شبکه هاي کامپيوتري

فـهـرست ۱

مقدمه

کتاب شبکه هاي کامپيوتري شامل دو بخش مفاهيم شبکه و سيستم عامل Windows 2003 Server است که توصيه ما به هنر آموزان محترم ، تدريس موازي اين دو بخش در کلاس است .

بديهي است که کارکردن با يک سيستم عامل شکبه اي مانند Windows 2003 Server بدون يادگيري مقدمات شبکه ميسر نخواهد بود ، بنابراين ممکن است هنرآموزان چند هفته اول به طور متوالی بخش مفاهيم شبکه را آموزش دهند . در اين مرحله توصيه می شود سيستم عامل Windows 2003 Server روی کامپيوتر ها نصب شده باشد و هنرجويان بدون اينکه با جنبه های فنی اين سيستم عامل در گير شوند دراين محيط يا سيستم عاملWindows XP مطالب را آموزش ديده و فعاليت های عملی را اجرا نمايند در برخی از فصل ها فعاليت عملی کمی ارايه شده و لازم است هنر آموزان متناسب با امکانات موجود فعاليت های عملی مرتبط با موضوع را طراحی و به هنر جويان ارايه نمايند.

در پايان از کليه عزيزاني که در تدوين اين کتاب ، ما را همراهي کرده اند ، سپاسگزاري مي کنيم .

مؤلفان

هدف کلي

آشنايی با مفاهيم شبکه های کامپيوتری و توانايی نصب شبکه و کار با سيستم عامل متداول شبکه

بخش اول مفاهیم شبکه

فصل اول- آشنايي با مفاهيم شبكه واجزاي آن

هدف هاي رفتاري

هنرجو پس از آموزش اين فصل مي تواند :

- هدف از ايجاد شبكه هاي كامپيوتري را بيان كند.
- اجزاي شبكه هاي كامپيوتري را شرح دهد.
- تقسيم بندي شبكه هاي كامپيوتري از نظر ابعاد و گستردگي فيزيكي راشرح دهد.
- تقسيم بندي شبكه هاي كامپيوتري از نظر مدل سرويس دهي را بيان كند

در دهه اخير شبكه هاي كامپيوتري به عنوان يكي از بسترهاي سريع و كم هزينه ارتباطي مطرح شده اند . اين سير تدريجي منجر به ايجاد روشي شده است كه با سازماندهي مناسب آن مي‌توان سريعتر از هر روش ديگري به اطلاعات مختلف دسترسي پيدا كرد . اطلاعاتي كه راه گشاي پيوندهاي گوناگون فرهنگي ، هنري ، خانوادگي و اجتماعي ، سياسي ، نظامي و همچنين مبادلات اقتصادي و تجاري اعم از خرد و كلان است و مي‌دانيم كه امروزه در عصر اطلاعات بسر مي‌بريم، هركه با هزينه كمتر و سرعت بيشتر بتواند به آن دسترسي پيدا كند موفق تر است .

تجارت جهاني روي اينترنت و شبكه هاي كامپيوتري به سرعت به عنوان مفاهيمی كارآمدمطرح می شود . فرقي نمي‌كند شما در كدام نقطه از كره زمين قرار داريد . در هر لحظه كه اراده كنيد مي‌توانيد اطلاعات مورد نياز خود را ، حتي بصورت صوت و تصوير زنده از شبكه بدست آوريد . اگر نياز به تبادل مالي داشته باشيد باز هم فرقي نمي‌كند ، پول الكترونيكي در دسترس شماست و به سرعت مي‌توانيد با كارت اعتباري خود اقدام به تبادل حفاظت شده ارزي نماييد .

موارد فوق را مي‌توان به صورت زير خلاصه كرد :

- دسترسي افراد به منابع متنوع در شبكه با در نظر گرفتن سطوح امنيتي قابل تعريف .(اشتراك منابع)
- برقراري سرويس هاي زنده صوتي تصويري بين افراد يا تيمهاي فعال در شبكه .
- تبادل نامه بين افراد مختلف .
- ايجاد بستري مناسب جهت ارتباط با اينترنت بمنظور دسترسي به شبكه جهاني اطلاعات .
- انجام كارهاي شخصي و اداري از هر نقطه در شبكه .
- مديريت و نظارت از راه دور .

۱-۱ – هدفهای برقراری شبکه کامپیوتری

هدف از ايجاد يك شبكه ی كامپيوتري عبارت است از:

- اشتراك منابع
- تبادل پيغام
- مديريت از راه دور

فعاليت عملي :

- اشتراك منابع : از طريق شبكه به كامپيوتر سرور متصل شده ، پوشه و چاپگر به اشتراك گذاشته شده را ببينيد . راهنمايي: ابتدا هنر آموز درس يك پوشه و يك چاپگر را در يكي از سيستم عاملهاي 2003 , XP , 2000 به اشتراك ميگذارد .
- تبادل پيغام : حداقل يكي از برنامه هاي زير را با تايپ نام برنامه در كادر گزينه Run براي انتقال پيغام آزمايش كنيد :
  - WinChat.exe
  - Net Meeting (conf.exe)
  - Command Prompt -> net send <computer_name> <message_text>

- مديريت از راه دور : به كمك هنر آموز درس ، يكي از برنامه هاي RA dmin , Ideal Administrator , DameWare يا Net Op School را اجرا كرده و با نظارت و كنترل از راه دور تحت شبكه را بررسي كنيد.

۱-۲ - اجزاي يك شبكة كامپيوتري :

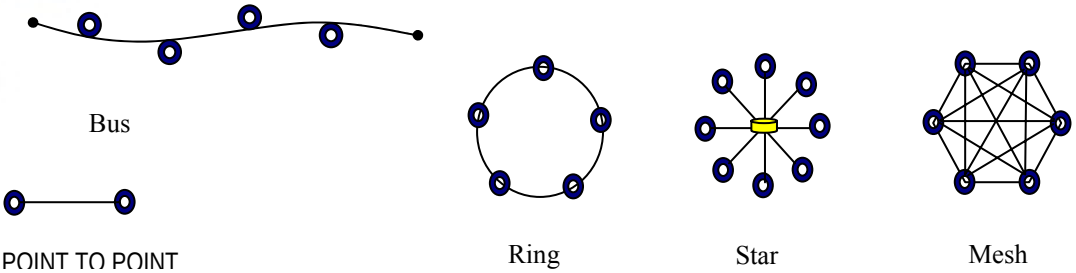
شبكة هاي كامپيوتري از ۴ جزء اصلي تشكيل مي شوند :

۱. Server : سرويس دهنده .
۲. Client : سرويس گيرنده .
} با نصب يك سختافزار ارتباطي مانند كارت شبكه يا مودم به شبكه متصل ميشوند.
۳. Communication Media : محيط انتقال (مثلاً كابل يا بي سيم)
۴. Protocol : مجموعة قوانيني كه با رعايت آنها سرويس دهي در شبكه برقرار ميشود .

بديهي است كه سرويس‌دهنده ها و سرويس‌گيرنده ها بايد طبق يك طرح و نقشة مشخص (بوسيلة محيط انتقال) به يكديگر متصل شوند كه به اين طرح و نقشه اصطلاحاً پيكربندی (Topology) شبكه گفته ميشود .

جزئيات هريك از موارد فوق بصورت خلاصه عبارتند از :

Servers (Services) : & Clients	File , Print , Application , Database , Fax , Email , Web , Communication , Time , Remote Access , Multimedia , . . .
Communication Media :	Wired : ▪ Metal : Coaxial , Twisted Pair ▪ Non Metal : Fiber Optic Wireless : ▪ Infra Red ▪ Laser ▪ Radio Waves
Protocols :	TCP/IP , IPX/SPX , NetBEUI , …
Topologies :	Bus , Ring , Star , Mesh , Point-to-Point



شكل ۱-۱

۳-۱- تقسيم بندي شبكه هاي كامپيوتري از نظر ابعاد و گستردگي فيزيكي : LAN , MAN, WAN

شبكه ها را از لحاظ اينكه فاصلة مابين اجزاي آنها چقدر بوده و اصطلاحاً چگونگي پراكندگي كامپيوترها به ۳ دستة كلي تقسيم مي‌كنند :

۱-۳-۱- شبكه هاي محلي ، Local Area Networks = LAN :

همانطور كه از اسم شبكه هاي محلي پيداست فاصلة اجزا در اين شبكه ها كم بوده و همه نزديك به يكديگر قرار دارند در زير چند مثال از اين شبكه ها ارايه شده است

- شبكه اي متشكل از ۲ كامپيوتر كه با يك قطعه كابل به فاصلة ۱۰۰ متر آنها را به يكديگر وصل كرده ايم .
- شبكة كامپيوتري يك ادارة كوچك واقع در يك ساختمان متشكل از ۲۰ كامپيوتر فعال (Active Node) .
- شبكة كامپيوتري يك سازمان واقع در ۵ ساختمان نزديك بهم با ۵۰۰ گره فعال (Active Node) .
- شبكة كامپيوتري يك برج ۱۱۰ طبقه با ۵۰۰۰ سيستم فعال (Active Node) .

۲-۳-۱- شبكه هاي گسترده ، Wide Area Networks = WAN :

فاصلة اجزا در اين شبكه ها نسبت به LAN طولاني‌تر است بطوريكه از نظر حسي ديگر نمي‌توان آنها را نزديك به يكديگر تصور كرد :
مثال ۱ : شبكه اي متشكل از ۲ كامپيوتر كه بوسيلة مودم از طريق خطوط مخابرات به يكديگر متصلند .
مثال ۲ : مجموع ۲ شبكة محلي كه هركدام واقع در ساختمان مختص به خود به فاصلة ۱۰ كيلومتر از يكديگر قرار دارند. يكي از ساختمانها واقع در مركز شهر و ديگري در حاشية غربي آن بوده و ارتباط آنها از طريق خطوط مخابرات يا روشهاي ديگري مانند بي‌سيم برقرار شده .
مثال ۳ : شبكة كامپيوتري شعبه هاي مختلف يك بانك در شهر.
مثال ۴ : شبكة كامپيوتري آموزش و پرورش واقع در تهران و شهرستانها .
مثال ۵ : شبكة اينترنت .

۳-۳-۱- شبكه هاي فرا منطقه اي ، Metropolitan Area Networks = MAN :

اين شبكه كه در ترجمه هاي فارسي به شبكه هاي شهري نيز معروفند از نظر وسعت مابين LAN و WAN قرار دارند .

مثال ۱ : برخي ترجيح مي‌دهند كه مثال ۳ از شبكه هاي WAN را MAN اطلاق كنند .

مثال ۲ : يك مجموعه بزرگ صنعتي يا نظامي واقع در محدودة ۳۰ كيلومتر مربعي كه از سوله هاي متفاوت تشكيل شده و در هر سوله يك LAN موجود است . به مجموع شبكه هاي اين كمپ نيز مي‌توان واژة MAN را اطلاق كرد . البته در اين مثال چندين شبكة LAN داريم كه در يك كمپ واقع شده اند لذا برخي (از جمله كمپاني معروف Cisco) ترجيح مي‌دهند از واژة Campus LAN يا Campus Area Networks = CAN استفاده كنند .

به هر حال به نظر مي‌رسد تقسيم بندي LAN و WAN كافيست .

شما و همسایة دیوار به دیوارتان و هرکدام یك دستگاه کامپیوتر دارید . از طریق یك کابل ، هر دو سیستم را به هم متصل میکنید ، در این حالت شبکه حاصلLAN است .

مثال دیگر- حال فرض کنید که امکان کابلکشي مستقیم ندارید. لذا پس از خرید و نصب مودم دوکامپیوتر مثال بالا را از طریق شبکة مخابرات به یکدیگر وصل میکنید شبکه حاصل WAN خواهد بود. در این مثال ها نشان داده شد که نوع شبکه را طول کابلها (محیط انتقال) تعیین مي کند نه فاصلة ظاهري بین کامپیوترها .

مقایسه شبکه های LAN و WAN

از نظر سرعت در شبکه‌هاي LAN و WAN مي توان گفت: سرعت به ابعاد و گستردگي شبکه بستگي ندارد اما معمولاً پیاده‌سازي تکنولوژي با سرعت بالا در ابعاد LAN کم هزینه‌تر و ساده‌تر از WAN انجام میشود لذا معمولاً سرعت در شبکه‌هاي LAN از WAN بیشتر است اما این یك قاعدة کلي نیست .به عنوان مثال مي توان شرایط زیر را در نظر گرفت:

- سرعت LAN بیشتر از WAN : وقتي با مودم به اینترنت متصل میشوید بعنوان یکي از اعضاي شبکة WAN محسوب شده و سرعت با مودم هاي خوب حدوداً 40 Kbps است . از طرفي کمترین سرعت در شبکه‌هاي LAN که البته در اواخر عمر خود قرار دارند 10 Mbps است . اگر سرعت LAN را بر WAN تقسیم کنیم میبینیم که حدوداً ۲۵۰ برابر بیشتر است !

- سرعت LAN کمتر از WAN : در شاهرگهاي اصلي اینترنت یا در ارتباطات میان‌قاره‌اي سرعت عموماً بیشتر از 155 Mbps است و اگر آنرا با سرعت معمول در شبکه‌هاي LAN یعني 100 Mbps مقایسه کنیم میبینیم که در همان حد یا بیشتر است .

انواع شبکه های بي سیم از نظر وسعت

WLANS[1]:شبکه WLANS ، امکان دستیابی کاربران ساکن در یک منطقه محدود نظیر محوطه یک دانشگاه و یا کتابخانه را به شبکه و یا اینترنت ، فراهم می نماید .

WPANS[2]: .با استفاده از شبکه WPANS ، امکان ارتباط بین دستگاههای شخصی در یک ناحیه محدود فراهم می شود . در این نوع شبکه ها از دو تکنولوژی متداول IR (Infra Red) و Bluetooth (IEEE 802.15) استفاده می شود .

WMANS[3]: . در این شبکه ها ، امکان ارتباط بین چندین شبکه موجود در یک شهر بزرگ فراهم خواهد شد . واین اغلب به عنوان شبکه های پشتیبان شبکه کابلی استفاده می شود .

WWANS[4]: . در شبکه های فوق ، ارتباط بین شهرها و یا حتی کشورها از طریق سیستم های ماهواره ای متفاوت فراهم می شود . این شبکه به سیستم های G۲ (نسل دوم) معروف هستند .

۴-۱- تقسیم بندي شبکه‌هاي کامپیوتري از نظر مدل سرویس دهي (Peer-to-Peer , Server-Based)

مفهوم Server و Client : سرویس دهي در یك شبکه به وسیله ی سیستمهایي صورت میگیرد که در اصطلاح سرویس دهنده (Server) نامیده میشوند . سیستمهایي

---

[1] –Wireless Local Area Networks
[2] –Wireless Personal Area Networks
[3] –Wireless Metropolitan Area Networks
[4] –Wireless Wide Area Networks

که از این سرویسها استفاده کنندر اصطلاح سرویس گیرنده (Client)نامیده میشوند برای سرویس گیرنده ها اصطلاح workstation نیز به کار می رود.

۱-۴-۱- شبکه Server-Based :

اگر در یك شبکه تعدادي از سیستمها فقط در نقش سرویس دهنده و تعدادي فقط در نقش سرویس گیرنده ظاهر شوند در آن صورت میگوییم مدل سرویس دهي آن شبکه Server-Based (به اختصار SB) است.

۱-۴-۲- شبکه Peer-to-Peer :

اگر در شبکه‌اي ، سیستمها همزمان علاوه بر ارایة سرویس ، از سرویسهاي بقیه هم استفاده کنند یا بعبارتي بطور همزمان هم سرویس دهنده باشند هم سرویس گیرنده در آن صورت میگوییم مدل سرویس دهي در آن شبکه Peer-to-Peer است (به اختصار PtP)

در مدل SB تجمع سرویسها روي سرویس دهندهs بوده و Clients هیچگونه سرویسي ارایه نمیدهند اما در مدل PtP هر سیستم میتواند علاوه بر دریافت سرویس خود سرویس دهنده نیز باشد یعني هر کامپیوتر هم سرویس گیرنده و هم سرویس دهنده است.

در یك سایت تعدادي از سیستمها فقط سرویس دهنده و بقیه فقط سرویس گیرنده هستند . مدل سرویس دهي SB است اما در یك سایت دیگر هرکدام از کاربران منابعي مانند پوشه ها یا چاپگرها را براي بقیه به اشتراك گذاشته‌اند . مدل سرویس دهي PtP است .
فرض کنید در ایرانشهر تعدادي مغازه و مراکز خدماتي وجود دارد و تعدادی مشتري و استفاده کنندة این خدمات هستند . مدل سرویس دهي آنها SB خواهد بود.

۱-۴-۳- مزایا و معایب هریك از مدلهاي SB , PtP

در مدل SB چون تمرکز سرویسها فقط در نقاط مشخصي است یعني سرویس دهنده ها بنابراین مدیریت سرویس سادهتر است . این مدیریت شامل کنترل دسترسي و امنیت ، نحوة ارایه ی سرویس به کاربران ، مونیتورینگ سرویس و چگونگي بهرهبرداري از آن و پارامترهاي دیگریست که براحتي میتوان آنها را در سرورها کنترل کرد در صورتیکه انجام این عملیات در مدل PtP پیچیده است ، چرا ؟ بعنوان مثال تصور کنید در یك شبکه حدود ۷۰۰ سیستم داشته باشیم که مدل سرویس دهي آنها PtP باشد ، یعني باید روي ۷۰۰ سیستم عملیات هاي فوق را انجام دهیم ! که عملي هزینهبر و کسلکننده است.

مدل Server Based :

مزیت : مدیریت جامع و متمرکز . مناسب براي استفاده در شبکه‌هاي متوسط و بزرگ .

عیب : چنانچه سرویس دهنده دچار مشکل شوند چه اتفاقي میافتد ؟ سرویس دهي در کل شبکه دچار اختلال میشود . راه حل این عیب را بعداً در مبحث Fault-Tolerance اشاره خواهیم کرد .

مدل Peer-to-Peer :

مزیت : چون مجموعة سرویسها در نقطة خاصي متمرکز نشده‌اند بلکه احتمالاً در نقاط مختلفي از شبکه پراکنده هستند بنابراین در صورت بروز مشکل ، سرویس دهي به صورت ناگهانی دچار اختلال کلي نمیشود .

عیب : مدیریت آن پیچیده بوده و هنگامي عملي است که تعداد سیستمها زیاد نبوده (شبکه‌هاي کوچك) یا اینکه کاربران در مورد نحوة اشتراك گذاري منابع و مدیریت سرویسها آموزشهاي لازم را دیده باشند .

۵-۱- انواع سرویسها یي که سرور ارایه مي دهد

همانطور که اشاره شد ، هر شبکة کامپیوتري از ۴ جزء تشکیل شده که به‌ترتیب از سمت چپ عبارتند از :

Client , Server , Communication Media & Protocol . مجدداً یادآوري مي‌کنیم که سرویس دهي در یك شبکه به وسیله ی سیستمهایي صورت مي‌گیرد که در اصطلاح " سرویس دهنده" نامیده مي‌شوند سیستمهایي که از این سرویسها استفاده کنند اصطلاحاُ سرویس گیرنده نامیده مي‌شوند . معمولاً در یك شبکه هر کامپیوتري که از نظر سخت افزاري نسبت به سایر کامپیوتر ها قوي تر باشد به عنوان سرویس دهنده در نظر گرفته مي شود، البته نوع انتخاب بستگي کامل به نوع سرویس خواهد داشت .

در این قسمت مي‌خواهیم با انواع سرویسها آشنایي بیشتري پیدا کنیم . بدیهي‌است با شناخت سرویسها مشتري آنها یعني Clients نیز شناخته خواهد شد .

سرویسهایي که در شبکه‌ها ارایه مي‌شوند ممکن است بسیار متنوع باشند هرچه تنوع مشتري و نیازهاي او بیشتر باشد تنوع سرویس نیز به همان نسبت افزایش مي‌یابد . آشنایي با همة سرویسها نیاز به بحث طولاني خواهد داشت با این حال معروفترین آنها را نام برده و چهار مورد را که کاربرد بیشتري دارند معرفي مي‌کنیم :

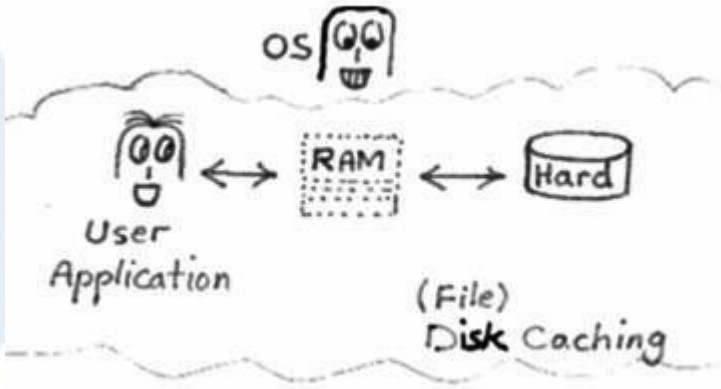
File , Print , Application , Database , Web , Mail , Fax , Modem (Communication) , Remote Access , Internet Sharing , Multimedia , CDROM (DVDROM) , . . .

۵-۱-۱ File Service

بطور مختصر و ساده File Server یعني " سریس دهنده فایل " . سخت‌افزاري است با وسایل ذخیره‌سازي حجیم ، سریع و پایدار (مانند دیسك سخت) که روي آن انواع پرونده‌ها با درنظر گرفتن سطوح امنیتي ، به وسیله ی کاربران از نقاط مختلف شبکه ذخیره و مورد استفاده قرار مي‌گیرد . البته سخت‌افزار به تنهایي کافي نبوده و باید نرم‌افزار خاص File Service نحوة ذخیره‌سازي ، بازیابي و مدیریت اینگونه کارها را به نحو احسن در شبکه انجام دهد .
براي ذخیره و بازیابي اطلاعات هرچند دیسك سخت[1] وسیله‌اي نسبتاً سریع براي ذخیره‌سازي و بازیابي اطلاعات است اما یك وسیله الکترو مکانیکي بوده و سرعت این وسایل هرچه‌قدر هم زیاد باشد ، نسبت به وسایل ذخیره‌سازي الکترونیکي محض مانند RAM بسیار ناچیز است لذا در اینگونه سرورها از حافظة RAM براي ذخیره‌سازي و بازیابي موقت اطلاعات کاربران تا هنگامي که سرور روشن است استفاده مي‌شود . بعبارتي کاربر یا برنامه‌اي که با فایل ذخیره شده روي دیسك سخت کار دارد بجاي در گیر شدن با یك وسیلة مکانیکي ، عملیات خود را بطور نامحسوس روي RAM انجام مي‌دهد و لذا سرعت به نحو چشمگیري افزایش مي‌یابد . بدیهي است سیستم عامل (یا نرم‌افزار فایل سرور) در زمانهاي مناسب بطور خودکار تغییرات انجام شده در RAM را ، روي دیسك سخت منتقل مي‌کند چرا که محل اصلي و پایدار براي ذخیره سازي اطلاعات است .
استفاده از RAM را براي ذخیره سازي موقت اطلاعات دیسك سخت که بمنظور افزایش سرعت انجام مي‌شود اصطلاحاً File Caching یا Disk Caching مي‌گویند .

---

[1] - معمولاً در سرور ها براي نگهداري اطلاعات زیاد در حد ترا بایت از دستگاهي به نام (NAS Server (network Attached Storage Server استفاده مي شود



شكل ۲-۱

برخي از فايل-سرورها عمليات تكميلي ديگري را نيز انجام مي‌دهند مانند :

- فشرده سازي خودكار اطلاعات هنگام ذخيره سازي پرونده ها روي ديسك بمنظور كاهش حجم فضاي اشغالي .
- رمزنگاري اطلاعات براي هركاربر با كليد رمز جداگانه بمنظور حفظ اطلاعات شخصي و محرمانه .

اين عمليات تكميلي هرچه كه باشند باري اضافه بر دوش پردازندة سرور محسوب مي‌شوند و اگر CPU قوي نباشد عمليات به كندي صورت گرفته ، شبكه را با پاسخهاي توام با تاخير مواجه مي‌كند .

ويژگي هاي يك File Server از نظر سخت‌افزاري :

- وسايل ذخيره‌سازي حجيم ، سريع و پايدار كه در حال حاضر معمولاً از ديسك سخت استفاده مي‌شود .
- حافظة RAM به ميزان كافي براي انجام عمليات File Caching .
- پردازندة سريع (CPU) براي آن دسته از سرورهايي كه عمليات تكميلي مانند فشرده سازي يا رمز نگاري را انجام مي‌دهند . البته بطور كلي وجود يك پردازندة سريع در سرور مخصوصاً آنهايي كه سيستم عامل گرافيكي دارند مانند Windows لازم است اما نقش آن به اندازه موارد اول و دوم در اولويت قرار ندارد .

نكته :

در مجموع براي تمامي سرورها بايد دقت داشته باشيم كه قدرت سخت‌افزاري سرور ، نقطة ارتباط سرور با شبكه (مانند كارت شبكه) ، بستر سخت‌افزاري شبكه و سرعت آن براي ارايه ی يك سرويس سريع و مطمئن بسيار تعيين كننده است و اين موضوع بعداً مورد بحث بيشتري قرار مي‌گيرد .

اگر در يك File Server حين انجام كار برق بطور ناگهاني قطع شده يا سرور بطور غيرعادي خاموش يا Reset شود برخي از تغييرات كه در حافظة RAM انجام شده و هنوز به وسيله ی OS به ديسك سخت منتقل نشده اند از بين مي‌رود بعبارت فني عمليات File Caching ناقص مي‌ماند لذا بسيار مهم است كه سرورها اولاً به UPS متصل بوده ، ثانياً هيچگاه آنها را بطور غيرعادي خاموش يا Reset نكنيم بلكه بايد طور معمولي خاموش شوند .

فرايند خاموش شدن معمولي (Shutdown) عبارت است از بسته شدن كلية پرونده هاي مورد استفاده ، انتقال اطلاعات تغييريافته از RAM به ديسك سخت. همانطور كه شما پس از پايان ساعات كار ، محل كار خود را مرتب مي‌كنيد ، سيستم عامل هم بايد اطلاعات را جمع و جور و مرتب كند . هرگونه

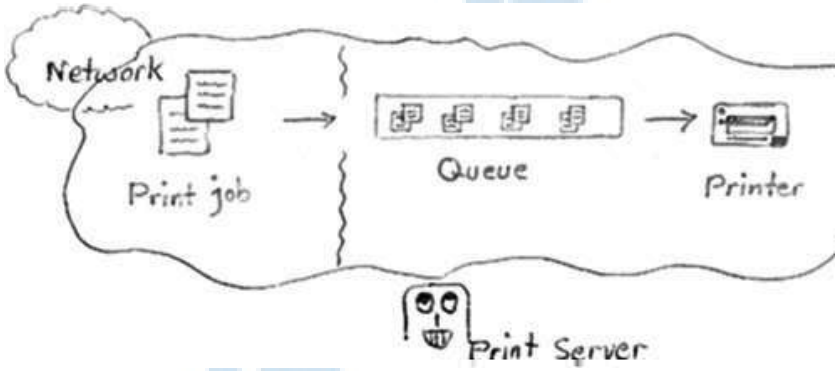
راه اندازي غيرعادي (مانند فشردن كليد روي Case) به منزلة رها كردن محل كار با يك ميز نامرتب و بهم ريخته است.

فعاليت عملي : آشنايي با File Server در Microsoft :

يك پوشه حاوي چندين فايل متنوع را به كمك هنر آموز درس در سيستم عامل XP , 2000 يا 2003 به اشتراك گذاشته و از طريق شبكه به آن دسترسي پيدا كنيد . در اين بخش نيازي به درگيرشدن در جزئيات Security و غيره نيست و هدف تثبيت مفهوم در ذهن هنرجوست . در اين صورت هر كامپيوتري كه پوشه خود را براي استفادة ديگران به اشتراك مي‌گذارد در عمل تبديل به يك File Server شده حتي اگر سيستم عامل آن به ظاهر سرور نباشد (مثلاً XP_Professional يا 2000_Professional باشد)

۲-۱-۵- Print Service

اين سرويس كه معمولاًبه وسيله ی Print Server ارائه مي‌شود سخت افزاری است (همراه با نرم افزار)كه تعدادي چاپگر متناسب با نيازهاي كاربران تحت كنترل آن قرار دارد . كارهاي چاپي (Print Jobs) كه در نقاط مختلف شبكه به به وسيله ی كاربران ارسال مي‌شود به وسيله ی اين سرور دريافت شده و ابتدا در يك صف (Queue) قرار مي‌گيرد سپس كار چاپي از صف تحويل چاپگر مربوطه مي‌شود . چاپگرها ممكن است از نظر فيزيكي مستقيماً به سرور متصل بوده يا غيرمستقيم از طريق سيستمهاي ديگر تحت مديريت سرور باشند ، مهم آنست كه چاپگرها تحت كنترل Print_Server اداره مي‌شوند .



شكل ۳-۱

در سرورهاي چاپ حرفه اي كه كارهاي چاپي ممكن است حجيم و از نظر تعداد زياد باشند ، محل فيزيكي ذخيره‌سازي اطلاعات صف (Queue) روي ديسك سخت است لذا براي يك سرور چاپ حرفه اي آنچه كه در درجة اول ويژگي سخت‌افزاري قرار دارد وجود فضاي كافي روي يك ديسك سخت خوب و مطمئن است . RAM و CPU در درجة دوم و سوم اهميت قرار مي‌گيرند .

در مورد سرعت يك Print Server بايد توجه داشت كه سرعت چاپ بستگي شديد به سرعت فيزيكي چاپ روي كاغذ دارد بعبارتي سرورهاي چاپ حتي ضعيفترين آنها داراي توانايي نسبتاً سريع دريافت تمامي كار چاپي و قراردادن آنها را در صف دارا هستند و آنچه كه تعيين كنندة اصلي سرعت است خصوصيت چاپگر است ، بنابراين :

ويژگي هاي يك Print Server از نظر سخت‌افزاري

- ديسك سخت با ظرفيت مناسب و مطمئن براي ذخيره‌سازي اطلاعات صف (Queue) .
- حافظة RAM كافي براي انجام عمليات احتمالي Caching (به اندازة File_Server اهميت ندارد مگر آنكه Print_Server صف را مستقيماً در RAM ذخيره كند)
- پردازندة سريع (CPU) براي انجام عمليات تبديل فرمتهاي چاپي خاص (Rendering) قبل از ارسال به چاپگرهاي خاص . (در خيلي از موارد نيازي

نيست چرا كه عمليات Rendering معمولاً در ايستگاه ها توسط ارسال كننده Print_Job صورت مي‌گيرد)

فعاليت عملي : آشنايي با Print Server در Microsoft :

ابتدا يك چاپگر را به كمك هنر آموز درس در سيستم عامل XP , 2000 يا 2003 تعريف كرده سپس به اشتراك گذاشته و از طريق شبكه به آن دسترسي پيدا كنيد . در اين بخش نيازي به درگيرشدن در جزئيات تنظيمات چاپگر ، Security و غيره نيست و هدف تثبيت مفهوم در ذهن هنرجوست . در اين حالت هر كامپيوتري كه چاپگر خود را براي استفادة ديگران به اشتراك مي‌گذارد در عمل تبديل به يك Print Server شده حتي اگر سيستم عامل آن به ظاهر سرور نباشد (مثلاً XP_Professional يا 2000_Professional باشد)

۳-۵-۱- Application Service

اين سرويس معمولاً به وسيله ی Application Server ارائه مي‌شود. فرض كنيد كه در شبكة سايت هنرستان متشكل از كامپيوترهاي Windows قرار داريد . آيكن مربوط به Network_Neighborhood يا My_Network_Places را باز كرده ، ليستي از كامپيوترهاي موجود در شبكه را مي‌بينيد . يكي از اين كامپيوترها بنام «كامپيوتر هنر آموز » است . كنجكاو شده و روي آيكن مربوط به آن Double-Click مي‌كنيد . كامپيوتر باز شده و مثلاً يك پوشه را روي آن مي‌بينيد كه به اشتراك گذاشته شده ، بعبارتي كامپيوتر هنر آموز يك File-Server است . پوشه Share شده را باز كرده و داخل آن چندين فايل متنوع با پسوندهاي bmp. و txt . يكي از فايل ها را انتخاب كرده و روي آيكن مربوطه Double-Click كنيد ، مي‌بينيم كه فايل باز مي‌شود . سوال اينست كه فايل مذكور كجا اجرا مي‌شود ؟ روي كامپيوتر هنر آموز يا روي كامپيوتر شما (كه مثلاً نام آن PC1 است) ؟

با كمي دقت پاسخ خواهيد داد كه روي PC1 . درست است چرا كه كامپيوتر هنر آموز فقط يك File Server است و نه يك Application Server . قرار نيست كه كامپيوتر هنر آموز براي ما فايل ها را باز كند يا برنامه ها را اجرا كند (مگر زماني كه كسي مستقيماً و نه از طريق شبكه روي خود كامپيوتر هنر آموز اقدام به اجراي برنامه كند) . كامپيوتر هنر آموز تنها محل نگهداري فايل مذكور است . وقتي كسي از طريق كامپيوتر خود (مثلاً PC1) و بواسطة شبكه روي آيكن فايلي كه روي كامپيوتر هنر آموز قرار داشته و به اشتراك گذاشته شده Double-Click مي‌كند ، اين فايل يا برنامه و بعبارتي Application از كامپيوتر هنر آموز به PC1 منتقل شده و روي پردازنده ، حافظه و خلاصه كامپيوتر ايستگاه PC1 اجرا مي‌شود .

حال اگر بخواهيم فايل روي كامپيوتر هنر آموز اجرا شده و PC1 كه به هر دليلي امكان اجراي آن برنامه را ندارد از آن استفاده ببرد چه بايد كرد ؟ پاسخ در استفاده از Application Server است .

تعريف : Application Server كامپيوتريست كه نرم افزارهاي كاربردي (Applications) را به درخواست كاربران براي آنها اجرا كرده و نتايج حاصل از اجرا را روي كامپيوتر خودشان نمايش مي‌دهد . هستة مركزي اجراي Application روي سرويس دهنده است و نه سرويس گيرنده . در اينجا سرويس گيرنده تنها بعنوان يك درخواست كننده براي اجرا عمل كرده و بقيه بعهدة سرويس دهنده است . اينكه چند درصد كار به وسيله ی سرور انجام مي‌شود و چند درصد به وسيله ی ايستگاه ، متغير بوده و بستگي به ماهيت Application و عملكرد سرويس دهنده دارد . گاهي اوقات ممكن است همة Application روي سرويس دهنده اجرا شده و ايستگاه فقط نتايج را استفاده كند و گاهي ممكن است بخش كوچكي از اجراي Application بعهدة سرويس گيرنده بوده و بقيه بعهدة سرور باشد .به عنوان مثال در برخي از Game Netها بازي ها در سرور نصب مي شود و بقيه

كامپيوتر ها كه به عنوان سرويس گيرنده هستند از برنامه استفاده مي كنند.

برخي از دلايل استفاده از App Server :

- امكانات سخت‌افزاري سرويس گيرنده ممكن است براي اجراي مستقيم برنامه كافي نباشد .مانند ATM (عابر بانك)
- چون برنامه عمدتاً بطور متمركز روي يك نقطه يعني سرويس دهنده اجرا مي‌شود بنابراين مديريت قويتري را مي‌توان روي آن اعمال كرد .
- در نرم افزارهاي تحت شبكه اي كه برنامه تك‌تك روي ايستگاه ها ي مختلف بطور كامل اجرا شده اما اطلاعات آنها در يك نقطة متمركز (مانند File Server) قرار دارد و از طرفي حجم تبادل اطلاعات مابين برنامة اجرايي روي ايستگاه ها و File Server زياد باشد باعث مي‌شود تا ترافيك شبكه بسرعت افزايش پيدا كرده و ضمن اشباع ترافيكي ، مشكلات امنيتي را نيز در پي داشته باشد لذا در اينگونه موارد بهتر است كه برنامه بجاي اجراي تك‌تك روي همة ايستگاه ها فقط روي App Server اجرا شده تا از پراكندگي تبادل اطلاعات مابين ايستگاه ها ي مختلف و File Server جلوگيري بعمل آمده و ترافيك تنها مابين Application Server و File Server باشد . درضمن كنترل اطلاعات نيز قويتر صورت مي‌گيرد . در اينگونه موارد معمولاً App Server و File Server از نظر فيزيكي روي يك كامپيوتر قرار مي‌گيرند . مثالي عملي از كاربرد اخير سرورهايي هستند تحت عنوان Database Server كه موضوع بحث بعديست .

ويژگيهاي يك Application Server از نظر سخت‌افزاري

- پردازندة قدرتمند ، چرا كه ممكن است تعداد زياد و متنوعي از نرم افزارها را بخواهد براي كاربران اجرا كند . حتي ممكن است نياز به كامپيوتر هاي چند پردازنده (Multi Processor) باشد .
- حافظة RAM زياد چرا كه برنامه‌ها هنگام اجرا همگي در RAM قرار مي‌گيرند .
- ديسك سخت و ساير منابع ديگر بسته به نياز و تنوع برنامه‌ها .

فعاليت عملي : آشنايي با Application Server در Microsoft :

ابتدا (روي كامپيوتري كه بعنوان سرويس دهنده در نظر گرفته ايد) سرويس Remote Desktop Server را به كمك هنر آموز درس در سيستم عامل 2003 Server فعال كرده (در 2000 Server بنام Terminal Server) سپس روي ايستگاه برنامة Remote Desktop Client را واقع در Programs->Accessories->Communications اجرا كنيد سپس به سرور متصل شده ، با نام Administrator وارد شده و Desktop مربوط به سرور را در اختيار بگيريد . چون اين Desktop مربوط به سرور است و نه ايستگاه لذا هر برنامه اي كه اجرا مي‌كنيد (مانند ماشين حساب) در واقع روي سرور اجرا مي‌شود . به كمك Task Manager نشان دهيد كه ماشين حساب در سرور اجرا شده نه در ايستگاه . در اين حالت هر كامپيوتري كه Desktop خود را براي استفادة ديگران در اختيار آنها مي‌گذارد در عمل تبديل به يك Application Server شده حتي اگر سيستم عامل آن به ظاهر سرور نباشد (مثلاً XP Professional) . با توجه به محدوديت سرويس Remote Desktop Server كه در حالت خاص خود فقط اجازة اتصال همزمان ۲ ايستگاه را مي‌دهد لذا بهتر است اين تمرين در گروههايي مركب از ۳ كامپيوتر انجام شود كه يكي از آنها داراي سيستم عامل 2003 بوده ، سرويس Remote Desktop را روي آن فعال شده و بعنوان سرور عمل مي‌كند . ۲ كامپيوتر ديگر نيز بعنوان سرويس گيرنده با هر سيستم عامل دلخواهي از مجموعة Microsoft مي‌توانند باشند حتي 98 . فقط بايد نرم افزار Remote Desktop Client روي آنها نصب باشد.

۴-۵-۱- آشنايي با Database Service كه معمولاً به وسيله ی Database Server ارايه مي‌شود :

فرض كنيد كه هنگام ثبت نام است و طي ۳ روز ۱۰۰۰ هنرجوي جديد مي‌خواهند نام خود را در دوره‌هاي آموزشي مورد پذيرش ثبت كنند . براي جلوگيري از ازدحام ، ۳ نفر از پرسنل موسسه را همزمان بعنوان مسوول درنظر گرفته و به هركدام يك كامپيوتر مجهز به نرم‌افزار ثبت‌نام را تحويل مي‌دهيم . با توجه به اينكه هر ۳ نفر بايد روي يك بانك اطلاعاتي مشترك كار كنند لذا يك شبكهٔ ساده متشكل از ۳ كامپيوتر مذكور برپا كرده و ضمناً يك FileServer براي ذخيره سازي بانك اطلاعاتي در نظر مي‌گيريم يعني در مجموع ۴ كامپيوتر . هر كدام از افراد ، نرم‌افزار ثبت‌نام را جداگانه روي ماشين خود اجرا كرده ، از طريق شبكه به بانك مربوطه كه مشترك بوده و روي FileServer ذخيره شده دسترسي پيدا كرده و عمليات ثبت ، گزارشگيري و . . . را انجام مي‌دهند . در پايان كار ثبت‌نام ، مدير موسسه گزارشاتي را مبني بر تنوع رشته‌هاي نام‌نويسي شده ، سن و سال هنرجويان ، ميزان شهرية پرداختي و . . . را درخواست مي‌كند . هريك از پرسنل مسوولیت تهية بخشي از گزارش را تقبل كرده ، نرم افزار خود را اجرا مي‌كنند و مشغول تهية گزارش مي‌شوند . در اين قسمت براي ادامهٔ كار مي‌توان دو حالت متفاوت را در نحوهٔ كار نرم‌افزار متصور شد :

حالت اول : هريك از برنامه‌هاي اجرا شده روي كامپيوترها ، بانك اطلاعاتي موجود بر FileServer را باز كرده ، كلية اقلام اطلاعاتي آنرا از طريق شبكه به كامپيوتر خود انتقال داده (دفعتاً يا تدريجي) سپس اطلاعات را در كامپيوتر خود بررسي كرده و در صورت صدق در شرايط آنرا چاپ كند . در اين حالت اگر بعنوان مثال ۱۰۰۰ ركورد در بانك موجود است ، هر كامپيوتر بايد همهٔ آنها را از طريق شبكه به كامپيوتر خود انتقال داده و عمليات پردازش را روي ماشين خودش انجام دهد (البته مي‌توان از تكنيكهايي استفاده كرد كه نياز به انتقال همهٔ ركوردها نباشد) . چون ۳ كامپيوتر مشغول به گزارشگيري هستند لذا تقريباً ۳۰۰۰ ركورد اطلاعاتي در ترافيك شبكه سهيم مي‌شوند . ممكن است با خود بگوييم كه ۳۰۰۰ ركورد را كامپيوترها سريع مي‌خوانند ، و زماني طول نخواهد كشيد. اين طرز فكر درست است اما تصور كنيد كه با يك بانك اطلاعاتي حجيم درگير شويم مثلاً بانك ادارهٔ ثبت احوال با فرض شصت ميليون ركورد ! در اينجا ديگر نمي‌توان مابين ترافيك شصت ميليون ركورد در شبكه و ۳ برابر آن يعني يكصد و هشتاد ميليون تفاوت قائل نشد .

حالت دوم : مشكلي كه در حالت قبلي وجود دارد آنست كه حجم ترافيك شبكه با افزايش اطلاعات بانك و تعداد كاربران بسرعت زياد شده و باعث اشباع شبكه مي‌شود بنابراين بهتر است هر كامپيوتر بجاي آنكه خودش رأساً مبادرت به خواندن اطلاعات بانك از File Server و پردازش آن در ايستگاه كند از سرور بخواهد كه عمليات را انجام دهد . بدين ترتيب كه يك Application Server روي همان File Server نصب كرده سپس از ايستگاه به سرور فرمان مي‌دهيم كه سرور اطلاعات را جستجو كند و فقط نتايج را براي ما ارسال نمايد نتيجه‌اي كه از اين كار به دست مي آيد آنست كه ديگر هيچ نيازي به انتقال حجيم اطلاعات در شبكه و پردازش آن در ايستگاه نبوده لذا هم ترافيك شبكه به حداقل مي‌رسد و هم پردازش ايستگاه سبك مي‌شود چرا كه ايستگاه فقط نتايج را از سرور دريافت كرده و براي كاربر نمايش مي‌دهد ، بنابراين :

تعريف : به يك Application Server كه روي بانكهاي اطلاعاتي كار مي‌كند اصطلاحاً Database Server (به اختصار DB Server) مي‌گوييم . پس مي‌بينيم كه DB Server يك سرور جديد نيست بلكه همان AppServer است كه براي كار روي بانكهاي اطلاعاتي طراحي شده و بعبارتي همان كاربرد سوم App Server است كه در بخش مربوطه اشاره شد . از سرورهاي معروف بانكهاي اطلاعاتي مي‌توان به Oracle و Microsoft SQL Server اشاره كرد كه با آنها در درس بانك اطلاعاتي آشنا مي شويد .

ويژگيهاي سخت‌افزاري يك Database Server

ويژگي هاي اين سرور نيز همانند App Server است علاوه بر اين ديسك سخت هم مثل CPU و RAM در درجة اول اهميت قرار مي‌گيرد . پس توجه همزمان به هر ۳ پارامتر مهم است .

سرور ها به چه سيستم عاملي نياز دارند؟
اما پاسخ به اين سوال مستلزم آشنايي و طبقه‌بندي محصولات سيستم عامل و ويژگيهاي مربوطه است كه خود بحث مفصلي است لذا به تيتر آنها اكتفا كرده و بحث پيرامون آنها را به توضيحات هنر آموز درس و تحقيقات خواننده واگذار مي‌كنيم، البته در اين مرحله نياز به دانستن و پرداختن به جزئيات في سيستم عاملها نبوده، آشنايي كلي، كاربرد و عموميت حوزة مصرفي آنها كفايت مي‌كند.

۶-۱- طبقه‌بندي محصولات Microsoft در زمينة سيستم عامل ها

شركت مايكروسافت بطور كلي در مورد سيستمهاي عامل، ۲ دسته محصول ارايه كرده است:

- سيستم عاملهايي كه براي نصب و كاربرد در سرويس گيرنده.
- سيستم عاملهايي كه براي نصب و كاربرد در سرور .
- در متن زير طبقه بندي اين سيستم عامل ها نشان داده شده است

Client Operating Systems :

- DOS Family : DOS (v1, ... , v6.2 , v6.22 , v7.0)
- Windows 3.x Family : Windows 3.1 , 3.11 (Windows for Workgroups)
- Windows 9x Family : Windows 95 , 97 (95 OSR2) , 98 , 98 SE , ME
- Windows NT Family :
- NT 3.51 Workstation
- NT 4.0 Workstation
- NT 5.0 : 2000 Professional
- NT 5.1 : XP (Home , Professional , Media center , Tablet PC)

Server Operating Systems :

- NT 3.51 Server
- NT 4.0 Server
- NT 5.0 : 2000 Server Family : (Server, Advanced Server, Data center)
- NT 5.2 : 2003 Server Family : (Standard, Enterprise, Data center, Web edition)

همانطور كه ديده مي‌شود ويندوز 2000 بنام NT 5.0 ، XP بنام NT 5.1 و 2003 بنام NT 5.2 نيز خوانده مي‌شوند . در كل به هر ۳ سيستم عامل ، خانوادة NT 5.x گفته مي‌شود.
XP فقط در گروه سرويس گيرنده و 2003 فقط در گروه Server قرار گرفته . بعبارت ديگر XP نسخة سرور نداشته و 2003 نيز نسخة Client ندارد.
هرچند خانوادة 9x و XP جايي در گروه سرورها ندارند اما خيلي از كاربران تجربة اشتراك گذاري پوشهها و چاپگرهاي خود را در آنها داشته‌اند، يعني كامپيوتري كه سيستم آن مثلاً 98 است تبديل به File Server يا Print Server مي‌شود. اين موضوع ناقض طبقه‌بندي فوق نيست ، بعبارتي هرچند 98 هم مي‌تواند در مواردي تبديل به سرور شود اما قرار نگرفتن آن در گروه سرورها بمعني آنست كه 98 يا XP عمدتاً براي كاربرد در ايستگاه ها طراحي شده اند.
مايكروسافت فقط خانوادة NT را براي كاربرد در سرورها پيشنهاد داده است.

نام برخي از محصولات كمپانيهاي ديگر در زمينة سيستم عامل ها (كه عمدتاً براي كار در سرورها استفاده مي‌شوند)

- UNIX (SCO , Solaris , BSD , Free BSD , AIX , HP , Linux , . . .)

- Novell Netware
- IBM OS/2 , IBM LAN Server
- Apple Macintosh (Used in Graphic Stations)

...

خانوادة UNIX تقريباً در همة زمينه‌ها كاربرد دارد . امروزه در ايران شبكه‌هاي بانكي ، شركت نفت ، شهرداري ، بيمه و . . . همگي از اين خانواده بعنوان سيستم عامل اصلي در سرورها بهره مي‌برند .
Novell در ايران عمدتاً بعنوان File Server و تا حدي Print Server بكار مي‌رود هرچند كه در خيلي از مكانها Database Server نيز روي Novell اجرا مي‌شود .

۷-۱- آشنايي با ويژگيهاي سيستم عامل های شبكه‌ای

سيستمهاي عامل كه در شبكه استفاده مي‌شوند بايد ويژگيهايي را افزون بر سيستمهاي عامل كه در كابردهاي خانگي مورد استفاده قرار مي‌گيرند داشته باشند . هرچند امروزه اكثر كاربران خانگي به محض اتصال به اينترنت عملاً بعنوان كاربر شبكه محسوب مي‌شوند بنابراين خصوصيات سيستمهاي عامل شبكه براي سيستمهاي خانگي نيز (در حدي كمتر) معني پيدا مي‌كند . برخي از اين ويژگيها به ترتيب اهميت عبارتند از :

- Security
- Multitasking
- Multi Processor Support
- Reliable & Stable
- Fault Tolerance
- Backup Utilities
- Simple & Unified Administrative Tools
- Support

با برخي از اين ويژگی ها قبلاً در درس سيستم عامل آشنا شده ايد.

۷-۱-۱- Security :

امنيت ، مهمترين ويژگي است . متاسفانه دنيا ايده‌ال نيست لذا درنظر گرفتن مسايل امنيتي هرچند كه باعث كندي سيستم مي‌شود اما بعنوان ركن كار هر سيستم عامل شبكه محسوب مي‌شود . امنيت براي سيستم عامل را مي‌توان در حوزه‌هاي مختلفي بررسي كرد بعنوان مثال :

الف) امنيت در حوزة دسترسي به ديسك و فايل-سيستم (Disk & File-System Security)
ب) امنيت در حوزة عملياتي كه كاربرد عام دارند مانند :
- تغيير ساعت سيستم (Changing System time)
- نصب نرم افزار ، سخت‌افزار و انجام تنظيمات (Hardware & Software Installation)
- اجراي برنامه‌ها و تغيير در پارامترهاي مربوطه (Running Applications & Services)

ج) امنيت در حوزة شبكه و اطلاعات تبادلي (Network Security)
د) امنيت در ورود به سيستم (System Login)

مثال : Dos ، Win 3.1 و خانوادة 9x جزو آندسته از سيستمهايي هستند كه امنيت چنداني مخصوصاً در حوزه‌هاي "الف" ، "ب" و "ت" ندارند . همه مي‌دانيم كه پس از روشن كردن يك كامپيوتر با سيستم 98 براحتي مي‌توان بدون هيچگونه گذر واژه اي وارد آن شده ، به هرجا روي ديسك دسترسي پيدا كرده (كه با FAT آماده شده) ، هربرنامه‌اي را نصب ، حذف يا اجرا كرده و هرگونه تغيير سخت‌افزاري را اعمال كرد ! در صورتيكه اين امر در خانوادة NT براحتي امكان‌پذير نيست ، فقط كاربراني كه عضو گروه Administrators باشند توانايي تام در انجام عمليات فوق را دارا هستند .

نكته : كاربراني كه هنگام نصب XP تعريف مي‌شوند همگي عضو گروه Administrators بوده و براي كاهش قدرت آنها بايد بعد از نصب از طريق برنامه مربوطه وارد عمل شد و گروه آن ها را به Lmited (users) تبديل كرد . چنانچه در XP فقط يك كاربر تعريف كنيم ، درآنصورت كامپيوتر پس از Boot شدن خودبخود وارد سيستم مي‌شود بدون آنكه گذر واژهي از ما خواسته شود ، در اين حالت سيستم عامل XP بطور خودكار همان يك كاربر را Auto Login مي‌كند و اين بمعناي نقض امنيت در ورود به سيستم نيست ، مي‌توان اين ويژگي را غيرفعال كرد . ضمناً اين خصوصيت يعني Auto Login در بقية اعضاي خانوادة NT نيز وجود دارد .

فعاليت عملي مربوط به ويژگي Security :

الف) نشان دهيد كه در XP كاربران تعريف شدة هنگام نصب ، عضو گروه Administrators هستند .

ب) نشان دهيد كه در XP ، يك كاربر عادي (عضو گروه Users) قادر به ايجاد فايل جديد در ريشة ديسك كه با فايل-سيستم NTFS فرمت شده نيست (پوشه جديد را مي‌توان درست كند اما فايل را خير)

ج) نشان دهيد كه در XP ، يك كاربر عادي (عضو گروه Users) نمي‌تواند ساعت سيستم را تغيير دهد .

د) نشان دهيد كه در XP ، يك كاربر عادي (عضو گروه Users) نمي‌تواند از طريق Device Manager يك سخت‌افزار را (مثلاً Mouse) غير فعال (Disable) كند .

۲-۷-۱- Multi Tasking :

چند وظيفه‌اي ، توانايي اجراي همزمان چندين برنامه با هم . اين ويژگي نيازي به شرح بيشتر نداشته و امروزه در تمامي سيستمها وجود دارد و يك ويژگي عادي بشمار مي‌رود . DOS بعنوان يك سيستم قديمي Multi task نيست اما بقيه تقريباً همگي Multi Task هستند منجمله Windows 3.x .

تقسيم زماني بين كارهاي مختلف و گردش سريع بين آنها . اين تكنيك در اصطلاحات فني Time_Sharing يا "اشتراك زماني" خوانده مي‌شود . تكنيك اشتراك زمان نه تنها در اجراي برنامه‌ها به وسيله CPU بلكه در مخابرات و شبكه نيز كاربردهاي فراواني در انتقال اطلاعات دارد و يكي از روشهايي است كه مي‌توان اطلاعات چندين فرستنده را روي يك محيط انتقال بطور همزمان ارسال كرد . البته اين تكنيك در اصطلاحات مخابراتي Time Division Multiplexing = TDM خوانده مي‌شود .

۲-۷-۳- Multi Processor Support :

پشتيباني از چندين پردازنده ، مي‌دانيم كه هرچه تعداد پردازنده‌هاي موجود بر روي يك برد اصلي بيشتر باشد كارها سريعتر انجام مي‌شود .
امروزه بردهاي چند پردازنده در ۲ زمينة عمده كاربرد دارند :
- سرورها ، مخصوصاً App Server و DB Server كه قبلاً اشاره شد .
- كامپيوترهايي كه عمليات سنگين گرافيكي و پويا را انجام مي‌دهند . (Graphic Workstations)

بنابراين در مواردي كه نياز به استفاده از بردهايي با بيش از يك CPU باشد لازم است تا سيستم عامل نيز بتواند آنها را شناسايي كرده و استفاده كند . در خانوادة Microsoft فقط سيستمهاي NT قادر به شناسايي و بهره‌برداري از چندين CPU هستند .

تحقيق : پشتيباني از چندين پردازنده در سيستم عامل ها با ۲ سياست كلي متقارن و نامتقارن انجام مي‌شود ، (SMP=Symmetric Multi Processing , AMP=Asymmetric

Multi Processing) ، هريك را به اختصار بررسي كرده و بگوييد كه مايكروسافت در سيستمهاي خود از كدام روش استفاده مي‌كند ؟

۴-۷-۱- تحمل خطا Fault Tolerance :

تحمل خطا ، عدم تأخير در ارائة سرويس و قدرت تحمل در هنگام بروز مشكل و خطاهاي عمدتاً سخت‌افزاري است بعبارت ديگر Fault Tolerance (باختصار FT) قابليتي است در سيستم عامل كه مي‌تواند هنگام بروز مشكلات از تجهيزات جايگزين استفاده كرده و بدون تأخير (يا با تأخير بسيار كوتاه) بطور خودكار به سرويس دهي ادامه دهد . نكتة اصلي در FT اينست كه هنگام بروز خطا اولاً زمان قطعي سرويس صفر يا بسيار كوتاه بوده و ثانياً عمليات جايگزيني بدون عوامل انساني و بطور خودكار صورت مي‌گيرد . مسوول سيستم در فرصت مناسب مي‌تواند عيوب را بررسي و رفع كند .

مثال ۱ : فرض كنيد كه يك File Server داريم كه تمامي اطلاعات خود را روي يك ديسك سخت ذخيره كرده‌است . اگر براي ديسك مشكلي بروز كند مثلاً بر اثر يك شوك الكتريكي در برق بخشي از قطعات آن بسوزد چه اتفاقي مي‌افتد ؟ بديهي‌است كه سرويس قطع مي‌شود ، چكار كنيم كه سرويس قطع نشود ؟

الف) شرايط سخت‌افزاري لازم را مهيا كنيد يعني از ابتدا ۲ ديسك سخت روي سيستم نصب كنيد .

ب) سيستم عاملي را انتخاب كنيد كه داراي قابليت FT در زمينة ديسك باشد . سيستم عامل در شرايط عادي هر اطلاعاتي را كه روي ديسك اول مي‌نويسد عيناً روي ديسك دوم نيز كپي مي‌كند بعبارتي ديسك دوم همانند آيينه‌ايست از ديسك اول (Disk Mirroring , Disk Duplexing) حال اگر به هر دليل يكي از ديسكها از كار بيافتد سيستم عامل مي‌تواند بدون لحظه‌اي تأخير اطلاعات را با ديسك دوم تبادل كند . مثال فوق در اصطلاحات كامپيوتري Disk_Fault_Tolerance با تكنيك Mirror يا Duplex يا RAID 1 خوانده مي‌شود . از ميان محصولات مايكروسافت ، سيستمهاي NT كه در گروه سرور قرار دارند همگي قابليت Disk Fault Tolerance را دارا هستند .

مثال ۲ : يك سرور داريم (از هر نوع دلخواه) كه با يك كارت شبكه (NIC) به شبكه متصل شده و كامپيوترها از آن سرويس مي‌گيرند . اگر براي كارت شبكه يا خط متصل به آن اتفاقي بيافتد چه مي‌شود ؟ بديهي‌است كه سرويس قطع مي‌شود اگر بخواهيم كه سرويس قطع نشود بايد:

الف) شرايط سخت‌افزاري لازم را مهيا كنيد يعني از ابتدا ۲ عدد NIC روي سيستم نصب كنيد .

ب) سيستم عاملي را انتخاب كنيد كه داراي قابليت FT در اين زمينه باشد . سيستم عامل در شرايط عادي اطلاعات را تقسيم كرده و از هر ۲ كارت براي ارسال و دريافت استفاده مي‌كند (كه البته باعث افزايش سرعت نيز مي‌شود) حال اگر به هر دليل يكي از كارتها از كار بيافتد ، سيستم از كارت ديگري براي ادامة كار استفاده مي‌كند . مثال فوق در اصطلاحات كامپيوتري NIC Fault Tolerance خوانده مي‌شود و در برخي از متون به آن Port Trunk يا Port Aggregation يا Link Aggregation مي‌گويند كه بعداً نيز مورد بحث قرار خواهد گرفت . از ميان محصولات مايكروسافت ، سيستمهاي NT اعم از سرويس گيرنده يا Server درصورتيكه كمپاني سازندة كارت شبكه درايور مناسب را براي محصول خود ارائه داده باشد مي‌توان از اين خاصيت بهره برد.

مثال ۳ : فرض كنيد كه يك سرور داريم (از هر نوع دلخواه) و اين سرور ممكن است هريك از موارد قبلي Fault tolerance را اعم از Disk يا NIC داشته باشد يا خير . اگر به هر دليل سرور بطور كامل از كار بيافتد چه مي‌شود ؟ بديهي‌است كه سرويس قطع مي‌شود ، چكار كنيم اختلالي در سرويس دهي بروز نكند ؟

الف) شرايط سخت‌افزاري لازم را مهيا كنيد يعني از ابتدا ۲ يا چند سرور را با تجهيزات ويژه به يكديگر متصل كنيد . به اين مجموعه از سرورها اصطلاحاً يك "خوشة سرور" يا Server Cluster گفته مي‌شود .

ب) سيستم عاملي را انتخاب كنيد كه داراي قابليت FT در زمينة Clustering باشد . كلية سيستمها در شرايط عادي اطلاعات مورد نياز را با يكديگر تبادل كرده (Synchronize) و چنانچه يكي از اعضاي Cluster (يعني يكي از سرورها) از كار افتد بقيه مي‌توانند بسرعت و بدون تأخير كار او را جبران كنند . از ميان محصولات مايكروسافت فقط چند سيستم از مجموعة NT در خانوادة سرور داراي قابليت Cluster هستند بعنوان مثال 2000 Server فاقد آن بوده اما 2000 Advanced Server و 2000 Data center Server داراي توانايي آن هستند .

۵-۷-۱- نرم افزار تهيه نسخه پشتيبان Backup Utilities :

امروزه اهميت تهية Backup براي يك كاربر باتجربه پوشيده نيست ، بالاخره هركس كه با كامپيوتر سروكار دارد با لحظه‌اي مواجه شود كه به هر دليل اطلاعات اصليش مخدوش يا غيرقابل دسترس شده است در اين حالت با نسخة پشتيبان مي توان اطلاعات را دو باره باز گرداند.

اطلاعات را در حالت كلي مي‌توان به دو دسته تقسيم كرد :

الف) اطلاعاتي كه كاربر مستقيماً و كم و بيش از آن آگاه بوده و اهميتش بر او پوشيده نيست مانند انواع پرونده‌ها يا حتي برنامه‌هاي كاربردي كه تهيه و نصب كرده است : (User Data)

ب) اطلاعاتي كه كاربر مستقيماً با آن سروكار ندارد بلكه براي سيستم عامل مهم است : (System Data)

اغلب كاربران پس از مدت كوتاهي با نحوة تهية Backup از اطلاعات خودشان يعني User Data آشنامي شود اما كمتر كاربر عادي پيدا مي‌شود كه طي مدت كوتاهي بتواند بطور كامل از System Data نيز Backup گرفته يا Restore كند چرا كه با توجه به پيچيدگي سيستم عاملها ، كسب آگاهي نسبت به ظرافتهاي سيستم عامل در زمان كوتاه امر ساده‌اي نبوده و نياز به تجربه و تخصص دارد .

چگونه مي توان از System Data بدون مهارت لازم Backup گرفت ؟

يك راه‌حل مناسب آنست كه سيستم عامل ابزارهاي قوي و عين حال User Friendly در اختيار كاربر بگذارد تا او بتواند اولاً براحتي اطلاعات را دسته‌بندي كند ثانياً بدون داشتن تخصص زياد قادر به تهية Backup از System Data باشد .خوشبختانه ابزارهاي تهية Backup در سيستمهاي NT 5.x داراي چنين توانائيهايي بوده و كاربر مي‌تواند در صورت داشتن مجوز ، تنها با علامتگذاري در قسمت "System State" اقدام به تهية پشتيبان از System_Data كند .

ممكن است بخواهيد بدانيد تفاوت بين ابزارهاي خاص تهية Backup (مانند NTBackup در NT 5.x) با ابزارهاي عمومي مديريت فايلها كه عملياتي مانند Copy-Paste را انجام مي دهند (مانند My Computer = Explorer) چيست ؟در جواب بايد گفت: قابليتهايي كه در ابزارهاي خاص وجود دارد در برنامه‌هاي عمومي (مانند My Computer) نيست . اهم اين قابليتها عبارتند از :

الف) به كمك ابزارهايي مانندNTBackup براحتي از System Data نسخة پشتيبان تهيه مي‌شود .

ب) با اين ابزارها ، از فايلهايي كه در حال استفاده هستند (Open Files) مي توان به راحتي نسخه پشتيبان تهية كرد.

ج) سياستهاي تهية Backup يا بعبارت فني Backup Policy در ابزارهاي خاص تنوع بيشتري دارد ، بدان معني كه انتخاب فايلها براي Backup مي‌توان با معيارهايي همچون "فقط فايلهاي تغييريافته" و . . . صورت گيرد . كه در ابزار هاي معمولي تنوع اين معيار ها كمتر است.

د) با ابزارهاي خاص مي‌توان انجام عمليات را بطور خودكار در موعد دلخواه زمانبندي كرد (Scheduling) .

ه) ابزارهاي خاص مي‌توانند از مجوزهاي امنيتي (ليست دسترسي افراد به فايلها = Access Control List) كه باختصار ACL خوانده مي‌شود نيز Backup گرفته و Restore كنند . منظور از ACL ليستي است در فايل-سيستمهايي مانند NTFS كه تعيين مي‌كند چه افرادي چه عملياتي را با يك فايل يا پوشه مي‌توانند انجام دهند . بديهي است كه ACL در FAT يا FAT 32 وجود ندارد چرا كه FAT امنيت ندارد .

فرايند Backup براي خود جزو مباحث مهم بوده و معمولاً در درس سيستم عامل پيشرفته يا سرور مورد بحث قرار مي‌گيرد با اينحال براي تثبيت نكات ياد شدة فوق ، انجام اين كار را اكيداً توصيه مي‌كنيم كه بايد به كمك هنر آموز درس انجام شود .

الف) نشان دهيد كه با NTBackup مي‌توان براحتي از اطلاعات سيستم Backup تهيه كرد .

ب) دقيقاً با كدام كاربر وارد سيستم شده‌ايد ؟ پس از پاسخ به اين سوال ، برنامة My Computer را اجرا كرده سپس پارتيشني را كه سيستم عامل روي آن نصب شده باز كرده (مثلاً ديسك :C) وارد پوشه Documents_and_Settings شويد . قاعدتاً بايد يك پوشه همنام با كاربري را كه با آن وارد سيستم شده‌ايد ببينيد . حال سعي كنيد كه (با استفاده از برنامة My Computer) از اين پوشه Copy-Paste بگيريد . آيا امكان‌پذير است ؟ قطعاً خير ! چرا كه يكي از فايلهاي موجود در اين پوشه (كه البته مخفي نيز هست) بنام NTUser.dat در حال استفاده بوده اصطلاحاً Open است و برنامة My Computer نمي‌تواند از آن كپي تهيه كند . حال با استفاده از برنامة NTBackup از همين پوشه كپي بگيريد . نتيجه چيست ؟ بلي ، امكان‌پذير است . بنابراين نشان داديد كه NTBackup قدرت بيشتري نسبت به My Computer در تهية پشتيبان از فايلها و پوشهها دارد .

۶-۷-۱- ابزار های مدیریتی Simple and Unified Administrative Tools :

ابزارهاي مديريتي ساده ، قدرتمند و يكپارچه . هر سيستم عاملي هرچقدر هم كه قوي باشد اما اگر پيكربندي ، تنظيمات و بطور كلي مديريت آن پيچيده باشد با عدم استقبال عامه مواجه مي‌شود و اين دقيقاً يكي از دلايلي است كه UNIX بويژه نسخه‌هاي قديمي‌تر فقط در بين متخصصين محبوبيت پيدا كرد (البته امروزه نسخه‌هاي جديدتر از اين حيث كامل هستند اما اندكي دير شده چرا كه مايكروسافت از اين طريق در بين كاربران عادي كاملاً جاي خود را تثبيت نموده است.

فعاليت عملي : آشنايي با يكي از ابزارهاي مديريتي قوي در NT 5.x :

يكي از برنامه‌هاي قدرتمند براي مديريت بخشهاي مختلف ، برنامه‌ايست بنام Computer Management . براي اجراي اين برنامه راههاي متفاوتي وجود دارد اما ۲ راه را بيان مي‌كنيم :

الف) روي آيكن My Computer واقع بر دسكتاپ كليك راست كرده ، گزينة Manage را انتخاب كنيد .

ب) از طريق Run تايپ كنيد : compmgmt.msc

پس از اجراي برنامه ، بررسي كنيد كه بوسيلة آن چه كارهايي را مي‌توان انجام داد .

۷-۷-۱- قابلیت اطمینان و پایداری Reliable and Stable :

قابل اطمينان و پايدار ، با يك مثال مفهوم اين ويژگي براي ما تثبيت مي‌شود ، تجربه شده است كه سيستم عامل ويندوز 98 برخلاف سيستم عامل

UNIXو LINUX پس از نصب چندين برنامة مختلف بهم مي ريزد حال بنظر شما چنين سيستمي مناسب شبكه و مخصوصاً سرور است ؟!

خوشبختانه سيستمهاي NT و مخصوصا" NT 5.x در وضعيت بسيار بهتري نسبت به خانوادة 9x قرار دارند و بدين لحاظ براي كاربرد در شبكه‌ها اعم از سرويس گيرنده يا سرور مناسبترند .

۸-۷-۱- پشتيبانی Support :

پشتيباني ، هر سيستم عاملي اعم از قوي يا ضعيف نياز به رشد و رفع مشكلات و نواقص دارد و اين ميسر نيست مگر با پشتيباني از طرف تهيه‌كننده‌گان يا تيمهاي جنبي . خوشبختانه در زمينة محصولات مايكروسافت با وجود نواقص بسيار مخصوصاً در زمينة امنيتي ، پشتيباني آن قوي بوده و اكثراً تجربة بروز رساني سيستم عاملهاي NT 5.x را از طريق برنامة Automatic Update داشته ايم .

