بسم الله الرحمن الرحیم

شبکه‌های رایانه‌ای

رشتهٔ کامپیوتر

گروه تحصیلی کامپیوتر

زمینهٔ خدمات

شاخهٔ آموزش فنی و حرفه‌ای

۴/۶ خوش‌رو، آرشین

ش ۸۶۷ خ / شبکه‌های رایانه‌ای/ مؤلفان : آرشین خوش رو، محمدعلی شاهی، سیدحمیدرضا ضیایی

۱۳۹۲ ــ تهران : شرکت چاپ و نشر کتاب‌های درسی ایران، ۱۳۹۲

۲۷۲ ص : مصور ــ (آموزش فنی و حرفه‌ای)

متون درسی رشتهٔ کامپیوتر گروه تحصیلی کامپیوتر، زمینهٔ خدمات

برنامه‌ریزی و نظارت، بررسی و تصویب محتوا : دفتر تألیف کتاب‌های درسی فنی‌وحرفه‌ای و کاردانش وزارت آموزش و پرورش

۱ شبکه‌های رایانه‌ای ــ کتاب‌های درسی (متوسطه) ۲ شبکه‌های محلی ــ کتاب‌های درسی (متوسطه) الف شاهی، محمدعلی ب ضیایی، سیدحمیدرضا ج ایران وزارت آموزش و پرورش دفتر تألیف کتاب‌های درسی فنی‌وحرفه‌ای و کاردانش د عنوان

۱۳۹۲

همکاران محترم و دانش‌آموزان عزیز :

پیشنهادات و نظرات خود را دربارهٔ محتوای این کتاب به نشانی تهران ـ صندوق پستی شمارهٔ ۴۸۷۴/۱۵ دفتر تألیف کتاب‌های درسی فنی‌وحرفه‌ای و کاردانش، ارسال فرمایند.

پیام‌نگار (ایمیل) tvoccd @roshd.ir

وب‌گاه (وب‌سایت) www.tvoccd.medu ir

محتوای این کتاب براساس تغییرات حوزه فناوری و نظرات هنرآموزان و گروه‌های آموزشی استان‌ها به وسیله حبیب رسا و منصور رسام‌نژاد زیر نظر کمیسیون تخصصی برنامه‌ریزی و تألیف کتاب‌های درسی رشته کامپیوتر در سال ۱۳۹۱ مورد بازبینی و اصلاح کلی قرار گرفته است.

وزارت آموزش و پرورش

سازمان پژوهش و برنامه‌ریزی آموزشی

برنامه‌ریزی محتوا و نظارت بر تألیف : **دفتر تألیف کتاب‌های درسی فنی وحرفه‌ای وکاردانش**

نام کتاب : **شبکه‌های رایانه‌ای ـ ۴۵۱/۴**

مؤلفان : **مهندس آرشین خوش‌رو، مهندس محمد علی شاهی و مهندس سیدحمیدرضا ضیایی**

اعضای کمیسیون تخصصی : **دکتر بتول عطاران، محمدرضا شکرریز، محمدرضا یمقانی، افشین اکبری، سید سعیدرضا سعادت یزدی، مهیار پازوکی، ملیحه طزری، شهناز علیزاده، زهرا عسگری رکن‌آبادی و سارو آواکیانس**

آماده‌سازی و نظارت بر چاپ و توزیع : **ادارهٔ کلّ نظارت بر نشر و توزیع مواد آموزشی**

تهران : خیابان ایرانشهر شمالی ـ ساختمان شمارهٔ ۴ آموزش و پرورش (شهید موسوی)

تلفن : ۹ـ۸۸۸۳۱۱۶۱، دورنگار : ۸۸۳۰۹۲۶۶، کدپستی : ۱۵۸۴۷۴۷۳۵۹،

وب‌سایت : **www.chap.sch.ir**

مدیر امور فنی و چاپ : **سیّد احمد حسینی**

طراح جلد : **محمدحسن معماری**

صفحه‌آرا : **راحله زادفتح‌اله**

حروفچین : **سیّده فاطمه محسنی، کبری اجابتی**

مصحح : **علی نجمی، صمد اصولی هلان**

امور آماده‌سازی خبر : **فاطمه پزشکی**

امور فنی رایانه‌ای : **حمید ثابت کلاچاهی، سیّده شیوا شیخ‌الاسلامی**

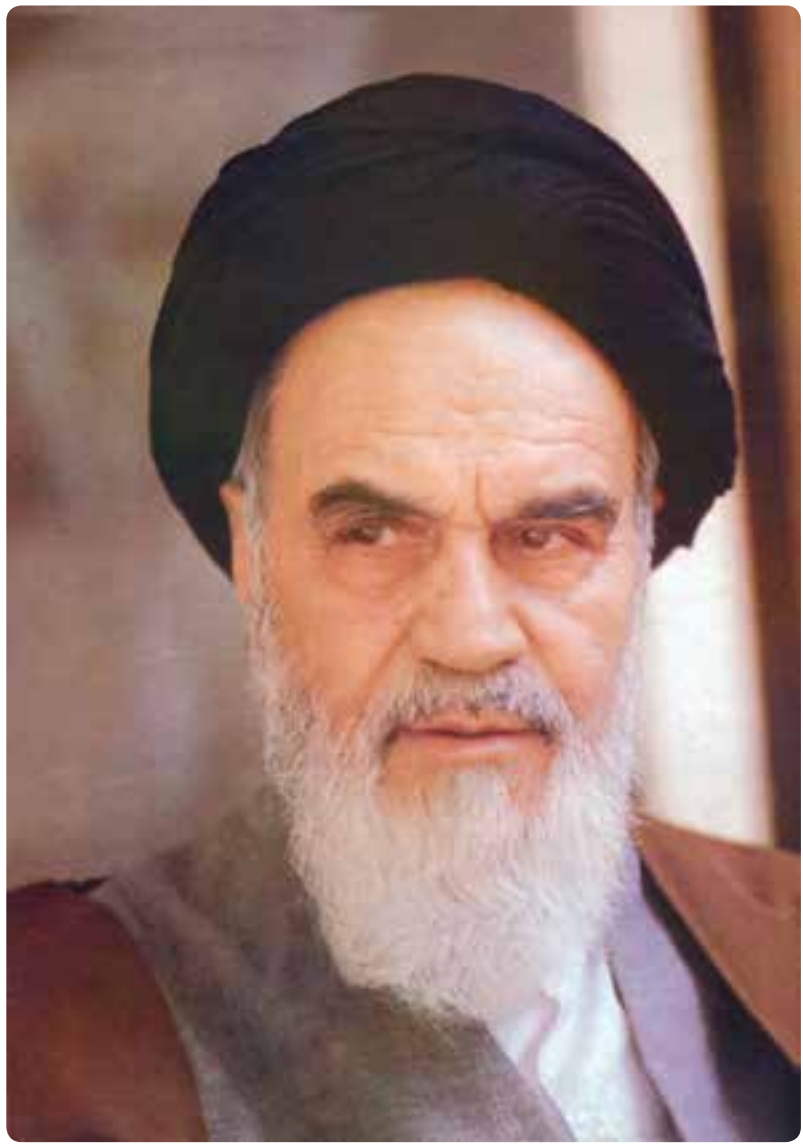
ناشر : **شرکت چاپ ونشر کتاب‌های درسی ایران : تهران ـ کیلومتر ۱۷ جادّهٔ مخصوص کرج ـ خیابان ۶۱ (دارو پخش)**

تلفن : ۵ ـ ۴۴۹۸۵۱۶۱، دورنگار : ۴۴۹۸۵۱۶۰، صندوق پستی : ۱۳۹ـ۳۷۵۱۵

چاپخانه : **شرکت چاپ و نشر کتاب‌های درسی ایران «سهامی خاص»**

سال انتشار و نوبت چاپ : **چاپ هفتم ۱۳۹۲**

شابک ۴-۱۵۰۹-۰۵-۹۶۴ ISBN 964-05-1509-4



شما عزیزان کوشش کنید که از ایـن وابستگی بیرون آیید و احتیاجات کشور خـودتان را بـرآورده سازید، از نیروی انسانی ایـمانی خـودتان غافل نباشید و از اتّکای به اجانب بپرهیزید.

امام خمینی «قدّس سرّه الشّریف»

فهرست

مقدمه

کتاب شبکه‌های رایانه‌ای شامل دو بخش مفاهیم شبکه و سیستم عامل Server ۲۰۰۸ Windows است که توصیه ما به هنرآموزان محترم، تدریس موازی این دو بخش در کلاس است

بدیهی است که کارکردن با یک سیستم عامل شبکه مانند Windows Server ۲۰۰۸ 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 می‌شود سیستم عامل Windows Server ۲۰۰۸ روی رایانه‌ها نصب شود و هنرجویان بدون اینکه با جنبه‌های فنی این سیستم عامل درگیر شوند در این محیط یا سیستم عامل ویندوز ۷ مطالب را آموزش دیده و فعالیت‌های عملی را اجرا نمایند در برخی از فصل‌ها فعالیت عملی کمی ارایه شده و لازم است هنرآموزان محترم متناسب با امکانات موجود فعالیت‌های عملی مرتبط با موضوع را طراحی و به هنرجویان ارایه نمایند

این کتاب دارای دو بخش تئوری و عملی می‌باشد که رنگ پا صفحه بخش تئوری آبی و بخش عملی و کارگاهی با رنگ سبز مشخص شده است که بخش‌های عملی، فعالیت‌های کارگاهی و بخش‌های مطالعه آزاد جنبه آزمون نظری ندارند

در پایان از کلیه عزیزانی که در تألیف این کتاب، ما را همراهی کرده‌اند، سپاسگزاری می کنیم

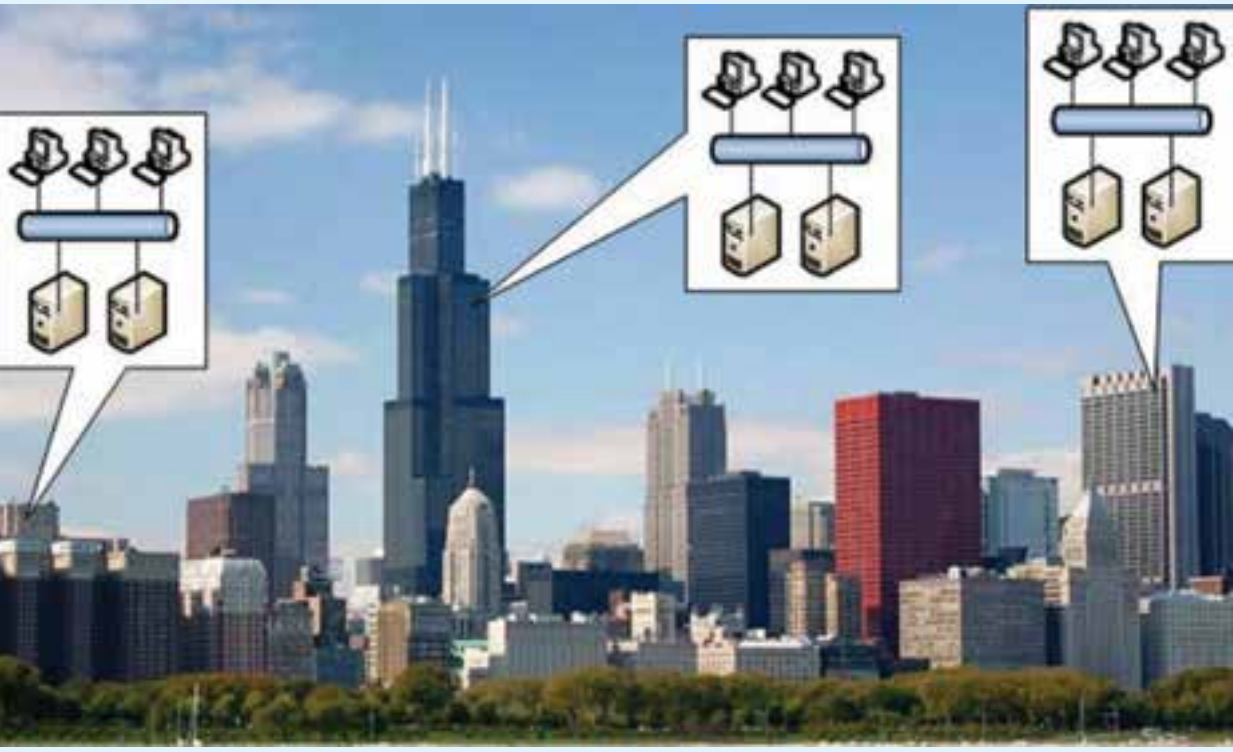
مؤلفان

هدف کلی

شناخت مفاهیم شبکه‌های رایانه‌ای و توانایی نصب شبکه و کار با سیستم عامل متداول شبکه

بخش اول

مفاهیم شبکه



فصل اول

مفاهیم شبکه و اجزای آن

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- هدف از ایجاد شبکه‌های رایانه‌ای را بیان کند.
- اجزای شبکه‌های رایانه‌ای را شرح دهد.
- تقسیم‌بندی شبکه‌های رایانه‌ای از نظر ابعاد و گستردگی فیزیکی را شرح دهد.
- تقسیم‌بندی شبکه‌های رایانه‌ای از نظر مدل سرویس‌دهی را بیان کند.

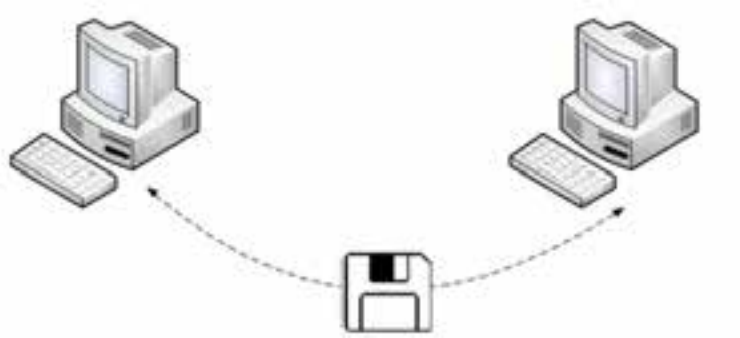
در دههٔ اخیر شبکه‌های رایانه‌ای به عنوان یکی از بسترهای سریع و کم‌هزینه ارتباطی مطرح شده‌اند. این سیر تدریجی منجر به ایجاد روشی شده است که با سازماندهی مناسب آن می‌توان سریع‌تر از هر روش دیگری به اطلاعات مختلف دسترسی پیدا کرد. اطلاعاتی که راه گشای پیوندهای گوناگون فرهنگی، هنری، خانوادگی و اجتماعی، سیاسی، نظامی و همچنین مبادلات اقتصادی و تجاری اعم از خرد و کلان است و می‌دانیم که امروزه در عصر اطلاعات به سر می‌بریم، هر که با هزینه کمتر و سرعت بیشتر بتواند به آن دسترسی پیدا کند موفق‌تر است.

تجارت جهانی روی اینترنت و شبکه‌های رایانه‌ای به سرعت به عنوان مفاهیم کارآمد مطرح می‌شود. فرقی نمی‌کند شما در کدام نقطه از کره زمین قرار دارید. در هر لحظه که اراده کنید می‌توانید اطلاعات مورد نیاز خود را، حتی به صورت صوت و تصویر زنده از شبکه به‌دست آورید. اگر نیاز به تبادل مالی داشته باشید باز هم فرقی نمی‌کند، پول الکترونیکی در دسترس شماست و به‌سرعت می‌توانید با کارت اعتباری خود اقدام به تبادل حفاظت شده ارزی نمایید.

۱ـ۱ـ مقدمه

قبل از این که شبکه‌های رایانه‌ای به وجود بیاید کاربران برای انتقال داده‌ها از دیسکت استفاده می‌کردند (شکل ۱ ۱) و اگر تعداد رایانه‌ها افزایش می‌یافت این موضوع به کاری طاقت فرسا و زمان‌بر

تبدیل می شد و همچنین امکان کارکردن همزمان بر روی یک سند وجود نداشت. یا اگر در یک اتاق کار بیش از یک رایانه وجود داشت، لازم بود به ازای هر رایانه یک چاپگر تهیه شود و یا این که با یک حافظه قابل حمل، سند مورد نظر برای چاپ به رایانه‌ای که متصل به چاپگر می باشد منتقل شود.

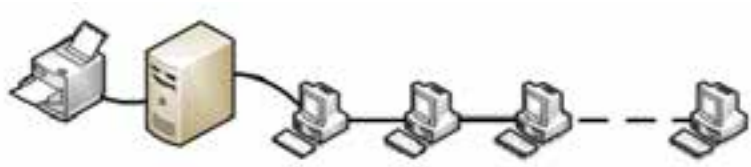


شکل ۱ــ۱ــ انتقال داده‌ها به کمک دیسکت

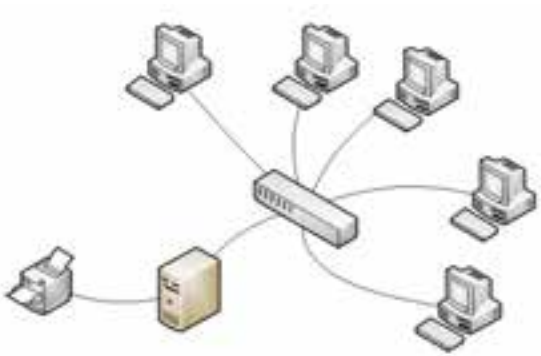
برخی اوقات لازم است به منظور تبادل اطلاعات و استفاده مشترک از منابع سخت افزاری و نرم افزاری، دو یا چند رایانه را به هم متصل کنیم؛ به این ترتیب یک شبکه رایانه‌ای ایجاد می‌شود.

شکل ۲ــ۱ــ ایجادشبکه‌های رایانه‌ای

منابع سخت افزاری می‌تواند شامل : چاپگر، درایو نوری و ... باشد و از مهمترین منابع نرم‌افزاری می‌توان به پوشه، پرونده‌ها و یا مستندات، صفحات اینترنتی و نرم‌افزارها اشاره کرد.



شکل ۳ــ۱ــ استفاده مشترک از منابع سخت افزاری



شکل ۴ــ۱

۲ــ۱ــ مزایای استفاده از شبکه‌های رایانه‌ای

مزایای استفاده از یک شبکه رایانه‌ای عبارت است از :

ــ اشتراک منابع[۱] نرم افزاری و سخت افزاری

ــ ارتباط بر خط[۲] : امکان تبادل پیغام و ارسال پرونده به صورت برخط یا آنلاین

ــ مدیریت و پشتیبانی متمرکز

ــ صرفه‌جویی در زمان و هزینه

فعالیت عملی

الف ــ اشتراک منابع : از طریق شبکه به رایانه سرویس دهنده متصل شده، پوشه و چاپگر به اشتراک گذاشته شده را ببینید.

راهنمایی : ابتدا هنرآموز درس یک پوشه و یک چاپگر را در یکی از سیستم عامل‌های ۲۰۰۰، 7، ۲۰۰۳ یا ۲۰۰۸ به اشتراک می گذارد.

ب ــ تبادل پیغام : حداقل یکی از برنامه های زیر را با تایپ نام برنامه در کادر گزینه RUN در ویندوز XP برای انتقال و پیغام آزمایش کنید :

WinChat.exe

NetMeeting (config.exe)

Command Prompt > net send

۱ــ Shar ng Resources

۲ــ On ne Commun cat on

راهنمایی : فرم کلی فرمان به صورت زیر است :

NET SEND {name * /DOMAIN[: name] /USERS} message

name : نام رایانه[1] مقصد (از آدرس IP[2] رایانه مقصد هم می‌توانید استفاده نمایید).

* : تمام افراد داخل شبکه.

/DOMAIN [: name] : در بخش Windows Server2008 تشریح خواهد شد.

/USERS : ارسال برای تمام کاربران متصل به سرور.

Message : متن پیغام

نکته ۱: علامت به معنی یا می باشد یعنی داخل { } شما فقط یکی از اجزای داخل آن را می‌توانید استفاده نمایید.

نکته ۲: اگر در هنگام ارسال پیغام با خطا مواجه شدید باید سرویس Messenger را فعال کنید (هم در رایانه مبدأ و هم در رایانه مقصد)

برای فعال کردن سرویس Messenger ابتدا از مسیر برنامه Services را اجرا کنید.

Start → Control Panel → Administrative Tools → Services

در پنجره Services در ستون Name برنامه Messenger را اجرا کنید در کادر ظاهر شده از بخش Startup Type : گزینه Automatic را انتخاب نمایید حال بر روی دکمه Start برای فعال کردن سرویس Messenger کلیک نمایید. و در انتها برای تأیید نهایی بر روی دکمه OK کلیک نمایید.

مثالی برای ارسال یک پیغام "How are you?"برای رایانه‌ای در شبکه به نام computer1

Net send computer1 How are you?

۱ــ برای پیدا کردن نام رایانه ابتدا بر روی My Computer کلیک راست نموده و سپس گزینه Computer Name را انتخاب نمایید.

۲ــ برای پیدا کردن آدرس IP کارت شبکه بر روی آیکن کارت شبکه در System Tray کلیک راست نموده و سپس گزینه Status را انتخاب نمایید و سپس بر روی زبانه Support کلیک کنید.

برای ارسال به تمام افراد شبکه

Net send* How are you?

در ویندوز 7، به جای فرمان Net send از فرمان msg استفاده می‌شود.

MSG {username sessionname sessionid @filename *}

[SERVER: servername] [/TIME: seconds] [/V] [/W] [message]

User name : نام کاربر موجود در شبکه (اگر نام کاربر رایانه خودتان را بنویسید پیغام برای شما ظاهر خواهد شد.)

Sessionname : نام ارتباط (اگر از ارتباط Console استفاده کنید پیغام برای رایانه خودتان نمایش داده می‌شود.)

Sessionid : شماره ارتباط (جلسه) (که برای رایانه خودتان عدد ۱ می‌باشد.)

@filename : نام فایل حاوی لیست کاربران، نام جلسه و IDها

* : تمام افراد داخل شبکه

/ SERVER [: name] : نام سرور (اگر ننویسید همان شبکه‌ای که در آن هستید در نظر می‌گیرد.)

/TIME: seconds : تعیین مدت زمانی که پیغام شما بر روی صفحه گیرنده نمایش داده شود (برحسب ثانیه). اگر از این سوئیچ استفاده نکنید تا ۶۰ ثانیه پیغام بر روی صفحه گیرنده باقی خواهد ماند.

/ V : نمایش اطلاعات در حال اقدام برای فرستنده

/ W : منتظر تأییدیه دریافت از گیرنده پیغام

Message : متن پیغام (اگر پیام ذکر نشود، منتظر نوشتن پیام می‌ماند و پایان پیام با z ctrl مشخص می‌شود.)

نکته ۱: علامت { } به معنی یا می‌باشد یعنی داخل { } شما فقط یکی از اجزای داخل آن را می‌توانید استفاده نمایید.

مثال ۱ : برای ارسال یک پیغام "How are you?" برای کاربری در شبکه به نام

user01 از فرمان زیر استفاده می‌شود :

msg user01 How are you?

به محض اجرای فرمان فوق در رایانه مقصد یک کادر که حاوی پیغام و نام فرستنده به همراه زمان ارسال ظاهر می‌شود.

مثال ۲ : برای ارسال به تمام افراد شبکه

msg* How are you?

مثال ۳ : ارسال پیغام Please Call به کاربر User01 به طوری‌که پیغام بر روی صفحه گیرنده فقط ۵ ثانیه نمایش داده می‌شود.

msg user01/time: 5 Please Call

مثال ۴ : ارسال پیغام Please Call به تمام کاربران به طوری‌که پیغام بر روی صحفه گیرنده‌ها فقط ۵ ثانیه نمایش داده شود و برای فرستنده نیز مشخصات ارسال نمایش داده شود.

msg */time: 5 /V Please Call

ج ــ مدیریت از راه دور : به کمک هنرآموز درس، یکی از برنامه‌های Dameware، Radmin، Ideal Administrator یا Net Support را اجرا کرده و مدیریت از راه دور شبکه را مشاهده و بررسی نمایید.

۳ــ۱ــ اجزای یک شبکه رایانه‌ای

شبکه‌های رایانه‌ای از اجزای زیر تشکیل می‌شوند :

ــ رایانه سرویس دهنده (Server)

ــ رایانه سرویس گیرنده (Client)

ــ محیط انتقال[۱] (کانال ارتباطی) (که می تواند سیمی[۲] و یا بی‌سیم[۳] باشد)

ــ سیستم عامل شبکه[۴]

ــ پروتکل (Protocol)

۱ــ Commun cat on Med a or Network Med a

۲ــ W re

۳ــ W re ess

۴ــ Network Operat ng System

در یک شبکه رایانه‌ای معمولاً یک رایانهٔ سرویس دهنده و یک یا چند رایانهٔ سرویس گیرنده بر اساس پروتکل[1] خاصی با یکدیگر به تبادل اطلاعات می‌پردازند و یا از منابع مشترک استفاده می‌کنند.

- **رایانه سرویس گیرنده** : رایانه‌ای است که درخواست استفاده از منابع موجود در شبکه را دارد که به رایانه‌های Workstation یا ایستگاه کاری نیز معروف هستند.
- **رایانه سرویس دهنده** : رایانه‌ای است که به درخواست رایانه‌های سرویس گیرنده پاسخ می‌دهد و منابع را با آنها به اشتراک می‌گذارد؛ مثلاً اجازه استفاده از چاپگر شبکه را به رایانهٔ سرویس‌گیرنده می‌دهد. همچنین مدیریت سرویس گیرنده‌ها را نیز بر عهده دارد.
- **پروتکل** : وقتی که شما بخواهید یک بسته پستی را برای شخص خاصی ارسال کنید، ابتدا باید بسته بندی آن را انجام داده و آدرس گیرنده و فرستنده را در محل خاصی بر روی بسته درج نموده و سپس به یک باجه پستی مراجعه نمایید همانطور که ملاحظه می‌کنید ارسال بسته پستی طبق مقررات و قوانین خاصی انجام می‌گیرد، به قوانین حاکم بر ارسال بسته‌های پستی پروتکل پستی می‌گویند. با توجه به مطالب فوق می‌توان گفت «مجموعه قوانینی که با رعایت آنها سرویس دهی در شبکه برقرار می شود پروتکل در شبکه می‌گویند.» در واقع می‌توان گفت که پروتکل؛ شیوه تقسیم بندی، ارسال و جمع بندی مجدد بسته‌های اطلاعاتی و زمان تبادل اطلاعات را کنترل می‌کند.
- **سیستم عامل شبکه** : برای مدیریت شبکه باید نرم افزار سیستم عامل قابلیت پشتیبانی از شبکه را داشته باشد و سیستم عامل شبکه، سیستم عاملی است که کنترل و مدیریت فعالیت‌های رایانه‌های موجود در شبکه را به منظور دستیابی به منابع مشترک و تبادل اطلاعات بر عهده دارد. سیستم عامل شبکه در بخش Windows Server 2008 این کتاب به طور کامل تشریح می شود.

۴ـ۱ـ تقسیم بندی شبکه‌های رایانه‌ای از نظر ابعاد و گستردگی فیزیکی

برای تقسیم‌بندی شبکه‌ها به لحاظ فاصله رایانه‌ای می‌توان آنها را به دو گروه عمده LAN[2] و WAN[3] تقسیم بندی نمود، ولی دو نوع دیگر تقسیم بندی به نام‌های CAN و MAN نیز وجود دارد که در این بخش به تشریح هر کدام از آنها می‌پردازیم.

- **شبکه‌های محلی یا LAN** : شبکه محلی پایه شبکه‌های دیگر است و کوچکترین فرم شبکه

۱ـ پروتکل رایج شبکه‌های رایانه‌ای TCP/IP می‌باشد که متعاقباًتشریح خواهد شد.

۲ـ Loca Area Network

۳ـ W de Area Network

می‌باشد. در شبکه محلی فاصله رایـانه ها نسبت به هم کم می‌بـاشد. شبکه محلی می‌توانـد از دو تـا چندصد رایانه با فاصله کم تشکیل شود.

در زیر چند نمونه از شبکه محلی آورده شده است :

الف) شبکه‌ای متشکل از دو رایانه با فاصله‌ای کمتر از ۱۰۰ متر

ب) شبکه رایانه‌های یک اداره واقع در یک ساختمان متشکل از ۱۰۰ رایانه

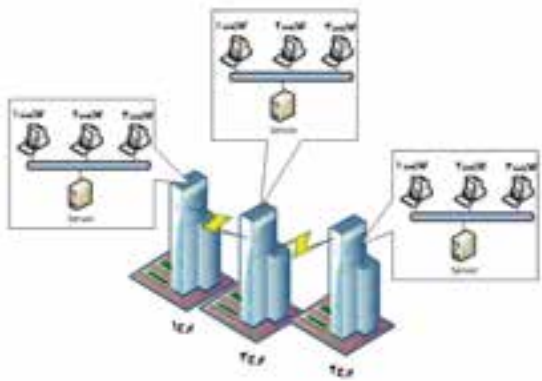
ج) شبکه رایانه‌ای یک برج ۵۰ طبقه با بیش از ۵۰۰ گره فعال[۱]

د) شبکه رایانه‌های موجود در کارگاه رایانه‌ای که شما در هنرستان از آن استفاده می‌کنید با ۲۰ رایانه.

شکل ۵ــ۱ــ شبکه های محلی یا LAN

• **شبکه دانشگاهی یا CAN**[۲] : شبکه‌ای که از چند شبکه محلی مجاور هم تشکیل شده است و معمولاً در محیط دانشگاهی یا محیط پادگان نظامی یا کارخانه‌های بزرگ مورد استفاده قرار می‌گیرد. در بعضی از برگردان‌ها به آن شبکه پردیس نیز می گویند.

در شکل ۶ــ۱ نمونه‌ای از شبکه CAN آورده شده است.



شکل ۶ــ۱ــ شبکه‌های دانشگاهی یا CAN

۱ــ هر وسیله‌ای که به یک شبکه رایانه‌ای متصل می‌شود، یک گره فعال یا Act ve Node نامیده می‌شود و می‌تواند یک رایانه و یا یک چاپگر یا ... باشد.

۲ــ Campus Area Network

شبکه رایانه‌های دانشگاه تهران از نوع CAN می‌باشد.

شبکه کارخانه ایران خودرو نیز از نوع CAN می‌باشد (ایران خودرو دارای فضای وسیعی است که دارای چندین سوله و واحدهای مختلف می‌باشد).

• **شبکه شهری یا MAN**[1] : شبکه‌ای که از چند شبکه محلی غیر مجاور در سطح یک شهر تشکیل شده باشد، یک شبکه شهری یا MAN می‌باشد. بر فرض شهری دارای سه منطقه آموزش و پرورش می‌باشد و بخواهیم سه منطقه آموزش و پرورش به هم متصل شوند نوع شبکه ایجاد شده، از نوع شبکه شهری می‌باشد به عنوان مثال دیگر اگر هنرستان های یک شهر به یکدیگر متصل شوند، باز هم شبکه ایجاد شده از نوع MAN می‌باشد.

در تصویر زیر نمونه‌ای از شبکه MAN آورده شده است.

شکل ۷ــ۱ــ شبکه‌شهری یا MAN

• **شبکه گسترده (وسیع) یا WAN**[2] : بزرگترین نوع شبکه به لحاظ وسعت بوده و معمولاً فضایی بزرگتر از یک شهر را در برمی‌گیرد و می‌تواند از نظر وسعت و فاصله در یک استان، کشور، قاره و یا کل جهان قرار بگیرد. یک شبکه گسترده یا WAN می‌تواند از ترکیب دو رایانه با فاصله دور تشکیل شود که از طریق خطوط تلفن با هم ارتباط دارند و یا این که از ترکیب دو یا چند شبکه LAN با فاصله دور و یا ترکیبی از چند شبکه MAN به وجود آمده باشد. به عبارت دیگر می‌توان گفت شبکه WAN به لحاظ وسعت جغرافیایی محدودیتی ندارد. کانال ارتباطی در این شبکه ها اغلب امواج مایکروویو یا ماهواره و خطوط مخابرات می باشد. به عنوان نمونه از شبکه‌های گسترده یا WAN

۱ــ Metropo tan Area Network

۲ــ W de Area Network

می‌توان به موارد زیر اشاره کرد :

ـ شبکه اینترنت بزرگترین شبکه گسترده WAN می باشد.

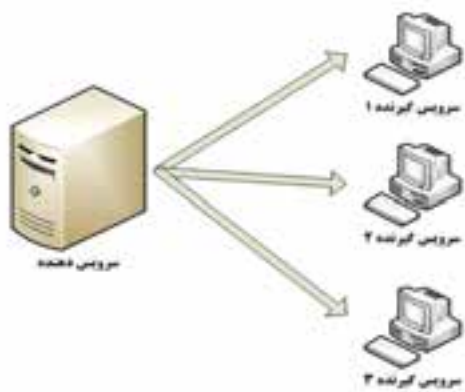
ـ شبکه بین شعب بانک‌های کشور، یک شبکه گسترده یا WAN می‌باشد.

ـ شبکه بین هنرستان‌های یک استان نیز یک شبکه گسترده یا WAN می‌باشد.

۵ـ۱ـ تقسیم‌بندی شبکه‌های رایانه‌ای از نظر مدل سرویس‌دهی

از نظر مدل سرویس‌دهی، شبکه‌ها را می‌توان به دو دسته زیر تقسیم نمود :

الف) شبکه مبتنی بر سرویس دهنده یا Server Base (SB) : در یک شبکه Server Base ساده یک رایانه فقط نقش سرویس دهنده را داشته و مابقی سیستم های شبکه در نقش سرویس گیرنده ظاهر می‌شوند و در شبکه های بزرگتر تعدادی از سیستم ها فقط نقش سرویس دهنده را دارند و سایر سیستم ها نقش سرویس گیرنده را دارند.



شکل ۸ـ۱ـ شبکه‌مبتنی بر سرویس‌دهنده SB

شبکه SB برای استفاده در شبکه‌های متوسط و بزرگ مناسب می باشد.

در شبکه SB رایانه سرویس دهنده نمی تواند به عنوان سرویس گیرنده نیز مورد استفاده قرار گیرد. در شبکه های بزرگ به بیش از یک سرویس دهنده نیاز می‌باشد به طوری که به هر سرویس دهنده یک سرویس خاص محول می شود. انواع سرویس‌ها در بخش Windows Server 2008 تشریح خواهد شد.

سیستم عامل‌های SB، از انواع خاصی می‌باشند مانند Novell و ویندوزهای سرور مایکروسافت

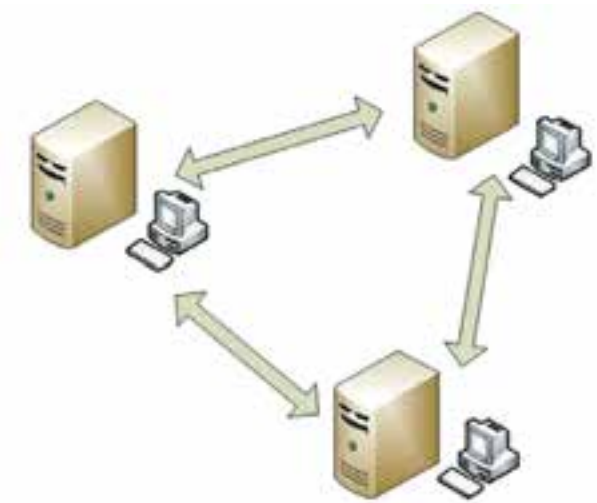
نصب، پیکربندی و مدیریت سیستم عامل های شبکه SB پیچیده بوده و نیاز به متخصص دارد ولی مزایای زیادی نسبت به PtP دارد.

یکی دیگر از مزایای SB بالا بودن امنیت در شبکه می‌باشد چون یک مدیر، سیاست‌های کلی را تعیین می‌کند و برای کلیه کاربران شبکه اعمال می‌کند.

در شبکه SB می‌توان هزاران کاربر یا سرویس گیرنده داشت. به طوری که سرویس گیرنده‌ها نیازی به داشتن سخت افزار قوی به لحاظ RAM و CPU ندارند.

یکی از معایب بزرگ شبکه SB این است که چنانچه سرویس‌دهنده دچار مشکل شود، سرویس‌دهی در کل شبکه دچار اختلال می شود . البته این عیب با پیش‌بینی‌های مناسب قابل حل می‌باشد که در بخش Windows Server 2008 تشریح خواهد شد.

ب) شبکه نظیربه نظیر یا Peer to Peer (PtP) : تمام رایانه‌ها به لحاظ سرویس دهنده بودن و سرویس گیرنده بودن با هم برابرند یعنی هر رایانه به طور همزمان هم سرویس دهنده و هم سرویس گیرنده می باشد و کاربران هر رایانه می‌توانند داده های خود را در شبکه به اشتراک بگذارند.



شکل ۹ــ۱ــ شبکه نظیر به نظیر PtP

به لحاظ اندازه شبکه به شبکه‌های PtP غالباً Workgroup یا گروه کاری می‌گویند. گروه کاری، گروه کوچکی از افراد می باشند، حدود ۱۰ رایانه یا کمتر که تشکیل شبکه PtP را می‌دهند.

شبکه PtP به نسبت شبکه ساده‌ای است زیرا هر رایانه هم می‌تواند نقش سرویس‌دهنده و هم

نقش سرویس گیرنده را داشته باشد و سرور مرکزی برای مدیریت شبکه وجود ندارد. و به لحاظ راه‌اندازی، هزینه کمتری نسبت به شبکه SB خواهد داشت. از بیشتر سیستم عامل‌های موجود می‌توان در شبکه PtP استفاده نمود و به نرم افزار خاصی برای کار با شبکه نیاز ندارند ولی امکان رشد در آن خیلی محدود می باشد.

در شبکه PtP هر کاربر مدیر خودش می‌باشد و چون مدیریت متمرکز وجود ندارد چنانچه مشکلی برای یکی از رایانه ها به‌وجود آید کل شبکه را دچار اختلال نمی‌کند.

برای جایی که تعداد رایانه‌ها کمتر از ۱۰ دستگاه می‌باشند، شبکه ptp انتخاب خوبی می‌باشد کاربران می‌توانند منابع خود را به اشتراک بگذارند.

در تمام سیستم عامل های موجود می توان از شبکه PtP استفاده نمود.

فعالیت عملی

هنرجویان ابتدا با کاربر Administrator وارد ویندوز شوند سپس پوشه‌ای را به دلخواه به اشتراک بگذارند و امکان دسترسی را به سایر رایانه‌های موجود در شبکه بدهند.

۶ـ ۱ـ انواع شبکه‌های بی‌سیم

شبکه‌های بی‌سیم با توجه به مسافتی که می‌توانند اطلاعات را تبادل کنند به چند گروه تقسیم می‌شوند :

(WWANs)[۱] : شبکه WAN به صورت بی‌سیم است که به وسیله سیستم ماهواره‌ای یا آنتن‌هایی که در جاهای مختلف نصب شده ارتباط را برقرار می‌کند. به عنوان مثال سیستم ارتباطی تلفن‌های همراه بر مبنای WWANs است.

(WMANs)[۲] : این شبکه ساختاری شبیه WWANs دارد با این تفاوت که وسعت سرویس‌دهی آن فقط در سطح شهرها است. در حال حاضر شبکه‌های WMANs می‌توانند به عنوان یك پشتوانه (Backup) برای شبکه‌های سیم مسی یا فیبر نوری مورد استفاده قرار گیرند. معمولاً WMANs از امواج رادیویی و نور مادون قرمز برای انتقال اطلاعات استفاده می‌کنند.

۱ـ W re ess W de Area Networks

۲ـ W re ess Metropo tan Area Networks

(WLANs)[1] : این فناوری برای استفاده در محیط های کوچک مانند شرکت‌ها یا فضای باز دانشکده‌ها یا اماکن عمومی با وسعت کم (مانند فرودگاه) می‌باشد. از این نوع فناوری بیشتر به‌صورت موقتی در ادارات و شرکت‌ها یا محل‌هایی که نصب سیم مسی سخت می‌باشد استفاده می‌شود. در جاهایی که کاربران محل مشخص و ثابتی را ندارند و می‌خواهند به همه اطلاعات دسترسی داشته باشند و یا این‌که کاربران از رایانه کیفی یا جیبی استفاده می‌کنند بسیار مناسب است.

WLANs به دو صورت مختلف مورد استفاده قرار می‌گیرد. در حالت اول رایانه‌های مجهز به کارت شبکه بی‌سیم (External، Internal) به دستگاه اکسس پوینت[2] متصل می‌شوند و دستگاه اکسس پوینت پل ارتباطی بین رایانه‌های بی‌سیم و شبکه داخلی موجود خواهد بود در این حالت کلیه رایانه‌های بی‌سیم علاوه بر ارتباط با یکدیگر به شبکه داخلی هم متصل می‌باشند. ولی در حالت دوم رایانه‌های مجهز به کارت شبکه بی‌سیم به صورت نظیر به نظیر به یکدیگر متصل می‌شوند و در این حالت ارتباط با شبکه داخلی وجود ندارد (به دلیل عدم استفاده از اکسس پوینت).

مطالعه آزاد

در سال ۱۹۹۷ انجمن IEEE استاندارد 802.11 را برای WLAN به تصویب رساند که از مشخصات آن انتقال داده‌ها با سرعت 1 تا 2Mbps بود. اما با آمدن استاندارد 802.11b سرعت به 11Mbps با فرکانس 2.4 GHz رسید. معمولاً شبکه‌هایی از این استاندارد استفاده می‌کنند ترافیک اطلاعاتی پایینی دارند و بیشتر برای اشتراک‌گذاری اینترنت و برنامه‌های سبک استفاده می‌شود. چرا که معمولاً سرعت اینترنت کمتر از 1Mbps است (البته بستگی به سرویس دهنده دارد.) و با توجه به سرعت این استاندارد به‌راحتی جوابگوی کاربران شبکه خواهد بود. در ضمن قیمت تجهیزاتی که با این استاندارد کار می‌کنند خیلی ارزان است.

استاندارد دیگری به نام 802.11g وجود دارد که در همان محدوده فرکانسی 2.4GHz کار می‌کند و به لحاظ سرعت بالایی که دارد، معمولاً برای عملیات اشتراک‌گذاری پرونده‌ها و اشتراک اینترنت مورد استفاده قرار می‌گیرد. سرعت این استاندارد 108Mbps است.

۱ــ W re ess Loca Area Networks

۲ــ Access Po nt

امروزه استاندارد 802.11a زیاد مورد استفاده قرار می‌گیرد. این استاندارد در محدوده فرکانسی 5.0GHz کار می‌کند و سرعت آن تا 108Mbps در ثانیه است و ترافیک بالای اطلاعاتی را به راحتی پشتیبانی می‌کند. در شرایطی از این استاندارد استفاده می‌شود که ترافیک اطلاعاتی روی فرکانس 2.4GHz زیاد باشد و دستگاه‌ها قادر به برقراری ارتباط روی این فرکانس نباشند. به عنوان مثال در مرکز شهر تهران در طول ۵ سال گذشته به دلیل این که بسیاری از مراکز برای برقراری ارتباط از دستگاه‌هایی با استاندارد 802.11b، 802.11g استفاده می‌کردند در حال حاضر محدوده فرکانسی 2.4GHz کامل یا اشباع است. و اگر کسی بخواهد ارتباط رادیویی بین دو شرکت در این محدوده وارد کند باید از استاندارد 802.11a استفاده کند.

نکته: قبل از استفاده از کارت شبکه بی‌سیم یا اکسس پوینت باید استاندارد آن بررسی شود چرا که کارت شبکه‌ای که فقط استاندارد 802.11b را پشتیبانی می‌کند قادر به برقراری ارتباط با کارت‌ها و یا تجهیزاتی که این استاندارد را پشتیبانی نمی‌کنند نیست.

آخرین استانداردی که انجمن IEEE برای ارتباط WLAN در سال ۲۰۰۸ ایجاد کرده 802.11n است. در واقع دستگاهی که این استاندارد را پشتیبانی کند می‌تواند با کلیه استانداردهای 802.11a/b/g ارتباط برقرار کند، سرعت برقراری ارتباط در این نوع از شبکه‌ها در بهترین شرایط به 300Mbps می‌رسد.

(WGAN)[1] : این شبکه مانند شبکه تلفن جهانی کنونی عمل می‌کند و کاربران می‌توانند در حالی که بین کشورها مسافرت می‌کنند متصل به شبکه باقی بمانند. از مزایای این شبکه دارا بودن پهنای باند کافی برای دسترسی به اینترنت است.

(WPANs)[2] :این فناوری قادر می‌سازد تا کاربران به صورت AD HOC با یکدیگر ارتباط برقرار کنند. AD HOC استانداردی است که ارتباط بی‌سیم بین رایانه و تجهیزات جانبی، مانند رایانه جیبی PDAs یا تلفن همراه و رایانه کیفی را برقرار می‌کند.

۱ــ W re ess G oba Area Networks

۲ــ W re ess Persona Area Networks

منظور از Personal Area در این فناوری فضایی حدود ۱۰ متر در اطراف رایانه شخصی یا رایانه کیفی است.

این نوع فناوری بیشتر برای اهداف خاص و از پیش تعیین شده استفاده می‌شود. به عنوان مثال یک رایانه مجهز به کارت شبکه بی‌سیم می‌تواند به‌صورت AD HOC اینترنت را به رایانه کیفی یا PDA منتقل کند یا تبادل اطلاعات داشته باشد در حال حاضر دو نوع فناوری WPANs به نام‌های بلوتوث (Bluetooth) و مادون قرمز (Infrared) وجود دارد.

مادون قرمز : در این فناوری از امواج مادون قرمز برای انتقال اطلاعات استفاده می‌شود. هر دو دستگاه فرستنده و گیرنده مجهز به این فناوری باید در دید مستقیم یکدیگر باشند و حداکثر فاصله آن‌ها نباید بیشتر از یک متر باشد. امروزه از این فناوری کمتر استفاده می‌شود. مادون قرمز فقط برای فضای کمتر از پنج متر طراحی شده و در صورت وجود مانع بین فرستنده و گیرنده سرعت انتقال اطلاعات کم شده یا حتی ارتباط قطع می‌شود. از فناوری مادون قرمز بیشتر در ساخت صفحه کلید و ماوس استفاده می‌کنند که فرستنده و گیرنده در فاصله کمی نسبت به هم قرار دارند.

بلوتوث : این فناوری جایگزین انتقال کابلی داده‌ها در فاصله کوتاه شده است و برای این کار از امواج رادیویی استفاده می‌کند و می‌تواند اطلاعات را تا مسافت ۱۰۰ متر انتقال دهد. امواج رادیویی می‌تواند از موانعی متعدد مانند دیوار و کیف دستی به راحتی عبور کند لذا داده‌ها در موقعیت‌هایی که بین آن‌ها موانعی قرار دارد به راحتی با این فناوری قابل انتقال است. از فناوری بلوتوث برای ارتباط بین تلفن همراه، رایانه جیبی، چاپگر و ... در فاصله‌های کم مورد استفاده می‌شود.

به طور کلی هدف اصلی طراحی فناوری بلوتوث حذف کابل ارتباطی مابین رایانه با تجهیزات جانبی مانند چاپگر، صفحه کلید ، ماوس، دوربین و ... می‌باشد. در طراحی این فناوری همواره سعی بر این بوده که این دستگاه از لحاظ قیمت و اندازه و توان مصرفی در حداقل باشد و به راحتی در دسترس همگان باشد.

اگرچه طراحی و تولید تجهیزات بی‌سیم قبل از ساخت فناوری بلوتوث بوده است اما امروزه مبنای طراحی همه تجهیزات بی‌سیم مطابق با استاندارد بلوتوث می‌باشد. مانند هدفون‌های بی‌سیم[۱] که برای تلفن همراه و رایانه استفاده می‌شود یا ارتباط اینترنتی مانند Internet bridges.

اگر چه امروزه فناوری بلوتوث با شبکه‌های بی‌سیم همواره در حال رقابت است اما بلوتوث فقط برای مسافت‌های کوتاه طراحی شده و به هیچ وجه برای مسافت‌های طولانی مورد استفاده قرار نمی‌گیرد.

۱ـ W re ess headsets

کاربردهای بلوتوث

هدست بلوتوث Headset : این دستگاه به‌راحتی قادر است با رایانه یا تلفن همراهی که روی آن تنظیم شده است ارتباط صوتی برقرار کند. با توجه به این‌که تلفن همراه معمولاً در هنگام روشن بودن و صحبت کردن در نزدیکی سر انسان قرار دارد. ممکن است تشعشعات تلفن همراه برای ما مضر باشد. البته صحت این موضوع در حال بررسی و تحقیق است.

