

بزرگترین مرجع کتابهای الکترونیکی فارسی و انگلیسی

بزرگترین مرکز دانلود نرم افزار تخصصی و کاربردی

بزرگترین مرکز دانلود کلیپهای اخلاقی موبایل

..... و

Free کاملاً



Email: Ramin.samad@yahoo.com



شبکه های کامپیوتری

www.IranMeet.com

فهرست ۱

۷	مقدمه
۸	بخش اول مفاهیم شبکه
۹	فصل اول- آشنایی با مفاهیم شبکه و اجزای آن
۹	۱-۱- هدفهای برقراری شبکه کامپیوتری
۱۰	۱-۲- اجزای يك شبکه کامپیوتری :
۱۱	۱-۳- تقسیم بندی شبکه‌های کامپیوتری از نظر ابعاد و گستردگی فیزیکی : LAN , MA, WAN
۱۱	۱-۳-۱- شبکه‌های محلی ، Local Area Networks = LAN :
۱۱	۱-۳-۲- شبکه‌های گسترده ، Wide Area Networks = WAN :
۱۱	۱-۳-۳- شبکه‌های فرا منطقه‌ای ، Metropolitan Area Networks = MAN :
۱۲	۱-۴- تقسیم بندی شبکه‌های کامپیوتری از نظر مدل سرویس دهی (Peer-to-Peer , Server-Based)
۱۳	۱-۴-۱- شبکه Server-Based :
۱۳	۱-۴-۲- شبکه Peer-to-Peer :
۱۳	۱-۴-۳- مزایا و معایب هر يك از مدل‌های SB , PtP
۱۴	۱-۵- انواع سرویس‌هایی که سرور ارائه می دهد
۱۴	۱-۵-۱- File Service
۱۶	۱-۵-۲- Print Service
۱۷	۱-۵-۳- Application Service
۱۸	۱-۵-۴- آشنایی با Database Service
۲۰	۱-۶- طبقه‌بندی محصولات Microsoft در زمینه سیستم عامل ها
۲۱	۱-۷- آشنایی با ویژگی‌های سیستم عامل های شبکه ای
۲۱	۱-۷-۱- Security :
۲۲	۱-۷-۲- Multi Tasking :
۲۲	۱-۷-۳- Multi Processor Support :
۲۳	۱-۷-۴- تحمل خطا Fault Tolerance :
۲۴	۱-۷-۵- نرم افزار تهیه نسخه پشتیبان Backup Utilities :
۲۵	۱-۷-۶- ابزار های مدیریتی Simple and Unified Administrative Tools :
۲۵	۱-۷-۷- قابلیت اطمینان و پایداری Reliable and Stable :
۲۶	۱-۷-۸- پشتیبانی Support :
۲۷	خود آزمایی و تحقیق
۲۸	فصل دوم سیستم های انتقال دیجیتال
۲۸	هدف های رفتاری
۲۸	۲-۱- ارسال موازی (Parallel)
۲۸	۲-۲- ارسال سریال
۲۹	۲-۲-۱- ارسال سریال غیر هم زمان
۲۹	۲-۲-۲- ارسال سریال هم زمان
۳۰	۲-۳- جهت انتقال اطلاعات
۳۰	۲-۳-۱- ارتباط یک طرفه
۳۰	۲-۳-۲- ارتباط دو طرفه غیر هم زمان
۳۱	۲-۳-۳- ارتباط دو طرفه هم زمان
۳۱	۲-۴- سیگنال های اطلاعات
۳۲	۲-۵- پهنای باند
۳۳	۲-۶- نویز
۳۵	خود آزمایی و تحقیق

۳۶	فصل سوم پیکر بندی شبکه و محیط انتقال.....
۳۶	۳-۱- توپولوژی انواع آن.....
۳۶	۳-۱-۱- توپولوژی خطی (Bus) :
۳۸	۳-۱-۲- توپولوژی حلقوی (Ring) :
۳۹	مزایا و معایب حلقوی (یکطرفه) نسبت به خطی :
۴۰	۳-۱-۳- توپولوژی ستاره‌ای (Star) :
۴۲	۳-۱-۴- توپولوژی مش (Mesh) :
۴۳	۳-۲- محیط های انتقال.....
۴۳	۳-۲-۱- گرومبندی محیطهای انتقال.....
۴۴	۳-۲-۲- بررسی محیطهای انتقال "سیمي" یا "کابلي" (Wired).....
۴۵	۳-۲-۴- کابل Twisted Pair = TP :
۴۸	۳-۲-۵- کابل نوري (Fiber Optic = FO) :
۵۰	۳-۳- کابل کشي UTP.....
۵۱	۳-۳-۱- طراحی و اجرای عملیات کابل کشي:.....
۵۱	۳-۳-۲- Duct.....
۵۲	۳-۳-۳- عوامل موثر در تعیین نوع کابل کشي:.....
۵۳	۳-۳-۴- اهمیت Earth:.....
۵۳	۳-۳-۵- تجهیزات مورد نیاز برای اتصال کابل به کانکتور.....
۵۴	۳-۳-۶- ایجاد کابل Straight.....
۵۷	۳-۳-۷- ایجاد کابل X-Over.....
۵۹	۳-۴- کارت شبکه و وظایف آن.....
۵۹	۳-۴-۱- وظایف کارت شبکه.....
۵۹	۳-۴-۲- آدرس شبکه.....
۶۰	۳-۴-۳- ارسال و کنترل داده ها:.....
۶۰	۳-۴-۴- پیکر بندی (configuration) کارت شبکه.....
۶۱	۳-۴-۵- اتصال کارت شبکه.....
۶۱	۳-۵- روشهای دسترسی به خط انتقال.....
۶۱	۳-۵-۱- روش دسترسی چندگانه تشخیص حامل باتشخیص بر خورد (CSMA/CD).....
63	<u>۳-۵-۲- روش عبور نشانه Token Passing</u>
۶۳	خود آزمایی و تحقیق.....
۶۴	فصل چهارم - معماری شبکه.....
۶۴	۴-۱- انواع معماری شبکه و ویژگی های آن ها.....
۶۴	۴-۱-۱- اترنت.....
۶۷	<u>۴-۱-۲- Token Ring</u>
۶۸	<u>۴-۲- FDDI</u>
۶۹	خود آزمایی و تحقیق.....
۷۰	فصل پنجم- آشنایی با پروتکلهای.....
۷۱	۵-۱- NetBEUI = NetBIOS Enhanced User Interface.....
۷۱	۵-۲- IPX/SPX = Internetworking Packet Exchange / Sequential Packet Exchange.....
۷۲	۵-۳- TCP/IP = Transmission Control Protocol / Internet Protocol.....
۷۳	۵-۴- سرویسهای TCP/IP.....
۷۳	۵-۴-۱- FTP = File Transfer Protocol.....
۷۴	۵-۴-۳- HTTP = Hyper Text Transfer Protocol.....
۷۴	۵-۴-۳- SMTP = Simple Mail Transfer Protocol , POP3= Post Office Protocol (version 3).....
۷۵	۵-۴-۴- NNTP = Network News Transfer Protocol.....
۷۶	۵-۴-۵- Telnet = Tele Network.....
۷۸	۵-۴-۶- RDP = Remote Desktop Protocol.....
۷۸	۵-۴-۷- SNMP = Simple Network Management Protocol.....
۸۰	۵-۴-۸- SNTP (NTP) : Simple Network Time Protocol.....
۸۱	۵-۵- آشنایی با مفهوم Host در پروتکل TCP/IP.....
۹۱	خود آزمایی و تحقیق.....

۹۲	فصل ششم- مدل مرجع OSI
۹۳	۶-۱ انواع لایه در مدل OSI
۹۳	۶-۱-۱ لایه فیزیکی
۹۳	۶-۱-۲ لایه پیوند دادها
۹۴	۶-۱-۳ لایه شبکه
۹۵	۶-۱-۴ لایه انتقال
۹۵	۶-۱-۵ لایه جلسه
۹۵	۶-۱-۶ لایه نمایش
۹۶	۶-۱-۷ لایه کاربردی
۹۶	۶-۷ مقایسه دو پروتکل در بخش های مختلف امنیتی
۹۹	خود آزمایی و تحقیق

۱۰۰	فصل هفتم - امنیت در شبکه
۱۰۰	۷-۱ دیواره آتش (Firewall)
۱۰۰	۷-۱-۱ ضرورت استفاده از دیواره آتش
۱۰۱	۷-۱-۲ سفارشی نمودن دیواره آتش
۱۰۲	۷-۱-۳ تنظیمات دیواره آتش در ویندوز:
۱۰۳	۷-۱-۴ تفاوت آنتی ویروس و دیواره آتش:
۱۰۳	۷-۱-۵ فعال نمودن دیواره آتش در روی ویندوز XP
۱۰۵	۷-۱-۶ بازکردن برنامه یا سرویس در دیواره آتش:
۱۰۷	۷-۲ سرویس دهنده Proxy

خود آزمایی و تحقیق

۱۰۹	خود آزمایی و تحقیق
۱۱۰	فصل هشتم- آشنایی با برخی از شبکه های WAN
۱۱۰	۸-۱ DSL
۱۱۰	۸-۱-۱ مزایا و معایب DSL:
۱۱۱	۸-۱-۲ اصول کار DSL:
۱۱۱	۸-۱-۳ سیستم های تفکیک سیگنال در DSL
۱۱۲	۸-۱-۴ انواع DSL:
۱۱۳	۸-۲ شبکه های محلی بدون سیم Wireless LAN
۱۱۵	خود آزمایی و تحقیق

بخش دوم

WINDOWS 2003 SERVER فصل نهم- مدیریت دسترسی به منابع

۱۱۶	فصل نهم- مدیریت دسترسی به منابع
۱۱۷	۹-۱ پوشه های به اشتراک گذاشته شده
۱۱۷	۹-۲ نحوه به اشتراک گذاشتن پوشه ها
۱۱۹	۹-۳ آدرس دهی به شبکه (UNC Path)
۱۲۰	۹-۴ پوشه های به اشتراک گذاشته شده : مخفی (Hidden shares)
۱۲۰	۹-۵ Administrative shares
۱۲۰	۹-۶ مجوز های پوشه های به اشتراک گذاشته شده
۱۲۱	۹-۶ محاسبه مجوز های مؤثر
۱۲۱	۹-۶-۱ محاسبه مجوز در پارتیشن های غیر NTFS
۱۲۲	۹-۶-۲ محاسبه مجوز در پارتیشن های NTFS
۱۲۲	۹-۷ درایو های شبکه
۱۲۴	خود آزمایی و تحقیق

فصل دهم- پیاده سازی و مدیریت چاپ در شبکه

۱۲۵ ۱۰-۱ آشنایی با اجزای چاپ در شبکه
۱۲۶ ۱۰-۲ نصب چاپگرها
۱۲۶ ۱۰-۲-۱ نصب و به اشتراک گذاشتن چاپگر روی سرور چاپ
۱۲۸ ۱۰-۲-۲ نصب چاپگر روی کلاینت
۱۳۰ ۱۰-۳ مجوزهای چاپ
۱۳۱ ۱۰-۴ نحوه اعطای مجوز به کاربران روی چاپگرها
۱۳۱ ۱۰-۵ نحوه مدیریت صف کارهای چاپی
۱۳۲ ۱۰-۶ تغییر آدرس Spool Folder
۱۳۲ ۱۰-۷ آشنایی با مجوزها :
۱۳۳ ۱۰-۷-۱ مجوزها در پارتیشن های NTFS
۱۳۴ ۱۰-۷-۲ وراثت در مجوزهای NTFS
۱۳۴ ۱۰-۸ مجوزهای مؤثر
۱۳۶ خود آزمایی و تحقیق

فصل یازدهم نصب و راه اندازی Active Directory

۱۳۷ ۱۱-۱ آشنایی با Domain و اجزاء Active Directory
۱۳۷ ۱۱-۱ نصب Active Directory
۱۴۴ ۱۱-۳ عضویت کلاینت ها در Domain
۱۴۴ ۱۱-۳-۱ نحوه عضویت کلاینت ها
۱۴۷ ۱۱-۳-۲ انواع log on
۱۴۸ خود آزمایی و تحقیق

فصل دوازدهم مدیریت Account ها

۱۴۹ ۱۲-۱ آشنایی با انواع Account ها و ابزارهای مدیریتی
۱۴۹ ۱۲-۱-۱ انواع Account ها
۱۴۹ ۱۲-۱-۲ ابزارهای مدیریت Active Directory :
۱۵۰ ۱۲-۲ مدیریت کاربران
۱۵۰ ۱۲-۲-۱ ایجادکردن کاربران جدید
۱۵۱ ۱۲-۲-۲ مشاهده مشخصات کاربران و تغییردادن آنها
۱۵۲ ۱۲-۲-۳ کاربر organizational unit :
۱۵۳ ۱۲-۲-۴ تکثیر کاربران
۱۵۴ ۱۲-۳ مدیریت computer Account ها
۱۵۴ ۱۲-۳-۱ کاربر computer Account
۱۵۴ ۱۲-۳-۲ نحوه ایجاد computer Account
۱۵۵ خود آزمایی و تحقیق

فصل سیزدهم مدیریت کاربران

۱۵۶ ۱۳-۱ آشنایی با انواع گروه ها
۱۵۶ ۱۳-۲ Global groups
۱۵۷ ۱۳-۲-۱ Domain Local Groups
۱۵۷ ۱۳-۲-۲ Universal Groups
۱۵۷ ۱۳-۳-۱ روش AGP
۱۵۸ ۱۳-۳-۲ روش A D L P
۱۵۸ ۱۳-۴ آشنایی با گروه های Built-in
۱۵۸ ۱۳-۴-۱ Built-in Global گروه های
۱۵۹ ۱۳-۴-۲ Built-in Domain Local گروه های
۱۵۹ ۱۳-۴-۳ Built-in system گروه های
۱۶۰ ۱۳-۵ پیاده سازی روش های مختلف اعطای مجوز به کاربران
۱۶۰ ۱۳-۵-۱ پیاده سازی روش A G P
۱۶۱ ۱۳-۵-۲ پیاده سازی روش A D L P
۱۶۲ خود آزمایی و تحقیق

فصل چهاردهم - DNS و روش های تبدیل اسم به IP

۱۶۳

۱۶۳	۱۴-۱ کاربردهای DNS
۱۶۳	۱۴-۲ آشنایی با اسامی اینترنتی
۱۶۳	۱۴-۲-۱ Host Name
۱۶۳	۱۴-۲-۱ ساختار اسامی اینترنتی
۱۶۴	۱۴-۳ اجزاء DNS
۱۶۴	۱۴-۳-۱ Name server
۱۶۵	۱۴-۲-۲ Zone
۱۶۵	۱۴-۳-۳ Resource Records
۱۶۵	۱۴-۴ - مراحل تبدیل اسم به IP در اینترنت
۱۶۷	۱۴-۵ - نصب و راه اندازی سرویس DNS
۱۶۷	۱۴-۵-۱ - نصب سرویس DNS
۱۶۸	۱۴-۵-۲ - ایجاد کردن Zone
۱۶۹	۱۴-۵-۳ - ایجاد Resource Records
۱۷۰	۱۴-۵-۴ تست کردن DNS برای انجام عمل Name Resolution
۱۷۱	خود آزمایی و تحقیق

۱۷۲	فصل پانزدهم- DHCP Server مقدماتی
۱۷۲	۱۵-۱ کاربرد DHCP Server
۱۷۲	۱۵-۲ اجزای DHCP
۱۷۴	۱۵-۳ - حالت های مختلف قرار گیری DHCP Server در شبکه
۱۷۵	۱۵-۴ - نصب DHCP Server
۱۷۶	۱۵- ۵ - پیکربندی سرور DHCP
۱۸۹	۱۵-۶ - Backup / Restore اطلاعات DHCP Server :
۱۹۲	۱۵-۷ - عیبیابی DHCP Server :
۱۹۵	خود آزمایی و تحقیق
۱۹۶	منابع
۱۹۷	ضمیمه ۱ برخی از اختصارات شبکه

مقدمه

کتاب شبکه های کامپیوتری شامل دو بخش مفاهیم شبکه و سیستم عامل Windows 2003 Server است که توصیه ما به هنر آموزان محترم ، تدریس موازی این دو بخش در کلاس است .

بدیهی است که کارکردن با یک سیستم عامل شبکه ای مانند Windows 2003 Server بدون یادگیری مقدمات شبکه میسر نخواهد بود ، بنابراین ممکن است هنرآموزان چند هفته اول به طور متوالی بخش مفاهیم شبکه را آموزش دهند . در این مرحله توصیه می شود سیستم عامل Windows 2003 Server روی کامپیوترها نصب شده باشد و هنرجویان بدون اینکه با جنبه های فنی این سیستم عامل درگیر شوند در این محیط یا سیستم عامل Windows XP مطالب را آموزش دیده و فعالیت های عملی را اجرا نمایند در برخی از فصل ها فعالیت عملی کمی ارایه شده و لازم است هنر آموزان متناسب با امکانات موجود فعالیت های عملی مرتبط با موضوع را طراحی و به هنر جویان ارایه نمایند.

در پایان از کلیه عزیزانی که در تدوین این کتاب ، ما را همراهی کرده اند ، سپاسگزار می کنیم .

مؤلفان

هدف کلی

آشنایی با مفاهیم شبکه های کامپیوتری و توانایی نصب شبکه و کار با سیستم عامل متداول شبکه

بخش اول مفاهیم شبکه



www.IranMeet.com

فصل اول- آشنایی با مفاهیم شبکه و اجزای آن

هدف های رفتاری

هنرجو پس از آموزش این فصل می تواند :

- هدف از ایجاد شبکه های کامپیوتری را بیان کند.
- اجزای شبکه های کامپیوتری را شرح دهد.
- تقسیم بندی شبکه های کامپیوتری از نظر ابعاد و گستردگی فیزیکی را شرح دهد.
- تقسیم بندی شبکه های کامپیوتری از نظر مدل سرویس دهی را بیان کند

در دهه اخیر شبکه های کامپیوتری به عنوان یکی از بسترهای سریع و کم هزینه ارتباطی مطرح شده اند . این سیر تدریجی منجر به ایجاد روشی شده است که با سازماندهی مناسب آن می توان سریعتر از هر روش دیگری به اطلاعات مختلف دسترسی پیدا کرد . اطلاعاتی که راه گشای پیوندهای گوناگون فرهنگی ، هنری ، خانوادگی و اجتماعی ، سیاسی ، نظامی و همچنین مبادلات اقتصادی و تجاری اعم از خرد و کلان است و می دانیم که امروزه در عصر اطلاعات بسر می بریم، هرکه با هزینه کمتر و سرعت بیشتر بتواند به آن دسترسی پیدا کند موفق تر است .

تجارت جهانی روی اینترنت و شبکه های کامپیوتری به سرعت به عنوان مفاهیمی کارآمد مطرح می شود . فرقی نمی کند شما در کدام نقطه از کره زمین قرار دارید . در هر لحظه که اراده کنید می توانید اطلاعات مورد نیاز خود را ، حتی بصورت صوت و تصویر زنده از شبکه بدست آورید . اگر نیاز به تبادل مالی داشته باشید باز هم فرقی نمی کند ، پول الکترونیکی در دسترس شماست و به سرعت می توانید با کارت اعتباری خود اقدام به تبادل حفاظت شده ارزی نمایید .

موارد فوق را می توان به صورت زیر خلاصه کرد :

- دسترسی افراد به منابع متنوع در شبکه با در نظر گرفتن سطوح امنیتی قابل تعریف . (اشتراک منابع)
- برقراری سرویس های زنده صوتی تصویری بین افراد یا تیمهای فعال در شبکه .
- تبادل نامه بین افراد مختلف .
- ایجاد بستری مناسب جهت ارتباط با اینترنت بمنظور دسترسی به شبکه جهانی اطلاعات .
- انجام کارهای شخصی و اداری از هر نقطه در شبکه .
- مدیریت و نظارت از راه دور .

۱-۱ - هدفهای برقراری شبکه کامپیوتری

هدف از ایجاد يك شبکه ی کامپیوتری عبارت است از:

- اشتراك منابع
- تبادل پیغام
- مدیریت از راه دور

فعالیت عملی :

- اشتراك منابع : از طريق شبکه به کامپیوتر سرور متصل شده ، پوشه و چاپگر به اشتراك گذاشته شده را ببینید . راهنمایی: ابتدا هنر آموز درس يك پوشه و يك چاپگر را در يكي از سيستم عاملهاي 2003 , XP , 2000 به اشتراك ميگذارد .
- تبادل پیغام : حداقل يكي از برنامه هاي زير را با تايپ نام برنامه در كادر گزينه Run براي انتقال پیغام آزمایش کنید :
 - WinChat.exe
 - Net Meeting (conf.exe)
 - Command Prompt -> net send <computer_name> <message_text>
- مدیریت از راه دور : به کمک هنر آموز درس ، يكي از برنامه هاي RA Net Op School يا dmin , Ideal Administrator , DameWare را اجرا کرده و با نظارت و کنترل از راه دور تحت شبکه را بررسی کنید.

۱-۲ - اجزای يك شبکه کامپیوتري :

شبکه های کامپیوتري از ۴ جزء اصلي تشكيل مي شوند :

۱. Server : سرویس دهنده .
۲. Client : سرویس گیرنده .
۳. Communication Media : محیط انتقال (مثلاً کارت شبکه یا مودم به شبکه متصل می شوند یا سیم)
۴. Protocol : مجموعه قوانینی که با رعایت آنها سرویس دهی در شبکه برقرار می شود .

بديهي است که سرویس دهنده ها و سرویس گیرنده ها باید طبق يك طرح و نقشه مشخص (بوسیله محیط انتقال) به یکدیگر متصل شوند که به این طرح و نقشه اصطلاحاً پیکربندی (Topology) شبکه گفته می شود .

جزئیات هریک از موارد فوق بصورت خلاصه عبارتند از :

Servers (Services) :
& Clients

File , Print , Application , Database , Fax , Email ,
Web , Communication , Time , Remote Access ,
Multimedia , ...

Communication Media :

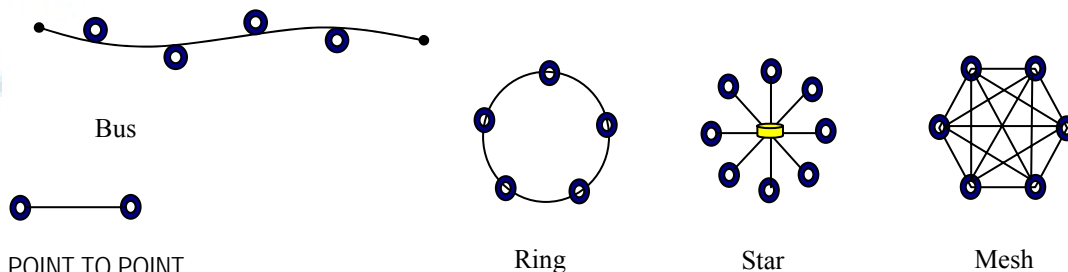
Wired :
 ▪ Metal : Coaxial , Twisted Pair
 ▪ Non Metal : Fiber Optic
 Wireless :
 ▪ Infra Red
 ▪ Laser
 ▪ Radio Waves

Protocols :

TCP/IP , IPX/SPX , NetBEUI , ...

Topologies :

Bus , Ring , Star , Mesh , Point-to-Point



شکل ۱-۱

۱-۳- تقسیم بندی شبکه های کامپیوتری از نظر ابعاد و گستردگی فیزیکی : LAN , MAN, WAN

شبکه ها را از لحاظ اینکه فاصله مابین اجزای آنها چقدر بوده و اصطلاحاً چگونگی پراکندگی کامپیوترها به ۳ دسته کلی تقسیم می کنند :

۱-۳-۱- شبکه های محلی ، Local Area Networks = LAN :

همانطور که از اسم شبکه های محلی پیداست فاصله اجزا در این شبکه ها کم بوده و همه نزدیک به یکدیگر قرار دارند در زیر چند مثال از این شبکه ها ارائه شده است

- شبکه ای متشکل از ۲ کامپیوتر که با یک قطعه کابل به فاصله ۱۰۰ متر آنها را به یکدیگر وصل کرده ایم .
- شبکه کامپیوتری یک اداره کوچک واقع در یک ساختمان متشکل از ۲۰ کامپیوتر فعال (Active Node) .
- شبکه کامپیوتری یک سازمان واقع در ۵ ساختمان نزدیک بهم با ۵۰۰ گره فعال (Active Node) .
- شبکه کامپیوتری یک برج ۱۱۰ طبقه با ۵۰۰۰ سیستم فعال (Active Node) .

۱-۳-۲- شبکه های گسترده ، Wide Area Networks = WAN :

فاصله اجزا در این شبکه ها نسبت به LAN طولانی تر است بطوریکه از نظر حسی دیگر نمی توان آنها را نزدیک به یکدیگر تصور کرد :

مثال ۱ : شبکه ای متشکل از ۲ کامپیوتر که بوسیله مودم از طریق خطوط مخابرات به یکدیگر متصلند .

مثال ۲ : مجموع ۲ شبکه محلی که هر کدام واقع در ساختمان مختص به خود به فاصله ۱۰ کیلومتر از یکدیگر قرار دارند. یکی از ساختمانها واقع در مرکز شهر و دیگری در حاشیه غربی آن بوده و ارتباط آنها از طریق خطوط مخابرات یا روشهای دیگری مانند بیسیم برقرار شده .

مثال ۳ : شبکه کامپیوتری شعبه های مختلف یک بانک در شهر.

مثال ۴ : شبکه کامپیوتری آموزش و پرورش واقع در تهران و شهرستانها .

مثال ۵ : شبکه اینترنت .

۱-۳-۳- شبکه های فرا منطقه ای ، Metropolitan Area Networks = MAN :

این شبکه که در ترجمه های فارسی به شبکه های شهری نیز معروفند از نظر وسعت مابین LAN و WAN قرار دارند .

مثال ۱ : برخی ترجیح می دهند که مثال ۳ از شبکه های WAN را MAN اطلاق کنند .

مثال ۲ : یک مجموعه بزرگ صنعتی یا نظامی واقع در محدوده ۳۰ کیلومتر مربعی که از سوله های متفاوت تشکیل شده و در هر سوله یک LAN موجود است . به مجموع شبکه های این کمپ نیز می توان واژه MAN را اطلاق کرد . البته در این مثال چندین شبکه LAN داریم که در یک کمپ واقع شده اند لذا برخی (از جمله کمپانی معروف Cisco) ترجیح می دهند از واژه Campus LAN یا Campus Area Networks = CAN استفاده کنند .

به هر حال به نظر می رسد تقسیم بندی LAN و WAN کافیست .

شما و همسایه دیوار به دیوارتان و هرکدام یک دستگاه کامپیوتر دارید . از طریق یک کابل ، هر دو سیستم را به هم متصل می‌کنید ، در این حالت شبکه حاصل LAN است .

مثال دیگر- حال فرض کنید که امکان کابل‌کشی مستقیم ندارید. لذا پس از خرید و نصب مودم دو کامپیوتر مثال بالا را از طریق شبکه 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 می کند نه فاصله ظاهری بین کامپیوترها .

مقایسه شبکه های LAN و WAN

از نظر سرعت در شبکه های LAN و WAN می توان گفت: سرعت به ابعاد و گستردگی شبکه بستگی ندارد اما معمولاً پیاده سازی تکنولوژی با سرعت بالا در ابعاد LAN کم هزینه تر و ساده تر از WAN انجام می‌شود لذا معمولاً سرعت در شبکه های LAN از WAN بیشتر است اما این یک قاعده کلی نیست . به عنوان مثال می توان شرایط زیر را در نظر گرفت:

- سرعت LAN بیشتر از WAN : وقتی با مودم به اینترنت متصل می‌شوید بعنوان یکی از اعضای شبکه WAN محسوب شده و سرعت با مودم های خوب حدوداً 40 Kbps است . از طرفی کمترین سرعت در شبکه های 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 شاهرگهای اصلی اینترنت یا در ارتباطات میان قاره ای سرعت عموماً بیشتر از 155 Mbps است و اگر آنرا با سرعت معمول در شبکه های LAN یعنی 100 Mbps مقایسه کنیم می‌بینیم که در همان حد یا بیشتر است .

انواع شبکه های بی سیم از نظر وسعت

1-WLANS: 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 .

2-WPANS: . 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 .

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

4-WWANS: . 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 G2 (نسل دوم) معروف هستند .

۴-۱- تقسیم بندی شبکه های کامپیوتری از نظر مدل سرویس دهی (Peer-to-Peer , Server-Based)

مفهوم Server و Client : سرویس دهی در یک شبکه به وسیله ی سیستمهایی صورت می‌گیرد که در اصطلاح سرویس دهنده (Server) نامیده می‌شوند . سیستمهایی

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

۱-۴-۲- شبکه Peer-to-Peer :

اگر در شبکه اي ، 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 دهی در آن شبکه Peer-to-Peer است (به اختصار P2P)

در مدل SB تجمع سرویسها روی سرویس دهنده s بوده و Clients هیچگونه سرویسی ارایه نمی دهند اما در مدل P2P هر سیستم میتواند علاوه بر دریافت سرویس خود سرویس دهنده نیز باشد یعنی هر کامپیوتر هم سرویس گیرنده و هم سرویس دهنده است.

در يك سایت تعدادي از سیستمها فقط سرویس دهنده و بقیه فقط سرویس گیرنده هستند . مدل سرویس دهی SB است اما در يك سایت دیگر هرکدام از کاربران منابعي مانند پوشه ها یا چاپگرها را برای بقیه به اشتراك گذاشته اند . مدل سرویس دهی P2P است .

فرض کنید در ایران شهر تعدادي مغازه و مراکز خدماتي وجود دارد و تعدادی مشتری و استفاده کننده این خدمات هستند . مدل سرویس دهی آنها SB خواهد بود.

۱-۴-۳- مزایا و معایب هریک از مدلهاي SB , P2P

در مدل SB چون تمرکز سرویسها فقط در نقاط مشخصی است یعنی سرویس دهنده ها بنابراین مدیریت سرویس ساده تر است . این مدیریت شامل کنترل دسترسی و امنیت ، نحوه ارایه ی سرویس به کاربران ، مونیتورینگ سرویس و چگونگی بهره برداري از آن و پارامترهاي دیگریست که بر احي می توان آنها را در سرورها کنترل کرد در صورتیکه انجام این عملیات در مدل P2P پیچیده است ، چرا ؟ بعنوان مثال تصور کنید در يك شبکه حدود ۷۰۰ سیستم داشته باشیم که مدل سرویس دهی آنها P2P باشد ، یعنی باید روی ۷۰۰ سیستم عملیات هاي فوق را انجام دهیم ! که عملی هزینه بر و کسل کننده است.

مدل Server Based :

مزیت : مدیریت جامع و متمرکز . مناسب برای استفاده در شبکه هاي متوسط و بزرگ .

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

مدل Peer-to-Peer :

مزیت : چون مجموعه سرویسها در نقطه خاصی متمرکز نشده اند بلکه احتمالاً در نقاط مختلفی از شبکه پراکنده هستند بنابراین در صورت بروز مشکل ، سرویس دهی به صورت ناگهانی دچار اختلال کلی نمی شود .

عیب : مدیریت آن پیچیده بوده و هنگامی عملی است که تعداد سیستمها زیاد نبوده (شبکه هاي کوچک) یا اینکه کاربران در مورد نحوه اشتراك گذاری منابع و مدیریت سرویسها آموزشهاي لازم را دیده باشند .

۵-۱- انواع سرویسها یی که سرور ارایه می دهد

همانطور که اشاره شد ، هر شبکه کامپیوتری از ۴ جزء تشکیل شده که به ترتیب از سمت چپ عبارتند از :

Client , Server , Communication Media & Protocol . مجدداً یادآوری می‌کنیم که سرویس دهی در یک شبکه به وسیله ی سیستمهایی صورت می‌گیرد که در اصطلاح " سرویس دهنده" نامیده می‌شوند سیستمهایی که از این سرویسها استفاده کنند اصطلاحاً سرویس گیرنده نامیده می‌شوند . معمولاً در یک شبکه هر کامپیوتری که از نظر سخت افزاری نسبت به سایر کامپیوترها قوی تر باشد به عنوان سرویس دهنده در نظر گرفته می شود، البته نوع انتخاب بستگی کامل به نوع سرویس خواهد داشت .

در این قسمت می‌خواهیم با انواع سرویسها آشنایی بیشتری پیدا کنیم . بدیهی است با شناخت سرویسها مشتری آنها یعنی Clients نیز شناخته خواهد شد .

سرویسهایی که در شبکه ها ارایه می‌شوند ممکن است بسیار متنوع باشند هرچه تنوع مشتری و نیازهای او بیشتر باشد تنوع سرویس نیز به همان نسبت افزایش می‌یابد . آشنایی با همه سرویسها نیاز به بحث طولانی خواهد داشت با این حال معروفترین آنها را نام برده و چهار مورد را که کاربرد بیشتری دارند معرفی می‌کنیم :

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

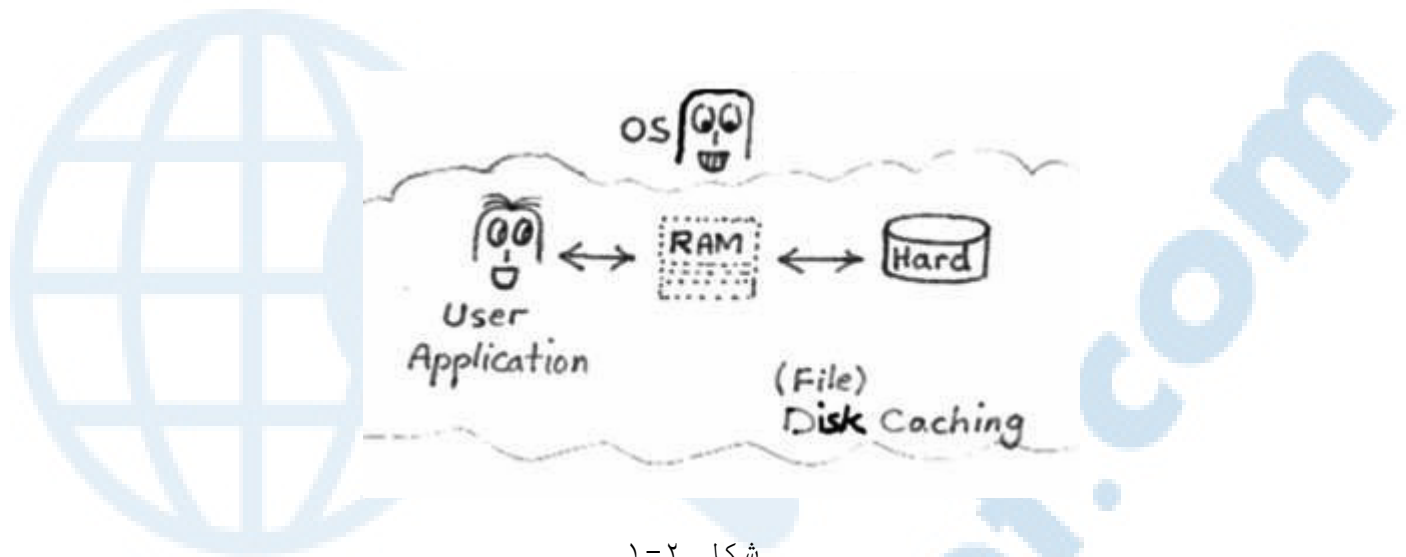
۱-۵-۱ - File Service

بطور مختصر و ساده File Server یعنی " سریس دهنده فایل " . سخت‌افزاری است با وسایل ذخیره‌سازی حجیم ، سریع و پایدار (مانند دیسک سخت) که روی آن انواع پرونده‌ها با در نظر گرفتن سطوح امنیتی ، به وسیله ی کاربران از نقاط مختلف شبکه ذخیره و مورد استفاده قرار می‌گیرد . البته سخت‌افزار به تنهایی کافی نبوده و باید نرم‌افزار خاص File Service نحوه ذخیره‌سازی ، بازیابی و مدیریت اینگونه کارها را به نحو احسن در شبکه انجام دهد .

برای ذخیره و بازیابی اطلاعات هرچند دیسک سخت وسیله‌ای نسبتاً سریع برای ذخیره‌سازی و بازیابی اطلاعات است اما یک وسیله الکترو مکانیکی بوده و سرعت این وسایل هرچه قدر هم زیاد باشد ، نسبت به وسایل ذخیره‌سازی الکترونیکی محض مانند RAM بسیار ناچیز است لذا در اینگونه سرورها از حافظه RAM برای ذخیره‌سازی و بازیابی موقت اطلاعات کاربران تا هنگامی که سرور روشن است استفاده می‌شود . بعبارتی کاربر یا برنامه‌ای که با فایل ذخیره شده روی دیسک سخت کار دارد بجای در گیر شدن با یک وسیله مکانیکی ، عملیات خود را بطور نامحسوس روی RAM انجام می‌دهد و لذا سرعت به نحو چشمگیری افزایش می‌یابد . بدیهی است سیستم عامل (یا نرم افزار فایل سرور) در زمانی مناسب بطور خودکار تغییرات انجام شده در RAM را ، روی دیسک سخت منتقل می‌کند چرا که محل اصلی و پایدار برای ذخیره سازی اطلاعات است .

استفاده از RAM را برای ذخیره سازی موقت اطلاعات دیسک سخت که بمنظور افزایش سرعت انجام می‌شود اصطلاحاً File Caching یا Disk Caching می‌گویند .

^۱ - معمولاً در سرور ها برای نگهداری اطلاعات زیاد در حد ترا بایت از دستگاهی به نام (NAS Server (network Attached Storage Server استفاده می شود



شکل ۱-۲

برخی از فایل-سرورها عملیات تکمیلی دیگری را نیز انجام می‌دهند مانند :

- فشرده سازی خودکار اطلاعات هنگام ذخیره سازی پرونده‌ها روی دیسک بمنظور کاهش حجم فضای اشغالی .
- رمزنگاری اطلاعات برای هرکاربر با کلید رمز جداگانه بمنظور حفظ اطلاعات شخصی و محرمانه .
- این عملیات تکمیلی هرچه که باشند باری اضافه بر دوش پردازنده سرور محسوب می‌شوند و اگر CPU قوی نباشد عملیات به کندي صورت گرفته ، شبکه را با پاسخهای توأم با تاخیر مواجه می‌کند .

ویژگی های يك File Server از نظر سخت‌افزاری :

- وسایل ذخیره‌سازی حجیم ، سریع و پایدار که در حال حاضر معمولاً از دیسک سخت استفاده می‌شود .
- حافظه RAM به میزان کافی برای انجام عملیات File Caching .
- پردازنده سریع (CPU) برای آن دسته از سرورهایی که عملیات تکمیلی مانند فشرده سازی یا رمزنگاری را انجام می‌دهند . البته بطور کلی وجود يك پردازنده سریع در سرور مخصوصاً آنهایی که سیستم عامل گرافیکی دارند مانند Windows لازم است اما نقش آن به اندازه موارد اول و دوم در اولویت قرار ندارد .

نکته :

در مجموع برای تمامی سرورها باید دقت داشته باشیم که قدرت سخت‌افزاری سرور ، نقطه ارتباط سرور با شبکه (مانند کارت شبکه) ، بستر سخت‌افزاری شبکه و سرعت آن برای ارایه ی يك سرویس سریع و مطمئن بسیار تعیین کننده است و این موضوع بعداً مورد بحث بیشتری قرار می‌گیرد .

اگر در يك File Server حین انجام کار برق بطور ناگهانی قطع شده یا سرور بطور غیرعادی خاموش یا Reset شود برخی از تغییرات که در حافظه RAM انجام شده و هنوز به وسیله ی OS به دیسک سخت منتقل نشده‌اند از بین می‌رود بعبارت فنی عملیات File Caching ناقص می‌ماند لذا بسیار مهم است که سرورها اولاً به UPS متصل بوده ، ثانیاً هیچگاه آنها را بطور غیرعادی خاموش یا Reset نکنیم بلکه باید طور معمولی خاموش شوند .

فرایند خاموش شدن معمولی (Shutdown) عبارت است از بسته شدن کلیه پرونده‌های مورد استفاده ، انتقال اطلاعات تغییر یافته از RAM به دیسک سخت. همانطور که شما پس از پایان ساعات کار ، محل کار خود را مرتب می‌کنید ، سیستم عامل هم باید اطلاعات را جمع و جور و مرتب کند . هرگونه

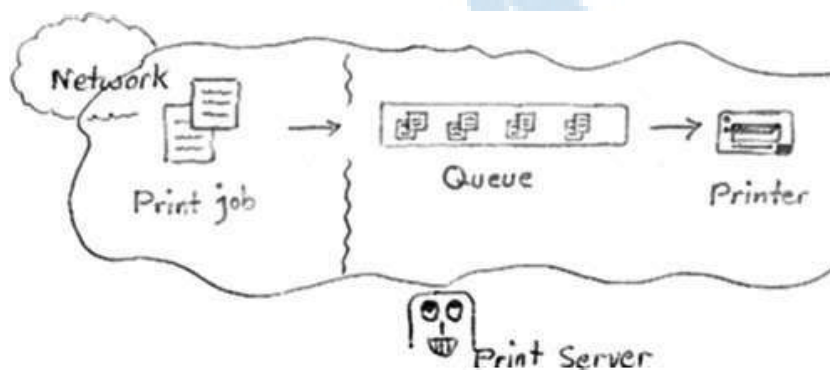
راه اندازی غیرعادی (مانند فشردن کلید روی Case) به منزله رها کردن محل کار با یک میز نامرتب و بهم ریخته است.

فعالیت عملی : آشنایی با File Server در Microsoft :

یک پوشه حاوی چندین فایل متنوع را به کمک هنر آموز درس در سیستم عامل 2000, XP یا 2003 به اشتراک گذاشته و از طریق شبکه به آن دسترسی پیدا کنید. در این بخش نیازی به درگیر شدن در جزئیات Security و غیره نیست و هدف تثبیت مفهوم در ذهن هنجروست. در این صورت هر کامپیوتری که پوشه خود را برای استفاده دیگران به اشتراک می‌گذارد در عمل تبدیل به یک File Server شده حتی اگر سیستم عامل آن به ظاهر سرور نباشد (مثلاً XP_Professional یا 2000_Professional باشد)

۲-۵-۱- Print Service

این سرویس که معمولاً به وسیله ی Print Server ارائه می‌شود سخت افزاری است (همراه با نرم افزار) که تعدادی چاپگر متناسب با نیازهای کاربران تحت کنترل آن قرار دارد. کارهای چاپی (Print Jobs) که در نقاط مختلف شبکه به وسیله ی کاربران ارسال می‌شود به وسیله ی این سرور دریافت شده و ابتدا در یک صف (Queue) قرار می‌گیرد سپس کار چاپی از صف تحویل چاپگر مربوطه می‌شود. چاپگرها ممکن است از نظر فیزیکی مستقیماً به سرور متصل بوده یا غیرمستقیم از طریق سیستم‌های دیگر تحت مدیریت سرور باشند، مهم آنست که چاپگرها تحت کنترل Print_Server اداره می‌شوند.



شکل ۳-۱

در سرورهای چاپ حرفه‌ای که کارهای چاپی ممکن است حجیم و از نظر تعداد زیاد باشند، محل فیزیکی ذخیره‌سازی اطلاعات صف (Queue) روی دیسک سخت است لذا برای یک سرور چاپ حرفه‌ای آنچه که در درجه اول ویژگی سخت‌افزاری قرار دارد وجود فضای کافی روی یک دیسک سخت خوب و مطمئن است. RAM و CPU در درجه دوم و سوم اهمیت قرار می‌گیرند.

در مورد سرعت یک Print Server باید توجه داشت که سرعت چاپ بستگی شدید به سرعت فیزیکی چاپ روی کاغذ دارد بعبارتی سرورهای چاپ حتی ضعیف‌ترین آنها دارای توانایی نسبتاً سریع دریافت تمامی کار چاپی و قراردادن آنها در صف دارا هستند و آنچه که تعیین‌کننده اصلی سرعت است خصوصیت چاپگر است، بنابراین:

ویژگی های یک Print Server از نظر سخت‌افزاری

- دیسک سخت با ظرفیت مناسب و مطمئن برای ذخیره‌سازی اطلاعات صف (Queue).
- حافظه RAM کافی برای انجام عملیات احتمالی Caching (به اندازه File_Server اهمیت ندارد مگر آنکه Print_Server صف را مستقیماً در RAM ذخیره کند)
- پردازنده سریع (CPU) برای انجام عملیات تبدیل فرمت‌های چاپی خاص (Rendering) قبل از ارسال به چاپگرهای خاص. (در خیلی از موارد نیازی

نیست چرا که عملیات Rendering معمولاً در ایستگاه ها توسط ارسال کننده Print_Job صورت می‌گیرد)

فعالیت عملی : آشنایی با Print Server در Microsoft :

ابتدا يك چاپگر را به كمك هنر آموز درس در سیستم عامل XP, 2000 یا 2003 تعريف کرده سپس به اشتراك گذاشته و از طريق شبکه به آن دسترسی پیدا کنید . در این بخش نیازی به درگیر شدن در جزئیات تنظیمات چاپگر ، Security و غیره نیست و هدف تثبیت مفهوم در ذهن هنرجوست . در این حالت هر کامپیوتري که چاپگر خود را براي استفاده دیگران به اشتراك می‌گذارد در عمل تبدیل به يك Print Server شده حتي اگر سیستم عامل آن به ظاهر سرور نباشد (مثلاً XP_Professional یا 2000_Professional باشد)

Application Service - ۱-۵-۳

این سرویس معمولاً به وسیله ی Application Server ارائه می‌شود. فرض کنید که در شبکه سایت هنرستان متشکل از کامپیوترهاي Windows قرار دارید . آيکن مربوط به Network_Neighborhood یا My_Network_Places را باز کرده ، لیستی از کامپیوترهاي موجود در شبکه را می‌بینید . یکی از این کامپیوترها بنام «کامپیوتر هنر آموز» است . کنجکا و شده و روی آيکن مربوط به آن Double-Click می‌کنید . کامپیوتر باز شده و مثلاً يك پوشه را روی آن می‌بینید که به اشتراك گذاشته شده ، عبارتی کامپیوتر هنر آموز يك File-Server است . پوشه Share شده را باز کرده و داخل آن چندین فایل متنوع با پسوندهاي .bmp و .txt . یکی از فایل ها را انتخاب کرده و روی آيکن مربوطه Double-Click کنید ، می‌بینیم که فایل باز می‌شود . سوال اینست که فایل مذکور کجا اجرا می‌شود ؟ روی کامپیوتر هنر آموز یا روی کامپیوتر شما (که مثلاً نام آن PC1 است) ؟

با کمی دقت پاسخ خواهید داد که روی PC1 . درست است چرا که کامپیوتر هنر آموز فقط يك File Server است و نه يك Application Server . قرار نیست که کامپیوتر هنر آموز برای ما فایل ها را باز کند یا برنامه ها را اجرا کند (مگر زمانی که کسی مستقیماً و نه از طریق شبکه روی خود کامپیوتر هنر آموز اقدام به اجرای برنامه کند) . کامپیوتر هنر آموز تنها محل نگهداری فایل مذکور است . وقتی کسی از طریق کامپیوتر خود (مثلاً PC1) و بواسطه شبکه روی آيکن فایلی که روی کامپیوتر هنر آموز قرار داشته و به اشتراك گذاشته شده Double-Click می‌کند ، این فایل یا برنامه و عبارتی Application از کامپیوتر هنر آموز به PC1 منتقل شده و روی پردازنده ، حافظه و خلاصه کامپیوتر ایستگاه PC1 اجرا می‌شود .

حال اگر بخواهیم فایل روی کامپیوتر هنر آموز اجرا شده و PC1 که به هر دلیلی امکان اجرای آن برنامه را ندارد از آن استفاده برد چه باید کرد ؟ پاسخ در استفاده از Application Server است .

تعريف : Application Server کامپیوتریست که نرم افزارهاي کاربردي (Applications) را به درخواست کاربران برای آنها اجرا کرده و نتایج حاصل از اجرا را روی کامپیوتر خودشان نمایش می‌دهد . هسته مرکزی اجرای Application روی سرویس دهنده است و نه سرویس گیرنده . در اینجا سرویس گیرنده تنها بعنوان يك درخواست کننده برای اجرا عمل کرده و بقیه بعهده سرویس دهنده است . اینکه چند درصد کار به وسیله ی سرور انجام می‌شود و چند درصد به وسیله ی ایستگاه ، متغیر بوده و بستگی به ماهیت Application و عملکرد سرویس دهنده دارد . گاهی اوقات ممکن است همه Application روی سرویس دهنده اجرا شده و ایستگاه فقط نتایج را استفاده کند و گاهی ممکن است بخش کوچکی از اجرای Application بعهده سرویس گیرنده بوده و بقیه بعهده سرور باشد . به عنوان مثال در برخی از Game Net ها بازی ها در سرور نصب می شود و بقیه

کامپیوتر ها که به عنوان سرویس گیرنده هستند از برنامه استفاده می کنند.

برخی از دلایل استفاده از App Server :

- امکانات سخت افزاری سرویس گیرنده ممکن است برای اجرای مستقیم برنامه کافی نباشد. مانند ATM (عابر بانک)
- چون برنامه عمدتاً بطور متمرکز روی یک نقطه یعنی سرویس دهنده اجرا می شود بنابراین مدیریت قویتری را می توان روی آن اعمال کرد.
- در نرم افزارهای تحت شبکه ای که برنامه تکتک روی ایستگاه های مختلف بطور کامل اجرا شده اما اطلاعات آنها در یک نقطه متمرکز (مانند File Server) قرار دارد و از طرفی حجم تبادل اطلاعات مابین برنامه اجرایی روی ایستگاه ها و File Server زیاد باشد باعث می شود تا ترافیک شبکه بسرعت افزایش پیدا کرده و ضمن اشباع ترافیکی، مشکلات امنیتی را نیز در پی داشته باشد لذا در اینگونه موارد بهتر است که برنامه بجای اجرای تکتک روی همه ایستگاه ها فقط روی App Server اجرا شده تا از پراکندگی تبادل اطلاعات مابین ایستگاه های مختلف و File Server جلوگیری بعمل آمده و ترافیک تنها مابین Application Server و File Server باشد. در ضمن کنترل اطلاعات نیز قویتر صورت می گیرد. در اینگونه موارد معمولاً App Server و File Server از نظر فیزیکی روی یک کامپیوتر قرار می گیرند. مثالی عملی از کاربرد اخیر سرورهایی هستند تحت عنوان Database Server که موضوع بحث بعدیست.

ویژگیهای یک Application Server از نظر سخت افزاری

- پردازنده قدرتمند، چرا که ممکن است تعداد زیاد و متنوعی از نرم افزارها را بخواهد برای کاربران اجرا کند. حتی ممکن است نیاز به کامپیوتر های چند پردازنده (Multi Processor) باشد.
- حافظه RAM زیاد چرا که برنامه ها هنگام اجرا همگی در RAM قرار می گیرند.
- دیسک سخت و سایر منابع دیگر بسته به نیاز و تنوع برنامه ها.

فعالیت عملی : آشنایی با Application Server در Microsoft :

ابتدا (روی کامپیوتری که بعنوان سرویس دهنده در نظر گرفته اید) سرویس Remote Desktop Server را به کمک هنر آموز درس در سیستم عامل Server 2003 فعال کرده (در Server 2000 بنام Terminal Server) سپس روی ایستگاه برنامه Remote Desktop Client را واقع در Programs->Accessories->Communications اجرا کنید سپس به سرور متصل شده، با نام Administrator وارد شده و Desktop مربوط به سرور را در اختیار بگیرید. چون این Desktop مربوط به سرور است و نه ایستگاه لذا هر برنامه ای که اجرا می کنید (مانند ماشین حساب) در واقع روی سرور اجرا می شود. به کمک Task Manager نشان دهید که ماشین حساب در سرور اجرا شده نه در ایستگاه. در این حالت هر کامپیوتری که Desktop خود را برای استفاده دیگران در اختیار آنها می گذارد در عمل تبدیل به یک Application Server شده حتی اگر سیستم عامل آن به ظاهر سرور نباشد (مثلاً XP Professional). با توجه به محدودیت سرویس Remote Desktop Server که در حالت خاص خود فقط اجازه اتصال همزمان ۲ ایستگاه را می دهد لذا بهتر است این تمرین در گروههایی مرکب از ۳ کامپیوتر انجام شود که یکی از آنها دارای سیستم عامل 2003 بوده، سرویس Remote Desktop را روی آن فعال شده و بعنوان سرور عمل می کند. ۲ کامپیوتر دیگر نیز بعنوان سرویس گیرنده با هر سیستم عامل دلخواهی از مجموعه Microsoft می توانند باشند حتی 98. فقط باید نرم افزار Remote Desktop Client روی آنها نصب باشد.

۴-۵-۱- آشنایی با Database Service که معمولاً به وسیله Database Server ارائه می شود :

فرض کنید که هنگام ثبت نام است و طی ۳ روز ۱۰۰۰ هنرجوی جدید می‌خواهند نام خود را در دوره‌های آموزشی مورد پذیرش ثبت کنند. برای جلوگیری از ازدحام، ۳ نفر از پرسنل موسسه را همزمان بعنوان مسوول در نظر گرفته و به هر کدام یک کامپیوتر مجهز به نرم افزار ثبت نام را تحویل می‌دهیم. با توجه به اینکه هر ۳ نفر باید روی یک بانک اطلاعاتی مشترک کار کنند لذا یک شبکه ساده متشکل از ۳ کامپیوتر مذکور برپا کرده و ضمناً یک FileServer برای ذخیره سازی بانک اطلاعاتی در نظر می‌گیریم یعنی در مجموع ۴ کامپیوتر. هر کدام از افراد، نرم افزار ثبت نام را جداگانه روی ماشین خود اجرا کرده، از طریق شبکه به بانک مربوطه که مشترک بوده و روی FileServer ذخیره شده دسترسی پیدا کرده و عملیات ثبت، گزارش‌گیری و... را انجام می‌دهند. در پایان کار ثبت نام، مدیر موسسه گزارشاتی را مبنی بر تنوع رشته‌های نام‌نویسی شده، سن و سال هنرجویان، میزان شهریه پرداختی و... را درخواست می‌کند. هر یک از پرسنل مسوولیت تهیه بخشی از گزارش را تقبل کرده، نرم افزار خود را اجرا می‌کنند و مشغول تهیه گزارش می‌شوند. در این قسمت برای ادامه کار می‌توان دو حالت متفاوت را در نحوه کار نرم افزار متصور شد:

حالت اول: هر یک از برنامه‌های اجرا شده روی کامپیوترها، بانک اطلاعاتی موجود بر FileServer را باز کرده، کلیه اقلام اطلاعاتی آنرا از طریق شبکه به کامپیوتر خود انتقال داده (دفعته یا تدریجی) سپس اطلاعات را در کامپیوتر خود بررسی کرده و در صورت صدق در شرایط آنرا چاپ کند. در این حالت اگر بعنوان مثال ۱۰۰۰ رکورد در بانک موجود است، هر کامپیوتر باید همه آنها را از طریق شبکه به کامپیوتر خود انتقال داده و عملیات پردازش را روی ماشین خودش انجام دهد (البته می‌توان از تکنیک‌هایی استفاده کرد که نیاز به انتقال همه رکوردها نباشد). چون ۳ کامپیوتر مشغول به گزارش‌گیری هستند لذا تقریباً ۳۰۰۰ رکورد اطلاعاتی در ترافیک شبکه سهم می‌شوند. ممکن است با خود بگوییم که ۳۰۰۰ رکورد را کامپیوترها سریع می‌خوانند، و زمانی طول نخواهد کشید. این طرز فکر درست است اما تصور کنید که با یک بانک اطلاعاتی حجیم درگیر شویم مثلاً بانک اداره ثبت احوال با فرض شصت میلیون رکورد! در اینجا دیگر نمی‌توان مابین ترافیک شصت میلیون رکورد در شبکه و ۳ برابر آن یعنی یکصد و هشتاد میلیون تفاوت قائل نشد.