خود آزمايي و تحقيق

۱- از لحاظ تقسيم بندي شبكه هاي كامپيوتري از نظر سرويس دهي شبكه اينترنت به كدام دسته تعلق دارد؟

۲- از لحاظ تقسيم بندي شبكه هاي كامپيوتري از نظر گستردگي فيزيكي سيستم بانكي شتاب به كدام دسته تعلق دارد؟

۳- سرويس هاي رايج در سبكه هاي كامپيوتري را نام ببريد؟

۴- نقش حافظه RAM را در هر يك از انواع File Server، Print Server، Applicatin Server بررسي كنيد؟

۵- داشتن چندين پردازنده در كدام يك از انواع سرور مي تواند مفيد باشد؟

۶- User Data و System Data را تعريف كنيد؟

۷- ويژگي سيستم عامل را نام ببريد؟

۸- تفاوت Multi Tasking و Multi Programing را بنويسيد.

۹- تحقيق كنيد كه يك سرور NAS به لحاظ سخت افزاري بايد چه قابليت هايي داشته باشد؟

۱۰- تحقيق كنيد كه حداقل سخت افزار لازم براي نصب هر يك از سيستم عاملهاي محصول مايكروسافت چيست و آنها را با هم مقايسه كنيد.

فصل دوم سيستم هاي انتقال ديجيتال

هدف هاي رفتاري

- روش ارسال اطلاعات به صورت موازي را بيان كند.
- روش هاي ارسال اطلاعات به صورت سري را شرح دهد.
- انواع روش هاي انتقال اطلاعات بر اساس جهت آنها را تعريف كند.
- سيگنال هاي اطلاعات و انواع آن را شرح دهد.
- پهناي باند را تعريف كند
- نويز و انواع آن را شرح دهد.

يكي از مسايل مهم در شبكه هاي كامپيوتري نحوه برقراری ارتباط بين كامپيوتر هاست . منظور از برقراری ارتباط اين است كه اطلاعات به چه ترتيبی ارسال شوند.می توان اين پرسش ها را مطرح كرد كه آيا روش ارسال به صورت بيت به بيت و جداگانه باشد يا گروهی از اطلاعات با هم و به صورت گروهی ارسال شوند يا اين كه آيا فرستنده آن ها را همانند يك ايستگاه فرستنده راديويی ارسال نمايد يا از روشی كه در مخابرات برای انتقال صورت به كار می رود ، استفاده شود .جواب اين پرسش ها اين است كه اطلاعات در شبكه به صورت كدهای دودويی ارسال می شوند . در سيستم دودويی فقط از دو كد صفر و يك استفاده می شود كه در كامپيوتر مقصد از تركيب اين كدها ، اعداد ، حروف و كاراكترهای ويژه به دست می آيد .

ارسال اطلاعات به صورت دودويی می تواند به دو صورت انجام شود:

۱. parallel (يا موازی)
۲. سريال (پشت سرهم)

در روش موازی تعدادی از بيت ها با هم و به صورت گروهی ارسال می شوند ولی در روش سريال ، بيت ها تك به تك و پشت سرهم ارسال می شوند . نحوه ارسال به صورت موازی فقط يك شيوه دارد ، در صورتی كه ارسال سريال از دو روش ارسال هم زمان (Synchronous) وغير هم زمان (Asynchronous) استفاده می شود.

۲-۱- ارسال موازی(Parallel)

در اين روش اطلاعات قبل از ارسال تبديل به كدهای باينری شده و يك به يك ارسال می شوند . برای مثال می توان گفت كه اين عمل مانند اين است كه يك نامه را تبديل به حروف تشكيل دهنده آن كرده و حروف را يك به يك ارسال كنيم.

حال تعدادی كد باينری داريم كه می خواهيم ارسال كنيم؛ اگر تعدادی از آن ها را تبديل به يك گروه كرده و باهم بفرستيم ارسال سريعتر انجام می شود و اين چيزی است كه در ارسال موازی اتفاق می افتد در اين روش تعدادی كاراكتر از طريق چند خط ارتباطی و به صورت هم زمان با هم ارسال می شوند ؛ اين خطوط می توانند در درون يك كابل شبكه يا يك شبكه بی سيم بنا شده باشند به صورت پيش فرض ۸ خط برای ارسال موازی در نظر گرفته شده است يعنی می توانيم حداكثر ۸ كد را هم زمان ارسال كنيم .

۲-۲- ارسال سريال

در ارسال سريال ، بيت ها به دنبال هم و به صورت سری انتقال می يابند ؛ به اين ترتيب كه بيت ها پشت سرهم قرار گرفته و يك رشته را می

سازند و این رشته به کامپیوتر مقصد راسال می شود . در حین ارسال ممکن است عوامل مختلفی مثل نویز و هم شنوایی که در همین واحد کار در مورد آن ها توضیح داده شده است ، روی اطلاعات اثر گذاشته و آن را خراب کنند . برای کنترل بیت ها و کمک به ارسال عاری از اشکال ، ابتدا و انتهای بیت ها با یک سری علامت به نام های بیت شروع[1] بیت پایان[2] مشخص می شود که در روش های مختلف ارسال سریال محل قرار گیری این علامت ها و محتوای آن ها متفاوت است . ارسال سریال به دو روش امکان پذیر است .

۱-۲-۲- ارسال سریال غیر هم زمان

دلیل نام گذاری این روش به غیر هم زمان این است که زمان بندی در هنگام ارسال اطلاعات مهم نیست و زمان بندی بین دو واحد فرستنده و گیرنده انجام می شود .
در این روش انتقال اطلاعات براساس الگوهای ارسال و دریافت که از قبل مشخص شده است ، انجام می شود و تا وقتی این الگوها رعایت شوند ارسال بدون وقفه انجام می پذیرد. در این روش هر ۸ بیت اطلاعات تبدیل به یک رشته شده و قبل از هر رشته یک Start Bit و پس از هر رشته یک Stop Bit قرار می گیرد . در صورتی که هر کدام از بیت ها هنگام ارسال آسیب ببینند ، آن بیت مشخص شده و دوباره ارسال می شود . در ارسال غیر هم زمان ۲۵% از کل ظرفیت خط ارتباطی صرف کنترل ترافیک شده و تنها۷۵% ظرفیت برای انتقال اطلاعات استفاده می شود .
توانایی کامپیوتر ها در ارسال و دریافت اطلاعات از نظر سرعت متفاوت است ؛ بنابراین ممکن است یک کامپیوتر بتوند در واحد زمان ، مقدار بیشتری اطلاعات به سمت کامپیوتر مقصد ارسال کند .
بدیهی است در چنین حالتی ، کامپیوتر گیرنده که با سرعت کمتری کار می کند نمی تواند تمامی اطلاعات ارسال شده را دریافت نماید ، در نتیجه مقداری از این اطلاعات در شبکه از بین می رود ، بنابراین در کامپیوترهایی که در حال تبادل اطلاعات هستند ، همواره سرعت ارسال و دریافت را باهم چک کرده و در صورت لزوم سرعت ارسال را کم یا زیاد می کنند . در روش انتقال غیر هم زمان هیچ زمان بندی برای ارسال یا دریافت صورت نمی گیرد و کنترل ترافیک به صورت لحظه ای انجام می شود . به همین دلیل در روش انتقال غیر هم زمان ،۷۵% ظرفیت خط انتقال صرف کنترل ترافیک می شود . منظور از ظرفیت خط انتقال تهمان پهنای باند است که در همین واحد کار توضیح داده شده است .

۲-۲-۲- ارسال سریال هم زمان

در روش ارسال هم زمان همانند روش ارسال غیر هم زمان اطلاعات ابتدا به کدهای دودویی تبدیل می شوند ، سپس تعدادی بیت که حاوی اطلاعات ارسالی هستند در امتداد یکدیگر قرار گرفته و یک رشته را تشکیل می دهند ، این رشته همانند رشته هایی که در روش ارسال غیر هم زمان ساخته می شوند ، به وجود می آیند ؛ سپس تعدادی از آن ها به هم متصل شده و رشته طولانی تری را پدید می آورند ، پس از آن ابتدا و انتهای این رشته به وسیله ی بیت شروع و بیت پایان مشخص می شود ؛ در این لحظه قبل از شروع ارسال ، دو کامپیوتر به وسیله ی سیستم زمان بندی داخلی، خود را با هم هماهنگ می کنند سپس کامپیوتر ارسال کننده ،ارسال را شروع کرده و کامپیوتر گیرنده اطلاعات را در یافت می کند .
زمان ارسال یا دریافت اطلاعات به وسیله ی سیستم زمان بندی برای هر دو کامپیوتر مشخص می شود ،در نتیجه هیچ گاه کامپیوترها ارسال اطلاعات را هم زمان با یکدیگر انجام نمی دهند و عمل انتقال اطلاعات به صورت نوبتی انجام می شود .

---

[1]-Start Bit

[2] -stop Bit

در روش ارسال هم زمان علاوه بر استفاده از سیستم انتقال سریع تر، عمل کنترل ترافیک نیز انجام نمی شود و از تمام ظرفیت خط انتقال برای ارسال و دریافت استفاده می شود ؛ به همین دلیل سرعت انتقال به مراتب بالاتر از روش غیر هم زمان است .

۲-۳- جهت انتقال اطلاعات

بین دو واحد فرستنده و گیرنده همیشه اطلاعاتی در حال جا به جا شدن است که در محیط های مختلف جهت آن متفاوت است . ارتباط بر اساس جهت های انتقال به سه گروه تقسیم می شوند؛

۱-یک طرفه[1]
۲-دوطرفه غیر هم زمان [2]
۳- دوطرفه هم زمان [3]

۲-۳-۱- ارتباط یک طرفه

در این روش یک فرستنده و یک گیرنده ثابت وجود دارد و هیچ گاه جای این دو عوض نمی شود . در روش یک طرفه ، اطلاعات به وسیله ی فرستنده ارسال وبه وسیله ی گیرنده دریافت می شود . برای مثال می توان به رادیو یا تلویزیون اشاره کرد . در هرکدام از این سیستم ها ، اطلاعات به وسیله ی یک فرستنده رادیویی یا تلویزیونی ارسال و به وسیله ی گیرنده که همان دستگاه ر ادیو یا تلویزیون است دریافت می شود و هیچگاه ارسال تعیین نمی کند . به این روش ارسال ، یک طرفه می گویند .

شکل ۱-۲ (ص۱۸) مفاهیم شبکه

۲-۳-۲- ارتباط دو طرفه غیر هم زمان

در روش دوطرفه غیر هم زمان ارسال دوطرفه ولی غیر هم زمان است یعنی دو واحد Aو B نمی توانند هم زمان برای یکدیگر اطلاعات ارسال کنند و این کار باید متناوب انجام شود. در واقع هنگامی که واحد A ارسال اطلاعات است ، واحد Bفقط باید دریافت کننده باشد و برعکس. برای مثال می توان به واکی – تاکی یا فرستنده – گیرنده های بی سیم اشاره کرد .

شکل ۲-۲- ۳ شکل ۲-۱ (الف) (ص ۱۹) مفاهیم شبکه

---
[1] - Simplex
[2] - Half-Duplex
[3] - Full-Duplex

۳-۳-۲- ارتباط دو طرفه هم زمان

در روش دوطرفه هم زمان هر دو واحد Aو B می توانند به صورت هم زمان فرستنده و گیرنده اطلاعات باشند . به طور مثال می توان از طریق دو دستگاه تلفن بدون هیچ مشکلی به صورت هم زمان و دو طرفه ارتباط برقرار کرد . انتقال اطلاعات در تلفن ، نمونه ای از انتقال اطلاعات به صورت دو طرفه هم زمان است .

شکل ۳-۲ شکل ۲-۱ (ب) (ص۱۹) مفاهیم شبکه

۴-۲-سیگنال های اطلاعات

مفهومی را که به انتقال اطلاعات از نقطه ای به نقطه دیگر و هم چنین یک سری ازپالس ها در کامپیوتر اشاره می کند ، سیگنال می نامند . امواج رادیویی وویدیویی نمونه ای از این سیگنال ها هستند .

سیگنال های اطلاعات می توانند به دوصورت دیجیتال یا آنالوگ باشند . سیگنال های آنالوگ شبیه یک موج هستند که در زمان های مختلف مقادیر مختلفی دارند یعنی از زمان شروع موج به جلو ، در هر لحظه این موج مقدار متفاوتی با لحظه قبلی دارد .این موج را معولا به طوری که در شکل ۳-۱ (الف) می بینید روی بردار نمایش می دهند . محور عمودی نمایانگر مقدار عددی موج و محور افقی نمایانگر زمان است.

شکل ۴-۲- شکل ۳- ۱ (الف) (ص۲۰) مفاهیم شبکه

صدای شخصی که در حال صحبت کردن است ، نمونه ای از یک سیگنال آنالوگ می باشد ؛به این صورت که صدا به صورت ممتد تولید شده و بلندی صدا دائما در حال تغییر است .

در مقابل ، سیگنال دیجیتال فقط دوحالت دارد بدین مفهوم که ارزش عددی سیگنال دیجیتال صفر یا یک است ؛یعنی در واحدهای زمانی مختلف فقط دو ارزش عددی متفاوت داریم . اگر بخواهیم مثالی برای یک سیگنال دیجیتال بیاوریم ، می توانیم به یک لامپ اشاره کنیم که فقط دو وضعیت خاموش یا روشن دارد . این موج را روی بردار به صورتی که در شکل ۲-۵ نمایش داده شده است ، می بینید.

شکل ۵-۲-شکل۳-۱ (ب) (ص۲۰)

مفاهیم شبکه

- سیگنال های Periodic و Aperiodic

هردونوع سیگنال های آنالوگ و دیجیتال به دو فرم Periodic و Aperiodicبه کار می روند .

الف -سیگنال های Periodic

اگر الگو یا همان شکل سیگنال ها در فاصله های زمانی مشخص تکرار شود ، به آن سیگنال Periodic می گویند .در سیگنال های اگر الگو کامل شود و در آستانه تکرار قرار گیرد ، به آن یک Cycle یا چرخه می گویند یک Period یا دوره ، به مقدار زمانی می گویند که یک چرخه یا Cycle در آن اتفاق می افتد .

شکل ۶-۲- شکل

۱-۴ (ص۲۱) مفاهیم شبکه

ب-سیگنال های Aperiodic

سیگنال های Aperiodic الگو و شکل مشخصی ندارند و الگوهای آن در فاصله های زمانی غیر قابل پیش بینی تکرار می شوند .

شکل ۷-۲- شکل

۱-۵ (ص۲۱) مفاهیم شبکه

۵-۲-پهنای باند[1]

یکی از مسایلی که به هنگام طراحی و راه اندازی شبکه همواره مورد توجه قرار می گیرد و از درجه اهمیت بالایی برخوردار است ، پهنای باند می باشد . پهنای باند به طور کلی تعریفی است که برای سیستم های انتقال آنالوگ استفاده می شود . هر سیستم انتقال آنالوگ توانایی محدودی در انتقال امواج دارد ؛ بدین صورت که پایین ترین و بالاترین فرکانسی که یک رسانه برای انتقال اطلاعات استفاده می کند ، مشخص است ؛ به طور مثال پایین ترین فرکانس ۳۰۰HZ و بالاترین فرکانس ۳۳۰۰HZ است .

واحد سنجش فرکانس هرتز[2] می باشد .حدفاصل این دو فرکانس یعنی فاصله بین پایین ترین و بالاترین عدد ، پهنای باند رسانه نامیده می شود . رسانه ای با مشخصات ذکر شده فقط قادر به ارسال سیگنال هایی است که در محدوده بین ۳۰۰ و ۳۳۰۰ هرتز قرار گرفته باشند . در واقع پهنای باند ، ظرفیت انتقال اطلاعات به وسیله ی رسانه است .

در سیستم های انتقال دیجیتال ، ظرفیت انتقال اطلاعات با واحد بیت در ثانیه [3] سنجیده می شود . برای مثال می توان به پهنای باند یک مودم اشاره نمود . منظور از مودم ۵۶Kbps این است که پهنای آن ۵۶۰۰۰ بیت در ثانیه می باشد.

---

[1]-Band Width
[2] - Hz
[3] -Bps

از عوامل موثر در پهنای باند طول ، قطر و جنس کابل است . طول کابل با پهنای باند نسبت معکوس و قطر کابل با پهنای باند نسبت مستقیم دارد یعنی هرچه طول کابل بیشتر شود ، پهنای باند کمتر شده و هرچه قطر کابل بیشتر شود ، پهنای باند نیز بیشتر می شود .

برای انتقال اطلاعات به دوروش از پهنای باند استفاده می شود . این دو روش عبارتند از :

۱- تک باند[1]
۲- باند پهن[2]

در روش تک باند از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود ؛ به این معنی که تک باند در هرلحظه فقط می تواند یک سیگنال را از خود عبوردهد ، در نتیجه ارسال نوبتی می شود و اطلاعات پشت سرهم وبه صورت سری ارسال می شوند . به این نوع شبکه تک باند گفته می شود . روش انتقال تک باند دلیل به وجود آمدن مفهوم packet است . از این روش در شبکه های محلی استفاده می شود.

در روش تک باند برای ارسال و در یافت اطلاعات به دورشته کابل نیاز است که یکی از کابل ها وظیفه ارسال اطلاعات را به عهده دارد و کابل دیگر دریافت اطلاعات را انجام می دهد . سیستم انتقال دیجیتال نیز از روش تک باند استفاده می کند.

روش دیگر انتقال ، انتقال باند پهن است. در سیستم انتقال باند پهن ، اطلاعات به صورت آنالوگ ارسال می شوند .به این ترتیب باند پهن می تواند از یک کابل ، یک یا چند سیگنال را به طور هم زمان عبور دهد . هر سیگنال به صورت جداگانه ارسال می شود و تداخلی بین سیگنال های متفاوت به وجود نمی آید . از این روش در شبکه تلویزیون کابلی استفاده می شود . در شبکه های محلی این روش کاربردی ندارد ولی در شبکه های WAN همواره مورد توجه است .

شکل ۸-۲- شکل ۶-۱ (ص۲۲) مفاهیم شبکه

۶-۲- نویز

ازجمله مشکلاتی که در شبکه به وجود می آید ، نویز است . نویز عامل خربی است که شکل سیگنال ها را تغییر می دهد و باعث بروز اختلال می شود .

عوامل مختلفی باعث به وجود آمدن نویز می شوند . تعدادی از این عوامل عبارتند از : حرارت ، القا و هم شنوایی.

حرارت : نویزهایی که در اثر حرارت ایجاد می شوند ، بدین گونه عمل می کنند که حرارت باعث می شود الکترون ها در جهات نامشخص شروع به حرکت

---
[1]- Base band
[2] - Broad band

نمایند ؛ این حرکت گاهی با سیگنال ها هم جهت شده و اندازه و شکل آن ها را که همان الگوی سیگنال هاست ، تغییر می دهد.

القا:نویزهای القایی نویزهایی هستند که موتورهای مکانیکی مثل موتور ماشین یا وسایل الکتریکی مانند موتورهای الکتریکی وسایل خانگی تولید می کنند ، این وسایل شبیه یک آنتن فرستنده عمل می کنند و می توانند نویز را ارسال کنند و کابل شبکه ، شبیه یک آنتن گیرنده نویزهای ارسال شده را در یافت می کند.

هم شنوایی[1]:هم شنوایی اثر میدان های مغناطیسی یک کابل مجاور خود است . نویزهایی که کابل های برق فشار قوی یا رعد و برق ایجاد می کنند نیز از انواع نویزهای القایی محسوب می شوند.

سرعت انتقال اطلاعات : به مقدار اطلاعاتی که در واحد زمان به وسیله ی تجهیزات شبکه ارسال می شود ، سرعت انتقال اطلاعات می گویندو واحد اندازه گیری آن bps است . سرعت انتقال اطلاعات در وسایل مختلف متفاوت است .

به طور مثال کارت های شبکه با سرعت 10Mbps توانایی انتقال ۱۰ مگابیت در ثانیه را دارند و کارت های ۱۰۰Mbps می توانند در ثانیه ۱۰۰ مگابیت اطلاعات به مقصد ارسال کنند . سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم دراد ، هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می شود .

نکته : پهنای باند ، ظرفیت انتقال یک رسانه یا کابل است . در صورتی که سرعت انتقال ، سرعت ارسال اطلاعات در واحد زمان است .

---

[1] -crosstalk

خود آزمايي و تحقيق

۱- سرعت ارسال اطلاعات در كدام يك از روش هاي سري و موازي بيشتر است؟

۲- در كدام يك روش هاي ارسال سريال هم زمان و غير هم زمان كنترل ترافيك امكان پذير است؟

۳- سيگنال چيست؟

۴- تفاوت سيگنال ديجيتال و آنالوگ را بنويسيد و با ذكر دليل مشخص كنيد كيفيت و سرعت كدام يك براي ارسال اطلاعات بهتر است؟

۵- نويز چيست؟ اثر نويز بر روي كدام يك از سيگنال هاي آنالوگ يا ديجيتال بيشتر است؟

۶- تحقيق كنيد كه گذرگاه هاي COM، LPT و USB از چه سيستمي براي انتقال اطلاعات استفاده مي كنند؟

۷- تحقيق كنيد كه واحدهاي Bps و bps چه تفاتي با هم دارند؟

فصل سوم پیکر بندی شبکه و محیط انتقال

هدف های رفتاری
انواع توپولوژي شبکه را شرح دهد.
انواع محيط هاي انتقال را شناسايي كند.
كابل كشي يك شبكه را انجام دهد.
كارت شبكه و وظايف آن را تعريف كند.
كابل رابط بين شبكه و سويیچ را ايجاد كند .
روش هاي دسترسي به خط انتقال را شناسايي كند.

۱-۳- توپولوژي انواع آن

اجزاي سخت‌افزاري در شبكه طبق يك طرح و نقشه بهم متصل مي‌شوند كه به آن اصطلاحاً توپولوژي شبكه مي‌گويند . در ابتدا ممكن است تصور كنيم كه توپولوژي فقط بمعني نقشة فيزيكي و ظاهري شبكه است و چگونگي گردش اطلاعات و همچنين نحوة دسترسي كامپيوترها به محيط انتقال در آن اهميتي ندارد اما اين حالت كافي نبوده و در توصيف و بررسي يك توپولوژي بايد علاوه بر چگونگي اتصال ظاهري ، نحوة تبادل اطلاعات را هم جزو توپولوژي بحساب آورد بنابراين توپولوژي را به شكل زير تعريف مي‌كنيم

تعريف توپولوژي :

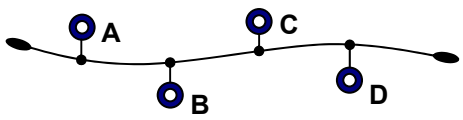
چگونگي اتصال ظاهري اجزا از طريق محيط انتقال به يكديگر .

نحوة دسترسي اجزا به محيط انتقال و گردش اطلاعات مابين آنها .

با اينحال در ادامة مبحث و شرح بيشتر ، گاهي اوقات به يكي از جنبه‌ها توجه بيشتري مي‌كنيم . (ضمناً براي ساده‌تر شدن مبحث ، فرض كنيد كه محيط انتقال از نوع "سيمي" است (كابل) و فعلاً محيطهاي انتقال بي‌سيم را منظور نمي‌كنيم

۱-۱-۳-توپولوژي خطي (Bus) :

جنبة ظاهري : كلية سيستمها از طريق يك قطعه كابل به يكديگر متصل شده و اطلاعات خود را از طريق آن تبادل مي‌كنند . نكتة اصلي در توپولوژي خطی آنست كه يك قطعه كابل بين كلية كامپيوترها مشترك بوده و همه از طريق همان يك قطعه با هم ارتباط دارند .



شكل ۱-۳

چگونگي دسترسي كامپيوترها به خط و نحوة گردش اطلاعات : هر سيستمي كه بخواهد اطلاعاتي را روي خط ارسال كند (مثلاً كامپيوتر A) ابتدا بايد ببيند خط آزاد است يا خير و اگر پاسخ مثبت بود اقدام به ارسال اطلاعات براي كامپيوتر(هاي) مقصد مي‌كند. (اين موضوع بعداً مورد بحث بيشتري قرار مي‌گيرد)

اگر كامپيوتر A بخواهد اطلاعاتي را براي B ارسال كند بقيه كامپيوتر ها (C,D) هم از اين اطلاعات باخبر مي‌شوند چون محيط انتقال مشترك بوده و كنترلي روي آن وجود ندارد . به محض آنكه سيگنال ارسال شده از A روي خط قرار بگيرد ، بسرعت در تمامي محيط انتقال منتشر شده و همه آنرا دريافت مي‌كنند اما بديهي‌است كه فقط گيرنده (گيرندگان) تعيين شده از طرف فرستنده آنرا مورد استفاده قرار مي‌دهد و بقية گيرندگان به آن دسترسي ندارند.

فرض كنيد در يك جمع نشسته‌ايد ، چه با يكنفر صحبت كنيد چه با همه ، نتيجه آنست كه همه صحبتهاي شما را مي‌شنوند اما بديهي‌است فقط فرد يا افرادي كه مخاطب شما هستند از آن استفاده برده و بقيه به امور شخصي خود مي‌پردازند . در اينجا هم علت مشابه است يعني محيط انتقال يا بعبارتي "هوا" براي همة افراد جمع مشترك بوده و سيگنال فرستنده يعني صحبتهاي گوينده به‌محض خروج از دهان او در تمام فضاي اطراف جمع (تا فاصله‌اي محدود و بسته به قدرت فرستنده) منتشر شده و همه آنرا مي‌شنوند.ولي فقط كسي كه مورد پرسش قرار دارد بايد پاسخ بگويد

برخورد يا Collision

فرض كنيم A درحال ارسال اطلاعات براي B باشد ، همزمان C هم ميخواهد اطلاعاتي را براي D بفرستد دراين حالت، چون فقط يك محيط انتقال وجود دارد كه آنهم بين همه مشترك است . به محض آنكه A اطلاعات خود را روي خط بفرستد ، خط اشغال شده و بقيه بايد صبر كنند تا ارسال A به اتمام رسيده و خط مجدداً آزاد شود. البته اگر كامپيوتر A كارش طولاني باشد بايد كار خود را به صورت مقطعي انجام دهد بدين معني كه پس از ارسال قسمتي از اطلاعات، خط را آزاد مي‌كند تا بقيه هم امكان دسترسي و استفاده از خط را داشته باشند .در صورتي كه به طور همزمان C نيز بخواهد براي D اطلاعاتي را ارسال نمايد باعث "تصادم اطلاعاتي" يا Collision شده و سيگنالها بهم مي‌ريزد . بنابر اين در يك لحظة مشخص فقط يك فرستنده مي‌تواند وجود داشته باشد .

البته خيلي از كاربران در شبكه‌هايي با توپولوژي خطی تجربة انتقال همزمان اطلاعات را مابين سيستمهاي مختلف داشته‌اند مثلاً در حالي كه يك فايل بزرگ 1 GByte از كامپيوتر A به B انتقال مي‌يابد ، همزمان C و D هم با يكديگر مشغول تبادل هستند . موضوع چيست ؟ آيا تناقضي با مثال فوق ندارد ؟ بايد گفت : كه در اين حالت كار بصورت مقطعي انجام مي‌شود . قبلاً در مبحث "ويژگي سيستم عامل ها" نيز اشاره شد به "اشتراك زمان" يا "تقسيم زمان" . با استفاده از اين تكنيك ، هر فرستنده كسري از زمان را (يا حجم محدودي از اطلاعات را) براي ارسال درنظر گرفته كه پس از به پايان رسيدن مجبور است خط را آزاد كرده تا ديگران نيز شانس ارسال را داشته باشند . در اين تكنيك هرچند كه بطور واقعي و در يك لحظة مشخص چندين فرستنده با هم وجود ندارند اما در مجموع همه مي‌توانند ارسال اطلاعات خود را با هم به پيش ببرند .

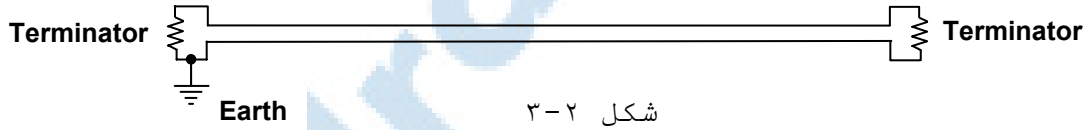
در تكنيك TDM در يك لحظة مشخص ، باز هم بطور واقعي فقط يك فرستنده محيط انتقال را در اختيار مي گيرد ، در عمل با مثالهايي روبرو مي‌شويم كه در آن واحد بطور همزمان و بطور كاملاً واقعي همة فرستنده‌ها با هم روي يك محيط انتقال مشترك كار مي‌كنند . فضاي مادي را بعنوان يك محيط انتقال مشترك در نظر بگيريد . مي‌دانيم كه در يك لحظه صدها فرستندة تلوزيوني ، راديويي ، مخابراتي و . . . امواج خود را در همين فضا پخش مي‌كنند و بعبارتي اطراف ما پر از امواج فرستنده‌هاي گوناگون است و با يكديگر تداخلي هم ندارند ، موضوع چيست ؟ توجيه اين واقعه استفاده از فركانسهاي مختلف براي ارسال داده ها مي باشد بعبارتي هيچ ۲ فرستنده‌اي (در يك محدودة معين) نبايد داراي فركانس يكسان باشند . به اين تكنيك اصطلاحاً "تقسيم فركانسي" يا Frequency Division Multiplexing = FDM گفته مي‌شود .

نتيجه‌گيري : در محيطهاي انتقال مشترك ، هيچ ۲ فرستنده‌اي نمي‌توانند همزمان با هم اقدام به ارسال اطلاعات كنند مگر آنكه از تكنيكهاي TDM يا FDM استفاده شود .

اثر قطع شدن كابل اصلي در توپولوژي خطي

اگر در توپولوژي خطي، قسمتي از كابل اصلي قطع شود تمامي شبكه از كار مي‌افتد بعنوان مثال حد فاصل بين B و C قطع مي‌شود اما ارتباط دو به دو مابين (A,B) و همچنين (C,D) برقرار است ، چرا مي‌گوييم كل شبكه از كار مي‌افتد ؟ علت آن است كه در شبكه‌هاي كامپيوتري از جريانهاي متناوب (Alternative Current = AC) براي ارسال اطلاعات استفاده مي‌شود، همچون امواج دريا . مي‌دانيم كه اگر امواج دريا پس از رسيدن به ساحل با يك مانع همچون تخته‌سنگ برخورد كنند بشدت برگشته و موج رفت و برگشت با يكديگر تصادم مي‌كنند (Collision) و اين تداخل باعث بهم ريختن شكل موج مي‌شود، اما اگر مانعي كه در ساحل وجود دارد يك ساحل شني نرم (يا در ذهن خود تصور كنيد يك ابر اسفنجي بزرگ) باشد ، موج به آرامي جذب ساحل شده و "موج برگشت" آنچنان شدتي براي بهم ريختن "موج رفت" ندارد . در شبكه‌هاي كامپيوتري نيز اوضاع به همين مفهوم است ، چنانچه يك قطعي در كابل رخ دهد ، اين قطعي مصادف با روبرو شدن موج با "هوا" است و مي‌دانيم كه "هوا" عايق الكتريسيته بوده و براي آن حكم تخته‌سنگ را دارد بنابراين موج در "نقطة قطع شده" برگشت كرده و با "موج رفت" تصادم مي‌كند (Collision) و اين برخورد باعث بهم ريختن شكل موج شده و در نتيجه تمامي قسمت را تحت تأثير قرار مي‌دهد .

نتيجه‌گيري كه از اين مبحث مي‌شود آنست كه در توپولوژي خطي بايد به‌گونه‌اي عمل كرد كه در هيچ قسمتي از كابل Collision اتفاق نيافتد و اين شامل ابتدا و انتهاي خط نيز مي‌شود . در طرفين خط بايد ترتيبي اتخاذ كرد تا امواج پس از رسيدن به آنجا اصطلاحاً جذب شده و تداخل درست نكنند و اين امر با قرار دادن مقاومتهايي (Resistor) در ابتدا و انتهاي خط كه اصطلاحاً به آنها Terminator گفته مي‌شود ميسر مي‌شود . مقدار اين مقاومتها بستگي به مشخصات الكتريكي كابل و پارامترهاي ديگر داشته و مثلاً در نوع خاصي از شبكه‌ها 50Ω است.



شكل ۲-۳

مزايا و معايب توپولوژي خطي :

مزايا :

- افزايش و كاهش سيستمها براحتي (تا حد مجاز) صورت مي‌گيرد .
- در كل ساده و كم‌هزينه است .

معايب :

- در صورت قطعي در يك قسمت از كابل اصلي ، تمامي شبكه از كار مي‌افتد ،
- عيب‌يابي آن وقت‌گير است
- نياز به نگهداري و مراقبت بيشتري نسبت به ساير توپولوژيهاي ديگر دارد .

۲-۱-۳-توپولوژي حلقوي (Ring) :

جنبة ظاهري : كلية كامپيوترها در يك حلقه به يكديگر متصل مي‌شوند . بديهي‌است وقتي مي‌گوييم حلقه ، منظور آنست كه آخرين كامپيوتر هم بايد به اولين متصل شود .

شكل ۳-۳

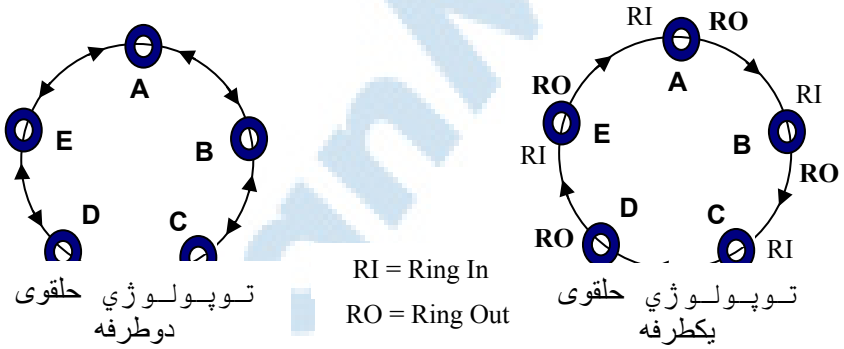
در شكل۳-۳-قسمت ب را نمي‌توان حلقوی به‌حساب آورد زيرا اگر به شكل دقت كنيد ! اين شبكه هيچ فرقي با شبكه خطی ندارد بجز آنكه سر و ته خط به يكديگر وصل شده است و در واقع هيچ مزيتي نسبت به خطی ندارد .

تفاوت توپولوژي خطی با توپولوژي حلقوی) : در توپولوژي حلقوی هر سيستم ، دو گذرگاه (Port) اما در توپولوژي خطی فقط يك گذرگاه براي عبور اطلاعات دارد.

چگونگي دسترسي كامپيوترها به خط و نحوة گردش اطلاعات : از نظر نحوة گردش اطلاعات ، دو نوع توپولوژي حلقوی را مي‌توان متصور شد :

الف) توپولوژي حلقوی يكطرفه : اطلاعات فقط در يك جهت گردش مي‌كند .

ب) توپولوژي حلقوی دوطرفه : اطلاعات در هردو جهت مي‌تواند گردش كند .



شكل ۳-۴

بزودي خواهيم ديد كه حلقوی دوطرفه در واقع حالت خاصي از توپولوژي Mesh است ، لذا در ساير متون وقتي صحبت از حلقوی مي‌شود عموماً منظور حلقوی يكطرفه است مگر صراحتاً خلاف آن ذكر شود .

مزايا و معايب حلقوی (يكطرفه) نسبت به خطی :

مزيت : در بخش "روشهاي دسترسي به محيط انتقال" خواهيم ديد كه نحوة گردش اطلاعات در حلقوی نسبت به خطی داراي مزاياي از قبيل اولويت‌بندي و زمانبندي است كه خطی از آن محروم است .

معايب :

۱. مصرف كابل در آن نسبت به توپولوژي خطی بيشتر است !
۲. همچون توپولوژي خطی اگر يك قسمت از حلقه قطع شود ، كل حلقوی از كار مي‌افتد البته نه بدليل Collision ، بلكه بدين سبب كه اطلاعات قادر به گردش كامل نخواهد بود .

درواقع قانون گردش اطلاعات در حلقه هاي يكطرفه بگونه اي طراحي شده كه اولاً هر اطلاعاتي كه از يك سيستم خارج مي‌شود بايد دور زده و سرجاي اول خود برگردد ، ثانياً همة سيستمها بايد قادر به تبادل اطلاعات باشند . بعنوان مثال در شكل حلقوی يكطرفه دقت كنيد ، اگر حد فاصل بين A و B قطع شود درآنصورت هرچند ممكن است تصور شود كه B مي‌تواند براي C ، D ، E و A اطلاعات بفرستد، اما عكس آن امكانپذير نيست و اين بمعناي آنست كه همة سيستمها نمي‌توانند به تبادل اطلاعات بپردازند، در نتيجه هردو قانون فوق نقض شده و حلقه بطور كامل غير قابل استفاده مي‌شود .

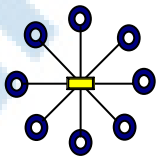
نكته : مشكل فوق در حلقه هاي دوطرفه (كه حالت خاصي از Mesh محسوب مي‌شوند) وجود ندارد .

پرسش: چرا در توپولوژی حلقوی (اعم از يكطرفه يا دوطرفه) ، از Collision بعنوان عاملي بازدارنده ياد نمي‌شود ؟

۳-۱-۳-توپولوژي ستاره اي (Star) :

- جنبة ظاهري : كلية كامپيوترها به يك نقطة مركزي بنام Hub متصل مي‌شوند.

نكته : واژة Hub بطور كلي يعني "نقطة مركزي" و نحوة عملكرد اين "نقطة مركزي" و همچنين نام دقيق آن بستگي به نوع شبكه اي دارد كه درآن استفاده مي‌شود. در اين بخش هرگاه صحبت از Hub مي‌شود منظور استفاده از آن در نوع خاص و رايجي از شبكه ها بنام شبكة Ethernet بوده كه موضوع فصول بعدي است.



شكل ۳-۴

چگونگي دسترسي كامپيوترها به محيط انتقال و گردش اطلاعات

بسته به نوع Hub ، نحوة گردش اطلاعات به دوحالت متفاوت انجام می شود :

- به‌محض‌آنكه يك سيستم اطلاعاتي را ارسال كند ، Hub اشغال شده و سيستمهاي ديگر نمي‌توانند بطور همزمان فرستندة اطلاعات باشند (همانند گردش اطلاعات در توپولوژي خطي) . دقت كنيد كه Hub ، خود بعنوان بخشي از محيط انتقال و توپولوژي بشمار مي‌رود .
- چنانچه يك سيستم اطلاعاتي را براي يك مقصد مشخص بفرستد ، بقية مسيرها براي عبور همزمان ديگر سيستمها باز هستند و اگر اطلاعاتي را براي همه بفرستد بديهي‌است كه همة خروجيها اشغال مي‌شوند. به اين نوع هاب مخصوص اصطلاحاً Switch Hub ، Hub Switch يا به‌اختصار Switch گفته مي‌شود. امروزه عمدتاً در شبكه‌هاي كامپيوتري با توپولوژي ستاره‌اي بجاي هاب معمولي از سوييچ استفاده مي‌شود كه از ويژگي هاي آن عملكرد هوشمندانه در پيدا كردن مقصد نسبت به Hub مي باشد.

در يك شبكه ، اگر ارسال اطلاعات فقط به سمت يك مقصد مشخص باشد اصطلاحاً واژة Unicast و اگر ارسال اطلاعات براي چند سيستم مشخص باشد واژة Multicast و اگر همگان مورد خطاب قرار گيرند واژة Broadcast بكار مي‌رود.

اگر مسير ارتباطي بين هاب و يك كامپيوتر قطع شود ، Collision حاصله در اين قسمت باعث تأثيرگذاري در كل شبكه نمي‌شود معمولاً طراحي اكثر هابهايي كه امروزه ساخته مي‌شود بگونه‌ايست كه اصطلاحاً "اجازة عبور Collision" را به خطوط ديگر نمي‌دهد.

در توپولوژي ستاره‌اي كه از يك هاب معمولي درآن استفاده مي‌شود ، اگر A اطلاعاتي را به مقصد B بفرستد ، ديگر سيستمها نيز از آن آگاهي مي‌يابند زيرا همانطور كه گفته شد، چگونگي گردش اطلاعات اگر هاب معمولي باشد مانند توپولوژي خطي است.در حالي كه در سوييچ، فقط گيرندة مربوطه اطلاعات را دريافت مي‌كند ، مگرآنكه گيرنده اصطلاحاً "همگان" باشند يا در واژه‌هاي كامپيوتري مقصد “Broadcast” باشد.

مزايا و معايب توپولوژي ستاره ای نسبت به توپولوژي خطي :

مزايا

- قطعي يك خط بطور معمول بقية شبكه را تحت تأثير قرار نمي‌دهد.
- اگر از Switch استفاده شود امكان تبادل اطلاعات دوبدو بصورت همزمان وجود دارد ، در نتيجه حجم ترافيك بيشتري در واحد زمان مي‌توانند انجام شود.
- اگر از Switch استفاده شود چون ترافيك مقصد به يك ايستگاه روي گذرگاههاي (Ports) ديگر ارسال نمي‌شود لذا ترافيك ناخواسته كاهش يافته و ضريب ايمني در تبادل اطلاعات افزايش مي‌يابد.

معايب

- اگر به‌هر دليلي "نقطة مركزي" از كار بيافتد ، كل شبكه از كار باز مي‌ايستد ، به‌همين دليل معمولاً Hub را از نظر فيزيكي در يك تابلوي مخصوص معروف به Rack نصب كرده و Rack را در يك مكان مطمئن و با شرايط محيطي مناسب قرار مي‌دهند. در شبكه‌هايي كه ضريب حساسيت آنها بيشتر است ، تركيبي از دو يا چند سويچ را در توپولوژي Mesh قرار داده و بدين‌ترتيب اگر يكي از سويچها از كار بيافتد ، سويچهاي ديگر بلافاصله وارد عمل شده و ترافيك از طريق آنها به عبور خود ادامه مي‌دهد. (Fault Tolerance)
- مصرف كابل و بطور كلي هزينة پياده‌سازي آن نسبت به خطي بيشتر است . البته در عوض هزينة نگهداري و رفع عيب (Maintenance & Trouble Shooting) پايينتر است زيرا كمتر دچار مشكل شده و عيب‌يابي درآن ساده‌تر و سريعتر انجام مي‌شود.

۴-۱-۳-توپولوژي مش (Mesh) :

جنبة ظاهري : در هر سيستم به تعداد لازم ، سخت‌افزار شبكه (Network Interface) نصب شده و همگي مستقيماً بصورت ۲ به ۲ به يكديگر متصل مي‌شوند. البته اين حالت ايده‌ال بوده كه اصطلاحاً گراف كامل (Complete Mesh) خوانده مي‌شود.

شكل ۳-۵ (ص ۳۸ مفاهيم شبكه)

در عمل ممكن است ارتباط ۲ به ۲ براي همه امكان‌پذير نباشد لذا توپولوژي به حالت يك گراف ناقص درمي‌آيد (Partial Mesh)

شكل ۳-۶

۲. چگونگي دسترسي كامپيوترها به محيط انتقال و گردش اطلاعات : چون هر سيستم ارتباط دوطرفه‌اي با بقيه داشته و از طرفي بيش از يك مسير براي رسيدن به مقصد وجود دارد لذا پس از انتخاب مسير بهينه ، اطلاعات به مقصد مي‌رسد. در توپولوژي مش بحث جديدي بنام مسيريابي Routing مطرح مي‌شود و به هر سيستمي كه كار مسيريابي را انجام دهد اصطلاحاً مسيرياب "Router" گفته مي‌شود.

مسير ياب(Router) : مسير ياب يا روتر به سخت‌افزاري گفته مي‌شود مجهز به حداقل ۲ كارت شبكه (Network Interface) كه نرم‌افزار مسيريابي (Routing) روي آن فعال شده و كار انتخاب مسير بهينه و هدايت ترافيك را روي اطلاعات انجام مي‌دهد. چون روتر محل عبور و تلاقي مسيرهاي مختلف براي تبادل ترافيك است لذا علاوه بر "پليس راهنمايي و رانندگي" ، در برخي از روترها "پليس ايست-بازرسي" نيز وجود داشته ، نوع و محتواي ترافيك را كنترل مي‌كند. بعبارت فني عمليات Filtering و Firewall را هم انجام مي‌دهند.

مثال۱ : يك كامپيوتر شخصي شامل يك كارت شبكه و مودم بهمراه نرم‌افزار مسيريابي را مي‌توان يك روترناميد.

مثال ۲ : يك كامپيوتر شخصي مجهز به چندين كارت شبكه يا مودم بهمراه نرم‌افزار مسيريابي را مي‌توان يك روتر ناميد.

مثال ۳ : سخت‌افزارهاي خاصي وجود دارند بهمراه نرم‌افزار مربوطه كه فقط بعنوان روتر استفاده مي‌شوند مانند روترهاي ساخت كمپاني Cisco .

مزايا و معايب توپولوژي Mesh نسبت به ساير توپولوژيها :

مزيت:چون بيش از يك مسير براي هدايت ترافيك وجود دارد بنابراين به احتمال زياد ، قطعي در يك مسير باعث اختلال كلي در ارتباط نمي‌شود و بالاخره شانسي براي رسيدن به مقصد وجود دارد ضمن آنكه بعضي از روترها در حالت عادي ترافيك را روي چندين مسير تقسيم مي‌كنند و بنابراين حجم تبادلات نيز افزايش مي‌يابد. خلاصه آنكه توپولوژي مش داراي ويژگي Redundancy يا Fault Tolerance و همچنين Load Balancing است

معايب Mesh نسبت به ساير توپولوژيها : بديهي است كه پيچيده‌تر و پرهزينه‌تر از بقيه است.

اصولاً انتخاب توپولوژي ربطي به ابعاد و گستردگي فيزيكي شبكه (LAN-WAN) ندارد اما بديهي‌است كه هرنوع توپولوژي را مي‌توان چه در LAN و چه در WAN استفاده كرد اما باتوجه به اينكه احتمال تأثيرگذاري عوامل بازدارنده در شبكه‌هاي WAN نسبت به LAN بيشتر است لذا معمولاً در شبكه‌هاي WAN از توپولوژي Mesh استفاده شده و خطی,ستاره ای,حلقوی را در LAN بكارمي‌برند. البته ستاره ای در WAN هم كاربرد دارد.

شبكه حلقوی دوطرفه (Bi-Directional)را مي‌توان حالت خاصي از Mesh به حساب آورد زيرا چنانچه اقطار يك مش كامل را حذف كنيم شكل حاصله يك مش ناقص خواهد شد كه همان شبكه حلقويدوطرفه است. رينگهاي دوطرفه در شبكه‌هاي صنعتي كه معمولاً Campus LAN هستند بكار مي‌رود. در اينگونه شبكه‌ها توپولوژي ستاره اي به‌تنهايي پاسخگوي سرعت و پايداري نبوده لذا مش وارد عمل مي‌شود . از طرفي چون "مش كامل" بسيار پيچيده و پرهزينه است بنابراين از مش‌هاي ناقص براي پياده‌سازي توپولوژي استفاده مي‌شود و شبكه حلقويدوطرفه يكي از بهترين انتخابها در اين زمينه بشمار مي‌رود.

۲-۳ محيط‌هاي انتقال

براي آنكه ايستگاه ها ي مختلف در يك شبكه بتوانند با يكديگر ارتباط برقرار كنند نياز به يك "محيط انتقال" مانند يك قطعه سيم دارند..

تعريف: به هر رسانه‌اي كه بتواند اطلاعات را به گردش درآورده و هدايت كند اصطلاحا" محيط انتقال مي‌گوييم.

با ذكر چند مثال مي خواهيم محيط انتقال را توضيح دهيم

مثال ۱: وقتي صحبت مي‌كنيم، امواج صوتي از طريق هوا بين گوينده و شنونده انتقال مي‌يابد در اين مثال "هوا" بعنوان محيط انتقال محسوب مي‌شود.

مثال ۲: يك فرستندة تلويزيوني، امواج الكترومغناطيسي را از طريق آنتن در فضاي اطراف خود پخش مي‌كند و اين امواج با سرعتي تقريباً معادل با سرعت نور به اطراف انتقال پيدا مي‌كنند لذا "فضاي مادي" بعنوان محيط انتقال محسوب مي‌شود.

مثال ۳: اطلاعاتي را با روشن و خاموش كردن يك منبع توليد نور از طريق يك رشته كابل نوري كه از تركيبات فشردة مخصوص ساخته شده است و نور را از خود هدايت مي‌كند ارسال مي كنيم كابل نوري در اينجا به عنوان محيط انتقال محسوب مي‌شود

مثال ۴: وقتي بوسيلة گوشي FF با فردي كه كنار در ورودي ايستاده صحبت كنيد صداي ما تبديل به انرژي الكتريكي شده و به وسيله ی الكترونها از طريق سيم مسي جريان مي‌يابد در اينصورت "سيم مسي" بعنوان محيط انتقال محسوب مي‌شود.

۱-۲-۳- گروه‌بندي محيطهاي انتقال

محيط هاي انتقال را مي توان به دو دسته كلي سيمي و بي سيم تقسيم كرد.

محيط انتقال سيمي(Wired)

- يك يا چند رشته سيم از جنس فلزات هادي يا آلياژهاي آنها مانند مس، آلومينيوم، . . . . براي انتقال الكتريسته.
- يك يا چند رشته سيم از جنس تركيبات مخصوص مانند پلاستيك فشرده و سيليس براي انتقال نور.

بي‌سيم(Wireless) (انتشار از طريق فضاي مادي)

- استفاده از نور مادون قرمز (Infra Red) مانند كنترل تلويزيون.
- استفاده از نور ليزر (Laser) كه در واقع تك فركانس است.
- استفاده از امواج راديويي(Radio Waves) در فركانسهاي مختلف مانند راديو، تلويزيون، ماهواره، مخابرات مايكروويو، بي‌سيمهاي شخصي و نظامي و ...

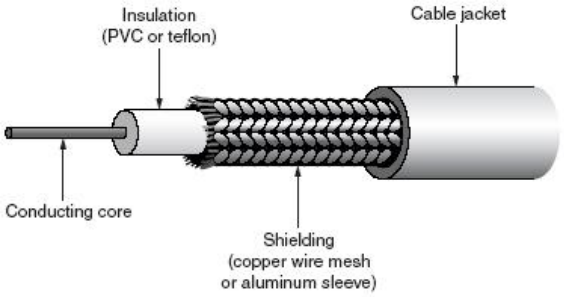
نكته: هر چند بوسيلة انتقال صوت (مثال۱) از طريق هوا هم مي‌توان اطلاعات را رد و بدل كرد اما اين شيوه در شبكه‌هاي كامپيوتري بدليل محدوديتهايي كه دارد استفاده نمي‌شود

۲-۲-۳- بررسي محيطهاي انتقال "سيمي" يا "كابلي" (Wired)

در شبكه‌هاي كامپيوتري ۳ نوع سيم (كابل) متداول بوده است:
الف) كابل "هم محور" يا Coaxial مانند كابل آنتن تلوزيون.
ب) كابل "زوج بهم تابيده" يا Twisted Pair مانند سيم تلفن.
ج) كابل "فيبر نوري" يا Fiber Optic كه معمولا" در سرعتهاي زياد يا مسافتهاي طولاني كاربرد داشته و نويز روي آن اثر ندارد.

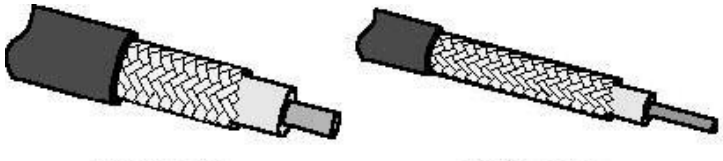
.

۳-۲-۳- كابل هم محور : در واقع كلمة Coaxial تركيبي است از Co + axial يعني "هم‌محور". علت اين نامگذاري از شكل پيداست:



شكل۷-۳

جريان الكتريكي از طريق هسته از سمت فرستنده به گيرنده گسيل شده و مسير برگشت خود را از طريق حفاظ(Shield) طي مي‌كند. حفاظ علاوه بر تأمين مسير برگشت براي الكترونها، وظيفة ديگري را نيز به عهده دارد و آن جذب نويزهاي حاصل از "القاي امواج الكترومغناطيسي در فضا" و هدايت آنها به زمين (Earth) است تا بدينوسيله از ايجاد نويز در هسته جلوگيري كند. البته يادمان باشد كه جلوگيري از القاي نويز روي هسته به وسيله ی حفاظ بصورت ۱۰۰% نبوده و نسبي است چنانچه شدت ميدان الكترو مغناطيسي اطراف كابل كابل هم محور قوي باشد در آنصورت حفاظ هم مقاومت چنداني نمي تواند بكند و اطلاعات هسته نويزي و مخدوش مي‌شود.
در كابلهاي هم محور هر چه قطر هسته و متناسب با آن غلظت بافت الياف فلزي حفاظ بيشتر باشد، مقاومت كابل در برابر عبور الكتريسته كمتر شده و لذا شدت جريان براي عبور با مانع كمتري مواجه مي‌شود و اين امر سبب مي‌شود در مسافتهاي طولاني‌تري بتوان از آن استفاده كرد از اين رو در شبكه‌هاي كامپيوتري دو نوع كابل هم محور از نظر ضخامت وجود دارد:
نازك، با قطر حدوداً 6.5mm معروف به Thin .
ضخيم، با قطر حدوداً 13mm معروف به Thick.



شكل۷-۳

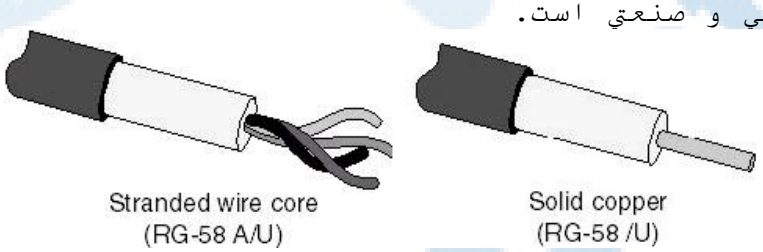
كابل Thin از Thick سبكتر و انعطافپذيرتر بوده و ارزانتر است اما در فواصل كوتاهتري بكار ميرود از طرفي وزن كابل Thick بعلت قطر بيشتر آن زياد شده قيمت آن افزايش يافته، انعطاف پذيري آن كمتر شده و كار با آن سختتر ميشود اما در عوض نسبت به Thin در فواصل طولانيتري استفاده ميشود.

سابقاً نوع خاصي از كابل كواكس Thin معروف به RG58 در شبكه هاي كامپيوتري استفادة بيشتري داشت كه آنرا دقيق تر بررسي ميكنيم. RG58 در سه مدل موجود است:

۱) RG58 U : كه در آن، هسته تك رشته (مفتولي) است. در اصطلاح معروف است به Solid Core

۲) RG58 A/U : كه در آن، هسته چند رشته (افشان) است. در اصطلاح به آن Stranded Core ميگويند كه انعطاف پذيري بيشتري نسبت به RG58 U دارد.

۳) RG58 C/U : نسخة نظامي A/U، در اصطلاح Military Version of A/U كه مناسب براي كاربرد در محيطهاي نظامي و صنعتي است.

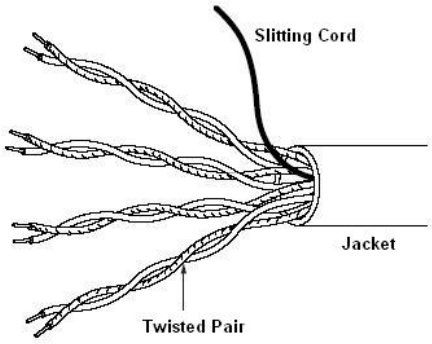


شكل۷-۳

نكته: بطور كلي سيمهاي مفتولي و افشان علاوه بر تفاوت در انعطافپذيري، در مشخصة الكتريكي (تحت فركانسهاي زياد) نيز با هم فرق دارند (اثر پوسته اي يا Skin Effect) اما اين تفاوت در شبكه هاي كامپيوتري با توجه به فركانس مورد استفاده و شدت جريان پايين چندان مد نظر نبوده و فقط مشخصة مكانيكي يعني انعطافپذيري مهم است.

۴-۲-۳- كابل Twisted Pair = TP :

اين كابل كه در مخابرات كاربرد فراواني دارد تشكيل شده از يك زوج سيم كه بهم تابيده شده اند :



شكل۸-۳

علت تابيدن سيمها بهم انست كه اولاً ميداني را در اطراف خود القا نكنند ثانياً اثرات نويز القا شده روي خود را خنثي كنند. در عمل كابلهاي TP از چندين زوج بهم تابيده تشكيل ميشوند و هر زوج براي يك كانال مخابراتي مورد استفاده قرار ميگيرد. البته ميتوان از تكنيكهاي TDM يا FDM استفاده كرده و چندين كانال مخابراتي را نيز بطور همزمان از يك زوج عبور داد.

مزايا و معايب اين كابل نسبت به هم محور به اختصار عبارتند از:

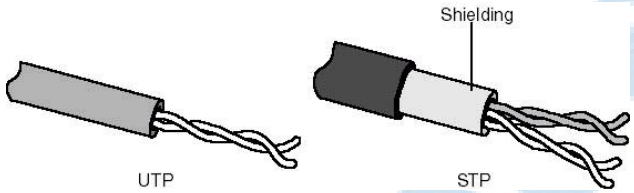
مزيت: ارزانتر بوده و در شبكة مخابرات به وفور از آن استفاده ميشود.

معايب : ۱ - نسبت به هم محور ، نويز روي TP اثر بيشتري دارد.

۲ - بروز يك مشكل جديد بنام هم شنوايي يا Cross Talk.

مزيت ياد شده باعث شد تا طراحان شبكه، ايدة استفاده از اين كابل را در شبكه هاي كامپيوتري در ذهن خود پرورش دهند و اين امر باعث پيدايش مودمها شد. مودم وسيله اي است كه اجازه مي‌دهد تا از طريق بستر مخابراتي موجود كه مملو از كابلهاي TP است يك شبكة كامپيوتري در ابعاد WAN (و البته سرعت نسبي پايين) برقرار كنيم.
سپس متخصصان شبكه به فكر استفاده از كابلهاي TP با كيفيت بهتر و بطور مستقل از مخابرات در ابعاد شبكه هاي LAN افتادند و اين امر با پيدايش كارتهاي شبكة مناسب كه كابل TP به آنها متصل مي‌شد محقق شد. امروزه اكثر شبكه هاي LAN از اين كابل بهره برده و توپولوژي آنها نيز ستاره ای است.
از طرفي عيب ياد شده در اين كابلها باعث شد تا نوعي خاص از TP كه داراي حفاظ نيز باشد ساخته شود كه به كابل STP معروف شد. بنابراين كابلهاي TP درحالت كلي به دو نوع تقسيم مي‌شوند:

UTP = Unshielded Twisted Pair
STP = Shielded Twisted Pair



شكل ۹-۳

مورد مصرف كابلهاي STP نسبت به نوع معمولي آن يعني UTP در محيطهايي است كه اثرات ميدانهاي الكترومغناطيسي در آنها قويتر است. البته بديهي است كه يك كابل STP نسبت به كابل هم محور Thin گرانتر است و لذا مزيت آن يعني "ارزانتر بودن" زير سوال مي‌رود اما با توجه به اينكه در شبكه هاي LAN ابعاد محدود بوده وفواصل كوتاه است اين "گراني" چندان خود را نشان نمي‌دهد.
در هرصورت تكنولوژي، سرمايه گذاري خود را در شبكه هاي كامپيوتري بر روي كابلهاي TP اعم از UTP يا STP گسترش داده و كار چنداني با هم محور ندارد.
اكثر كابلهاي TP متداول در شبكه از۴ زوج كه در كنار يكديگر تحت يك پوشش كلي قرار گرفته اند. از طرفي گفتيم كه بهم تابيدن سيمها باعث مي‌شود تا ميداني در اطراف سيمها القا نشود اما اين موضوع قطعي نبوده و به هر حال يك زوج سيم بهم تابيده كه از آن جرياني عبور مي‌كند باعث القاي ميداني هر چند ضعيف در اطراف خود مي‌شود و همين مي‌تواند سبب ايجاد اختلال در زوجهاي مجاور شود. زوجهاي مجاور نيز هر كدام بنوبة خود چنين مشكلي را براي بقيه بوجود مي‌آورند. به اين پديده اصطلاحاً همشنوايي يا Cross Talk گفته مي‌شود و اكثر ما تجربة آنرا بصورت "خط روي خط افتادن" در مخابرات داشته ايم. بعنوان مثال ديگري از اين پديده، يك جمع كوچك را تصور كنيد مثلاً شامل ۸ نفر كه افراد دو به دو گروه‌بندي شده و همزمان اعضاي هر گروه با يكديگر صحبت مي‌كنند. هر چقدر هم افراد آهسته صحبت كنند با اينحال روي بقيه تأثير گذاشته و براي ديگران حكم نويز و پارازيت و اختلال را دارد. براي كاهش اين اثر چه پيشنهادي داريد؟
پاسخ را در تبصرة ۵ همين بخش خواهيم ديد.
كابلهاي TP صرف نظر از UTP يا STP، بر اساس حداكثر سرعت و نوع كاربردي كه در شبكه ها دارند به چند دسته يا Category تقسيم مي‌شوند كه عبارت است از:

جدول ۱-۳

نام گروه	سرعت	كاربرد
Category 1 = Cat 1	-	مورد مصرف در شبكه هاي مخابراتي
Category 2 = Cat 2	4 Mbps	مورد مصرف در شبكه هاي با سرعت حداكثر

مورد مصرف در شبکه هاي با سرعت حداکثر	10 Mbps	Category 3 = Cat 3
مورد مصرف در شبکه هاي با سرعت حداکثر	* 16 Mbps	Category 4 = Cat 4
مورد مصرف در شبکه هاي با سرعت حداکثر	** 100 Mbps	Category 5 = Cat 5
مورد مصرف در شبکه هاي با سرعت از	100 Mbps – تا سقف 1000 Mbps	Category 5e = Cat 5e
مورد مصرف در شبکه هاي با سرعت	1 Gbps – و بالاتر	Category 6 = Cat 6

*: کابل CAT 4 توانائي انتقال تا نرخ 20 Mbps را نيز دارد اما در عمل شبکه هايي که از اين کابل بهره مي‌برند تا حداکثر 16 Mbps از آنرا استفاده مي‌کنند.
**: در برخي از متون به 1000 Mbps نيز اشاره شده اما بهتر است اطمينان نکرده و براي سرعتهاي 1000 از کابلهاي با نمرة بالاتر مثلاً Cat5e يا Cat 6 استفاده کنيم.

بطور کلي در مورد همة کابل هاي فوق دقت داشته باشيد که سرعتهاي نوشته شده الزاماً بيانگر حداکثر ظرفيت کابل نيست بلکه بيانگر سرعت تجهيزاتي است که از آنها براي انتقال اطلاعات استفاده مي‌کنند. بعنوان مثال يك زوج از Cat3 تا حدود 30 Mbps نيز مي‌تواند اطلاعات را از خود عبور دهد و در نوع خاصي از شبکه ها که بعداً به آن اشاره خواهيم کرد، ۳ زوج از يك کابل Cat3 با هم مي‌توانند تا 100 Mbps اطلاعات را عبور دهند. کابل Cat3 در مجموع داراي ۴ زوج يا ۸ رشته سيم است.

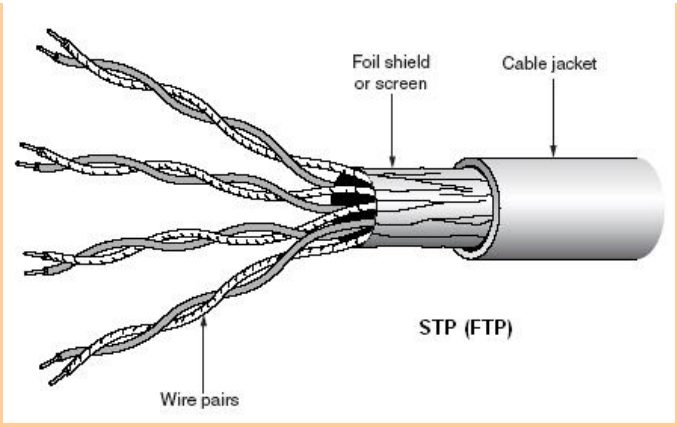
در مورد Cat 1 سرعت را عنوان نکرديم؟ علت آنست که براي انتقال اطلاعات از طريق شبکة مخابرات معمولاً از مودم استفاده مي‌کنيم و مودمها نيز انواع گوناگون با تکنولوژيها و استانداردهاي متفاوت داشته و سرعت در آنها متنوع است. همچنين سرعت در شبکه هاي مخابراتي که در واقع از ديدگاه کامپيوتري يك شبکة WAN محسوب مي‌شود بستگي به فاصله، شرايط محيطي، کيفيت خطوط و اتصالات و همچنين تقويت کننده هاي بين راه دارد. لذا ترجيح داديم حرفي از سرعت به ميان نياوريم با اين حال از تجارب شخصي هر کس مي‌داند که مثلاً با استفاده از مودمهاي Dial up از نوع آنالوگ و در صورت مطلوب بودن شرايط مي‌توان تا سرعتهاي حدوداً 33 Kbps دست پيدا کرد و يا با استفاده از مودمهاي DSL که در واقع ديجيتالي هستند مي‌توانيم در فواصل کوتاه (تا حداکثر ۳ الي ۵ کيلومتر) و شرايط مطلوب به سرعتهاي حدوداً 2 Mbps هم دسترسي داشته باشيم.

رايج ترين شبکه هاي LAN به لحاظ سابقة تاريخي آنها تا به امروز عبارتند از:

کابل Thin Coax RG58 با سرعت 10 Mbps در توپولوژي خطي : تقريباً منسوخ شده اند.
کابل Twisted Pair Cat3 با سرعت 10 Mbps در توپولوژي ستاره ای : تقريباً منسوخ شده اند.
کابل TP Cat5 يا Cat5e با سرعت 100 Mbps در توپولوژي ستاره ای : امروزه بسيار رايج است.
کابل TP Cat5e يا Cat6 با سرعت 1000 Mbps در توپولوژي ستاره ای : رفته‌رفته جاي خود را باز مي‌کنند.

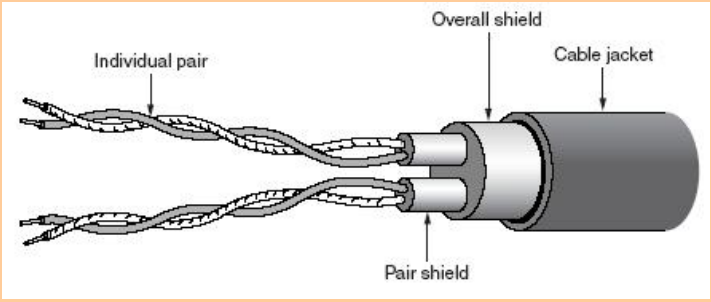
مطالعه آزاد

ممکن است به کابلهاي TP که از فويل آلومينيوم بعنوان حفاظ استفاده مي‌کنند اصطلاحاً FTP گفته شود.



شكل ۳-۱۰

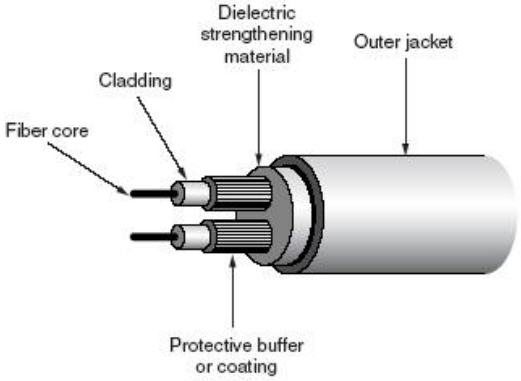
برخي از كابلهاي TP براي هر زوج نيز يك حفاظ در نظر مي‌گيرند اعم از كلاف سيمي بافته شده (زره) يا فويل آلومينيوم و مزيت آنهم در آنست كه Cross Talk را كم مي‌كند. در برخي علاوه برآنكه هر زوج داراي حفاظ خاص خود است، يك حفاظ كلي نيز روي همة آنها كشيده مي‌شود و در نتيجه واژه‌هاي SSTP، SFTP، FSTP ، FFTP براي توصيف آنها بكار مي‌روند. در هرصورت هرچه كه باشند داراي حفاظ بوده و در محيطهاي نويزي تا حد مجاز تعريف شده مي‌توانند بكار روند.



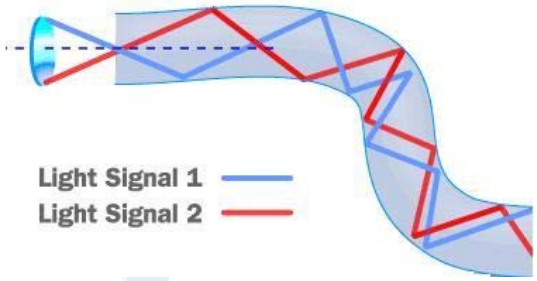
شكل ۳-۱۱

۳-۲-۵- كابل نوري (Fiber Optic = FO) :

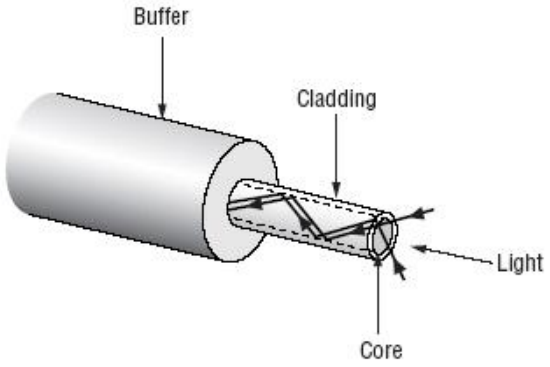
فيبر نوري از تركيبات خاص پلاستيك فشرده يا سيليس ساخته مي‌شوند و مي توانند پالس هاي نور را از يك سمت به سمت ديگر هدايت كنند (شكل ۳-۱۲).