پل ارتباطی اینترنت Internet Bridge : اگر تلفن همراه مجهز به بلوتوث باشد از طریق سرویس Dial Up Networking (DUN) می‌توان با اینترنت ارتباط برقرار کرد و سپس رایانه‌ای که از طریق بلوتوث به تلفن همراه متصل است می‌تواند از اینترنت استفاده کند بدون این‌که به دستگاه مودم متصل باشد.

تبادل اطلاعات File exchange : در این روش تبادل اطلاعات به‌صورت نظیر به نظیر انجام می‌شود. زمانی که بلوتوث رایانه فعال شود به طور خودکار شروع به شناسایی سایر دستگاه‌های نزدیک به خود می‌کند و بعد از صدور مجوز از طرف ارسال کننده اقدام به ارسال اطلاعات می‌کند.

چاپ (Printing) : بعضی از چاپگرها مجهز به این فناوری هستند. رایانه‌ها و تلفن‌های همراه می‌توانند با شناسایی این چاپگرها اقدام به چاپ اسناد و پرونده‌ها به چاپگر مزبور نمایند.

جدول ۱ــ۱ــ انواع بلوتوث از نظر برد و توان مصرفی

توان دستگاه	محدوده دسترسی
۱ میلی‌وات	۱ متر
۱ میلی وات	۱ متر

خودآزمایی و پژوهش

۱ــ شبکه اینترنت از نظر سرویس دهی به کدام دسته شبکه‌های رایانه‌ای تعلق دارد؟

۲ــ در تقسیم بندی شبکه‌های رایانه‌ای از نظر گستردگی فیزیکی، سیستم بانکی شتاب به کدام دسته تعلق دارد؟

ــ سرویس‌های رایج در شبکه‌های رایانه‌ای را نام ببرید.

فصل دوم

سیستم‌های انتقال اطلاعات

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- روش ارسال اطلاعات به صورت موازی را بیان کند.
- روش‌های ارسال اطلاعات به صورت سری را شرح دهد.
- انواع روش‌های انتقال اطلاعات براساس جهت آنها را تعریف کند.
- سیگنال‌های اطلاعات و انواع آن را شرح دهد.
- پهنای باند را تعریف کند.
- نویز و انواع آن را شرح دهد.

یکی از مسایل مهم در شبکه‌های رایانه‌ای انتقال اطلاعات در کانال‌های ارتباطی (سیم، کابل، رسانه انتقال) است. در این کانال‌ها بین دستگاه فرستنده و دستگاه گیرنده شیوه‌های مختلف ارسال وجود دارد. می‌توان این پرسش‌ها را مطرح کرد که آیا روش ارسال به‌صورت بیت به بیت و جداگانه باشد یا گروهی از اطلاعات با هم ارسال شوند یا این پرسش که آیا فرستنده آنها را همانند یک ایستگاه فرستنده رادیویی ارسال نماید یا از روشی که در مخابرات برای انتقال صوت به کار می‌رود، استفاده شود. از این رو انتقال اطلاعات را می‌توان براساس پارامترهای مختلفی دسته‌بندی کرد :

- مد انتقال
- همزمانی و غیر همزمانی
- جهت انتقال اطلاعات

۱ـ ۲ـ مد انتقال

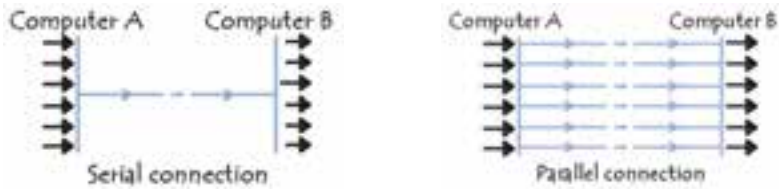
تعداد بیت‌هایی که به طور همزمان از طریق کانال ارتباطی ارسال می‌شوند را مد انتقال می‌نامند. در این حالت ارسال اطلاعات به دو صورت می‌باشد.

■ پشت سرهم (Serial)

■ موازی (Parallel)

در ارسال سریال، بیت‌ها به‌صورت تک به تک و پشت سر هم انتقال می‌یابند. برای کنترل بیت‌ها،ابتدا و انتهای بیت‌ها با یک سری علامت به نام‌های بیت شروع[1] و بیت پایان[2] مشخص می‌شود که در روش‌های مختلف ارسال سریال محل قرارگیری این علامت‌ها و محتوای آنها متفاوت است.

در روش موازی تعدادی از بیت‌ها (nبیت) به صورت هم زمان و با هم و به صورت گروهی از طریق تعدادی کانال (nکانال) ارسال می‌شوند (شکل ۱ــ۲).



شکل ۱ــ۲ــ ارسال سری و موازی

مطالعه آزاد

۲ــ۲ــ همزمانی و غیر همزمانی اطلاعات

توانایی رایانه‌ها در ارسال و دریافت اطلاعات از نظر سرعت متفاوت است؛ بنابراین ممکن است یک رایانه بتواند در واحد زمان، مقدار بیشتری اطلاعات به سمت رایانه مقصد ارسال کند. بدیهی است در چنین حالتی، رایانه گیرنده که با سرعت کمتری کار می‌کند نمی‌تواند تمامی اطلاعات ارسال شده را دریافت نماید، در نتیجه مقداری از این اطلاعات در شبکه از بین می‌رود، بنابراین رایانه‌هایی که در حال تبادل اطلاعات هستند، همواره سرعت ارسال و دریافت را با هم بررسی کرده، در صورت لزوم سرعت را کم یا زیاد می‌کنند.

در هر دو روش ارسال هم زمان[3] و غیر هم زمان[4]، اطلاعات ابتدا به کدهای دودویی تبدیل می‌شوند، سپس تعدادی بیت که حاوی اطلاعات ارسالی هستند در امتداد

۱ــ Sta t B t

۲ــ Stop B t

۳ــ Synchronous transm ss on

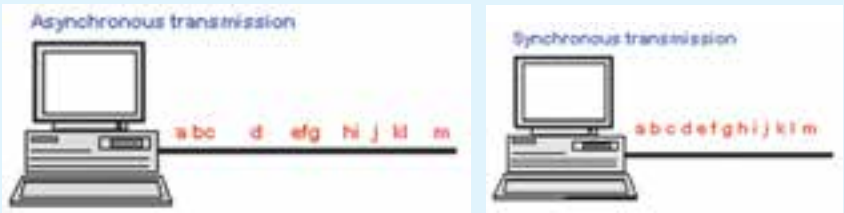
۴ــ Asynchronus transm ss on

یکدیگر قرار گرفته و یک رشته را تشکیل می‌دهند، سپس تعدادی از آنها به هم متصل شده و رشته طولانی‌تری را پدید می‌آورند، پس از آن ابتدا و انتهای این رشته به وسیلهٔ بیت شروع و بیت پایان مشخص می‌شود.

در روش انتقال غیر هم زمان هیچ زمان بندی برای ارسال یا دریافت صورت نمی‌گیرد و کنترل ترافیک به صورت لحظه‌ای انجام می‌شود. به همین دلیل در روش انتقال غیر هم زمان، ۲۵٪ ظرفیت خط انتقال صرف کنترل ترافیک می‌شود. منظور از ظرفیت خط انتقال همان پهنای باند است که در همین فصل توضیح داده شده است.

ولی در روش ارسال هم زمان قبل از شروع ارسال، دو رایانه به‌وسیلهٔ سیستم زمان‌بندی داخلی خود با هم هماهنگ می‌شوند. سپس رایانه ارسال کننده، ارسال را شروع کرده و رایانه گیرنده اطلاعات را دریافت می‌کند.

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



شکل ۲ــ۲ــ انتقال هم‌زمان و غیر هم‌زمان

۳ــ۲ــ جهت انتقال اطلاعات

بین دو واحد فرستنده و گیرنده همیشه اطلاعاتی در حال جابه‌جا شدن است که در محیط‌های مختلف جهت آن متفاوت است. ارتباط براساس جهت‌های انتقال به سه گروه تقسیم می‌شوند :

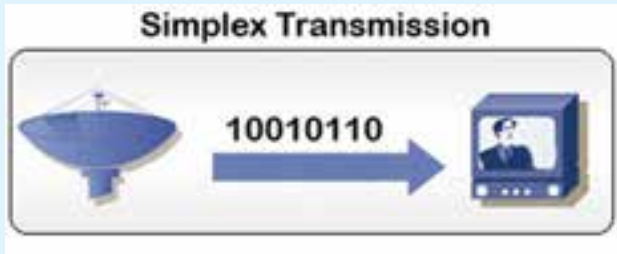
۱ــ یک طرفه[۱]

۲ــ دوطرفه غیرهم زمان[۲]

۳ــ دو طرفه هم زمان[۳]

۱ــ S mp ex ۲ــ Ha f Dup ex ۳ــ Fu Dup ex

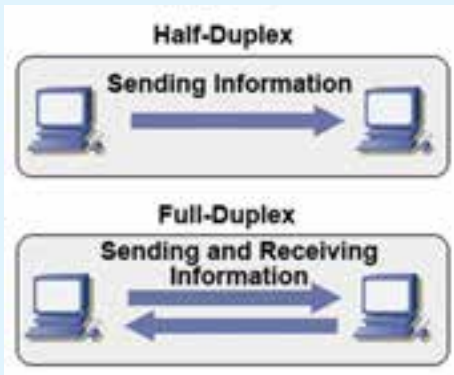
۱ــ۳ــ۲ــ ارتباط یک طرفه : در این روش یک فرستنده ثابت و چند گیرنده ثابت وجود دارد و هیچ‌گاه جای این دو عوض نمی‌شود. در روش یک طرفه، اطلاعات به‌وسیلهٔ فرستنده ارسال و به‌وسیلهٔ گیرنده دریافت می‌شود. برای مثال می‌توان به رادیو یا تلویزیون اشاره کرد. در هر کدام از این سیستم‌ها، اطلاعات توسط یک فرستنده رادیویی یا تلویزیونی ارسال و توسط گیرنده که همان دستگاه رادیو یا تلویزیون است دریافت می‌شود و هیچ‌گاه جهت ارسال تغییر نمی‌کند. به این روش ارسال، یک طرفه می‌گویند.



شکل ۳ــ۲ــ ارتباط یک‌طرفه ساده

۲ــ۳ــ۲ــ ارتباط دو طرفه غیر هم‌زمان یا ناقص : در روش دو طرفه غیر هم‌زمان ارسال دو طرفه ولی غیر هم‌زمان است یعنی دو واحد A و B نمی‌توانند هم‌زمان برای یکدیگر اطلاعات ارسال کنند و این کار باید متناوب انجام شود. در واقع هنگامی که واحد A ارسال‌کننده اطلاعات است، واحد B فقط باید دریافت کننده باشد و برعکس، برای مثال می‌توان به واکی ــ تاکی یا فرستنده ــ گیرنده‌های بی‌سیم اشاره کرد.

۳ــ۳ــ۲ــ ارتباط دو طرفه غیرهم‌زمان یا کامل : در روش دو طرفه هم‌زمان هر دو واحد A و B می‌توانند به صورت هم زمان فرستنده و گیرنده اطلاعات باشند. به طور مثال می‌توان از طریق دو دستگاه تلفن بدون هیچ مشکلی به صورت هم زمان و دو طرفه ارتباط برقرار کرد. انتقال اطلاعات در تلفن، نمونه‌ای از انتقال اطلاعات به صورت دو طرفه هم زمان



شکل ۴ــ۲ــ ارتباط دوطرفه ناقص و کامل

است.

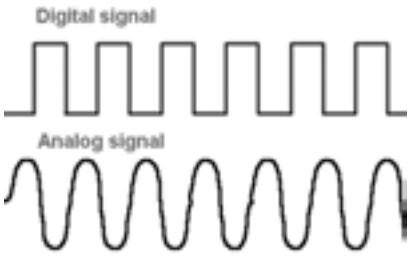
۴ــ۲ــ سیگنال‌های اطلاعات

مفهومی را که به انتقال اطلاعات از نقطه‌ای به نقطه دیگر و همچنین یک‌سری از پالس‌ها در رایانه اشاره می‌کند، سیگنال می‌نامند. امواج رادیویی و ویدیویی نمونه‌ای از این سیگنال‌ها هستند.

سیگنال‌های اطلاعات می‌توانند به دو صورت دیجیتال یا آنالوگ باشند. سیگنال‌های آنالوگ شبیه یک موج هستند که در زمان‌های 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 روی بردار نمایش می‌دهند (شکل ۵ــ۲).

صدای شخصی که در حال صحبت کردن است، نمونه‌ای از یک سیگنال آنالوگ می‌باشد؛ به این صورت که صدا به صورت ممتد تولید شده و بلندی صدا دائماً 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، می‌توانیم به یک لامپ اشاره کنیم که فقط دو وضعیت خاموش



شکل ۵ــ۲ــ نمونه‌ای از شکل تابع موج دیجیتال و آنالوگ

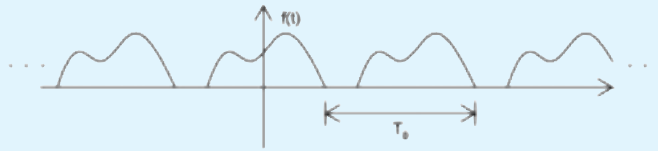
مطالعه آزاد

یا روشن دارد (شکل ۵ــ۲).

۱ــ۴ــ۲ــ سیگنال‌های متناوب (Periodic) و نامتناوب (Aperiodic) :

هر دو نوع سیگنال‌های آنالوگ و دیجیتال به دو فرم متناوب و نامتناوب به کار می‌روند.

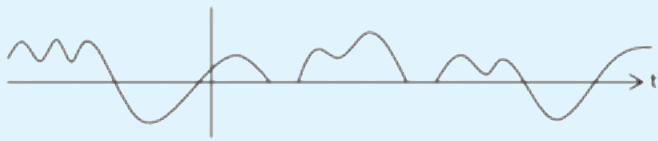
الف) سیگنال‌های متناوب : اگر الگو یا همان شکل سیگنال‌ها در فاصله‌های زمانی مشخص تکرار شود، به آن سیگنال متناوب می‌گویند. در سیگنال‌ها اگر الگو کامل شود و در آستانه تکرار قرار گیرد، به آن یک Cycle یا چرخه می‌گویند یک Period یا



شکل ۶ــ۲ــ شکل موج آنالوگ متناوب

دوره، به مقدار زمانی می‌گویند که یک چرخه یا Cycle در آن اتفاق می‌افتد.

ب) سیگنال‌های نامتناوب: سیگنال‌های نامتناوب الگو و شکل مشخصی



شکل ۷ــ۲ــ شکل موج آنالوگ نامتناوب

ندارند و الگوهای آن در فاصله‌های زمانی مشخص تکرار نمی‌شوند.

۵ــ۲ــ پهنای باند[1]

یکی از مسأله‌هایی که به هنگام طراحی و راه‌اندازی شبکه همواره مورد توجه قرار می‌گیرد و از درجه اهمیت بالایی برخوردار است، پهنای باند می‌باشد. هر سیستم انتقال آنالوگ توانایی محدودی در انتقال امواج دارد؛ بدین‌صورت که پایین‌ترین و بالاترین فرکانسی که یک رسانه برای انتقال اطلاعات استفاده می‌کند، مشخص است؛ به‌طور مثال پایین‌ترین فرکانس ۳۰۰Hz و بالاترین فرکانس ۳۳۰۰Hz است.

واحد سنجش فرکانس هرتز[2] می‌باشد. فاصله بین پایین‌ترین و بالاترین فرکانس، پهنای باند رسانه نامیده می‌شود. رسانه‌ای با مشخصات ذکر شده فقط قادر به ارسال سیگنال‌هایی است که در محدوده بین ۳۰۰ و ۳۳۰۰ هرتز قرار گرفته باشند. در واقع پهنای باند، ظرفیت انتقال اطلاعات به‌وسیلهٔ رسانه است.

از عوامل مؤثر در پهنای باند رسانه‌های کابلی طول، قطر و جنس کابل است. طول

۱ــ Band W dth

۲ــ Hz

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 می‌شود.

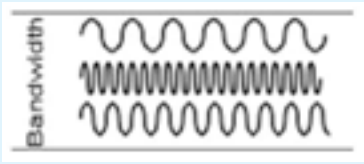
برای انتقال اطلاعات به دو روش از پهنای باند استفاده می‌شود. این دو روش عبارتند از :

- تک‌باند[1]
- باند پهن[2]

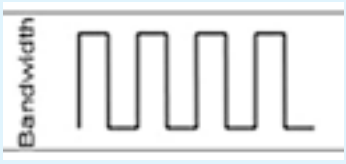
در روش تک باند از تمام پهنای باند برای ارسال یا دریافت اطلاعات استفاده می‌شود؛ به این معنی که تک‌باند در هر لحظه فقط می‌تواند یک سیگنال را از خود عبور دهد، درنتیجه ارسال نوبتی می‌شود و اطلاعات پشت سر هم و به‌صورت سری ارسال می‌شوند. به این نوع شبکه تک‌باند گفته می‌شود.

در روش تک‌باند برای ارسال و دریافت اطلاعات به دو رشته کابل نیاز است که یکی از کابل‌ها وظیفه ارسال اطلاعات را به عهده دارد و کابل دیگر دریافت اطلاعات را انجام می‌دهد. سیستم انتقال دیجیتال نیز از روش تک‌باند استفاده می‌کند (شکل ۸ ــ ۲).

روش دیگر انتقال، انتقال باند پهن است. باند پهن می‌تواند از یک کابل، یک یا چند سیگنال را به‌طور هم‌زمان عبور دهد. هر سیگنال به‌صورت جداگانه ارسال می‌شود و تداخلی بین سیگنال‌های متفاوت به‌وجود نمی‌آید. از این روش در شبکه تلویزیون کابلی استفاده می‌شود. در شبکه‌های محلی این روش کاربردی ندارد ولی در شبکه‌های WAN همواره مورد توجه است (شکل ۸ ــ ۲).



الف) باند پهن (Broad band)



ب) تک باند (Base band)

شکل ۸ــ۲

۱ــ Base band

۲ــ Broad band

۶ـ۲ـ نویز

از جمله مشکلاتی که در شبکه به‌وجود می‌آید، نویز است. نویز عامل مخربی است که شکل سیگنال‌ها را تغییر می‌دهد و باعث بروز اختلال می‌شود.

عوامل مختلفی باعث به‌وجود آمدن نویز می‌شوند. تعدادی از این عوامل عبارتند از : حرارت، القا و هم‌شنوایی.

حرارت : حرارت باعث می‌شود الکترون‌ها در جهات نامشخص شروع به حرکت نمایند؛ این حرکت گاهی با سیگنال‌ها هم‌جهت شده و اندازه و شکل آنها را که همان الگوی سیگنال‌هاست، تغییر می‌دهد و این به معنی ایجاد نویز است.

القا : نویزهای القایی نویزهایی هستند که موتورهای مکانیکی مثل موتور ماشین یا وسایل الکتریکی مانند موتورهای الکتریکی 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] : به اثرگذاری میدان مغناطیسی یک کابل از کابل مجاور آن هم شنوایی گفته می‌شود. نویزهایی که کابل‌های برق فشار قوی یا رعد و برق ایجاد می‌کنند، از انواع نویزهای هم‌شنوایی محسوب می‌شوند.

۷ـ۲ـ سرعت انتقال اطلاعات

به مقدار اطلاعاتی که در واحد زمان به‌وسیلهٔ تجهیزات شبکه ارسال می‌شود، سرعت انتقال اطلاعات می‌گویند و واحد اندازه‌گیری آن بیت بر ثانیه (bps) است. سرعت انتقال اطلاعات در وسایل مختلف متفاوت است.

به‌طور مثال کارت‌های شبکه با سرعت ۱۰Mbps توانایی انتقال ۱۰ مگابیت در ثانیه را دارند و کارت‌های ۱۰۰Mbps می‌توانند در ثانیه ۱۰۰ مگابیت اطلاعات را به مقصد ارسال کنند. منظور از مودم ۵۶ Kbps این است که دارای سرعت ۵۶۰۰۰ بیت در ثانیه می‌باشد.

سرعت انتقال اطلاعات با پهنای باند ارتباط مستقیم دارد، هرچه پهنای باند بیشتر شود سرعت انتقال اطلاعات نیز بیشتر می‌شود. از طرفی سرعت انتقال با نویز نسبت معکوس دارد و نویز در این زمینه عامل محدودکننده‌ای است.

۱ـ Crossta k

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

خودآزمایی و پژوهش

۱ــ سرعت ارسال اطلاعات در کدام‌یک از روش‌های سری یا موازی بیشتر است؟

۲ــ سیگنال چیست؟

۳ــ نویز چیست؟ اثر نویز بر روی کدام‌یک از سیگنال‌های آنالوگ یا دیجیتال بیشتر است؟

فصل سوم

پیکربندی شبکه و روش‌های دسترسی به خط انتقال

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- انواع هم‌بندی شبکه را شرح دهد.
- مزایا و معایب هر کدام از هم‌بندی‌های شبکه را شرح دهد.
- روش‌های دسترسی به خط انتقال را شناسایی کند.

۱ـ۳ـ انواع هم بندی

اجزای یک شبکه را می توان به روش‌های مختلف طبق یک طرح یا نقشهٔ مشخص به هم متصل نمود که به این طرح و نقشه اتصال، پیکربندی (هم بندی[۱]) شبکه می‌گویند. به عبارت دقیق‌تر هم‌بندی دارای دو حالت فیزیکی و منطقی می‌باشد، در حالت فیزیکی چگونگی اتصال ظاهری اجزای شبکه مشخص می‌شود که به وسیله کابل به هم متصل می‌شوند و حالت منطقی آن، نحوهٔ تبادل اطلاعات و چگونگی دسترسی رایانه‌ها به محیط انتقال را مشخص می‌کند[۲].

۱ـ۱ـ۳ـ هم بندی خطی (BUS)

جنبه ظاهری یا فیزیکی: تمام سیستم‌ها با یک قطعه کابل به یکدیگر متصل شده‌اند.

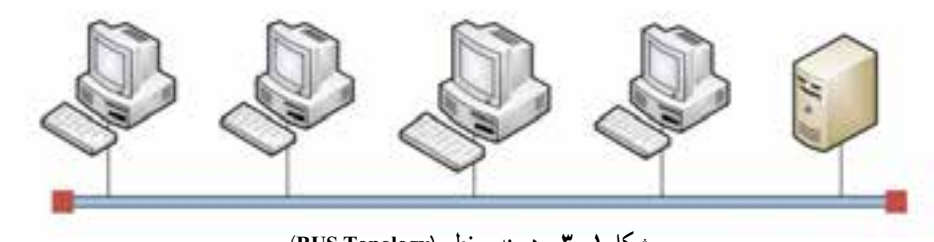
جنبه منطقی: زمانی که یک رایانه اطلاعات را ارسال می‌کند به تمام رایانه‌ها ارسال می شود و رایانه‌ای که دارای آدرس مشخص می‌باشد اطلاعات را دریافت کرده و سایر رایانه ها اطلاعات را به خط اصلی برمی‌گردانند.

چون درکابل شبکه خطی، سیگنال‌ها پس از رسیدن به انتهای خط (فضای باز) دوباره به خط اصلی برمی‌گردند و باعث تداخل و مختل شدن کل شبکه می‌شوند، به همین دلیل باید در ابتدا و انتهای

۱ـ Topo ogy

۲ـ با استفاده از نرم افزار V s o (یکی از نرم افزارهای مجموعه M crosoft Off ce) می‌توان نقشه اتصالات شبکه را به راحتی ترسیم نمود.

خط شبکه از «ترمیناتور[1]» استفاده شود. ترمیناتور حاوی یک مقاومت الکتریکی است که وابسته به مشخصات کابل و پارامترهای دیگر می‌باشد که در نوع خاصی از شبکه ها ۵۰ اهم می‌باشد.



شکل ۱ــ۳ــ هم‌بندی خطی (BUS Topology)

مزایای هم‌بندی خطی

ــ ساده‌ترین نوع هم‌بندی می‌باشد.

ــ ارزان‌ترین نوع هم‌بندی می‌باشد.

ــ نسبت به بقیه هم‌بندی‌ها کابل کمتری مصرف می‌شود.

ــ افزایش یا کاهش سیستم‌ها به راحتی انجام می‌شود (البته تا حد مجاز).

معایب هم‌بندی خطی

ــ سرعت پایین‌تری نسبت به بقیه هم‌بندی‌ها دارد.

ــ در صورت قطع شدن یک قسمت از کابل اصلی، ارتباط تمامی اجزای شبکه قطع می‌شود و شبکه از کار می‌افتد. (چون فضای باز ایجاد می‌شود و باعث تداخل و انعکاس سیگنال‌ها می‌گردد)

ــ اگر یکی از ترمیناتورها قطع یا خراب شود، ارتباط تمامی اجزای شبکه قطع می‌شود و شبکه از کار می افتد.

ــ عیب یابی شبکه مشکل و زمان‌بر می باشد.

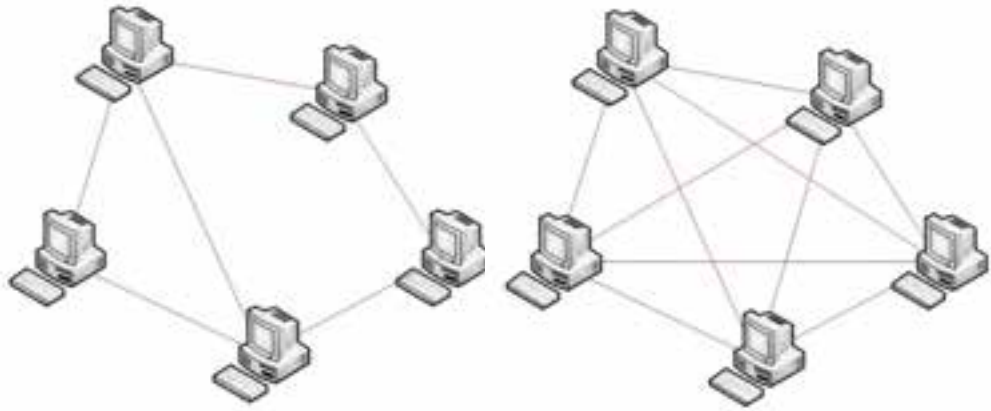
ــ یک تکنولوژی قدیمی است.

۲ــ۱ــ۳ــ هم بندی مشبک (Mesh)

جنبه ظاهری: تمام رایانه‌های شبکه دو به دو با یک کابل مستقل به هم متصل می‌باشند که این حالت ایده‌آل می‌باشد و به آن مش کامل می‌گویند. به طوری که تعداد رایانه‌های متصل در شبکه n باشد $n\ 1$ کابل به هر رایانه متصل می‌شود. (شکل ۲ــ۳)

۱ــ Term nator

اگر یکی از اتصالات برقرار نباشد به آن هم‌بندی، مش ناقص می‌گویند.



هم‌بندی مشبک (Mesh) کامل　　هم‌بندی مشبک (Mesh) ناقص

شکل ۲ــ۳

مزایای هم‌بندی مشبک

ــ اگر یکی از ارتباط‌ها قطع شود از مسیر دیگری ارتباط برقرار می‌شود.

ــ مطمئن‌ترین و پایدارترین نوع ارتباط را نسبت به سایر هم‌بندی‌ها دارا می‌باشد.

معایب هم‌بندی مشبک (Mesh)

ــ به دلیل استفاده زیاد کارت شبکه و کابل، پیچیده ترین و گران ترین نوع هم‌بندی می‌باشد.

۳ــ۱ــ۳ــ هم بندی ستاره‌ای (Star)

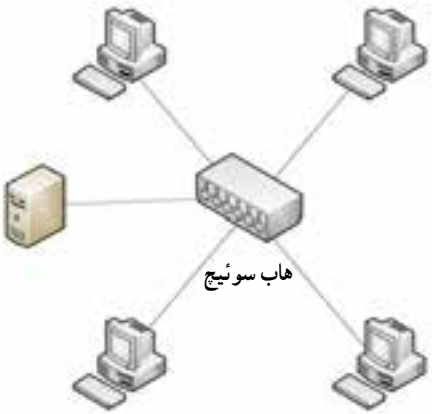
جنبه ظاهری: تمام رایانه‌های شبکه توسط یک کابل مستقل به یک نقطه مرکزی به نام Hub Switch متصل می‌شوند.

نکته: واژه Hub به طور 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 هاب می‌شود منظور استفاده از آن در نوع خاص و رایجی از شبکه‌ها به نام شبکه Ethernet سوئیچ، Hub هوشمند است.

در هم بندی ستاره‌ای اگر از Hub معمولی استفاده شود، سیگنال‌ها به تمام رایانه‌های متصل به هاب ارسال خواهند شد ولی اگر از سوئیچ استفاده شود، سیگنال‌ها فقط به رایانه(های) مقصد ارسال می‌گردند.

جنبه منطقی: سیگنال‌ها از رایانه فرستنده به سوئیچ ارسال می‌شود سپس سوئیچ آنها را به سایر رایانه‌های شبکه ارسال می‌کند.



شکل ۳ــ۳ــ هم‌بندی ستاره‌ای

مزایای هم‌بندی ستاره‌ای

ــ قطع شدن یک کابل به طور معمول بر روی بقیه شبکه تأثیری نمی‌گذارد مگر این که مربوط به سرویس دهنده باشد(در SB)

ــ در صورت استفاده از سوئیچ، سیگنال‌ها فقط به رایانه مقصد ارسال می‌شوند نه تمام رایانه‌ها. و این امر باعث کاهش حجم ترافیک می‌شود.

ــ در صورت استفاده از سوئیچ، امکان تبادل اطلاعات دو به دو به صورت هم‌زمان وجود خواهد داشت.

ــ هزینه نگهداری و رفع عیب آن نسبت به هم‌بندی خطی پایین تر است.

معایب هم‌بندی ستاره‌ای

ــ اگر به هر دلیلی دستگاه مرکزی از کار بیفتد، کل شبکه از کار می‌افتد.

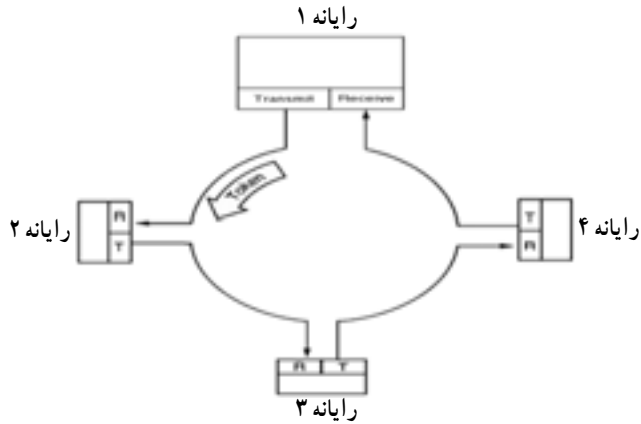
اگر به هر دلیلی «نقطه مرکزی» از کار بیفتد کل شبکه از کار باز می‌ایستد، به همین دلیل معمولاً هاب را از نظر فیزیکی در یک تابلوی مخصوص معروف به Rack نصب کرده و Rack را در یک مکان مطمئن و با شرایط محیطی مناسب قرار می‌دهند. در شبکه‌هایی که ضریب حساسیت آن ها بیشتر است، ترکیبی از دو

یا چند سوئیچ را (درهم بندی Mesh) قرار داده و بدین ترتیب اگر یکی از سوئیچ‌ها از کار بیفتد، سوئیچ‌های دیگر بلافاصله وارد عمل شده و ترافیک از طریق آن ها به عبور خود ادامه می‌دهد (تحمل خطا).

ــ مصرف کابل و هزینه پیاده سازی آن نسبت به هم بندی خطی بیشتر می‌باشد.

۴ــ۱ــ۳ــ هم بندی حلقوی (Ring)

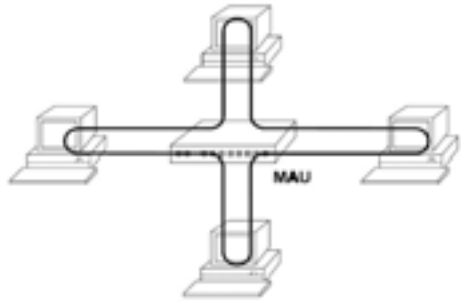
ــ هر رایانه به صورت منطقی (نه فیزیکی) به رایانه مجاور خود متصل می‌باشد و آخرین رایانه نیز به اولین رایانه متصل می باشد و رایانه‌ها تشکیل یک حلقه را می‌دهند (شکل ۴ ۳).



شکل ۴ــ۳ــ هم‌بندی حلقوی

ولی در عمل برای اتصال حلقه‌ای رایانه‌ها از یک دستگاه مرکزی به نام MAU[1] (واحد دسترسی چندگانه) استفاده می شود و تمام رایانه‌ها با یک کابل به MAU متصل می‌شوند (مانند هم‌بندی ستاره‌ای)

هم‌بندی



مسیر ارتباطی در MAU و رایانه‌ها در هم‌بندی

شکل ۵ــ۳ــ واحد دسترسی چندگانه درهم‌بندی

۱ــ Mu t Access Un t

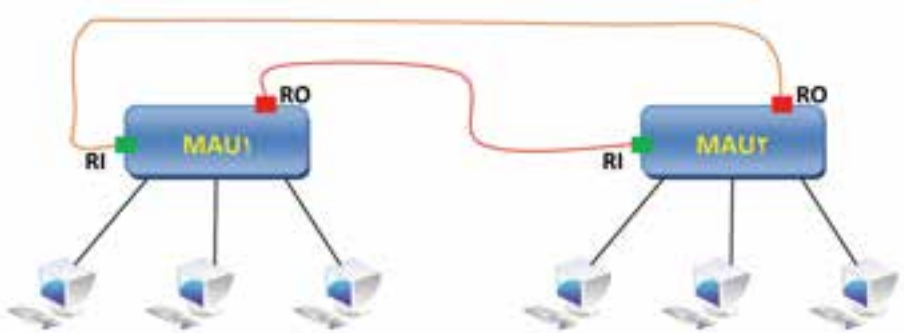
شبکه‌های طراحی شده با هم‌بندی حلقه‌ای را شبکهٔ Token Ring یا Token Passing نیز می‌گویند، زیرا انتقال اطلاعات در این شبکه‌ها بر اساس گردش یک بسته مخصوص به نام Token می‌باشد.

از نظر نحوه گردش Token دو نوع هم‌بندی حلقوی وجود دارد :

۱ــ هم‌بندی حلقوی یک طرفه : Tokenها فقط در یک جهت حرکت می‌کنند.

۲ــ هم‌بندی حلقوی دو طرفه : Tokenها در هر دو جهت حرکت می‌کنند.در واقع نوع ناقص هم بندی Mesh می‌باشد.

اگر بخواهیم دو تا شبکه حلقوی را به یکدیگر متصل کنیم باید Ring out (RO) سوئیچ اول را به Ring In (RI)سوئیچ ۲ متصل نموده و همچنین Ring out (RO) سوئیچ دوم را به Ring In (RI) سوئیچ اول وصل کنیم.



شکل ۶ــ۳ــ ارتباط دو شبکه حلقوی

مزایای هم‌بندی حلقوی

ــ نحوه گردش اطلاعات دارای اولویت بندی و زمان بندی است تا تداخل به وجود نیاید.

ــ برای شبکه‌های با ترافیک بالا مناسب می‌باشد. چون تداخل وجود ندارد.

معایب هم بندی حلقوی

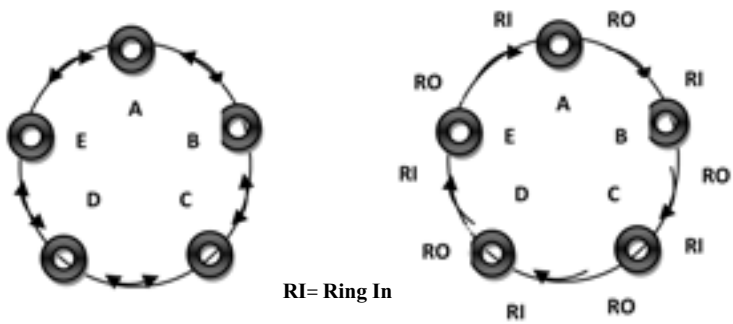
ــ اگر عیبی در MAU بوجود بیاید، کل شبکه از کار خواهد افتاد.

ــ افزودن یا کاستن رایانه‌ها در شبکه به سادگی ممکن نیست.

ــ مصرف کابل و هزینه پیاده سازی آن نسبت به هم‌بندی خطی بیشتر می‌باشد.

مانند هم‌بندی خطی اگر یک قسمت از حلقه قطع شود، کل شبکه از کار می‌افتد به این علت که اطلاعات قادر به گردش کامل نخواهند بود.

درواقع قانون گردش اطلاعات در حلقه‌های یک طرفه به گونه‌ای 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. به عنوان مثال در شکل اگر حدفاصل بین A و B قطع شود در آن صورت هرچند ممکن است تصور شود B می‌تواند برای C، D، E و A اطلاعات بفرستد، اما عکس آن امکان پذیر نیست و به این معنا که همه سیستم‌ها نمی‌توانند به تبادل اطلاعات بپردازند، در نتیجه هر دو قانون فوق نقض شده و حلقه به طور کامل غیر قابل استفاده می‌شود. این مشکل در حلقه‌های دوطرفه (که حالت خاصی از Mesh محسوب می‌شوند) وجود ندارد.



شکل ۷ــ۳ــ هم‌بندی حلقوی یک‌طرفه و دو طرفه

نکته: شبکه حلقوی دو طرفه را می‌توان حالت خاصی از مش به حساب آورد زیرا چنانچه قطرهای یک مش کامل را حذف کنیم شکل حاصله یک مش ناقص خواهد شد که همان شبکه حلقوی دو طرفه است.

اصولاً انتخاب هم‌بندی ربطی به ابعاد و گستردگی فیزیکی شبکه (LAN یا WAN) ندارد و بدیهی است که هر نوع هم‌بندی را می‌توان چه در شبکه محلی و چه در شبکه گسترده استفاده کرد اما با توجه به اینکه احتمال تأثیرگذاری عوامل بازدارنده در شبکه‌های گسترده نسبت به شبکه‌های محلی بیشتر است لذا معمولاً در شبکه‌های گسترده از هم‌بندی مش استفاده شده و هم‌بندی‌های خطی، ستاره‌ای، حلقوی را در شبکه محلی به کار می‌برند، البته ستاره‌ای نیز در WAN کاربرد دارد.

۲ـ۳ـ روش‌های دسترسی[۱] به خط انتقال

به مجموعه قوانینی که تعیین می‌کنند داده‌ها چگونه در کابل شبکه قرار گیرند و یا اینکه داده‌ها چگونه از کابل شبکه دریافت شوند «روش دسترسی» می‌گویند. هنگامی که داده‌ها در شبکه درحال حرکت هستند، روش‌های دسترسی به تنظیم ترافیک شبکه کمک می‌کند.

فرض کنید چندین قطار در ریل راه آهن در حال حرکت هستند، همانطور که می‌دانید مسیرها در ایستگاه راه آهن از هم جدا می‌شوند. قطارها در طول مسیر از قوانین خاصی پیروی می‌کنند تا زمان خاصی به ایستگاه راه آهن رسیده و برخورد به وجود نیاید (هر چند این مقایسه کامل نیست).

در شبکه، رایانه‌ها به کابل شبکه؛ دسترسی اشتراکی دارند. با این حال اگر دو رایانه همزمان داده در کابل شبکه قرار دهند احتمال برخورد وجود خواهد داشت.

ضمناً اگر رایانه‌های موجود در شبکه از روش‌های دسترسی مختلف استفاده کنند کل شبکه از کار خواهد افتاد چون به ازای روش‌های دسترسی مختلف، نوع کابل شبکه نیز متفاوت خواهد بود.

روش های دسترسی؛ از دسترسی همزمان رایانه ها به کابل شبکه جلوگیری می کنند. و یا به عبارت دیگر باعث حصول اطمینان از ارسال و دریافت داده بر اساس یک فرآیند منظم می شوند.

انواع روش‌های رایج برای دسترسی به خط انتقال

الف) روش دسترسی چندگانه تشخیص حامل[۲] (با تشخیص برخورد[۳]) CSMA/CD

ب) روش عبور نشانه[۴]

ج) روش اولویت تقاضا[۵]

- **روش CSMA/CD** : هر رایانه اعم از سرویس دهنده یا سرویس گیرنده کابل شبکه را برای ترافیک چک می‌کند. یعنی فقط وقتی که رایانه تشخیص دهد یا حس کند(Sense) کابل شبکه آزاد است و ترافیکی روی شبکه وجود ندارد داده را روی کابل ارسال می‌کند و تا زمانی که داده روی کابل به مقصد نرسد رایانه دیگری نمی تواند روی کابل داده ارسال کند.

این روش شبیه صحبت در یک اتاق شلوغ است. در چنین اتاقی شخصی که می‌خواهد صحبت کند باید با گوش دادن، مطمئن شود که فرد دیگری درحال صحبت نیست و سپس اقدام به

۱ـ Access Method

۲ـ Carr er Sense Mu t p e Access

۳ـ Co s on detect on

۴ـ Token Pass ng

۵ـ Demand pr or ty methods

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، می‌تواند به صحبت خود ادامه دهد و بقیه باید تا پایان صحبت منتظر بمانند. هرگاه پس از برقراری سکوت، دو نفر باهم شروع به صحبت کنند، هردو سکوت کرده، پس از طی یک زمان کوتاه نامشخص، یکی از آنها شروع به صحبت خواهد کرد. این دقیقاً روشی است که در CSMA/CD از آن استفاده می‌شود :

ـ رایانه «تشخیص می‌دهد» که کابل آزاد است یعنی ترافیک در کابل وجود ندارد (Sense).

ـ رایانه می‌تواند داده‌ها را ارسال نماید.

ـ اگر داده‌ها در کابل وجود داشته باشند، تا زمانی که داده به مقصد خود برسند و کابل مجدداً آزاد گردد، هیچ رایانه‌ای داده‌ای را منتقل نمی‌کند.

یادآوری : اگر دو یا چند رایانه دقیقاً به طور همزمان روی کابل شبکه داده ارسال کنند برخورد[1] به وجود می‌آید و وقتی چنین اتفاقی بیفتد، دو رایانه درگیر برای یک دوره زمانی تصادفی، انتقال را متوقف می سازند و سپس سعی در ارسال مجدد می‌نمایند.

فرض کنیم A در حال ارسال اطلاعات برای B باشد، هم زمان C هم می‌خواهد اطلاعاتی را برای D بفرستد در این حالت، چون فقط یک محیط انتقال وجود دارد که آن هم 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 برسد و خط مجدداً آزاد شود . البته اگر رایانه 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 می کند 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 برخورد (Collision) شده، سیگنال ها به هم می ریزد. بنابراین در یک لحظه مشخص فقط یک فرستنده می‌تواند وجود داشته باشد.

CSMA/CD به عنوان روش کشمکش یا روش رقابتی[2] شناخته می‌شود زیرا رایانه‌های شبکه برای به دست آوردن فرصتی در ارسال داده‌ها، باهم رقابت می کنند.

در روش دسترسی CSMA/CD هر چقدر تعداد رایانه‌ها بیشتر شود ترافیک شبکه نیز بیشتر خواهد شد. در نتیجه برای اجتناب از برخورد، شبکه کند می‌شود.

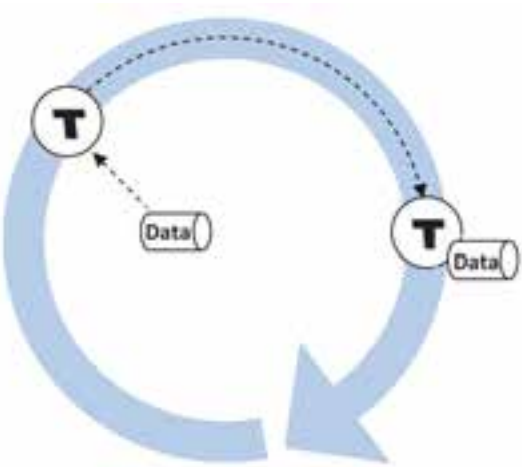
قابلیت تشخیص برخورد پارامتر مهمی در محدودیت فاصله در CSMA/CD می باشد. روش

۱ـ Co s on

۲ـ Content on Method

دسترسی CSMA/CD دارای پایین ترین سطح محبوبیت بین روش های دسترسی دیگر می باشد.

• **روش عبور نشانه (Token Passing)** : در عبور نشانه، بسته خاصی به نام نشانه (Token) به صورت حلقوی از طریق کابل از یک رایانه به رایانه دیگر گردش می‌کند. وقتی رایانه‌ای بخواهد داده‌ها را در طول شبکه ارسال کند باید منتظر نشانه (Token) آزاد بماند. وقتی نشانه آزاد تشخیص داده شد، رایانه می‌تواند داده‌ها را انتقال دهد.



شکل ۸ــ۳

مادامی‌که نشانه توسط یک رایانه مورد استفاده قرار می‌گیرد، سایر رایانه‌ها نمی‌توانند داده‌ای را منتقل کنند چون در این روش در هر لحظه فقط یک رایانه می‌تواند از نشانه استفاده کند. در این روش رقابت و برخورد وجود ندارد و هیچ زمانی برای ارسال مجدد داده صرف نمی‌شود و ترافیکی هم بر روی شبکه به وجود نمی‌آید.

• **روش اولویت تقاضا** : این روش از روش‌های جدید دسترسی به خط انتقال می‌باشدکه توسط مؤسسه مهندسان برق و الکترونیک(IEEE) مورد تأئید قرار گرفته است. در این روش کنترل دسترسی شبکه از ایستگاه کاری به هاب انتقال می‌یابد. (این روش دسترسی در هم‌بندی ستاره‌ای استفاده می‌شود). رایانه‌ای که می‌خواهد داده ارسال کند آن را به هاب واگذار می‌کند.

در روش اولویت تقاضا، ارتباط بین رایانه فرستنده با هاب و هاب با رایانه مقصد بر قرار می‌باشد. این روش دارای راندمان بیشتری نسبت به روش CSMA/CD می باشد.

در روش اولویت تقاضا از ۴ زوج سیم استفاده می شود که این کار باعث خواهد شد تا رایانه‌ها به طور همزمان هم ارسال و هم دریافت داده داشته باشند.

مطالعه آزاد

۳ـ۳ـ معماری شبکه

معماری شبکه، استانداردهایی می‌باشد که برای چگونگی اتصال رایانه‌ها با یکدیگر و نحوه ارسال اطلاعات تعریف شده است. در این استانداردها نوع کابل شبکه، اتصالات، هم‌بندی، نحوه دسترسی به خطوط انتقال و سرعت انتقال مشخص شده است. چندین نوع معماری شبکه وجود دارد که هنگام راه‌اندازی شبکه از آنها استفاده می‌شود. انواع معماری شبکه عبارتند از :

- اترنت[۱]
- Token Ring
- FDDI

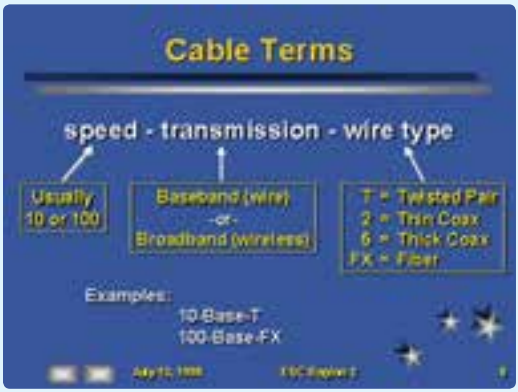
۱ـ۳ـ۳ـ اترنت : اترنت یکی از انواع متداول معماری شبکه است. در این معماری از روش CSMA/CD برای دسترسی به خط انتقال یا همان کابل شبکه استفاده می‌شود. هم‌بندی پیش‌فرض برای اترنت، هم‌بندی فیزیکی خطی تعریف شده است. نوع کابلی که در هر هم‌بندی استفاده می‌شود نیز در قوانین همان هم‌بندی مشخص شده است.

هم‌بندی‌های مختلف اترنت عبارتند از :

- 10Base2
- 10Base5
- 10BaseT
- 10BaseFL
- 100Basex
- 1000Basex
- 1000BaseT

۱ـ Ethernet

در استانداردهایی که نام برده شد، عدد اول نمایانگر سرعت انتقال است مثلاً 10Base2 با سرعت 10Mbps کار می‌کند. Base نشان‌دهنده Base band بودن هم‌بندی و عبارت پس از آن نوع کابل را نشان می‌دهد.



شکل ۹ــ۳ــ اجزای تشکیل‌دهنده نام در معماری‌های مختلف

در معماری اترنت علاوه بر موارد ذکر شده نحوه ساخته شدن بسته‌های اطلاعاتی، اندازه آنها، اطلاعات اضافی که باید در بسته‌های اطلاعاتی قرار گیرد و کابل‌کشی شبکه مشخص شده است. در ادامه برخی از استانداردهای متداول دراترنت توضیح داده خواهد شد.