حالت دوم: مشکلی که در حالت قبلی وجود دارد آنست که حجم ترافیک شبکه با افزایش اطلاعات بانک و تعداد کاربران بسرعت زیاد شده و باعث اشباع شبکه می‌شود بنابراین بهتر است هر کامپیوتر بجای آنکه خودش رأساً مبادرت به خواندن اطلاعات بانک از File Server و پردازش آن در ایستگاه کند از سرور بخواهد که عملیات را انجام دهد. بدین ترتیب که یک Application Server روی همان File Server نصب کرده سپس از ایستگاه به سرور فرمان می‌دهیم که سرور اطلاعات را جستجو کند و فقط نتایج را برای ما ارسال نماید نتیجه‌ای که از این کار به دست می‌آید آنست که دیگر هیچ نیازی به انتقال حجیم اطلاعات در شبکه و پردازش آن در ایستگاه نبوده لذا هم ترافیک شبکه به حداقل می‌رسد و هم پردازش ایستگاه سبک می‌شود چرا که ایستگاه فقط نتایج را از سرور دریافت کرده و برای کاربر نمایش می‌دهد، بنابراین:

تعریف: به یک Application Server که روی بانک‌های اطلاعاتی کار می‌کند اصطلاحاً Database Server (به اختصار DB Server) می‌گوییم. پس می‌بینیم که DB Server یک سرور جدید نیست بلکه همان AppServer است که برای کار روی بانک‌های اطلاعاتی طراحی شده و به عبارتی همان کاربرد سوم App Server است که در بخش مربوطه اشاره شد. از سرورهای معروف بانک‌های اطلاعاتی می‌توان به Oracle و Microsoft SQL Server اشاره کرد که با آنها در درس بانک اطلاعاتی آشنا می‌شوید.

ویژگیهای سخت‌افزاری یک Database Server

ویژگی های این سرور نیز همانند App Server است علاوه بر این دیسک سخت هم مثل CPU و RAM در درجه اول اهمیت قرار می‌گیرد. پس توجه همزمان به هر ۳ پارامتر مهم است.

سرور ها به چه سیستم عاملی نیاز دارند؟
اما پاسخ به این سوال مستلزم آشنایی و طبقه‌بندی محصولات سیستم عامل و ویژگیهای مربوطه است که خود بحث مفصلی است لذا به تیزر آنها اکتفا کرده و بحث پیرامون آنها را به توضیحات هنر آموز درس و تحقیقات خواننده واگذار می‌کنیم، البته در این مرحله نیاز به دانستن و پرداختن به جزئیات فنی سیستم عاملها نبوده، آشنایی کلی، کاربرد و عمومیت حوزه مصرفی آنها کفایت می‌کند.

۶-۱- طبقه‌بندی محصولات Microsoft در زمینه سیستم عامل ها

شرکت مایکروسافت بطور کلی در مورد سیستمهای عامل، ۲ دسته محصول ارائه کرده است:

- سیستم عاملهایی که برای نصب و کاربرد در سرویس گیرنده.
- سیستم عاملهایی که برای نصب و کاربرد در سرور.
- در متن زیر طبقه بندی این سیستم 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 که دیده می‌شود ویندوز 2000 بنام NT 5.0 ، XP بنام NT 5.1 و 2003 بنام NT 5.2 نیز خوانده می‌شوند. در کل به هر ۳ سیستم عامل ، خانواده NT 5.x گفته می‌شود.

XP فقط در گروه سرویس گیرنده و 2003 فقط در گروه Server قرار گرفته .
بعبارت دیگر XP نسخه سرور نداشته و 2003 نیز نسخه Client ندارد.
هرچند خانواده 9x و XP جایی در گروه سرورها ندارند اما خیلی از کاربران تجربه اشتراك گذاري پوشهها و چاپگرهاي خود را در آنها داشته‌اند، يعني کامپيوتري که سیستم آن مثلاً 98 است تبدیل به File Server یا Print Server می‌شود. این موضوع ناقض طبقه‌بندی فوق نیست ، بعبارتی هرچند 98 هم می‌تواند در مواردی تبدیل به سرور شود اما قرار نگرفتن آن در گروه سرورها بمعنی آنست که 98 یا XP عمدتاً برای کاربرد در ایستگاه ها طراحی شده‌اند.

مایکروسافت فقط خانواده NT را برای کاربرد در سرورها پیشنهاد داده است.

نام برخی از محصولات کمپانیهای دیگر در زمینه سیستم عامل ها (که عمدتاً برای کار در سرورها استفاده می‌شوند)

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

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

...
خانواده UNIX تقریباً در همه زمینها کاربرد دارد . امروزه در ایران شبکه‌های بانکی ، شرکت نفت ، شهرداری ، بیمه و . . . همگی از این خانواده بعنوان سیستم عامل اصلی در سرورها بهره می‌برند .
Novell در ایران عمدتاً بعنوان File Server و تا حدی Print Server بکار می‌رود هرچند که در خیلی از مکانها Database Server نیز روی Novell اجرا می‌شود .

۷-۱- آشنایی با ویژگیهای سیستم عامل های شبکه ای

سیستمهای عامل که در شبکه استفاده می‌شوند باید ویژگیهایی را افزون بر سیستمهای عامل که در کاربردهای خانگی مورد استفاده قرار می‌گیرند داشته باشند . هرچند امروزه اکثر کاربران خانگی به محض اتصال به اینترنت عملاً بعنوان کاربر شبکه محسوب می‌شوند بنابراین خصوصیات سیستمهای عامل شبکه برای سیستمهای خانگی نیز (در حدی کمتر) معنی پیدا می‌کند .
برخی از این ویژگیها به ترتیب اهمیت عبارتند از :

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

با برخی از این ویژگیها قبلاً در درس سیستم عامل آشنا شده اید .

۱-۷-۱ - Security :

امنیت ، مهمترین ویژگی است . متأسفانه دنیا ایده‌ال نیست لذا در نظر گرفتن مسایل امنیتی هرچند که باعث کندي سیستم می‌شود اما بعنوان رکن کار هر سیستم عامل شبکه محسوب می‌شود . امنیت برای سیستم عامل را می‌توان در حوزه‌های مختلفی بررسی کرد بعنوان مثال :

الف) امنیت در حوزه دسترسی به دیسک و فایل-سیستم (Disk & File-System Security)
ب) امنیت در حوزه عملیاتی که کاربرد عام دارند مانند :

- تغییر ساعت سیستم (Changing System time)
- نصب نرم افزار ، سخت افزار و انجام تنظیمات (Hardware & Software Installation)
- اجرای برنامه‌ها و تغییر در پارامترهای مربوطه (Running Applications & Services)

ج) امنیت در حوزه شبکه و اطلاعات تبادل (Network Security)
د) امنیت در ورود به سیستم (System Login)

مثال : Dos ، Win 3.1 و خانواده 9x جزو آندسته از سیستمهایی هستند که امنیت چندانی مخصوصاً در حوزه‌های "الف" ، "ب" و "ت" ندارند . همه می‌دانیم که پس از روشن کردن يك کامپیوتر با سیستم 98 براحتی می‌توان بدون هیچگونه گذر واژه ای وارد آن شده ، به هرجا روی دیسک دسترسی پیدا کرده (که با FAT آماده شده) ، هربرنامه‌ای را نصب ، حذف یا اجرا کرده و هرگونه تغییر سخت‌افزاری را اعمال کرد ! در صورتیکه این امر در خانواده NT براحتی امکان‌پذیر نیست ، فقط کاربرانی که عضو گروه Administrators باشند توانایی تام در انجام عملیات فوق را دارا هستند .

نکته : کاربرانی که هنگام نصب XP تعریف می‌شوند همگی عضو گروه Administrators بوده و برای کاهش قدرت آنها باید بعد از نصب از طریق برنامه مربوطه وارد عمل شد و گروه آن‌ها را به Limited (users) تبدیل کرد . چنانچه در XP فقط يك کاربر تعریف کنیم ، در آنصورت کامپیوتر پس از Boot شدن خود وجود وارد سیستم می‌شود بدون آنکه گذر واژه‌ی از ما خواسته شود ، در این حالت سیستم عامل XP بطور خودکار همان يك کاربر را Auto Login می‌کند و این بمعنای نقض امنیت در ورود به سیستم نیست ، می‌توان این ویژگی را غیرفعال کرد . ضمناً این خصوصیت یعنی Auto Login در بقیه اعضای خانواده NT نیز وجود دارد .

فعالیت عملی مربوط به ویژگی Security :

(الف) نشان دهید که در XP کاربران تعریف شده هنگام نصب ، عضو گروه Administrators هستند .

(ب) نشان دهید که در XP ، يك کاربر عادی (عضو گروه Users) قادر به ایجاد فایل جدید در ریشه دیسک که با فایل-سیستم NTFS فرمت شده نیست (پوشه جدید را می‌توان درست کند اما فایل را خیر)

(ج) نشان دهید که در XP ، يك کاربر عادی (عضو گروه Users) نمی‌تواند ساعت سیستم را تغییر دهد .

(د) نشان دهید که در XP ، يك کاربر عادی (عضو گروه Users) نمی‌تواند از طریق Device Manager يك سخت‌افزار را (مثلاً Mouse) غیر فعال (Disable) کند .

Multi Tasking - ۱-۷-۲ :

چند وظیفه‌ای ، توانایی اجرای همزمان چندین برنامه با هم . این ویژگی نیازی به شرح بیشتر نداشته و امروزه در تمامی سیستمها وجود دارد و يك ویژگی عادی بشمار می‌رود . DOS بعنوان يك سیستم قدیمی Multi task نیست اما بقیه تقریباً همگی Multi Task هستند منجمله Windows 3.x .

تقسیم زمانی بین کارهای مختلف و گردش سریع بین آنها . این تکنیک در اصطلاحات فنی Time_Sharing یا "اشترک زمانی" خوانده می‌شود . تکنیک اشترک زمان نه تنها در اجرای برنامه‌ها به وسیله CPU بلکه در مخابرات و شبکه نیز کاربردهای فراوانی در انتقال اطلاعات دارد و یکی از روشهایی است که می‌توان اطلاعات چندین فرستنده را روی يك محیط انتقال بطور همزمان ارسال کرد . البته این تکنیک در اصطلاحات مخابراتی Time Division Multiplexing = TDM خوانده می‌شود .

Multi Processor Support - ۱-۷-۳ :

پشتیبانی از چندین پردازنده ، می‌دانیم که هرچه تعداد پردازنده‌های موجود بر روی يك برد اصلی بیشتر باشد کارها سریعتر انجام می‌شود . امروزه بردهای چند پردازنده در ۲ زمینه عمده کاربرد دارند :

- سرورها ، مخصوصاً App Server و DB Server که قبلاً اشاره شد .
- کامپیوترهایی که عملیات سنگین گرافیکی و پویا را انجام می‌دهند . (Graphic Workstations)

بنابراین در مواردی که نیاز به استفاده از بردهای با بیش از يك CPU باشد لازم است تا سیستم عامل نیز بتواند آنها را شناسایی کرده و استفاده کند . در خانواده Microsoft فقط سیستمهای NT قادر به شناسایی و بهره‌برداری از چندین CPU هستند .

تحقیق : پشتیبانی از چندین پردازنده در سیستم عامل‌ها با ۲ سیاست کلی متقارن و نامتقارن انجام می‌شود ، (SMP=Symmetric Multi Processing , AMP=Asymmetric

(Multi Processing) ، هريك را به اختصار بررسی کرده و بگوئید که میکروسافت در سیستمهای خود از کدام روش استفاده می‌کند ؟

۴-۷-۱- تحمل خطا Fault Tolerance :

تحمل خطا ، عدم تأخیر در ارائه سرویس و قدرت تحمل در هنگام بروز مشکل و خطاهای عمدتاً سخت‌افزاری است بعبارت دیگر Fault Tolerance (باختصار FT) قابلیت است در سیستم عامل که می‌تواند هنگام بروز مشکلات از تجهیزات جایگزین استفاده کرده و بدون تأخیر (یا با تأخیر بسیار کوتاه) بطور خودکار به سرویس دهی ادامه دهد . نکته اصلی در FT اینست که هنگام بروز خطا اولاً زمان قطعی سرویس صفر یا بسیار کوتاه بوده و ثانیاً عملیات جایگزینی بدون عوامل انسانی و بطور خودکار صورت می‌گیرد . مسوول سیستم در فرصت مناسب می‌تواند عیوب را بررسی و رفع کند .

مثال ۱ : فرض کنید که یک File Server داریم که تمامی اطلاعات خود را روی یک دیسک سخت ذخیره کرده است . اگر برای دیسک مشکلی بروز کند مثلاً بر اثر یک شوک الکتریکی در برق بخشی از قطعات آن بسوزد چه اتفاقی می‌افتد ؟ بدیهی است که سرویس قطع می‌شود ، چکار کنیم که سرویس قطع نشود ؟

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا ۲ دیسک سخت روی سیستم نصب کنید .

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه دیسک باشد . سیستم عامل در شرایط عادی هر اطلاعاتی را که روی دیسک اول می‌نویسد عیناً روی دیسک دوم نیز کپی می‌کند بعبارتی دیسک دوم همانند آینه ایست از دیسک اول (Disk Mirroring , Disk Duplexing) حال اگر به هر دلیل یکی از دیسکها از کار بیافتد سیستم عامل می‌تواند بدون لحظه‌ای تأخیر اطلاعات را با دیسک دوم تبادل کند . مثال فوق در اصطلاحات کامپیوتری Disk_Fault_Tolerance یا Mirror یا Duplex یا RAID 1 خوانده می‌شود . از میان محصولات میکروسافت ، سیستمهای NT که در گروه سرور قرار دارند همگی قابلیت Disk Fault Tolerance را دارا هستند .

مثال ۲ : یک سرور داریم (از هر نوع دخواه) که با یک کارت شبکه (NIC) به شبکه متصل شده و کامپیوترها از آن سرویس می‌گیرند . اگر برای کارت شبکه یا خط متصل به آن اتفاقی بیافتد چه می‌شود ؟ بدیهی است که سرویس قطع می‌شود اگر بخواهیم که سرویس قطع نشود باید:

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا ۲ عدد NIC روی سیستم نصب کنید .

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در این زمینه باشد . سیستم عامل در شرایط عادی اطلاعات را تقسیم کرده و از هر ۲ کارت برای ارسال و دریافت استفاده می‌کند (که البته باعث افزایش سرعت نیز می‌شود) حال اگر به هر دلیل یکی از کارتها از کار بیافتد ، سیستم از کارت دیگری برای ادامه کار استفاده می‌کند . مثال فوق در اصطلاحات کامپیوتری NIC Fault Tolerance خوانده می‌شود و در برخی از متون به آن Port Trunk یا Port Aggregation یا Link Aggregation می‌گویند که بعداً نیز مورد بحث قرار خواهد گرفت . از میان محصولات میکروسافت ، سیستمهای NT اعم از سرویس گیرنده یا Server در صورتیکه کمپانی سازنده کارت شبکه درایور مناسب را برای محصول خود ارائه داده باشد می‌توان از این خاصیت بهره برد .

مثال ۳ : فرض کنید که یک سرور داریم (از هر نوع دخواه) و این سرور مکن است هريك از موارد قبلی Fault tolerance را اعم از Disk یا NIC داشته باشد یا خیر . اگر به هر دلیل سرور بطور کامل از کار بیافتد چه می‌شود ؟ بدیهی است که سرویس قطع می‌شود ، چکار کنیم اختلالی در سرویس دهی بروز نکند ؟

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا ۲ یا چند سرور را با تجهیزات ویژه به یکدیگر متصل کنید. به این مجموعه از سرورها اصطلاحاً یک "خوشه سرور" یا Server Cluster گفته می‌شود.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه Clustering باشد. کلیه سیستمها در شرایط عادی اطلاعات مورد نیاز را با یکدیگر تبادل کرده (Synchronize) و چنانچه یکی از اعضای Cluster (یعنی یکی از سرورها) از کار افتد بقیه می‌توانند بسرعت و بدون تأخیر کار او را جبران کنند. از میان محصولات مایکروسافت فقط چند سیستم از مجموعه NT در خانواده سرور دارای قابلیت Cluster هستند بعنوان مثال 2000 Server فاقد آن بوده اما 2000 Advanced Server و 2000 Data center Server دارای توانایی آن هستند.

۵-۷-۱- نرم افزار تهیه نسخه پشتیبان Backup Utilities :

امروزه اهمیت تهیه Backup برای یک کاربر باتجربه پوشیده نیست، بالاخره هرکس که با کامپیوتر سروکار دارد با لحظه‌ای مواجه شود که به هر دلیل اطلاعات اصلی‌ش خدوش یا غیرقابل دسترس شده است در این حالت با نسخه پشتیبان می‌توان اطلاعات را دوباره بازگرداند.

اطلاعات را در حالت کلی می‌توان به دو دسته تقسیم کرد :

الف) اطلاعاتی که کاربر مستقیماً و کم و بیش از آن آگاه بوده و اهمیتش بر او پوشیده نیست مانند انواع پرونده‌ها یا حتی برنامه‌های کاربردی که تهیه و نصب کرده است : (User Data)

ب) اطلاعاتی که کاربر مستقیماً با آن سروکار ندارد بلکه برای سیستم عامل مهم است : (System Data)

اغلب کاربران پس از مدت کوتاهی با نحوه تهیه Backup از اطلاعات خودشان یعنی User Data آشنا می‌شود اما کمتر کاربر عادی پیدا می‌شود که طی مدت کوتاهی بتواند بطور کامل از System Data نیز Backup گرفته یا Restore کند چرا که با توجه به پیچیدگی سیستم عاملها، کسب آگاهی نسبت به ظرافتهای سیستم عامل در زمان کوتاه امر ساده‌ای نبوده و نیاز به تجربه و تخصص دارد.

چگونه می‌توان از System Data بدون مهارت لازم Backup گرفت ؟

یک راه حل مناسب آنست که سیستم عامل ابزارهای قوی و عین حال User Friendly در اختیار کاربر بگذارد تا او بتواند اولاً بر راحتی اطلاعات را دسته‌بندی کند ثانیاً بدون داشتن تخصص زیاد قادر به تهیه Backup از System Data باشد. خوشبختانه ابزارهای تهیه Backup در سیستمهای NT 5.x دارای چنین تواناییهایی بوده و کاربر می‌تواند در صورت داشتن مجوز، تنها با علامتگذاری در قسمت "System State" اقدام به تهیه پشتیبان از System_Data کند.

ممکن است بخواهید بدانید تفاوت بین ابزارهای خاص تهیه Backup (مانند NTBackup در NT 5.x) با ابزارهای عمومی مدیریت فایلها که عملیاتی مانند Copy-Paste را انجام می‌دهند (مانند My Computer = Explorer) چیست؟ در جواب باید گفت: قابلیت‌هایی که در ابزارهای خاص وجود دارد در برنامه‌های عمومی (مانند My Computer) نیست. اهم این قابلیت‌ها عبارتند از :

الف) به کمک ابزارهایی مانند NTBackup بر راحتی از System Data نسخه پشتیبان تهیه می‌شود.

ب) با این ابزارها، از فایل‌هایی که در حال استفاده هستند (Open Files) می‌توان به راحتی نسخه پشتیبان تهیه کرد.

ج) سیاست‌های تهیه Backup یا بعبارت فنی Backup Policy در ابزارهای خاص تنوع بیشتری دارد، بدان معنی که انتخاب فایلها برای Backup می‌تواند با معیارهایی همچون "فقط فایل‌های تخیریفته" و... صورت گیرد. که در ابزارهای معمولی تنوع این معیارها کمتر است.

د) با ابزارهاي خاص مي‌توان انجام عمليات را بطور خودكار در موعده دخواه 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-سيستمهاي مانند NTFS كه تعيين مي‌كند چه افراي 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 شده 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 کدام كاربر وارد سيستم شده ايد؟ پس از پاسخ به اين سوال، برنامه My Computer را اجرا کرده سپس پارتيشني را كه سيستم عامل روي آن نصب شده باز کرده (مثلاً ديسك C:) وارد پوشه Documents_and_Settings شويد. قاعدتاً بايد يك پوشه همنام با كاربري را كه با آن وارد سيستم شده ايد ببينيد. حال سعي كنيد كه (با استفاده از برنامه My Computer) از اين پوشه Copy-Paste بگيريد. آيا امكان پذير 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 برنامه My Computer نمي‌تواند از آن كپي تهيه كند. حال با استفاده از برنامه NTBackup از همن پوشه كپي بگيريد. نتيجه چيست؟ بلي، امكان پذير است. بنابراين نشان داديد كه NTBackup قدرت بيشترتي نسبت به My Computer در تهيه پشتيبان از فايلها و پوشهها دارد.

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

ابزارهاي مديریتی ساده، قدرتمند و يکپارچه. هر سيستم عاملي هرچقدر هم كه قوي باشد اما اگر پيكربندي، تنظيمات و بطور كلي مديریت آن پيچيده باشد با عدم استقبال عامه مواجه مي‌شود و اين دقيقاً يكي از دلایلي 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.

فعالیت عملی : آشنایی با یکی از ابزارهاي مديریتی قوي در NT 5.x :

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

الف) روي آيکن My Computer واقع بر دسكتاپ كليك راست کرده، گزینه Manage را انتخاب كنيد.

ب) از طريق Run تايپ كنيد : compmgmt.msc

پس از اجراي برنامه، بررسی كنيد كه بوسیله آن چه كارهايي را مي‌توان انجام داد.

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

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

UNIX و LINUX پس از نصب چندین برنامه مختلف بهم می ریزد حال بنظر شما چنین سیستمی مناسب شبکه و مخصوصاً سرور است؟!

خوشبختانه سیستمهای NT و مخصوصاً " NT 5.x در وضعیت بسیار بهتری نسبت به خانواده 9x قرار دارند و بدین لحاظ برای کاربرد در شبکه ها اعم از سرویس گیرنده یا سرور مناسبترند .

۸-۷-۱- پشتیبانی Support :

پشتیبانی ، هر سیستم عاملی اعم از قوی یا ضعیف نیاز به رشد و رفع مشکلات و نواقص دارد و این میسر نیست مگر با پشتیبانی از طرف تهیه کننده گان یا تیمهای جنپی . خوشبختانه در زمینه محصولات میکروسافت با وجود نواقص بسیار مخصوصاً در زمینه امنیتی ، پشتیبانی آن قوی بوده و اکثراً تجربه بروز رسانی سیستم عاملهای NT 5.x را از طریق برنامه Automatic Update داشته ایم .

خود آزمایي و تحقیق

- ۱- از لحاظ تقسیم بندی شبکه های کامپیوتری از نظر سرویس دهی شبکه اینترنت به کدام دسته تعلق دارد؟
- ۲- از لحاظ تقسیم بندی شبکه های کامپیوتری از نظر گستردگی فیزیکی سیستم بانکی شتاب به کدام دسته تعلق دارد؟
- ۳- سرویس های رایج در شبکه های کامپیوتری را نام ببرید؟
- ۴- نقش حافظه RAM را در هر یک از انواع File Server ، Print Server ، Applicatin Server بررسی کنید؟
- ۵- داشتن چندین پردازنده در کدام یک از انواع سرور می تواند مفید باشد؟
- ۶- User Data و System Data را تعریف کنید؟
- ۷- ویژگی سیستم عامل را نام ببرید؟
- ۸- تفاوت Multi Tasking و Multi Programing را بنویسید.
- ۹- تحقیق کنید که یک سرور NAS به لحاظ سخت افزاری باید چه قابلیت هایی داشته باشد؟
- ۱۰- تحقیق کنید که حداقل سخت افزار لازم برای نصب هر یک از سیستم عامل های محصول میکروسافت چیست و آنها را با هم مقایسه کنید.

فصل دوم سیستم های انتقال دیجیتال

هدف های رفتاری

- روش ارسال اطلاعات به صورت موازی را بیان کند.
- روش های ارسال اطلاعات به صورت سری را شرح دهد.
- انواع روش های انتقال اطلاعات بر اساس جهت آنها را تعریف کند.
- سیگنال های اطلاعات و انواع آن را شرح دهد.
- پهنای باند را تعریف کند
- نویز و انواع آن را شرح دهد.

یکی از مسایل مهم در شبکه های کامپیوتری نحوه برقراری ارتباط بین کامپیوتر هاست. منظور از برقراری ارتباط این است که اطلاعات به چه ترتیبی ارسال شوند. می توان این پرسش ها را مطرح کرد که آیا روش ارسال به صورت بیت به بیت و جداگانه باشد یا گروهی از اطلاعات با هم و به صورت گروهی ارسال شوند یا این که آیا فرستنده آن ها را همانند یک ایستگاه فرستنده رادیویی ارسال نماید یا از روشی که در مخابرات برای انتقال صورت به کار می رود، استفاده شود. جواب این پرسش ها این است که اطلاعات در شبکه به صورت کدهای دودویی ارسال می شوند. در سیستم دودویی فقط از دو کد صفر و یک استفاده می شود که در کامپیوتر مقصد از ترکیب این کدها، اعداد، حروف و کاراکترهای ویژه به دست می آید.

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

۱. parallel (یا موازی)
۲. سریال (پشت سرهم)

در روش موازی تعدادی از بیت ها با هم و به صورت گروهی ارسال می شوند ولی در روش سریال، بیت ها تک به تک و پشت سرهم ارسال می شوند. نحوه ارسال به صورت موازی فقط یک شیوه دارد، در صورتی که ارسال سریال از دو روش ارسال هم زمان (Synchronous) و غیر هم زمان (Asynchronous) استفاده می شود.

۱-۲- ارسال موازی (Parallel)

در این روش اطلاعات قبل از ارسال تبدیل به کدهای باینری شده و یک به یک ارسال می شوند. برای مثال می توان گفت که این عمل مانند این است که یک نامه را تبدیل به حروف تشکیل دهنده آن کرده و حروف را یک به یک ارسال کنیم.

حال تعدادی کد باینری داریم که می خواهیم ارسال کنیم؛ اگر تعدادی از آن ها را تبدیل به یک گروه کرده و باهم بفرستیم ارسال سریعتر انجام می شود و این چیزی است که در ارسال موازی اتفاق می افتد در این روش تعدادی کاراکتر از طریق چند خط ارتباطی و به صورت هم زمان با هم ارسال می شوند؛ این خطوط می توانند در درون یک کابل شبکه یا یک شبکه بی سیم بنا شده باشند به صورت پیش فرض ۸ خط برای ارسال موازی در نظر گرفته شده است یعنی می توانیم حداکثر ۸ کد را هم زمان ارسال کنیم.

۲-۲- ارسال سریال

در ارسال سریال، بیت ها به دنبال هم و به صورت سری انتقال می یابند؛ به این ترتیب که بیت ها پشت سرهم قرار گرفته و یک رشته را می

سازند و این رشته به کامپیوتر مقصد ارسال 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^۱ بیت پایان^۲ 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 تنها ۷۵٪ ظرفیت برای انتقال اطلاعات استفاده می شود .

توانایی کامپیوترها در ارسال و دریافت اطلاعات از نظر سرعت متفاوت است ؛ بنابراین ممکن است یک کامپیوتر بتواند 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 همان 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 دریافت 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^۱
- ۲- دوطرفه غیر هم زمان^۲
- ۳- دوطرفه هم زمان^۳

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 و به 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 رادیو یا تلویزیون است دریافت می شود و هیچگاه ارسال تعییر نمی کند. به این روش ارسال، یک طرفه می گویند.

شکل ۲-۱ (ص ۱۸) 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 A و 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 B فقط باید دریافت کننده باشد و برعکس. برای مثال می توان به واکتی - تاکتی 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 A و 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 ۲-۳ شکل ۱-۲ (ب) (ص ۱۹) مفاهیم شبکه

۴-۲-۴- سیگنال های اطلاعات

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

سیگنال های اطلاعات می توانند به دو صورت 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 ۱-۳ (الف) می بینید روی بردار نمایش می دهند. محور عمودی نمایانگر مقدار عددی موج و محور افقی نمایانگر زمان است.

شکل ۲-۴ - شکل ۱-۳ (ب)

(الف) (ص ۲۰) 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 دو حالت 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 ۲-۵ - شکل ۱-۳ (ب) (ص ۲۰)

مفاهیم شبکه

- سیگنال های Periodic و Aperiodic

هردو نوع سیگنال های آنالوگ و دیجیتال به دو فرم Periodic و Aperiodic به 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

۴-۱ (ص ۲۱) 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

۵-۱ (ص ۲۱) مفاهیم شبکه

۵-۲- پهنای باند^۱

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 ۳۰۰ Hz و بالاترین فرکانس ۳۳۰۰ Hz است .

واحد سنجش فرکانس **هرتز**^۲ می باشد . حدها 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^۳ 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 .

^۱-Band Width

^۲ - Hz

^۳-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^۱

۲- باند پهن^۲

در روش تک باند از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می شود ؛ به این معنی که تک باند در هر لحظه فقط می تواند یک سیگنال را از خود عبور دهد ، در نتیجه ارسال نوبتی می شود و اطلاعات پشت سرهم و به 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 دریافت 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 (ص ۲۲) مفاهیم شبکه

۶-۲-۶ - نویز

از جمله مشکلاتی که در شبکه به وجود می آید ، نویز است . نویز عامل مخربی 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

^۱ - Base band

^۲ - Broad band

نمایند؛ این حرکت گاهی با سیگنال‌ها هم جهت شده و اندازه و شکل آن‌ها را که همان الگوی سیگنال‌هاست، تغییر می‌دهد.

القا: نویزهای القایی نویزهایی هستند که موتورهای مکانیکی مثل موتور ماشین یا وسایل الکتریکی مانند موتورهای الکتریکی و وسایل خانگی تولید می‌کنند، این وسایل شبیه یک آنتن فرستنده عمل می‌کنند و می‌توانند نویز را ارسال کنند و کابل شبکه، شبیه یک آنتن گیرنده نویزهای ارسال شده را دریافت می‌کند.

هم‌شنوایی^۱: هم‌شنوایی اثر میدان‌های مغناطیسی یک کابل مجاور خود است. نویزهایی که کابل‌های برق فشار قوی یا رعد و برق ایجاد می‌کنند نیز از انواع نویزهای القایی محسوب می‌شوند.

سرعت انتقال اطلاعات: به مقدار اطلاعاتی که در واحد زمان به وسیله تجهیزات شبکه ارسال می‌شود، سرعت انتقال اطلاعات می‌گویند و واحد اندازه‌گیری آن bps است. سرعت انتقال اطلاعات در وسایل مختلف متفاوت است.

به طور مثال کارت‌های شبکه با سرعت 10Mbps توانایی انتقال ۱۰ مگابایت در ثانیه را دارند و کارت‌های ۱۰۰Mbps می‌توانند در ثانیه ۱۰۰ مگابایت اطلاعات به مقصد ارسال کنند. سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم دارد، هر چه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می‌شود.

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

^۱-crosstalk

خود آزمایي و تحقیق

- ۱- سرعت ارسال اطلاعات در کدام يك از روش هاي سري و موازي بیشتر است؟
- ۲- در کدام يك روش هاي ارسال سریال هم زمان و غير هم زمان کنترل ترافیک امکان پذیر است؟
- ۳- سیگنال چیست؟
- ۴- تفاوت سیگنال دیجیتال و آنالوگ را بنویسید و با ذکر دلیل مشخص کنید کیفیت و سرعت کدام يك براي ارسال اطلاعات بهتر است؟
- ۵- نویز چیست؟ اثر نویز بر روي کدام يك از سیگنال هاي آنالوگ یا دیجیتال بیشتر است؟
- ۶- تحقیق کنید که گذرگاه هاي COM، LPT و USB از چه سيستمي براي انتقال اطلاعات استفاده مي کنند؟
- ۷- تحقیق کنید که واحدهاي Bps و bps چه تفاتي با هم دارند؟

فصل سوم پیکر بندی شبکه و محیط انتقال

هدف های رفتاری
 انواع توپولوژی شبکه را شرح دهد.
 انواع محیط های انتقال را شناسایی کند.
 کابل کشی یک شبکه را انجام دهد.
 کارت شبکه و وظایف آن را تعریف کند.
 کابل رابط بین شبکه و سویچ را ایجاد کند.
 روش های دسترسی به خط انتقال را شناسایی کند.

۳-۱- توپولوژی انواع آن

اجزای سخت افزاری در شبکه طبق یک طرح و نقشه بهم متصل می‌شوند که به آن اصطلاحاً **توپولوژی شبکه** می‌گویند. در ابتدا ممکن است تصور کنیم که توپولوژی فقط بمعنی نقشه فیزیکی و ظاهری شبکه است و چگونگی گردش اطلاعات و همچنین نحوه دسترسی کامپیوترها به محیط انتقال در آن اهمیتی ندارد اما این حالت کافی نبوده و در توصیف و بررسی یک توپولوژی باید علاوه بر چگونگی اتصال ظاهری، نحوه تبادل اطلاعات را هم جزو توپولوژی بحساب آورد بنابراین توپولوژی را به شکل زیر تعریف می‌کنیم

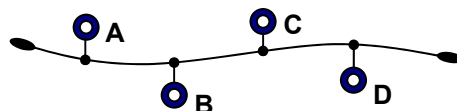
تعریف توپولوژی :

- چگونگی اتصال ظاهری اجزا از طریق محیط انتقال به یکدیگر .
- نحوه دسترسی اجزا به محیط انتقال و گردش اطلاعات مابین آنها .

با اینحال در ادامه مبحث و شرح بیشتر، گاهی اوقات به یکی از جنبه‌ها توجه بیشتری می‌کنیم. (ضمناً برای ساده‌تر شدن مبحث، فرض کنید که محیط انتقال از نوع "سیم" است (کابل) و فعلاً محیطهای انتقال بی‌سیم را منظور نمی‌کنیم)

۳-۱-۱- توپولوژی خطی (Bus) :

جنبه ظاهری : کلیه سیستمها از طریق یک قطعه کابل به یکدیگر متصل شده و اطلاعات خود را از طریق آن تبادل می‌کنند. نکته اصلی در توپولوژی خطی آنست که یک قطعه کابل بین کلیه کامپیوترها مشترک بوده و همه از طریق همان یک قطعه با هم ارتباط دارند.



شکل ۳-۱

چگونگی دسترسی کامپیوترها به خط و نحوه گردش اطلاعات : هر سیستمی که بخواهد اطلاعاتی را روی خط ارسال کند (مثلاً کامپیوتر A) ابتدا باید ببیند خط آزاد است یا خیر و اگر پاسخ مثبت بود اقدام به ارسال اطلاعات برای کامپیوتر(های) مقصد می‌کند. (این موضوع بعداً مورد بحث بیشتری قرار می‌گیرد)

اگر کامپیوتر A بخواهد اطلاعاتی را برای B ارسال کند بقیه کامپیوتر ها (C,D) هم از این اطلاعات باخبر میشوند چون محیط انتقال مشترک بوده و کنترلی روی آن وجود ندارد. به محض آنکه سیگنال ارسال شده از A روی خط قرار بگیرد، بسرعت در تمامی محیط انتقال منتشر شده و همه آنرا دریافت میکنند اما بدیهی است که فقط گیرنده (گیرندگان) تعیین شده از طرف فرستنده آنرا مورد استفاده قرار میدهد و بقیه گیرندگان به آن دسترسی ندارند.

فرض کنید در یک جمع نشسته اید، چه با یک نفر صحبت کنید چه با همه، نتیجه آنست که همه صحبت‌های شما را میشوند اما بدیهی است فقط فرد یا افرادی که مخاطب شما هستند از آن استفاده برده و بقیه به امور شخصی خود می‌پردازند. در اینجا هم علت مشابه است یعنی محیط انتقال یا عبارتی "هوا" برای همه افراد جمع مشترک بوده و سیگنال فرستنده یعنی صحبت‌های گوینده به محض خروج از دهان او در تمام فضای اطراف جمع (تا فاصله‌ای محدود و بسته به قدرت فرستنده) منتشر شده و همه آنرا میشوند. ولی فقط کسی که مورد پرسش قرار دارد باید پاسخ بگوید

برخورد یا Collision

فرض کنیم A در حال ارسال اطلاعات برای B باشد، همزمان C هم میخواهد اطلاعاتی را برای D بفرستد در این حالت، چون فقط یک محیط انتقال وجود دارد که آنهم بین همه مشترک است. به محض آنکه A اطلاعات خود را روی خط بفرستد، خط اشغال شده و بقیه باید صبر کنند تا ارسال A به اتمام رسیده و خط مجدداً آزاد شود. البته اگر کامپیوتر A کارش طولانی باشد باید کار خود را به صورت مقطعی انجام دهد بدین معنی که پس از ارسال قسمتی از اطلاعات، خط را آزاد میکند تا بقیه هم امکان دسترسی و استفاده از خط را داشته باشند. در صورتی که به طور همزمان C نیز بخواهد برای D اطلاعاتی را ارسال نماید باعث "تصادم اطلاعاتی" یا Collision شده و سیگنالها بهم میریزد. بنابر این در یک لحظه مشخص فقط یک فرستنده میتواند وجود داشته باشد.

البته خیلی از کاربران در شبکه‌هایی با توپولوژی خطی تجربه انتقال همزمان اطلاعات را مابین سیستم‌های مختلف داشته‌اند مثلاً در حالی که یک فایل بزرگ 1 GByte از کامپیوتر A به B انتقال می‌یابد، همزمان C و D هم با یکدیگر مشغول تبادل هستند. موضوع چیست؟ آیا تناقضی با مثال فوق ندارد؟ باید گفت: که در این حالت کار بصورت مقطعی انجام میشود. قبلاً در مبحث "ویژگی سیستم عامل‌ها" نیز اشاره شد به "اشتراک زمان" یا "تقسیم زمان". با استفاده از این تکنیک، هر فرستنده کسری از زمان را (یا حجم محدودی از اطلاعات را) برای ارسال در نظر گرفته که پس از به پایان رسیدن مجبور است خط را آزاد کرده تا دیگران نیز شانس ارسال را داشته باشند. در این تکنیک هرچند که بطور واقعی و در یک لحظه مشخص چندین فرستنده با هم وجود ندارند اما در مجموع همه میتوانند ارسال اطلاعات خود را با هم به پیش ببرند.

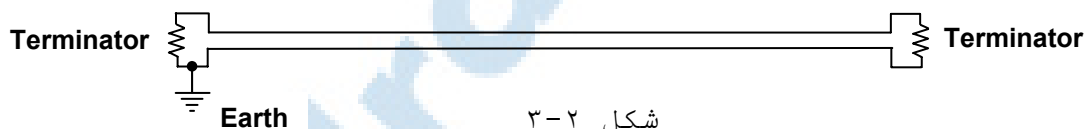
در تکنیک TDM در یک لحظه مشخص، باز هم بطور واقعی فقط یک فرستنده محیط انتقال را در اختیار می‌گیرد، در عمل با مثالهایی روبرو می‌شویم که در آن واحد بطور همزمان و بطور کاملاً واقعی همه فرستنده‌ها با هم روی یک محیط انتقال مشترک کار میکنند. فضای مادی را بعنوان یک محیط انتقال مشترک در نظر بگیرید. میدانیم که در یک لحظه صدها فرستنده تلویزیونی، رادیویی، مخابراتی و... امواج خود را در همین فضا پخش میکنند و عبارتی اطراف ما پر از امواج فرستنده‌های گوناگون است و با یکدیگر تداخلی هم ندارند، موضوع چیست؟ توجیه این واقعه استفاده از فرکانس‌های مختلف برای ارسال داده‌ها می‌باشد عبارتی هیچ ۲ فرستنده‌ای (در یک محدوده معین) نباید دارای فرکانس یکسان باشند. به این تکنیک اصطلاحاً "تقسیم فرکانسی" یا Frequency Division Multiplexing = FDM گفته میشود.

نتیجه‌گیری : در محیط‌های انتقال مشترک ، هیچ ۲ فرستنده‌ای نمی‌توانند همزمان با هم اقدام به ارسال اطلاعات کنند مگر آنکه از تکنیک‌های TDM یا FDM استفاده شود .

اثر قطع شدن کابل اصلی در توپولوژی خطی

اگر در توپولوژی خطی، قسمتی از کابل اصلی قطع شود تمامی شبکه از کار می‌افتد بعنوان مثال حد فاصل بین B و C قطع می‌شود اما ارتباط دو به دو مابین (A,B) و همچنین (C,D) برقرار است ، چرا می‌گوییم کل شبکه از کار می‌افتد ؟ علت آن است که در شبکه‌های کامپیوتری از جریان‌های متناوب (Alternative Current = AC) برای ارسال اطلاعات استفاده می‌شود، همچون امواج دریا . می‌دانیم که اگر امواج دریا پس از رسیدن به ساحل با یک مانع همچون تخته‌سنگ برخورد کنند بشدت برگشته و موج رفت و برگشت با یکدیگر تصادم می‌کنند (Collision) و این تداخل باعث بهم ریختن شکل موج می‌شود، اما اگر مانعی که در ساحل وجود دارد یک ساحل شنی نرم (یا در ذهن خود تصور کنید یک ابر اسفنجی بزرگ) باشد ، موج به آرامی جذب ساحل شده و "موج برگشت" آنچنان شدتی برای بهم ریختن "موج رفت" ندارد . در شبکه‌های کامپیوتری نیز اوضاع به همین مفهوم است ، چنانچه یک قطعی در کابل رخ دهد ، این قطعی مصادف با روبرو شدن موج با "هوا" است و می‌دانیم که "هوا" عایق الکتریسیته بوده و برای آن حکم تخته‌سنگ را دارد بنابراین موج در "نقطه قطع شده" برگشت کرده و با "موج رفت" تصادم می‌کند (Collision) و این برخورد باعث بهم ریختن شکل موج شده و در نتیجه تمامی قسمت را تحت تأثیر قرار می‌دهد .

نتیجه‌گیری که از این مبحث می‌شود آنست که در توپولوژی خطی باید به‌گونه‌ای عمل کرد که در هیچ قسمتی از کابل Collision اتفاق نیفتد و این شامل ابتدا و انتهای خط نیز می‌شود . در طرفین خط باید ترتیبی اتخاذ کرد تا امواج پس از رسیدن به آنجا اصطلاحاً جذب شده و تداخل درست نکنند و این امر با قرار دادن مقاومتهایی (Resistor) در ابتدا و انتهای خط که اصطلاحاً به آنها Terminator گفته می‌شود میسر می‌شود . مقدار این مقاومتها بستگی به مشخصات الکتریکی کابل و پارامترهای دیگر داشته و مثلاً در نوع خاصی از شبکه‌ها 50Ω است.



شکل ۲-۳

مزایا و معایب توپولوژی خطی :

مزایا :

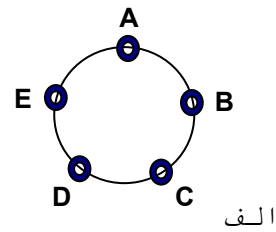
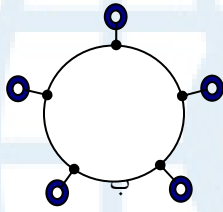
- افزایش و کاهش سیستمها بر راحتی (تا حد مجاز) صورت می‌گیرد .
- در کل ساده و کم‌هزینه است .

معایب :

- در صورت قطعی در یک قسمت از کابل اصلی ، تمامی شبکه از کار می‌افتد ،
- عیب‌یابی آن وقت‌گیر است
- نیاز به نگهداری و مراقبت بیشتری نسبت به سایر توپولوژی‌های دیگر دارد .

۲-۱-۳- توپولوژی حلقوی (Ring) :

جنبه ظاهری : کلیه کامپیوترها در یک حلقه به یکدیگر متصل می‌شوند . بدیهی‌است وقتی می‌گوییم حلقه ، منظور آنست که آخرین کامپیوتر هم باید به اولین متصل شود .



شکل ۳-۳

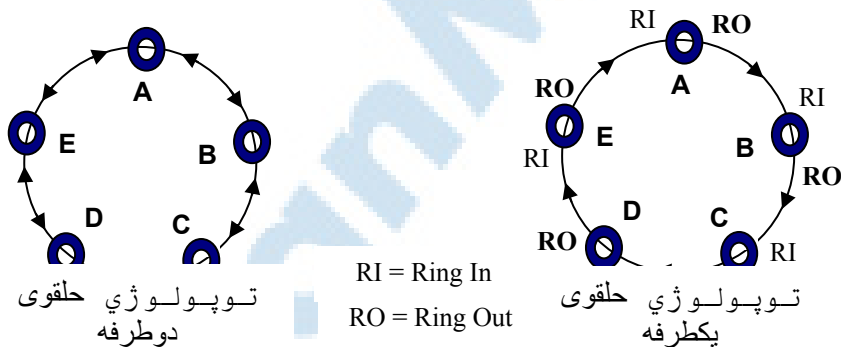
در شکل ۳-۳-قسمت ب را نمی‌توان حلقوی به حساب آورد زیرا اگر به شکل دقت کنید! این شبکه هیچ فرقی با شبکه خطی ندارد بجز آنکه سر و ته خط به یکدیگر وصل شده است و در واقع هیچ مزیتی نسبت به خطی ندارد.

تفاوت توپولوژی خطی با توپولوژی حلقوی: در توپولوژی حلقوی هر سیستم، دو گذرگاه (Port) اما در توپولوژی خطی فقط یک گذرگاه برای عبور اطلاعات دارد.

چگونگی دسترسی کامپیوترها به خط و نحوه گردش اطلاعات: از نظر نحوه گردش اطلاعات، دو نوع توپولوژی حلقوی را می‌توان متصور شد:

الف) توپولوژی حلقوی یکطرفه: اطلاعات فقط در یک جهت گردش می‌کند.

ب) توپولوژی حلقوی دوطرفه: اطلاعات در هر دو جهت می‌تواند گردش کند.



شکل ۳-۴

بزودی خواهیم دید که حلقوی دوطرفه در واقع حالت خاصی از توپولوژی Mesh است، لذا در سایر متون وقتی صحبت از حلقوی می‌شود عموماً منظور حلقوی یکطرفه است مگر صراحتاً خلاف آن ذکر شود.

مزایا و معایب حلقوی (یکطرفه) نسبت به خطی:

مزیت: در بخش "روشهای دسترسی به محیط انتقال" خواهیم دید که نحوه گردش اطلاعات در حلقوی نسبت به خطی دارای مزایایی از قبیل اولویت‌بندی و زمان‌بندی است که خطی از آن محروم است.

معایب:

۱. مصرف کابل در آن نسبت به توپولوژی خطی بیشتر است!
۲. همچون توپولوژی خطی اگر یک قسمت از حلقه قطع شود، کل حلقوی از کار می‌افتد البته نه بدلیل Collision، بلکه بدین سبب که اطلاعات قادر به گردش کامل نخواهد بود.

در واقع قانون گردش اطلاعات در حلقه‌های یکطرفه بگونه‌ای طراحی شده که اولاً هر اطلاعاتی که از یک سیستم خارج می‌شود باید دور زده و سرجای اول خود برگردد، ثانیاً همه سیستمها باید قادر به تبادل اطلاعات باشند. بعنوان مثال در شکل حلقوی یکطرفه دقت کنید، اگر حد فاصل بین A و B قطع شود در آنصورت هرچند ممکن است تصور شود که B می‌تواند برای C، D، E و A اطلاعات بفرستد، اما عکس آن امکانپذیر نیست و این بمعنای آنست که همه سیستمها نمی‌توانند به تبادل اطلاعات بپردازند، در نتیجه هر دو قانون فوق نقض شده و حلقه بطور کامل غیر قابل استفاده می‌شود.

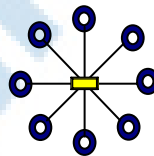
نکته: مشکل فوق در حلقه‌های دوطرفه (که حالت خاصی از Mesh محسوب می‌شوند) وجود ندارد.

پرسش: چرا در توپولوژی حلقوی (اعم از یکطرفه یا دوطرفه)، از Collision بعنوان عاملی بازدارنده یاد نمی‌شود؟

۳-۱-۳- توپولوژی ستاره‌ای (Star):

- جنبه ظاهری: کلیه کامپیوترها به یک نقطه مرکزی بنام Hub متصل می‌شوند.

نکته: واژه Hub بطور کلی یعنی "نقطه مرکزی" و نحوه عملکرد این "نقطه مرکزی" و همچنین نام دقیق آن بستگی به نوع شبکه‌ای دارد که در آن استفاده می‌شود. در این بخش هرگاه صحبت از Hub می‌شود منظور استفاده از آن در نوع خاص و رایجی از شبکه‌ها بنام شبکه Ethernet بوده که موضوع فصول بعدی است.



شکل ۳-۴

چگونگی دسترسی کامپیوترها به محیط انتقال و گردش اطلاعات

بسته به نوع Hub ، نحوه گردش اطلاعات به دو حالت متفاوت انجام می شود :

- به محض آنکه یک سیستم اطلاعاتی را ارسال کند ، Hub اشغال شده و سیستمهای دیگر نمیتوانند بطور همزمان فرستنده اطلاعات باشند (همانند گردش اطلاعات در توپولوژی خطی) . دقت کنید که Hub ، خود بعنوان بخشی از محیط انتقال و توپولوژی بشمار می رود .
- چنانچه یک سیستم اطلاعاتی را برای یک مقصد مشخص بفرستد ، بقیه مسیرها برای عبور همزمان دیگر سیستمها باز هستند و اگر اطلاعاتی را برای همه بفرستد بدیهی است که همه خروجیها اشغال میشوند. به این نوع هاب مخصوص اصطلاحاً **Switch Hub** ، **Hub Switch** یا به اختصار **Switch** گفته می شود. امروزه عمدتاً در شبکه های کامپیوتری با توپولوژی ستاره ای بجای هاب معمولی از سویچ استفاده می شود که از ویژگی های آن عملکرد هوشمندانه در پیدا کردن مقصد نسبت به Hub می باشد.
- در یک شبکه ، اگر ارسال اطلاعات فقط به سمت یک مقصد مشخص باشد اصطلاحاً واژه **Unicast** و اگر ارسال اطلاعات برای چند سیستم مشخص باشد واژه **Multicast** و اگر همگان مورد خطاب قرار گیرند واژه **Broadcast** بکار می رود.
- اگر مسیر ارتباطی بین هاب و یک کامپیوتر قطع شود ، Collision حاصله در این قسمت باعث تأثیرگذاری در کل شبکه نمی شود معمولاً طراحی اکثر هابهایی که امروزه ساخته می شود بگونه ایست که اصطلاحاً "اجازه عبور Collision" را به خطوط دیگر نمی دهد.
- در توپولوژی ستاره ای که از یک هاب معمولی در آن استفاده می شود ، اگر A اطلاعاتی را به مقصد B بفرستد ، دیگر سیستمها نیز از آن آگاهی می یابند زیرا همانطور که گفته شد، چگونگی گردش اطلاعات اگر هاب معمولی باشد مانند توپولوژی خطی است. در حالی که در سویچ، فقط گیرنده مربوطه اطلاعات را دریافت می کند ، مگر آنکه گیرنده اصطلاحاً "همگان" باشند یا در واژه های کامپیوتری مقصد "Broadcast" باشد.

مزایا و معایب توپولوژی ستاره ای نسبت به توپولوژی خطی :

مزایا

- قطعی یک خط بطور معمول بقیه شبکه را تحت تأثیر قرار نمی دهد.
- اگر از Switch استفاده شود امکان تبادل اطلاعات دودو بصورت همزمان وجود دارد ، در نتیجه حجم ترافیک بیشتری در واحد زمان می تواند انجام شود.
- اگر از Switch استفاده شود چون ترافیک مقصد به یک ایستگاه روی گذرگاههای (Ports) دیگر ارسال نمی شود لذا ترافیک ناخواسته کاهش یافته و ضریب ایمنی در تبادل اطلاعات افزایش می یابد.

معایب

- اگر به هر دلیلی "نقطه مرکزی" از کار بیافتد ، کل شبکه از کار باز می ایستد ، به همین دلیل معمولاً Hub را از نظر فیزیکی در یک تابلوی مخصوص معروف به Rack نصب کرده و Rack را در یک مکان مطمئن و با شرایط محیطی مناسب قرار می دهند. در شبکه هایی که ضریب حساسیت آنها بیشتر است ، ترکیبی از دو یا چند سویچ را در توپولوژی Mesh قرار داده و بدین ترتیب اگر یکی از سویچها از کار بیافتد ، سویچهای دیگر بلافاصله وارد عمل شده و ترافیک از طریق آنها به عبور خود ادامه می دهد. (Fault Tolerance)
- مصرف کابل و بطور کلی هزینه پیاده سازی آن نسبت به خطی بیشتر است . البته در عوض هزینه نگهداری و رفع عیب (Maintenance & Trouble Shooting) پایینتر است زیرا کمتر دچار مشکل شده و عیبیابی در آن ساده تر و سریعتر انجام می شود.

۴-۱-۳- توپولوژی مش (Mesh) :

جنبه ظاهري : در هر سیستم به تعداد لازم ، سختافزار شبکه (Network Interface) نصب شده و همگی مستقیماً بصورت ۲ به ۲ به یکدیگر متصل می‌شوند. البته این حالت ایده‌آل بوده که اصطلاحاً گراف کامل (Complete Mesh) خوانده می‌شود.

شکل ۳-۵ (ص ۳۸ مفاهیم شبکه)

در عمل ممکن است ارتباط ۲ به ۲ برای همه امکان‌پذیر نباشد لذا توپولوژی به حالت یک گراف ناقص درمی‌آید (Partial Mesh)

شکل ۳-۶

۲. چگونگی دسترسی کامپیوترها به محیط انتقال و گردش اطلاعات : چون هر سیستم ارتباط دوطرفه‌ای با بقیه داشته و از طرفی بیش از یک مسیر برای رسیدن به مقصد وجود دارد لذا پس از انتخاب مسیر بهینه ، اطلاعات به مقصد می‌رسد. در توپولوژی مش بحث جدیدی بنام مسیریابی Routing مطرح می‌شود و به هر سیستمی که کار مسیریابی را انجام دهد اصطلاحاً مسیریاب "Router" گفته می‌شود.