شكل۳-۱۲ ساختمان فيبر نوري

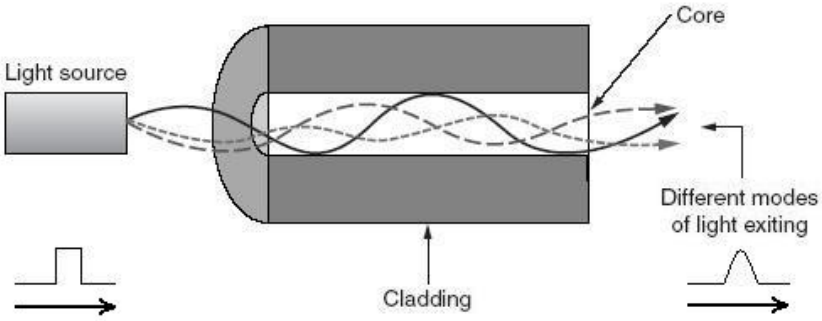


شكل۱۳-۳- هدايت نور در فيبر نوري



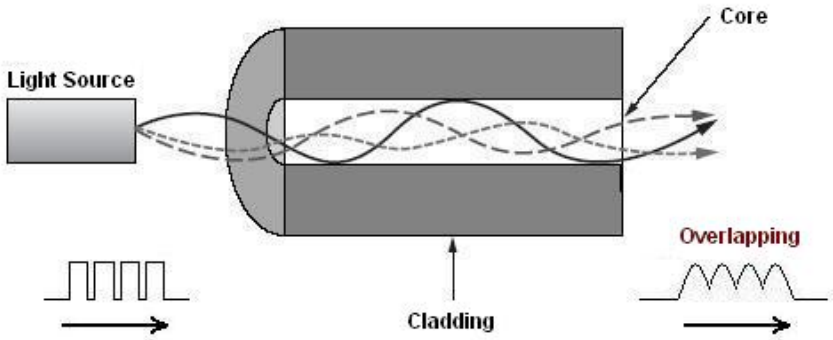
شكل۱۴-۳

قسمت مركزي كابل كه نور از آن عبور مي‌كند معروف به هسته (Core)بوده و لاية انعكاس دهنده نيز به Clad مشهور است. جنس Core/Claddig هردو يكي است و تفاوت در ضريب شكست شان است . همانطور كه از شكل ۱۵-۳ نشان داده شده است وقتي يك پالس نوري از ابتداي خط ارسال مي‌شود بدليل اختلاف مسير در شعاعهاي مختلف نور، پالس خروجي به همان شكل نبوده و كمي تغيير شكل مى دهد:



شكل۱۵-۳

حال چنانچه فركانس فرستنده از حد معيني بيشتر شود پالسهاي خروجي با يكديگر همپوشاني پيدا مي‌كنند (Overlapping) و اين باعث بروز خطا مي‌شود.
چنانچه ضخامت هسته طوري باشد كه اجازة عبور چندين شعاع نوري را در زواياي مختلف بدهد به آن كابل نوري MM = Multi Mode گفته مي‌شود.



شكل ۳-۱۶

مزاياى كابل نورى با توجه به خصوصيات آن عبارتست از:

- امكان استفاده درفواصل طولانيتر.
- نرخ انتقال بيشتر.
- عدم نويزپذيري نسبت به ميدانهاي الكترومغناطيسي.
- امنيت بيشتر. سرقت اطلاعات از سيمهاي فلزي بوسيلة اتصال مستقيم يك سيم بصورت انشعاب و يا بطور غير مستقيم از طريق القاي امواج، امريست امكانپذير، اما در مورد فيبرهاي نوري بدليل ظريف بودن هسته نميتوان براحتي و بدون صرف وقت و امكانات از كابل انشعاب گرفت ضمن آنكه القاي امواج نيز در مورد فيبر نوري بيمعني است. بنابراين سرقت اطلاعات از فيبرنوري بسيار دشوارتر از سيمهاي فلزي است و در نتيجه امنيت انتقال اطلاعات از طريق فيبرنوري بيشتر است.
- ارتباط راحت مابين ساختمانهاي مختلف كه داراي چاههاي ارت مستقل از يكديگرند. (عدم بروز پديدة Ground Loop)

فرض كنيد كه ارتباط شبكه اي مابين ۲ ساختمان از طريق كابل هم محور باشد. براي دفع نويز بسمت زمين و جلوگيري از تأثيرگذاري آن روي اطلاعات، قسمت حفاظ كابل هم محور به Earth متصل ميشود. حتي اگر حفاظ مستقيماً به ارت وصل نباشد، از طريق كانكتور متصل به آن و بدنة يكي از كامپيوترها كه با ارت ارتباط داشته باشد به زمين وصل ميشود. چنانچه چاه ارت هردو ساختمان يكي باشد مشكلي بروز نميكند اما اگر ساختمانها داراي چاههاي ارت جداگانه اي باشند درآنصورت بعلت مغايرت بين مشخصات فيزيكي چاهها از نظر رطوبت نسبي و . . . ، جرياني ضعيف از يكسو به سوي ديگر برقرار ميشود كه اصطلاحاً به آن Ground Loop گفته ميشود. اين جريان در واقع خود بعنوان يك عامل مزاحم محسوب ميشود. حال اگر ارتباط مابين ساختمانها را از طريق فيبرنوري برقرار كنيم Ground Loop در كار نخواهد بود چون از فيبرنوري اساساً الكتريسيته عبور نميكند.

تحقيق، در مورد تركيبات روكش انواع كابلها ى نورى و خصوصيات آن تحقيق كنيد

ضد جوندگي: Anti Rodent

ضد رطوبت و آب: Anti Humidity, Water Blocking

روكش مسلح: Armored

ضد توليد گاز سمي: Halogen Free (Plenum Grade)

۳-۳- كابل كشي UTP

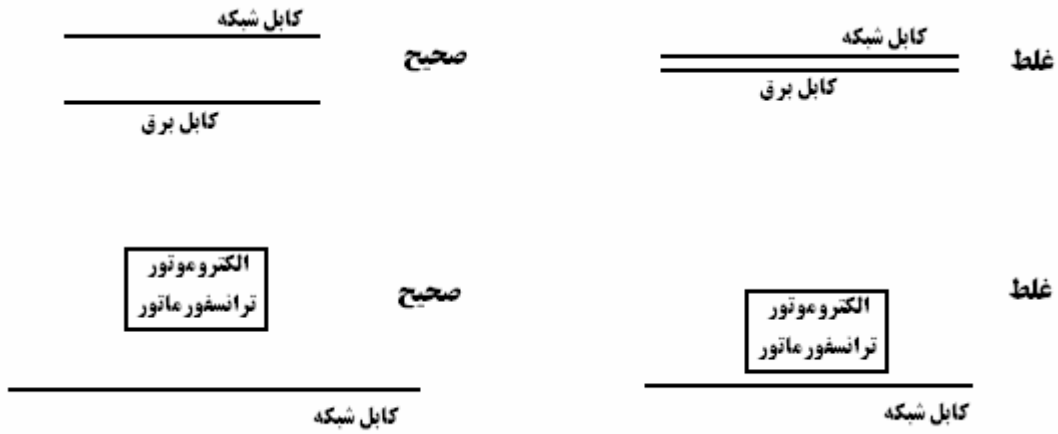
مراحل مهم پياده سازى سخت افزارى يک شبكه كامپيوترى را مى توان به ترتيب زير بيان كرد.

- تصميم گيرى در مورد نوع شبكه
- تهيه نقشه اجرايى
- انتخاب و تهيه سخت افزار مورد نياز

- نصب تجهيزات
- كابل كشي و نصب كابل
- برقراری اتصالات

۱-۳-۳- طراحي و اجراي عمليات كابلكشي:

نكات مهم هنگام طراحي و اجراي عمليات كابلكشي :كابلهاي "فلزي" مانند كابل هم محور يا Twisted Pair تحت تأثير ميدانهاي الكترومغناطيسي فضاي اطراف خود قرار گرفته و روي آنها Noise ايجاد مي‌شود. اينگونه ميدانها در مجاورت كابلهاي برق و مخصوصاً وسايل الكتريكي داراي "سيم پيچ" مانند انواع الكتروموتورها اعم از كاربردهاي خانگي يا صنعتي و انواع ترانسفورماتورها و ترانسفورمرها بيشتر بوده و بطور كلي بايد از عبور كابل در مجاورت نزديك با كابل برق يا وسايل فوق پرهيز كرد:



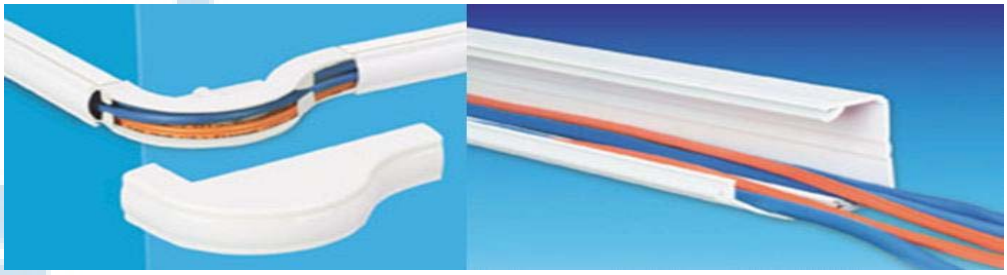
شكل ۳-۱۷

چنانچه‌كابلهاي برق و شبكه به‌موازات هم باشند درآنصورت حداقل فاصله‌ايكه بايد بين آنها بايد رعايت شود بستگي به شدت ميدان الكترومغناطيسي كابل برق دارد كه آنهم تابعي‌است از جريان الكتريكي عبوري از كابل. در عمل بسته به اين شدت جريان، حداقل از 5 Cm تا 30 Cm يا بيشتر فاصله بين كانالهاي برق و شبكه قرار مي‌دهند.

۲-۳-۳- Duct

به كانالهايي كه روي ديوار براي عبور كابل نصب مي‌شود اصطلاحاً Duct يا Trunk گفته مي‌شود و از نظر جنس بردو نوعند:

پلاستيكي و فلزي.



شكل ۳-۱۸

نكته برخي از كانالها داراى ۲ يا ۳ قسمت مجزا هستند و از آنها مي‌توان براي عبور كابل هاى برق و شبكه در كنار هم استفاده كرد اما بديهي‌است كه در اينگونه موارد بايد:

اولاً ديوارة حايل بين قسمتها بايد ترجيحاً فلزي بوده ثانياً شدت جريان عبوري از كابل برق زياد نباشد ثالثاً كابل شبكه در صورت امكان داراي حفاظ باشد رابعاً بدنة كانال اگر فلزي است به Earth متصل شود.

۳-۳-۳- عوامل موثر در تعيين نوع كابل كشی:

- سنگينی ترافيک شبکه ،
- طول كابل كشی
- بودجه تعيين شده برای كابل كشی
- نيازهای ايمنی شبكه
- نوع كابل كدام های موجود

جدول ۲-۳ خلاصه مقایسه کابلها

مشخصات	کواکسیال نازک	کواکسیال ضخیم	زوج به هم تابیده	فیبر نوری
هزینه کابل	ارزان	گران	ارزان	متوسط
طول کابلsegment	۱۸۵ متر	۵۰۰ متر	۱۰۰ متر	۲کیلومتر(۹۰کیلومتر)
سرعت انتقال	۱۰Mbps	۱۰Mbps	۴ تا ۱۰۰ Mbps	۱۰۰Mbpsیا بیشتر (بیشتر از 1Gbps)
نصب	نصب آسان	نصب آسان	خیلی آسان با امکان نصب قبلی	نصب دشوار (نیاز به متخصص و تجهیزات مخصوص دارد)
تداخل	مقاومت خوب در مقابل تداخل	مقاومت خوب در مقابل تداخل	مستعد برای تداخل	مستعد تداخل نمی باشد.
سایر خصوصیات	نیاز به اجزای پشتیبانی کمتری نسبت به ضخیم و T.P.دارد.	نیاز به اجزای پشتیبانی کمتری نسبت به ضخیم و T.P.دارد	همانند سیم تلفن ، اغلب در ساختمانها، از قبل نصب می شود.	از داده ها ، صوت و تصویر ، با ایمنی بالایی پشتیبانی می کند.

۴-۳-۳- اهمیت Earth:

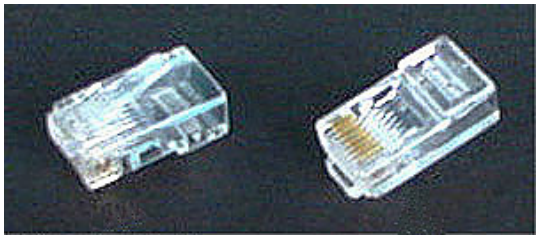
ارت بعنوان يك عامل مهم در تخلية نويز در كابلهاي داراي حفاظ بشمار مي‌رود (مانندكابل هم محور يا STP). چنانچه در شبكه‌اي از اين كابلها استفاده شود و حفاظ به ارت متصل نشود كاركرد شبكه توأم با اختلال خواهد بود كه اين اختلال بشكل خطا در انتقال اطلاعات، كندي سرعت و حتي قطعي موقتي خود را نشان مي‌دهد. بنابراين توصيه مي‌شود حتماً چاه ارت مناسب براي كامپيوترها، شبكه و تجهيزات مربوطه تهيه شده و هرگز از ارت مربوط به برق‌گير (كه روي بام برجها نصب مي‌شود) براي شبكه استفاده نشود.

۵-۳-۳- تجهیزات مورد نیاز برا ي اتصال کابل به کانکتور

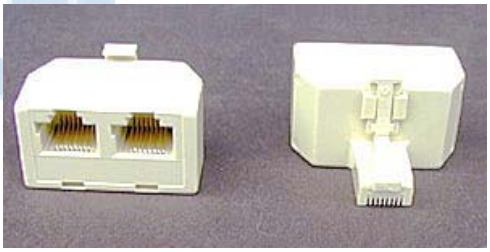
تجهیزات مورد نیاز برای ایجاد کابل های UTP عبارتند از :

- کانکتورهای RJ-45
- کابل UTP
- آچار پرس RJ-45
- سیم لخت کن

که در شکل ۱۹-۳ نشان داده شده است.



الف

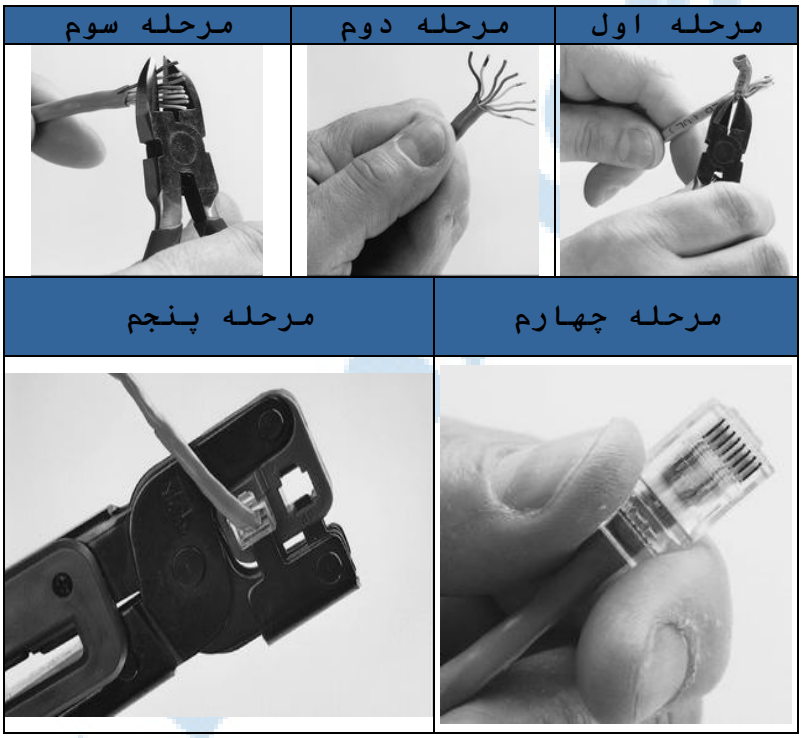


ب

ج
شکل ۳-۱۹

۳-۳-۶- ایجاد کابل Straight

مراحل ایجاد یک کابل : شکل ۳-۱۸ مراحل لخت کردن سیم و اتصال کانکتور را نشان می دهد.



شکل ۳-۲۰

مدل های متفاوت کابل کشی کابل های

به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت T-568A و T-568B استفاده می شود . تفاوت دو مدل فوق مربوط به رنگ زوج هائی است که به یکدیگر متصل می شوند.در کابل های UTP از کانکتورهای استاندارد و چهار زوج سیم بهم تابیده استفاده می گردد :

- زوج اول : آبی و سفید/ آبی
- زوج دوم : نارنجی و سفید /نارنجی
- زوج سوم : سبز و سفید/ سبز
- زوج چهارم : قهوه ای و سفید / قهوه ای

در شبکه های ۱۰/۱۰۰ Mbit از زوج های دو و سه استفاده شده و زوج های یک و چهار به عنوان رزو باقی می ماند . در شبکه های گیگا اترنت از

تمامی چهار زوج استفاده می گردد. کابل های CAT5 متداولترین نوع کابل UTP بوده که دارای انعطاف مناسب بوده و نصب آن ها به راحتی انجام می شود .

ایجاد یک کابل UTP به منظور اتصال کامپیوتر به هاب (معروف به کابل های Straight) اترنت عموما" با استفاده از هشت کابل به همراه هشت پین ماژولار plugs/jacks ، داده را حمل می کند . کانکتور استاندارد، RJ-45 نامیده شده و مشابه کانکتور استاندارد RJ-11 است که در تلفن استفاده می گردد. یک رشته کابل CAT5 شامل چهار زوج سیم بهم تابیده است که هر زوج دارای دو رشته سیم با رنگ هائی خاص است . (یک رشته رنگی و یک رشته سفید با نواری به رنگ رشته زوج مربوط) . به منظور تسهیل در امر نگهداری ، می بایست به اندازه ضروری سیم های بهم تابیده را از حالت پیچش خارج نمود (مثلا" حدود یک سانتیمتر) . زوج های در نظر گرفته شده برای اترنت ده و یکصد مگابیت به رنگ نارنجی و سبز می باشند . از دو زوج دیگر (رنگ قهوه ای و آبی) می توان به منظور یک خط اترنت دوم و یا اتصالات تلفن استفاده نمود .

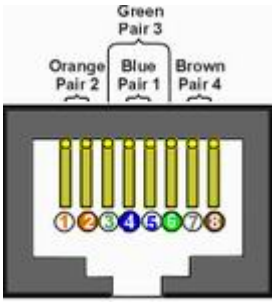
به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T&AT ، A۲۵۸) ، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است .

شماره پین های استاندارد T568B

همانگونه که در جدول زیر مشاهده می گردد ، شماره پین های فرد همواره سفید بوده که با یک نوار رنگی پوشش داده می شوند .

جدول ۳-۳

کد رنگ ها در استاندارد B۵۶۸T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید/ نارنجی	دوم	TxData+
دو	نارنجی	دوم	TxData-
سه	سفید / سبز	سوم	RecvData+
چهار	آبی	یک	
پنج	سفید / آبی	یک	
شش	سبز	سوم	RecvData-
هفت	سفید/قهوه ای	چهارم	
هشت	قهوه ای	چهارم	



شکل ۳-۲۱ استاندارد B۵۶۸T

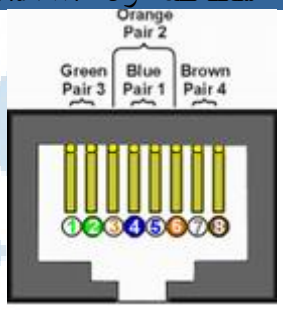
شماره پین های استاندارد T568A

در استاندارد T568A ، اتصالات سبز و نارنجی برعکس شده است ، بنابراین زوج های یک و دو بر روی چهار پین وسط قرار می گیرند (سازگاری با اتصالات telco (voice .

جدول ۳-۴

کد رنگ ها در استاندارد A۵۶۸T			
شماره پین	رنگ	زوج	کاربرد
یک	سفید/ سبز	سوم	RecvData+
دو	سبز	سوم	RecvData-
سه	سفید / نارنجی	دوم	TxData+
چهار	آبی	یک	
پنج	سفید / آبی	یک	
شش	نارنجی	دوم	TxData-
هفت	سفید/قهوه ای	چهارم	
هشت	قهوه ای	چهارم	

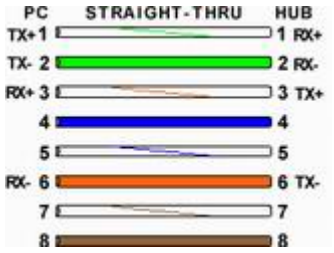
استاندارد A۵۶۸T



شکل۲۲ -۳

موارد استفاده کاربرد کابل straight

یک کابل straight ،به طور معمول برای برقراري اتصال بین کامپیوتر و هاب / سوئیچ به کار می رود .



شکل۲۳-۳

شکل ۳-۲۳ یک اتصال استاندارد straight در کابل های CAT5 را نشان می دهد که از آن به منظور اتصال یک کامپیوتر به هاب استفاده می گردد . با اینکه در ظاهر +TX یک طرف به +TX طرف دیگر متصل نشده است ولي. زمانی که کامپیوتر شخصی به هاب متصل می گردد ، هاب به صورت اتوماتیک و با استفاده از مدارات داخلی خود کابل را X-over نموده و بدین ترتیب ، پین شماره یک از کامپیوتر (+ TX) به پین شمار یک هاب (+ RX) متصل می شود . در صورتی که هاب عملیات x-over را انجام ندهد (در زمان استفاده از درگاه Uplink) ، پین شماره یک کامپیوتر (+ TX) به پین شماره یک هاب (+ TX) متصل می گردد . بنابراین مهم نیست که چه نوع عملیاتی را با درگاه HUB انجام می دهیم (Uplink و یا نرمال) ، سیگنال های نسبت داده شده به هشت پین سمت کامپیوتر شخصی ، همواره یکسان باقی مانده و هاب با توجه به نوع استفاده از درگاه (نرمال و یا Uplink) عملیات لازم را انجام خواهد داد .

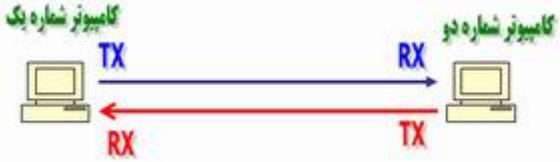
۳-۳-۷- ایجاد کابل X-Over

کابل های کراس CAT5 UTP که از آنان با نام X-over نیز نام برده می شود ، یکی از متداولترین کابل های استفاده شده پس از کابل های Straight می باشند . با استفاده از کابل های فوق ، می توان دو کامپیوتر را بدون داشتن هاب یا سوئیچ به یکدیگر متصل نمود. با توجه به این که هاب عملیات X-over را به صورت داخلی انجام می دهد ، در زمانی که یک کامپیوتر را به یک هاب متصل می کنید ، فقط به کابل Straight نیاز است. و در صورتی که قصد اتصال دو کامپیوتر به هم را بدون استفاده از هاب دارید ، می بایست عملیات X-over را به صورت دستی انجام دهید و کابل X-over را ایجاد نمایید.

عملکرد کابل های X-over

در زمان مبادله داده بین دو کامپیوتر، یکی از آنان به عنوان دریافت کننده و دیگری به عنوان فرستنده ایفای وظیفه می نماید . تمامی عملیات ارسال داده از طریق کابل های شبکه انجام می شود .یک کابل شبکه از چندین رشته سیم دیگر تشکیل می گردد. از برخی رشته سیم ها به منظور ارسال داده و از برخی دیگر به منظور دریافت داده استفاده می شود. در ساخت کابل X-over از اصول فوق استفاده شده و TX (ارسال) یک سمت به RX (دریافت) سمت دیگر، متصل می گردد .

اتصال دو کامپیوتر به یکدیگر با
استفاده از یک کابل X-over



شکل۳-۲۴

کابل CAT5 X-over

به منظور ایجاد کابل های کراس CAT5 صرفا" از یک روش استفاده می گردد. همانگونه که قبلا" اشاره گردید ، یک کابل X-over پین TX یک سمت را به پین RX سمت دیگر متصل می نماید (و برعکس) . شکل زیر شماره پین های یک کابل CAT5 معمولی X-over را نشان می دهد .

شماره پین های یک کابل CAT5 X-over

.

شکل ۲۵-۳

همانگونه که در شکل ۲۵-۳ مشاهده می کنید در کابل X-over از پین های شماره یک ، دو ، سه و شش استفاده می گردد . پین های یک و دو بمنزله یک زوج بوده و پین های سه و شش زوج دیگر را تشکیل می دهند . از پین های چهار ، پنج ، هفت و هشت استفاده نمی گردد . (فقط چهار پین از هشت پین کانکتور ، استفاده می شود) .

کاربرد کابل های X-over

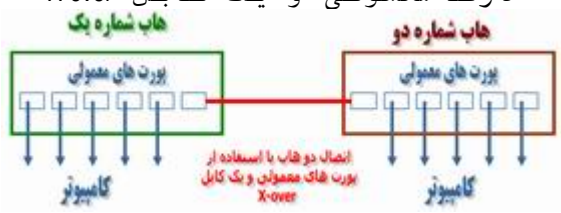
از کابل های X-over تنها برای اتصال دو کامپیوتر استفاده نمی شود بلکه از آن می توان در دستگاه های متفاوتی نظیر سوئیچ یا هاب نیز استفاده کرد . در صورتی که قصد داشته باشیم دو هاب را به یکدیگر متصل نمائیم ، معمولا" از درگاه uplink استفاده می گردد. درگاهفوق ، بخش های tx و rx را کراس نمی نماید. شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل Straight و از طریق درگاه Uplink را نشان می دهد :

اتصال دو هاب با استفاده از درگاه Uplink
و یک کابل Straight

شکل ۲۶-۳

با توجه به وجود درگاه uplink ، نیازی به استفاده از یک کابل x-over نخواهد بود . در صورتی که امکان استفاده از درگاه uplink وجود نداشته باشد و بخواهیم دو هاب را با استفاده از درگاههای معمولی به یکدیگر متصل نمائیم ، می توان از یک کابل X-over استفاده نمود . شکل زیر نحوه اتصال دو هاب به یکدیگر با استفاده از یک کابل X-over را و بدون استفاده از درگاه Uplink نشان می دهد :

اتصال دو هاب با استفاده از
درگاهمعمولی و یک کابل X-over



شکل ۲۷-۳

۳-۴- کارت شبکه و وظایف آن

کارتهای شبکه ، به عنوان میانجی(Interface) فیزیکی یا رابط بین کامپیوتر و کابل شبکه ، عمل می کنند . کارتها در شکاف (Slot) توسعه هر کامپیوتر و سرویس دهنده شکبه نصب می شوند .
پس از آنکه که کارت شبکه متعصب گردید ، کابل شبکه به درگاه کارت متصل می شود تا ارتباط واقعی فیزیکی بین کامپیوتر و باقیمانده شبکه را برقرار می سازد.

شکل ۳-۲۸ شکل ۵-۱۶ ص ۳۴ آشنایی باشبکه

۳-۴-۱- وظایف کارت شبکه

وظایف کارت شبکه عبارت است از:

- آماده سازی داده های کامپیوتر برای انتقال به کابل شبکه
- ارسال داده ها به کامپیوتر دیگر
- کنترل جریان داده ها بین کامپیوتر و سیستم کابل کشی

کارت شبکه همچنین داده های وارده شونده را از کابل در یافت می کند و آن را به داده های قابل پردازش در CPU تبدیل می کند

آماده سازی داده ها : قبل از آنکه داده ها بتوانند از طریق شبکه ارسال شوند ، کارت شبکه باید آن را از از شکل قابل پردازش در کامپیوتر به شکل قابل انتقال از طریق کابل شبکه تغییر دهد.

داده ها در داخل کامپیوتر از طرق مسیرهایی به نام گذرگاهها (BUS) حرکت می نمایند . آنها چندین مسیر داده ای هستند که به طور موازی و پهلوی هم قرار گرفته اند ، چون چندین مسیر پهلو به پهلو هستند ، داده ها می توانند به جای عبور تکی در هر لحظه به صورت گروهی با یکدیگر عبور کنند .

در کابل شبکه ، داده ها باید در جریان تک بیتی حرکت نمایند . وقتی داده ها از کابل شبکه عبور می کنند گفته می شود به صورت انتقال سریال (serial) حرکت می نمایند زیرا هر بیت به دنبال بیت دیگر جریان دارد . به عبارت دیگر ، کابل بزرگراه یک باند می باشد . داده ها در این بزرگراه ها همیشه در هر لحظه فقط یک باند حرکت دارند . کامپیوتر ها یا داده ها را می فرستند و یا در یافت می دارند .

کارت شبکه ، عبور داده ها را به صورت موازی و به شکل گروهی می گیرد و آنها را طوری مجددا می سازد که از طریق مسیر سریال به پهنای ۱ بیت در کابل شبکه جریان یابند . این کار با تبدیل سیگنالهای دیجیتال کامپیوتر به سیگنالهای الکتریکی ونوری که می توانند از طریق کابلهای شبکه حرکت نمایند انجام می گیرد . قطعه مسئولاین کار ، فرستنده گیرنده (Transciever) است .

۳-۴-۲- آدرس شبکه

علاوه بر تبدیل داده ، کارت شبکه محل کارت یا آدرس را به باقیمانده شبکه نشان می دهد تا از تمام کارتهای دیگر شبکه تمیز داده شود.
آدرسهای شبکه از کمیته IEEE (تلفظ می شود آی تریپل ای ، مخفف انستیتوی مهندسان برق والکترونیک) تعیین می گردد. این کمیته ، محدوده ای از آدرسها را به هریک از سازندگان کارتهای شبکه اختصاص می دهد . سازندگان

به طور سخت افزاری ، این آدرسها را در تراشه (Chip) های روی کارت قرار می دهند . با این روش ، هر کارت ، و در نتیجه هر کامپیوتر ، آدرس منحصر به فردی در شبکه دارد .
داده ها اغلب می توانند سریعتر از کارت شبکهای که آنها را اداره می کنندحرکت نمایند. به این دلیل داده به بافر (RAM)کارت فرستاده می شوندو در آنجا به طور موقت هم در ارسال و هم در دریافت ، نگهداری می شوند.

۳-۴-۳- ارسال و کنترل داده ها:

قبل از آن که کارت شبکه ، عملا داده ها را به شبکه ارسال نماید ، محاوره ای الکترونیکی با کارت گیرنده انجام می دهد به طوری که هر دو کارت با موارد زیر موموافق باشند:

- میزان داده های ارسالی قبل از تایید
- هرکارت قبل از سرریز شدن داده چه مقدار داده را می تواند نگهدری نماید.
- سرعت انتقال داده ها

اگر کارت با سرعت بالاتر ، برای ارتباط آهسته تر مورد نیاز باشد ، هر دو کارت نیازمند یافتن سرعت انتقال مشترکی هستند که هر دو بتوانند انجام دهند . هر کارت به کارت دیگر علامت می دهد و با این عمل ، عوامل (پارامترهای) خود را به دیگری اطلاع و یا خودش را با عوامل دیگری تنظیم می نماید .
وقتی تمام جزییات ارتباط تعیین گردید ، دو کارت ، شروع به ارسال و در یافت داده ها می نمایند.

۴-۳-۴-پیکر بندی (configuration) کارت شبکه

کارتهای شبکه ، اغلب دارای گزینه های قابل پیکر بندی هستند که باید برای کارکرد صحیح کارت شبکه تنظیم گردند . مثلا :

- وقفه IRQ (Interrupt)
- آدرس پایه درگاه ورودی – خروجی(Base I/O port)
- آدرس پایه حافظه (Base Memory)
- نحوه تنظیم گزینه ها در کارتهای شبکه متفاوت است . گاهی امکان دارد به کمک جامپر (jamper) روی کارت تنظیم نمود.

بعضی کارتها به کمک کلیدهای ریزی (DIP Switch) بر روی کارت شبکه پیکر بندی می شوند . در اغلب کارتهای شبکه که بدون جامپر(Jamper less) و DIP Switch هستند ، تنظیم پیکر بندی در آنها با نرم افزاری که همراه کارت شبکه فر وخته می شود ، انجام می گیرد . نحوه تنظیم پیکر بندی ، در دفترچه های راهنما یا فایلهای راهنما ، همراه کارت شبکه ، مشخص می گردد.
وقفه (IRQ): خطوط تقاضای وقفه ، خطوط سخت افزاری هستند که از طریق آنها دستگاههایی مانند پورتهای ورودی / خروجی ، صفحه کلید ، درایوهای دیسک و کارتهای شبکه می توانند و قفه ها یا تقاضاها را برای گرفتن خدمات ، به CPU کامپیوتر برسانند.
خطوط درخواست وقفه در سخت افزار داخلی کامپیوتر تعبیه شده و سطوح مختلفی از تقدم را به گونه ای اختصاص می دهد که CPU بتواند اهمیت نسبی تقاضاهای خدمات وارد شده را تعیین نماید.
وقتی کارت شبکه تقاضایی برای کامپیوتر می فرستد ، از وقفه ، یعنی سیگنال الکترونیکی ارسالی بهCPU کامپیوتر استفاده می کند .
هر قسمت سخت افزاری در کامپیوتر باید از خط تقاضای وقفه یا IRQ متفاوتی بهره بگیرد . خط وقفه ، زمانی که قسمت سخت افزاری کامپیوتر پیکر بندی می شود ، مشخص می گردد.
آدرس پایه I/Q: درگاه ورودی / خروجی (I/Q) پایه مسیری را مشخص می کند که از طریق آن داده ها بین سخت افزار کامپیوتر (ازقبیل کارت شبکه) و CPU آن جریان می یابد. CPU، هر پورتی را با آن آدرس می شناسد.

هر قسمت سخت افزاری در سیستم ، باید شماره درگاهI/O پایه متفاوتی داشته باشد . آدرسهای پایه پورتها (اعداد مبنای شانزده) که برای کارت شبکه به کار می روند ، نباید قبلا از سوی قسمت دیگری استفاده شده باشد.
آدرس پایه حافظه : آدرس پایه حافظه ، محلی را در حافظه کامپیوتر (RAM) مشخص می کند . این محل ، به صورت ناحیه بافر برای ذخیره کرده داده های دریافتی و ارسالی از کارت شبکه به کار می رود . البته بعضی کارتهای شبکه تعریفی برای آدرس پایه حافظه ندارند زیرا آنها از هیچ یک از آدرسهای RAM سیستم استفاده نمی کنند .
معماری گذرگاه داده ها : در محیط کامپیوتر های شخصی ، معماریهای مختلفی برای گذرگاه داده ها در کامپیوتر وجود دارد . از جمله معروف ترین این گذرگاهها می توان به استاند ارد ISA(آیزا) و PCI(پی سی آی) اشاره نمود . هرنوع گذرگاه به طوری فیزیکی از سایر گذرگاه ها جداست . ضروری است که کارت شبکه و گذرگاه هماهنگ باشند.
نکته: امروزه بيشتر بردهاي اصلي داراي كارت شبكه به صورت On Board هستند و از گذرگاه هاي داخلي برد اصلي استفاده مي كنند.

۵-۴-۳-اتصال کارت شبکه

کارت شبکه ، سه عمل مهم زیر را در هماهنگی فعالیتهای بین کامپیوتر و کابل انجام می دهد :

- انجام اتصال فیزیکی با کابل
- تولید سیگنالهای الکتریکی که از کابل می گذرند .
- پیروی از قوانین مشخص نحوه دسترسی به کابل به منظور انتخاب کارت مناسب شبکه ، لازم است ابتدا نوع کابل و اتصالات آن تعیین شده باشند . هرنوع کابل خصوصیات فیزیکی متفاوتی دارد که کارت شبکه باید با آن مطابقت نماید . هر کارت برای پذیرش نوع خاصی از کابل مانند هم محور ، زوج به هم تابیده شده یا فیبر نوری ، ساخته شده است . برخی از کارتهای شبکه بیش از یک اتصال میانجی دارند . مثلا بعضی از کارت شبکه ها ، دو درگاه اتصال هم محور نازک (BNC) و زوج به هم تابیده شده (RJ-45) را دارند

۵-۳- روشهای دسترسی به خط انتقال

مجموع قوانینی که تعریف می کنند کامپیوتر چگونه داده ها را در کابل شبکه قرار می دهد و آنها را ازکابل می گیرد «روش دسترسی » نامیده می شود از آنجا که در اکثر سیستمهای شبکه ،کانال ارتباطی در یک زمان معین تنها می تواند در اختیار یک ایستگاه باشد و ازطرف دیگر ، هر یک از ایستگاههای شبکه در هر لحظه ممکن است احتیاج به استفاده از کانال ارتباطی داشته باشند ، رعایت یک روش و قانون مشخص برای دسترسی به خط انتقال ،لازم است .
روشهای رایج برای دسترسی به خط انتقال عبارت اند از :

- روش دسترسی چندگانه تشخیص حامل باتشخیص برخورد (CSMA/CD)
- روش عبور نشانه (Token passing)

۵-۳-۱- روش دسترسی چندگانه تشخیص حامل باتشخیص برخورد (CSMA/CD)

این روش شبیه روش صحبت در یک اتاق شلوغ است .در چنین اتاقی شخصی که می خواهد صحبت کند باید با گوش دادن ، مطمئن شود که فرد دیگری در حال صحبت نیست و سپس اقدام به صحبت کند . اگر شخص دیگری در حال صحبت کردن است ، نفر اول باید تا پایان صحبت شخص دوم سکوت کند . این شخص ، پس از اتمام صحبت فردی که زودتر از دیگران شروع به صحبت کرده است ، می تواند به صحبت خود ادامه دهد و بقیه باید تا پایان صحبت منتظر بمانند . هر گاه پس از برقراری سکوت ،دونفر با هم شروع به صحبت کنند ، هردو

سکوت کرده ، پس از طی یک زمان کوتاه نامشخص ، یکی از آنها شروع به صحبت خواهد کرد . این دقیقا روشی است که در CSMA/CD از آن استفاده می شود :

۱- کامپیوتر « تشخیص می دهد » که کابل آزاد است یعنی ترافیکی در کابل وجود ندارد . (Sense)

۲- کامپیوتر می تواند داده ها را ارسال نماید.

۳- اگر داده ها در کابل وجود د اشته باشند ، تا زمانی که داده ها به مقصد خود برسند و کابل مجددا آزاد گردد ، هیچ کامپیوتر ای داده ای را انتقال نمی دهد .

اگر دویا چند کامپیوتر دقیقا به طور همزمان ، داده ها را ارسال نمایند ، برخورد(Collision) داده ها پیش خواهد آمد . وقتی چنین اتفاقی نیفتند ، دو کامپیوتر درگیر برای یک دوره زمانی تصادفی ، انتقال را متوقف می سازند و سپس سعی در ارسال مجدد می نمایند .

CSMA/CD به عنوان روش کشمش شناخته می شود زیرا کامپیوتر های شبکه برای به دست آوردن فرصتی در ارسال داده ها ، با هم رقابت یا کشمکش می کنند .

وجود تعداد زیادی کامپیوتر در شبکه ، موجب بروز ترافیک سنگین تر در شبکه می گردد . در ترافیک سنگین تر ، برخورد ها افزایش می یابند . پس از هر برخورد هر دو کامپیوتر باید برای ارسال مجدد داده ها تلاش نمایند ، که موجب پایین آمدن سرعت شبکه می گردد.

بروز برخوردهابا افزایش تعداد کامپیوتر ها در شبکه افزایش می یابد . برنامه کاربردی بانکهای اطلاعاتی نسبت به برنامه دیگر در ایجاد ترافیک سنگین تر شبکه ، نیز نقش دارند. بنابراین ، شبکه با روش دسترسی CSMA/CD با کاربران زیادی که چندین برنامه کاربردی بانکهای اطلاعاتی را اجرا می کنند ، ممکن است شبکه را به حد توقف (سرعت بسیار کند و آهسته) بکشاند.

۲-۵-۳- روش عبور نشانه (Token passing)

در عبور نشانه ، بسته خاصی به نام (Token) دور کابل حلقوی ، کامپیوتر به کامپیوتر گردش می کند . وقتی هر کامپیوتر ای در حلقه بخواهد داده ها را در طول شبکه ارسال نماید ، باید منتظر نشانه آزاد بماند . وقتی نشانه آزاد تشخیص داده شد ، کامپیوتر می تواند داده ها را انتقال دهد . داده ها به صورت بسته ها منتقل می شوند و اطلاعات اضافی مانند آدرس دهی به بسته ها متصل می گردد .

در حالی که نشانه از سوی یک کامپیوتر مورد استفاده قرار می گیرد ، سایر کامپیوتر ها نمی توانند داده ای منتقل نمایند .مزیت این روش در آن است که چون در هر لحظه فقط یک کامپیوتر می تواند از نشانه استفاده نماید، کشمکش و برخوردی پیش نمی آید و حتما پس ازطی زمانی مشخص ، نوبت ارسال داده به هر کامپیوتر خواهد رسید.

خود آزمايي و تحقيق

۱- توپولوژي چيست؟ انواع آن را شرح دهيد.

۲- پديده برخورد يا Collision در كدام يك از انواع توپولوژي روي مي دهد؟ چرا؟

۳- در كدام يك از انواع توپولوژي، با قطع شدن قسمتي از كابل، كل شبكه از كار مي افتد؟

۴- انواع توپولوژي ها را از لحاظ مصرف كابل، سرعت، هزينه، عيب يابي و اشكال زدايي مقايسه كنيد.

۵- انواع محيط هاي انتقال سيمي يا كابلي را از لحاظ سرعت، امنيت، هزينه، مسافت و نويز بررسي كنيد.

۶- حداقل فاصله بين كابل شبكه و كابل برق بايد چقدر باشد؟

۷- عوامل موثر در تعيين نوع كابل را نام ببريد.

۸- سرعت كدام يك از روش هاي دسترسي به خط بيشتر است؟ دليل آن را بنويسيد.

۹- چه عواملي در سرعت دسترسي به خط موثر است؟

۱۰- تحقيق كنيد كه آيا مي توان در كابل كشي يك شبكه از همه انواع كابل (مانند Cat5، Cat6، Fiber و ...) استفاده كرد؟ سرعت و راندمان شبكه در اين حالت چگونه است؟

۱۱- تحقيق كنيد كه براي اتصال چندين Switch يا HUB از چه نوع كابلي بايد استفاده گردد؟

فصل چهارم - معماری شبکه

هدف هاي رفتاري

انواع معماري شبکه و ويژگيهاي آن ها را شرح دهد.

تکنولوژي FDDI را تعريف کند.

معماری شبکه ، استانداردهایی که برای نحوه اتصال کامپیوتر ها با یکدیگر و نحوه ارسال اطلاعات تعریف شده است . در این استانداردها نوع کابل شبکه ، اتصالات ، توپولوژی ، نحوه دسترسی به خطوط انتقال و سرعت انتقال مشخص شده است .

۱-۴- انواع معماری شبکه و ویژگی های آن ها

چندین نوع معماری شبکه وجود دارد که هنگام راه اندازی شبکه از آن ها استفاده . می شود . انواع معماری شبکه عبارتند از :

- اترنت[1]
- Token Ring

۱-۱-۴- اترنت

اترنت یکی از انواع متداول معماری شبکه است . دراین معماری از روش CSMA/CD برای دسترسی به خط انتقال یا همان کابل شبکه استفاده می شود . توپولوژی پیش فرض برای اترنت ، توپولوژی فیزیکی خطی تعریفی شده است . توپولوژی های شبکه مثل توپولوژی خطی که از توپولوژی منطقی خطی استفاده می کنند از اترنت بهره می برند . نوع کابلی که در هر توپولوژی استفاده می شود نیز در قوانین همان توپولوژی مشخص شده است .

توپولوژی های مختلف اترنت عبارتند از :

- 10Base2
- 10Base5
- 10BaseT
- 10Base FL
- 100VG-ANYLAN
- 100Base x

نکته : در استانداردهایی که نام برده شد ، عدد اول نمایانگر سرعت انتقال است مثلا10Base2باسرعت 10bps کار می کند. Base نشان دهنده Base band بودن توپولوژی و عبارت پس از آن نوع کابل را نشان می دهد.

در معماری اترنت علاوه بر موارد ذکر شده نحوه ساخته شدن بسته های اطلاعاتی ، اندازه آن ها ، اطلاعات اضافی که باید در بسته های اطلاعاتی قرار گیرد و کابل کشی شبکه مشخص شده است . در ادامه برخی از استانداردهای متداول توضیح داده خواهد شد .

استانداردهای IEEE

---

[1] -Ethernet

- 10Base2

10Base 2برای انتقال داده ها از کابل هم محور Thinnet استفاده می کند که مشخصات این کابل در فصل دوم توضیح داده شد . کانکتورهای این شبکه از نوع BNC بوده ودوسرکابل باید به وسیله ی Terminator مسدود شودتا شبکه فعال شود .ازمزایای10Base 2نصب ساده و هزینه راه اندازی بسیار کم آن است . توپولوژی 10Base2 همان توپولوژی خطی است .
قوانینی که در 10Base 2 باید رعایت شود ، عبارتند از :

- حداقل طول کابلی که کامپیوترها را به هم متصل می کند نباید کمتر از ۰/۵ متر باشد.
- برای اتصالT-connector به کامپیوتر نباید از استفاده کرد وباید آن را مستقیما 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 می شود .
- با استفاده از هاب یاRepeater می توان حداکثر فاصله بین اولین و آخرین کامپیوتر را تا ۹۲۵ متر افزایش داد کامپیوترهانبایدخارج از این محدوده باشند.
- در فواصل بین هر دو Repeaterنمی توان بیش از ۳۰ دستگاه کامپیوتر به شبکه متصل کرد.
- ابتدا و انتهای کابل باید با Terminator مسدود شود . Terminatorشبکه 10Base2 ، یک مقاومت ۵۰ اهمی است که سیگنال های الکتریکی به وجود آمده در کابل شبکه را مصرف کرده و از باقی ماندن آن در شبکه جلوگیری می کند.

برای دست یافتن به حداکثر فاصله کامپیوترها یعنی ۹۲۵ متر، پنج Segment خواهیم داشت که با چهار دستگاه Repeater به هم متصل شده اند که فقط از سه Segment آن می توان استفاده کرد . این Segment ها شماره های ۱،۲ و ۵ هستند . این قانون به قانون ۳-۴-۵ معروف است.

شکل ۱-۴ (ص ۸۴) مفاهیم شبکه

- 10Base 5

در 10Base 5از کابل کواکسیال Thicknet برای اتصال کامپیوترها به یکدیگر استفاده می شود.
هر کامپیوتر به وسیله ی یک کابل AUT یا DIX به یک عدد Transceiver که به کابل شبکه متصل شده است ، وصل می شود و هر دو انتهای کابل با Terminatorمسدود می شود . اولین مزیت
10Base5 مسافت نسبتا زیادی است که تحت پوشش خود قرار میدهد . قوانینی که در مورد
10Base5 وجود دارد عبارتند از :

- حداقل طول کابل که برای اتصال دو کامپیوتر استفاده می شود ۲/۵ متر است .
- حداکثر طول کابل یا حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه ۵۰۰ متر است .

- حداکثر فاصله بین اولین و آخرین کامپیوتر شبکه با استفاده از Repeater ۲۵۰۰ متر است
- یکی از Terminator ها باید به زمین متصل شود .
- اندازه کابلی که کامپیوتر را به Transceiver متصل می کند ، نباید بیشتر از ۵۰ متر باشد.
- حداکثر تعداد کامپیوترها در هر Segment ۱۰۰ دستگاه است .
- قانون ۳-۴-۵ در مورد 10Base 5 نیز صادق است .

شکل ۴-۲ (ص ۸۵) مفاهیم شبکه

10Base T

برای راه اندازی شبکه10Bese T از کابل های TP یا زوج به هم تابیده استفاده می شود که حداکثرسرعت آن 10Mbps است. در این استاندارد هر کامپیوتری که می خواهد به شبکه متصل شود مستقیما به وسیله ی یک کابل به هاب وصل شده و هاب ، ارتباط کامپیوترها را برقرار می کند . اتصالات این توپولوژی از نوع RJ-45 است .Segment های مختلف می توانند به وسیله ی کابل های کواکسیال یا فیبر نوری به یکدیگر متصل شوند. برخی از انواع دستگاه هایی که می توانند جایگزین هاب شوند ، هوشمند بوده و می توانند ترافیک شبکه را کنترل کرده و آن را کاهش دهند . از مشخصه های بارز این شبکه گران قیمت بودن هزینه راه اندازی و نصب آن است. 10BaseT در ظاهر یک شبکه ستاره ای است ولی عملکرد آن همانند شبکه های خطی می باشد در این مورد به طور خلاصه می توان گفت توپولوژی فیزیکی آن ، ستاره ای ولی توپولوژی منطقی آن خطی است .
قوانین 10BaseT عبارتند از:

- حداکثر تعداد کامپیوتری که این شبکه به هم متصل می کند ، ۱۰۲۴ دستگاه کامپیوتر است.
- کابل ها باید از نوع زوج به تابیده Category3، Category4 یا Categor5 باشند (نوع کابل از نظر داشتن محافظ تفاوتی نمی کند ، می توان از هر دو کابل UTPیا STP استفاده کرد).
- حداکثر فاصله هر کامپیوتر تا هاب ، ۱۰۰ متر است .
- حداقل طول کابل (فاصله بین کامپیوتر تا هاب) ۲/۵ متر است .

شکل ۴-۳ (ص۸۶) مفاهیم شبکه

10Base FL

10Base FL یکی از خصوصیات شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده می کند . سرعت انتقال در این شبکه 10Mpbs است . مهم ترین 10Base FL مسافت زیادی است که تحت پوشش قرار می دهد . این مسافت ۲ کیلومتر است . از مزایای دیگر این شبکه این است که عوامل خارجی ، تاثیری روی اطلاعات داخل فیبر ندارند . به عبارت دیگر ، در فیبر نوری هم شنوایی و جود ندارد و اطلاعات سالم به مقصد می رسد .
دو استاندارد دیگر به نام های 10Base FB و 10BaseFP نیز مورد استفاده قرار می گیرد .10BaseFB یک شبکه اترنت هم زمان است[1] و برای اتصال دو تقویت کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قراردارد ، استفاده می شود . استاندارد دیگر 10BASE FP است که یک شبکه ستاره ای با استفاده از فیبر نوری می باشد که برای Backbone شبکه ها مورد استفاده قرار می گیرد . در 10Base FP نور به جای سیگنال های الکترونیکی مسئولیت انتقال اطلاعات را برعهده دارد .

100Base X

ساختار شبکه 100BaseX همانند شبکه10BaseT است (سرعت این شبکه 100Mbps است)با این تفاوت که 100BaseX با سه مدل کابل کشی متفاوت مورد استفاده قرار می گیرد . این سه مدل عبارتند از:

- 100Base TX؛در این مدل از دو کابل category ازنوع UTP یا STP به صورت همزمان استفاده می شود.
- 100Base FX: در این مدل از دورشته فیبر نوری در کنار هم استفاده می شود.
- 100Base T4: در این مدل ۴ رشته کابل ۵ یا ۴, Category3 در کنار هم استفاده می شود .
- 100Base X: بانام Fast Ethernet نیز شناخته می شود.

و 100BaseX
این استاندارد ، شبکه ای را توضیح می دهد که در آن سرعت انتقال اطلاعات یک گیگابایت در ثانیه است و برای انتقال اطلاعات از فیبر نوری استفاده می شود. این استاندارد خود از چند قسمت تشکیل شده است که عبارتند از :

۱- 1000Base sx
۲- 1000Base LX/LH
۳- 1000Basezx

تفاوت استاندارد های ذکرشده در طول کابل ها و نوع فیبر نوری است که در آن ها استفاده می شود.

1000Base T

در اين استاندارد، از كابل‌هاي زوج به هم تابيده براي راه اندازي شبكه‌اي با سرعت يك گيگابيت در ثانيه استفاده مي‌شود. اين كابل‌ها از نوع Cat5 و كانكتورهاي آن نيز از نوع RJ-45 است. نحوه ارسال اطلاعات در اين استاندارد به گونه‌اي است كه سيستم، توانايي انتقال اطلاعات با سرعت يك گيگابيت در ثانيه را پيدا مي كند. كابل Cat5 نام ديگر كابل زوج به هم تابيده است.

Token Ring ۴-۱-۲

شبكه Token Ring از نظر ظاهري يك شبكه ستاره‌اي است ولي به صورت Token Passing كار مي‌كند. در اين شبكه يك حلقه منطقي به وجود مي‌آيد و Token در امتداد حلقه حركت كرده و به كامپيوترها مي‌رسد. هر كامپيوتري كه به ارسال اطلاعات نياز داشته باشد، Token را نگه داشته و اطلاعات خود را به سوي مقصد ارسال مي‌كند. اطلاعات ارسال شده در همان حلقه مجازي و در امتداد حركت Token مسير خود را طي مي‌كند تا به كامپيوتر مقصد برسد. كامپيوتر مقصد در صورت صحيح بودن اطلاعات ارسالي، در جواب يك بسته به

[1] -Synchronous Ethernet

نام Acknowledge به کامپیوتر مبدأ ارسال میکند. کامپیوتر مبدأ نیز Token اصلي را از بين برده و يك Token جديد توليد مينمايد و آن را در امتداد مسير Token قبلي به حركت در ميآورد. اين روند به همين صورت ادامه خواهد يافت.

در شبکه Token Ring در محل اتصال کامپیوترها به جاي هاب از دستگاهي به نام MAU استفاده ميشود. سرعت انتقال اطلاعات در اين شبکه 4Mbps يا 16Mbps است. کارتهاي 16Mbps ميتوانند با سرعت 4Mbps نيز فعاليت کنند.

شکل ۴-۴ (مفاهيم شبکه)

در شبکه Token Ring از کابلهاي زوج به هم تابيده استفاده ميشود. اگر از کابل UTP دراين توپولوژي استفاده شود، حداکثر طول کابل ميتواند ۴۵ متر باشد و اين شبکه فقط با سرعت ۴ مگابيت در ثانيه کار ميکند و اگر از کابل STP استفاده شود، حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابيت در ثانيه اطلاعات منتقل ميشود.

FDDI ۴-۲

FDDI، تکنولوژي يك شبکه با سرعت ۱۰۰ مگابيت در ثانيه است که براي ارتباط از فيبر نوري استفاده ميکند. در اين تکنولوژي به جاي فيبر نوري ميتوان از کابل مسي نيز استفاده کرد ولي در صورت استفاده از کابل مسي حداکثر فاصله مجاز در شبکه کمتر ميشود. FDDI به عنوان Backbone در محلهايي که تعداد زيادي کامپيوتر در آن قرار دارد ، استفاده ميشود. از جمله اين محيطها ميتوان به دانشگاه ها اشاره کرد. در FDDI ميتوان ۵۰۰ گره را در مسافت ۱۰۰ کيلومتر به يکديگر متصل کرد. توپولوژي فيزيکي اين شبکه حلقوي است. نحوه به وجود آمدن اين حلقه به اين صورت است که يك حلقه ۱۰۰ کيلومتري از فيبر نوري ساخته ميشود و در هر ۲ کيلومتر يك تقويت کننده قرار ميگيرد. براي جلوگيري از اختلالاتي که در اثر قطع شدن فيبر نوري به وجود ميآيد، از دو حلقه فيبر نوري در کنار هم استفاده ميشود تا در صورتي که يکي از رشته ها قطع شود، رشته دوم وارد عمل شده و جايگزين رشته اول شود.

خود آزمایی و تحقیق

۱- انواع معماري شبكه را نام ببريد و ويژگيهاي هر يك را از لحاظ حداقل و حداكثر طول كابل بين دو كامپيوتر، سرعت و نوع كابل و تجهيزات جانبي بررسي كنيد.

۲- FDDI چيست؟

۳- براي جل.گيري از اختلالاتي كه در اثر قطع شدن فيبرنوري به وجود مي آيد، چه بايد كرد؟

۴- تفاوت اصلي استانداردهاي IEEE در چيست؟

۵- تحقيق كنيد كه تفاوت MAU و HUB در چيست؟

فصل پنجم- آشنايي با پروتكلها

هدف هاي رفتاري
انواع پروتكلهاي رايج در شبكه تعريف كند.
سرويس هاي رايج در پروتكل TCP/IP را شناسايي كند.
سرويس هاي رايج در سبكه اينترنت را شرح دهد.
مفهوم Host در پروتكل TCP/IP را بيان كند.
انواع دامنه هاي رايج را بيان كند.
مراح ثبت Domain را شرح دهد.
انواع كلاس هاي IP را شناسايي كند.

بهره‌برداري از امكانات سخت‌افزاري و برقراري ارتباط بين اجزاي مختلف شبكه نياز به يك مجموعه از قوانين و دستورالعملهاي مشترك دارد كه به آن قوانين اصطلاحاً پروتكل مي‌گوييم.

مثال : كلاس درس خود را بعنوان يك شبكه درنظر بگيريد. هريك از اجزاي اين شبكه عبارتند از :
هدف : ارايه سرويس آموزشی
هنرجويان : بعنوان سر
هنر آموز درس : بعنوا
هوا : بعنوان محيط انت
گوش و دهان : بعنوان رابط شبكه (Network Interface)
چه چيزي را مي‌توان بعنوان پروتكل در كلاس متصور شد ؟
شايد بتوانيم "حضور بموقع هنر آموز درس و هنرجو در كلاس ، داشتن ساعات تنفس بمنظور استراحت ، ارائة درس به زبان قابل فهم هنرجويان (مثلاً فارسي) ، ارائة روشهايي منظم بمنظور پرسش و پاسخ ، برگزاري آزمون و . . . " را بعنوان پروتكل كلاس درنظر بگيريم . همانطور كه از عبارات فوق پيداست پروتكل مجموعه قوانيني است كه اگر آنها را رعايت نكنيم ارائة سرويس آموزشي (يعني هدف از برقراري شبكه) غيرممكن خواهد شد..
تعريف : پروتكل مجموعة قوانيني نرم افزاري است كه رعايت آنها باعث بهره‌برداري از امكانات سخت‌افزاري و برقراري سرويس در شبكه مي‌شود.
البته در عمل براي هر "تكنولوژي سخت‌افزاري مدرن " نياز به نرم افزار مناسب بعنوان "قانون يا پروتكل" براي برنامه‌ريزي ، مديريت و بهره‌برداري از آن داريم و بعبارتي واژة "پروتكل نرم افزاري" ، يك واژة عام در عرصة IT بشمار مي‌رود (مثلاً سيستم عامل نرم افزاريست شامل پروتكل هاي بسيار متنوع براي برنامه‌ريزي ، بهره‌برداري و مديريت منابع مختلف يك كامپيوتر) با اين‌حال نظر به اهميت واژة "پروتكل" در شبكه‌هاي كامپيوتري بطور خاص آنرا مورد بحث قرار مي دهيم.
۳ مورد از پروتكلهاي معروف در شبكه‌ها (مخصوصاً شبكه‌هاي متشكل از كامپيوترهاي شخصي) عبارتند از :
الف) NetBEUI
ب) IPX/SPX
ج) TCP/IP

NetBEUI =NetBIOS Enhanced User Interface – ۵ – ۱

اين پروتكل كه نسخة اولية آن به NetBIOS معروف بود به وسيله ی تيمي براي شركت IBM طراحي و پياده‌سازي شد و هدف از آن برقراري ارتباط مابين سيستمهاي مختلف در يك شبكة كوچك بود. در شبكه‌هاي بزرگ نكات و مسائلي مطرح مي‌شود از قبيل امنيت، چگونگي تبادل ترافيك در حجم زياد، مسيريابي، و . . . كه اين مسائل در شبكه‌هاي كوچك اكثراً وجود نداشته يا كمرنگ است و چون NetBIOS براي شبكه‌هاي كوچك طراحي شده‌بود لذا اينگونه نكات نيز درآن ديده نشد يا بصورت جدي به آن پرداخته نشد. بعنوان مثال، اين پروتكل قابليت مسير يابی" Routable " ندارد و حجم ترافيك Broadcast درآن زياد است، مي‌دانيم كه در شبكه‌هاي بزرگ، روترها ارتباط مابين بخشهاي مختلف شبكه را برقرار كرده و لذا مسيريابي جزو الزامات در ارتباط بين آنهاست. همچنين در شبكه‌هاي بزرگ، ترافيك بطور طبيعي از حجم بيشتري برخوردار است لذا بايد سعي كرد تا از ايجاد Broadcast حتي‌المقدور خودداري شود و متأسفانه در NetBIOS يا NetBEUI هيچكدام از اين مسائل مد نظر قرار نگرفته البته ايرادي به آن وارد نيست چون از ابتدا هدف آن استفاده در محيطهاي كوچك بوده است.

مثال: قوانين وضع شده در حوزه‌هاي مختلف (مثلاً ترافيكي و امنيتي) براي يك روستاي كوچك طبيعتاً با يك شهر بزرگ مانند تهران متفاوت بوده و در تهران مشكلات بسيار بيشتر از يك روستاي كوچك است.

بطور خلاصه مي‌توانيم ويژگيهاي NetBEUI را مطابق زير فهرست كنيم. دقت كنيد كه غير از مورد اول كه جزء مزاياي پروتكل است بقية موارد از نقاط ضعف و عيوب آن بشمار مي‌رود:

۱	پيكربندي بسيار ساده	Very Simple Configuration
۲	كاربرد در شبكه‌هاي كوچك	Small Networks
۳	قابليت مسيريابي ندارد	Non Routable
۴	ترافيك BC در آن زياد است. *	High Broadcast Traffic

* BC=Broadcast

امروزه اين پروتكل تقريباً منسوخ شده‌است و درميان محصولات مايكروسافت نيز از XP به بعد بطور مستقيم در ليست پروتكلها ديده نمي‌شود.

نكته: هرچند امروزه اكثر نرم‌افزارها سرويسهاي شبكه‌اي خود را روي پروتكل TCP/IP عرضه مي‌كنند اما بااين‌حال برخي از برنامه‌هاي قديمي‌تر هنوز براساس پروتكل NetBIOS يا NetBEUI كار مي‌كنند. براي اينگونه برنامه‌ها، مايكروسافت سرويسي را در سيستم عامل هاي ويندوز خود پيش‌بيني كرده كه حكم يك واسطه و مبدل را دارد يعني سرويسهاي NetBIOS را روي بستر TCP/IP ارائه مي‌دهد و در نتيجه براي Application محيط NetBIOS شبيه سازي مي شود. اين سرويس معروف به = NetBT NetBIOS over TCP/IP بوده و بطور معمول در كلية ويندوزها فعال است.

IPX/SPX = Internetworking Packet Exchange / Sequential Packet Exchange – ۵ – ۲

پروتكل IPX/SPX به وسيله ی شركت Xerox طراحي شد و بعداً به وسيله ی شركت Novell تكميل و مورد استفادة عملي قرار گرفت لذا اكثراً به‌محض آنكه نام پروتكل را مي‌شنوند به ياد Novell مي‌افتند. البته در سيستمهاي Novell نسخه‌هاي 4.0 و عمدتاً 5.0 به بعد، از TCP/IP نيز

مي‌توان استفاده كرد. پروتكل IPX/SPX هيچيك از نقاط ضعف NetBIOS را نداشته و بسيار پروتكل قدرتمندي است اما قابليت TCP/IP باعث شده است كه از IPX/SPX كمتر استفاده شود.

مهم ترين ويژگي هاي اين پروتكل عبارتند از :

۱ پيكربندي نسبتاً ساده	Simple Configuration
۲ در هر ابعادي از شبكه، كوچك يا بزرگ قابل استفاده است.	Any Scale of Network
۳ قابليت مسيريابي دارد.	Routable
۴ حق انتخاب در انتقال اطلاعات بصورت "عادي"(CL) يا "سفارشي"(CO)	Connection Oriented (SPX) & Connection less Services (IPX)
۵ عمدتاً در محيطهايي كه سيستم عاملهاي قديمي Novell يافت مي‌شوند كاربرد دارد.	Old Novell Netware Networks

TCP/IP = Transmission Control Protocol / Internet Protocol ۳-۵-

پروتكل TCP/IP در ابتدا به وسيله ی وزارت دفاع آمريكا و در سيستم عامل UNIX ايجاد شد. امروزه اين پروتكل تقريباً كلية رقبا را كنار زده و در اكثر شبكه‌ها اعم از كوچك و بزرگ و به وسيله ی كلية سيستم عاملها پشتيباني مي‌شود. در اهميت TCP/IP توجه به اين نكته كافيست كه ارتباط در اينترنت بدون TCP/IP تقريباً غيرممكن است و اكثر سرويسهاي اينترنت تحت قوانين TCP/IP عرضه مي‌شوند.
مهمترين خصوصيات اين پروتكل بطور خلاصه عبارتند از :

۱- پشتيباني انواع شبكه	Supports any network scale (small . . Large) or (Low Traffic . . . High Traffic)
۲- پشتيباني انواع سيستم عامل	Supported by all Operating Systems.
۳-مورد استفاده به عنوان پروتكل اصلي	Used as a primary protocol in the Internet
۴- مسير يابي	Routable
۵-حق انتخاب در انتقال اطلاعات به صورت عادي و سفارشي	Connection Oriented Services (TCP) , Connection less Services (UDP)
۷- ارسال گروهي	Multicasting
۸- پيكر بندي پيچيده	Complex Configuration

- اولين ويژگي در TCP/IP (همانند IPX/SPX) آنست كه مي‌تواند در هر ابعادي از شبكه استفاده شود اعم از شبكه‌هاي كوچك يا بزرگ ، ترافيك كم يا ترافيك زياد و بالاخره اعم از اينكه به اينترنت متصل باشد يا خير.
- چون TCP/IP در كلية سيستم عاملهاي مدرن امروزي پشتيباني مي‌شود لذا زبان مشترك براي ارتباط بين آنها بشمار مي‌رود.
- TCP/IP از ابتدا تا به امروز بعنوان پروتكل اصلي مورد استفاده در اينترنت بوده است.
- در TCP/IP الگوريتم هاي متنوع مسيريابي (Routing) براي انتخاب مسير بهينه از ميان روترها تعبيه شده و بدين سبب يكي از مهمترين پروتكلها براي استفاده در شبكه‌هاي WAN بشمار مي‌رود. همانطور كه قبلاً گفتيم در شبكه‌هاي WAN اغلب توپولوژي حاصله از نوع Mesh است و در نقاط مرزي مابين شبكه‌ها از Router استفاده مي‌شود لذا پروتكل مورد استفاده بايد داراي قابليت مسيريابي (Routing) باشد.

- سرويس انتقال اطلاعات بصورت سفارشي "Connection Oriented" معروف به TCP و سرويس انتقال اطلاعات بصورت عادي "Connection less" معروف به UDP از ديگر بخشهاي متنوع اين پروتكل است.
- Multicasting بمعني ارسال اطلاعات براي گروهي از استفاده‌كنندگان است.

يادآوري : بطور كلي ۳ نوع مخاطب در شبكه‌ها وجود دارد :
الف) Unicast : ارسال براي فقط يكنفر.
ب) Broadcast : ارسال براي همه تا محدودة مجاز (دفعتاً).
ج) Multicast : ارسال براي گروهي از استفاده‌كنندگان تا محدودة مجاز (دفعتاً).

Multicasting از ديگر خصوصيات TCP/IP است كه به كمك آن براحتي مي‌توان سيستم ها ، افراد يا نيازها را گروه‌بندي كرده و اطلاعات را براي تمام اعضاي گروه ارسال كرد.

فرض كنيد كه يك دستگاه Multimedia Server مي‌خواهد برنامة كاملاً مشخصي، مثلاً فيلمی را براي ۵۰۰ نفر مشترك كه در سه شبكه مختلف هستند پخش كند از اين تعداد، ۳۰۰ نفر در شبكة اول، ۱۵۰ نفر در شبكة دوم، و ۵۰ نفر در شبكة سوم هستند. ارتباط مابين شبكه‌ها از طريق روترهاي R1، R2 و R3 برقرار شده. چه روشهايي را براي پخش برنامة مذكور پيشنهاد مي‌كنيد؟ حالات مختلف را بررسي مي‌كنيم:

الف) كلية مشتركين هركدام يك به يك با سرور ارتباط برقرار كرده و سرور براي هركدام بطور جداگانه برنامه را پخش كند. بعبارت ديگر بصورت Unicast.

ب) سرور برنامه را Broadcast كند كه در اين صورت با ۲ مشكل مواجه مي‌شويم:

۱- Broadcast ترافيك شبكه را افزايش داده ضمن آنكه بقية كاربران ديگر كه نيازي به دريافت برنامه را از سرور ندارند درگير ترافيك ناخواسته مي‌شوند.

۲- روترها اجازة عبور ترافيك Broadcast را نمي‌دهند لذا مشتركين شبكه‌هاي شماره ۲و۳ قادر به دريافت برنامه نخواهند بود.

