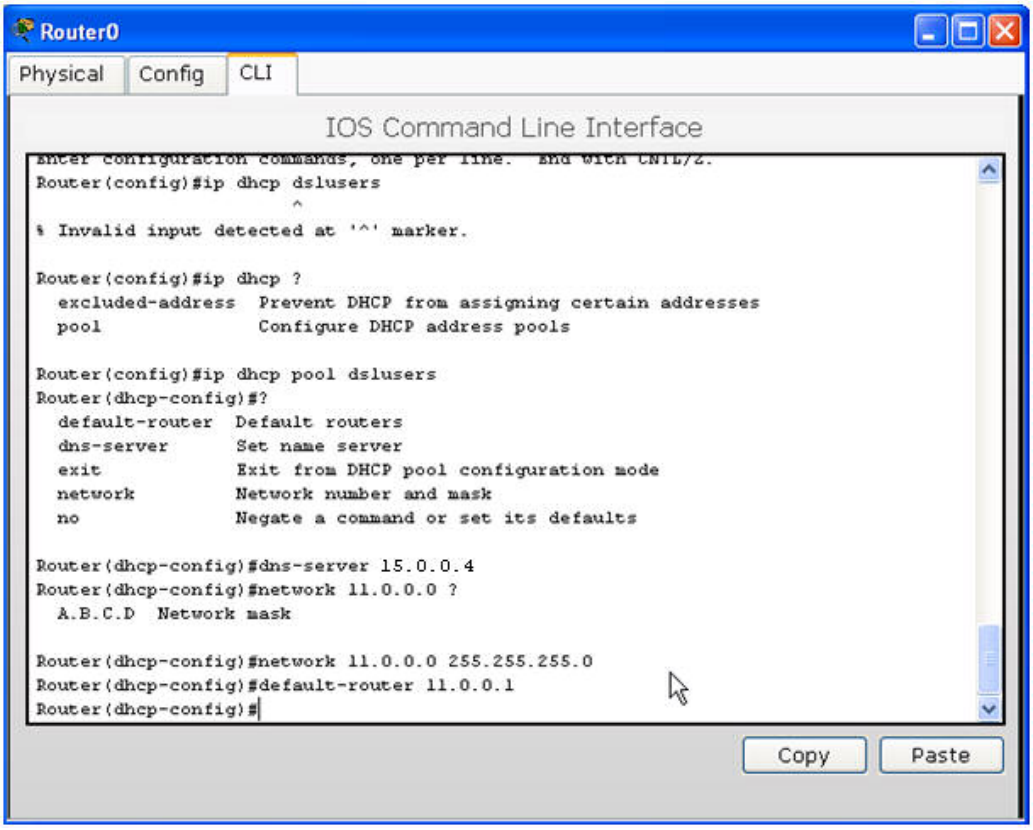

Router0
Physical
Config
CLI
IOS Command Line Interface
.
Processor board ID PT0123 (0123)
PT2005 processor: part number 0, mask 01
Bridging software.
X.25 software, Version 3.0.0.
3 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board
Create a dhcp pool with the name dslusers.
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state t
o up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state t
o up
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
Copy
Paste


Router0
Physical
Config
CLI
IOS Command Line Interface
X.25 software, Version 3.0.0.
3 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
Invalid input warning is shown when the command is not entered correctly.
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp dslusers
% Invalid input detected at '^' marker.
Router(config)#
Copy
Paste
Router0
Physical
Config
CLI
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp dslusers
% Invalid input detected at '^' marker.
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
Router(config)#ip dhcp pool dslusers
Router(dhcp-config)#
Copy
Paste

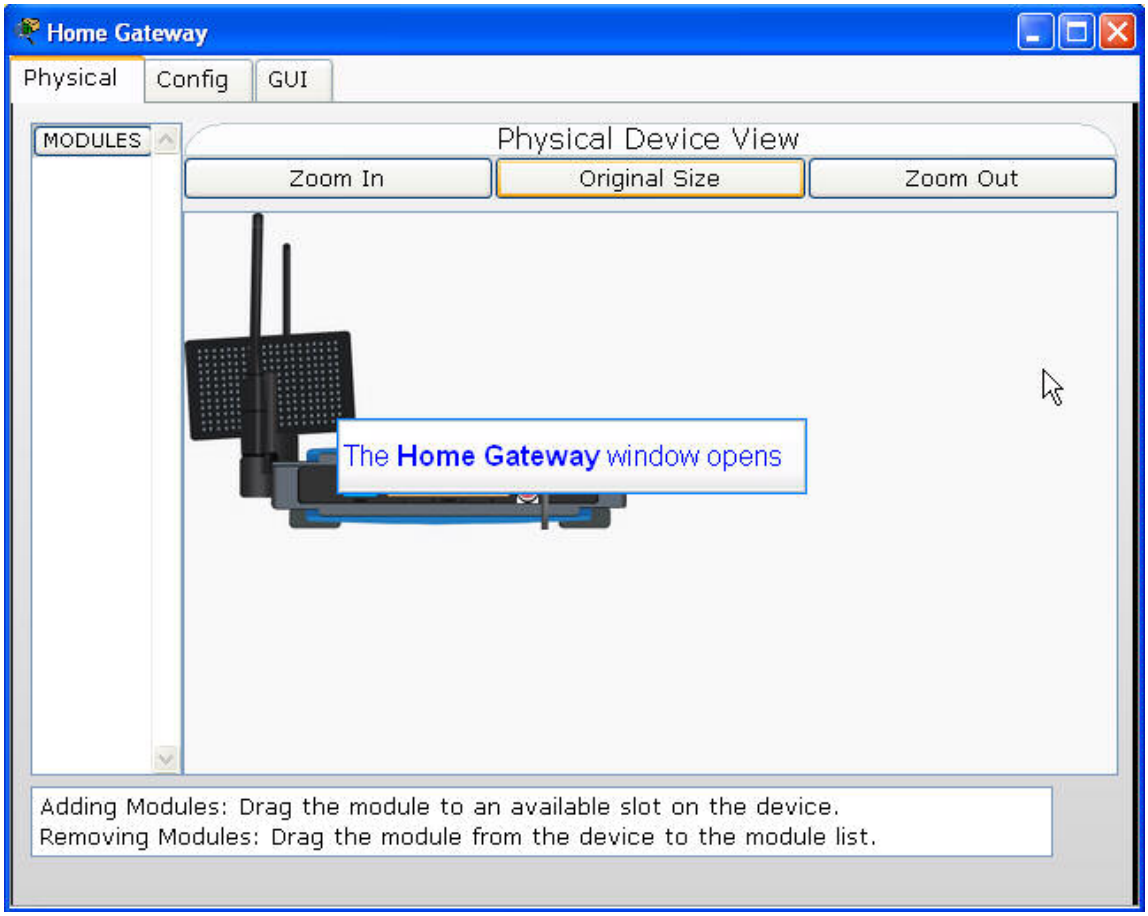

Router0
Physical
Config
CLI
IOS Command Line Interface
Press RETURN to get started!
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to up
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp dslusers
% Invalid input detected at '^' marker.
Specify the DNS Server for this DHCP pool.
Router(config)#ip dhcp pool dslusers
Router(dhcp-config)#
Copy
Paste


Router0
Physical
Config
CLI
IOS Command Line Interface
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp dslusers
% Invalid input detected at '^' marker.
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
Router(config)#ip dhcp pool dslusers
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
exit Exit from DHCP pool configuration mode
network Network number and mask
Specify the scope of the addresses for this pool.
Router(dhcp-config)#dns-server 15.0.0.4
Router(dhcp-config)#network
Copy
Paste

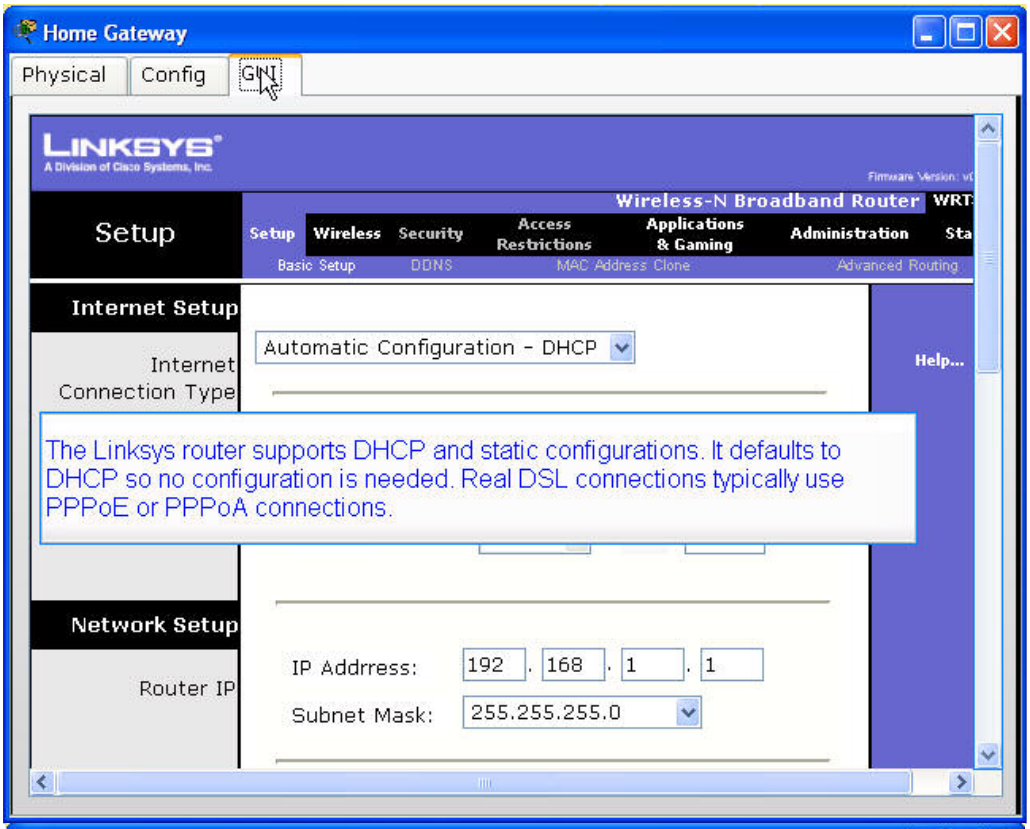

Router0
Physical
Config
CLI
IOS Command Line Interface
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip dhcp dslusers
^
% Invalid input detected at '^' marker.
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
Router(config)#ip dhcp pool dslusers
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
Router(dhcp-config)#dns-server 15.0.0.4
Router(dhcp-config)#network 11.0.0.0 ?
A.B.C.D Network mask
Specify the default gateway for this DHCP pool
Router(dhcp-config)#network 11.0.0.0 255.255.255.0
Router(dhcp-config)#default-
Copy
Paste

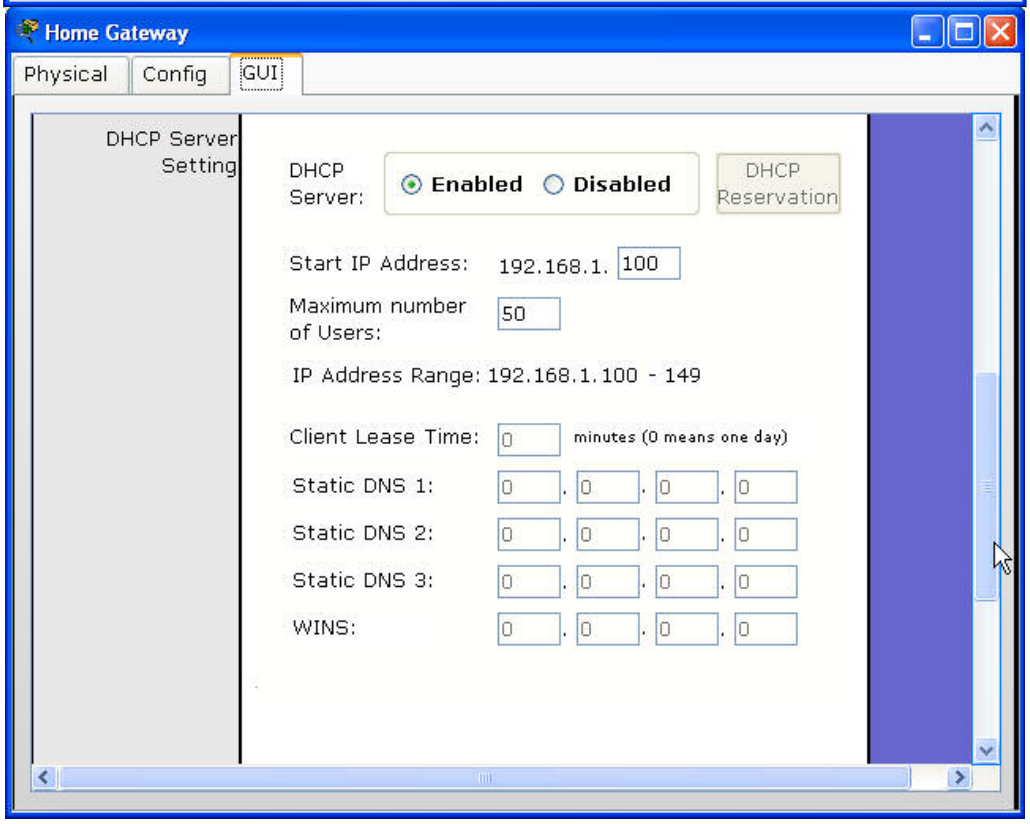

Router0
Physical
Config
CLI
IOS Command Line Interface
Router(config)#ip dhcp dslusers
^
% Invalid input detected at '^' marker.
Router(config)#ip dhcp ?
excluded-address Prevent DHCP from assigning certain addresses
pool Configure DHCP address pools
Router(config)#ip dhcp pool dslusers
Router(dhcp-config)#?
default-router Default routers
dns-server Set name server
exit Exit from DHCP pool configuration mode
network Network number and mask
no Negate a command or set its defaults
Router(dhcp-config)#dns-server 15.0.0.4
Router(dhcp-config)#network 11.0.0.0 ?
A.B.C.D Network mask
Router(dhcp-config)#network 11.0.0.0 255.255.255.0
Router(dhcp-config)#default-router 11.0.0.1
Router(dhcp-config)#
Copy
Paste