10Base2 : برای انتقال داده‌ها از کابل هم‌محور Thinnet استفاده می‌کند. کانکتورهای این شبکه از نوع BNC بوده و دو سر کابل باید به‌وسیلهٔ (Terminator) مسدود شود تا شبکه فعال شود. از مزایای 10Base2 نصب ساده و هزینه راه‌اندازی بسیار کم آن است. هم‌بندی 10Base2 همان هم‌بندی خطی است.

قوانینی که در 10Base2 باید رعایت شود، عبارتند از :

حداقل طول کابلی که رایانه‌ها را به هم متصل می‌کند نباید کمتر از ۰/۵ متر باشد.

فاصله اولین و آخرین رایانه در شبکه نباید بیش از ۱۸۵ متر باشد. این فاصله از روی اندازه کابل اندازه‌گیری می‌شود.

در فواصل بین هر دو Repeater نمی‌توان بیش از ۳۰ دستگاه رایانه به شبکه متصل کرد.

ابتدا و انتهای کابل باید با ترمیناتور مسدود شود. ترمیناتور شبکه 10Base2، یک مقاومت ۵۰ اهمی است که سیگنال‌های الکتریکی به‌وجود آمده در کابل شبکه را مصرف کرده و از باقی ماندن آن در شبکه جلوگیری می کند.

برای دست یافتن به حداکثر فاصله رایانه‌ها یعنی ۹۲۵ متر، **پنج** سگمنت (Segment) خواهیم داشت که با **چهار** دستگاه Repeater به هم متصل شده‌اند که فقط از **سه** سگمنت آن می‌توان استفاده کرد (این سگمنت‌ها شماره‌های ۱، ۲ و ۵ هستند). این قانون به قانون **۳ــ۴ــ۵** معروف است.

10Base5 : در 10Base5 از کابل کواکسیال Thicknet برای اتصال رایانه‌ها به یکدیگر استفاده می‌شود.

هر رایانه به‌وسیلهٔ یک کابل AUI یا DIX به یک عدد Transceiver که به کابل شبکه متصل شده است، وصل می‌شود و هر دو انتهای کابل با ترمیناتور مسدود می‌شود. اولین مزیت10Base5 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 رایانه استفاده می‌شود ۲/۵ متر است.

شکل ۱۰ــ۳ــ انواع کابل مورد استفاده در معماری‌ها

حداکثر طول کابل یا حداکثر فاصله بین اولین و آخرین رایانه شبکه ۵۰۰ متر است.

حداکثر فاصله بین اولین و آخرین رایانه شبکه با استفاده از Repeater، ۲۵۰۰ متر است.

یکی از ترمیناتورها باید به زمین متصل شود.

اندازه کابلی که رایانه را به Transceiver متصل می‌کند، نباید بیشتر از ۵۰ متر باشد.

حداکثر تعداد رایانه‌ها در سگمنت ۱۰۰ دستگاه است.

قانون ۳ـ۴ـ۵ در مورد 10Base5 نیز صادق است.

10Base T : برای راه‌اندازی شبکه 10Base T از کابل‌های TP یا زوج به هم تابیده استفاده می‌شود که حداکثر سرعت آنها 10Mbps است. در این استاندارد هر رایانه‌ای که می‌خواهد به شبکه متصل شود مستقیماً توسط یک کابل به هاب وصل شده و هاب، ارتباط رایانه‌ها را برقرار می‌کند. اتصالات این هم‌بندی از نوع RJ 45 است. سگمنت‌های مختلف می‌توانند به‌وسیلهٔ کابل‌های کواکسیال یا فیبر نوری به یکدیگر متصل شوند. برخی از انواع دستگاه‌هایی که می‌توانند جایگزین هاب شوند، هوشمند بوده و می‌توانند ترافیک شبکه را کنترل کرده و آن را کاهش دهند. از مشخصه‌های بارز این شبکه گران قیمت بودن هزینه راه‌اندازی و نصب آن است. 10Base T در ظاهر یک شبکه ستاره‌ای است ولی عملکرد آن همانند شبکه‌های خطی می‌باشد در این مورد به‌طور خلاصه می‌توان گفت هم‌بندی فیزیکی آن، ستاره‌ای ولی هم‌بندی منطقی آن خطی است.

قوانین 10BaseT عبارتند از :

حداکثر تعداد رایانه‌ای که این شبکه به هم متصل می‌کند، ۱۰۲۴ دستگاه رایانه است.

کابل‌ها باید از نوع زوج به تابیده Category3، Category4 یا Category5 باشند (نوع کابل از نظر داشتن محافظ تفاوتی نمی‌کند، می‌توان از هر دو کابل UTP یا STP استفاده کرد).

حداکثر فاصله هر رایانه تا هاب، ۱۰۰ متر است.

حداقل طول کابل (فاصله بین رایانه تا هاب) ۲/۵ متر است.

10Base FL : شبکه اترنتی است که برای انتقال اطلاعات از فیبر نوری استفاده می‌کند. سرعت انتقال در این شبکه 10Mbps است. مهم‌ترین ویژگی 10BaseFL مسافت زیادی است که تحت پوشش قرار می‌دهد. این مسافت ۲ کیلومتر است. از مزایای دیگر این شبکه این است که عوامل خارجی، تأثیری روی اطلاعات داخل فیبر ندارند. به عبارت دیگر، در فیبرنوری هم شنوایی وجود ندارد و اطلاعات سالم به مقصد می‌رسد.

دو استاندارد دیگر به نام‌های 10BaseFB و 10BaseFP نیز مورد استفاده قرار می‌گیرد. 10BaseFB که یک شبکه اترنت هم زمان است[1] و برای اتصال دو تقویت‌کننده فیبر نوری به یکدیگر که در مسیر بین دو ایستگاه قرار دارد، استفاده می‌شود. استاندارد دیگر 10BaseFP است که یک شبکه ستاره‌ای با استفاده از فیبر نوری می‌باشد که برای Backbone[2] شبکه‌ها مورد استفاده قرار می‌گیرد. در فیبرهای نوری، نور به جای سیگنال‌های الکترونیکی مسئولیت انتقال اطلاعات را برعهده دارد.

100Base X :

ساختار شبکه 100BaseX همانند شبکه 10BaseT است (سرعت این شبکه 100Mbpsاست) با این تفاوت که 100BaseX با سه مدل کابل‌کشی متفاوت مورد استفاده قرار می‌گیرد. این سه مدل عبارتند از :

ـ 100Base TX : در این مدل می‌توان از دو نوع کابل UTP یا STP به صورت همزمان استفاده شود.

ـ 100Base FX : در این مدل از دو رشته فیبر نوری در کنار هم استفاده می‌شود.

ـ 100Base T4 : در این مدل ۴ رشته کابل 5 یا Category3 .4، در کنار هم استفاده می‌شود.

1000Base X :

با نام Fast Ethernet نیز شناخته می‌شود. این استاندارد، شبکه‌ای را توضیح می‌دهد که در آن سرعت انتقال اطلاعات یک گیگابیت در ثانیه است و برای انتقال اطلاعات از فیبرنوری استفاده می‌شود. این استاندارد خود از چند مدل تشکیل شده است که عبارتند از :

ـ 1000Base sx

ـ 1000Base LX/LH

۱ـ Synchronous Ethernet

۲ـ Backbone بخشی از معماری شبکه‌های کامپیوتری می‌باشد که ارتباط داخلی بین چند شبکه را به‌وجود می‌آورد. این ارتباط شامل تبادل اطلاعات بین چند شبکه LAN یا WAN می‌شود.

معمولاً توان و ظرفیت Backbone بیشتر از شبکه‌هایی است که به آن متصل هستند. به عنوان مثال اگر شبکه LAN در یک محیط 00/Mbps باشد سرعت Backbone که ارتباط بین شبکه‌های LANرا به‌وجود می‌آورد 000/Mbps می‌باشد.

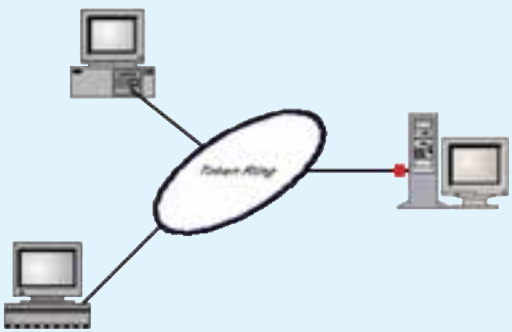
ـ 1000Basezx

تفاوت استانداردهای ذکر شده در طول کابل‌ها و نوع فیبر نوری است که در آنها استفاده می‌شود.

1000Base T :

در این استاندارد، از کابل‌های زوج به هم تابیده برای راه‌اندازی شبکه‌ای با سرعت یک گیگابیت در ثانیه استفاده می‌شود. این کابل‌ها از نوع Cat6 و کانکتورهای آن نیز از نوع RJ 45 است. نحوه ارسال اطلاعات در این استاندارد به گونه‌ای است که سیستم، توانایی انتقال اطلاعات یک گیگابیت در ثانیه را پیدا می‌کند. کابل T.P نام دیگر کابل زوج به هم تابیده است.

۲ـ۳ـ۳ـ Token Ring : معماری Token Ring از نظر ظاهری، یک شبکه ستاره‌ای را توصیف می‌کند که به روش عبور نشانه (Token Passing) کار می‌کند. در این شبکه یک حلقه منطقی به‌وجود می‌آید و نشانه در امتداد حلقه حرکت کرده و به رایانه‌ها می‌رسد. هر رایانه‌ای که به ارسال اطلاعات نیاز داشته باشد، نشانه را نگه داشته و اطلاعات خود را به سوی مقصد ارسال می‌کند. اطلاعات ارسال شده در همان حلقه مجازی و در امتداد حرکت نشانه مسیر خود را طی می‌کند تا به رایانه مقصد برسد. رایانه مقصد در صورت صحیح بودن اطلاعات ارسالی، در جواب یک بسته به نام Acknowledge به رایانه مبدأ ارسال می‌کند. رایانه مبدأ نیز نشانه اصلی را از بین برده و یک نشانه جدید تولید می‌نماید و آن را در امتداد مسیر نشانه قبلی به حرکت درمی‌آورد. این روند به همین صورت ادامه خواهد یافت.

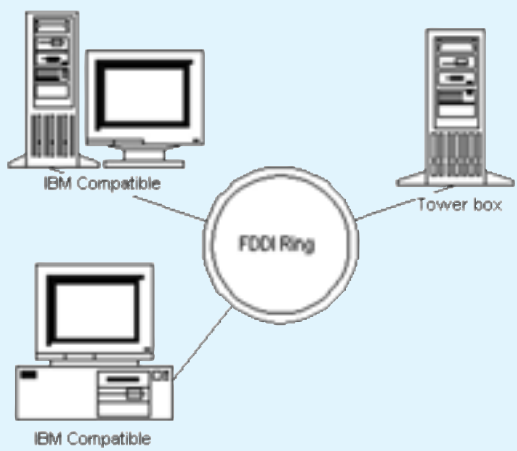


شکل ۱۱ـ۳ـ شبکه Token Ring

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

در شبکه Token Ring از کابل‌های زوج به هم تابیده استفاده می‌شود. اگر از کابل UTP در این هم‌بندی 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.

۳ــ۳ــ۳ــ FDDI[1] : FDDI، معماری یک شبکه با سرعت ۱۰۰ مگابیت در ثانیه است که برای ارتباط از فیبر نوری استفاده می‌کند. در این فناوری 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 به‌عنوان Backbone در محل‌هایی که تعداد زیادی رایانه 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. هم‌بندی فیزیکی این شبکه حلقوی است. نحوه به‌وجود آمدن این حلقه به این صورت است که یک حلقه ۱۰۰ کیلومتری از فیبر نوری ساخته می‌شود و در هر دو کیلومتر یک تقویت‌کننده 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.



شکل ۱۲ــ۳ــ شبکه FDDI

۱ــ F ber D str buted Data Interface

خودآزمایی و پژوهش

۱ــ هم‌بندی چیست؟ انواع آن را شرح دهید.

۲ــ پدیده برخورد یا Collision در کدام یک از انواع هم‌بندی روی می‌دهد؟ چرا؟

۳ــ در کدام یک از انواع هم‌بندی، با قطع شدن قسمتی از کابل، کل شبکه از کار می‌افتد؟

۴ــ انواع هم‌بندی‌ها را از لحاظ مصرف کابل، سرعت، هزینه، عیب‌یابی و اشکال زدایی مقایسه کنید.

۵ــ سرعت کدام یک از روش‌های دسترسی به خط بیشتر است؟ دلیل آن را بنویسید.

۶ــ چه عواملی در سرعت دسترسی به خط مؤثر است؟

۷ــ پژوهش کنید که تفاوت MAU و هاب در چیست؟

فصل چهارم

محیط‌های انتقال و اجزای آن

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- انواع محیط‌های انتقال را شناسایی کند.
- انواع کابل‌های مورد استفاده در شبکه را نام ببرد.
- اتصالات مورد نیاز برای کابل‌کشی شبکه را نام ببرد.
- کابل‌کشی یک شبکه را انجام دهد.
- کارت شبکه و وظایف آن را تعریف کند.
- کابل رابط بین شبکه و سوییچ را ایجاد کند.

۱ـ۴ـ محیط‌های انتقال

برای آن که 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 محیط انتقال را توضیح می‌دهیم.

مثال ۱ : وقتی صحبت می‌کنیم، امواج صوتی از طریق هوا بین گوینده و شنونده انتقال می‌یابد. در این مثال «هوا» به عنوان 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» به عنوان 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 هدایت می کند ارسال می کنیم. کابل نوری در این جا به عنوان محیط انتقال محسوب می‌شود.

مثال ۴ : وقتی به وسیله گوشی آیفون با فردی که کنار در ورودی ایستاده صحبت می کنید صدای شما تبدیل به انرژی الکتریکی شده و به وسیله الکترون‌ها از طریق سیم مسی جریان می‌یابد در این‌صورت «سیم مسی» به عنوان محیط انتقال محسوب می‌شود.

برای جابجا شدن داده‌ها در شبکه، به بستری نیاز می‌باشد که به آن محیط انتقال می گویند. محیط انتقال به دو دسته کلی سیمی‌و بی سیم تقسیم می‌شود.

● **محیط انتقال بی سیم (Wireless)**

در انتقال بی سیم از فضای مادی به عنوان محیط انتقال استفاده می‌شود که برای انتقال از سه روش استفاده می‌شود :

ـــ **اشعه مادون قرمز**[۱] **(Infra red)** : در این فناوری از امواج مادون قرمز برای انتقال اطلاعات استفاده می‌شود در شبکه کامپیوتری مادون قرمز حداکثر فاصله رایانه‌ها یا وسایل جانبی ۵ متر می‌باشد. هر دو دستگاه فرستنده و گیرنده مجهز به این فناوری باید در دید مستقیم یکدیگر باشند (مانند کنترل تلویزیون) سه فن‌آوری مادون قرمز در شبکه‌های محلی وجود دارد.

● ***IrDA ـــ SIR***[۲] : مادون قرمز با سرعت کم (Slow speed Infrared) که سرعت انتقالی معادل ۱۱۵ کیلوبیت بر ثانیه دارد.

● ***IrDA ـــ MIR*** : مادون قرمز با سرعت متوسط (Medium speed Infrared) که سرعت انتقالی معادل ۱/۱۵ مگابیت بر ثانیه دارد.

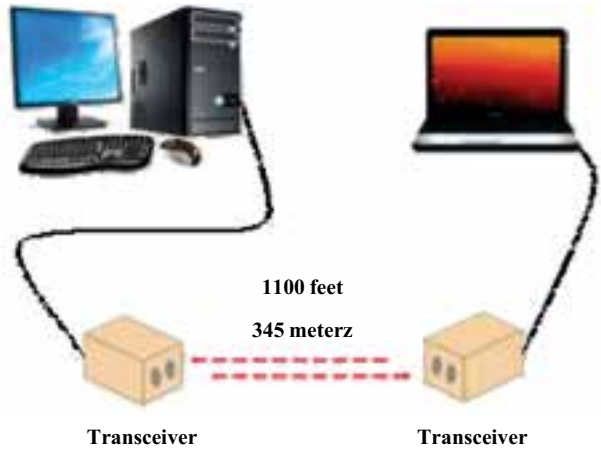
● ***IrDA ـــ FIR*** : مادون قرمز با سرعت بالا (Fast speed Infrared) که سرعت انتقالی معادل ۴ مگابیت بر ثانیه دارد

ـــ **نور لیزر (Laser)** : شبیه مادون قرمز بوده ولی برای فاصله بیشتر استفاده می‌شود. شکل صفحه بعد نمونه‌ای شماتیک از ارتباط دو رایانه با استفاده نور لیزر را نشان می‌دهد.

---

۱ ـ نور نامرئی با فرکانس بالا

۲ـ Infrared Data Assoc at on



شکل ۱ــ۴ ــ ایجاد شبکه بین دو رایانه با استفاده از نور لیزر

ــ **امواج رادیویی (Radio waves)** : در فرکانس‌های مختلف که بیشترین کاربرد را در بین شبکه‌های بی سیم دارد یکی از مزایای استفاده از امواج رادیویی برای انتقال داده، توانایی عبور امواج رادیویی از موانع فیزیکی می‌باشد (البته مقداری از پهنای باند کاهش می‌یابد).

● **محیط انتقال سیمی(کابلی) Wired**

محیط انتقال سیمی‌خود به دو دسته تقسیم می‌شود :

الف) کابل مسی : که از یک یا چند رشته سیم مسی[1] برای انتقال سیگنال‌های الکتریکی استفاده می‌شود.

ب) کابل فیبر نوری[2] : که از چند رشته تار نازک از جنس ترکیبات مخصوص مانند پلاستیک فشرده یا سیلیس که ضریب شکستی نزدیک به ضریب شکست شیشه دارند، استفاده می‌شود.

در محیط انتقال سیمی(کابلی) Wired سه نوع کابل متداول وجود دارد :

الف) کابل هم محور Coaxial مانند کابل آنتن تلویزیون رنگی

ب) کابل «زوج به هم تابیده» (Twisted Pair) مانند سیم تلفن

ج) کابل «فیبر نوری»

الف) کابل هم محور Coaxial : در واقع ترکیبی از Co و Axial به معنی هم محور می‌باشد

۱ــ ممکن است از آلیاژهای ترکیبی مس و آلومینیوم نیز استفاده شود.

۲ــ Opt c F ber Cab e

و از چهار بخش تشکیل شده است.

ـــ ***مغز مسی (Copper Core)*** که وظیفه آن هدایت سیگنال الکتریکی می‌باشد که می‌تواند تک رشته‌ای یا چند رشته‌ای باشد.

ـــ ***عایق داخلی (Inner Insulator)*** : عایق بین مغز مسی و محافظ سیمی(توری) است.

ـــ ***محافظ توری (بافته شده)سیمی(Shielding Wire Mesh)*** : از سیگنال‌های انتقالی در مقابل نویز حفاظت می‌کند.

ـــ ***عایق بیرونی (Outer Insulator)***

شکل ۲ــ۴ ــ کابل شبکه هم محور یا Coaxial

نکته: از کابل کواکسیال در هم‌بندی خطی استفاده می‌شود.

ب) کابل «زوج به هم تابیده» (TP) : در ساده‌ترین شکل کابل TP از یک زوج سیم مسی شبیه سیم تلفن تشکیل شده‌اند، اما کابل‌هایی که در شبکه رایانه‌ها مورد استفاده قرار می‌گیرند شامل چهار زوج سیم می‌باشند. علت تابیده بودن سیم‌ها به هم آن است که اولاً میدان مغناطیسی در اطراف خود بر اثر القاء به وجود نیاورند و ثانیاً اثرات نویز القاء شده روی خود را تا اندازه‌ای خنثی نمایند.

هر زوج برای یک کانال ارتباطی مخابراتی مورد استفاده قرار می‌گیرد. کابل TP در هم‌بندی ستاره‌ای و حلقوی مورد استفاده قرار می‌گیرد.

شکل ۳ــ۴ــ کابل زوج به هم تابیده TP

● **مزایا و معایب کابل TP**

۱ــ کابل TP توانایی انتقال بالاتری نسبت به Coaxial دارد.

۲ــ نویز اثر بیشتری روی TP دارد.

۳ــ مشکل همشنوایی[۱] (Cross Talk) در TP وجود دارد.

۴ــ کابل TP نسبت به Coaxial ارزان‌تر می‌باشد.

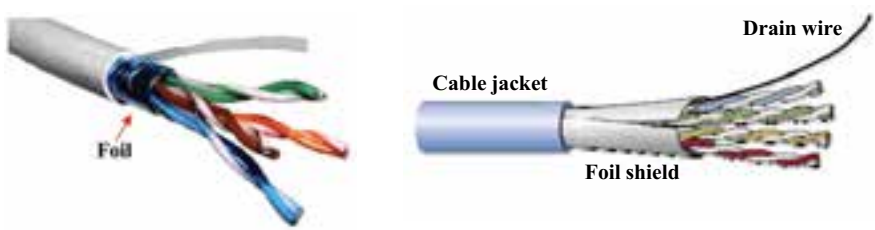
۵ــ کابل TP نسبت به Coaxial مقاومت کمتری در مقابل میرایی سیگنال‌ها دارد.

کابل‌های TP در دو نوع محافظ‌دار (Shielded) و بدون‌محافظ (Unshielded) ساخته می‌شوند که به نام‌های STP[۲] و UTP[۳] در بازار موجود می‌باشند.

کابل زوج به هم تابیده STP یا محافظ دار — کابل زوج به هم تابیده UTP یا بدون محافظ

شکل ۴ــ۴ــ کابل زوج به هم تابیده STP و UTP

نکته: اگر محافظ کابل TP از جنس فویل آلومینیومی باشد به آن FTP[۴] می‌گویند.



شکل ۵ــ۴ــ کابل FTP

۱ــ علی رغم اینکه به هم تابیدن سیم‌ها باعث می‌شود تا از ایجاد میدان در اطراف سیم‌ها جلوگیری شود. ولی میدان ضعیفی به وجود می‌آید و باعث پدیده همشنوایی بر زوج سیم مجاور می‌شود

۲ــ Sh e ded Tw sted Pa r

۳ــ Unsh e ded Tw sted Pa r

۴ــ Fo sh e d Tw sted Pa r

نکته: اگر هر زوج سیم به طور جداگانه محافظ (فویل آلومینیوم یا سیم بافته شده) داشته و مجموعه آنها نیز محافظ داشته باشند، به آن نوع کابل SSTP می‌گویند که به دوصورت FFTP، SFTP وجود دارند.

شکل ۶ــ۴ــ کابل SFTP

کابل TP صرف‌نظر از UTP یا STP بودن براساس حداکثر سرعت و نوع کاربردی که در شبکه‌های رایانه‌ای دارند، به چند دسته یا Category تقسیم می‌شوند که به صورت عدد Cat مانند (Cat 5) نمایش داده می‌شوند.

جدول ۱ــ۴ــ رده‌های مختلف کابل زوج سیم به هم تابیده

نام گروه	سرعت	فرکانس کار
Cat ۱	حداکثر ۱ Mbps	
Cat ۲	حداکثر ۴ Mbps	
Cat[۱]۳	حداکثر ۱ Mbps	۱۶ MHz
Cat[۲]۴	حداکثر ۲ Mbps	۲ MHz
Cat ۵	حداکثر ۱ Mbps	۱ MHz
Cat ۵e[۳]	حداکثر ۱ Mbps	۱ MHz
Cat ۶	حداکثر ۱Gbps	۲۵ــ۲ MHz
Cat ۶a[۴]	حداکثر ۱ Gbps	۵ MHz
Cat ۷[۵]	حداکثر ۱ Gbps	۶ MHz

۱ــ به طور عمده در سیستم کابل کشی آی بی ام برای شبکه‌های Token R ng استفاده می‌شود

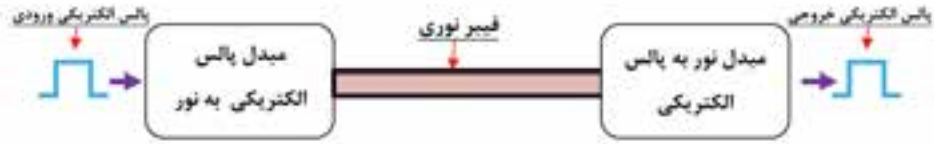
۲ــ فقط در شبکه Token R ng با حداکثر تا ۱۶ مگابیت بر ثانیه مورد استفاده قرار گرفت.

۳ــ با چهار رشته سیم (دو زوج) حداکثر سرعت ۱۰۰ Mbps و با ۸ رشته سیم (۴ زوج) دارای سرعت حداکثر ۱۰۰۰ Mbps می‌باشد و e مخفف enhanced می‌باشد.

۴ــ a مخفف Augmented به معنی تکمیل شده می‌باشد.

۵ــ از سال ۲۰۱۰ وارد بازار شده است و از سوکت GG۴۵ برای اتصال به کابل از آن استفاده می‌شود.

ج) **کابل «فیبر نوری»** : فیبر نوری یکی از محیط‌های انتقال داده با سرعت بالا است. فیبر نوری داده‌های دیجیتال (پالس‌های الکتریکی[1]) را به صورت پالس‌های نور[2] هدایت می‌کند پس در دو انتهای فیبر نوری مبدل‌های پالس الکتریکی به نور و بالعکس وجود خواهد داشت.



شکل ۷ــ۴ــ دیاگرام انتقال داده در فیبر نوری

یک کابل فیبر نوری از پنج بخش تشکیل شده است :

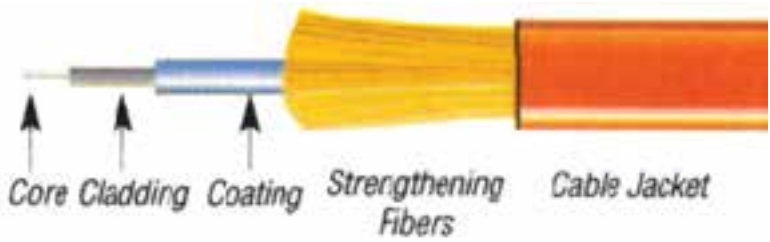
۱ــ هسته (Core) : هسته نازک شیشه ای در مرکز فیبر که سیگنال‌های نوری در آن حرکت می‌نمایند.

۲ــ روکش (Cladding) : بخش خارجی فیبر بوده که دورتادور هسته را احاطه کرده و باعث برگشت نورمنعکس شده به هسته می‌گردد.

۳ــ بافر رویه (Buffer Coating). روکش پلاستیکی رنگی که باعث حفاظت و نگهداری فیبر می‌شود و همچنین برای تشخیص فیبر در سر دیگر کابل برای اتصال سوکت‌ها.

۴ــ الیاف قوی (Strengthening fibers) : برای بالا بردن قدرت کشش کابل فیبر نوری

۵ــ روکش بیرونی کابل (Cable Jacket) : روکش پلاستیکی بیرونی کابل فیبر نوری



شکل ۸ ــ۴ــ اجزای تشکیل‌دهنده یک کابل فیبر

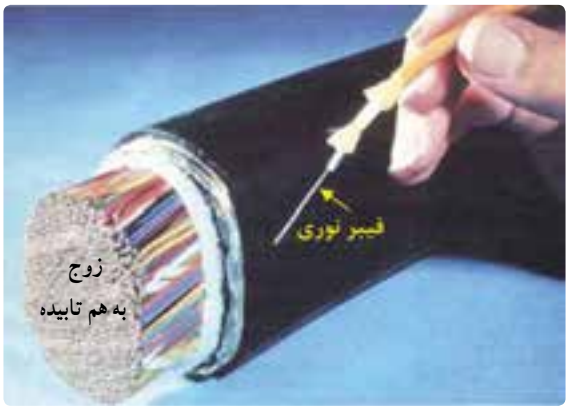
۱ــ E ectr ca Pu se

۲ــ L ght Pu se

از آنجایی که تار فیبر نوری انتقال داده را در یک جهت انجام می‌دهد، به همین منظور برای اتصال کابل فیبر نوری به کارت شبکه از دو تار فیبر نوری استفاده می‌شود. (یک تار برای ارسال و یک تار برای دریافت).

شکل ۹ــ۴ــ کابل فیبر نوری برای اتصال به کارت شبکه تک رشته‌ای

یک تار فیبر نوری معادل ۹۰۰ زوج سیم مسی قدرت انتقال اطلاعات را دارد.



شکل ۱۰ــ۴ــ مقایسه فیبر نوری با کابل مسی

فیبرهای نوری در دو گروه عمده ارائه می‌گردند :

ــ ***فیبرهای تک حالته (Single ـ Mode) یا SM***. به‌منظور ارسال یک سیگنال در هر فیبر استفاده می‌شود.

ــ ***فیبرهای چندحالته(Multi ـ Mode) یا MM***. به‌منظور ارسال چندین سیگنال در یک فیبر استفاده می‌شود.

فیبرهای تک حالته (SM) دارای یک هسته کوچک (به قطر ۶ تا ۸ میکرون) بوده، اما فیبرهای چند حالته (MM) دارای هسته بزرگتر (به قطر ۵۰ تا ۱۰۰ میکرون) می‌باشند.

شکل۱۱ــ۴ــ فیبر تک حالته و چند حالته

تا فاصله ۱۰ کیلومتر از فیبرهای MM و برای فواصل بیشتر از ۱۰ کیلومتر از فیبرهای SM استفاده می‌گردد.

● **مزایا و معایب فیبر نوری** : فیبر نوری در مقایسه با سیم‌های مسی دارای مزایای زیر است :

۱ــ امکان استفاده در فواصل طولانی‌تر.

۲ــ نرخ انتقال بیشتر(پهنای باند فیبر نوری به منظور ارسال اطلاعات به مراتب بیشتر از سیم مسی است).

۳ــ عدم نویزپذیری نسبت به میدان‌های مغناطیسی.

۴ــ امنیت بیشتر به دلیل عدم امکان انشعاب گرفتن در بین مسیر بدون داشتن امکانات پیشرفته و تخصصی.

۵ــ تضعیف ناچیز (تضعیف سیگنال در فیبر نوری به‌مراتب کمتر از سیم مسی است).

۶ــ عدم اتصالی در فیبر نوری، بر خلاف سیم‌های مسی که با از بین رفتن روکش سیم امکان اتصالی وجود دارد.

فعالیت کارگاهی

۲ــ۴ــ طراحی و پیاده سازی یک شبکه رایانه‌ای به لحاظ سخت‌افزاری

مراحل پیاده سازی سخت افزاری یک شبکه رایانه‌ای را می‌توان به ترتیب زیر بیان نمود.

۱ــ تصمیم‌گیری در مورد نوع شبکه تعیین نوع کانال ارتباطی (سیمی‌و بی سیم)

۲ــ تهیه نقشه اجرایی : یکی از مهمترین بخش‌های طراحی شبکه، تهیه نقشه شبکه است که معمولاً از نقشه پلان ساختمان استفاده می‌شود که در آن مسیر عبور کابل‌ها و محل نصب پریزهای شبکه و سرور و سایر تجهیزات شبکه مشخص می‌شود

که با استفاده از نقشه اجرایی می‌توان میزان کابل مصرفی و تعداد پریزهای شبکه و... را تعیین نمود برای نمونه پلان یک ساختمان اداری در دو حالت ساده و با چیدمان نشان داده شده است.

شکل ۱۲ــ۴ــ نقشه پلان ساده یک ساختمان اداری

پلان یک اداره با چیدمان

شکل ۱۳ــ۴ــ نقشه پلان یک ساختمان اداری با چیدمان آن

۳ــ انتخاب و تهیه سخت افزار مورد نیاز با توجه به دو مرحله قبلی انجام می‌گیرد که در ادامه به طور کامل تشریح خواهد شد.

۴ــ کابل کشی یا نصب و راه اندازی محیط انتقال (برای شبکه‌های سیمی).

۵ــ ایجاد اتصالات و نصب قطعات (ایجاد اتصالات در شبکه سیمی مورد استفاده قرار می‌گیرد).

۱ــ۲ــ۴ــ انتخاب و تهیه سخت افزار مورد نیاز در شبکه سیمی

سخت‌افزارها در شبکه به دو دسته Passive Devices (وسایل غیرفعال یا منفعل) و Active Devices (وسایل فعال) تقسیم‌بندی می‌شوند :

● **Active Device** : تجهیزات فعال، معمولاً دارای منبع تغذیه هستند و توانایی تولید یا بازسازی سیگنال را دارند به عبارت دیگر، به تجهیزاتی که قابلیت کنترل سیگنال‌های الکتریکی را دارند تجهیزات فعال یا Active Devices می‌گویند مانند کارت شبکه یا NIC[۱] (کنترل کننده رابط شبکه) یا سوئیچ‌ها[۲]

● **Pa ssive Device** : تجهیزات غیرفعال، تجهیزاتی هستند که در مقابل سیگنال الکترونیکی (یا نوری)، رفتاری غیرفعال دارند. به عبارت دیگر، این تجهیزات توانایی تقویت سیگنال را ندارند و تنها نظاره‌گر عبور آن‌ها هستند که ممکن است منجر به تضعیف سیگنال نیز بشود، نمونه‌ای از تجهیزات غیرفعال عبارتند از :

انواع کابل‌ها، پریز شبکه و کیستون، رک، داکت یا ترانک (کانال پلاستیکی)، آچارهای شبکه.

الف) کارت شبکه یا NIC : رابط فیزیکی بین رایانه‌ها و کابل شبکه می‌باشد و یک Active Device محسوب می‌شود پس باید تمام رایانه‌ها در شبکه اعم از سرویس‌دهنده و سرویس‌گیرنده مجهز به کارت شبکه باشند. کارت شبکه دارای اسامی دیگری چون LAN Card و Network Adapter می‌باشد.

کارت شبکه باید متناسب با کابل شبکه انتخاب شود، یعنی کارت شبکه باید هم از لحاظ نوع کابل (کواکسیال یا زوج به هم تابیده) و هم از لحاظ سرعت باید متناسب

۱ــ Network Interface Contro er

۲ــ Sw tch

با یکدیگر باشند مثلاً اگر نوع کابل شبکه از نوع Cat6 انتخاب شده است و قرار است رایانه‌ها با سرعت ۱۰۰۰ مگا بیت بر ثانیه با یکدیگر در ارتباط باشند باید از کارت شبکه Gigabit استفاده شود. یا اگر جایی قرار است به جای کابل مسی از فیبر نوری استفاده شود باید کارت شبکه دارای درگاه فیبر نوری باشد.

معمولاً کارت‌های شبکه رایانه سرویس‌دهنده دارای پردازنده مجزا از پردازنده سیستم بوده و در شکاف توسعه PCI_Express در برد اصلی جایگذاری می‌شوند، اما سایر کارت‌های شبکه در شکاف توسعه PCI در برد اصلی جایگذاری می‌گردند.

● ***انواع کارت شبکه با کابل سیمی:*** کارت شبکه داخلی[1] که در شکاف توسعه روی برد اصلی جایگذاری می‌شود و امروزه غالباً در دو نوع زیر وجود دارند

● ***PCI :*** برای سرعت حداکثر ۱۰۰۰ مگابیت بر ثانیه که غالباً برای رایانه‌های سرویس گیرنده مورد استفاده قرار می‌گیرد(شکل ۱۴ـ۴).

● ***PCI ـــ Express :*** برای سرعت بالاتر از ۱۰۰۰ مگابیت برثانیه و برای سرویس‌دهنده‌ها استفاده می‌شود. (شکل۱۴ـ۴).

ـ کارت شبکه مخصوص لپ تاپ PCMCIA[2] یا PC card لازم به ذکر است که اغلب لپ تاپ‌ها دارای کارت شبکه بیسیم می‌باشد.

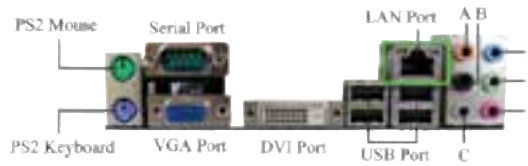
ـ کارت شبکه USB (شکل ۱۴ـ۴)

امروزه اکثر بردهای اصلی رایانه‌های شخصی مجهز به کارت شبکه Onboard می‌باشند که با درگاه RJ_۴۵ و با سرعتGbps ۱ و یا Mbps ۱۰۰ می‌توانند در مدار قرار گیرند. در شکل ۱۴ـ۴ نمونهٔ کارت‌های شبکه نمایش داده شده است. به کارت شبکه ای که دارای دو درگاه (پورت) مختلف هستند کارت شبکه ترکیبی (Combo) می‌گویند.

۱ـ Interna

۲ـ Persona Computer Memory Card Internat ona Assoc at on

کارت شبکه Token Ring



شکل ۱۴ــ۴ــ انواع کارت‌های شبکه

انواع کارت شبکه در شبکه فیبر نوری

● در شبکه فیبرنوری نیز دو نوع کارت شبکه وجود دارد :

۱ــ PCI یا PCI ــ Express که برروی شکاف توسعه برروی برد اصلی جایگذاری می‌شود.

۲ــ کارت شبکه فیبر نوری PCMCIA

شکل ۱۵ــ۴ــ انواع کارت شبکه در شبکه فیبر نوری

● وظایف کارت شبکه

۱ــ آماده سازی داده از رایانه برای انتقال به کابل شبکه.

۲ــ ارسال داده به رایانه‌های دیگر در شبکه.

۳ــ کنترل جاری شدن داده‌ها بین رایانه و سیستم کابل کشی.

۴ــ دریافت داده از کابل شبکه و تبدیل آنها به داده‌های قابل پردازش برای پردازنده مرکزی رایانه[۱].

ب) سوئیچ‌ها در شبکه

یکی دیگر از تجهیزات فعال شبکه، سوئیچ‌ها می‌باشند، باید توجه داشت که هاب (HUB) در شبکه هم‌بندی ستاره‌ای یک وسیله فعال به شمار نمی‌آید بلکه یک وسیله Passive می‌باشد، زیرا هیچ کنترلی بر روی داده دریافتی ندارد.

۱ــ CPU

شکل ۱۶ــ۴ــ انواع سوئیچ

یکی دیگر از قطعات فعال در شبکه فیبر نوری، مبدل فیبر به سوکت RJ45 می‌باشد.

شکل ۱۷ــ۴ــ مبدل فیبر نوری به سوکت RJ45

Passive Devices

الف) پریز شبکه

پریزهای شبکه در دو نوع وجود دارند، مدل روکار و مدل تو کار

پریزهای شبکه توکار دارای دو بخش اصلی جعبه پایه (Base Box) و درپوش (Face Plate) می‌باشند و کیستون بر روی درپوش نصب می‌شود و معمولاً برای کابل کشی توکار استفاده شده و داخل دیوار نصب می‌شوند (البته می‌توان به صورت روکار هم مورد استفاده قرار داد.)

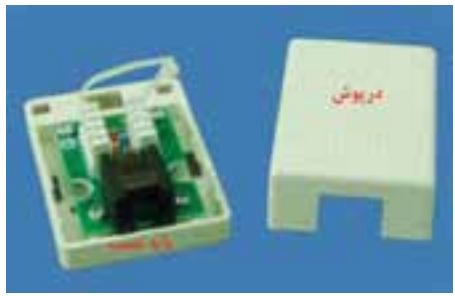
Face Plate 4 port | Face Plate 3 port | Face Plate 1 port | Base Box

شکل ۱۸ــ۴ــ پریز شبکه توکار

نوع دیگری از پریزهای توکار وجود دارد که در کف زمین نصب می‌شوند.

شکل ۱۹ــ۴ــ پریز توکار برای کف

پریزهای روکار دارای دو بخش پایه و درپوش می‌باشند و کیستون بر روی پایه نصب شده و پایه نیز برروی دیوار با چسب دورو و یا با پیچ و رول پلاک نصب می‌گردد.



پریز روکار درپوش‌دار یا Shutter

پریز روکار بدون درپوش با کیستون

شکل ۲۰ــ۴ــ اجزای پریز روکار

کیستون: کابل‌ها به کیستون متصل می‌شوند و کیستون‌ها دارای رنگ‌بندی مشخص جهت اتصال کابل می‌باشند و در دونوع معمولی و بدون ابزارعرضه می‌شود.

کیستون بدون ابزار: برای مونتاژکابل بر روی آن به ابزار خاصی نیاز نمی‌باشد.

شکل ۲۱ــ۴ــ کیستون بدون ابزار

کیستون معمولی: برای مونتاژ کابل بر روی آن به ابزار خاصی به نام پانچ[1] یا منگنه نیاز می‌باشد.

شکل ۲۲ــ۴ــ کیستون معمولی

ب) ابزار پانچ: از این ابزار برای مونتاژ کابل بر روی کیستون استفاده می‌شود.

شکل ۲۳ــ۴ــ ابزار پانچ

ج) Patch chord cable : کابلی است که به عنوان رابط بین رایانه و پریز شبکه (کیستون) و همچنین رابط بین پانچ پانل (قطعه‌ای که داخل رک نصب می‌شود) و سوئیچ به کار می‌رود و در طول‌های نیم متر تا ۵ متر موجود می‌باشد.

پچ کورد به صورت آماده در بازار عرضه می‌شود و با وجود آن نیازی به سوکت زدن به سرکابل‌ها نمی‌باشد.

۱ــ Punch

پچ کورد UTP　　پچ کورد فیبر نوری　　پچ کورد STP

شکل ۲۴ــ۴ــ انواع پچ کورد

د) ***Patch Panel*** : در هنگام کابل‌کشی یک سر کابل به داخل پریز شبکه (کیستون) متصل بوده و سر دیگر آن به پچ پانل متصل می‌گردد، برای اتصال کابل به پچ پانل از ابزار پانچ استفاده می‌شود (مانند کیستون). در پچ پانل نیز جدول رنگ برای اتصال کابل وجود دارد پچ پانل‌ها معمولاً در اندازه‌های ۱۲؛ ۱۶؛ ۲۴؛ ۳۶ و ۴۸ عرضه می‌شوند.

پچ پانل‌ها در دو مدل Unloaded و Loaded ساخته می‌شوند. در پچ پانل‌های Loaded تمامی‌پورت با کیستون پر شده است اما مدل Unloaded بدون کیستون بوده و به دلخواه می‌توان در هر کدام از پورت‌ها کیستون قرار داد.

در انتها به کمک کابل‌های پچ کورد نیم یا یک متری از پشت پچ پانل، آن را به سوئیچ متصل می‌کنند.

شکل ۲۵ــ۴ــ اتصال کابل‌ها به پچ پانل

شکل ۲۶ــ۴ــ انواع پچ پانل بدون کیستون Unloaded Patch

شکل ۲۷ــ۴ــ پچ پانل با کیستون Loaded Patch Panel

شکل ۲۸ــ۴ــ کابل‌کشی پشت پچ پانل Loaded Patch Panel

برای دسته‌بندی کابل‌ها از بست‌های پلاستیکی استفاده می‌شود.

شکل ۲۹ــ۴ــ بست پلاستیکی بر دسته‌بندی کابل‌ها

هـ) ***Cable Management*** : برای نظم دادن به کابل های پچ کورد از کانال‌های درپوش داری به نام Cable Management استفاده می‌شود.

شکل ۳۰ــ۴ــ Cable Management

و) ***رک (Rack)*** : رک یک محفظه فلزی است که تجهیزات شبکه مانند پچ پانل؛ سوئیچ ؛ مودم ؛ Cable Management (در بعضی از مدل‌ها رایانه سرویس‌دهنده و

رایانه پشتیبان سرور) و UPS در آن نگهداری می‌شود. واحد اندازه رک یونیت (Unit) می‌باشد و هر یونیت معادل ۵ سانتی‌متر می‌باشد. درحال حاضر اندازه رک‌ها از ۴U تا ۴۴U می‌باشد. به طور کلی دو مدل کلی رک وجود دارد : رک دیواری و رک ایستاده.

رک دیواری : به دیوار مهار(پیچ) می‌شوند و در واحدهای کوچک کاربرد دارد.

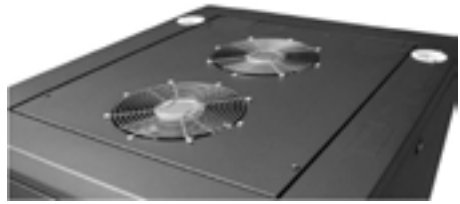
شکل ۳۱ــ۴ــ رک دیواری

رک ایستاده : از این رک‌ها جهت قرارگیری در مرکز شبکه (اتاق سرور) استفاده می‌شود این مدل رک‌ها ورودی‌های کابل از بالا و پایین و همچنین امکان باز شدن از چهار طرف را فراهم می‌آورند در این نوع رک علاوه بر سوئیچ‌ها و پچ پانل؛ امکان قرارگیری رایانه سرویس‌دهنده و پشتیبان سرویس دهنده و هم‌چنین UPS در داخل آن وجود دارد.

شکل ۳۲ــ۴ــ انواع رک‌های ایستاده

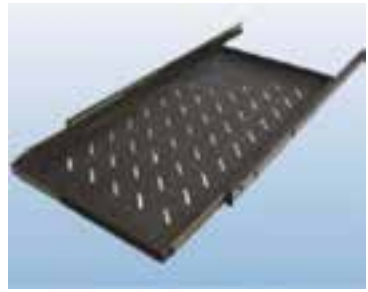
اجزای مهم رک عبارتند از :

● ***Fan*** : برای خنک نگهداشتن و تهویه صحیح تجهیزات داخل رک از تعدادی فن در سقف و کف رک استفاده می‌شود.



شکل ۳۳ــ۴ــ فن‌های رک

● ***Shelf Sliding (قفسه کشویی)*** : به سینی داخل رک گفته می‌شود و کاربرد آن برای قرار دادن صفحه نمایش ؛ ماوس و صفحه کلید و همچنین رایانه می‌باشد این سینی دارای دو نوع متحرک و ثابت بوده و نوع متحرک آن غالباً در رک‌های ایستاده مورد استفاده قرار می‌گیرد.



شکل ۳۴ــ۴ــ قفسه کشویی داخل رک

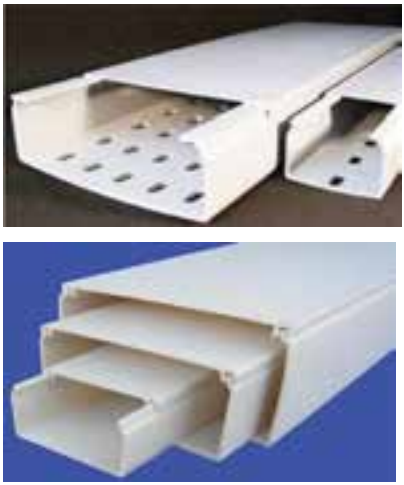
● ***Power Module (ماژول برق)*** : قطعه ای است که دارای چند پریز برق بوده و برای تغذیه سوئیچ‌ها و رایانه و مانیتور داخل رک مورد استفاده قرار می‌گیرد و معمولاً ماژول‌های برقی دارای ۴ و یا ۸ پریز می‌باشند.

شکل ۳۵ــ۴ــ ماژول برق در داخل رک

● ***Light Panel*** *:* محلی برای قرار گرفتن لامپ فلورسنت در بالای رک به منظور تأمین روشنایی درون رک Light Panel و معمولاً یک یونیت را اشغال می‌کند.

● ***Thermometer (دماسنج)*** *:* این دماسنج در بالاترین قسمت رک نصب شده و به طور مداوم دمای داخل آن را اندازه گیری کرده و نمایش می‌دهد در بعضی از رک‌ها این امکان وجود دارد که در حرارت خاصی فن رک‌ها شروع به کار کنند.

ز) Trunk و Duct *:* داکت محفظه‌ای است غالباً از جنس پلاستیک که برای قرار گرفتن کابل‌های شبکه داخل آن مورد استفاده قرار می‌گیرد.



شکل ۳۶ــ۴ــ داکت

ترانک‌ها علاوه بر فضا جهت عبور کابل، معمولاً مکانیزمی دارند که می‌توان بر روی آنها پریز برق، پریز شبکه و انواع پریزها را داخل ماژول‌های خاص قرار داد و ماژول‌ها را درون بدنه ترانک نصب نمود. ترانک‌ها همچنین قابل پارتیشن‌بندی می‌باشند، پارتیشن قطعه‌ای است که در داخل ترانک قرار گرفته و آن را به دو یا سه قسمت مجزا برای کابل‌های برق و تلفن و... تقسیم‌بندی می‌کند تا از ایجاد نویز جلوگیری گردد. ضمناً داکت‌ها حجم کمتری نسبت به ترانک‌ها اشغال می‌کنند. جنس ترانک‌ها معمولاً از PVC مقاوم در برابر ضربه و حرارت بوده و بادوام‌تر و مطمئن‌تر و شیک‌تر از داکت‌ها می‌باشند.