ج) كلية مشتركين را در يك گروه قرار داده و سرور برنامه را براي گروه Multicast كند. روترها نيز طوري پيكربندي مي‌شوند كه ترافيك Multicast را عبور دهند.

پرسش: به‌نظر شما كداميك از راه‌حلهاي فوق بهتر بوده و ترافيك كمتري را ايجاد مي‌كند؟

بالاخره آخرين خصوصيت TCP/IP كه درواقع عيب آن بشمار مي‌رود اينست كه پيكربندي پيچيده‌اي دارد. علت اين پيچيدگي را مي‌توان در تنوع سرويسهاي ارائه شده جستجو كرد. TCP/IP بسيار پروتكل كامل و متنوعي‌است و طبيعتاً اين تنوع ، پيچيدگي در پيكربندي را بدنبال خواهد داشت. البته تعبيه‌كنندگان TCP/IP تمهيداتي انديشيده‌اند تا قدري از پيچيدگي پيكربندي در آن كاسته شود (Automatic/Dynamic Configuration) و در واقع در اغلب اوقات، كاربران نيازي به درگير شدن باپيچيدگي هاي پيكربندي ندارند.

۴-۵- سرويسهاي TCP/IP

TCP/IP از سرويس هاي متنوعي تشكيل شده كه اغلب نيازهاي كاربران در شبكه‌ها را مستقيماً و بدون نياز به هرگونه برنامه‌نويسي اضافي پاسخ مي‌دهد. اغلب اين سرويسها براي كاربران آشنا بوده و در كاربردهاي روزمرة خود در اينترنت از آنها استفاده مي‌كنند. به موارد زير توجه كنيد :

۱-۵-۴ FTP[1] = File Transfer Protocol

[1] - در درس بسته هاي نرم افزاري ۳ با FTP به طور مشروح تر آشنا مي شويد

يكي از ضروري‌ترين كارهايي كه اغلب كاربران در شبكه بدان نياز دارند انتقال فايل است. TCP/IP مستقيماً داراي سرويسي است كه انتقال فايل را براحتي بين ماشينهاي مختلف با سخت‌افزارهاي متنوع و سيستم عاملهاي گوناگون امكان‌پذير مي‌سازد و آن FTP است. FTP از دو قسمت تشكيل شده :

الف) FTP Client

ب) FTP Server

كاربر با اجراي نرم‌افزار FTP Client به FTP Server متصل شده و با توجه به مجوزهاي امنيتي مربوطه مي‌تواند فايلهاي مورد نياز را از سرور دريافت كرده (Download–Receive) يا آنها را روي سرور ذخيره كند. (Upload-Send)

در سيستم عاملهاي Microsoft نرم‌افزارهاي گوناگوني بعنوان FTP Client وجود دارند مثلاً مي‌توانيم به IE (Internet Explorer) اشاره كنيم كه از خود مايكروسافت است يا دستور ftp.exe كه در حالت Text از Command_Prompt اجرا مي‌شود. نرم‌افزارهاي ديگر مانند Cute FTP ، FTP Pro ، DAP و . . . نيز همگي نقش FTP Client را بازي مي‌كنند.

نرم‌افزارهايي كه بعنوان FTP Server در مايكروسافت استفاده مي‌شوند نيز موجود بوده و بعنوان مثال مي‌توان به IIS اشاره كرد. IIS بسته‌ايست شامل چندين سرويس كه يكي از آنها FTP Server است.

فعاليت عملي، آشنايي با سرويس FTP : در اين بخش هنر آموز درس FTP Server را از قبل روي يك كامپيوتر با سيستم عامل 2000 يا 2003 سرور پيكربندي كرده و هنرجويان با اجراي FTP Client در كامپيوترهاي خود (ترجيحاً IE) چند فايل را از سرور دريافت (Download) كنيد. در اين مرحله به هيچ عنوان نيازي به فراگيري پيكربندي FTP Server نبوده و هنرجويان فقط از آن استفاده مي‌كنند.

۳-۴-۵- HTTP = Hyper Text Transfer Protocol

يك راه بسيار رايج براي دستيابي به اطلاعات كه همگي با آن آشنا هستيم استفاده از سرويس HTTP است. همانند FTP، اين سرويس نيز از دو بخش تشكيل شده :

الف) HTTP Client : كه به Web Client ، Web Browser يا به اختصار Browser هم مشهور است.

ب) HTTP Server : كه به Web Server نيز معروف است.

كاربران نرم‌افزار HTTP Client را (مانند IE ، Netscape ، Fire Fox و . . .) اجرا كرده و درخواست دسترسي به اطلاعات يا حتي اجراي برنامه را به سرور ارسال مي‌كنند (HTTP Request). سرور اين درخواست را بررسي كرده و پس از آماده كردن پاسخ ، آنها را قالب خاصي معروف به Web Page به سمت Client ارسال مي‌كند. سرويس گيرنده اين صفحات را دريافت كرده و با فرمت مناسب به كاربر نشان مي‌دهد. همانطور كه مي‌دانيم زبان مورد استفاده در صفحات وب اكثراً HTML يا XML است.

فعاليت عملي، آشنايي با سرويس HTTP : هرچند اغلب هنرجويان و حتي كاربران عادي با اين سرويس آشنا هستند اما براي حفظ انسجام مطالب بيان‌شده ، هنر آموز درس مي‌تواند Web Server را بهمراه يك Web Page بسيار ساده از قبل آماده كرده و كاربران با HTTP Client (ترجيحاً IE) به آن دسترسي پيدا كنند. شايان ذكر است كه Web Server در مايكروسافت ، بخشي از بستة IIS است.

۳-۴-۵- SMTP = Simple Mail Transfer Protocol , POP3= Post Office Protocol (version 3)

هر دو سرويس فوق براي ارسال و دريافت EMail استفاده مي‌شوند. به شكل زير دقت كنيد :

شكل ۱-۵

همانطور كه از شكل پيداست كاربر براي تهيه ، ارسال ، دريافت و خواندن نامه از نرم‌افزار Mail Client استفاده مي‌كند. دو مورد از نرم‌افزارهاي معروف كه بعنوان Mail Client در مايكروسافت استفاده مي‌شوند عبارتند از Outlook_Express و Microsoft_Outlook (به اختصار OE و MO) . پس از اجراي Mail Client و پيكربندي آن ، كاربر مي‌تواند متن نامة خود را تايپ كرده ، در صورت نياز عكس يا فايلهاي ديگري را به آن پيوست كرده (Attachment) و پس از تعيين گيرنده و موضوع نامه (Subject) آنرا ارسال كند. به محض فشردن كليد Send تمامي محتواي نامه بهمراه ضمائم پيوست ، با پروتكل SMTP به‌سمت Mail Server ارسال مي‌شود. Mail Server پس از دريافت نامه از سوي كاربر به بررسي آدرس گيرنده مي‌پردازد و چنانچه گيرنده شخصي خارج از حوزة پستي خودش باشد آنرا با SMTP به Mail Server حوزة گيرنده تحويل مي‌دهد. Mail Server گيرنده پس از دريافت نامه از Mail Server فرستنده آنرا در پوشه مناسب كه در واقع صندوق پستي شخص گيرنده است ذخيره مي‌كند و فرايند ارسال نامه به اتمام مي‌رسد. حال از اين‌جا به بعد شخص گيرنده خودش وظيفه دارد كه در صورت تمايل به Mail Server حوزة خود متصل شده و با پروتكل POP3 نامه‌هايش را از سرور دريافت كرده و در صندوق پستي محلي واقع در كامپيوتر خودش منتقل كند. همانطور كه مي‌بينيم فرايند فوق تا حدي با روش عمومي ادارة پست در ارسال نامه متفاوت است چرا كه پستچي نامه را تا دم در منزل مي‌آورد اما در Email ما بايد خودمان به ادارة پست (Mail Server) مراجعه و پس از نشان دادن مجوز ، نامه را از صندوق پستي برداريم.

پروتكل HTTP از آن دسته پروتكل هايي است كه براي انتقال Email نيز از آن بهره مي‌برند. بعنوان مثال مي‌توان انتقال نامه از طريق yahoo يا Gmail را نام برد. براي تبادل نامه از طريق yahoo چگونه عمل مي‌كنيم؟

NNTP = Network News Transfer Protocol – ۵ – ۴ – ۴

سرويس NNTP سرويسي‌است براي دسترسي به اطلاعاتي كه به وسيله ی افراد مختلف ارسال شده و مشتركاً مورد استفاده قرار مي‌گيرد. اين سرويس نيز از دو قسمت تشكيل شده :

الف) NNTP Client : كه به News Client نيز معروف است.

ب) NNTP Server : كه به News Server نيز مشهور است.

روال كار بدين صورت است كه ابتدا به وسيله ی News Client به يك News Server متصل شده سپس گروه خبري را انتخاب و درآن عضو مي‌شويم(Subscribe) پس از عضويت در گروه خبري ، اطلاعات و اخبار متنوع در زمينة موردنظر از Server به سرويس گيرنده انتقال پيدا كرده و

اعضا در صورت تمايل مي‌توانند نظرات يا پرسشهاي خود را درمورد خبرها ارسال كنند يا خبر و سوال جديدي را به سرور ارسال كنند. شكل و شمايل كار بسيار شبيه به EMail است يعني اخباري كه در يك News Server ارائه مي‌شود همچون EMail شامل موضوع خبر (Subject) ، فرستندة خبر و تاريخ ارسال است و بدين سبب مي‌توان گفت كه NNTP بسيار شبيه به يك Mail Box است با اين تفاوت كه شخصي نبوده و بطور مشترك مورد استفادة همة اعضا قرار مي‌گيرد. در مايكروسافت ، نرم افزاري كه بعنوان News Client مورد استفاده قرار مي‌گيرد همان Mail Client است يعني Outlook Express منتهي بجاي پيكربندي براي Mail Account بايد آنرا براي News Account تنظيم كنيم.

Telnet = Tele Network – ۵ – ۴ – ۵

ترمينال عبارت است از وسيله‌اي كه براي ارسال و دريافت اطلاعات استفاده مي‌شود (مثلاً يك Keyboard و يك Monitor) اما هيچگونه پردازشي روي اطلاعات در آن صورت نمي‌گيرد و اصولاً پردازش اطلاعات در سيستم مركزي (Central System) انجام مي‌شود. منظور از سيستم مركزي ، مجموعه‌ايست داراي توانايي براي پردازش اطلاعات و اجراي دستورالعملها يعني مجموعه‌اي كه شامل CPU ، RAM ، HDD و . . . است. سيستم مركزي مي‌تواند يك كامپيوتر شخصی باشد ، مي‌تواند يك Mini Computer ، Main Frame يا يك Super Computer باشد. سيستم مركزي حتي مي‌تواند يكي از تجهيزات فعال مورد استفاده در شبكه باشد مثلاً يك Router ، Switch يا Hub. البته بديهي‌است كه در مورد اخير (تجهيزات شبكه) هدف ما از اتصال ترمينال به مثلاً يك روتر ، پردازش اطلاعات و اجراي Application براي كاربر نيست بلكه هدف پيكربندي يا كنترل آنست.

مثال ۱: تا چند سال پيش كه كامپيوترهاي شخصي رواج پيدا نكرده‌بودند ، كامپيوترهاي Main frame بعنوان سيستم مركزي براي پردازش اطلاعات استفاده مي‌شدند و كاربران به وسيلة يكي از روشهاي رايج در آن زمان (مثلاً Keyboard و Monitor كه در مجموع به آن ترمينال مي‌گوييم) با Main frame ارتباط برقرار مي كردند. بديهي است هيچگونه پردازشي در ترمينال روي اطلاعات انجام نمي‌شد و فقط بعنوان ورودي و خروجي استفاده مي‌شد.

مثال ۲: در برخي از بانكها ، جلوي هر كارمند باجه ، فقط يك مونيتور ، كي‌برد و يك چاپگر كوچك قرار دارد اما خبري از Case و ملحقات داخلي آن نيست ! چرا ؟ پردازش كجا انجام مي‌شود ؟ تجهيزات جلوي كارمند فقط بعنوان ترمينال استفاده مي‌شوند. پس سيستم مركزي كجاست ؟ اگر دقت كنيم در گوشه‌اي از بانك يك كامپيوتر شخصی قرار دارد كه بعنوان سرور عمل كرده و نقش سيستم مركزي را بازي مي‌كند و درواقع محل اجراي نرم افزارهاي بانكي و پردازش اطلاعات است. ترمينالها از طريق سخت‌افزار و كنترلر مناسب به آن متصل مي‌شوند.

مثال ۳: مدير شبكه (Network Administrator) مي‌تواند ترمينال را به Router متصل كرده ، آنرا پيكربندي كند و از مسيرهاي مختلفي كه روتر با آنها ارتباط دارد آگاهي پيدا كند. مي‌تواند مسيري را ببندد يا باز كند و . . .

روش اتصال ترمينالها به سيستم مركزي

راههاي متنوعي براي اتصال ترمينالها به سيستم مركزي وجود دارد ، كه به ۳ مورد آن اشاره مي‌كنيم :

۱ – Serial Port

۲ – USB

اکثر ترمینالها داراي يك Serial Port از نوع RS232 هستند که با کابل مناسب به سیستم مرکزي متصل مي‌شوند.
براي درك بهتر همان مثال بانکي (مثال ۳) را در نظر بگیرید. فرض کنید بانك داراي ۵ دستگاه ترمینال است و سیستم مرکزي نیز یك کامپیوتر شخصی معمولي با سخت‌افزار مناسب است. چگونه مي‌توان ۵ ترمینال را از طریق RS232 به کامپیوتر شخصی متصل کرد؟ مي‌دانیم هر کامپیوتر شخصی در حالت عادي حداکثر داراي ۲ عدد Serial Port است : Com1 & Com2 که آنهم ممکن است به وسیله ی Mouse و Modem اشغال باشد! راه حل آنست که از یك سخت‌افزار ویژه براي توسعة Serial Port استفاده کنیم. این کارتها معمولاً به Multi Port معروفند. پس از نصب کارت مذکور در کامپیوتر شخصی ، پورتهاي سریال افزایش یافته و مي‌توان ترمینالها را متصل کرد : Com3 ، Com4 ، Com5 و الي آخر.
برخي از ترمینالها براي اتصال خود با سیستم مرکزي مجهز به USB Port هستند و بالاخره برخي دیگر از آنها داراي یك کارت شبکه مثلاً با استاندارد 10BaseT یا 100BaseTX بوده که ترمینال را به شبکه وصل مي‌کند ، از طرفي چون سیستم مرکزي نیز خودش به شبکه متصل مي‌شود بنابراین ارتباط مابین Terminal و Central System برقرار مي‌شود. البته ترمینالهایي که داراي Network Interface هستند بنوعي در حد یك کامپیوتر شخصی محسوب مي‌شوند با این تفاوت که از آنها فقط به قصد یك ترمینال استفاده مي‌شود.

از نظر نحوة نمایش اطلاعات ، ترمینالها به ۲ دستة کلي تقسیم مي‌شوند:
الف) ترمینالهاي Text : فقط بصورت "متني" اطلاعات را نمایش مي‌دهند.
ب) ترمینالهاي Graphic : علاوه بر "متن" ، داراي توانایي ترسیم اشکال گرافیکي با رنگهاي متنوع نیز هستند.

تعریف Terminal Emulator : ممکن است در شبکه‌اي بجاي ترمینال از یك کامپیوتر شخصی استفاده کنند. مزیت استفاده از کامپیوتر شخصی بجاي ترمینال آنست که این کامپیوتر خود داراي توانایي پردازش اطلاعات است بنابراین مي‌توان علاوه بر کاربرد آن بعنوان یك ترمینال ، نرم افزارهاي متنوع دیگري را نیز مستقیماً روي آن اجرا کرد. اما در صورت نیاز چگونه مي‌توان کامپیوتر شخصی را تبدیل به یك ترمینال براي اتصال به سیستم مرکزي کرد؟ پاسخ بسیار ساده است : کافیست نرم افزار مناسب را روي آن اجرا کرد. این نرم افزارهاي در حالت کلي به "شبیه‌ساز ترمینال" یا "مقلد ترمینال" یا به زبان انگلیسي Terminal Emulator مشهورند و همچون ترمینالها داراي ۲ دستة کلي Text و Graphic در زمینة نحوة نمایش اطلاعاتند. طریقة اتصال سخت‌افزاري یك کامپیوتر شخصی که بعنوان ترمینال استفاده مي‌شود با Central System همچون نحوة ارتباط ترمینالهاست یعني :
الف) RS232 Serial Port
ب) USB
ج) Network
نرم افزارهاي Terminal Emulator که اطلاعات را بصورت Text نشان مي‌دهند بسیار متنوعند ، از آن جمله مي‌توان به Term95 ، PC Anywhere ، Kermit ، Closeup و Hyper Terminal اشاره کرد. مي‌دانیم که Hyper_Terminal تحت Windows اجرا مي‌شود اما در واقع فقط بصورت Text مي‌تواند اطلاعات را نمایش دهد.

با توجه به مقدمة فوق می توانیم Telnet را که از سرویسهاي TCP/IP است تعریف کنیم

اگر راه ارتباطي يك كامپيوتر شخصی با Central System از طريق شبكه باشد و پروتكل مورد استفاده نيز TCP/IP باشد در آنصورت Telnet عبارت است از يك سرويس Terminal Emulator كه اطلاعات را بصورت Text نشان مي‌دهد.
همچون ديگر سرويسها ، Telnet نيز از ۲ بخش تشكيل شده :
الف) Telnet Client : كه روي كامپيوتر شخصی اجرا مي‌شود و آنرا تبديل به ترمينال مي‌كند (در مايكروسافت : Telnet.exe)
ب) Telnet Server : يا Telnet Daemon يا به اختصار telnetd كه روي Central System اجرا شده و اطلاعات را از ترمينال Telnet)سرويس گيرنده(دريافت و پس از پردازش به وسيله ی سيستم مركزي ، براي ترمينال ارسال مي‌كند.

فعاليت عملي، آشنايي با سرويس Telnet : ابتدا بايد سيستم مركزي را انتخاب كرد. (مثلاً يك كامپيوتر با سيستم عامل UNIX ، يك كامپيوتر با سيستم عامل NT ، يك Router ، يك Wireless Access Point ، . .) سپس بايد مطمئن شد كه سرويس Telnet Server روي آن نصب و فعال است. (تا اينجاي كار بايد به وسيله ی هنر آموز درس انجام شود.) سپس هنرجويان نرم افزار Telnet Client را روي كامپيوترهاي خود اجرا كرده (Telnet.exe) و بدين ترتيب كامپيوتر آنها تبديل به يك ترمينال مي‌شود. قدم بعدي آنست كه به سيستم مركزي متصل شده و با آن به تبادل اطلاعات پرداخت. (اگر به اينترنت متصل هستيد ، مي‌توانيد سايتهاي بسياري را پيدا كنيد كه با telnet مي‌توان با آنها ارتباط گرفت منتهي بايد مجوز ورود را هم در صورت درخواست وارد كنيد. برخي از سايتها اجازة مي‌دهند با كاربر guest به سيستم Login كنيم. بعنوان مثال مي‌توانيد به از طريق Run فرمان زير را تايپ كرده و نتيجه را ببينيد، (كاربر را guest وارد كنيد) :

telnet victoria.tc.ca

۵-۴-۶ RDP = Remote Desktop Protocol

همانند Telnet است با اين تفاوت كه گرافيكي است. در مايكروسافت ، برنامة Remote Desktop از سرويس RDP استفاده كرده و كامپيوتر شخصی را تبديل به يك ترمينال گرافيكي مي‌كند.
همچون ديگر سرويسهاي TCP/IP ، RDP نيز از ۲ بخش تشكيل شده :
الف) RDP Client : كه به Terminal Client نيز معروف بوده و در مايكروسافت ، همان برنامة Remote_Desktop است (mstsc.exe)
ب) RDP Server : كه به Terminal Server نيز مشهور بوده و در مايكروسافت ، همان سرويس Remote_Desktop است كه از طريق System Properties فعال مي‌شود. البته در ويندوزهاي 2000 Server يا 2003 Server يك نسخة كاملتر از اين سرويس بنام Terminal Service از طريق زير نصب و فعال مي‌شود:
Add/Remove Programs -> Windows Components -> Terminal Service

فعاليت عملي، آشنايي با سرويس RDP : قبلاً در فصل ۱ دستورالعملهاي لازم براي فعال‌سازي RDP بكمك هنر آموز درس گفته‌شد لذا در صورت حضور ذهن هنرجو ، نيازي به تكرار تمرين نيست.

۵-۴-۷ SNMP = Simple Network Management Protocol

يكي از مسايل مهمي كه هر Administrator در شبكه‌هاي متوسط و بزرگ با آن مواجه است ، مديريت شبكه بشكل جامع و حتي‌المقدور يكپارچه است.

مثال ۱: مي‌خواهيم يك سويچ حرفه‌اي از شركت 3Com را مديريت كنيم بدين‌معني كه سويچ را پيكربندي كرده ، وضعيت آنرا از نظر ميزان ترافيك تبادلي در پورتهاي مختلف و خطاهاي بوجودآمده بررسي كنيم. پورتهاي آنرا ببنديم، بازكنيم و . . . . يكي از راههاي جالب براي مديريت سويچ كه در داخل آن تعبيه شده استفاده از HTTP است، منظور آنست كه سويچ خودش بطور داخلي (built-in) مجهز به يك Web Server است. مدير شبكه مي‌تواند Web Client خود را اجرا كرده (مثلاً IE) و فرمان ارتباط با سويچ را تايپ كند : http://<Switch_IP_Address> . بدين‌وسيله ارتباط با وب-سرور داخلي در سويچ برقرار شده و مي‌توانيم آنرا مديريت كنيم.

مثال ۲: مي‌خواهيم يك روتر از شركت Cisco را مديريت كنيم. از طريق Command Prompt فرمان زير را اجرا كرده و با آن ارتباط telnet برقرار مي‌كنيم و. . . <Router_IP_Address>

در مثال فوق ارتباط ما با روتر از طريق سرويس Telnet برقرار شده.

مثال ۳: مي‌خواهيم يك سرور 2000 را از طريق كامپيوتر خودمان مديريت كنيم. ابتدا نرم‌افزار Terminal Server را (كه در XP و 2003 بنامهاي Remote Desktop Service نيز معروف است) نصب و فعال كرده، سپس به وسيله ی برنامة Remote_Desktop_Client با آن ارتباط برقرار كرده و Desktop مربوط به سرور را در اختيار مي‌گيريم. حال براحتي مي‌توانيم سرور را در اختيار داشته باشيم

در مثال فوق ارتباط ما با سرور از طريق سرويس RDP برقرار شده.

مثال ۴: براي مديريت از راه دور يك كامپيوتر با سيستم عامل XP ، علاوه بر بهره‌گيري از Remote Desktop ، مي‌توان از برنامة Computer Management نيز استفاده كرد. براي اين كار با Administrator وارد سيستم شده، برنامة مذكور را اجرا كنيد (My Computer -> Manage)كليك راست پس از اجراي برنامه روي اولين آيكن يعني Computer Management (Local) راست كليك كرده و Connect to another computer را انتخاب كنيد. سپس با تايپ‌كردن نام يا آدرس كامپيوتر مقصد به آن متصل شده و از اين به بعد مي‌توانيم آنرا مديريت كنيم. براي عملكرد صحيح لازم است تا password مربوط به Administrator روي هردو كامپيوتر مبدأ و مقصد دقيقاً يكسان باشد.

در مثال فوق ارتباط ما از طريق سرويسهاي خاصي كه مايكروسافت تعبيه كرده برقرار شده.(RPC & Pipe)

نتيجه‌گيري: براي مديريت راههاي گوناگوني وجود دارد كه بستگي به تجهيزات، سيستم عامل، پروتكل مورد استفاده و پارامترهاي ديگر دارد اما آيا راه يكپارچه‌اي نيز هست؟ پاسخ مثبت بوده و راه‌حل، استفاده از SNMP است.

SNMP از دو بخش تشكيل شده:

الف) SNMP Agent : كه مسئول جمع‌آوري اطلاعات بوده و بايد روي هر سيستم ، تك به تك فعال شود.

ب) SNMP Viewer : كه به SNMP Manager نيز مشهور بوده و مسئول گردآوري و تجزيه و تحليل اطلاعات جمع‌آوري شده به وسيله ی كلية Agent ها در تمامي شبكه است.

شكل۲-۵

به شكل دقت كنيد. هر سيستمي كه بخواهد با SNMP مديريت شود بايد Agent را روي آن نصب و فعال كرد. كار Agent آنست كه اطلاعات مديريتي را جمع‌آوري كرده و آنها را در يك بانك اطلاعاتي محلي (Local

MIB = Management Information Base ذخیره می‌کند. بعنوان مثال (Database معروف به
اگر در یك شبکه ۱۰۰۰ سیستم داریم که می‌خواهیم آنها را با SNMP مدیریت کنیم باید روي همگي آنها Agent را فعال کنیم. در مایکروسافت، Agent از طریق زیر نصب و فعال می‌شود :
Add/Remove Programs -> Windows Components -> Management & Monitoring Tools
(وارد قسمت Details شده و فقط Simple Network Management Protocol را انتخاب کنید)
براي پیکربندي آن نیز باید از طریق سرویسهاي ویندوز وارد عمل شد. (در صورت نیاز بکمك هنر آموز درس انجام شود)
و اما اطلاعات جمع‌آوري شده به وسیله ی Agent را چگونه گردآوري و تجزیه تحلیل کنیم؟ کافیست روي یك کامپیوتر مثلاً متعلق به مدیر شبکه، نرم افزار SNMP Manager را نصب کنیم. یکي از بهترین نرم افزارهاي در این زمینه Solarwinds است (www.solarwinds.net). پس از پیکربندي نرم افزار می‌توان به سایر سیستمهاي مجهز به Agent در شبکه متصل شده و اطلاعات جمع‌آوري شده در MIB را گردآوري و تجزیه تحلیل کرد.

فعالیت عملي، آشنایي با سرویس SNMP : با توجه به اینکه مدیریت شبکه نیاز به تجربه و دانستن مقدمات پیشرفته‌تري دارد لذا در این مرحله نیازي به آشنایي عملي با SNMP نیست، با اینحال در صورت تمایل و داشتن فرصت کافي، هنر آموزمحترم می‌تواند ، خود Agent و Viewer را نصب و پیکربندي کرده و نحوة مدیریت شبکه را در حالات بسیار ساده به هنرجویان نشان دهد.

۸-۴-۵- SNTP (NTP) : Simple Network Time Protocol

ساعت دقیق در شبکه هایي که اطلاعات مالي، پرسنلي، مدیریت پروژه و . . . در آنها نگهداري می‌شود بسیار مهم است. در یك شبکه چگونه می‌توان مطمئن شد که ساعت در کلیة سیستمها بطور صحیح تنظیم شده؟
در اینجا NTP بکمك آمده و زمان را بین سرویس گیرنده و سرویس دهنده یکسان (Synchronize) می‌کند . در واقع NTP از دو بخش تشکیل شده :
الف) NTP Client : که به Time Client هم معروف است.
ب) NTP Server : که به آن Time Server نیز می‌گویند.
پس از پیکربندي، NTP Client در زمانهاي مشخص با NTP Server ارتباط برقرار کرده و ساعت خود را با ساعت سرور تنظیم می‌کند و بدین‌ترتیب ساعت تمام کامپیوترهاي شبکه دقیقاً یکسان شده و نیازي به تنظیم دستي نیست.
بد نیست بدانیم که Time Server خود می‌تواند یك Time Client باشد براي یك سرور دیگر. خوشبختانه در اینترنت، مراجع دقیقي بعنوان NTP Server وجود دارند (معروف به ساعت اتمي) که سرورهاي محلي می‌توانند زمان دقیق را از آنها دریافت کنند بعنوان مثال می‌توان به time.nist.gov اشاره کرد.

فعالیت عملي، آشنایي با سرویس NTP :

با کاربر Administrator وارد XP شده و روي آیکن Time واقع در سمت راست Taskbar دابل-کلیك کنید.

سومین قسمت از صفحة Time با نام Internet Time را باز کنید. لیستي از سرورهاي مرجع را می‌بینید که می‌توانید یکي از آنها را انتخاب و ساعت خود را با آن Update کنید. در شبکه هاي متوسط و بزرگ نیز می‌توان یك سرور 2000 یا 2003 را بعنوان Time Server در نظر گرفته و سپس کلیة سیستمهاي دیگر را با آن به هنگام (Update)کرد .

البته این امر در صورتی با موفقیت انجام می‌شود که اولاً سرویسی معروف به Windows Time در لیست سرویسهای ویندوز Start باشد، ثانیاً Date (روز و ماه و سال) از قبل صحیح باشد، ثالثاً Time Zone را Tehran انتخاب کرده‌باشیم، رابعاً اختلاف ساعت ما با ساعت واقعی بیش از ۱۲ ساعت نباشد، خامساً در بین راه یا حتی روی ماشین خودمان UDP Port 123 باز باشد.

۵-۵- آشنایی با مفهوم Host در پروتکل TCP/IP

Host را در فارسی به "میزبان" ترجمه می‌کنند. حال باید دید که "میزبان TCP/IP" به چه معنی است.

تعریف: به هر سیستم در شبکه که از پروتکل TCP/IP برای ارتباط استفاده کند اصطلاحاً یک TCP/IP Host یا "میزبان TCP/IP" می‌گوییم.

به دیگر بیان، در شبکه‌های کامپیوتری که اجزای آن از پروتکل TCP/IP استفاده می‌کنند، به هر سیستمی که TCP/IP روی آن پیکربندی و فعال شده و بتوان با قوانین TCP/IP با آن ارتباط گرفت یک Host گفته می‌شود.

مثال ۱: کلیهٔ کامپیوترهای شخصی در یک شبکه که پروتکل TCP/IP روی آنها تنظیم و فعال شده اعم از اینکه سرویس گیرنده باشند یا سرویس دهنده، هرکدام برای خود یک Host مستقل به حساب می‌آیند.

مثال ۲: یک روتر را می‌توان یک TCP/IP Host بشمار آورد، چرا که می‌توان و باید TCP/IP را روی آن پیکربندی و فعال تا آنرا از آن طریق کنترل کرد.

مثال ۳: برخی از سویچهای حرفه‌ای توانایی پیکربندی و کنترل خود را از طریق TCP/IP به مدیر شبکه می‌دهند، پس این سویچها نیز TCP/IP Host هستند.

مثال ۴: برخی از دوربینهای دیجیتال مستقیماً به شبکه متصل شده (10Base T / 100Base TX) و می‌توان بکمک TCP/IP با آنها ارتباط برقرار کرده و تصاویر را از آنها دریافت کرد. در این حالت، دوربین، یک TCP/IP Host است.

مثال ۵: برخی از UPS ها توانایی اتصال مستقیم به شبکه را دارند. می‌توان از طریق یک کامپیوتر شخصی و پروتکل TCP/IP آنها را کنترل کرد. چنین UPS هایی در واقع مثال دیگری‌است از TCP/IP Host.

مثال ۶: چاپگرهایی هستند که مستقیماً به شبکه متصل شده و کامپیوترهای شخصی می‌توانند کارهای چاپی خود را از طریق TCP/IP به آنها ارسال کنند، پس این چاپگرها نیز بیانگر TCP/IP Host هستند.

هر Host در TCP/IP دارای ۲ مشخصهٔ اصلی و بارز است. بعبارت دیگر هر Host را می‌توان با ۲ خصوصیت از بقیهٔ Host ها تفکیک کرد. این دو مشخصه عبارتند از :

الف) نام (Host Name)

ب) آدرس(Host Address = IP Address)

نکته: اگر بخواهیم اصل ماجرا را درنظر بگیریم، آدرس در اولویت اول قرار داشته و هر Host باید حداقل یک آدرس منحصربفرد داشته باشد. مشخصهٔ "نام" برای سهولت در کار کاربران بوده اما برای پروتکل TCP/IP چندان مهم نیست. در واقع هنگامی که یک کاربر برای برقراری ارتباط با یک TCP/IP Host از "نام" استفاده می‌کند (مثلاً http://www.yahoo.com) پروتکل TCP/IP به زحمت افتاده و باید آدرس مربوط به نام را پیدا کند چون مهم برای او IP Address است. به‌عبارت دیگر پروتکل با مکانیزمهایی که بعدا مورد بحث قرار می‌گیرد ابتدا اسم را به IP تبدیل کرده (مثلاً یکی از آدرسهای www.yahoo.com می‌شود 216.109.118.76) و بعد ارتباط با سایت آغاز می‌شود: http://216.109.118.76.

اجازه دهيد كمي بيشتر در مورد اسامي Host و قوانين مربوطه صحبت كنيم:

شرح بيشتر Host Name :
گفتيم كه براي سهولت بيشتر كاربران، براي اكثر "ميزبانهاي مهم" (Host) يك يا چند نام انتخاب مي‌شود. بديهي است كه اين نامها بايد از قوانيني تبعيت كرده و ضمناً مورد تأييد "مراكز ثبت اسامي" نيز قرار بگيرند، به زبان ديگر بايد اسم را ثبت (Register) كرد. چنانچه اسم يك Host ثبت نشود درآنصورت استفاده از نام معمولاً محدود به كاربردهاي داخلي شده و اغلب كاربران "خارج از شبكة داخلي" نام را نمي‌شناسند چرا كه رسماً ثبت نشده.
مثال: هركدام از ما انسانها مجازيم در محدودة خانوادگي خودمان يا ميان دوستان و آشنايان هراسمي را به خودمان بدهيم اما هنگامي كه مي‌خواهيم خود را رسماً به همه معرفي كنيم يا ديگران ما را رسماً صدا بزنند بديهي‌است كه از اين اسامي كذايي و متنوعي كه روي خودمان گذاشته‌ايم استفاده نخواهند كرد بلكه "اسم شناسنامه‌اي" ما را كه در ادارة ثبت احوال درج شده بكار مي‌برند چرا كه همگان "ادارة ثبت احوال" را بعنوان "مركز معتبر ثبت اسامي" قبول دارند.
اكنون نگاهي دقيقتر به قالب اسامي داشته باشيم، بطور كلي مي‌توانيم دو قالب را براي نامگذاري تصور كنيم. با دقت به مثالهاي زير موضوع روشن مي‌شود:
قالب اول: هريك از اسامي زير بعنوان يك Host Name مي‌تواند در پروتكل TCP/IP استفاده شود:

Shiva	Reza	Server22	Client80	PC1
C2	C1	Palang	Moon	Star

قالب دوم:

7)	www.tamin.org	1)	www.yahoo.com
8)	www.sharif.edu	2)	mail.yahoo.com
9)	sina.sharif.ac.ir	3)	www.neda.net.ir
10)	www.itrc.ac.ir	4)	ftp.dlink.com
11)	time.nist.gov	5)	ftp.microsoft.com
12)	www.dci.ir	6)	www.sanjesh.org

پرسش: تفاوت بين قالب اول و دوم در چيست؟ بروشني پيداست كه قالب دوم كامل تر است، اصطلاحاً اگر اسمي در قالب اول باشد به آن اسم مستعار Alias يا Unqualified و اگر در قالب دوم باشد به آن FQDN = Fully Qualified Domain Name مي‌گويند.
معمولاً اسامي قالب اول در محدودة داخلي شبكه‌ها استفاده شده، نيازي به ثبت ندارند اما اسامي قالب دوم عمدتاً ثبت شده و در اينصورت چه در محدودة داخلي و چه افراد خارج از شبكة داخلي مي‌توانند از آنها براي مراجعه به Host استفاده كنند.(همانطوركه تأكيد شد، اسامي اعم از قالب اول يا دوم در ابتداي كار به وسيله ی TCP/IP به آدرس تبديل مي‌شوند)

پرسش: يك اسم در قالب دوم (FQDN) معمولاً از چه قسمتهايي تشكيل مي‌شود؟
در جواب می توان گفت به‌ترتيب از سمت چپ:
الف) نام يا سرويسي كه Host ارائه مي‌دهد يا نقشي كه Host بازي مي‌كند. (Host Role or Host Service)
مثال:

mail =	Mail server	www =	Web Server

ftp = FTP Server time = Time Server
news = News (NNTP) Server

ب) نام شرکت، سازمان، مجموعه یا شخصي که Host بدان تعلق دارد. (Company Name)
مثال:
yahoo , google, sun, microsoft, IRIB, Bank-Keshavarzi, . . .

ج) حوزة فعاليت ميزبان. (Activities)
مثال:
com, net, org, gov, mil, edu, ac, info, int, biz, tv, ws, . . .

د) وابستگي منطقه اي و محلي اعم از فرهنگي، اجتماعي، . . . يا زبان استفاده شده در سايت. (Locality)
مثال:
ir = Iran tr = Turkey uk = United Kingdom ca= Canada fr = France
iq = Iraq tw = Taiwan us = United States

نكته ۱: براي ديدن ليست كاملي از كدهاي دو حرفي مربوط به كشورهاي مختلف كافي‌است در google عبارت زير را جستجو كنيد: "Country codes" يا مستقيماً به سايت www.iana.org مراجعه كنيد.
نكته ۲: با توجه به مثالهاي قالب دوم ممكن است برخي از اجزاي ياد شده در FQDN موجود نباشد مثلاً در اكثر آنها "بند ت" (Locality) ديده نمي‌شود يا يك از اسامي دانشگاه شريف با sina شروع مي‌شود و "سينا" بيانگر سرويس نيست بلكه فقط يك اسم است. در مثال ديگري مربوط به سايت شركت ديتا www.dci.ir مي‌بينيم كه حوزة فعاليت درآن ديده نمي‌شود اما به هر حال FQDN هرچه‌قدر هم كه ناقص باشد، اجزاي آن بايد از چپ به راست ترتيب ياد شده را رعايت كنند و نبايد آنها را جابجا كرد مثلاً www.com.yahoo صحيح نيست.
Domain يعني چه؟
به اين مثالها توجه كنيد:

www. microsoft.com
Domain
www.neda.net.ir
Domain

به عبارت ديگر مي‌توان گفت كه در يك FQDN چنانچه بخش ابتدائي سمت چپ را كه (بيانگر نام سرويس است) كنار بگذاريم، به‌مجموع بقية قسمتها Domain گفته مي‌شود كه شامل نام شركت، حوزة فعاليت و كشور مي‌شود.
بنابراين FQDN بطور كلي از دو بخش تشكيل شده:

جدول

FQDN =	Service Name	+	Domain Name
	www		microsoft.com
	ftp		dlink.com
	time		nist.gov
	msnews		microsoft.com

Sub Domain به زير مجموعه هاي يك Domain اصطلاحا "SubDomain مي‌گويند. در عمل معمولا" از SubDomain براي نشان دادن شركتها، زيرگروهها يا ساختارهاي فرعي در يك مجموعة بزرگ استفاده مي‌شود.
مثال: يك شركت بزرگ كامپيوتري را درنظر بگيريد كه علاوه بر شركت اصلي، از ۳ شركت زيرمجموعه براي فعاليتهاي سخت‌افزار، نرم افزار و شبكه استفاده مي‌كند. براي شركت اصلي، يك Domain بنام a.net را درنظر گرفته آنرا ثبت مي‌كنيم. حال با توجه به

گستردگي فعاليتهاي بزرگرايان و طبيعتاً شركتهاي زيرمجموعه، بد نيست كه براي هركدام از زيرمجموعه‌ها نيز يك domain درنظر بگيريم :

براي شركت سخت‌افزار : hardware.a.net

براي شركت نرم افزار : software.a.net

براي شركت شبكه : network.a.net

هريك از domain هاي فوق را اصطلاحاً يك SubDomain از a.net مي‌ناميم.

چنانچه شركت اصلي و بخشهاي تابعه، هريك براي خود Web-Server داشته باشند در آنصورت داراي اسامي زير خواهند بود:

وب سرور شركت اصلي	www.a.net
وب سرور شركت سخت‌افزار	www.hardware.a.net
وب سرور شركت نرم افزار	www.software.a.net
وب سرور شركت شبكه	www.network.a.net

در كامپيوترهايي كه از سيستم عاملهاي خانوادة Microsoft بهره برده و در ضمن پروتكل TCP/IP روي آنها فعال مي‌شود، ۲ اسم مد نظر قرار مي‌گيرد:

الف) هنگام نصب OS يك اسم حداكثر ۱۵ كاراكتري به كامپيوتر داده مي‌شود كه بايد درمحدودة شبكة داخلي منحصر بفرد بوده تكراري نباشد. اين اسم به Computer Name يا NetBIOS Name معروف است. (لزومي ندارد كه حتماً" پروتكل NetBIOS روي كامپيوتر نصب باشد، در هر صورت به آن NetBIOS Name مي‌گويند). مي‌دانيم كه در سيستم عامل XP يا 2003 براي تغيير NetBIOS Name از System Properties وارد عمل شده، قسمت Computer Name را انتخاب و پس از فشردن كليد Change ، نام كامپيوتر را تغيير داده و تأييد OK مي‌زنيم.

ب) TCP/IP Name كه همان Host Name در پروتكل TCP/IP بوده و به Full Computer Name نيز معروف است و ممكن است در قالب اول يا دوم باشد. بصورت پيش فرض در كامپيوترهايي كه عضو Work Group باشند TCP/IP Name دقيقاً" برابر با NetBIOS Name است از طرفي چون NetBIOS Name عمدتاً" ساده و تك قسمتي بوده لذا TCP/IP Name هم بصورت تك قسمتي برابر با آن مي‌شود يعني در قالب اول است.

اگر كامپيوتر به عضويت Domain در Active Directory درآيد آنگاه TCP/IP Name بصورت زير در مي‌آيد:

TCP/IP Name = NetBIOS Name + Active Directory Domain Name

يعني TCP/IP Name در قالب دوم مي‌شود.

به‌هرحال براي تغيير Domain در TCP/IP Name از طريق System Properties وارد عمل شده و قسمت Computer Name را انتخاب و پس از فشردن كليد Change و متعاقب آن كليد More ، نام Domain را در قسمت Primary DNS Suffix for this computer وارد كرده و تأييد OK كنيد. با تأييد مجدد (OK) ، سيستم عامل از شما مي‌خواهد تا كامپيوتر را Restart كنيد. پس از Restart ، وارد Command Prompt شده و با اجراي دستور ipconfig /all و بررسي خطوط اوليه ، نتيجة كار خود را بررسي كنيد.

فعاليت عملي: هر گروه از هنرجويان كه يكدستگاه كامپيوتر مستقل در اختيار دارند بدخواه يك Domain Name انتخاب كرده سپس Full Computer Name را در سيستم خود تغيير دهند.

البته همانطور كه گفته شده اسامي TCP/IP در قالب دوم تا هنگامي‌كه رسماً در "مراكز شناخته‌شدة ثبت اسامي" يا به زبان فني (DNS Server) ثبت نشوند نمي‌توانند مورد استفادة بقيه قرار گيرند لذا فعاليت عملي فوق صرفاً" براي آشنايي بيشتر هنرجو با Full Computer Name و مفهوم FQDN بوده، توصيه مي‌شود كه حتماً انجام شود.

در این قسمت به توضیحات پیرامون Host Name خاتمه داده و مبحث IP Address را آغاز میکنیم:

Host Address = IP Address

هر Host در پروتکل TCP/IP باید "حداقل" یك آدرس منحصر بفرد داشته باشد که به آن IP Address میگویند.
نکته ۱: فعلا" راجع به اینکه چرا میگوییم "حداقل"، حرفی نمیزنیم.
نکته ۲: "منحصر بفرد بودن" زماني مهم است که شبکه ها با یکدیگر در ارتباط باشند وگرنه هنگامي که هیچگونه ارتباطي (با روتر) بین شبکه ها برقرار نیست چه اهمیتي دارد که آدرسهاي مورد استفاده در یك شبکه با دیگر شبکه ها تکراري باشد.
نکته ۳: ممکن است شبکه ها به یکدیگر متصل باشند و آدرسهاي تکراري در آنها پیدا شود این امر در صورتي که اصطلاحا" عمل "ترجمة آدرس" یا Network Address Translation = NAT روي آنها صورت بگیرد اشکالي ندارد. بحث راجع به NAT را به دوره هاي پیشرفته‌تر موکول میکنیم.
IP Address یك عدد ۴ بایتي (۲۳ بیتي) بوده که به‌فرم w.x.y.z تنظیم میشود. بدیهي است که 0<w,x,y,z <255 .
البته اعداد مرزي یعني 0 و 255 را باید طبق قوانین خاصي استفاده کرد که به تفصیل مورد بحث قرار میگیرد. حال براي آنکه بتوانیم اجزاي IP Address و چگونگي تنظیم آنرا درك کنیم بهتراست نگاهي سریع به شکلهاي ۱ تا ۴ داشته‌باشیم.
در این شکلها مجموعاً ۴ شبکة متفاوت ترسیم شده که با دقت در آدرسهاي بکاررفته میتوانیم نکات زیر را کشف کنیم:
الف) هر آدرس از ۲ قسمت تشکیل شده: یك قسمت در سمت چپ که بین تمامي سیستمهاي بکار رفته در هر شبکه مشترك است و یك قسمت در سمت راست که براي هر سیستم منحصر بفرد است. بعبارت دیگر IP Address از دو بخش زیر تشکیل شده:

a) Network ID or Net ID
b) Host ID or Node ID

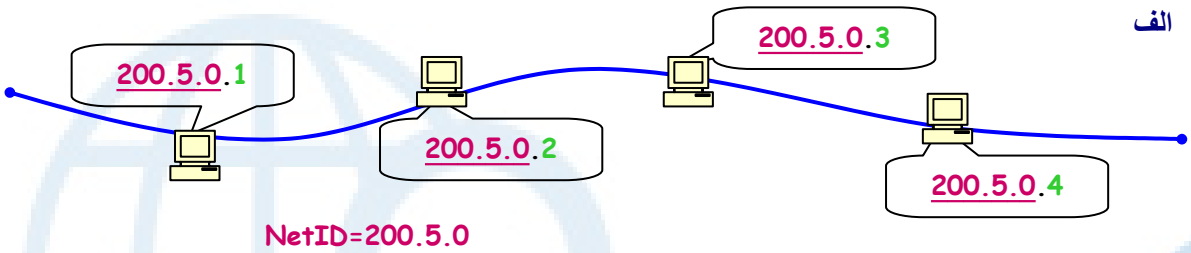
ب) از مقایسه شکلها با یکدیگر در مییابیم که شبکه هاي مختلف هرکدام NetID هاي مختلفي دارند و تکراري نیست.
ج) NetID ممکن است ۳ بایت (شکلهاي ۱و۲) یا ۲ بایت (شکل ۳) یا ۱ بایت (شکل ۴) باشد. بدیهي‌است که هرچه تعداد بایتهاي NetID بیشتر باشد شبکه هاي بیشتري را میتوان شماره‌گذاري کرد اما از آن طرف تعداد Host هاي موجود در شبکه محدودتر میشود. بسته به اینکه تعداد بایتهاي Net ID چند رقم باشد ۳ کلاس متفاوت ازIP_Address پدید مي آید:

Net ID = 1 byte (8 bits) => Class A
Net ID = 2 bytes (16 bits) => Class B
Net ID = 3 bytes (24 bits) => Class C

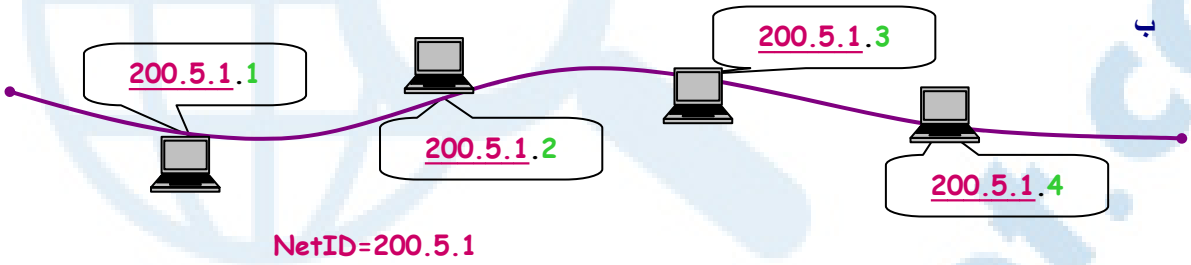
به شکل هایزیر توجه کنید هریك از شکلهاي ۱ تا ۴ به ترتیب از کلاسیهای زیر استفاده میکنند؟

الف : Class C ب: Class C ج: Class B د : Class A

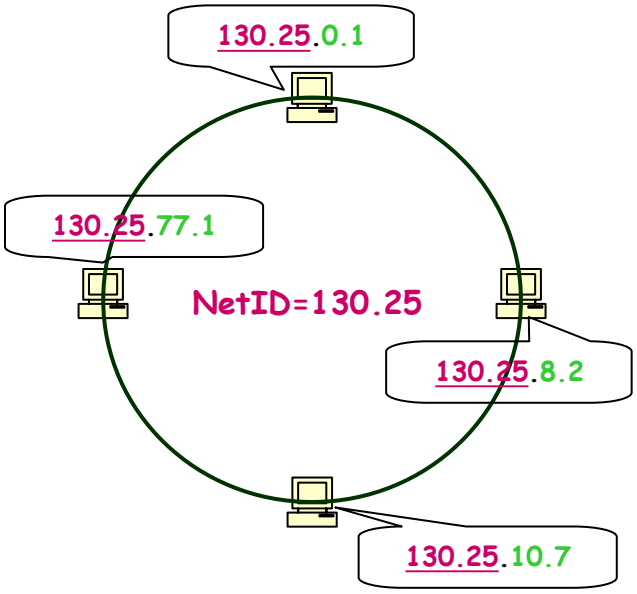
الف


200.5.0.1
200.5.0.2
200.5.0.3
200.5.0.4
NetID=200.5.0

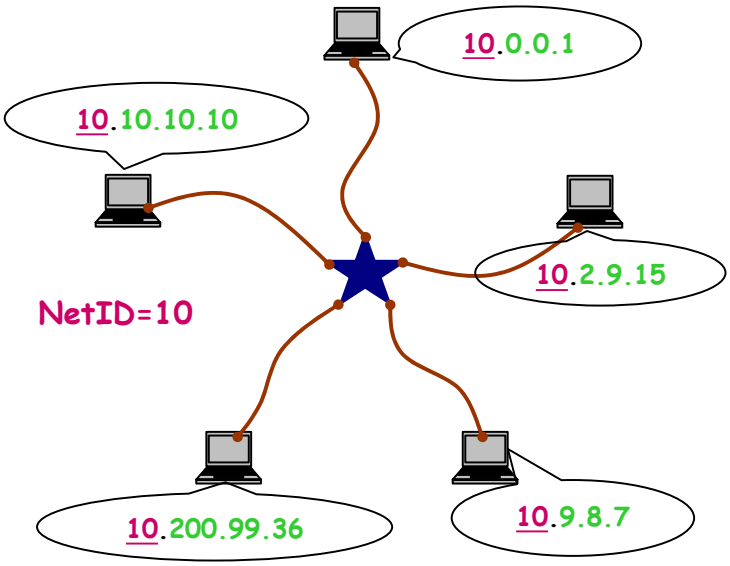
ب


200.5.1.1
200.5.1.2
200.5.1.3
200.5.1.4
NetID=200.5.1

ج


130.25.0.1
130.25.77.1
NetID=130.25
130.25.8.2
130.25.10.7

د


10.0.0.1
10.10.10.10
10.2.9.15
NetID=10
10.200.99.36
10.9.8.7

در هريك از شكلهاي فوق از مقايسة اعداد با يكديگر براحتي مي‌توانيم وجه مشترك آنها يعني NetID را تشخيص داده و بسرعت كلاس آنرا تعيين كنيم اما اگر يك IP Address را به تنهايي به ما نشان داده و بگويند در چه كلاسي است چه جوابي براي آن داريم؟ مثلا" به ما بگويند 10.1.2.15 در چه كلاسي است؟ (يعني NetID چيست و HostID كدام است؟) در اينجا جدول زير به ما كمك مي‌كند.

W	Class
1-126	A
128-191	B
192-223	C

يعني از روي رقم اول سمت چپ (W) مي‌توانيم بفهميم كه يك آدرس در چه كلاسي است.

تمرين: هريك از آدرسهاي زير در چه كلاسي است؟

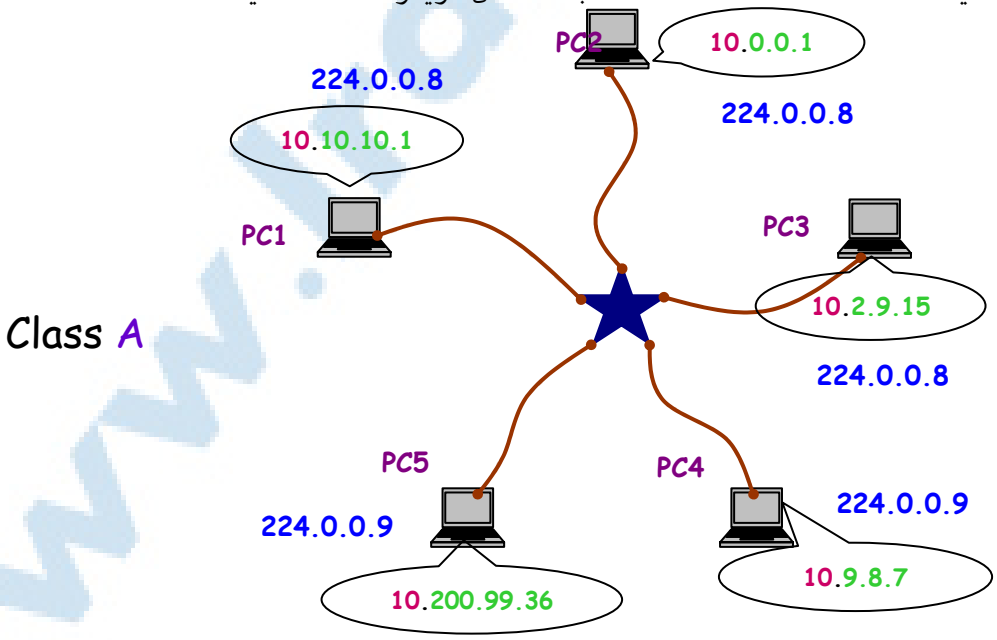
10.20.30.40
1.1.1.1
100.90.80.70
120.0.0.1
128.26.3.1
191.1.1.5
217.219.21.3

و اما هنرجويان با توجه به محدوده اعداد باينري كه از ۰ تا ۲۵۵ تغيير مي‌كند ممكن است سؤالات زير را از خود بپرسند:

۱) آيا w نمي‌تواند با صفر شروع شود؟ خير IP Address نمي‌تواند با عدد 0 آغاز گردد.

۲) عدد ۱۲۷ كجا رفت؟ هر آدرسي كه بصورت 127.x.y.z باشد اصطلاحا" Loop back خوانده مي‌شود. در ادامه در مبحث "ابزارهاي TCP/IP " راجع به آن صحبت خواهيم كرد.

۳): تكليف اعداد بين ۲۲۴ تا ۲۵۵ چه مي‌شود؟ ابتدا براي تعيين تكليف اعداد ۲۲۴ تا ۲۳۹ به شكل زير دقت كنيد:



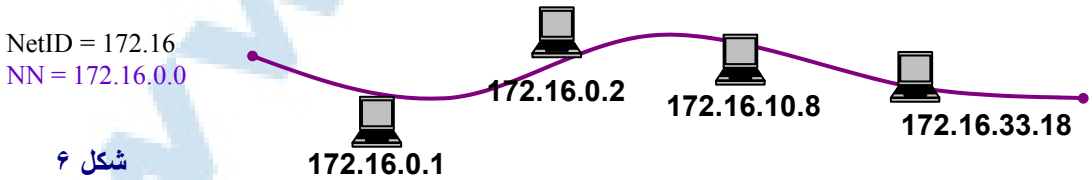
همانطور كه از شكل فوق پيداست هر Host علاوه برآنكه يك آدرس منحصر بفرد در (مثلاً) كلاس C دارد يك آدرس ديگر را كه با عدد ۲۲۴ شروع مي‌شود دارا بوده كه اولاً اجباري نبوده ثانياً دست بر قضا ! با برخي از سيستمهاي مجاور تكراري است.

به نظر شما کاربرد چنین آدرسهایی در چیست؟ اینگونه آدرسها که اصطلاحاً در کلاس D هستند برای Multicasting استفاده می‌شوند. بعنوان مثال اگر یك کاربر در سیستم متعلق به خود فرمان ارسال اطلاعات را به آدرس 224.0.0.8 دهد درآنصورت سیستمهای PC1, PC2, PC3همگی آنرا دریافت و پردازش خواهند کرد و این یعنی Multicasting.
بنابراین آدرسهای موجود در کلاس A ، B و C برای Unicast و کلاس D برای Multicast استفاده می‌شوند.
و اما محدوده 240 – 255 در رقم اول هیچگاه (تا زمان نگارش این کتاب) مورد استفاده عملیاتی قرار نگرفته و صرفاً جنبهٔ آزمایشی داشته است لذا برای آن کاربرد تعریف‌شده‌ای وجود ندارد.
در مجموع، توضیحات بیان شده در مورد آدرسها را در جدول زیر خلاصه می‌کنیم:

Class	Usage	W	Net ID	Host(Node) ID
A	Unicast	1 – 126	1 Byte (8 bits)	3 Bytes
B	Unicast	128 – 191	2 Bytes (16 bits)	2 Bytes
C	Unicast	192 – 223	3 Bytes (24 bits)	1 Byte
D	Multicast	224 - 239		

تا اینجای کار از هنرجویان انتظار می‌رود که بتوانند کاربرد هریك از کلاسهای A,B,C,D را به استثنای Loop back دقیقاً توضیح دهند.
اکنون که با فرمت IP Adderss آشنایی مختصری پیدا کردیم می‌توانیم قوانین آدرس دهی را دقیقتر بررسی کنیم:
قانون اول: در یك شبکه مشخص، هر Host باید حداقل یك آدرس منحصر بفرد در یکی از کلاسهای A، B یا C را داشته باشد. ضمناً هر شبکه دارای NetID جداگانه‌ای از سایر شبکه‌های دیگر است.
قانون دوم: در یك شبکهٔ مشخص برایآنکه کلیهٔ Host ها بتوانند مستقیماً و بدون واسطه با یکدیگر ارتباط داشته باشند، باید دارای Net ID یکسان باشند.
قانون سوم: Host ID نمی‌تواند همگی با هم 0 باشد یا همگی با هم 255 باشد.
قانون چهارم: Net ID نمی‌تواند همگی با هم 0 باشد یا همگی با هم 255 باشد. در عمل این اتفاق نمی‌افتد زیرا رقم اول یعنی w همواره جزئی از NetID بوده و از جدول پیداست که هیچگاه 0 نیست.

شرح بیشتر قانون سوم: چنانچه تمامی بیتهای مربوط به HostID برابر با 0 باشد در آنصورت به عدد حاصله اصطلاحاً آدرس شبکه یا Network Number (به اختصار NN) گفته می‌شود. می‌توان گفت که NN برابراست با NetID بعلاوهٔ HostID هنگامی که تمامی بیتهای آن صفر است. شکل زیر را ببینید:



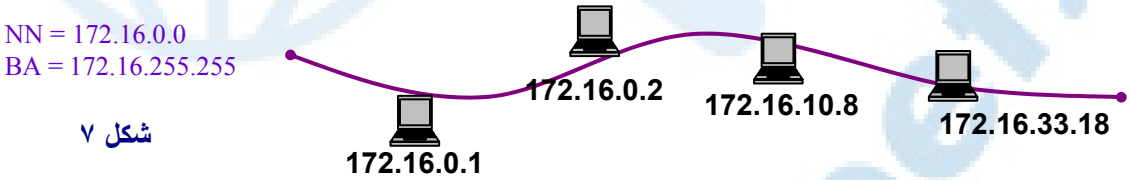
شکل ۶

شبکهٔ فوق را اصطلاحاً می‌گویند: شبکهٔ 172.16.0.0

براي درك بهتر به مثالهاي زير نيز توجه كنيد كه همگي بيانگر آدرس شبكه هستند:

Class A	11.0.0.0 , 78.0.0.0 , 123.0.0.0 , 1.0.0.0
Class B	130.24.0.0 , 142.5.0.0 , 191.7.0.0 , 150.50.0.0
Class C	192.1.1.0 , 192.168.1.0 , 220.5.4.0 , 217.219.90.0

در واقع هيچكدام از اعداد فوق را نميتوان بعنوان آدرس يك Host استفاده كرد زيرا بيانگر شمارة شبكه هستند.
و اما چنانچه تمامي رقمهاي مربوط به HostID ، همگي با هم 255 باشند (از ديدگاه باينري، تمامي بيتهاي مربوطه، "1" باشد) آنگاه عدد حاصله براي Broadcast Address استفاده ميشود يعني براي ارسال اطلاعات به تمامي سيستمهاي موجود در همان شبكه. بنابراين Broadcast Address براي شبكة يادشده ميشود : 172.16.255.255



شكل ۷

مثال: اگر كاربري فرمان ارسال اطلاعات را براي 172.16.0.2 صادر كند، فقط يك Host كه دقيقاً داراي آدرس مذكور است اطلاعات را پردازش خواهد كرد(Unicast)، اما اگر فرمان ارسال اطلاعات براي 172.16.255.255 صادر شود، در آنصورت كلية سيستمهاي شكل ۷ اطلاعات را دريافت و پردازش خواهند كرد.(Broadcast)

براي درك بهتر به مثالهاي زير نيز توجه كنيد كه همگي بيانگر آدرس شبكه هستند:

Class A	11.255.255.255 , 78.255.255.255 , 123.255.255.255 , 1.255.255.255
Class B	130.24.255.255 , 142.5.255.255 , 191.7.255.255 , 150.50.255.255
Class C	192.1.1.255 , 192.168.1.255 , 220.5.4.255 , 217.219.90.255

پرسش: در آدرس دهي براي شبكة خود از كدام كلاس استفاده ميكنيد؟ بستگي به تعداد Host هاي بكار رفته در شبكه دارد. به مثالهاي زير دقت كنيد:
مثال۱: شبكه‌اي داريم متشكل از 160 x Host كه با توجه به توسعة آن ممكن است به 230 x Host افزايش پيداكند از كدام كلاس استفاده كنيم؟ هريك از كلاسهاي A,B,C را ميتوان بكار برد اما نظر به اينكه تعداد Host از ۲۳۰ عدد بيشتر نميشود بهتر است از كلاس C استفاده كنيم و بعبارت ديگر آدرسها را هدر ندهيم. بنابراين بايد يك Net ID منحصر بفرد در كلاس C را كه در شبكه‌هاي ديگر استفاده نشده باشد انتخاب كرده و آنرا به شبكة خود اختصاص دهيم اما از كجا بدانيم كه NetID آزاد و استفاده نشده كدام است؟ براي اينكار خوشبختانه يك متولي وجود دارد كه مسوولیت تخصيص فضاي آدرسها را بعهده داشته و براي انتخاب NetID به آن مراجعه ميكنند. اين متولي همان IANA است (www.IANA.org) كه البته براي منطقة اروپا كار را به www.ripe.net تفويض كرده است و چون در ايران معمولا" از آدرسهاي اروپايي استفاده ميشود لذا به ripe مراجعه كرده و فرم درخواست IP را تكميل ميكنيم و پس از طي تشريفات مربوطه يك NetID منحصر بفرد در اختيار ما قرار داده ميشود. (در حال حاضر اينكار در ايران از طريق شركت ديتا وابسته به مخابرات انجام ميشود: www.dci.ir) فرض كنيم كه در مثال ياد شده ، NetID اختصاص يافته براي شركت ما عدد 213.217.24 باشد. بهتر است بگوييم شمارة شبكة ما (Network Number) برابر با 213.217.24.0 است . با در اختيار داشتن Network

Number مذكور براحتي مي‌توانيم كلية Host ها را از ۱ تا حداكثر ۲۵۴ شماره‌گذاري كنيم. به ترتيب زير:

First Host = 213.217.24.1
Second Host = 213.217.24.2
Third Host = 213.217.24.3
.
.
Last Host = 213.217.24.254

البته در مثال فوق 230 x Host داشتيم و بنابراين آدرس آخرين Host مي‌شود: 213.217.24.230 ، اما با توجه به توان بالقوة كلاس C ، براي هر NetID مي‌توانيم تا حداكثر 254 x Host را شماره‌گذاري كنيم و لذا آدرس آخرين Host را 213.217.24.254 نوشتيم و از اين پس در بقية مثالها نيز چنين خواهيم كرد.

بديهي است طبق قوانين گفته شده اعداد 0 و 255 كاربرد خاص خود را داشته و نمي‌توانند براي شماره‌گذاري Host استفاده شوند:

Network Number = 213.217.24.0
Broadcast Address= 213.217.24.255

بطور كلي در حل اينگونه مسائل بايد ۴ مرحله را طي كنيم:

مرحلة اول: تعيين كلاس با توجه به حداكثر تعداد Host.

مرحلة دوم: اخذ شماره شبكة معتبر يا به زبان فني: (Valid Network Number) يا (Valid IP Address)

مرحلة سوم: تعيين آدرس اولين Host الي آخرين Host.

مرحلة چهارم: تعيين Broadcast Address.

خود آزمایی و تحقیق

۱- پروتکل چیست؟ انواع رایج آن را نام ببرید.

۲- ویژگیهای عمده TCP/IP را نسبت به دو پروتکل SPX/IPX و Net BEUI بنویسید.

۳- سرویس های رایج در پروتکل TCP/IP را نام ببرید.

۴- تفاوت عموه و اساسي ترمینال با یك کامپیوتر PC چیست؟

۵- کدام سرویس TCP/IP از ترمینال استفاده مي کند؟ براي اتصال به سیستم مرکزي به چه چیزهایي نیاز دارد؟

۶- وظیفه Windows time چیست؟

۷- نام پروتکلي که ارسال ایمیل را انجام مي دهد چیست؟

۸- وظیفه Terminal Service را شرح دهید.

۹- Host چیست؟ خصوصیت اصلي هر Host را نام ببرید.

۱۰- مراحل ثبت Domain را شرح دهید.

۱۱- کار SubDomain چیست؟

۱۲- Loop Back چیست؟

۱۳- تحقیق کنید که TCP/IP نسخه ۶ چیست و چه تفاوتي با نسخه ۴ دارد؟

۱۴- تحقیق کنید که چند کاربر مي توانند به طور هم زمان از RDP استفاده کنند.

۱۵- تحقیق کنید که چه دستوراتي در محیط FTP رایج است؟

۱۶- تحقیق کنید که Domain هاي org. ، inf. ، prof. ، gov. ، ac. ، com. ، net. ، edu. در چه حوزه هایي مورد استفاده قرار مي گیرند.

۱۷- تحقیق کنید که تفاوت Valid IP و InValid IP در چیست؟

فصل ششم- مدل مرجع OSI

هدف های رفتاری

انواع لایه ها در مدل OSI را شرح دهد.

تفاوت هاي دو مدل TCP/IP و OSI را بیان کند.

مکانیزم هاي به کار گرفته شده در تجهیزات امنیتي شبکه را شناسایي کند.

تبادل داده ها در یك محیط شبکه اي ، مبتني بر استانداردهایي مي باشد یکي از این استاندارد ها، استانداردي به نام OSI است که از طریق سازمان ISO تدوین و معرفي شده است .پروتکل هاي شبکه نیز براساس این استاندارد تدوین و تولید شده اند.

در این استاندارد تمامي فعالیت هایي که سبب مي شد اطلاعات از طریق شبکه و از کامپیوتري به کامپیوتر دیگر منتقل شود در یك ساختار ۷ لایه اي به نام Open System Iterconnection (OSI) قرار گرفت .

این استاندارد تمامي فرایند تبدیل اطلاعات را از حالتي که در کامپیوتر قابل استفاده است تا حالتي که از طریق کابل شبکه قابل ارسال باشد ، در بر مي‌گرفت .

هرکدام از این لایه ها قسمتي از فرآیند تغییر شکل اطلاعات را در بر مي گیرند . اطلاعات از هفتمین لایه وارد این چرخه شده و پس از تغییر شکل در هر لایه به لایه بعدي خود منتقل مي شود .

این عمل آن قدر ادامه پیدامي کند تا تغییر شکل کامل شود و محصول فرآیند تبدیل که یك بسته اطلاعاتي یا Packet است ،به دست آمده و از لایه اول خارج شود .

OSI Reference Modl

۷- کاربردي	(Application)
۶- نمایش	(Presentation)
۵- جلسه	(Session)
۴- انتقال	(Transport)
۳- شبکه	(Net work)
۲- پیوند داده ها	(Data Link)
۱- فیزیکي (Physical)	

شكل ۱-۶

نكته : نكته اي كه در مورد لايه ها مي توان به آن اشاره كرد اين است كه هر لايه فقط با لايه هاي قبلي ، بعدي و لايه نظير خود در كامپيوتر مقصد ارتباط دارد .

شكل ۲-۶

۱-۶ انواع لايه در مدل OSI

لايه اول يا لايه فيزيكي در پايين ترين سطح قراردارد و به طور مستقيم با تو پولوژي شبكه در ارتباط است . لايه هفتم يا همان لايه كاربردي با كاربر در ارتباط بوده و ازكاربر داده ها را دريافت كرده و به شبكه انتقال مي دهد و برعكس.