مسیریاب (Router) : مسیریاب یا روتر به سخت‌افزاری گفته می‌شود مجهز به حداقل ۲ کارت شبکه (Network Interface) که نرم‌افزار مسیریابی (Routing) روی آن فعال شده و کار انتخاب مسیر بهینه و هدایت ترافیک را روی اطلاعات انجام می‌دهد. چون روتر محل عبور و تلاقی مسیرهای مختلف برای تبادل ترافیک است لذا علاوه بر "پلیس راهنمایی و رانندگی" ، در برخی از روترها "پلیس ایست-بازرسی" نیز وجود داشته ، نوع و محتوای ترافیک را کنترل می‌کند. بعبارت فنی عملیات Filtering و Firewall را هم انجام می‌دهند.

مثال ۱ : یک کامپیوتر شخصی شامل یک کارت شبکه و مودم همراه نرم‌افزار مسیریابی را می‌توان یک روتر نامید.

مثال ۲ : یک کامپیوتر شخصی مجهز به چندین کارت شبکه یا مودم همراه نرم‌افزار مسیریابی را می‌توان یک روتر نامید.

مثال ۳ : سخت‌افزارهای خاصی وجود دارند همراه نرم‌افزار مربوطه که فقط بعنوان روتر استفاده می‌شوند مانند روترهای ساخت کمپانی Cisco .

مزایا و معایب توپولوژی Mesh نسبت به سایر توپولوژیها :

مزیت: چون بیش از یک مسیر برای هدایت ترافیک وجود دارد بنابراین به احتمال زیاد ، قطعی در یک مسیر باعث اختلال کلی در ارتباط نمی‌شود و بالاخره شانس برای رسیدن به مقصد وجود دارد ضمن آنکه بعضی از روترها در حالت عادی ترافیک را روی چندین مسیر تقسیم می‌کنند و بنابراین حجم تبادلات نیز افزایش می‌یابد. خلاصه آنکه توپولوژی مش دارای ویژگی Redundancy یا Fault Tolerance و همچنین Load Balancing است

معایب Mesh نسبت به سایر توپولوژیها : بدیهی است که پیچیده‌تر و پرهزینه‌تر از بقیه است.

اصولاً انتخاب توپولوژی ربطی به ابعاد و گستردگی فیزیکی شبکه (LAN-WAN) ندارد اما بدیهی است که هر نوع توپولوژی را می‌توان چه در LAN و چه در WAN استفاده کرد اما با توجه به اینکه احتمال تأثیرگذاری عوامل بازدارنده در شبکه‌های WAN نسبت به LAN بیشتر است لذا معمولاً در شبکه‌های WAN از توپولوژی Mesh استفاده شده و خطی، ستاره ای، حلقوی را در LAN بکار می‌برند. البته ستاره ای در WAN هم کاربرد دارد.

شبکه حلقوی دوطرفه (Bi-Directional) را می‌توان حالت خاصی از Mesh به حساب آورد زیرا چنانچه اقطار یک مش کامل را حذف کنیم شکل حاصله یک مش ناقص خواهد شد که همان شبکه حلقوی دوطرفه است. رینگ‌های دوطرفه در شبکه‌های صنعتی که معمولاً Campus LAN هستند بکار می‌رود. در اینگونه شبکه‌ها توپولوژی ستاره‌ای به تنهایی پاسخگوی سرعت و پایداری نبوده لذا مش وارد عمل می‌شود. از طرفی چون "مش کامل" بسیار پیچیده و پرهزینه است بنابراین از مش‌های ناقص برای پیاده‌سازی توپولوژی استفاده می‌شود و شبکه حلقوی دوطرفه یکی از بهترین انتخابها در این زمینه بشمار می‌رود.

۲-۳ محیط‌های انتقال

برای آنکه ایستگاه‌های مختلف در یک شبکه بتوانند با یکدیگر ارتباط برقرار کنند نیاز به یک "محیط انتقال" مانند یک قطعه سیم دارند.

تعریف: به هر رسانه‌ای که بتواند اطلاعات را به گردش درآورده و هدایت کند اصطلاحاً "محیط انتقال" می‌گوییم.

با ذکر چند مثال می‌خواهیم محیط انتقال را توضیح دهیم

مثال ۱: وقتی صحبت می‌کنیم، امواج صوتی از طریق هوا بین‌گوینده و شنونده انتقال می‌یابد در این مثال "هوا" بعنوان محیط انتقال محسوب می‌شود.

مثال ۲: یک فرستنده تلویزیونی، امواج الکترومغناطیسی را از طریق آنتن در فضای اطراف خود پخش می‌کند و این امواج با سرعتی تقریباً معادل با سرعت نور به اطراف انتقال پیدا می‌کنند لذا "فضای مادی" بعنوان محیط انتقال محسوب می‌شود.

مثال ۳: اطلاعاتی را با روشن و خاموش کردن یک منبع تولید نور از طریق یک رشته کابل نوری که از ترکیبات فشرده مخصوص ساخته شده است و نور را از خود هدایت می‌کند ارسال می‌کنیم کابل نوری در اینجا به عنوان محیط انتقال محسوب می‌شود

مثال ۴: وقتی بوسیله گوشی FF با فردی که کنار در ورودی ایستاده صحبت کنید صدای ما تبدیل به انرژی الکتریکی شده و به وسیله ی الکترون‌ها از طریق سیم مسی جریان می‌یابد در اینصورت "سیم مسی" بعنوان محیط انتقال محسوب می‌شود.

۱-۲-۳- گروه‌بندی محیط‌های انتقال

محیط‌های انتقال را می‌توان به دو دسته کلی سیمی و بی سیم تقسیم کرد.

محیط انتقال سیمی (Wired)

- یک یا چند رشته سیم از جنس فلزات هادی یا آلیاژهای آنها مانند مس، آلومینیوم، برای انتقال الکتریسته.
- یک یا چند رشته سیم از جنس ترکیبات مخصوص مانند پلاستیک فشرده و سیلیس برای انتقال نور.

بی‌سیم (Wireless) (انتشار از طریق فضای مادی)

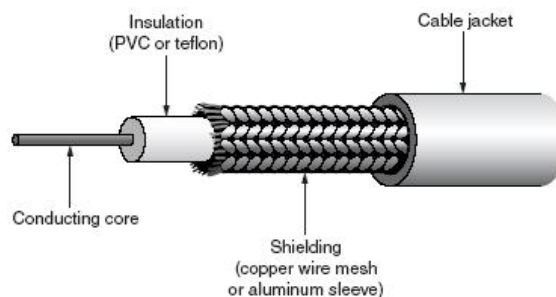
- استفاده از نور مادون قرمز (Infra Red) مانند کنترل تلویزیون.
- استفاده از نور لیزر (Laser) که در واقع تک فرکانس است.
- استفاده از امواج رادیویی (Radio Waves) در فرکانسهای مختلف مانند رادیو، تلویزیون، ماهواره، مخابرات مایکروویو، بی‌سیمهای شخصی و نظامی و

نکته: هر چند بوسیله انتقال صوت (مثالاً) از طریق هوا هم می‌توان اطلاعات را رد و بدل کرد اما این شیوه در شبکه‌های کامپیوتری بدلیل محدودیتهایی که دارد استفاده نمی‌شود

۲-۲-۳- بررسی محیطهای انتقال "سیمي" یا "کابلي" (Wired)

در شبکه‌های کامپیوتری ۳ نوع سیم (کابل) متداول بوده است:
 الف) کابل "هم محور" یا Coaxial مانند کابل آنتن تلویزیون.
 ب) کابل "زوج بهم تابیده" یا Twisted Pair مانند سیم تلفن.
 ج) کابل "فیبر نوری" یا Fiber Optic که معمولاً در سرعت‌های زیاد یا مسافت‌های طولانی کاربرد داشته و نویز روی آن اثر ندارد.

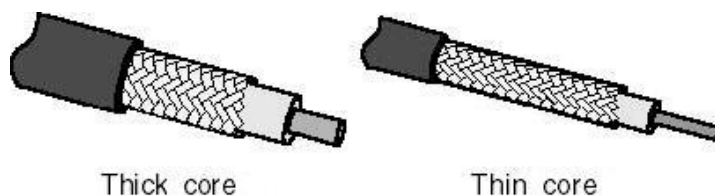
۳-۲-۳- کابل هم محور: در واقع کلمه Coaxial ترکیبی است از Co + axial یعنی "هم‌محور". علت این نامگذاری از شکل پیداست:



شکل ۷-۳

جریان الکتریکی از طریق هسته از سمت فرستنده به گیرنده گسیل شده و مسیر برگشت خود را از طریق حفاظ (Shield) طی می‌کند. حفاظ علاوه بر تأمین مسیر برگشت برای الکترون‌ها، وظیفه دیگری را نیز به عهده دارد و آن جذب نویزهای حاصل از "القای امواج الکترومغناطیسی در فضا" و هدایت آنها به زمین (Earth) است تا بدینوسیله از ایجاد نویز در هسته جلوگیری کند. البته یادمان باشد که جلوگیری از القای نویز روی هسته به وسیله حفاظ بصورت ۱۰۰٪ نبوده و نسبی است چنانچه شدت میدان الکترومغناطیسی اطراف کابل کابل هم محور قوی باشد در آنصورت حفاظ هم مقاومت چندانی نمی‌تواند بکند و اطلاعات هسته نویزی و مخدوش می‌شود.

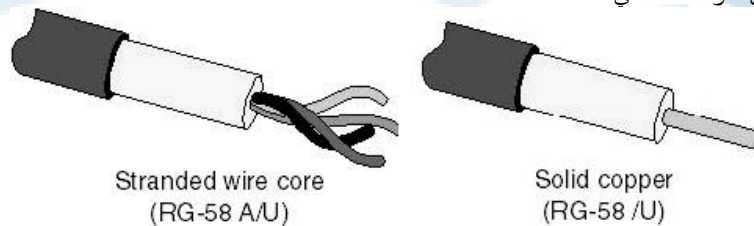
در کابلهای هم محور هر چه قطر هسته و متناسب با آن غلظت بافت الیاف فلزی حفاظ بیشتر باشد، مقاومت کابل در برابر عبور الکتريسته کمتر شده و لذا شدت جریان برای عبور با مانع کمتری مواجه می‌شود و این امر سبب می‌شود در مسافت‌های طولانی‌تری بتوان از آن استفاده کرد از این رو در شبکه‌های کامپیوتری دو نوع کابل هم محور از نظر ضخامت وجود دارد:
 نازک، با قطر حدوداً 6.5mm معروف به Thin.
 ضخیم، با قطر حدوداً 13mm معروف به Thick.



شکل ۷-۳

کابل Thin از Thick سبکتر و انعطافپذیرتر بوده و ارزانتر است اما در فواصل کوتاهتری بکار می‌رود از طرفی وزن کابل Thick بعلاوه قطر بیشتر آن زیاد شده قیمت آن افزایش یافته، انعطاف پذیری آن کمتر شده و کار با آن سخت‌تر می‌شود اما در عوض نسبت به Thin در فواصل طولانی‌تری استفاده می‌شود. سابقاً نوع خاصی از کابل کوکس Thin معروف به RG58 در شبکه‌های کامپیوتری استفاده بیشتری داشت که آنرا دقیق‌تر بررسی می‌کنیم. RG58 در سه مدل موجود است:

- (۱) RG58 U : که در آن، هسته تک رشته (مفتولی) است. در اصطلاح معروف است به Solid Core
- (۲) RG58 A/U : که در آن، هسته چند رشته (افشان) است. در اصطلاح به آن Stranded Core می‌گویند که انعطاف پذیری بیشتری نسبت به RG58 U دارد.
- (۳) RG58 C/U : نسخه نظامی A/U، در اصطلاح Military Version of A/U که مناسب برای کاربرد در محیط‌های نظامی و صنعتی است.

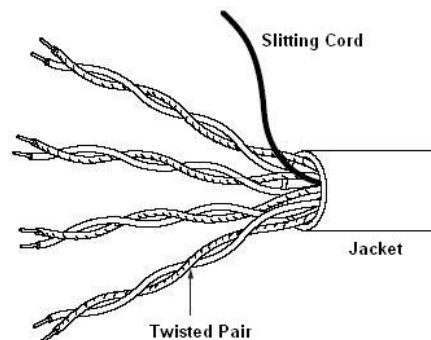


شکل ۷-۳

نکته: بطور کلی سیم‌های مفتولی و افشان علاوه بر تفاوت در انعطاف‌پذیری، در مشخصه الکتریکی (تحت فرکانسهای زیاد) نیز با هم فرق دارند (اثر پوسته‌ای یا Skin Effect) اما این تفاوت در شبکه‌های کامپیوتری با توجه به فرکانس مورد استفاده و شدت جریان پایین چندان مد نظر نبوده و فقط مشخصه مکانیکی یعنی انعطاف‌پذیری مهم است.

۴-۲-۳- کابل Twisted Pair = TP :

این کابل که در مخابرات کاربرد فراوانی دارد تشکیل شده از یک زوج سیم که بهم تابیده شده‌اند :



شکل ۸-۳

علت تابیدن سیم‌ها بهم آنست که اولاً میدانی را در اطراف خود القا نکنند ثانیاً اثرات نویز القا شده روی خود را خنثی کنند. در عمل کابل‌های TP از چندین زوج بهم تابیده تشکیل می‌شوند و هر زوج برای یک کانال مخابراتی مورد استفاده قرار می‌گیرد. البته می‌توان از تکنیک‌های TDM یا FDM استفاده کرده و چندین کانال مخابراتی را نیز بطور همزمان از یک زوج عبور داد.

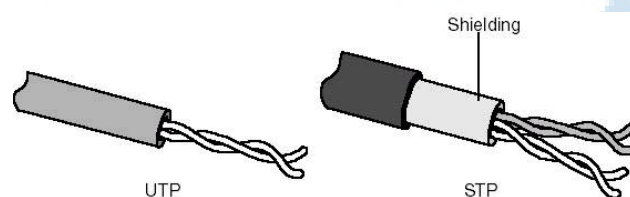
- مزایا و معایب این کابل نسبت به هم محور به اختصار عبارتند از:
- مزیت: ارزانتر بوده و در شبکه مخابرات به وفور از آن استفاده می‌شود.
 - معایب: ۱ - نسبت به هم محور، نویز روی TP اثر بیشتری دارد.
 - ۲ - بروز یک مشکل جدید بنام هم شنوایی یا Cross Talk.

مزیت یاد شده باعث شد تا طراحان شبکه، ایده استفاده از این کابل را در شبکه های کامپیوتری در ذهن خود پرورش دهند و این امر باعث پیدایش مودمها شد. مودم وسیله ای است که اجازه می دهد تا از طریق بستر مخابراتی موجود که مملو از کابلهای TP است یک شبکه کامپیوتری در ابعاد WAN (و البته سرعت نسبی پایین) برقرار کنیم.

سپس متخصصان شبکه به فکر استفاده از کابلهای TP با کیفیت بهتر و بطور مستقل از مخابرات در ابعاد شبکه های LAN افتادند و این امر با پیدایش کارتهای شبکه مناسب که کابل TP به آنها متصل می شد محقق شد. امروزه اکثر شبکه های LAN از این کابل بهره برده و توپولوژی آنها نیز ستاره ای است. از طرفی عیب یاد شده در این کابلها باعث شد تا نوعی خاص از TP که دارای حفاظ نیز باشد ساخته شود که به کابل STP معروف شد. بنابراین کابلهای TP در حالت کلی به دو نوع تقسیم می شوند:

UTP = Unshielded Twisted Pair

STP = Shielded Twisted Pair



شکل ۹-۳

مورد مصرف کابلهای STP نسبت به نوع معمولی آن یعنی UTP در محیطهایی است که اثرات میدانهای الکترومغناطیسی در آنها قویتر است. البته بدیهی است که یک کابل STP نسبت به کابل هم محور Thin گرانتر است و لذا مزیت آن یعنی "ارزانتر بودن" زیر سوال می رود اما با توجه به اینکه در شبکه های LAN ابعاد محدود بوده و فواصل کوتاه است این "گرانی" چندان خود را نشان نمی دهد.

در هر صورت تکنولوژی، سرمایه گذاری خود را در شبکه های کامپیوتری بر روی کابلهای TP اعم از UTP یا STP گسترش داده و کار چندان با هم محور ندارد.

اکثر کابلهای TP متداول در شبکه از ۴ زوج که در کنار یکدیگر تحت یک پوشش کلی قرار گرفته اند. از طرفی گفتیم که بهم تابیدن سیمها باعث می شود تا میدانی در اطراف سیمها القا نشود اما این موضوع قطعی نبوده و به هر حال یک زوج سیم بهم تابیده که از آن جریانی عبور می کند باعث القای میدانی هر چند ضعیف در اطراف خود می شود و همین می تواند سبب ایجاد اختلال در زوجهای مجاور شود. زوجهای مجاور نیز هر کدام بنوبه خود چنین مشکلی را برای بقیه بوجود می آورند. به این پدیده اصطلاحاً همشنوایی یا Cross Talk گفته می شود و اکثر ما تجربه آنرا بصورت "خط روی خط افتادن" در مخابرات داشته ایم. بعنوان مثال دیگری از این پدیده، یک جمع کوچک را تصور کنید مثلاً شامل ۸ نفر که افراد دو به دو گروه بندی شده و همزمان اعضای هر گروه با یکدیگر صحبت می کنند. هر چقدر هم افراد آهسته صحبت کنند با اینحال روی بقیه تأثیر گذاشته و برای دیگران حکم نویز و پارازیت و اختلال را دارد. برای کاهش این اثر چه پیشنهادی دارید؟

پاسخ را در تبصره ۵ همین بخش خواهیم دید. کابلهای TP صرف نظر از UTP یا STP، بر اساس حداکثر سرعت و نوع کاربردی که در شبکه ها دارند به چند دسته یا Category تقسیم می شوند که عبارت است از :

جدول ۱-۳

نام گروه	سرعت	کاربرد
Category 1 = Cat 1	-	مورد مصرف در شبکه های مخابراتی
Category 2 = Cat 2	4 Mbps	مورد مصرف در شبکه های با سرعت حداکثر

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

*: کابل CAT 4 توانایی انتقال تا نرخ 20 Mbps را نیز دارد اما در عمل شبکه هایی که از این کابل بهره می‌برند تا حداکثر 16 Mbps از آنرا استفاده می‌کنند.

** : در برخی از متون به 1000 Mbps نیز اشاره شده اما بهتر است اطمینان نکرده و برای سرعتی 1000 از کابلهای با نمره بالاتر مثلاً Cat5e یا Cat 6 استفاده کنیم.

بطور کلی در مورد همه کابل های فوق دقت داشته باشید که سرعتی نوشته شده الزاماً بیانگر حداکثر ظرفیت کابل نیست بلکه بیانگر سرعت تجهیزاتی است که از آنها برای انتقال اطلاعات استفاده می‌کنند. بعنوان مثال یک زوج از Cat 3 تا حدود 30 Mbps نیز می‌تواند اطلاعات را از خود عبور دهد و در نوع خاصی از شبکه ها که بعداً به آن اشاره خواهیم کرد، ۳ زوج از یک کابل Cat3 با هم می‌توانند تا 100 Mbps اطلاعات را عبور دهند. کابل Cat3 در مجموع دارای ۴ زوج یا ۸ رشته سیم است.

در مورد Cat1 سرعت را عنوان نکردیم؟ علت آنست که برای انتقال اطلاعات از طریق شبکه مخابرات معمولاً از مودم استفاده می‌کنیم و مودمها نیز انواع گوناگون با تکنولوژیها و استانداردهای متفاوت داشته و سرعت در آنها متنوع است. همچنین سرعت در شبکه های مخابراتی که در واقع از دیدگاه کامپیوتری یک شبکه WAN محسوب می‌شود بستگی به فاصله، شرایط محیطی، کیفیت خطوط و اتصالات و همچنین تقویت کننده های بین راه دارد. لذا ترجیح دادیم حرفی از سرعت به میان نیاوریم با این حال از تجارب شخصی هر کس می‌داند که مثلاً با استفاده از مودمهای Dial up از نوع آنالوگ و در صورت مطلوب بودن شرایط می‌توان تا سرعتی حدوداً 33 Kbps دست پیدا کرد و یا با استفاده از مودمهای DSL که در واقع دیجیتالی هستند می‌توانیم در فواصل کوتاه (تا حداکثر ۳ کیلومتر) و شرایط مطلوب به سرعتی حدوداً 2 Mbps هم دسترسی داشته باشیم.

رایج ترین شبکه های LAN به لحاظ سابقه تاریخی آنها تا به امروز عبارتند از:

کابل Thin Coax RG58 با سرعت 10 Mbps در توپولوژی خطی : تقریباً منسوخ شده اند.

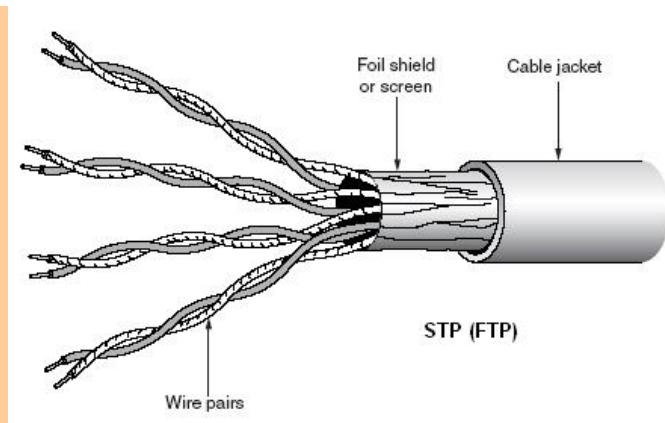
کابل Twisted Pair Cat3 با سرعت 10 Mbps در توپولوژی ستاره ای : تقریباً منسوخ شده اند.

کابل TP Cat5 یا Cat5e با سرعت 100 Mbps در توپولوژی ستاره ای : امروزه بسیار رایج است.

کابل TP Cat5e یا Cat6 با سرعت 1000 Mbps در توپولوژی ستاره ای : رفته رفته جای خود را باز می‌کنند.

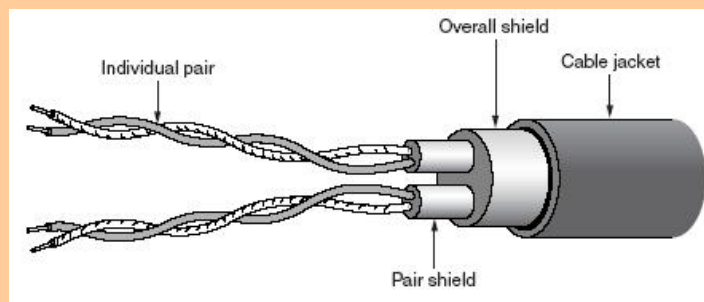
مطالعه آزاد

مکن است به کابلهای TP که از فویل آلومینیوم بعنوان حفاظ استفاده می‌کنند اصطلاحاً FTP گفته شود.



شکل ۳-۱۰

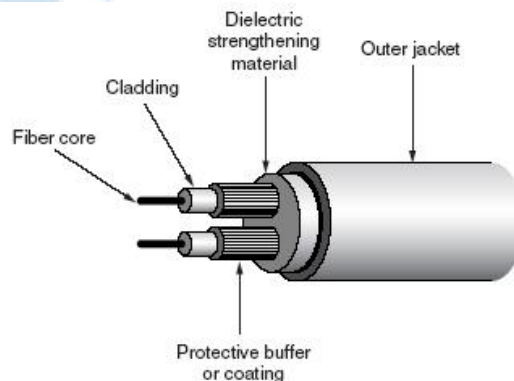
برخی از کابل‌های TP برای هر زوج نیز یک حفاظ در نظر می‌گیرند اعم از کلاف سیمی بافته شده (زره) یا فویل آلومینیوم و مزیت آن‌هم در آنست که Cross Talk را کم می‌کند. در برخی علاوه بر آنکه هر زوج دارای حفاظ خاص خود است، یک حفاظ کلی نیز روی همه آنها کشیده می‌شود و در نتیجه واژه‌های SFTP، FFTP، SFTP، FFTP برای توصیف آنها بکار می‌روند. در هر صورت هرچه که باشند دارای حفاظ بوده و در محیط‌های نویزی تا حد مجاز تعریف شده می‌توانند بکار روند.



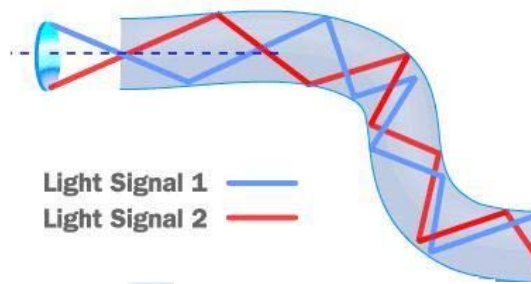
شکل ۳-۱۱

۵-۲-۳- کابل نوری (Fiber Optic = FO) :

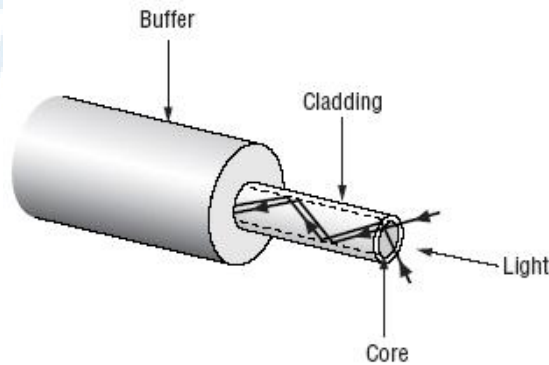
فیبر نوری از ترکیبات خاص پلاستیک فشرده یا سیلیس ساخته می‌شوند و می‌تواند پالس‌های نور را از یک سمت به سمت دیگر هدایت کند (شکل ۳-۱۲).



شکل ۳-۱۲ ساختمان فیبر نوری

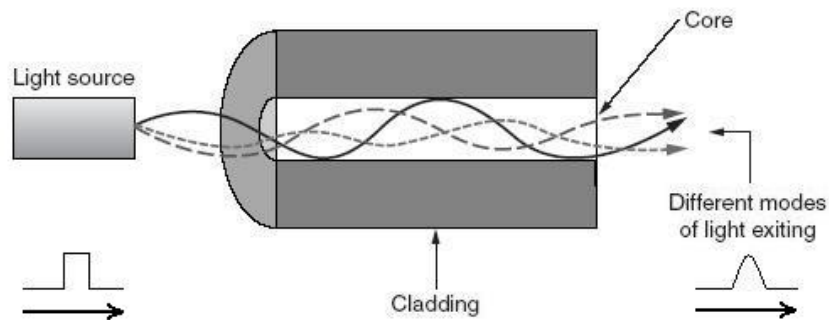


شکل ۱۳-۳- هدایت نور در فیبر نوری



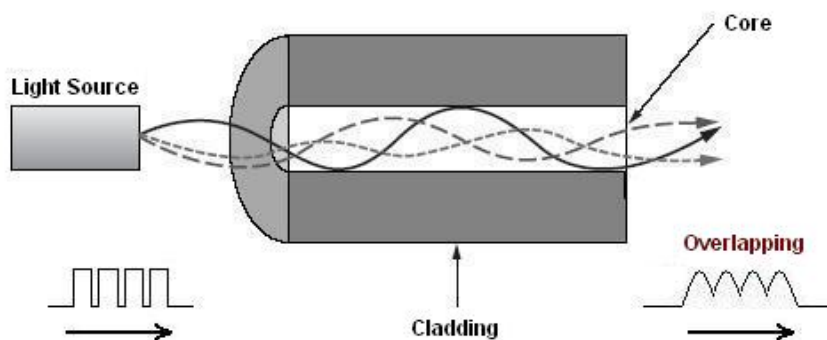
شکل ۱۴-۳

قسمت مرکزی کابل که نور از آن عبور می‌کند معروف به هسته (Core) بوده و لایه انعکاس دهنده نیز به Clad مشهور است. جنس Core/Cladding هر دو یکی است و تفاوت در ضریب شکست شان است. همانطور که از شکل ۱۵-۳ نشان داده شده است وقتی یک پالس نوری از ابتدای خط ارسال می‌شود بدلیل اختلاف مسیر در شعاعهای مختلف نور، پالس خروجی به همان شکل نبوده و کمی تغییر شکل می‌دهد:



شکل ۱۵-۳

حال چنانچه فرکانس فرستنده از حد معینی بیشتر شود پالسهای خروجی با یکدیگر همپوشانی پیدا می‌کنند (Overlapping) و این باعث بروز خطا می‌شود. چنانچه ضخامت هسته طوری باشد که اجازه عبور چندین شعاع نوری را در زوایای مختلف بدهد به آن کابل نوری MM = Multi Mode گفته می‌شود.



شکل ۱۶-۳

مزایای کابل نوری با توجه به خصوصیات آن عبارتست از:

- امکان استفاده در فواصل طولانی‌تر.
- نرخ انتقال بیشتر.
- عدم نویزپذیری نسبت به میدانهای الکترومغناطیسی.
- امنیت بیشتر. سرقت اطلاعات از سیمهای فلزی بوسیله اتصال مستقیم یک سیم بصورت انشعاب و یا بطور غیر مستقیم از طریق القای امواج، امریست امکان‌پذیر، اما در مورد فیبرهای نوری بدلیل ظریف بودن هسته نمی‌توان بر راحتی و بدون صرف وقت و امکانات از کابل انشعاب گرفت ضمن آنکه القای امواج نیز در مورد فیبر نوری بی‌معنی است. بنابراین سرقت اطلاعات از فیبرنوری بسیار دشوارتر از سیمهای فلزی است و در نتیجه امنیت انتقال اطلاعات از طریق فیبرنوری بیشتر است.
- ارتباط راحت مابین ساختمانهای مختلف که دارای چاههای ارت مستقل از یکدیگرند. (عدم بروز پدیده Ground Loop)

فرض کنید که ارتباط شبکه‌ای مابین ۲ ساختمان از طریق کابل هم محور باشد. برای دفع نویز بسمت زمین و جلوگیری از تأثیرگذاری آن روی اطلاعات، قسمت حفاظ کابل هم محور به Earth متصل می‌شود. حتی اگر حفاظ مستقیماً به ارت وصل نباشد، از طریق کانکتور متصل به آن و بدنه یکی از کامپیوترها که با ارت ارتباط داشته باشد به زمین وصل می‌شود. چنانچه چاه ارت هر دو ساختمان یکی باشد مشکلی بروز نمی‌کند اما اگر ساختمانها دارای چاههای ارت جداگانه‌ای باشند در آن صورت بعلمت مغایرت بین مشخصات فیزیکی چاهها از نظر رطوبت نسبی و . . . ، جریانی ضعیف از یکسو به سوی دیگر برقرار می‌شود که اصطلاحاً به آن Ground Loop گفته می‌شود. این جریان در واقع خود بعنوان یک عامل مزاحم محسوب می‌شود. حال اگر ارتباط مابین ساختمانها را از طریق فیبرنوری برقرار کنیم Ground Loop در کار نخواهد بود چون از فیبرنوری اساساً الکتریسته عبور نمی‌کند.

تحقیق، در مورد ترکیبات روکش انواع کابلها ی نوری و خصوصیات آن تحقیق کنید

ضد جوندگی: Anti Rodent

ضد رطوبت و آب: Anti Humidity, Water Blocking

روکش مسلح: Armored

ضد تولید گاز سمی: Halogen Free (Plenum Grade)

۳-۳- کابل کشی UTP

مراحل مهم پیاده سازی سخت افزاری یک شبکه کامپیوتری را می‌توان به ترتیب زیر بیان کرد.

- تصمیم‌گیری در مورد نوع شبکه
- تهیه نقشه اجرایی
- انتخاب و تهیه سخت افزار مورد نیاز

- نصب تجهیزات
- کابل کشی و نصب کابل
- برقراری اتصالات

۱-۳-۳- طراحی و اجرای عملیات کابل کشی:

نکات مهم هنگام طراحی و اجرای عملیات کابل کشی: کابل های "فلزی" مانند کابل هم محور یا Twisted Pair تحت تأثیر میدان های الکترومغناطیسی فضای اطراف خود قرار گرفته و روی آنها Noise ایجاد می شود. اینگونه میدانها در مجاورت کابل های برق و مخصوصاً وسایل الکتریکی دارای "سیم پیچ" مانند انواع الکتروموتورها اعم از کاربردهای خانگی یا صنعتی و انواع ترانسفورماتورها و ترانسفورمرها بیشتر بوده و بطور کلی باید از عبور کابل در مجاورت نزدیک با کابل برق یا وسایل فوق پرهیز کرد:



شکل ۱۷-۳

چنانچه کابل های برق و شبکه به موازات هم باشند در آن صورت حداقل فاصله ای که باید بین آنها رعایت شود بستگی به شدت میدان الکترومغناطیسی کابل برق دارد که آنهم تابعی است از جریان الکتریکی عبوری از کابل. در عمل بسته به این شدت جریان، حداقل از 5 Cm تا 30 Cm یا بیشتر فاصله بین کانال های برق و شبکه قرار می دهند.

۲-۳-۳- Duct

به کانال هایی که روی دیوار برای عبور کابل نصب می شود اصطلاحاً Duct یا Trunk گفته می شود و از نظر جنس بر دو نوعند: پلاستیکی و فلزی.



شکل ۱۸-۳

نکته برخی از کانالها دارای ۲ یا ۳ قسمت مجزا هستند و از آنها می توان برای عبور کابل های برق و شبکه در کنار هم استفاده کرد اما بدیهی است که در اینگونه موارد باید:

اولاً دیواره حایل بین قسمتها باید ترجیحاً فلزی بوده ثانیاً شدت جریان عبوری از کابل برق زیاد نباشد ثالثاً کابل شبکه در صورت امکان دارای حفاظ باشد رابعاً بدنه کانال اگر فلزی است به Earth متصل شود.

۳-۳-۳- عوامل موثر در تعیین نوع کابل کشی:

- سنگینی ترافیک شبکه ،
- طول کابل کشی
- بودجه تعیین شده برای کابل کشی
- نیازهای ایمنی شبکه
- نوع کابل کدام های موجود

جدول ۲-۳ خلاصه مقایسه کابلها

مشخصات	کواکسیال نازک	کواکسیال ضخیم	زوج به هم تابیده	فیبر نوری
هزینه کابل طول کابل segment سرعت انتقال نصب	ارزان ۱۸۵ متر ۱۰Mbps	گران ۵۰۰ متر ۱۰Mbps	ارزان ۱۰۰ متر ۴ تا ۱۰۰ Mbps	متوسط ۲ کیلومتر (۹۰ کیلومتر) ۱۰۰Mbps یا بیشتر (بیشتر از 1Gbps) نصب دشوار (نیاز به متخصص و تجهیزات مخصوص دارد) مستعد تداخل نمی باشد. از داده ها ، صوت و تصویر ، با ایمنی بالایی پشتیبانی می کند.
تداخل	مقاومت خوب در مقابل تداخل	مقاومت خوب در مقابل تداخل	مستعد برای تداخل	
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.	

۴-۳-۳- اهمیت Earth:

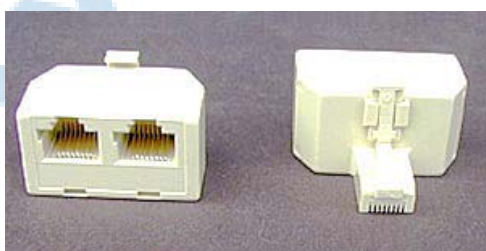
ارت بعنوان يك عامل مهم در تخلیه نویز در کابلهاي داراي حفاظ بشمار می رود (مانند کابل هم محور یا STP). چنانچه در شبکه اي از این کابلها استفاده شود و حفاظ به ارت متصل نشود کارکرد شبکه توأم با اختلال خواهد بود که این اختلال بشکل خطا در انتقال اطلاعات، کندی سرعت و حتی قطعی موقتی خود را نشان می دهد. بنابراین توصیه می شود حتماً چاه ارت مناسب برای کامپیوترها، شبکه و تجهیزات مربوطه تهیه شده و هرگز از ارت مربوط به برقگیر (که روی بام برجها نصب می شود) برای شبکه استفاده نشود.

۵-۳-۳- تجهیزات مورد نیاز برای اتصال کابل به کانکتور

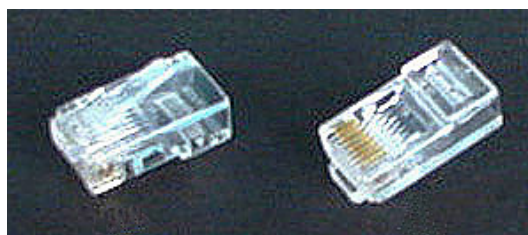
تجهیزات مورد نیاز برای ایجاد کابل های UTP عبارتند از :

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

که در شکل ۱۹-۳ نشان داده شده است.



ب



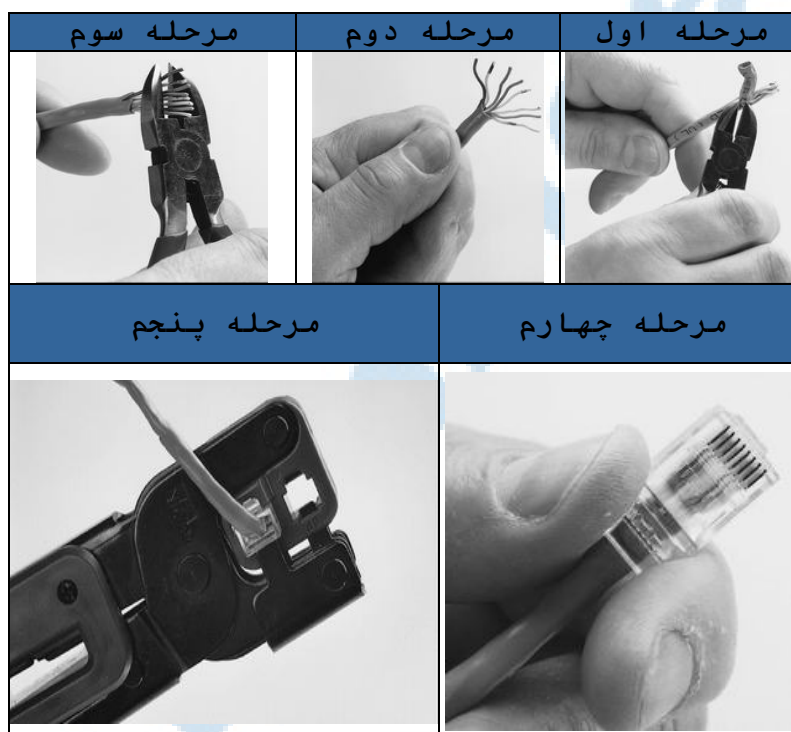
الف



ج
شکل ۱۹-۳

۶-۳-۳- ایجاد کابل Straight

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



شکل ۲۰-۳

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 گیگاترنت 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 عموماً 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 (مثلاً 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 .

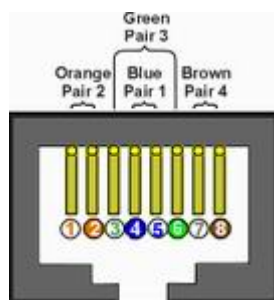
به منظور کابل کشی کابل های UTP از دو استاندارد متفاوت با نام T-568B (یا EIA) و T-568A (یا T&AT ، A۲۵۸) ، استفاده می گردد . تنها تفاوت موجود بین آنان ترتیب اتصالات است .

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	TxDat+
دو	نارنجی	دوم	TxDat-
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

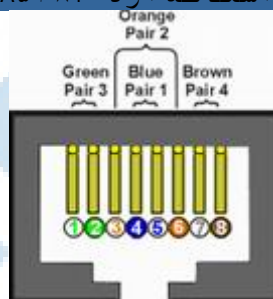
شماره پین های استاندارد T568A

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	

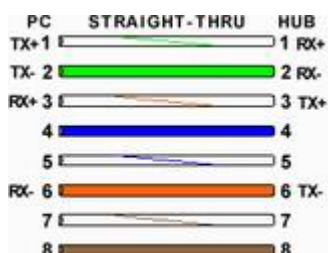
استاندارد A۵۶۸T



شکل ۲۲-۳

موارد استفاده کاربرد کابل straight

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



شکل ۲۳-۳

شکل ۲۳-۳ 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 ولی 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 شماره 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 .

۷-۳-۳- 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



شکل ۲۴-۳

کابل CAT5 X-over

به منظور ایجاد کابل های کراس CAT5 صرفاً از یک روش استفاده می گردد . همانگونه که قبلاً 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 ۳-۲۵

همانگونه که در شکل ۳-۲۵ 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 ، معمولاً از درگاه uplink استفاده می گردد. درگاه فوق ، 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 :

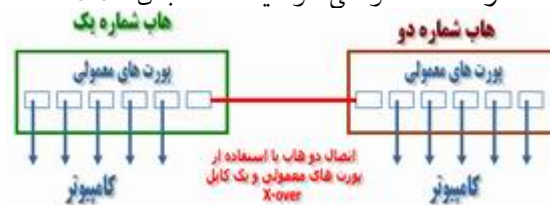
اتصال دو هاب با استفاده از درگاه Uplink
و یک کابل Straight



شکل ۳-۲۶

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 درگاه های 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
درگاه معمولی و یک کابل X-over



شکل ۳-۲۷

۳-۴- کارت شبکه و وظایف آن

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

شکل ۳-۲۸ ۵-۱۶ ص ۳۴ آشنایی با شبکه

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 می‌کند و آن را به داده های قابل پردازش در CPU تبدیل می‌کند

آماده سازی داده ها : قبل از آنکه داده ها بتوانند از طریق شبکه ارسال شوند ، کارت شبکه باید آن را 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 می‌نمایند . آنها چندین مسیر داده ای هستند که به طور موازی و پهلوئی هم قرار گرفته اند ، چون چندین مسیر پهلو به پهلو هستند ، داده ها می‌توانند 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 می‌کنند گفته می‌شود به صورت انتقال سریال (serial) حرکت می‌نمایند زیرا هر بیت به دنبال بیت دیگر جریان دارد . به عبارت دیگر ، کابل بزرگراه یک بانده می‌باشد . داده ها در این بزرگراه ها همیشه در هر لحظه فقط یک بانده حرکت دارند . کامپیوتر ها یا داده ها را می‌فرستند و یا در یافت می‌دارند .

کارت شبکه ، عبور داده ها را به صورت موازی و به شکل گروهی می‌گیرد و آنها را طوری مجدداً می‌سازد که از طریق مسیر سریال به پهنای ۱ بیت در کابل شبکه جریان یابند . این کار با تبدیل سیگنالهای دیجیتالی کامپیوتر به سیگنالهای الکتریکی ونوری که می‌توانند از طریق کابلهای شبکه حرکت نمایند انجام می‌گیرد . قطعه مسئول این کار ، فرستنده گیرنده (Transceiver) است .

۳-۴-۲- آدرس شبکه

علاوه بر تبدیل داده ، کارت شبکه محل کارت یا آدرس را به باقیمانده شبکه نشان می‌دهد تا از تمام کارتهای دیگر شبکه تمیز داده شود . آدرسهای شبکه از کمیته IEEE (تلفظ می‌شود آی تریپل ای ، مخفف انستیتوی مهندسان برق والکترونیک) تعیین می‌گردد . این کمیته ، محدوده ای از آدرسها را به هریک از سازندگان کارتهای شبکه اختصاص می‌دهد . 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 شبکه‌های که آنها را اداره می کنند حرکت نمایند. به این دلیل داده به بافر (RAM) کارت فرستاده می شوند و 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 ، عملاً 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 موافق باشند:

- میزان داده های ارسالی قبل از تایید
- هرکارت قبل از سرریز شدن داده چه مقدار داده را می تواند نگهداری 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 جزئیات ارتباط تعیین گردید ، دو کارت ، شروع به ارسال و دریافت داده ها می نمایند.

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

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

- وقفه (Interrupt) IRQ
- 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 فرخته 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 وقفه 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 به CPU 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/O: درگاه ورودی / خروجی (I/O) پایه مسیری را مشخص می کند که از طریق آن داده ها بین سخت افزار کامپیوتر (از قبیل 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 درگاه I/O پایه متفاوتی داشته باشد . آدرسهای پایه پورتهای (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 استاندارد ISA (آیزا) و PCI (پی سی آی) اشاره نمود . هنوع گذرگاه به طوری فیزیکی از سایر گذرگاه ها جداست . ضروری است که کارت شبکه و گذرگاه هماهنگ باشند .

نکته : امروزه بیشتر بردهای اصلی دارای کارت شبکه به صورت On Board هستند و از گذرگاه های داخلی برد اصلی استفاده می کنند .

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 . هنوع 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 از کابل 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 از طرف 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 برخوردار (CSMA/CD)
- روش عبور نشانه (Token passing)

۱-۵-۳- روش دسترسی چندگانه تشخیص حامل باتشخیص برخوردار (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 داشته باشند ، تا زمانی که داده ها به مقصد خود برسند و کابل مجددا آزاد گردد ، هیچ کامپیوتری داده ای را انتقال نمی دهد .

اگر دو یا 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 کشف شناخته می شود زیرا کامپیوتر های شبکه برای به دست آوردن فرصتی در ارسال داده ها ، با هم رقابت یا کشف 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 برخوردها با 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 کامپیوتری 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 ، کشف و برخوردی پیش نمی آید و حتما پس از طی زمانی مشخص ، نوبت ارسال داده به هر کامپیوتر خواهد رسید .

خود آزمایي و تحقیق

- ۱- توپولوژی چیست؟ انواع آن را شرح دهید.
- ۲- پدیده برخورد یا Collision در کدام یک از انواع توپولوژی روی می دهد؟ چرا؟
- ۳- در کدام یک از انواع توپولوژی، با قطع شدن قسمتی از کابل، کل شبکه از کار می افتد؟
- ۴- انواع توپولوژی ها را از لحاظ مصرف کابل، سرعت، هزینه، عیب یابی و اشکال زدایی مقایسه کنید.
- ۵- انواع محیط های انتقال سیمی یا کابلی را از لحاظ سرعت، امنیت، هزینه، مسافت و نویز بررسی کنید.
- ۶- حداقل فاصله بین کابل شبکه و کابل برق باید چقدر باشد؟
- ۷- عوامل موثر در تعیین نوع کابل را نام ببرید.
- ۸- سرعت کدام یک از روش های دسترسی به خط بیشتر است؟ دلیل آن را بنویسید.
- ۹- چه عواملی در سرعت دسترسی به خط موثر است؟
- ۱۰- تحقیق کنید که آیا می توان در کابل کشی یک شبکه از همه انواع کابل (مانند Cat5، Cat6، Fiber و...) استفاده کرد؟ سرعت و راندمان شبکه در این حالت چگونه است؟
- ۱۱- تحقیق کنید که برای اتصال چندین Switch یا HUB از چه نوع کابلی باید استفاده گردد؟

فصل چهارم - معماری شبکه

هدف های رفتاری

انواع معماری شبکه و ویژگیهای آن ها را شرح دهد.

تکنولوژی FDDI را تعریف 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^۱
- Token Ring

۱-۴-۱-۱- اترنت

اترنت یکی از انواع متداول معماری شبکه است . در این 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 مثلاً 10Base2 با سرعت 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

^۱ -Ethernet

10Base 2 برای 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 و دوسرکابل باید به وسیله ی Terminator مسدود شود تا شبکه فعال شود . از مزایای 10Base 2 نصب ساده و هزینه راه اندازی بسیار کم آن است . توپولوژی 10Base 2 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 اتصال T-connector به کامپیوتر نباید از استفاده کرد و باید آن را مستقیماً به کامپیوتر متصل نمود.
- فاصله اولین و آخرین کامپیوتر در شبکه نباید بیش از ۱۸۵ متر باشد . این فاصله از روی اندازه کابل اندازه گیری می شود .
- با استفاده از هاب یا Repeater می توان حداکثر فاصله بین اولین و آخرین کامپیوتر را تا ۹۲۵ متر افزایش داد کامپیوتر ترهان باید خارج از این محدوده باشند.
- در فواصل بین هر دو Repeater می توان بیش از ۳۰ دستگاه کامپیوتر به شبکه متصل کرد.
- ابتدا و انتهای کابل باید با Terminator مسدود شود . Terminator شبکه 10Base2 ، یک مقاومت ۵۰ اهمی است که 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 5 از 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 Terminator مسدود می شود . اولین مزیت 10Base5 مسافت نسبتاً 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 10Base5 نیز صادق است .

شکل ۲-۴ (ص ۸۵) مفاهیم

شبکه

10Base T

برای راه اندازی شبکه 10Base T از کابل های TP یا زوج به هم تابیده استفاده می شود که حداکثر سرعت آن 10Mbps است. در این استاندارد هر کامپیوتری که می خواهد به شبکه متصل شود مستقیماً 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 Category5 باشند (نوع کابل از نظر داشتن محافظ تفاوتی نمی کند ، می توان از هر دو کابل UTP یا STP استفاده کرد) .
- حداکثر فاصله هر کامپیوتر تا هاب ، ۱۰۰ متر است .
- حداقل طول کابل (فاصله بین کامپیوتر تا هاب) ۲/۵ متر است .

شکل ۳-۴ (ص ۸۶) 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 10Mbps 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 و برای اتصال دو تقویت کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قرار دارد ، 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 شبکه 10BaseT 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 از نوع 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 :

1000Base sx -۱

1000Base LX/LH -۲

1000Basezx -۳

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

1000Base T

در این استاندارد، از کابل های زوج به هم تابیده برای راه اندازی شبکه ای با سرعت یک گیگابایت در ثانیه استفاده می شود. این کابل ها از نوع Cat5 و کانکتورهای آن نیز از نوع RJ-45 است. نحوه ارسال اطلاعات در این استاندارد به گونه ای است که سیستم، توانایی انتقال اطلاعات با سرعت یک گیگابایت در ثانیه را پیدا می کند. کابل Cat5 نام دیگر کابل زوج به هم تابیده است.

Token Ring ۴-۱-۲

شبکه Token Ring از نظر ظاهری یک شبکه ستاره ای است ولی به صورت Token Passing کار می کند. در این شبکه یک حلقه منطقی به وجود می آید و Token در امتداد حلقه حرکت کرده و به کامپیوترها می رسد. هر کامپیوتری که به ارسال اطلاعات نیاز داشته باشد، Token را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت Token مسیر خود را طی می کند تا به کامپیوتر مقصد برسد. کامپیوتر مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به

¹ -Synchronous Ethernet

نام Acknowledge به کامپیوتر مبدأ ارسال می‌کند. کامپیوتر مبدأ نیز Token اصلی را از بین برده و یک Token جدید تولید می‌نماید و آن را در امتداد مسیر Token قبلی به حرکت در می‌آورد. این روند به همین صورت ادامه خواهد یافت.

در شبکه Token Ring در محل اتصال کامپیوترها به جای هاب از دستگاهی به نام MAU استفاده می‌شود. سرعت انتقال اطلاعات در این شبکه 4Mbps یا 16Mbps است. کارتهای 16Mbps می‌توانند با سرعت 4Mbps نیز فعالیت کنند.

شکل ۴-۴ (مفاهیم شبکه)

در شبکه Token Ring از کابل‌های زوج به هم تابیده استفاده می‌شود. اگر از کابل UTP در این توپولوژی استفاده شود، حداکثر طول کابل می‌تواند ۴۵ متر باشد و این شبکه فقط با سرعت ۴ مگابیت در ثانیه کار می‌کند و اگر از کابل STP استفاده شود، حداکثر طول کابل ۱۰۱ متر و با سرعت ۱۶ مگابیت در ثانیه اطلاعات منتقل می‌شود.

FDDI ۴-۲

FDDI، تکنولوژی یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده می‌کند. در این تکنولوژی به جای فیبر نوری می‌توان از کابل مسی نیز استفاده کرد ولی در صورت استفاده از کابل مسی حداکثر فاصله مجاز در شبکه کمتر می‌شود. FDDI به عنوان Backbone در محل‌هایی که تعداد زیادی کامپیوتر در آن قرار دارد، استفاده می‌شود. از جمله این محیط‌ها می‌توان به دانشگاه‌ها اشاره کرد. در FDDI می‌توان ۵۰۰ گره را در مسافت ۱۰۰ کیلومتر به یکدیگر متصل کرد. توپولوژی فیزیکی این شبکه حلقوی است. نحوه به وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر نوری ساخته می‌شود و در هر ۲ کیلومتر یک تقویت کننده قرار می‌گیرد. برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبر نوری به وجود می‌آید، از دو حلقه فیبر نوری در کنار هم استفاده می‌شود تا در صورتی که یکی از رشته‌ها قطع شود، رشته دوم وارد عمل شده و جایگزین رشته اول شود.

خود آزمایی و تحقیق

۱- انواع معماری شبکه را نام ببرید و ویژگیهای هر یک را از لحاظ حداقل و حداکثر طول کابل بین دو کامپیوتر، سرعت و نوع کابل و تجهیزات جانی بررسی کنید.

۲- FDDI چیست؟

۳- برای جلوگیری از اختلالاتی که در اثر قطع شدن فیبرنوری به وجود می آید، چه باید کرد؟

۴- تفاوت اصلی استانداردهای IEEE در چیست؟

۵- تحقیق کنید که تفاوت MAU و HUB در چیست؟

فصل پنجم - آشنایی با پروتکلها

هدف های رفتاری
انواع پروتکلهاي رایج در شبکه تعریف کند.
سرویس های رایج در پروتکل TCP/IP را شناسایی کند.
سرویس های رایج در سبکه اینترنت را شرح دهد.
مفهوم Host در پروتکل TCP/IP را بیان کند.
انواع دامنه های رایج را بیان کند.
مراح ثبت Domain را شرح دهد.
انواع کلاس های IP را شناسایی کند.

بهره برداری از امکانات سخت افزاری و برقراری ارتباط بین اجزای مختلف شبکه نیاز به یک مجموعه از قوانین و دستورالعملهای مشترک دارد که به آن قوانین اصطلاحاً پروتکل می‌گوییم.

مثال : کلاس درس خود را بعنوان یک شبکه در نظر بگیرید. هریک از اجزای این شبکه عبارتند از :
هدف : آرایه سرویس آموزشی

هنرجویان : بعنوان کسر
هنر آموز درس : بعنوان گوش و دهان : بعنوان رابط شبکه
هوا : بعنوان محیط آنه
(Network Interface)

چه چیزی را می‌توان بعنوان پروتکل در کلاس متصور شد ؟
شاید بتوانیم "حضور بموقع هنر آموز درس و هنرجو در کلاس ، داشتن ساعات تنفس بمنظور استراحت ، ارائه درس به زبان قابل فهم هنرجویان (مثلاً فارسی) ، ارائه روشهایی منظم بمنظور پرسش و پاسخ ، برگزاری آزمون و . . ." را بعنوان پروتکل کلاس در نظر بگیریم . همانطور که از عبارات فوق پیداست پروتکل مجموعه قوانینی است که اگر آنها را رعایت نکنیم ارائه سرویس آموزشی (یعنی هدف از برقراری شبکه) غیرممکن خواهد شد .