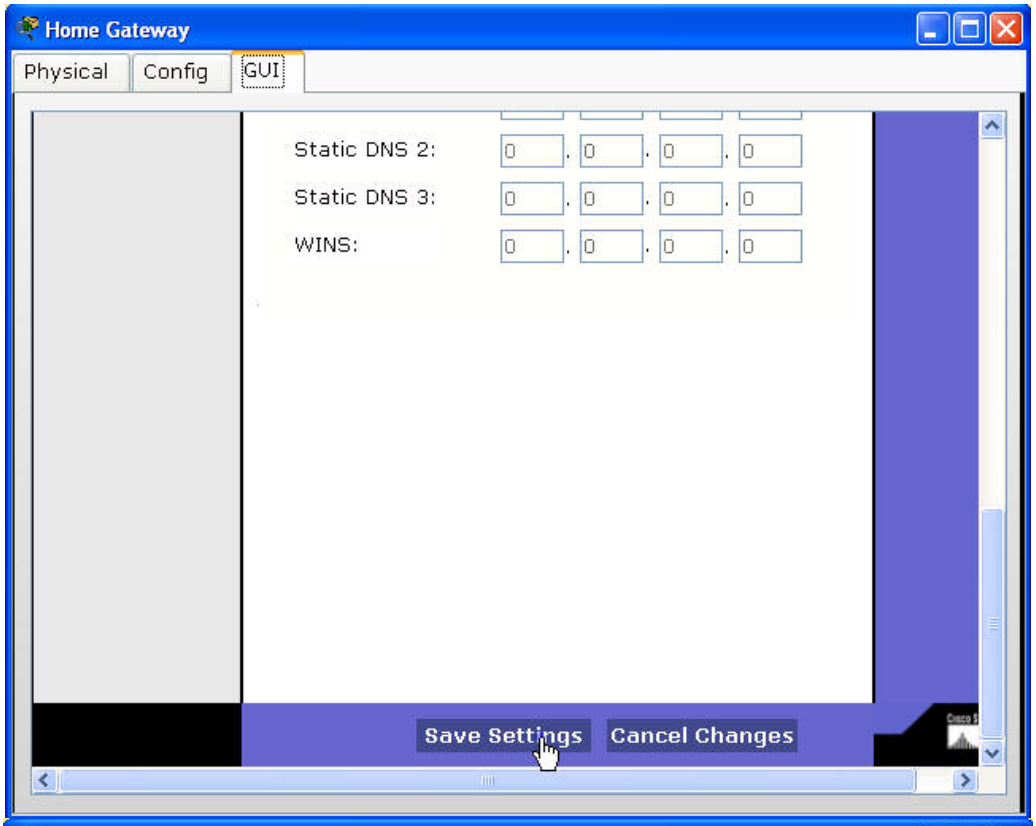
در پایان تنظیمات را ذخیره کنید. حال باید مسیریاب بیسیم Linksys را پیکربندی کنیم. روی آن کلیک کنید تا پنجره تنظیمات آن باز شود. بر روی برگه GUI کلیک کنید و تنظیمات را مطابق تصاویر دنبال کنید.

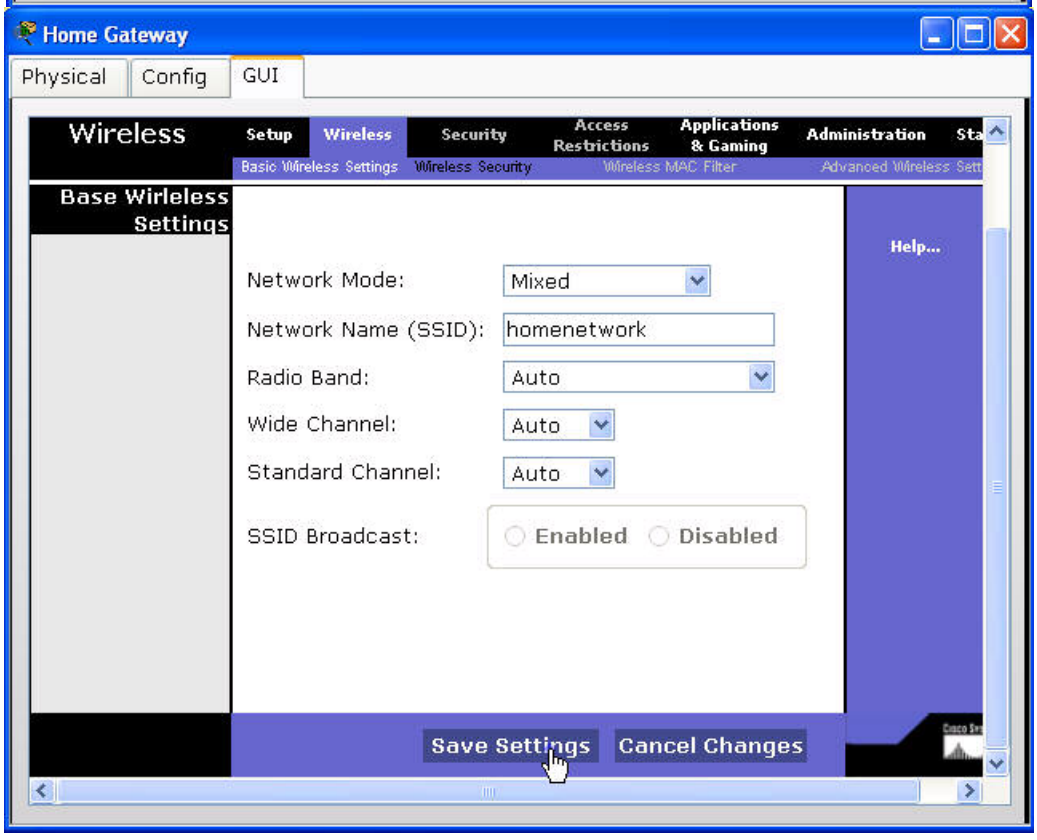


در این قسمت تنظیمات DHCP را می توان در حالت اتوماتیک قرار داد یا به صورت دستی تنظیم کرد. دقت کنید که واسط Linksys به صورت تحت وب است و در صورت هرگونه تغییر در تنظیمات هر صفحه ، باید همان صفحه به طور جداگانه ذخیره شود.

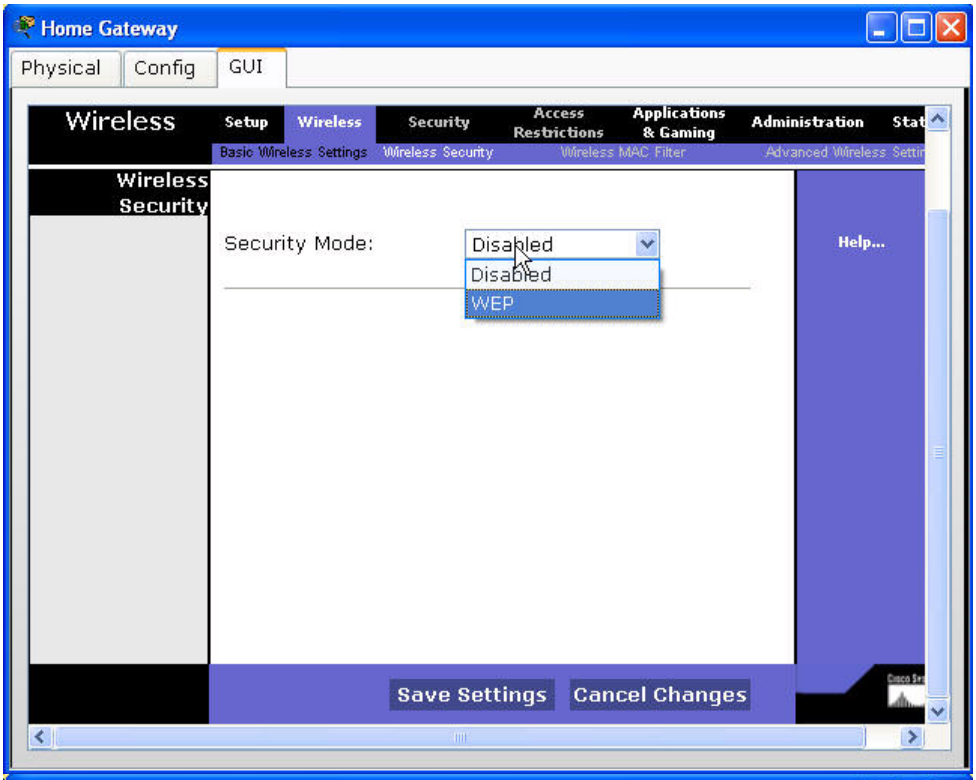

Home Gateway
Physical
Config
GUI
LINKSYS
A Division of Cisco Systems, Inc.
Wireless-N Broadband Router
Setup
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Internet Setup
Internet Connection Type
Automatic Configuration - DHCP
Help...
The Linksys router supports DHCP and static configurations. It defaults to DHCP so no configuration is needed. Real DSL connections typically use PPPoE or PPPoA connections.
Network Setup
Router IP
IP Address:
192 . 168 . 1 . 1
Subnet Mask:
255.255.255.0

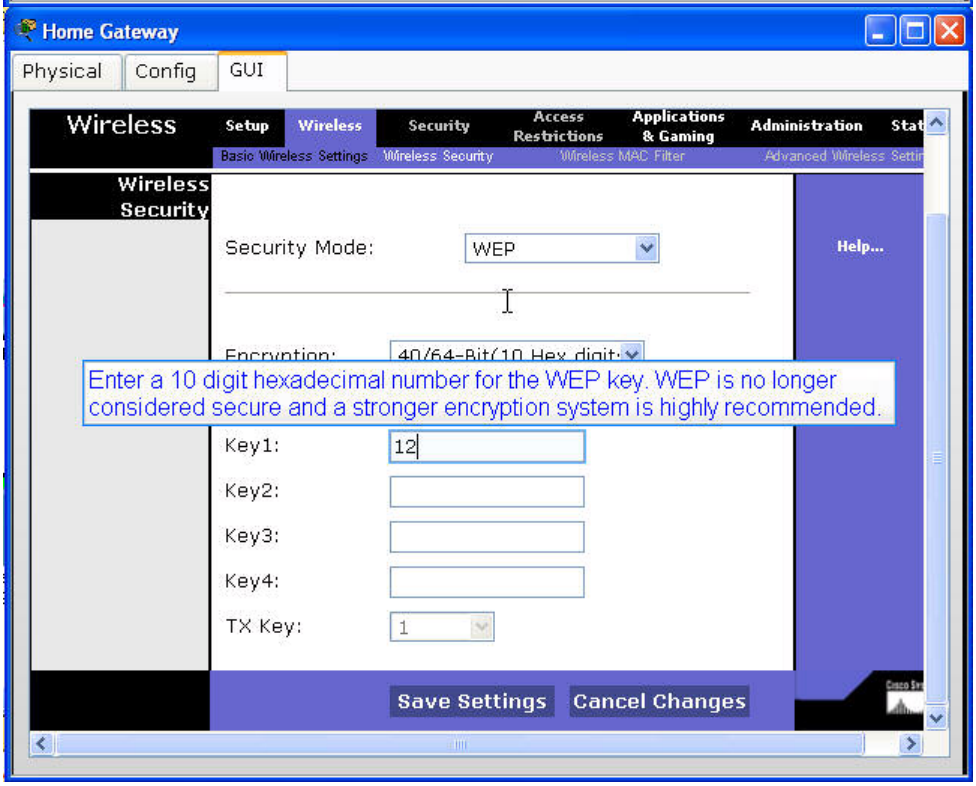

Home Gateway
Physical
Config
GUI
DHCP Server Setting
DHCP Server:
Enabled
Disabled
DHCP Reservation
Start IP Address:
192.168.1.
100
Maximum number of Users:
50
IP Address Range: 192.168.1.100 - 149
Client Lease Time:
0
minutes (0 means one day)
Static DNS 1:
Static DNS 2:
Static DNS 3:
WINS:

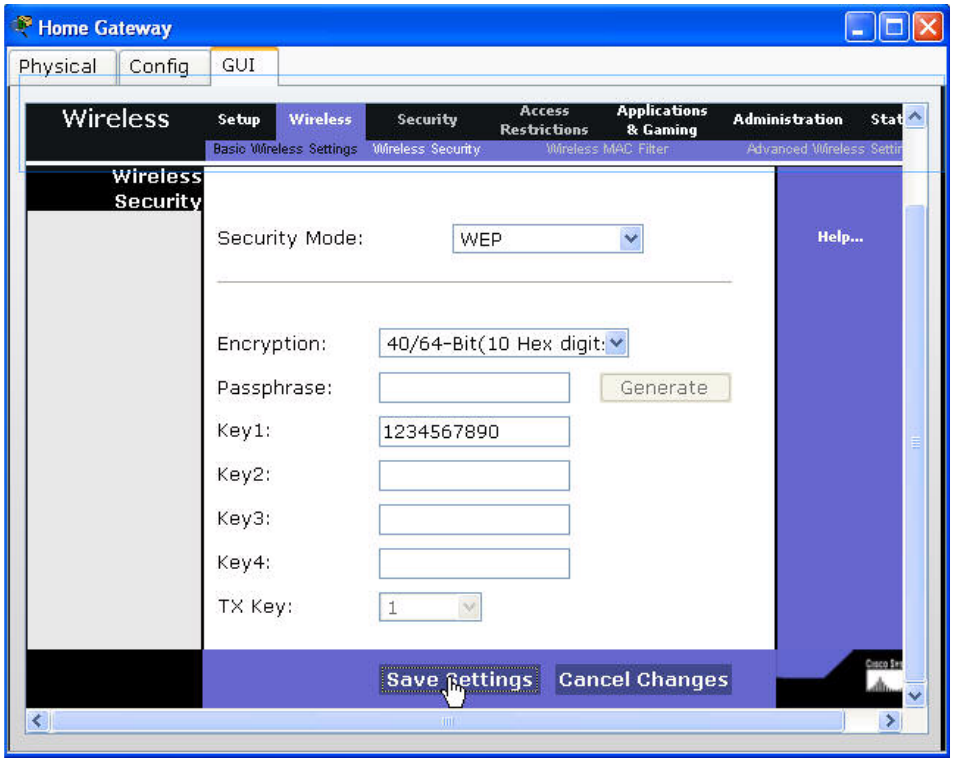

Home Gateway
Physical
Config
GUI
Static DNS 2:
Static DNS 3:
WINS:
Save Settings
Cancel Changes


Home Gateway
Physical
Config
GUI
Wireless
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Basic Wireless Settings
Wireless Security
Wireless MAC Filter
Base Wirleless Settings
Help...
Network Mode:
Mixed
Network Name (SSID):
homenetwork
Radio Band:
Auto
Wide Channel:
Auto
Standard Channel:
Auto
SSID Broadcast:
Enabled
Disabled
Save Settings
Cancel Changes

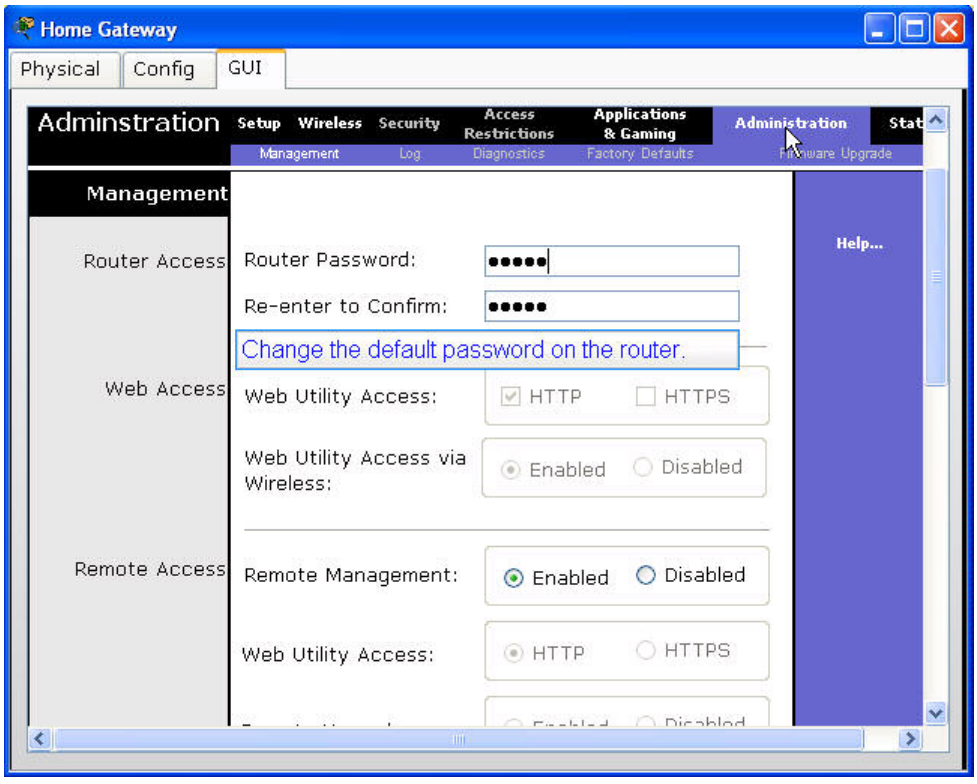
در این قسمت می توانید تنظیمات امنیتی را فعال کرده و یک کلید برای احراز هویت کاربرانی که قصد اتصال به صورت بیسیم دارند تعیین کنید.