۱-۱-۶ لايه فيزيكي

لايه فيزيكي، اولين لايه مدل OSI بوده و در پايين ترين سطح اين مدل قرار گرفته است . در اين لايه نحوه اتصال دو كامپيوتر به يكديگر از طريق كابل هاي شبكه ، نحوه اتصال كابل شكه به كامپيوتر ، توپولوژي هاي شبكه و سرعت هاي آن ها توضيح داده شده است . اين لايه مسئول تبديل اطلاعات از بيت ها (صفر و يك ديجيتال) به سيگنال هاي الكتريكي است . به طور كلي مي توان گفت اين لايه فقط ولتاژ، اتصالات ،كارت شبكه و جريان الكتريكي را مي شناسد.

۲-۱-۶ لايه پيوند دادها

لايه پيوند داده ها دومين لايه مدل OSI است . وظيفه اين لايه اين است كه اطلاعات را براي ارسال آماده كند و در واقع اطلاعاتي را كه از لايه بالاتر يعني لايه شبكه دريافت مي كند به واحدهاي كوچك تري به نام قاب تبديل كرده و آن ها را ارسال كند . هم چنين اين لايه وظيفه دارد كه اطلاعات را براي ارسال صحيح و بدون خطا كنترل كرده و به كامپيوتر فرستنده صحت اطلاعات را اعلام كند . اين لايه خود از دو زير لايه به نام هاي LIC و MAC تشكيل شده است . هر كدام از اين زير لايه ها وظايفي را به عهده دارند كه شرح آن ها به اين قرار است :

زير لايه LLC وظايفي برعهد دارد كه عبارتند از : برقرار ارتباط نظير به نظير بين دو كامپيوتر فرستنده و گيرنده ، ايجاد قاب ها و كنترل خطاهايي كه در اثر عوامل محيطي بر رسانه به وجود مي آيد . اين زير لايه عمل كنترل خطا را به اين صورت انجام مي دهد كه هر قاب را ساخته و مرزهاي ابتدا وانتهاي آن را مشخص مي كند. سپس قاب ها را شماره گذاري و ارسال مي كند . كامپيوتر مقصد قاب هاي ارسال شده را دريافت كرده و به ترتيب شماره ، آن ها را پشت سرهم قرار مي دهد واطلاعات را دوباره بازسازي مي كند . زير لايه LLC در كامپيوتر گيرنده پس از دريافت هر قاب يك پاسخ براي كامپيوتر فرستنده مي فرستد. به اين پاسخAcknowledge گفته مي شود . كامپيوتري كه فرستنده اطلاعات است با دريافت اينAcknowledge متوجه مي شود كه قاب مذكور به طور صحيح و بدون بروز مشكل به مقصد رسيده است . كامپيوتر فرستنده تا مدتي منتظر مي ماند تا براي تمامي قاب هاي ارسال شده، Acknowledge دريافت نمايد . در صورتي كه LLC براي قابي Acknowledge دريافت نكند ، متوجه مي شود كه قاب مذكور آسيب ديده يا به مقصد نرسيده است ؛ در اين حالت قاب مورد نظر را از روي شماره آن دوباره ساخته و براي كامپيوتر مقصد ارسال مي كند . اين زير لايه با اين روش سالم رسيدن اطلاعات به مقصد را تضمين مي كند.

زير لايه ديگري كه در لايه پيوند داده ها قرار دارد ، زير لايه MAC است . اين زير لايه چند وظيفه برعهده دارد . يكي از وظايف آن كنترل نحوه دسترسي به خطوط انتقال است .

از وظايف ديگر اين زير لايه كنترل آدرس فيزيكي كارت هاي شبكه كامپيوتر فرستنده و گيرنده است . هركارت شبكه براي خود يك آدرس فيزيكي منحصر به فرد دارد كه غير قابل تغيير است . اين آدرس به وسيله ي كارخانه سازنده در كارت شبكه حك مي شود .

Flag	Address	Control information	Data	Parity	Flag

شكل ۳-۶ Data-Link

۳-۱-۶ لايه شبكه

لايه شبكه ،سومين لايه استاندارد OSIاست . يافتن آدرس كامپيوترهاي مبدأ و مقصد و ايجاد يك مسير ارتباطي بين مبدأ و مقصد و هم چنين مسير يابي در شبكه هاي بزرگ مثل شبكه اينترنت يا امثال آن وظيفه اصلي اين لايه است . اين لايه پيچيده ترين لايه OSI است ،زيرا عمل مسير يابي كه فرآيند بسيار پيچيده اي است در اين لايه اتفاق مي افتد . اين لايه علاوه بر مسير يابي مي تواند اعمال ديگري از جمله كنترل ترافيك را نيز انجام دهد . بدين معني كه در صورتي كه بار ترافيك در مسير عبور بسته اطلاعاتي بالا رود ، اين لايه وجود ترافيك را تشخيص داده و مسير جديدي را كه ترافيك كمتري دارد براي عبور بسته ها انتخاب مي كند . يكي ديگر از اعمالي كه اين لايه انجام مي دهد ،زماني است كه يك بسته اطلاعاتي براي رسيدن به مقصد مجبور است از شبكه اي به شبكه ديگر بر ود . در اين شرايط ممكن است مشكلات زيادي بروز نمايد . يكي از اين مشكلات اين است كه روش آدرس دهي كامپيوتر ها در شبكه مبدأ و مقصد متفاوت و نامتجانس است . رفع اين مشكل و مرتبط كردن دوشبكه نامتجانس نيز از ديگر وظايف اين لايه است .

شكل ۴-۶ Network layer

۴-۶-۱- لايه انتقال

وظيفه اصلي لايه انتقال ، دريافت داده ها از لايه جلسه ، در صورت نياز شكستن داده ها به واحدهاي كوچك تر ، انتقال آن ها به لايه شبكه و حصول اطمينان از دريافت صحيح داده ها در انتهاي ديگر (كامپيوتر مقصد) است .

از وظايف ديگر لايه انتقال اين است كه اين لايه بايد مراقب برقراري و قطع اتصال در شبكه باشد . هم چنين اين لايه مكانيزمي براي كنترل جريان ارسال داده ها در اختيار دارد ، به طوري كه اين مكانيزم سبب مي شود كامپيوتر فرستنده ، داده ها را باسرعتي ارسال كند كه كامپيوتر گيرنده قادر به دريافت آن ها باشد . اين مكانيزم زماني كاربرد پيدا مي كند كه يك كامپيوتر سريع بخواهد اطلاعاتي را ارسال نمايد و كامپيوتر گيرنده ، قدرت و سرعتي كمتر از كامپيوتر فرستنده داشته باشد . در اين شرايط لايه انتقال ، سرعت ارسال كامپيوتر فرستنده را تاحد سرعت كامپيوتر گيرنده اطلاعات پايين مي آورد .

۵-۶-۱ لايه جلسه

پنجمين لايه OSI ، لايه جلسه است . اين لايه هم چون لايه انتقال ، ارسال معمولي دادها را فراهم مي كند اما خدمات پيشرفته اي را نيز ارايه مي كند كه كاربردهاي مفيدي دارد . يكي از خدمات جلسه ، مديريت بر ارتباط بين كامپيوترهاست ؛ بدين معني كه وقتي دو كامپيوتر باهم ارتباط برقرار مي كنند ، ترافيك مي تواند در يك لحظه يك طرفه يا دو طرفه باشد . اگر اين ترافيك يك طرفه باشد ، لايه جلسه مي تواند در حفظ نوبت كمك كند .

يكي ديگر ازخدمات اين لايه ، مديريت Token است . در بعضي پروتكل ها لازم است هيچ كدام از طرفين ، كاري را هم زمان شروع نكنند . براي مديريت بر فعاليت هاي لايه جلسه ،Token هايي تهيه مي شود كه بين مبدأ و مقصد قابل مبادله اند . در اين شرايط فقط طرفي كه Token را در اختيار دارد مي تواند فعاليت كند و طرف مقابل بايد منتظر باشد تا نوبت او براي استفاده از Token فرا برسد.

يكي ديگر از اعمال لايه جلسه اين است كه روي قسمت هايي از رشته داده ها را علامت گذاري مي كند ؛ در صورتي كه بسته اي هنگام ارسال مفقود يا خراب شود ، لايه جلسه بسته را از روي كدهاي آن شناسايي و دوباره ارسال مي كند .

۶-۶-۱ لايه نمايش

لايه نمايش ششمين لايه OSI است. اين لايه داده ها را به روش استاندارد كد گذاري مي كند .

اكثر كامپيوترها اطلاعاتي مانند نام افراد ، تاريخ ، مقادير پول و اطلاعات مشابه ديگري را ارسال مي كنند .

اين اطلاعات به صورت كاراكتر بوده و هيچ كدام رشته هاي دودويي نيستند.

كدهاي نمايش رشته هاي كاراكتري ، اعداد صحيح و غيره ممكن است د ركامپيوترهاي مختلف متفاوت باشد .براي اين كه كامپيوترها با كدهاي مختلف بتوانند با يكديگر ارتباط برقرار كنند ، اطلاعاتي كه انتقال مي يابند بايد با استفاده از كدهاي استاندارد تعريف و ارسال شوند تا در تمامي كامپيوتر ها و با سيستم عامل هاي متفاوت قابل دريافت و درك باشند .

۶-۱-۷ لايه كاربردي

هفتمين لايه مدل OSI است . اين لايه حاوي پروتكل هاي گوناگون است كه همه نرم افزارهاي كاربردي براي ارتباط شبكه اي از آن ها استفاده مي كنند .

لايه كاربردي بزرگ ترين لايه در استاندارد OSI است . اين لايه شامل سيگنال هايي است كه خدمات سودمندي از قبيل انتقال فايل وكنترل يك كامپيوتر از راه دور را به كاربر ارايه مي دهد ، در صورتي كه لايه هاي پايين تر فقط در تبادل اطلاعات بين فرستنده و گيرنده نقش دارند . هم چنين اين لايه مي توانند ارتباط برنامه هاي مختلفي را كه در محيط شبكه وجود دارند ، بايكديگر برقراركند.

به عنوان مثال ، صدها نوع نرم افزار در دنيا وجود دارد كه هركدام روش خاص خود را براي نوشتن ، ويرايش و حركت مكان نما روي صفحه انجام مي دهند ، در صورتي كه اين لايه وجود نداشت ،ممكن بود در اجراي برنامه ها و ويرايش آن ها دچار مشكل شويم . براي حل اين مشكل لايه كاربردي ، اطلاعات لازم را از اين برنامه ها گرفته و بايك استاندارد مشخص آن ها را به كامپيوتر مقصد مي فرستد.

وظيفه ديگر لايه كاربردي انتقال فايل است . در سيستم فايل هاي مختلف ، نام گذاري فايل ها ، روش نمايش خطوط متن و غيره متفاوت است . اين كار نيز همانند وظايفي از قبيل پست الكترونيك ، كنترل كامپيوتر از راه دور و جستجو در بخش هاي مختلف درون حافظه ، وظيفه لايه كاربردي است

۶-۲-مقايسه دو پروتكل در بخش های مختلف امنيتی

در ادامه، حملات، سرويس ها و مكانيزم ها و تجهيزات امنيتي در لايه هاي مختلف در قالب جداول ۱-۲-۳-۴ با يكديگر مقايسه مي شوند و همانطور كه در جداول مذكور نشان داده شده است مي توان نتيجه گرفت كه بيشترين حملات به ترتيب در لايه IP,TCP ، كاربرد و ميزبان به شبكه است و سرويس ها و مكانيزم ها بيشتر در لايه IP به چشم مي خورد و تجهيزات امنيتي با بهره گيري از مكانيزم هاي مختلف بيشتر در لايه IP,TCP و كاربرد ، كاربري دارند .

در جدول ۵ تجهيزات امنيتي از نظر پارامترهاي مختلف با يكديگر مقايسه مي شوند و مورد ارزيابي قرار مي گيرند، استفاده از تجهيزات سخت افزاري نظير فايروال، سوئيچ ها و مسيريابهاي مديريت پذير، گران است و هزينه پشتيباني آنها نيز بالاست و از پيچيدگي نسبتا بالايي برخوردارند. در تجهيزات نرم افزاري نيز هزينه پشتيباني بدليل لزوم Update مرتب ، بالا است ولي هزينه استقرار و پيچيدگي پائين است.

جدول ۱. مقايسه تهديدات امنيتي در لايه هاي چهارگانه TCP/IP

تهديد /لايه	Host to Network	IP	TCP	Application
Trojan,Virus,Worm				*
SQL-Injection				*
TCP/IP Spoofing		*	*	
Session Hijacking			*	*
Port Scan			*	*
Physical Attacks	*			
Phishing			*	*
Password Attacks				*
Packet Sniffing		*	*	
Dos/DDos Attacks		*	*	*
Network Layer Attacks		*		
Application Layer Attacks				*
Buffer Over Flow Attacks		*	*	*
Replay	*	*	*	*
Traffic Analysis	*	*	*	
Message Modification	*	*	*	

جدول ۲. اهداف امنيتي در منابع شبكه

منابع / اهداف	شبكه				كاربران شبكه
	سخت افزارها	نرم افزارها	اطلاعات	ارتباطات	
محرمانگي			*	*	
صحت	*	*	*	*	
قابليت	*	*	*	*	
محافظت	*		*	*	
تشخيص هويت					*
صدور					*
حريم خصوصي					*✓
آگاهي رساني					

جدول ۳. سرويس هاي امنيتي در لايه هاي مختلف TCP/IP

سرويس/لايه	Host to	IP	TCP	Application
محرمانگي	*	*	*	*
تاييد هويت	*	*	*	*
رد انكار				*
كنترل جامعيت و		*	*	

جدول ۴. مكانيزم هاي امنيتي مربوط به لايه هاي مختلف TCP/IP

مكانيزم/لايه	Host to	IP	TCP	Application
رمزنگاري	*	*	*	*
امضاء ديجيتال		*	*	*
كنترل دستيابي		*	*	*
درستي و صحت داده		*	*	*
كنترل مسيريابي		*		
رد انكار ( )		*		*

جدول ۵. مقايسه تجهيزات امنيتي در لايه هاي چهارگانه TCP/IP

تجهيزات امنيتي	Host to Network	IP	TCP	Application
حفاظت فيزيكي	*			
رمزنگاري	*	*	*	*
IP Sec		*		
SSL			*	
Firewall		*	*	*
AntiVirus				*
AAA Server	*	*	*	*
VPN	*	*	*	*
PGP				*
IDS/IPS		*	*	*

خود آزمایی و تحقیق

۱- به طور کلي وظایف لایه ها در مدل OSI چیست؟

۲- Packet چیست؟

۳- یافتن آدرس کامپیوتر مقصد و مبدا وظیفه کدام لایه است؟

۴- پروتکل هاي شبکه در کدام لایه قرار دارند؟

۵- تجهیزات امنیتي مانند Firewall و Anti Virus ها در کدام لایه شبکه بهتر عمل مي کنند؟

۶- تحقیق کنید که تجهیزات امنیتي مانند Firewall و ... از لحاظ سخت افزاري و نرم افزاري چه تفاوتهایي با هم دارند؟

فصل هفتم - امنیت در شبکه

هدف های رفتاری

دیواره آتش را تعریف کند و با آن کار کند.

تفاوت آنتي ویروس و دیواره آتش را بیان کند.

عملکرد سرویس دهنده Proxy را تعریف کند.

امنیت در شبکه دارای سطوح مختلفی است ، یک مدیر شبکه برای محدود کردن کاربران غیر مجاز می تواند از سطح نام کاربری و گذرواژه استفاده کند .در حالی که اگر این شبکه به شبکه ی دیگر متصل شود ، مدیر شبکه نیاز به سطح امنیتی بالاتری خواهد داشت که این سطح امنیتی با نام کاربری و گذرواژه میسرنخواهد بود .

بنابراین ، مدیر شبکه نیاز به نصب دیواره آتش (Fire wall) به صورت سخت افزاری و نرم افزاری خواهد داشت.

رعایت امنیت در شبکه یکی از موارد ضروری است که مدیر شبکه و حتی کاربران باید رعایت نمایند با توجه به این که در سال دوم آنتی ویروس آموزش داده شده است در این فصل دیواره آتش و proxyمورد بحث قرار می گیرد.

۱-۷- دیواره آتش (Firewall)

دیواره آتش به صورت نرم افزاري یا سخت افزاری موجوداست که اطلاعات ارسالی بین دوشبکه داخلي را کنترل و فیلتر می نماید. به عنوان مثال ، هنگام اتصال به اینترنت شما از یک دیواره آتش برای دسترسی به اطلاعات باید عبور کنید.

بدون استفاده از دیواره آتش تمام کامپیوترهای موجود در یك شبکه داخلی ، قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت بوده و از طرف دیگر کامپیوترهاي دیگر توانايي ورود به کامپیوتر هاي شبکه داخلي یا شخصي را خواهند داشت. کاربران شبکه داخلي قادر به استفاده از برنامه هائی همچون FTP یا Telnet بمنظور ارتباط مستقیم با افراد حقوقی و یا حقیقی موجود بر روی اینترنت بوده و عدم رعایت مسائل ایمنی به وسیله ی پرسنل یك شبکه داخلي، می تواند زمینه دستیابی به اطلاعات موجود در شبکه داخلی را برای افراد غیر مجاز فراهم نماید.

۱-۱-۷- ضرورت استفاده از دیواره آتش

در صورتي که از دیواره آتش استفاده نشود شبکه از جنبه هاي مختلف به خطر مي افتد برخي از این موارد ي که شبکه ها یا کاربران به وسیله ی حمله کنندگان به شبکه های کامپیوتری تهدید مي شوند عبارتند از

- Application Backdoors . اغلب نرم افزارهای موجود که روی کامپیوتر تان نصب می کنید ،ممکن است دارایBugهای باشند که هکرها از طریق این کانال ها ی نفوذی می توانند به کامپیوترشما رخنه کرده و سبب خرابی یا سوء استفاده از اطلاعات شوند.

- Remote Login . امکان برقراری ارتباط از راه دور با کامپیوتر و کنترل آن توسط کاربر ممکن است . افراد غیرمجاز نیز از این طریق می توانند به کامپیوتر و اطلاعات درون آن دسترسی داشته باشند. دامنه عملیات فوق می تواند از مشاهده و

دستیابی به برخی از فایل ها تا اجرای برخی برنامه ها بر روی کامپیوتر باشد.

- SMTP session hijacking . پروتکل SMTP رایج ترین روش برای ارسال e-mail است . با دستیابی به لیستی از آدرس های e-mail ، یک شخص قادر به ارسال e-mail به هزاران کاربر دیگر خواهد شد.

- **اشکالات سیستم های عامل** . سیستم های عامل نظیر سایر برنامه های کاربردی ممکن است دارای Backdoors باشند.

- **بمباران با E-mail به منظور اختلال در ترافیک :** . یک شخص قادر به ارسال صدها و هزاران e-mail مشابه در مقاطع زمانی متفاوت است . با توجه به وضعیت فوق سیستم پست الکترونیکی قادر به دریافت تمام نامه های ارسالی نخواهد بود.

- **ماکرو.** اغلب برنامه های کاربردی این امکان را برای کاربران خود فراهم می نمایند که مجموعه ای از اسکریپت ها را بمنظور انجام عملیات خاصی نوشته و نرم افزار مربوطه آنها را اجراء نماید. اسکریپت های فوق " ماکرو " نامیده می شوند. حمله کنندگان به شبکه های کامپیوتری با آگاهی از واقعیت فوق، اقدام به ایجاد اسکریپت های خاص خود نموده که با توجه به نوع برنامه ممکن است داده ها را حذف و یا سبب از کار افتادن کامپیوتر گردند.

- **ویروس** . رایج ترین روش برای آسیب رساندن به اطلاعات، ویروس است . همانطور که می دانید ویروس یک برنامه کوچک است که قادر به تکثیر خود بر روی کامپیوتر دیگر است . عملکرد ویروس ها بسیار متفاوت بوده و از اعلام یک پیام ساده تا حذف تمام داده ها را می تواند شامل گردد.

زمانیکه در شبکه داخلي از دیواره آتش استفاده شود، وضعیت کاملا" تغییر مي کند و مسئولین شبکه می توانند با استفاده از .دیواره آتش مجموعه سیاست های امنیتی را در مقابل افرا غیرمجاز بر روي خطوط خود پیاده سازی کنند. به عنوان مثال مجوز ها و محدودیت هاي زیر را اعمال نمایند:

- تمام کامپیوترهای موجود در شبکه مجاز به استفاده از اینترنت می باشند ، ولي کارمندان خاص نتوانند از اینترنت براي ارسال و دریافت Email استفاده نمایند
- امکان دسترسي از راه دور براي مشاهده فایل ها یا تغییر آن ها به وسیله ی افراد خارج از شبکه یا افراد داخلي غیر مسئول بگیرند

۲-۱-۷- سفارشي نمودن دیواره آتش

دیواره آتش را می توان بر اساس شرایط مورد نظر به صورت سفارشی نصب و پیکربندی کرد.

- **کلمات و عبارات.** در این روش در دیواره آتش کلمات یا عباراتی مشخص مي شود تا امکان محدود کردن دسترسي با توجه به آن عبارات انجام شود در این حالت بسته های اطلاعاتی که در حال مبادله است بررسي وهر بسته اطلاعاتی که حاوی کلمات مشخص شده باشد، به وسیله ی دیواره آتش دسترسي به آن محدود خواهد شد.

- **اسامی دامنه ها (Domain)** . با توجه به این که تمام سرویس دهندگان بر روی اینترنت دارای اسامی منحصر بفرد با نام " اسامی دامنه" می باشند. بر این مبنا و با استفاده از دیواره

آتش ، مي توان دستيابی به سايت هائی را محدود يا صرفا" امكان استفاده از يک سايت خاص را فراهم كرد.

- **آدرس های IP** . همانطور كه مي دانيد هر كامپيوتر روی اينترنت دارای يک آدرس منحصر بفرد با نام IP است . به عنوان مثال، اگر كاربر يک آدرس IP خارج از شبكه، بدون مجوز فايل های زيادی را از سرويس دهنده دريافت نمايد (اين كار ترافيك شبكه را افزايش مي دهد) ،ديواره آتش می تواند با شناسايي IPمورد نظر و محدود نمودن آن ترافيک مربوطه را كنترل نمايد.

- **پروتكل ها** . پروتكل نحوه ارتباط بين سرويس دهنده و سرويس گيرنده را مشخص می نمايد . با استفاده از ديواره آتش می توان، پروتكل های مورد نظر را محدود كرد. مثلا" پروتكل وب ، http و پروتكل مربوط به دريافت يا ارسال فايل ها Ftp است

برخی از پروتكل های رايج كه بر روی آنها فيلتر اعمال مي شود بشرح زير می باشند :

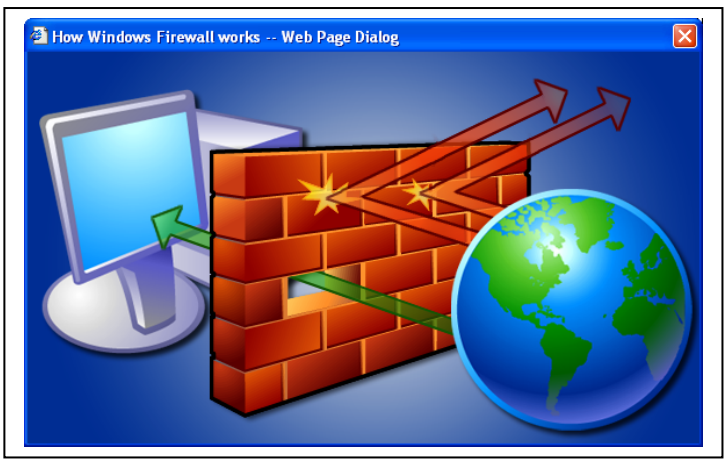
- IP– (Internet Protocol)
- TCP– (Transport Control Protocol)
- HTTP– (Hyper Text Transfer Protocol) .
- FTP – (Protocol File Transfer) .
- SMTP (Simple Mail Transfer Protocol)

- **درگاه ها** . بر روی اينترنت ، خدمات هر سرويس دهنده ، با استفاده از درگاههای شماره گذاری شده ارائه می شود. مثلا" سرويس دهنده وب اغلب از درگاه۸۰ و سرويس دهنده FTP از درگاه۲۱ استفاده می نمايد. يک سازمان ممكن است با استفاده از ديواره آتش بر روي درگاه خاصي محدوديت ايجاد نمايد با امكان دستيابی به آن تحت كنترل باشد.

علاوه بر ديواره آتش نرم افزاري ، مي توان از ديواره آتش سخت افزاري نيز استفاده كرد . امنيت ديواره آتش های سخت افزاری بمراتب بيشتر از ديواره آتش های نرم افزاری است .

۳-۱-۷- تنظيمات ديواره آتش در ويندوز:

همانطور كه گفته شد برای جلوگيری از دسترسی غيرمجاز كاربران شبكه يا اينترنت از ديواره آتش استفاده می شود. اين دسترسی ميتواند شامل انواع برنامه های مخرب و ويروس ها و كرمها (worms)باشد كه به صورت يک طرفه بدون اينكه درخواستی برای آن ارسال شده باشد، وارد كامپيوتر شده و سيستم را دچار اختلال می كند.



شکل ۱-۷

۷-۱-۴- تفاوت آنتی ویروس و دیواره آتش:

به طور کلی سه تفاوت کلی مابین این دو دسته برنامه ها وجود دارد.

۱. یکی از وظیفه های دیواره آتش جلوگیری از ورود ویروس ها و کرمها به داخل کامپیوتر است. اما تشخیص نوع ویروس و غیر فعال کردن آن و جلوگیری از تهدیدات امنیتی (security threats) و عدم انتشار ویروس به روی شبکه بر عهده آنتی ویروس است. به همین خاطر تاکید ویندوز بر این است که حتما یک آنتی ویروس را در کنار دیواره آتش ویندوز استفاده شود.

۲. گرفتن تاییدیه یا مجوز برای اجرای برنامه هایی که ممکن است با خارج از کامپیوتر در حال برقراری ارتباط باشند، مانند انواع messenger به عهده دیواره آتش است. در حالی که زمانی که ما یک ایمیل ناشناس را باز می کنیم که حاوی یک برنامه مخرب است ، جلوگیری از اجرای چنین برنامه هایی بر عهده آنتی ویروس ها است. علاوه بر این ،آنتی ویروس ها میتوانند جلوی Spam یا ایمیل ها ی ناشناس که به طور ناخواسته برای ما ارسال میشوند را بگیرد

در دیواره آتش این امکان وجود داردکه یک Log file یا فایل وقایع نگار درست کنیم که گزارش کاملی از ارتباطات موفق یا ناموفق از کامپیوتر ما را ثبت کند.

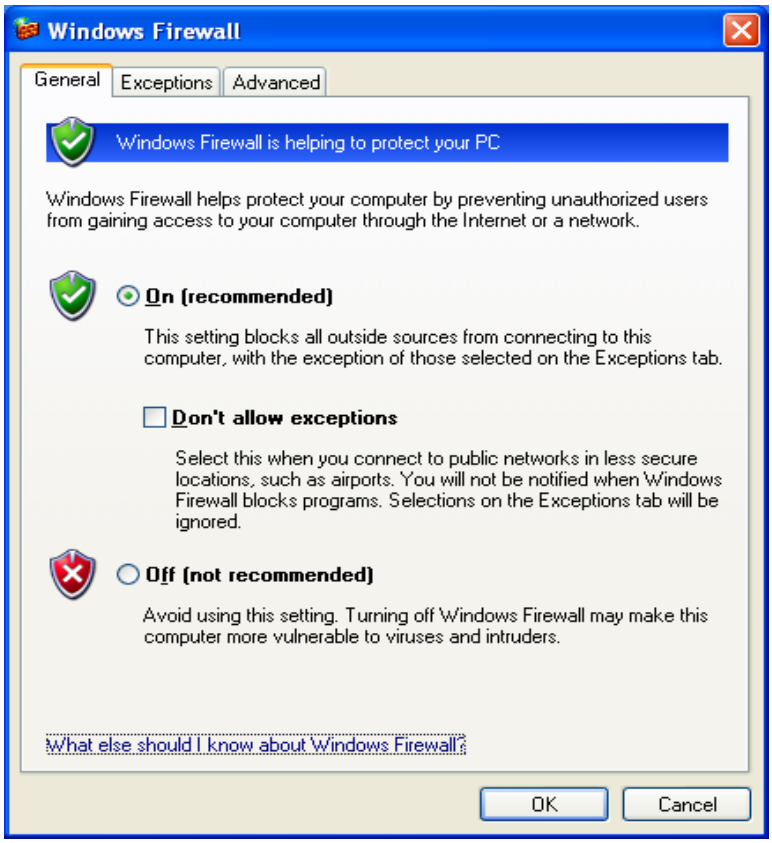
۷-۱-۵- فعال نمودن دیواره آتش در روی ویندوز XP

برای فعال کردن برنامه دیواره آتش ابتدا آنرا از مسیر زیر اجرا نمایید:

Start > Control Panel > windows firewall

نکته : فقط در صورتی که Service Pack 2.0 روی ویندوز XP نصب شده باشد، می توان دیواره آتش اجرا کرد.و نسخه های قبلی فاقد این ویژگی می باشند.

حال پنجره ای شبیه به شکل زیر نمایش داده خواهد شد.



شکل ۲-۷

همانطور که مشاهده می کنید دیواره آتش ویندوز به طور پیش فرض فعال میباشد. در صورتی که از برنامه دیواره آتش به جز ویندوز استفاده می کنید ،بهتر است که این گزینه را غیر فعال نمایید.

حال اگر وضعیت On(recommended) را انتخاب کنیم کلیه دسترسی ها از داخل یا خارج از شبکه مسدود (Block) می شود به جز برنامه ها یا درگاه که در زبانه exceptions (استثناء) تعریف شوند.

انتخاب وضعیت Don't allow exceptions برای زمانی مفید است که کامپیوتر ما در یک محیط نا امن قرار دارد مانند Laptop مجهز به کارت شبکه بی سیم در یک فرودگاه یا یک مکان عمومی که هیچ نظارتی بر منابع شبکه آن نیست. با انتخاب این گزینه دیگر تعاریف در زبانه exceptions نادیده گرفته می شود. و از ورود کلیه اطلاعات ممانعت به عمل میآید.

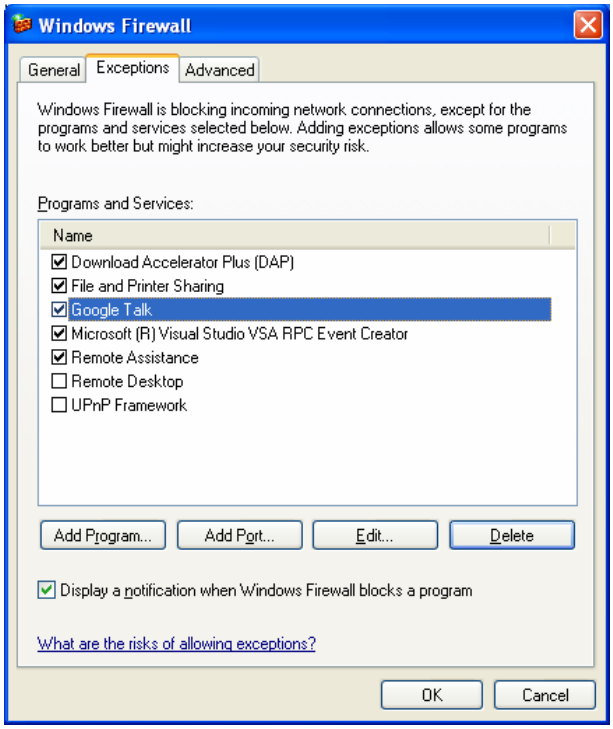
با انتخاب Off(Not recommended) دیواره آتش غیر فعال شده و کامپیوتر در برابر برنامه های مزاحم که بدون اجازه شروع به کارمیکنند آسیب پذیر خواهد بود.

زبانه Exceptions :

با انتخاب این زبانه می توانیم برای بعضی از برنامه های کاربردی یا سرویس هایی که دیواره آتش آنرا مسدود کرده است. استثنا قائل شویم و ورود اطلاعات از سوی بعضی شبکه ها را به سوی کامپیوتر خودمان باز کنیم تا بعضی برنامه ها بهتر کار کنند،که البته این کار ممکن است در بعضی مواقع امنیت سیستم را دچار اختلال کند.

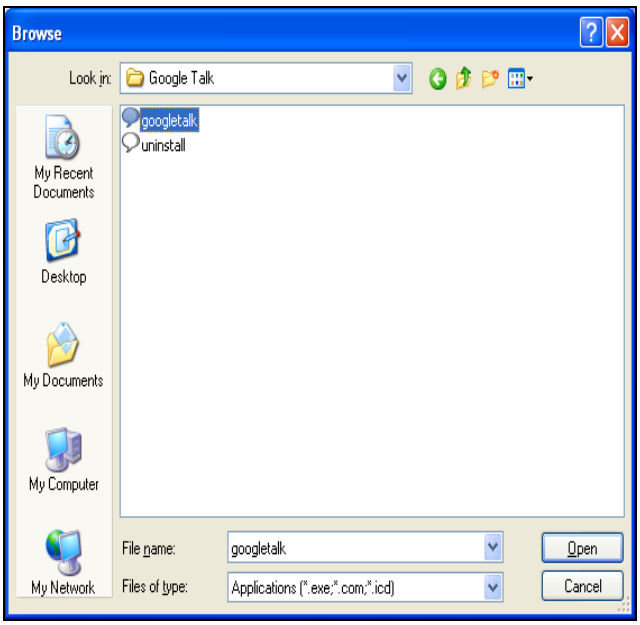
به عنوان مثال، اگر ما بخواهیم از برنامه هایی نظیر Google talk, Download accelerator (DAP) استفاده کنیم در حالتی که دیواره آتش ویندوز فعال است امکان تبادل اطلاعات با خارج از شبکه غیر ممکن است اما اگر این برنامه ها در لیست استثنا ها تعریف شود. ارتباط به راحتی برقرار می شود. مانند شکل زیر:

شکل ۳-۷



۶-۱-۷-بازکردن برنامه یا سرویس در دیواره آتش:

۱-برای باز کردن برنامه ها در صورتی که دیواره آتش از اجرای آنها جلوگیری کرده باشد. ابتدا باید با کلیک بروی گزینه Add Program نام برنامه مورد نظر خود را از لیست ظاهر شده انتخاب نماییم . در صورتی که برنامه مورد نظر در لیست نباشد. با کلیک بروی گزینه Browse می‌توانیم مسیر برنامه را وارد کنیم (شکل ۴-



شکل۴-۷

پس از تایید برنامه , امکان استفاده از آن برای ما امکان پذیر میباشد.

۲- بعضی از برنامه های کاربردی شامل سرویس های خاصی هستند که این سرویس ها برای ارتباط با سرور خود ازدرگاه ها ی خاصی استفاده می کنند به عنوان مثال برنامه Yahoo Messenger شامل سرویسهای متنوعی است که این سرویسها برای تبادل اطلاعات در شبکه از درگاه های زیر استفاده می کنند.

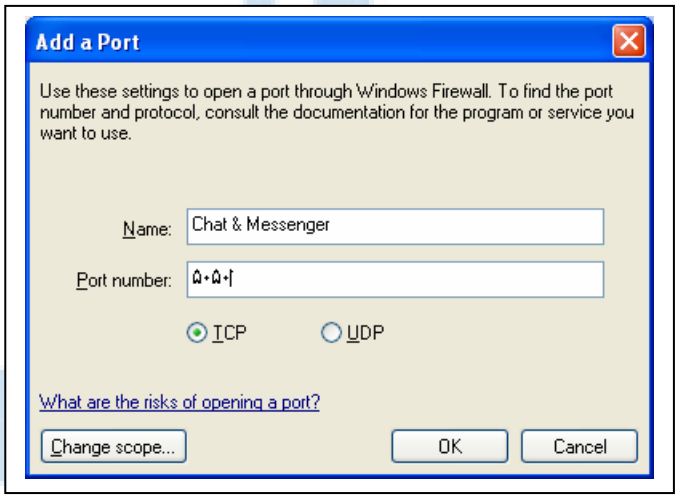
جدول

Chat & Messenger	TCP Port 5050: Client Access only
Insider/Room Lists	TCP Port 80: Client Access only
File Transfer	TCP Port 80: Server Access.
Voice Chat	UDP 5000-5010 TCP 5000-5001: Client Access
WebCam	TCP Port 5100: Client Access
Super Webcam	TCP Port 5100: Server Access

مثلا برای استفاده از Webcam در برنامه فوق با ید درگاه شماره ۵۱۰۰ از نوع TCP را بروی کامپیوتر خود باز کنیم .

حال برای باز کردن درگاه های فوق در دیواره آتش به شکل زیر عمل میکنیم .

ابتدا بروی دکمه Add Port کلیک میکنیم . سپس مطابق با شکل ۵-۷



شکل ۵-۷

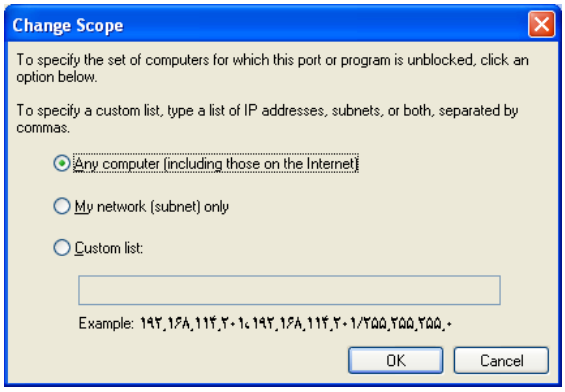
ابتدا نام درگاه و سپس شماره آنرا وارد میکنیم. در قسمت بعد نوع درگاه به لحاظ TCP,UDP را نیز تعیین میکنیم .

نکته :

بعد از وارد کردن شماره درگاه حتما باید میدان یا ناحیه ای که این درگاه ها باید در آن فعال باشند ، تعیین کنید تا از دسترسی غیر مجاز به کامپیوتر شما جلوگیری شود.

برای این منظور روی گزینه Change Scope کلیک کنید.

شکل ۶-۷



مطابق شکل سه حالت را می توانید انتخاب کنید.

- Any Computer در این حالت تمامی کامپیوتر هایی که به سیستم شما متصل است ، می توانند از این درگاه استفاده کنند (حتی شبکه اینترنت).
- My Network این حالت فقط شامل کامپیوتر های داخل شبکه می شود که کلاس و محدوده ی IP آن با کامپیوترشما سازگار است.
- Custom List در این حالت می توانید یک محدوده ی IP به خصوص تعیین کنید که نسبت به حالت های قبلی محدودتر است. مطابق زیر:

192.168.2.12 , 192.168.2.234 / 255.255.255.0

نکات مهم در باز کردن درگاه ها :

۱- فقط در گاه ها را باز کنید که به آنها نیاز دارید.
۲- هرگز برنامه ها یا در گاه ها که برای شما ناشناس هستند را باز نکنید.
۳- برنامه ها یا در گاه ها که به مدت طولانی مدت به آنها نیاز ندارید، را پیوسته بسته نگه دارید.

کار عملی :

تعیین کنید برنامه های Google Talk , msn messenger از چه در گاه ها برای ارتباط استفاده می کنند.

برنامه را برای امکان ارتباط با شبکه به دیواره آتش معرفی کنید.

۷-۲- سرویس دهنده Proxy

سرویس دهنده Proxy اغلب با یک دیواره آتش ترکیب می گردد. سرویس دهنده Proxy بمنظور دستیابی به صفحات وب به وسیله ی سایر کامپیوترها استفاده می گردد. زمانیکه کامپیوتری درخواست یک صفحه وب را می نماید، صفحه مورد نظر به وسیله ی سرویس دهنده Proxy بازیابی و در ادامه برای کامپیوتر متقاضی ارسال خواهد شد. بدین ترتیب تمام ترافیک (درخواست و پاسخ) بین درخواست کننده یک صفحه وب و پاسخ دهنده از طریق سرویس دهنده Proxy انجام می گیرد.

سرویس دهنده Proxy می تواند کارائی استفاده از اینترنت را افزایش دهد. پس از دستیابی به یک صفحه وب ، صفحه فوق بر روی سرویس دهنده Proxy نیز ذخیره (Cache) می گردد. در صورتیکه در

آینده قصد استفاده از صفحه فوق را داشته باشید، صفحه مورد نظر از روی سرویس دهنده Proxy در اختیار شما گذاشته می شود(الزامی به برقراری ارتباط مجدد و درخواست صفحه مورد نظر نخواهد بود)

خود آزمایی و تحقیق

۱- دیوار آتش چیست؟

۲- آیا وجود دیواره آتش در یك شبکه ضروري است؟ چرا؟

۳- یك کامپیوتر از چه جنبه هایي ممکن است مورد حمله قرار بگیرد؟

۴- ماکرو چیست؟

۵- آیا مي توان از دیواره آتش به جاي ضدویروس استفاده کرد؟ چرا؟

۶- کار زبانه **Exceptions** در پنجره **Firewall** چیست؟

۷- تحقیق کنید که چه برنامه هاي دیواره آتش رایجي وجود دارد؟

فصل هشتم- آشنايي با برخي از شبكه هاي WAN

هدف هاي رفتاري

تكنولوژي DSL را تعريف كند
مزايا و معايب DSL را بيان كند.
شبكه هاي محلي بدون سيم را تعريف كند.

۸-۱ DSL[1]-

DSLيك تكنولوژي دسترسي به اينترنت مي باشد كه با استفاده ازخطوط تلفن ارتباطي با سرعت بيش از ۱/۵۴۴ مگابايت را برقرار مي نمايد. از مزاياي DSL اين است كه مي تواند به طور همزمان داده و صوت را منتقل نمايد .بنابر اين ضمن برقرار ماندن ارتباط تلفني مي توان با استفاده از آن ارتباط اينترنتي نيز برقرار نمود .

در حال حاضر اكثر كاربران خانگي شبكه اينترنت و حتي برخي سازمان ها از طريق مودم هاي آنالوگ به وصل مي شوند . افزايش سريع حجم داده هاي اينترنت و نياز به انتقال صوت و تصوير ، محدوديت هايي را براي انتقال داده ها با مودم هاي معمولي شده است لذا براي كاهش اين محدوديت ها تكنولوژي هاي پيشرفته اي مورد استفاده قرار مي گيرد .

فركانسهاي استفاده شده در مخابرات ۴ كيلو هرتز است تكنولوژي DSL با استفاده از فركانسهاي بالاتر از و با تكامل Digital Signal Processing (DSP) قادر به ارسال داده ها با سرعت هاي خيلي بالاتر نسبت به مودم هاي آنالوگ مي باشد.

۸-۱-۱- مزايا ومعايب DSL:

- برقراري DSL نياز به كابل كشي جديد ندارد و با استفاده از خطوط تلفن امكان اتصال به DSLوجود د ارد.
- هنگام برقراري ارتباط اينترنتي با DSL نيازبه قطع شدن مكالمه تلفني نيست و خط تلفن آزاد است.
- سرعت برقراري ارتباط با DSL (۱,۵ Mbps) در مقايسه با سرعت مودم هاي معمولي(56 Kbps) به مراتب بالاتر است.

معايب:

- فاصله بين سرويس گيرنده و سرويس دهنده خدمات اينترنت در سرعت ارتباط موثر است و با افزايش فاصله سرويس گيرنده از مركز ارايه سرويس DSL سرعت كاهش مي يابد .
- اين سرويس داراي محدوديت فاصله تا ۵۴۶۰ متر مي باشد

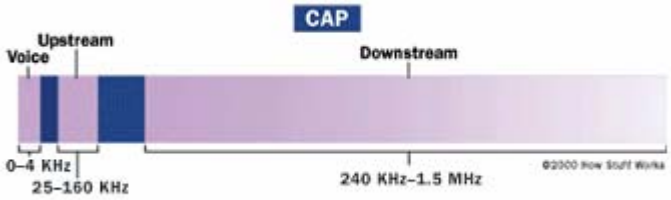
[1] - Distributed Subscriber Line

- امكان دريافت اين سرويس درهمه مناطق به دليل متداول نبودن آن وجود ندارد.
- هزينه اوليه برقراري سرويس DSL بالاتر است.

۲-۱-۸- اصول كار DSL:

همانطور كه مي دانيد سيستم تلفن استاندارد با يك زوج سيم مسي(TP) انجام مي شود از طرف ديگر سيم هاي مسي داراي مقدار زيادي فضا براي حمل اطلاعاتي بيش از مكالمات تلفني هستند و مي توانند طيف وسيعي از فركانسها را بيش از چيزي كه در انتقال صوتي استفاده مي شود پشتيباني كنند.DSL با استفاده از اين فضاي اضافي ارتباط اينترنتي را برقرار مي نمايد بدون اينكه در كيفيت ارسال مكالمات مشكلي ايجاد كند.

تكنولوژي DSL مي تواند حداكثر سرعت DownStream 8 مگابيت در ثانيه در فاصله حدود ۱۸۲۰ متر و سرعت UpStream تا ۶۴۰ كيلوبيت برثانيه را در اختيار كاربران قرار دهد(شكل ۱-۸).



شكل۱-۸

در عمل بهترين سرعتهاي موجود امروزي در مسيرDownStream تكنولوژي DSL به ميزان ۱,۵ مگابيت بر ثانيه است و سرعت UpStream بين ۶۴ تا ۶۴۰ كيلوبيت بر ثانيه مي باشد .

تحقيق كنيد در سرويس DSL دليل افت سرعت در فواصل دورتر چرا شديدا كاهش مي يابد ؟

۳-۱-۸- سيستم هاي تفكيك سيگنال در DSL

قبلاً اشاره شد كه DSL از سيم هاي تلفن براي برقراري ارتباط اينترنتي استفاده مي كند بناب اين لازم است كه به نحوي سيگنال هاي ارتباط تلفني و اينترنتي را به نحوي كنترل نمايد براي تفكيك وكنترل سيگنال ها در گذشته از سيستم CAP استفاده مي شد و امروز بيشتر از سيستمي به نام DMT[1] استفاده مي شود (شكل۱-۸).

سيستم CAP سيگنالهاي موجود در خط تلفن را به سه باند متمايز از هم تقسيم مي كند:

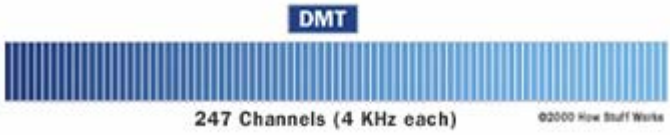
- مكالمات صوتي در باند صفر تا ۴ كيلو هرتز
- كانال UpStream باند ۲۵ تا ۱۶۰ كيلو هرتز
- كانالDownStream در فركانس۲۴۰ كيلوهرتز تا فركانسي

اين سيستم با سه كانال كاملا جدا امكان تداخل بين كانالهاي روي يك خط يا بين سيگنالها در خطوط مختلف را به حداقل مي رساند.

سيستم ديگري كه براي كنترل سيگنال ها استفاده مي شود سيستم DMT است ، سيستم DMT نيزسيگنالها را به سه كانال جداگانه تقسيم مي كند ، و مجموعه را ۲۴۷ كانال تقسيم مي كند .ازبين اين ۲۴۷ كانال جداگانه كه هريك ۴ كيلو هرتز پهنا دارند ، از دوتاي آنها

[1] Discrete Multi Tone

استفاده مي كند .هركانال دائما تحت نظارت قرار دارد تا اگر كيفيت سيگنال مطلوب نباشد ، از سيگنال كانال ديگري استفاده شود . اين سيستم دائما بهترين كانال را براي ارسال و دريافت پيدا مي كند .



شكل۲-۸

فرستنده /گيرنده DSL يا Transciever :

اغلب مشتركين خانگي از فرستنده / گيرنده DSL به عنوان مودم ياد مي كنند .

فرستنده / گيرنده را مي توان با چند روش به يك دستگاه سمت مشترك متصل نمود . اغلب سيستمهاي خانگي از ارتباط USB يا اترنت 10-Base-T استفاده مي كنند . در حاليكه اغلب فرستنده /گيرنده هاي DSL عرضه شده به وسيله ISP ها وشركت تلفن ، فرستنده /گيرنده مي باشند ، اما دستگاههاي مورد نظر در شركتهاي تجاري تركيبي از Router ها ، Switch ها و يا ساير تجهيزات شبكه بندي هستند.

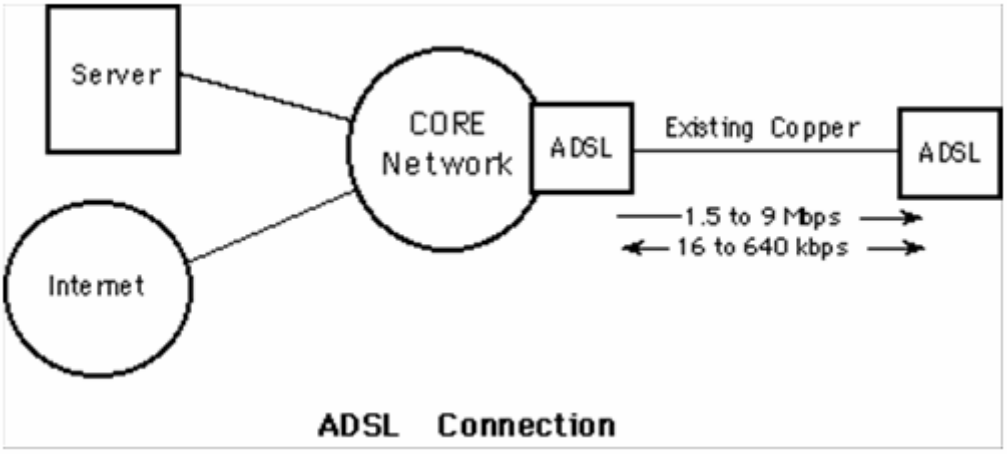
۴-۱-۸- انواع DSL :

سرويسDSL انواع گوناگوني دارد . از قبيل ADSL، IDSL ، CDSL، DSL Lite، HDSL، RADSL، VDSL ولي در عمل از انواع ADSL و VDSL بيشتر از بقيه موارد استفاده مي شود .

ADSL[1] :

با توجه به شكل ۱-۸ پهناي باند بيشتري در DownStream نسبت به UP Stream وجود دارد و از طرف ديگر كاربران اينترنت ، به طور معمول خيلي بيشتر از آن چيزي كه اطلاعات مي فرستند ، از شبكه اطلاعات دريافت مي كنند . سرعت انتقالات در ADSL براي ارسال اطلاعات به مشتري بيشتر از 6Mbps براي دريافت اطلاعات و بيشتر از 640Kbps براي ارسال و دريافت اطلاعات مشترك (در هر دو مسير) مي باشد به اين دليل اين سرويس را نامتقارن مي نامند.

[1] -Asymmetric Digital subscriber Line



شكل ۳-۸- دريافت و ارسال در ADSL

مدار ADSL به يك مودم ADSL متصل مي گردد در خط ADSL سه كانال اطلاعاتي مختلف ايجاد مي شود : يك كانال پرسرعت براي DownStream ، يك كانال دوطرفه با سرعت متوسط و يك كانال براي سرويس تلفن اصلي ، اگر ADSL خراب شود ، سرويس تلفن اصلي برقرار مي ماند .

VDSL[1]:

VDSL يك تكنولوژي توسعه يافته است و در مسافتهاي كوتاه (حدود ۳۰۰ متر) سرعت انتقال بسيار بالايي (بين51Mpbsتا 55Mpbs) دارد .در بسياري از موارد همراه با سرويس ADSL به كار گرفته مي شود

۲-۸- شبكه هاي محلي بدون سيم Wireless LAN

شبكه هاي محلي بي سيم (WLAN) فن آوري جديدي در شبكه محلي است كه استفاده كنندگان را قادر مي سازد به شبكه يك سازمان در هر مكاني از آن سازمان دسترسي پيدا كنند ، بدون آن كه نيازي به اتصال فيزيكي به شبكه مذكور داشته باشند .

همانطور كه قبلاً گفته شد شبكه هاي محلي بدون سيم از فركانس راديويي يا امواج مادون قرمز ، به عنوان سيگنال هاي ارتباطي و ازهوا به عنوا رسانه انتقال ، استفاده مي كنند .

توپولوژي WLAN

براي پياده سازي شبكه WLAN ، هر ايستگاه داراي يك كارت شبكه بدون سيم (Wireless NIC) مي باشد و مي تواند با هر ايستگاه ديگري كه در محدوده باشد ارتباط برقرار نمايد . ساده ترين اين ارتباط مي تواند به صورت نقطه به نقطه به وسيله ی دو ايستگاه (Point-to-Point) باشد .

شكل ۴-۸- شبكه Point-to-Point (شكل ۲۱-۵ ص۳۸ آشنايي با شبكه)

[1] - Very High Data Rate DSL

نوع ديگر پيكربندي شامل استفاده از وسيله اي به نام نقطه اتصال (Access Point) است . AP وسيله اي است كه ايستگاه ها ي بدون سيم را قادر مي سازد تا به شبكه محلي متصل گردند .

شكل ۴-۸ نشان مي دهد كه يك Access Point از طريق يك سيم به شبكه LAN متصل شده است . ارتباط ايستگاه ها ي بدون سيم را از طريق هوا به كمك ارتباط كابلي كه با HUB دارد ، برقرار مي سازد . به عنوان يك پل ارتباطي بين ايستگاه ها ي بدون سيم و شبكه محلي عمل مي كند.

شكل ۵-۸ارتباط ايستگاه ها ي بدون سيم با شبكه محلي به وسيله ی AP (شكل -۵-۲۲ ص۳۹ آشنايي با شبكه)

ناحيه اي كه به وسيله ی يك AP تحت پوشش قرار مي گيرد سلول (Cell)ناميده مي شود وسعت ناحيه تحت پوشش و تعداد ايستگاه ها ي كه مي توانند ازطريق يك AP با شكه ارتباط برقرار نمايند ، محدود مي باشد و با افزايش ناحيه و تعداد ايستگاه ها ، بايد تعداد AP را افزايش داد.

ازمهمترين مزاياي شبكه هاي محلي بدون سيم مي توان به موارد زير اشاره نمود :

- نيازي به سيم كشي براي هر ايستگاه كاري نيست
- در زمان بر قراري ارتباط امكان حركت وجود دارد و استفاده كنند ه مي توانند بدون اينكه ارتباط خود را قطع كند رايانه خود را جابجا نمايد.

شكل ۶-۸ شبكه WLAN با چند Access Point صفحه ۳۹ آشنايي با شبكه

خود آزمايي و تحقيق

۱. تکنولوژي DSL بر چه اساسي مبتني است؟

۲. VDSLمخفف چه واژه هايي است و به چه مفهومي مي باشد.

۳. مزاياي شبکه WLANرا بنويسيد.

۴. وظيفه AP در شبکه WLAN چيست؟

۵. معايب DSL چيست؟

۶. انواع DSL را نام ببريد.

۷. تفاوت عمده خطوط DSL با خطوط Dialup در چيست؟

بخش دوم

Windows 2003 Server

فصل نهم- مديريت دسترسی به منابع

هدف هاي رفتاري
ويژگي هاي پوشه هاي به اشتراك گذاشته شده را بيان كند.
پوشه ها را به اشتراك بگذارد و به آنها مجوز يدهد.
از پوشه هاي به اشتراك گذاشته شده در شبكه را استفاده كند.
مجوزهاي مديريتي ايجاد كند.
مجوزهاي مؤثر را محاسبه كند.

۱- ۹- پوشه های به اشتراک گذاشته شده

زمانی که بخواهیم کاربران به فایلهای یک پوشه از طریق شبکه بتوانند دسترسی پیداکنند ،آن را به اشتراک می گذاریم .بعد ازاین عمل ، کاربرانی که به آنها مجوز اعطا شده باشد می توانند از منابع موجود در آن استفاده نمایند. برای دسترسی ساده تر به اطلاعات مي توان فايل ها را در پوشه های متفاوتی به اشتراک گذاشت.

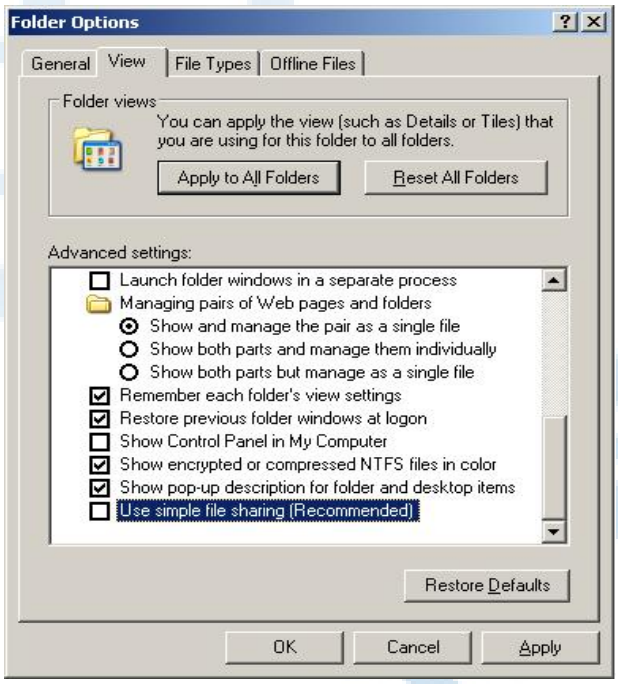
. برخي ازويژگی پوشه های به اشتراک گذاشته شده عبارتند از::

۱- در My computer زیرپوشه های به اشتراک گذاشته شده یک دست به نشانه اشتراک گذاشتن ظاهر می شود.
۲- شما فقط پوشه ها را می توانید به اشتراک بگذارید ویک فایل را نمی توان به اشتراک گذاشت .برای انجام این کار آن فایل را می توانید داخل یک پوشه کپی کنید و سپس آن پوشه را به اشتراک بگذارید.
۳- به اشترک گذاشتن یک ویژگی مربوط به سیستم عامل می باشد:بنابراین شما می توانید یک پوشه را درهر فایل سیستمی که ویندوز پشتیبانی می کند به اشتراک بگذارید (FAT,FAT32,CDFS,NTFS) با این تفاوت که اگر آن پوشه در پارتیشنی با فایل سیستم NTFSباشد ،قابلیت کنترل بیشتری را دراختیار مدیر شبکه قرار میدهد.
۴- فقط اعضای گروه های power users،administrators در کامپیوترهای عضوDomain می توانند یک پوشه را به ترتیب در روی DCها و کامپیوترهای عضوDomain به اشتراک بگذارند.
۵- اگر پوشه ای که می خواهیم به اشتراک بگذاریم در داخل یک پارتیشین NTFS باشد ، برای به اشتراک گذاشتن آن ، کاربر علاوه بر عضویت در گروهای ذکر شده باید حداقل مجوز دسترسی Read روی آن پوشه باید داشته باشد.

۹-۲- نحوه به اشتراک گذاشتن پوشه ها

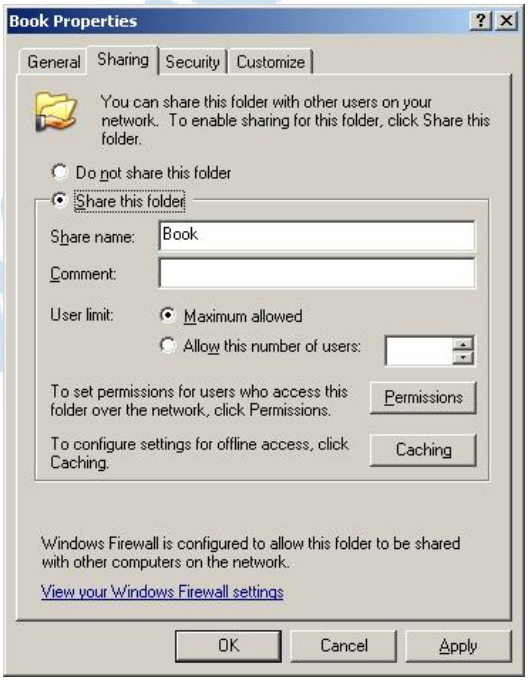
یک پوشه را به روشهای مختلف می توان به اشتراک گذاشت . درزیر به دوروش اشاره می شود.

نکته : اگر پوشه ای که به اشتراک می گذارید در یک کامپیوتر با سیستم عامل xp قرارداشته باشد یک گزینه use simple file sharing را در زبانه Folder option واقع در control panel باید برداشته باشید تا بتوانید به روشی که گفته خواهد شد آنرا به اشتراک بگذارید. (شکل ۱-۹)



شکل ۱-۹

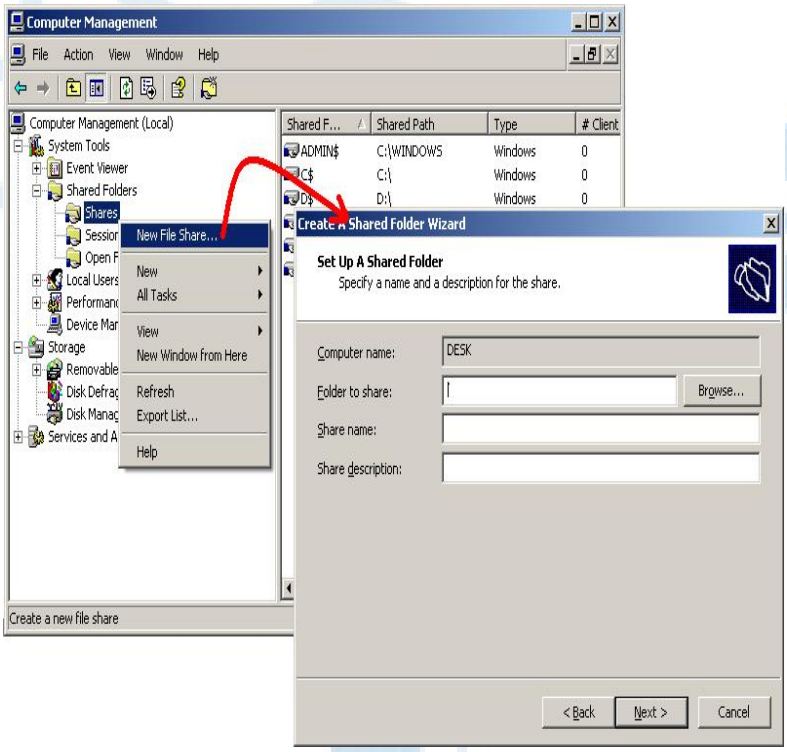
روش اول : در my computer روی یک پوشه کلیک راست کرده و ازمنویی که ظاهر می شود گزینه sharing and security را انتخاب نمایید. سپس گزینه share this folder انتخاب نمائید و در قسمت share name یک اسم منحصر به فرد در آن تایپ نمائید و سپس روی گزینه okکلیک کنید. (شکل ۲-۹)



(شکل ۲-۹)

روش دوم : در این روش شما با استفاده از computer management یک پوشه را به اشتراک می گذارید . ابتدا computer management را از control panel/ Administrative اجراء نمایید .

- روی shares در share folder از System Tools کلیک کرده و ازمنوی Actionگزینه New shareرا انتخاب نمائید .
- در ویزاردی که ظاهر می شود آدرس پوشه ای را که میخواهید به اشتراک بگذارید ، تایپ نموده و سپس یک اسم در قسمت share name واردکرده و گزینه Next را انتخاب نمایید . (شکل ۳-۹)

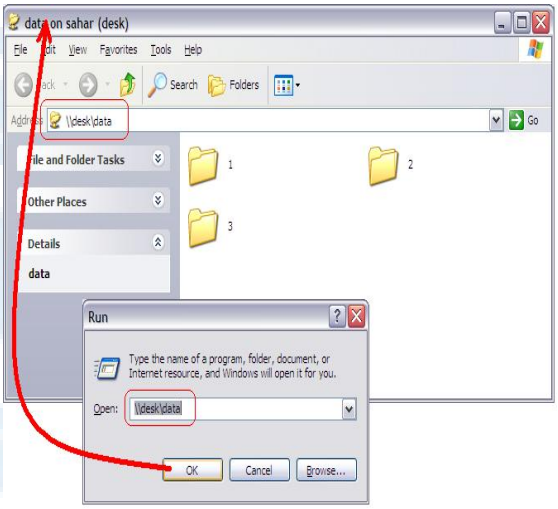


شکل ۳-۹

- در صفحه بعد نحوه اعطای مجوز روی پوشه به اشتراک گذاشته شده سؤال می شودگزینهNext را انتخاب نمائید .
- پنجره دیگری ظاهر شده و سؤال می کند که آیا پوشه دیگری را میخواهید به اشتراک بگذارید.گزینه No را انتخاب کنید .مشاهده خواهیدکردکه یک گزینه به لیست پوشه های به اشتراک گذاشته شده اضافه خواهد شد.

۳-۹ - آدرس دهی به شبکه (UNC Path)

کاربران براي دیدن فایل های یک پوشه به اشتراک گذاشته شده می توانند از آدرس دهی UNC استفاده نمائید . این نوع آدرس دهی به صورت \\ computername \ share name می باشد . به عنوان مثال براي دیدن فایل های داخل یک پوشه به اشتراک گذاشته شده به نام Data دریک کامپیوتری به نام desk می توانیم در start / Run ، \\ Desk\ Data را تایپ کنیم و سپس روی گزینه ok کلیک کنید تا محتویات آن را نمایش دهد. (شکل ۴-۹)



شکل ۹-۴

۹-۴-پوشه های به اشتراک گذاشته شده : مخفی (Hiden shares)

برای به اشتراک گذاشتن مخفیانه یک پوشه کافیست که در انتهای share name یک علامت $ قرار دهید تا زمانیکه کاربران پوشه های به اشتراک گذشته آن کامپیوتر را می بینند، آن پوشه نمایش داده نخواهد شد .بنابراین کاربران برای استفاده از اطلاعات آن پوشه باید در computer name/share name $Run را واردکنند تا فایل های آن به نمایش در آورده شوند.

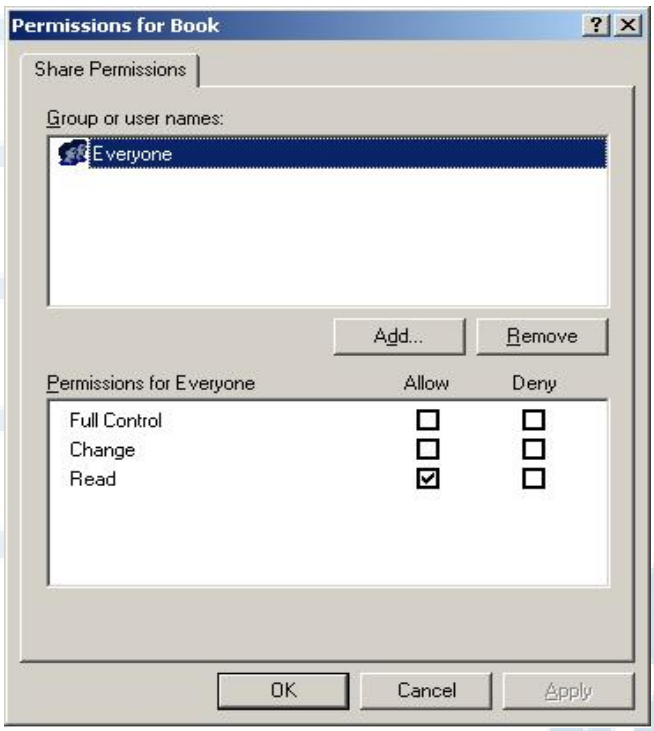
۹-۵- Administrative shares

اشتراک هایی وجود دارند که براي انجام کارهای مدیریتی می توانند مورد استفاده قرارگیرند . از جمله آنها می توان به موارد زیر اشاره نمود:

- C$,d$,E$,....: ریشه تمامی درایوها به صورت مخفی به اشتراک گذاشته می شوند و فقط اعضای گروه Administrative share اجازه دسترسی به آنها را ازطریق شبکه را خواهند داشت .
- Admin$: پوشه ویندوز در تمامی کامپیوترها به نام Admin$ به اشتراک گذاشته می شود و شما می توانید به آن از طریق شبکه دسترسی پیداکنید.
- Ipc$: کاربردی برای کاربران و مدیران شبکه نداشته بلکه براي مدیریت از راه دور و دسترسی کاربران به پوشهای به اشتراک گذاشته شده مورد استفاده قرار می گیرد .

۹-۶- مجوزهای پوشه های به اشتراک گذاشته شده

این مجوزها به کاربران فقط زمانی اعمال می شوند که به پوشه مربوطه از طریق شبکه دسرتسی پیدا می کنند و دسترسی از همان کامپیوتر هیچ محدودیتی ایجاد نمی کند . این مجوزها سه نوع می باشند (شکل ۹-۵)



شکل ۹-۵

- Read: این مجوز به صورت پیش فرض به گروه Everyoneروی هر پوشه به اشتراک گذاشته ای داده شده است به کمک این مجوز می توان :
  - اسامی فایل ها و پوشه را مشاهده نمود.
  - محتویات و خواص فایل ها را مشاهد نمود.
  - برنامه ها را اجرا نمود.
- Change: این مجوز تمام قابلیت های مجوز Read را دارا بوده و علاوه بر آن اجازه می دهد که
  - فایل ها و یا پوشه ها را ایجاد و یا اضافه کنیم
  - محتویات فایل ها را تغییر دهیم
  - فایل ها و پوشه ها را حذف نمائید.
- Full control: این مجوز تمامی قابلیت های Change, Read را داشته ، همچنین اجازه می دهد که مجوزهای NTFS فایل ها و پوشه ها را تغییر دهید.