تعریف : پروتکل مجموعه قوانینی نرم افزاری است که رعایت آنها باعث بهره برداری از امکانات سخت افزاری و برقراری سرویس در شبکه می‌شود.

البته در عمل برای هر "تکنولوژی سخت افزاری مدرن " نیاز به نرم افزار مناسب بعنوان "قانون یا پروتکل" برای برنامه ریزی ، مدیریت و بهره برداری از آن داریم و بعبارتی واژه "پروتکل نرم افزاری" ، یک واژه عام در عرصه IT بشمار می‌رود (مثلاً سیستم عامل نرم افزاریست شامل پروتکل های بسیار متنوع برای برنامه ریزی ، بهره برداری و مدیریت منابع مختلف یک کامپیوتر) با این حال نظر به اهمیت واژه "پروتکل" در شبکه های کامپیوتری بطور خاص آنرا مورد بحث قرار می دهیم .

۳ مورد از پروتکلهاي معروف در شبکه ها (مخصوصاً شبکه های متشکل از کامپیوترهاي شخصی) عبارتند از :

الف) NetBEUI

ب) IPX/SPX

ج) TCP/IP

۱-۵ - NetBEUI = NetBIOS Enhanced User Interface

این پروتکل که نسخه اولیه آن به NetBIOS معروف بود به وسیله تیمی برای شرکت IBM طراحی و پیاده‌سازی شد و هدف از آن برقراری ارتباط مابین سیستم‌های مختلف در یک شبکه کوچک بود. در شبکه‌های بزرگ نکات و مسائلی مطرح می‌شود از قبیل امنیت، چگونگی تبادل ترافیک در حجم زیاد، مسیریابی، و . . . که این مسائل در شبکه‌های کوچک اکثراً وجود نداشته یا کم‌رنگ است و چون NetBIOS برای شبکه‌های کوچک طراحی شده بود لذا اینگونه نکات نیز در آن دیده نشد یا بصورت جدی به آن پرداخته نشد. بعنوان مثال، این پروتکل قابلیت مسیر یابی "Routable" ندارد و حجم ترافیک Broadcast در آن زیاد است، می‌دانیم که در شبکه‌های بزرگ، روترها ارتباط مابین بخش‌های مختلف شبکه را برقرار کرده و لذا مسیریابی جزو الزامات در ارتباط بین آنهاست. همچنین در شبکه‌های بزرگ، ترافیک بطور طبیعی از حجم بیشتری برخوردار است لذا باید سعی کرد تا از ایجاد Broadcast حتی‌المقدور خودداری شود و متأسفانه در NetBIOS یا NetBEUI هیچکدام از این مسائل مد نظر قرار نگرفته البته ایرادی به آن وارد نیست چون از ابتدا هدف آن استفاده در محیط‌های کوچک بوده است.

مثال: قوانین وضع شده در حوزه‌های مختلف (مثلاً ترافیکی و امنیتی) برای یک روستای کوچک طبیعتاً با یک شهر بزرگ مانند تهران متفاوت بوده و در تهران مشکلات بسیار بیشتر از یک روستای کوچک است.

بطور خلاصه می‌توانیم ویژگی‌های NetBEUI را مطابق زیر فهرست کنیم. دقت کنید که غیر از مورد اول که جزء مزایای پروتکل است بقیه موارد از نقاط ضعف و عیوب آن بشمار می‌رود:

Very Simple Configuration	۱	پیکربندی بسیار ساده
Small Networks	۲	کاربرد در شبکه‌های کوچک
Non Routable	۳	قابلیت مسیریابی ندارد
High Broadcast Traffic	۴	ترافیک BC در آن زیاد است. * * BC=Broadcast

امروزه این پروتکل تقریباً منسوخ شده است و درمیان محصولات مایکروسافت نیز از XP به بعد بطور مستقیم در لیست پروتکل‌ها دیده نمی‌شود.

نکته: هرچند امروزه اکثر نرم افزارها سرویس‌های شبکه‌ای خود را روی پروتکل TCP/IP عرضه می‌کنند اما با این حال برخی از برنامه‌های قدیمی‌تر هنوز براساس پروتکل NetBIOS یا NetBEUI کار می‌کنند. برای اینگونه برنامه‌ها، مایکروسافت سرویسی را در سیستم عامل‌های ویندوز خود پیش‌بینی کرده که حکم یک واسطه و مبدل را دارد یعنی سرویس‌های NetBIOS را روی بستر TCP/IP ارائه می‌دهد و در نتیجه برای Application محیط NetBIOS شبیه سازی می‌شود. این سرویس معروف به NetBT = NetBIOS over TCP/IP بوده و بطور معمول در کلیه ویندوزها فعال است.

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

پروتکل IPX/SPX به وسیله شرکت Xerox طراحی شد و بعداً به وسیله شرکت Novell تکمیل و مورد استفاده عملی قرار گرفت لذا اکثراً به محض آنکه نام پروتکل را می‌شنوند به یاد Novell می‌افتند. البته در سیستم‌های Novell نسخه‌های 4.0 و عمدتاً 5.0 به بعد، از TCP/IP نیز

می‌توان استفاده کرد. پروتکل IPX/SPX هیچ‌یک از نقاط ضعف NetBIOS را نداشته و بسیار پروتکل قدرتمندی است اما قابلیت TCP/IP باعث شده است که از IPX/SPX کمتر استفاده شود.

مهم ترین ویژگی های این پروتکل عبارتند از :

Simple Configuration	۱ پیکربندی نسبتاً ساده
Any Scale of Network	۲ در هر ابعادی از شبکه، کوچک یا بزرگ قابل استفاده است.
Routable	۳ قابلیت مسیریابی دارد.
Connection Oriented (SPX) & Connection less Services (IPX)	۴ حق انتخاب در انتقال اطلاعات بصورت "عادی" (CL) یا "سفارشی" (CO)
Old Novell Netware Networks	۵ عمدتاً در محیطهایی که سیستم‌عاملهای قدیمی Novell یافت می‌شوند کاربرد دارد.

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

پروتکل TCP/IP در ابتدا به وسیله ی وزارت دفاع آمریکا و در سیستم عامل UNIX ایجاد شد. امروزه این پروتکل تقریباً کلیه رقبا را کنار زده و در اکثر شبکه‌ها اعم از کوچک و بزرگ و به وسیله ی کلیه سیستم‌عاملها پشتیبانی می‌شود. در اهمیت TCP/IP توجه به این نکته کافیست که ارتباط در اینترنت بدون TCP/IP تقریباً غیرممکن است و اکثر سرویسهای اینترنت تحت قوانین TCP/IP عرضه می‌شوند. مهمترین خصوصیات این پروتکل بطور خلاصه عبارتند از :

Supports any network scale (small . . . Large) or (Low Traffic . . . High Traffic)	۱- پشتیبانی انواع شبکه
Supported by all Operating Systems.	۲- پشتیبانی انواع سیستم عامل
Used as a primary protocol in the Internet	۳- مورد استفاده به عنوان پروتکل اصلی
Routable	۴- مسیریابی
Connection Oriented Services (TCP) , Connection less Services (UDP)	۵- حق انتخاب در انتقال اطلاعات به صورت عادی و سفارشی
Multicasting	۷- ارسال گروهی
Complex Configuration	۸- پیکربندی پیچیده

- اولین ویژگی در TCP/IP (همانند IPX/SPX) آنست که می‌تواند در هر ابعادی از شبکه استفاده شود اعم از شبکه‌های کوچک یا بزرگ ، ترافیک کم یا ترافیک زیاد و بالاخره اعم از اینکه به اینترنت متصل باشد یا خیر.
- چون TCP/IP در کلیه سیستم‌عاملهای مدرن امروزی پشتیبانی می‌شود لذا زبان مشترک برای ارتباط بین آنها بشمار می‌رود.
- TCP/IP از ابتدا تا به امروز بعنوان پروتکل اصلی مورد استفاده در اینترنت بوده است.
- در TCP/IP الگوریتم‌های متنوع مسیریابی (Routing) برای انتخاب مسیر بهینه از میان روترها تعبیه شده و بدین سبب یکی از مهمترین پروتکلها برای استفاده در شبکه‌های WAN بشمار می‌رود. همانطور که قبلاً گفتیم در شبکه‌های WAN اغلب توپولوژی حاصله از نوع Mesh است و در نقاط مرزی مابین شبکه‌ها از Router استفاده می‌شود لذا پروتکل مورد استفاده باید دارای قابلیت مسیریابی (Routing) باشد.

- سرویس انتقال اطلاعات بصورت سفارشی "Connection Oriented" معروف به TCP و سرویس انتقال اطلاعات بصورت عادی "Connection less" معروف به UDP از دیگر بخشهای متنوع این پروتکل است.

- Multicasting بمعنی ارسال اطلاعات برای گروهی از استفاده‌کنندگان است.

یادآوری: بطور کلی ۳ نوع مخاطب در شبکه‌ها وجود دارد:

الف) Unicast: ارسال برای فقط یک نفر.

ب) Broadcast: ارسال برای همه تا محدوده مجاز (دفعته).

ج) Multicast: ارسال برای گروهی از استفاده‌کنندگان تا محدوده مجاز (دفعته).

Multicasting از دیگر خصوصیات TCP/IP است که به کمک آن براحتی می‌توان سیستم‌ها، افراد یا نیازها را گروه‌بندی کرده و اطلاعات را برای تمام اعضای گروه ارسال کرد.

فرض کنید که یک دستگاه Multimedia Server می‌خواهد برنامه کاملاً مشخصی، مثلاً فیلمی را برای ۵۰۰ نفر مشترک که در سه شبکه مختلف هستند پخش کند از این تعداد، ۳۰۰ نفر در شبکه اول، ۱۵۰ نفر در شبکه دوم، و ۵۰ نفر در شبکه سوم هستند. ارتباط مابین شبکه‌ها از طریق روترهای R1، R2 و R3 برقرار شده. چه روشهایی را برای پخش برنامه مذکور پیشنهاد می‌کنید؟ حالات مختلف را بررسی می‌کنیم:

الف) کلیه مشترکین هرکدام یک به یک با سرور ارتباط برقرار کرده و سرور برای هرکدام بطور جداگانه برنامه را پخش کند. بعبارت دیگر بصورت Unicast.

ب) سرور برنامه را Broadcast کند که در این صورت با ۲ مشکل مواجه می‌شویم:

۱- Broadcast ترافیک شبکه را افزایش داده ضمن آنکه بقیه کاربران دیگر که نیازی به دریافت برنامه را از سرور ندارند درگیر ترافیک ناخواسته می‌شوند.

۲- روترها اجازه عبور ترافیک Broadcast را نمی‌دهند لذا مشترکین شبکه‌های شماره ۲ و ۳ قادر به دریافت برنامه نخواهند بود.

ج) کلیه مشترکین را در یک گروه قرار داده و سرور برنامه را برای گروه Multicast کند. روترها نیز طوری پیکربندی می‌شوند که ترافیک Multicast را عبور دهند.

پرسش: به نظر شما کدامیک از راه‌حلهای فوق بهتر بوده و ترافیک کمتری را ایجاد می‌کند؟

بالاخره آخرین خصوصیت TCP/IP که در واقع عیب آن بشمار می‌رود اینست که پیکربندی پیچیده‌ای دارد. علت این پیچیدگی را می‌توان در تنوع سرویسهای ارائه شده جستجو کرد. TCP/IP بسیار پروتکل کامل و متنوعی است و طبیعتاً این تنوع، پیچیدگی در پیکربندی را بدنبال خواهد داشت. البته تعبیه‌کنندگان TCP/IP تمهیداتی اندیشیده‌اند تا قدری از پیچیدگی پیکربندی در آن کاسته شود (Automatic/Dynamic Configuration) و در واقع در اغلب اوقات، کاربران نیازی به درگیر شدن با پیچیدگی‌های پیکربندی ندارند.

۴-۵- سرویسهای TCP/IP

TCP/IP از سرویس‌های متنوعی تشکیل شده که اغلب نیازهای کاربران در شبکه‌ها را مستقیماً و بدون نیاز به هرگونه برنامه‌نویسی اضافی پاسخ می‌دهد. اغلب این سرویسها برای کاربران آشنا بوده و در کاربردهای روزمره خود در اینترنت از آنها استفاده می‌کنند. به موارد زیر توجه کنید:

۱-۴-۵- FTP¹ = File Transfer Protocol

¹ - در درس بسته‌های نرم‌افزاری ۳ با FTP به طور مشروح‌تر آشنا می‌شوید

یکی از ضروری‌ترین کارهایی که اغلب کاربران در شبکه بدان نیاز دارند انتقال فایل است. TCP/IP مستقیماً دارای سرویسی است که انتقال فایل را برحی بین ماشینهای مختلف با سخت‌افزارهای متنوع و سیستم عاملهای گوناگون امکان‌پذیر می‌سازد و آن FTP است. از دو قسمت تشکیل شده :

الف) FTP Client

ب) FTP Server

کاربر با اجرای نرم‌افزار FTP Client به FTP Server متصل شده و با توجه به مجوزهای امنیتی مربوطه می‌تواند فایل‌های مورد نیاز را از سرور دریافت کرده (Download-Receive) یا آنها را روی سرور ذخیره کند. (Upload-Send)

در سیستم عاملهای Microsoft نرم‌افزارهای گوناگونی بعنوان FTP Client وجود دارند مثلاً می‌توانیم به IE (Internet Explorer) اشاره کنیم که از خود مایکروسافت است یا دستور [ftp.exe](#) که در حالت Text از Command Prompt اجرا می‌شود. نرم‌افزارهای دیگر مانند Cute FTP ، FTP Pro ، DAP و . . . نیز همگی نقش FTP Client را بازی می‌کنند. نرم‌افزارهایی که بعنوان FTP Server در مایکروسافت استفاده می‌شوند نیز موجود بوده و بعنوان مثال می‌توان به IIS اشاره کرد. بسته ایست شامل چندین سرویس که یکی از آنها FTP Server است.

فعالیت عملی، آشنایی با سرویس FTP : در این بخش هنر آموز درس FTP Server را از قبل روی یک کامپیوتر با سیستم عامل 2000 یا 2003 سرور پیکربندی کرده و هنجویان با اجرای FTP Client در کامپیوترهای خود (ترجیحاً IE) چند فایل را از سرور دریافت (Download) کنید. در این مرحله به هیچ عنوان نیازی به فراگیری پیکربندی FTP Server نبوده و هنجویان فقط از آن استفاده می‌کنند.

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

یک راه بسیار رایج برای دستیابی به اطلاعات که همگی با آن آشنا هستیم استفاده از سرویس HTTP است. همانند FTP، این سرویس نیز از دو بخش تشکیل شده :

الف) HTTP Client : که به Web Client ، Web Browser یا به اختصار Browser هم مشهور است.

ب) HTTP Server : که به Web Server نیز معروف است. کاربران نرم‌افزار HTTP Client را (مانند IE ، Netscape ، Fire Fox و . . .) اجرا کرده و درخواست دسترسی به اطلاعات یا حتی اجرای برنامه را به سرور ارسال می‌کنند (HTTP Request). سرور این درخواست را بررسی کرده و پس از آماده کردن پاسخ ، آنها را قالب خاصی معروف به Web Page به سمت Client ارسال می‌کند. سرویس‌گیرنده این صفحات را دریافت کرده و با فرمت مناسب به کاربر نشان می‌دهد. همانطور که می‌دانیم زبان مورد استفاده در صفحات وب اکثراً HTML یا XML است.

فعالیت عملی، آشنایی با سرویس HTTP : هرچند اغلب هنجویان و حتی کاربران عادی با این سرویس آشنا هستند اما برای حفظ انسجام مطالب بیان‌شده ، هنر آموز درس می‌تواند Web Server را به همراه یک Web Page بسیار ساده از قبل آماده کرده و کاربران با HTTP Client (ترجیحاً IE) به آن دسترسی پیدا کنند. شایان ذکر است که Web Server در مایکروسافت ، بخشی از بسته IIS است.

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

3)

هر دو سرویس فوق برای ارسال و دریافت EMail استفاده می‌شوند. به شکل زیر دقت کنید :

شکل ۱-۵

همانطور که از شکل پیداست کاربر برای تهیه ، ارسال ، دریافت و خواندن نامه از نرم افزار Mail Client استفاده می‌کند. دو مورد از نرم افزارهای معروف که بعنوان Mail Client در مایکروسافت استفاده می‌شوند عبارتند از Outlook_Express و Microsoft_Outlook (به اختصار OE و MO) . پس از اجرای Mail Client و پیکربندی آن ، کاربر می‌تواند متن نامه خود را تایپ کرده ، در صورت نیاز عکس یا فایل‌های دیگری را به آن پیوست کرده (Attachment) و پس از تعیین گیرنده و موضوع نامه (Subject) آنرا ارسال کند. به محض فشردن کلید Send تمامی محتوای نامه به همراه ضمايم پیوست ، با پروتکل SMTP به سمت Mail Server ارسال می‌شود. Mail Server پس از دریافت نامه از سوی کاربر به بررسی آدرس گیرنده می‌پردازد و چنانچه گیرنده شخصی خارج از حوزه پستی خودش باشد آنرا با SMTP به Mail Server حوزه گیرنده تحویل می‌دهد. Mail Server پس از دریافت نامه از Mail Server فرستنده آنرا در پوشه مناسب که در واقع صندوق پستی شخص گیرنده است ذخیره می‌کند و فرایند ارسال نامه به اتمام می‌رسد. حال از اینجا به بعد شخص گیرنده خودش وظیفه دارد که در صورت تمایل به Mail Server حوزه خود متصل شده و با پروتکل POP3 نامه‌هایش را از سرور دریافت کرده و در صندوق پستی محلی واقع در کامپیوتر خودش منتقل کند. همانطور که می‌بینیم فرایند فوق تا حدی با روش عمومی اداره پست در ارسال نامه متفاوت است چرا که پستی نامه را تا دم در منزل می‌آورد اما در Email ما باید خودمان به اداره پست (Mail Server) مراجعه و پس از نشان دادن مجوز ، نامه را از صندوق پستی برداریم.

پروتکل HTTP از آن دسته پروتکل‌هایی است که برای انتقال Email نیز از آن بهره می‌برند. بعنوان مثال می‌توان انتقال نامه از طریق yahoo یا Gmail را نام برد. برای تبادل نامه از طریق yahoo چگونه عمل می‌کنیم؟

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

سرویس دسترسی به گروه‌های خبری (News Groups) ، به زبان ساده NNTP سرویسی است برای دسترسی به اطلاعاتی که به وسیله ی افراد مختلف ارسال شده و مشترکاً مورد استفاده قرار می‌گیرد. این سرویس نیز از دو قسمت تشکیل شده :

الف) NNTP Client : که به News Client نیز معروف است.

ب) NNTP Server : که به News Server نیز مشهور است.

روال کار بدین صورت است که ابتدا به وسیله ی News Client به يك News Server متصل شده سپس گروه خبری را انتخاب و در آن عضو می‌شویم (Subscribe) پس از عضویت در گروه خبری ، اطلاعات و اخبار متنوع در زمینه مورد نظر از Server به سرویس گیرنده انتقال پیدا کرده و

اعضا در صورت تمایل می‌توانند نظرات یا پرسش‌های خود را درمورد خبرها ارسال کنند یا خبر و سوال جدیدی را به سرور ارسال کنند. شکل و شمایل کار بسیار شبیه به EMail است یعنی اخباری که در یک News Server ارائه می‌شود همچون EMail شامل موضوع خبر (Subject)، فرستنده خبر و تاریخ ارسال است و بدین سبب می‌توان گفت که NNTP بسیار شبیه به یک Mail Box است با این تفاوت که شخصی نبوده و بطور مشترک مورد استفاده همه اعضا قرار می‌گیرد. در مایکروسافت، نرم‌افزاری که بعنوان News Client مورد استفاده قرار می‌گیرد همان Mail Client است یعنی Outlook Express منتهی بجای پیکربندی برای Mail Account باید آنرا برای News Account تنظیم کنیم.

Telnet = Tele Network-۵-۶-۵

ترمینال عبارت است از وسیله‌ای که برای ارسال و دریافت اطلاعات استفاده می‌شود (مثلاً یک Keyboard و یک Monitor) اما هیچگونه پردازشی روی اطلاعات در آن صورت نمی‌گیرد و اصولاً پردازش اطلاعات در سیستم مرکزی (Central System) انجام می‌شود. منظور از سیستم مرکزی، مجموعه‌ایست دارای توانایی برای پردازش اطلاعات و اجرای دستورالعملها یعنی مجموعه‌ای که شامل CPU، RAM، HDD و . . . است. سیستم مرکزی می‌تواند یک کامپیوتر شخصی باشد، می‌تواند یک Mini Computer، Main Frame یا یک Super Computer باشد. سیستم مرکزی حتی می‌تواند یکی از تجهیزات فعال مورد استفاده در شبکه باشد مثلاً یک Router، Switch یا Hub. البته بدیهی است که در مورد اخیر (تجهیزات شبکه) هدف ما از اتصال ترمینال به مثلاً یک روتر، پردازش اطلاعات و اجرای Application برای کاربر نیست بلکه هدف پیکربندی یا کنترل آنست.

مثال ۱: تا چند سال پیش که کامپیوترهای شخصی رواج پیدا نکرده بودند، کامپیوترهای Main frame بعنوان سیستم مرکزی برای پردازش اطلاعات استفاده می‌شدند و کاربران به وسیله یکی از روشهای رایج در آن زمان (مثلاً Keyboard و Monitor) که در مجموع به آن ترمینال می‌گوییم) با Main frame ارتباط برقرار می‌کردند. بدیهی است هیچگونه پردازشی در ترمینال روی اطلاعات انجام نمی‌شد و فقط بعنوان ورودی و خروجی استفاده می‌شد.

مثال ۲: در برخی از بانکها، جلوی هر کارمند باجه، فقط یک مونیتور، کی‌برد و یک چاپگر کوچک قرار دارد اما خبری از Case و ملحقات داخلی آن نیست! چرا؟ پردازش کجا انجام می‌شود؟ تجهیزات جلوی کارمند فقط بعنوان ترمینال استفاده می‌شوند. پس سیستم مرکزی کجاست؟ اگر دقت کنیم در گوشه‌ای از بانک یک کامپیوتر شخصی قرار دارد که بعنوان سرور عمل کرده و نقش سیستم مرکزی را بازی می‌کند و درواقع محل اجرای نرم‌افزارهای بانکی و پردازش اطلاعات است. ترمینالها از طریق سخت‌افزار و کنترلر مناسب به آن متصل می‌شوند.

مثال ۳: مدیر شبکه (Network Administrator) می‌تواند ترمینال را به Router متصل کرده، آنرا پیکربندی کند و از مسیره‌های مختلفی که روتر با آنها ارتباط دارد آگاهی پیدا کند. می‌تواند مسیری را ببندد یا باز کند و . . .

روش اتصال ترمینالها به سیستم مرکزی

راههای متنوعی برای اتصال ترمینالها به سیستم مرکزی وجود دارد، که به ۳ مورد آن اشاره می‌کنیم:

۱- Serial Port

۲- USB

Network - 3

اکثر ترمینالها دارای یک Serial Port از نوع RS232 هستند که با کابل مناسب به سیستم مرکزی متصل می‌شوند. برای درک بهتر همان مثال بانکی (مثال ۳) را در نظر بگیرید. فرض کنید بانک دارای ۵ دستگاه ترمینال است و سیستم مرکزی نیز یک کامپیوتر شخصی معمولی با سخت‌افزار مناسب است. چگونه می‌توان ۵ ترمینال را از طریق RS232 به کامپیوتر شخصی متصل کرد؟ می‌دانیم هر کامپیوتر شخصی در حالت عادی حداکثر دارای ۲ عدد Serial Port است: Com1 & Com2 که آنهم ممکن است به وسیله ی Mouse و Modem اشغال باشد! راه حل آنست که از یک سخت‌افزار ویژه برای توسعه Serial Port استفاده کنیم. این کارتها معمولاً به Multi Port معروفند. پس از نصب کارت مذکور در کامپیوتر شخصی، پورتهای سریال افزایش یافته و می‌توان ترمینالها را متصل کرد: Com3، Com4، Com5 و الی آخر. برخی از ترمینالها برای اتصال خود با سیستم مرکزی مجهز به USB Port هستند و بالاخره برخی دیگر از آنها دارای یک کارت شبکه مثلاً با استاندارد 10BaseT یا 100BaseTX بوده که ترمینال را به شبکه وصل می‌کند، از طرفی چون سیستم مرکزی نیز خودش به شبکه متصل می‌شود بنابراین ارتباط مابین Terminal و Central System برقرار می‌شود. البته ترمینالهایی که دارای Network Interface هستند بنوعی در حد یک کامپیوتر شخصی محسوب می‌شوند با این تفاوت که از آنها فقط به قصد یک ترمینال استفاده می‌شود.

از نظر نحوه نمایش اطلاعات، ترمینالها به ۲ دسته کلی تقسیم می‌شوند:

الف) ترمینالهای Text: فقط بصورت "متنی" اطلاعات را نمایش می‌دهند.
ب) ترمینالهای Graphic: علاوه بر "متن"، دارای توانایی ترسیم اشکال گرافیکی با رنگهای متنوع نیز هستند.

تعریف Terminal Emulator: ممکن است در شبکه‌ای بجای ترمینال از یک کامپیوتر شخصی استفاده کنند. مزیت استفاده از کامپیوتر شخصی بجای ترمینال آنست که این کامپیوتر خود دارای توانایی پردازش اطلاعات است بنابراین می‌توان علاوه بر کاربرد آن بعنوان یک ترمینال، نرم‌افزارهای متنوع دیگری را نیز مستقیماً روی آن اجرا کرد. اما در صورت نیاز چگونه می‌توان کامپیوتر شخصی را تبدیل به یک ترمینال برای اتصال به سیستم مرکزی کرد؟ پاسخ بسیار ساده است: کفایت نرم‌افزار مناسب را روی آن اجرا کرد. این نرم‌افزارهای در حالت کلی به "شبیه‌ساز ترمینال" یا "مقلد ترمینال" یا به زبان انگلیسی Terminal Emulator مشهورند و همچون ترمینالها دارای ۲ دسته کلی Text و Graphic در زمینه نحوه نمایش اطلاعاتند. طریقه اتصال سخت‌افزاری یک کامپیوتر شخصی که بعنوان ترمینال استفاده می‌شود با Central System همچون نحوه ارتباط ترمینالهاست یعنی:

الف) RS232 Serial Port

ب) USB

ج) Network

نرم‌افزارهای Terminal Emulator که اطلاعات را بصورت Text نشان می‌دهند بسیار متنوعند، از آن جمله می‌توان به Term95، PC Anywhere، Kermit، Closeup و Hyper Terminal اشاره کرد. می‌دانیم که Hyper Terminal تحت Windows اجرا می‌شود اما در واقع فقط بصورت Text می‌تواند اطلاعات را نمایش دهد.

با توجه به مقدمه فوق می‌توانیم Telnet را که از سرویسهای TCP/IP است تعریف کنیم

اگر راه ارتباطی یک کامپیوتر شخصی با Central System از طریق شبکه باشد و پروتکل مورد استفاده نیز TCP/IP باشد در آن صورت Telnet عبارت است از یک سرویس Terminal Emulator که اطلاعات را بصورت Text نشان می‌دهد.

همچون دیگر سرویسها ، Telnet نیز از ۲ بخش تشکیل شده :
 الف) Telnet Client : که روی کامپیوتر شخصی اجرا می‌شود و آنرا تبدیل به ترمینال می‌کند (در مایکروسافت : Telnet.exe)
 ب) Telnet Server : یا Telnet Daemon یا به اختصار telnetd که روی Central System اجرا شده و اطلاعات را از ترمینال (سرویس گیرنده) دریافت و پس از پردازش به وسیله سیستم مرکزی ، برای ترمینال ارسال می‌کند.

فعالیت عملی، آشنایی با سرویس Telnet : ابتدا باید سیستم مرکزی را انتخاب کرد. (مثلاً یک کامپیوتر با سیستم عامل UNIX ، یک کامپیوتر با سیستم عامل NT ، یک Router ، یک Wireless Access Point ، . . .) سپس باید مطمئن شد که سرویس Telnet Server روی آن نصب و فعال است. (تا اینجا کار باید به وسیله هنر آموز درس انجام شود.) سپس هنجویان نرم افزار Telnet Client را روی کامپیوترهای خود اجرا کرده (Telnet.exe) و بدین ترتیب کامپیوتر آنها تبدیل به یک ترمینال می‌شود. قدم بعدی آنست که به سیستم مرکزی متصل شده و با آن به تبادل اطلاعات پرداخت. (اگر به اینترنت متصل هستید ، می‌توانید سایتهای بسیاری را پیدا کنید که با telnet می‌توان با آنها ارتباط گرفت منتهی باید مجوز ورود را هم در صورت درخواست وارد کنید. برخی از سایتهای اجازه می‌دهند با کاربر guest به سیستم Login کنیم. بعنوان مثال می‌توانید به از طریق Run فرمان زیر را تایپ کرده و نتیجه را ببینید، (کاربر را guest وارد کنید) :

telnet victoria.tc.ca

RDP = Remote Desktop Protocol - ۵-۶-۶

همانند Telnet است با این تفاوت که گرافیکی است. در مایکروسافت ، برنامه Remote Desktop از سرویس RDP استفاده کرده و کامپیوتر شخصی را تبدیل به یک ترمینال گرافیکی می‌کند.
 همچون دیگر سرویسهای TCP/IP ، RDP نیز از ۲ بخش تشکیل شده :
 الف) RDP Client : که به Terminal Client نیز معروف بوده و در مایکروسافت ، همان برنامه Remote_Desktop است (mstsc.exe)
 ب) RDP Server : که به Terminal Server نیز مشهور بوده و در مایکروسافت ، همان سرویس Remote_Desktop است که از طریق System Properties فعال می‌شود. البته در ویندوزهای 2000 Server یا 2003 Server یک نسخه کاملتر از این سرویس بنام Terminal Service از طریق زیر نصب و فعال می‌شود:
 Add/Remove Programs -> Windows Components -> Terminal Service

فعالیت عملی، آشنایی با سرویس RDP : قبلاً در فصل ۱ دستورالعملهای لازم برای فعالسازی RDP بکمک هنر آموز درس گفته شد لذا در صورت حضور ذهن هنجو ، نیازی به تکرار تمرین نیست.

SNMP = Simple Network Management Protocol - ۵-۶-۷

یکی از مسایل مهمی که هر Administrator در شبکه‌های متوسط و بزرگ با آن مواجه است ، مدیریت شبکه بشکل جامع و حتی المقدور یکپارچه است.

مثال ۱: می‌خواهیم یک سویچ حرفه‌ای از شرکت 3Com را مدیریت کنیم بدین‌معنی که سویچ را پیکربندی کرده، وضعیت آنرا از نظر میزان ترافیک تبادل در پورتهای مختلف و خطاهای بوجود آمده بررسی کنیم. پورتهای آنرا ببندیم، بازکنیم و . . . یکی از راههای جالب برای مدیریت سویچ که در داخل آن تعبیه شده استفاده از HTTP است، منظور آنست که سویچ خودش بطور داخلی (built-in) مجهز به یک Web Server است. مدیر شبکه می‌تواند Web Client خود را اجرا کرده (مثلاً IE) و فرمان ارتباط با سویچ را تایپ کند: `http://<Switch_IP_Address>`. بدین‌وسیله ارتباط با وب-سرور داخلی در سویچ برقرار شده و می‌توانیم آنرا مدیریت کنیم.

مثال ۲: می‌خواهیم یک روتر از شرکت Cisco را مدیریت کنیم. از طریق Command Prompt فرمان زیر را اجرا کرده و با آن ارتباط برقرار می‌کنیم و . . .

`<Router_IP_Address>`

در مثال فوق ارتباط ما با روتر از طریق سرویس Telnet برقرار شده.

مثال ۳: می‌خواهیم یک سرور 2000 را از طریق کامپیوتر خودمان مدیریت کنیم. ابتدا نرم‌افزار Terminal Server را (که در XP و 2003 بنامهای Remote Desktop Service نیز معروف است) نصب و فعال کرده، سپس به وسیله برنامه Remote_Desktop_Client با آن ارتباط برقرار کرده و Desktop مربوط به سرور را در اختیار می‌گیریم. حال براحتمی‌توانیم سرور را در اختیار داشته باشیم

در مثال فوق ارتباط ما با سرور از طریق سرویس RDP برقرار شده. مثال ۴: برای مدیریت از راه دور یک کامپیوتر با سیستم عامل XP، علاوه بر بهره‌گیری از Remote Desktop، می‌توان از برنامه Computer Management نیز استفاده کرد. برای این کار با Administrator وارد سیستم شده، برنامه مذکور را اجرا کنید (-> My Computer) کلیک راست (-> Manage) پس از اجرای برنامه روی اولین آیکن یعنی Computer Management (Local) راست کلیک کرده و Connect to another computer را انتخاب کنید. سپس با تایپ کردن نام یا آدرس کامپیوتر مقصد به آن متصل شده و از این به بعد می‌توانیم آنرا مدیریت کنیم. برای عملکرد صحیح لازم است تا password مربوط به Administrator روی هردو کامپیوتر مبدأ و مقصد دقیقاً یکسان باشد.

در مثال فوق ارتباط ما از طریق سرویسهای خاصی که میکروسافت تعبیه کرده برقرار شده. (RPC & Pipe)

نتیجه‌گیری: برای مدیریت راههای گوناگونی وجود دارد که بستگی به تجهیزات، سیستم عامل، پروتکل مورد استفاده و پارامترهای دیگر دارد اما آیا راه یکپارچه‌ای نیز هست؟ پاسخ مثبت بوده و راه حل، استفاده از SNMP است.

SNMP از دو بخش تشکیل شده:

الف) SNMP Agent: که مسئول جمع‌آوری اطلاعات بوده و باید روی هر سیستم، تک به تک فعال شود.

ب) SNMP Viewer: که به SNMP Manager نیز مشهور بوده و مسئول گردآوری و تجزیه و تحلیل اطلاعات جمع‌آوری شده به وسیله کلیه Agent ها در تمامی شبکه است.

شکل ۲-۵

به شکل دقت کنید. هر سیستمی که بخواهد با SNMP مدیریت شود باید Agent را روی آن نصب و فعال کرد. کار Agent آنست که اطلاعات مدیریتی را جمع‌آوری کرده و آنها را در یک بانک اطلاعاتی محلی (Local)

Database) معروف به MIB = Management Information Base ذخیره می‌کند. بعنوان مثال اگر در یک شبکه ۱۰۰۰ سیستم داریم که می‌خواهیم آنها را با SNMP مدیریت کنیم باید روی همگی 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)

برای پیکربندی آن نیز باید از طریق سرویس‌های ویندوز وارد عمل شد. (در صورت نیاز بکمک هنر آموز درس انجام شود) و اما اطلاعات جمع‌آوری شده به وسیله ی Agent را چگونه گردآوری و تجزیه تحلیل کنیم؟ کافیست روی یک کامپیوتر مثلاً متعلق به مدیر شبکه، نرم افزار Solarwinds را نصب کنیم. یکی از بهترین نرم افزارهای در این زمینه Solarwinds است (www.solarwinds.net). پس از پیکربندی نرم افزار می‌توان به سایر سیستم‌های مجهز به Agent در شبکه متصل شده و اطلاعات جمع‌آوری شده در MIB را گردآوری و تجزیه تحلیل کرد.

فعالیت عملی، آشنایی با سرویس SNMP : با توجه به اینکه مدیریت شبکه نیاز به تجربه و دانستن مقدمات پیشرفته‌تری دارد لذا در این مرحله نیازی به آشنایی عملی با SNMP نیست، با این حال در صورت تمایل و داشتن فرصت کافی، هنر آموز محترم می‌تواند، خود Agent و Viewer را نصب و پیکربندی کرده و نحوه مدیریت شبکه را در حالات بسیار ساده به هنرجویان نشان دهد.

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

ساعت دقیق در شبکه‌هایی که اطلاعات مالی، پرسنلی، مدیریت پروژه و . . . در آنها نگهداری می‌شود بسیار مهم است. در یک شبکه چگونه می‌توان مطمئن شد که ساعت در کلیه سیستمها بطور صحیح تنظیم شده؟

در اینجا NTP به‌کمک 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 پیکربندی، NTP Client در زمانهای مشخص با NTP Server ارتباط برقرار کرده و ساعت خود را با ساعت سرور تنظیم می‌کند و بدین ترتیب ساعت تمام کامپیوترهای شبکه دقیقاً یکسان شده و نیازی به تنظیم دستی نیست.

بد نیست بدانیم که Time Server خود می‌تواند یک Time Client باشد برای یک سرور دیگر. خوشبختانه در اینترنت، مراجع دقیقی بعنوان NTP Server وجود دارند (معروف به ساعت اتمی) که سرورهای محلی می‌توانند زمان دقیق را از آنها دریافت کنند بعنوان مثال می‌توان به time.nist.gov اشاره کرد.

فعالیت عملی، آشنایی با سرویس NTP :

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

سومین قسمت از صفحه Time با نام Internet Time را باز کنید. لیستی از سرورهای مرجع را می‌بینید که می‌توانید یکی از آنها را انتخاب و ساعت خود را با آن Update کنید. در شبکه‌های متوسط و بزرگ نیز می‌توان یک سرور 2000 یا 2003 را بعنوان Time Server در نظر گرفته و سپس کلیه سیستم‌های 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 کرده باشیم، 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: کلیه 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 دیگری است 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 مشخصه اصلی و بارز است. بعبارت دیگر هر Host را می‌توان با ۲ خصوصیت از بقیه 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 در نظر بگیریم، آدرس در اولویت اول قرار داشته و هر Host باید حداقل یک آدرس منحصر بفرد داشته باشد. مشخصه "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. به عبارت دیگر پروتکل با مکانیزمهایی که بعداً 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 دهید کمی بیشتر در مورد اسامی Host و قوانین مربوطه صحبت کنیم:

شرح بیشتر Host Name :

گفتیم که برای سهولت بیشتر کاربران، برای اکثر "میزبانه‌های مهم" (Host) یک یا چند نام انتخاب می‌شود. بدیهی است که این نامها باید از قوانینی تبعیت کرده و ضمناً مورد تأیید "مراکز ثبت اسامی" نیز قرار بگیرند، به زبان دیگر باید اسم را ثبت (Register) کرد. چنانچه اسم یک Host ثبت نشود در آن صورت استفاده از نام معمولاً محدود به کاربردهای داخلی شده و اغلب کاربران "خارج از شبکه داخلی" نام را نمی‌شناسند چرا که رسماً ثبت نشده. مثال: هرکدام از ما انسانها مجازیم در محدوده خانوادگی خودمان یا میان دوستان و آشنایان هر اسمی را به خودمان بدهیم اما هنگامی که می‌خواهیم خود را رسماً به همه معرفی کنیم یا دیگران ما را رسماً صدا بزنند بدیهی است که از این اسامی کذایی و متنوعی که روی خودمان گذاشته‌ایم استفاده نخواهند کرد بلکه "اسم شناسنامه‌ای" ما را که در اداره ثبت احوال درج شده بکار می‌برند چرا که همگان "اداره ثبت احوال" را بعنوان "مرکز معتبر ثبت اسامی" قبول دارند.

اکنون نگاهی دقیقتر به قالب اسامی داشته باشیم، بطور کلی می‌توانیم دو قالب را برای نامگذاری تصور کنیم. با دقت به مثالهای زیر موضوع روشن می‌شود:

قالب اول: هر یک از اسامی زیر بعنوان یک Host Name می‌تواند در پروتکل TCP/IP استفاده شود:

PC1 Star	Client80 Moon	Server22 Palang	Reza C1	Shiva C2
1) www.yahoo.com	2) mail.yahoo.com	3) www.neda.net.ir	4) ftp.dlink.com	5) ftp.microsoft.com
6) www.sanjesh.org	7) www.tamin.org	8) www.sharif.edu	9) sina.sharif.ac.ir	10) www.itrc.ac.ir
			11) time.nist.gov	12) www.dci.ir

قالب دوم:

پرسش: تفاوت بین قالب اول و دوم در چیست؟ بروشني پيدا است كه قالب دوم كامل تر است، اصطلاحاً اگر اسمی در قالب اول باشد به آن اسم مستعار Alias یا Unqualified و اگر در قالب دوم باشد به آن FQDN = Fully Qualified Domain Name می‌گویند.

معمولاً اسامی قالب اول در محدوده داخلی شبکه‌ها استفاده شده، نیازی به ثبت ندارند اما اسامی قالب دوم عمدتاً ثبت شده و در این صورت چه در محدوده داخلی و چه افراد خارج از شبکه داخلی می‌توانند از آنها برای مراجعه به Host استفاده کنند. (همانطور که تأکید شد، اسامی اعم از قالب اول یا دوم در ابتدای کار به وسیله ی TCP/IP به آدرس تبدیل می‌شوند)

پرسش: یک اسم در قالب دوم (FQDN) معمولاً از چه قسمتهایی تشکیل می‌شود؟

در جواب می‌توان گفت به ترتیب از سمت چپ:

الف) نام یا سرویسی که Host ارائه می‌دهد یا نقشی که Host بازی می‌کند. (Host Role or Host Service)

مثال:

www = Web Server mail = Mail server

ftp = FTP Server
news = News (NNTP) Server

time = Time Server

(ب) نام شرکت، سازمان، مجموعه یا شخصی که Host بدان تعلق دارد.
(Company Name)

مثال:

yahoo, google, sun, microsoft, IRIB, Bank-Keshavarzi, ...

(ج) حوزه فعالیت میزبان. (Activities)

مثال:

com, net, org, gov, mil, edu, ac, info, int, biz, tv, ws, ...

(د) وابستگی منطقه ای و محلی اعم از فرهنگی، اجتماعی، ... یا زبان استفاده شده در سایت. (Locality)

مثال:

ir = Iran
iq = Iraq

tr = Turkey
tw = Taiwan

uk = United Kingdom
us = United States

ca = Canada

fr = France

نکته ۱: برای دیدن لیست کاملی از کدهای دو حرفی مربوط به کشورهای مختلف کافی است در google عبارت زیر را جستجو کنید: "Country codes" یا مستقیماً به سایت www.iana.org مراجعه کنید.

نکته ۲: با توجه به مثالهای قالب دوم ممکن است برخی از اجزای یاد شده در FQDN موجود نباشد مثلاً در اکثر آنها "بندت" (Locality) دیده نمی‌شود یا یک از اسامی دانشگاه شریف با sina شروع می‌شود و "سینا" بیانگر سرویس نیست بلکه فقط یک اسم است. در مثال دیگری مربوط به سایت شرکت دیتا www.dci.ir می‌بینیم که حوزه فعالیت در آن دیده نمی‌شود اما به هر حال FQDN هرچه قدر هم که ناقص باشد، اجزای آن باید از چپ به راست ترتیب یاد شده را رعایت کنند و نباید آنها را جابجا کرد مثلاً www.com.yahoo صحیح نیست.
Domain یعنی چه؟

به این مثالها توجه کنید:

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

به عبارت دیگر می‌توان گفت که در یک FQDN چنانچه بخش ابتدایی سمت چپ را که (بیانگر نام سرویس است) کنار بگذاریم، به مجموع بقیه قسمتها Domain گفته می‌شود که شامل نام شرکت، حوزه فعالیت و کشور می‌شود.

بنابراین FQDN بطور کلی از دو بخش تشکیل شده:

جدول

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

Sub Domain به زیر مجموعه‌های یک Domain اصطلاحاً "SubDomain" می‌گویند. در عمل معمولاً از SubDomain برای نشان دادن شرکتها، زیرگروهها یا ساختارهای فرعی در یک مجموعه بزرگ استفاده می‌شود.

مثال: یک شرکت بزرگ کامپیوتری را در نظر بگیرید که علاوه بر شرکت اصلی، از ۳ شرکت زیرمجموعه برای فعالیتهای سخت‌افزار، نرم‌افزار و شبکه استفاده می‌کند. برای شرکت اصلی، یک Domain بنام a.net را در نظر گرفته آنرا ثبت می‌کنیم. حال با توجه به

گسترده‌گی فعالیت‌های بزرگ‌رایان و طبیعتاً شرکت‌های زیرمجموعه، بد نیست که برای هر کدام از زیرمجموعه‌ها نیز يك domain در نظر بگیریم:

برای شرکت سخت‌افزار : hardware.a.net
 برای شرکت نرم‌افزار : software.a.net
 برای شرکت شبکه : network.a.net

هریک از domain های فوق را اصطلاحاً يك SubDomain از a.net می‌نامیم. چنانچه شرکت اصلی و بخش‌های تابعه، هر یک برای خود Web-Server داشته باشند در آن صورت دارای اسامی زیر خواهند بود:

وب سرور شرکت اصلی
 www.a.net
 وب سرور شرکت سخت‌افزار
 www.hardware.a.net
 وب سرور شرکت نرم‌افزار
 www.software.a.net
 وب سرور شرکت شبکه
 www.network.a.net

در کامپیوترهایی که از سیستم عامل‌های خانواده Microsoft بهره برده و در ضمن پروتکل TCP/IP روی آنها فعال می‌شود، ۲ اسم مد نظر قرار می‌گیرد:

الف) هنگام نصب OS يك اسم حداکثر ۱۵ کاراکتری به کامپیوتر داده می‌شود که باید در محدوده شبکه داخلی منحصر بفرد بوده تکراری نباشد. این اسم به Computer Name یا NetBIOS Name معروف است. (لزومی ندارد که حتماً پروتکل NetBIOS روی کامپیوتر نصب باشد، در هر صورت به آن NetBIOS Name می‌گویند). می‌دانیم که در سیستم عامل XP یا 2003 برای تغییر NetBIOS Name از System Properties وارد عمل شده، قسمت Computer Name را انتخاب و پس از فشردن کلید Change، نام کامپیوتر را تغییر داده و تأیید OK می‌زنیم.

ب) TCP/IP Name که همان Host Name در پروتکل TCP/IP بوده و به Full Computer Name نیز معروف است و ممکن است در قالب اول یا دوم باشد. بصورت پیش فرض در کامپیوترهایی که عضو Work Group باشند TCP/IP Name دقیقاً برابر با NetBIOS Name است از طرفی چون NetBIOS Name عمدتاً ساده و تک قسمتی بوده لذا TCP/IP Name هم بصورت تک قسمتی برابر با آن می‌شود یعنی در قالب اول است.

اگر کامپیوتر به عضویت Domain در Active Directory درآید آنگاه TCP/IP Name بصورت زیر در می‌آید:

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

یعنی TCP/IP Name در قالب دوم می‌شود.

به هر حال برای تغییر Domain در TCP/IP Name از طریق System Properties وارد عمل شده و قسمت Computer Name را انتخاب و پس از فشردن کلید Change و متعاقب آن کلید More، نام Domain را در قسمت Primary DNS Suffix for this computer وارد کرده و تأیید OK کنید. با تأیید مجدد (OK)، سیستم عامل از شما می‌خواهد تا کامپیوتر را Restart کنید. پس از Restart، وارد Command Prompt شده و با اجرای دستور ipconfig /all و بررسی خطوط اولیه، نتیجه کار خود را بررسی کنید.

فعالیت عملی: هر گروه از هنجریان که یک‌دستگاه کامپیوتر مستقل در اختیار دارند بدخواه يك Domain Name انتخاب کرده سپس Full Computer Name را در سیستم خود تغییر دهند.

البته همانطور که گفته شده اسامی TCP/IP در قالب دوم تا هنگامی که رسماً در "مراکز شناخته‌شده ثبت اسامی" یا به زبان فنی (DNS Server) ثبت نشوند نمی‌توانند مورد استفاده بقیه قرار گیرند لذا فعالیت عملی فوق صرفاً برای آشنایی بیشتر هنجری با Full Computer Name و مفهوم FQDN بوده، توصیه می‌شود که 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" یک آدرس منحصر بفرد داشته باشد که به آن IP Address می‌گویند.

نکته ۱: فعلاً راجع به اینکه چرا می‌گوییم "حداقل"، حرفی نمی‌زنیم.

نکته ۲: "منحصر بفرد بودن" زمانی مهم است که شبکه‌ها با یکدیگر در ارتباط باشند و گرنه هنگامی که هیچگونه ارتباطی (با روتر) بین شبکه‌ها برقرار نیست چه اهمیتی دارد که آدرسهای مورد استفاده در یک شبکه با دیگر شبکه‌ها تکراری باشد.

نکته ۳: ممکن است شبکه‌ها به یکدیگر متصل باشند و آدرسهای تکراری در آنها پیدا شود این امر در صورتی که اصطلاحاً "عمل ترجمه آدرس" یا Network Address Translation = NAT روی آنها صورت بگیرد اشکالی ندارد. بحث راجع به NAT را به دوره‌های پیشرفته‌تر موکول می‌کنیم. IP Address یک عدد ۴ بایتی (۲۳ بیتی) بوده که به فرم w.x.y.z تنظیم می‌شود. بدیهی است که $0 < w,x,y,z < 255$.

البته اعداد مرزی یعنی 0 و 255 را باید طبق قوانین خاصی استفاده کرد که به تفصیل مورد بحث قرار می‌گیرد. حال برای آنکه بتوانیم اجزای IP Address و چگونگی تنظیم آنرا درک کنیم بهتر است نگاهی سریع به شکلهای ۱ تا ۴ داشته باشیم.

در این شکلها مجموعاً ۴ شبکه متفاوت ترسیم شده که با دقت در آدرسهای بکاررفته می‌توانیم نکات زیر را کشف کنیم:

الف) هر آدرس از ۲ قسمت تشکیل شده: یک قسمت در سمت چپ که بین تمامی سیستمهای بکار رفته در هر شبکه مشترک است و یک قسمت در سمت راست که برای 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 شبکه‌های مختلف هرکدام NetID های مختلفی دارند و تکراری نیست.

ج) NetID ممکن است ۳ بایت (شکلهای ۱ و ۲) یا ۲ بایت (شکل ۳) یا ۱ بایت (شکل ۴) باشد. بدیهی است که هرچه تعداد بایتهای NetID بیشتر باشد شبکه‌های بیشتری را می‌توان شماره‌گذاری کرد اما از آن طرف تعداد Host های موجود در شبکه محدودتر می‌شود. بسته به اینکه تعداد بایتهای Net ID چند رقم باشد ۳ کلاس متفاوت از IP Address پدید می‌آید:

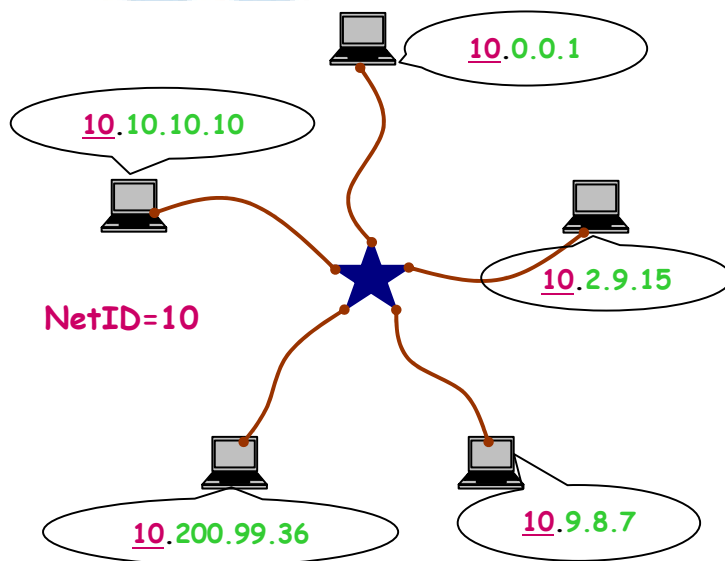
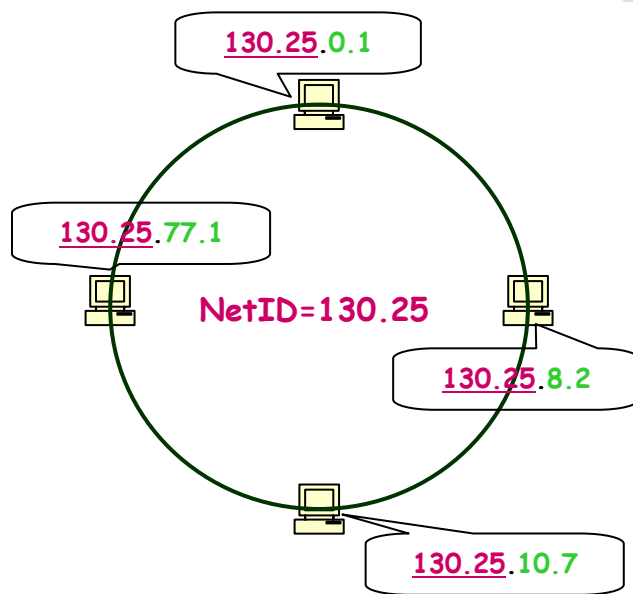
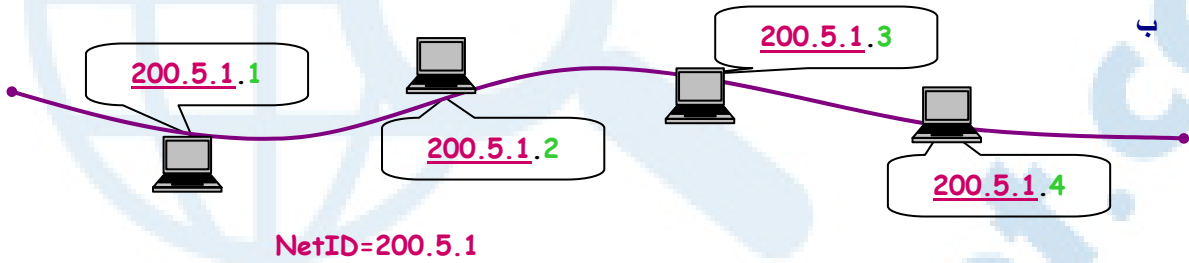
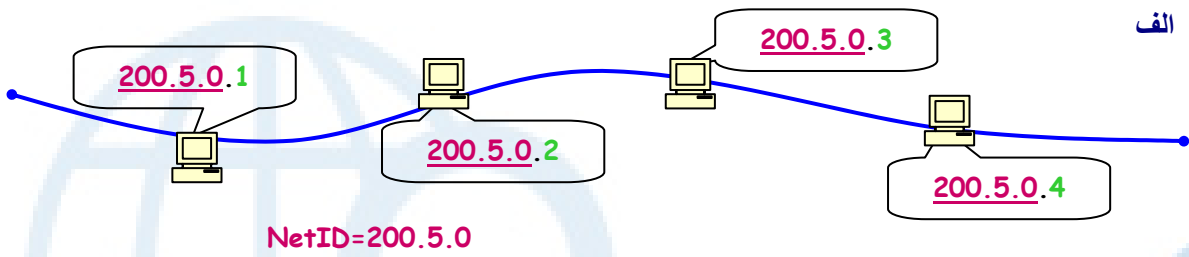
Net ID = 1 byte (8 bits) => Class A

Net ID = 2 bytes (16 bits) => Class B

Net ID = 3 bytes (24 bits) => Class C

به شکل‌های زیر توجه کنید هر یک از شکلهای ۱ تا ۴ به ترتیب از کلاسهای زیر استفاده می‌کنند؟

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



در هريك از شكلهاي فوق از مقايسه اعداد با يكديگر برآحي مي‌توانيم وجه مشترك آنها يعني NetID را تشخيص داده و بسرعت كلاس آنرا تعيين كنيم اما اگر يك IP Address را به تنهائي به ما نشان داده و بگويند در چه كلاسي است چه جوابي براي آن داريم؟ مثلاً " 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

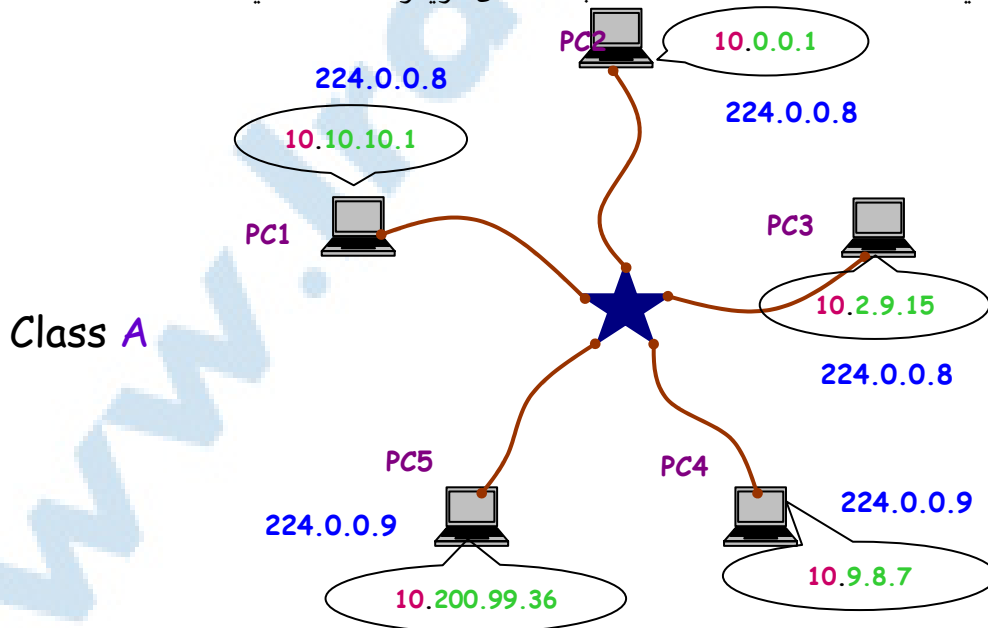
يعني از روي رقم اول سمت چپ (W) مي‌توانيم بفهميم كه يك آدرس در چه كلاسي است.