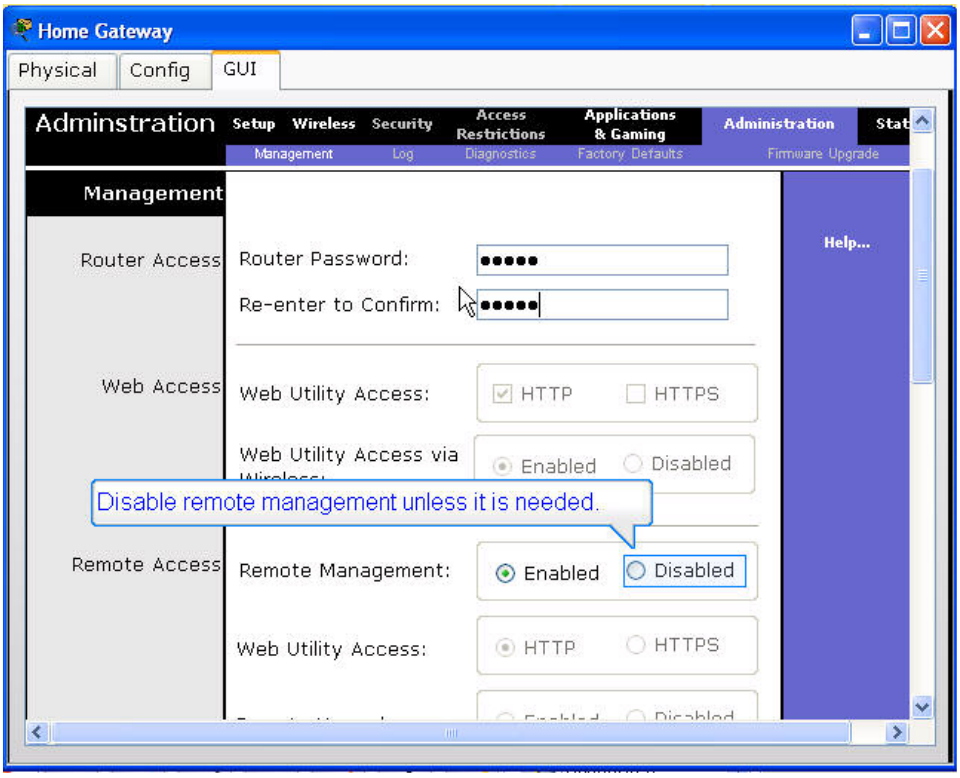




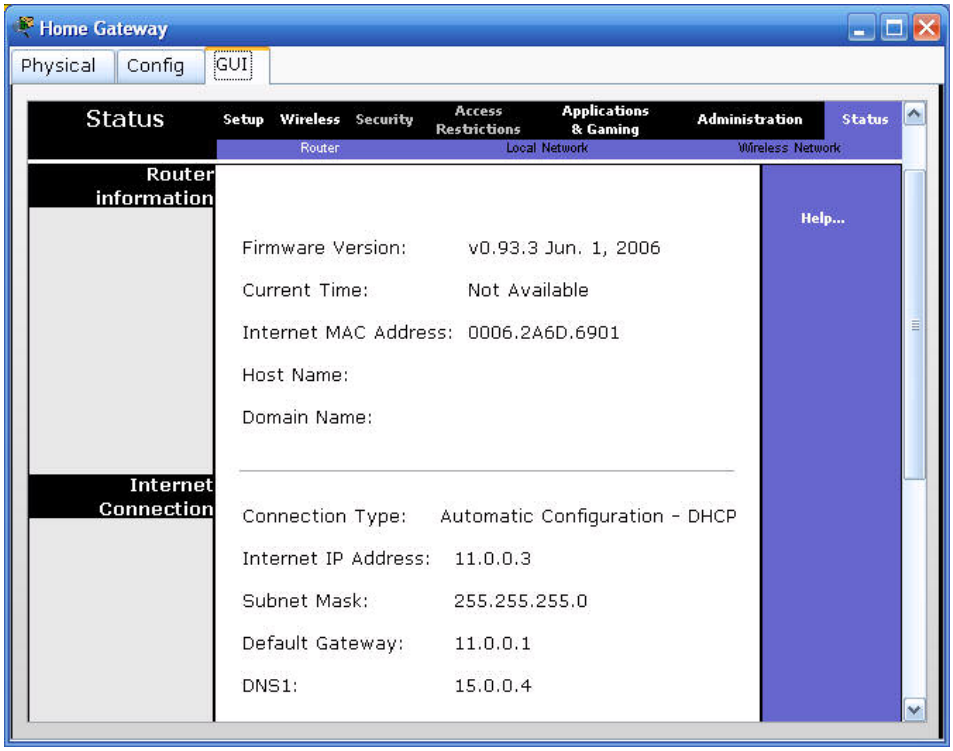


در این قسمت می توانید یک نام و کلمه عبور برای ورودی به تنظیمات Linksys از راه دور و از طریق مرورگر رایانه های شخصی تعیین کنید.

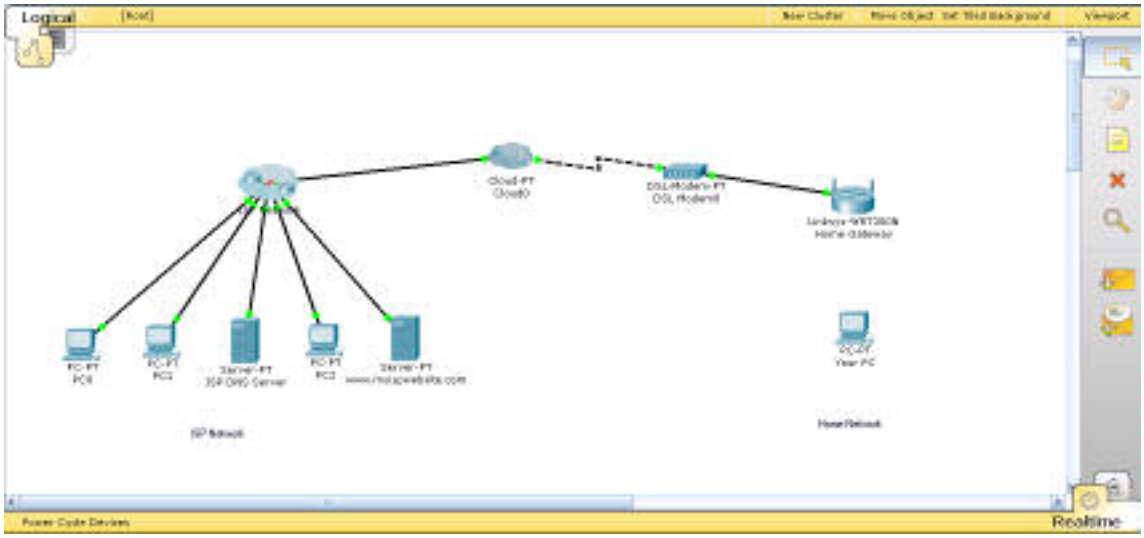




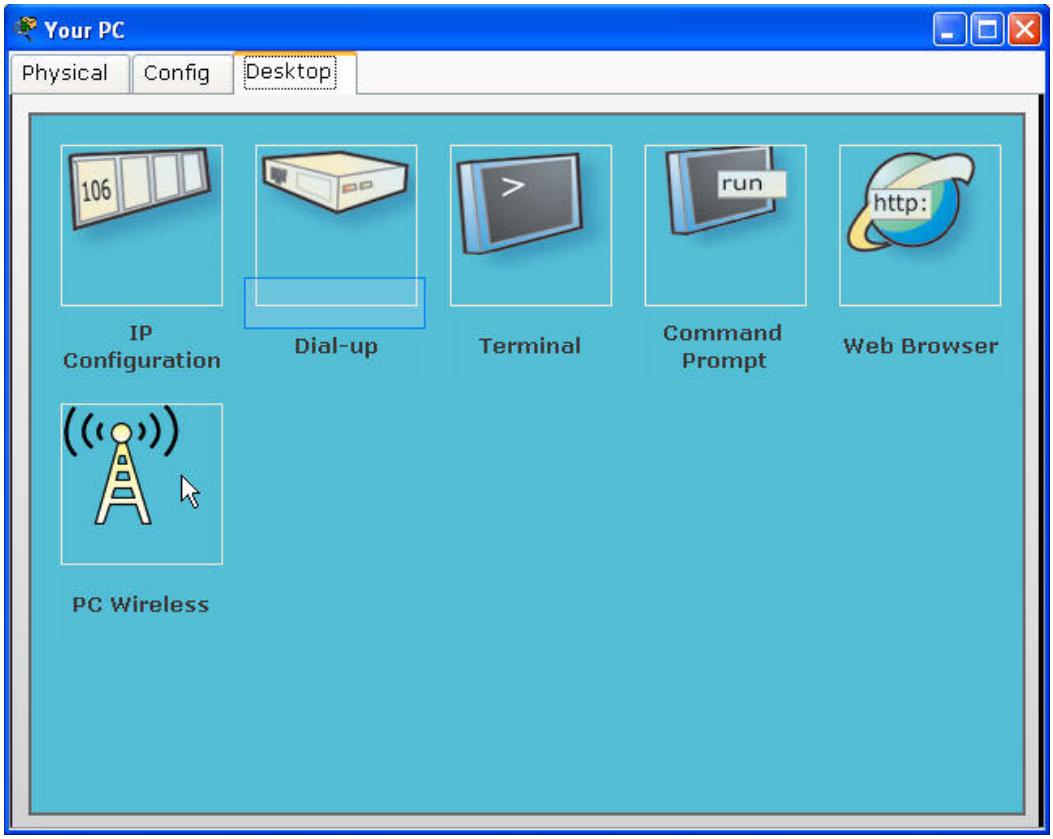
در قسمت Status وضعیت مسیریاب به طور خلاصه نمایش داده شده است.



با مراجعه به صفحه اصلی مشاهده خواهید کرد که ارتباط بین Your PC و مسیریاب LinkSys در شبکه خانگی ما قطع شده است. علت آن فعال کردن تنظیمات امنیتی است که می بایست برای برقراری اتصال پیکربندی شوند.



بر روی YourPC کلیک کنید و سپس وارد برگه Desktop شوید.

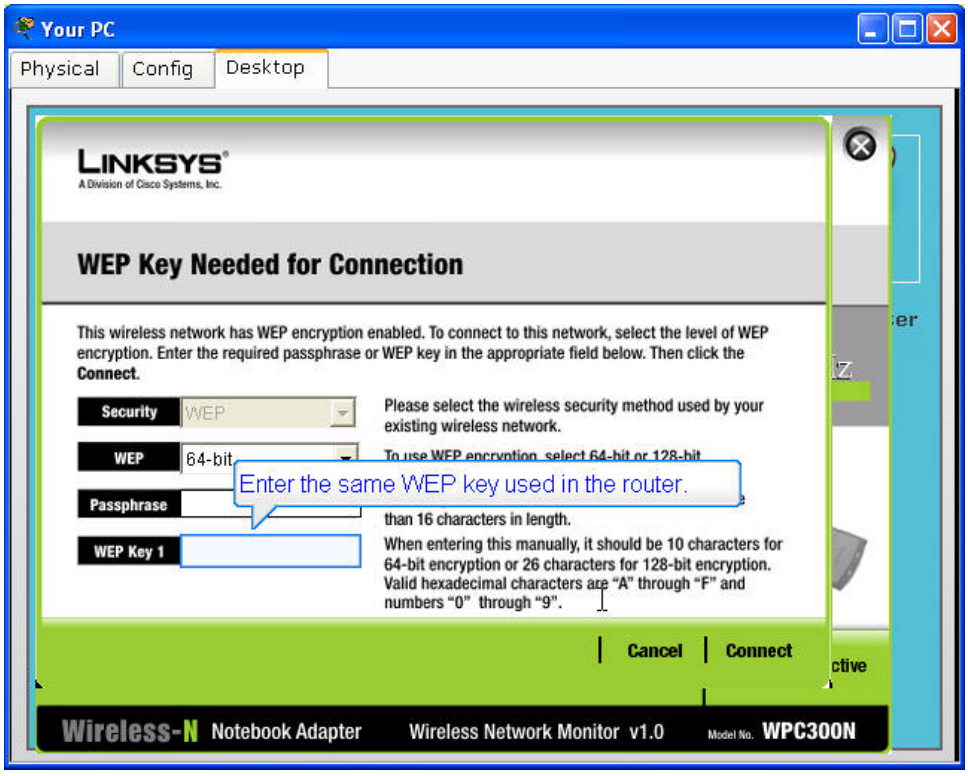


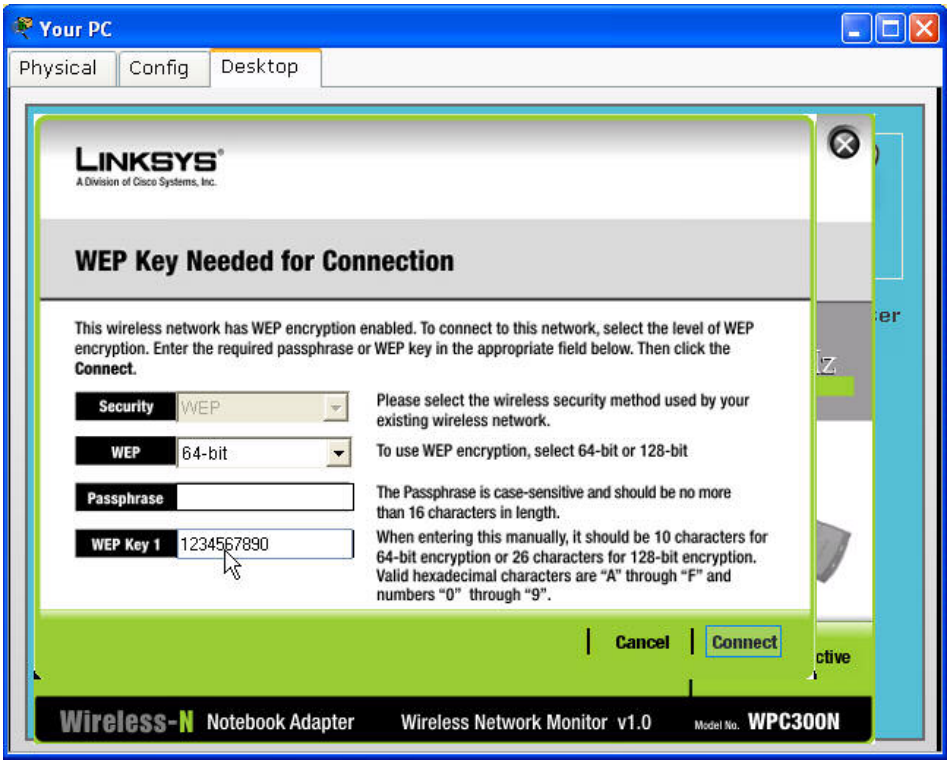
بر روی PC Wireless کلیک کنید تا تنظیمات شبکه بی سیم ظاهر شود.