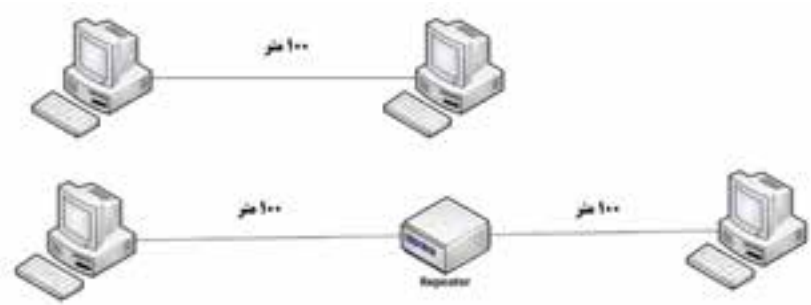
شکل ۳۷ــ۴ــ ترانک

در صورتی که لازم باشد کابل کشی شبکه به صورت روکار صورت پذیرد، مطابق با نقشه شبکه باید بخش پایین داکت یا ترانک روی دیوار نصب شده سپس کابل‌ها داخل کانال قرار گرفته و در نهایت باید درپوش داکت یا ترانک بسته شود.

داکت‌ها در اندازه‌های ۱ تا ۱۰ سانتی متر موجود می‌باشد و ترانک‌ها در عرض‌های ۲ تا ۲۰ سانتی‌متر ساخته می‌شوند.

ح) کابل شبکه و کانکتورها : کابل‌های شبکه معمولاً در بسته‌های ۱۰۰؛ ۳۰۵؛ ۵۰۰ و ۱۰۰۰ متری عرضه می‌گردند. باید توجه داشت که قبل از تهیه کابل با استفاده نقشه ؛ متراژ کابل مورد نیاز محاسبه گردد. در هنگام استفاده از کابل ابتدا باید متراژ دورترین گره محاسبه شده و به ترتیب از دورترین تا نزدیکترین گره متراژ مورد نیاز محاسبه و مجموع آن‌ها برآورد گردد.

ما در این فصل می خواهیم از کابل های زوج به هم تابیده و فیبر نوری استفاده شود. باید توجه داشت که حداکثر طول هر سگمنت کابل زوج به هم تابیده نباید از ۱۰۰ متر بیشتر باشد و برای فواصل بیش از ۱۰۰ متر باید از سوئیچ تقویت‌کننده سیگنال (Repeater) استفاده نمود.



شکل ۳۸ــ۴ــ استفاده از Repeater برای فواصل بیش از ۱۰۰ متر در کابل زوج سیم به هم تابیده

کابل زوج به هم تابیده از کابل‌های رایج در شبکه می‌باشند و از چهار زوج سیم به هم تابیده تشکیل شده است (هشت رشته که چهار رشته رنگی و چهار رشته دیگر مخلوط رنگ سفید با رنگ زوج مربوطه می‌باشد)

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

شکل ۳۹ــ۴

شماره‌گذاری زوج‌ها بر اساس استاندارد T568B[1] می‌باشد.

در شبکه‌های با سرعت ۱۰ و ۱۰۰ مگابیت بر ثانیه از دو زوج سیم استفاده می‌شود (زوج‌های دو (نارنجی) و سه (سبز)) و زوج‌های یک. چهار سیم (دو زوج) به عنوان رزرو باقی می‌مانند به طوری از دو زوج رزرو هم می‌توان به عنوان خط اترنت دوم و یا اتصالات تلفن استفاده نمود.

در شبکه‌های با سرعت ۱۰۰۰ مگابیت بر ثانیه (یا گیگابیت بر ثانیه) از هر چهار زوج استفاده می‌شود.

در کابل زوج به هم تابیده از سوکت RJ45 شبیه سوکت تلفن ولی با هشت پایه استفاده می‌شود.

شکل ۴۰ــ۴ــ سوکت Rj45

ط) آچار پرس RJ45 و سیم چین و روکش بردار[2] : این ابزارها به عنوان ابزارهای کار برای ایجاد اتصالات سوکت به کابل شبکه مورد استفاده قرار می‌گیرد.

آچار پرس RJ45 روکش‌بردار سیم‌چین

شکل ۴۱ــ۴ــ ابزارهای کار برای ایجاد اتصالات سوکت به کابل شبکه

۱ ــ در بخش‌های بعدی تشریح خواهد شد

۲ ــ Str pper برای برداشتن روکش خارجی کابل

ی) تستر کابل شبکه : برای بررسی اینکه کابل به درستی به سوکت‌های دو طرف کابل وصل شده است یا خیر؛ مورد استفاده قرار می‌گیرد.

شکل ۴۲ــ۴ــ تستر کابل شبکه

نحوه کار با تستر شبکه به این صورت است که یک سر کابل به قسمت اصلی تستر (A) به سوکت RJ45 متصل شده و سر دیگر کابل به قسمت فرعی (B) تستر متصل می‌شود. سپس تستر را روشن کرده تا LEDهای روی تستر اصلی و فرعی به ترتیب از شماره ۱ تا ۸ روشن شوند، مرتب روشن شدن LEDها نشان‌دهنده تماس درست سوکت با کابل و هم چنین ترتیب درست اتصالات براساس رنگ‌بندی می‌باشد چنانچه ترتیب روشن شدن LEDها در دو بخش A و B تستر هماهنگ نباشد به این معنی است که رنگ‌بندی اتصالات به درستی رعایت نشده است.

۲ــ۲ــ۴ــ کابل کشی و ایجاد چاه زمین (در صورت استفاده از کابل‌های STP) : عوامل مؤثر در تعیین نوع کابل کشی عبارتند از :

۱ــ سنگینی ترافیک شبکه

۲ــ طول کابل کشی

۳ــ بودجه تعیین شده برای کابل‌کشی

۴ــ نیازهای ایمنی شبکه

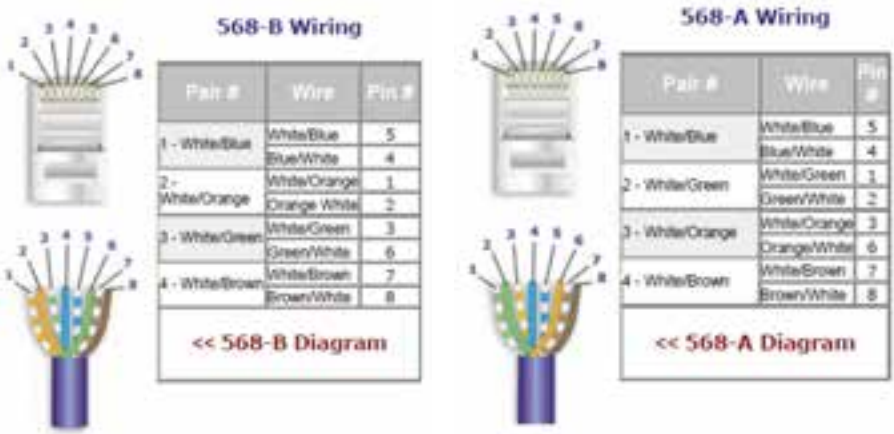
۵ــ نوع کابل‌های موجود

در نیازهای ایمنی شبکه یکی از نکات مورد توجه رعایت فاصله مناسب با کابل برق و وسایل الکتریکی دارای سیم‌پیچ یا بوبین (مانند انواع موتورهای الکتریکی و ترانسفرماتورها) می‌باشد. زمانی که کابل برق به موازات کابل شبکه می‌باشد متناسب با جریان عبوری از کابل برق حداقل فاصله بین کانال برق و شبکه باید بین ۵ تا ۳۰ سانتی‌متر و در شرایطی نیز بیش از آن باشد.

۳ــ۲ــ۴ــ ایجاد اتصالات و نصب قطعات : دو نوع استاندارد برای کابل‌کشی توسط سازمان TIA[۱] (انجمن صنعتی مخابرات) ارائه گردیده است که تنها تفاوت این دو استاندارد در رنگ‌بندی آن‌ها در اتصالات می‌باشد و تفاوت دیگری با هم ندارند در این دو نوع استاندارد از سوکت RJ45 برای اتصالات دو سر کابل‌ها استفاده می‌گردد.

۱ــ T568A : معمولاً از این استاندارد در اروپا و کانادا استفاده می‌شود رنگ‌بندی آن در شکل ۴۳ــ۴ آمده است.

۲ــ T568B : معمولاً از این استاندارد در ایران استفاده می‌شود رنگ بندی آن در شکل ۴۳ــ۴ نشان داده شده است. (در آمریکا نیز از این استاندارد استفاده می‌گردد).



شکل ۴۳ــ۴ــ رنگ‌بندی استانداردهای T568A و T568B

۱ــ Te ecommun cat on Industr a Assoc at on

با توجه به رنگ‌بندی دو استاندارد مشخص می‌شود که شماره‌های فرد همواره سفید با نوار رنگی می‌باشد.

مراحل اتصال کانکتور RJ45 به دو سر کابل

مرحله اول : ابتدا ۲۵ میلی متر از روکش کابل را با استفاده از ابزار روکش بردار (Stripper) بردارید.

شکل ۴۴ــ۴ــ روکش‌برداری از کابل شبکه

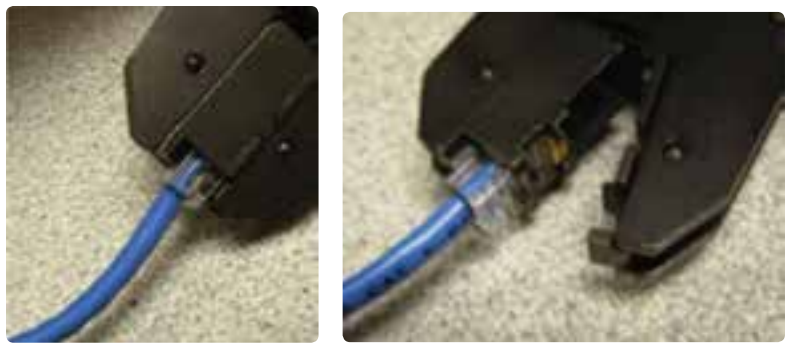
مرحله دوم : زوج‌ها را از هم جدا کنید و سپس با استفاده از انگشتان دست (انگشت شست و انگشت اشاره) بر اساس یکی از استانداردها (568A یا 568B) سیم‌ها را صاف و مرتب نموده و در فاصله ۱۲ الی۱۳میلی متری از روکش کابل سیم‌ها را با استفاده از سیم چین یا قیچی برش کابل قطع کنید.توجه داشته باشید که زاویه سیم‌چین و سیم‌های مرتب شده حدوداً ۹۰ درجه باشد.

شکل ۴۵ــ۴ــ برش سیم‌های کابل شبکه

مرحله سوم : بار دیگر به ترتیب رنگ‌بندی سیم‌ها دقت کرده و سپس سیم را به داخل سوکت هدایت کنید به طوری که سیم‌ها به طور کامل وارد سوکت شوند. باید توجه داشته باشید حداقل ۵ میلی‌متر از روکش کابل داخل سوکت باشد. برای اطمینان کابل را به داخل سوکت فشار دهید.

شکل ۴۶ــ۴ــ سوکت زدن به سر کابل

مرحله چهارم : سوکت را داخل انبر شبکه قرار داده و با فشار اهرم‌های انبر سوکت را پرس نمایید.



شکل ۴۷ــ۴ــ پرچ سوکت‌های کابل شبکه

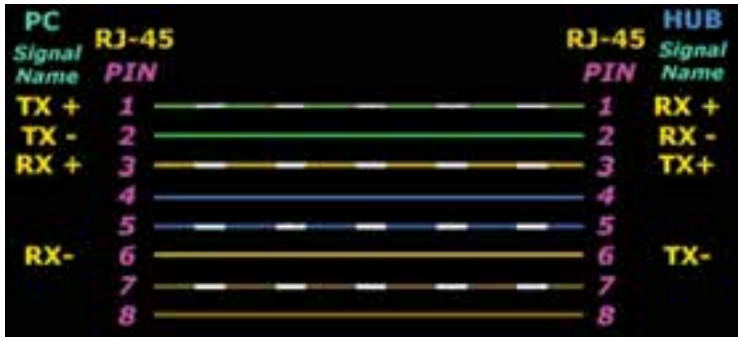
نکته: اگر روکش کابل را از اندازه مجاز بیشتر بر دارید سوکت بر روی روکش کابل پرس نمی‌شود.

شکل ۴۸ــ۴ــ روکش‌برداری مناسب و نامناسب کابل‌های شبکه

همانطور که پیش تر اشاره شد، در شبکه 100Mbps تنها از دو زوج (یا چهار رشته شماره ۱و۲و۳و۴) برای انتقال استفاده می‌شود و از سایر پایه‌ها استفاده نشده است در شکل ۴۷ــ۴، tx به معنای ارسال کننده و rx به معنای دریافت‌کننده می‌باشد) اما در شبکه‌های 1000mbps از تمام هشت رشته سیم برای ارسال و دریافت استفاده می‌شود. سوئیچ، پس از دریافت سیگنال از پایه TX یک ایستگاه آن را روی پایه RX ایستگاه مقصد ارسال می‌نماید. اما اگر در مواقعی لازم باشد دو رایانه یا دو سوئیچ را مستقیماً به یکدیگر متصل نماییم، از چه کابلی استفاده کنیم؟ یعنی درحالتی برای جابه‌جا کردن سیگنال از پایه ارسال به پایه دریافت از سوئیچ استفاده نمی‌شود، باید جابه‌جایی در سطح کابل انجام شود.

کابل Straight یا مستقیم : اگر در زمان سوکت زدن دو سر کابل از یک استاندارد (568A و 568B) استفاده شود کابل را Straight می‌گویند و به‌طور معمول برای اتصال رایانه به پریز شبکه (کیستون) یا برای اتصال مستقیم رایانه به سوئیچ یا پانل مورداستفاده قرار می‌گیرد.

در زمان استفاده از کابل Straight اگر سرعت شبکه ۱۰ یا ۱۰۰ مگابیت برثانیه باشد فقط از ۴ رشته سیم استفاده می‌شود (از زوج‌های سبز و نارنجی استفاده می‌گردد).



شکل ۴۹ــ۴ــ اتصالات کابل Straight برای کابل Cat5 با سرعت ۱۰ یا ۱۰۰ مگابیت بر ثانیه با استاندارد

بنابراین زمانی که رایانه به‌هاب یا سوئیچ متصل می‌شود، پایه TX رایانه به پایه RX سوئیچ متصل شده و سوئیچ به صورت خودکار با استفاده از مدارات داخلی خود پایه TX یک رایانه را به پایه TX رایانه دیگر وصل می‌کند.

کابل Crossover یا متقاطع : اگر در زمان سوکت زدن دو سر کابل از دو نوع استاندارد (568A و 568B) استفاده شود کابل را Crossover یا متقاطع می‌گویند. کابل متقاطع به طور معمول برای اتصال دو رایانه به یکدیگر بدون داشتن‌هاب یا سوئیچ استفاده می‌شود. البته برای اتصال دو سوئیچ به هم نیز مورد استفاده قرار می‌گیرد. ضمناً اگر هاب دارای درگاه Uplink باشد، با استفاده از کابل Straight می‌توان دو هاب را به هم متصل نمود، چون Uplink جای TX و RX را با هم عوض نمی‌کند.

علت متقاطع نامیدن کابل به این دلیل می‌باشد که پایه‌های طرف اول به همان پایه‌های طرف دوم متصل نمی‌شوند بلکه مطابق شکل ۵۰ ــ۴ اتصالات جابجا می‌شوند.

شکل ۵۰ــ۴

نحوه اتصال کابل به پریز شبکه یا کیستون

۱ــ حدود ۴ سانتی متر روکش کابل را با استفاده از ابزار روکش بردار (Stripper) بردارید.

شکل ۵۱ــ۴

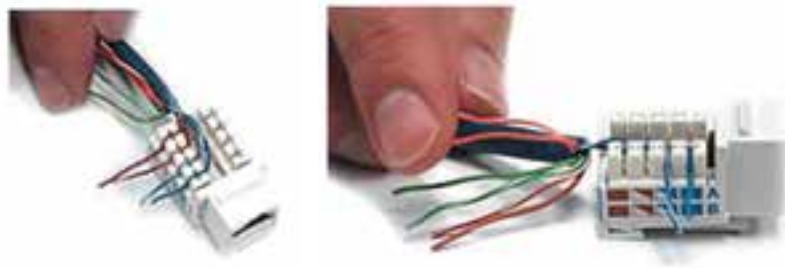
۲ــ زوج‌ها را از هم جدا کنید و سپس با استفاده از انگشتان دست (انگشت شست و انگشت اشاره) بر اساس یکی از استانداردها (568A و یا 568B) سیم‌ها را صاف و مرتب کنید (چهار رشته یک طرف و چهار رشته طرف دیگر).

شکل ۵۲ــ۴

۳ــ درپوش کیستون را بردارید.

شکل ۵۳ــ۴

۴ــ سیم‌ها را مطابق با رنگ تعبیه شده بر اساس استاندارد A یا B داخل شیارها قرار دهید.



شکل ۵۴ــ۴

۵ــ با استفاده از ابزار پانچ ضمن جازدن کامل سیم در شیار قسمت اضافه سیم نیز قطع می‌گردد.

شکل ۵۵ــ۴

۶ــ درپوش کیستون را در جای اصلی قرار دهید و کیستون را در Face plate جاگذاری کنید.

شکل ۵۶ــ۴

۴ــ۲ــ۴ــ تجهیزات شبکه بی سیم

الف) کارت شبکه بی سیم : سه نوع کارت شبکه بی سیم وجود دارد :

۱ــ کارت شبکه بی‌سیم که در شکاف توسعه روی برد اصلی جایگذاری می‌شود و امروزه غالباً در دو نوع زیر وجود دارند.

PCI و PCI_Express

۲ــ کارت شبکه مخصوص لپ تاپ PCMCIA [۱] یا PC card (شکل۵۷ــ۴) لازم به ذکر است که اغلب لپ تاپ‌ها دارای کارت شبکه بی سیم می‌باشند.

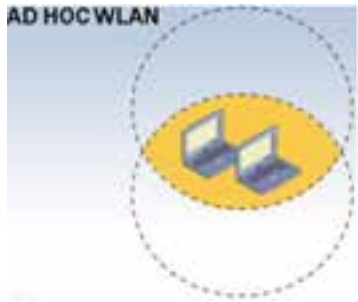
۳ــ کارت شبکه بی‌سیم USB که می‌توان هم به رایانه‌های رومیزی و هم لپ تاپ متصل نمود.

شکل ۵۷ــ۴ــ انواع کارت شبکه‌های بی‌سیم

ب) Access Point [۲] یا A.P : هنگامی که لازم باشد بین رایانه‌های یک شبکه که دارای کارت شبکه بی‌سیم هستند ارتباط برقرار شود، از Access Point استفاده می‌شود البته این موضوع زمانی ضرورت پیدا می‌کند که تعداد رایانه‌ها از پنج دستگاه بیشتر باشد، چون در تعداد کمتر از پنج رایانه می‌توان بدون استفاده از اکسس پوینت با تکنولوژی Ad Hoc رایانه‌ها را با هم به صورت شبکه به یکدیگر متصل نمود.

۱ــ Persona Computer Memory Card Internat ona Assoc at on

۲ــ نقطه دسترسی



شکل ۵۸ــ۴ــ تکنولوژی AdHoc

می‌توان گفت که دستگاه A.P در واقع نقش سوئیچ در شبکه ستاره‌ای را دارا می‌باشد و کار تقویت سیگنال رادیویی را هم برای ارتباط بهتر فراهم می‌نماید. در بعضی از A.Pها این امکان وجود دارد که از آنها به عنوان مسیریاب[۱] استفاده نماییم.

انواع Access Point

۱ــ A.P داخلی یا Indoor

۲ــ A.P خارجی یا Outdoor

شکل ۵۹ــ۴ــ انواع دستگاه اکسس پوینت

۱ــ Router

نقش آنتن در شبکه بی سیم

آنتن یکی از تجهیزات مهم در شبکه بی‌سیم می‌باشد که انتخاب نامناسب آن در کاهش کارایی شبکه نقش مهمی‌دارد.

انواع آنتن به لحاظ محل قرار گیری

۱ــ آنتن های داخلی (Indoor) : در فضای بسته داخل ساختمان مورد استفاده قرار می‌گیرد و معمولاً از ۲db تا ۱۰db ساخته می‌شوند.

۲ــ آنتن‌های خارجی (Outdoor) : بیرون از ساختمان و برای ارتباط راه دور (تا چند صد کیلومتر) استفاده می‌شود.

شکل ۶۰ــ۴ــ انواع آنتن به لحاظ محل قرارگیری

برای اتصال A.P داخلی به آنتن‌های خارجی (outdoor) از کابل کواکسیال مخصوص استفاده می‌شود.

شکل ۶۱ــ۴ــ کابل اتصال A.P به آنتن

انواع آنتن برای ارتباط بین دو یا چند شبکه (A.P)

۱ــ آنتن‌های یک به یک : جهت آنتن‌های یک به یک به سمت همدیگر تنظیم می‌شود. درصورتی که جهت دو آنتن بیش از ۴۵ درجه اختلاف داشته باشند ارتباط بر قرار نخواهد شد، زیرا در آنتن‌های یک به یک امواج به طور مستقیم ارسال می‌شوند. دو نوع آنتن یک جهته وجود دارد.

الف) آنتن‌های یک جهته پانلی[۱]

ب) آنتن‌های یک جهته سهمی‌وار[۲]

ب) آنتن یک‌جهته سهمی‌وار

الف) آنتن یک جهته پانلی

شکل ۶۲ــ۴ــ انواع آنتن یک جهته

۱ــ d rect ona Pane

۲ــ Parabo c

۲ــ آنتن‌های یک به چند : وقتی که در دفتر مرکزی یک آنتن وجود داشته و لازم باشد به چند شعبه دیگر از طریق بی سیم ارتباط برقرار شود، آنتن یک به چند را در مرکز قرار داده و در نقاط دیگر (شعبه‌ها) آنتن‌های نوع یک را قرار می‌دهند. که جهت آنتن‌های نوع یک به سمت آنتن مرکزی (آنتن یک به چند) تنظیم می‌شود. آنتن‌های یک به چند به صورت استوانه‌ای می‌باشند و به آنتن‌های Omni معروف می‌باشند.

الف) آنتن‌های یک یا چند Outdoor

ب) آنتن‌های یک به چند Indoor

شکل ۶۳ــ۴ــ انواع آنتن‌های یک

خودآزمایی و پژوهش

۱ــ تفاوت محیط‌های انتقال بی‌سیم و با سیم چیست؟

۲ــ انواع محیط‌های با سیم کدامند؟

۳ــ کاربرد کابل Straight و Cross چیست؟

۴ــ زوج سیم‌های استفاده شده در استاندارد T568A و T568B کدام است؟

۵ــ چند مورد از سخت‌افزارهای مورد نیاز در شبکه‌های فیبر نوری را نام ببرید.

۶ــ وظایف کارت شبکه کدامند؟

۷ــ انواع محیط‌های انتقال سیمی یا کابلی را از لحاظ سرعت، امنیت، هزینه، مسافت و نویز بررسی کنید.

۸ ــ حداقل فاصله بین کابل شبکه و کابل برق باید چقدر باشد؟

۹ــ عوامل مؤثر در تعیین نوع کابل را نام ببرید.

۱۰ــ پژوهش کنید که آیا می‌توان در کابل کشی یک شبکه از همه انواع کابل (مانند Cat5 ,Fiber, Cat6 و...) استفاده کرد؟ سرعت و راندمان شبکه در این حالت چگونه است؟

۱۱ــ پژوهش کنید که برای اتصال چند سوئیچ یا هاب از چه نوع کابلی باید استفاده گردد؟

مطالعه آزاد

فصل پنجم

مدل مرجع OSI

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- انواع لایه‌ها در مدل OSI را شرح دهد.
- کار هرکدام از لایه‌های TCP IP و OSI را بداند.
- تفاوت‌های دو مدل TCP/IP و OSI را بیان کند.
- مکانیزم‌های به کار گرفته شده در تجهیزات امنیتی شبکه را شناسایی کند.

برای تبادل داده‌ها در یک محیط شبکه‌ای، نیاز به وجود استاندارد است. دو استاندارد رایج در این زمینه عبارت است از TCP IP[1] و OSI[2].

TCP IP استانداردی است که به صورت عملی ابتدا پیاده شده سپس به صورت استاندارد درآمده است اما استاندارد OSI مفاهیم تئوری لایه‌بندی در شبکه را به خوبی نشان داده و به صورت عملی پیاده نشده است. OSI از طریق سازمان ISO تدوین و معرفی شد و پروتکل‌های شبکه براساس این استاندارد تدوین و تولید شده‌اند. در این استاندارد تمامی فعالیت‌هایی که سبب می‌شد اطلاعات از طریق شبکه و از رایانه‌ای به رایانه دیگر منتقل شود در یک ساختار ۷ لایه‌ای به نام OSI قرار گرفت.

این استاندارد تمامی فرآیند تبدیل اطلاعات را از حالتی که در رایانه قابل استفاده است تا حالتی که از طریق کابل شبکه قابل ارسال باشد، دربر می‌گیرد.

هرکدام از این لایه‌ها قسمتی از فرآیند تغییر شکل اطلاعات را دربرمی‌گیرند. اطلاعات از هفتمین لایه وارد این چرخه شده و پس از تغییر شکل در هر لایه به لایه بعدی خود منتقل می‌شود.

۱ــ Transm ss on Contro Protoco / Internet Protoco

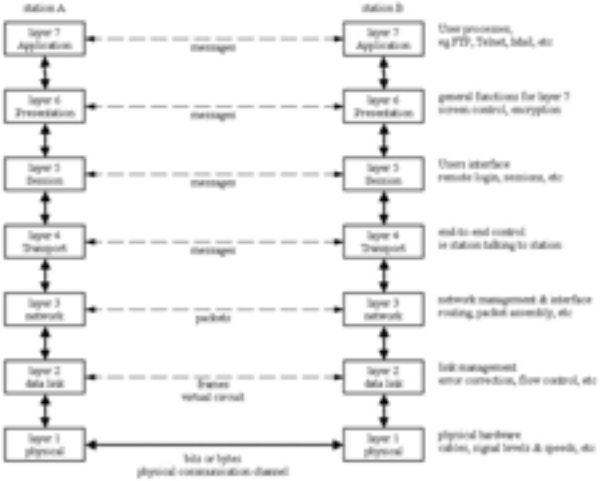
۲ــ Open System Interconnect on

این عمل آن قدر ادامه پیدا می کند تا تغییرشکل کامل شود و محصول فرآیند تبدیل که یک بسته اطلاعاتی (Packet) است، به‌دست آمده و از لایه اول خارج شود. لایه‌های شبکه در استاندارد OSI عبارت است از :

جدول ۱ــ۵ــ لایه‌های مدل OSI

Application	لایه کاربردی
Presentation	لایه نمایش
Session	لایه جلسه
Transport	لایه انتقال
Network	لایه شبکه
Data Link	لایه پیوند داده‌ها
Physical	لایه فیزیکی

نکته‌ای که در مورد لایه‌ها می‌توان به آن اشاره کرد این است که هر لایه فقط با لایه‌های قبلی، بعدی و لایه نظیر خود در رایانه مقصد ارتباط دارد. در سیستم مبدأ این لایه‌ها از بالا به پایین اطلاعات مورد نیاز لایه زیرین خود را فراهم می کنند و در سیستم مقصد از پایین به بالا، لایه‌ها اطلاعات موردنیاز لایه بالایی را فراهم می کنند.



شکل ۱ــ۵ــ لایه‌ها در مدل OSI

۱ـ۵ ـ انواع لایه در مدل OSI

لایه اول یا لایه فیزیکی در پایین‌ترین سطح قرار دارد و به‌طور مستقیم با همبندی شبکه در ارتباط است. لایه هفتم یا همان لایه کاربردی با کاربر در ارتباط بوده و از کاربر داده‌ها را دریافت کرده و به شبکه انتقال می‌دهد و برعکس. در ادامه به بررسی لایه‌ها می‌پردازیم.

۱ـ۱ـ۵ ـ لایه فیزیکی : لایه فیزیکی، اولین لایه مدل OSI بوده و در پایین‌ترین سطح این مدل قرار گرفته است. این لایه در ارتباط مستقیم با سخت‌افزار بوده و ویژگی‌های فیزیکی شبکه نظیر : اتصالات، ولتاژ و زمان را مشخص می‌نماید. در این لایه نحوه اتصال دو رایانه به یکدیگر از طریق کابل‌های شبکه، نحوه اتصال کابل شبکه به رایانه، همبندی‌های شبکه و سرعت‌های آن‌ها مشخص شده است. این لایه مسئول تبدیل اطلاعات از بیت‌ها (صفر و یک دیجیتال) به سیگنال‌های الکتریکی و ارسال آن‌ها به صورت مجموعه‌ای از سیگنال‌ها در فرستنده و دریافت سیگنال‌ها از شبکه و تبدیل آن‌ها به بیت است. (در گیرنده)

۲ـ۱ـ۵ ـ لایه پیوند داده‌ها : لایه پیوند داده‌ها دومین لایه مدل OSI است. وظیفه این لایه آماده کردن اطلاعات برای ارسال است و در واقع اطلاعاتی را که از لایه بالاتر یعنی لایه شبکه دریافت می‌کند به واحدهای کوچک‌تری به نام قاب[۱] تبدیل کرده و آن‌ها را ارسال می‌کند. هم‌چنین این لایه وظیفه دارد که اطلاعات را برای ارسال صحیح و بدون خطا کنترل کرده و به رایانه فرستنده صحت اطلاعات را اعلام کند. این لایه خود از دو زیرلایه به نام‌های LLC[۲] و MAC[۳] تشکیل شده است. هرکدام از این زیرلایه‌ها وظایفی را به عهده دارند که شرح آن‌ها به این قرار است :

زیرلایه LLC برقراری ارتباط نظیر به نظیر بین دو رایانه فرستنده و گیرنده، ایجاد قاب‌ها و کنترل خطاهایی که در اثر عوامل محیطی بر رسانه به‌وجود می‌آید را برعهده دارد. این زیرلایه عمل کنترل خطا را به این صورت انجام می‌دهد که هر قاب را ساخته و مرزهای ابتدا و انتهای آن را مشخص می‌کند. سپس قاب‌ها را شماره‌گذاری و ارسال می‌کند. رایانه مقصد قاب‌های ارسال شده را دریافت کرده و به ترتیب شماره، آن‌ها را پشت سرهم قرار می‌دهد و اطلاعات را دوباره بازسازی می‌کند. زیرلایه LLC در رایانه گیرنده پس از دریافت هر قاب یک پاسخ برای رایانه فرستنده می‌فرستد. به این پاسخ Acknowledge گفته می‌شود. رایانه‌ای که فرستنده اطلاعات است با دریافت این Acknowledge متوجه می‌شود که قاب مذکور به‌طور صحیح و بدون بروز مشکل به مقصد رسیده است. رایانه فرستنده

۱ـ Frame

۲ـ Log ca L nk Contro

۳ـ Med um Access Contro

تا مدتی منتظر می‌ماند تا برای تمامی قاب‌های ارسال شده، Acknowledge دریافت نماید. در صورتی که LLC برای قابی Acknowledge دریافت نکند، متوجه می‌شود که قاب مذکور آسیب دیده یا به مقصد نرسیده است؛ در این حالت قاب موردنظر را از روی شماره آن دوباره ساخته و برای رایانه مقصد ارسال می‌کند. این زیر لایه با این روش سالم رسیدن اطلاعات به مقصد را تضمین می‌کند.

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

از وظایف دیگر این زیرلایه کنترل آدرس فیزیکی[1] کارت‌های شبکه رایانه فرستنده و گیرنده است. هرکارت شبکه برای خود یک آدرس فیزیکی منحصر به فرد دارد که غیرقابل تغییر است. این آدرس به‌وسیلهٔ کارخانه سازنده در کارت شبکه حک می‌شود.

تقریباً در اکثر شبکه‌های امروزی از سوئیچ که تمامی گره‌های شبکه به آن متصل می‌گردند، استفاده می‌شود. با این که سوئیچ‌ها برای انواع شبکه‌ها، گزینه‌ای مناسب می‌باشند، ولی همزمان با رشد شبکه و افزایش تعداد ایستگاه‌ها و سرویس‌دهندگان، شاهد بروز مسائل خاصی خواهیم بود. ایستگاه‌های متصل به سوئیچ قادر به ارتباط با یکدیگر بوده و هریک به عنوان عضوی از یک Broadcast Domain مشابه می‌باشند. بدین ترتیب، در صورتی که ایستگاهی یک پیام Broadcast را ارسال نماید، سایر ایستگاه‌های متصل شده به سوئیچ نیز آن را دریافت خواهند کرد. سوئیچ‌ها، دستگاه‌های لایه دوم (مدل مرجع OSI) می‌باشند.

۳ــ۱ــ۵ــ لایه شبکه : لایه شبکه، سومین لایه استاندارد OSI است. یافتن آدرس رایانه‌های مبدأ و مقصد و ایجاد یک مسیر ارتباطی بین مبدأ و مقصد و همچنین مسیریابی در شبکه‌های بزرگ (مانند شبکه اینترنت یا امثال آن) وظیفه اصلی این لایه است. این لایه پیچیده‌ترین لایه OSI است، زیرا عمل مسیریابی که فرآیند بسیار پیچیده‌ای است در این لایه اتفاق می‌افتد. این لایه اطلاعاتی را که از لایه بالاتر یعنی لایه انتقال دریافت می‌کند به واحدهای کوچک‌تری به نام بسته[2] تبدیل کرده و آن‌ها را ارسال می‌کند.

این لایه علاوه بر مسیریابی می‌تواند 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 بسته‌ها انتخاب می‌کند. یکی دیگر از اعمالی که این لایه انجام می‌دهد، زمانی است که یک بسته اطلاعاتی برای رسیدن به مقصد مجبور است از شبکه‌ای به شبکه دیگر برود. در این شرایط ممکن است مشکلات زیادی بروز نماید؛

۱ــ MAC Address ۲ــ Packet

مثلاً ممکن است روش آدرس‌دهی رایانه‌ها در شبکه مبدأ و مقصد متفاوت و نامتجانس باشد؛ رفع این مشکل و مرتبط کردن دو شبکه نامتجانس از دیگر وظایف این لایه است.

همان‌گونه که قبلاً اشاره گردید، اکثر سوئیچ‌ها در لایه دوم مدل OSI فعالیت می‌نمایند. مدلی از سوئیچ وجود دارد که شباهت زیادی با مسیریاب[1] دارد و قادر به فعالیت در لایه سوم مدل OSI است.

زمانی که مسیریاب یک بسته اطلاعاتی را دریافت می‌نماید، در لایه سوم به دنبال آدرس‌های مبدأ و مقصد گشته تا مسیر مربوط به بسته اطلاعاتی را مشخص نماید. سوئیچ استاندارد از آدرس‌های MAC به منظور مشخص کردن آدرس مبدأ و مقصد استفاده می‌نمایند (از طریق لایه دوم).

۴ــ۱ــ۵ــ لایه انتقال : وظیفه اصلی لایه انتقال، دریافت داده‌ها از لایه جلسه، در صورت نیاز شکستن داده‌ها به واحدهای کوچک‌تر به نام قطعه[2]، انتقال آن‌ها به لایه شبکه و حصول اطمینان از دریافت صحیح داده‌ها در انتهای دیگر (رایانه مقصد) است.

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

۵ــ۱ــ۵ــ لایه جلسه : پنجمین لایه OSI، لایه جلسه است. این لایه هم‌چون لایه انتقال، ارسال معمولی داده‌ها را فراهم می‌کند اما خدمات پیشرفته‌ای را نیز ارایه می‌کند که کاربردهای مفیدی دارد. یکی از خدمات لایه جلسه، مدیریت بر ارتباط بین رایانه‌هاست؛ بدین معنی که وقتی دو رایانه باهم ارتباط برقرار می‌کنند، ترافیک می‌تواند در یک لحظه یک طرفه یا دو طرفه باشد. اگر این ترافیک یک‌طرفه باشد، لایه جلسه می‌تواند در حفظ نوبت کمک کند.

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

یکی دیگر از اعمال لایه جلسه این است که روی قسمت‌هایی از رشته داده‌ها را علامت‌گذاری

۱ــ Router ۲ــ Segment

می‌کند؛ در صورتی که بسته‌ای هنگام ارسال مفقود یا خراب شود، لایه جلسه بسته را از روی کدهای آن شناسایی و دوباره ارسال می‌کند.

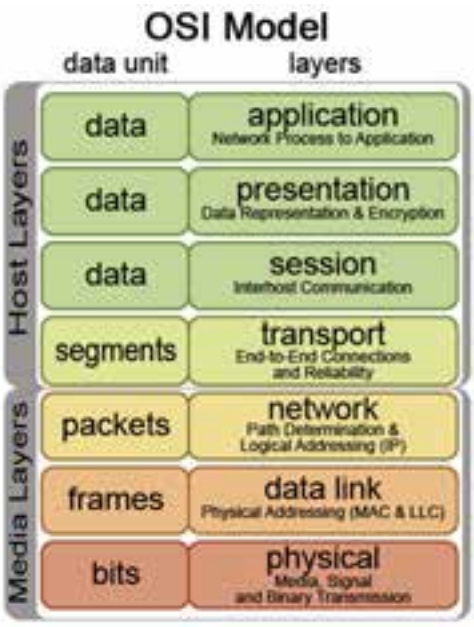
۶ــ۱ــ۵ــ لایه نمایش : لایه نمایش ششمین لایه OSI است. این لایه داده‌ها را به روش استاندارد کدگذاری می‌کند.

اکثر رایانه‌ها اطلاعاتی مانند نام افراد، تاریخ، مقدار پول و اطلاعات مشابه دیگری را ارسال می‌کنند. این اطلاعات به صورت کاراکتر بوده و هیچ کدام رشته‌های دودویی نیستند.

کدهای نمایش رشته‌های کاراکتری، اعداد صحیح و... ممکن است در رایانه‌های مختلف متفاوت باشد. برای این که رایانه‌ها با کدهای مختلف بتوانند با یکدیگر ارتباط برقرار کنند، اطلاعاتی که انتقال می‌یابند باید با استفاده از کدهای استاندارد تعریف و ارسال شوند تا در تمامی رایانه‌ها و با سیستم عامل‌های متفاوت قابل دریافت و درک باشند.

۷ــ۱ــ۵ــ لایه کاربردی : هفتمین لایه مدل OSI است و همه نرم‌افزارهای کاربردی برای ارتباط شبکه‌ای از آن‌ها استفاده می‌کنند.

لایه کاربردی بزرگ‌ترین لایه در استاندارد OSI است. این لایه شامل سیگنال‌هایی است که خدمات سودمندی از قبیل انتقال پرونده و کنترل یک رایانه از راه دور را به کاربر ارایه می‌دهد، در صورتی که لایه‌های پایین‌تر فقط در تبادل اطلاعات بین فرستنده و گیرنده نقش دارند. همچنین این لایه می‌تواند ارتباط برنامه‌های مختلفی را که در محیط شبکه وجود دارند، با یکدیگر برقرار کند.



شکل ۲ــ۵ــ واحدهای اطلاعات در لایه‌های مختلف مدل OSI

به عنوان مثال، صدها نوع نرم‌افزار در دنیا وجود دارد که هرکدام روش خاص خود را برای نوشتن، ویرایش و حرکت مکان‌نما روی صفحه انجام می‌دهند، در صورتی که این لایه وجود نداشت، ممکن بود در اجرای برنامه‌ها و ویرایش آن‌ها دچار مشکل شویم. برای حل این مشکل لایه کاربردی، اطلاعات لازم را از این برنامه‌ها

گرفته و با یک استاندارد مشخص آن‌ها را به رایانه مقصد می‌فرستد.

وظیفه دیگر لایه کاربردی، انتقال پرونده است. در سیستم فایل‌های مختلف، نام‌گذاری پرونده‌ها، روش نمایش خطوط متن و غیره متفاوت است. این کار به همراه وظایفی از قبیل پست الکترونیک، کنترل رایانه از راه دور و جستجو در بخش‌های مختلف درون حافظه، وظیفه لایه کاربردی است.

۲ــ۵ــ مدل TCP/IP و مقایسه دو پروتکل در بخش‌های مختلف

TCP/IP استاندارد دیگری است که برای اتصال رایانه‌ها در شبکه مورد استفاده قرار می‌گیرند. به تعریف دیگر قرارداد کنترل انتقال اطلاعات می‌باشد. در جدول ۲ــ۵ این دو استاندارد در کنار هم نمایش داده شده و با هم مقایسه شده‌اند.

جدول ۲ــ۵ــ مقایسه لایه‌های OSI و TCP/IP

مدل مرجع OSI	مدل چهار لایه TCP/IP
لایه کاربرد	لایه کاربرد (Application)
لایه ارایه	
لایه جلسه	لایه انتقال (Transport)
لایه انتقال	
لایه شبکه	لایه شبکه (Internet)
لایه پیوند داده‌ها	لایه وسط شبکه (Network Internet)
لایه فیزیکی	

همان‌طور که از جدول پیداست TCP/IP از چهار لایه تشکیل شده که در زیر چهارلایه TCP/IP را بررسی می‌کنیم.

■ **لایه واسط شبکه** : در این لایه تمام استانداردهای سخت‌افزاری و انواع پروتکل شبکه تعریف شده است. در این لایه می‌توان بین نرم‌افزار و سخت‌افزار شبکه ارتباط برقرار کرد.

■ **لایه شبکه** : در این لایه پروتکل IP آدرس‌دهی و تنظیم می‌شود. در کل وظیفه این لایه دادن اطلاعات در مورد شبکه و آدرس‌دهی در آن می‌باشد که مسیریاب‌ها از آن بسیار استفاده می‌کنند.

■ **لایه انتقال** : ابتدایی‌ترین وظیفه این لایه آگاهی از وضعیت بسته‌ها می‌باشد و در مرحله بعد وظیفه این لایه انتقال اطلاعاتی می‌باشد که نیاز به امنیت ندارد و سرعت برای آن‌ها مهم‌تر است.

■ **لایه کاربرد** : در این لایه برنامه‌های کاربردی قرار دارند و لایهٔ نرم‌افزاری شبکه است و همچنین لایه پروتکل‌های نرم‌افزاری نیز می‌باشد. از مهم‌ترین نکات درخصوص این لایه قرار داشتن، پروتکل انتقال پرونده (FTP) و پروتکل مدیریت پست الکترونیک (SMTP) و بقیه برنامه‌های کاربردی در این لایه می‌باشد.

بیشترین حملات برنامه‌های مخرب به ترتیب در لایه انتقال، شبکه، کاربردی و واسط شبکه است و سرویس‌ها و مکانیزم‌ها بیشتر در لایه شبکه به‌چشم می‌خورد و تجهیزات امنیتی با بهره‌گیری از مکانیزم‌های مختلف، بیشتر در لایه انتقال، شبکه و کاربرد، وجود دارند.

خودآزمایی و پژوهش

۱ــ به‌طور کلی وظایف لایه‌ها در مدل OSI چیست؟

۲ــ بسته و قاب و قطعه چیست و هرکدام در چه لایه‌ای معنی پیدا می‌کند؟

۳ــ یافتن آدرس رایانه مقصد و مبدأ وظیفه کدام لایه است؟

۴ــ لایه شبکه چه کاری انجام می‌دهد؟

۵ــ دو زیر لایه پیوند داده کدام است؟

۶ــ کار خطایابی و مسیریابی در کدام لایه‌ها انجام می‌شود؟

فصل ششم

آشنایی با پروتکل TCP/ IP و سرویس‌های آن

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- سرویس‌های رایج در پروتکل TCP/IP را شناسایی کند.
- سرویس‌های رایج در شبکه اینترنت را شرح دهد.
- مفهوم Host در پروتکل TCP/IP را بیان کند.
- انواع دامنه‌های رایج را بیان کند.
- مراحل ثبت Domain را شرح دهد.
- انواع کلاس‌های IP را شناسایی کند.

۱ـ۶ـ نقش پروتکل در شبکه

بهره‌برداری از امکانات سخت‌افزاری و برقراری ارتباط بین اجزای مختلف شبکه نیاز به یک مجموعه از قوانین و دستورالعمل‌های مشترک دارد که به آن قوانین اصطلاحاً پروتکل می‌گوییم.

پروتکل مجموعه قوانینی است که اگر آنها را رعایت نکنیم ارائهٔ سرویس (یعنی هدف از برقراری شبکه) غیرممکن خواهد شد.

تعریف: پروتکل مجموعه قوانینی نرم‌افزاری است که رعایت آنها باعث بهره‌برداری از امکانات سخت‌افزاری و برقراری سرویس در شبکه می‌شود.

نقش پروتکل در رایانه ارسال کننده داده:

- شکستن داده‌ها به بخش‌های کوچکتر، به نام بسته[۱]
- اضافه‌کردن اطلاعات آدرس مقصد به بسته
- آماده‌سازی داده‌ها برای انتقال از طریق کارت شبکه بر روی کابل شبکه.

۱ـ Packet

نقش پروتکل در رایانه دریافت کننده داده

- دریافت بسته‌های داده از کابل شبکه
- ایجاد نواری از بسته‌های ارسالی از رایانه فرستنده
- کپی کردن بسته‌ها به بافر برای دوباره اسمبل کردن به عنوان داده
- پذیرش داده‌ها به شکل برنامه قابل استفاده

توجه اگر پروتکل‌های استفاده شده در رایانه‌های فرستنده و گیرنده با هم متفاوت باشند امکان دریافت درست داده‌ها در رایانه گیرنده وجود نخواهد داشت و یا اینکه بسته‌های دریافتی در رایانه گیرنده قابل استفاده نخواهد بود.

زمانی که داده‌ها بخواهند در یک شبکه LAN بین رایانه‌ها منتقل شوند کار چندان پیچیده نیست، اما اگر شما بخواهید بین چند شبکه LAN ارتباط بر قرار کنید، ممکن است از پروتکل‌های مختلفی استفاده نمایید که در اینجا باید یک هماهنگ کننده پروتکل‌ها وجود داشته باشد نتایج این هماهنگی به عنوان لایه‌بندی شناخته شده است.

۲ـ۶ـ پروتکل TCP/IP[۱]

TCP/IP، یکی از مهم‌ترین پروتکل‌های استفاده شده در شبکه‌های کامپیوتری است و اولین بار در سیستم عامل UNIX مورد استفاده قرار گرفت. اینترنت بعنوان بزرگترین شبکه موجود، از پروتکل فوق به منظور ارتباط دستگاه‌های متفاوت استفاده می‌نماید. در اهمیت TCP/IP توجه به این نکته کافی است که ارتباط در اینترنت بدون TCP/IP تقریباً غیرممکن است و اکثر سرویس‌های اینترنت تحت قوانین TCP/IP عرضه می‌شوند.

TCP/IP مجموعه کاملی از پروتکل‌های تعریف شده برای استفاده در شبکه‌های خصوصی و اینترنت می‌باشد، ولی نام آن در واقع ترکیبی از دو پروتکل زیر می‌باشد :

الف) پروتکل کنترل انتقال TCP

ب) پروتکل اینترنت IP

مهم‌ترین خصوصیات این پروتکل به‌طور خلاصه عبارتند از :

۱ـ قابل استفاده در انواع شبکه‌ها

۲ـ پشتیبانی به وسیله انواع سیستم عامل‌ها

۱ـ Transm ss on Contro Protoco / Internet Protoco

۳ــ مورد استفاده به عنوان پروتکل اصلی[۱] اینترنت

۴ــ قابلیت مسیر یابی

۵ــ حق انتخاب در انتقال اطلاعات به صورت اتصال گرا[۲] و بدون اتصال[۳]

۷ــ ارسال گروهی

۸ــ پیکربندی پیچیده

از ویژگی‌های مهم پروتکل TCP/IP می‌توان به موارد زیر اشاره کرد :

- اولین ویژگی در TCP/IP آن است که می‌تواند در هر ابعادی از شبکه استفاده شود (از شبکه‌های کوچک یا بزرگ، با ترافیک کم یا ترافیک زیاد، با اتصال به اینترنت و بدون اتصال به اینترنت)
- چون TCP/IP در کلیهٔ سیستم عامل‌های مدرن امروزی پشتیبانی می‌شود بنابراین زبان مشترک ارتباط بین سیستم عامل‌ها می‌باشد.
- TCP/IP از ابتدا تا به امروز بعنوان پروتکل اصلی مورد استفاده در اینترنت بوده است.
- در TCP/IP الگوریتم‌های متنوع مسیریابی[۴] برای انتخاب مسیر بهینه از میان روترها(مسیریاب‌ها) تعبیه شده و به همین خاطر یکی از مهم‌ترین پروتکل‌ها برای استفاده در شبکه‌های WAN به شمار می‌رود. همان طور که قبلاً اشاره شد هم بندی غالب شبکه‌های WAN از نوع Mesh می‌باشد 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 یا اتصال گرا «Connection Oriented» معروف به TCP و سرویس انتقال اطلاعات بصورت عادی یا بدون اتصال «Connection less» معروف به UDP از دیگر بخش‌های متنوع این پروتکل می‌باشد.
- Multicasting به معنی ارسال اطلاعات برای گروهی از استفاده‌کنندگان (مخاطبین) می‌باشد.
- بالاخره آخرین خصوصیت TCP/IP که درواقع عیب آن به شمار می‌رود این است که پیکربندی پیچیده‌ای دارد. علت این پیچیدگی را می‌توان در تنوع سرویس‌های ارائه شده جستجو کرد. TCP/IP پروتکل بسیار کامل و متنوعی‌است، در نتیجه این تنوع، پیچیدگی در پیکربندی را به دنبال خواهد داشت.