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 0 تا 255 تغيير مي‌كند ممكن است سؤالات زير را از خود بپرسند:
 (1) آيا W نمي‌تواند با صفر شروع شود؟ خير IP Address نمي‌تواند با عدد 0 آغاز گردد.

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

(3) : تكليف اعداد بين 224 تا 255 چه مي‌شود؟ ابتدا براي تعيين تكليف اعداد 224 تا 239 به شكل زير دقت كنيد:



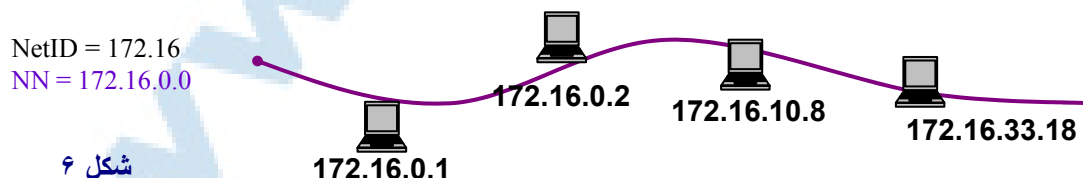
همانطور كه از شكل فوق پيدااست هر Host علاوه برآنكه يك آدرس منحصر بفرد در (مثلاً) كلاس C دارد يك آدرس ديگر را كه با عدد 224 شروع مي‌شود دارا بوده كه اولاً اجباري نبوده ثانياً دست بر قضا! با برخي از سيستمهاي مجاور تكراري است.

به نظر شما کاربرد چنین آدرسهای در چیست؟ اینگونه آدرسها که اصطلاحاً در کلاس D هستند برای Multicasting استفاده می‌شوند. بعنوان مثال اگر یک کاربر در سیستم متعلق به خود فرمان ارسال اطلاعات را به آدرس 224.0.0.8 دهد در آنصورت سیستمهای PC1, PC2, PC3 همگی 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 جنبه آزمایشی داشته است لذا برای آن کاربرد تعریف شده‌ای 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 اینجا کار از هنرجویان انتظار می‌رود که بتوانند کاربرد هر یک از کلاسهای A,B,C,D را به استثنای Loop back دقیقاً توضیح دهند. اکنون که با فرمت IP Adresses آشنایی مختصری پیدا کردیم می‌توانیم قوانین آدرس دهی را دقیق‌تر بررسی کنیم: قانون اول: در یک شبکه مشخص، هر Host باید حداقل یک 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 یک شبکه مشخص برای آنکه کلیه 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 برابر است با NetID بعلاوه HostID هنگامی که تمامی بیت‌های آن صفر است. شکل زیر را ببینید:



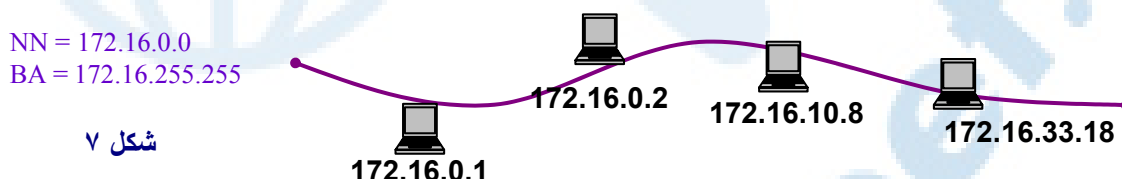
شکل ۶

شبکه فوق را اصطلاحاً می‌گویند: شبکه 172.16.0.0

برای درک بهتر به مثالهایی زیر نیز توجه کنید که همگی بیانگر آدرس شبکه 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 هیچکدام از اعداد فوق را نمی‌توان بعنوان آدرس یک Host استفاده کرد زیرا بیانگر شماره شبکه هستند. و اما چنانچه تمامی رقمهای مربوط به HostID، همگی با هم 255 باشند (از دیدگاه باینری، تمامی بیت‌های مربوطه، "1" باشد) آنگاه عدد حاصله برای Broadcast Address استفاده می‌شود یعنی برای ارسال اطلاعات به تمامی سیستم‌های موجود در همان شبکه. بنابراین Broadcast Address برای شبکه یادشده می‌شود: 172.16.255.255



مثال: اگر کاربری فرمان ارسال اطلاعات را برای 172.16.0.2 صادر کند، فقط یک Host که دقیقاً دارای آدرس مذکور است اطلاعات را پردازش خواهد کرد (Unicast)، اما اگر فرمان ارسال اطلاعات برای 172.16.255.255 صادر شود، در آن صورت کلیه سیستم‌های شکل ۷ اطلاعات را دریافت و پردازش خواهند کرد. (Broadcast)

برای درک بهتر به مثالهایی زیر نیز توجه کنید که همگی بیانگر آدرس شبکه 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 دهی برای شبکه خود از کدام کلاس استفاده می‌کنید؟ بستگی به تعداد Host های بکار رفته در شبکه دارد. به مثالهایی زیر دقت کنید:

مثال ۱: شبکه‌ای داریم متشکل از Host x 160 که با توجه به توسعه آن ممکن است به Host x 230 افزایش پیدا کند از کدام کلاس استفاده کنیم؟ هر یک از کلاس‌های A,B,C را می‌توان بکار برد اما نظر به اینکه تعداد Host از ۲۳۰ عدد بیشتر نمی‌شود بهتر است از کلاس C استفاده کنیم و بعبارت دیگر آدرسها را هدر ندهیم. بنابراین باید یک Net ID منحصر بفرد در کلاس C را که در شبکه‌های دیگر استفاده نشده باشد انتخاب کرده و آنرا به شبکه خود اختصاص دهیم اما از کجا بدانیم که NetID آزاد و استفاده نشده کدام است؟ برای اینکار خوشبختانه یک متولی وجود دارد که مسوولیت تخصیص فضای آدرسها را بعهده داشته و برای انتخاب NetID به آن مراجعه می‌کنند. این متولی همان IANA است (www.IANA.org) که البته برای منطقه اروپا کار را به www.ripe.net تفویض کرده است و چون در ایران معمولاً از آدرسهای اروپایی استفاده می‌شود لذا به ripe مراجعه کرده و فرم درخواست IP را تکمیل می‌کنیم و پس از طی تشریفات مربوطه یک NetID منحصر بفرد در اختیار ما قرار داده می‌شود. (در حال حاضر اینکار در ایران از طریق شرکت دیتا وابسته به مخابرات انجام می‌شود: www.dci.ir) فرض کنیم که در مثال یاد شده، NetID اختصاص یافته برای شرکت ما عدد 213.217.24 باشد. بهتر است بگوییم شماره شبکه ما (Network Number) برابر با 213.217.24.0 است. با در اختیار داشتن Network

Number مذکور برآحتي مي‌توانيم كلية Host ها را از ۱ تا حداکثر 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 Host x 230 داشتيم و بنا بر اين آدرس آخرين Host ميشود: 213.217.24.230 ، اما با توجه به توان بالقوة كلاس C ، براي هر NetID مي‌توانيم تا حداکثر Host x 254 را شماره‌گذاري كنيم و لذا آدرس آخرين Host را 213.217.24.254 نوشتيم و از اين پس در بقیة مثالها نیز چنين خواهيم كرد.

بدیهي است طبق قوانین گفته شده اعداد 0 و 255 کاربرد خاص خود را داشته و نمی‌توانند برای شماره‌گذاري Host استفاده شوند:

Network Number = 213.217.24.0
Broadcast Address = 213.217.24.255

بطور كلي در حل اینگونه مسائل باید ۴ مرحله را طی كنيم:

مرحله اول: تعیین کلاس با توجه به حداکثر تعداد Host .

مرحله دوم: اخذ شماره شبکه معتبر یا به زبان فني: (Valid Network Number) یا (Valid IP Address)

مرحله سوم: تعیین آدرس اولین Host الي آخرين Host .

مرحله چهارم: تعیین 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 عمده و اساسی ترمینال با یک کامپیوتر PC چیست؟
- ۵- کدام سرویس TCP/IP از ترمینال استفاده می کند؟ برای اتصال به سیستم مرکزی به چه چیزهایی نیاز دارد؟
- ۶- وظیفه Windows time چیست؟
- ۷- نام پروتکلی که ارسال ایمیل را انجام می دهد چیست؟
- ۸- وظیفه Terminal Service را شرح دهید.
- ۹- Host چیست؟ خصوصیت اصلی 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 تفاوتی با نسخه ۴ دارد؟
- ۱۴- تحقیق کنید که چند کاربر می توانند به طور هم زمان از RDP استفاده کنند.
- ۱۵- تحقیق کنید که چه دستوراتی در محیط FTP رایج است؟
- ۱۶- تحقیق کنید که Domain های .org ، .inf ، .prof ، .gov ، .ac ، .com ، .net ، .edu در چه حوزه هایی مورد استفاده قرار می 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 های دو مدل TCP/IP و OSI را بیان کند.
مکانیزم های به کار گرفته شده در تجهیزات امنیتی شبکه را شناسایی کند.

تبادل داده ها در یک محیط شبکه ای ، مبتنی بر استانداردهایی می باشد یکی از این استانداردها ، استاندارد به نام OSI است که از طریق سازمان ISO تدوین و معرفی شده است . پروتکل های شبکه نیز براساس این استاندارد تدوین و تولید شده اند .

در این استاندارد تمامی فعالیت هایی که سبب می شد اطلاعات از طریق شبکه و از کامپیوتری به کامپیوتر دیگر منتقل شود در یک ساختار ۷ لایه ای به نام Open System Interconnection (OSI) قرار گرفت .

این استاندارد تمامی فرایندهای تبدیل اطلاعات را از حالتی که در کامپیوتر قابل استفاده است تا حالتی که از طریق کابل شبکه قابل ارسال باشد ، در بر می گرفت .

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

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

OSI Reference Model

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

شکل ۱-۶

نکته : نکته ای که در مورد لایه ها می توان به آن اشاره کرد این است که هر لایه فقط با لایه های قبلی ، بعدی و لایه نظیر خود در کامپیوتر مقصد ارتباط دارد .

شکل ۲-۶

۱-۶ انواع لایه در مدل OSI

لایه اول یا لایه فیزیکی در پایین ترین سطح قرار دارد و به طور مستقیم با توپولوژی شبکه در ارتباط است . لایه هفتم یا همان لایه کاربردی با کاربر در ارتباط بوده و از کاربر داده ها را دریافت کرده و به شبکه انتقال می دهد و برعکس.

۱-۱-۶ لایه فیزیکی

لایه فیزیکی، اولین لایه مدل OSI بوده و در پایین ترین سطح این مدل قرار گرفته است . در این لایه نحوه اتصال دو کامپیوتر به یکدیگر از طریق کابل های شبکه ، نحوه اتصال کابل شبکه به کامپیوتر ، توپولوژی های شبکه و سرعت های آن ها توضیح داده شده است . این لایه مسئول تبدیل اطلاعات از بیت ها (صفر و یک دیجیتال) به سیگنال های الکتریکی است . به طور کلی می توان گفت این لایه فقط ولتاژ، اتصالات ، کارت شبکه و جریان الکتریکی را می شناسد .

۲-۱-۶ لایه پیوند داده ها

لایه پیوند داده ها دومین لایه مدل OSI است . وظیفه این لایه این است که اطلاعات را برای ارسال آماده کند و در واقع اطلاعاتی را که از لایه بالاتر یعنی لایه شبکه دریافت می کند به واحدهای کوچک تری به نام قاب تبدیل کرده و آن ها را ارسال کند . هم چنین این لایه وظیفه دارد که اطلاعات را برای ارسال صحیح و بدون خطا کنترل کرده و به کامپیوتر فرستنده صحت اطلاعات را اعلام کند . این لایه خود از دو زیر لایه به نام های LIC و MAC تشکیل شده است . هر کدام از این زیر لایه ها وظایفی را به عهده دارند که شرح آن ها به این قرار است :

زیر لایه LLC وظایفی برعهده دارد که عبارتند از: برقرار ارتباط نظیر به نظیر بین دو کامپیوتر فرستنده و گیرنده، ایجاد قاب ها و کنترل خطاهایی که در اثر عوامل محیطی بر رسانه به وجود می آید. این زیر لایه عمل کنترل خطا را به این صورت انجام می دهد که هر قاب را ساخته و مرزهای ابتدا و انتهای آن را مشخص می کند. سپس قاب ها را شماره گذاری و ارسال می کند. کامپیوتر مقصد قاب های ارسال شده را دریافت کرده و به ترتیب شماره، آن ها را پشت سرهم قار می دهد و اطلاعات را دوباره بازسازی می کند. زیر لایه LLC در کامپیوتر گیرنده پس از دریافت هر قاب یک پاسخ برای کامپیوتر فرستنده می فرستد. به این پاسخ Acknowledge گفته می شود. کامپیوتری که فرستنده اطلاعات است با دریافت این Acknowledge متوجه می شود که قاب مذکور به طور صحیح و بدون بروز مشکل به مقصد رسیده است. کامپیوتر فرستنده تا مدتی منتظر می ماند تا برای تمامی قاب های ارسال شده، Acknowledge دریافت نماید. در صورتی که LLC برای قابی Acknowledge دریافت نکند، متوجه می شود که قاب مذکور آسیب دیده یا به مقصد نرسیده است؛ در این حالت قاب مورد نظر را از روی شماره آن دوباره ساخته و برای کامپیوتر مقصد ارسال می کند. این زیر لایه با این روش سالم رسیدن اطلاعات به مقصد را تضمین می کند.

زیر لایه دیگری که در لایه پیوند داده ها قرار دارد، زیر لایه MAC است. این زیر لایه چند وظیفه برعهده دارد. یکی از وظایف آن کنترل نحوه دسترسی به خطوط انتقال است.

از وظایف دیگر این زیر لایه کنترل آدرس فیزیکی کارت های شبکه کامپیوتر فرستنده و گیرنده است. هرکارت شبکه برای خود یک آدرس فیزیکی منحصر به فرد دارد که غیر قابل تغییر است. این آدرس به وسیله ی کارخانه سازنده در کارت شبکه حک می شود.

Flag	Address	Control information	Data	Parity	Flag
------	---------	---------------------	------	--------	------

شکل ۳-۶ Data-Link

۳-۱-۶ لایه شبکه

لایه شبکه، سومین لایه استاندارد OSI است. یافتن آدرس کامپیوترهای مبدأ و مقصد و ایجاد یک مسیر ارتباطی بین مبدأ و مقصد و هم چنین مسیر یابی در شبکه های بزرگ مثل شبکه اینترنت یا امثال آن وظیفه اصلی این لایه است. این لایه پیچیده ترین لایه OSI است، زیرا عمل مسیر یابی که فرآیند بسیار پیچیده ای است در این لایه اتفاق می افتد. این لایه علاوه بر مسیر یابی می تواند اعمال دیگری از جمله کنترل ترافیک را نیز انجام دهد. بدین معنی که در صورتی که بار ترافیک در مسیر عبور بسته اطلاعاتی بالا رود، این لایه وجود ترافیک را تشخیص داده و مسیر جدیدی را که ترافیک کمتری دارد برای عبور بسته ها انتخاب می کند. یکی دیگر از اعمالی که این لایه انجام می دهد، زمانی است که یک بسته اطلاعاتی برای رسیدن به مقصد مجبور است از شبکه ای به شبکه دیگر برود. در این شرایط ممکن است مشکلات زیادی بروز نماید. یکی از این مشکلات این است که روش آدرس دهی کامپیوتر ها در شبکه مبدأ و مقصد متفاوت و نامتجانس است. رفع این مشکل و مرتبط کردن دوشبکه نامتجانس نیز از دیگر وظایف این لایه است.

شکل ۴-۶ Network layer

۴-۱-۶- لایه انتقال

وظیفه اصلی لایه انتقال، دریافت داده‌ها از لایه جلسه، در صورت نیاز شکستن داده‌ها به واحدهای کوچک‌تر، انتقال آن‌ها به لایه شبکه و حصول اطمینان از دریافت صحیح داده‌ها در انتهای دیگر (کامپیوتر مقصد) است.

از وظایف دیگر لایه انتقال این است که این لایه باید مراقب برقراری و قطع اتصال در شبکه باشد. هم‌چنین این لایه مکانیزمی برای کنترل جریان ارسال داده‌ها در اختیار دارد، به طوری که این مکانیزم سبب می‌شود کامپیوتر فرستنده، داده‌ها را با سرعتی ارسال کند که کامپیوتر گیرنده قادر به دریافت آن‌ها باشد. این مکانیزم زمانی کاربرد پیدا می‌کند که یک کامپیوتر سریع بخواهد اطلاعاتی را ارسال نماید و کامپیوتر گیرنده، قدرت و سرعتی کمتر از کامپیوتر فرستنده داشته باشد. در این شرایط لایه انتقال، سرعت ارسال کامپیوتر فرستنده را تا حد سرعت کامپیوتر گیرنده اطلاعات پایین می‌آورد.

۵-۱-۶- لایه جلسه

پنجمین لایه OSI، لایه جلسه است. این لایه هم‌چون لایه انتقال، ارسال معمولی داده‌ها را فراهم می‌کند اما خدمات پیشرفته‌ای را نیز ارائه می‌کند که کاربردهای مفیدی دارد. یکی از خدمات جلسه، مدیریت بر ارتباط بین کامپیوترهاست؛ بدین معنی که وقتی دو کامپیوتر باهم ارتباط برقرار می‌کنند، ترافیک می‌تواند در یک لحظه یک طرفه یا دو طرفه باشد. اگر این ترافیک یک طرفه باشد، لایه جلسه می‌تواند در حفظ نوبت کمک کند.

یکی دیگر از خدمات این لایه، مدیریت Token است. در بعضی پروتکل‌ها لازم است هیچ‌کدام از طرفین، کاری را هم‌زمان شروع نکنند. برای مدیریت بر فعالیت‌های لایه جلسه، Token‌هایی تهیه می‌شود که بین مبدأ و مقصد قابل مبادله‌اند. در این شرایط فقط طرفی که Token را در اختیار دارد می‌تواند فعالیت کند و طرف مقابل باید منتظر باشد تا نوبت او برای استفاده از Token فرا برسد.

یکی دیگر از اعمال لایه جلسه این است که روی قسمت‌هایی از رشته داده‌ها را علامت‌گذاری می‌کند؛ در صورتی که بسته‌ای هنگام ارسال مفقود یا خراب شود، لایه جلسه بسته را از روی کدهای آن شناسایی و دوباره ارسال می‌کند.

۶-۱-۶- لایه نمایش

لایه نمایش ششمین لایه OSI است. این لایه داده‌ها را به روش استاندارد کدگذاری می‌کند.

اکثر کامپیوترها اطلاعاتی مانند نام افراد، تاریخ، مقادیر پول و اطلاعات مشابه دیگری را ارسال می‌کنند.

این اطلاعات به صورت کاراکتر بوده و هیچ کدام رشته های دودویی نیستند.

کدهای نمایش رشته های کاراکتری، اعداد صحیح و غیره ممکن است در کامپیوترهای مختلف متفاوت باشد. برای این که کامپیوترها با کدهای مختلف بتوانند با یکدیگر ارتباط برقرار کنند، اطلاعاتی که انتقال می یابند باید با استفاده از کدهای استاندارد تعریف و ارسال شوند تا در تمامی کامپیوترها و با سیستم عامل های متفاوت قابل دریافت و درک باشند.

۷-۱-۶ لایه کاربردی

هفتمین لایه مدل OSI است. این لایه حاوی پروتکل های گوناگون است که همه نرم افزارهای کاربردی برای ارتباط شبکه ای از آن ها استفاده می کنند.

لایه کاربردی بزرگ ترین لایه در استاندارد OSI است. این لایه شامل سیگنال هایی است که خدمات سودمندی از قبیل انتقال فایل و کنترل یک کامپیوتر از راه دور را به کاربر ارائه می دهد، در صورتی که لایه های پایین تر فقط در تبادل اطلاعات بین فرستنده و گیرنده نقش دارند. هم چنین این لایه می تواند ارتباط برنامه های مختلفی را که در محیط شبکه وجود دارند، با یکدیگر برقرار کند.

به عنوان مثال، صدها نوع نرم افزار در دنیا وجود دارد که هرکدام روش خاص خود را برای نوشتن، ویرایش و حرکت مکان نما روی صفحه انجام می دهند، در صورتی که این لایه وجود نداشت، ممکن بود در اجرای برنامه ها و ویرایش آن ها دچار مشکل شویم. برای حل این مشکل لایه کاربردی، اطلاعات لازم را از این برنامه ها گرفته و بایک استاندارد مشخص آن ها را به کامپیوتر مقصد می فرستد.

وظیفه دیگر لایه کاربردی انتقال فایل است. در سیستم فایل های مختلف، نام گذاری فایل ها، روش نمایش خطوط متن و غیره متفاوت است. این کار نیز همانند وظایفی از قبیل پست الکترونیک، کنترل کامپیوتر از راه دور و جستجو در بخش های مختلف درون حافظه، وظیفه لایه کاربردی است.

۲-۶-۲-مقایسه دو پروتکل در بخش های مختلف امنیتی

در ادامه، حملات، سرویس ها و مکانیزم ها و تجهیزات امنیتی در لایه های مختلف در قالب جداول ۱-۲-۳-۴ با یکدیگر مقایسه می شوند و همانطور که در جداول مذکور نشان داده شده است می توان نتیجه گرفت که بیشترین حملات به ترتیب در لایه IP, TCP، کاربرد و میزبان به شبکه است و سرویس ها و مکانیزم ها بیشتر در لایه IP به چشم می خورد و تجهیزات امنیتی با بهره گیری از مکانیزم های مختلف بیشتر در لایه IP, TCP و کاربرد، کاربری دارند.

در جدول ۵ تجهیزات امنیتی از نظر پارامترهای مختلف با یکدیگر مقایسه می شوند و مورد ارزیابی قرار می گیرند، استفاده از تجهیزات سخت افزاری نظیر فایروال، سوئیچ ها و مسیریابهای مدیریت پذیر، گران است و هزینه پشتیبانی آنها نیز بالاست و از پیچیدگی نسبتا بالایی برخوردارند. در تجهیزات نرم افزاری نیز هزینه پشتیبانی بدلیل لزوم Update مرتب، بالا است ولی هزینه استقرار و پیچیدگی پائین است.

جدول ۱. مقایسه تهدیدات امنیتی در لایه های چهارگانه TCP/IP

Application	TCP	IP	Host to Host	تهدید / لایه
*				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 امنیتی در منابع شبکه

کاربران شبکه	شبکه				منابع اهداف
	ارتباطات	اطلاعات	نرم	سخت	
	*	*			محرمانگی
	*	*	*	*	صحت
	*	*	*	*	قابلیت
	*	*		*	محافظت
*					تشخیص هویت
*					مسئولیت
*✓					حریم خصوصی
					آگاهی رسانی

جدول ۳. سرویس های امنیتی در لایه های مختلف TCP/IP

Application	TCP	IP	Host to	سرویس/لایه
*	*	*	*	محرمانگی
*	*	*	*	تایید هویت
*				رد انکار
	*	*		کنترل جامعیت و

جدول ۴. مکانیزم های امنیتی مربوط به لایه های مختلف TCP/IP

Application	TCP	IP	Host to	مکانیزم/لایه
*	*	*	*	رمزنگاری
*	*	*		امضای دیجیتال
*	*	*		کنترل دستیابی
*	*	*		درستی و صحت داده
		*		کنترل مسیریابی
*		*		رد انکار)

جدول ۵. مقایسه تجهیزات امنیتی در لایه های چهارگانه TCP/IP

Application	TCP	IP	Host to Network	تجهیزات امنیتی
			*	حفاظت فیزیکی
*	*	*	*	رمزنگاری
		*		IP Sec
	*			SSL
*	*	*		Firewall
*				AntiVirus
*	*	*	*	AAA Server
*	*	*	*	VPN
*				PGP
*	*	*		IDS/IPS

خود آزمایی و تحقیق

- ۱- به طور کلی وظایف لایه ها در مدل OSI چیست؟
- ۲- Packet چیست؟
- ۳- یافتن آدرس کامپیوتر مقصد و مبدا وظیفه کدام لایه است؟
- ۴- پروتکل های شبکه در کدام لایه قرار دارند؟
- ۵- تجهیزات امنیتی مانند Firewall و Anti Virus ها در کدام لایه شبکه بهتر عمل می کنند؟
- ۶- تحقیق کنید که تجهیزات امنیتی مانند Firewall و ... از لحاظ سخت افزاری و نرم افزاری چه تفاوتی با هم دارند؟

فصل هفتم - امنیت در شبکه

هدف های رفتاری

دیواره آتش را تعریف کند و با آن کار کند.
تفاوت آنتی 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 میسر نخواهد 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 proxy مورد بحث قرار می گیرد.

۷-۱- دیواره آتش (Firewall)

دیواره آتش به صورت نرم افزاری یا سخت افزاری موجود است که اطلاعات ارسالی بین دوشبکه داخلی 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 یک شبکه داخلی ، قادر به ارتباط با هر سایت و هر شخص بر روی اینترنت بوده و از طرف دیگر کامپیوترهای دیگر توانایی ورود به کامپیوتر های شبکه داخلی یا شخصی را خواهند داشت. کاربران شبکه داخلی 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 یک شبکه داخلی، می تواند زمینه دستیابی به اطلاعات موجود در شبکه داخلی را برای افراد غیر مجاز فراهم نماید.

۷-۱-۱- ضرورت استفاده از دیواره آتش

در صورتی که از دیواره آتش استفاده نشود شبکه از جنبه های مختلف به خطر می افتد برخی از این مواردی که شبکه ها یا کاربران به وسیله ی حمله کنندگان به شبکه های کامپیوتری تهدید می شوند عبارتند از

Application Backdoors - اغلب نرم افزارهای موجود که روی کامپیوترتان نصب می کنید ، ممکن است دارای Bug های باشند که هکرها از طریق این کانال ها ی نفوذی می توانند به کامپیوتر شما 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.

- **مباران 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 بنظور 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 داخلی از دیواره آتش استفاده شود ، وضعیت کاملاً تغییر می کند و مسئولین شبکه می توانند با استفاده از دیواره آتش مجموعه سیاست های امنیتی را در مقابل افرا غیرمجاز بر روی خطوط خود پیاده سازی کنند . به عنوان مثال مجوز ها و محدودیت های زیر را اعمال نمایند :

- تمام کامپیوترهای موجود در شبکه مجاز به استفاده از اینترنت می باشند ، ولی کارمندان خاص نتوانند از اینترنت برای ارسال و دریافت Email استفاده نمایند
- امکان دسترسی از راه دور برای مشاهده فایل ها یا تغییر آن ها به وسیله ی افراد خارج از شبکه یا افراد داخلی غیر مسئول بگینند

۲-۱-۷- سفارشی 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 می شود تا امکان محدود کردن دسترسی با توجه به آن عبارات انجام شود در این حالت بسته های اطلاعاتی که در حال مبادله است بررسی و هر بسته اطلاعاتی که حاوی کلمات مشخص شده باشد ، به وسیله ی دیواره آتش دسترسی 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 دستیابی به سایت هائی را محدود یا صرفاً " امکان استفاده از یک سایت خاص را فراهم کرد .

- **آدرس های IP** . همانطور که می دانید هر کامپیوتر روی اینترنت دارای یک آدرس منحصر بفرد با نام IP است . به عنوان مثال، اگر کاربر یک آدرس IP خارج از شبکه، بدون مجوز فایل های زیادی را از سرویس دهنده دریافت نماید (این کار ترافیک شبکه را افزایش می دهد) ، دیواره آتش می تواند با شناسایی IP مورد نظر و محدود نمودن آن ترافیک مربوطه را کنترل نماید .

- **پروتکل ها** . پروتکل نحوه ارتباط بین سرویس دهنده و سرویس گیرنده را مشخص می نماید . با استفاده از دیواره آتش می توان، پروتکل های مورد نظر را محدود کرد. مثلاً " پروتکل وب ، http و پروتکل مربوط به دریافت یا ارسال فایل ها Ftp است

برخی از پروتکل های رایج که بر روی آنها فیلتر اعمال می شود بشرح زیر می باشند :

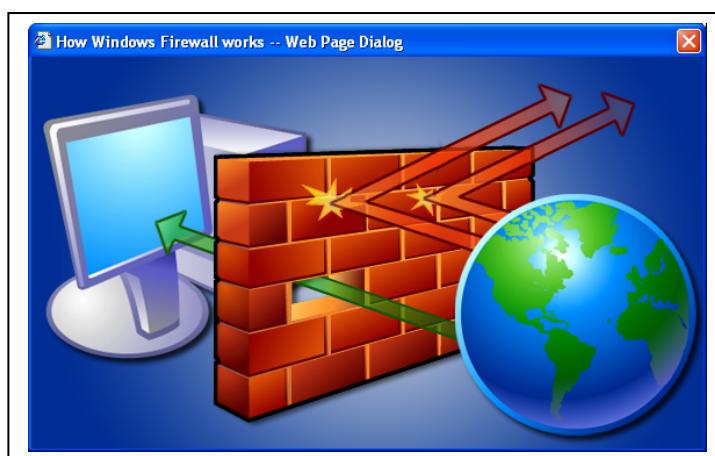
- IP - (Internet Protocol)
- TCP - (Transport Control Protocol)
- HTTP - (Hyper Text Transfer Protocol)
- FTP - (Protocol File Transfer)
- SMTP (Simple Mail Transfer Protocol)

- **درگاه ها** . بر روی اینترنت ، خدمات هر سرویس دهنده ، با استفاده از درگاه های شماره گذاری شده ارائه می شود. مثلاً " سرویس دهنده وب اغلب از درگاه ۸۰ و سرویس دهنده FTP از درگاه ۲۱ استفاده می نماید . یک سازمان ممکن است با استفاده از دیواره آتش بر روی درگاه خاصی محدودیت ایجاد نماید با امکان دستیابی به آن تحت کنترل باشد .

علاوه بر دیواره آتش نرم افزاری ، می توان از دیواره آتش سخت افزاری نیز استفاده کرد . امنیت دیواره آتش های سخت افزاری بمراتب بیشتر از دیواره آتش های نرم افزاری است .

۳-۱-۷- تنظیمات دیواره آتش در ویندوز:

همانطور که گفته شد برای جلوگیری از دسترسی غیرمجاز کاربران شبکه یا اینترنت از دیواره آتش استفاده می شود. این دسترسی میتواند شامل انواع برنامه های مخرب و ویروس ها و کرمها (worms) باشد که به صورت یک طرفه بدون اینکه درخواستی برای آن ارسال شده باشد، وارد کامپیوتر شده و سیستم را دچار اختلال می کند .



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 های ناشناس که به طور ناخواسته برای ما ارسال میشوند را بگیرد
- در دیواره آتش این امکان وجود دارد که یک Log file یا فایل وقایع نگار درست کنیم که گزارش کاملی از ارتباطات موفق یا ناموفق از کامپیوتر ما را ثبت کند.

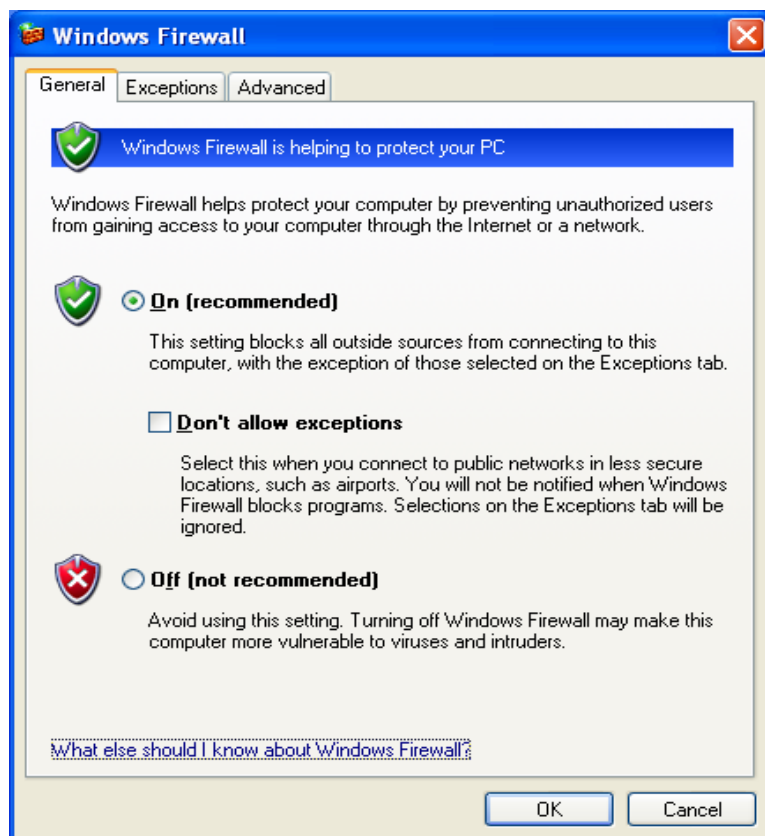
۷-۱-۵- فعال نمودن دیواره آتش در روی ویندوز XP

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 می باشد. 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 (استثنا) 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 می آید.

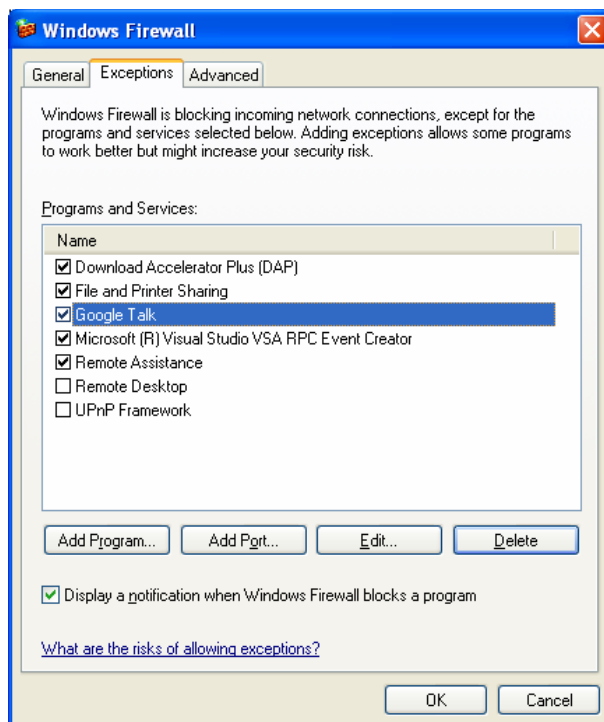
با انتخاب Off(Not recommended) دیواره آتش غیر فعال شده و کامپیوتر در برابر برنامه های مزاحم که بدون اجازه شروع به کار میکنند آسیب پذیر خواهد بود.

زبانه : Exceptions

با انتخاب این زبانه می توانیم برای بعضی از برنامه های کاربردی یا سرویس هایی که دیواره آتش آنها 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.

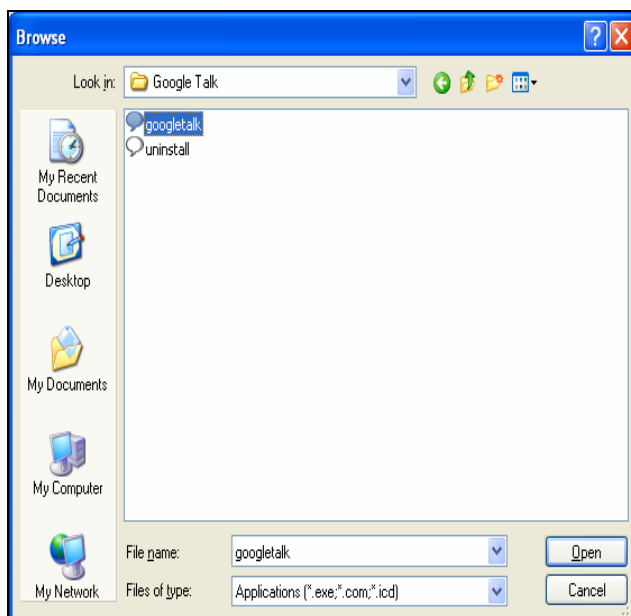
به عنوان مثال، اگر ما بخواهیم از برنامه هایی نظیر Google talk، Download accelerator (DAP) استفاده کنیم در حالی که دیواره آتش ویندوز فعال است امکان تبادل اطلاعات با خارج از شبکه غیر ممکن است اما اگر این برنامه ها در لیست استثنا ها تعریف شود. ارتباط به راحتی برقرار می شود. مانند شکل زیر:

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 نمایم. در صورتی که برنامه مورد نظر در لیست نباشد. با کلیک بروی گزینه Browse می‌توانیم مسیر برنامه را وارد کنیم (شکل ۴-۱)



شکل ۴-۷

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 از درگاه های 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.

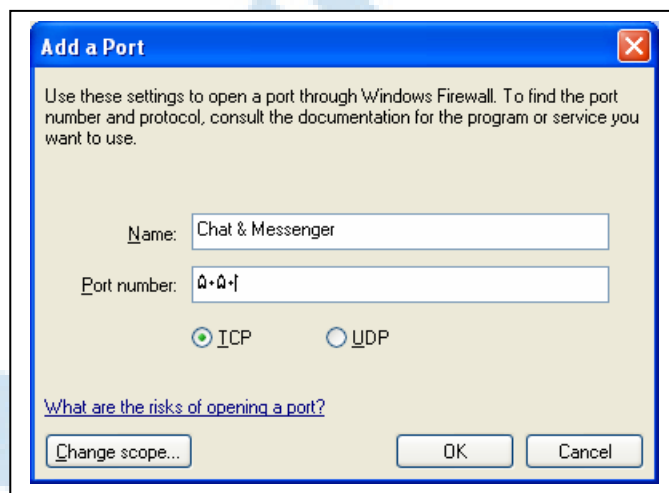
جدول

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

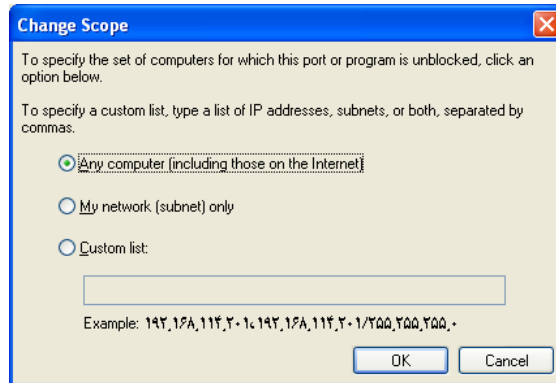


شکل ۵-۷

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 کامپیوتر شما 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 درگاه ها که برای شما ناشناس هستند را باز نکنند.
- ۳- برنامه ها یا درگاه 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 درگاه 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 يك شبکه ضروري است؟ چرا؟
- ۳- يك کامپیوتر از چه جنبه هاي ممکن است مورد حمله قرار بگيرد؟
- 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 رایجی وجود دارد؟

فصل هشتم - آشنایی با برخی از شبکه

های WAN

هدف های رفتاری

تکنولوژی DSL را تعریف کند
مزایا و معایب DSL را بیان کند.
شبکه های محلی بدون سیم را تعریف کند.

۸-۱-۱ DSL

DSL یک تکنولوژی دسترسی به اینترنت می باشد که با استفاده از خطوط تلفن ارتباطی با سرعت بیش از ۱/۵۴۴ مگابایت را برقرار می نماید. از مزایای DSL این است که می تواند به طور همزمان داده و صوت را منتقل نماید. بنابراین این ضمن برقرار ماندن ارتباط تلفنی می توان با استفاده از آن ارتباط اینترنتی نیز برقرار نمود.

در حال حاضر اکثر کاربران خانگی شبکه اینترنت و حتی برخی سازمان ها از طریق مودم های آنالوگ به وصل می شوند. افزایش سریع حجم داده های اینترنت و نیاز به انتقال صوت و تصویر، محدودیت هایی را برای انتقال داده ها با مودم های معمولی شده است لذا برای کاهش این محدودیت ها تکنولوژی های پیشرفته ای مورد استفاده قرار می گیرد.

فرکانسهای استفاده شده در مخابرات ۴ کیلو هرتز است تکنولوژی DSL با استفاده از فرکانسهای بالاتر از و با تکامل Digital Signal Processing (DSP) قادر به ارسال داده ها با سرعت های خیلی بالاتر نسبت به مودم های آنالوگ می باشد.

۸-۱-۱-۱ مزایا و معایب DSL:

- برقراری DSL نیاز به کابل کشی جدید ندارد و با استفاده از خطوط تلفن امکان اتصال به DSL وجود دارد.
- هنگام برقراری ارتباط اینترنتی با DSL نیازی به قطع شدن مکالمه تلفنی نیست و خط تلفن آزاد است.
- سرعت برقراری ارتباط با DSL (۱,۵ Mbps) در مقایسه با سرعت مودم های معمولی (56 Kbps) به مراتب بالاتر است.

معایب:

- فاصله بین سرویس گیرنده و سرویس دهنده خدمات اینترنت در سرعت ارتباط موثر است و با افزایش فاصله سرویس گیرنده از مرکز رایانه سرویس DSL سرعت کاهش می یابد.
- این سرویس دارای محدودیت فاصله تا ۵۴۶۰ متر می باشد

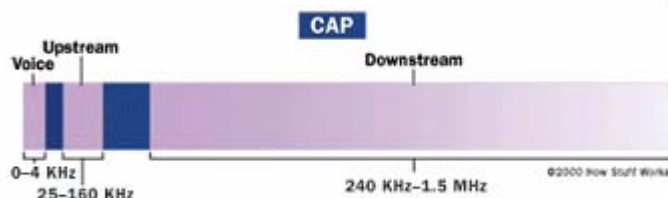
¹ - Distributed Subscriber Line

- امکان دریافت این سرویس در همه مناطق به دلیل متداول نبودن آن وجود ندارد.
- هزینه اولیه برقراری سرویس DSL بالاتر است.

۲-۱-۸- اصول کار DSL:

همانطور که می دانید سیستم تلفن استاندارد با یک زوج سیم مسی (TP) انجام می شود از طرف دیگر سیم های مسی دارای مقدار زیادی فضا برای حمل اطلاعاتی بیش از مکالمات تلفنی هستند و می توانند طیف وسیعی از فرکانسها را بیش از چیزی که در انتقال صوتی استفاده می شود پشتیبانی کنند. DSL با استفاده از این فضای اضافی ارتباط اینترنتی را برقرار می نماید بدون اینکه در کیفیت ارسال مکالمات مشکلی ایجاد کند.

تکنولوژی DSL می تواند حداکثر سرعت DownStream 8 مگابیت در ثانیه در فاصله حدود ۱۸۲۰ متر و سرعت UpStream تا ۶۴۰ کیلوبیت برثانیه را در اختیار کاربران قرار دهد (شکل ۱-۸).



شکل ۱-۸

در عمل بهترین سرعتهای موجود امروزی در مسیر DownStream تکنولوژی DSL به میزان ۱,۵ مگابیت بر ثانیه است و سرعت UpStream بین ۶۴ تا ۶۴۰ کیلوبیت بر ثانیه می باشد.

تحقیق کنید در سرویس DSL دلیل افت سرعت در فواصل دورتر چرا شدیداً کاهش می یابد؟

۳-۱-۸- سیستم های تفکیک سیگنال در DSL

قبلاً اشاره شد که DSL از سیم های تلفن برای برقراری ارتباط اینترنتی استفاده می کند بناب این لازم است که به نحوی سیگنال های ارتباط تلفنی و اینترنتی را به نحوی کنترل نماید برای تفکیک و کنترل سیگنال ها در گذشته از سیستم CAP استفاده می شد و امروز بیشتر از سیستمی به نام DMT¹ استفاده می شود (شکل ۱-۸).

سیستم CAP سیگنالهای موجود در خط تلفن را به سه باند متمایز از هم تقسیم می کند:

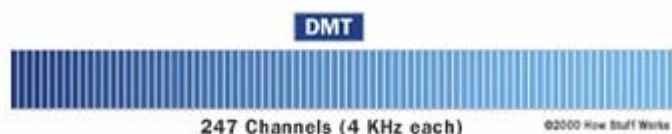
- مکالمات صوتی در باند صفر تا ۴ کیلو هرتز
- کانال UpStream باند ۲۵ تا ۱۶۰ کیلو هرتز
- کانال DownStream در فرکانس ۲۴۰ کیلوهرتز تا فرکانسی

این سیستم با سه کانال کاملاً جدا امکان تداخل بین کانالهای روی یک خط یا بین سیگنالها در خطوط مختلف را به حداقل می رساند.

سیستم دیگری که برای کنترل سیگنال ها استفاده می شود سیستم DMT است، سیستم DMT نیز سیگنالها را به سه کانال جداگانه تقسیم می کند، و مجموعه را ۲۴۷ کانال تقسیم می کند. از بین این ۲۴۷ کانال جداگانه که هر یک ۴ کیلو هرتز پهنا دارند، از دوتای آنها

¹ Discrete Multi Tone

استفاده می کند. هرکانال دائما تحت نظارت قرار دارد تا اگر کیفیت سیگنال مطلوب نباشد، از سیگنال کانال دیگری استفاده شود. این سیستم دائما بهترین کانال را برای ارسال و دریافت پیدا می کند.



شکل ۲-۸

فرستنده / گیرنده DSL یا Transciever:

اغلب مشترکین خانگی از فرستنده / گیرنده DSL به عنوان مودم یاد می کنند.

فرستنده / گیرنده را می توان با چند روش به یک دستگاه سمت مشترک متصل نمود. اغلب سیستمهای خانگی از ارتباط USB یا اترنت 10-Base-T استفاده می کنند. در حالیکه اغلب فرستنده / گیرنده های DSL عرضه شده به وسیله ISP ها و شرکت تلفن، فرستنده / گیرنده می باشند، اما دستگاههای مورد نظر در شرکتها، تجاری ترکیبی از Router ها، Switch ها و یا سایر تجهیزات شبکه بندی هستند.

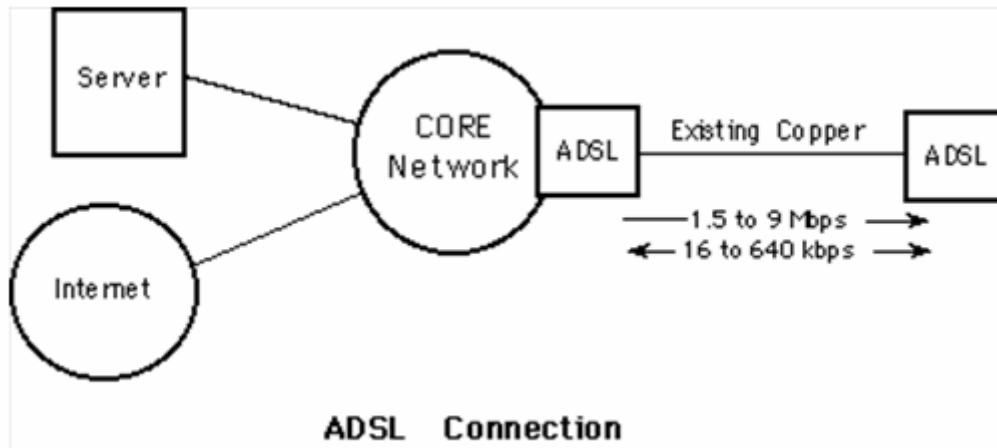
۴-۱-۸- انواع DSL:

سرویس DSL انواع گوناگونی دارد. از قبیل ADSL، IDSL، CDSL، DSL Lite، HDSL، RADSL، VDSL و ADSL و VDSL بیشتر از بقیه موارد استفاده می شود.

ADSL¹:

با توجه به شکل ۱-۸ پهنای باند بیشتری در DownStream نسبت به UP Stream وجود دارد و از طرف دیگر کاربران اینترنت، به طور معمول خیلی بیشتر از آن چیزی که اطلاعات می فرستند، از شبکه اطلاعات دریافت می کنند. سرعت انقل و انتقالات در ADSL برای ارسال اطلاعات به مشتری بیشتر از 6Mbps برای دریافت اطلاعات و بیشتر از 640Kbps برای ارسال و دریافت اطلاعات مشترک (در هر دو مسیر) می باشد به این دلیل این سرویس را نامتقارن می نامند.

¹ -Asymmetric Digital subscriber Line



شکل 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 .

:VDSL¹

VDSL يك تكنولوژي توسعه يافته است و در مسافتهاي کوتاه (حدود ۳۰۰ متر) سرعت انتقال بسيار بالايي (بين 51Mbps تا 55Mbps) دارد . در بسياري از موارد همراه با سرويس ADSL به كار گرفته مي شود .

۲-۸- شبکه هاي محلي بدون سيم Wireless LAN

شبکه هاي محلي بي سيم (WLAN) فن آوري جديدي در شبکه محلي است که استفاده کنندگان را قادر مي سازد به شبکه يك سازمان در هر مكاني از آن سازمان دسترسي پيدا کنند ، بدون آن که نيازي به اتصال فيزيكي به شبکه مذکور داشته باشند .

همانطور که قبلاً گفته شد شبکه هاي محلي بدون سيم از فرکانس راديويي يا امواج مادون قرمز ، به عنوان سيگنال هاي ارتباطي و از هوا به عنوان رسانه انتقال ، استفاده مي کنند .

توپولوژي WLAN

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

شکل ۴-۸- شبکه Point-to-Point (شکل ۲۱-۵ ص ۳۸ آشنایي با شبکه)

¹ - Very High Data Rate DSL

نوع دیگر پیکربندی شامل استفاده از وسیله ای به نام نقطه اتصال (Access Point) است. AP وسیله ای است که ایستگاه های بدون سیم را قادر می سازد تا به شبکه محلی متصل گردند.

شکل ۴-۸ نشان می دهد که یک Access Point از طریق یک سیم به شبکه LAN متصل شده است. ارتباط ایستگاه های بدون سیم را از طریق هوا به کمک ارتباط کابلی که با HUB دارد، برقرار می سازد. به عنوان یک پل ارتباطی بین ایستگاه های بدون سیم و شبکه محلی عمل می کند.

شکل ۵-۸ ارتباط ایستگاه های بدون سیم با شبکه محلی به وسیله ی AP (شکل ۵-۲۲ ص ۳۹ آشنایی با شبکه)

ناحیه ای که به وسیله ی یک AP تحت پوشش قرار می گیرد سلول (Cell) نامیده می شود و سعت ناحیه تحت پوشش و تعداد ایستگاه های که می توانند از طریق یک AP با شبکه ارتباط برقرار نمایند، محدود می باشد و با افزایش ناحیه و تعداد ایستگاه ها، باید تعداد AP را افزایش داد.

از مهمترین مزایای شبکه های محلی بدون سیم می توان به موارد زیر اشاره نمود:

- نیازی به سیم کشی برای هر ایستگاه کاری نیست
- در زمان برقراری ارتباط امکان حرکت وجود دارد و استفاده کنند ه می تواند بدون اینکه ارتباط خود را قطع کند رایانه خود را جابجا نماید.

خود آزمایي و تحقیق

۱. تکنولوژی DSL بر چه اساسی مبتنی است؟
۲. VDSL چه واژه هایی است و به چه مفهومی می باشد.
۳. مزایای شبکه WLAN را بنویسید.
۴. وظیفه AP در شبکه WLAN چیست؟
۵. معایب DSL چیست؟
۶. انواع DSL را نام ببرید.
۷. تفاوت عمده خطوط DSL با خطوط Dialup در چیست؟

بخش دوم

Windows 2003 Server



www.IranMeet.com

فصل نهم - مدیریت دسترسی به منابع

هدف های رفتاری
 ویژگی های پوشه های به اشتراک گذاشته شده را بیان کند.
 پوشه ها را به اشتراک بگذارد و به آنها مجوز بدهد.
 از پوشه های به اشتراک گذاشته شده در شبکه را استفاده کند.
 مجوزهای مدیریتی ایجاد کند.
 مجوزهای مؤثر را محاسبه کند.