در برگه Connect روی دکمه refresh کلیک کنید تا شبکه های بی سیم فعلی مشاهده شوند.

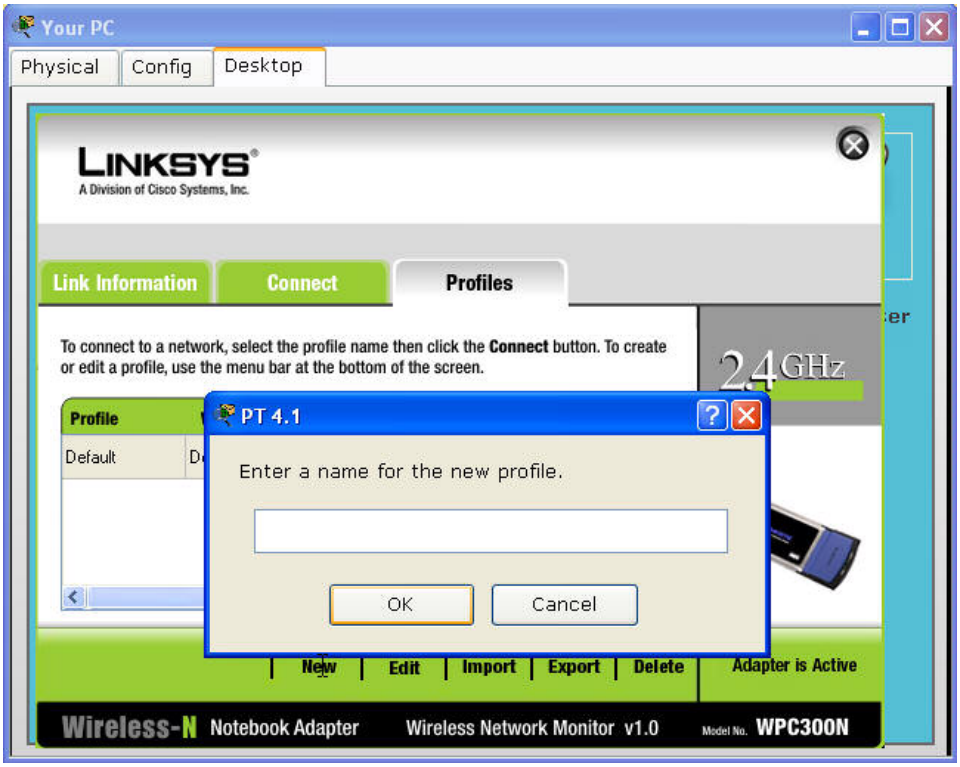


در صورتی که بر روی connect کلیک کنید، کلید احراز هویت از شما درخواست می شود.

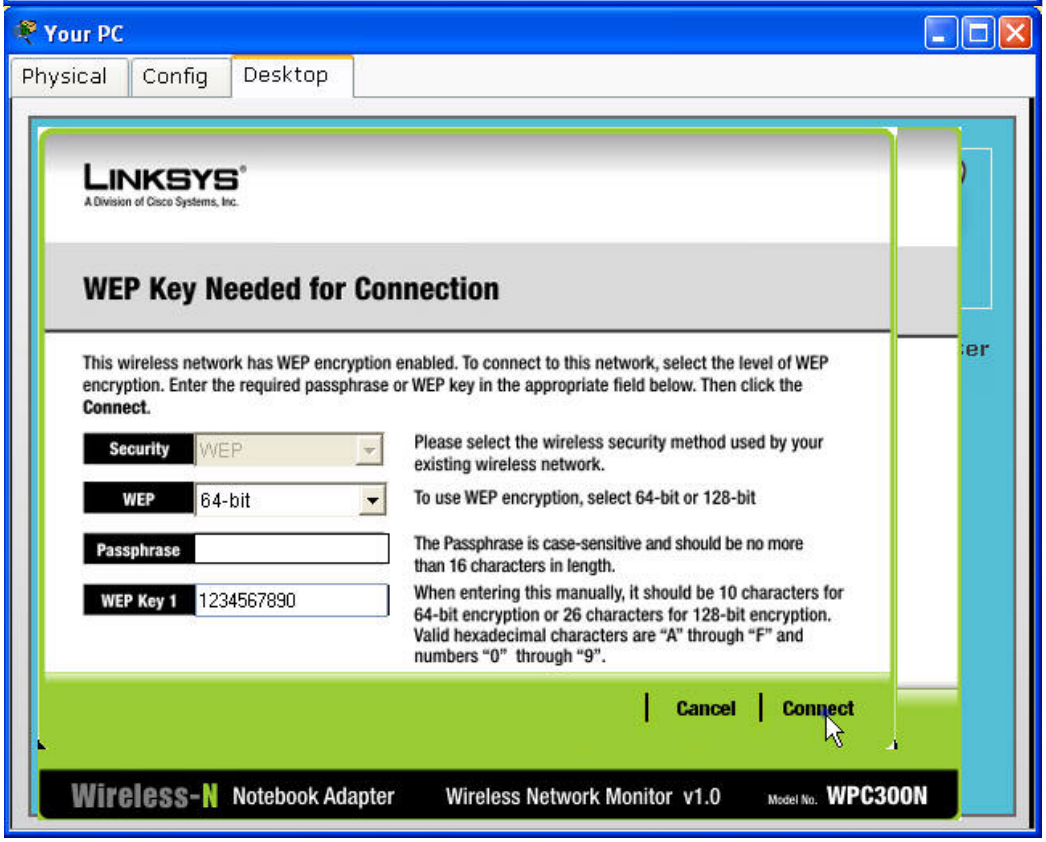




شما می توانید تنظیمات مربوط به شبکه را جهت دسترسی سریعتر در آینده در یک Profile ذخیره کنید.

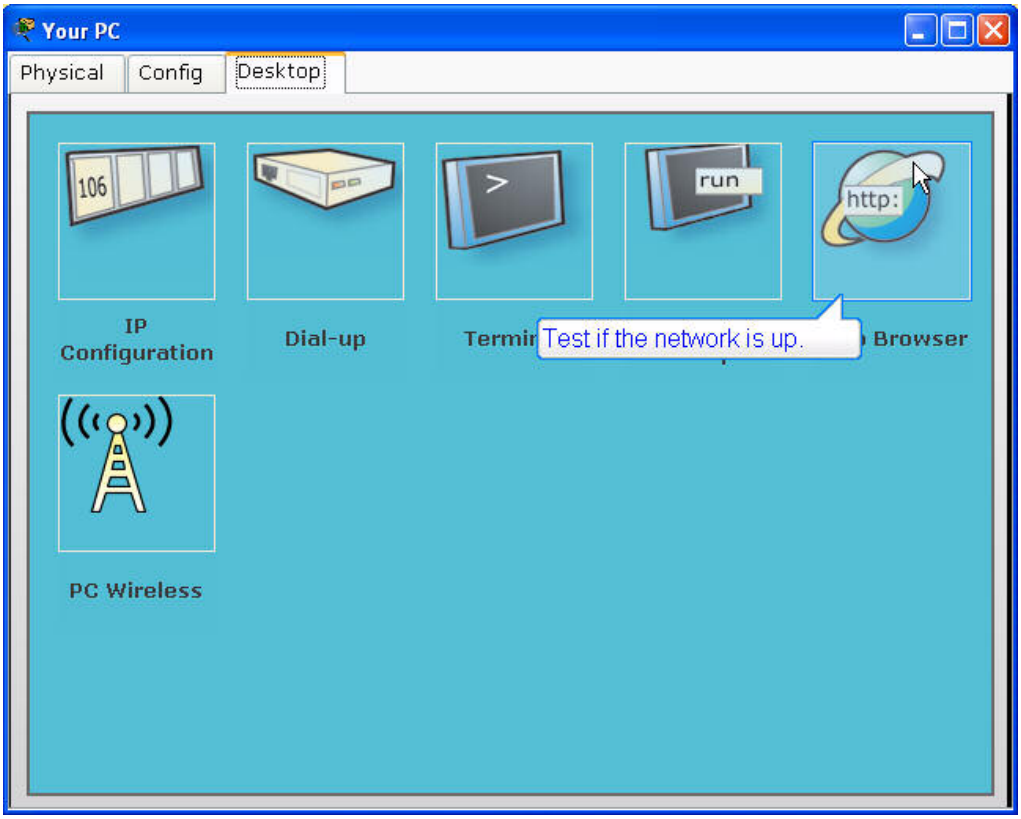



Your PC
Physical
Config
Desktop
LINKSYS
A Division of Cisco Systems, Inc.
Creating a Profile
Available Wireless Networks
Please select the wireless network that you want to connect to, then click the Connect button to continue. If you are not sure which network to choose, first try the one with the strongest signal.
Wireless Network Name
CH
Signal
Security
homenetwork
6
100%
WEP
Refresh
Connect
Exit
Advanced Setup
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N

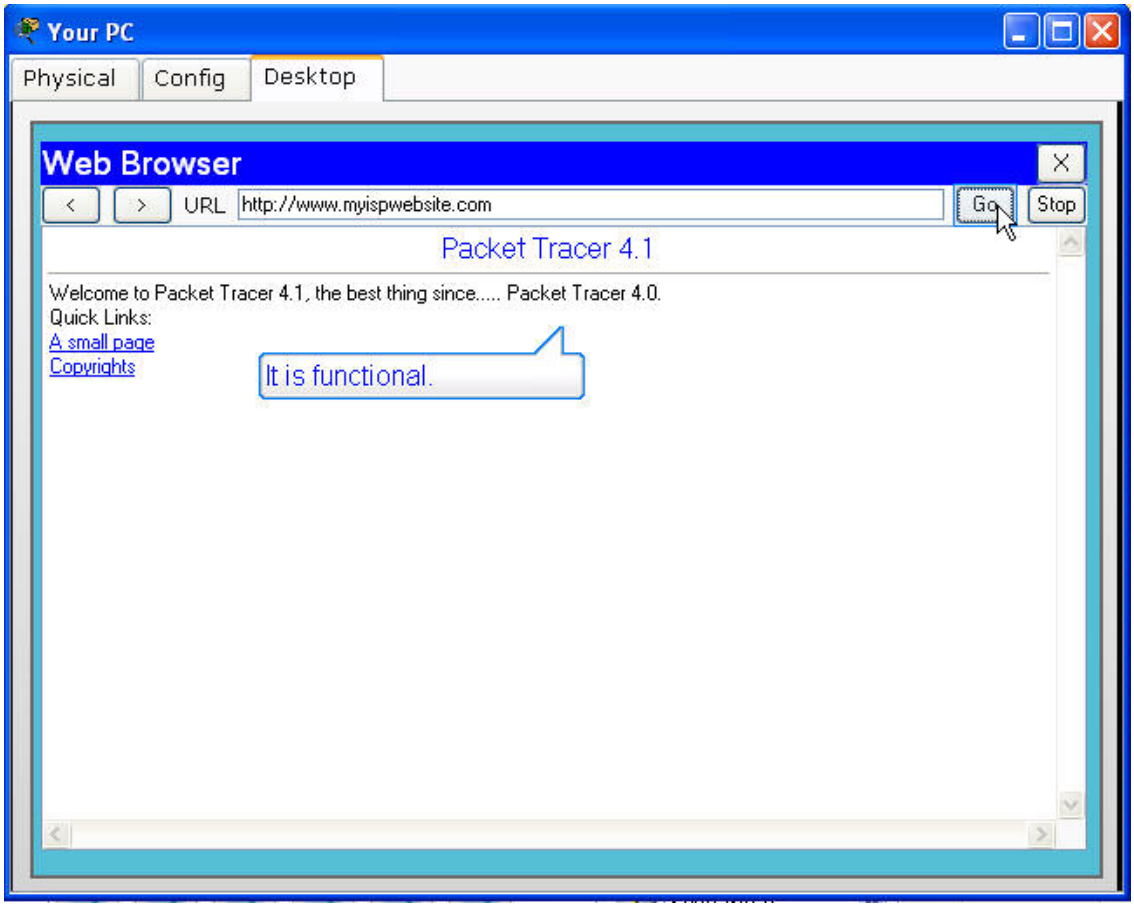

Your PC
Physical
Config
Desktop
LINKSYS
A Division of Cisco Systems, Inc.
WEP Key Needed for Connection
This wireless network has WEP encryption enabled. To connect to this network, select the level of WEP encryption. Enter the required passphrase or WEP key in the appropriate field below. Then click the Connect.
Security
WEP
Please select the wireless security method used by your existing wireless network.
WEP
64-bit
To use WEP encryption, select 64-bit or 128-bit
Passphrase
The Passphrase is case-sensitive and should be no more than 16 characters in length.
WEP Key 1
1234567890
When entering this manually, it should be 10 characters for 64-bit encryption or 26 characters for 128-bit encryption. Valid hexadecimal characters are "A" through "F" and numbers "0" through "9".
Cancel
Connect
Wireless-N Notebook Adapter
Wireless Network Monitor v1.0
Model No. WPC300N