۹-۶- محاسبه مجوزهای مؤثر

۹-۶-۱ محاسبه مجوز در پارتیشن های غیر NTFS

محاسبه مجوز در پارتیشن های غیرNTFS بدین صورت است که اجتماع Shared Permissionهای کاربر و گروهایی که عضوشان می باشید را حساب کنید، مگر اینکه یک مجوز Deny‌شده باشد.

جدول ۹-۱ بایک مثال مجوز مؤثر کاربر user1 راکه عضو گروهای group1،group2 می باشد را نشان می دهد

جدول ۹-۱

	shared Permission
User 1	Read

Group 1	----------
Group 2	Change
Effective shared Permission	Change

۹-۶-۲ محاسبه مجوز در پارتیشن های NTFS

در این پارتیشن ها شیوه محاسبه مجوز بدین صورت است که در ابتدا مجوزمؤثرNTFS و مجوز مؤثر پوشه به اشتراک گذاشته را به صورت جداگانه و با قوانینی که قبلا به آنها اشاره شده محاسبه کرده و سپس اشتراک آن دو مجوز مؤثر برای دسترسی از طریق شبکه خواهد بود . جدول زیر مجوز مؤثر کاربر user1 را که عضو گروهای group2،group1 می باشد را نشان میدهد.

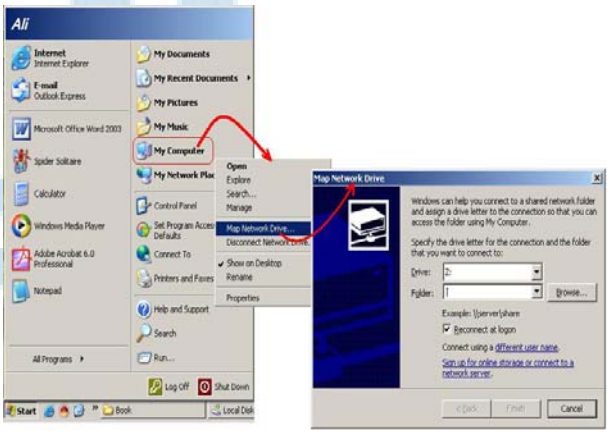
جدول ۹-۲

Group	shared Permission	NTFS Permission
USER 1	READ	READ
GROUP 1	CHANGE	WRITE
GROUP 2	FULL CONTROL	WRITE (Deny)
EFFECTIVE	FULL CONTROL	READ
FROM EFFECTIVE NETWORK	READ	READ

۹-۷ درایوهای شبکه

براي دسترسی به پوشه های به اشتراک گذاشته شده می توان از درایوهای شبکه استفاده نمود . به این ترتیب که به جای استفاده از آدرس های UNC از درایوهای شبکه استفاده نمود.

- برای انجام این کار روی My Computer یا My Network Places کلیک راست کرده و ازمنویی که ظاهر می شود ...Map Network Driver را انتخاب نمائید .
- حال در پنجره ای که ظاهر می شود از گزینه Drive ، درایو مورد نظر را انتخاب نموده و مقابل گزینه Folder آدرس UNC پوشه مربوطه را وارد کنید و سپس روی گزینه Finish کلیک کنید . (شکل ۹-۶)



شکل ۹-۶

اگر وارد My Computer شوید ملاحظه خواهید کرد که یک درایو شبکه به لیست درایوهای موجود اضافه شده است.

فعالیت عملی

درايوي يه نام U براي به اشتراك گذاشتن پوشه مورد نظر خود انتخاب و چند تصوير براي گروه عضو شبكه به اشتراك بگذاريد

خود آزمايي و تحقيق

۱- چگونه مي توان دسترسي هم زمان به يك پوشه به اشتراك گذاشته شده را محدود كرد؟

۲- چگونه مي توان يك پوشه را به صورت مخفي به اشتراك گذاشت؟

۳- منابع قابل اشتراك گذاري در شبكه را نام ببريد.

۴- تفاوت صدور مجوز در پارتيشن NTFS و پارتيشن هاي ديگر را بيان كنيد.

۵- Map Drive چيست؟ چگونه مي توان آن را ساخت؟

۶- تحقيق كنيد كه چگونه مي توان از طريق خط فرمان يك پوشه را به اشتراك گذاشت؟

فصل دهم- پیاده سازی و مدیریت چاپ در شبکه

هدف هاي رفتاري

اجزاي چاپ در شبکه را تعریف کند.
بر روي سرور چاپ و کلاینت ها چاپگر نصب کند.
مجوز دسترسی کاربران به چاپگرهای به اشتراک گذاشته شده کنترل کند.
بتواند صف کارهاي چاپي را کنترل کند.
Spool Folder را تعریف کند و بتواند آدرس آن را تغییر دهد.
مجوزهاي دسترسي در پارتیشن هاي NTFS را شرح دهد.

۱۰-۱ آشنایی با اجزای چاپ در شبکه

یکي از امکاناتي که شبکه در اختیار ما قرار مي دهد به اشتراك گذاشتن منابع فیزیکي است و از این طریق علاوه این که مي توانید مدیریت مناسبي بر انجام امور داشته باشید با استفاده از آن مي توانید با صرفه جویي در هزینه ها بهره وري را افزایش دهید در این فصل به اشتراك گذاشته شدن چاپگر به عنوان یکي از منابع مهم در ادارات و شرکت ها مورد بررسي قرار مي گیرد قبل از شروع لازم است با برخي از واژه های مختلف چاپ در شبکه آشنا شوید

- Printer[1]: به نرم افزار رابط بین دستگاه چاپ و کاربران « چاپگر» گفته می شود .چاپگرها به دونوع تقسیم می شوند :
  - Local printer: به چاپگری اطلاق می شود که می خواهیم در کامپیوتر خود نصب کرده و از آن استفاده کنیم و یا در شبکه به اشتراك بگذاریم .به عبارت دیگر اگر کامپیوتر خود را بخواهیم به Print server تبدیل کنیم ، از این نوع چاپگر باید استفاده کنیم .
  - Network printer: اگر بخواهیم ازیک چاپگر به اشتراك گذاشته شده در شبکه به عنوان یککلاینتاستفاده کنیم ازاین نوع چاپگر استفاده خواهیم کرد.
- Print Device: به دستگاه چاپ گفته می شود . دستگاه های چاپ به دونوع تقسیم می شوند :
- Local print Device: به دستگاه چاپی گفته می شود که مستقیما به یکی از درگاه های کامپیوتر متصل می شود.
- Network Interface print Device: به دستگاه چاپی گفته می شود که به وسیله ی کارت شبکه به شبکه متصل می شود .
- Print server: به سروری گفته می شود که یک چاپگر در آن نصب و به اشتراك گذاشته می شود .
- Print Queue: به کارهای چاپی که در یک چاپگر منتظر چاپ شدن می باشند ، گفته می شود.

---

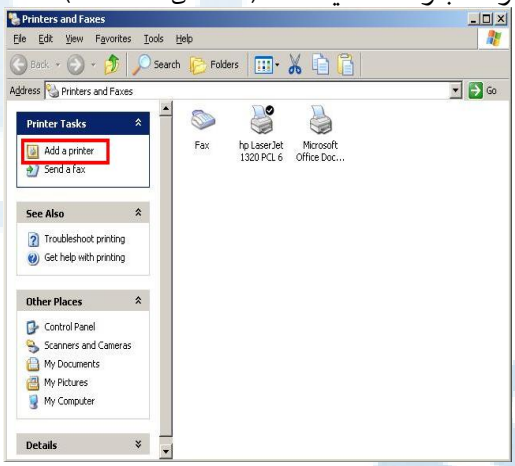
[1] - اصطلاح چاپ که در درس مباني کامپیوتر به دستگاه چاپگر اطلاق شد یك اصطلاح غلط متداول است که در آن درس پذیرفته شده است.

- Print job: به یک سندی که برای چاپ و به یک چاپگر فرستاده می شود ، اطلاق می گردد .

۲-۱۰- نصب چاپگرها

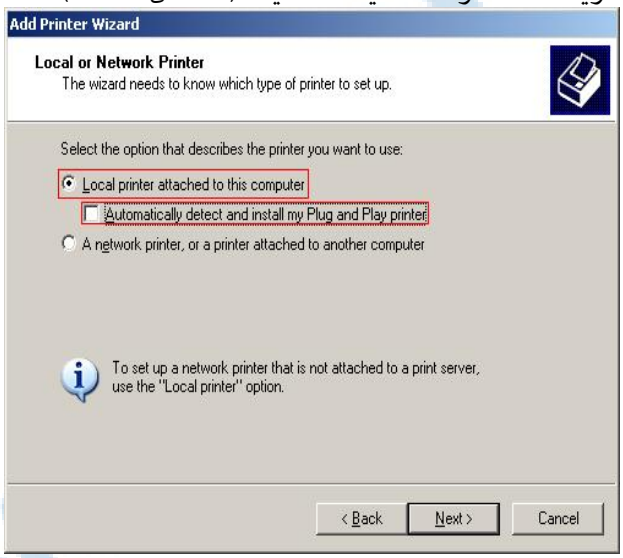
۱-۲-۱۰- نصب و به اشتراک گذاشتن چاپگر روی سرور چاپ

- برای نصب چاپگر Add a printer را از مسیر Control panel \ printers and faxes مطابق شکل زیر اجرا کنید. (شکل ۱-۱۰)



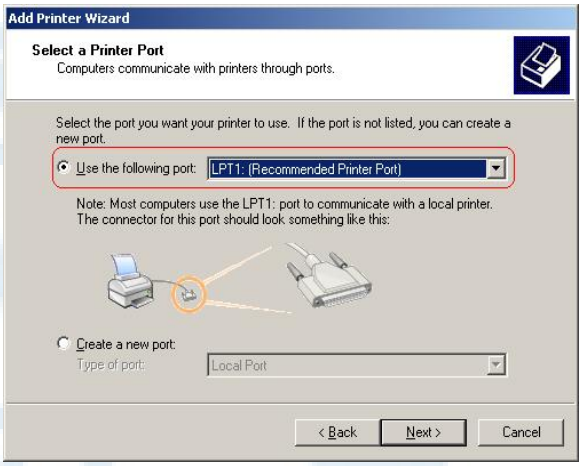
شکل ۱-۱۰

- از ویزاردی که ظاهر می شود گزینهNext راکلیک کنید. در صفحه بعد براي نصب چاپگر و به اشتراک گذاشتن آن گزینه اول را مطابق شکل ۲-۱۰ انتخاب نموده و تیک گزینه ...Automatically detectرا برداریدو گزینه Nextرا کلیک کنید (شکل۲-۱۰)



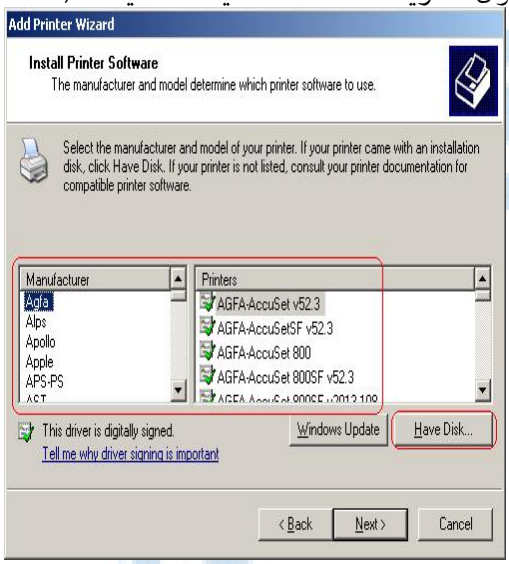
شکل ۲-۱۰

- در صفحه بعد مطابق شکل ۳- ۱۰ گزینه Use the following port را انتخاب کرده و ازلیست مقابل آن LPT1 (یا هر درگاهدیگری که دستگاه به آن متصل است) را انتخاب کرده و روی گزینه Next کلیک کنید. (شکل ۳-۱۰)



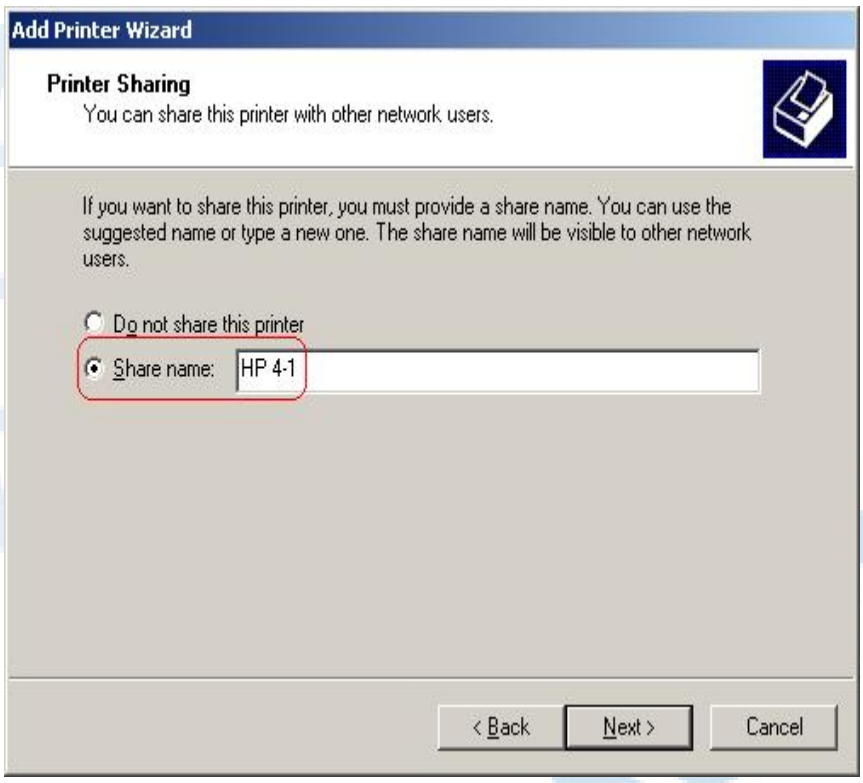
شکل ۳-۱۰

- در صفحه بعد از لیست چاپگرهای نمایش داده شده چاپگر خودرا انتخاب کنید. در صورتی که چاپگر را درلیست نتوانستیم پیداکنید ، درایور چاپگر را به کمک گزینه Have disk معرفی کنیدوروی گزینه Next کلیک کنید.(شکل ۴-۱۰)



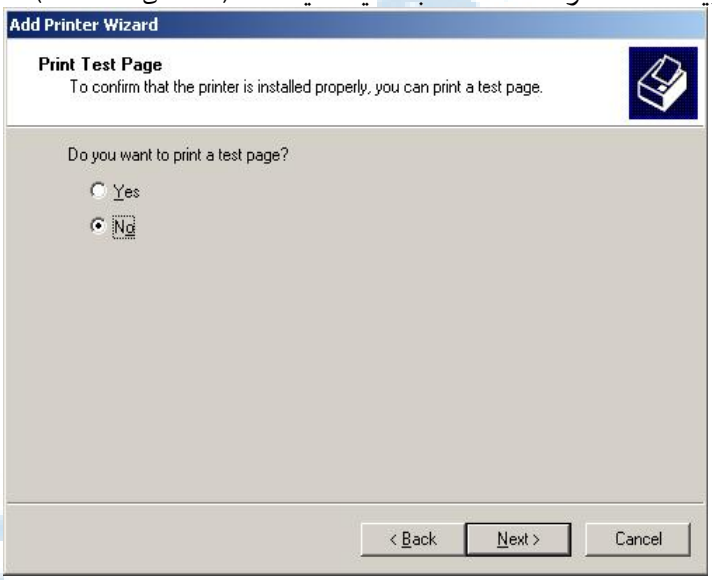
شکل ۴-۱۰

- در صفحه بعد یک اسم برای چاپگر انتخاب نموده و روی گزینه Next کلیک کنید.
- در صفحه بعد ی مطابق شکل ۵-۱۰ گزینه Share Name را انتخاب نموده و مقابل آن یک اسم که در این کامپیوتر منحصر به فرد باشد تایپ کنید. این اسم برای کاربرانی که ازطریق شبکه به این کامپیوتر متصل می شوند نمایش داده می شود . سپس روی گزینه Next کلیک کنید. .(شکل ۵-۱۰)



(شکل ۵-۱۰)

- اطلاعات صفحه بعد خارج از موضوع کتاب می باشد و از آن صرفنظر کنیدوروی گزینه Next کلیک کنید. در صفحه بعد براي حصول اطمینان از صحت درایور چاپگر گزینه Yes ودرغیر این صورت گزینه No را انتخاب میکنید. (شکل ۶-۱۰)

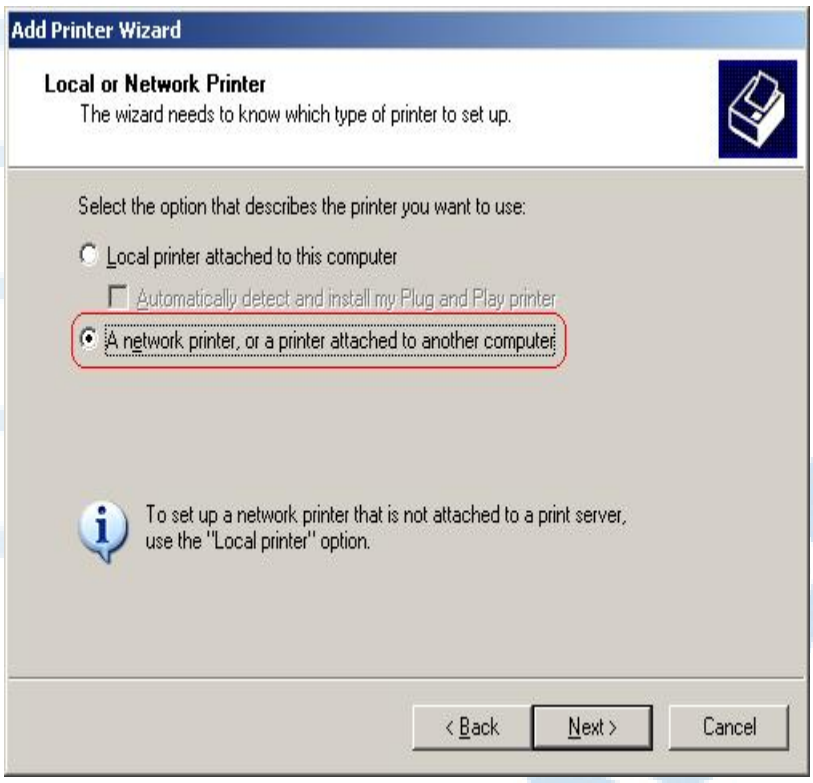


(شکل ۶-۱۰)

- در صورت انتخاب گزینه Yes یک صفحه بصورت آزمایش براي چاپ به دستگاه چاپ ارسال خواهد شد .در صفحه بعد روی گزینه Finish کلیک کنیدتا نصب چاپگر را به پایان برسانید.

۱۰-۲-۲ نصب چاپگر روی کلاینت

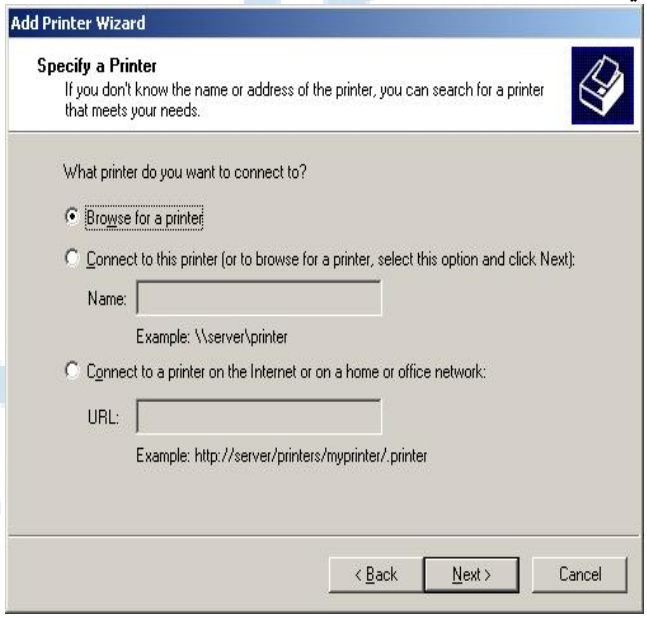
حال دریکی ازکلاینت های شبکه گزینه Add a printer را از مسیر Control Panel \ Printer And Faxes انتخاب کرده سپس گزینه نشان داده شده را مطابق شکل ۷-۱۰ انتخاب و روی گزینه Next کلیک کنید.



(شکل ۷-۱۰)

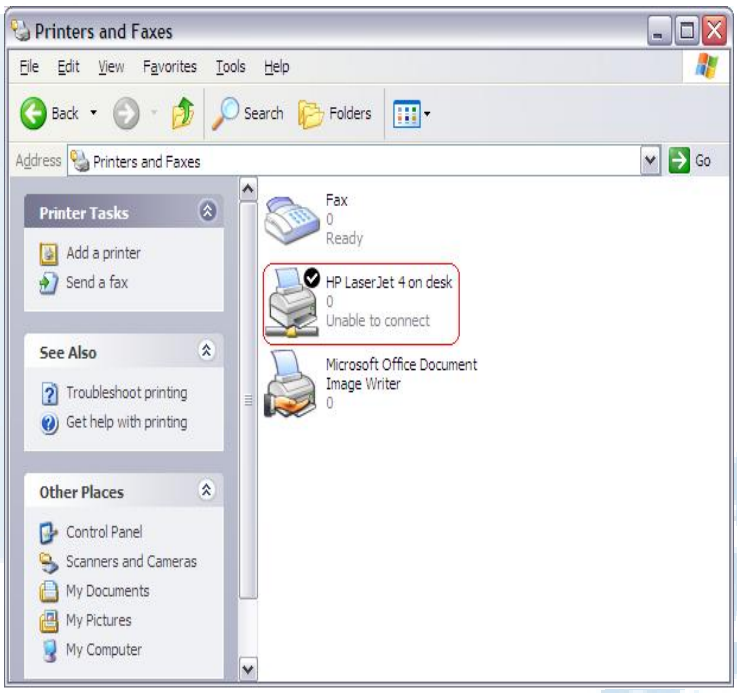
در این صفحه مطابق شکل ۸-۱۰ گزینه:

- Browse for A printer: را برای انتخاب یک چاپگر از لیست چاپگرهای شبکه ، انتخاب کنید.
- Connect to this printer را به منظور تایپ آدرسUNC یک چاپگر خاص انتخاب کنید
- Connect to a printer on the internet... را به منظور استفاده از یک چاپگری که در اینترنت روی یک سرور چاپ به اشتراک گذاشته شده انتخاب کنید شکل (۸-۱۰)



شکل (۸-۱۰)

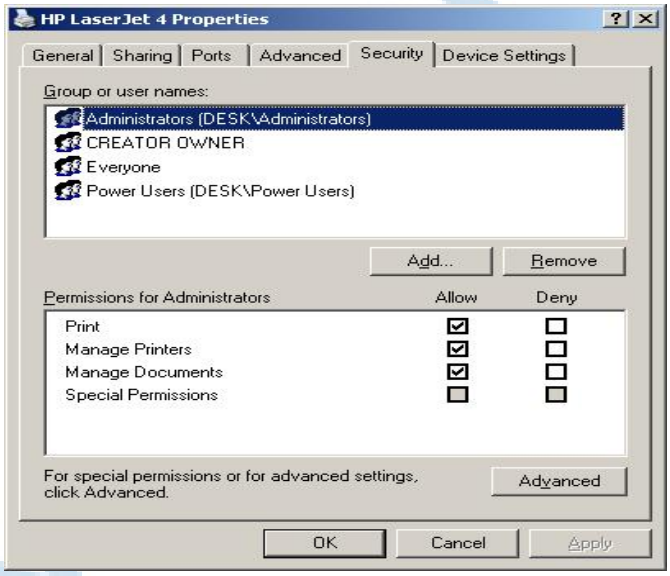
- سپس ویزارد را مشابه نصب چاپگر روی سرور چاپ ادامه داده و گزینه Finish را در صفحه آخرانتخاب نمائید تا نصب چاپگر روی کلاینت به پایان برسد . که دراین صورت مشاهده می کنید که یک چاپگر درکلاینت اضافه شده است . شکل (۹-۱۰)



شکل (۹-۱۰)

۳-۱۰ مجوزهای چاپ

در ویندوز می توان با استفاده از سطوح دسترسی مختلف دسترسی کاربران را به چاپگرهای به اشتراک گذاشته شده کنترل کرد . به این منظور از سطوح دسترسی زیر میتوان استفاده نمود:شکل (۱۰-۱۰)



شکل ۱۰-۱۰

- Print:به کمک این مجوز کاربر می تواند به یک چاپگر متصل شده و اسناد خودرابرای چاپ به آن ارسال کنید .
- Manage printers: این مجوز علاوه براین که تمامی کارایی مجوز Print را دراختیار کاربر می گذارد، به کاربر امکان مدیریت کامل چاپگر رانیز می دهد ، طوری که کاربر می تواند یک چاپگر را pause ویا Restart نماید یا چاپگر را به اشتراک بگذارد ، مجوزهای کاربران را روی چاپگر تغییردهد و همچنین ویژگی های مختلف چاپگر را تغییر دهد.
- Manage document:کاربر به کمک این مجوز می تواند اسنادی را که کاربران دیگر به چاپگر ارسال نموده اند، Restart،Resume،pause

ویا cancel نماید . به وسیله این مجوز کاربر نمی تواند اسناد خودرا به چاپگر ارسال نماید.

زمانی که کاربر روی چاپگر دارای مجوز بوده و همچنین عضو گروه هایی باشد که آنها نیز دارای مجوز باشند، مجموع مجوزها، مجوز نهایی آن کاربر خواهد بود . اما اگر مجوزی برای کاربر یا یکی از گروههایی که کاربر در آن عضویت دارد منع شده باشد (Deny) ، آن مجوز بیشترین اولویت را خواهد داشت

مجوزهای پیش فرض که به گروه های مختلف اعطا می شود ، در جدول زیر خلاصه شده است :

جدول ۱-۱۰ مجوز هاي پیش فرض

گروه ها	Manage printer	Manage Document	Print
Administrator	*	*	*
Creator owner	–	*	–
Everyone	–	–	*
Power users	*	*	*
Print operators	*	*	*
Server operators	*	*	*

۱۰-۴- نحوه اعطای مجوز به کاربران روی چاپگرها

براي اعطای مجوز کافیست که روی چاپگر مربوطه کلیک راست کرده وگزینه Properties را انتخاب نمائید وسپس در زبانه Security می توانید لیست کاربران و گروها وهمچنین مجوزهای آنهارا مشاهد نموده وبا استفاده از کلیدهای Add یا Removeبه کاربران و گروهای مختلف مجوز اعطا نمائید .

۱۰-۵- نحوه مدیریت صف کارهای چاپی

براي انجام این کار می توانید روی چاپگر مربوط دوبار کلیک کنید. پنجره ای مطابق شکل ۱۱-۱۰ ظاهر شده ولیست تمامی کارهای چاپی را نمایش می دهد اگر روی یک کارچاپی کلیک راست نمائید ، منویی ظاهر می شود که شامل فرمان های زیر خواهد بود :

Pause: به کمک این گزینه می توان یک کار چاپ را به صورت موقتی متوقف نمود.
Restart: با این فرمان می توانید کار چاپی را یک بار دیگر از ابتدا به دستگاه چاپ ارسال نمائید.
Cancel: با این فرمان می توانید از چاپ شدن کار چاپی جلوگیری نموده و آنرا از صف کارهای چاپی حذف نمائید.
Properties: این گزینه باعث نمایش ویژگی های کارچاپی شده و به شما اجازه می دهد که اولویت کارچاپی نسبت به کارهای چاپی دیگر را تعیین نمایید .
همچنین می توانید تعیین نمائید که به یک کاربر خاص بعدازچاپ شدن کار چاپی یک پیغام ارسال نماید ونهایتاً اینکه می توانید تعیین کنید که کار چاپی در یک بازه زمانی مشخص بتواند چاپ شود .

شکل ۱۱-۱۰

۶-۱۰- تغییر آدرس Spool Folder

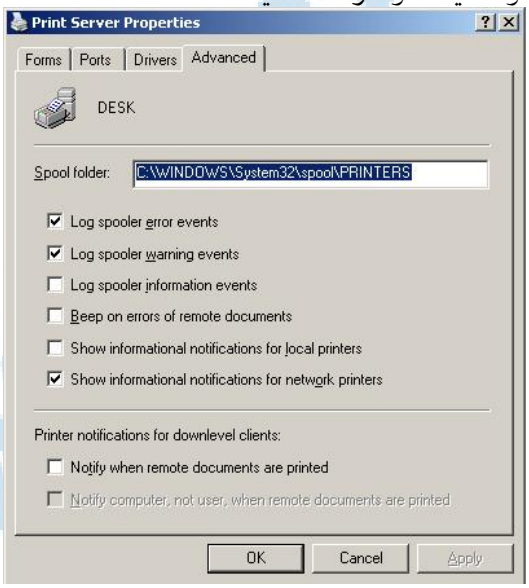
هنگامیکه در ویندوز یک فایلی را چاپ می کنید . آن فایل به طور مستقیم به دستگاه چاپ ارسال نمی شود در ابتدا آن کار چاپی به وسیله ی یکی از سرویس های ویندوز به نام Print Spooler د رداخل یک فایلی نوشته شده وسپس درصف قرارداده می شود.

به این عمل اصطلاحاً spooling می گویند . این عمل باعث می شود که برنامه ای که از آن برای چاپ استفاده می کنید. مستقیما درگیر کارچاپ نشده و شما بتوانید به کارتان با آن برنامه ادامه دهید. فایل هایی که به این شیوه تولید می شوند بانام Spool Folder قرار می گیرند .

دریک سرور چاپ که تعداد کارهای چاپی در آن زیاد باشد ، شما می توانید آدرس این پوشه رابه یک درایو دیگر تغییر دهید .

این عمل می تواند به دلیل افزایش فضای آزاد برای Spooling و یا بازدهی بهتر آن عمل باشد.

- براي انجام این کار گزینه Server Properties را ازمنوی Printers And Faxes انتخاب کرده و روی زبانه Advanced کلیک کنید
- در قسمت Spool Folder در پنجره باز شده.(شکل ۱۰-۱۰) آدرس جدید را می توانید وارد کنید.



شکل (۱۲-۱۰

۷- ۱۰- آشنایی با مجوزها :

مجوزها بیانگر نوع دسترسی که به کاربر یا گروه و یا کامپیوتر برروی یک object اعطا شده می باشند .

بعنوان مثال شما می توانید به یک کاربر اجازه دسترسی به محتویات یک فایل را یدهید و درعین حال به کاربر دیگر مجوز

اعمال تغییرات روی همان فایل داده و سایر کاربران را از دسترسی به آن فایل منع کنید .

یا به عنوان مثالی دیگر ، می توانید مجوزهای یک چاپگر را طوری تغییردهید که بعضی از کاربران بتوانند تنظیمات آن را تغییر دهند درصورتیکه بقیه کاربران فقط بتوانند به آن چاپگر کار چاپی ارسال کنند .

البته مجوزها را می توان روی objectهای مختلفی مثل فایل ها و پوشه ها ، چاپگرها ، Active directory، object های رجیستری و غیره انتصاب داد.اما دراین کتاب فقط در ارتباط با مجوزهای فایل ها و پوشه ها و چاپگرها و پوشه ها ی به اشتراک گذاشته شده بحث خواهیم نمود.

مجوزهایی که به کاربران یا گروها برروی یک object انتصاب می دهید ، به نوع آن object بستگی دارد .

به عنوان مثال مجوزهای فایل ها متفاوت از مجوزهای چاپگرها می باشند.

۱-۷ -۱۰ - مجوزها در پارتیشین های NTFS

پارتیشن های با فایل سیستم NTFSدارای قابلیت هایی هستند که در پارتیشن های بافایل سیستم FATیا FAT32وجود ندارند.ازجمله این قابلیت ها می توان به مواردی چون NTFS Compression، NTFS Encryption، Disk Quota، NTFS permission s، نمود

NTFS permissions مجوزهایی هستند که می توان روی یک فایل یا پوشه به کاربران انتساب داد. با استفاده از این مجوزها می توان میزان دسترسی یک کاربر به یک فایل یا پوشه از طریق my computer ویا از طریق شبکه را تعیین نمود . به این معنی که مجوزها هم به صورت Localو هم ازطریق شبکه ایجاد می کنند .

مجوزهای standard, special

مجوزهای دسترسی در پارتیشن های NTFSبه دو دسته standard, special تقسیم می شوند

مجوزهایstandard ، بیشترین مجوزهای مورد استفاده مدیران شبکه می باشند و مجوزهای special مجوزهایی هستند که جزئی از مجوزهای standardبوده و همچنین کمتر مورد استفاده قرار می گیرند به عبارت دیگر یک مجوز standard از تعدادی مجوز specialتشکیل شده است .

براي نمایش مجوزها ابتدا روی یک فایل یا پوشه کلیک سمت راست کرده و گزینه propertiesو سپس در پنجره نمایش داده شده زبانه securityرا انتخاب کنید.

نکته : اگر سیتم عامل مورد استفاده ویندوز xp professionalباشد به صورت پیش فرض این زبانه نمایش داده نمی شود . برای نمایش آن باید یک گزینه use sirple file sharingرا در control panel / folder option/ view tab بردارید .

شکل ۱۳-۱۰ مجوزهای standard

در پنجره ای که ظاهر می شود روی کلید Advancedکلیک کنید و در پنجره بعدی یکی از گزینه ها راانتخاب کرده و سپس کلید Editرا انتخاب نمائید تا لیست مجوزهای special نشان داده شوند.

شکل ۱۴-۱۰ مجوزهای special و Advanced Tab

جدول زیر لیست مجوزهای NTFSروی فایل ها و پوشه ها را توضیح می دهد.
این مجوزاجازه می دهد که بتوانید فایل ها و پوشه ها در داخل یک پوشه ، مجوزها و مالک و Readخصلت های یک فایل یا پوشه را ببینید .

اجازه می دهد که یک فایل یا پوشه در داخل یک پوشه ایجاد کنید . خصلت های موجود روی یک فایل یا پوشه را writerتغییر دهید و همچنین مالک ولیست مجوزها را ببینید.
اسامی فایل ها وپوشه ها در داخل یک پوشه را لیست می کند List folder contents

تمامی مجوزهایی که Read ، List folder contents در اختیار ما قرار میدهد و Read Execute همچنین اجازه میدهد که فایلها ی اجرایی داخل یک پوشه را اجرا کنید.

تمامی مجوزهای بیان شده د ربالا + مجوز Delete کردن فایل ها و پوشه ها Modify

Full control = Modify + Delete subfolders and files + change permissions + Take ownership
مجوزهای لیست شده د ردیف Full control جزو مجوزهای special می باشند.

۲-۷-۱۰- وراثت در مجوزهای NTFS

هنگامیکه یک درایو را فرمت میکنید یک پوشه به نام ریشه (Root folder)
به صورت اتوماتیک در آن ایجاد می شود. اگر روی درایو مربوط کلیک راست کرده و گزینه properties را انتخاب نمائید ، درزبانه security لیست مجوزهایی که به صورت پیش فرض روی پوشه ریشه انتساب داده شده را خواهید دید. در این حالت به شما اجازه داده می شود که مجوزها را تغییردهید .(تیک مجوزها به رنگ سبز نمایش داده می شوند.)
حال اگر درداخل آن درایو یک فایل یا پوشه ای ایجادکنید ، تمامی مجوزها از ریشه به آن فایل یا پوشه به ارث خواهند رسید.
اگر مجوزهای موجود برروی فایل یا پوشه را ملاحظه کنید ، متوجه خواهید شد که آنها را در ستون Allow نمی توانید تغییر دهید (به رنگ خاکستری نمایش داده می شوند .) ، در حالت کلی زمانی که یک فایل یا پوشه جدید ایجاد می کنید ، مجوزها را از پوشه ای که در داخل آن قراردارد (parent folder) به ارث خواهد گرفت.

۸-۱۰- مجوزهای مؤثر

اگر یک کاربر مجوزی روی یک منبع داشته و عضو گروهایی باشد که آنها نیز دارای مجوزی روی آن منبع باشند ، مجوز مؤثر آن کاربر روی آن منبع به شرح زیرمحاسبه خواهد شد .
در این حالت اجتماع مجوزهایی که به کاربر یا به گروها اعطا شده ، مجوز مؤثر کاربرخواهد بود .فقط در حالتی که یک مجوز Denyشده باشد به مجوزهایی که درهمان رده Allow شده باشند برتری خواهد داشت و قابل محاسبه نخواهد بود

خود آزمایی و تحقیق

۱- تفاوت Printer و Print Device در چیست؟

۲- وراثت را در NTFS توضیح دهید؟

۳- مجوز موثر چیست؟

۴- Spool Folder چیست؟

۵- تفاوت دو مجوز Special و Standard را بنویسید.

۶- تحقیق کنید آیا گروه Creator Owner مي تواند از چاپگر استفاده کند.

۷- تحقیق کنید که چه روش دیگري براي نصب چاپگر در روي شبکه وجود دارد.

فصل یازدهم-نصب و راه اندازی Active Directory

هدف های رفتاری

- Domain و اجزاي Active directory را تعریف کند.
- بتواند Active Directory نصب کند.
- نحوه عضویت کلاینت ها و انواع Log on ها را شرح دهد.

۱-۱۱ آشنایی با Domain و اجزاء Active Directory

همانطوری که در بخش های قبلی اشاره شده است ، مدل workgroup درشبکه های مایکروسافت یک مدل ساده می باشد.
بدین معنی که در این شبکه مدیر مرکزی وجود ندارد و هر کاربر مدیر کامپیوتر خود محسوب می شود .دریک چنین مدلی اگر بخواهید یک policyبرای کامپوترها و یاکاربران تعیین کنید ، آن را به صورت جداگانه د ریکایک کامپیوترها باید تنظیم کنید . اما در صورت راه اندازی Domain این امکان وجود دارد که یک نفر بتواند تمامی کاربران ، کامپیوترها و منابع را در شبکه از طریق هر کامپیوتری مدیریت نماید .
همچنین در این حالت می توان یک policy خاص را فقط یک بار تعریف نمود و آن policy به تمامی کامپیوترها و یا کاربرانی که مد نظر می باشند ، اعمال خواهد شد.
براي راه اندازی Domain برنامه ای به نام Active Directoryرا در یک سرور standard aloneباید نصب کنید . بعد از نصب برنامه آن سرور به Domain controller (DC) تبدیل خواهد شد.
DCوظیفه authetication در Domain رابه عهده دارد ، بدین معنی که زمانی که یک کاربر از روی یککلاینتها به Domain می خواهد Logon کند ، اسم و گذر واژه کاربر به صورت کد شده به DCفرستاده می شود .DC که اطلاعات تمامی کاربران د رDomain را دارا می باشد ، اطلاعات دریافتی را با اطلاعاتی که خود از کاربران دارد مقایسه می کند ودر صورتی که صحت داشته باشد یک کارت شناسایی که اصطلاحاً آن را بانام Aecess Taken می شناسید به کاربر ارسال کرده و درستی اطلاعات آن کاربر را بهکلاینتاطلاع می دهد .
از این به بعد براي دسترسی کاربر به تمامی منابع موجود در Domain از کارت شناسایی مذکور استفاده می شود .

۱-۱۱- نصب Active Directory

براي نصب Active Directory و راه اندازی اولین DC در Domain از صحت مواردیکه در زیر بیان شده اطمینان حاصل کنید:
یک کارت شبکه در سیستم شما نصب شده و ضمناً به شبکه متصل می باشد.

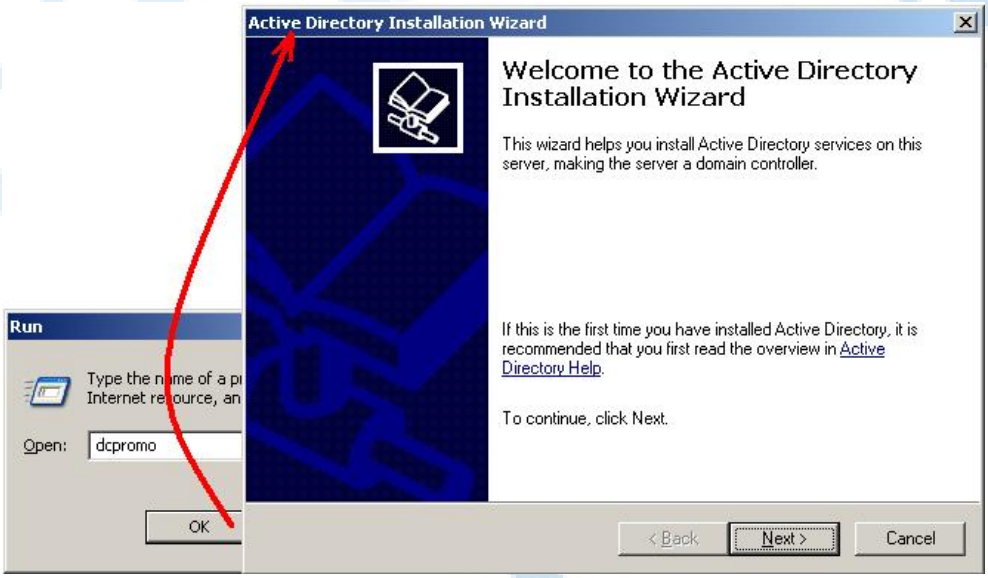
درصورتیکه کارت شبکه در سیستم شما موجود نمی باشد و یا در صورت وجود به شبکه متصل نمی باشد ، حتماً باید یک کارت شبکه مجازی (Microsoft Loopbak Adapter) نصب نمائید.

یک آدرس IP به صورت ثابت به کارت شبکه انتصاب داده شده وهمان IPدر قسمت Preferred DNS Serverوارد شده باشد.

CD ویندوز سرور 2003 دردرایو CD موجود بوده و یا پوشه I386ازهمان CD در دیسك سخت دیسك کامپیوتر کپی شده باشد. البته لازم به توضیح است که براي نصب Active Directoryنیازی به CD سرور نمی باشد ولی چون در حین نصب سرویس DNS نیز نصب خواهد به CD سرور 2003 نیاز خواهید داشت.

حتماً با کاربر Administator و یا کاربر دیگری که عضو گروه Administators می باشد Logon کرده باشید.

حال در Start/Runفرمان DCPromo را تایپ و اجرا نمائید . ویزاردی مطابق با شکل زیر ظاهر خواهد شد.



شکل ۱-۱۱

این ویزارد در صورتی که Active Directory نصب نباشد ، آن را نصب نموده و در غیر این صورت آن را حذف خواهد کرد.
گزینه Nextرا انتخاب کنید.

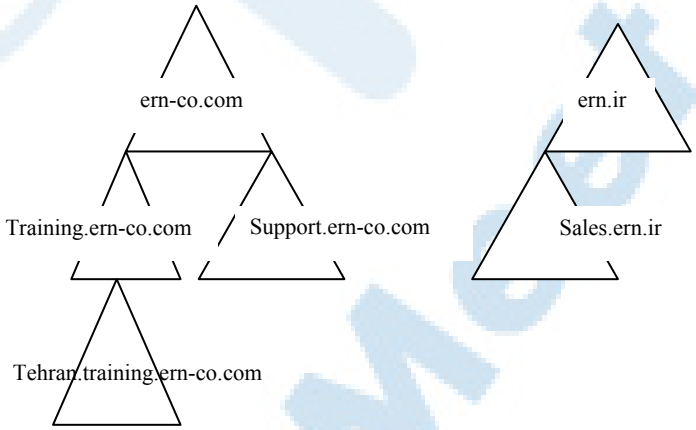
پنجره Next را انتخاب کنید. حال پنجره شکل ۳-۱۱ ظاهر خواهد شد . دراین پنجره از ما سؤال می شود که DCجدید : Domain controller for a new domain :یک DCدر Domainجدید خواهد بود

Additional domain controller for an existing domain : یک DC اضافه در Domainموجود خواهد بود
دراین پنجره ما گزینه اول را انتخاب کنید. چون هیچ Domain ي ایجاد نشده است و ما اولین DCبرای یک Domainرا می خواهید راه اندازی کنید و سپس گزینه Nextرا انتخاب کنید. پنجره ای مطابق با شکل ۳-۴ ظاهر خواهد شد .
دراین پنجره نوع Domainکه می خواهید ایجاد کنید سؤال شده است :
Domain ina new forest : Domain در یک جدید
Child Domain in an existing domaintree : child domain ازیک Domain tree موجود
Domain tree in an existing forest : یک root domainجدید در یک forestموجود.

شکل۲-۱۱

با توجه به اینکه مباحث مطرح شده د راین قسمت خارج از بحث این کتاب می باشد ، به طور خلاصه به ساختاری Active directoryبه کمک شکل ۳-۱۱ اشاره کنید.

ساختار Active Directory از یک مجموعه به نام forest (جنگل) تشکیل می شود هر forestمی تواند شامل یک یا تعدادی Domain Tree (درختdomain) بشود . هر Domain Tree از یک یا تعدادی Domainتشکیل می شود طوری که اولین Domainرا با نام Root domain وسایر domainها را با نام child domainمی شناسید هر domainیک اسم اینترنتی یا DNSخواهد داشت و اسامی domainها ی موجود در یک Treeبه هم وابسته خواهند بود. به عنوان مثال اگر اسم اولین domainدر ern-co.com,Tree میتوانید اسامی training.ern-co.com، Tehran.training.ern-co.com,support.ern-co.com, رابرای domainهای child انتخاب کنید .



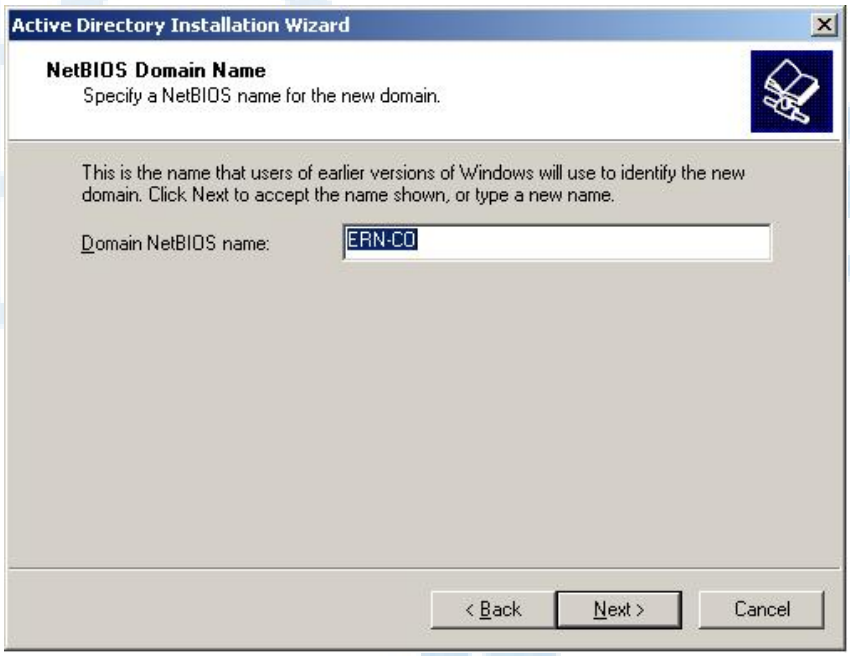
شکل ۳-۱۱

- حال در شکل ۲-۱۱ با توجه به اینکه یک forestجدید می خواهید ایجاد کنید، گزینه اول را انتخاب کرده وسپس گزینه Next را کلیک کنید.
- در پنجره باز شده شکل ۴-۱۱ اسم اینترنتی یا DNSهای Domainاز ما خواسته شده است .

شکل ۳-۱۱

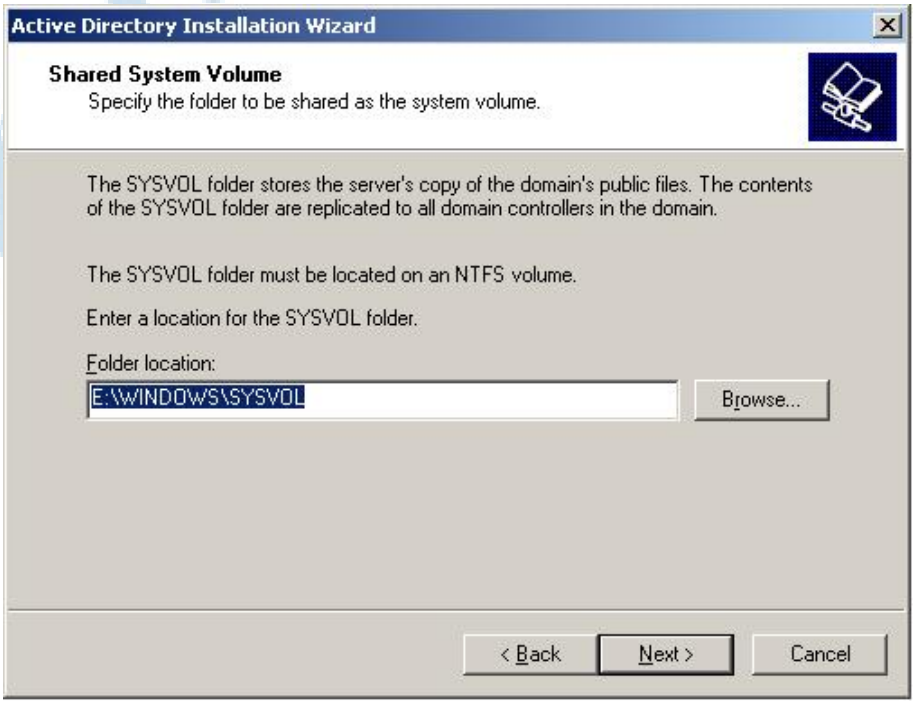
در این پنجره اسم ern-co.comرا واردکرده و گزینه Nextرا انتخاب کنید. دراین مدت ویزارد سراغ DNSسرور می رود تا اطمینان حاصل کند که ازقبل

Domainی با نام ern-co.com ایجاد نشده است همچنین هر Domainباید یک اسم NetBiosداشته باشد که در مثال بیان شده این اسم به صورت پیش فرض ERN-COخواهد بود . عمل دیگری که دراین مرحله انجام می شود این است که اسم ERN-CO در شبکه منحصر به فرد می باشد یا نه در صورت مثبت بودن جواب پنجره شکل ۳-۷ ظاهر شده و ERN-CO را به عنوان اسم NetBios پیش فرض پیشنهاد خواهد داد.



شکل ۴-۱۱

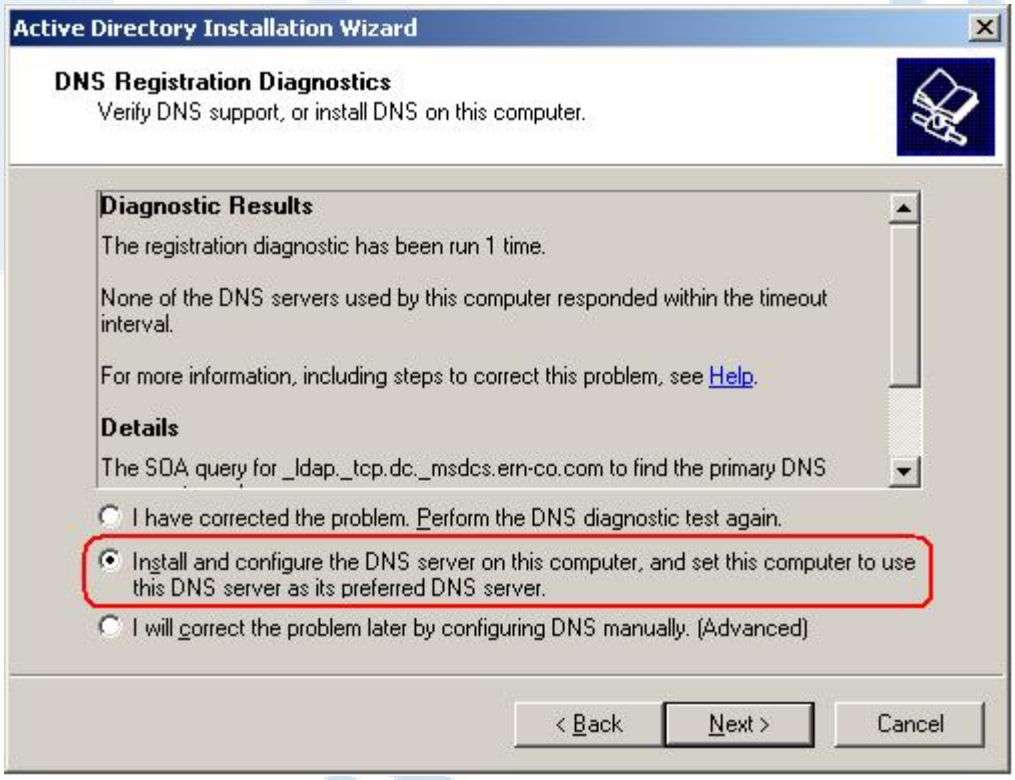
- سپس گزینه Next را انتخاب کنید
- پنجره شکل ۵-۱۱ ظاهر خواهد شد . در این پنجره آدرس پوشه ای که در آن فایل اطلاعات Active Directoryو Log fileهای آن ذخیره می شوند ، سؤال شده است به صورت پیش فرض یک پوشه به نام NTDSدر همان پوشه ای که ویندوز نصب شده است ، پیشنهاد می شود آدرس های پیش فرض را قبول کرده و گزینه Next را انتخاب کنید.
- پنجره شکل ۵-۱۱ به نمایش در خواهد آمد در این پنجره آدرس یک پوشه به نام sysvolازما خواسته شده است . دراین پوشه اطلاعاتی از Domainکه یک کپی از آن به نام DCفرستاده می شود . نگهداری شده واین پوشه حتماً باید در یک پارتیشن با فایل سیستم NTFS قرار داشته باشد . آدرس پیش فرض را قبول کرده و گزینه Next را انتخاب کنید.



شکل ۱۱-۵

نکته: در صورتی که درایوی که ویندوز نصب شده فایل سیستم NTFS نداشته باشد ، قبل از اجرای dcpromo باید فرمان زیررا اجرا کنید تا فایل سیستم آن به NTFS تبدیل شود convert d:/fs:ntfs

- در پنجره باز شده شکل ۱۱-۶ گزینه دوم راانتخاب کرده وگزینه Next



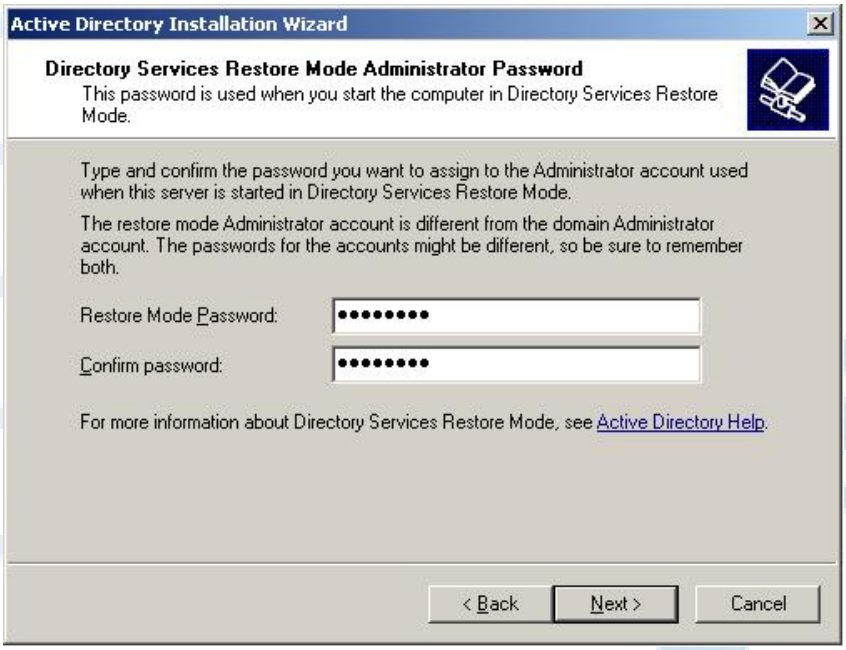
را انتخاب کنید.

شکل ۱۱-۶

- در پنجره شکل ۱۱-۷ گزینه دوم را انتخاب کرده و گزینه Next را کلیک کنید

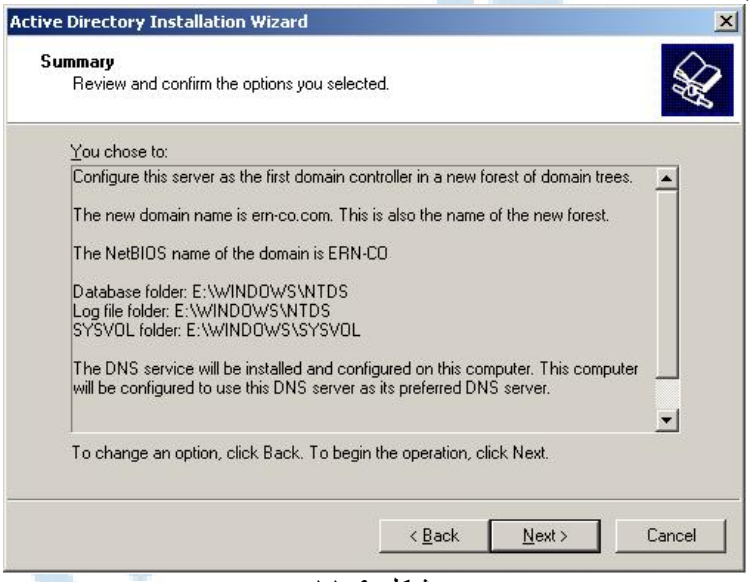
شکل ۱۱-۷

- در پنجره شکل ۱۱-۸ یک گذر واژه برای کاربر Administrator برای برگرداندن اطلاعات Active Directory از Back up از ما خواسته می شود .
- در این پنجره یک گذر واژه به صورت دلخواه دوبار واردکرده و سپس گزینه Next را انتخاب کنید.



شکل۸-۱۱

- در پنجره شکل ۳-۱۰ خلاصه تنظیماتی را که دراین ویزارد ما انجام داده اید نمایش داده است . آنها را مرور کرده و گزینه Next را انتخاب کنید.



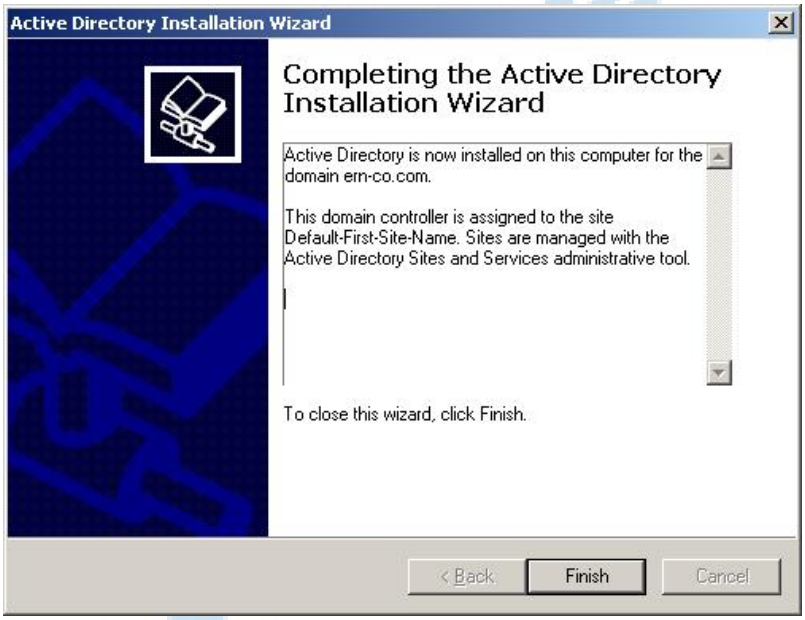
شکل ۹-۱۱

در این حال پنجره شکل ۳-۱۳ ظاهرشده و Active Dierctoryرا نصب می کند و مراحل نصب را برای ما گزارش می کند .

شکل ۹-۱۱

نکته: درحین نصب این سرویس اگر CDویندوز 2003را در درایو قرار نداده باشید، آن را از شما خواهد خواست که دراین حالت باید آدرس پوشه I386رابه آن معرفی کنید تا فایل های لازم براي نصب از روی آن کپی شوند.

بعداز چند دقیقه عمل نصب به پایان رسیده و پنجره شکل ۳-۱۴ ظاهر می شود.



شکل ۱۰-۱۱

در این پنجره گزینه Finishراانتخاب کنید این عمل باعث می شود که پنجره شکل ۳-۱۵ ظاهرشود . در این پنجره گزینه Restart Nowرا انتخاب کنیدتا کامپیوتر ری ست شود.

شکل ۱۲-۱۱

نکته :بعداز نصب این سرویس مدت زمانی که طول می کشد تا سرور بالا بیاید طولانی تر خواهد شد . در صورتی که این مدت زمان خیلی طولانی شد

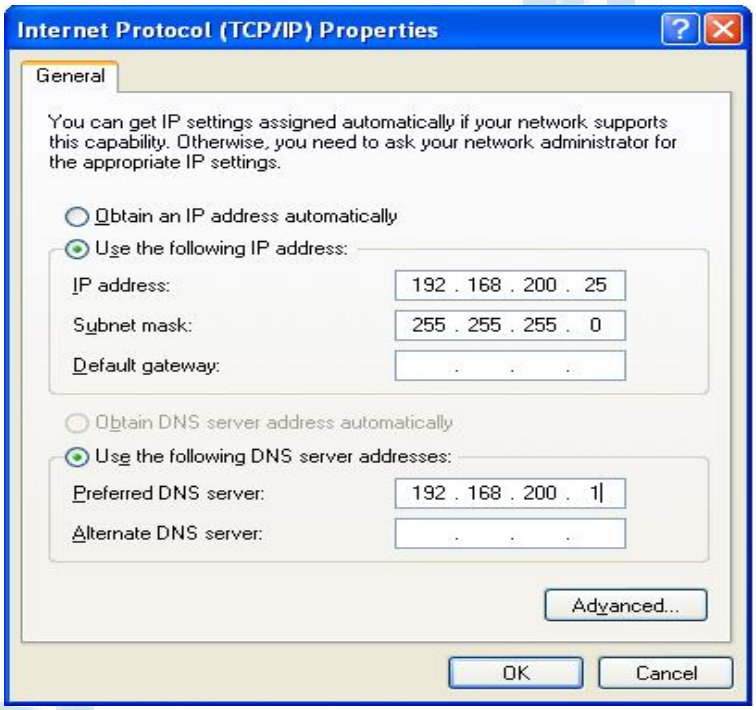
از انجام تنظیمات DNSکه در چند صفحه قبل به آن اشاره گردیده است اطمینان حاصل کنید.

۱۱-۳ عضویت کلاینت ها در Domain

تا این مرحله یک Domainبا یک DCراه اندازی شده است حال می خواهیدکلاینتها را به عضویت Domainدر بیاورید . تا کاربران بتوانند ازروی آن ها به
Domain،Logonکرده و به منابع آن دسترسی پیدا کنند .

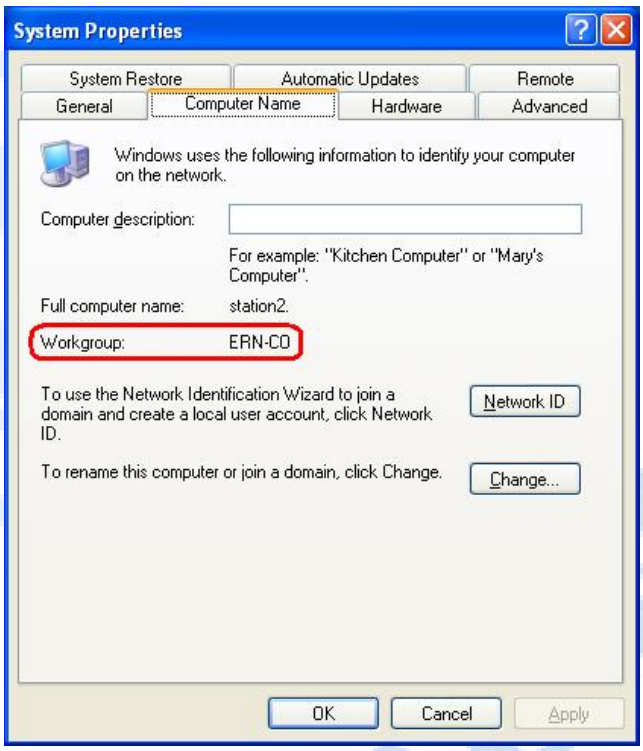
۱-۳-۱۱ نحوه عضویت کلاینت ها

حال در یک کلاینت که سیستم عامل آن ویندوز xpمی باشدباکاربر Administratorواردشده و تنظیمات زیر را در آن انجام می دهید .
۱- control panel/Network connectionروی
properties,local area connectionگرفته و در پنجره ای که ظاهر می شود گزینه Internet protocol (tcp/ip) را انتخاب نموده و سپس روی گزینه propertiesکلیک کنید.
در پنجره ای که ظاهر می شود مطابق شکل ۳-۱۶ یکIPبه صورت منحصر بفرد واردکرده ودر قسمت preferred DNS server
IPیDCرا واردکرده وروی گزینه OKکلیک کنید.



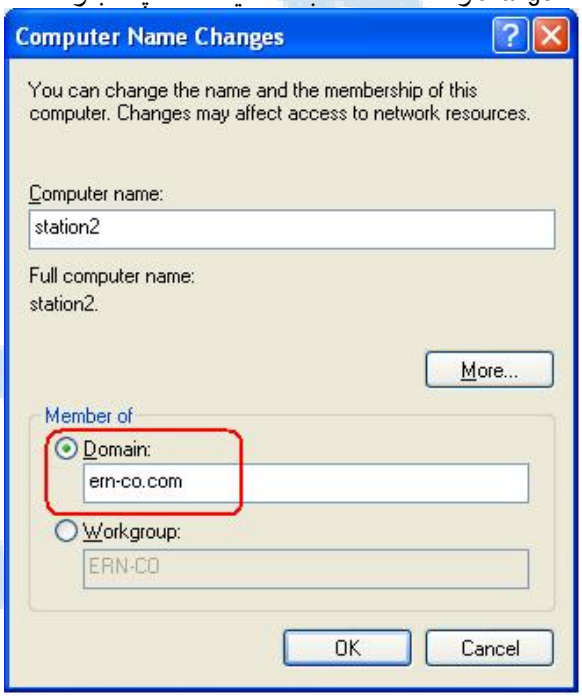
شکل ۳-۱۱

در control panel/system propertiesزبانه comuter nameرا انتخاب کنید (شکل ۳-۱۷)



شکل ۱۴-۱۱

در این پنجره مشاهده می کنید که این کامپیوتر عضو یک workgroup بانام ERN-CO می باشد حال گزینه change را انتخاب کنید تا پنجره شکل ۳-۱۸ ظاهر شود .



شکل ۱۵-۱۱

در این پنجره گزینه Domain را انتخاب کرده ودر مقابل آن اسم DNS ی Domain یعنی ern-co.com ویا اسم NetBIOS آن یعنی ERN-CO را واردکرده وسپس روی گزینه OK کلیک کنید
پنجره جدیدی مطابق شکل ۱۶-۱۱ ظاهر شده واسم و گذر واژه کاربری را که اجازه عضو کردن کلاینتها در Domain را دارد از ما می خواهد.

شکل ۱۶-۱۱

درقسمتuser name ,Administratorو درقسمت password گذر واژه آن کاربر را وارد کنید بعد از چند ثانیه پنجره زیر ظاهر شده و اعلام خوش آمد گویی به ern-co.comرا می دارد.

شکل ۱۷-۱۱

در پنجره های ظاهر شده روی okکلیک کرده و سپس گزینه yesرا انتخاب کنید تا کامپیوتر دو باره راه اندازي شود .
حال بعد از راهنداز دو باره شدنه در پنجره logon toیک لیست می باشد که اگر آن را باز کنید دو گزینه ملاحظه خواهیدکرد این دوگزینه اسم

Domainواسم وخود کامپیوتر می باشد.

شکل ۱۸-۱۱

۲-۳-۱۱ انواع log on

دراین قسمت ازانواعlog onکردن به ویندوز به دونوع اشاره کنید:

Log on locally :

اگر در لیست ظاهر شده در شکل ۳-۲۱ گزینه This computerراانتخاب کنید و بایک اسم و گذر واژه ی که در Domainایجاد شده (مثلاً کاربر Administrator) log onکنید عمل authenticationتوسط همان کامپیوتر انجام خواهدشد . اما دراین حالت کاربر فقط به منابع همان کامپیوتر دسترسی خواهد داشت.

Log on ti domain :

اگر درلیست مذکور گزینه ERN-COرا انتخاب کنید همانطوری که قبلاًهم توضیح داده شد ه مشخصات کاربر به DCفرستاده می شود authenticationتوسط آن انجام خواهد شد در این حالت کاربر می تواند به تمامی منابع Domain بدون نیاز مجدد به واردکردن اسم وگذر واژه پیداکند.