۱ــ Pr mary Protoco

۲ــ Connect on Or ented

۳ــ Connect on ess

۴ــ Rout ng

البته با توجه به وجود امکان پیکربندی خودکار و پویا[1] در TCP/IP در اکثر مواقع، کاربران نیازی به درگیر شدن با پیچیدگی‌های پیکربندی ندارند.

۳ـ۶ـ 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 :

۱ـ۳ـ۶ـ FTP[2] : یکی از کارهای ضروری که اغلب کاربران در شبکه بدان نیاز دارند انتقال پرونده است. TCP/IP مستقیماً دارای سرویسی است که انتقال پرونده را به‌راحتی بین ماشین‌های مختلف با سخت‌افزارهای متنوع و سیستم‌عامل‌های گوناگون امکان‌پذیر می‌سازد و آن FTP است.

FTP 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 پرونده‌های موردنیاز را از سرویس‌دهنده دریافت کرده (Download_Receive) یا آن‌ها را روی سرویس‌دهنده ذخیره کند. (Upload_Send)

در سیستم عامل‌های مایکروسافت نرم‌افزارهای گوناگونی به عنوان 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 به‌عنوان FTP Server در مایکروسافت استفاده می‌شوند نیز موجود بوده و به‌عنوان مثال می‌توان به IIS اشاره کرد. IIS بسته‌ای است شامل چندین سرویس که یکی از آن‌ها FTP Server است.

۱ـ Automat c/Dynam c Conf gurat on

۲ـ F e Transfer Protoco در درس بسته‌های نرم‌افزاری (۳) با FTP به‌طور مشروح‌تر آشنا می‌شوید.

فعالیت عملی

آشنایی با سرویس FTP

در این بخش هنرآموز درس FTP Server را از قبل روی یک رایانه با سیستم‌عامل 2000 یا 2003 سرور پیکربندی کرده و هنرجویان با اجرای FTP Client در رایانه‌های خود (ترجیحاً IE) چند پرونده را از سرویس‌دهنده دریافت (Download) کنند. در این مرحله به هیچ عنوان نیازی به فراگیری پیکربندی FTP Server نبوده و هنرجویان فقط از آن استفاده می‌کنند.

۲ــ۳ــ۶ــ HTTP[1] : 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 سرویس‌دهنده ارسال می‌کنند (HTTP Request). سرویس‌دهنده این درخواست را بررسی کرده و پس از آماده کردن پاسخ، آن‌ها را در قالب خاصی معروف به Web Page به سمت سرویس‌گیرنده ارسال می‌کند. سرویس گیرنده این صفحات را دریافت کرده و با قالب 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

هر چند اغلب هنرجویان و حتی کاربران عادی با این سرویس آشنا هستند اما برای حفظ انسجام مطالب بیان شده، هنرآموز 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 بستهٔ IIS است.

۱ــ Hyper Text Transfer Protoco

۳ــ۳ــ۶ــ POP3[۱] **و SMTP**[۲] : هر دو سرویس فوق برای EMail استفاده می‌شوند. کاربر برای تهیه، ارسال، دریافت و خواندن نامه از نرم‌افزار Mail Client استفاده می‌کند. دو مورد از نرم‌افزارهای معروف که به عنوان Mail Client در مایکروسافت استفاده می‌شوند عبارتند از Outlook Express و Outlook ــ Microsoft (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 پرونده‌های دیگری را به آن پیوست کرده[۳] و پس از تعیین گیرنده و موضوع نامه[۴] آن را ارسال کند. به محض فشردن کلید Send تمامی محتوای نامه به همراه ضمائم پیوست، با پروتکل SMTP به سمت Mail Server ارسال می‌شود. Mail Server پس از دریافت‌نامه از سوی کاربر به بررسی آدرس گیرنده می‌پردازد و اگر گیرنده شخصی خارج از حوزهٔ پستی خودش باشد آن‌را با SMTP به Mail Server حوزه گیرنده تحویل می‌دهد. Mail Server گیرنده پس از دریافت نامه از Mail Server فرستنده آن‌را در پوشه مناسب که در واقع صندوق‌پستی شخص گیرنده است ذخیره می‌کند و فرایند ارسال‌نامه 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 سرویس‌دهنده دریافت کرده و در صندوق پستی محلی واقع در رایانه خودش منتقل کند. همان‌طور که می‌بینیم فرایند فوق تا حدی با روش عمومی اداره پست در ارسال‌نامه متفاوت است چرا که پستچی نامه را تا دم در منزل می‌آورد اما در Email ما باید خودمان به ادارهٔ پست (Mail Server) مراجعه و پس از نشان دادن مجوز، نامه را از صندوق پستی برداریم.

پژوهش

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

۱ــ Post Off ce Protoco (vers on3)

۲ــ S mp e Ma Transfer Protoco

۳ــ Attachment

۴ــ Subject

مطالعه آزاد

۴ــ۳ــ۶ــ NNTP[۱] : سرویس دسترسی به گروه‌های خبری (News Groups)، به زبان ساده NNTP سرویسی است برای دسترسی به اطلاعاتی که به وسیلهٔ 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 به‌وسیلهٔ News Client به یک 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 موردنظر از Server به سرویس گیرنده انتقال پیدا کرده و اعضا در صورت تمایل می‌توانند نظرات یا پرسش‌های خود را در مورد خبرها ارسال کنند یا خبر و سؤال جدیدی را به سرویس‌دهنده ارسال کنند. در مایکروسافت، نرم‌افزاری که به عنوان News Client مورد استفاده قرار می‌گیرد همان Mail Client است یعنی Outlook Express منتهی به‌جای پیکربندی برای Mail Account باید آن‌را برای News Account تنظیم کنیم.

۵ــ۳ــ۶ــ Telnet[۲] : 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.

مطالعه آزاد

منظور از سیستم مرکزی، مجموعه‌ای است دارای توانایی برای پردازش اطلاعات و اجرای دستورالعمل‌ها یعنی مجموعه‌ای که شامل CPU، RAM، HDD و ... است. سیستم مرکزی می‌تواند یک رایانه 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، سوئیچ یا Hub. البته

۱ــ Network News Transfer Protoco

۲ــ Te e Network

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 آن است.

مثال ۱ : در برخی از بانک‌ها، جلوی هر کارمند باجه، فقط یک صفحه نمایش، صفحه کلید و یک چاپگر کوچک قرار دارد اما خبری از کیس و ملحقات داخلی آن نیست! چرا؟ پردازش کجا انجام می‌شود؟ تجهیزات جلوی کارمند فقط به عنوان ترمینال استفاده می‌شوند. پس سیستم مرکزی کجاست؟ اگر دقت کنیم در گوشه‌ای از بانک یک رایانه شخصی قرار دارد که به عنوان سرویس‌دهنده عمل کرده و نقش سیستم مرکزی را بازی می‌کند و در واقع محل اجرای نرم‌افزارهای بانکی و پردازش اطلاعات است. ترمینال‌ها از طریق سخت‌افزار و کنترلر مناسب به آن متصل می‌شوند.

راه‌های متنوعی برای اتصال ترمینال‌ها به سیستم مرکزی وجود دارد، که عبارتنداز :

Serial Port

USB

Network

از نظر نحوهٔ نمایش اطلاعات، ترمینال‌ها به دو دسته کلی تقسیم می‌شوند :

الف) ترمینال‌های Text *:* فقط به صورت «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 به‌جای ترمینال از یک رایانه شخصی استفاده کنند. مزیت استفاده از رایانه شخصی به‌جای ترمینال آن است که این رایانه خود دارای توانایی پردازش اطلاعات است بنابراین می‌توان علاوه بر کاربرد آن به عنوان یک ترمینال، نرم‌افزارهای متنوع دیگری را نیز مستقیماً روی آن اجرا کرد. اما در صورت نیاز چگونه می‌توان رایانه شخصی را تبدیل به یک ترمینال برای اتصال به سیستم مرکزی کرد؟ پاسخ بسیار ساده است : کافی است نرم‌افزار مناسب را روی آن اجرا کرد. این نرم‌افزارها در حالت کلی به «شبیه‌ساز ترمینال» یا «مقلد ترمینال» یا به زبان

انگلیسی Terminal Emulator مشهورند و همچون ترمینال‌ها دارای دو دستهٔ کلی Text و Graphic در زمینهٔ نحوهٔ نمایش اطلاعاتند. طریقه اتصال سخت‌افزاری یک رایانه شخصی که به عنوان ترمینال استفاده می‌شود با Central System همچون نحوهٔ ارتباط ترمینال‌هاست .

نرم‌افزارهای Terminal Emulator که اطلاعات را به صورت Text نشان می‌دهند بسیار متنوعند، از آن جمله می‌توان به Term ۹۵، PC Anywhere ، Kermit ، Closeup و Hyper Terminal اشاره کرد. می‌دانیم که Hyper Terminal تحت Windows اجرا می‌شود اما در واقع فقط به‌صورت Text می‌تواند اطلاعات را نمایش دهد.

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

اگر راه ارتباطی یک رایانه 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 به صورت Text نشان می‌دهد.

همچون دیگر سرویس‌ها، Telnet نیز از دو بخش تشکیل شده :

الف) Telnet Client : که روی رایانه شخصی اجرا می‌شود و آن‌را تبدیل به ترمینال می‌کند (در مایکروسافت : Telnet.exe).

ب) Telnet Server : یا Telnet Doemon یا به اختصار telnetd که روی Central System اجرا شده و اطلاعات را از ترمینال Telnet سرویس گیرنده دریافت و پس از پردازش به‌وسیلهٔ سیستم مرکزی، برای ترمینال (کلاینت) Client ارسال می‌کند.

فعالیت عملی **آشنایی با سرویس Telnet**

ابتدا باید سیستم مرکزی را انتخاب کرد. (مثلاً یک رایانه با سیستم عامل UNIX، یک رایانه با سیستم‌عامل NT، یک Router، یک Wireless Access Point، ...) سپس باید مطمئن شد که سرویس Telnet Server روی آن نصب و فعال است. (تا این جای کار باید به وسیلهٔ هنرآموز درس انجام شود.). سپس هنرجویان نرم‌افزار Telnet Client را روی رایانه‌های خود اجرا کرده (Telnet.exe) و بدین ترتیب رایانه آن‌ها

تبدیل به یک ترمینال می‌شود. قدم بعدی آن است 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 سایت‌ها اجازه می‌دهند با کاربر guest به سیستم Login کنیم. به عنوان مثال می‌توانید از طریق Run فرمان زیر را تایپ کرده و نتیجه را ببینید، (کاربر را guest وارد کنید) :

telnet victoria.tc.ca

۶ــ۳ــ۶ــ RDP[1] : همانند Telnet است با این تفاوت که گرافیکی است. در مایکروسافت، برنامه Remote Desktop از سرویس RDP استفاده کرده و رایانه شخصی را تبدیل به یک ترمینال گرافیکی می کند.

همچون دیگر سرویس‌های TCP/IP، RDP نیز از دو بخش تشکیل شده :

الف) RDP Client : که به Terminal Client نیز معروف بوده و در مایکروسافت، همان برنامه Remote–Desktop است (mstsc.exe)[2].

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 سرور 2000 یا 2003 یک نسخه کامل‌تر از این سرویس به نام Terminal Service از طریق زیر نصب و فعال می‌شود :

Add/Remove Programs → Windows Components → Terminal Service

فعالیت عملی

آشنایی با سرویس RDP

روی رایانه سرویس‌دهنده، سرویس Remote Desktop server را به کمک هنرآموز درس فعال کرده، سپس روی سرویس گیرنده برنامه Remote Desktop Client را اجرا کنید (دستور Mstsc.exe)

۱ــ Remote Desktop Protoco

۲ــ شکل کلی این دستور در فصل ۱۴ آمده است.

حال به سرویس‌دهنده متصل شده با نام Administrator وارد شده و میز کار مربوط به سرویس‌دهنده را در اختیار بگیرید.

۷ــ۳ــ۶ــ SNMP[۱] : یکی از مسایل مهمی که هر Administrator در شبکه‌های متوسط و بزرگ با آن مواجه است، مدیریت شبکه به شکل جامع و حتی‌المقدور یکپارچه است.

مثال : برای مدیریت از راه دور یک رایانه با سیستم عامل ویندوز اکس پی، 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(برای این کار روی My Computer کلیک راست و گزینه Computer Management را انتخاب و پس از اجرای آن، Connect to another Computer را انتخاب کنید). سپس با تایپ کردن نام یا آدرس رایانه 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 هر دو رایانه مبدأ و مقصد دقیقاً یکسان باشد.

در مثال فوق ارتباط ما از طریق سرویس‌های خاصی که مایکروسافت تعبیه کرده برقرار شده است.

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 راه‌حل، 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 وسیلهٔ کلیه Agentها در تمامی شبکه است.

هر سیستمی که بخواهد با SNMP مدیریت شود باید Agent را روی آن نصب و فعال کرد. کار Agent آن است که اطلاعات مدیریتی را جمع‌آوری کرده و آنها را در یک بانک اطلاعاتی محلی (Local Database) معروف به MIB[۲] ذخیره می‌کند. به عنوان 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

۱ــ S mp e Network Management Protoco ۲ــ Management Informat on Base

ویندوز 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 با کمک هنرآموز درس انجام شود).

و اما اطلاعات جمع‌آوری شده به وسیلهٔ Agent را چگونه گردآوری و تجزیه تحلیل کنیم؟ کافی است روی یک رایانه مثلاً متعلق به مدیر شبکه، نرم‌افزار SNMP Manager را نصب کنیم. یکی از نرم‌افزارهای مناسب در این زمینه Solarwinds است (www.solarwinds.net). پس از پیکربندی نرم‌افزار می‌توان به سایر سیستم‌های مجهز به Agent در شبکه متصل شده و اطلاعات جمع‌آوری شده در MIB را گردآوری و تجزیه و 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، هنرآموز محترم می‌تواند، خود Agent و Viewer را نصب و پیکربندی کرده و نحوهٔ مدیریت شبکه را در حالات بسیار ساده به هنرجویان نشان دهد.

۸ــ۳ــ۶ــ SNTP(NTP)[1] : 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 به‌طور صحیح تنظیم شده است؟

در این‌جا NTP به کمک 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

۱ــ S mp e Network T me Protoco

ساعت خود را با ساعت سرویس‌دهنده تنظیم می‌کند و بدین ترتیب ساعت تمام رایانه‌های شبکه دقیقاً یکسان شده و نیازی به تنظیم دستی نیست.

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

فعالیت عملی

آشنایی با سرویس NTP

با کاربر Administrator وارد ویندوز اکس پی شده و روی نشانه Time واقع در سمت راست Taskbar دوبار ــ کلیک کنید.

سومین قسمت از صفحه Time با نام Internet Time را باز کنید. لیستی از سرویس‌دهنده‌های 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 به عنوان 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 :

۱ــ سرویسی معروف به Windows Time در لیست سرویس‌های ویندوز Start باشد.

۲ــ Date (روز و ماه و سال) از قبل صحیح باشد.

۳ــ Time Zone را Tehran انتخاب کرده باشیم.

۴ــ اختلاف ساعت ما با ساعت واقعی بیش از ۱۲ ساعت نباشد.

۵ــ در بین راه یا حتی روی ماشین خودمان UDP Port 123 باز باشد.

۴ــ۶ــ 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 TCP/IP برای ارتباط استفاده کند اصطلاحاً یک TCP/IP Host یا «میزبان TCP/IP» می‌گوییم.

مثال۱ : کلیه رایانه‌های شخصی در یک شبکه که پروتکل TCP/IP روی آن‌ها تنظیم و فعال

شده اعم از این‌که سرویس گیرنده باشند یا سرویس دهنده، هر کدام برای خود یک Host مستقل به حساب می‌آیند.

مثال۲ : یک روتر را می‌توان یک TCP/IP Host بشمار آورد، به دلیل این که می‌توان TCP/IP را روی آن پیکربندی و فعال کرد و روتر را از طریق آن کنترل کرد.

مثال۳ : برخی از سوئیچ های حرفه‌ای توانایی پیکربندی و کنترل خود را از طریق TCP/IP به مدیر شبکه می‌دهند، پس این سوئیچ‌ها نیز TCP/IP Host هستند.

مثال ۴ : برخی ازUPSها توانایی اتصال مستقیم به شبکه را دارند. می‌توان از طریق یک رایانه شخصی و پروتکل TCP/IP آن‌ها را کنترل کرد. چنین UPSهایی در واقع مثال دیگری از TCP/IP Host هستند.

مثال ۵ : چاپگرهایی هستند که مستقیماً به شبکه متصل شده و رایانه‌های 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 دو مشخصه اصلی و بارز است. به عبارت دیگر هر Host را می‌توان با دو خصوصیت از بقیه Hostها تفکیک کرد. این دو مشخصه عبارتند از :

الف) نام (Host Name TCP/IP 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 به‌فرد 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 آدرس http:// www.sanjesh.org می‌شود ۹۲.۲۴۲.۱۹۵.۱) و بعد ارتباط با سایت آغاز می‌شود.

۱ــ۴ــ۶ــ Host Name : گفتیم که برای سهولت بیشتر کاربران، برای اکثر «میزبان‌های 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 آن‌صورت استفاده از نام معمولاً محدود به کاربردهای داخلی شده و اغلب کاربران «خارج از شبکه داخلی» نام را نمی‌شناسند چرا که رسماً ثبت نشده است.

مثال : فرض کنید کسی در محدوده خانوادگی خود یا میان دوستان وآشنایان نام «نرگس» را برای خود انتخاب کند اما نام شناسنامه‌ای وی «فرزانه» باشد. طبیعی است هنگامی که می‌خواهد خود را رسماً به همه معرفی کند «اسم شناسنامه‌ای» خودش که در اداره ثبت احوال درج شده به کار می‌برد زیرا همگان «اداره ثبت احوال» را به عنوان «مرکز معتبر ثبت اسامی» قبول دارند. اما افراد خانواده وی یا دوستان نزدیک وی می‌توانند با نام مستعار او را صدا بزنند.

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

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

Narges	Reza	Server22	Client80	PC1
C2	C1	Palang	Moon	Star

قالب دوم :

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

پرسشی

تفاوت بین قالب اول و دوم در چیست؟به‌روشنی پیداست که قالب دوم کامل‌تر است،اصطلاحاً اگراسمی در قالب اول باشد به آن اسم مستعار Alias یا Unqualified و اگر در قالب دوم باشد به آن Fully Qualified Domain Name FQDN می‌گویند.

معمولاً اسامی قالب اول در محدودهٔ 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 به‌وسیلهٔ TCP/IP به آدرس تبدیل می‌شوند).

اگر بخواهیم بگوییم 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 کهHost ارائه می‌دهد یا نقشی که Host بازی می‌کند[1].

مثال :

www	Web Server	mail	Mail server
ftp	FTP Server	time	Time Server
news	News (NNTP) Server		

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

مثال :

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

ج) حوزهٔ فعالیت میزبان. (Activities)

مثال :

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

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

مثال :

ir lran tr Turkey uk United Kingdom ca Canada
iq Iraq tw Taiwan us United States 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.

۱ـ Host Ro e or Host Serv ce

نکته ۱ : با توجه به مثال‌های قالب دوم ممکن است برخی از اجزای یاد شده در FQDN موجود نباشد مثلاً در اکثر آن‌ها «بند د» (Locality) دیده نمی‌شود یا یکی 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 حوزهٔ فعالیت در آن دیده نمی‌شود اما به هر حال FQDN هر چه‌قدر هم که ناقص باشد، اجزای آن باید از چپ به راست ترتیب یاد شده رارعایت کنند و نباید آن‌ها را جابه‌جا کرد مثلاً www.com.yahoo صحیح نیست.

به این مثال‌ها توجه کنید :

www.microsoft.com ↓ Domain

www.neda.net.ir ↓ Domain

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 به‌طورکلی از دو بخش تشکیل شده :

جدول ۱ــ۶

FQDN =	Service Name	+	Domain Name
	www		microsoft com
	time		dlink com
	msnews		microsoft com

به زیرمجموعه‌های یک Domain اصطلاحاً SubDomain می‌گویند. در عمل معمولاً از SubDomain برای نشان دادن شرکت‌ها، زیرگروه‌ها یا ساختارهای فرعی در یک مجموعهٔ بزرگ استفاده می‌شود.

مثال : یک شرکت بزرگ رایانه‌ای را در نظر بگیرید که علاوه بر شرکت اصلی، از سه شرکت زیرمجموعه برای فعالیت‌های سخت‌افزار، نرم‌افزار و شبکه استفاده می‌کند. برای شرکت اصلی، یک

Domain به‌نام a.net را در نظر گرفته آن‌را ثبت می‌کنیم. حال با توجه به گستردگی فعالیت‌های شرکت بزرگ‌رایانه‌ای و طبیعتاً شرکت‌های زیرمجموعه، بد نیست که برای هر کدام از زیرمجموعه‌ها نیز یک domain در نظر بگیریم :

برای شرکت سخت‌افزار : hardware.a.net

برای شرکت نرم‌افزار : software.a.net

برای شرکت شبکه : network.a.net

هر یک از domainهای فوق را اصطلاحاً یک SubDomain از a.net می‌نامیم.

اگر 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 رایانه‌هایی که از سیستم‌عامل‌های خانوادهٔ مایکروسافت بهره برده و در ضمن پروتکل TCP/IP روی آن‌ها فعال می‌شود، دو اسم مدنظر قرار می‌گیرد :

الف) هنگام نصب OS یک اسم حداکثر ۱۵ کاراکتری به رایانه داده می‌شود که باید در محدوده شبکه داخلی منحصر به‌فرد بوده و تکراری نباشد. این اسم به Computer Name یا NetBIOS Name معروف است (لزومی ندارد که حتماً پروتکل NetBIOS روی رایانه نصب باشد، در هر صورت به آن NetBIOS Name می‌گویند). می‌دانیم که در سیستم‌عامل 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 رایانه 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 قالب اول یا دوم باشد. به صورت پیش‌فرض در رایانه‌هایی 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 به صورت تک قسمتی برابر با آن می‌شود یعنی در قالب اول است.

اگر رایانه به عضویت Domain در Active Directory درآید آنگاه TCP/IP Name به صورت زیر درمی‌آید :

TCP/IP Name NetBIOS Name Active Directory Domain Name

یعنی TCP/IP Name در قالب دوم می‌شود.

فعالیت عملی

هر گروه از هنرجویان که یک دستگاه رایانه مستقل در اختیار دارند به‌دلخواه یک Domain Name انتخاب کرده سپس Full Computer Name را در سیستم خود تغییر دهند.

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)، سیستم‌عامل از شما می‌خواهد تا رایانه 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.

البته همان‌طور که گفته شده اسامی TCP/IP در قالب دوم تا هنگامی که رسماً در «مراکز شناخته شده ثبت اسامی» یا به زبان فنی (DNS Server) ثبت نشوند نمی‌توانند مورد استفاده بقیه قرار گیرند، لذا فعالیت عملی فوق صرفاً برای آشنایی بیشتر هنرجو 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 :

۲ــ۴ــ۶ــ IP Address Host Address : در پروتکل TCP/IP دو نوع آدرس برای IP وجود دارد :

الف) آدرس IP نسخه ۴ که به آن IPv4 می‌گویند.

ب) آدرس IP نسخه ۶ که به آن IPv6 می‌گویند.

در این کتاب ما به تشریح کامل IPv4 خواهیم پرداخت (ویندوز XP فقط از IPv4 پشتیبانی می‌کند که به صورت IP نمایش داده می‌شود)

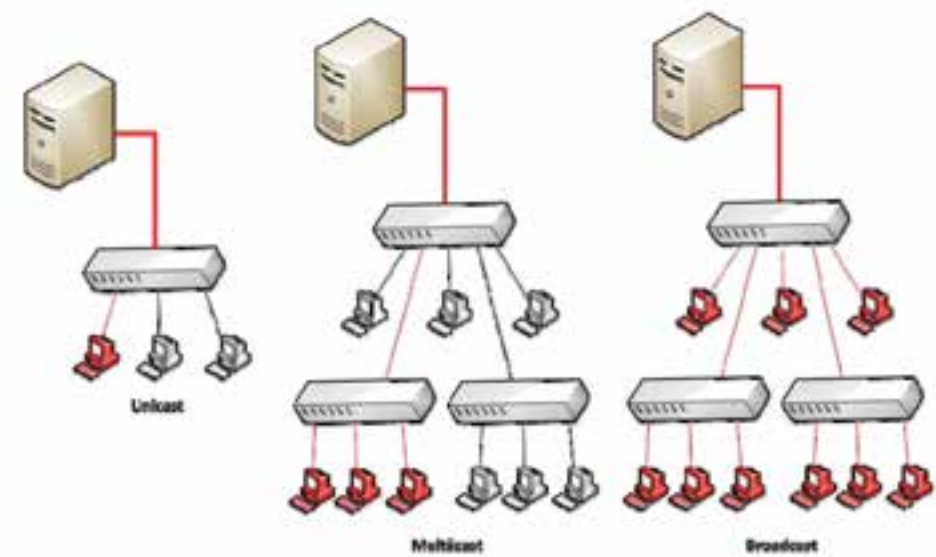
استانداردهای اینترنت برای انواع آدرس‌های IPv4 عبارتند از :

الف) Unicast : برای یک رابط شبکه در یک زیر شبکه اختصاص می‌یابد (یک مخاطب) برای ارتباط یک به یک استفاده می‌شود مانند آدرس یک منزل در شهر به عنوان یک گیرنده.

ب) Multicast : به یک یا چند رابط شبکه واقع در زیرشبکه‌های مختلف اختصاص می‌یابد(چند مخاطب) و برای ارتباط یک به چند استفاده می‌شود.

ج) Broadcast : به تمام رابط‌های شبکه در یک زیر شبکه اختصاص داده می‌شود (برای تمام مخاطب‌های یک زیر شبکه) و برای ارتباط یک به همه در یک زیر شبکه مورد استفاده قرار می‌گیرد.

شکل ۱ــ۶ مقایسه گرافیکی بین انواع ارسال در شبکه را نشان می‌دهد رایانه‌هایی که با رنگ قرمز مشخص شده اند به عنوان دریافت کننده (مخاطب) می‌باشند :



شکل ۱ــ۶ــ استانداردهای اینترنت

۳ــ۴ــ۶ــ آدرس‌های Unicast در IPv4 : آدرس‌های Unicast در IPv4 محل قرار گرفتن مخاطب را در شبکه تعیین می‌کنند، مانند آدرس منزل یک شخص در یک شهر. بنابراین آدرس‌های Unicast در IPv4 باید در سطح جهان منحصر به فرد بوده و دارای قالب یکسان باشد.

(البته می‌توان برای چند شبکه مستقل که قرار نیست با هم در ارتباط باشند آدرس‌های IP یکسانی در نظر گرفت).

هر آدرس IPv4 دارای دو بخش پیشوند زیر شبکه و ID میزبان به صورت زیر می‌باشد :

IPv4 Address Subnet prefix host ID

Subnet prefix (پیشوند زیر شبکه) به عنوان شناسه شبکه[۱] یا آدرس شبکه[۲] شناخته می‌شود و تمام گره‌های شبکه در یک زیر شبکه باید دارای Subnet prefix یکسانی بوده. و پیشوند زیر شبکه باید در کل شبکه‌های TCP/IP منحصر به فرد باشد با توجه به مطالب فوق می‌توان IPv4 Address Subnet prefix host ID را به صورت زیر نیز تعریف نمود :

IPv4 Address Network ID Host ID

Host ID (ID میزبان) غالباً به عنوان آدرس میزبان[۳] شناخته می‌شود و برای شناسایی گره‌ها در زیر شبکه به کار می‌رود. ID میزبان نیز باید در یک زیر شبکه منحصر به فرد باشد. می‌توان به جای Host ID از Node ID نیز استفاده نمود.

IP Address در مجموعه یک عدد ۳۲ بیتی یا ۴ بایتی است که به فرم w.x.y.z تنظیم می‌شود. به طوری که ممکن است از ۴ بایت ممکن یک تا ۳ بایت برای پیشوند زیر شبکه و یا یک تا ۳ بایت برای ID میزبان در نظر گرفته شود.

۴ـ۴ـ۶ـ کلاس‌های آدرس در IPv4 : آدرس‌های IPv4 دارای کلاس‌های مختلفی است که میزان بیت یا بایت اختصاص یافته به پیشوند زیر شبکه و Host ID را مشخص می‌کند. این کلاس‌ها همچنین تعداد شبکه‌ها و تعداد میزبان‌ها را نیز تعیین می‌کنند. به طور کلی پنج نوع کلاس در IPv4 داریم که با نام‌های کلاس A، B، C، D و E شناخته می‌شود. کلاس A ، B و C برای Unicast می‌باشد . کلاس D برای Multicast رزرو شده و کلاس E نیز برای کارهای آزمایشگاهی رزرو شده است.

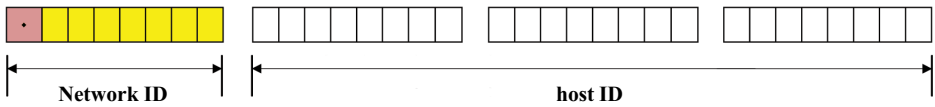
الف) کلاس A : برای شبکه‌هایی که دارای میزبان‌های خیلی زیاد هستند مورد استفاده قرار می‌گیرد، به طوری که ۸ بیت اول برای پیشوند زیر شبکه و ۲۴ بیت باقیمانده برای میزبان مورد استفاده قرار می‌گیرد قالب آدرس دهی در کلاس A به صورت زیر است :

۱ـ Network dent f er

۲ـ Network Address

۳ـ Host Address

Network.host.host.host



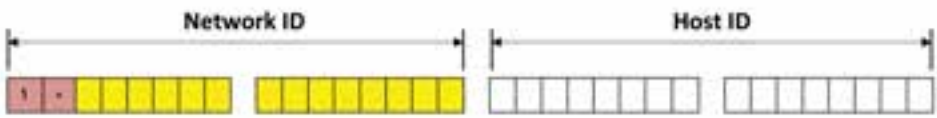
شکل ۲ــ۶ــ کلاس آدرس A

کلاس A تا ۱۶۷۷۷۲۱۴ میزبان را می‌تواند آدرس‌دهی کند و بجای هر host در قالب آدرس‌دهی می‌توان از اعداد ۱ تا ۲۵۴ را استفاده نمود. توجه داشته باشید در واقع اعداد اختصاص یافته به هر host در قالب کلی 2^8 یعنی از ۰ تا ۲۵۵ می‌باشد ولی اعداد ۰ و ۲۵۵ در شرایط خاصی استفاده می‌شود.

کلاس A تا ۱۲۶ شبکه را پشتیبانی می‌کند یعنی به جای Network می‌توان از اعداد ۱ تا ۱۲۶ را استفاده نمود. در کلاس A اولین بیت سمت چپ همیشه باید صفر باشد با توجه به صفر بودن اولین بیت سمت چپ پس ما ۷ بیت داریم که می‌توانند ۱ باشند بنابراین 2^7 ۱ یعنی ۱۲۷ شبکه خواهیم داشت اما چون عدد ۱۲۷ برای Loop back ذخیره شده است ما فقط می‌توانیم تا عدد ۱۲۶ را برای کلاس A استفاده نماییم.

ب) کلاس B : کلاس B برای شبکه‌های متوسط تا بزرگ مورد استفاده قرار می‌گیرد به طوری که ۱۶ بیت اول برای شبکه و ۱۶ بیت باقیمانده برای میزبان مورد استفاده قرار می‌گیرد. قالب آدرس‌دهی در کلاس B به صورت زیر است :

Network.Network.host.host



شکل ۳ــ۶ــ کلاس آدرس B

در کلاس B اولین بیت سمت چپ در Network ID همیشه 1 و دومین بیت همیشه 0 می‌باشد یعنی بایت اول در حالت حداکثری برابر 10111111 می‌باشد (یعنی عدد ۱۹۱) پس نتیجه می‌گیریم که در کلاس B اولین بایت یا همان w می‌تواند اعداد ۱۲۸ تا ۱۹۱ باشد

کلاس B تا ۱۶۳۸۴ شبکه را پشتیبانی می‌کند همچنین می‌توان در کلاس B تا ۶۵۵۳۴ میزبان را آدرس دهی نمود.

(۶۵۵۳۴ ۲ ^{16}۲ تمام صفر و تمام یک استفاده نمی‌شود.)

ج) کلاس C : کلاس C برای آدرس دهی شبکه‌های کوچک استفاده می‌شود به طوری که ۲۴ بیت (۳ بایت) اول برای شبکه و ۸ بیت (۱بایت) باقیمانده برای میزبان مورد استفاده قرار می‌گیرد. قالب آدرس دهی در کلاس C به صورت زیر است :

Network . Network . Network . host

شکل ۴ــ۶ــ کلاس آدرس C

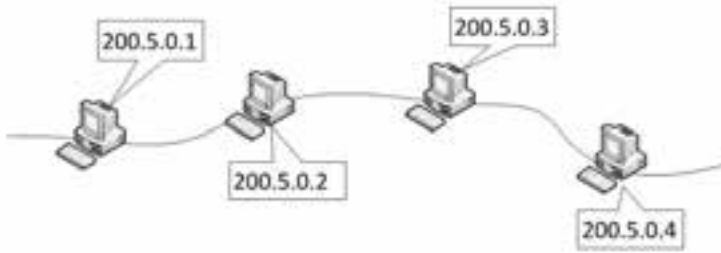
در کلاس C اولین و دومین بیت سمت چپ در Network ID همیشه 1 و سومین بیت همیشه 0 می‌باشد یعنی بایت اول در حالت حداکثری برابر 11011111 می‌باشد (یعنی عدد ۲۲۳) پس نتیجه می‌گیریم که در کلاس C اولین بایت یا همان w می‌تواند اعداد ۱۹۲ تا ۲۲۳ باشد.

کلاس C تا ۲۰۹۷۱۵۲ شبکه را پشتیبانی می‌کند همچنین در این کلاس می‌توان تا ۲۵۴ میزبان را آدرس دهی نمود.

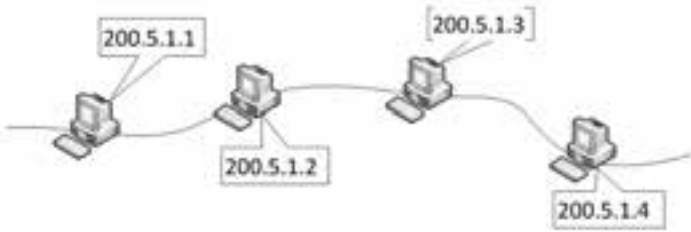
جدول ۱ــ۶ ــ خلاصه کلاس‌های Unicast

نام کلاس	مقدار W	بخش شبکه	بخش میزبان	آدرس‌های شبکه	آدرس‌های میزبان
A	۱ــ۱۲۶	w	x y z	۱۲۶	۱۶۲۷۷۲۱۴
B	۱۲۸ــ۱۹۱	w x	y z	۱۶۳۸۴	۶۵۵۳۴
C	۱۹۲ــ۲۲۳	w x y	z	۲ ۹۷۱۵۲	۲۵۴

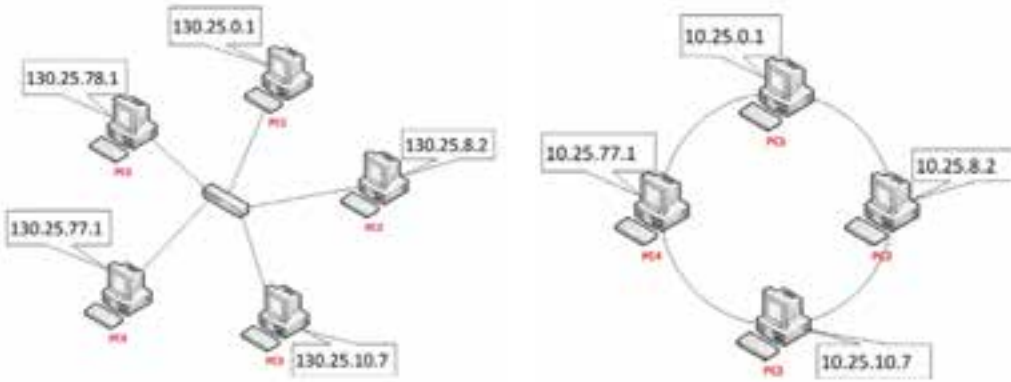
به شکل ۵ــ۶ توجه کنید :



الف)



ب)



ج)

د)

شکل ۵ــ۶

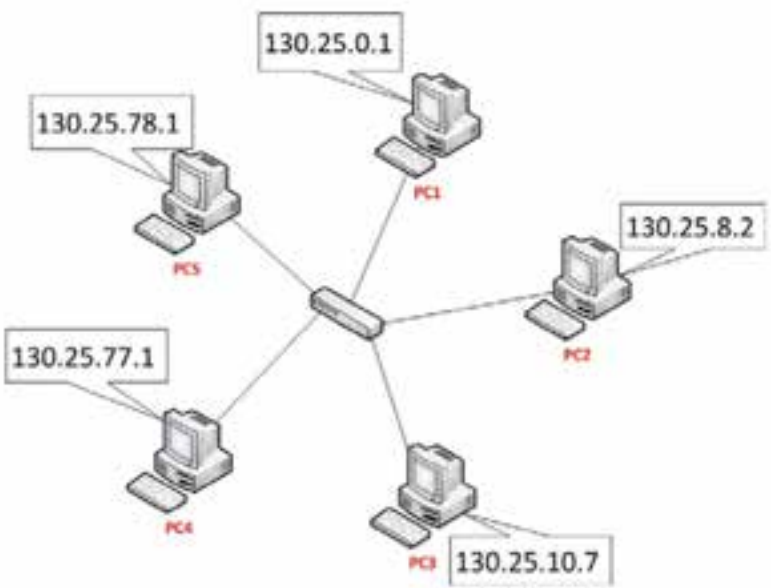
در شکل ۵ــ۶ــالف w برابر ۲۰۰ می‌باشد در نتیجه از کلاس C در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که 200.5.0 Network ID می‌باشد و Host ID هر گره ۱،۲،۳ و ۴ می‌باشد.

در شکل۵ــ۶ــب w برابر ۲۰۰ می‌باشد در نتیجه از کلاس C در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که 200.5.1 Network ID می‌باشد و Host ID هر گره ۱،۲،۳ و ۴ می‌باشد.

در شکل ۵ــ۶ــ ج w برابر ۱۰ می‌باشد در نتیجه از کلاس A در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID 10 می‌باشد و Host ID (PC1) 25.0.1 و Host ID (PC2) 25.8.2 و Host ID (PC3) 25.10.7 و Host ID (PC4) 25.77.1 می‌باشد.

در شکل ۵ــ۶ــ د w (برابر 130 می‌باشد در نتیجه از کلاس B در IPv4 استفاده شده است بنابراین می‌توان نتیجه گرفت که Network ID 130.25 می‌باشد و Host ID (PC1) 0.1 و Host ID (PC2) 8.2 و Host ID (PC3) 10.7 و Host ID (PC4) 77.1 و Host ID (PC5) 78.1 می‌باشد.

نکته ۱ : چنانچه تمام بیت‌های مربوط به Host ID برابر 0 باشد در آن صورت به IP آدرس شماره شبکه یا Network Number که به اختصار به آن NN می‌گویند برای مثال در شکل۶ــ۶ Network ID 130.25 در نتیجه 130.25.0.0 NN خواهد بود. از شماره شبکه یا NN نمی‌توان برای یک گره استفاده نمود.



شکل ۶ــ۶

نکته ۲ : اگر اعداد مربوط به Host ID برابر ۲۵۵ باشد عدد حاصله برای Broadcast Address نامیده می‌شود و برای ارسال به تمام سیستم‌های موجود در همان شبکه مورد استفاده قرار می‌گیرد که اصطلاحاً به آن BA گفته می‌شود. با توجه به مثال قبل می‌توان گفت که 130.25.255.255 BA می‌باشد.

اگر کاربری فرمان ارسال اطلاعات را برای 130.25.10.7 صادر کند فقط یک Host یا Node که دارای آدرس مشخص شده می‌باشد اطلاعات را دریافت (پردازش) خواهد کرد که اصطلاحاً Unicast گفته می‌شود ولی اگر فرمان ارسال اطلاعات برای 130.25.255.255 صادر شود ، تمام گره‌های متصل به شبکه‌های با آدرس شبکه 130.25 Network ID اطلاعات را دریافت و پردازش خواهد نمود. که اصطلاحاً Broadcast نامیده می‌شود.

د) کلاس D : همان طور که قبلاً اشاره شد کلاس D برای Multicast رزرو شده است. 4 بیت اول در کلاس D به صورت 1110 می‌باشد یعنی بایت اول در حالت حداکثری برابر 11101111 می‌باشد (یعنی عدد 239) پس نتیجه می‌گیریم که در کلاس D اولین بایت یا همان w می‌تواند اعداد ۲۲۴ تا ۲۳۹ باشد یعنی کلاس D از رنج 224.0.0.0 تا 239.255.255.255 می‌باشد.

هـ) کلاس E : برای کارهای آزمایشگاهی(تحقیقاتی) رزرو شده است ۴ بیت اول در کلاس E همیشه به صورت 1111 می‌باشد یعنی بایت اول در حالت حداقلی برابر 11110000 می‌باشد (یعنی عدد ۲۴۰) و حداکثر مقدار برابر 11111111 می‌باشد(یعنی عدد 255) پس نتیجه می‌گیریم که در کلاس E اولین بایت یا همان w می‌تواند اعداد ۲۴۰ تا ۲۵۵ باشد.

آدرس‌های IPv4 در شبکه به وسیله رایانه‌ها به صورت رشته ای از بیت‌ها دیده می‌شود که به صورت ۴ گروه ۸ تایی می‌باشند از بیت‌ها،به عنوان مثال : 130.1.16.1 به صورت زیر دیده می‌شود :

10000010 00000001 00010000 00000001

IPv4 از آدرس چندپخشی(Multicast) برای ارائه بسته‌های اطلاعاتی از یک منبع به چند مقصد استفاده می‌کند .همچنین IPv4 آدرس‌های Broadcast را برای ارائه بسته‌های اطلاعاتی از یک منبع به همه رابط‌های بر روی زیر شبکه به کار می‌برد .

۵ــ۴ــ۶ــ آدرس‌های ویژه در IPv4

۱ــ آدرس 0.0.0.0 : به آدرس IPv4 نامشخص معروف می‌باشد و فقط برای آدرس منبع ،

زمانی که گره با IPv4 پیکربندی نشده باشد و با استفاده از سرویس DHCP بخواهد IPv4 خود را به دست آورد مورد استفاده قرار می‌گیرد.

۲ــ آدرس 127.0.0.1 : به نام آدرس Loop back معروف می‌باشد و یک گره را برای ارسال بسته‌ها به خودش فعال می‌کند.

۶ ــ۴ــ۶ــ ماسک زیر شبکه یا Subnet Mask : ماسک زیر شبکه برای نشان دادن شناسه مربوط به شبکه و همچنین شناسه مربوط به میزبان می‌باشد. که بیت‌های هر بخش آن یا همه صفر و یا همه ۱ هستند (یعنی اعداد ۰ و ۲۵۵) به طوری که برای تعیین شناسه شبکه ، به ازای هر بخش آدرس شبکه ؛ عدد ۲۵۵ قرار می‌گیرد و به ازای هر بخش میزبان عدد صفر جایگزین می‌شود و عدد ۲۵۵ به مفهوم ثابت بودن آدرس IP در یک زیر شبکه می‌باشد و عدد ۰ به مفهوم عدد متغیر ۱ تا ۲۵۴ می‌باشد. ضمناً با استفاده از ماسک زیر شبکه می‌توان کلاس شبکه را تعیین نمود. به مثال‌های زیر توجه کنید :

۱ــ اگر آدرس IPv4 یک گره برابر عدد 192.168.1.1 باشد در آن صورت Subnet Mask آن به صورت 255.255.255.0 خواهد بود. و آدرس IP از نوع کلاس C می‌باشد.

۲ــ اگر آدرس IPv4 یک گره برابر عدد 10.10.1.1 باشد در آن صورت Subnet Mask آن به صورت 255.0.0.0 خواهد بود. و آدرس IP از نوع کلاس A می‌باشد.

حتماً مشاهده کرده‌اید که هنگام واردکردن IP بخشی نیز برای واردکردن آدرس Default Gateway داریم. این آدرس معمولاً دو کاربرد اصلی دارد :

ــ آدرس کامپیوتری که اینترنت را برای کلاینت Share کرده است.

هنگامی‌که یک کامپیوتر در شبکه به اینترنت وصل است و باید اینترنت را در اختیار بقیه قرار دهد چنین حالتی پیش می‌آید. البته همیشه به این سادگی و فقط با تنظیم Gateway کارها انجام نمی‌شود اما این یکی از ساده‌ترین حالت‌هاست.

ــ آدرس پورت روتر در سمتی از سگمنت[۱] که کلاینت در آن قرار دارد تا بدین وسیله به روتر وصل شود و در نتیجه با سگمنت‌های دیگر ارتباط برقرار کند.

نوع کلاس مورد استفاده برای آدرس‌دهی شبکه خود بستگی به تعداد Hostهای به‌کار رفته در شبکه دارد. به مثال زیر دقت کنید :

مثال : شبکه‌ای داریم متشکل از ۱۶۰ Host که با توجه به توسعه آن ممکن است به ۲۳۰ Host

---

۱ــ Segment : به بخشی از شبکه که سیستم‌های آن دارای یک Network ID هستند اشاره می‌کند و گاهی به بخشی از شبکه که بین تجهیزات شبکه‌ای مثل دو روتر یا دو سوئیچ قرار دارد گفته می‌شود.

افزایش پیدا کند از کدام کلاس استفاده کنیم؟ هر یک از کلاس‌های A,B,C را می‌توان به کار برد اما نظر به اینکه تعداد Host از ۲۳۰ عدد بیشتر نمی‌شود بهتر است از کلاسC استفاده کنیم و به عبارت دیگر آدرس‌ها را هدر ندهیم. بنابراین باید یک Net ID منحصر به‌فرد در کلاس C را که در شبکه‌های دیگر استفاده نشده باشد انتخاب کرده و آن را 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 مسؤولیت تخصیص فضای آدرس‌ها را به عهده 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 به‌فرد در اختیار ما قرار داده می‌شود. فرض کنیم که در مثال یاد شده، NetID اختصاص یافته برای شرکت ما عدد ۲۱۳,۲۱۷,۲۴ باشد. بهتر است بگوییم شماره شبکه ما (Network Number) برابر با ۲۱۳,۲۱۷,۲۴,۰ است. با در اختیار داشتن Network Number مذکور به‌راحتی می‌توانیم کلیهٔ Hostها را از ۱ تا حداکثر ۲۵۴ شماره‌گذاری کنیم. به ترتیب زیر :

First Host ۲۱۳,۲۱۷,۲۴,۱ Second Host ۲۱۳,۲۱۷,۲۴,۲

Third Host ۲۱۳,۲۱۷,۲۴,۳

:

Last Host ۲۱۳,۲۱۷,۲۴,۲۵۴

البته در مثال فوق ۲۳۰ هاست داشتیم و بنابراین آدرس آخرین Host می‌شود : 213.217.24.230، اما با توجه به توان بالقوهٔ کلاس C، برای هر NetID می‌توانیم تا حداکثر Host ۲۵۴ را شماره‌گذاری کنیم و لذا آدرس آخرین Host را 213.217.24.254 نوشتیم و از این پس در بقیهٔ مثال‌ها نیز چنین خواهیم کرد.

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

Network Number 213.217.24.0

Broadcast Address 213.217.24.255

به‌طورکلی در حل این‌گونه مسائل باید ۴ مرحله را طی کنیم :

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

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

مرحله سوم : تعیین آدرس اولین Host الی آخرین Host.