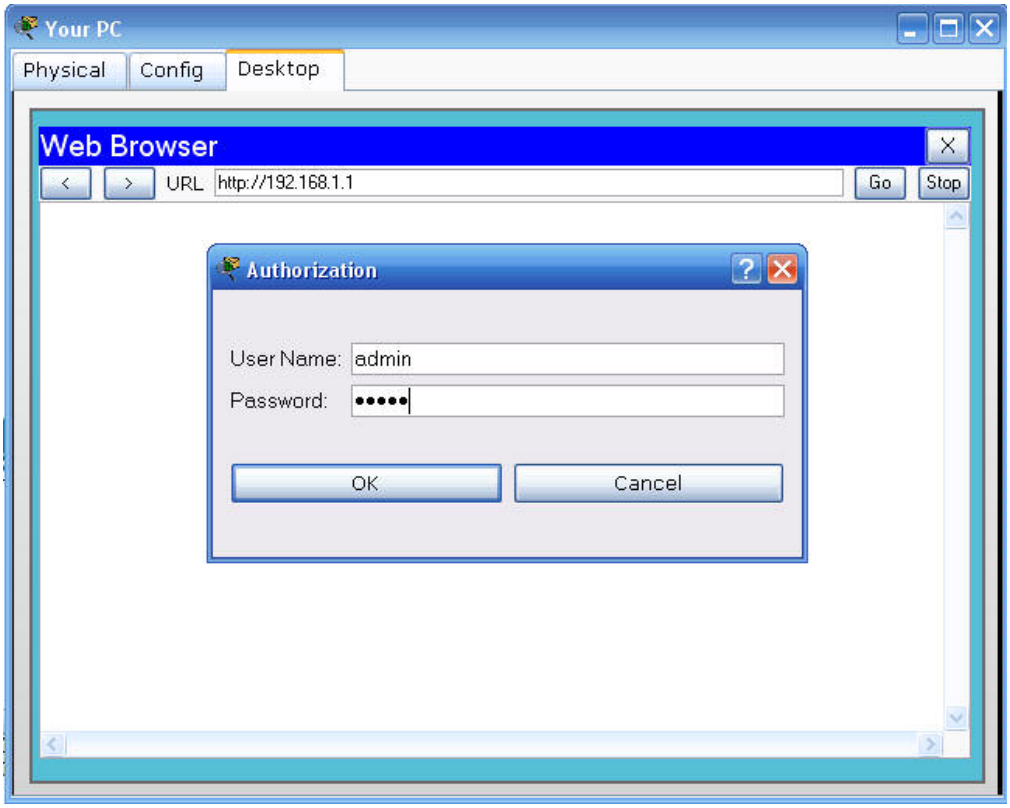
حال برای بررسی وضعیت اتصال مرور گر وب را باز کنید.

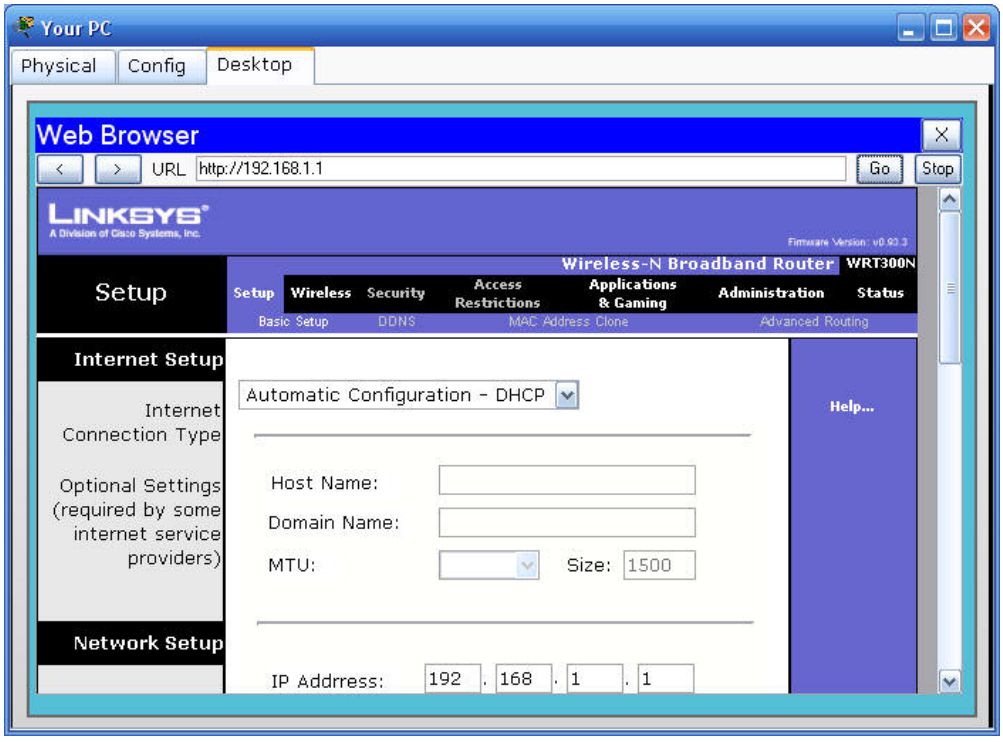


آدرس سایت www.myispwebsite.com را که قبلا در سرور dns نیز آن را اضافه کردید وارد کنید. در صورتیکه تنظیمات شبکه را تا به اینجا به خوبی انجام داده باشید، می بایست صفحه وب به شما نمایش داده شود.



علاوه براین شما می توانید به تنظیمات مسیریاب Linksys نیز دسترسی داشته باشید. آدرس IP مسیریاب را در نوار آدرس وارد کنید. پس از ورود نام کاربری و کلمه عبور (در حالت پیش فرض هر دو admin هستند) می توانید تنظیمات را از طریق وب انجام دهید.


Your PC
Physical
Config
Desktop
Web Browser
URL
http://192.168.1.1
Go
Stop
Authorization
User Name:
admin
Password:
OK
Cancel


Your PC
Physical
Config
Desktop
Web Browser
URL
http://192.168.1.1
Go
Stop
LINKSYS
Wireless-N Broadband Router
WRT300N
Setup
Wireless
Security
Access Restrictions
Applications & Gaming
Administration
Status
Basic Setup
DDNS
MAC Address Clone
Advanced Routing
Internet Setup
Internet Connection Type
Automatic Configuration - DHCP
Optional Settings (required by some internet service providers)
Host Name:
Domain Name:
MTU:
Size:
1500
Help...
Network Setup
IP Address:
192
168
1
1

۴۱-۱۸-Activity Wizard

Activity Wizard یک ابزار ارزیابی است که به شما امکان ایجاد سناریو های شبکه دلخواه و متنوعی را برای دیگر کاربران فراهم می آورد. این ابزار مخصوصا برای اساتید جهت ایجاد تمرین (فعالیت) برای دانشجویان مفید است. زمانی که دانشجویان یک فعالیت را شروع می کنند، با یک شبکه اولیه و مجموعه ای از دستورالعمل ها مواجه هستند. دانشجویان باید دستورالعمل ها را دنبال کرده و فعالیت را تکمیل کنند. آن ها می توانند شبکه کامل شده خود را با راه حل آن بررسی کنند. نکته مهم این است که استاد بر روی همه حالت های فعالیت کنترل کامل دارد.



ترتیب معمول ایجاد فعالیت به صورت زیر است:

۱- ایجاد شبکه پاسخ و تنظیم آیتم های ارزیابی، تست های اتصال و فیدبک کلی

۲- ایجاد شبکه اولیه که نقطه شروع دانشجویان است. معمولا مشابه شبکه پاسخ است که برخی ویژگی های آن حذف شده، یا برخی تنظیمات پیکربندی وجود ندارد یا دستگاه ها اشتباه پیکربندی شده اند و...

۳- قرار دادن محدودیت هایی بر روی برخی ویژگی ها و قابلیت ها در طول انجام فعالیت

۴- تنظیمات متغییرهای مدیریت برای افزودن پویایی به فعالیت

۵- نوشتن یا دستورالعمل واضح برای فعالیت

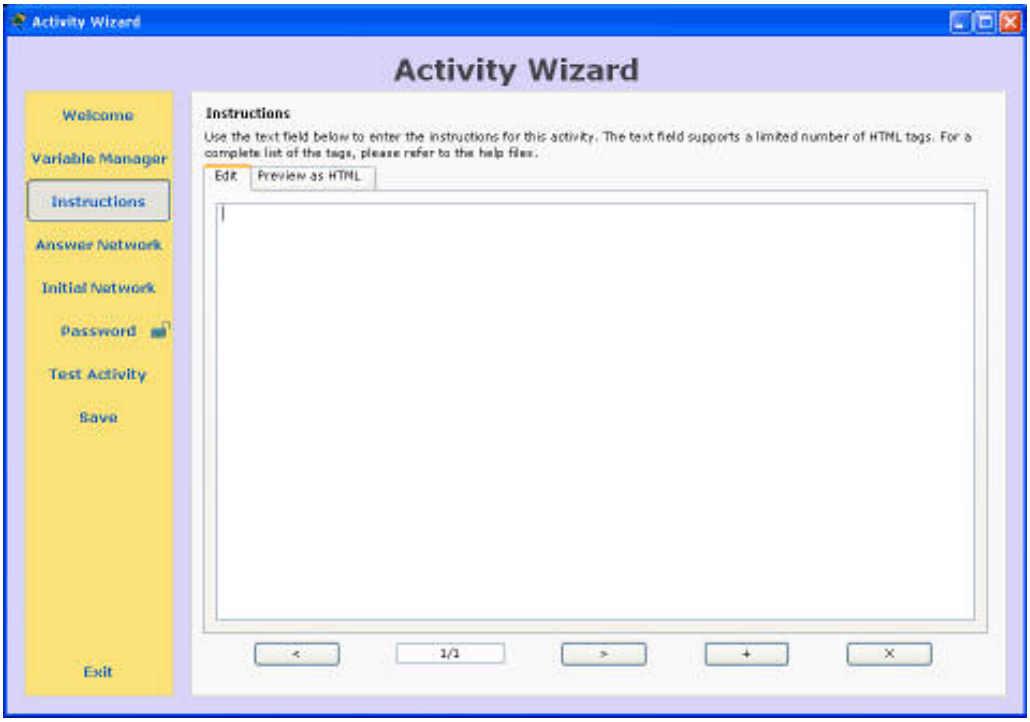
۶- محافظت از فعالیت با کلمه عبور برای جلوگیری از تغییرات ناخواسته

۷- ذخیره کردن فعالیت.

دسترسی به Activity Wizard از منوی file امکان پذیر است. با اجرای این دستور شما می توانید انتخاب کنید که از فضای کار فعلی بعنوان پاسخ استفاده شود یا یک فضای کار جدید ایجاد شود. توسط Activity Menu در سمت چپ می توانید حالت های مختلف فعالیت را تنظیم کنید و بعد از ایجاد فعالیت، با استفاده از Save در Activity Menu می توانید آنرا ذخیره نمایید(با فرمت pka).

پانل دستورالعمل ها (Instructions)

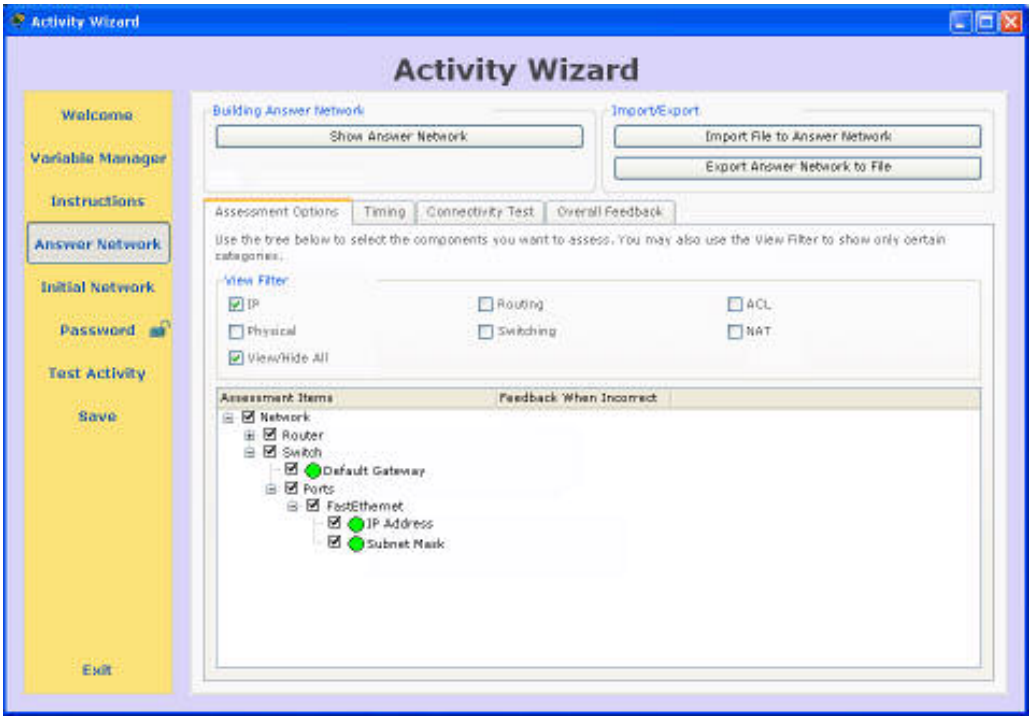
شما دستورالعملهای دانشجویان را جهت انجام فعالیت در این پانل می نویسید. وقتی دانشجویان فایل فعالیت را بازکنند، این دستورالعمل ها در پنجره جداگانه ای نمایش داده خواهد شد تا قابل مشاهده باقی بماند. این دستورالعمل ها باید به وضوح اهداف فعالیت را شرح دهند. اگر محدودیت خاصی وجود دارد باید روش مورد نظر اشاره شود تا موجب سردرگمی دانشجو با آیتم ها و توابع قفل شده نگردد. برای قالب بندی دستورالعمل شما می توانید از تگ های HTML استفاده کنید. این امکان وجود دارد که دستورالعمل ها را در چندین صفحه جداگانه بنویسید تا شلوغی صفحه کاهش داده شود.