خود آزمایی و تحقیق

۱- Domain Controller چیست؟ وظایف و ویژگي هاي آن را شرح دهید.

۲- Forest چیست؟

۳- Child Domain را با ذکر مثال تعریف کنید؟

۴- انواع Log on را توضیح دهید و تفاوت اسامي آن را بنویسید.

۵- آیا یك کامپیوتر مي تواند به طور همزمان عضو چند DC باشد؟

۶- تحقیق کنید که چه روش دیگري براي نصب Active Directory وجود دارد؟

فصل دوازدهم مدیریت Acount ها

هدف های رفتاری

- انواع Account ها و ابزارهاي مديريتي را شناسايي كند.
- بتواند كاربران را مديريت كند.
- بتواند مديريت Computer Account ها را انجام دهد.

۱-۱۲ آشنایی با انواع Acountها و ابزارهای مدیریتی

۱-۱-۱۲ انواع Acountها

در Active Directory، Acountها به سه دسته تقسیم می شوند:
۱- user Accounts به ازای هر کاربر در Domain یک user Accountباید ایجادکنید ازاین نوع Accountها براي log on کردن به Domainو دسترسی به منابع آن استفاده می شود
۲-computer Account: به ازای هرکلاینتو یا سرور و هر DCکه عضو Domainهستند یک computer Accountوجوددارد و از آن ها براي اعمال کردن policyها authentication استفاده می شود
۳-Group Accounts: براي مديريت راحت كاربران واعطای مجوز به آنها و همچنین اعمال policyها به آنها از این نوع Accountها استفاده مي شود كه در فصل بعد مورد بررسی قرار خواهندگرفت.

۲-۱-۱۲- ابزارهای مدیریت Active Directory:

بعداز نصبActive Directory سه ابزار برای مدیریت آن در Administrative Toolsاضافه می شود:
۱- Active Directory users and computers: ازاین ابزار براي مديريت انواع Accountهای اشاره شده در قسمت قبل استفاده می شود
۲- Active Directory sites and services: ازاین ابزا براي مديريت siteهای Active Directory استفاده می شود این ابزار خارج از بحث این کتاب می باشد .
Active Directory Domain and Trusts: از این ابزار براي مديريت Domainها وایجاد رابطه های اعتماد (trusts) بین آنها استفاده می شود
این ابزار خارج ار موضوع این کتاب می باشد.
Starts/Administrative toolsروی گزینه Active Directory users and computerکلیک کنید پنجره شکل ۱-۱۰ ظاهر می شود.

شکل ۱-۱۲

گزینه ern-co.comرا بازکنید چندین پوشه درداخل آن نمایش داده می شوند تمامی کاربرانی که به صورت پیش فرض در Domain ایجاد می شوند داخل پوشه usersقراردارند به ازای تمامی کامپیوترهایی که عضو Domainمی شوند یک computer

Accountدر پوشه computersایجاد می شود بخشی از گروههایی که هنگام ایجاد Domainبوجود می آیند در پوشه Built-inقراردارند.

۱۲-۲ مدیریت کاربران

۱۲-۲-۱ ایجادکردن کاربران جدید

درActive Directory users and computerروی پوشه usersکلیک راست کرده و گزینه Newو سپس userرا انتخاب کنید .
پنجره شکل ۱۲-۲ ظاهر خواهد شد.

شکل ۱۲-۲

درقسمت Fairst name:نام کاربر را واردکنید (مثلاً Ali)
Last name: نام خانوادگی کاربر را واردکنید. (مثلاًRahmati)
Full name: نام کامل کاربر که از نام و نام خانوادگی کاربر تشکیل شده به صورت اتوماتیک نمایش داده خواهد شد . (Ali Rahmati)
Logon name : اسمی را که کاربر با آن به logon،Domain خواهد کرد واردکنید (مثلاًARahmati)
Pre-windows 2000 logon name :همان اسمی را که درقسمت Logon name واردکرده اید نمایش خواهدداد.
گزینه Nextراانتخاب کنید تا پنجره شکل ۱۲-۳ نمایش داده شود.

شکل ۱۲-۳

توجه کنید که اسمی که درقسمتLogon name واردمی کنید در Domainباید منحصر بفردباشد.
دراین پنجره گذر واژه کاربر جدید ازماسؤال می شود که دوباربایدآن راواردکنید.
نکته: یک policyبه صورت پیش فرض در Domainهای 2003وجوددارکه باعث می شود گذر واژه هایی را که برای کاربران انتخاب می کنید complexبوده وحداقل ۷کاراکتر طول داشته باشند بدین معنی که از گذر واژه های تکراری ویا گذر واژه هایی که فقط ازاعداد و یافقط از حروف تشکیل شده اند نمی توان استفاده نمود . بعنوان مثال شما می توانید از گذر واژه Passworrd استفاده نمائید
گزینه های بعدی گزینه هایی هستند که قبلاً در ایجاد کردن کاربران جدید درویندوز xpانها را فراگرفته اید حال گزینه Nextرا انتخاب کنیدتا پنجره شکل۴-۱۰ نمایش داده شود در این پنجره خلاصه مشخصات کاربرنمایش داده شده است .

شکل ۴-۱۲

حال روی گزینه finishکلیک کنید کاربرجدید ایجاد می شود توجه کنید که در پوشه usersاسم کامل کاربر یعنی full nameنمایش داده می شود.

۲-۲-۱۲-مشاهده مشخصات کاربران و تغییردادن آنها

اگر Active Directory users and computerروی یک کاربر کلیک راست کرده وگزینه propertiesرا انتخاب نمائید پنجره جدید مطابق شکل ۵-۱۲ ظاهر شده که دران مشخصات کامل آن کاربر رادیده و می توانید آنها را تغییردهید.

شکل ۵-۱۲

به عنوان مثال در این قسمت به چند مورداز مشخصات کاربران اشاره کنید.

زبانه Accountگزینه logon hours... :

اگر روی این گزینه کلیک کنید پنجره شکل۴-۶ نمایش داده خواهدشد در این پنجره به شما نشان میدهد که این کاربر در چه ساعاتی از شبانه روز در یک هفته اجازه logonکردن به Domainرادارد شما این محدودیت را به ازای هر ساعت در شبانه روز و هر روز در هفته می توانیدتعیین کنید

شکل ۶-۱۲

خانه هایی که به رنگ آبی پرشده اند بیانگر این می باشد که در آن ساعت و دران روز کاربر اجازه logonکردن دارد
شمابه راحتی می توانید با کلیک کردن روی یک خانه آن را به رنگ آبی و یا به رنگ سفید در آورید.

زبانه Accountگزینه logon to...

با کلیک کردن روی این گزینه پنجره شکل ۱۰-۷ نمایش داده می شود
در این پنجره تنظیمات پیش فرض طوری انجام شده که کاربر مربوط با کلیک کردن ار روی هرکامپیوتری به Domain، logonکند شمابا انتخاب گزینه The following

computerمی توانید برای کاربر محدودیت ایجاد کنید تا فقط از روی کامپیوترهایی که مدنظر شما می باشد بتوانندlogonکند برای انجام این کار در قسمت computer name اسامی کامپیوترها را یک به یک نوشته و بازدن گزینه Add انها را به لیست اضافه کنید

شکل ۷-۱۲

زبانه Accountگزینه Account expires :

به وسیله ی این گروه شما می توانید محدودیت زمانی برای فعال بودن کاربر تعریف نمائید تنظیم پیش فرض این گزینه روی neverمی باشد
بدین معنی که اعتبار این کاربر منقضی نخواهد شد شما می توانید با انتخاب گزینه :End of و انتخاب تاریخ از لیست و تقویم مقابل ، یک تاریخ انقضا برای کاربر انتخاب نمائید.

شکل ۸-۱۲

زبانه Member of

دراین زبانه به شما نشان می دهدکه کاربر عضو چه گروهایی می باشدشما با انتخاب گزینه Addمی توانید کاربررابه عضویت گروه های دیگری نیزدر آورید.

۱۲-۲-۳ کاربر organizational unit :

در هرسازمان براي مدیریت ساده تر و ساختار یافته از یک سری واحدهای سازمانی استفاده می شود بعنوان مثال استفاده از واحدهای مختلف نظیر کارگزینی ،اموراداری، حسابداری ، آموزش ، روابط عمومی ، IT .....در بسیاری از شرکت ها وسازمان ها معمول ومرسوم می باشد.
درهر واحدسازمانی تعدادی کارمندو مقداری منابع مثل کامپیوتر ، چاپگر و ... یک مدیربرای آن واحد و غیره وجود دارد . طوری که مدیریت آن واحد سازمان به مدیر در یک شبکه بزرگ نیز براي مدیریت راحت تر شبکه ، می توانید در یک Domain، واحدهای مختلف سازمانی ایجادنمائید که به آنها اصطلاحاً organizational unitمی گویند و به اختصار با نام ouبه آنها اشاره کنید.
هر ouمی تواند تعداد زیادی کاربر ، کامپیوتر ، پرینتروحتماً مدیر داشته باشد
حتما می توانید policyهای خاص برای آنها در نظربگیرید و در واقع یک Domainرابه تعدادی ouتقسیم کرده و منابع و کاربران رانیز بین آنها تقسیم نموده و حتی مدیریت آنها را نیز به کاربران خاص واگذار کنید
براي ایجاد یک ouجدید این عملیات را انجام می دهید :

ابتدا Active Directory users and computer را اجرا کنید سپس روی ern-co.com کلیک راست کرده وگزینه New وسپس organizational unit را انتخاب کنید (مطابق شکل ۹-۱۲)

شکل ۹-۱۲

در پنجره ای که ظاهر میشوددر قسمت Name نام ou جدید را وارد کنیدو سپس گزینه ok را کلیک کنید
مشاهده خواهید کرد که یک ou جدید ایجاد شده است حال دراین ou می توانید کاربران جدید ایجاد نمائید و یا کاربران و کامپیوترهای موجود را به داخل آن انتقال دهید براي ایجاد کاربران جدید در داخل ouv روی ou کلیک راست کرده و گزینه new و سپس user را انتخاب نمائید و کاربر را به همان صورتی که قبلاً اشاره شد ایجاد نمائید

۱۲-۲-۴ تکثیر کاربران

درقسمت قبل درارتباط با یک Domain بحث کردیم که شامل تعداد زیاد ou نیز می باشد فرض کنید کاربرانی که در این ou ها ایجاد می کنید بسته به واحد سازمانی مشخصاتی متفاوت ازهم داشته باشند بعنوان مثال کاربران یک واحد درروزهاو ساعات خاصي ازهفته بتوانند logon کنند یاتاریخ انقضا آنها اخر سال باشد یا عضو گروهای خاص باشند ازروی کامپیوترهای خاص بتوانند logon کنند و غیره... به طوریکه این مشخصات متفاوت از مشخصات واحدهای دیگر باشد
دراین حالت هرزمان که شمایک کاربر جدید برای این واحد ایجاد می کنید تمامی این تنظیمات را از نو برای آن کاربر باید انجام دهید وبایددقت کنید که اشتباهی صورت نگیرد حال اگرمشخصات کاربران واحدهای مختلف متفاوت باشند کاربرای شما سخت تر هم خواهدشد
راه حل بهتری که داریم این است که یک کاربر نمونه برای هر واحد ایجاد کنید برای هرکدام از آنها مشخصات را براساس نیاز آن واحد تعیین کنید و سپس آن کاربر را Disable مي کنید
حال برای کاربر جدیدی که میخواهید در آن واحدایجاد کنید کافی است که یک کپی از کاربر نمونه آن واحد ایجاد کنید دراین صورت مشخصات آن کاربر نمونه برای کاربر جدید نیز کپی خواهدشدمراحل زیر شیوه انجام این کار را بیان می کند

۱-یک ou به نام sales ایجادنمائید
۲- یک کاربر نمونه بانام -sales-temp ایجاد نمائید توجه کنید که این کاربر به دلایل امنیتی حتماً Disable شود.
۳- حال مشخصات کاربر را به صورت دلخواه تعیین کنید بعنوان مثال آن کاربر روزهای جمعه اجازه logon نداشته باشد تاریخ اعتبار تاسه ماه دیگر باشد به عضویت یکی دوگروه جدید درآید فقط از روی کامپیوتر های xp1,xp2 بتواند logon کند و گزینه password never expires درزبانه Account انتخاب شود.
۴- حال روی کاربر مربوطه کلیک راست کرده وگزینه copy را انتخاب نمائید پنجره شکل ۱۰-۱۲ ظاهر خواهدشد
دراین ویزارد مشخصات کاربر جدید را واردنمائید تا کاربر جدید ایجاد شود

شکل ۱۰-۱۲

۵- مشخصات کاربر جدید را بازبینی نمائید متوجه خواهید شد که تمامی مشخصاتی که برای کاربر sales-temp- واردکرده بودید برای کاربر جدید نیز اعمال شده اند.

۱۲-۳ مدیریت computer Accountها

۱۲-۳-۱ کاربرد computer Account

computer Accountها نیز مثل یک کاربریکی از objectهای Active Directory می باشد .
این Accountها برای سیستم های عامل زیر که عضو Domain می شوند وجود دارند:
۱- windows NT
۲- windows 2000
۳- windows xp
۴- windows 2003

به عبارت دیگر فقط برای سیستم های عاملی که تکنولوژی NTدارند Computer Accountدر Active Directoryایجاد می شود ازاین objectها براي authenticationواعمال کردن policyها در Domain استفاده می شود
که از آن جمله به مواردی چون اعمال بازبيني(auditing) نصب برنامه ها به صورت اتوماتیک روی کامپیوترها می توان نام برد
بدین معنی که کاربران اجازه logonکردن از روی کامپیوترهایی رادارند که برای آن کامپیوتر در Active،Directoryیک computer Accountوجود داشته باشد در صورت غیر فعال شدن یک computer Account هیچ کاربری اجازه logonازروی آن رانخواهد داشت البته بحث اعمال کردن policyها ونصب اتوماتیک برنامه ها خارج ازبحث کلاس می باشد.

۱۲-۳-۲- نحوه ایجاد computer Account

هر کامپیوتری که عضوDomainمیشود بصورت اتوماتیک برای آن کامپیوتر Acctive Directoryیک computer Account درپوشه computerدر داخل Domain ایجاد می شود برای DCها این objectها دریک ouبه نام Domain controllers ایجاد می شوند.

خود آزمایی و تحقیق

۱- انواع Account را نام ببرید.

۲- وظیفه ي Account expires چیست و رابطه آن را با Password never expires بنویسید.

۳- یک OU به عنوان Student ایجاد کرده که دارای ویژگی های زیر باشد .

الف- فقط روزهای زوج از ساعت ۱۰ الی۱۴ بتوانند Logon کنند.

ب- فقط روی ۳ عدد از کلاینت ها بتوانند Logon کنند.

ج- بتوانند چاپگر را مدیریت کنند.

د- بتوانند تنظیمات شبکه ، IP سیستم ها را عوض کنند.

ه- بتوانند از طریق Dial up به شبکه متصل شوند.

فصل سیزدهم مدیریت کاربران

هدف های رفتاری
انواع گروه هاي کاربران را شناسايي کند.
به روش هاي AGP و ADLP به کاربران و گروه ها مجوز دهد.
گروه هاي Built-in را شناسايي کند.

۱۳-۱ آشنایی با انواع گروه ها

در Dpmain های ۲۰۰۳ دو دسته بندی برای گروه ها وجود دارد :

- Group Types
- Group scops

Group Type بیانگر نوع گروه بوده و گروه ها از این نظر به دو نوع تقسیم می شوند :

۱- Security Groups
۲- Distribution Groups

گروه های از نوع Securityگروه هایی هستند که از آنها بیشتر برای مجودز دادن استفاده می شود . به عنوان مثال اگر بخواهید یک پوشه را برای یک گروه share کنید نوع گروه باید Security باشد .
گروه های ازنوع Distribution گروه هایی هستند که فقط به منظور e-mail مورد استفاده قرار می گیرند .

۱- Group scopes :

- Global
- Domain local
- Universal

گروه هایی که دراین کتاب مورد بحث می باشند همه از نوع Security می باشند . بنابراین در هر قسمتی که در آن از نوع گروه نام می برید ، منظورمانscops مربوط به آن گروه می باشد .
Group scopes بیانگر محدوده عمل کرد یک گروه وانواع object هایی است که می توانند به عضویت آن در آیند . همانطوری که اشاره شد دراین متن از واژه " نوع گروه " به جای Group scopes استفاده خواهید کرد .

۱۳-۲ Global groups

گروه هایGlobal گروه هایی هستند که به منظور دسته بندی منطقی کاربران مورد استفاده قرار می گیرند این دسته بندی معمولا براساس نوع کار یا محل جعرافیایی کاربرانی باشد . به عنوان مثال کاربرانی که در واحد فروش کار می کنند را می توانید در یک گروه دسته بندی کنید یا کاربرانی که در ساختمان شماره یک قرار دارند ، می توانند در یک گروه دسته بندی شوند . براي ایجاد یک گروه از نوع global بر روی Domain یا OU[1] ی مورد نظرکلیک سمت راست نموده و در منویی که ظاهرمی شود گزینه New و سپس groupرا انتخاب کنید. پنجره شکل ۵-۳ نمایش داده خواهد شد .

---

[1] OU برای ایجاد واحدهای مدیریتی داخلActive Directoryداخل Domain از اخل

شکل ۱-۱۳

در قسمت Group Type گزینه Security و در قسمت Group scopes گزینه Global را انتخاب کرده و یک اسم برای گروه انتخاب کنیدو سپس گزینه ok را کلیک کنید.
توجه: برای شناسایی راحت گروه ها در لیست هایی که نمایش داده می شوند توصیه می شود که برای اسم گروه ها از پیشوند G استفاده شود . بعنوان مثال بجای اسم sale توصیه می شود که از G sale استفاده شود.

۱۳-۲-۱ Domain Local Groups

از این گروه ها معمولا برای اعطای مجوز استفاده می شود . برای ایجاد این نوع گروه رویDomain یا OU مربوط کلیک راست کرده و از منوی ظاهر شده گزینه New و سپس گزینه Organization را انتخاب کنید. پنجره شکل ۵-۴ ظاهر می شود .

شکل ۲-۱۳

در این پنجره گزینه های Security وDomain Local را مطابق شکل انتخاب نموده و همچنین یک اسم برای گروه انتخاب کنیدو سپس روی کلید ok کلیک کنید.

۱۳-۲-۲ Univer sal Groups

از این نوع گروه ها برای مجوز دادن به کاربران در شبکه هایی که بیش از یک Domain دارند ، استفاده می شود .
استفاده از این گروه ها خارج از موضوع بحث در این کتاب می باشد .
۱۳-۳ روش های اعطای مجوز به کاربران
از روش های مختلفی براي اعطای مجوز به کاربران به کمک گروه ها می توان استفاده نمود در این جا به چند روش اشاره کنید.

۱۳-۳-۱ روش AGP

در این روش کاربران (Account) ها را در گروه های مختلف از نوع Global دسته بندی می شوند. همانطوری که قبلا هم بیان شد ، این دسته بندی از نظر نوع کار و محل جغرافیایی کاربران انجام می شود . سپس مجوز (permission) لازم به گروه ها اعطا می شود .

شکل ۱۳-۳

از این روش در شبکه هایی که تعداد object ها زیاد نیست می توان استفاده کرد.

۱۳-۳-۲ روش A DL P

در این روش کاربران (Account) ها را در گروه های مختلف از نوع Global دسته بندی کنید.
سپس گروه هایی از نوع Domain Local ایجاد کرده و به آنها مجور (Permission) لازم را اعطا کنید. حال تمامی گروه های Global که لازم است مجوزهای مربوط را داشته باشند ، به عضویت گروه های Domain Local در می آورید.

شکل ۱۳-۵

از این روش در شبکه هایی که تعداد object های زیادی دارند و یا شبکه هایی که از چندین Domain تشکیل شده اند .استفاده می شود.

۱۳-۴ آشنایی با گروه های Built-in

گروه هایBuilt-in گروه هایی هستند که زمان نصب Active Directory به صورت اتوماتیک ایجادمی شوند . این گروه ها را در ابزار Active Directory Users & Computer در پوشه های Built-in و Users می توان مشاهده نمود.

۱۳-۴-۱ گروه های Built –in Global

این گروه ها در پوشه users در ابزار Active Directory Users & Computer قرار دارند و عبارتند از:

۱. Domain users: این گروه شامل تمامی کاربران Domain می شود .هر کاربری که در Domain ایجاد می شود ، به صورت اتو ماتیک به عضویت این گروه در می آید .
۲. Domain Admins : اعضای این گروه می توانندDomain را مدیریت کنندوبه عنوان مدیر Domain شناخته می شوند . فقط Admini strator همان Domain به صورت پیش فرض عضو این گروه می باشد .
۳. Enterprise Admins: اعضای این گروه می توانند Forest را مدیریت کنند . یعنی توان مدیریت در تمامی Domain های Forest را خواهند داشت .

بصورت پیش فرض Administrators اولین Domain عضو این گروه می باشد . این گروه به صورت پیش فرض از نوع Global می باشد . اما اگر سطح کارکرد Domain را به Native 2000 یا به Server 2003 تغییر دهید ، این گروه به صورت اتو ماتیک به نوع Universal تبدیل خواهد شد .

شکل ۱۳-۶

۱۳-۴-۲ گروه های Built-in Domain Local

شکل ۱۳-۷

این گروه هادر پوشه Built-in در ابزار Active Directory Users & Compute قراردارند .

عبارتنداز :

Administrators : اعضای این گروه می توانند DC ها را مدیریت کنند و تمامی مجوزها روی این کامپیوترها خواهند داشت .

Server operatars: اعضای این گروه می توانند در انجام بعضی از کارهای مدیریتی به مدیر شبکه کمک کنند بعنوان مثال می توانندعملیات زیر را روی DC ها انجام دهند .

- Log on کردن
- Shut down کردن
- فرمت کردن درایوها
- تغییر ساعت

- Account operators: اعضای این گروه می توانند عملیات مدیریتی همچون ایجاد ، حذف و ... را روی Accountها (شامل :کاربران ، گره ها و کامپیوتر) انجام دهند . به عنوان مثال اعضای این گروه می توانند یک کاربر و یک گروه ایجاد کرده و آن کاربر را به عضویت آن گروه در آورند.
- Print operators: اعضای این گروه می توانند چاپگرهای Domain را مدیریت نمایند.
- Backup operators : اعضای این گروه می توانندعملیات Backup گرفتن از اطلاعات و برگرداندن اطلاعات (Restore کردن) را انجام دهند.
- Network configuration operators: اعضای این گروه می توانند تنظیمات شبکه را تغییر دهند . به عنوان مثال این اعضا می توانند آدرس IP را روی کارت شبکه DC تغییر دهند.

۱۳-۴-۳ گروه های Buit-in system

این گروه ها ،گروه هایی هستند که لیست اعضای آن ها را نمی توان دید و یا تغییرداد . اما می توانید از آنها برای انجام کارهای مدیریتی استفاده کنید ، به عنوان مثال می توانید به این گروه ها مجوز اعطا کنید . این گروه ها عبارتند از:

- Every one: این گروه شامل تمامی کاربرانی می شود که به یک کامپیوتر متصل می باشند (تمامی کاربران شناخته شده و یا ناشناخته)
- Authenticated users: تمامی کاربران که عمل authentication برای آن ها اتفاق می افتد یا به عبارت دیگر دارایaccount می باشند.

- Anonymous Logon: این گروه شامل کاربرانی است که به صورت ناشناس به یک کامپیوتر متصل می شوند.
- Dialup: این گروه شامل کاربرانی است که از طریق Dialup به کامپیوتر متصل می شوند.
- Network: شامل کاربرانی است که از طریق شبکه به یک کامپیوتر متصل می شوند.

زمانی که به کاربران مجوز اعطا کنیددر لیستی که نمایش داده می شود ،می توانید لیست گروه های سیستمی را مشاهده کنید.

۱۳-۵ پیاده سازی روش های مختلف اعطای مجوز به کاربران

۱۳-۵-۱ پیاده سازی روش AGP

در این روش ابتدا یک گروه از نوع Global به همان شیوه ای که در مراحل قبل یاد گرفتید بانام G sale ایجاد کنید .
سپس مطابق شکل ۱۳-۸ از این گروه Properties گرفته و در زبانه Members لیست اعضای این گروه را مشاهده می کنید.

شکل ۱۳-۸

حال اگر کلید Add کلیک کنید پنجره شکل ۱۳-۹ نمایش داده خواهد شد . در این پنجره می توانیداسامی کاربران را تایپ کرده و به لیست اضافه نمائید و یابراي انتخاب کاربران از لیست روی کلید Advanced کلیک کرده و سپس روی گزینه Find Nam کلیک نمائید تا لیستی از کاربران و گروه ها نمایش داده شوند.

شکل ۱۳-۹

حال کاربران مورد نظر را به کمک کلیدهای Ctrlو یا Shift انتخاب کرده و به لیست اضافه نمائید.
مشاهده خواهید کرد که این کاربران در زبانه Members لیست شده اند . روی گزینه ok کلیک کنید.
حال در هر جایی که منابع قرار دارند به این گروه مجوز می دهید . به عنوان مثال فرض کنید که یک پوشه به اشتراک گذاشته شده بانه Sale Data وجود دارد . روی این پوشه کلیک راست کرده و زبانه Sharing and security را انتخاب کنید، در پنجره ظاهر شده روی Permissions کلیک کنید تا پنجره شکل ۵-۱۰ ظاهرشود.

شکل ۱۳-۱۰

در این پنجره گروه Everyone را حذف کرده و سپس گروه G sale را به لیست اضافه کرده و مجوزهای لازم را به آن انتساب دهید.

۱۳-۵-۲ پیاده سازی روش A DL P

این روش مشابه روش قبلی می باشد با این تفاوت که گروه رابانام DL Sale ایجاد کرده و نوع آن را Domain Local انتخاب کنید . بقیه مراحل مشابه مثال قبل می باشد .

پیاده سازی روش A G DL P

در این روش ابتدا یک دسته بندی منطقی برای کاربران در نظر گرفته و سپس گروه های ازنوع Globalرا ایجاد کنید و کاربران را براساس آن دسته بندی به عضویت گروه های مختلف در آورید . سپس یک گروه ازنوع Domain Local ایجاد نمائید و مجوزهای لازم روی منبع مورد نظر را به آن اعطا نمائید . به عنوان مثال یک گروه بانام DL HP B20 Users از نوع Domain Local ایجاد نمود و مجوز Print را روی یک چاپگر به اشتراک گذاشته شده به آن اعطا کنید .

شکل ۱۳-۱۱

حال تمامی گروه های از نوع Global را که قرار است مجوز Print روی این چاپگر داشته باشند، به عضویت گروه DL HP B20 Users در آورید.

شکل ۱۳-۱۲

خود آزمایی و تحقیق

۱- تفاوت Scaring Group و Distribution Group در چیست؟

۲- تفاوت روش AGP و ADLP را بنویسید.

۳- چطور مي توان در يك سطح وزارتخانه براي كاربران مجوزهاي لازم را صادر كرد؟

۴- اگر بخواهیم برای یک مدرسه، شبکه ای ایجاد کنیم که شامل کلیه دانش آموزان و معلمان و مدیران باشند از کدام روش باید برای اعطای مجوز به کاربران استفاده کنیم؟ توضیح دهید.

فصل چهاردهم – DNSو روش هاي تبديل اسم به IP

هدف های رفتاری

کاربردهای DNS را بیان کند.

اسامي اينترنتي و Host Name را شناسايي كند.

اجزاء DNS را توضیح دهد.

مراحل تبديل اسم به IP را در اينترنت شرح دهد.

يك سرويس DNS نصب و راه اندازي كند.

سرويس DNS را براي انجام عمل Name Resolution تست كند.

۱۴-۱ کاربردهای DNS

DNS یکی از سرویس های بسیار مهم در شبکه می باشد . از این سرویس در اینترنت بیشتربه منظور تبدیل اسم به IP استفاده می شود .در Domainهای ۲۰۰۳ نیز از این سرویس براي تبدیل اسم به IP استفاده می شود . یکی از کاربردهای دیگر این سرویس معرفی سرویس دهنده های مختلف در شبکه می باشد . به عنوان مثال یک کلاینت که عضو Domain می باشد .DC ها را به کمک DNS پیدا می کند و DNS لیستی از DC های Domain را به کلاینت ها معرفی می کند . تنظیمات DNS برای کارآیی و پایداری Domain بسیار حائز اهمیت می باشد ، به همین دلیل از DNS به عنوان نبض Domain های ۲۰۰۰و ۲۰۰۳ می توان یاد کرد .

۱۴-۲ آشنایی با اسامی اینترنتی

۱۴-۲-۱ Host Name

اسامی اینترنتی ، اسامی هستند که از چند قسمت تشکیل شده اند. این قسمت ها با نقطه (.) از قسمت های دیگر جدا می شوند . به عنوان مثال www.ern.co.com از سه قسمت تشکیل شده است که با نقطه از همدیگرجداشده است . به اسامی اینترنتی به اصطلاح FQDN (Fully Qualified Domain Name) گفته می شود . یک FQDN از دوقسمت تشکیل می شود . همانطوری که در شکل ۱۴-۱ مشاهده می کنید به قسمت سمت چپ Host Name و به قسمت سمت راست Domain Name یا DNS Sffix اطلاق می شود

شکل ۱۴-۱ www.ern.co.com

Host name Domain name

در بسیاری از حالت هاه به جایFQDN از واژه Host name استفاده می شود.

۱۴-۲-۱ ساختار اسامی اینترنتی

به منظور تبدیل راحت اسم به IP ، اسامی اینترنتی از چند قسمت تشکیل می شوند و براي نام گذاری کامپیوترها ازیک ساختار سلسله مراتبی استفاده می شود . این ساختار سلسله مراتبی که یک ساختار درختی می باشد . شکل ۱۴-۲ نمایی از این ساختار درختی را نشان می دهد.

شکل۲-۱۴

همانطوری که در شکل مشاهده می کنید ، تمامی اسامی اینترنتی به یک نقطه ختم می شوند . البته لازم به توضیح است که کاربران اینترنتی معمولا این نقطه را در انتهای اسامی اینترنتی وارد نمی کنند و این نقطه را به صورت اتوماتیک به اسامی اضافه می شود .
این قسمت از اسامی اینترنتی با نام Root Level شناخته می شود پس می توان نتیجه گرفت که آخرین نقطه در اسامی اینترنتی بخشی از آن اسم نیز می باشد (برخلاف سایر نقطه ها که به عنوان جداکننده مورد استفاده قرار می گیرند) .
قسمت دوم از سمت راست این اسامی معمولا اسامی دویا سه کاراکتری هستند که بیانگر نوع فعالیت Domainو یا محل جغرافیایی آن Domain می باشد .
به عنوان مثال .com بیانگر فعالیت های تجارتی ، ir بیانگر کشور ایران ،.edu بیانگر فعالیت های آموزشی ، .ca بیانگر کشور کانادا و ... می باشند .
به اسامی مربوط به این سطح اسامی Top level گفته می شود .
قسمت بعد در اسامی اینترنتی مربوط به اسامی شرکتها واشخاص و... می باشد . این اسامی به وسیله ی اشخاص و یا شرکت ها اجاره می شوند . به عنوان مثال Microsoft، ern-co اسامی مربوط به این سطح می باشد که به آن ها اسامی secondary گفته می شود .
نظارت براسامی اینترنتی و تشخیص آن ها به عهده شرکت Internic می باشد .
ایجاد subdomain ها به شرکت های مربوط واگذار می شود . به عنوان مثال در داخل Microsoft (شکل۲-۱۴) یک subdomain به نام Training ایجاد شده است . ایجاد ونگهداری این subdomain به عهده شرکت مایکروسافت می باشد .
اسامی hostها یا subdomain ها از پائین ساختار درختی شروع شده و به ریشه ختم می گردد .
به عنوان مثال در شکل۲-۱۴ یک host با نام www وجود دارد که FQDNآن www.ern.co.com می باشد . یا یک host دیگری به نام web server1 وجوددارد که FQDN آن webserver1.Training.Microsoft.com. می باشد .شکل ۳-۱۴ قسمت مختلف این اسم را تشریح می کند .

شکل۳-۱۴

۱۴-۳ اجزاء DNS

۱۴-۳-۱ Name server

به DNS سرور ، Name server نیز اطلاق می شود و یک سرور ۲۰۰۳ است که سرویس DNS روی آن نصب گردیده است .

۱۴-۲-۲ Zone

یک DNS سروراطلاعات مربوط به Domainهای مختلف را می تواند نگهداری کرده وبه کاربران در ارتباط با آنها سرویس دهد. برای نگهداری اطلاعات Domainدر DNS از Zone استفاده می شود. به عبارت دیگر بانک اطلاعاتی DNS سرور همان Zone می باشد.
در شکل ۱۴-۲ به هرکدام از گزینه های Secondary level مثل Microsoft یک Domain گفته می شود. زمانی که این Domain ها را در DNS می خواهیم پیاده سازی کنید آنها را با Zone ایجاد خواهید کرد . بنابر این در شکل و نمودارها از واژه Domain و در عمل از Zone استفاده می شود.
Zone ها به دو دسته کلی تقسیم می شوند.

۱. Forward Lookup Zones: Zon هایی هستند که برای تبدیل اسم IP مورد استفاده قرار می گیرند.
۲. Revers Lookup Zones: Zon هایی هستند که برای تبدیلIP به اسم از آنها استفاده کنید.

۱۴-۳-۳ Resource Records

در یک Zone اطلاعات مربوط به یک Domain نگهداری می شود . این اطلاعات به صورت رکورد ثبت و نگهداری می شوند . به عنوان مثال اسم و IP یک host در یک رکورد از نوع host نگهداری می شوند . رکورد از نوع hostبیشترین استفاده را در DNS دارا می باشدولی از انواع رکوردها در یک Zone می توان استفاده نمودکه تعدادی از این نوع رکوردها عبارتند از:

- Host Record : از این رکورد به منظور تبدیل اسم به IP استفاده می شود.
- Point Record:ازاین رکورد به منظور تبدیل IP به اسم استفاده می شود.
- SRV Record: از این رکورد به منظور معرفی سرورهایی که سرویس های خاص را ارائه می کنند ، استفاده می شود.
- NS Record : ازاین رکورد براي معرفی Name server (DNS)
- SOA Record: از این رکورد براي معرفی اطلاعاتی در ارتباط با یکZone استفاده می شود.
- Alias Record: از این رکورد براي استفاده از اسم مستعار بجای FQDN کاربرد دارد .

۱۴-۴ – مراحل تبدیل اسم به IP در اینترنت

در شکل ۱۴-۴ با ساختار اسامی اینترنتی آشنا شدید . حال میخواهیم مراحل تبدیل اسم به IP را توضیح دهیم.
فرض کنید که یک کاربری در Internet Explerer آدرس www.microsoft.com را وارد می کند تا به سایت وب مایکروسافت متصل شود . همانطوری که می دانیدبرای اتصال به یک سرور باید IP آن سرور را داشته باشید . می خواهید مراحلی را که اتفاق می افتد تا کلاینت بتواند IP آن سرور را پیدا کند ، تشریح کنید .
شکل ۱۴-۴ این مراحل را نشان می دهد .

شکل ۱۴-۴ مراحل تبدیل اسم به IP

قبل از توضیح مراحل سرور های مورد استفاده در این شکل را تعریف کنید

Root Name server: این سرورها همانند ساختار Root Domain (ریشه) را نگهداری می کند .

آدرس های IP مربوط به Top Level Name servers به وسیله ی این سرورها نگهداری می شود .۱۳ سروراز این نوع سرورها در اینترنت به کاربران اینترنتی سرویس دهی می کنند .

این تعداد ثابت بوده و IP آن ها در DNS سرورجدیدی که راه اندازی کنیدبه صورت پیش فرض وجود دارد .

Top Level Name servers: این سرورها ساختار Domain های Secondare Level را نگهداری می کند.

به عنوان مثالCom Name server ساختار Com Domain رانگهداری می کند.

Secondarey Level Name server: این سرورها رکوردهای مربوط به Domain های خود را نگهداری می کنند . راه اندازی و نگهداری از هرکدام از این سرورها به شرکت ها و یا افرادی که اسم مربوط راثبت نموده اند واگذار می شود . به عنوان مثال IP سروری با نام www در Microsoft Domain را از Microsoft Name server می توانید سوال کنید.

مرحله ۱: در این مرحله کلاینت در خواست خود برای تبدیل webserver1.training.microsoft.com به IP آن سرور را به Local Nme server (DNS سرورISP) ارسال می کند. این سرورموظف است که IP مربوط به اسم درخواست شده را پیدا کرده و آن رابه کلاینت ارسال کنند ، در غیر این صورت جواب منفی کلاینت ارسال خواهد کرد.

مرحله ۲ : سرور Local در بانک اطلاعاتی خود آن اسم را جستجو می کند ولی با توجه به اینکه مسئولیت آن Zoneبا این سرور نیست ، هیچ رکوردی پیدا نمی کند و به همین دلیل آن ا سم را به Root Nam Server ارسال می کند و از آن سرورIP آن اسم را تقاضا می کند.

مرحله۳: Root Name server: IP اسم درخواست شده را نمی داند اما آن اسم را بررسی کرده و متوجه می شود که قبل از آخرین نقطه ،کلمه Com قرار گرفته است (همانطوری که قبلا بیان شده است این نقطه به صورت اتوماتیک به انتهای هراسمی اضافه می شود) . بنابراین لیستی از Com Name server را تهیه کرده و آن را به Local Name server ارسال می کند. این پاسخ بدنی معنی است که Local Name server سوال خود را باید از یکی از Come Name server ها پس گیری نماید.

مرحله ۴: تا این مرحله Local Name server توانسته است Com Name server IP را پیدا کند . بنابراین یک درخواست به آن سرور ارسال کرده و IP را از آن در خواست می کند .

مرحله ۵: این سرور نیز IP اسم در خواست شده را نمی داند ، اما با بررسی آن اسم ، متوجه کلمه Microsoft قبل از کلمه com می شود. سپس لیستی ازIP ی DNS سرورهای مایکروسافت را تهیه و آن را به سرور Local ارسال می کند . این پاسخ بدین معنی است که آن اسم از DNS سرور مایکروسافت باید پرسیده شود.

مرحله ۶: تا این مرحله سرور Local توانسته است IPی DNS سرور مایکرو سافت را پیداکند . بنابراین درخواست خود را به آن سرور ارسال می کند.

مرحله ۷: با توجه به این که مسئولیت Zone مربوط به Microsoft.com به عهده این سرور می باشد ، رکورد webserver1.training subdomain را در Zone پیدا کرده و IP آن را به DNS سرورLocal ارسا ل می کند .

مرحله ۸: حال سرور Local توانسته است IP درخواست شده به وسیله ی کلاینت را پیدانماید.

بنابراین آن را در حافظه DNS Cache خود کپی کرده و نتیجه را به کلاینت ارسال می کند . کپی کردن آن اسم و IP در Cache باعث می شود که اگر کلاینت دیگری همان سوال را از سرور Local بپرسد ، DNS دیگر این مراحل را طی نکرده و از حافظه Cache خود IP را به کلاینت ارسال کند.

مرحله ۹: حال که کلاینت توانسته است IP مربوط Web server1.traning.micro soft.com را پیدا کند ، در خواست خود را برای گرفتن سرویس وب به IP ارسال می کند.

مرحله ۱۰: webserver1 نیز در خواست کلاینت را دریافت کرده واطلاعات درخواست شده کلاینت را برای او ارسال می کند.

۱۴-۵- نصب و راه اندازی سرویسDNS

۱۴-۵-۱ نصب سرویس DNS

زمانی که Active Directory را روی اولین سرور(DC) نصب کنید، سرویس DNS نیز به صورت اتوماتیک نصب می شود . اما همانطوری که قبلا هم بیان شد ، این سرویس فقط مخصوص Domainنیست و روی سرورهای Stand alone نیز می توانید آن را نصب کنید.

براي نصب این سرویس از

Start/Contr Panel/Add or Remove Program/Add/ Remove windows components/Networking services

گزینه Domain Name system را تیک زده و گزینه ok و سپس روی کلید Next کلیک کنید . بعد از مدت کوتاهی CD ویندوز سرور ۲۰۰۳ را از شما خواهد خواست .CD را درداخل درایو قرار داده و پوشه I386 را به آن معرفی کنید .

فایل های لازم کپی شده و ویزارد به پایان خواهد رسید.

شکل ۱۴-۵

شکل ۱۴-۶

به این ترتیب سروری که دارید به یک DNS سرور تبدیل شده است و می تواند به کلاینت ها براي اتصال به اینترنت سرویس دهی کند . این سرور به صورت پیش فرض تعداد۱۳ Root Name server موجود در اینترنت را می شناسد

به منظور دیدن IP این سرورها از Start/Administrative Tools گزینه DNS را انتخاب کنید.

شکل۷-۱۴

کنسول DNS مطابق شکل ۸-۱۴ ظاهر خواهد شد . روی سرور(در این مثال فرض شده اسم سرور Training می باشد)کلیک راست کرده و گزینه Properties را انتخاب نمائید.

شکل ۸-۱۴

زبانه Root hintsرا انتخاب نمائید. مشاهده می کنید که اسمی و IP های Root Name server های اینترنتی نمایش داده می شوند.

۱۴-۵-۲ ایجاد کردن Zone

حال فرض کنیدکه یک Domain با نام ern-co.net دارید ویک Zone به همین نام می خواهید راه اندازی کنید .
برای انجام این کار مطابق شکل ۹-۱۳ روی گزینه Forward Lookup Zone در کنسول DNS کلیک راست کرده و از منویی که ظاهر می شود گزینه New Zone را انتخاب کنید.

شکل ۹-۱۴

شکل ۱۰-۱۴

مطابق شکل ۱۰-۱۴ یک ویزارد برای ایجاد Zone ظاهر خواهد شد . گزینه Next را انتخاب کنید.

پنجره شکل۱۱-۱۴ به نمایش در خواهد آمد . در این پنجره نوع Zone از ما سوال می شود . گزینه Primary Zone را انتخاب کرده گزینه ...store the zone را از حالت انتخاب خارج کنید سپس روی Next کلیک کنید .

توجه: توضیح انواع Zone ها خارج از بحث این کتاب می باشد.

در صفحه بعد اسم Zone از شما سوال می شود . ern-co.net را در قسمت Zone Name وارد کنید و روی گزینه Next کلیک کنید.

شکل ۱۲-۱۴

پنجره شکل ۱۳-۱۴ ظاهر خواهدشد .در این پنجره اسم فایل Zone از شما سوال می شود . به صورت پیش فرض برای این فایل اسم ern-co.net.dns پیشنهاد شده است .

شکل ۱۳-۱۴

اسم پیش فرض راقبول کرده و روی گزینه Next کلیک کنید.
پنجره شکل ۱۴-۱۴ ظاهر می شود . در این پنجره گزینه پیش فرض را قبول کرده و روی گزینه Next کلیک کنید.

شکل ۱۴-۱۴

در این پنجره خلاصه مشخصات Zone را که وارد کردید نمایش می دهد . روی گزینه Finish کلیک کنید . ملاحظه خواهید کرد که یک Zone به نام ern-co.net ایجاد شده است .

۱۴-۵-۳ ایجاد Resource Records

روی Zone ی که در مرحله قبل ایجاد کردیدکلیک کنید. همانطوری که مشاهده می کنید دو رکورد از نوع های SOA و NS به صورت پیش فرض ایجاد شده اند . روی Zone کلیک راست کرده و از منویی که ظاهر می شود گزینه New Host را انتخاب کنید .
پنجره اي مطابق شکل ۱۵-۱۴ نمایش داده می شود.

شکل۱۵-۱۴

در این پنجره در قسمت Name، WWW و در قسمت IP Address، IP یکی از سرورهای شبکه یا همین سرور را واردکنید . روی گزینه Add Host کلیک کنید . همانطوری که در شکل ۱۶-۱۰ مشاهده می کنید یک رکورد از نوع Host در Zone ایجاد شده است .

شکل ۱۶-۱۴

۱۶-۵-۴ تست کردن DNS برای انجام عمل Name Resolution

رکوردی که در مرحله قبل ایجاد کردید به منظور تبدیل اسم به IP (Name Resolution) مورد استفاده قرار می گیرد.
حال می خواهید یک Query به DNS سرور ارسال کنید و IP یک host با نام www.ern-co.next را سوال کنیم . برای انجام این کار از دو روش می توان استفاده کرد .
روش اول: استفاده از فرمان Ping
در هر کامپیوتری که IPی DNS آن بهIP ی DNS سرورجاری (یعنی training) تنظیم شده باشد،فرمان www.ern-co.next ping را اجرا کنید .
مطابق شکل ۱۷-۱۴ مشاهده خواهید کرد که IP آن host توسطDNS سرور پیداشده و به کامپیوترشما برگردانده می شود.

شکل ۱۷-۱۴

روش دوم : استفاده از فرمان nslookup

در این روش از فرمان nslookup برای تست کردنDNS سرور استفاده کنید. برای انجام این کار در Start/Run فرمان cmd را تایپ کرده و آن را اجرا کنید تا پنجره command prompt ظاهر شود.
فرمانnslookup را اجرا کنید . همانطوری که مشاهده می کنید اعلان فرمان به<تغییر یافته است . در این قسمت هر اسمی را که وارد کنید به DNS سرور پیش فرض فرستاده می شود و IP آن اسم درخواست می شود. درصورتی که DNS جواب را پیدا کند ، آن را مشاهده خواهید کرد.
شکل ۱۸-۱۴ شیوه استفاده از این فرمان را نشان می دهد.

شکل ۱۸-۱۴

خود آزمایی و تحقیق

فصل پانزدهم- مقدماتي DHCP Server

هدف های رفتاری

فواید DHCP Server را بیان کند
اجزاي DHCP توضیح دهد
حالت هاي مختلف قرارگيري DHCP Server در شبکه را شرح دهد.
نصب DHCP Server را انجام دهد
پيکربندي DHCP Server شرح دهد
پيکربندي DHCP Server را انجام دهد.
Backup / Restore از اطلاعات DHCP Server نسخه پشتيبان گرفته و جايگزين نمايد
عيب‌يابي DHCP را انجام دهد.

۱۵-۱. کاربرد DHCP Server

برای آنکه بتوان از یک TCP/IP Host در شبکه استفاده کرد باید حداقل موارد زیررا روی آن بطور مناسب تعریف کرد .

IP Address
Subnet Mask

اگر Host با شبکه های دیگر نیز در ارتباط باشد (مثلا اینترنت) لازم است تا پارامترهای دیگری را نیز روی آن تعریف کنیم :

-Router (Default Gateway)
-DNS Server IP Address

در عمل ممکن است حالات دیگری نیز پیش آید که در آن باید پارامترهای بیشتری رابرای یک Host تعریف کرد مانند WINS Server و Node Type

مي توان گفت پيکربندی یک Host در پروتکلTCP/IP چنانچه شبکه به اندازه کافي بزرگ باشد امری پیچیده و دقیق است و نیاز به یک مدیریت متمرکز دارد در پاسخ به این نیاز است که DHCP Server بوجود آمده است .DHCP[1] پروتکلی است که پیکربندی یک Host را به طور خودکار انجام می دهد و مدیر شبکه یا کاربران را از پیکربندی دستی (Static Manual) بی نیاز می کند بنابراین می توان فایده DHCP را به صورت زیر فهرست کرد :

۱) پرهیز از تداخل پیکربندی (IP Conflict) و اعمال سلیقه های شخصی
۲) سادگی و تمرکز در مدیریت Host Configuration

البته استفاده از DHCP مشکلاتی رانیز ایجاد می کند از جمله اینکه Client ها در هنگام فرایند راه اندازی باید با سرورDHCP ارتباط گرفته و پیکربندی مناسب را از آن دریافت کنند که این مسئله از طرفی باعث افزایش ترافیک شبکه شده و ازطرف دیگر در صورت نبودن سرور DHCP یاتاخیر در پاسخ از جانب آن سبب می شود تا ایستگاه ها نتوانند پیکربندی لازم خود را برای ارتباط در شبکه دریافت کنند .

۱۵-۲. اجزای DHCP

DHCP از دوقسمت تشکیل شده :

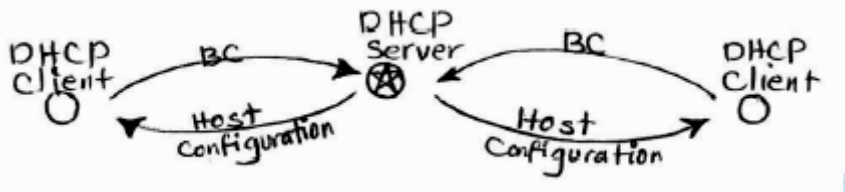
-DHCP Client
- DHCP Server

منظور از DHCP Client ، سرویسی است که درطی فرایند راه اندازی ، با سرورDHCP ارتباط گرفته و پیکربندی لازم را از آن در یافت می کند . بدیهی است که این سرور باید روی کلیه ایستگاه هایی که پیکربندی آنها می خواهد به طور خودکار (Automatic Dynamic) انجام شود ، فعال شود .

---

[1] Dynamic Host Configuration Protocol

درسیستم عامل ویندوز نسخه ها 2000XP و 2003 با مراجعه به کنسول سرویس ها (Server.msc) می توان فعال بودن این سرویس را بررسی کرد . وضعیت سرویس باید در حالت Started باشد.



شکل ۱-۱۵

همانطور که از شکل ۱-۱۵ پیدا است ، DHCP Client پس از فعال شدن روی ایستگاه ها با استفاده از Broad cast (به اختصارBC) سرور را پیداکرده و بعد از طی مراحلی کوتاه ، پیکربندی لازم را از سرور دریافت می کند.

حال چنانچه DHCP Server در شبکه نباشد یا در زمان مناسب به دلایلی مانند ترافیک شبکه نتواند پاسخ لازم را به ایستگاه بدهد در آنصورت بسته به رفتار سیستم عامل ایستگاه ممکن است یکی از حالات زیر اتفاق افتد :

الف) Client پیکربندی نمی شود. در مایکروسافت سیستم عاملهای win95 و NT4.0 چنین رفتاری دارند که با مراجعه به Command prompt و وارد کردن دستور ipconfig یا winipcfg می بینیم که آدرس به صورت 0.0.0.0 است و این موضوع یعنی نشان می دهد آدرس در Client پیکربندی نشده است .

ب) Client بطور خودکار و تصادفی یک آدرس به خود می دهد . سیستم عاملهای win98، Me ، xp2000و 2003چنین رفتاری دارند که با مراجعه به Command Prompt و واردکردن دستورipconfig یا winIPcfg می بینیم که آدرس تصادفی در محدوده 169.254.x.y با subnet Mask کلاس B یعنی 255.255.0.0 روی آن تنظیم شده . این مکانیزم تخصیص آدرس به طور تصادفی اصطلاحا APIPA[1] خوانده می شود .

متاسفانه APIPA مکانیزم مناسبی برای پیکربندی در شبکه ها نیست چرا که :

- غیر از IP&Mask پارامتر دیگری را تنظیم نمی کند (ازقبیل Router یا DNS)
- ترافیک شبکه را افزایش می دهد (می خواهد چک کند که آیاد آدرس تکراری است یا خیر)
- غیر از 169.254.X.Y محدوده دیگری را نمی توان روی آن تنظیم کرد .

به عبارت دیگر APIPA قابل تنظیم نیست.

ج- Client بطور خودکار با آدرس از پیش تعریف شده تنظیم شود . در سیستم عامل ویندوز نسخه های xp و 2003 چنین قابلیتی است که اگر سرور DHCP را پیدا نکنند با آدرس و سایر پارامترهای دیگری که ازقبل تعریف شده است خود را تنظیم می کنند.این حالت اصطلاحا"Alternate configuration" خوانده می شود .

نکته: در فرایند APIPA پس از آنکه Client آدرس را به صورت تصادفی برای خودانتخاب کرد آن را تا مدتی کوتاه (حدود ۵ دقیقه) نگه داشته و سپس مجددا به دنبال سرور DHCP می گردد که البته این جستجو با Broadcast انجام می شود . حال اگر بتواند از آن جواب بگیرد در آن صورت پیکربندی خود را از طبق دستورالعمل سرور انجام می دهد و درغیر این صورت یعنی نگرفتن پاسخ از سرور DHCP همان آدرس تصادفی قبلی را استفاده می کند و

[1] Automatic Private IP Addressing

این فرایند مرتب تکرار می شود یعنی حدودا هر ۵ دقیقه یکبار ایستگاه به دنبال سرور است آن هم با Broadcast و این افزایش ترافیک بیش از حد در شبکه های متوسط و بزرگ .

۳-۱۵- حالت های مختلف قرار گیری DHCP Server در شبکه

به طور کلی این حالت ها به ۲ دسته ساده و پیشرفته تقسیم می شوند . در این مبحث فقط حالت ساده قرارگیری سرور DHCP رادر شبکه (ها) بررسی می کنیم.

حالت اول ، هر شبکه یک سرور DHCP مستقل دارد :

شکل ۲-۱۵

مزیت این حالت در آن است که چون هر شبکه دارای سرور DHCP جداگانه ای برای خود است در صورت بروز اختلال در یکی از سرورها ، شبکه دچاراختلال نمی شود.

عیب ای سناریو در آن است که شاید تهیه سرور مستقل برای هرشبکه مقرون به صرفه نباشد و در Network1 ۱۰۰عدد به نظر نمی رسد که انتخاب یک سرور DHCP جداگانه برای ۱۰ ایستگاه بخواهیم سرورDHCP قابل توجیه باشد .

حالت دوم ، سرورDHCP مشترک بین چندین شبکه :

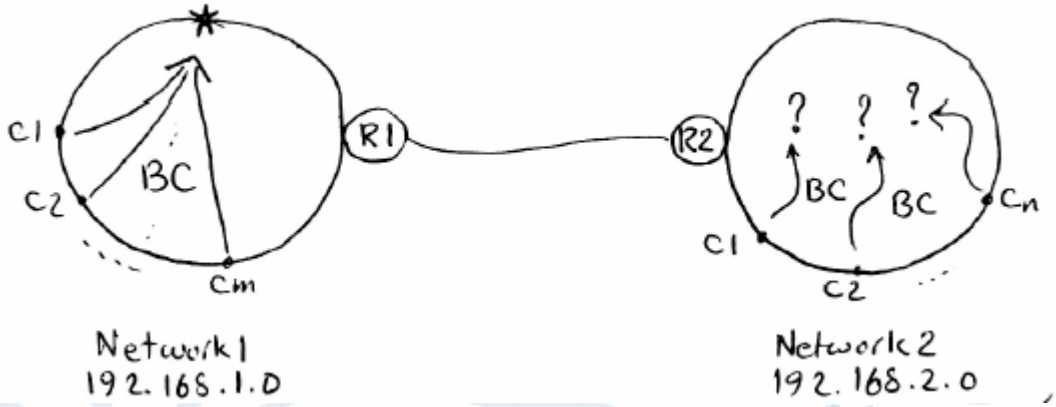
شکل ۳-۱۵

همانطور که از شکل ۳-۱۵ پیدا است مشکلی برای ایستگاه های Net1 وجود ندارد زیرا BCآنها مستقیم و بدون واسطه به سرور DHCP می رسداما وضعیت BC های مربوط به Net2 خبری از DHCP Server نیست و ازطرفی روترها نیز به طور عمده جلوی عبور ترافیک BC را می بندند.

این مشکل به وسیله ی سرویس DRA[1] حل می شود بدین ترتیب DRA ، BC های مربوط به ایستگاه ها را در یافت کرده و آن را به صورت Unicast به سمت سرور DHCP هدایت می کند .DRAباید در Net2 قرار گیرد تا بتواند BC های مربوط را از ایستگاه دریافت کند.

هرچند می توان DRA را درون Net2 قرارداد اما بهتر است در صورت امکان آن را روی روتر R2 فعال کرد . امروزه اکثر روترها از سرویس DRA پشتیبانی می کنند و درصورت نیاز باید آن را پیکربندی و فعال کرد:

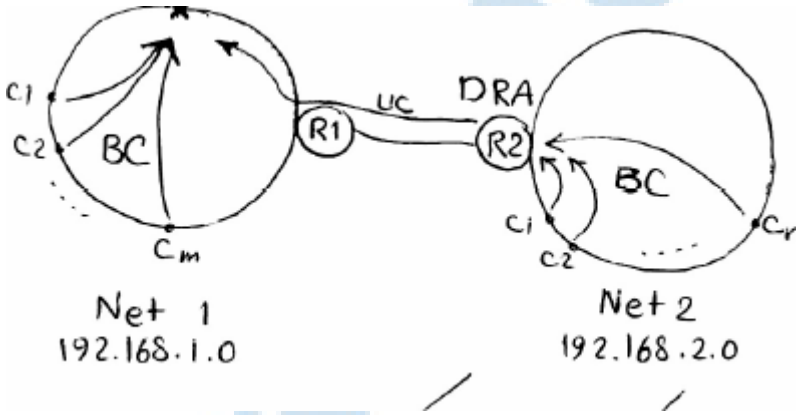
[1] DHCP Relay Agent



شکل ۴-۱۵

حالت سوم ، سرور DHCP مشترک بین چندین شبکه :

عنوان این حالت شبیه به حالت دوم است اما شکل آن فرق می کند . فرض کنید که ۳ شبکه مختلف داریم که همگی بایک روتر به یکدیگر متصل شده اند . به نظر شما بهترین موقعیت برای قرارگیری سرورDHCP کجاست؟



شکل ۵-۱۵

در صورت امکان بهتر است سرور DHCP روی روتر باشد . برخی از روترها چنین قابلیتی دارند (مانند روترهای Cisco) . در این حالت نیازی به DRA نیست زیرا که روتر که به عبارتی سرور DHCP نیز هست مستقیما BC های ایستگاه ها را از هر ۳ شبکه دریافت کرده و پاسخ مناسب را به آنها می دهد :

شکل ۶-۱۵-

۱۵-۴. نصب DHCP Server

قبل ازاقدام به نصب سرور DHCP باید مقدمات زیر را فراهم کرد .

- ۱)سخت افزار مناسب برای سرور مخصوصا کارت شبکه ، RAM،CPU .
- ۲) غیر فعال بودن نرم افزارها و سرویسها ی غیر ضروری روی سرور.
- ۳) تخصیص IP Address به سرور به صورت Static (Manual).

نصب سرویس DHCP :

در سیستم عامل های ویندوز سرور (2000server یا 2003 server) توانایی نصب DHCP Server راوجود دارد اما روی Professional اعم از 2000 یا xp نمی توان DHCP Server نصب کرد . برای نصب مراحل زیر راطی کنید:

Add or Remove program\Windows components\Networking services\DHCP

پس از اتمام ، کنسول سرویس ها را اجرا کرده (services.msc) و تایید کنید که سرویس DHCP Server در لیست مربوط ظاهر شده و فعال است (started).

۵ -۱۵. پیکربندی سرور DHCP

مهمترین قسمت در پیکربندی DHCP تعریف محدوده ای است که در آن IP Address به همراه سایر پارامترهای دیگر مشخص شده و DHCP Client طی فرایند راه اندازی آن را از سرور دریافت می کند .به این محدوده اصطلاحا Scop گفته می شود.

برای پیکربندی scop کنسول DHCP را از بخش Adminn startive اجرا کرده یا از طریق Run فرمان زیر را تایپ کنید :

.dhcp mgmt.msc

پس از اجرای زمان باید آیکن مربوط به سرور با یک فلش سبز رنگ کوچک روی آن ظاهر شود که به معنی فعال بودن سرویس DHCP است .سپس آیکن سرور را انتخاب کرده و پس از کلیک راست روی آن گزینه New Scope را انتخاب کنید .

یک Wizardبرای تعریف Scope شامل دو بخش است :

الف) مشخصات اولیه شامل:

-Name Description
-IP Address Range Assigned to client & Subnet Mask
-IP Address Range Excluded (Not Assign to clients)
- Lease Duration

ب) مشخصات ثانوی که به Scope options معروف بوده و شامل:

-Router IP Address (Default Gateway)
-DNS Server IP Address
-Domin Name
-Win Setrver IP Address
-Node Type

توضیح هریک از پارامترهای اولیه عبارتند از :

- نام Scope یک عبارت توصیفی کوتاه (Description) که بیانگر محدوده شبکه ای است که Scope به آن سرویس میدهد . واردکردن Description الزامی نبوده و اختیاری است .
- محدوده آدرسی که باید به ترتیب به ایستگاه ها داده شود . مثلا از 192.168.1.21 الی 192.168.1.200
- آدرس یا محدوده آدرس هایی که ازمیان بند قبل نباید به ایستگاه داده شود . .مثلا فرض کنید ازمیان 192.168.1.21 الی 1.200 آدرس های زیر ازقبل به صورت ایستا روی برخی از محدوده ایستگاه تنظیم شده و باید به همان صورت نیز باقی بماند :

-192.168.1.51 → 1.55
-192.168.1.75
-192.168.1.101

اصطلاحا به این محدوده " محدوده نبایدها " گفته می شود (Exclusion Range)

منظور از Lease Duration مدت زمانی است که آدرس به همراه سایر پارامترهای دیگر" احیا" (تمدید) شود.به عبارت دیگر IP Address به ایستگاه ها برای مدتی مقرر "اجاره " داده می شود .هرچند می توان آدرس و دیگر پارامترها را به طور نامحدود به یک ایستگاه تخصیص داد اما این کار توصیه نمی شود چرا که در صورت مثلا از رده خارج شدن یک Client از شبکه هیچ گاه آدرس آن نمی تواند به ایستگاه دیگری داده شود بنابراین بهتر است که مدت زمان اجاره نامحدود نباشد .

طول این زمان به طور پیش فرض آن ۸ روز است . اما می توان گفت چنان چه در یک شبکه میزان جابجایی کامپیوترها نسبتا کم است و از طرفی محدوده آدرس نیز نسبت به کامپیوترها بیشتر است در آن صورت مدت زمان اجاره را طولانی انتخاب کرده و در صورتی که جابجایی کامپیوترها زیاد باشد (مثلامی خواهیم ایستگاه های قدیمی را از رده خارج کرده و ایستگاه های جدیدی جایگزین کنیم یا به عنوان مثال تعداد کامپیوترهای Notebook که به شبکه وارد می شوند و از آن خارج می گردند زیاد است)و از طرفی محدوده آدرسها به نسبت تعداد کامپیوترها محدود است و در آن صورت مدت زمان اجاره را کوتاه انتخاب می کنیم .به بیانی دقیق تر مدت زمان اجاره بستگی به میزان عرضه و تقاضای IP دارد هرچه نسبت عرضه به تقاضا بیشتر باشد مدت زمان را طولانی تر و هرچه نسبت تقاضا به عرضه بیشتر شود مدت زمان را کوتاه تر انتخاب می کنیم .

توضیح هریک از پارامترهای ثانوی نیزعبارتند از :

- آدرس روتری که ایستگاه ها به واسطه آن به شبکه های دیگر راه پیدا می کنند . در کامپیوترهای مبتنی بر سیستم عامل ویندوز هنگامی که دستور ipconfig را وارد می کنیم این پارامتر تحت عنوانDefault Gateway دیده می شود .
- آدرس DNS Server که باید اسامی TCP/IP را به آدرس آنها برگرداند.

می دانیم که در پروتکل TCP/IP هنگامی که مثلا می نویسیم http://ww.yahoo.com فایده ای برای TCP/IP نداشته و باید آدرس سایت yahoo را پیداکند . وظیفه تبدیل اسم TCP/IPبه آدرس IP به عهده DNS Server بوده و هر Host نیازمند دانستن آدرس DNS Server است .

سایر پارامترهای ثانوی را به دلیل آنکه در حالت خاص استفاده می شوند در این مبحث بررسی نمی کنیم.

برای آنکه پیکربندیScope را بهتر درک کنیم لازم است تا عملا مثالی را بررسی کنیم .

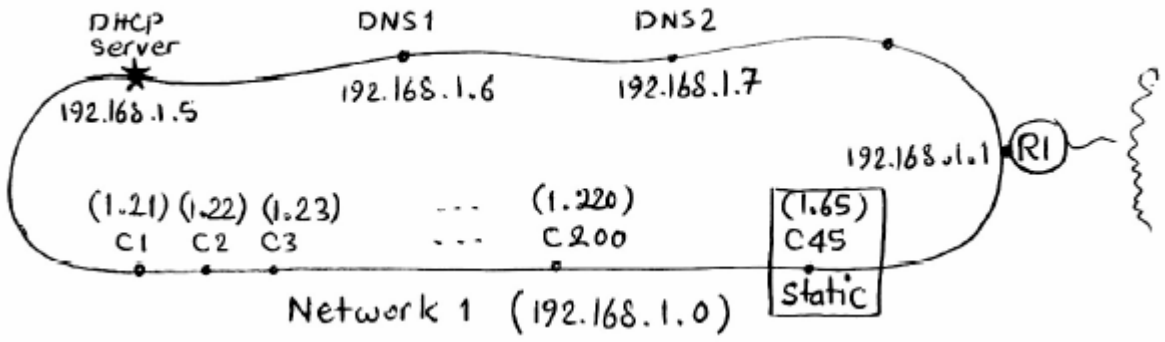
قبل از انجام عملیات باید به ۲ نکته توجه کرد :

الف) موقعیت DHCP Server در شبکه چگونه است ؟

ب) ایستگاه ها چه پارامترهایی را می خواهند دریافت کنند ؟

توجه به بند الف چگونگی" پیکربندی DHCP Server "را تعیین می کند وتوجه به بند ب به ما یاد آور می شود که "چه چیزی" را می خواهیم پیکربندی کنیم .

مثال ۱: حالت زیر را در نظر گرفته و سرور DHCP را بر اساس آن پیکربندی کنید:



شکل۷-۱۵

همانطور که از شکل ۷-۱۵ پیدا است Network تشکیل شده از 200 ایستگاه به نام های c1 الی200c که همگی آنها به استثنای c45 (به آدرس 192.168.1.65) آدرس خود را از سرور DHCP به دست می آورند .سیستم c45 دارای آدرس Manual (static) بوده و از DHCP استفاده نمی کند .آدرس روتر 192.168.1.1 بوده و ۲ دستگاه نیز به عنوان سرور DNS در شبکه وجود دارند که البته آدرس آنها نیز Static است .