مرحله چهارم : تعیین Broadcast Address.

مطالعه آزاد

تا قبل از ویندوز ویستا ، فقط نسخه ۴ آدرس IP در شبکه ها استفاده می‌شد (IPv4) که تا حدود ۴ میلیارد آدرس IP را پشتیبانی می کرد با توجه به افزایش تعداد شبکه‌ها ، در ویندوز ویستا، ویندوز ۷ و ویندوز ۲۰۰۸ سرورنسخه ۶ برای IP ایجاد شد (IPv6).

IPv6 به جای ۳۲ بیت از ۱۲۸بیت برای آدرس دهی IP استفاده می کند و در واقع از ۸ بخش۱۶بیتی تشکیل شده است. و مقداردهی آن به صورت هگزا دسیمال می‌باشد و با : از یکدیگر جدا می شوند.

FE80: BA98: 7654: 3210: FEDC: BA98: 7654: 3210

آدرس دهی درIPv6 به دو قسمت تقسیم می شود به طوری که ۶۴ بیت اول (۸ بخش اول) برای آدرس دهی شبکه و ۶۴بیت دوم (۸ بخش دوم) برای آدرس دهی میزبان استفاده می شود :

بخش آدرس دهی شبکه در واقع همان Prefix Subnet (پیشوند زیر شبکه) می‌باشد.

IPv6 ایمن تر از IPV4 می باشد. پروتکل IPv6 قادر به حمایت از ۵۰ اکتیلیون (هر اکتیلیون معادل یک عدد به همراه ۴۸ صفر است) آدرس IP است.

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

۲ــ سرویس‌های رایج در پروتکل TCP/IP را نام ببرید.

۳ــ تفاوت عمده و اساسی ترمینال با یک رایانه PC چیست؟

۴ــ کدام سرویس TCP/IP از ترمینال استفاده می‌کند؟ برای اتصال به سیستم مرکزی به چه چیزهایی نیاز دارد؟

۵ــ وظیفه Windows time چیست؟

۶ــ نام پروتکلی که ارسال ایمیل را انجام می‌دهد چیست؟

۷ــ وظیفه Terminal Service را شرح دهید.

۸ــ Host چیست؟ خصوصیت اصلی هر Host را نام ببرید.

۹ــ مراحل ثبت Domain را شرح دهید.

۱۰ــ کار SubDomain چیست؟

۱۱ــ پژوهش کنید آدرس Loop Back چیست؟

۱۲ــ پژوهش کنید که TCP/IP نسخه ۶ چیست و چه تفاوتی با نسخه ۴ دارد؟

۱۳ــ پژوهش کنید که چند کاربر می‌توانند به طور هم‌زمان از RDP استفاده کنند.

۱۴ــ پژوهش کنید که چه دستوراتی در محیط FTP رایج است؟

۱۵ــ پژوهش کنید که Domainهای .org,.inf,.prof,.gov,.ac,.com,.net,.edu در چه حوزه‌هایی مورد استفاده قرار می‌گیرند.

۱۶ــ پژوهش کنید که تفاوت Valid IP و InValid IP در چیست؟

فصل هفتم

امنیت در شبکه

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- دیواره آتش را تعریف کند و با آن کار کند.
- تفاوت آنتی ویروس و دیواره آتش را بیان کند.

امنیت در شبکه دارای سطوح مختلفی است، یک مدیر شبکه برای محدود کردن کاربران غیرمجاز می‌تواند از سطح نام کاربری و گذرواژه استفاده کند. در حالی که اگر این شبکه به شبکهٔ 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 (Firewall) به صورت سخت‌افزاری و نرم‌افزاری خواهد داشت.

رعایت امنیت در شبکه یکی از موارد ضروری است که مدیر شبکه و حتی کاربران باید رعایت نمایند با توجه به اینکه در سال دوم آنتی‌ویروس آموزش داده شده است در این فصل دیواره آتش[1] مورد بحث قرار می‌گیرد.

۱ـ۷ـ دیواره آتش (Fire wall)

دیواره آتش یکی از موثرترین و مهمترین روش‌های پیاده‌سازی امنیت شبکه می‌باشد که تا حد زیادی از دسترسی غیرمجاز دنیای بیرون به منابع داخلی شبکه جلوگیری می‌کند. دیواره آتش می‌تواند یک دستگاه سخت‌افزاری و یا یک برنامه نرم‌افزاری و یا ترکیبی از هر دو باشد که اطلاعات ورودی از اینترنت یا شبکه به سیستم را بررسی کرد. و براساس تنظیمات اعمالی، کلیه دسترسی‌های شبکه را کنترل

۱ـ Firewall

می‌نماید، به‌طوری که به برخی از درخواست‌ها اجازه ورود به شبکه داده شده و به برخی دیگر اجازه ورود داده نمی‌شود. دیواره آتش سخت‌افزاری معمولاً در شبکه‌های بزرگ مورد استفاده قرار می‌گیرد. به دیواره آتش نرم‌افزاری، دیواره آتش داخلی و به دیواره آتش سخت‌افزاری، دیواره آتش خارجی می‌گویند.

دیواره آتش سخت‌افزاری در بین شبکه شما و یک شبکه دیگر در سازمان دیگر و یا اینترنت قرار گرفته و سطوح امنیتی را برای شما فراهم می‌کند. دیواره آتش نرم‌افزاری نیز برای برقراری لایه امنیتی استفاده می‌شوند. در برخی از سیستم‌عامل‌ها این نوع دیواره آتش نصب شده است که باید آن را پیکربندی و فعال نمایید.

دیواره آتش از دسترسی هکرها و برنامه‌های مخرب (مانند کرم‌ها) به رایانه شما از طریق شبکه یا اینترنت جلوگیری می‌کند. یک دیواره آتش همچنین می‌تواند از ارسال برنامه‌های مخرب از طریق رایانه شما به شبکه نیز جلوگیری کند. از طریق دیواره آتش می‌توان با انجام تنظیمات مربوطه از اجرای یک برنامه خاص جلوگیری نمود. دیاگرام ساده‌ای از دیواره آتش در شکل ۱ــ۷ آورده شده است :

شکل ۱ــ۷ــ تصویر عملکرد دیواره آتش

دیواره آتش به لحاظ سطح استفاده به دو دسته تقسیم می‌شود :

دیواره آتش شخصی یا رومیزی (Desktop or personal firewalls) : که برای محافظت از یک میزبان طراحی شده است. دیواره آتش شخصی نرم‌افزاری است که برای محافظت از یک رایانه که به اینترنت متصل است مورد استفاده قرار می‌گیرد. علاوه‌بر دیواره آتش پیش‌فرض ویندوز، شرکت‌های دیگری نیز برای رایانه‌های شخصی دیواره آتش تولید کرده‌اند که

Zone Alarm ، cillin Trend Micro's PC و Symantec نمونه‌ای از این شرکت‌ها می‌باشند.

دیواره آتش شبکه یا سروری (Network firewalls) : که برای محافظت از شبکه در برابر حملات طراحی شده است و بالاترین سطح حفاظت را در اختیار کاربران سازمانی قرار می‌دهد. یکی از ویژگی‌های دیواره آتش شبکه، مدیریت متمرکز می‌باشد که با استفاده از آن می‌توان تمام کاربران شبکه را مورد حفاظت قرار داد.

با استفاده از دیواره آتش شبکه علاوه بر حفاظت دسترسی از خارج، می‌توان برای محدود کردن دسترسی اعضای شبکه به خارج از شبکه نیز پیکربندی لازم را انجام داد.

توجه داشته باشید که دیواره آتش یک سطح حفاظتی را ارائه می‌کند ولی هرگز عدم تهاجم به سیستم شما را تضمین نمی‌کند. همچنین دیواره آتش برای مقابله با خطرات شناخته شده طراحی شده است. استفاده از دیواره آتش به همراه سایر امکانات حفاظتی مانند نرم‌افزارهای آنتی‌ویروس و رعایت توصیه‌های ایمنی می‌تواند یک سطح مطلوب از امنیت را برای شما و شبکه فراهم سازد.

یک دیواره آتش معمولاً نمی‌تواند از ورود ویروس‌ها جلوگیری کند. اغلب دیواره‌های آتش بخش‌های مربوط به آدرس مبدأ و مقصد و شماره پورت مبدأ و مقصد شبکه‌های ورودی را مورد بررسی قرار می‌دهند و به جزئیات داده توجهی ندارند.

> **نکته ۱:** یک دیواره آتش نمی‌تواند شبکه و منابع آن را از خرابکاران داخلی محافظت کند.

۲ـ۷ـ وظایف دیواره آتش

وظایف دیواره آتش به شرح ذیل دسته‌بندی می‌شود :

ـ **مدیریت و کنترل ترافیک شبکه** : که به‌عنوان اولین و اساسی‌ترین وظیفه دیواره آتش می‌باشد.

ـ **ثبت و گزارش وقایع** : ثبت وقایع یکی از مشخصه‌های بسیار مهم یک دیواره آتش به‌شمار می‌رود. مدیر شبکه می‌تواند با کمک اطلاعات ثبت شده به کنترل ترافیک ایجاد شده توسط کاربران مجاز بپردازد. در یک روال ثبت مناسب، مدیر می‌تواند به راحتی به بخش‌های مهم از اطلاعات ثبت شده دسترسی پیدا کند.

همچنین یک دیواره آتش خوب باید بتواند علاوه‌بر ثبت وقایع، در شرایط بحرانی، مدیر شبکه را

از وقایع مطلع کند و برای وی اخطار بفرستد.

توصیه می‌شود در حالت پیش‌فرض تنظیمات زیر برای دیواره آتش انجام گیرد :

۱ــ دیواره آتش فعال باشد.

۲ــ دیواره آتش برای تمام نقاط شبکه فعال باشد (منزل یا محل کار، مکان عمومی، و یا دامنه).

۳ــ دیواره آتش برای تمام اتصالات شبکه فعال باشد.

۴ــ تمام اتصالات ورودی غیرضروری مسدود شوند.

فعالیت کارگاهی

۳ــ۷ــ تنظیمات دیواره آتش در ویندوز

در اینجا این سؤال مطرح می‌شود که چگونه می‌توان از فعال‌بودن دیواره آتش در ویندوز ۲۰۰۸ سرور اطمینان حاصل نمود؟ در ویندوز ۲۰۰۸ سرور آتش به‌طور پیش‌فرض فعال می‌باشد ولی برای اطمینان از فعال‌بودن آن ابتدا باید برنامه دیواره آتش را با استفاده از روش‌های زیر اجرا نمود :

روش اول : از Control Panel برنامه Windows Firewall را اجرا کنید.

روش دوم : در کادر Start Search در منوی Start عبارت Firewall را تایپ نموده و سپس برنامه Windows Firewall را اجرا نمایید.

در این هنگام پنجره Windows Firewall نمایش داده شود (شکل ۲ــ۷) که حالت فعال‌بودن (on) دیواره آتش در شکل به‌خوبی مشخص می‌باشد.

شکل ۲ــ۷ــ دیواره آتش در ویندوز ۲۰۰۸ سرور

اگر دیواره آتش غیرفعال (off) باشد پنجره مربوطه به صورت شکل ۳ـ۷ نمایش داده خواهد شد و رایانه شما در حالت خطر یا ریسک قرار خواهد داشت.

شکل ۳ـ۷ـ دیواره آتش در حالت غیرفعال

برای فعال یا غیرفعال‌کردن دیواره آتش بر روی گزینه Change setting شکل ۲ـ۷ یا ۳ـ۷ کلیک نمایید تا پنجره تنظیمات دیواره آتش نمایش داده شود.

الف) پنجره تنظیمات دیواره آتش در حالت فعال

ب) پنجره تنظیمات دیواره آتش در حالت غیرفعال

شکل ۴ـ۷

نکته : زمانی گزینه Block all incoming connections در شکل ۴ــ۷ــ الف را فعال می‌کنند که شما می‌خواهید بالاترین سطح حفاظت را داشته باشید و یا اینکه شما با یک شبکه با امنیت خیلی پایین در ارتباط هستید. توجه داشته باشید که فعال‌کردن این گزینه باعث می‌شود تا تمامی ارتباطات بیرونی محدود شود.

۴ــ۷ــ استثناء کردن یک برنامه یا سرویس با استفاده از زبانه Exceptions

با استفاده از زبانه Exceptions می‌توان برای بعضی از برنامه‌های کاربردی استثناء قائل شد و یا اینکه بعضی از درگاه‌ها[۱] را برای تبادل اطلاعات باز گذاشت. در این زبانه بعضی از برنامه‌ها به‌صورت پیش‌فرض استثناء شده‌اند و بعضی‌ها نیز انتخاب نشده‌اند که قابل انتخاب می‌باشند. همچنین می‌توان با استفاده از دکمه Add Program برنامه جدیدی را به لیست استثناها اضافه نمود. توجه داشته باشید فقط برنامه‌هایی را که به‌طور دستی اضافه نموده‌اید می‌توانید با استفاده دکمه delete حذف نمایید. البته این کار باید با دقت لازم انجام شود تا امنیت سیستم شما دچار اختلال نشود.

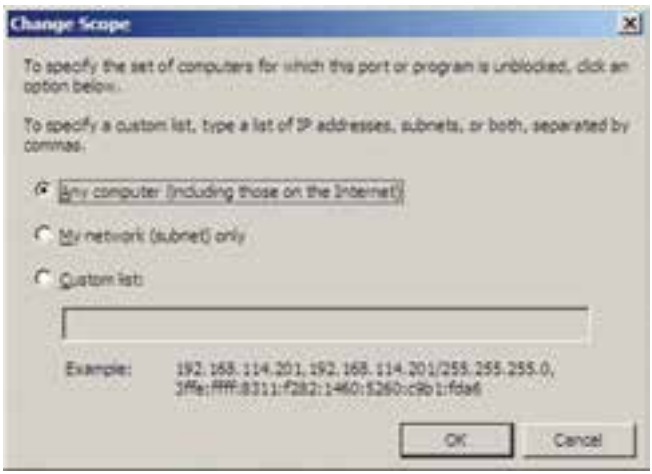
شکل ۵ ــ۷ــ کادر تنظیمات Exceptions

۱ Ports

یکی از نکات مهم در زمان اضافه کردن برنامه جدید به لیست استثناها این است که می‌توان برای آن برنامه دامنه استفاده کاربران را تعیین نمود. بعد ازکلیک‌کردن بر روی دکمه ...Add Program کادر Add a Program ظاهر می‌گردد که شما می‌توانید دامنه کاربرانی که بتوانند از برنامه مورد نظر استفاده کنند را انتخاب نمایید (شکل ۶ــ۷).

شکل ۶ــ۷ــ کادر اضافه‌کردن برنامه به لیست استثناها

برای انتخاب دامنه مجموعه رایانه‌ها بر روی دکمه... Change scope کلیک کنید تا کادر انتخاب دامنه ظاهر گردد (شکل ۷ــ۷).



شکل ۷ــ۷ــ کادر انتخاب دامنه

در کادر Change scope سه انتخاب وجود دارد :

۱ــ **Any computer(Including those on the Internet)** : تمام رایانه‌ها حتی رایانه‌های در اینترنت (پایین‌ترین سطح امنیتی)

۲ــ **My Network (Subnet) Only** : فقط رایانه‌های موجود در شبکه‌ای که دارای subnet یکسانی با این رایانه می‌باشند.

۳ــ **Custom list** : می‌توان آدرس‌های IP رایانه‌های خاصی که مد نظر می‌باشند را اضافه نمود. (بالاترین سطح امنیتی)

کار عملی

تعیین کنید برنامه‌های netsupport ، Msn Messenger و Google Talk از چه درگاه‌هایی برای ارتباط استفاده می‌کنند. برنامه را برای امکان ارتباط با شبکه به دیواره آتش معرفی کنید.

خودآزمایی و پژوهش

۱ــ دیواره آتش چیست؟

۲ــ آیا وجود دیواره آتش در یک شبکه ضروری است؟ چرا؟

۳ــ آیا می‌توان از دیواره آتش به جای ضدویروس استفاده کرد؟ چرا؟

۴ــ کار زبانه Exceptions در پنجره Firewall چیست؟

۵ــ پژوهش کنید که چه برنامه‌های دیواره آتش رایجی وجود دارد؟

بخش دوم

سیستم عامل ویندوز ۲۰۰۸ سرور

فصل هشتم

سیستم عامل‌های شبکه‌ای

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- ویژگی‌های سیستم‌عامل‌های شبکه‌ای را بیان کند.
- انواع سیستم‌عامل‌های شبکه را شناسایی کند.
- مشخصات اصلی سیستم‌عامل ویندوز ۲۰۰۸ سرور را بیان نماید.
- نسخه‌های مختلف ویندوز ۲۰۰۸ سرور را شناسایی نماید.

۱ـ۸ـ آشنایی با ویژگی‌های سیستم عامل‌های شبکه‌ای

سرویس دهنده‌ها و در کل شبکه‌ها به چه سیستم عاملی نیاز دارند؟ پاسخ به این سؤال مستلزم آشنایی با ویژگی‌هایی است که در ادامه بررسی می‌شود. سیستم عامل‌هایی که در شبکه استفاده می‌شوند باید ویژگی‌هایی را افزون بر سیستم عامل‌هایی که در کاربردهای خانگی مورد استفاده قرار می‌گیرند داشته باشند. هرچند امروزه اکثر کاربران خانگی به محض اتصال به اینترنت عملاً به‌عنوان کاربر شبکه محسوب می‌شوند بنابراین خصوصیات سیستم عامل‌های شبکه برای سیستم‌های خانگی نیز (در حدی کمتر) معنی پیدا می‌کند. برخی از این ویژگی‌ها به ترتیب اهمیت عبارتند از :

- Security (امنیت)
- Multitasking (چند وظیفه‌ای)
- Multi Processor Support (پشتیبانی از چندین پردازنده)
- Reliable & Stable (قابلیت اطمینان و پایداری)
- Fault Tolerance (تحمل خطا)
- Backup Utilities (نرم افزار تهیه نسخه پشتیبان)
- Simple & Unified Administrative Tools (ابزارهای مدیریتی)
- Support (پشتیبانی)

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

۱ــ۱ــ۸ــ امنیت[۱] : مهم‌ترین ویژگی است. مسایل امنیتی هر چند که باعث کندی سیستم می‌شود اما به عنوان رکن کار هر سیستم عامل شبکه محسوب می‌شود. امنیت برای سیستم عامل را می‌توان در حوزه‌های مختلفی بررسی کرد به عنوان مثال :

الف) امنیت در حوزهٔ دسترسی به دیسک و فایل ــ سیستم (System Security Disk & File)

ب) امنیت در حوزهٔ 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 تبادلی (Network Services)

د) امنیت در ورود به سیستم (System Login)

مثال : سیستم عامل‌های DOS و خانواده 9x جزو آن‌دسته از سیستم‌هایی هستند که امنیت چندانی مخصوصاً در حوزه‌های «الف»، «ب» و «ج» ندارند. پس از روشن کردن یک رایانه با سیستم عامل ویندوز 98 به راحتی می‌توان بدون هیچگونه گذر واژه‌ای وارد آن شده، به هرجا روی دیسک دسترسی پیدا کرده (که با FAT آماده شده)، هر برنامه‌ای را نصب، حذف یا اجرا کرده و هرگونه تغییر سخت افزاری را اعمال کرد. در صورتی که این امر در خانواده NT به راحتی امکان پذیر نیست، فقط کاربرانی که عضو گروه Administrators باشند اختیار کامل در انجام عملیات فوق را دارا هستند.

نکته : کاربرانی که هنگام نصب ویندوز اکس پی تعریف می‌شوند همگی عضو گروه Administrators بوده و برای کاهش قدرت آنها می‌توان گروه آنها را به Limited users تبدیل کرد. چنانچه در ویندوز اکس پی فقط یک کاربر تعریف کنیم، در آن صورت رایانه پس از Boot شدن خود به خود وارد سیستم می‌شود بدون آنکه گذر واژه‌ای از ما خواسته شود، در این حالت سیستم عامل ویندوز اکس پی به طور خودکار همان یک کاربر را Auto Login می‌کند و این به معنای نقض امنیت در ورود به سیستم نیست، می‌توان این ویژگی را غیرفعال کرد. ضمناً این خصوصیت یعنی Auto Login در بقیه اعضای خانوادهٔ ویندوز NT نیز وجود دارد.

۱ــ Secur ty

فعالیت عملی **مربوط به ویژگی امنیت**

الف) نشان دهید که در ویندوز اکس پی کاربران تعریف شده هنگام نصب، عضو گروه Administrators هستند.

ب) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروه Users) قادر به ایجاد پرونده جدید در ریشه دیسک که با فایل ــ سیستم NTFS قالب بندی شده نیست (پوشه جدید را می‌تواند درست کند اما پرونده را خیر).

ج) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروه Users) نمی‌تواند ساعت سیستم را تغییر دهد.

د) نشان دهید که در ویندوز اکس پی، یک کاربر عادی (عضو گروهUsers) نمی‌تواند از طریق Device Manager یک سخت افزار را (مثلاً Mouse) غیر فعال (Disable) کند.

هـ) بررسی کنید که آیا برنامه‌ای یا روشی وجود دارد که بتوان به کمک آن گذر واژهٔ Administrator را پیدا کرد یا تغییر داد؟

۲ــ۱ــ۸ــ چند وظیفه‌ای[۱] : توانایی اجرای هم‌زمان چندین برنامه با هم است. این ویژگی نیازی به شرح بیشتر نداشته و امروزه در تمامی سیستم‌ها وجود دارد و یک ویژگی عادی به شمار می‌رود. سیستم عامل DOS به عنوان یک سیستم عامل قدیمی Multi task نیست اما سیستم عامل‌های خانواده ویندوز همگی چند وظیفه‌ای هستند.

۳ــ۱ــ۸ــ پشتیبانی از چندین پردازنده[۲] : می‌دانیم که هر چه تعداد پردازنده‌های موجود روی یک برد اصلی بیشتر باشد کارها سریع‌تر انجام می‌شود. امروزه بردهای چند پردازنده در دو زمینهٔ عمده کاربرد دارند :

ــ سرویس دهنده‌ها،

ــ رایانه‌هایی که عملیات سنگین گرافیکی و پویا را انجام می‌دهند (Graphic Workstations).

بنابراین در مواردی که نیاز به استفاده از بردهایی با بیش از یک CPU باشد لازم است تا سیستم عامل نیز بتواند آنها را شناسایی کرده و استفاده کند. در سیستم عامل‌های شرکت مایکروسافت، فقط سیستم عامل‌های خانواده ویندوز NT قادر به شناسایی و بهره‌برداری از چندین CPU هستند.

۱ــ Mu t Task ng

۲ــ Mu t Processo Support

پژوهش

پشتیبانی از چندین پردازنده در سیستم عامل ها با ۲ سیاست کلی متقارن و نامتقارن (SMP Symmetric Multi Processing, AMP Asymmetric Multi Processing)، انجام می‌شود، هر یک را به اختصار بررسی کرده و بگویید که مایکروسافت در سیستم‌های خود از کدام روش استفاده می کند؟

۴ــ۱ــ۸ــ تحمل خطا[1] : عدم تأخیر در ارایه سرویس و قدرت تحمل در هنگام بروز مشکل و خطاهای عمدتاً سخت‌افزاری است به عبارت دیگر تحمل خطا (به‌اختصار FT) قابلیتی است در سیستم عامل که می‌تواند هنگام بروز مشکلات از تجهیزات جایگزین استفاده کرده و بدون تأخیر (یا با تأخیر بسیار کوتاه) به طور خودکار به سرویس دهی ادامه دهد. نکته اصلی در FT این است که هنگام بروز خطا اولاً زمان قطع شدن سرویس بسیار کوتاه بوده، ثانیاً عملیات جایگزینی بدون عوامل انسانی و به‌طور خودکار صورت می گیرد. مسئول سیستم در فرصت مناسب می‌تواند اشکال‌ها را بررسی و رفع کند.

مثال ۱ : فرض کنید که یک سرویس‌دهنده 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. برای اینکه سرویس همواره پایدار بماند باید :

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

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت FT در زمینه دیسک باشد.

در شرایط عادی سیستم عامل هر اطلاعاتی را که روی دیسک اول می‌نویسد عیناً روی دیسک دوم نیز کپی می کند (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.

یادآوری : این کار در تکنیک RAID1 انجام می‌شود که در درس سخت افزار بررسی شده است.

از میان محصولات مایکروسافت، سیستم عامل‌های ویندوز NT که در گروه سرویس‌دهنده قرار

۱ــ Fau t To erance

دارند همگی قابلیت Disk Fault Tolerance را دارا هستند.

مثال ۲ : یک سرویس‌دهنده داریم (از هر نوع دلخواه) که با یک کارت شبکه (NIC) به شبکه متصل شده و رایانه‌ها 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 دو عدد NIC روی سیستم نصب کنید.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت تحمل خطا در این زمینه باشد. سیستم عامل در شرایط عادی اطلاعات را تقسیم کرده و از هر دو 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 ادامهٔ کار استفاده می‌کند. مثال فوق در اصطلاحات رایانه‌ای NIC Fault Tolerance[1] خوانده می‌شود و از میان محصولات مایکروسافت، سیستم عامل‌های خانواده ویندوز NT اعم از سرویس گیرنده یا سرویس‌دهنده در صورتی که کمپانی سازندهٔ کارت شبکه درایور مناسب را برای محصول خود ارایه داده باشد می‌توانند از این خاصیت بهره ببرند.

مثال ۳ : فرض کنید که یک سرویس‌دهنده داریم (از هر نوع دلخواه) و این سرویس‌دهنده ممکن است هر یک از موارد قبلی تحمل خطا را اعم از Disk یا NIC داشته باشد یا خیر. اگر به هر دلیل سرویس‌دهنده به طور کامل از کار بیافتد چه می‌شود؟ بدیهی است که سرویس قطع می‌شود، چه کار کنیم اختلالی در سرویس‌دهی بروز نکند؟

الف) شرایط سخت‌افزاری لازم را مهیا کنید یعنی از ابتدا دو یا چند سرویس‌دهنده را با تجهیزات ویژه به یکدیگر متصل کنید. به این مجموعه از سرویس‌دهنده‌ها اصطلاحاً یک «خوشه سرور» یا Server Cluster گفته می‌شود.

ب) سیستم عاملی را انتخاب کنید که دارای قابلیت تحمل خطا در زمینهٔ Clustering باشد. کلیهٔ سیستم‌ها در شرایط عادی اطلاعات مورد نیاز را به یکدیگر تبادل کرده (Synchronize) و چنانچه یکی از اعضای Cluster (یعنی یکی از سرویس‌دهنده‌ها) از کار بیافتد بقیه می‌توانند به سرعت و بدون تأخیر کار او را جبران کنند. از میان محصولات مایکروسافت فقط چند سیستم عامل از مجموعهٔ NT در خانوادهٔ سرویس‌دهنده‌ها دارای قابلیت Cluster هستند به عنوان مثال Server 2000 فاقد آن بوده اما Advanced Server 2000 , Data center Server 2000 دارای قابلیت Cluster هستند.

۱ــ در برخی از متون به آن Port Trunk یا Port Aggregat on یا L nk Aggregat on می‌گویند.

۵ــ۱ــ۸ــ نرم افزار تهیه نسخه پشتیبان : امروزه اهمیت تهیهٔ پشتیبان برای یک کاربر با تجربه پوشیده نیست، اگر در لحظه‌ای متوجه شود که به هر دلیل اطلاعات اصلی‌اش مخدوش یا غیرقابل دسترس شده‌است در این حالت با نسخه پشتیبان می‌تواند اطلاعات را دوباره بازگرداند.

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

الف) اطلاعاتی که کاربر به صورت مستقیم از اهمیت آن آگاهی دارد، مانند انواع پرونده‌ها یا حتی برنامه‌های کاربردی که تهیه و نصب کرده است (User Data).

ب) اطلاعاتی که کاربر به طور مستقیم با آن سروکار ندارد بلکه برای سیستم عامل مهم است (System Data).

اغلب کاربران پس از مدت کوتاهی با نحوهٔ تهیه پشتیبان از اطلاعات خودشان آشنا می‌شوند اما کمتر کاربر عادی پیدا می‌شود که طی مدت کوتاهی بتواند به طور کامل از اطلاعات سیستمی نیز پشتیبان گرفته یا بازیابی[۱] 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 اطلاعات سیستمی بدون مهارت لازم پشتیبان گرفت؟

یک راه حل مناسب آن است که سیستم عامل ابزارهای قوی و در عین حال کاربر پسند[۲] در اختیار کاربر بگذارد تا او بتواند اولاً به راحتی اطلاعات را دسته‌بندی کند ثانیاً بدون داشتن تخصص زیاد قادر به تهیه پشتیبان از اطلاعات سیستمی باشد. خوشبختانه ابزارهای تهیهٔ پشتیبان در سیستم عامل‌های ویندوز NT 5 .x دارای چنین توانایی‌هایی بوده و کاربر می‌تواند در صورت داشتن مجوز، تنها به علامت‌گذاری در قسمت «System State» به تهیه پشتیبان از System Data اقدام کند.

تفاوت بین ابزارهای خاص تهیه پشتیبان (مانند NTBackup در ویندوزNT 5.x) با ابزارهای عمومی مدیریت پرونده‌ها که عملیاتی مانند کپی را انجام می‌دهند در این است که قابلیت‌هایی در این ابزارها وجود دارد که در برنامه‌های عمومی (مانند My Computer) نیست. مهمترین این قابلیت‌ها عبارتند از :

الف) به کمک ابزارهایی مانند NTBackup به راحتی از اطلاعات سیستمی نسخهٔ پشتیبان تهیه می‌شود.

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

۱ــ Restore ۲ــ User Fr end y

ج) سیاست‌های تهیه پشتیبان (Backup Policy) در ابزارهای خاص تنوع بیشتری دارد، بدان معنی که می‌توان برای تهیه پشتیبان با معیارهایی همچون «فقط پرونده‌های تغییر یافته» و ... اقدام کرد که درابزارهای معمولی تنوع این معیارها کمتر است.

د) با ابزارهای خاص می‌توان انجام عملیات را به طور خودکار در موعد دلخواه زمانبندی کرد (Scheduling).

هـ) ابزارهای خاص می‌توانند از مجوزهای امنیتی (لیست دسترسی افراد به پرونده‌ها[1] که به‌اختصار ACL خوانده می‌شود نیز پشتیبان گرفته و بازیابی کنند. منظور از ACL لیستی است در فایل سیستم‌هایی مانند NTFS که تعیین می‌کند چه افرادی چه عملیاتی را با یک پرونده یا پوشه می‌توانند انجام دهند. بدیهی است که ACL در FAT یا FAT 32 وجود ندارد چرا که FAT امنیت ندارد.

فرایند پشتیبان گیری برای خود جزو مباحث مهم بوده و معمولاً در درس سیستم عامل پیشرفته مورد بحث قرار می‌گیرد با این‌حال برای تثبیت نکات یاد شدهٔ فوق، اکیداً توصیه می‌کنیم که انجام این کار باید به کمک هنرآموز درس انجام شود.

الف) نشان دهید که با NTBackup می‌توان به راحتی از اطلاعات سیستم پشتیبان تهیه کرد.

ب) دقیقاً با کدام کاربر وارد سیستم شده‌اید؟ پس از پاسخ به این سؤال، برنامهٔ My Computer را اجرا کرده سپس پارتیشنی را که سیستم عامل روی آن نصب شده باز کرده (مثلاً دیسک C :) وارد پوشه Documents and Settings شوید. قاعدتاً باید یک پوشه همنام با کاربری را که با آن وارد سیستم شده‌اید ببینید. حال سعی کنید که (با استفاده از برنامهٔ My Computer) از این پوشه کپی بگیرید. آیا امکان‌پذیر است؟ قطعاً خیر! چرا که یکی از پرونده‌های موجود در این پوشه (که البته مخفی نیز هست) به نام NTUser.dat در حال استفاده بوده (اصطلاحاً باز است) و برنامهٔ My Computer نمی‌تواند از آن کپی تهیه کند. حال با استفاده از برنامهٔ NTBackup از همین پوشه کپی بگیرید. نتیجه چیست؟ بلی، امکان‌پذیر است. بنابراین نشان دادید که NTBackup قدرت بیشتری نسبت به My Computer در تهیهٔ پشتیبان از پرونده‌ها و پوشه‌ها دارد.

۶ــ۱ــ۸ــ ابزارهای مدیریتی ساده، قدرتمند و یکپارچه[2] : هر سیستم عاملی هر چقدر هم که قوی باشد اما اگر پیکربندی، تنظیمات و به طور کلی مدیریت آن پیچیده باشد با عدم استقبال عامه مواجه می‌شود و این دقیقاً یکی از دلایلی است که سیستم عامل UNIX به ویژه نسخه‌های قدیمی‌تر فقط در بین متخصصین محبوبیت پیدا کرد.

۱ــ Access Contro L st

۲ــ S mp e and Un f ed Adrond Too s

فعالیت عملی

آشنایی با یکی از ابزارهای مدیریتی قوی در ویندوز NT 5.x

یکی از برنامه‌های قدرتمند برای مدیریت بخش‌های مختلف، برنامه‌ای است به نام Computer Management. برای اجرای این برنامه راه‌های متفاوتی وجود دارد دراینجا دو راه را بیان می‌کنیم.

الف) روی نشانه My Computer در میزکار کلیک راست کرده، گزینهٔ Manage را انتخاب کنید.

ب) از طریق Run تایپ کنید : Compmgmt.msc

پس از اجرای برنامه، بررسی کنید که به وسیلهٔ آن چه کارهایی را می‌توان انجام داد.

۷ــ۱ــ۸ــ قابلیت اطمینان و پایداری[۱] : با یک مثال مفهوم این ویژگی برای ما تثبیت می‌شود، تجربه شده است که سیستم عامل ویندوز 98 برخلاف سیستم عامل UNIX و LINUX پس از نصب چندین برنامهٔ مختلف به هم می‌ریزد حال به‌نظر شما چنین سیستمی مناسب شبکه و مخصوصاً سرویس دهنده است؟!

سیستم عامل‌های ویندوز NT و مخصوصاً NT 5.x در وضعیت بسیار بهتری نسبت به خانوادهٔ ویندوز 9x قرار دارند و بدین لحاظ برای کاربرد در شبکه‌ها اعم از سرویس گیرنده یا سرویس دهنده مناسب‌ترند.

۸ــ۱ــ۸ــ پشتیبانی[۲] : هر سیستم عاملی اعم از قوی یا ضعیف نیاز به رشد و رفع مشکلات و نواقص دارد و این با پشتیبانی از طرف تهیه کنندگان آن یا تیم‌های جنبی میسر می‌شود. در زمینهٔ محصولات مایکروسافت با وجود نقص‌های بسیار به ویژه در زمینهٔ امنیتی، پشتیبانی آن قوی بوده و اکثراً تجربهٔ به هنگام سازی سیستم عامل‌های ویندوز NT 5 .x را از طریق برنامه Automatic Update داشته‌ایم.

۲ــ۸ــ انواع سیستم عامل‌های شبکه

شرکت مایکروسافت به طور کلی در مورد سیستم عامل، دو دسته محصول ارایه کرده است :

- سیستم عامل‌هایی برای نصب و کاربرد در سرویس گیرنده.

۱ــ Re ab e and Stab e

۲ــ Support

■ سیستم عامل‌هایی برای نصب و کاربرد در سرویس دهنده.

در متن زیر طبقه‌بندی این سیستم عامل‌ها نشان داده شده است :

1– 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)

NT 6.0 Windows Vista

NT 6.1 Windows 7

2 – 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)

NT 6.D: Window 2008 server

NT 6.1 Windows 2008 server (R2)

همان‌طور که مشاهده می کنید ویندوز 2000 به نام ویندوز NT5.0، XP به نام NT 5.1 و 2003 به نام NT 5 .2 نیز خوانده می‌شوند. در کل به هر سه سیستم عامل، خانواده ویندوز NT 5.x گفته می‌شود. ویندوز اکس پی فقط در گروه سرویس گیرنده و ویندوز 2003 فقط در گروه سرویس دهنده قرار گرفته است. به عبارت دیگر ویندوز اکس پی نسخه سرویس‌دهنده نداشته و ویندوز 2003 نیز نسخه

سرویس‌گیرنده ندارد.

هر چند خانواده ویندوز 9x و XP جایی در گروه سرویس دهنده‌ها ندارند اما خیلی از کاربران تجربه به اشتراک گذاری پوشه‌ها و چاپگرهای خود را در آنها داشته‌اند، یعنی رایانه‌ای که مثلاً سیستم عامل آن ویندوز 98 است تبدیل به فایل سرور یا سرویس دهنده چاپ می‌شود. این موضوع نقض کنندهٔ طبقه‌بندی فوق نیست، به عبارتی هر چند ویندوز اکس پی هم می‌تواند در مواردی تبدیل به سرویس دهنده شود اما قرار نگرفتن آن در گروه سرویس‌دهنده‌ها به معنی آن است که این سیستم عامل عمدتاً برای کاربرد در ایستگاه‌ها طراحی شده است.

مایکروسافت فقط خانواده ویندوز NT را برای کاربرد در سرویس دهنده‌ها پیشنهاد داده است.

نام برخی از محصولات شرکت‌های دیگر در زمینه سیستم عامل‌ها (که عمدتاً برای کار در سرویس دهنده‌ها استفاده می‌شوند) عبارتند از :

- UNIX (SCO , Solaris, BSD, Free BSD, AIX,HP, Linux, . . .)
- Novell Netware
- IBM OS/2, IBM LAN Server
- Apple Macinatosh (Used inGraphic Stations)

خانواده UNIX تقریباً در همه زمینه‌ها کاربرد دارد. امروزه در ایران شبکه‌های بانکی، شرکت نفت، شهرداری، بیمه و ... همگی از این خانواده به عنوان سیستم عامل اصلی در سرویس‌دهنده‌ها بهره می‌برند.

فعالیت کارگاهی

۳ـ۸ـ ویندوز ۲۰۰۸ سرور

ویندوز ۲۰۰۸ سرور از جدیدترین نسخه‌های سیستم عامل سروری برای شبکه، توسط شرکت مایکروسافت به بازار عرضه شده است. ویندوز ۲۰۰۸ سرور با نام کد شده Longhorn نوشته شده است و محیطی شبیه ویندوز ویستا یا ویندوز ۷ دارد و در دو گروه ۳۲ و ۶۴ بیتی ارائه می‌شود که معماری[۱] x86 آن از نوع ۳۲ بیتی می‌باشد و معماری x64

۱ـ Arch tecture

برای ۶۴ بیتی مورد استفاده قرار می‌گیرد و دارای ویرایش‌های زیر است :

۱ــ ویرایش وب (Web Edition) : ساده ترین ویرایش Windows Server 2008 بوده و برای ایجاد یک سرویس دهنده وب مورد استفاده که سرویس IIS نسخه ۷ را برای رایانه سرویس دهنده فراهم می‌کند. این نسخه حداکثر از چهار پردازنده و چهار گیگا بایت RAM برای ۳۲ بیتی و ۳۲ گیگا بایت RAM برای ۶۴ بیتی پشتیبانی می‌کند.

۲ــ ویرایش استاندارد (Standard Edition) : برای شرکت‌های کوچک تا متوسط طراحی شده است که ۱۰۰ تا ۵۰۰ رایانه را در شبکه می‌تواند پشتیبانی نماید و برای به اشتراک گذاشتن فایل و چاپگر مورد استفاده قرار می‌گیرد، همچنین از ۴ پردازنده پشتیبانی می‌کند.

۳ــ ویرایش مرکز داده (Datacenter Edition) : بالاترین نسخه ویندوز ۲۰۰۸ سرور می‌باشد برای برنامه‌های خیلی پیچیده با محاسبات خیلی زیاد مورد استفاده قرار می‌گیرد و تا ۶۴ پردازنده و ۵۱۲ گیگا بایت RAM را پشتیبانی می‌کند. ضمناً می‌توانید کلاسترهایی با ۸ رایانه را در آن ایجاد نمایید (کلاستر یعنی چنانچه یکی از رایانه‌ها خراب شد، رایانه دیگری به طور خودکار ادامه کار سرویس دهی در شبکه را انجام دهد). از مجازی سازی[۱] نیز پشتیبانی می‌کند یعنی می‌توان چند سیستم عامل را روی رایانه سرویس‌دهنده نصب کرده و به طور همزمان از آنها استفاده نمود (مجازی سازی از امکانات جدید ویندوز ۲۰۰۸ سرور می‌باشد)

۴ــ ویرایش مؤسسات (Enterprise Edition) : مدلی بین ویرایش استاندارد و مرکز داده می‌باشد که برای شرکت‌هایی که بین ۵۰۰ تا ۲۰۰۰ کاربر دارند مورد استفاده قرار می‌گیرد. این نسخه تا ۸ پردازنده و تا ۶۴ گیگابایت RAM را پشتیبانی می‌کند. در اینجا نیز می توان کلاسترهایی با ۸ رایانه در آن ایجاد نمود و از مجازی سازی نیز پشتیبانی می‌کند.

۵ــ ویرایش ذخیره سازی (Windows Storage Server 2008) : از ویرایش‌های جدید ویندوز ۲۰۰۸ سرور می‌باشد و برای کارهای به اشتراک گذاری فایل و چاپگر بهینه‌سازی شده است.

۱ــ V rtua zat on

۶ــ ویرایشی بر پایه پردازنده‌های ایتانیوم (Windows Server 2008 for Itanium Based System) : از ویرایش‌های جدید ویندوز ۲۰۰۸ سرور بر اساس پردازنده‌های ۶۴ بیتی ایتانیوم می‌باشد.

۱ــ۳ــ۸ــ دلایل استفاده از ویندوز ۲۰۰۸ سرور

الف) وجود ابزارهای خود تشخیص[۱] و کنترل از راه دور[۲]

ب) مدیریت کنسول سرور جدید

ج) انعطاف بیشتر در تنظیمات اختصاصی

د) پشتیبانی از مجازی سازی[۳]

ح) وجود ابزار جدید PowerShell

و) حفاظت قوی‌تر از درایوها مانند BitLocker Drive Encryption

ز) بهبود TCP/IP (اضافه شدن TCP/IPv6)

هـ) امکان نصب هسته سرور[۴] در محیط متنی به طور مستقل با ۸۶ فرمان

ط) پشتیبانی از سرور خوشه‌ای (سرور کلاستر)

ویندوز ۲۰۰۸ سرور را در دو حالت کاری می‌توان مورد استفاده قرار داد :

۱ــ Workgroup

۲ــ Domain

بعضی از نقش‌ها[۵] در هر دو حالت کاری قابل استفاده می‌باشند و بعضی از نقش‌ها(Roles) نیز فقط در Domain قابل استفاده می‌باشند.

در موقع خاموش کردن ویندوز ۲۰۰۸ سرور باید دلیلی داشت و آن دلیل را باید در کادر Comment در پنجره Shut Down مشخص نمود زیرا معمولاً سرورها به طور دائم مشغول سرویس‌دهی هستند و به ندرت خاموش یا راه اندازی مجدد می شوند.

۱ــ Se f ــ d agnost cs

۲ــ Remote Contro Too s

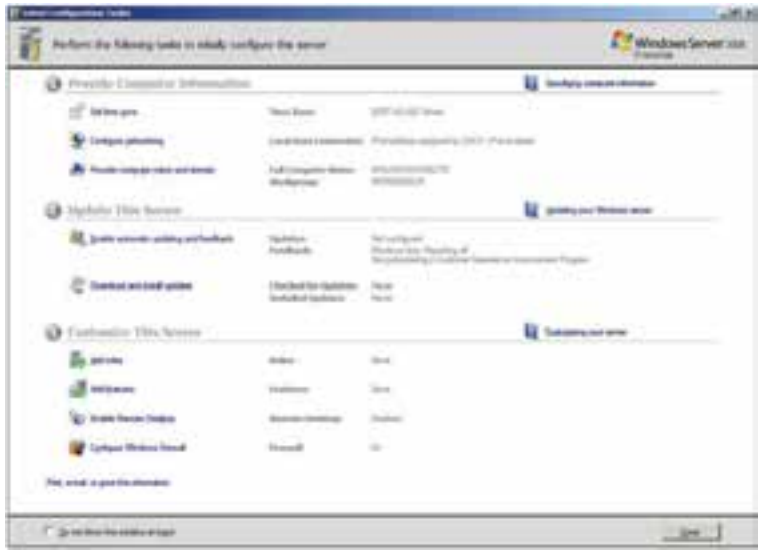
۳ــ V rtua zat on

۴ــ Se ver Core

۵ــ Ro es

شکل ۱ــ۸

بعد از اینکه اولین بار با کاربر مدیر وارد محیط ویندوز می‌شوید صفحه پیکربندی اولیه وظایف[1] ظاهر می‌شود. که در شکل ۲ــ۸ نمایش داده شده است.



شکل ۲ــ۸ــ صفحه پیکربندی اولیه ویندوز ۲۰۰۸ سرور

۱ــ In t a Conf gurat on Task Screen

در این صفحه شما می‌توانید تنظیماتی چون منطقه زمانی، اضافه کردن آدرس‌های IP و پیکربندی آنها، نامگذاری رایانه و اتصال آن به گروه کاری یا دامنه[1]، به روز رسانی ویندوز، اضافه کردن نقش‌ها[2] و اضافه کردن اجزای ویندوز[3] و غیره را انجام دهید.

بعد از نصب ویندوز ۲۰۰۸ سرور، باید آن را فعال[4] کنید. چون ویندوزی را که شما نصب کرده‌اید ۳۰ روزه می‌باشد و بعد ۳۰ روز شما فقط می‌توانید آن را فعال نمایید و امکان وارد شدن به محیط اصلی را نخواهید داشت (البته این کار با کراک کردن غیر فعال خواهد شد.)

۲ـ۳ـ۸ـ نصب سرویس‌ها در ویندوز ۲۰۰۸ سرور

برای نصب سرویس‌ها ابتدا باید برنامه Server Manager (مدیریت سرویس دهنده) را از مسیر زیر اجرا نمود

Start → Administrative Tools → Server Manager

شکل ۳ـ۸

در پنجره Server Manager در سمت چپ بر روی Roles برای کار با سرویس‌ها کلیک نمایید. سپس از منوی Action گزینه Add Role را انتخاب نمایید

۱ـ Doma n
۲ـ Ro es
۳ـ Features
۴ـ Act vate

و یا از کادر سمت راست بر روی گزینه Add Role کلیک نمایید تا بتوانید سرویس جدیدی را نصب کنید.

۳ــ۳ــ۸ــ انواع سرویس‌ها در ویندوز ۲۰۰۸ سرور

۱ــ File Services

۲ــ Active Directory Domain Services

۳ــ Print Services

۴ــ و . . .

که در فصل‌های بعدی سرویس‌های مذکور تشریح خواهد شد.

خودآزمایی و پژوهش

۱ــ ویژگی‌های مهم سیستم عامل‌های سرویس دهنده را نام ببرید.

۲ــ امنیت در سیستم عامل‌های شبکه‌ای در چه حوزه‌هایی بررسی می‌شود؟

۳ــ User Data و System Data را تعریف کنید.

۴ ــ تفاوت چند وظیفه‌ای و چند برنامه‌ای را بنویسید.

ــ پژوهش کنید که حداقل سخت افزار لازم برای نصب هر یک از سیستم عامل‌های محصول مایکروسافت چیست و آنها را با هم مقایسه کنید.

فصل نهم

سرویس‌های پرونده در ویندوز ۲۰۰۸

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- مفهوم سرویس پرونده را بیان کند.
- فناوری‌های مختلف DFS را بیان کند.
- سرویس پرونده را نصب نماید.
- درایوها، پوشه‌ها و پرونده‌ها را به اشتراک بگذارد.

۱ـ۹ـ اشتراک پرونده‌ها در ویندوز ۲۰۰۸

یکی از کارهای اصلی در ویندوز سرور در یک سازمان معمولی استفاده از سرویس پرونده می‌باشد. با استفاده از این سرویس می‌توان چندین پوشه یا درایو را به اشتراک گـذاشت تا کـاربـران شبکـه از طریق برنامه‌هـای Windows Explorer، My Network Place و Map drive به آنها دسترسی داشته باشند.