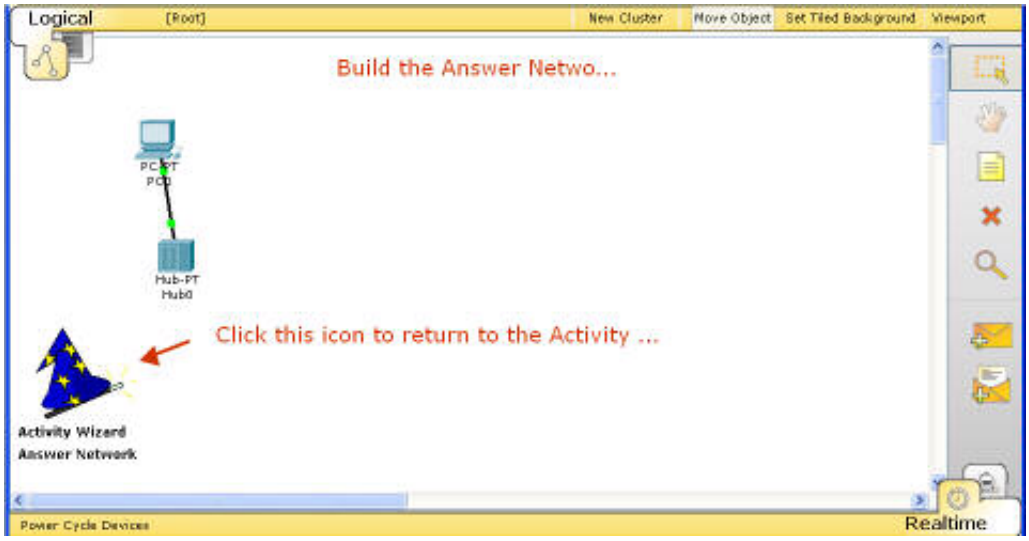
تگ های HTML پشتیبانی شده توسط این قسمت شامل موارد زیر می باشد:

- <p>
-
- <b>
- <i>
- <pre>
- <font>
- <img>

پانل شبکه پاسخ (Answer Network)



در پانل شبکه پاسخ، شما می توانید شبکه نهایی (راه حل) را ایجاد کنید و عناصر مورد ارزیابی را مشخص کنید. روی Show Answer Network کلیک کنید تا فضای کار جهت ایجاد شبکه نمایش داده شود. در این قسمت شما می توانید یک فایل pkt که قبلا ایجاد کرده اید را نیز import کنید و از شبکه آن استفاده نمایید. در هر صورت پس از تکمیل شبکه پاسخ، می توانید آن را به صورت یک فایل pkt ذخیره کنید (export).

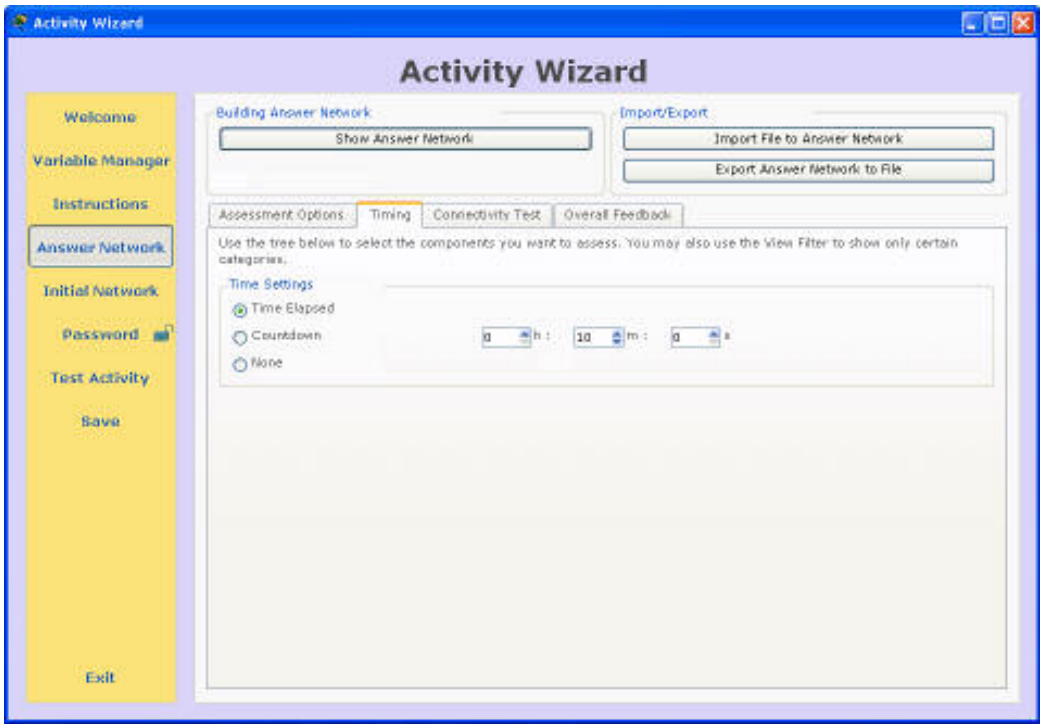


تنظیم آیتم های ارزیابی

آیتم های ارزیابی باید با پیکربندی های موجود در شبکه پاسخ منطبق باشد. شما می توانید آیتم های مورد نظر را در درخت نمایش داده شده فعال کنید. برای راحتی کار می توانید ویژگی های خاصی را از درخت پنهان نمایید. این کار با استفاده از فیلترهای مختلفی که در قسمت بالای کادر قرار دارد انجام می شود. برای مثال با غیر فعال کردن فیلتر Routing همه گروه های مرتبط با مسیریابی از جمله مسیرهای استاتیک، پویا و RIP پنهان خواهد شد. همچنین شما می توانید آیتم هایی را برای فیدبک مشخص کنید تا امکان راهنمایی دانشجویان در صورت انجام اشتباه فعالیت، در زمان مشاهده نتیجه فراهم آورده شود.

تنظیمات زمان

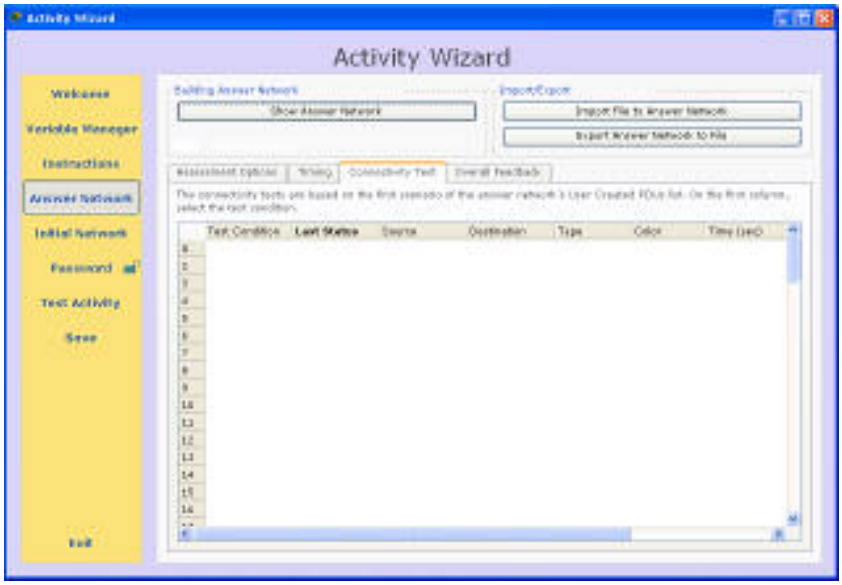
شما می توانید تنظیماتی را در مورد زمان بندی فعالیت انجام دهید. مثلا زمان سپری شده (Time Elapsed) را نمایش دهید یا یک محدودیت زمانی (Countdown) اعمال کنید.



بررسی اتصالات

ویژگی Connectivity Testing روش دیگری برای ارزیابی است. برخلاف آیتم های ارزیابی که پیکربندی های شبکه را بررسی کرده و آن را با پیکربندی شبکه پاسخ مقایسه می کنند، این

قسمت بر اساس PDU های realtime ای است که در حین مشاهده نتیجه بررسی می گردند. این بررسی بر اساس PDU های ایجاد شده در اولین سناریوی شبکه پاسخ انجام می شود.



فیدبک کلی (Overall Feedback)

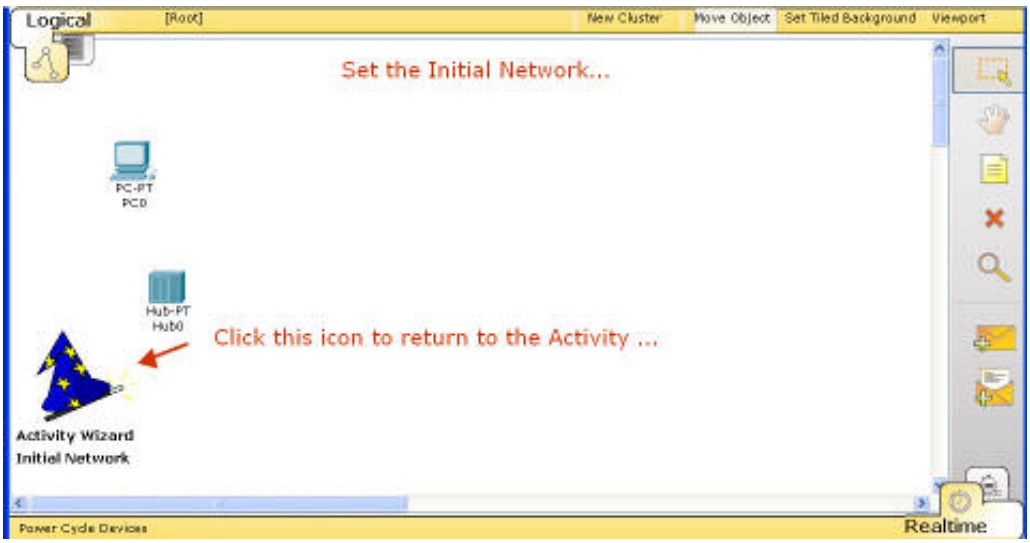
این قسمت به شما امکان تنظیم پیغام های دلخواه را برای فعالیت های کامل شده یا نا تمام فراهم می آورد. پیغام های Completed Feedback زمانی که فعالیت ۱۰۰ درصد کامل شد نمایش داده می شوند. در غیر اینصورت پیغام های Incomplete Feedback نمایش داده خواهد شد. این قسمت از تگ های HTML پشتیبانی نمی کند.



پانل شبکه اولیه (Initial Network)



در این قسمت شما می توانید تعیین کنید که دانشجویان از چه نقطه ای فعالیت خود را آغاز کنند. یک گزینه ساده برای شروع این است که به آسانی شبکه پاسخ را کپی نموده و بخش هایی از آن را ویرایش کنید. این کار با دکمهShow Initial Network انجام می شود. گزینه دیگر وارد کردن فایل با استفاده از Import File to Init Network است. بعد از ایجاد شبکه اولیه می توانید آن را Export کنید.



استفاده از Locking Tree

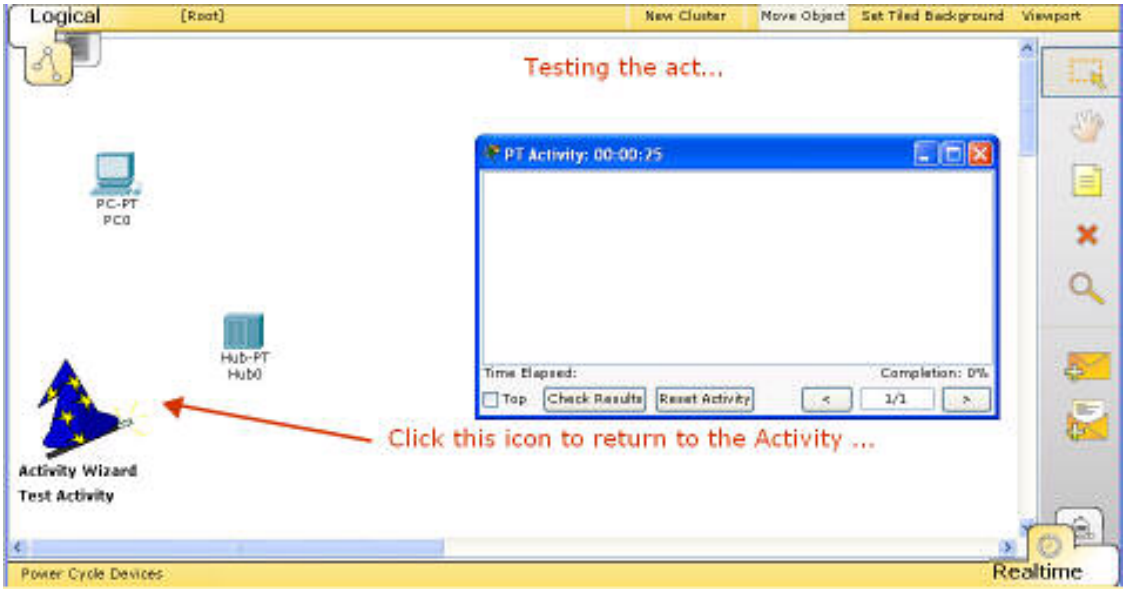
درخت نمایش داده شده در این قسمت برای قفل کردن توابعی است که نمی خواهید دانشجو به آنها دسترسی داشته باشد. برای مثال می توانید از این که دانشجو به فضای کار فیزیکی سوئیچ کند جلو گیری کنید. (در گروه Interface). البته باید مراقب توابعی که قفل می کنید باشید تا مانع از رسیدن به جواب نشوند.

تعیین کلمه عبور



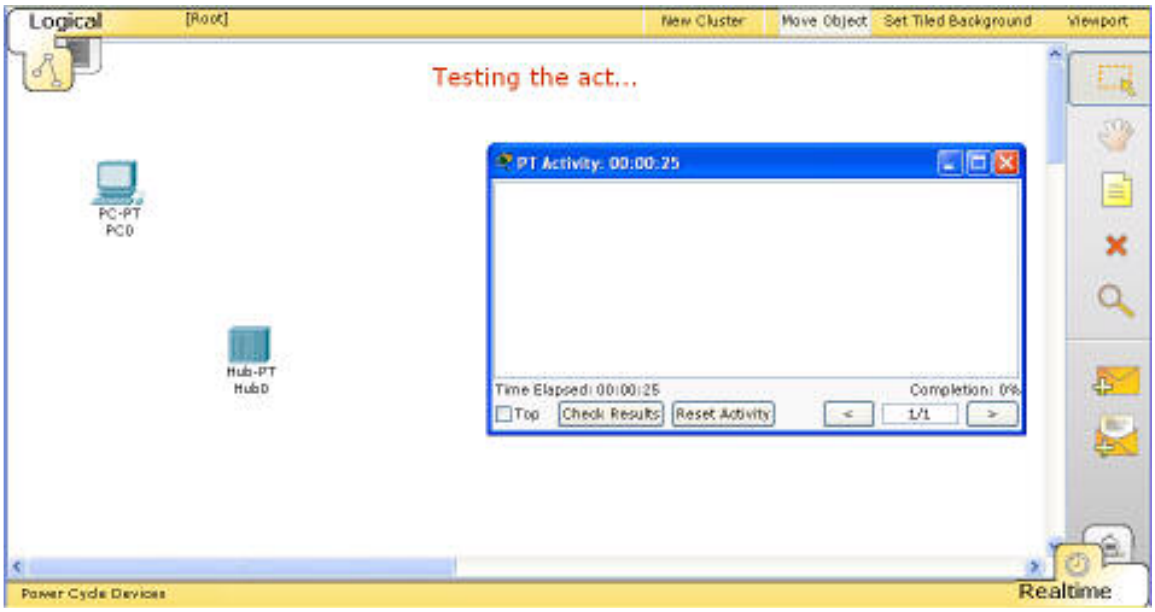
در این پانل شما می توانید برای فایل فعالیت یک کلمه عبور تعیین کنید. در صورت عدم تعیین کلمه عبور، هر کس می تواند این فایل را باز کند و با دسترسی به Activity Wizard پارامترهای آنرا تغییر دهد. این قسمت سبب می شود به طور انحصاری فقط مولف امکان تغییر یک فعالیت را داشته باشد.