فرض کنید میزان جابجایی در شبکه کم است و به عبارت دیگر شبکه در حالت پایدار است . با توجه به داده های فوق ابتدا پیکربندی scope را فهرست کرده و سپس عملا اجرا می کنیم :

پارامترهای اولیه:

-Name :Scope1
-Description :Assigning Address to Network1
-IP Address Range : 192.168.1.21…192.168.1.250
-Subnet Mask: 24 bits(255.255.255.0)

(دقت کنید که محدوده آدرس ها را بیشتر از تعداد ایستگاه ها انتخاب می کنیم تا محدودیت کمتر شود)

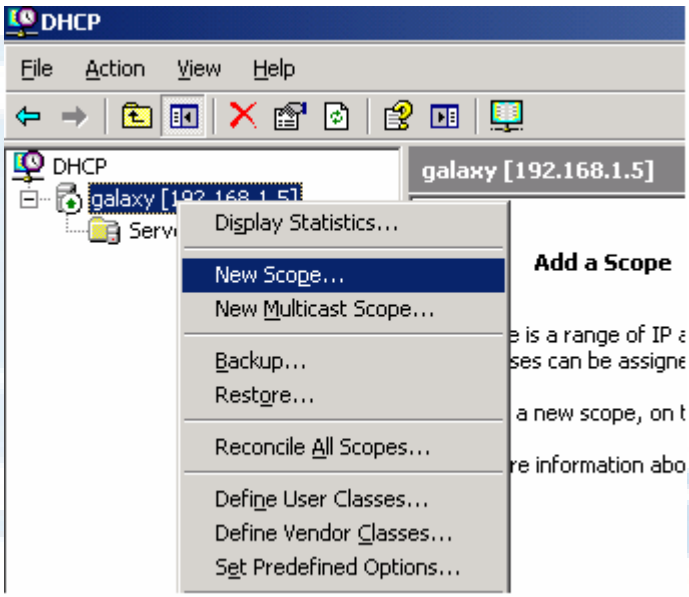
-Exclusion Range:192.168.1.65
-Lease Duration:60 Days

پارامترهای ثانونی:

-Router : 192.168.1.1
-DNS Server: 192.168.1.6&192.168.1.7

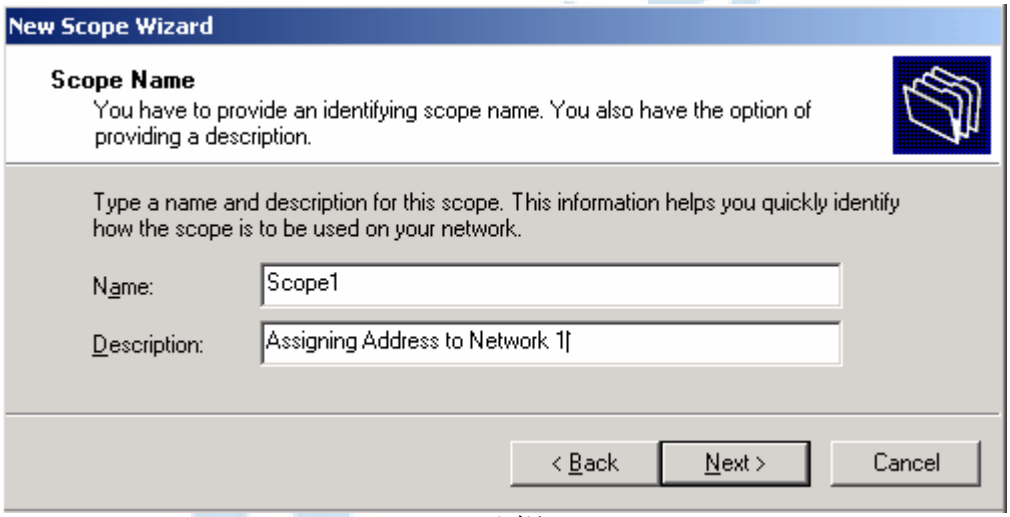
حال کنسول DHCP را روی سرور اجرا کرده و کار پیکربندی را آغاز کنید

ابتدا روي آيكن سرور كليك راست كنيد و گزينة New Scope را براي تعريف محدودة جديد انتخاب نماييد:



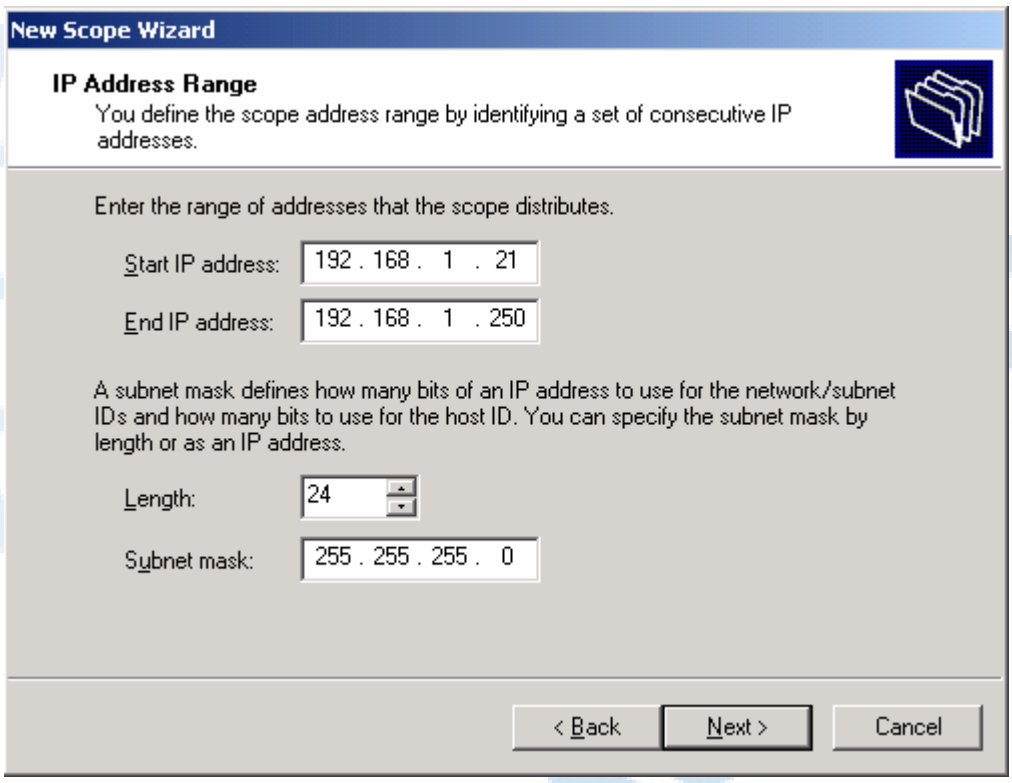
شکل ۸-۱۵

سپس نام Scope را وارد کرده و یک Description مناسب (اختیاري) براي آن بنویسید:



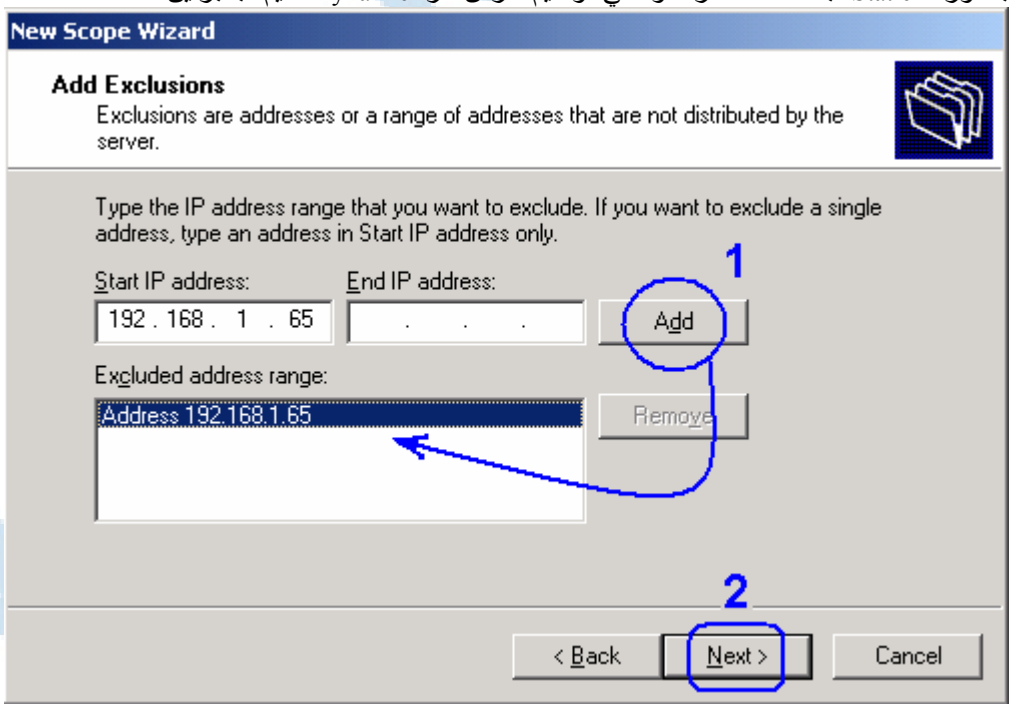
شکل ۹-۱۵

اکنون نوبت به تعیین محدوده آدرس هایي است که باید به ایستگاه ها تخصیص یابد:



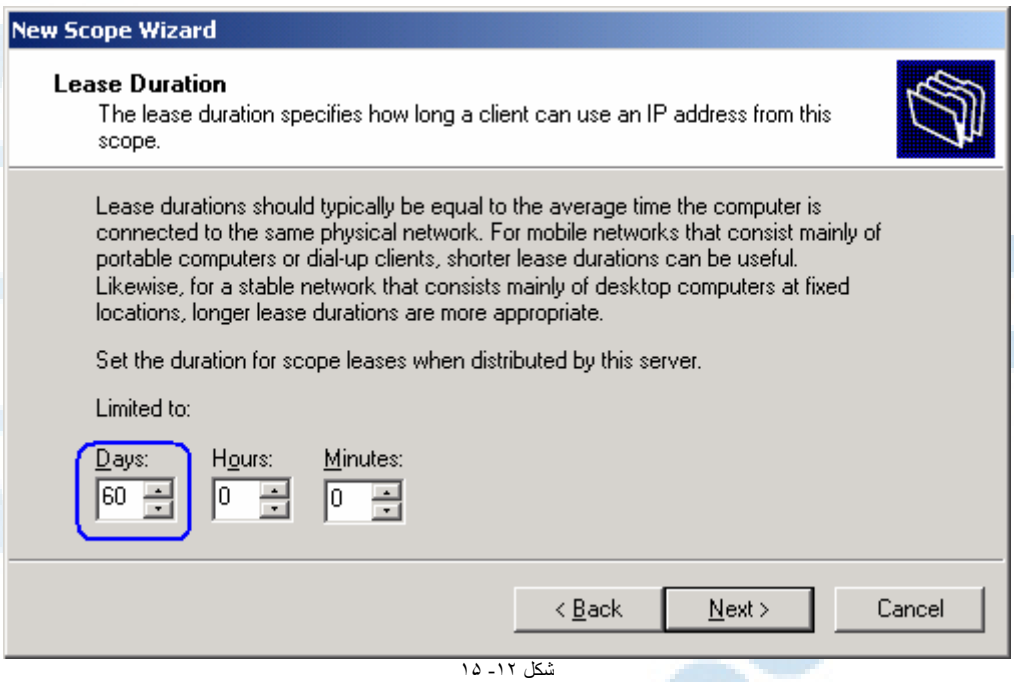
شکل ۱۰-۱۵

طبق طرح ، آدرس ۱۹۲,۱۶۸,۱,۶۵ نباید از طریق DHCP Server به ایستگاه ها داده شود چرا که یکي از سیستم ها آنرا بصورت Static قبلاً استفاده کرده و نمي‌خواهیم آدرس آنرا Dynamic کنیم، بنابراین:



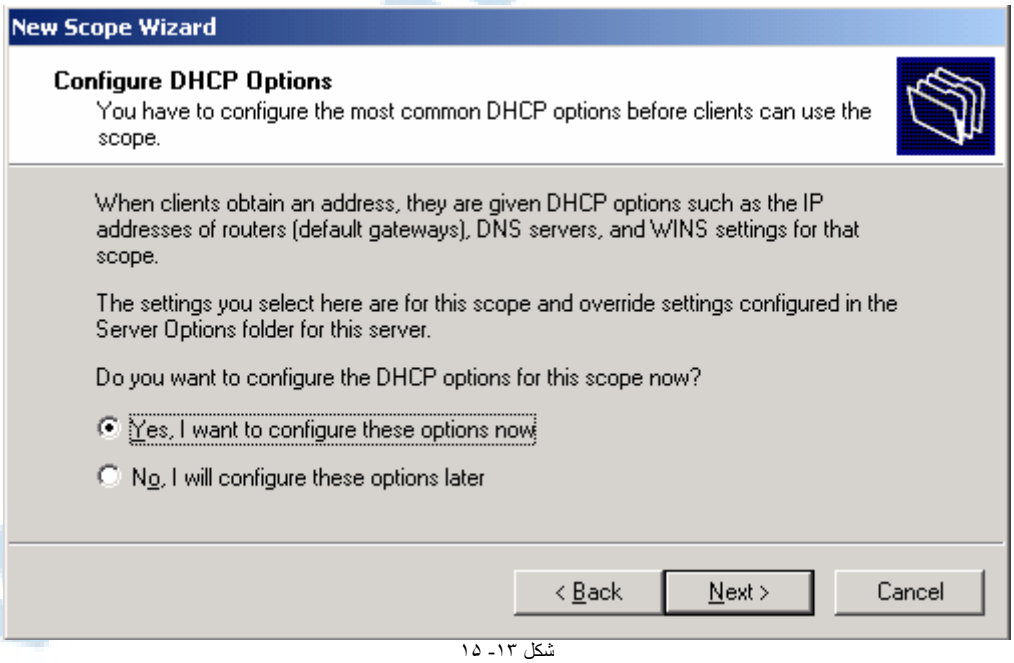
شکل ۱۱-۱۵

با توجه به پایداري Client ها، زمان اجاره را مثلاً ۶۰ روز انتخاب کنید:



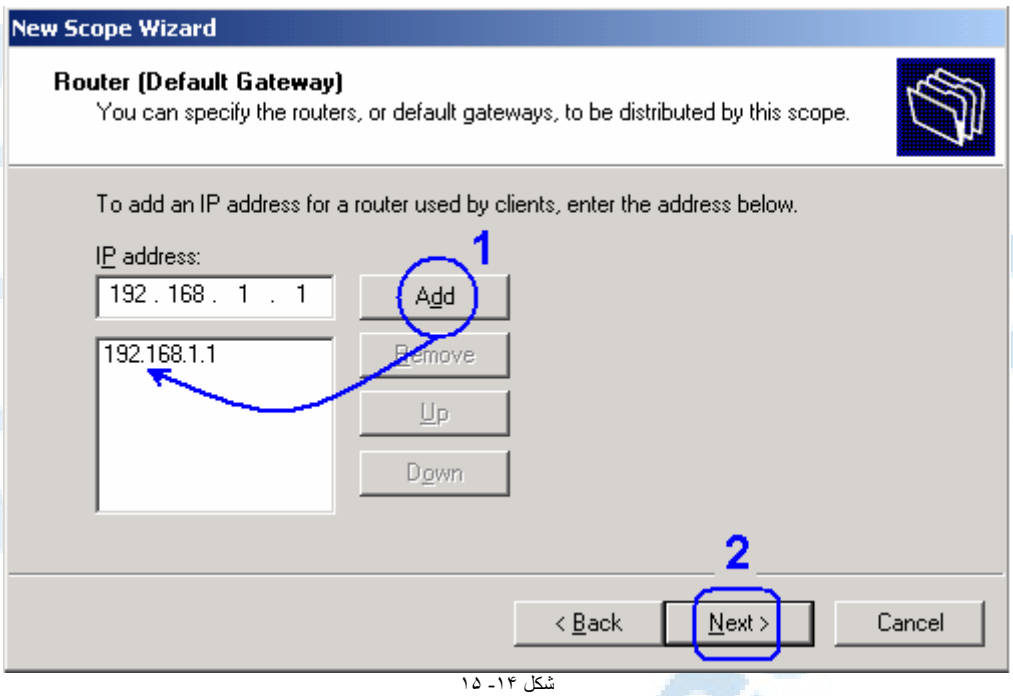
شکل ۱۲- ۱۵

تا اینجای کار فقط پارامترهای اولیه را تعیین کرده ایم، حال نوبت به پارامترهای ثانوی می‌رسد که به Scope Options معروف هستند. برای تنظیم این پارامترها بهتر است مطابق شکل زیر Wizard را ادامه داده و به تعیین آنها بپردازیم، با این حال می‌توان آنها را بعداً هم تعریف کرد. در هر صورت فرقی نمی‌کند، فقط دقت داشته باشید چنانچه تعریف پارامترهای ثانوی را به بعد موکول کنیم درآنصورت برای آنکه DHCP Server بتواند به Client ها IP بدهد باید حتماً Scope مربوطه را خودمان فعال یا اصطلاحاً Activate کنیم و اینکار با کلیک راست روی Scope و انتخاب گزینهٔ Activate صورت می‌گیرد. در اینجا چون ادامهٔ کار را با همین Wizard انجام می‌دهیم لذا پس از اتمام کار، Scope بطور خودکار Activate خواهد شد:



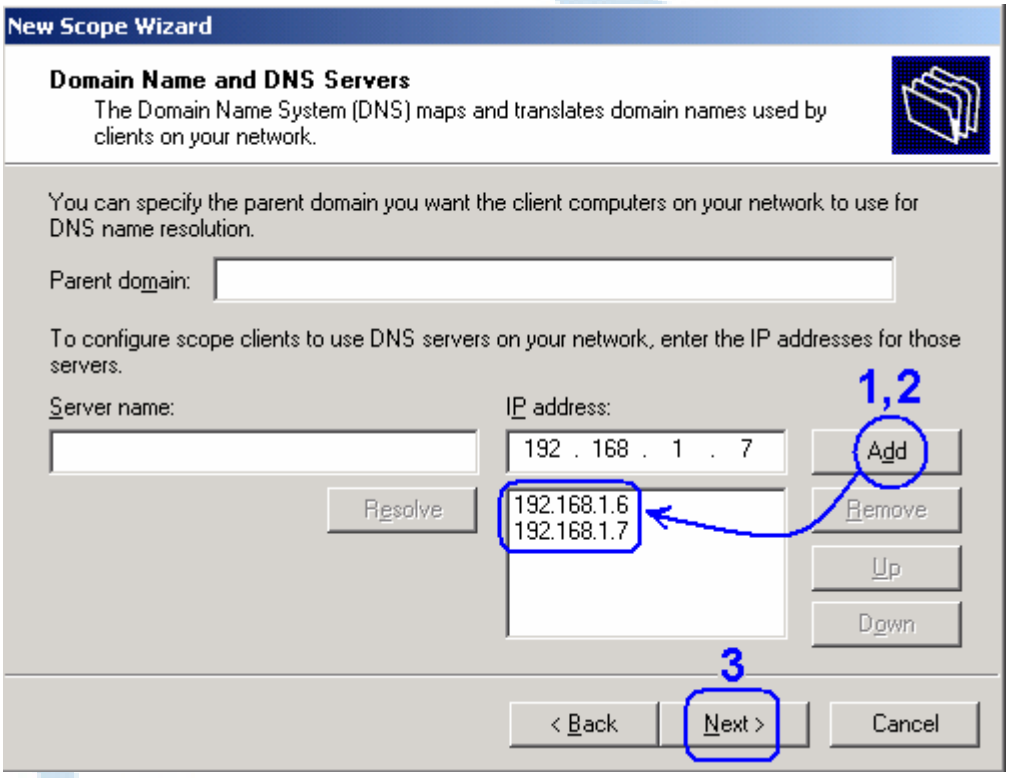
شکل ۱۳- ۱۵

اولین پارامتر ثانوی عبارت‌است از تعیین آدرس روتر یا بعبارتی همان Default Gateway:



شکل ۱۴- ۱۵

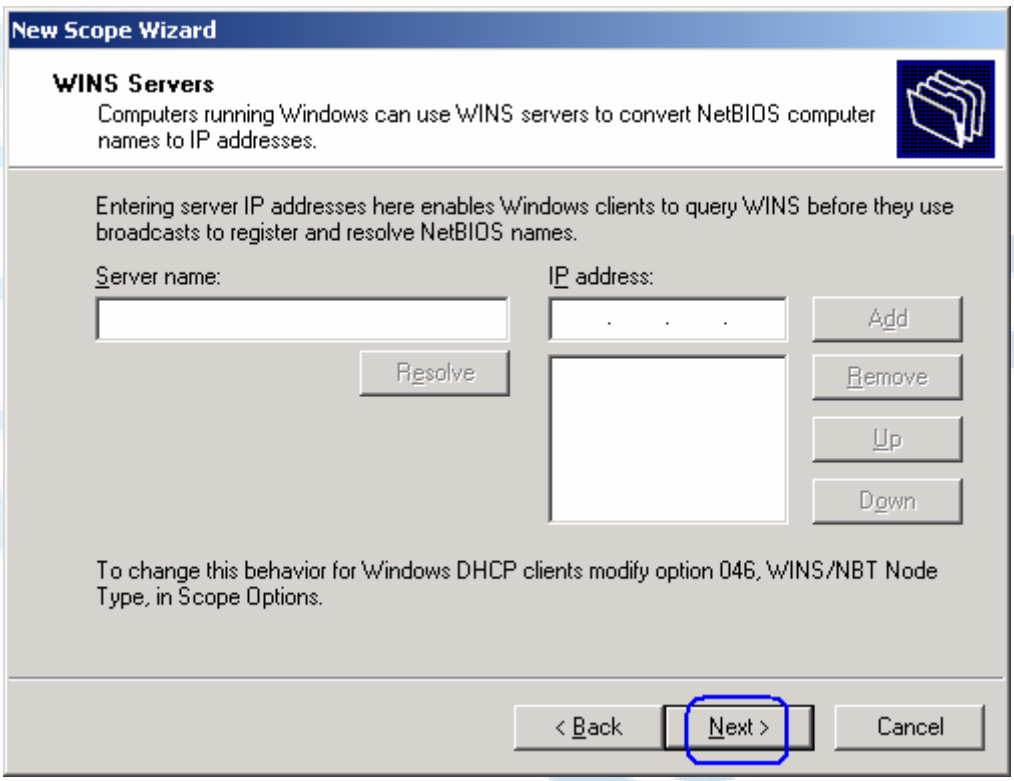
سپس باید آدرس DNS Server(s) را تعیین کنیم، چون در مثال مذکور ۲ دستگاه DNS Server داریم لذا هردو را به Client ها معرفی کنید:



شکل ۱۵- ۱۵

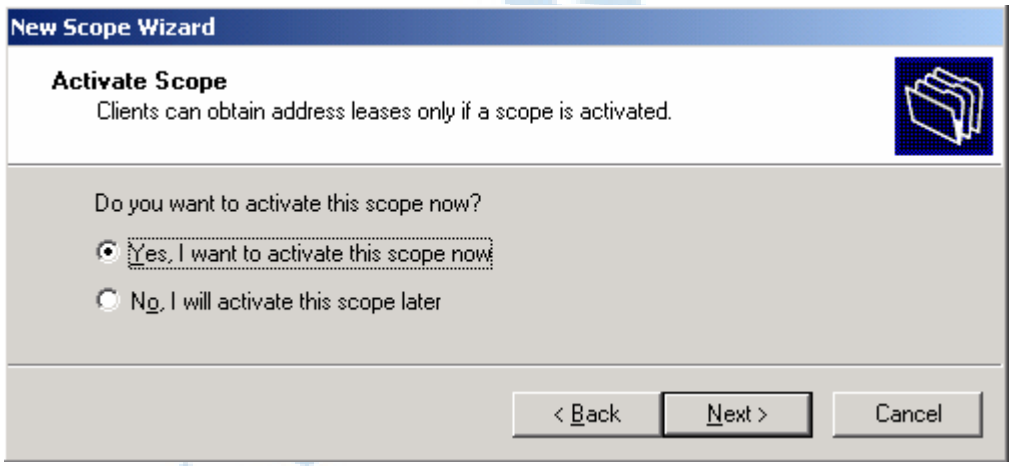
البته در مرحلهٔ فوق میتوانیم نام Domain را نیز که میخواهیم به FQDN Client ها تعلق گیرد تعیین کنیم، اما بدلیل عدم درخواست صورت مسأله از آن صرف نظر کردیم.

حال نوبت به تعیین آدرس WINS Server میرسد که آنرا هم با توجه به عدم نیاز در صورت مسأله بدون مقدار رد کنید:



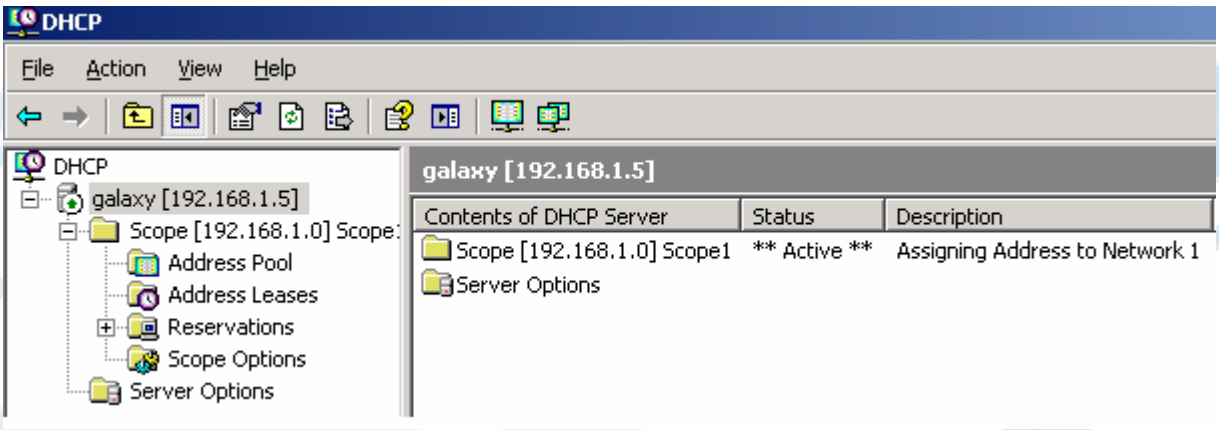
شکل ۱۶- ۱۵

اکنون در آخرین مرحله، باید Scope را فعال کنیم:



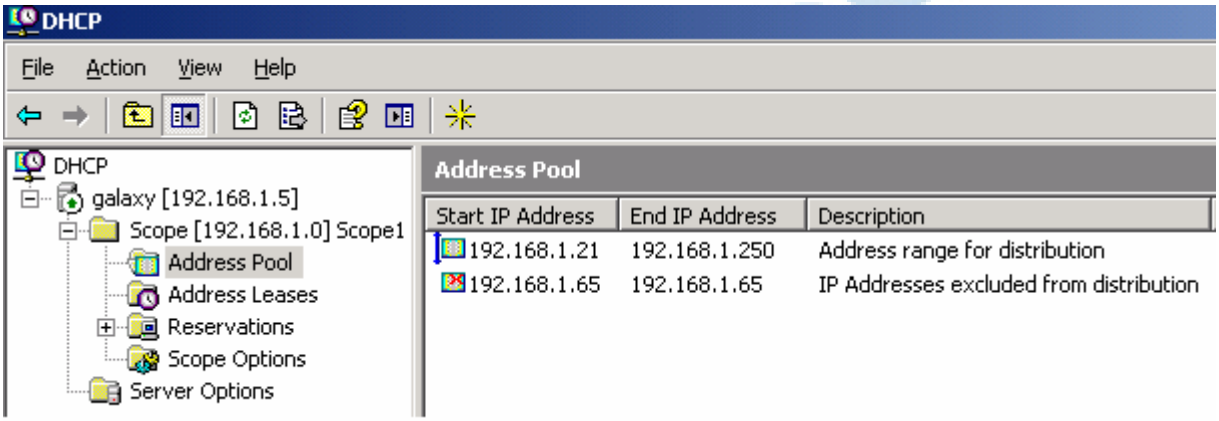
شکل ۱۷- ۱۵

کار را به اتمام رسانده (Finish) سپس Scope را از زیر شاخهٔ سرور انتخاب کنید تا بتوانید نتایج تنظیمات و همچنین نحوهٔ بهره‌برداری Client ها از آنرا ببینید:



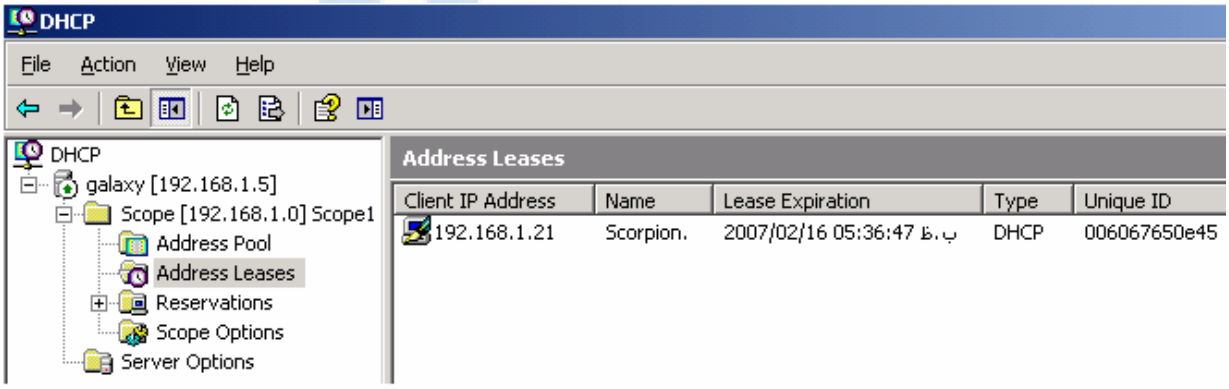
شکل ۱۸- ۱۵

در ابتدا قسمت Address Pool را انتخاب کنید، چه مشاهده می‌کنید؟ بله، محدوده آدرسهایی که می‌تواند به Client ها داده شود(Distribution Range) و همچنین آدرسهایی که نباید داده شود(Exclusion Range):



شکل ۱۹- ۱۵

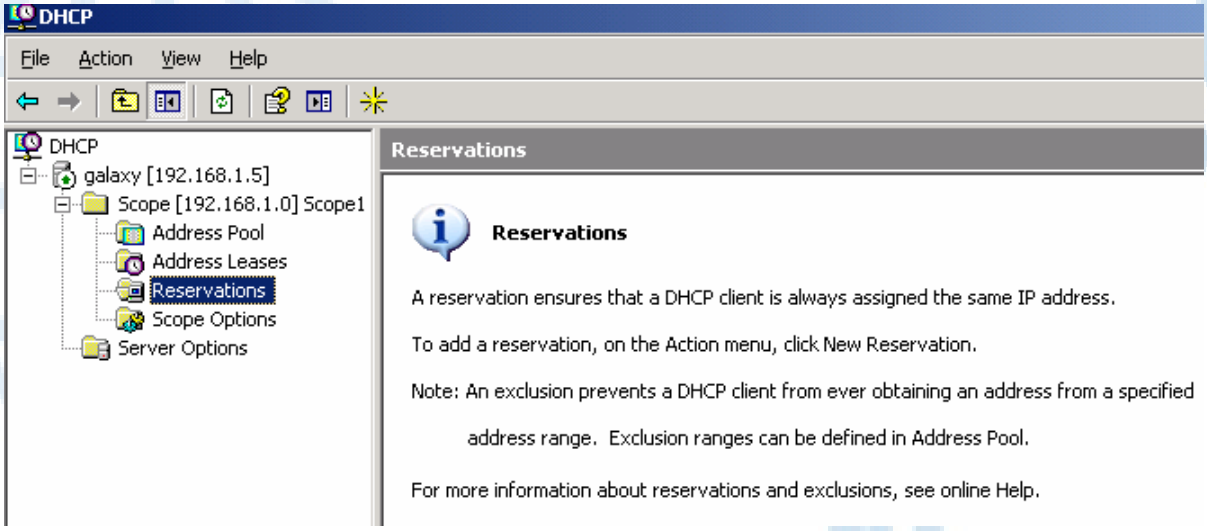
چنانچه قسمت Address Leases را انتخاب کنید می‌توانید آدرسهایی را که تاکنون Client ها از سرور گرفته‌اند بهمراه مشخصات Client و همچنین پایان زمان اجاره مشاهده کنید:



شکل ۲۰- ۱۵

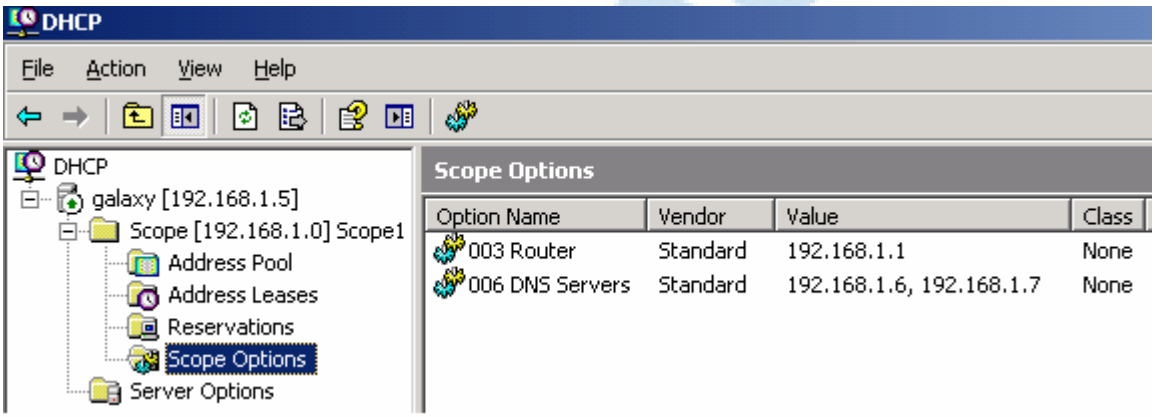
اگر می‌خواهید آدرسی مشخص را برای یک Client بطور دائمی تخصیص دهید می‌توانید آدرس را برای آن ذخیره کنید. برای این کار لازم است تا MAC Client Address را داشته باشید. برای بدست آوردن MAC Address یک کامپیوتر راههای مختلفی وجود دارد اما استفاده از دستور ipconfig /all یا دستور getmac

راجتر است. در سناريوي يادشده آدرسي براي ذخيره تعيين نكرديم لذا ليست خالي است:



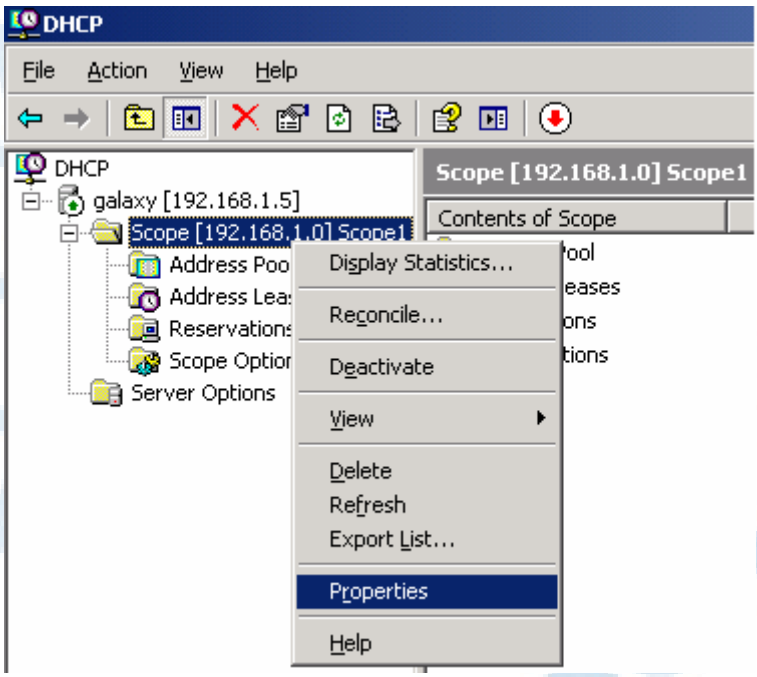
شكل ٢١- ١٥

اكنون قسمت Scope Options را انتخاب كرده و تأييد كنيد كه پارامترهاي ثانوي تنظيم شده يعني Router و DNS Server هردو وجود دارند:

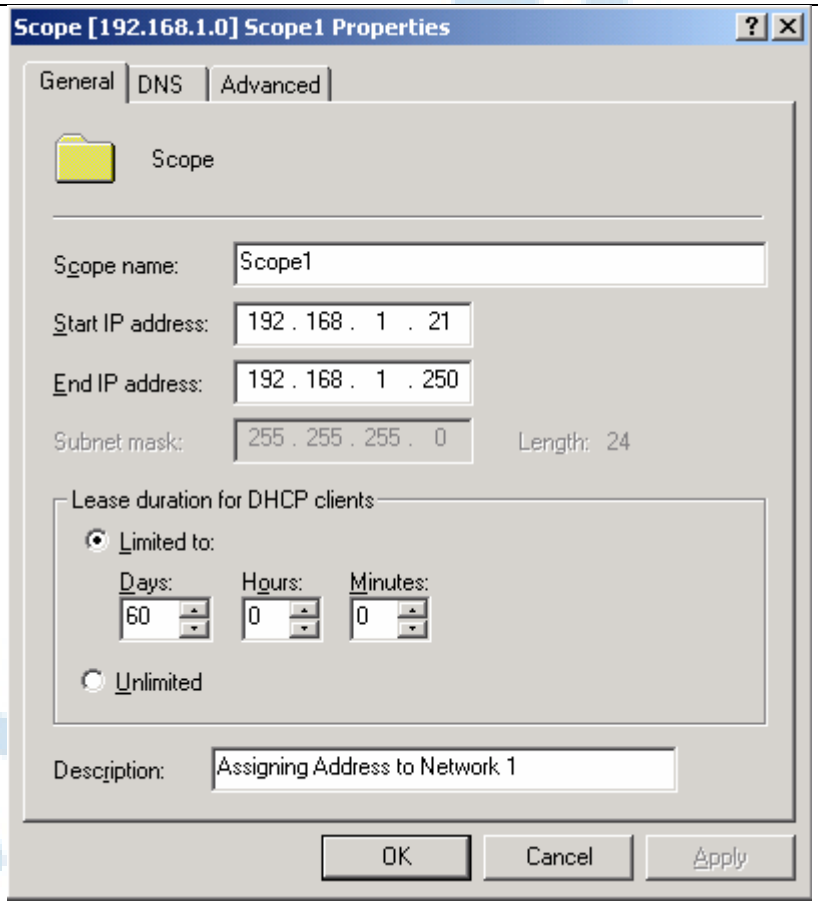


شكل ٢٢- ١٥

مي‌توانيد اكثر پارامترهاي Scope را تغيير دهيد. بعنوان مثال براي گسترش يا كاهش محدوده آدرسها يا تغيير زمان اجاره مطابق زير عمل كنيد:

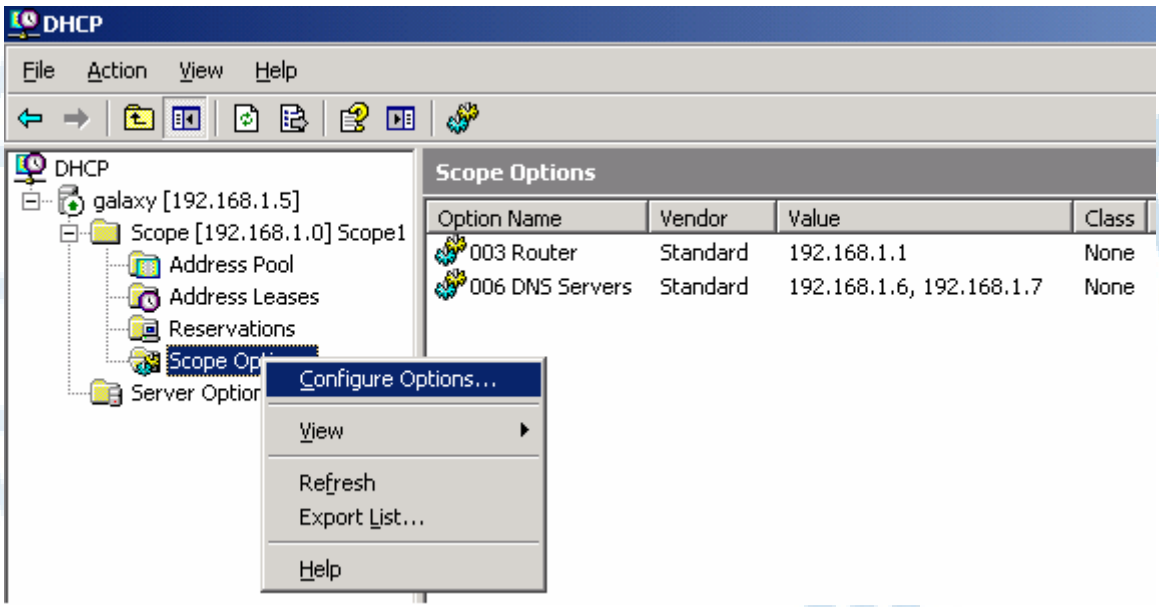


شکل ۲۳- ۱۵

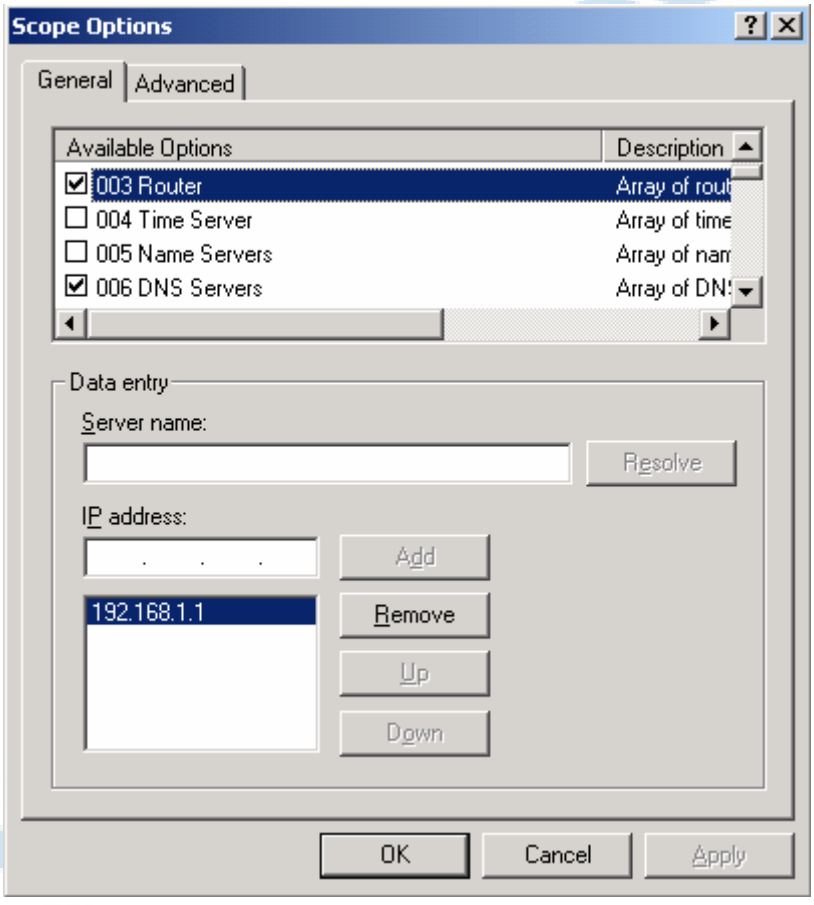


شکل ۲۴- ۱۵

همچنین برای تغییر پارامترهای ثانوی میتوانید مانند شکلهای زیر عمل کنید:



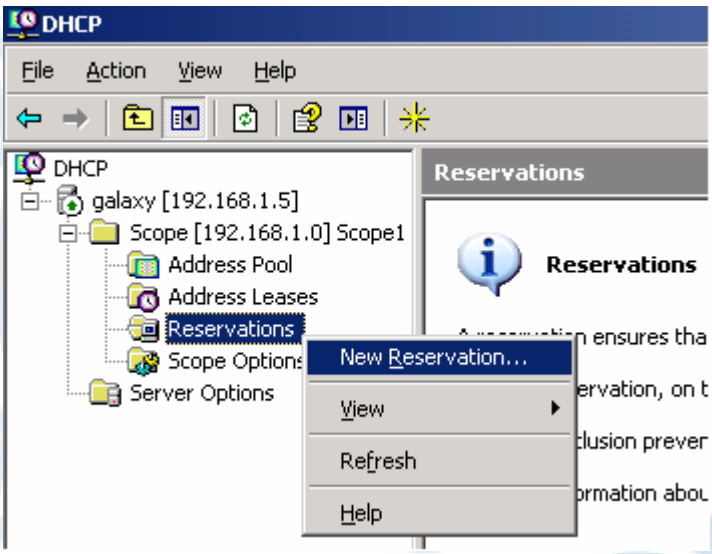
شکل ۲۵- ۱۵



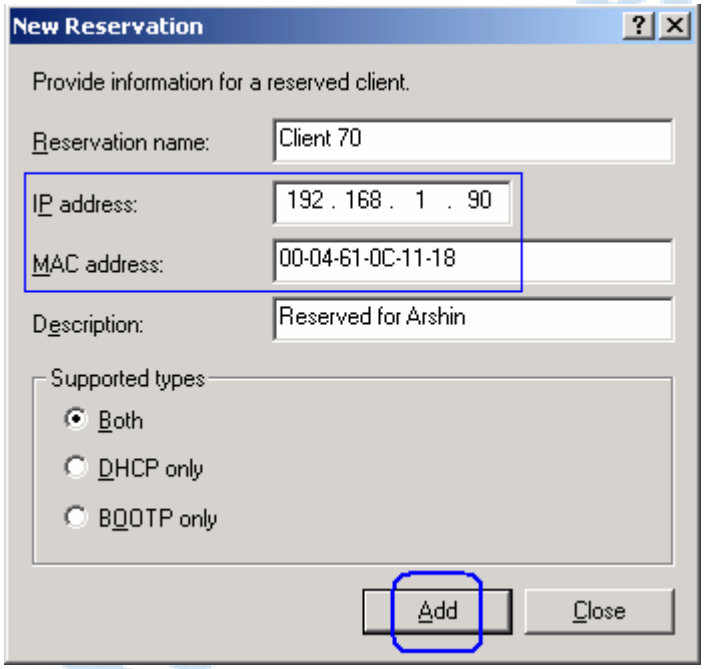
شکل ۲۶- ۱۵

البته با Double Click روي يكي از Scope Options نيز همان نتيجة فوق بدست مي آيد.

در صورت نياز به ذخيره آدرس، از قسمت Reservation حركت را شروع كنيد. همانطور كه اشاره شد ابتدا بايد Client MAC Address را بدانيد. فرض كنيد مي‌خواهيم آدرس 192.168.1.90 را براي Client70 ذخيره كنيم كه MAC آن برابر با 00-04-61-0C-11-18 بوده و كاربر آن شخصي بنام Arshin است. البته دانستن نام كاربر براي پيكربندي لازم نبوده و صرفاً جنبة اطلاع‌رساني دارد:

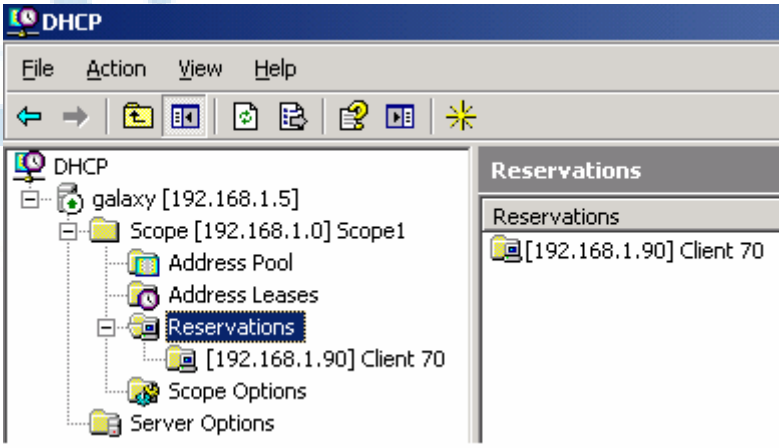


شکل ۲۷ – ۱۵



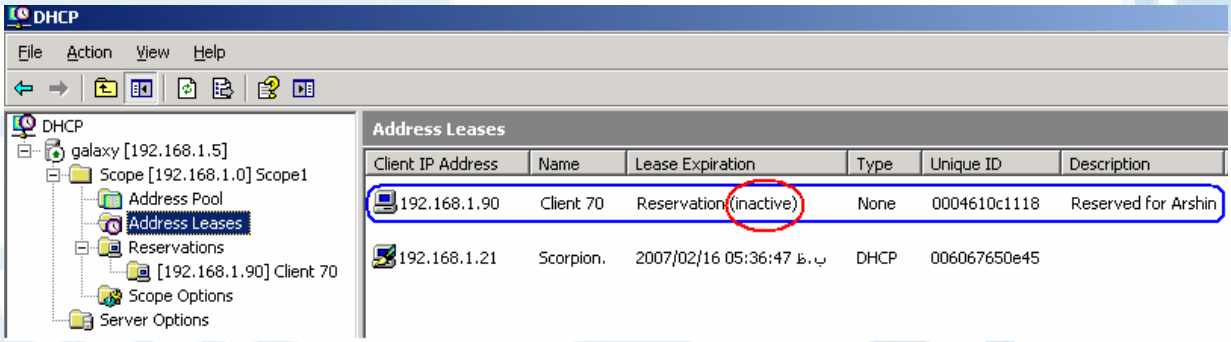
شکل ۲۸ – ۱۵

نتیجهٔ کار بصورت زیر ظاهر میشود:



شکل ۲۹ – ۱۵

سپس قسمت Address Lease را انتخاب کرده و تأیید کنید که آدرس فوق در لیست مربوطه ظاهر شده است. در صورتیکه Client هنوز آدرس را دریافت نکرده باشد نتیجه مانند شکل بصورت Inactive دیده می‌شود و به محض تخصیص آدرس به Client تبدیل به Active خواهد شد:



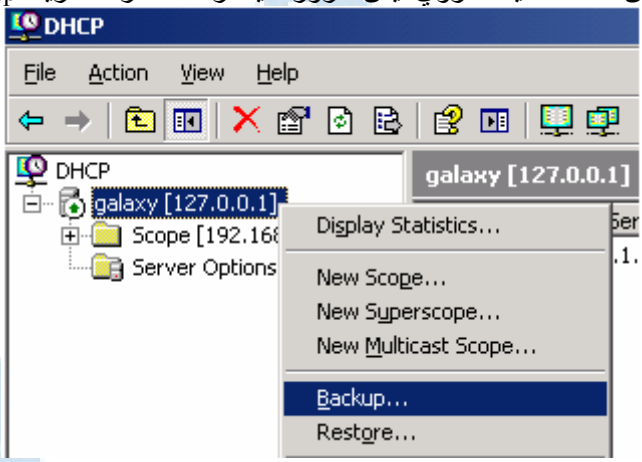
شکل ۳۰- ۱۵

بسیار خوب! تا اینجا توانسته‌ایم پیکربندی یک DHCP Server را برای یک سناریوی ساده به پایان رسانده و نتیجه را ببینیم.

۱۵-۶- Backup / Restore اطلاعات DHCP Server :

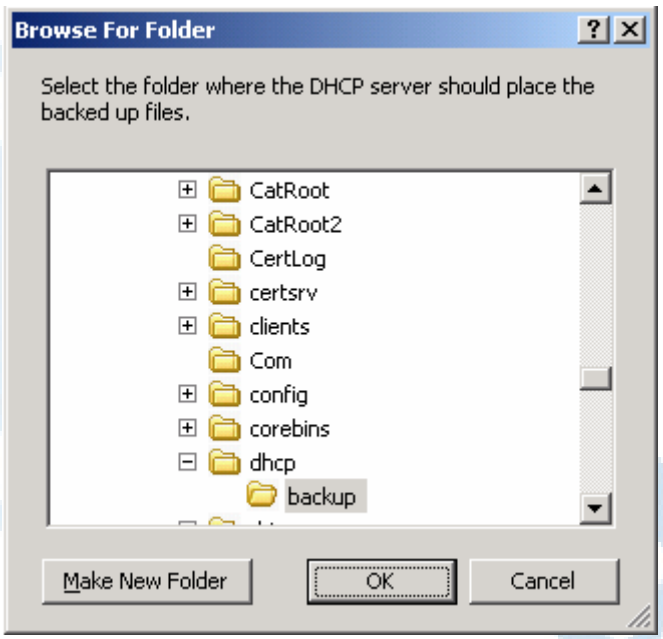
هرچند نصب و پیکربندی DHCP Server در سناریوهای ساده چندان کار سختی نیست اما در موارد پیچیده‌تر لازم است تا گاهی اوقات از اطلاعات Scope و همچنین وضعیت تخصیص آدرسها به Client های مختلف Backup تهیه شود. این نسخه‌های Backup کمک می‌کنند تا هنگام بهم ریختن اطلاعات Scope یا هنگام انتقال DHCP Server از یک سرور به سرور دیگر یا نصب مجدد سرور بتوان بسرعت اطلاعات را برگرداند.

روش تهیهٔ Backup: بسیار آسان است. کافیست روی آیکن سرور کلیک راست کرده، گزینهٔ Backup را انتخاب کنید:



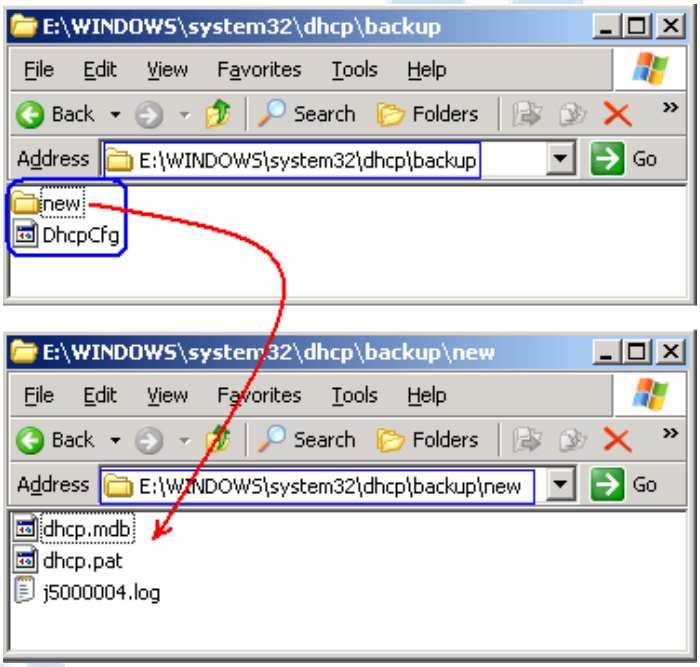
شکل ۳۱- ۱۵

در این مرحله باید محل ذخیره‌سازی Backup را تعیین کنیم که پیشفرض آن واقع در مسیر زیر است:



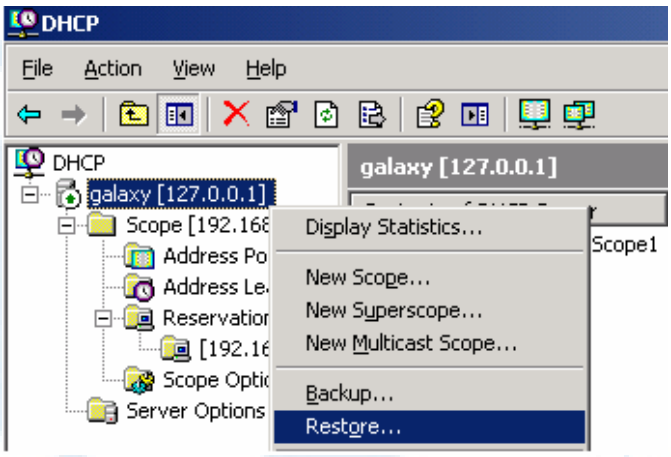
شکل ۳۲-۱۵

پس از اتمام کارپوشه فوق را باز کرده و تأیید کنید که Backup بدرستي گرفته شده:



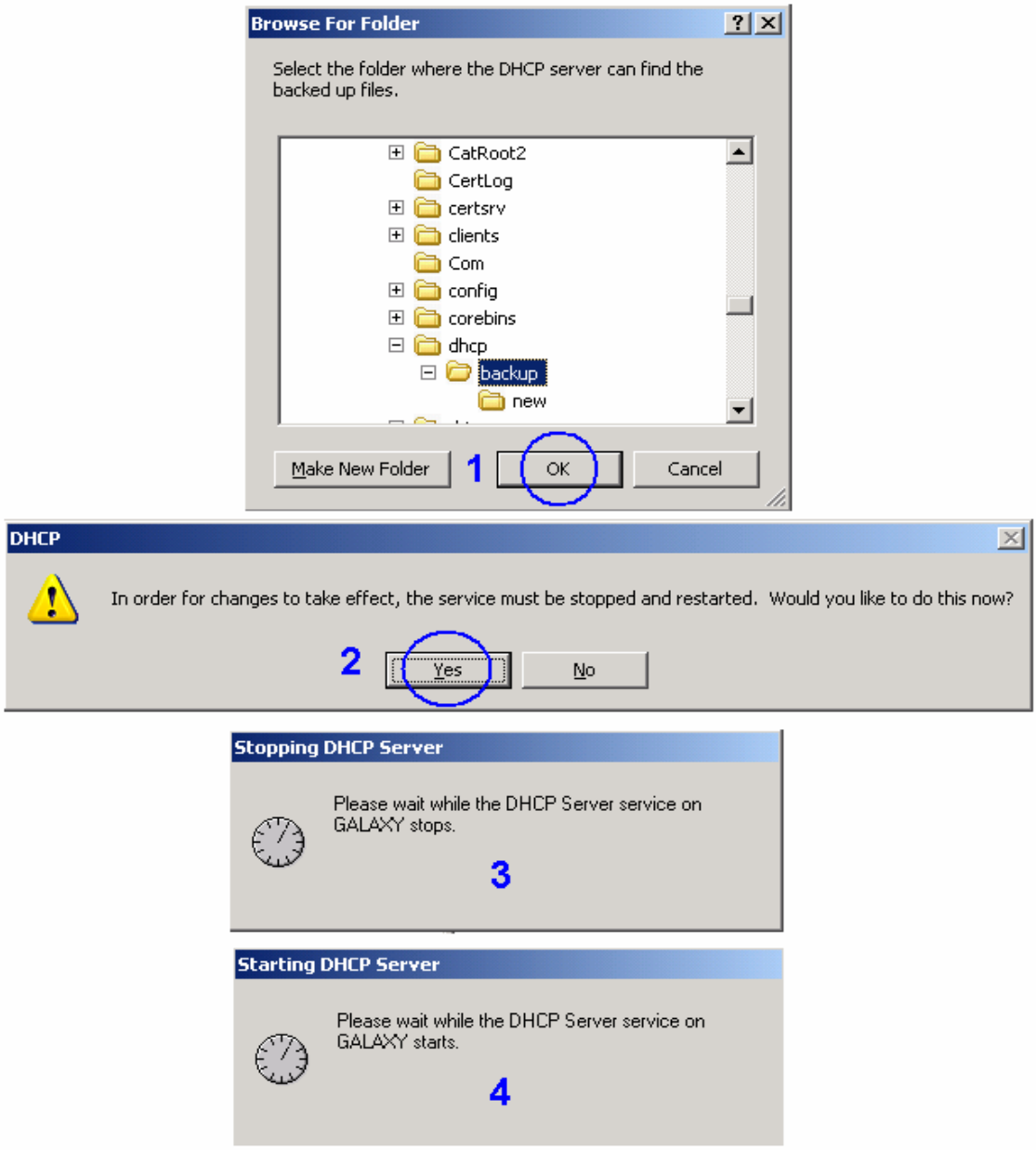
شکل ۳۳- ۱۵

مراحل Restore نیز مشابه بوده و به شکل زیر است:



شکل ۳۴- ۱۵

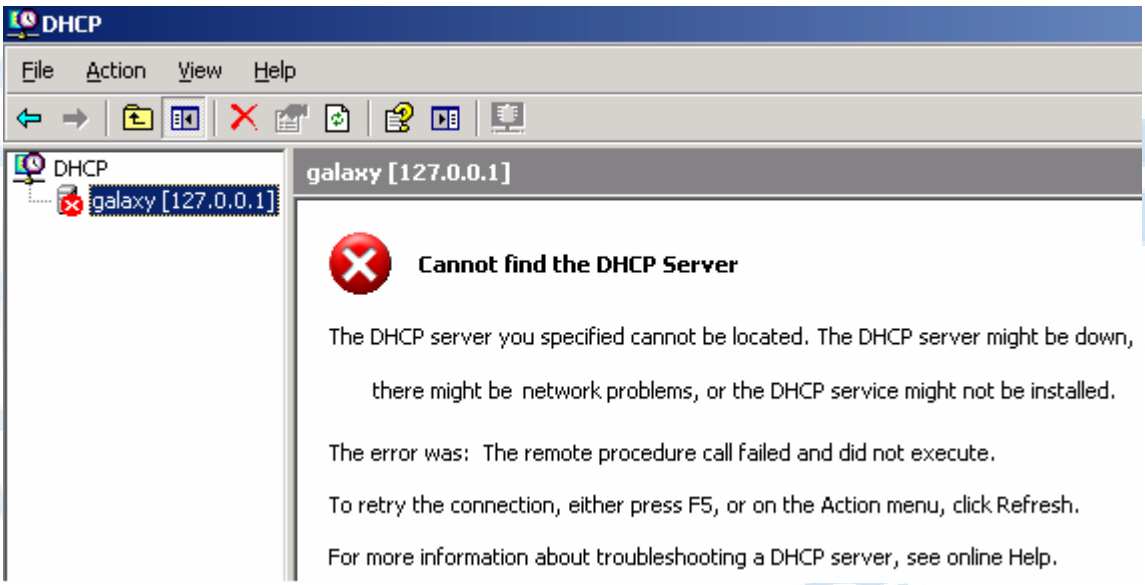
پس از تعیین مسیر، تأییدیة غیرفعال کردن یا (Stop) سرویس DHCP Server را جهت ادامة کار قبول کرده تا فرایند Restore بدرستي به پایان رسد. در انتها سرویس بطور خودکار Start خواهد شد.



۷-۱۵- عیبیابی DHCP Server :

رایج ترین اشکالاتی که ممکن است در DHCP Server عبارتند از:

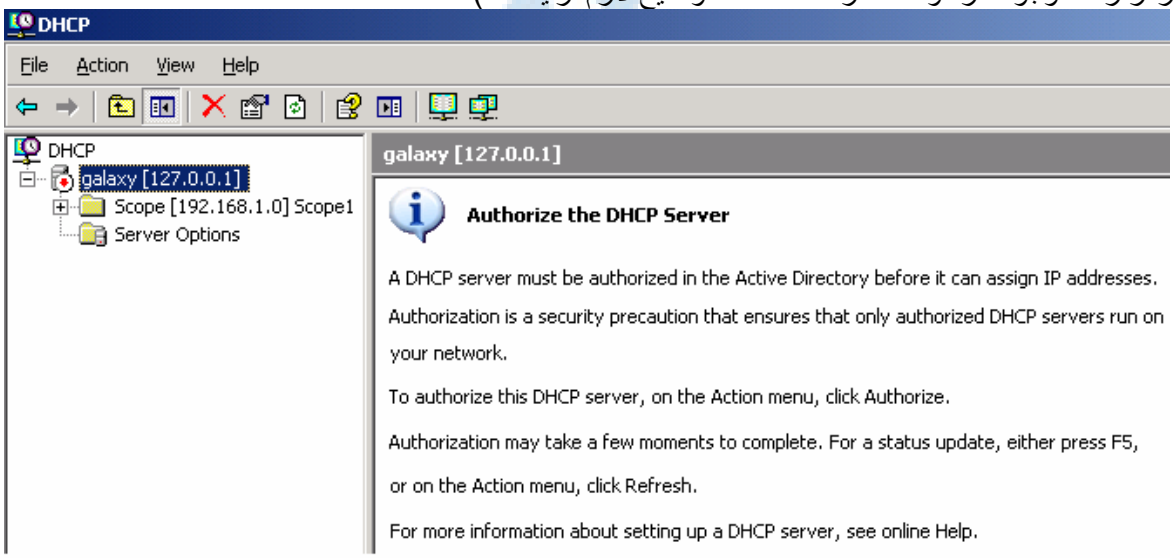
۱. سرویس DHCP Server به هر دلیل غیرفعال است. براي چك كردن آن از كنسول سرویسها وارد عمل شده (Services.msc) و تأیید كنید كه وضعیت سرور بصورت Started باشد. در حالتي كه سرویس DHCP Server غیرفعال باشد اگر كنسول DHCP را اجرا كنیم با چنین وضعیتي روبرو مي‌شویم:



شكل ۳۵ - ۱۵

نكته: به طريق مشابه ممكن است سرويس DHCP Client روي Client غيرفعال شده باشد كه بايد آنرا بررسي كرد. البته چنانچه هيچ ايستگاهي نتواند از سرور آدرس بگيرد بعيد است مشكل از سمت Client ها باشد و به احتمال زياد بايد علت را درون سرور يا ارتباط سرور با شبكه جستجو كرد.

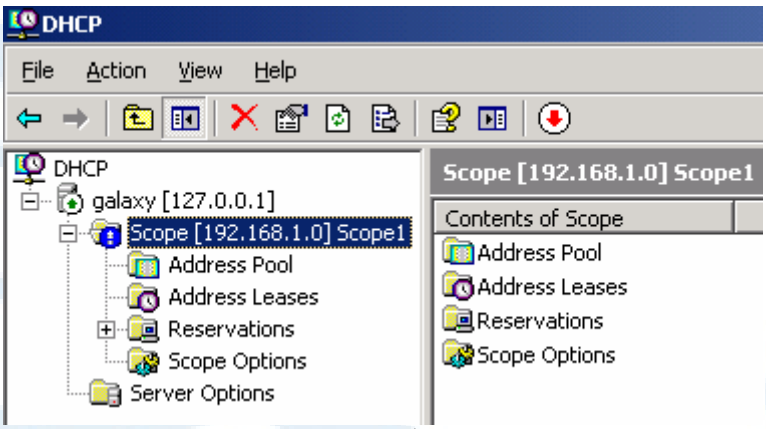
۲. DHCP Server مجاز به سرويس دهي در شبكه نيست! اصطلاحاً Authorize نشده. چنين حالتي زماني اتفاق مي‌افتد كه DHCP Server در محيط Active Directory كار مي‌كند. در اين مواقع DHCP Server بايد از جانب Domain Controller مجاز به سرويس دهي شود. به شكل زير توجه كنيد كه در آن مشكل كاملاً مشخص است: (روي آيكن سرور علامت فلش قرمز رنگ وجود دارد و سمت راست صفحه توضيح لازم ارايه شده)



شكل ۳۶ - ۱۵

براي كسب اجازه كافيست روي آيكن سرور كليك راست كرده و گزينة Authorize را انتخاب نماييم. پس از طي زماني كوتاه و احياناً چندبار Refresh كردن صفحه يا بستن و بازكردن مجدد كنسول DHCP بايد آيكن قرمز رنگ برطرف شده‌باشد.

۳. Scope پر شده است. بديهي است در چنين حالتي Client ها ي جديد نمي‌توانند آدرس بگيرند اما Client ها يي كه قبلاً از سرور آدرسي را دريافت كرده و هنوز اجارة آنها تمام نشده به كار خود ادامه داده و ضمناً در زمان مقتضي قرارداد خود را تمديد خواهند كرد. بعبارت ديگر جاي خود را به اين سادگي از دست نمي‌دهند!!. هنگامي كه Scope پر مي‌شود، با صحنة زير مواجه مي‌شويم: (علامت تعجب آبي‌رنگ در كنار Scope)



شكل ۳۷-۱۵

پرسش: بەنظر شما در چنين مواقعي بهترين كار براي رفع مشكل چيست؟

۴. Network Number كارت شبكة DHCP Server (يا كارت شبكة DHCP Relay Agent) با Network Number هيچيك از Scope هاي تعريف شده همخواني ندارد. در چنين حالاتي DHCP Server نمي‌تواند تشخيص دهد كه از كدام Scope بايد به Client ها سرويس دهد. چنانچه يك Scope بيشتر نباشد و حالت فوق بروز كند باز هم سرور قادر به تخصيص آدرس به Client ها نيست.

مثال: فرض كنيد در مثال ۱، آدرس كارت شبكة DHCP Server بجاي 192.168.1.5 اشتباهاً 192.168.2.5 وارد شود. همين اشتباه به ظاهر كوچك كافي است تا سرور به هيچ ايستگاهي سرويس ندهد چرا كه Scope تعريف شده در آن براي شبكة 192.168.1.0 تعريف شده و نه براي 192.168.2.0.

۵. گاهي اوقات Administrator اشتباهي را مرتكب مي‌شود بدين شرح كه DHCP Relay Agent و DHCP Server را هردو توأماً روي يك كامپيوتر نصب مي‌كند. چون هردو سرويس روي يك شماره Port عمل مي‌كنند (UDP Port 67) لذا مشكل Port Conflict بروز كرده و ممكن است هيچيك كار خود را درست انجام ندهند!

۶. اين احتمال نيز وجود دارد كه يك Firewall روي DHCP Client يا روي DHCP Server يا بين آنها قرار گرفته و مانع عبور ترافيك مربوطه مي‌شود. بايد دقت كرد براي آنكه پروتكل DHCP بتواند كار خود را انجام دهد بايد UDP Ports 67, 68 مسدود نباشد.

براي آزمايش صحت عملكرد ارتباط بين DHCP Client و DHCP Server يك راه ساده نيز وجود دارد كه از روي Client بايد انجام شود: استفاده از فرمان ipconfig /release براي آزاد كردن آدرس اخذ شده از سرور و فرمان ipconfig /renew براي كسب مجدد آدرس و ساير پارامترها. چنانچه فرمان اخير درست كار كند به معني صحت عملكرد DHCP Server است و بشرط آنكه Scope پر نشده باشد بايد مشكل Client هايي را كه نمي‌توانند آدرس بگيرند در خود آنها يا راه ارتباطي آنها با شبكه جستجو كرد.

خود آزمایی و تحقیق

تمرین ۱ :

DHCP را روی سرور نصب و راه اندازی کرده و آدرس IP را از کلیه کامپیوترهای کلاینت پاک کرده و آن را به صورت اتوماتیک فعال کنید .سپس آزمایش کنید که آیا کامپیوتر از سرور IP دریافت کرده یا نه ؟

دوم : از طریق آیکون شبکه روی نوار وظیفه به دوروش یکی به صورت **Command line**

تحقیق:

چگونه می توان یک **IP** بخصوصی را برای یک کلاینت رزور نمود ؟

تمرین ۲:

چگونه می توان از روی سرور **IP** و **Mac address** یک **Client** را پیدا کرد

ضمیمه ۱ برخی از اختصارات شبکه

سر نام	شرح انگلیسی	شرح فارسی
ADSL	Asymmetric Digital Subscriber Line	
COM	Communication	
DSL	Digital Subcarrier Line	
EM	Electronic Mail	
FTP	File Transfer Protocol	
HTML	Hypertext Markup Language	
HTTP	Hypertext Transfer Protocol	
ICP	Internet Central Provider	
ICS	Internet Connection Sharing	
ID	Identifier	
IE	Internet Explorer	
IP	Internet Protocol	
ISDN	Integrated Services Digital Network	
ISP	Internet Service Provider	
LAN	Local Area Network	
NET	Network	
ORG	Organization	
PtP	Point to Point	
TCP	Transmission Control Protocol	
URL	Universal Resource Locator	
VPN	Virtual Private Network	
WAN	Wide Area Network	
WWW	World Wide Web	
DHCP	Dynamic Host Control Protocol	
FDDI	Fiber Distributed Data Interface	
FTP	File Tranfer Protocol	
IPX	Internetwork Packet Exchange	
MAN	Metro Politan Area Network	
OSI		
POP3		
SMTP	Simple Network	