۱-۹- پوشه های به اشتراک گذاشته شده

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

برخی از ویژگی 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 و یک 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 اشتراک گذاشتن یک ویژگی مربوط به سیستم عامل می باشد: بنابراین شما می توانید یک پوشه را در هر فایل سیستمی که ویندوز پشتیبانی می کند به اشتراک بگذارید (FAT, FAT32, CDFS, NTFS) با این تفاوت که اگر آن پوشه در پارتیشن با فایل سیستم NTFS باشد، قابلیت کنترل بیشتری را در اختیار مدیر شبکه قرار میدهد.

۴- فقط اعضای گروه های administrators, power users در کامپیوترهای عضو Domain می توانند یک پوشه را به ترتیب در روی DC ها و کامپیوترهای عضو Domain به اشتراک بگذارند.

۵- اگر پوشه ای که می خواهیم به اشتراک بگذاریم در داخل یک پارتیشن NTFS باشد، برای به اشتراک گذاشتن آن، کاربر علاوه بر عضویت در گروه های ذکر شده باید حداقل مجوز دسترسی Read روی آن پوشه باید داشته باشد.

۲-۹- نحوه به اشتراک گذاشتن پوشه ها

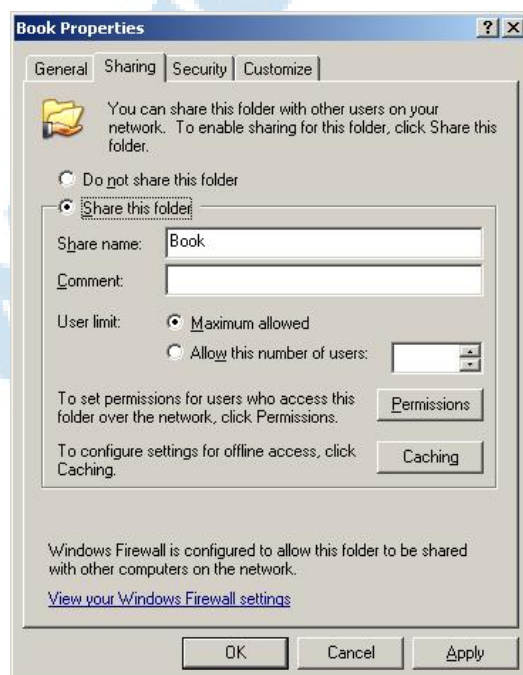
یک پوشه را به روش های مختلف می توان به اشتراک گذاشت. در زیر به دوروش اشاره می شود.

نکته : اگر پوشه ای که به اشتراک می گذارید در یک کامپیوتر با سیستم عامل xp قرار داشته 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 ۹-۱)



شکل ۹-۱

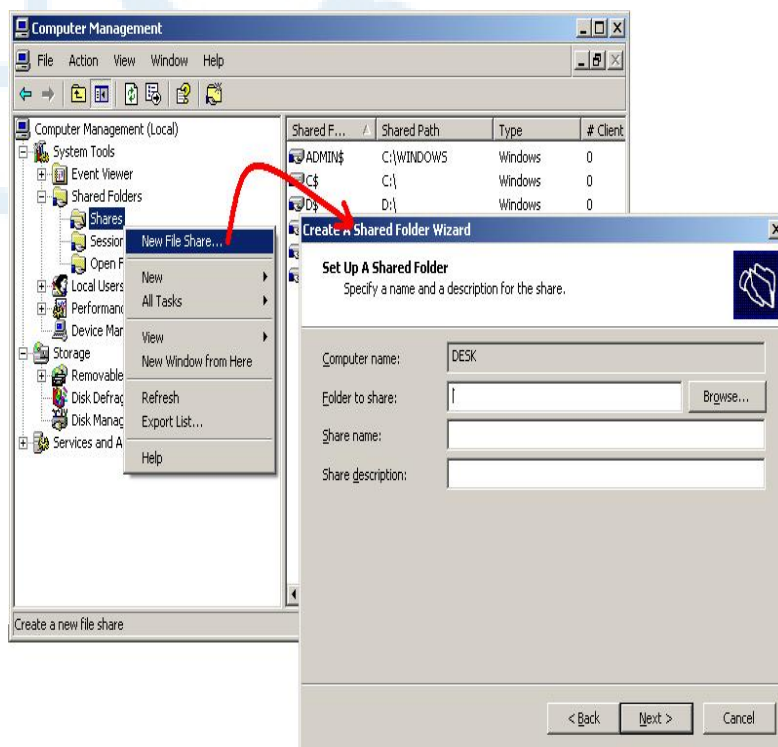
روش اول : در my computer روی یک پوشه کلیک راست کرده و آزمینوی که ظاهر می شود گزینه sharing and security را انتخاب نمایید . سپس گزینه share this folder را انتخاب نمائید و در قسمت share name یک اسم منحصر به فرد در آن تایپ نمائید و سپس روی گزینه ok کلیک کنید. (شکل ۹-۲)



(شکل ۹-۲)

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 از منوی Action گزینه New share را 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 وارد کرده و گزینه Next را انتخاب نمایید . (شکل ۳-۹)

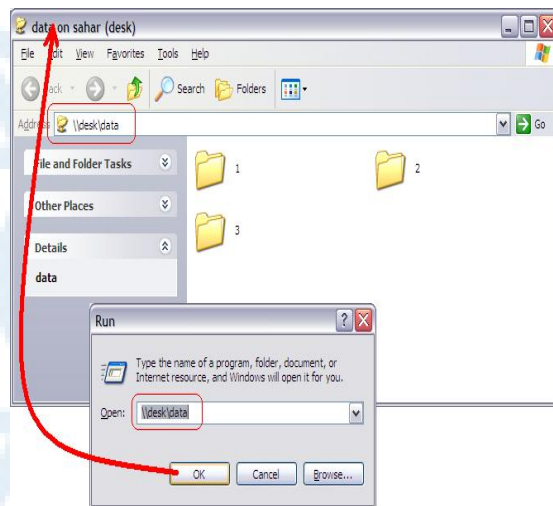


شکل ۳-۹

- در صفحه بعد نحوه اعطای مجوز روی پوشه به اشتراک گذاشته شده سؤال می شود گزینه Next 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 خواهید کرد که یک گزینه به لیست پوشه های به اشتراک گذاشته شده اضافه خواهد شد .

۳-۹ - آدرس دهی به شبکه (UNC Path)

کاربران برای دیدن فایل های یک پوشه به اشتراک گذاشته شده می توانند از آدرس دهی UNC استفاده نمایند . این نوع آدرس دهی به صورت `\\ computername \ share name` می باشد . به عنوان مثال برای 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 (Hidden shares)

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

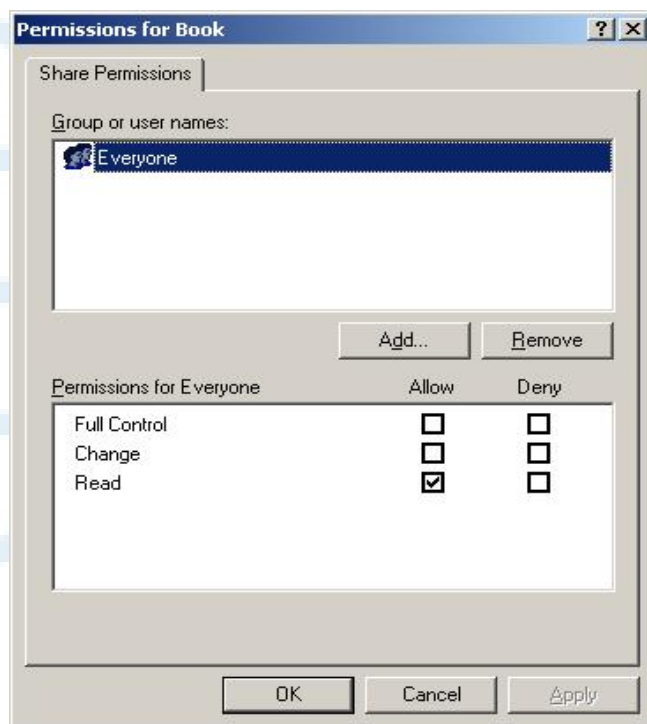
۹-۵- Administrative shares

اشتراک هایی وجود دارند که برای 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 از طریق 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 پیدا کنید.
- lpc\$: کاربردی برای کاربران و مدیران شبکه نداشته بلکه برای مدیریت از راه دور و دسترسی کاربران به پوشه های 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 دسترسی 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 Everyone روی 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 مشاهده 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 غیر NTFS بدین صورت است که اجتماع Shared Permission های کاربر و گروهایی که عضوشان می باشید را حساب کنید، مگر اینکه یک مجوز Deny شده باشد.

جدول ۹-۱ بایک مثال مجوز مؤثر کاربر user1 را که عضو گروه های 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 مجوز مؤثر NTFS 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 group1، group2 می باشد را نشان می دهد.

جدول ۹-۲

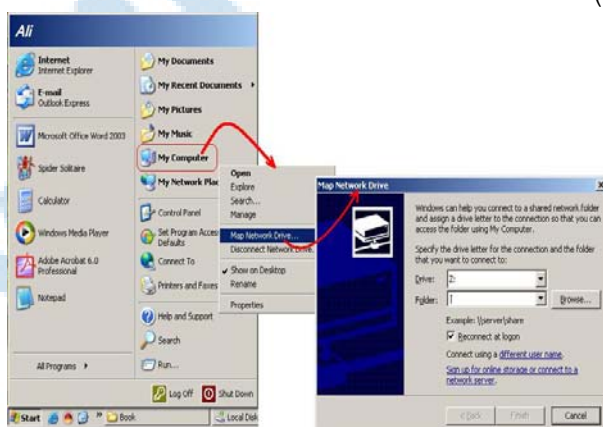
Group	shared Permission	NTFS Permission
USER 1	READ	READ
GROUP 1	CHANGE	WRITE
GROUP 2	FULL CONTROL	WRITE (Deny)
EFFECTIVE	FULL CONTROL	READ
FROM EFFECTIVE NETWORK	READ	READ

۹-۷ درایوهای شبکه

برای 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 از منویی 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.

درایوی به نام U برای به اشتراک گذاشتن پوشه مورد نظر خود
انتخاب و چند تصویر برای گروه عضو شبکه به اشتراک بگذارید



خود آزمایي و تحقیق

- 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 پارتیشن NTFS و پارتیشن هاي ديگر را بيان كنيد.
- ۵- Map Drive چيست؟ چگونه مي توان آن را ساخت؟
- ۶- تحقیق 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 های رفتاری

اجزای چاپ در شبکه را تعریف کند.
بر روی سرور چاپ و کلاینت ها چاپگر نصب کند.
مجوز دسترسی کاربران به چاپگرهای به اشتراک گذاشته شده کنترل کند.
بتواند صف کارهای چاپی را کنترل کند.
Spool Folder را تعریف کند و بتواند آدرس آن را تغییر دهد.
مجوزهای دسترسی در پارتیشن های NTFS را شرح دهد.

۱-۱۰ آشنایی با اجزای چاپ در شبکه

یکی از امکاناتی که شبکه در اختیار ما قرار می دهد به اشتراک گذاشتن منابع فیزیکی است و از این طریق علاوه این که می توانید مدیریت مناسبی بر انجام امور داشته باشید با استفاده از آن می توانید با صرفه جویی در هزینه ها بهره وری را افزایش دهید در این فصل به اشتراک گذاشته شدن چاپگر به عنوان یکی از منابع مهم در ادارات و شرکت ها مورد بررسی قرار می گیرد قبل از شروع لازم است با برخی از واژه های مختلف چاپ در شبکه آشنا شوید

- **Printer¹**: به نرم افزار رابط بین دستگاه چاپ و کاربران «چاپگر» گفته می شود. چاپگرها به دوتنوع تقسیم می شوند:
- o **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 اشتراک بگذاریم. به عبارت دیگر اگر کامپیوتر خود را میخواهیم به **Print server** تبدیل کنیم، از این نوع چاپگر باید استفاده کنیم.
- o **Network printer**: اگر میخواهیم از یک چاپگر به اشتراک 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 دوتنوع تقسیم می شوند:
- **Local print Device**: به دستگاه چاپی گفته می شود که مستقیماً 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 اشتراک گذاشته می شود.
- **Print Queue**: به کارهای چاپی که در یک چاپگر منتظر چاپ شدن می باشند، گفته می شود.

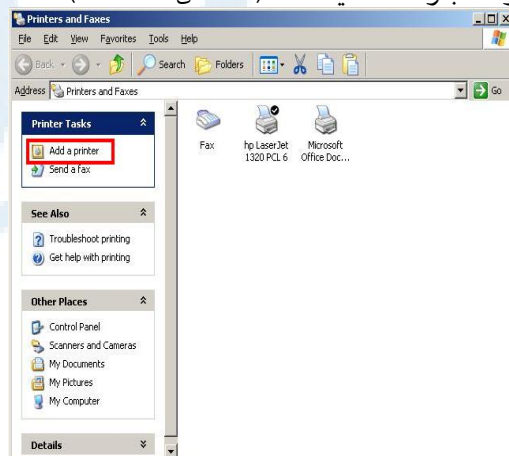
اصطلاح چاپ که در درس مبانی کامپیوتر به دستگاه چاپگر اطلاق شد يك اصطلاح غلط متداول است که در آن درس پذیرفته شده -
¹است.

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

۱۰-۲- نصب چاپگرها

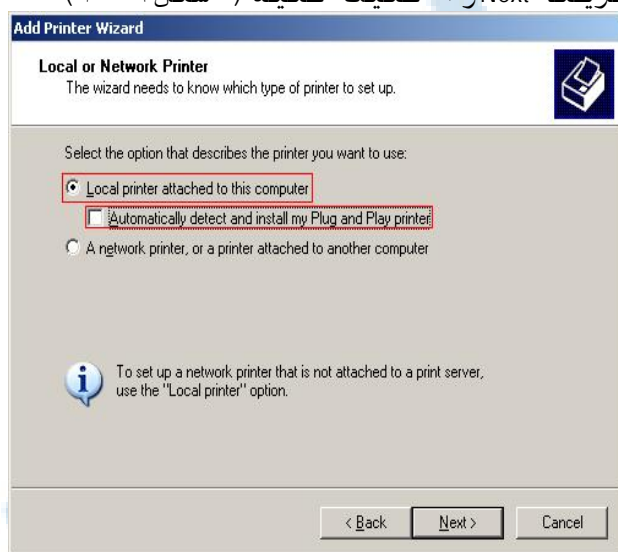
۱-۱۰-۲- نصب و به اشتراک گذاشتن چاپگر روی سرور چاپ

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



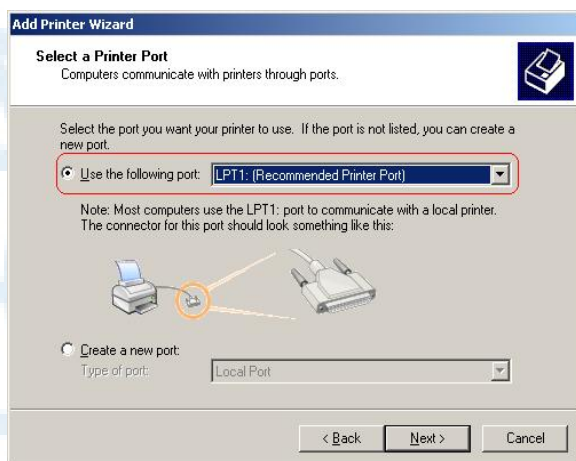
شکل ۱-۱۰-۱

- از ویزاردی که ظاهر می شود گزینه Next را کلیک کنید. در صفحه بعد برای نصب چاپگر و به اشتراک گذاشتن آن گزینه اول را مطابق شکل ۱۰-۲ انتخاب نموده و تیک گزینه Automatically detect... را بردارید و گزینه Next را کلیک کنید (شکل ۱۰-۲)



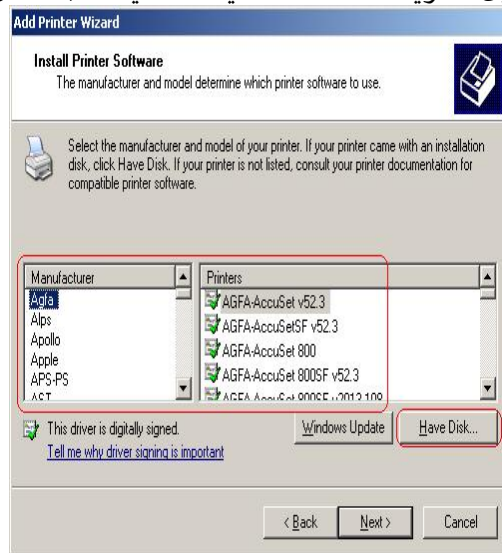
شکل ۱۰-۲

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



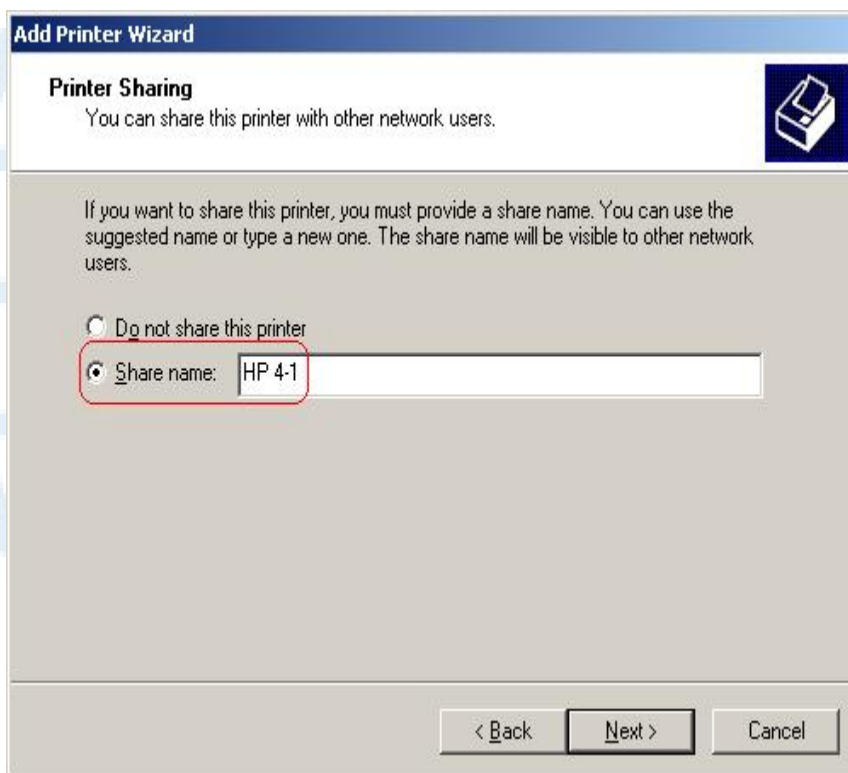
شکل ۱۰-۳

- در صفحه بعد از لیست چاپگرهای نمایش داده شده چاپگر خود را انتخاب کنید. در صورتی که چاپگر را در لیست نتوانستیم پیدا کنیم، درایور چاپگر را به کمک گزینه Have disk معرفی کنید (شکل ۱۰-۴).



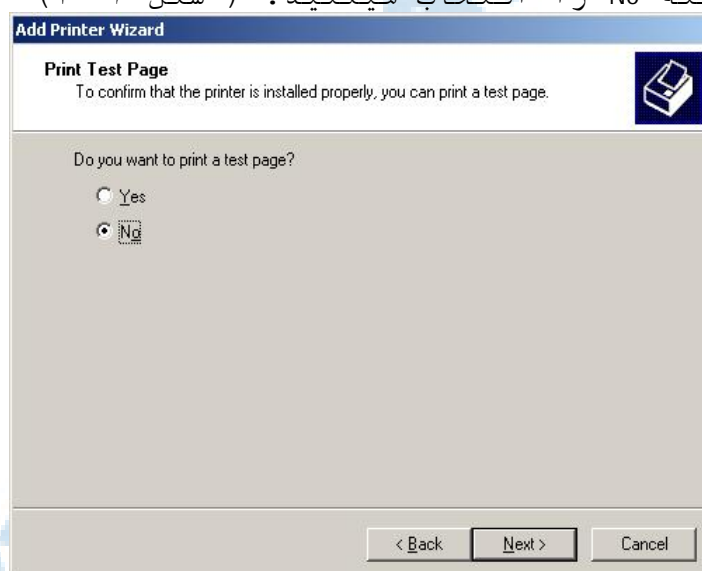
شکل ۱۰-۴

- در صفحه بعد یک اسم برای چاپگر انتخاب نموده و روی گزینه Next کلیک کنید.
- در صفحه بعدی مطابق شکل ۱۰-۵ 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 از طریق شبکه به این کامپیوتر متصل می شوند نمایش داده می شود. سپس روی گزینه Next کلیک کنید. (شکل ۱۰-۵)



(شکل ۱۰-۵)

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

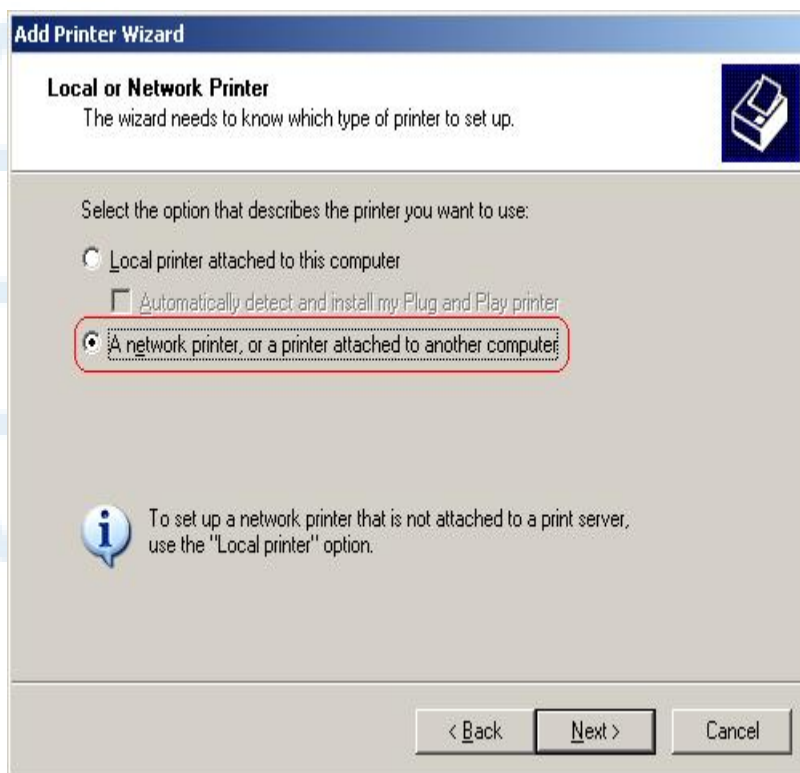


(شکل ۱۰-۶)

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

۱۰-۲-۲ نصب چاپگر روی کلاینت

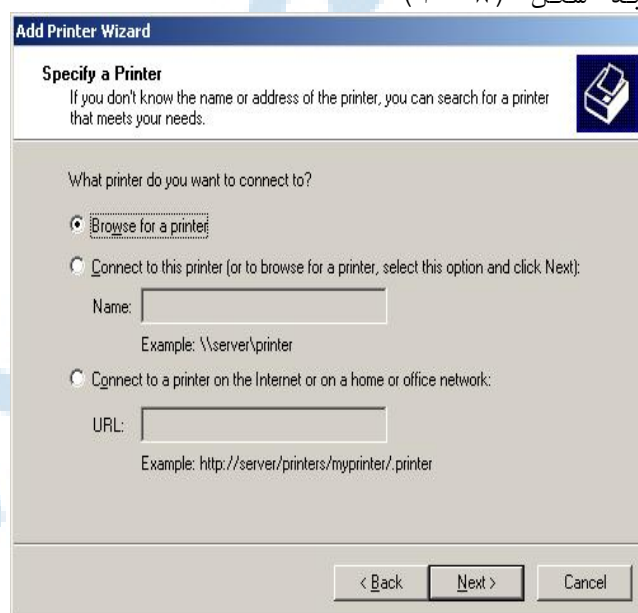
- حال در یکی از کلاینت های شبکه گزینه Add a printer را از مسیر Control Panel \ Printer And Faxes انتخاب کرده سپس گزینه نشان داده شده را مطابق شکل ۱۰-۷ انتخاب و روی گزینه Next کلیک کنید.



(شکل ۷-۱۰)

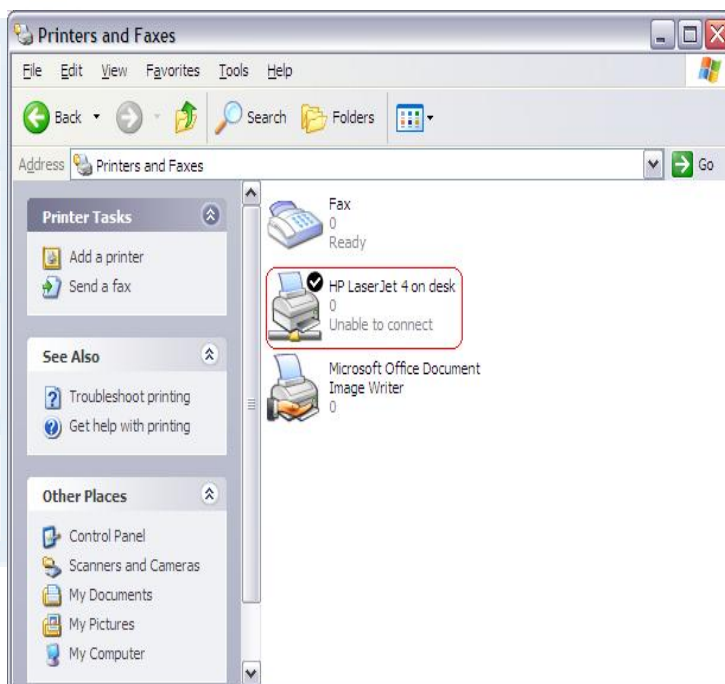
در این صفحه مطابق شکل ۸-۱۰ گزینه :

- Browse for A printer : را برای انتخاب یک چاپگر از لیست چاپگرهای شبکه ، انتخاب کنید.
- Connect to this printer : را به منظور تایپ آدرس UNC 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)

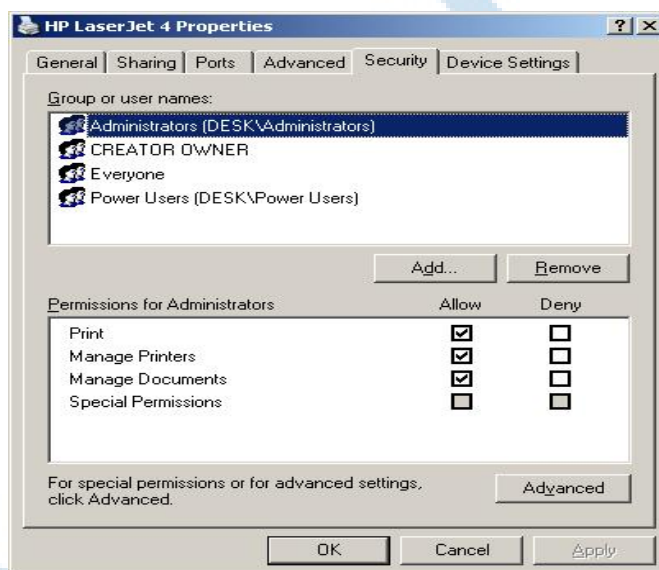
- سپس ویزارد را مشابه نصب چاپگر روی سرور چاپ ادامه داده و گزینه Finish را در صفحه آخر انتخاب نمائید تا نصب چاپگر روی کلاینت به پایان برسد . که در این صورت مشاهده می کنید که یک چاپگر در کلاینت اضافه شده است . شکل (۹-۱۰)



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 خود را برای چاپ به آن ارسال کنید .
- Manage printers: این مجوز علاوه بر این که تمامی کارایی مجوز Print را در اختیار کاربر می گذارد، به کاربر امکان مدیریت کامل چاپگر را نیز می دهد ، طوری که کاربر می تواند یک چاپگر را pause و یا Restart نماید یا چاپگر را به اشتراک بگذارد ، مجوزهای کاربران را روی چاپگر تغییر دهد 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، pause، Resume، Restart

و یا cancel نماید . به وسیله این مجوز کاربر نمی تواند اسناد خود را 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 های 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

برای اعطای مجوز کفایت که روی چاپگر مربوطه کلیک راست کرده و گزینه Properties را انتخاب نمائید و سپس در زبانه Security می توانید لیست کاربران و گروهها و همچنین مجوزهای آنها را مشاهده نموده و با استفاده از کلیدهای Add یا Remove به کاربران و گروههای مختلف مجوز اعطا نمائید .

۱۰-۵- نحوه مدیریت صف کارهای چاپی

برای 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 نمائید .

همچنین می توانید تعیین نمائید که به یک کاربر خاص بعد از چاپ شدن کار چاپی یک پیغام ارسال نماید و نهایتاً اینکه می توانید تعیین کنید که کار چاپی در یک بازه زمانی مشخص بتواند چاپ شود .

شکل ۱۰-۱۱

۱۰-۶- تغییر آدرس Spool Folder

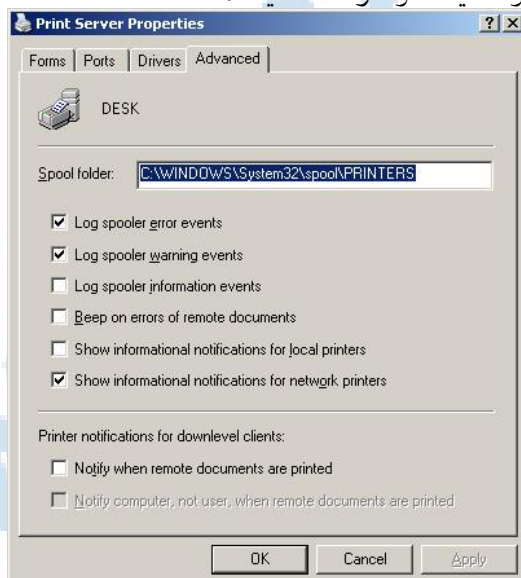
هنگامیکه در ویندوز یک فایلی را چاپ می کنید . آن فایل به طور مستقیم به دستگاه چاپ ارسال نمی شود در ابتدا آن کار چاپی به وسیله ی یکی از سرویس های ویندوز به نام Print Spooler در داخل یک فایلی نوشته شده و سپس درصاف قرار داده می شود.

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

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

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

- برای انجام این کار گزینه Server Properties را از منوی 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 (۱۰-۱۲)

۷- ۱۰- آشنایی با مجوزها :

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

بعنوان مثال شما می توانید به یک کاربر اجازه دسترسی به محتویات یک فایل را بدهید 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 تغییر دهید که بعضی از کاربران بتوانند تنظیمات آن را تغییر دهند در صورتیکه بقیه کاربران فقط بتوانند به آن چاپگر کار چاپی ارسال کنند .

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

مجوزهایی که به کاربران یا گروهها بر روی یک object انتصاب می دهید ، به نوع آن object بستگی دارد .

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

۷-۱ - ۱۰ - مجوزها در پارتیشن های NTFS

پارتیشن های با فایل سیستم NTFS دارای قابلیت هایی هستند که در پارتیشن های با فایل سیستم FAT یا FAT32 وجود ندارند. از جمله این قابلیت ها می توان به مواردی چون NTFS Compression ، NTFS Encryption ، Disk ، NTFS permission s ، Quota اشاره 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 و یا از طریق شبکه را تعیین نمود . به این معنی که مجوزها هم به صورت Local و هم از طریق شبکه ایجاد می کنند .

مجوزهای standard, special

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

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

برای نمایش مجوزها ابتدا روی یک فایل یا پوشه کلیک سمت راست کرده و گزینه properties و سپس در پنجره نمایش داده شده زبانه security را انتخاب کنید.

نکته : اگر سیستم عامل مورد استفاده ویندوز xp professional باشد به صورت پیش فرض این زبانه نمایش داده نمی شود . برای نمایش آن باید یک گزینه simple file sharing use را در control panel / folder option/ view tab بردارید .

در پنجره ای که ظاهر می شود روی کلید Advanced کلیک کنید و در پنجره بعدی یکی از گزینه ها را انتخاب کرده و سپس کلید Edit را انتخاب نمایید تا لیست مجوزهای special نشان داده شوند.

شکل ۱۴-۱۰ مجوزهای special و Advanced Tab

جدول زیر لیست مجوزهای NTFS روی فایل ها و پوشه ها را توضیح می دهد.

این مجوز اجازه می دهد که بتوانید فایل ها و پوشه ها در داخل یک پوشه ، مجوزها و مالک و Read خصلت 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 writer تغییر دهید و همچنین مالک و لیست مجوزها را ببینید .

اسامی فایل ها و پوشه 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 در بالا + مجوز Delete کردن فایل ها و پوشه ها Modify

Full control = Modify + Delete subfolders and files + change permissions + Take ownership

مجوزهای لیست شده در 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 نمایید ، درزبان 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 تغییر دهید . (تیک مجوزها به رنگ سبز نمایش داده می شوند.)

حال اگر در داخل آن درایو یک فایل یا پوشه ای ایجاد کنید ، تمامی مجوزها از ریشه به آن فایل یا پوشه به ارث خواهند رسید .

اگر مجوزهای موجود بر روی 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 قرار دارد (parent folder) به ارث خواهد گرفت.

۸-۱۰- مجوزهای مؤثر

اگر یک کاربر مجوزی روی یک منبع داشته و عضو گروهی باشد که آنها نیز دارای مجوزی روی آن منبع باشند ، مجوز مؤثر آن کاربر روی آن منبع به شرح زیر محاسبه خواهد شد .
در این حالت اجتماع مجوزهایی که به کاربر یا به گروهها اعطا شده ، مجوز مؤثر کاربر خواهد بود . فقط در حالتی که یک مجوز Deny شده باشد به مجوزهایی که در همان 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 می تواند از چاپگر استفاده کند.
- ۷- تحقیق کنید که چه روش دیگری برای نصب چاپگر در روی شبکه وجود دارد.

فصل یازدهم-نصب و راه اندازی Active Directory

هدف های رفتاری

- Domain و اجزای Active directory را تعریف کند.
- بتواند Active Directory نصب کند.
- نحوه عضویت کلاینت ها و انواع Logon ها را شرح دهد.

۱-۱۱ آشنایی با Domain و اجزاء Active Directory

همانطوری که در بخش های قبلی اشاره شده است ، مدل workgroup در شبکه 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 . در یک چنین مدلی اگر بخواهید یک policy برای کامپیوترها و یا کاربران تعیین کنید ، آن را به صورت جداگانه در یک 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 .

برای راه اندازی Domain برنامه ای به نام Active Directory را در یک سرور standard alone باید نصب کنید . بعد از نصب برنامه آن سرور به (DC) Domain controller تبدیل خواهد شد .

DC وظیفه authentication در Domain را به عهده دارد ، بدین معنی که زمانی که یک کاربر از روی یک کلاینتها به Domain می خواهد Logon کند ، اسم و گذر واژه کاربر به صورت کد شده به DC فرستاده می شود . DC که اطلاعات تمامی کاربران در Domain را دارا می باشد ، اطلاعات دریافتی را با اطلاعاتی که خود از کاربران دارد مقایسه می کند و در صورتی که صحت داشته باشد یک کارت شناسایی که اصطلاحاً آن را بانام Access Taken می شناسید به کاربر ارسال کرده و درستی اطلاعات آن کاربر را به کلاینت اطلاع می دهد . از این به بعد برای دسترسی کاربر به تمامی منابع موجود در Domain از کارت شناسایی مذکور استفاده می شود .

۱-۱۱-۱- نصب Active Directory

برای 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 .

در صورتیکه 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 و همان IP در قسمت Preferred DNS Server وارد شده باشد .

CD ویندوز سرور 2003 در درایو CD موجود بوده و یا پوشه I386 از همان CD در دیسک سخت دیسک کامپیوتر کپی شده باشد. البته لازم به توضیح است که برای نصب Active Directory نیازی 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 Administrator و یا کاربر دیگری که عضو گروه Administrators می باشد Logon کرده باشید.

حال در Start/Run فرمان 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 Next را انتخاب کنید.

پنجره Next را انتخاب کنید. حال پنجره شکل ۱۱-۳ ظاهر خواهد شد . در این پنجره از ما سؤال می شود که DC جدید: Domain controller for a new domain: یک DC در Domain جدید خواهد بود

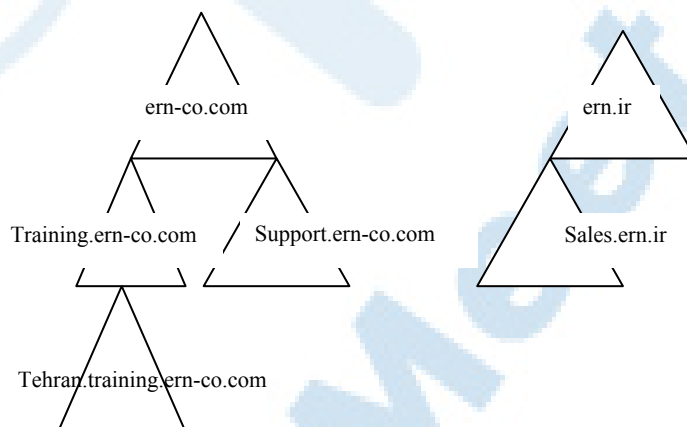
Additional domain controller for an existing domain: یک DC اضافه در Domain موجود خواهد بود در این پنجره ما گزینه اول را انتخاب کنید. چون هیچ Domain ی ایجاد نشده است و ما اولین DC برای یک Domain را می خواهیم راه اندازی کنید و سپس گزینه Next را انتخاب کنید. پنجره ای مطابق با شکل ۳-۴ ظاهر خواهد شد . در این پنجره نوع Domain که می خواهید ایجاد کنید سؤال شده است :

- Domain in a new forest : در یک جدید
- Child Domain in an existing domain tree : Child Domain از یک Domain موجود
- Domain tree in an existing forest : یک root domain جدید در یک forest موجود.

شکل ۲-۱۱

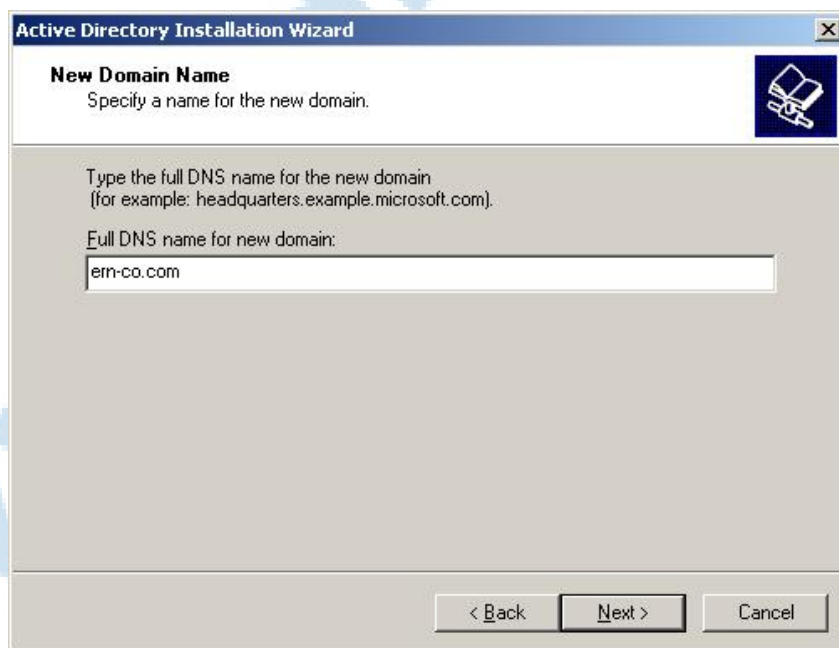
با توجه به اینکه مباحث مطرح شده در این قسمت خارج از بحث این کتاب می باشد ، به طور خلاصه به ساختاری Active directory به کمک شکل ۳-۱۱ اشاره کنید.

ساختار Active Directory از یک مجموعه به نام forest (جنگل) تشکیل می شود هر forest می تواند شامل یک یا تعدادی Domain Tree (درخت domain) بشود. هر Domain Tree از یک یا تعدادی Domain تشکیل می شود طوری که اولین Domain را بانام Root domain و سایر domain ها را بانام child domain می شناسید هر domain یک اسم اینترنتی یا DNS خواهد داشت و اسمی domain های موجود در یک Tree به هم وابسته خواهند بود. به عنوان مثال اگر اسم اولین domain در ern-co.com, Tree ern-co.com, می تواند اسمی training.ern-co.com, Tehran.training.ern-co.com, support.ern-co.com, رابرای domain های child انتخاب کنید.



شکل ۱۱-۳

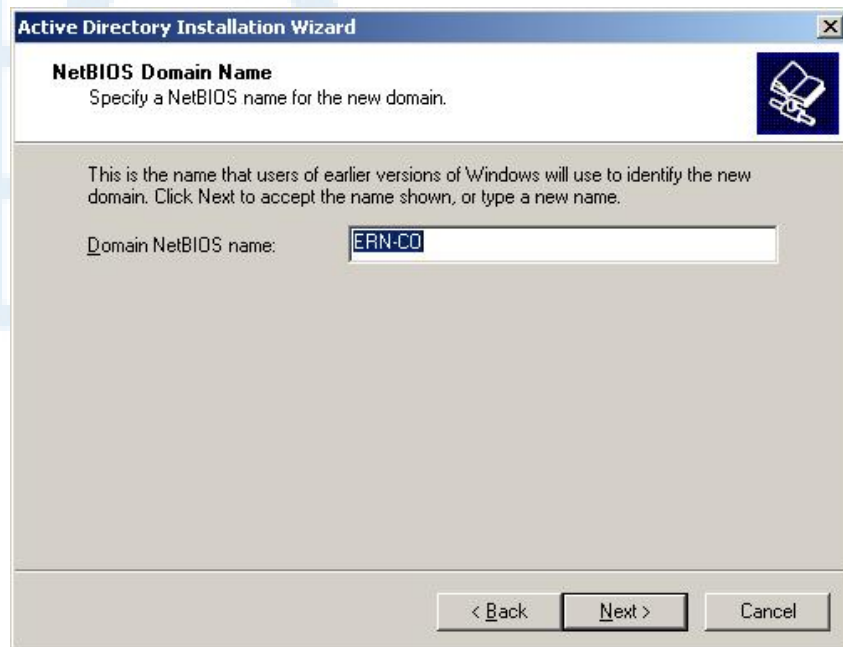
- حال در شکل ۱۱-۲ با توجه به اینکه یک forest جدید می خواهید ایجاد کنید، گزینه اول را انتخاب کرده و سپس گزینه Next را کلیک کنید.
- در پنجره باز شده شکل ۱۱-۴ اسم اینترنتی یا DNS های Domain از ما خواسته شده است.



شکل ۱۱-۳

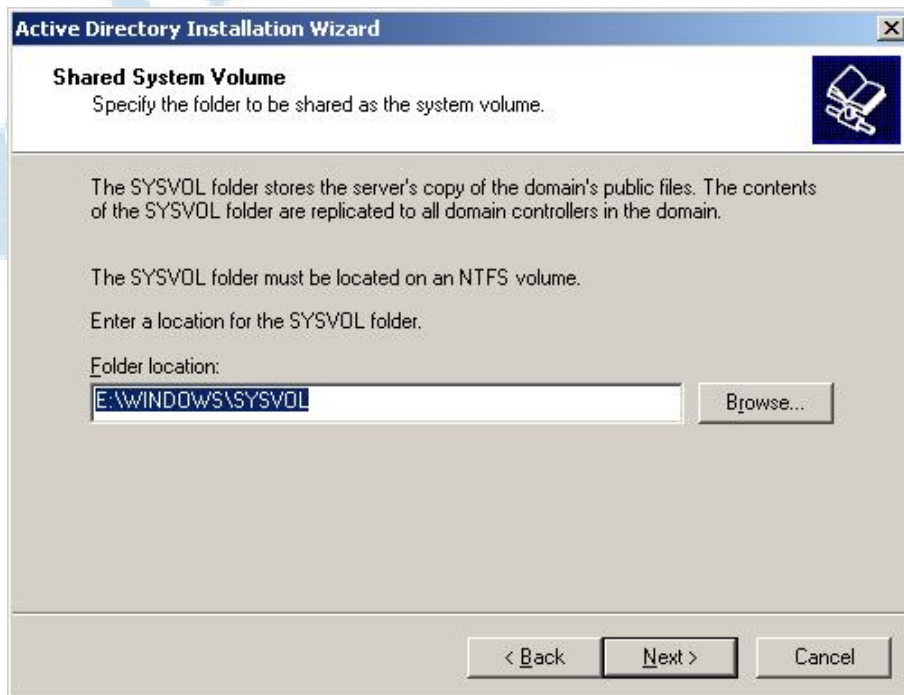
در این پنجره اسم ern-co.com را وارد کرده و گزینه Next را انتخاب کنید. در این مدت ویزارد سراغ DNS سرور می رود تا اطمینان حاصل کند که از قبل

Domain با نام ern-co.com ایجاد نشده است همچنین هر Domain باید یک اسم NetBios داشته باشد که در مثال بیان شده این اسم به صورت پیش فرض ERN-CO خواهد بود. عمل دیگری که در این 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

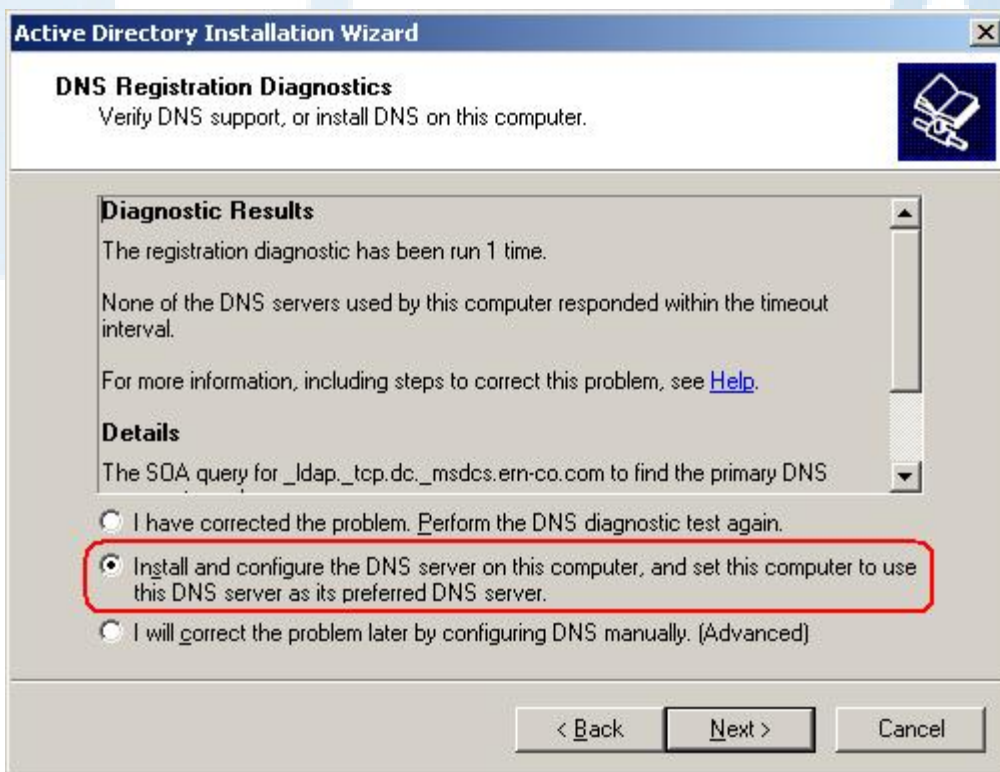
- سپس گزینه Next را انتخاب کنید
- پنجره شکل ۵-۱۱ ظاهر خواهد شد. در این پنجره آدرس پوشه ای که در آن فایل اطلاعات Active Directory و Log file های آن ذخیره می شوند، سؤال شده است به صورت پیش فرض یک پوشه به نام NTDS در همان پوشه ای که ویندوز نصب شده است، پیشنهاد می شود آدرس های پیش فرض را قبول کرده و گزینه Next را انتخاب کنید.
- پنجره شکل ۵-۱۱ به نمایش در خواهد آمد در این پنجره آدرس یک پوشه به نام sysvol از ما خواسته شده است. در این پوشه اطلاعاتی از Domain که یک کپی از آن به نام DC فرستاده می شود. نگهداری شده و این 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 زیر را اجرا کنید تا فایل سیستم آن به NTFS تبدیل شود
`convert d:/fs:ntfs`

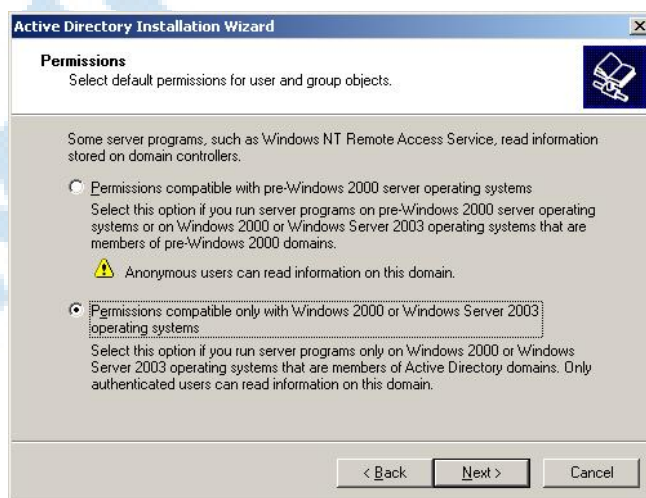
- در پنجره باز شده شکل ۱۱-۶ گزینه دوم را انتخاب کرده و گزینه Next



را انتخاب کنید.

شکل ۱۱-۶

- در پنجره شکل ۱۱-۷ گزینه دوم را انتخاب کرده و گزینه Next را کلیک کنید



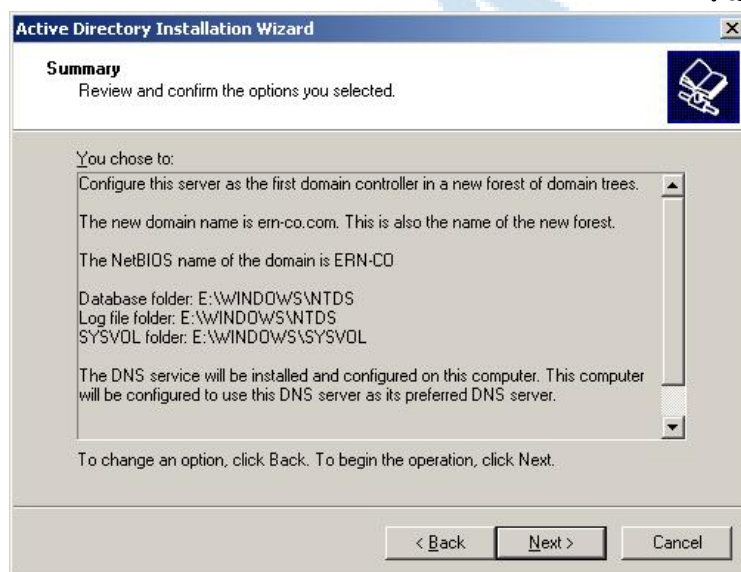
شکل ۱۱-۷

- 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 دخواه دوبار وارد کرده و سپس گزینه Next را انتخاب کنید.



شکل ۸-۱۱

- در پنجره شکل ۳-۱۰ خلاصه تنظیماتی را که در این 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 ظاهر شده و Active Directory را نصب می کند و مراحل نصب را برای ما گزارش می کند.



شکل ۱۱-۹

نکته: درحین نصب این سرویس اگر CD ویندوز 2003 را در درایو قرار نداده باشید، آن را از شما خواهد خواست که در این حالت باید آدرس پوشه I386 را به آن معرفی کنید تا فایل های لازم برای نصب از روی آن کپی شوند.

بعد از چند دقیقه عمل نصب به پایان رسیده و پنجره شکل ۱۱-۳ ظاهر می شود.



شکل ۱۱-۱۰

در این پنجره گزینه Finish را انتخاب کنید این عمل باعث می شود که پنجره شکل ۱۱-۳ ظاهر شود. در این پنجره گزینه Restart Now را انتخاب کنید تا کامپیوتر ریست شود.



شکل ۱۱-۱۲

نکته: بعد از 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 DNS که در چند صفحه قبل به آن اشاره گردیده است اطمینان حاصل کنید.

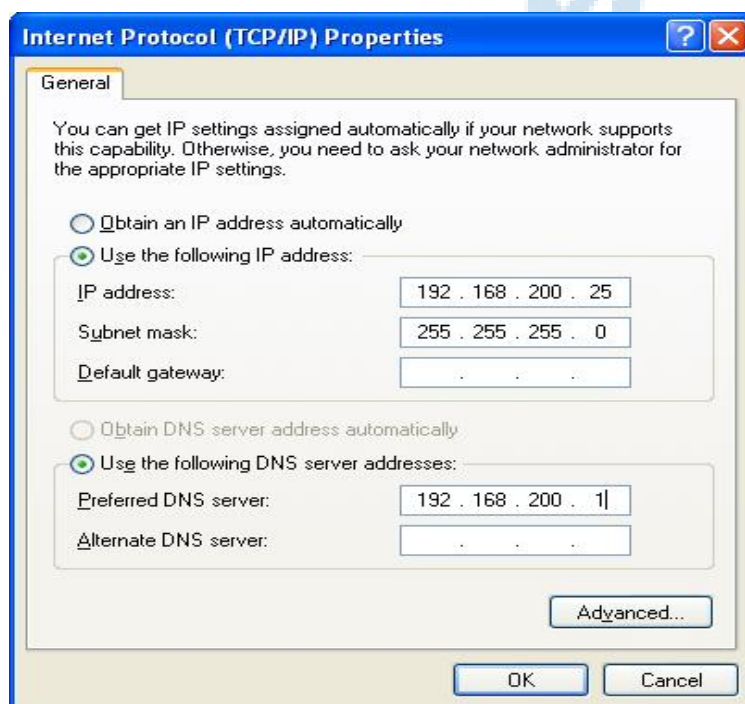
۱۱-۳ عضویت کلاینت ها در Domain

تا این مرحله یک Domain با یک DC راه اندازی شده است حال می خواهید کلاینتها را به عضویت Domain در بیاورید. تا کاربران بتوانند از روی آن ها به Domain، Logon کرده و به منابع آن دسترسی پیدا کنند.