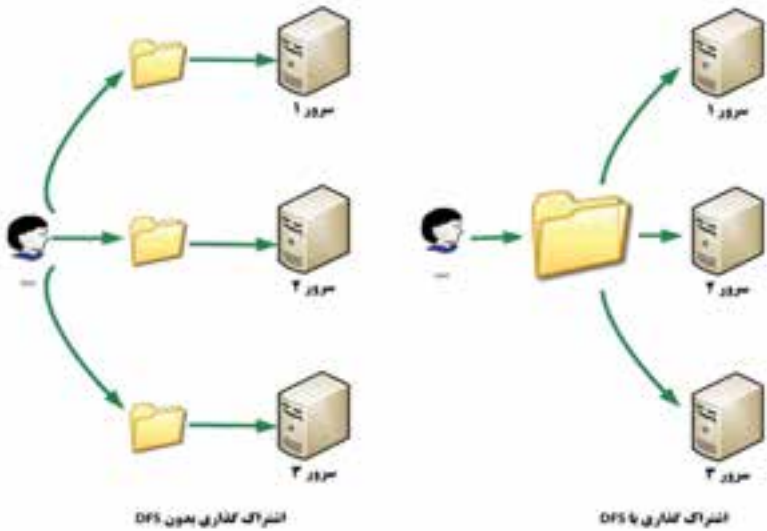
یکی از ویژگی سرویس پرونده در ویندوز ۲۰۰۸ سرور، سیستم پرونده توزیع شده DFS [۱] می‌باشد. DFS قابلیتی است که به وسیله آن می‌توان تمام منابع اشتراکی برروی شبکه را درون یک ریشه (کتابخانه‌ای از لینک‌ها) قرارداد تا کاربران شبکه بتوانند با لینک‌های موجود درون آن به محل اصلی آن منابع متصل شوند. این قابلیت برای شبکه‌های متوسط تا بزرگ طراحی شده است.

در ویندوز ۲۰۰۸ سرور DFS به دو تکنولوژی مجزا تقسیم می‌شود :

الف) فضای نامگذاری DFS Namespace : به مدیران شبکه اجازه می‌دهد تمام منابع اشتراکی موجود در شبکه که در سرورهای مختلفی قرار دارند را به صورت یک گروه جمع آوری کنند.

۱ـ D str buted F e System

ب) همسان‌سازی اطلاعات DFS Replication : می‌توان بر روی هر کدام از منابع که بر روی هر یک از سرورها قرار دارد تغییرات را انجام داد. با استفاده از همسان‌سازی اطلاعات می‌توان به جای انتقال کل پرونده فقط تغییرات را انتقال داد.



شکل ۱ــ۹ ــ قابلیت DFS

ویژگی رمزگذاری سیستم پرونده یا EFS [۱] : امکان رمز گذاری روی پوشه‌های به اشتراک گذاشته شده را فراهم می‌کند.

فعالیت کارگاهی

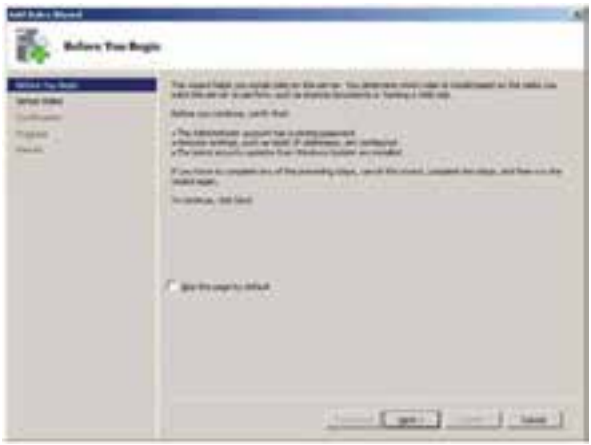
۲ــ۹ــ مراحل نصب File Server

۱ــ از مسیر زیر، برنامه Server Manager را اجرا کنید (حتماً باید با کاربر مدیر Log on شده باشید).

Start → Administrative Tools → Server Manager

۱ــ Enc ypt ng F e System

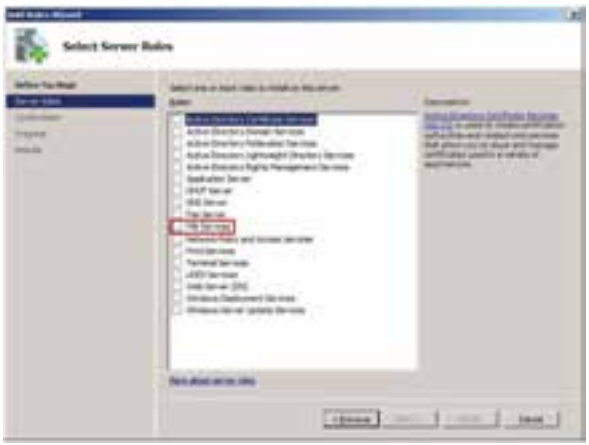
۲ــ در پنجره Server Manager ابتدا بر روی Roles در کادر سمت چپ، کلیک نموده سپس از منوی Action گزینه Add Role را انتخاب نمایید تا کادر Before You Begin برای تذکراتی قبل از نصب سرویس ظاهر شود



شکل ۲ــ۹

۳ــ در کادر Before You Begin بر روی دکمه Next کلیک نمایید تا کادر انتخاب نقش‌های سرور (Server Roles) ظاهر شود

۴ــ در کادر Select Server Role گزینه File Services را انتخاب نموده سپس بر روی Next کلیک نمایید.

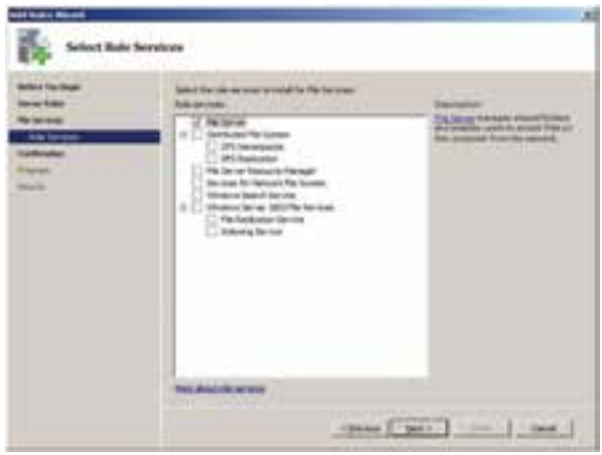


شکل ۳ــ۹

۵ــ در کادر توضیحات سرویس‌های پرونده بر روی دکمه Next کلیک کنید تا کادر انتخاب File Services ظاهر شود.

شکل ۴ــ۹

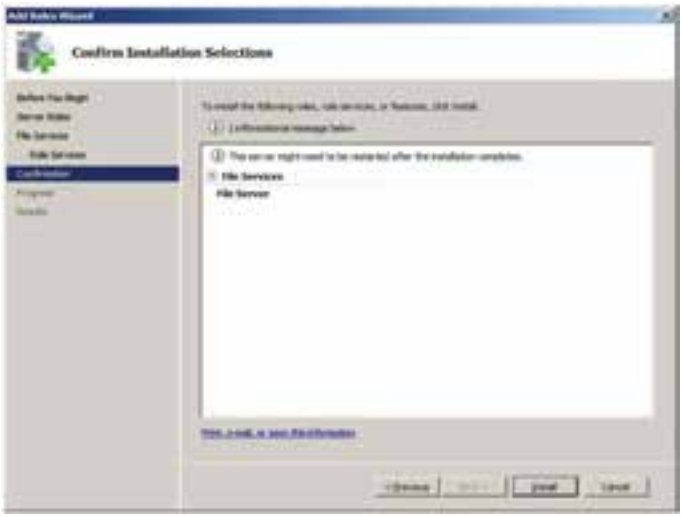
۶ــ در کادر Select Role Services گزینه File Service را انتخاب نموده و بر روی گزینه Next کلیک نمایید تا وارد پنجره تأیید نصب سرویس شوید.



شکل ۵ــ۹

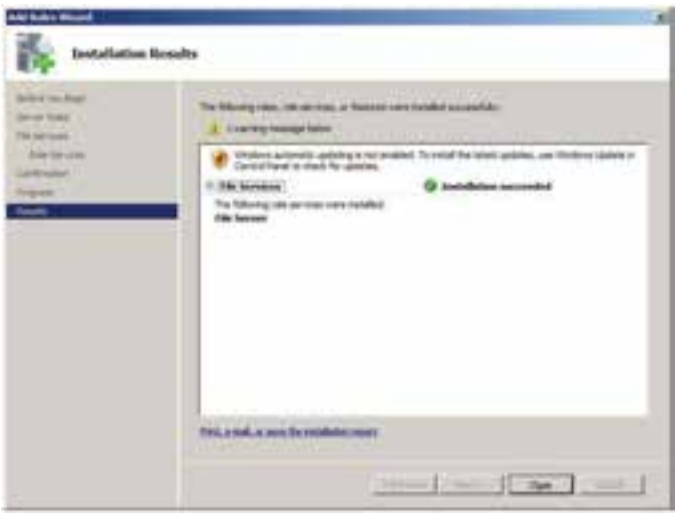
نکته: شما نمی‌توانید Index Service و Windows Search Service را روی یک ماشین اجرا کنید.

۷ــ در پنجره Confirm Installation Selection بر روی دکمه Install کلیک نموده تا سرویس پرونده به طور کامل نصب شود.



شکل ۶ــ۹

۸ ــ بعد از نصب ، پنجره نتایج نصب(Installation Results) ظاهر می‌شود.



شکل ۷ــ۹

۹ــ برای اتمام عملیات نصب بر روی دکمه Close کلیک نمایید.

همان‌طور که ملاحظه کردید File Service نیازی به نصب سرویس دیگری نداشته یا لازم نیست که حتماً رایانه شما به یک Domain Server (سرور دامنه) تبدیل شود.

بعد از اتمام نصب سرویس پرونده، در صفحه اصلی Server Manager گزینه File Service به Roles اضافه می‌شود.

برای به اشتراک گذاشتن درایوها ، پوشه‌ها و پرونده‌ها سه روش وجود دارد : که در این کتاب فقط روش اول مورد بررسی قرار می‌گیرد.

- با استفاده از ویزارد به اشتراک گذاشتن پوشه
- با استفاده از رابط گرافیکی مرورگر ویندوز
- با استفاده از خط فرمان

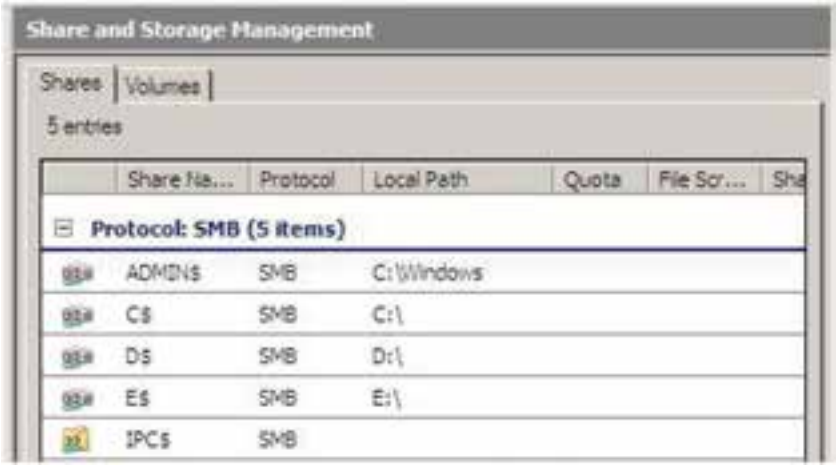
روش به اشتراک گذاشتن پوشه با استفاده از ویزارد

الف) برنامه Server Manager را باز کنید.

ب) در سمت چپ بر روی علامت جلوی Roles کلیک نموده سپس بر روی علامت جلوی File Services کلیک نمایید.

شکل ۸ــ۹

ج) بر روی گزینه Share and Storage Management کلیک نمایید تا لیست درایوها و پوشه‌های به اشتراک گذاشته شده پیش فرض نمایش داده شود.



شکل ۹ــ۹

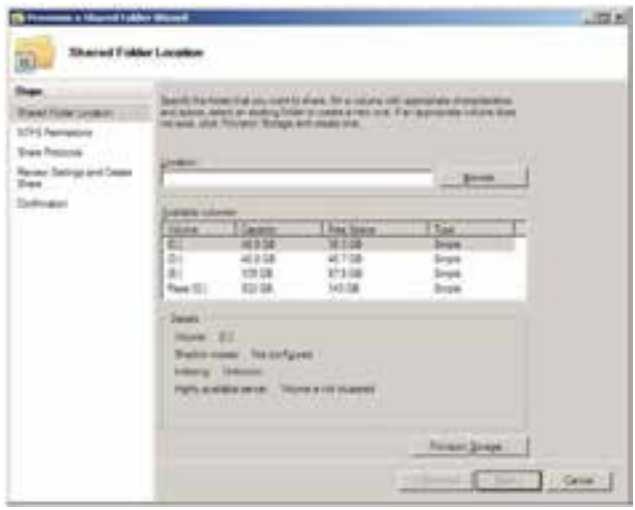
لازم به ذکر است وقتی که شما از File Services استفاده می‌کنید، ریشه تمام درایوها به صورت مخفی به اشتراک گذاشته می‌شوند[1] مانند : C$ برای درایو : C و D$ برای درایو : D.

در زبانه Volumeهم فقط لیست درایوهای به اشتراک گذاشته شده ، نمایش داده می‌شود.

شکل ۱۰ــ۹

۱ــ قرار دادن علامت $ در انتهای نام پوشه یا درایو به اشتراک گذاشته شده، آن را به صورت مخفی به اشتراک می‌گذارد.

د) بر روی گزینه Provision Share link (در بخش Action که در سمت پنجره Server manager قرار دارد) برای نمایش ویزارد به اشتراک گذاشتن کلیک کنید.

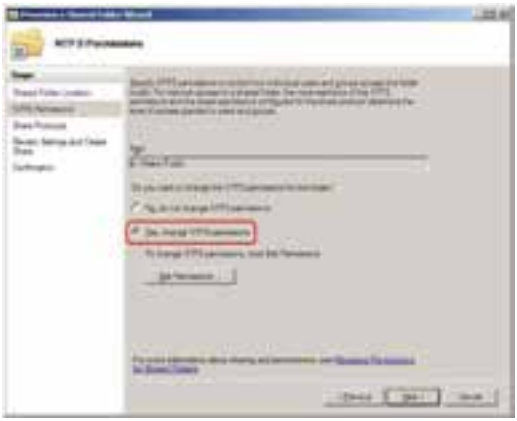


شکل ۱۱ــ۹

هـ) در صفحه Shared Folder Location با کلیک بر روی دکمه ... Browse در ساختار درختی نمایش داده شده ، پوشه مورد نظر را برای به اشتراک گذاشتن انتخاب نمایید.

شکل ۱۲ــ۹

و) پس از انتخاب پوشه مورد نظر و کلیک برروی دکمه Next صفحه انتخاب مجوز[1] NTFS نمایش داده می‌شود. (مجوزها بیانگر نوع دسترسی کاربر یا گروه یا رایانه بر روی یک شئ می‌باشد. مجوزها را می‌توان بر روی اشیای مختلفی مانند پرونده‌ها و پوشه‌های معمولی و به اشتراک گذاشته ــ چاپگرها و... نسبت داد ضمناً نوع مجوز با توجه به اشیای مختلف متفاوت خواهد بود).



شکل ۱۳ــ۹

شکل ۱۴ــ۹

در کادر NTFS Permissions دو انتخاب وجود دارد که انتخاب پیش‌فرض عدم تغییر در مجوزها می‌باشد (گزینه، do not change NTFS permission No). اما در انتخاب دوم می‌توان مجوزها را به دلخواه تغییر داد مانند شکل ۱۴ــ۹.

۱ــ Perm ss ons

مجوزهای NTFS به دو دسته مجوز ویژه و مجوز استاندارد تقسیم می‌شوند،به صورتی‌که مجوز استاندارد از تعدادی مجوز ویژه تشکیل شده است. جدول ۱ــ۹ مجوزهای استاندارد (ستون‌های جدول) و مجوزهای ویژه (ردیف‌های جدول) را نشان می‌دهد.

در کادر انتخاب مجوز، **شش نوع مجوز استاندارد** وجود دارد، انواع مجوزها در NTFS (NTFS Permissions) عبارت‌اند از :

۱ــ مجوز Read : برای نمایش محتوای پوشه و همچنین نمایش ویژگی‌های یک پوشه یا پرونده و همچنین برای نمایش مجوزها و مالک مورد استفاده قرارمی‌گیرد.

۲ــ مجوز Write : به کاربر اجازه می‌دهد داخل پوشه مورد نظر پرونده یا پوشه‌ای را ایجاد نماید.

۳ــ مجوز List Folder Contents : فقط می توان لیست پوشه ها و پرونده‌های موجود در فهرست به اشتراک گذاشته را مشاهده نمود.

۴ــ مجوز Read Execute : ضمن این که تمامی‌مجوزهایی را که Read و List Folder Contents را در اختیار قرار می‌دهد، امکان اجرای پرونده‌های موجود داخل پوشه به اشتراک گذاشته را می‌دهد.

نکته: اگر شما مجوز Read Execute را انتخاب نمایید، مجوزهای Read و List Folder Contents به‌طور خودکار انتخاب می‌شوند و اگر شما هر کدام از مجوزهای Read و List Folder Contents را حذف کنید، مجوز Read Execute به طور خودکار حذف خواهد شد.

۵ــ مجوز Modify : ضمن داشتن مجوزهای ۱ تا ۴ ، مجوز حذف کردن(Delete) پرونده و پوشه را در اختیار کاربر قرار می‌دهد. همچنین می توان ویژگی‌های پوشه یا پرونده را تغییر داد.(Write Attributes)

نکته: اگر شما هر کدام از مجوزهای ۱ تا ۴ را حذف کنید، مجوز Modify نیز حذف خواهد شد.

۶ــ مجوز Full Control : علاوه بر داشتن مجوز Modify ، مجوز تغییر مجوز[۱] را دارد و همچنین می‌تواند مالک[۲] پوشه یا پرونده را تغییر دهد. همچنین کاربر می‌تواند زیر پوشه‌ها و پرونده‌های داخل پوشه را نیز حذف نماید.

Full Control Modify Delete subfolder and files Change Permissions Take Ownership

مجوزهای Change Permissions، Delete subfolder and files، Take Ownership، Delete و Write Attributes جزء مجوزهای ویژه می‌باشند. مجوزها در دو ستون Allow (اعطای مجوز) و Deny (برداشتن مجوز) لیست شده‌اند.

برای دسترسی به لیست **مجوزهای ویژه** ابتدا بر روی دکمه Advanced در کادر Permissions کلیک نموده تا وارد صفحه Advanced Security Settings شوید سپس بر روی دکمه Edit در زبانه Permissions کلیک نمایید تا لیست کامل مجوزها نمایش داده شود.

شکل ۱۵ــ۹

۱ــ Change Perm ss ons ۲ــ Ownersh p

جدول ۱ــ۹ــ لیست کامل مجوزها بر روی پرونده و پوشه در NTFS

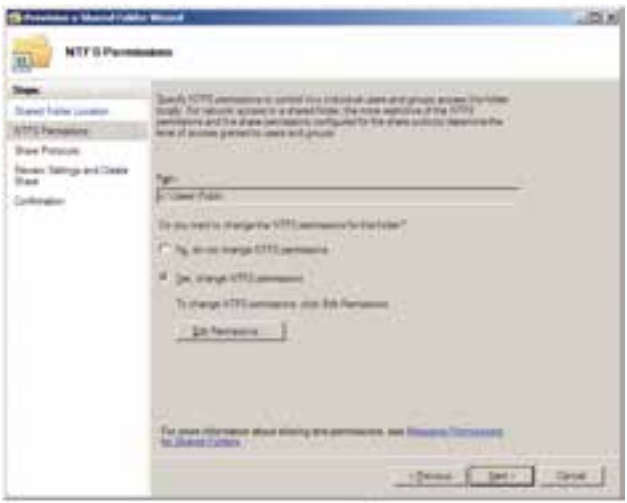
Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	×	×	×	×		
List Folder/Read Data	×	×	×	×	×	
Read Attributes	×	×	×	×	×	
Read Extended Attributes	×	×	×	×	×	
Create Files/Write Data	×	×				×
Create Folders/Append Data	×	×				×
Write Attributes	×	×				×
Write Extended Attributes	×	×				×
Delete Subfolders and Files	×					
Delete	×	×				
Read Permissions	×	×	×	×	×	×
Change Permissions	×					
Take Ownership	×					
Synchronize	×	×	×	×	×	×

پژوهش

در جدول ۱ــ۹ درباره مجوزهایی که در کتاب توضیح داده نشده است تحقیق کنید.

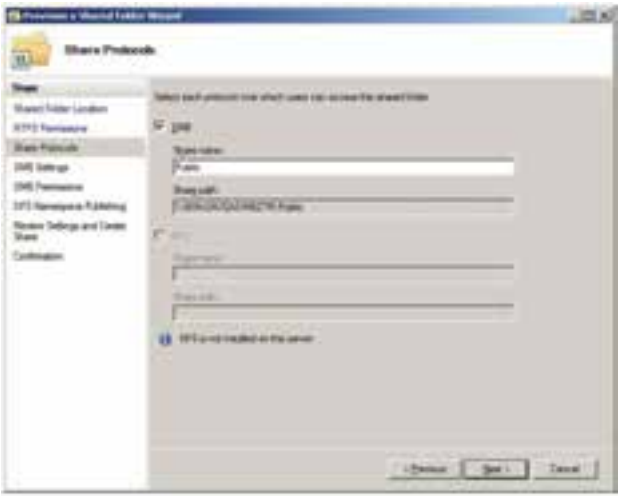
نکته ۱: امکان انتخاب همزمان دو ستون Deny و Allow وجود ندارد.

نکته ۲: اگر کاربری همزمان عضو دو گروه باشد به طوری که یک گروه بر روی پوشه مورد نظر مجوز خاصی داشته باشد(Allow) و گروه دیگر بر روی همان پوشه Deny شده باشد ، Deny بر Allow اولویت دارد.



شکل ۱۶ــ۹

ز) بعد از تعیین مجوز در پنجره NTFS Permissions بر روی دکمه Next کلیک نمایید. تا وارد صفحه تعیین پروتکل اشتراک گذاری شوید.



شکل ۱۷ــ۹

پروتکل SMB[1] پروتکلی است که توسط IBM برای به اشتراک‌گذاری پرونده و پوشه و چاپگر و.... ایجاد شده است.

ح) با کلیک بر روی دکمه Next در پنجره Share Protocols وارد پنجره تنظیمات SMB خواهید شد به‌طوری که در این پنجره می‌توانید درج توضیحات دلخواهی را برای مسیر به اشتراک گذاشته شده بنویسید همچنین با کلیک کردن بر روی دکمه Advanced می‌توانید تنظیمات موردنظر را انجام دهید.

شکل ۱۸ــ۹

ط) با کلیک بر روی دکمه Next در کادر SMB Settings پنجره مجوزهای SMB ظاهر می‌گردد.

شکل ۱۹ــ۹

۱ــ Server Message B ock

شکل ۲۰ــ۹

اگر بر روی دکمه Permission کلیک نمایید کادر انتخاب مجوز پوشه به اشتراک گذاشته ظاهر می‌گردد.

با توجه به شکل ۱۹ــ۹، برای پوشه‌های به اشتراک گذاشته شده، سه مجوز وجود دارد، مجوزهای پوشه به اشتراک گذاشته شده :

۱ــ Read

۲ــ Change

۳ــ Full Control

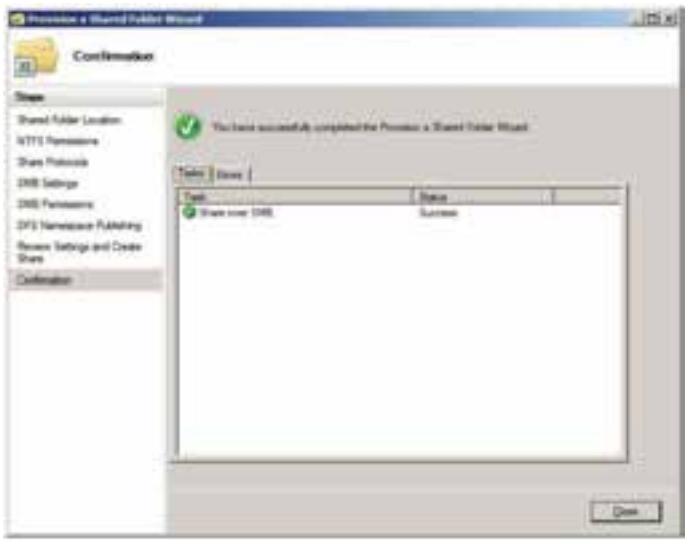
ی) در پنجره DFS Namespace publishing بر روی Next کلیک نمایید، تا وارد پنجره پیش نمایش تنظیمات انجام شده، شوید.

شکل ۲۱ــ۹

ک) در پنجره پیش نمایش تنظیمات بر روی دکمه Create کلیک نمایید.

شکل ۲۲ــ۹

ل) در آخرین مرحله پنجره تأیید عملیات ظاهر می‌گردد.



شکل ۲۳ــ۹

نکته: پوشه به اشتراک گذاشته شده دارای علامت  می‌باشد (مانند نماد به اشتراک گذاشته در Windows XP نمی‌باشد.)

خودآزمایی و پژوهش

۱ــ دو تکنولوژی مختلف در قابلیت DFS ویندوز سرور ۲۰۰۸ کدام است؟

۲ــ برای به اشتراک گذاشتن درایوها ، پوشه‌ها و پرونده‌ها چند روش وجود دارد؟ توضیح دهید.

۳ــ انواع مجوزها در NTFS چیست؟

۴ــ تفاوت انواع مجوزها در NTFS و FAT۳۲ را در قالب یک تحقیق به کلاس ارائه دهید.

۵ــ مجوزهای ویژه در NTFS کدامند و چگونه می‌توان به آن‌ها دست یافت؟

۶ــ مجوز پوشه‌های به اشتراک گذاشته شده شامل چه مواردی است؟

فصل دهم

پیاده‌سازی و مدیریت چاپ در شبکه

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- اجزای چاپ در شبکه را تعریف کند.
- بر روی سرویس دهنده چاپ و سرویس گیرنده‌ها چاپگر نصب کند.
- مجوز دسترسی کاربران به چاپگرهای به اشتراک گذاشته شده را کنترل کند.
- بتواند صف کارهای چاپی را کنترل کند.
- Spool Folder را تعریف کند و بتواند آدرس آن را تغییر دهد.

فعالیت کارگاهی

۱ـ۱۰ـ آشنایی با اجزای چاپ در شبکه

یکی از امکاناتی که شبکه در اختیار ما قرار می‌دهد به اشتراک گذاشتن منابع فیزیکی است و از این طریق علاوه بر این که می‌توانید مدیریت مناسبی برانجام امور داشته باشید، با صرفه‌جویی در هزینه‌ها بهره‌وری را افزایش دهید. دراین فصل به اشتراک گذاشته شدن چاپگر به عنوان یکی ازمنابع مهم در ادارات و شرکت‌ها مورد بررسی قرار می‌گیرد. قبل از شروع لازم است با برخی از واژه‌های مختلف چاپ در شبکه آشنا شوید.

■ **Printer** : به نرم افزار و سخت افزاری که با آن می‌توان عمل چاپ را انجام داد «چاپگر» گفته می‌شود. چاپگرها به دو نوع تقسیم می‌شوند :

الف) Local Printer : به چاپگری اطلاق می‌شود که مستقیم در یک رایانه نصب می‌شود و می‌توان به صورت محلی یا اشتراکی در شبکه ازآن استفاده کرد.

ب) ***Network Printer*** : چاپگری که در شبکه به اشتراک گذاشته شده و با نصب راه‌انداز آن در رایانه خود می‌توان به عنوان یک سرویس گیرنده ازآن استفاده نمود.

■ **Print server** : به سرویس‌دهنده‌ای گفته می‌شود که یک چاپگر در آن نصب و به اشتراک گذاشته می‌شود.

■ **Print Queue** : به کارهای چاپی که در یک چاپگر منتظرچاپ شدن می‌باشد گفته می‌شود.

■ **Print job** : به سندی که برای چاپ به یک چاپگر فرستاده می‌شود،اطلاق می‌گردد.

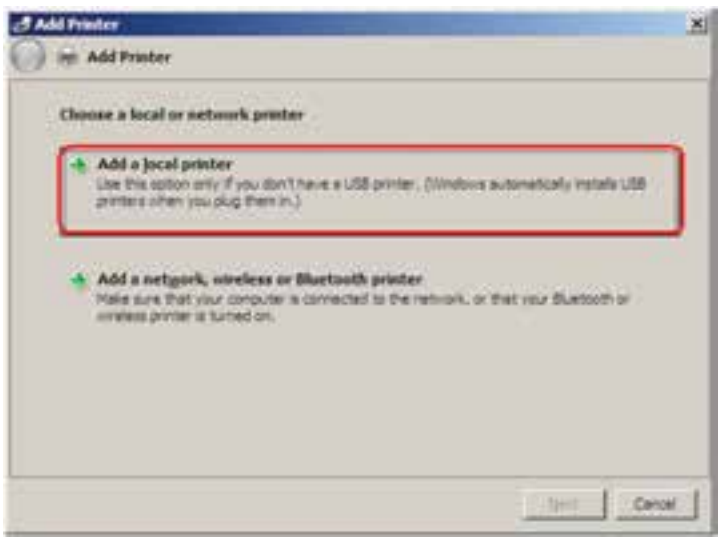
۲ـ۱۰ـ نصب چاپگرها

۱ـ۲ـ۱۰ـ نصب و به اشتراک گذاشتن چاپگر روی شبکه

۱ـ برای نصب چاپگر جدید، گزینه Add a Printer را از مسیر زیر اجرا کنید.

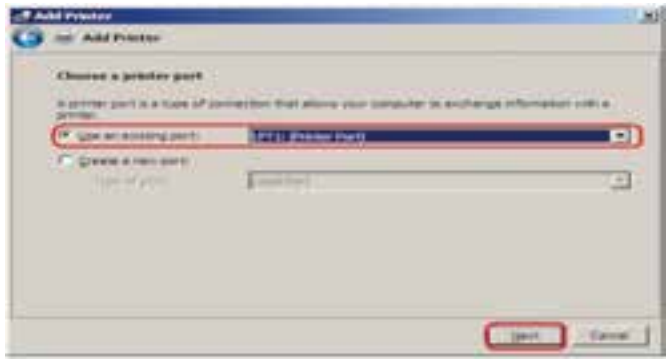
Start → Control Panel → Printers

۲ـ در کادر Add Printer بر روی گزینه Add a local printer کلیک کنید (شکل ۱ـ۱۰).



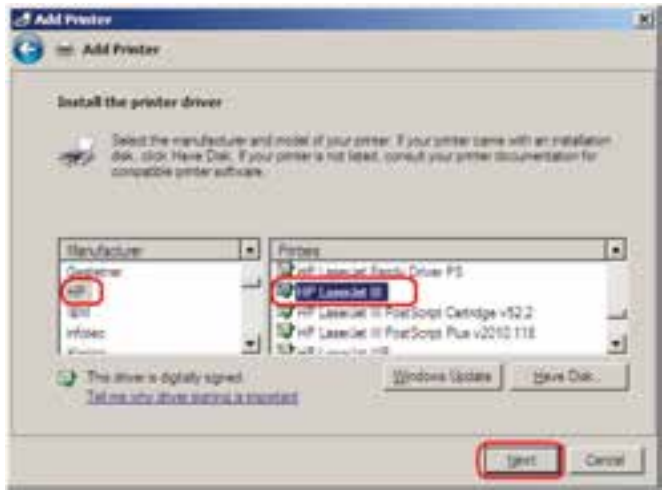
شکل ۱ـ۱۰

۳ــ درصفحه بعدی مطابق شکل ۲ــ۱۰ گزینه Use an existing port را انتخاب و از لیست مقابل آن LPTI (یا هر درگاه دیگری را که دستگاه به آن متصل است) را انتخاب کرده و روی دکمه Next کلیک کنید.



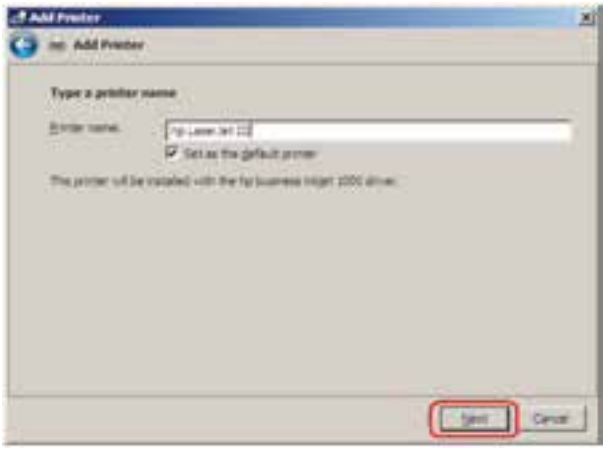
شکل ۲ــ۱۰

۴ــ درصفحه بعد (Install the printer driver) ابتدا از بخش Manufacture نام کارخانه سازنده چاپگر را انتخاب نموده و از بخش printers مدل چاپگر مورد نظر را انتخاب نمایید(مثلاً HP LaserJet III). سپس روی دکمه Next کلیک کنید. در صورتی که چاپگر مورد نظردر لیست وجود نداشت، درایور چاپگر را به کمک دکمه Have Disk معرفی کنید.



شکل ۳ــ۱۰

۵ــ در کادر Type a printer name یک اسم برای چاپگر انتخاب نموده (به‌طور پیش فرض نام انتخاب شده قبلی درج شده است) و روی گزینه Next کلیک کنید.

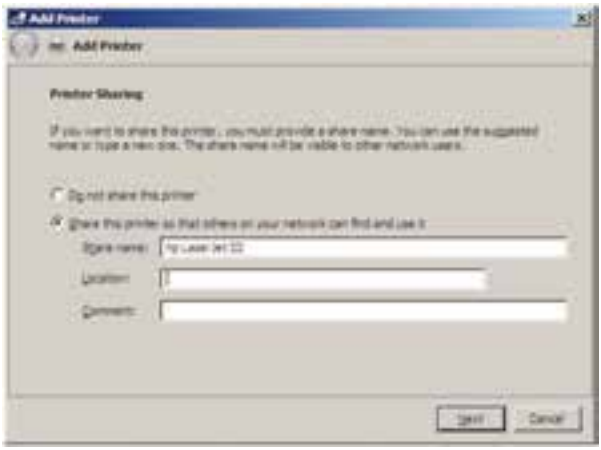


شکل ۴ــ۱۰

۶ــ در صفحه Printer Sharing مطابق شکل ۵ــ۱۰ گزینه

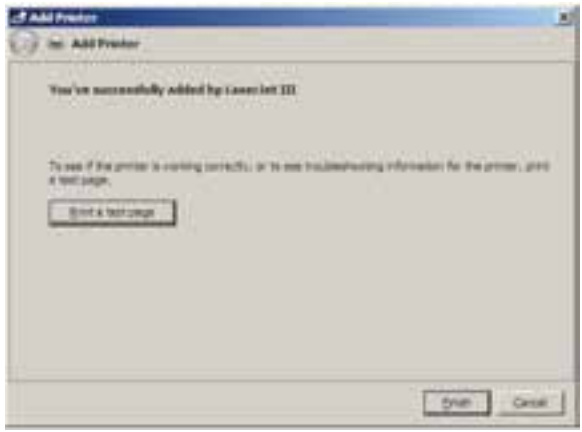
Share this printer so that others on your network can find and use it

را انتخاب نموده و نام مورد نظر را برای چاپگر به اشتراک گذاشته شده وارد نمایید. این اسم برای کاربرانی که از طریق شبکه به این رایانه متصل می‌شوند نمایش داده می‌شود. سپس روی دکمه Next کلیک کنید.



شکل ۵ــ۱۰

۷ــ در آخرین کادر ظاهر شده برای پایان عملیات نصب، بر روی دکمه Finish کلیک کنید (در صورت اتصال چاپگر می‌توانید با انتخاب دکمه Print a test page چاپگر خود را آزمایش کنید).



شکل ۶ــ۱۰

چاپگری که به اشتراک گذاشته شود و به‌عنوان چاپگر پیش فرض نیز انتخاب شده باشد، به صورت شکل ۷ــ۱۰ نمایش داده می‌شود.

شکل ۷ــ۱۰

۲ــ۲ــ۱۰ــ نصب چاپگر روی سرویس گیرنده : حال در یکی از سرویس گیرنده‌های شبکه گزینه Add a Printer را از مسیر Control Panel←Printer and Faxes را انتخاب کرده سپس گزینه نشان داده شده را مطابق شکل ۸ــ۱۰ انتخاب و گزینه Next را کلیک کنید.

شکل ۸ــ۱۰

در این صفحه مطابق شکل ۹ــ۱۰ گزینهٔ :

■ **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.

(مانند \\ ComputerName\PrinterName)

■ **Connect to a printer on the internet ...** : را به منظور استفاده از چاپگری که در اینترنت روی یک سرویس دهنده چاپ به اشتراک گذاشته شده انتخاب کنید.

شکل ۹ــ۱۰

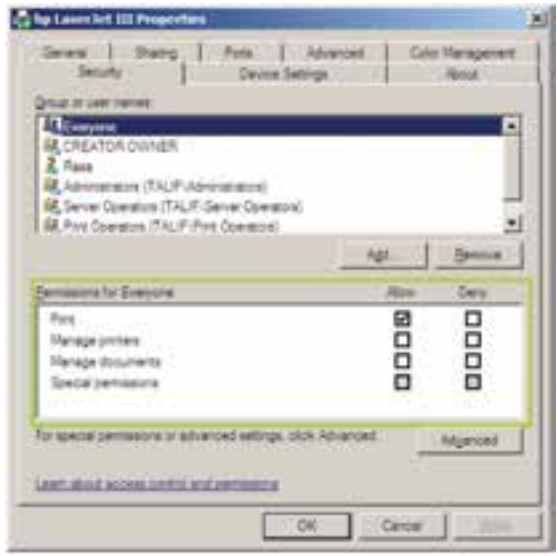
سپس ویزارد را مشابه نصب چاپگر محلی ادامه داده و دکمه Finish را در صفحه آخر انتخاب کنید تا نصب چاپگر روی سرویس گیرنده به پایان برسد.در این صورت مشاهده می‌کنید که یک چاپگر در سرویس گیرنده اضافه شده است.

بعد از اتمام نصب چاپگر روی سرویس گیرنده شکل چاپگر نصب شده به صورت شکل ۱۰ــ۱۰ می‌باشد.

شکل ۱۰ــ۱۰

۳ــ۱۰ــ مجوزهای چاپ

در ویندوز می‌توان با استفاده از سطوح دسترسی مختلف، دسترسی کاربران را به چاپگرهای به اشتراک گذاشته شده کنترل کرد (شکل ۱۱ــ۱۰).



شکل ۱۱ــ۱۰

سطوح دسترسی کاربران به چاپگرهای به اشتراک گذاشته شده عبارتند از :

■ **Print** : به کمک این مجوز کاربر می‌تواند به یک چاپگرمتصل شده و اسناد

خود را برای چاپ به آن ارسال کند.

■ **Manage Printers** : این مجوز علاوه بر این که کارایی مجوز Print را در اختیار کاربر می‌گذارد، به کاربر امکان مدیریت کامل چاپگر را نیز می‌دهد،به طوری که کاربر می‌تواند یک چاپگر متوقف یا راه اندازی کند، مجوزهای کاربران را روی چاپگر تغییر دهد و همچنین ویژگی‌های مختلف چاپگر را تغییر دهد.

■ **Manage Document** :کاربر به کمک این مجوز می‌تواند اسنادی را که کاربران دیگر به چاپگر ارسال نموده‌اند، Pause (توقف موقت)،Resume (از حالت توقف موقت خارج کردن) یا Cancel (لغو چاپ) نماید.به وسیله این مجوز کاربر نمی‌تواند اسناد خود را به چاپگر ارسال کند.

زمانی که کاربر برای دسترسی به یک چاپگر مجوز داشته باشد و همچنین عضو گروه‌هایی باشدکه آن‌ها نیز دارای مجوز باشند. مجموع مجوزها، مجوز نهایی آن کاربر خواهد بود. اما اگر مجوزی برای کاربر با 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 گروه‌های مختلف اعطا می‌شود، در جدول ۱ــ۱۰ خلاصه شده است :

جدول ۱ــ۱۰ــ مجوزهای پیش فرض

گروه‌ها	Manage Printers	Manage Documents	Print
Administartors	*	*	*
Creator Owner	–	*	–
Everyone	–	–	*
Power Users	*	*	*
Print Operators	*	*	*
Server Operators	*	*	*

۴ــ۱۰ــ نحوه اعطای مجوز به کاربران روی چاپگرها

برای اعطای مجوزکافی است که روی چاپگر مربوطه کلیک راست کرده و گزینه Properties را انتخاب نمایید و سپس در زبانه Security لیست کاربران، گروه‌ها و

همچنین مجوزهای آن‌ها را مشاهده نموده و با استفاده از دکمه‌های Add یا Remove به کاربران و گروه‌های مختلف مجوز اضافه یا حذف نمایید.

۵ـ۱۰ـ نحوه مدیریت صف کارهای چاپی

برای انجام دادن این کار می‌توانید روی چاپگر مربوطه دوبار کلیک کنید. در پنجره ظاهرشده، لیست تمام کارهای چاپی را نمایش می‌دهد. اگر روی یک کار چاپی کلیک راست نمایید، منویی ظاهر می‌شود که شامل فرمان‌های زیرخواهد بود :

■ **Pause** : به کمک این گزینه می‌توان یک کار چاپ را به صورت موقت متوقف کرد.

■ **Restart** : کار چاپی را یک بار دیگر از ابتدا به چاپگر ارسال می‌کند.

■ **Cancel** : با این فرمان می‌توانید از چاپ شدن کار چاپی جلوگیری نموده و آن را از صف کارهای چاپی حذف نمایید.

■ **Properties** : این گزینه باعث نمایش ویژگی‌های کار چاپی شده وبه شما اجازه می‌دهد که اولویت کار چاپی را نسبت به کارهای چاپی دیگر تعیین نمایید.

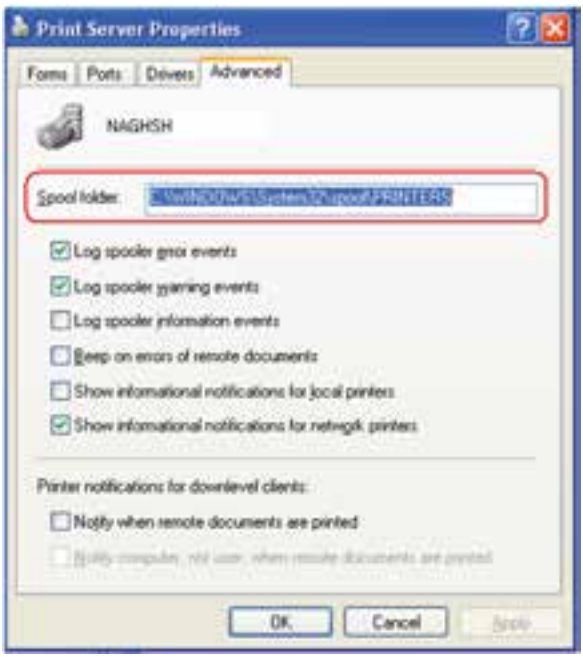
هم چنین می‌توانید تعیین کنید که به یک کاربرخاص بعد از چاپ شدن کارچاپی یک پیغام ارسال نمایید یا تعیین کنید که کار چاپی در یک بازه زمانی مشخص بتواند چاپ شود.

۶ـ۱۰ـ تغییر آدرس Spool Folder در سرویس گیرنده و سرویس‌دهنده

هنگامی که در ویندوز پرونده‌ای را چاپ می‌کنید، آن پرونده به طور مستقیم به دستگاه چاپ ارسال نمی‌شود در ابتدا آن کار چاپی به وسیلهٔ یکی ازسرویس‌های ویندوز به نام Print Spooler در داخل پرونده‌ای نوشته شده و سپس در صف قرار داده می‌شود.

به این عمل در اصطلاح Spooling می‌گویند. این عمل باعث می‌شود برنامه‌ای که کاربر در آن دستور چاپ را صادر کرده است مستقیماً درگیر کار چاپ نشود و به کار خود ادامه دهد. پرونده‌هایی که به این شیوه تولید می‌شوند در یک پوشه با نام Spool Folder قرار می‌گیرند.

اگر در یک سرویس دهنده چاپ تعداد کارهای چاپی زیاد باشد، می‌توان آدرس این پوشه را به یک درایو دیگر تغییر داد تا فضای آزاد برای Spooling افزایش یابد و بازدهی بیشتر شود. برای انجام این کار در پنجره Printers and Faxes چاپگر مورد نظر را انتخاب کرده و از منوی File گزینه Server Properties را باز کنید و زبانه Advanced را فعال کنید. سپس در قسمت Spool Folder (شکل ۱۲ــ۱۰) آدرس جدید را وارد کنید.



شکل ۱۲ــ۱۰

خودآزمایی و پژوهش

۱ــ تفاوت Printer و Print Server درچیست؟

۲ــ Spool Folder چیست؟

۳ــ بررسی کنید آیا گروه Creator owner می‌تواند از چاپگر استفاده کند؟

۴ــ بررسی کنید که چه روش دیگری برای نصب چاپگر درروی شبکه وجود دارد؟

فصل یازدهم

مدیریت کاربران و رایانه‌ها

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- انواع Accountها و ابزارهای مدیریتی را شناسایی کند.
- بتواند کاربران را مدیریت کند.
- بتواند مدیریت Computer Accountها را انجام دهد.
- انواع گروه‌های کاربران را شناسایی کند.
- به کاربران و گروه‌ها با روش‌های AGP و ADLP مجوز دهد.
- گروه‌های Build ـ in را شناسایی کند.

فعالیت کارگاهی

۱ـ۱۱ـ کاربران و گروه‌ها[1] در ویندوز ۲۰۰۸ سرور به صورت مستقل یا Stand ـ alone

بعد از نصب ویندوز، کاربران و گروه‌ها مانند ویندوزهای غیر سروری (ویندوز XP، ویندوز Vista یا ویندوز ۷) کنترل می‌شوند. برای دسترسی به بخش مدیریتی کاربران و گروه‌ها می‌توانید از مسیر زیر استفاده نمایید.

Start → Administrative Tools → Computer Management → Local Users and Groups

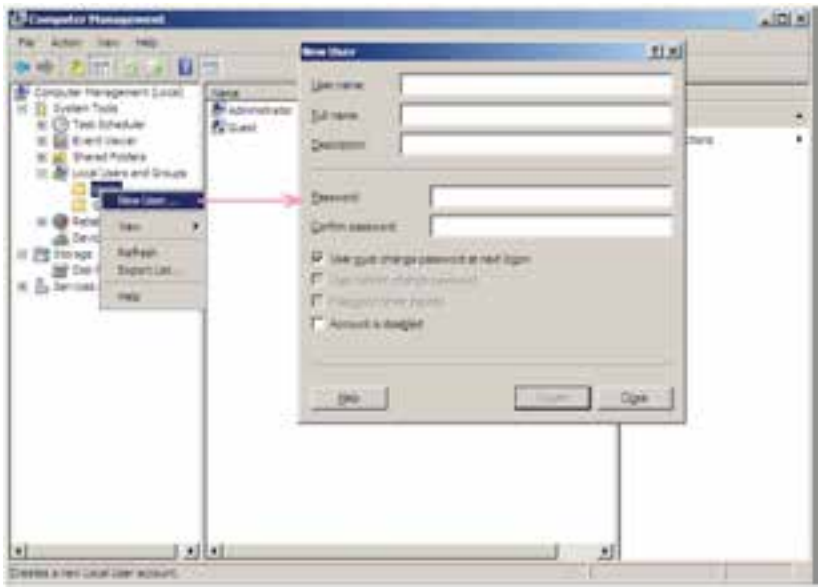
وقتی ویندوز را نصب می‌کنید کاربران Administrator(مدیر) و Guest (میزبان)به عنوان کاربران پیش فرض وجود دارند ولی کاربر میزبان غیر فعال می‌باشد (علامت فلش رو

۱ـ Users and Groups

به پایین جلوی نام کاربر به مفهوم غیرفعال بودن آن کاربر می‌باشد) (مانند شکل ۱ــ۱۱).

شکل ۱ ــ ۱۱

برای اضافه کردن یک کاربر در بخش Local Users and Groups بر روی گزینه Users کلیک راست نموده و گزینه New Users را انتخاب نمایید (شکل ۲ــ۱۱).



شکل ۲ ــ ۱۱

در شکل ۲ــ۱۱ در کادر New User موارد زیر برای تکمیل نمودن مشخصات کاربر جدید استفاده می‌شود

- **User Name** : نام کاربر برای ورود به ویندوز یا Logon شدن
- **Full Name** : نام کامل کاربر که اختیاری است ضمناً اگر نام کامل کاربر را

مشخص نکنید، User name به عنوان نام کامل کاربر در نظر گرفته می‌شود.