آزمایش فعالیت (Test the Activity)



وقتی که شما برگه Test Activity را انتخاب کنید، می توانید به طور آزمایشی فعالیت ایجاد شده را اجرا کنید و آنرا از دیدگاه دانشجو مشاهده کنید. این کار به شما فرصت بررسی نهایی فعالیت را قبل از ذخیره کردن آن می دهد.

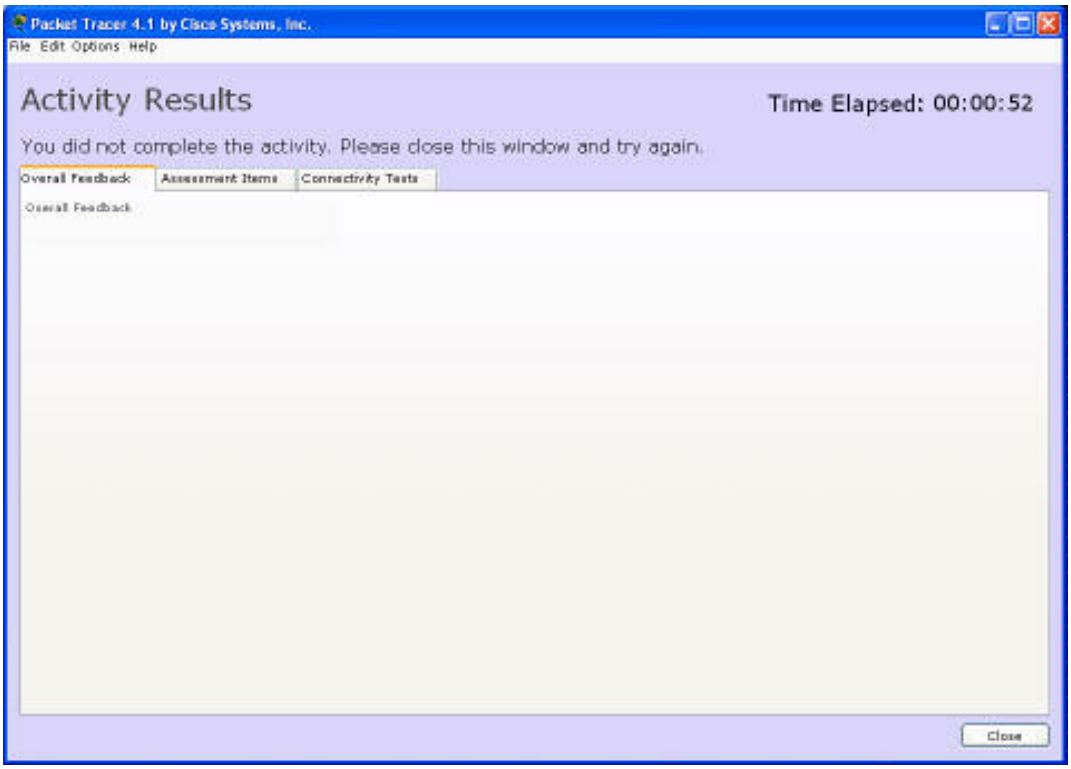
اجرای فایل فعالیت



شما می توانید با بازکردن یک فعالیت که قبلا به صورت pka ذخیره کرده اید، فعالیت را آغاز کنید. ابتدا پنجره توضیحات را مشاهده خواهید کرد که به شما نحوه تکمیل فعالیت را شرح می دهد. در این پنجره درصد پیشرفت فعالیت نمایش داده خواهد شد و هر ۳ ثانیه به روز رسانی می شود. با استفاده از دکمه Check Results می توانید پیشرفت فعالیت خود را مشاهده کنید. اگر همه تیک ها سبز باشد، فعالیت کاملا به پایان رسیده است. تیک سفید نشان دهنده ناتمام ماندن است و ضربدر قرمز نشان دهنده اشتباه بود جواب است. با استفاده از Reset Activity می توانید به تنظیمات اولیه برگردید و فعالیت را از ابتدا آغاز کنید.

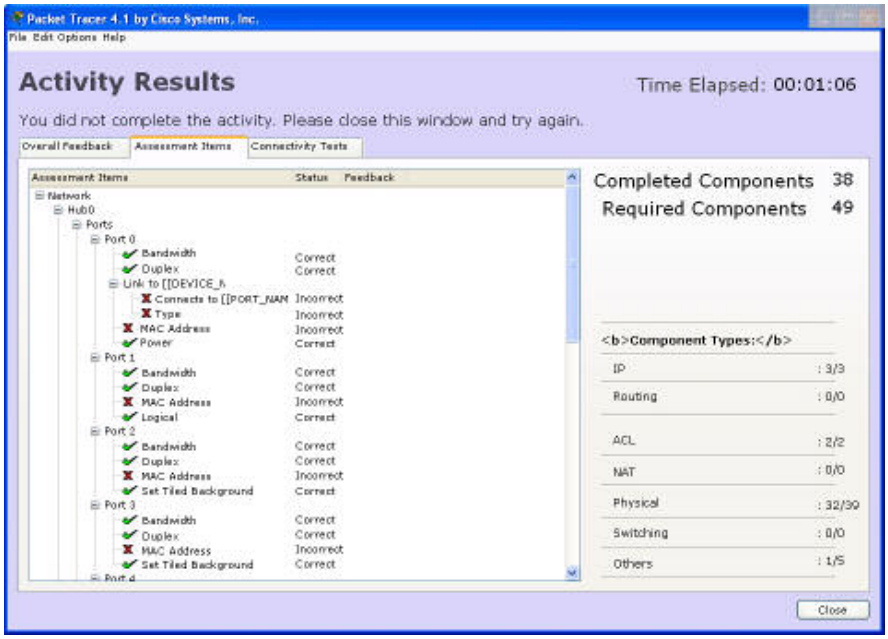
Overall Feedback

اگر فعالیت ۱۰۰ درصد تکمیل شده باشد، پیغام Completed Feedback نمایش داده خواهد شد. در غیر اینصورت پیغام Incomplete Feedback نمایش داده می شود.



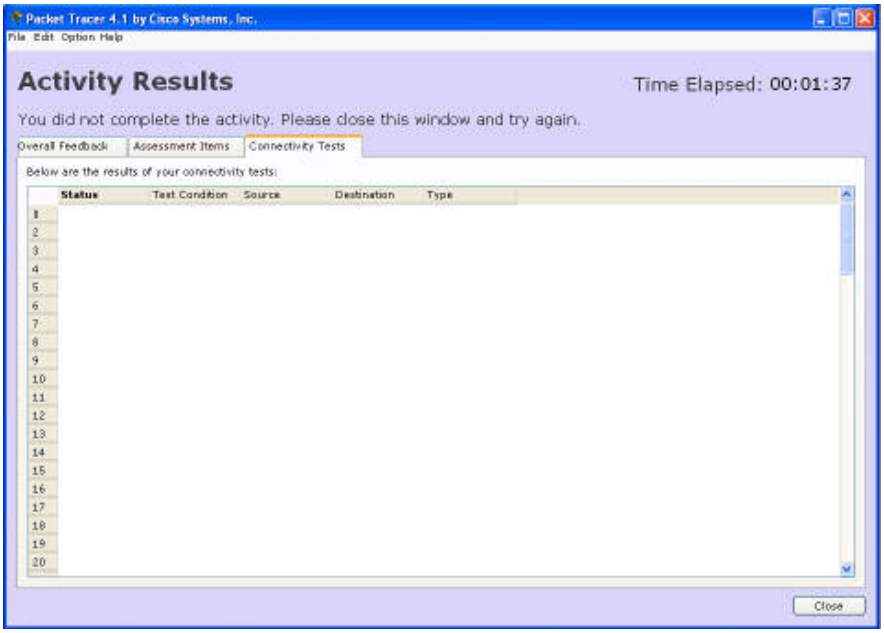
آیتم های ارزیابی

صفحه زیر نتایج آیتمهای ارزیابی را نمایش می دهد. برای هر آیتم یک پیغام نشان می دهد که پاسخ شما صحیح است یا غلط.



بررسی اتصال

صفحه زیر نتایج Connectivity Test است که با شرایط شبکه پاسخ مورد مقایسه قرار میگیرد.



بعنوان یک کاربر عادی می توان از دستور Save برای ذخیره کردن فعالیت جاری استفاده کرد و بعدا آن را تکمیل نمود. در چنین مواقعی بهتر است فایل را با نام جدیدی غیر از فعالیت اصلی ذخیره کنید. البته وقتی فایل را باز کنید خواهید توانست توسط Reset Activity فعالیت را از اول آغاز کنید.

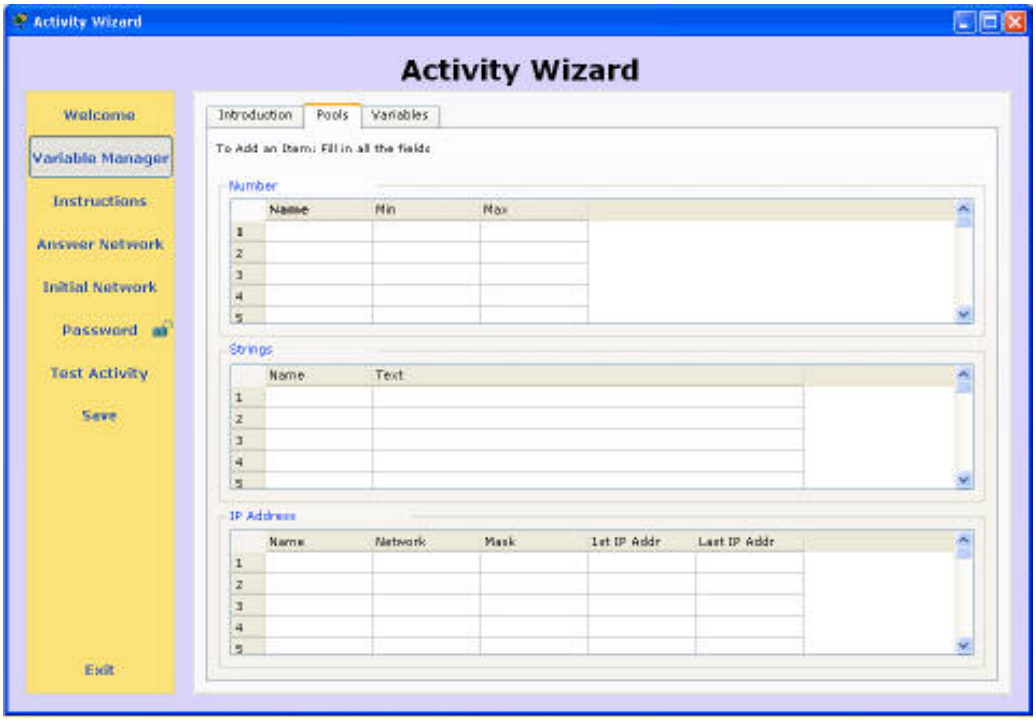
مدیریت متغییر ها (Variable Manager)



در پانل Variable Manager شما می توانید فعالیت های خود را پویا کنید. اعداد، رشته ها، آدرس های IP می توانند به متغییرها نسبت داده شده و بعدا به صورت تصادفی در هر بار اجرای فعالیت مورد استفاده قرار گیرند. برای فعال کردن Variable Manager گزینه **Show Variable Manager Interface را فعال کنید.**

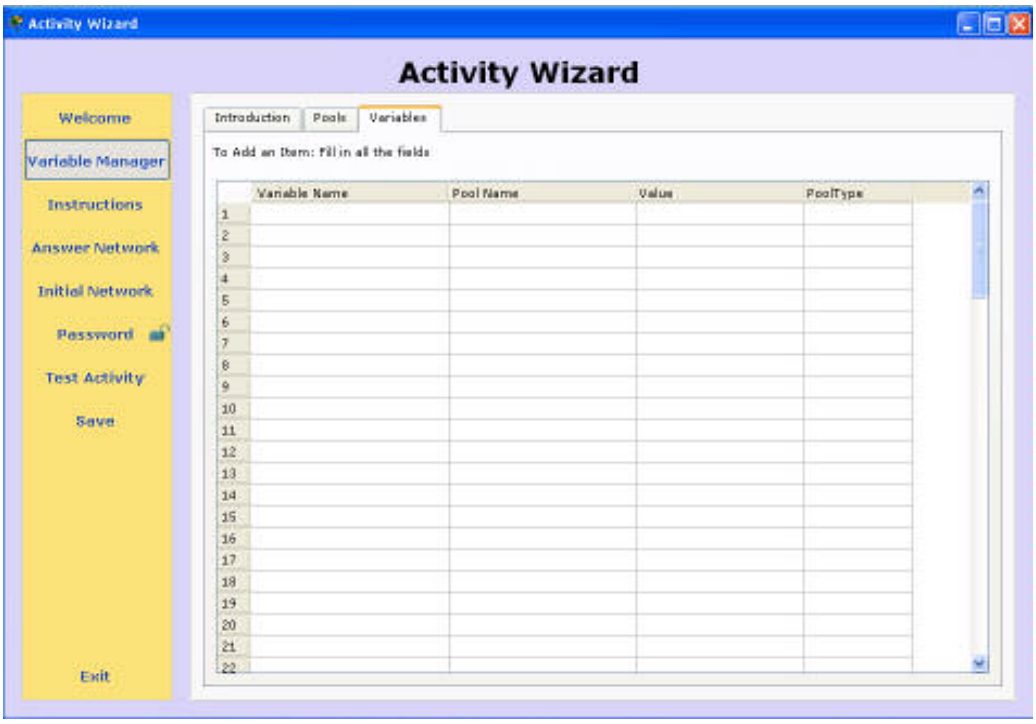
ایجاد استخر (Pool)

در برگه Pools می توانید تعدادی دسته های عددی، رشته ای و آدرس IP ایجاد کنید. برای نوع عددی می توانید بازه اعداد را مشخص کنید، رشته ها را می توانید توسط ; از هم جدا کنید.



ایجاد متغییرها

در برگه Variables می توانید متغییرهایی را تعیین کنید که مقدار خود را از دسته های تعریف شده در استخر فوق دریافت می کنند.