۱۱-۳-۱ نحوه عضویت کلاینت ها

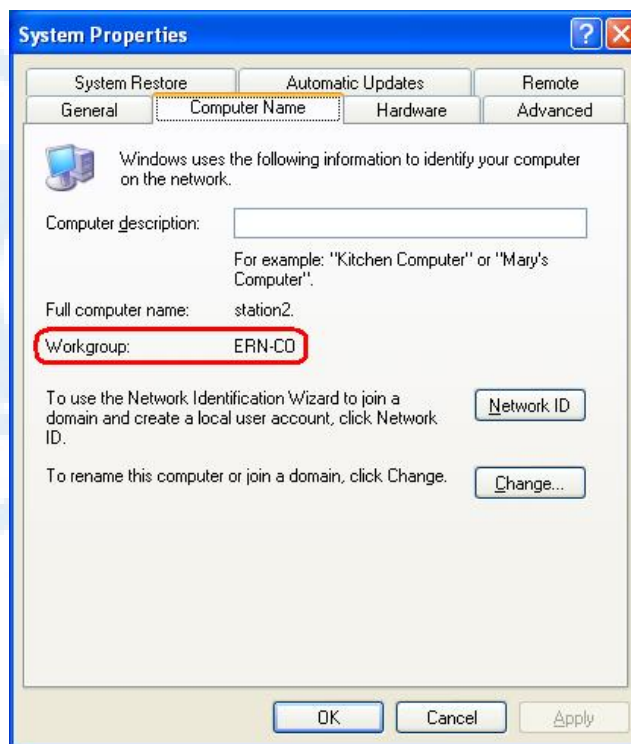
حال در یک کلاینت که سیستم عامل آن ویندوز XP می باشد با کاربر Administrator وارد شده و تنظیمات زیر را در آن انجام می دهید.

۱- control panel/Network connection روی properties, local area connection گرفته و در پنجره ای که ظاهر می شود گزینه Internet protocol (tcp/ip) را انتخاب نموده و سپس روی گزینه properties کلیک کنید. در پنجره ای که ظاهر می شود مطابق شکل ۱۶-۳ یک IP به صورت منحصر بفرد وارد کرده و در قسمت preferred DNS server ای DC را وارد کرده و روی گزینه OK کلیک کنید.



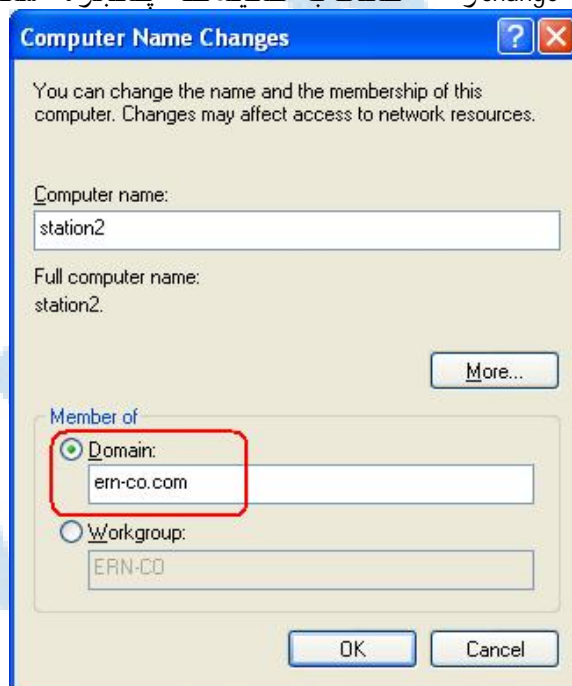
شکل ۱۱-۱۳

در control panel/system properties زبانه computer name را انتخاب کنید (شکل ۱۷-۳)



شکل ۱۱-۱۴

در این پنجره مشاهده می کنید که این کامپیوتر عضو یک workgroup به نام ERN-CO می باشد حال گزینه change را انتخاب کنید تا پنجره شکل ۱۱-۱۵ ظاهر شود .



شکل ۱۱-۱۵

در این پنجره گزینه Domain را انتخاب کرده و در مقابل آن اسم DNS ی Domain یعنی ern-co.com و یا اسم NetBIOS آن یعنی ERN-CO را وارد کرده و سپس روی گزینه OK کلیک کنید پنجره جدیدی مطابق شکل ۱۱-۱۶ ظاهر شده و اسم و گذر واژه کاربری را که اجازه عضو کردن کلاینتها در Domain را دارد از ما می خواهد.



شکل ۱۱-۱۶

در قسمت user name, Administrator و در قسمت password گذر واژه آن کاربر را وارد کنید بعد از چند ثانیه پنجره زیر ظاهر شده و اعلام خوش آمد گویی به ern-co.com را می‌دارد.



شکل ۱۱-۱۷

در پنجره های ظاهر شده روی OK کلیک کرده و سپس گزینه yes را انتخاب کنید تا کامپیوتر دو باره راه اندازی شود. حال بعد از راه انداز دو باره شده در پنجره logon to لیست می‌باشد که اگر آن را باز کنید دو گزینه ملاحظه خواهید کرد این دوگزینه اسم



Domain و اسم خود کامپیوتر می‌باشد.

شکل ۱۱-۱۸

۱۱-۳-۲ انواع log on

در این قسمت از انواع log on کردن به ویندوز به دو نوع اشاره کنید:
: Log on locally

اگر در لیست ظاهر شده در شکل ۳-۲۱ گزینه This computer را انتخاب کنید و بایک اسم و گذر واژه ی که در Domain ایجاد شده (مثلاً کاربر Administrator) log on کنید عمل authentication توسط همان کامپیوتر انجام خواهد شد. اما در این حالت کاربر فقط به منابع همان کامپیوتر دسترسی خواهد داشت.

: Log on to domain

اگر در لیست مذکور گزینه ERN-CO را انتخاب کنید همانطوری که قبلاً هم توضیح داده شده مشخصات کاربر به DC فرستاده می شود authentication توسط آن انجام خواهد شد در این حالت کاربر می تواند به تمامی منابع Domain بدون نیاز مجدد به وارد کردن اسم و گذر واژه پیدا کند.

خود آزمایی و تحقیق

- ۱- Domain Controller چیست؟ وظایف و ویژگی های 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 اسامی آن را بنویسید.
- ۵- آیا یک کامپیوتر می تواند به طور همزمان عضو چند DC باشد؟
- ۶- تحقیق کنید که چه روش دیگری برای نصب Active Directory وجود دارد؟

فصل دوازدهم مدیریت Account ها

هدف های رفتاری

- انواع Account ها و ابزارهای مدیریتی را شناسایی کند.
- بتواند کاربران را مدیریت کند.
- بتواند مدیریت Computer Account ها را انجام دهد.

۱۲-۱ آشنایی با انواع Account ها و ابزارهای مدیریتی

۱۲-۱-۱ انواع Account ها

در Active Directory، Account ها به سه دسته تقسیم می شوند:

- ۱- user Accounts به ازای هر کاربر در Domain یک user Accounts ایجاد کنید از این نوع Account ها برای log on کردن به Domain و دسترسی به منابع آن استفاده می شود
- ۲- computer Account: به ازای هرکلاینتو یا سرور و هر DC که عضو Domain هستند یک computer Account وجود دارد و از آن ها برای اعمال کردن policy ها authentication استفاده می شود
- ۳- Group Accounts: برای مدیریت راحت کاربران و اعطای مجوز به آنها و همچنین اعمال policy ها به آنها از این نوع Account ها استفاده می شود که در فصل بعد مورد بررسی قرار خواهند گرفت.

۱۲-۱-۲ - ابزارهای مدیریت Active Directory:

- بعد از نصب Active Directory سه ابزار برای مدیریت آن در Administrative Tools اضافه می شود:
- ۱- Active Directory users and computers: از این ابزار برای مدیریت انواع Account های اشاره شده در قسمت قبل استفاده می شود
 - ۲- Active Directory sites and services: از این ابزار برای مدیریت site های Active Directory استفاده می شود این ابزار خارج از بحث این کتاب می باشد.
 - Active Directory Domain and Trusts: از این ابزار برای مدیریت Domain ها و ایجاد رابطه های اعتماد (trusts) بین آنها استفاده می شود این ابزار خارج از موضوع این کتاب می باشد.
- ۱۰-۱ روی Start/Administrative tools گزینه Active Directory users and computer کلیک کنید پنجره شکل ۱۰-۱ ظاهر می شود.

شکل ۱۲-۱

گزینه erna-co.com را باز کنید چندین پوشه در داخل آن نمایش داده می شوند تمامی کاربرانی که به صورت پیش فرض در Domain ایجاد می شوند داخل پوشه users قرار دارند به ازای تمامی کامپیوترهایی که عضو Domain می شوند یک computer

Account در پوشه computers ایجاد می شود بخشی از گروهایی که هنگام ایجاد Domain بوجود می آیند در پوشه Built-in قرار دارند.

۱۲-۲ مدیریت کاربران

۱۲-۲-۱ ایجاد کردن کاربران جدید

در Active Directory users and computer روی پوشه users کلیک راست کرده و گزینه New و سپس user را انتخاب کنید . پنجره شکل ۱۲-۲ ظاهر خواهد شد.

شکل ۱۲-۲

در قسمت Fairst name: نام کاربر را وارد کنید (مثلاً Ali)
Last name: نام خانوادگی کاربر را وارد کنید. (مثلاً Rahmati)
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 Domain، logon، خواهد کرد وارد کنید (مثلاً ARahmati)
Pre-windows 2000 logon name: همان اسمی را که در قسمت Logon name وارد کرده اید نمایش خواهد داد.
گزینه Next را انتخاب کنید تا پنجره شکل ۱۲-۳ نمایش داده شود.

شکل ۱۲-۳

توجه کنید که اسمی که در قسمت Logon name وارد می کنید در Domain باید منحصر بفرد باشد.
در این پنجره گذر واژه کاربر جدید از مسائل می شود که دوبار باید آن را وارد کنید.
نکته: یک policy به صورت پیش فرض در Domain های 2003 وجود دارد که باعث می شود گذر واژه هایی را که برای کاربران انتخاب می کنید complex بوده و حداقل 7 کاراکتر طول داشته باشند بدین معنی که از گذر واژه های تکراری و یا گذر واژه هایی که فقط از اعداد و یا فقط از حروف تشکیل شده اند نمی توان استفاده نمود . بعنوان مثال شما می توانید از گذر واژه Password استفاده نائید
گزینه های بعدی گزینه هایی هستند که قبلاً در ایجاد کردن کاربران جدید در ویندوز xp آنها را فرا گرفته اید حال گزینه Next را انتخاب کنید تا پنجره شکل ۱۰-۴ نمایش داده شود در این پنجره خلاصه مشخصات کاربر نمایش داده شده است .

شکل ۱۲-۴

حال روی گزینه finish کلیک کنید کاربر جدید ایجاد می شود توجه کنید که در پوشه users اسم کامل کاربر یعنی full name نمایش داده می شود.

۱۲-۲-۲-مشاهده مشخصات کاربران و تغییر دادن آنها

اگر Active Directory users and computer روی یک کاربر کلیک راست کرده و گزینه properties را انتخاب نمائید پنجره جدید مطابق شکل ۱۲-۵ ظاهر شده که در آن مشخصات کامل آن کاربر را دیده و می توانید آنها را تغییر دهید.

شکل ۱۲-۵

به عنوان مثال در این قسمت به چند مورد از مشخصات کاربران اشاره کنید.

زبان Account گزینه logon hours...

اگر روی این گزینه کلیک کنید پنجره شکل ۱۲-۶ نمایش داده خواهد شد در این پنجره به شما نشان میدهد که این کاربر در چه ساعاتی از شبانه روز در یک هفته اجازه logon کردن به Domain دارد شما این محدودیت را به ازای هر ساعت در شبانه روز و هر روز در هفته می توانید تعیین کنید

شکل ۱۲-۶

خانه هایی که به رنگ آبی پر شده اند بیانگر این می باشد که در آن ساعت و در آن روز کاربر اجازه logon کردن دارد
شما به راحتی می توانید با کلیک کردن روی یک خانه آن را به رنگ آبی و یا به رنگ سفید در آورید.

زبان Account گزینه logon to...

با کلیک کردن روی این گزینه پنجره شکل ۱۲-۷ نمایش داده می شود در این پنجره تنظیمات پیش فرض طوری انجام شده که کاربر مربوط با کلیک کردن از روی هر کامپیوتری به Domain، logon کند شما با انتخاب گزینه The following

computer می توانید برای کاربر محدودیت ایجاد کنید تا فقط از روی کامپیوترهایی که مدنظر شما می باشد بتوانند logon کنند برای انجام این کار در قسمت computer name اسامی کامپیوترها را یک به یک نوشته و بازدن گزینه Add آنها را به لیست اضافه کنید

شکل ۷-۱۲

زبان Account گزینه Account expires :

به وسیله ی این گروه شما می توانید محدودیت زمانی برای فعال بودن کاربر تعریف نمائید تنظیم پیش فرض این گزینه روی never می 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

Member of زبان

در این زبان به شما نشان می دهد که کاربر عضو چه گروهایی می باشد شما با انتخاب گزینه Add می توانید کاربر را به عضویت گروه های دیگری نیز در آورید.

۱۲-۲-۳ کاربر organizational unit :

در هر سازمان برای مدیریت ساده تر و ساختار یافته از یک سری واحدهای سازمانی استفاده می شود بعنوان مثال استفاده از واحدهای مختلف نظیر کارگزینی ، امور اداری ، حسابداری ، آموزش ، روابط عمومی ، IT..... در بسیاری از شرکت ها و سازمان ها معمول و مرسوم می باشد. در هر واحد سازمانی تعدادی کارمند و مقداری منابع مثل کامپیوتر ، چاپگر و ... یک مدیر برای آن واحد و غیره وجود دارد . طوری که مدیریت آن واحد سازمان به مدیر در یک شبکه بزرگ نیز برای مدیریت راحت تر شبکه ، می توانید در یک Domain ، واحدهای مختلف سازمانی ایجاد نمائید که به آنها اصطلاحاً organizational unit می گویند و به اختصار با نام OU به آنها اشاره کنید. هر OU می تواند تعداد زیادی کاربر ، کامپیوتر ، پرینتر و حتماً مدیر داشته باشد

حتماً می توانید policy های خاص برای آنها در نظر بگیرید و در واقع یک Domain را به تعدادی OU تقسیم کرده و منابع و کاربران را نیز بین آنها تقسیم نموده و حتی مدیریت آنها را نیز به کاربران خاص واگذار کنید برای ایجاد یک OU جدید این عملیات را انجام می دهید :

ابتدا Active Directory users and computer را اجرا کنید سپس روی ernal-co.com کلیک راست کرده و گزینه New سپس organizational unit را انتخاب کنید (مطابق شکل ۹-۱۲)

شکل ۹-۱۲

در پنجره ای که ظاهر میشود در قسمت Name نام OU جدید را وارد کنید و سپس گزینه ok را کلیک کنید مشاهده خواهید کرد که یک OU جدید ایجاد شده است حال در این OU می توانید کاربران جدید ایجاد نمائید و یا کاربران و کامپیوترهای موجود را به داخل آن انتقال دهید برای ایجاد کاربران جدید در داخل OU 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

۴-۲-۱۲ تکثیر کاربران

در قسمت قبل در ارتباط 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 از هم داشته باشند بعنوان مثال کاربران یک واحد در روزها و ساعات خاصی از هفته بتوانند logon کنند یا تاریخ انقضا آنها آخر سال باشد یا عضو گروهی خاص باشند از روی کامپیوترهای خاص بتوانند logon کنند و غیره... به طوریکه این مشخصات متفاوت از مشخصات واحدهای دیگر باشد در این حالت هر زمان که شما یک کاربر جدید برای این واحد ایجاد می کنید تمامی این تنظیمات را از نو برای آن کاربر باید انجام دهید و باید دقت کنید که اشتباهی صورت نگیرد حال اگر مشخصات کاربران واحدهای مختلف متفاوت باشند کاربری شما سخت تر هم خواهد شد راه حل بهتری که داریم این است که یک کاربر نمونه برای هر واحد ایجاد کنید برای هر کدام از آنها مشخصات را بر اساس نیاز آن واحد تعیین کنید و سپس آن کاربر را Disable می کنید حال برای کاربر جدیدی که میخواهید در آن واحد ایجاد کنید کافی است که یک کپی از کاربر نمونه آن واحد ایجاد کنید در این صورت مشخصات آن کاربر نمونه برای کاربر جدید نیز کپی خواهد شد مراحل زیر شیوه انجام این کار را بیان می کند

- ۱- یک OU به نام sales ایجاد نمائید
- 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 دخواه تعیین کنید بعنوان مثال آن کاربر روزهای جمعه اجازه logon نداشته باشد تاریخ اعتبار تا سه ماه دیگر باشد به عضویت یکی دو گروه جدید درآید فقط از روی کامپیوترهای xp1, xp2 بتواند logon کند و گزینه password never expires در زبانه Account انتخاب شود.
- ۴- حال روی کاربر مربوطه کلیک راست کرده و گزینه copy را انتخاب نمائید پنجره شکل ۱۰-۱۲ ظاهر خواهد شد در این ویزارد مشخصات کاربر جدید را وارد نمائید 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 وارد کرده بودید برای کاربر جدید نیز اعمال شده اند.

۱۲-۳ مدیریت computer Account ها

۱۲-۳-۱ کاربرد computer Account

computer Account ها نیز مثل یک کاربریکی از object های Active Directory

می باشد .
این Account ها 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 NT دارند Computer Account در Active Directory ایجاد می شود از این object ها برای authentication و اعمال کردن policy در Domain استفاده می شود که از آن جمله به مواردی چون اعمال بازبینی (auditing) نصب برنامه ها به صورت اتوماتیک روی کامپیوترها می توان نام برد بدین معنی که کاربران اجازه logon کردن از روی کامپیوترهایی را دارند که برای آن کامپیوتر در Active Directory، یک computer Account وجود داشته باشد در صورت غیر فعال شدن یک computer Account هیچ کاربری اجازه logon از روی آن را نخواهد داشت البته بحث اعمال کردن policy و نصب اتوماتیک برنامه ها خارج از بحث کلاس می باشد.

۱۲-۳-۲ نحوه ایجاد computer Account

هر کامپیوتری که عضو Domain میشود بصورت اتوماتیک برای آن کامپیوتر Active Directory یک computer Account در پوشه computer در داخل Domain ایجاد می شود برای DC ها این object ها در یک ou به نام Domain controllers ایجاد می شوند.

خود آزمایی و تحقیق

۱- انواع Account را نام ببرید.

۲- وظیفه ی 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 الی ۱۴ 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 های کاربران را شناسایی کند.
به روش های AGP و ADLP به کاربران و گروه ها مجوز دهد.
گروه های Built-in را شناسایی کند.

۱۳-۱ آشنایی با انواع گروه ها

در Dpmain های ۲۰۰۳ دو دسته بندی برای گروه ها وجود دارد :

- Group Types

- Group scopes

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 Security گروه هایی هستند که از آنها بیشتر برای مجوز دادن استفاده می شود . به عنوان مثال اگر بخواهید یک پوشه را برای یک گروه share کنید نوع گروه باید Security باشد .

گروه های از نوع 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 در این کتاب مورد بحث می باشند همه از نوع Security می باشند . بنابراین در هر قسمتی که در آن از نوع گروه نام می برید ، منظورمان scopes مربوط به آن گروه می باشد .

Group scopes بیانگر محدوده عمل کرد یک گروه و انواع object هایی است که می توانند به عضویت آن در آیند . همانطوری که اشاره شد در این متن از واژه " نوع گروه " به جای Group scopes استفاده خواهید کرد .

۱۳-۲ Global groups

گروه های Global گروه هایی هستند که به منظور دسته بندی منطقی کاربران مورد استفاده قرار می گیرند این دسته بندی معمولاً براساس نوع کار یا محل جغرافیایی 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 . برای ایجاد یک گروه از نوع global بر روی Domain یا OU^۱ ی مورد نظر کلیک سمت راست نموده و در منویی که ظاهر می شود گزینه New و سپس group را انتخاب کنید . پنجره شکل ۳-۵ نمایش داده خواهد شد .

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 کنید و 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 Gsale استفاده شود.

Domain Local Groups ۱۳-۲-۱

از این گروه ها معمولا برای اعطای مجوز استفاده می شود. برای ایجاد این نوع گروه روی Domain یا OU مربوط کلیک راست کرده و از منوی ظاهر شده گزینه New و سپس گزینه Organization را انتخاب کنید. پنجره شکل ۴-۵ ظاهر می شود.

شکل ۲-۱۳

در این پنجره گزینه های Security و Domain Local را مطابق شکل انتخاب نموده و همچنین یک اسم برای گروه انتخاب کنید و سپس روی کلید ok کلیک کنید.

Universal Groups ۱۳-۲-۲

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 برای اعطای مجوز به کاربران به کمک گروه ها می توان استفاده نمود در این جا به چند روش اشاره کنید.

AGP روش ۱۳-۳-۱

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 ۳-۱۳

از این روش در شبکه هایی که تعداد object ها زیاد نیست می توان استفاده کرد.

۱۳-۳-۲ روش A D L 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 مجوز (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 ۳-۱۴

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 های Built-in گروه هایی هستند که زمان نصب Active Directory به صورت اتوماتیک ایجاد می 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:

1. Domain users: این گروه شامل تمامی کاربران Domain می شود. هر کاربری که در Domain ایجاد می شود، به صورت اتوماتیک به عضویت این گروه در می آید.
2. Domain Admins: اعضای این گروه می توانند Domain را مدیریت کنند و به عنوان مدیر Domain شناخته می شوند. فقط Administrator همان Domain به صورت پیش فرض عضو این گروه می باشد.
3. 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 2000 Native یا به 2003 Server تغییر دهید، این گروه به صورت اتوماتیک به نوع Universal تبدیل خواهد شد.

شکل ۶-۱۳

۱۳-۴-۲ گروه های Built-in Domain Local

شکل ۷-۱۳

این گروه هادر پوشه Built-in در ابزار Active Directory Users & Compute قرار دارند

عبارتند از :

Administrators : اعضای این گروه می توانند DC ها را مدیریت کنند و تمامی مجوزها روی این کامپیوترها خواهند داشت .
Server operators : اعضای این گروه می توانند در انجام بعضی از کارهای مدیریتی به مدیر شبکه کمک کنند بعنوان مثال می توانند عملیات 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 Account ها (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 توانند عملیات 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 Built-in system گروه های

این گروه ها ، گروه هایی هستند که لیست اعضای آن ها را نمی توان دید و یا تغییر داد . 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 دارای account 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 کنید در لیستی که نمایش داده می شود، می توانید لیست گروه های سیستمی را مشاهده کنید.

۵-۱۳ پیاده سازی روش های مختلف اعطای مجوز به کاربران

۱-۵-۱۳ 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 ۸-۱۳ از این گروه Properties گرفته و در زبانه Members لیست اعضای این گروه را مشاهده می کنید.

شکل ۸-۱۳

حال اگر کلید Add کلیک کنید پنجره شکل ۹-۱۳ نمایش داده خواهد شد . در این پنجره می توانید اسمی کاربران را تایپ کرده و به لیست اضافه نمائید و یابرای 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 ۹-۱۳

حال کاربران مورد نظر را به کمک کلیدهای Ctrl و یا Shift انتخاب کرده و به لیست اضافه نمائید.

مشاهده خواهید کرد که این کاربران در زبانه Members لیست 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 ظاهر شود.

شکل ۱۰-۱۳

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.

۲-۵-۱۳ پیاده سازی روش A DL P

این روش مشابه روش قبلی می باشد با این تفاوت که گروه را بانام 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 از نوع Global را ایجاد کنید و کاربران را براساس آن دسته بندی به عضویت گروه های مختلف در آورید . سپس یک گروه از نوع 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 ۱۱-۱۳

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 ۱۲-۱۳

خود آزمایی و تحقیق

- ۱- تفاوت Scaring Group و Distribution Group در چیست؟
- ۲- تفاوت روش AGP و ADLP را بنویسید.
- ۳- چطور می توان در يك سطح وزارتخانه براي کاربران مجوزهاي لازم را صادر کرد؟
- 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 - DNS و روش های تبدیل اسم به IP

هدف های رفتاری

کاربردهای DNS را بیان کند.

اسامی اینترنتی و Host Name را شناسایی کند.

اجزاء DNS را توضیح دهد.

مراحل تبدیل اسم به IP را در اینترنت شرح دهد.

یک سرویس DNS نصب و راه اندازی کند.

سرویس DNS را برای انجام عمل Name Resolution تست کند.

۱-۱۴ کاربردهای DNS

DNS یکی از سرویس های بسیار مهم در شبکه می باشد . از این سرویس در اینترنت بیشتر به منظور تبدیل اسم به IP استفاده می شود . در Domain های ۲۰۰۳ نیز از این سرویس برای 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 ۲۰۰۰ و ۲۰۰۰۳ می توان یاد کرد .

۲-۱۴ آشنایی با اسامی اینترنتی

۱-۲-۱۴ 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 همدیگر جدا شده است . به اسامی اینترنتی به اصطلاح FQDN (Fully Qualified Domain Name) گفته می شود . یک FQDN از دو قسمت تشکیل می شود . همانطوری که در شکل ۱-۱۴ مشاهده می کنید به قسمت سمت چپ Host Name و به قسمت سمت راست Domain Name یا DNS Suffix اطلاق می شود

شکل ۱-۱۴ www.ern.co.com

Host name Domain name

در بسیاری از حالت ها به جای FQDN از واژه Host name استفاده می شود .

۱-۲-۱۴ ساختار اسامی اینترنتی

به منظور تبدیل راحت اسم به IP ، اسامی اینترنتی از چند قسمت تشکیل می شوند و برای نام گذاری کامپیوترها از یک ساختار سلسله مراتبی استفاده می شود . این ساختار سلسله مراتبی که یک ساختار درختی می باشد . شکل ۲-۱۴ نمایی از این ساختار درختی را نشان می دهد .

شکل ۲-۱۴

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 Domain و یا محل جغرافیایی آن Domain می باشد . به عنوان مثال .com. بیانگر فعالیت های تجاری ، 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 و اشخاص 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 (شکل ۲-۱۴) یک subdomain به نام Training ایجاد شده است . ایجاد و نگهداری این subdomain به عهده شرکت مایکروسافت می باشد . اسامی host ها یا subdomain ها از پائین ساختار درختی شروع شده و به ریشه ختم می گردد .

به عنوان مثال در شکل ۲-۱۴ یک host با نام www وجود دارد که FQDN آن www.ern.co.com می باشد . یا یک host دیگری به نام web server1 وجود دارد که FQDN آن webserver1.Training.Microsoft.com می باشد . شکل ۳-۱۴ قسمت مختلف این اسم را تشریح می کند .

شکل ۳-۱۴

۳-۱۴ اجزاء DNS

۱-۳-۱۴ Name server

به DNS سرور ، Name server نیز اطلاق می شود و یک سرور ۲۰۰۳ است که سرویس DNS روی آن نصب گردیده است .

Zone ۱۴-۲-۲

یک DNS سرور اطلاعات مربوط به Domain های مختلف را می تواند نگهداری کرده و به کاربران در ارتباط با آنها سرویس دهد. برای نگهداری اطلاعات Domain در 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 تبدیل IP به اسم از آنها استفاده کنید.

Resource Records ۱۴-۳-۳

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 host بیشترین استفاده را در DNS دارا می باشد ولی از انواع رکوردها در یک Zone می توان استفاده نمود که تعدادی از این نوع رکوردها عبارتند از:

- Host Record: از این رکورد به منظور تبدیل اسم به IP استفاده می شود.
- Point Record: از این 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: از این رکورد برای معرفی (DNS) Name server
- SOA Record: از این رکورد برای معرفی اطلاعاتی در ارتباط با یک Zone استفاده می شود.
- Alias Record: از این رکورد برای 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 می خواهیم مراحل تبدیل اسم به IP را توضیح دهیم.

فرض کنید که یک کاربری در Internet Explorer آدرس www.microsoft.com را وارد می کند تا به سایت وب مایکروسافت متصل شود. همانطوری که می دانید برای اتصال به یک سرور باید IP آن سرور را داشته باشید. می خواهید مراحل 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 سرور از این نوع سرورها در اینترنت به کاربران اینترنتی سرویس دهی می کنند .

این تعداد ثابت بوده و IP آن ها در DNS سرور جدیدی که راه اندازی کنید به صورت پیش فرض وجود دارد .

Top Level Name servers: این سرورها ساختار Domain های Secondare Level را نگهداری می کند .

به عنوان مثال Com Name server ساختار Com Domain را نگهداری می کند .

Secondarey Level Name server: این سرورها رکوردهای مربوط به Domain های خود را نگهداری می کنند . راه اندازی و نگهداری از هر کدام از این سرورها به شرکت ها و یا افرادی که اسم مربوط را ثبت 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 Name server (DNS سرور) ارسال می کند . این سرور موظف است که IP مربوط به اسم درخواست شده را پیدا کرده و آن را به کلاینت ارسال کند ، 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 Zone با این سرور نیست ، هیچ رکوردی پیدا نمی کند و به همین دلیل آن اسم را به Root Name Server ارسال می کند و از آن سرور IP آن اسم را تقاضا می کند .

مرحله ۳: **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 هر اسمی 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 Com Name server ها پس گیری نماید .

مرحله ۴: تا این مرحله Local Name server توانسته است IP Com Name server را پیدا کند . بنابراین یک درخواست به آن سرور ارسال کرده و IP را از آن درخواست می کند .

مرحله ۵: این سرور نیز IP اسم درخواست شده را نمی داند ، اما با بررسی آن اسم ، متوجه کلمه Microsoft قبل از کلمه com می شود . سپس لیستی از IP 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 IP DNS سرور مایکروسافت را پیدا کند . 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 سرور Local ارسال 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 و اطلاعات درخواست شده کلاینت را برای او ارسال می کند.

۵-۱۴- نصب و راه اندازی سرویس DNS

۱-۵-۱۴ 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 Domain نیست و روی سرورهای Stand alone نیز می توانید آن را نصب کنید.

برای 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 در داخل درایو قرار داده و پوشه I386 را به آن معرفی کنید.

فایل های لازم کپی شده و ویزارد به پایان خواهد رسید.

شکل ۵-۱۴

شکل ۶-۱۴

به این ترتیب سروری که دارید به یک DNS سرور تبدیل شده است و می تواند به کلاینت ها برای اتصال به اینترنت سرویس دهی کند. این سرور به صورت پیش فرض تعداد ۱۳ Root Name server موجود در اینترنت را می شناسد

به منظور دیدن IP این سرورها از Start/Administrative Tools گزینه DNS را انتخاب کنید.

شکل ۷-۱۴

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

زبان Root hints را انتخاب نمائید. مشاهده می کنید که اسمی و IP های Root Name server های اینترنتی نمایش داده می شوند.

۲-۵-۱۴ ایجاد کردن Zone

حال فرض کنید که یک Domain با نام ern-co.net دارید و یک 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 شکل ۱۱-۱۴ 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 ۱۴-۱۲

پنجره شکل ۱۴-۱۳ ظاهر خواهد شد . 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 ۱۴-۱۳

اسم پیش فرض را قبول 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 کردید کلیک 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 ای مطابق شکل ۱۴-۱۵ نمایش داده می شود .

شکل ۱۴-۱۵

در این پنجره در قسمت Name، WWW و در قسمت IP، IP Address یکی از سرورهای شبکه یا همین سرور را وارد کنید . 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 ۱۶-۱۶

۴-۵-۱۶ 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 IP ای DNS آن به IP ی DNS سرور جاری (یعنی training) تنظیم شده باشد، فرمان www.ern-co.next ping را اجرا کنید . مطابق شکل ۱۶-۱۷ مشاهده خواهید کرد که IP آن host توسط DNS سرور پیدا شده و به کامپیوتر شما برگردانده می شود .

شکل ۱۶-۱۷

روش دوم : استفاده از فرمان nslookup

در این روش از فرمان nslookup برای تست کردن DNS 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 . فرمان nslookup 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 . در صورتی که DNS جواب را پیدا کند ، آن را مشاهده خواهید کرد . شکل ۱۶-۱۸ شیوه استفاده از این فرمان را نشان می دهد .

شکل ۱۶-۱۸

خود آزمایی و تحقیق



فصل پانزدهم - DHCP Server مقدماتی

هدف های رفتاری

- فوائد DHCP Server را بیان کند
- اجزای DHCP توضیح دهد
- حالت های مختلف قرارگیری DHCP Server در شبکه را شرح دهد.
- نصب DHCP Server را انجام دهد
- پیکربندی DHCP Server شرح دهد
- پیکربندی DHCP Server را انجام دهد.
- Backup / Restore از اطلاعات DHCP Server نسخه پشتیبان گرفته و جایگزین نماید
- عیب‌یابی DHCP را انجام دهد.

۱-۱۵. کاربرد DHCP Server

برای آنکه بتوان از یک TCP/IP Host در شبکه استفاده کرد باید حداقل موارد زیر را 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 را برای یک Host تعریف کرد مانند WINS Server و Node Type می توان گفت پیکربندی یک Host در پروتکل TCP/IP چنانچه شبکه به اندازه کافی 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.¹ DHCP 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 را نیز ایجاد می کند از جمله اینکه Client ها در هنگام فرایند راه اندازی باید با سرور DHCP ارتباط گرفته و پیکربندی مناسب را از آن دریافت کنند که این مسئله از طرفی باعث افزایش ترافیک شبکه شده و از طرف دیگر در صورت نبودن سرور DHCP یا تاخیر در پاسخ از جانب آن سبب می شود تا ایستگاه ها نتوانند پیکربندی لازم خود را برای ارتباط در شبکه دریافت کنند .

۲-۱۵. اجزای DHCP

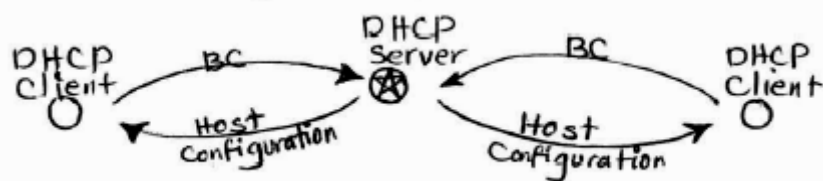
DHCP از دو قسمت تشکیل شده :

-DHCP Client
- DHCP Server

منظور از DHCP Client ، سرویسی است که در طی فرایند راه اندازی ، با سرور DHCP ارتباط گرفته و پیکربندی لازم را از آن دریافت 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

در سیستم 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 Broadcast (به اختصار BC) سرور را پیدا کرده و بعد از طی مراحل 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 آن صورت بسته به رفتار سیستم عامل ایستگاه ممکن است یکی از حالات زیر اتفاق افتد :

الف) Client پیکربندی نمی شود. در مایکروسافت سیستم عامل های 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 عامل های win98، Me، xp2000 و 2003 چنین رفتاری دارند که با مراجعه به Command Prompt و وارد کردن دستور ipconfig 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 اصطلاحاً^۱ APIPA خوانده می شود .

متأسفانه APIPA مکانیزم مناسبی برای پیکربندی در شبکه ها نیست چرا که :

- غیر از IP&Mask پارامتر دیگری را تنظیم نمی کند (از قبیل 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 قابلیت است که اگر سرور DHCP را پیدا نکنند با آدرس و سایر پارامترهای دیگری که از قبل تعریف شده است خود را تنظیم می کنند. این حالت اصطلاحاً "Alternate configuration" خوانده می شود .

نکته: در فرایند APIPA پس از آنکه Client آدرس را به صورت تصادفی برای خود انتخاب کرد آن را تا مدتی کوتاه (حدود ۵ دقیقه) نگه داشته و سپس مجدداً 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 در غیر این صورت یعنی نگرفتن پاسخ از سرور DHCP همان آدرس تصادفی قبلی را استفاده می کند و

^۱ Automatic Private IP Addressing

این فرایند مرتب تکرار می شود یعنی حدوداً 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 .

۱۵-۳- 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 را در شبکه (ها) بررسی می کنیم .

حالت اول ، هر شبکه یک سرور DHCP مستقل دارد :

شکل ۱۵-۲

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 دچار اختلال نمی شود .

عیب ای سناریو در آن است که شاید تهیه سرور مستقل برای هر شبکه مقرون به صرفه نباشد و در Network1 ۱۰۰ عدد به نظر نمی رسد که انتخاب یک سرور DHCP جداگانه برای ۱۰ ایستگاه بجوایم سرور DHCP قابل توجیه باشد .

حالت دوم ، سرور DHCP مشترک بین چندین شبکه :

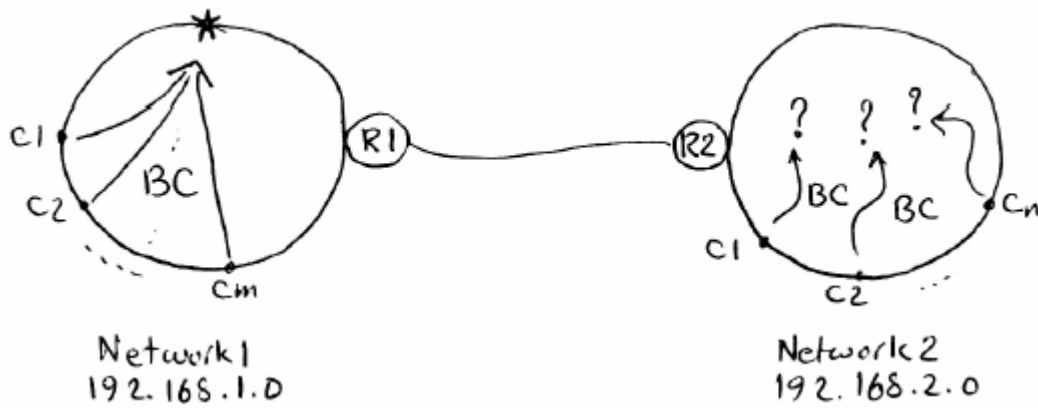
شکل ۱۵-۳

همانطور که از شکل ۱۵-۳ پیدا است مشکلی برای ایستگاه های Net1 وجود ندارد زیرا BC آنها مستقیم و بدون واسطه به سرور DHCP می رسد اما وضعیت BC های مربوط به Net2 خرابی از DHCP Server نیست و از طرفی روترها نیز به طور عمده جلوی عبور ترافیک BC را می بندند .

این مشکل به وسیله ی سرویس DRA¹ حل می شود بدین ترتیب DRA ، BC های مربوط به ایستگاه ها را دریافت کرده و آن را به صورت Unicast به سمت سرور DHCP هدایت می کند . DRA باید 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 در صورت نیاز باید آن را پیکربندی و فعال کرد :

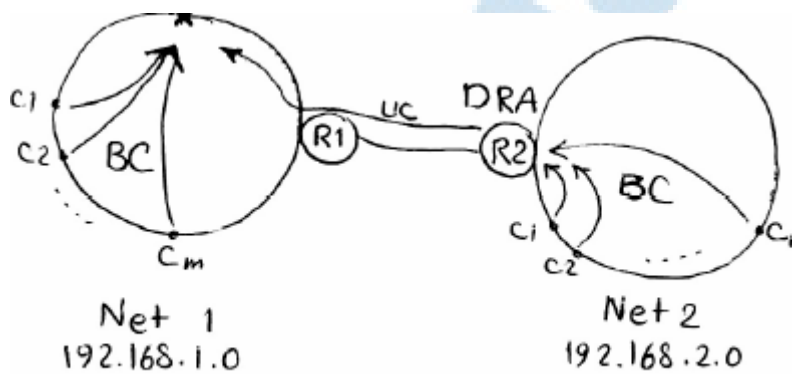
¹ DHCP Relay Agent



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 سرور DHCP 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 مستقیماً BC های ایستگاه ها را از هر ۳ شبکه دریافت کرده و پاسخ مناسب را به آنها می دهد :

شکل ۶-۱۵-

۴-۱۵ . نصب DHCP Server

- قبل از اقدام به نصب سرور DHCP باید مقدمات زیر را فراهم کرد .
- (۱) سخت افزار مناسب برای سرور خصوصا کارت شبکه ، CPU، RAM.
- (۲) غیر فعال بودن نرم افزارها و سرویسهای 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 را وجود دارد اما روی Professional اعم از 2000 یا xp نمی توان DHCP Server نصب کرد . برای نصب مراحل زیر را طی 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 Wizard برای 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 . وارد کردن Description الزامی نبوده و اختیاری است .
- محدوده آدرسی که باید به ترتیب به ایستگاه ها داده شود . مثلا از 192.168.1.200 الی 192.168.1.21
- آدرس یا محدوده آدرس هایی که از میان بند قبل نباید به ایستگاه داده شود . مثلا فرض کنید از میان 192.168.1.21 الی 1.200 آدرس های زیر از قبل 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

اصطلاحاً 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 مثلاً 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 چنانچه در یک شبکه میزان جابجایی کامپیوترها نسبتاً 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 (مثلاً می 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 نیز عبارتند 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 عنوان Default Gateway دیده می شود .
- آدرس DNS Server که باید اسمی TCP/IP را به آدرس آنها برگرداند .
می دانیم که در پروتکل TCP/IP هنگامی که مثلاً می نویسیم <http://www.yahoo.com> فایده ای برای TCP/IP نداشته و باید آدرس سایت yahoo را پیدا کند .
وظیفه تبدیل اسم TCP/IP به آدرس IP به عهده DNS Server بوده و هر Host نیازمند دانستن آدرس DNS Server است .

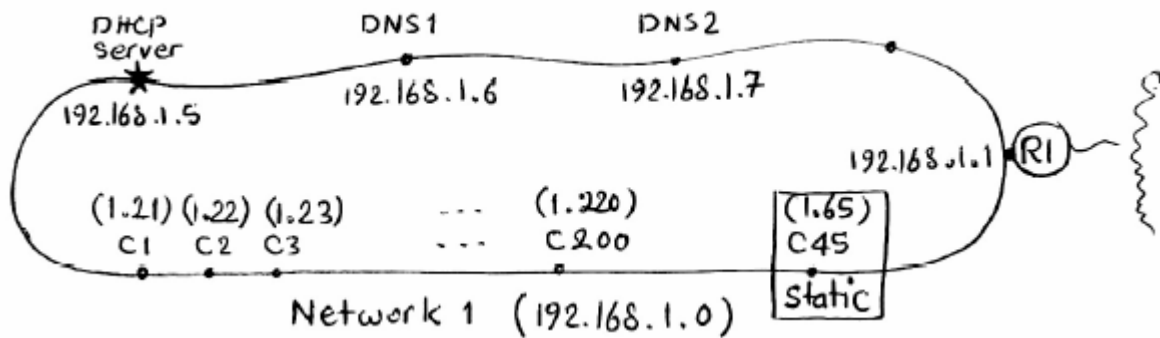
سایر پارامترهای ثانوی را به دلیل آنکه در حالت خاص استفاده می شوند در این مبحث بررسی نمی کنیم .

برای آنکه پیکربندی Scope را بهتر درک کنیم لازم است تا عملاً 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 چگونه " پیکربندی DHCP Server " را تعیین می کند و توجه 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 :



شکل ۷-۱۵

همانطور که از شکل ۷-۱۵ پیدا است Network تشکیل شده از 200 ایستگاه به نام های c1 الی c200 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 عمل 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)

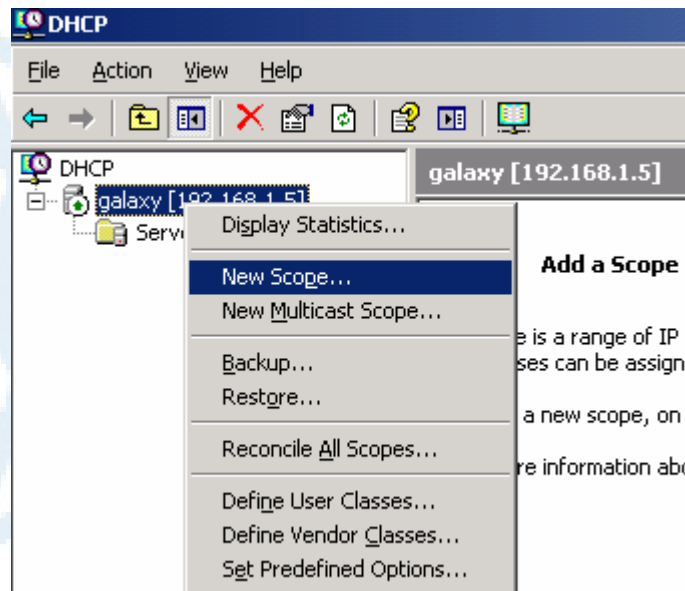
- Exclusion Range:192.168.1.65
- Lease Duration:60 Days

پارامترهای ثانوی:

- Router : 192.168.1.1
- DNS Server: 192.168.1.6&192.168.1.7

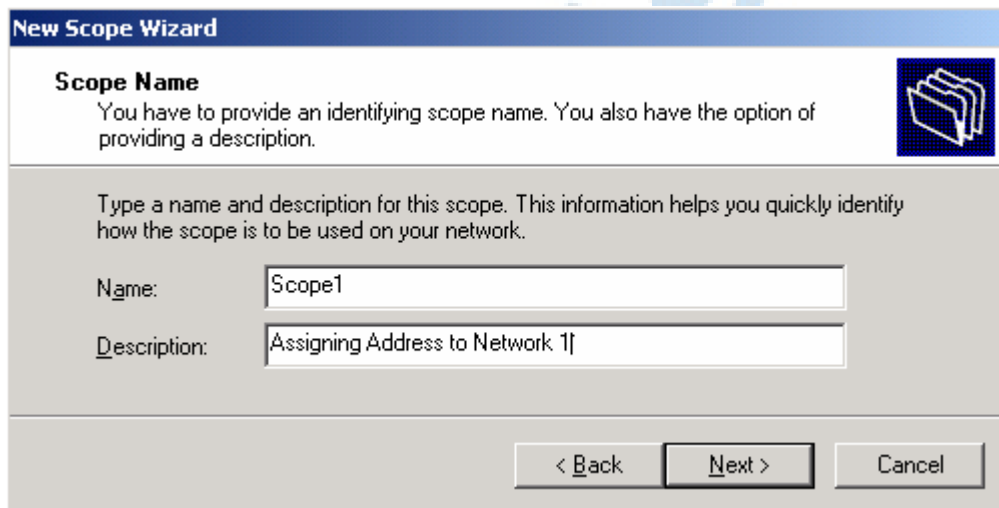
حال کنسول DHCP را روی سرور اجرا کرده و کار پیکربندی را آغاز کنید:

ابتدا روی آیکن سرور کلیک راست کنید و گزینه New Scope را برای تعریف محدوده جدید انتخاب نمایید:



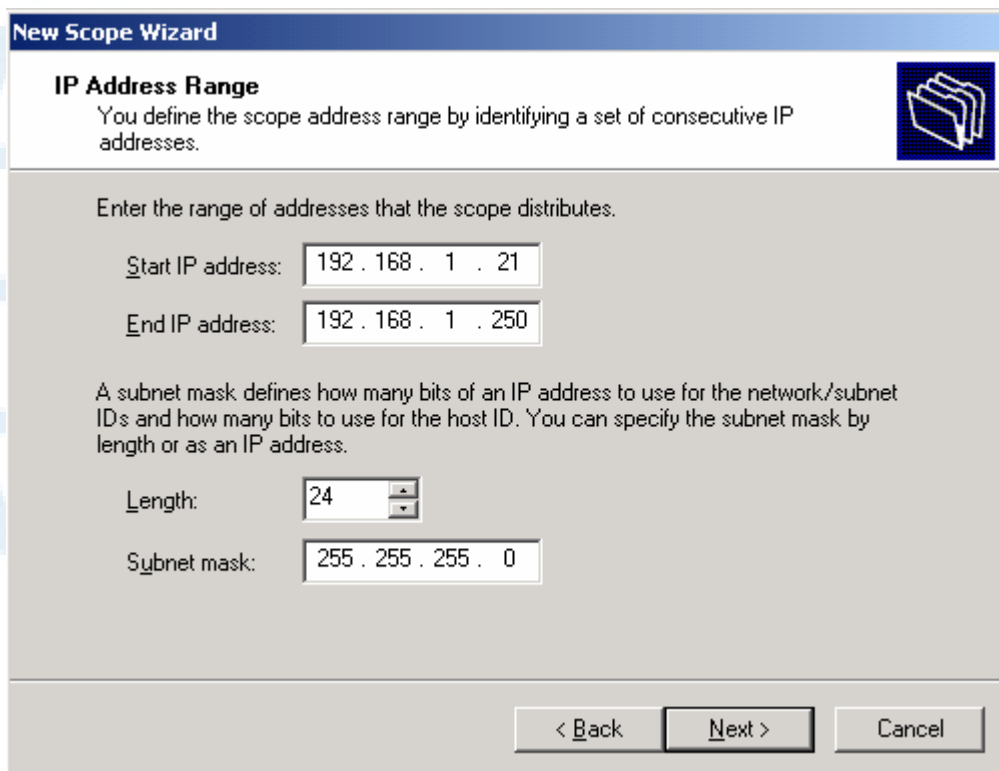
شکل ۱۵-۸

سپس نام Scope را وارد کرده و یک Description مناسب (اختیاری) برای آن بنویسید:



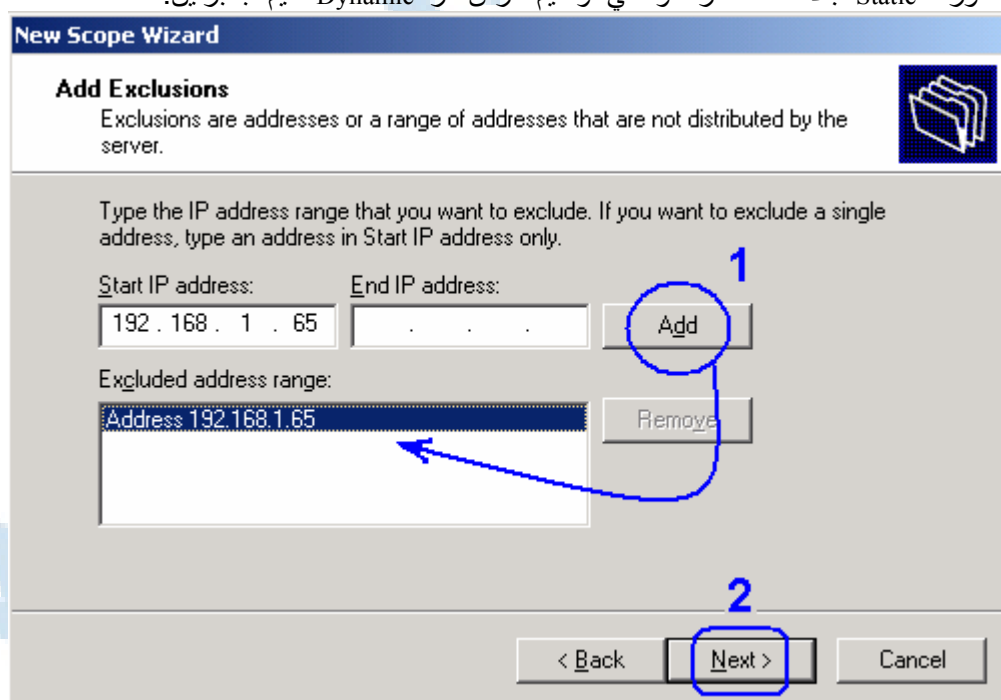
شکل ۱۵-۹

اکنون نوبت به تعیین محدوده آدرس هایی است که باید به ایستگاه ها تخصیص یابد:



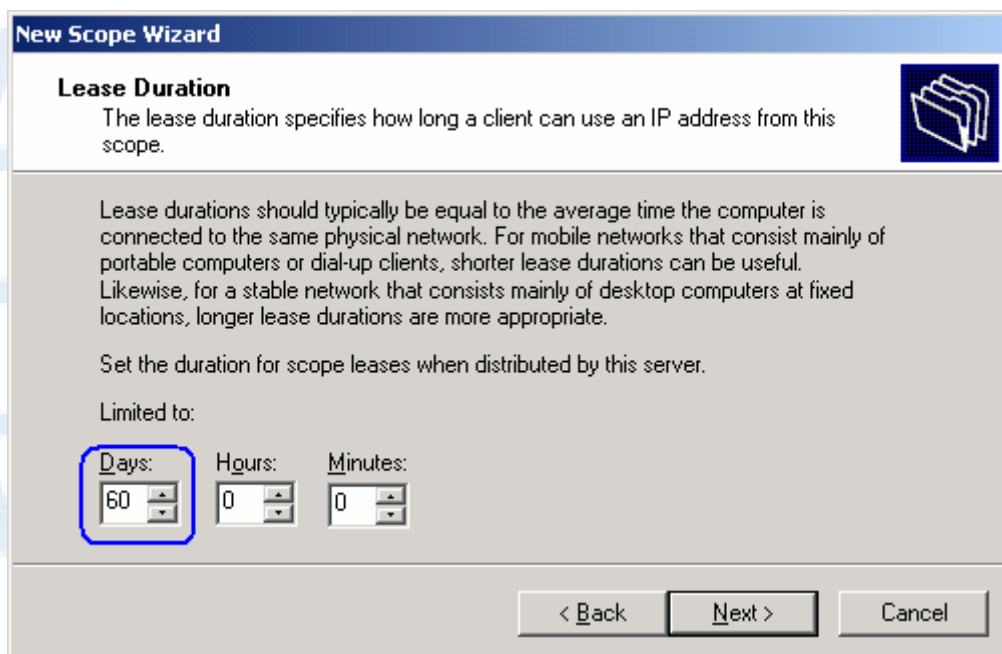
شکل ۱۵-۱۰

طبق طرح ، آدرس ۱۹۲,۱۶۸,۱,۶۵ نباید از طریق DHCP Server به ایستگاه ها داده شود چرا که یکی از سیستم ها آنرا بصورت Static قبلاً استفاده کرده و نمی‌خواهیم آدرس آنرا Dynamic کنیم، بنابراین:



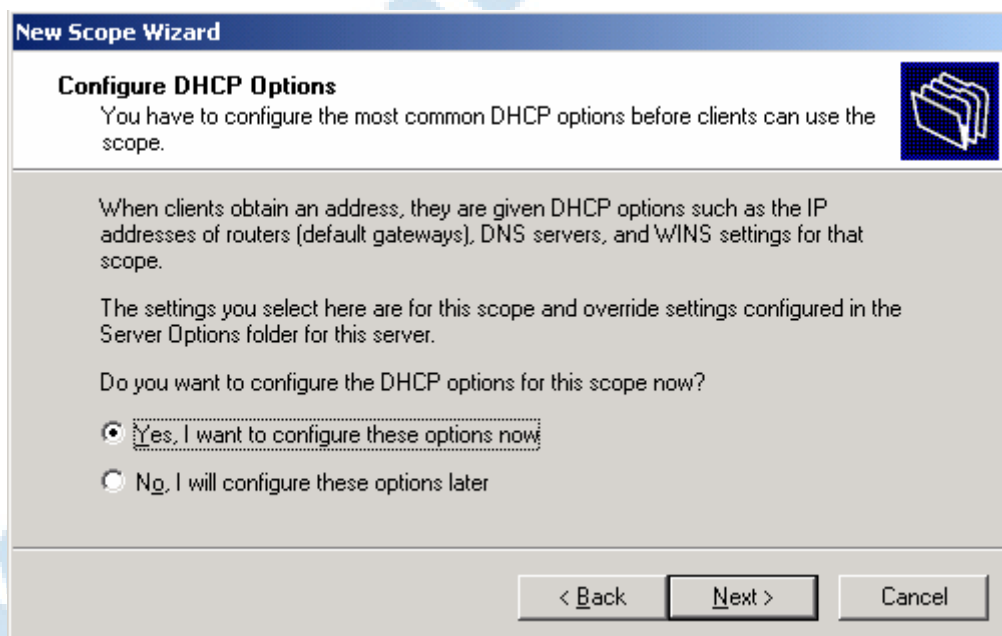
شکل ۱۵-۱۱

با توجه به پایداری Client ها، زمان اجاره را مثلاً ۶۰ روز انتخاب کنید:



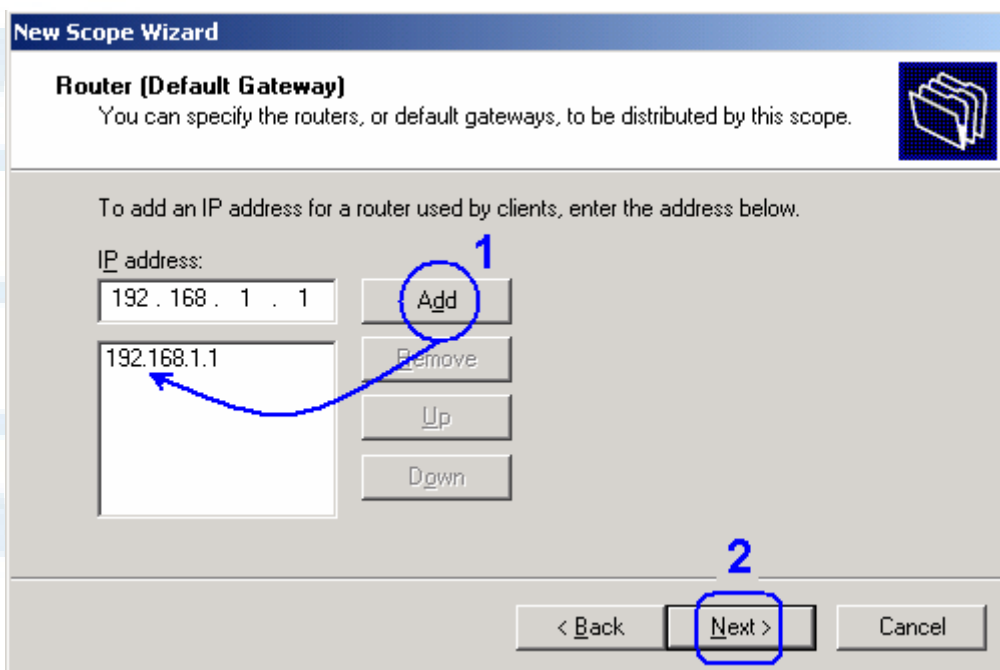
شکل ۱۲-۱۵

تا اینجا 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 پردازیم، 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 در آن صورت 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 گزینه Activate صورت می‌گیرد. در اینجا چون ادامه کار را با همین Wizard انجام می‌دهیم لذا پس از اتمام کار، Scope بطور خودکار Activate خواهد شد:



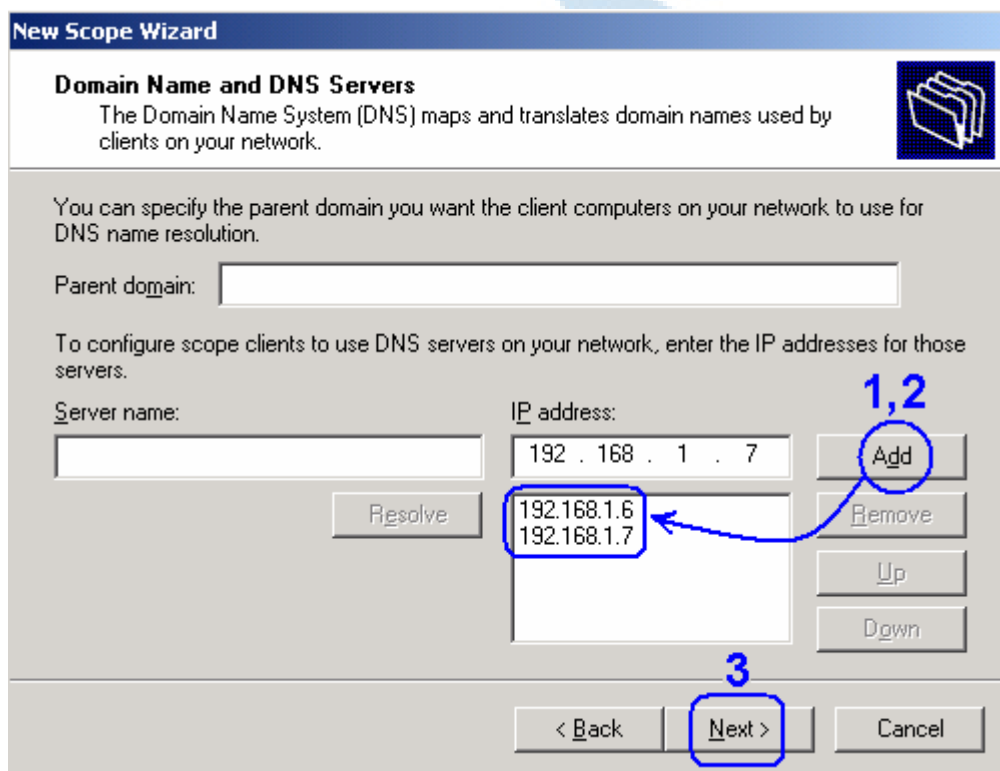
شکل ۱۳-۱۵

اولین پارامتر ثانوی عبارت است از تعیین آدرس روتر یا عبارتی همان
: Default Gateway



شکل ۱۴-۱۵

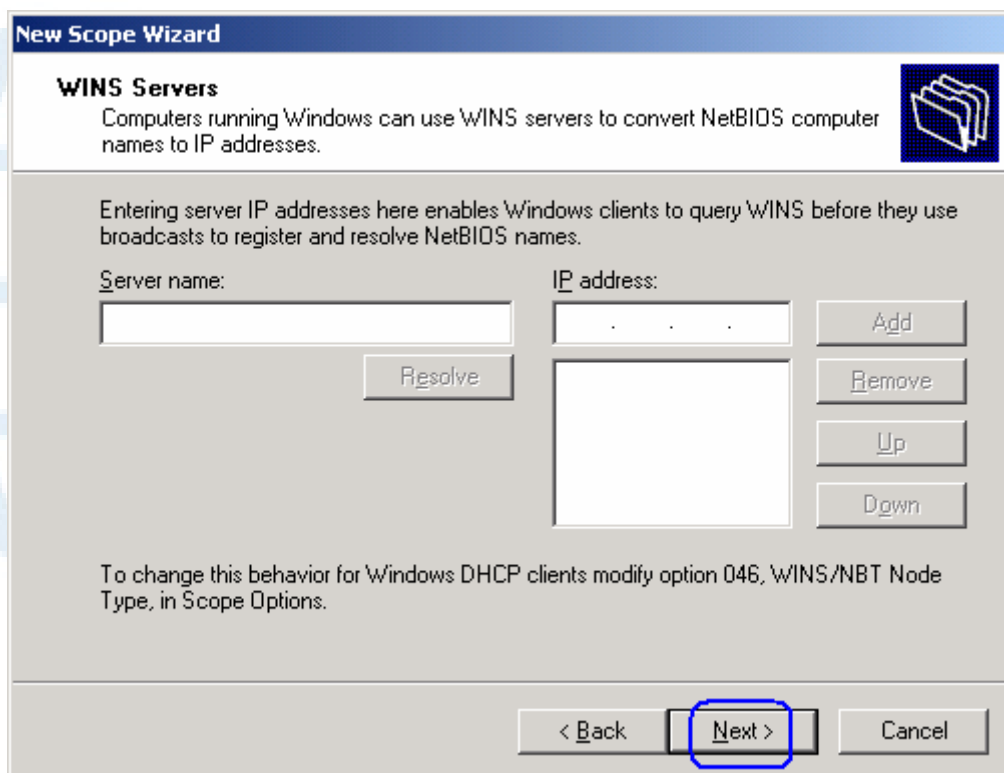
سپس باید آدرس DNS Server(s) را تعیین کنیم، چون در مثال مذکور ۲ دستگاه DNS Server داریم لذا هر دو را به Client ها معرفی کنید:



شکل ۱۵-۱۵

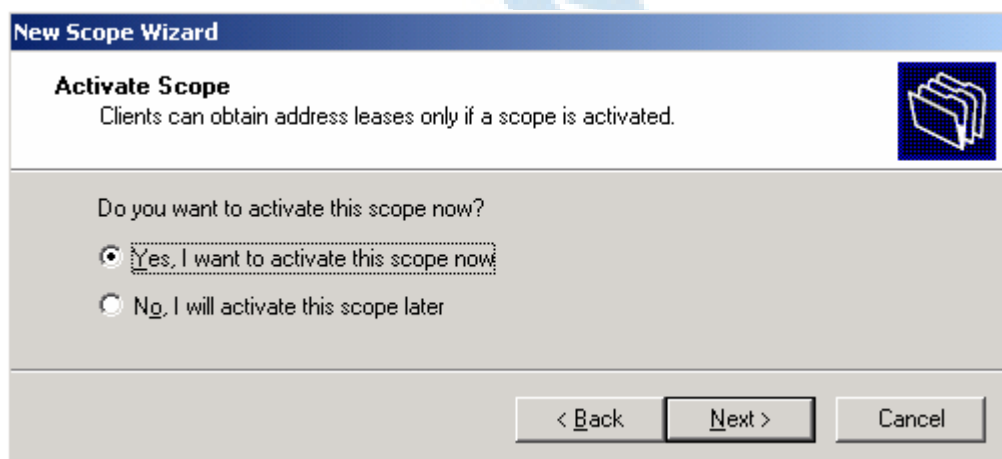
البته در مرحله فوق می‌توانیم نام Domain را نیز که می‌خواهیم به FQDN Client ها تعلق گیرد تعیین کنیم، اما بدلیل عدم درخواست صورت مسأله از آن صرف نظر کردیم.

حال نوبت به تعیین آدرس WINS Server می‌رسد که آنرا هم با توجه به عدم نیاز در صورت مسأله بدون مقدار رد کنید:



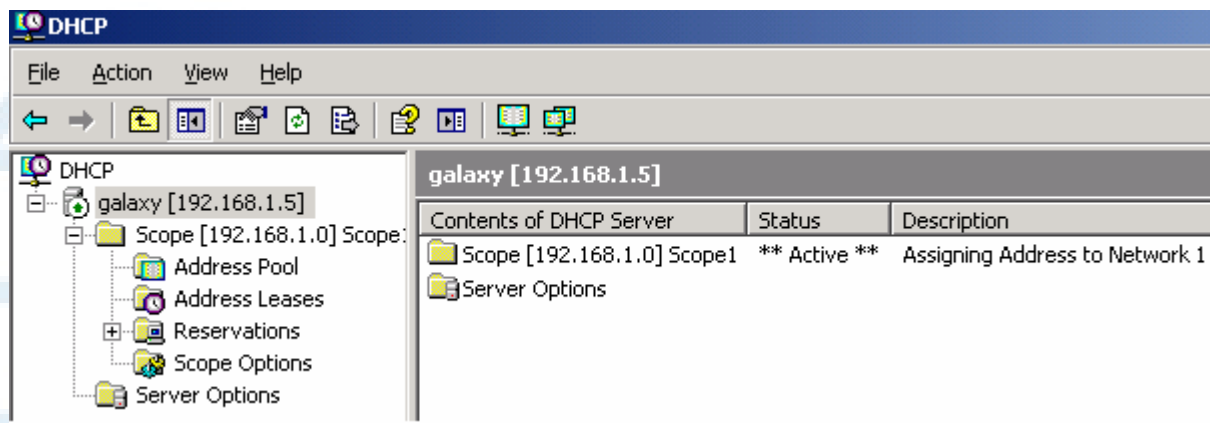
شکل ۱۶ - ۱۵

اکنون در آخرین مرحله، باید Scope را فعال کنیم:



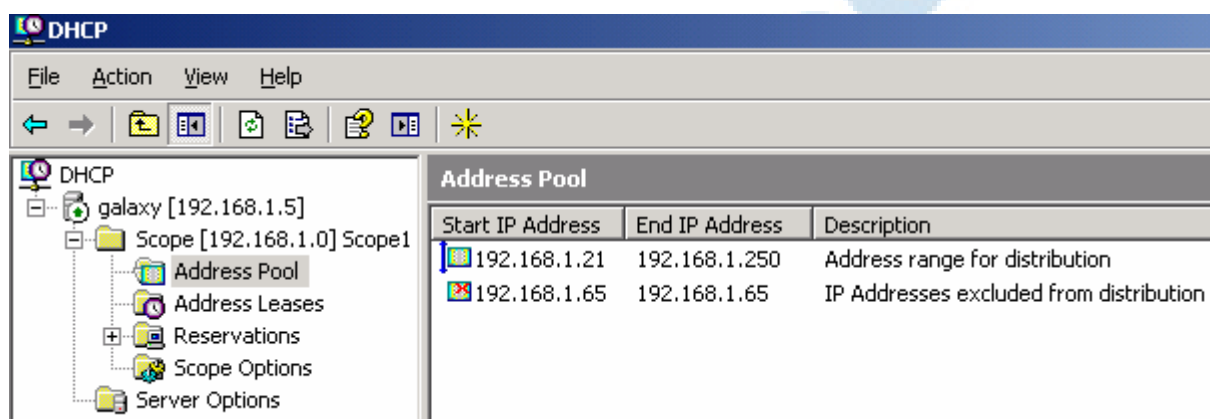
شکل ۱۷ - ۱۵

کار را به اتمام رسانده (Finish) سپس Scope را از زیر شاخه سرور انتخاب کنید تا بتوانید نتایج تنظیمات و همچنین نحوه بهره‌برداری Client ها از آنرا ببینید:



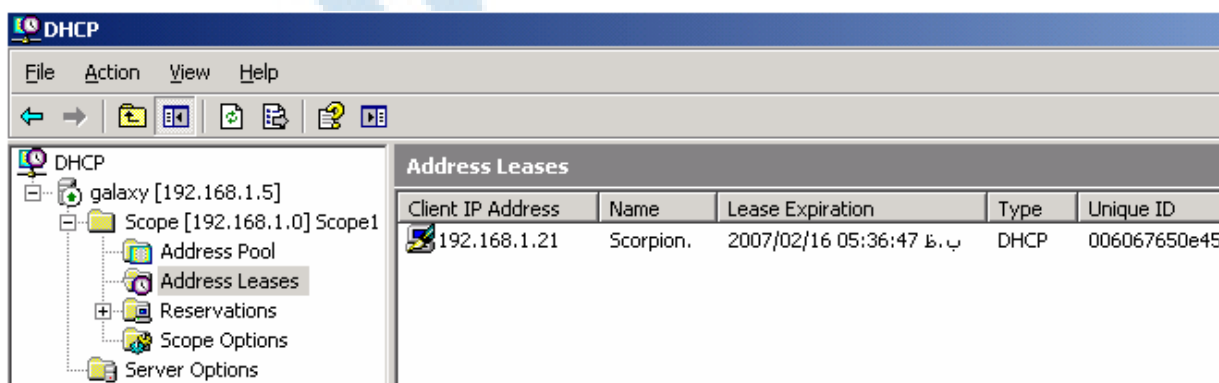
شکل ۱۸ - ۱۵

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

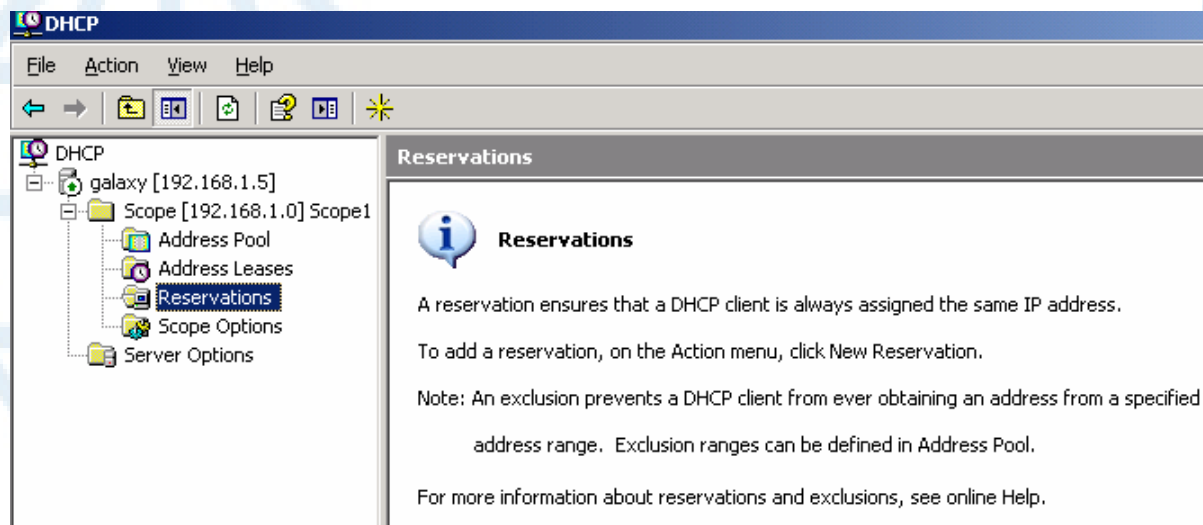
چنانچه قسمت Address Leases را انتخاب کنید می‌توانید آدرس‌هایی را که تاکنون Client ها از سرور گرفته‌اند به‌مراه مشخصات Client و همچنین پایان زمان اجاره مشاهده کنید:



شکل ۲۰ - ۱۵

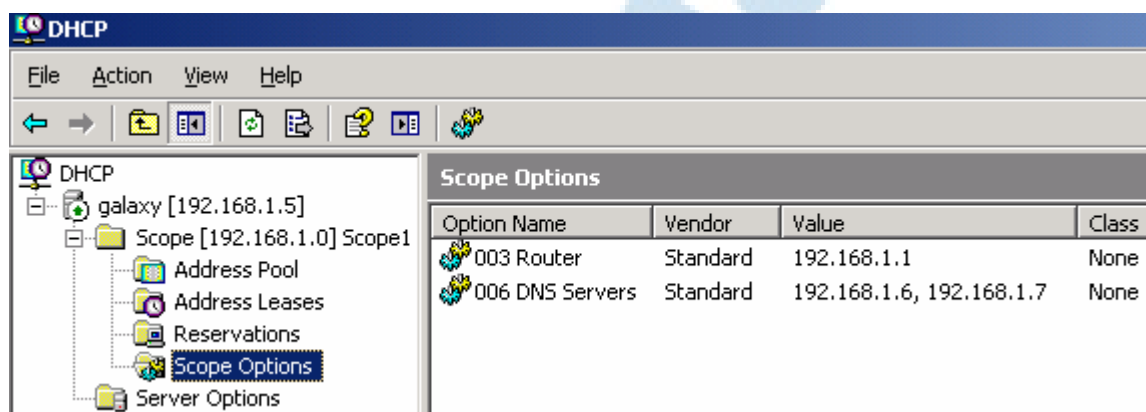
اگر می‌خواهید آدرس‌های مشخص را برای یک Client بطور دائمی تخصیص دهید می‌توانید آدرس را برای آن ذخیره کنید. برای این کار لازم است تا MAC Client Address را داشته باشید. برای بدست آوردن MAC Address یک کامپیوتر راه‌های مختلفی وجود دارد اما استفاده از دستور ipconfig /all یا دستور getmac

رایتر است. در سناریوی یادشده آدرسی برای ذخیره تعیین نکردیم لذا لیست خالی است:



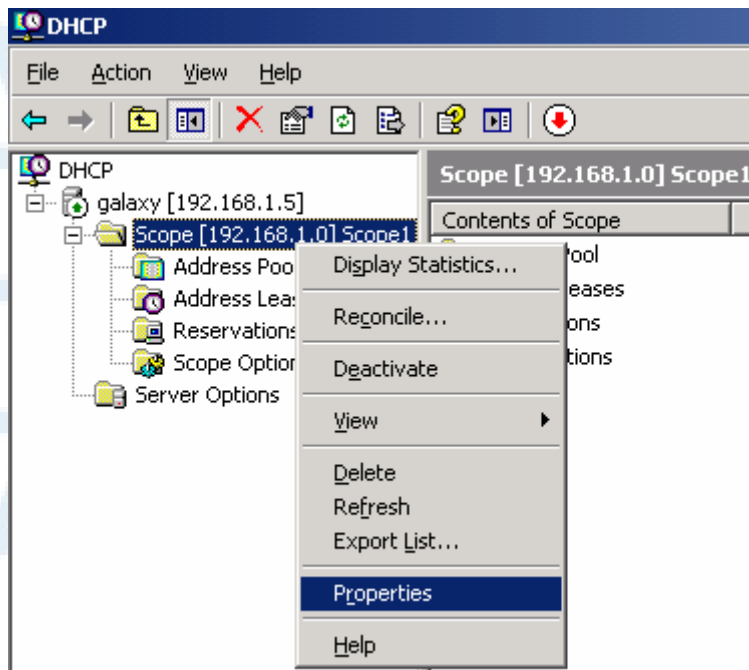
شکل ۲۱ - ۱۵

اکنون قسمت Scope Options را انتخاب کرده و تأیید کنید که پارامترهای ثانوی تنظیم شده یعنی Router و DNS Server هر دو وجود دارند:

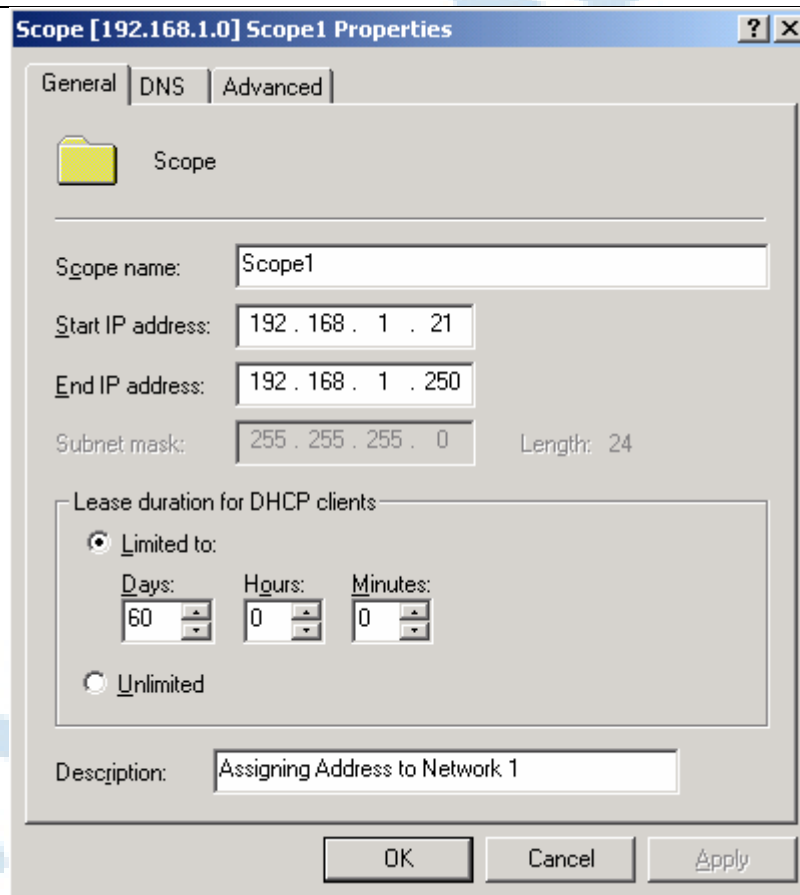


شکل ۲۲ - ۱۵

می‌توانید اکثر پارامترهای Scope را تغییر دهید. بعنوان مثال برای گسترش یا کاهش محدوده آدرسها یا تغییر زمان اجاره مطابق زیر عمل کنید:

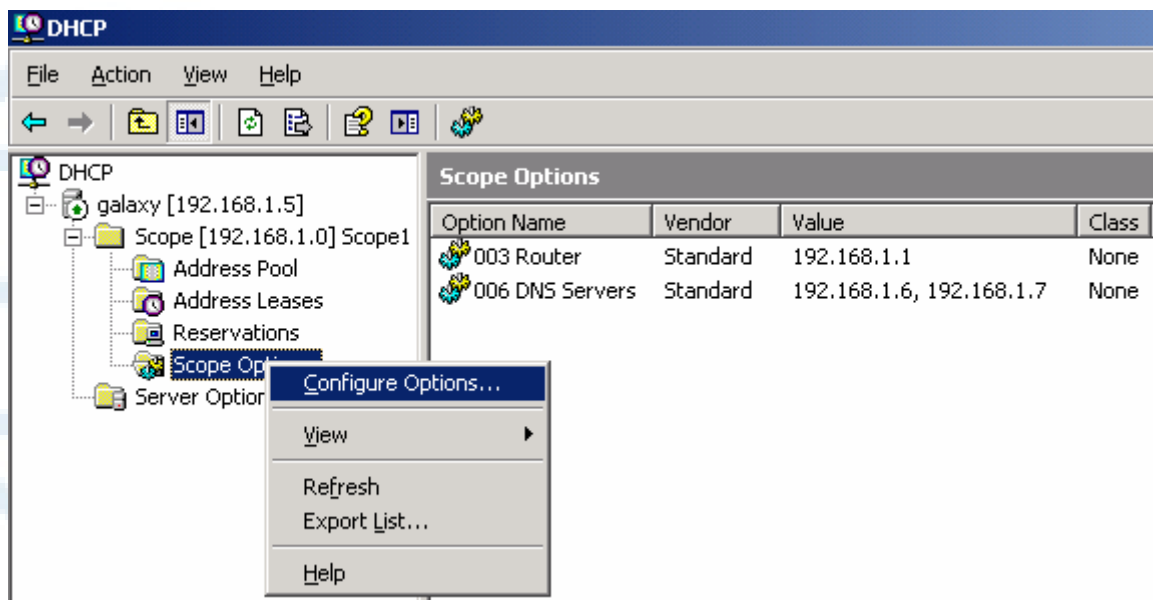


شکل ۲۳ - ۱۵

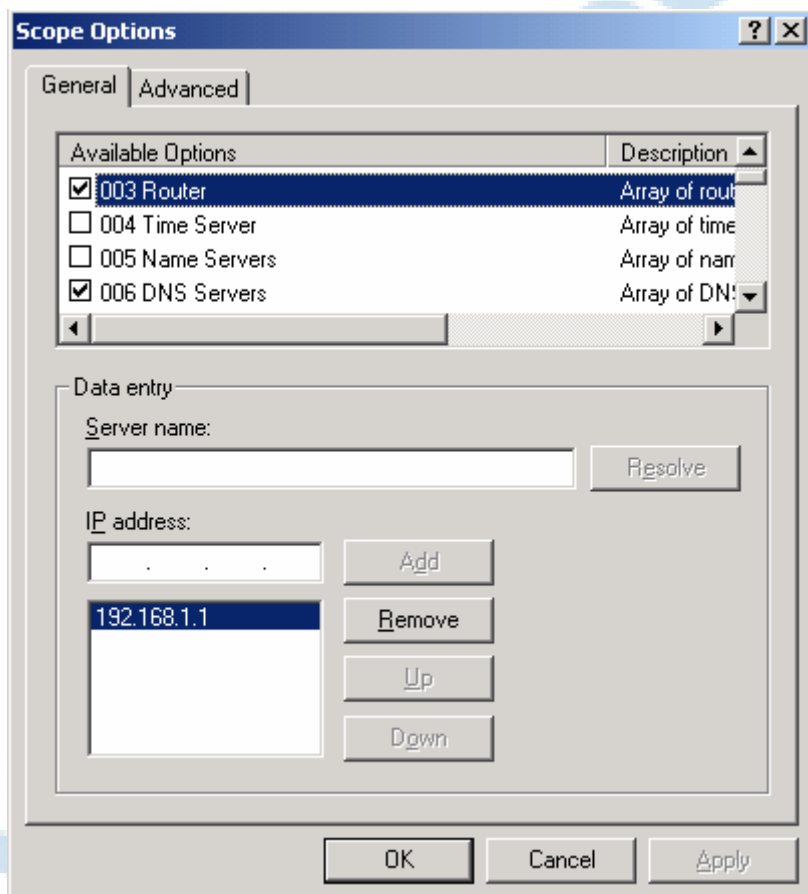


شکل ۲۴ - ۱۵

همچنین برای تغییر پارامترهای ثانوی می‌توانید مانند شکل‌های زیر عمل کنید:



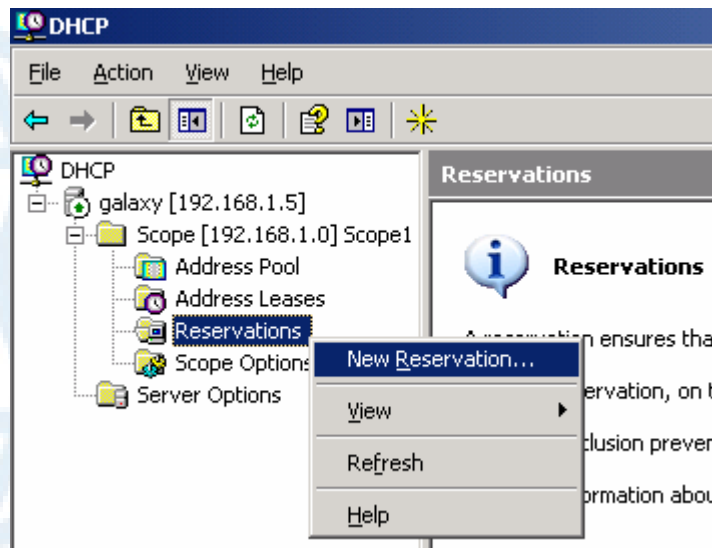
شکل ۲۵ - ۱۵



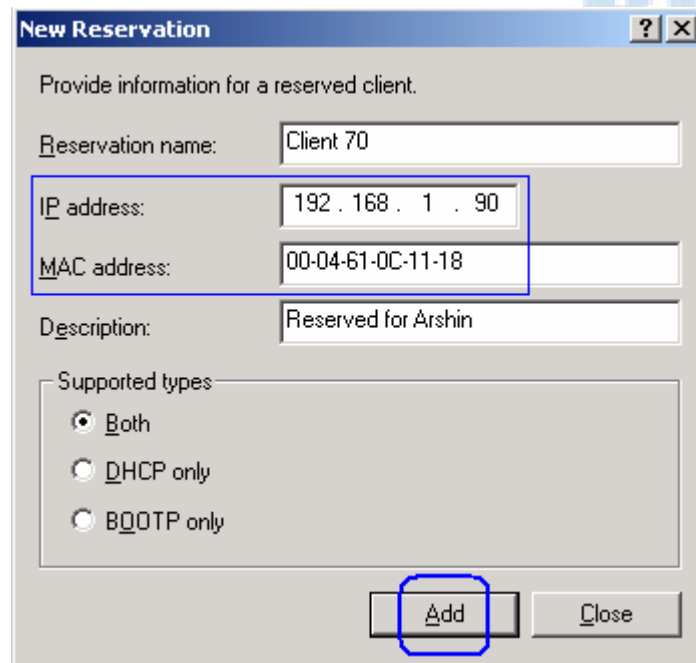
شکل ۲۶ - ۱۵

البته با Double Click روی یکی از Scope Options نیز همان نتیجه فوق بدست می‌آید.

در صورت نیاز به ذخیره آدرس، از قسمت Reservation حرکت را شروع کنید. همانطور که اشاره شد ابتدا باید Client MAC Address را بدانید. فرض کنید می‌خواهیم آدرس 192.168.1.90 را برای Client70 ذخیره کنیم که MAC آن برابر با 00-04-61-0C-11-18 بوده و کاربر آن شخصی بنام Arshin است. البته دانستن نام کاربر برای پیکربندی لازم نبوده و صرفاً جنبه اطلاع‌رسانی دارد:

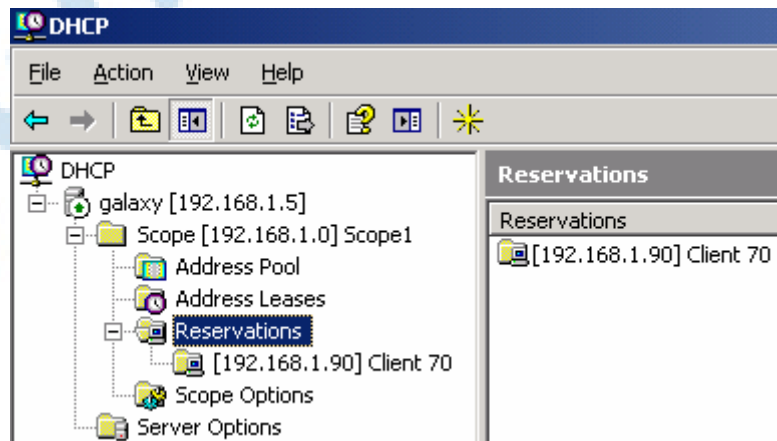


شکل ۲۷ - ۱۵



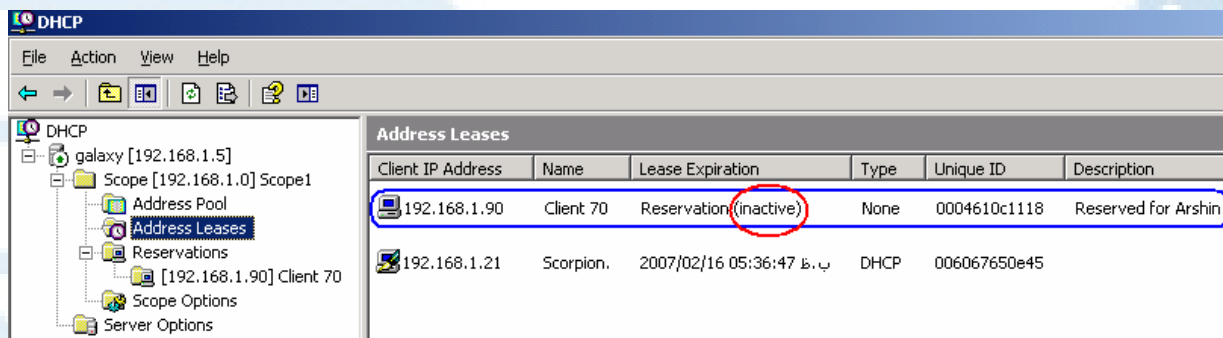
شکل ۲۸ - ۱۵

نتیجه 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:



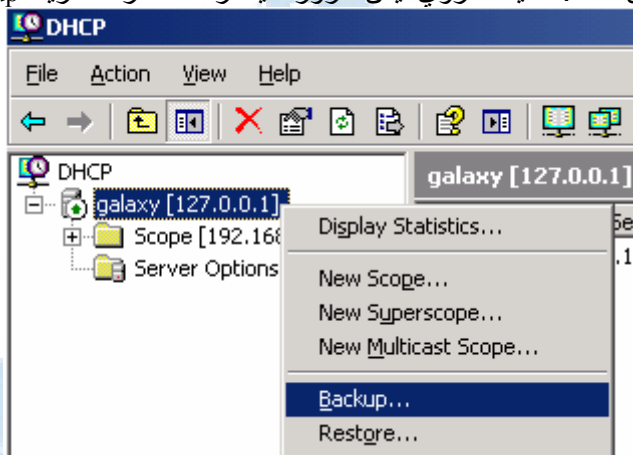
شکل ۳۰- ۱۵

بسیار خوب! تا اینجا توانسته ایم پیکربندی یک DHCP Server را برای یک سناریوی ساده به پایان رسانده و نتیجه را ببینیم.

۶-۱۵- Backup / Restore اطلاعات DHCP Server :

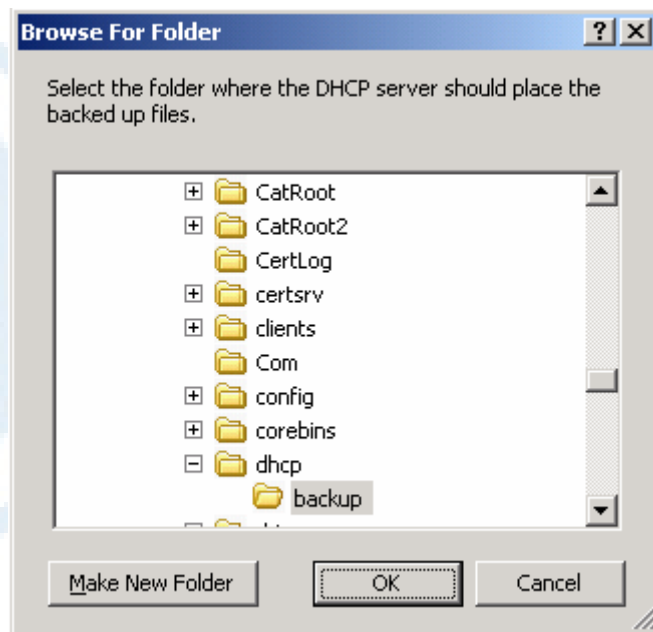
هرچند نصب و پیکربندی DHCP Server در سناریوهای ساده چندان کار سختی نیست اما در موارد پیچیده‌تر لازم است تا گاهی اوقات از اطلاعات Scope و همچنین وضعیت تخصیص آدرسها به Client های مختلف Backup تهیه شود. این نسخه‌های Backup کمک می‌کنند تا هنگام بهم ریختن اطلاعات Scope یا هنگام انتقال DHCP Server از یک سرور به سرور دیگر یا نصب مجدد سرور بتوان با سرعت اطلاعات را برگرداند.

روش تهیه Backup: بسیار آسان است. کفایت روی آیکن سرور کلیک راست کرده، گزینه Backup را انتخاب کنید:



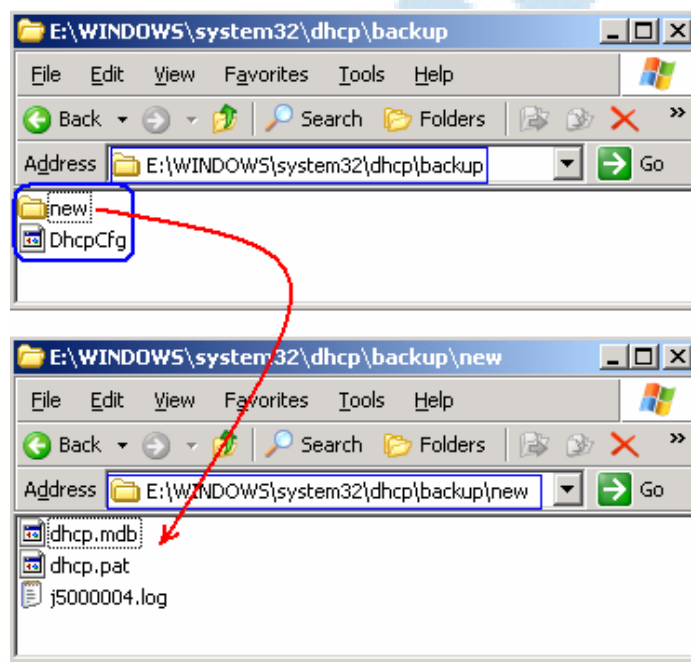
شکل ۳۱- ۱۵

در این مرحله باید محل ذخیره‌سازی Backup را تعیین کنیم که پیش‌فرض آن واقع در مسیر زیر است:



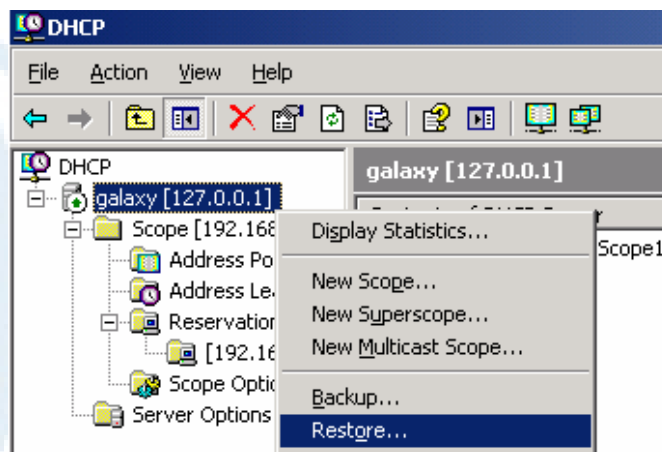
شکل ۱۵-۳۲

پس از اتمام کارپوشه فوق را باز کرده و تأیید کنید که Backup بدرستی گرفته شده :



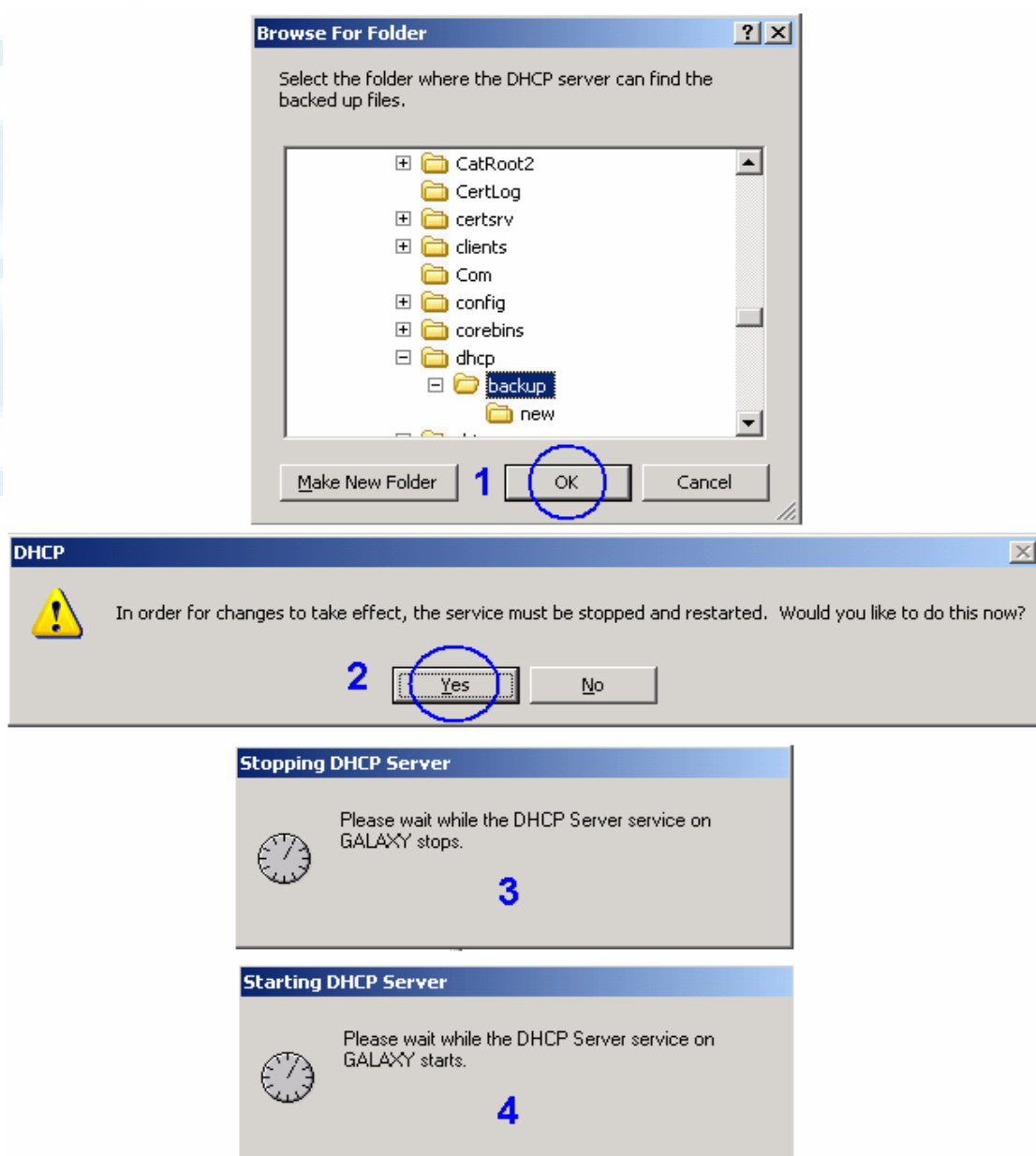
شکل ۱۵-۳۳

مراحل Restore نیز مشابه بوده و به شکل زیر است:



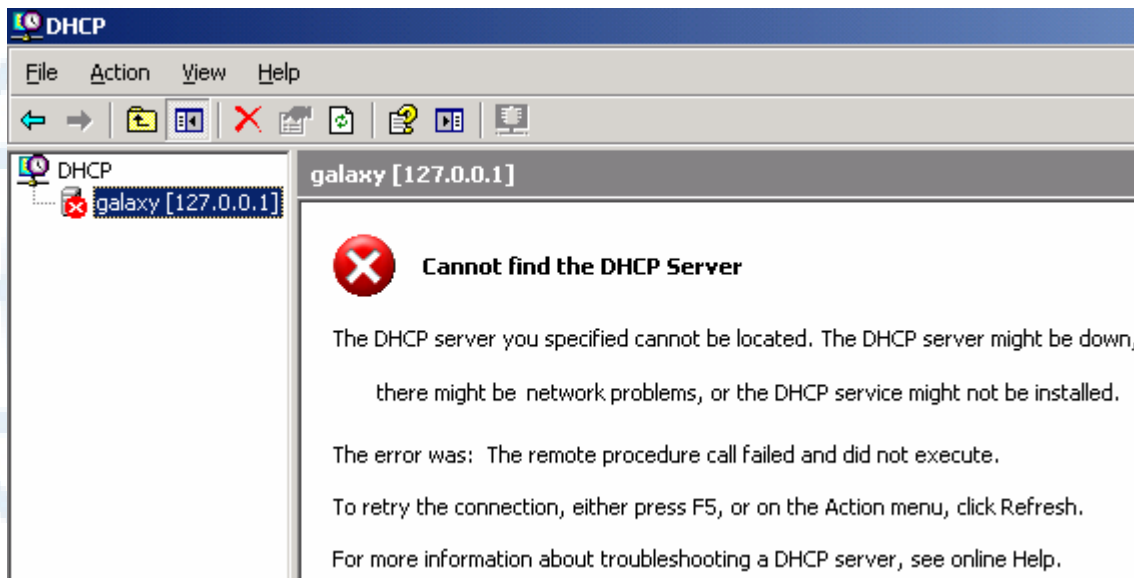
شکل ۳۴ - ۱۵

پس از تعیین مسیر، تأییدیه غیرفعال کردن یا (Stop) سرویس DHCP Server را جهت ادامه کار قبول کرده تا فرایند Restore بدرستی به پایان رسد. در انتها سرویس بطور خودکار Start خواهد شد.



۷-۱۵ - عیبیابی DHCP Server :

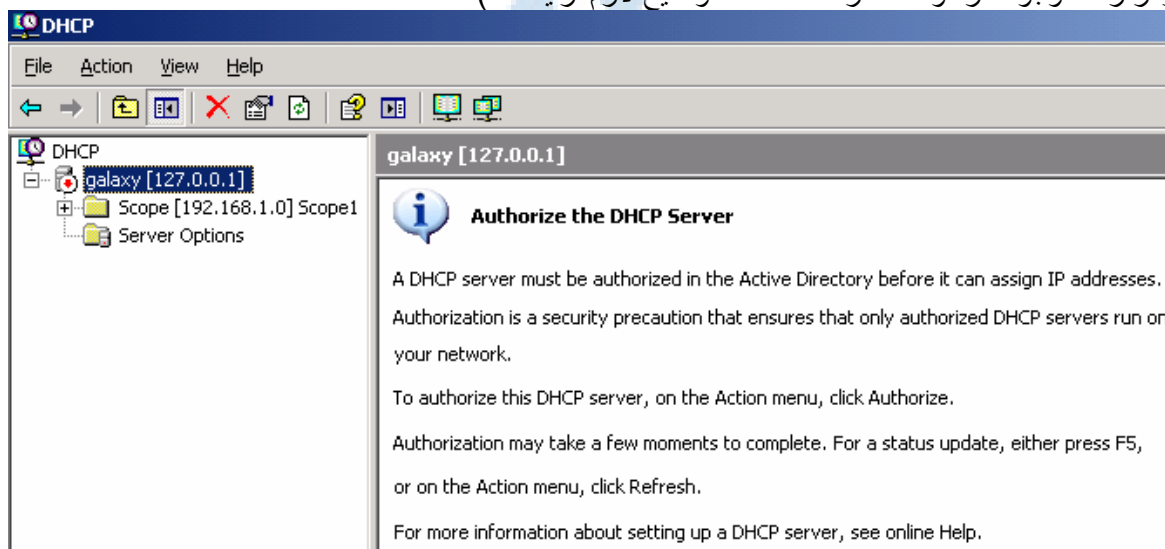
رایج ترین اشکالاتی که ممکن است در DHCP Server عبارتند از:
۱. سرویس DHCP Server به هر دلیل غیرفعال است. برای چک کردن آن از کنسول سرویسها وارد عمل شده (Services.msc) و تأیید کنید که وضعیت سرور بصورت Started باشد. در حالتی که سرویس DHCP Server غیرفعال باشد اگر کنسول DHCP را اجرا کنیم با چنین وضعیتی روبرو می‌شویم:



شکل ۳۵ - ۱۵

نکته: به طریق مشابه ممکن است سرویس DHCP Client روی Client غیرفعال شده باشد که باید آنرا بررسی کرد. البته چنانچه هیچ ایستگاهی نتواند از سرور آدرس بگیرد بعید است مشکل از سمت Client ها باشد و به احتمال زیاد باید علت را درون سرور یا ارتباط سرور با شبکه جستجو کرد.

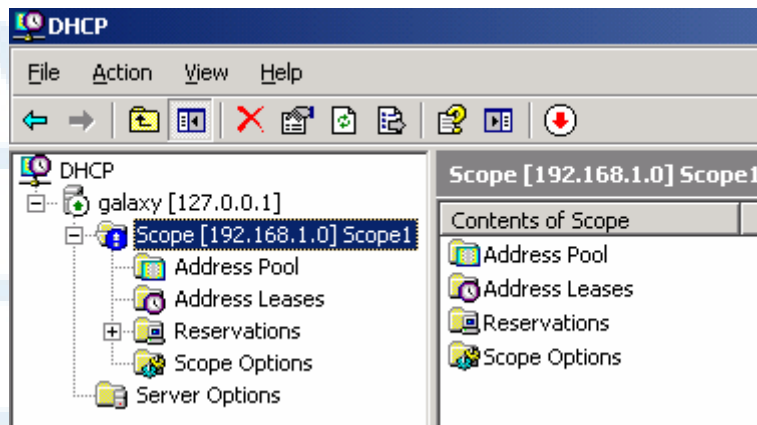
۲. DHCP Server مجاز به سرویس دهی در شبکه نیست! اصطلاحاً Authorize نشده. چنین حالتی زمانی اتفاق می افتد که DHCP Server در محیط Active Directory کار می کند. در این مواقع DHCP Server باید از جانب Domain Controller مجاز به سرویس دهی شود. به شکل زیر توجه کنید که در آن مشکل کاملاً مشخص است: (روی آیکن سرور علامت فلش قرمز رنگ وجود دارد و سمت راست صفحه توضیح لازم ارائه شده)



شکل ۳۶ - ۱۵

برای کسب اجازه کفایت روی آیکن سرور کلیک راست کرده و گزینه Authorize را انتخاب نمایم. پس از طی زمانی کوتاه و احياناً چندبار Refresh کردن صفحه یا بستن و بازکردن مجدد کنسول DHCP باید آیکن قرمز رنگ برطرف شده باشد.

۳. Scope پر شده است. بدیهی است در چنین حالتی Client ها نمی توانند آدرس بگیرند اما Client ها بی که قبلاً از سرور آدرسی را دریافت کرده و هنوز اجاره آنها تمام نشده به کار خود ادامه داده و ضمناً در زمان مقتضی قرارداد خود را تمدید خواهند کرد. عبارت دیگر جای خود را به این سادگی از دست نمی دهند!! هنگامی که Scope پر می شود، با صحنه زیر مواجه می شویم: (علامت تعجب آبی رنگ در کنار Scope)



شکل ۳۷-۱۵

پرسش: به نظر شما در چنین مواقعی بهترین کار برای رفع مشکل چیست؟

۴. Network Number کارت شبکه DHCP Server (با کارت شبکه DHCP Relay Agent) با Network Number هیچیک از Scope های تعریف شده همخوانی ندارد. در چنین حالاتی DHCP Server نمی‌تواند تشخیص دهد که از کدام Scope باید به Client ها سرویس دهد. چنانچه یک Scope بیشتر نباشد و حالت فوق بروز کند باز هم سرور قادر به تخصیص آدرس به Client ها نیست.

مثال: فرض کنید در مثال ۱، آدرس کارت شبکه DHCP Server بجای 192.168.1.5 اشتباهاً 192.168.2.5 وارد شود. همین اشتباه به ظاهر کوچک کافی است تا سرور به هیچ ایستگاهی سرویس ندهد چرا که Scope تعریف شده در آن برای شبکه 192.168.1.0 تعریف شده و نه برای 192.168.2.0.

۵. گاهی اوقات Administrator اشتباهی را مرتکب می‌شود بدین شرح که DHCP Server و DHCP Relay Agent را هر دو توأم روی یک کامپیوتر نصب می‌کند. چون هر دو سرویس روی یک شماره Port عمل می‌کنند (UDP Port 67) لذا مشکل Port Conflict بروز کرده و ممکن است هیچیک کار خود را درست انجام ندهند!

۶. این احتمال نیز وجود دارد که یک Firewall روی DHCP Client یا روی DHCP Server یا بین آنها قرار گرفته و مانع عبور ترافیک مربوطه می‌شود. باید دقت کرد برای آنکه پروتکل DHCP بتواند کار خود را انجام دهد، UDP Ports 67 مسدود نباشد.

برای آزمایش صحت عملکرد ارتباط بین DHCP Client و DHCP Server یک راه ساده نیز وجود دارد که از روی Client باید انجام شود: استفاده از فرمان ipconfig /release برای آزاد کردن آدرس اخذ شده از سرور و فرمان ipconfig /renew برای کسب مجدد آدرس و سایر پارامترها. چنانچه فرمان اخیر درست کار کند به معنی صحت عملکرد DHCP Server است و بشرط آنکه Scope پر نشده باشد باید مشکل Client ها را که نمی‌توانند آدرس بگیرند در خود آنها یا راه ارتباطی آنها با شبکه جستجو کرد.

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 ؟

به دوروش یکی به صورت **Command line** دوم : از طریق آیگون شبکه روی نوار وظیفه

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



www.IranMeet.com

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 Transfer Protocol	
IPX	Internetwork Packet Exchange	
MAN	Metro Politan Area Network	
OSI		
POP3		
SMTp	Simple Network	