اختصاص متغییر ها

وقتی که show Variable Manager Interface فعال باشد، شما می توانید متغییرها را در متن های دستورالعمل، آیتم های ارزیابی و آیتم های اولیه مورد استفاده قرار دهید. در پانل Instruction مکان نما را در جایی که متغییر باید استفاده شود قرار دهید و روی Insert در Variable Manager Interface کلیک کنید. در مورد Assessments Items و Initial Items تنها موارد نشان داده شده با نقطه سبز رنگ می توانند از متغییرها استفاده کنند.

نحوه افزودن متغییرها به آیتم های ارزیابی

بیشتر پیکربندی های شبکه پاسخ آیتم های ارزیابی متناظری دارند. برای ارزیابی هر آیتم دلخواه، آیتم را فعال کنید. رفتار پیشفرض این است که پیکربندی های شبکه کاربر با آنچه در شبکه پاسخ قرار دارد مقایسه می شود. برای فعالیت های پیشرفته‌تر، آیتمهای ارزیابی می توانند با متغییر جایگزین شوند. در این حالت پیکربندی کاربر با متغییر تعریف شده مقایسه می شود. متغییرهای تنها می توانند با مقادیر پیکربندی شده جایگزین شوند. برای جایگزینی به یکی از دو روش زیر عمل کنید:

- با استفاده از واسط Variable Manager روی ← کلیک کنید.
- روی آیتم ارزیابی یک بار کلیک کنید. یک فیلد متنی ظاهر می شود. متن را با متغییر جایگزین کنید.

انواع آیتم های ارزیابی

آیتم های ارزیابی که می توانند با متغییرها جایگزین شوند انواعی دارند. مقدار متغییر باید متناسب با قوانین زیر تعریف شود:

Boolean: کمتر یا مساوی صفر false و بیشتر یا مساوی یک true است.

Enum: یک عدد مشخص کننده مقدار است (در جداول زیر این اعداد مشخص شده اند)

Number: یک عدد مبنای ۱۰

IP Addresses: باید دارای فرمت مقابل باشند 192.168.1.1

Mac Addresses: باید دارای فرمت ABCD.ABCD.ABCD باشند

Strings: هر رشته دلخواه

Special: رشته های خاصی که باید منطبق با فرمت نمایش داده شده در زیر باشد.

Cisco Device			
Name	**Variable**	**Type**	**Comment**
Host Name	y	String	
Startup Config			
Config-Register	y	Number	
Banner MOTD	y	String	
Enable Password	y	String	
Service Password Encryption	y	Boolean	
Clock Timezone	y	String	
VTY Lines			
Boot System Files			
<system file>	y	String	
Flash Files			
<flash file names>		String	

Cloud Device			
Name	**Variable**	**Type**	**Comment**
Frame-Relay Connections			
<Connection Node>	y	Special	<fromPortName> <sublink> : <toPortName> <sublink>
DSL Connections			
<DSL Connections>	y	Special	<fromPortName> : <toPortName>
Cable Connections			
<Cable Connections>	y	Special	<fromPortName> : <toPortName>

All Devices			
Name	**Variable**	**Type**	**Comment**
Power	y	Boolean	

PC			
Name	**Variable**	**Type**	**Comment**
Default Gateway	y	IP Address	

Routers			
Name	**Variable**	**Type**	**Comment**
User Names			
<User Name Password Pair>	y	Special	<username>-<password>

Switches			
Name	**Variable**	**Type**	**Comment**
VLANS		HEAD	
<VlanNumber>		Number	
<VlanName>		String	
VLAN Name			
Default Gateway	y	IP Address	

Terminal Line Devices			
Name	**Variable**	**Type**	**Comment**
Enable Secret	y	String	

Linksys			
Name	**Variable**	**Type**	**Comment**
Internet Connection	y	Enum	Dhcp = 0, 1=PPPoE, 2=Static
Router IP			
Ports			
Internet			
IP Address			
Subnet Mask			
LAN			
IP Address			
Subnet Mask			
Default Gateway	y	IP Address	
DNS Server IP			
Security Mode	y	Enum	0 = None, 1=WEP
Single Port Forwarding			
Password	y	String	
Remote Management	y	Boolean	

Cloud Pots Port			
Name	**Variable**	**Type**	**Comment**
Phone Number		Special	<areacode>-<prefix>-<number>

Cloud Serial Port			
Name	**Variable**	**Type**	**Comment**
Frame Relay LMI Type	y	Enum	0 = Ansi, 1= Cisco, 2 = Q933a
Sublinks <sublink name>	y	String	

Frame Relay Sub Interface Port			
Name	**Variable**	**Type**	**Comment**
Type (Point-to-Point/ MultiPoint)	y	Enum	0 = Multipoint, PointToPoint = 1

Port			
Name	**Variable**	**Type**	**Comment**
Power	y	Boolean	
Bandwidth	y	Boolean	
Duplex	y	Boolean	
MAC Address	y	Mac Address	
MAC Address	y	Mac Address	
Clock Rate	y	String	
Description	y	String	

Host Port			
Name	**Variable**	**Type**	**Comment**
IP Address	y	IP Address	
Subnet Mask	y	IP Address	

Router Port			
Name	**Variable**	**Type**	**Comment**
Access-group In	y		
Access-group Out	y		
CDP Enabled	y	Boolean	
NAT Mode	y	Enum	0 = None, 1 = NatInside, 2 = eNatOutside
Bandwidth Info	y	Number	
Delay	y	Number	
EIGRP Hello Interval			
RIP Split Horizon	y	Boolean	
EIGRP Summary Addresses			
Autonomous System		Number	
OSPF Authentication	y		
OSPF Authentication Key	y	String	
OSPF Cost	y	Number	
OSPF Dead-Interval	y	Number	
OSPF Hello-Interval	y	Number	
OSPF Message Digest Key			
Key ID [[ID]]	y	Number	
OSPF Priority	y	Number	
Keepalive	y	Boolean	
Encapsulation			
Keepalive	y	Boolean	
PPP			
Authentication	y	Enum	0 = No Authentication, 1 =Chap , 2 = Pap, 3 = PapChap, 4 = ChapPap
Frame Relay			
Encapsulation Type	y	Enum	0 = Cisco, 1 = IETF, 2 = Default
LMI Type	y	Enum	0 = Ansi, 1 =Cisco , 2 = Q933a
IP Maps			
802.1Q			
VLAN ID	y	Number	
Native VLAN			

Switch Port			
Name	**Variable**	**Type**	**Comment**
Port Mode	y	Boolean	
Access VLAN	y	Number	
Native VLAN	y	Number	
Trunk VLANs			
<name>	y	String	
Voice Vlan	y	Number	
Nonegotiate	y	Boolean	
Dynamic Mode	y	Enum	0 = Dynamic Desirable, 1 = Dynamic Auto, 2 = Operation Trunk, 3 = Operation Access

Terminal Line			
Name	**Variable**	**Type**	**Comment**
RS232			
VTY Line		Number	
Console Line			
Speed	y	Number	
Data Bits	y	Number	
Parity	y	Enum	0 = Even, 1 =Mark , 2 =None , 3 = Odd, 4 =Space
Stop Bits	y	String	
Flow Control	y	Enum	0 = None, 1 = Hardware, 2 =Software
History Size	y	Number	
MOTD Banner	y	Boolean	
Login	y	Enum	0 = No Login, 1 = Login, 3 = Login Local
Password	y	String	
Session Limit	y	Number	
Access Control In	y	String	
Access Control Out	y	String	

Routing			
Name	**Variable**	**Type**	**Comment**
Routes			
Static Routes			

<static route>	y	Special	<destinationPrefix>- <destionationPrefixBits>- <forwardRoutersIP>-0
Default Networks			
<default network>	y	IP Address	

RIP			
Name	**Variable**	**Type**	**Comment**
RIP			
Version	y	Number	
Auto Summary	y	Boolean	
Default Information Originate	y	Boolean	
Timers Basic			
Networks			
<network address>	y	IP Address	
Passive Interface		HEAD	
Default	y	Boolean	

EIGRP			
Name	**Variable**	**Type**	**Comment**
Autonomous System #		Number	
Auto Summary	y	Boolean	
Networks		Head	
<network address String>	y	Special	<networkNumber> <eigrpWildcardBits>
Passive Interface			
Default Metrics	y	Boolean	
Variance	y	Number	

OSPF			
Name	**Variable**	**Type**	**Comment**
Process ID		Number	
Area			

Authentication			
Area #	y	Number	
Default Information Originate	y	Enum	0 =No Default Info Originate , 1 = Default Info Originate, 2 = Default Info Originate Always
Log Adjacengy Changes	y	Enum	0 =No Log Change , 1 = Log Change, 2 = Log Change Detail
Passive Interface Default			
Networks			
<route String>	y	Special	<networkNumber> <OSPFWildcardMask> <areaIdNumber>

Port Security			
Name	**Variable**	**Type**	**Comment**
Static MAC			
<mac address>	y	Mac Address	
Type	y	Enum	0 = Shutdown, 1 =Protect , 2 =Restrict
Maximum Static MACs	y	Number	

CDP			
Name	**Variable**	**Type**	**Comment**
CDP Enabled		Boolean	

ACL			
Name	**Variable**	**Type**	**Comment**
<ACL Name>	y	String	

DHCP Pool			
Name	**Variable**	**Type**	**Comment**
Pool		String	
DNS server IP	y	IP Address	

DHCP Server			
Name	**Variable**	**Type**	**Comment**
DHCP Enable	y	Boolean	
Start IP Address	y	IP Address	
Max User	y	IP Address	
Default Gateway	y	IP Address	
DNS Server IP	y	IP Address	
Pools			
Excluded Addresses			
<addresses>	y	IP Address	

NAT			
Name	**Variable**	**Type**	**Comment**
NAT			
Pools			
<pool name>	y	String	
Inside Source List			
<list number>	y	Number	
Inside Source Static			
<static entry>	y	Special	<udp|tcp> <insideLocalIP> <portNumber> <InsideGlobalIp> <portNumber>

STP			
Name	**Variable**	**Type**	**Comment**
VLANs			
<Vlan Number>	y	Number	
Priority			

Wireless			
Name	**Variable**	**Type**	**Comment**
Wireless			
SSID			
Security Mode			
WEP Key			

HTTP Server			
Name	**Variable**	**Type**	**Comment**
HTTP Enable	y	Boolean	

VTP			
Name	**Variable**	**Type**	**Comment**
VTP			
Domain Name	y	String	
VTP Mode	y	Enum	0 =VtpServer , 1 =VtpClient , 2 = VtpTransparent
VTP Password	y	String	
VTP Version	y	Number	

TFTP			
Name	**Variable**	**Type**	**Comment**
TFTP Enable	y	Boolean	

DNS Client			
Name	**Variable**	**Type**	**Comment**
IP Domain-Lookup	y	Boolean	
IP Name Server	y	IP Address	
IP Host			
Host <ipaddress>	y	IP Address	

DNS Server			
Name	**Variable**	**Type**	**Comment**
DNS Enable	y	Boolean	

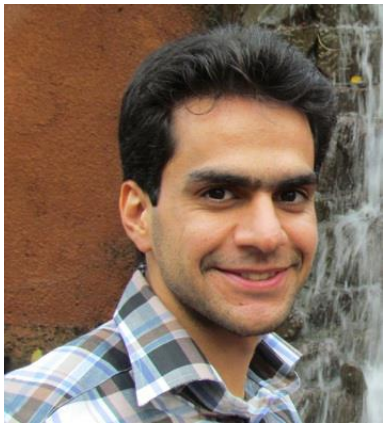
Domain Name			
<name>	y	String	

به پایان آمد این دفتر حکایت همچنان باقیست

امام صادق (علیه السلام) **فرمودند** :

مَن تَعَلَّمَ العِلمَ وَ عَمِلَ بِهِ وَ عَلَّمَ لِلّهِ دُعِیَ فی مَلَکوتِ السَّماواتِ عَظیما فَقیلَ: تَعَلَّمَ لِلّهِ وَ عَمِلَ لِلّهِ وَ عَلَّمَ لِلّهِ

هر کس برای خدا دانش بیاموزد و به آن عمل کند و به دیگران آموزش دهد، در ملکوت آسمان ها به بزرگی یاد شده و می گویند: **برای خدا آموخت و برای خدا عمل کرد و برای خدا آموزش داد.**



درباره مؤلف:

مهندس رضا رمضانی در سال ۱۳۸۵ با کسب رتبه ۱۷ کنکور کشوری و رتبه ۱ در استان اصفهان وارد دانشگاه شده و در سال ۱۳۸۷ موفق شدند رتبه ۴ کشوری در مسابقات علمی کامپیوتر را کسب کنند. همچنین ایشان در سال ۱۳۸۹ توانستند عنوان دانشجوی نخبه را کسب نمایند و سر انجام نیز در همین سال با کسب بالاترین معدل در چهار دوره گذشته دانشجویان رشته مهندسی کامپیوتر فارغ‌التحصیل شدند. ایشان بلافاصله در سال ۱۳۸۹ وارد مقطع کارشناسی ارشد دانشگاه صنعتی اصفهان شده و در سال ۱۳۹۰ (۲۰۱۱) به عنوان رهبر تیم ایران در مسابقات جهانی Max-Sat Evaluation USA 2011 شرکت نمودند. ایشان مجددا در سال ۱۳۹۱ به عنوان تنها نماینده ایران تحت عنوان IUT_RR_RV و IUT_RR_LS در مسابقات Max-Sat Evaluation 2012 کشور ایتالیا شرکت نموده و موفق به کسب مقام دوم شدند (سایت مسابقات جهانی: http://www.maxsat.udl.cat/12/results). ایشان در سال ۱۳۹۱ با کسب بالاترین معدل بین تمامی دانشجویان ارشد مهندسی کامپیوتر (نرم‌افزار، هوش‌مصنوعی و معماری کامپیوتر) از دانشگاه صنعتی اصفهان فارغ التحصیل شدند. از زمینه‌های کاری ایشان می‌توان Web & Windows Programming، Soft Computing، Parallel Processing، Web Mining، Semantic Web، Linked Data، Software Fault Tolerance، Dependable OS را نام برد. از جمله پروژه های انجامی ایشان نیز می توان به اتوماسیون سازمان صنایع و معادن استان اصفهان، سیستم پزشکی کل استان فارس و مدیریت آزمایشگاه های شرکت هواپیما سازی ایران (هسا)، کنترل Board Press صنایع گیتی پسند اشاره کرد. همچنین ایشان در سال ۱۳۹۰ به عضویت بنیاد ملی نخبگان نیروهای مسلح در آمده و در سال ۱۳۹۱ نیز جایزه بورسیه سالانه دانشگاه صنعتی اصفهان را دریافت نمودند. ایشان در حال حاضر به عنوان یکی از جوانترین دانشجویان دکتری کشور، در دانشگاه فردوسی مشهد مشغول به تحصیل می‌باشند.