■ **Description** : توضیحی برای معرفی بیشتر کاربر که اختیاری است.

■ **Password** : برای تعیین گذر واژه

■ **Confirm Password** : تأیید گذر واژه وارد شده در Password

■ **User must change password at the next logon** : در صورت فعال بودن کاربر در Logon بعدی باید گذر واژه را عوض کند. اگر غیر فعال شود دو گزینه غیر فعال مشخص شده، فعال خواهد شد.

■ **User cannot change password** : درصورت فعال بودن، کاربر نمی‌تواند گذر واژه مربوط به خودش را عوض کند.

■ **Password never expire** : درصورت فعال بودن گذر واژه تاریخ انقضا نخواهد داشت.

■ **Account is disable** : برای غیرفعال کردن کاربر استفاده می‌شود (مثلاً زمانی که قرار است کاربری برای چند روز به مرخصی برود و کسی نتواند با نام کاربری آن کاربر Logon شود). همچنین کاربر مدیر سیستم می‌تواند آن را مجدداً فعال کند.

بعد از ایجاد کاربر جدید با کلیک راست بر روی نام کاربر می‌توان با استفاده از گزینه Properties به کادر ویژگی‌های کاربر دسترسی داشت (مانند شکل ۳ــ۱۱).

شکل ۳ ــ ۱۱

در کادر User Properties زبانه Member of می‌توان تعیین کرد که کاربر شما عضو کدام گروه باشد، به‌طور پیش فرض کاربر ایجاد شده عضو گروه Users می‌باشد. همچنین می‌توان کاربران را به عضویت گروه‌های مختلفی درآورد و یا گروه جدیدی ایجاد نمود و کاربران مورد نظر را به آن گروه اضافه کرد.

۲ـ۱۱ـ نحوه ایجاد گروه جدید در ویندوز ۲۰۰۸ سرور در حالت مستقل[۱]

برای اضافه کردن یک کاربر در بخش Local Users and Groups بر روی گزینه Groups کلیک راست نموده و گزینه New Group را انتخاب نمایید (شکل ۴ـ۱۱).

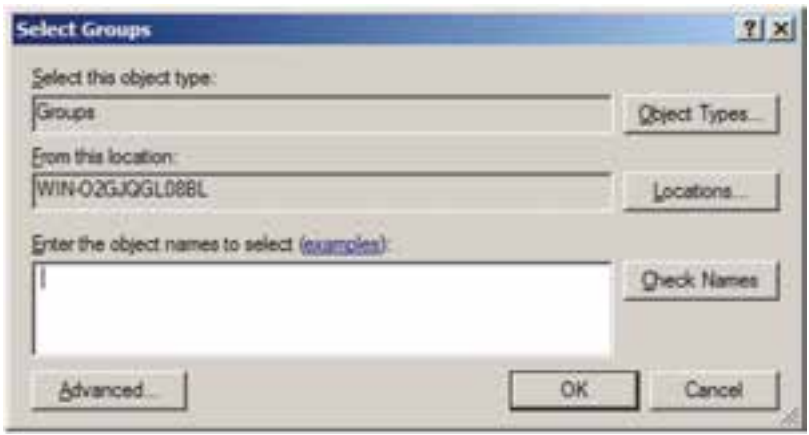
شکل ۴ ـ ۱۱

در کادر Group name : نام گروه را Marketing وارد کنید.

برای اضافه کردن کاربران به گروه در زبانه Member Of بر روی دکمه Add کلیک نموده و در پنجره Select Groups به دو روش می‌توان کاربران را به گروه اضافه نمود :

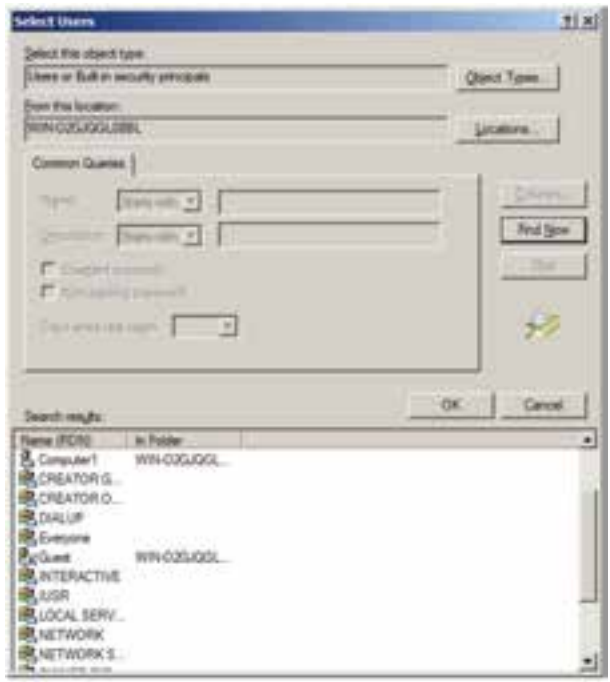
الف) وارد کردن نام کاربر در کادر Enter the Object name to select و برای اطمینان، روی Check names کلیک کنید تا مطمئن شوید که گروه وارد شده، موجود می‌باشد.

۱ ـ Stand ـ a one



شکل ۵ــ۱۱

ب) برای پیدا کردن کاربر مورد نظر ابتدا بر روی دکمه Advanced کلیک کنید سپس در کادر جدید بر روی دکمه Find کلیک کنید تا لیست گروه‌های موجود نمایش داده شود (شکل ۶ــ۱۱).



شکل ۶ــ۱۱

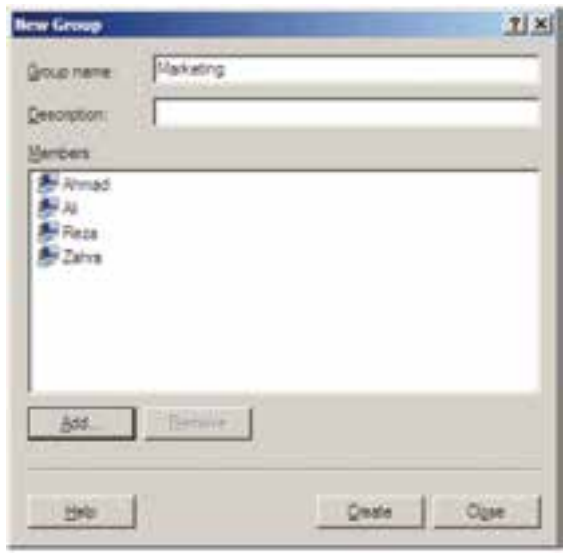
نکته ۱: با انجام اعمال مدیریتی روی گروه، تمام کاربران گروه دارای مجوز دسترسی یکسانی خواهند بود.

نکته ۲: وقتی که بعضی از سرویس‌ها را نصب می‌کنید، گروه‌هایی متناظر با نوع سرویس به سیستم اضافه می‌شود.

در فصل بعدی با نصب Active Directory وضعیت مدیریت کاربران و گروه‌ها به طور کلی تغییر خواهد کرد.

۱ــ در زمان ایجاد کاربر جدید گزینه‌های Account is disable و Password never expires به چه منظور استفاده می‌شود؟

۲ــ گروه Marketing را با کاربران نمایش داده شده در شکل ۷ــ۱۱ ایجاد نمایید.



شکل ۷ــ۱۱

۳ــ پوشه‌هایی در درایو D ایجاد کنید، سپس به گروه Marketing مجوز دسترسی کامل بدهید.

فصل دوازدهم

نصب و راه اندازی Active Directory

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- Domain و اجزای Active Directory را تعریف کند.
- Active Directory را نصب کند.
- نحوهٔ عضویت سرویس گیرنده‌ها و انواع Log on ها را شرح دهد.

۱ـ۱۲ـ آشنایی با Active Directory Domain Services یا AD DS

همان‌طور که در فصل اول اشاره شد در شبکه دو مدل سرویس‌دهی وجود دارد : نظیر به نظیر (Workgroup) و مبتنی بر سرور. در مدل سرویس دهی نظیر به نظیر (Workgroup) که یک مدل ساده محسوب می‌شود، مدیر مرکزی وجود ندارد و هر کاربر مدیر رایانه خودش می‌باشد. در چنین مدلی اگر لازم باشد یک سیاست[۱] امنیتی یا مدیریتی برای رایانه‌ها یا کاربران شبکه تعیین شود، باید به صورت جداگانه در تک تک رایانه‌ها تنظیمات مربوطه انجام گیرد. اما در صورت نصب سیستم عامل سروری (مانند ویندوز ۲۰۰۸ سرور) و راه اندازی Domain، این امکان وجود دارد که بتوان تمامی رایانه‌ها یا کاربران با منابع موجود در شبکه را به صورت متمرکز مدیریت نمود یا اینکه یک سیاست امنیتی یا مدیریتی را بر روی تمام رایانه‌های موجود در شبکه اعمال کرد.

باید توجه داشت که Domain را فقط در یک سیستم عامل سروری می‌توان راه‌اندازی نمود که در این کتاب از سیستم عامل ویندوز ۲۰۰۸ سرور ویرایش مؤسسات[۲] استفاده خواهد شد.

برای راه اندازی Domain باید سرویس Active Directory را در یک سرویس‌دهنده Stand ــ alone نصب کنید (وقتی که شما ویندوز ۲۰۰۸ سرور نصب می‌کنید و رایانه شما عضو

---

۱ ــ Po cy

۲ــ W ndows Server 2008 Enterpr se

Workgroup می‌باشد (حالت پیش فرض نصب) رایانه شما یک سرویس دهنده Stand ـ alone می‌باشد). توجه داشته باشید که بعد از نصب Active Directory سرویس دهنده به یک کنترل‌کننده دامنه Domain Controller تبدیل می‌شود که اصطلاحاً به آن DC می‌گویند.

۲ـ۱۲ـ اجزای Active Directory

وقتی که شما می‌خواهید یک تماس تلفنی برقرار نمایید، شماره مورد نظر را از دفترچه تلفن پیدا می‌کنید؛ یا وقتی که در یک ساختمان اداری بزرگ به دنبال اتاق خاصی می‌گردید، به راهنمای طبقات مراجعه می‌کنید و یا در کتابخانه در هنگام جستجوی یک کتاب خاص، به فهرست منابع مراجعه می‌کنید. دفترچه تلفن، راهنمای طبقات و فهرست منابع یک نوع دایرکتوری(Directory) محسوب می‌شوند.

دایرکتوری‌های شبکه، اطلاعاتی درباره منابع موجود روی شبکه مانند کاربران، رایانه‌ها، چاپگرها، پوشه‌های به اشتراک گذاشته شده را نگهداری می‌کنند. دایرکتوری‌ها بخش اساسی هر سیستم عامل سروری می‌باشند. در سیستم عامل‌های قدیمی به ازای هربخش، یک دایرکتوری مجزا وجود داشت. در سیستم عامل‌های جدید یک دایرکتوری به نام Active Directory تمام اطلاعات را نگهداری می‌کند که در ویندوز ۲۰۰۸ سرور به Active Directory Domain Service یا AD DS تغییر نام پیدا کرده است (لازم به ذکر است در ویندوز ۲۰۰۰ و ۲۰۰۳ سرور، سرویس دایرکتوری به Active Directory یا AD مشهور بود).

بعد از نصب AD DS رایانه شما به یک DC یا Domain Controller تبدیل می‌شود. DC اطلاعات امنیتی و بانک اطلاعاتی اشیای دایرکتوری را نگهداری می‌کند و وظیفه آن احراز هویت[۱] در Domain می‌باشد، یعنی زمانی که کاربر می‌خواهد از روی سرویس گیرنده به Domain وارد شود، نام و گذر واژه[۲] کاربر به صورت کد شده به DC ارسال می‌شود. DC که اطلاعات تمام کاربران Domain را دارد، اطلاعات دریافتی را با اطلاعات خود مقایسه می‌کند، در صورتی که اطلاعات درست باشد صحت اطلاعات کاربر را به سرویس‌گیرنده اطلاع می‌دهد، به‌طوری که از آن به بعد، کاربر می‌تواند برای دسترسی به تمامی‌منابع موجود در Domain دسترسی داشته باشد.

۱ـ Authent cat on

۲ـ Password

۳ـ۱۲ـ مراحل نصب AD DS در ویندوز ۲۰۰۸ سرور

عملیاتی را که باید قبل از شروع به نصب AD DS انجام داد عبارت‌اند از :

ـ **تنظیم کارت شبکه[1] برای دادن IP استاتیک** : از دو روش می‌توان به تنظیمات IP دسترسی پیدا نمود :

الف) با استفاده از فرمان ncpa.cpl (اجرای فرمان از طریق کادر Run)

Start →Run → ncpa.cpl

ب) از Control Panel برنامه Network and Sharing اجرا کنید، سپس گزینه Manage network connections را انتخاب نمایید.

شکل ۱ـ۱۲

با اجرای هر کدام از دو روش قبلی پنجره Network Connections ظاهر می‌گردد. حال بر روی Local Area Connection کلیک راست نموده و سپس گزینه Properties را انتخاب نمایید.

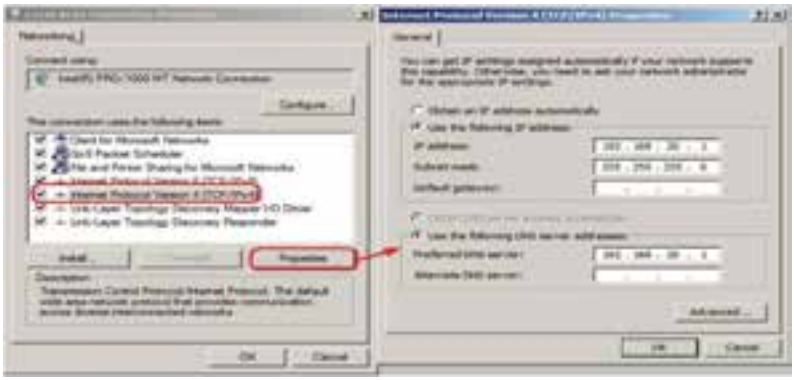
۱ـ امروزه تمام مادربردها دارای کارت شبکه Onboard می‌باشند. در صورتی که سیستم شما مجهز به کارت شبکه نبود با استفاده از گزینه Add hardware در Contro Pane یک کارت شبکه مجازی نصب کنید. ضمناً لازم است کارت شبکه رایانه مورد نظر به شبکه هم متصل باشد.

شکل ۲ــ۱۲

لازم به یادآوری است که برای سرورهای زیر ساخت[۱] در شبکه مانند DC، DNS،DHCP باید IP کارت شبکه را به‌صورت استاتیک (دستی) تنظیم نمایید. بنابراین اولین قدم در نصب AD DS تنظیم کردن IP کارت شبکه به صورت استاتیک می‌باشد.

در ادامه در کادر Local Area Connection Properties (شکل ۳ــ۱۲) ابتدا گزینه Internet Protocol version 4 (TCP/IPv4) را انتخاب نموده و بر روی دکمه Properties کلیک نمایید تا کادر Internet Protocol version 4 (TCP/IPv4) Properties برای تنظیمات IP ظاهر گردد.

۱ــ Infrastructure servers



شکل ۳ــ۱۲

گزینه Use the fallowing IP Address : را برای تنظیم IP استاتیک انتخاب نمایید و در آدرس 192.168.20.1 (کلاس C) را در کادر IP Address وارد نمایید. Subnet Mask به طورخودکار به 255.255.255.0 تبدیل می‌شود.

نکته ۱: به ازای کلاس‌های مختلف IPv4 مقدار Subnet Mask مطابق با جدول ۱ــ۱۲ تغییر خواهد کرد. عدد 255 به معنی ثابت بودن عدد Network در IPv4 می‌باشد.

جدول ۱ــ۱۲ــ مقدار subnet mask به ازای کلاس‌های مختلف IPV4

Class IPv4	A	B	C
Subnet Mask	255 0 0 0	255 255 0 0	255 255 255 0

AD برای فعالیت به DNS نیاز دارد. باید توجه داشت که DNS را هم می‌توان از قبل نصب نمود و هم این که درحین نصب AD، آن را برای نصب فعال کرد (که به نصب همزمان AD DS با DNS Server اصطلاحاً Integrated یا مجتمع می‌گویند) پس می‌توان Preferred DNS Server را هم به صورت 192.168.20.1 را وارد کنید.

نکته ۱: اگر DNS سرور شما به‌طور جداگانه روی سرور دیگری در شبکه پیاده‌سازی شده باشد باید آدرس IP آن سرور را در DNS server قرار دهید.

توصیه می‌شود نام رایانه را نیز تغییر دهید، برای این کار بر روی My Computer کلیک راست نموده و گزینه Properties را انتخاب نمایید و در زبانه Computer Name دکمه Change را برای تغییر نام رایانه، به نام دلخواه (مثلاً Server۱) انتخاب نمایید، توجه داشته باشید که بعد از تغییر نام، باید سیستم را مجدداً راه اندازی (Restart) کنید.

نکته ۳: باید کاربر مدیر (Administrator) حتماً دارای کلمه عبور باشد،یعنی کلمه عبور کاربر مدیر(administrator) نمی‌تواند تعریف نشده باشد و با زدن کلید enter به جای کلمه عبور وارد شود.

۴ـ۱۲ـ مراحل اصلی نصب AD DS

به دو روش می‌توان AD DS را نصب نمود :

الف) با استفاده از فرمان dcpromo

ب) با استفاده از ویزارد نصب

مراحل نصب AD DS با استفاده از ویزارد نصب به صورت زیر می‌باشد :

۱ـ از مسیر زیر برنامه Server Manager را اجرا کنید.

Start → Administrative Tools → Server Manger

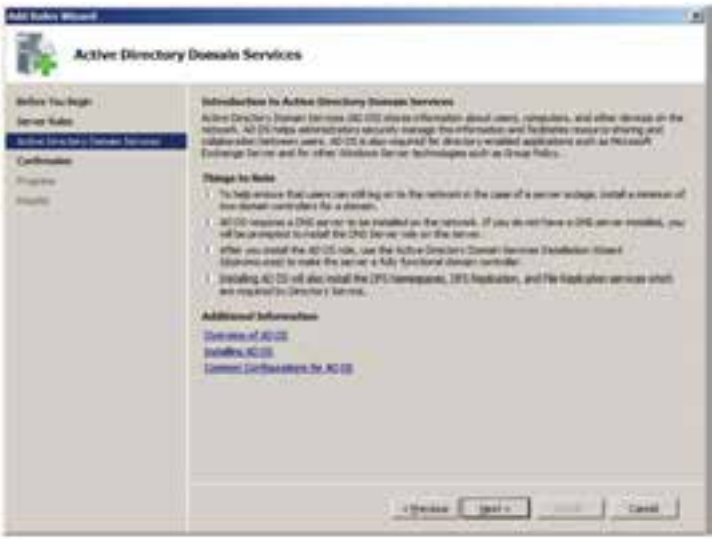
۲ـ در برنامه Server Manger روی Roles کلیک کنید، سپس بر روی Add Roles کلیک نمایید. تا Roleهای قابل نصب نمایش داده شوند، همان طور که مشاهده می‌کنید ۵ نقش (Role) در ارتباط با AD وجود دارد. حال گزینه Active Directory Domain services را در کادر Se lec t Server Roles انتخاب نمایید و سپس بر روی Next کلیک کنید.

شکل ۴ـ۱۲

نکته : با استفاده از گزینه Add Role از منوی Action هم می‌توان به پنجره Select Server Roles دسترسی پیدا نمود.

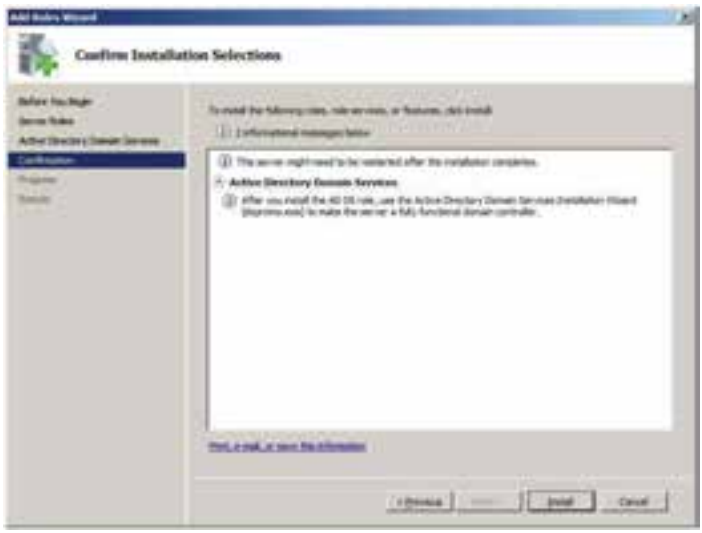
شکل ۵ــ۱۲

۳ــ در کادر توضیحات مختصر راجع به AD DS،بر روی Next کلیک کنید.



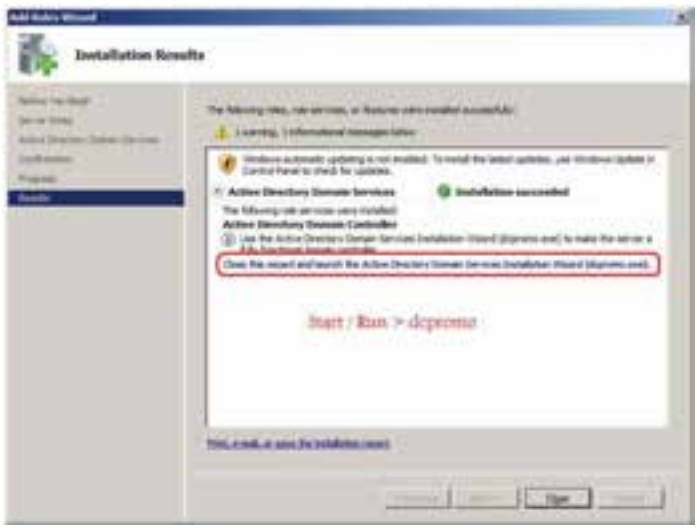
شکل ۶ــ۱۲

۴ــ در کادر Confirm Installation Selections بر روی دکمه Install کلیک کنید تا عملیات نصب شروع شود.



شکل ۷ــ۱۲

۵ــ صبر کنید تا کادر Installation Results ظاهر گردد.



شکل ۸ــ۱۲

برای ادامه کار احتیاج به اجرای برنامه Dcpromo داریم که برای اجرای آن دو راه وجود دارد :

الف) در پنجره Install Results بر روی لینکی که حاوی dcpromo.exe می‌باشد کلیک نمایید.

ب) فرمان dcpromo را از طریق Start→Run اجرا نمایید.

شکل ۹ــ۱۲

۶ــ برای ادامه نصب بر روی دکمه Next کلیک کنید تا کادر Operating System Compatibility که توضیحاتی برای سازگاری سیستم عامل می‌باشد نمایش داده شود، همچنین در انتهای کادر، آدرسی اینترنتی برای انجام تنظیمات مورد نظر قرار داده شده است.

شکل ۱۰ــ۱۲

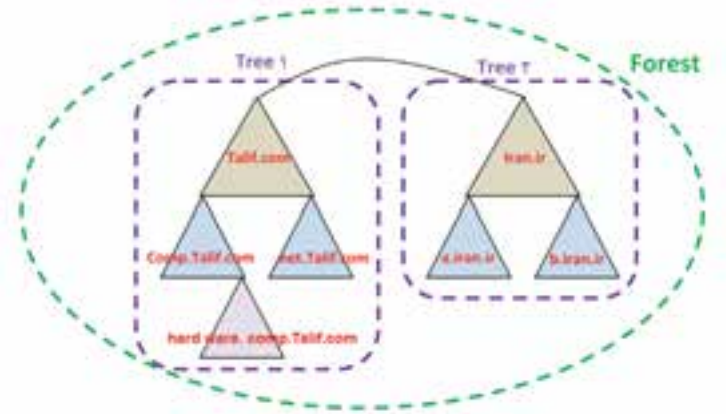
۷ــ در کادر Operating System Compatibility بر روی Next کلیک کنید.

شکل ۱۱ــ۱۲

۸ ــ در کادر Choose a Deployment Configuration چون شما اولین بار است اقدام به نصب AD می‌کنید، باید گزینه Create a new domain in a new forest را انتخاب کنید.(یعنی ایجاد یک Domain جدید در یک forest[1] جدید)

در اینجا باید اشاره کرد که DC فهرستی از Domainها را به صورت سلسله مراتبی ذخیره می‌کند، بنابراین Domain واحد اصلی ساختار منطقی AD می‌باشد و AD از یک مجموعه به نام Forest (جنگل) تشکیل شده است و Forest (جنگل) نیز از یک یا چند Tree (درخت) تشکیل می‌شود. به عبارت دیگر Tree از یک یا چند Domain در فضای نام (Namespace) پیوسته تشکیل شده است که به صورت سلسله مراتبی می‌باشد (مانند شکل ۱۲ــ۱۲).

۱ــ جنگل



شکل ۱۲ــ۱۲

هر کدام از مثلث‌ها در شکل ۱۲ــ۱۲ یک Domain می‌باشند و هر ردیف پایین‌تر به عنوان Child Domain (دامنه فرزند) برای ردیف بالایی می‌باشد و Domain بالاتر به عنوان Parent Domain (دامنه والدین) شناخته می‌شود. اولین Domain تعریف شده در یک Forest را Root Domain نیز می‌گویند.

۹ــ در صفحه Name the Forest Root Domain ، در کادر FQDN of the forest root Domain باید آدرس کامل یا FQDN را وارد نمایید. آدرس Talif.com را به عنوان آدرس Domain در نظر بگیرید (که به عنوان دامنه ریشه می‌باشد) سپس Nextرا کلیک کنید.

شکل ۱۳ــ۱۲

۱۰ــ بعد از وارد کردن نام دامنه ریشه، باید سطح عملکرد Forest را تعیین کنید، در اینجا شما می‌توانید سه سطح را تعیین کنید که عبارتند از ،Windows Server2003 Windows Server 2008 و Windows Server 2000.

شکل ۱۴ــ۱۲

توجه داشته باشید اگر شما Windows Server 2008 را انتخاب کنید، دیگر نمی‌توانید از DC این سرور در ویندوزهای سرور نسخه پایین‌تر مانند Windows Server 2000 یا 2003 در Forest استفاده نمایید.

۱۱ــ AD DS برای نصب، به DNS Server نیاز دارد، از صفحهٔ Additional Domain Cont roller Options چنانچه قبلاً سرویس DNS را نصب نکرده باشید می‌توانید DNS Server را با فعال کردن آن نصب کنید. اگر از قبل DNS Server را در این سرور نصب کرده باشید گزینه DNS Server غیر فعال خواهد بود.

شکل ۱۵ــ۱۲

با کلیک بر روی دکمه Next کادر هشدار شکل ۱۶ــ۱۲ ظاهر می‌شود، چنانچه شما بخواهید AD DS را با DNS Server به صورت مجتمع نصب کنید بر روی دکمه Yes کلیک کنید.

شکل ۱۶ــ۱۲

۱۲ــ در کادرLocation for Database, log file, and SYSVOLمی‌توانید محل ذخیره پوشه بانک اطلاعاتی(Database folder)، پوشه پرونده‌های Log مربوط به دایرکتوری (Log files folder) و ولوم پوشه (SYSVOL)[1] را تعیین کنید.

شکل ۱۷ــ۱۲

۱ــ در این پوشه اطلاعاتی از Doma n که یک کپی از آن به نام DC فرستاده می‌شود، نگهداری شده و این پوشه حتماً باید در یک پارتیشن با پرونده سیستم NTFS قرار داشته باشد.

۱۳ــ در صفحه Directory Services Restore Mode Administrator Password می‌توانید برای حالت بازیابی (Restore Mode) رمز در نظر بگیرید این رمز بهتر است با رمز کاربر مدیر ورود به ویندوز متفاوت باشد.

شکل ۱۸ــ۱۲

۱۴ــ پس از ورود رمز، روی Next کلیک کنید تا وارد صفحه Summary شوید.

شکل ۱۹ــ۱۲

۱۵ــ در صفحه Summary اگر بخواهید از تنظیمات انجام شده خروجی بگیرید، بر روی دکمه Export Settings کلیک نموده و نام محل ذخیره را تعیین نمایید.

۱۶ــ در ادامه بر روی Next کلیک کنید تا تنظیمات کامل شود. توجه داشته باشید که بعد از انجام تنظیمات سیستم باید دوباره راه اندازی (Restart) شود. گاهی اوقات گذر از این مرحله ممکن است چند دقیقه تا چند ساعت طول بکشد.

شکل ۱۲ــ۲۰

۱۷ــ صبر کنید تا کادر پیغام پایان عملیات ویزارد نصب، ظاهر شود و سپس بر روی دکمه Finish کلیک کنید و در کادر ظاهر شده، حتماً بر روی گزینه Restart Now برای راه اندازی مجدد سیستم عامل کلیک نمایید.

شکل ۱۲ــ۲۱

شکل ۱۲ـ۲۲

بعد از نصب AD DS و راه‌اندازی مجدد، سیستم کندتر بالا می‌آید. حالا رایانه ما به یک کنترل کننده دامنه (DC) تبدیل شده است.

۱۲ـ۵ـ تغییرات بعد از نصب AD DS در سیستم

اگر به بخش Administrative Tools مراجعه کنید، خواهید دید که آیتم‌هایی به آن در رابطه با Active Directory اضافه شده است که عبارتند از :

۱ـ Active Directory Users and Computer

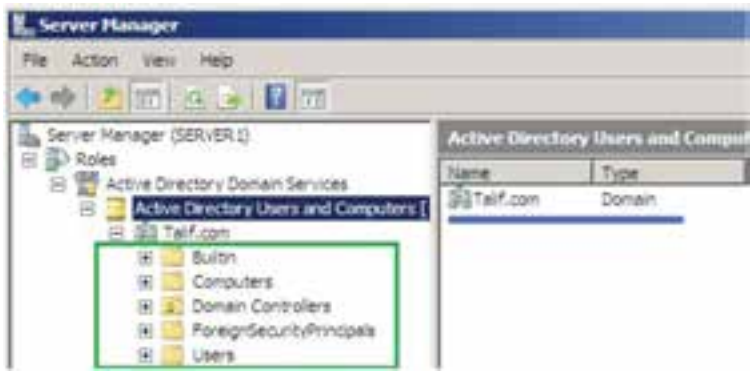
۲ـ Active Directory Domains and Trusts

۳ـ Active Directory Sites and Services

۴ـ Group Policy Management

۵ـ DNS (به خاطر فعال کردن DNS Server در حین نصب AD DS)

حال اگر برنامه Server Manager را باز کنید خواهید دید که در نام دامنه Talif.com در آن ثبت شده است. داخل دامنه Talif.com پوشه‌های مختلفی وجود دارد (شکل ۱۲ـ۲۳).

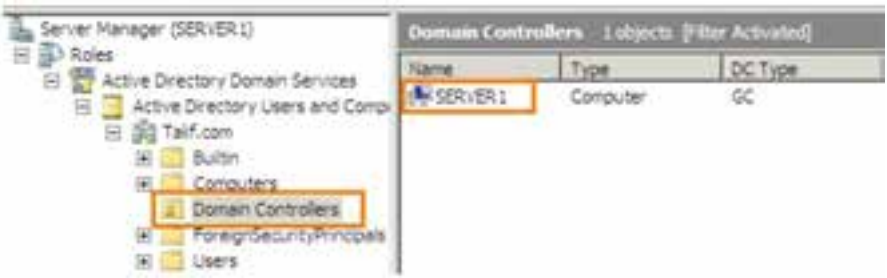


شکل ۱۲ـ۲۳

در پوشه Built ـ in لیست کاربران و گروه‌های کاربری داخل شبکه قرار دارد.

در پوشه Computers لیست رایانه‌های شبکه را نشان می‌دهد که عضو Domain هستند. وقتی که شما با رایانه‌ای به دامنه Talif.com متصل می‌شوید (Join) نام آن رایانه در فهرست Computers اضافه می‌شود.

پوشه Domain Controller لیست DC های داخل شبکه را نمایش خواهد داد. درحال حاضر رایانه جاری که DC روی آن نصب شده است نمایش داده می‌شود.



شکل ۲۴ـ۱۲

پوشه ForeignSecurityPrincipals حاوی آیتم‌هایی است که از یک دامنه دیگر وارد دامنه ما شده‌اند، مانند : دیسک سختی که داخل آن فهرست‌های اشتراکی وجود دارد و مربوط به دامنه‌های دیگرمی‌باشد و وارد دامنه ما شده است.

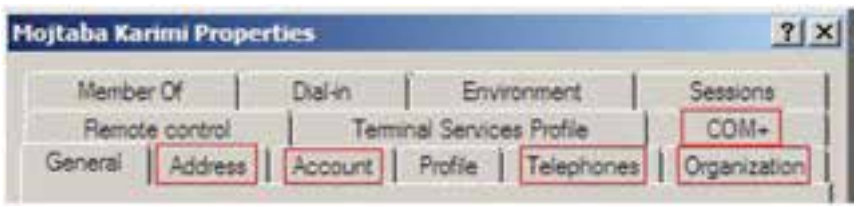
پوشه Users لیست کاربرانی که روی رایانه ما نصب شده‌اند را نمایش می‌دهد. ضمناً اگر DC دیگری هم وجود داشته باشد و به رایانه ما متصل باشد، لیست کاربران آن دامنه نیز قابل رؤیت خواهد بود.

در Server Manager در بخش Configuration همانطور که ملاحظه می‌کنید Local Groups and Users را نمی‌بینید و این به خاطر تبدیل رایانه ما به DC می‌باشد. لیست کاربران و گروه‌ها به صورت مشترک در پوشه Users وجود دارند.

حال اگر بر روی یک کاربر در Users کلیک راست کنید گزینه‌های بیشتری مانند شکل ۲۵ـ۱۲ رؤیت می‌شود.

شکل ۱۲ـ۲۵

حال اگر در پوشهٔ Users ویژگی‌های یک کاربر را نمایش بدهید، ملاحظه خواهید کرد که زبانه‌های بیشتری به کادر ویژگی‌های کاربر اضافه شده است. از ۸ زبانه در حالت Stand ـ alone به ۱۳ زبانه در حالت DC ارتقاء یافته است. (زبانه‌هایی که با کادر قرمز مشخص شده‌اند پس از نصب AD اضافه شده‌اند)

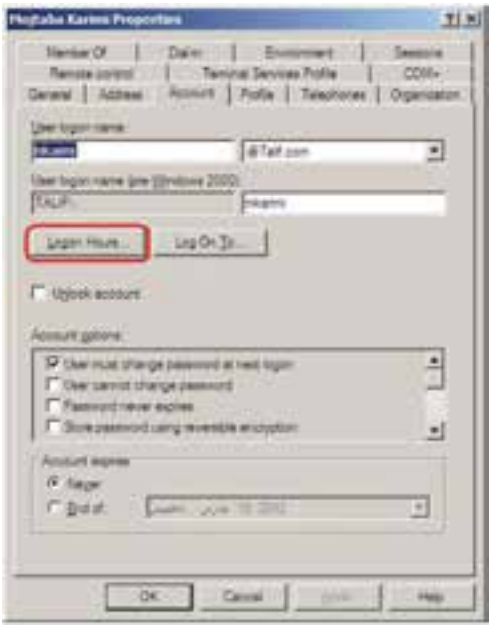


شکل ۱۲ـ۲۶

توجه داشته باشید در زبانه‌هایی که از قبل در حالت Stand ـ alone وجود داشته‌اند در حالت DC دارای مشخصات بیشتر و جزیی‌تر می‌باشند مانند زبانه General که نسبت به قبل، مشخصاتی مانند اداره، شماره تلفن، ایمیل و آدرس وب سایت به آن اضافه شده است (شکل ۱۲ـ۲۷).

شکل ۲۷ــ۱۲

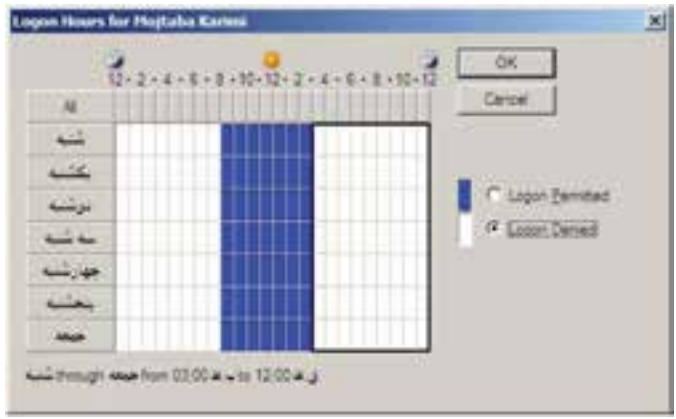
در زبانه Account یا حساب کاربری می‌توانید در User Logon Name نام کاربری برای Logon شدن را وارد کنید. البته اگر Logon Name را مشخص نکنید همان اسم کاربر به عنوان Logon Name در نظر گرفته می‌شود. در کادر بعدی نام دامنه را انتخاب کنید (Talif.com). اگر چند Domain داشته باشید لیست Domainها قابل انتخاب می‌باشد.



شکل ۲۸ــ۱۲

همچنین می‌توانید برای حسابتان تاریخ انقضا (Account Expire) مشخص کنید. پیش فرض گزینه Never می‌باشد یعنی کاربر تاریخ انقضا نداشته باشد و با تعیین تاریخ در بخش End of، می‌توانید تاریخ انقضا برای کاربر تعیین کنید.

در Logon Hours می‌توانید ساعت‌هایی را که کاربر می‌تواند در آن ساعت‌های خاص در ایام هفته Logon کند را مشخص کنید.



شکل ۲۹ــ۱۲

با توجه به شکل ۲۹ــ۱۲ خانه‌هایی که به رنگ آبی پر شده‌اند بیانگر این می‌باشد که در آن ساعت از روز هفته، کاربر اجازهٔ logon کردن را دارد و در بقیه ساعات روز در هفته کاربر اجازه Logon کردن را ندارد. برای تعیین ساعت‌های دلخواه ابتدا با انتخاب گزینه‌های Logon Permitted (ورود مجاز) و Logon Denied (عدم ورود) و با کلیک کردن روی سلول‌های مورد آن را به رنگ آبی (ورود مجاز) و یا به رنگ سفید (ورود غیرمجاز) درآورید.

شکل ۳۰ــ۱۲

با استفاده از Log On To در زبانه Account می‌توان مشخص نمود کاربر جاری از تمام رایانه‌های عضو دامنه بتواند Logon شود یا اینکه از رایانه‌های خاصی بتواند وارد شبکه شود. در حالت پیش فرض کاربر از تمام رایانه‌های موجود در شبکه می‌تواند Logon شود.

زبانه Address برای ورود یا تعیین مشخصات آدرس دقیق پستی کاربر می‌باشد.

شکل ۱۲ـ۳۱

در زبانه Telephone می‌توانید شماره تلفن منزل، شماره پیجر، شماره تلفن همراه و یا شماره فاکس را وارد کنید.

شکل ۱۲ـ۳۲

در زبانه Organization می‌توان اطلاعات مربوط به مشخصات اداری کاربر از قبیل عنوان شغلی[1]، گروه یا دپارتمان، نام شرکت و مدیر کاربر در شبکه و همچنین گزارشی راجع به کاربر را تعیین نمود.

شکل ۳۳ـ۱۲

با زبانه Member of می‌توان تعیین کرد که کاربر شما عضو کدام گروه می‌باشد به طور مثال کاربر ایجاد شده عضو گروه Domain Users می‌باشد.

۶ـ۱۲ـ گروه‌ها در AD DS

در AD کادر ایجاد گروه نیز با کادر گروه در Stand ـ alone متفاوت می‌باشد.

در زمان ایجاد گروه باید نوع و دامنه گروه را مشخص کنید

Group Type (نوع گروه) که شامل دو قسمت می‌باشد :

الف) Security Group (گروه امنیتی) : برای مجوز دادن استفاده می‌شود.

ب) Distribution Group (گروه توزیع) : از آنها به عنوان لیست استفاده

۱ـ Job T t e

می‌شود مانند استفاده از لیست برای ارسال ایمیل گروهی

Group scopes (حوزه گروه) بیانگر محدوده عملکرد یک گروه می‌باشد که شامل سه نوع می‌باشد :

۱ــ **Domain Local Group** : اعضای گروه می‌توانند از گروه‌های دیگر نیز باشند و فقط به منابع یک Domain دسترسی دارند.

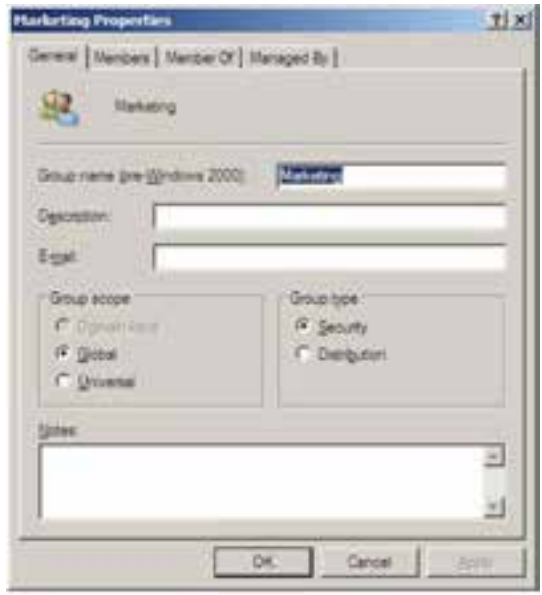
۲ــ **Global Group** : اعضای این گروه شامل حساب‌ها و گروه‌هایی است که در آن دامنه تعریف شده‌اند. اعضای این گروه می‌توانند به تمام دامنه‌های Forest دسترسی داشته باشند.

۳ــ **Universal Group** : اعضای این گروه می‌تواند از دامنه‌ای در جنگل یا درخت باشد. و می‌تواند به منابع تمام دامنه‌ها دسترسی داشته باشد.

برای ایجاد گروه جدید با کلیک راست بر روی Users می‌توانید گزینه New و سپس Group را انتخاب نمایید.

شکل ۳۴ــ۱۲

بعد از ایجاد گروه جدید با دابل کلیک بر روی نام گروه و یا کلیک راست بر روی نام گروه و انتخاب گزینه Properties کادر ویژگی گروه نمایش داده می‌شود.



شکل ۳۵ــ۱۲

در زبانه Members لیست گروه‌هایی که عضو گروه جاری هستند را نمایش می‌دهد و امکان اضافه کردن گروه جدید به لیست هم وجود دارد.

شکل ۳۶ــ۱۲

در زبانه Member Of می‌توان لیست گروه‌هایی که، گروه جاری عضو آنها می‌باشد را نمایش داد و همچنین می‌توان گروه جاری را به عضویت گروه‌های دیگر درآورد.

شکل ۳۷ــ۱۲

در کادر ویژگی گروه‌ها، زبانه Managed By نسبت به Stand ــ alone جدید می‌باشد که توسط آن می‌توانید نام مدیر گروه را مشخص کنید. با انتخاب نام مدیر گروه، مشخصات مدیر که در User Properties ثبت کرده‌اید در این زبانه نیز نمایش داده می‌شود.

شکل ۳۸ــ۱۲

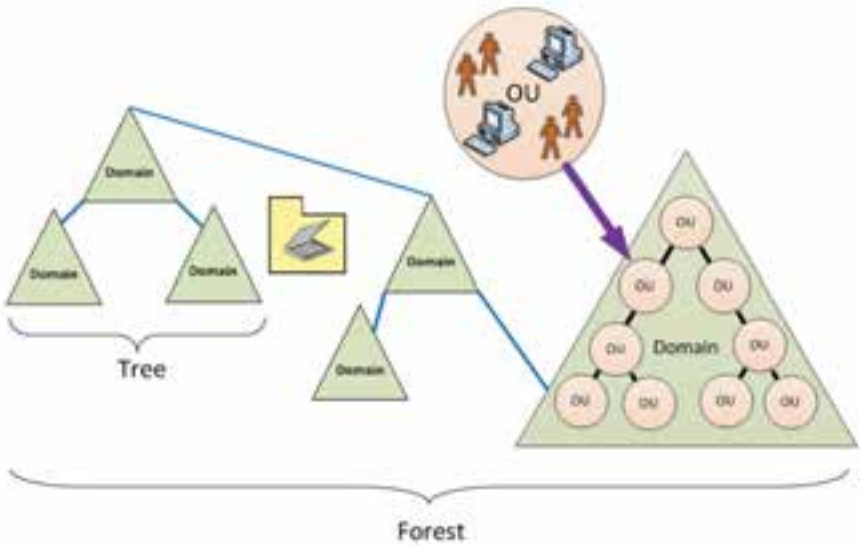
۷ـ۱۲ـ کاربرد Organizational Unit

در هر سازمان برای مدیریت ساده‌تر و ساختار یافته از یک سری واحدهای سازمانی استفاده می‌شود. به عنوان مثال استفاده از واحدهای مختلف نظیر کار گزینی، امور اداری، حسابداری، آموزش، روابط عمومی، IT و... در بسیاری از شرکت‌ها و سازمان‌ها معمول و مرسوم می‌باشد.

در هر واحد سازمانی تعدادی کارمند و مقداری منابع مثل رایانه، چاپگر و... یک مدیر برای آن واحد وجود دارد. برای مدیریت راحت‌تر شبکه، می‌توانید در یک Domain، واحدهای مختلف سازمانی ایجاد نمایید که به آن‌ها اصطلاحاً Organizational Unit می‌گویند و به اختصار با نام OU به آن‌ها اشاره می‌شود.

هر OU می‌تواند تعداد زیادی کاربر، رایانه، چاپگر و حتماً مدیر داشته باشد و حتی می‌توان سیاست‌های خاص برای آن‌ها در نظر گرفت.

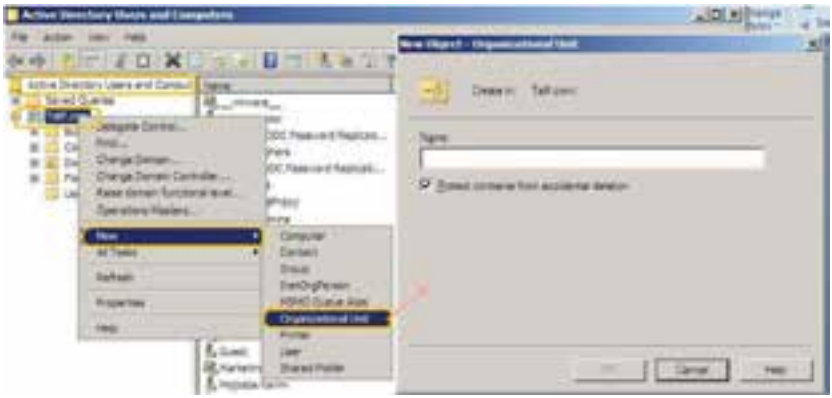
در واقع یک Domain را می‌توان به تعدادی OU تقسیم کرده و منابع و کاربران را نیز بین آن‌ها تقسیم نمود و حتی مدیریت آن‌ها را نیز به کاربران خاص واگذار نمود.



شکل ۱۲ـ۳۹

برای ایجاد یک OU جدید مراحل زیر را انجام دهید :

ابتدا برنامه Active Directory User and Computer از مسیر Start → Administrative Tools را اجرا کنید. بر روی Talif.com کلیک راست نموده و گزینه Organization Unit از New را انتخاب نمایید (مطابق شکل ۴۰ـ۱۲).



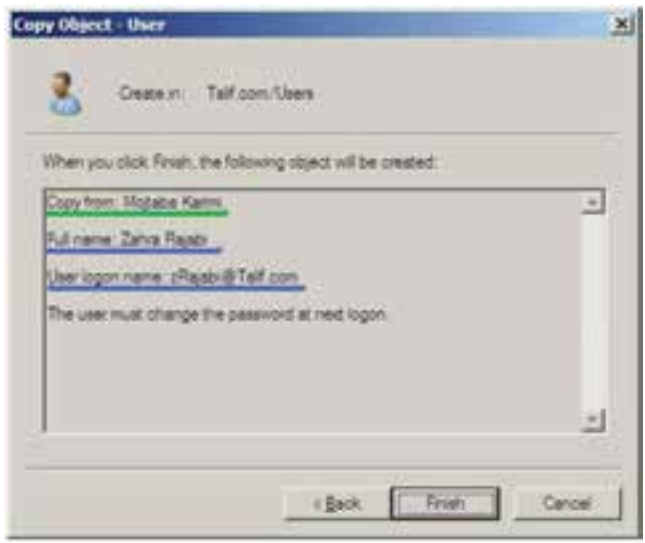
شکل ۴۰ـ۱۲

در کادر New Object ـ Organization Unit نام OU مورد نظر را وارد کنید. (مثلاً Customer1)

با کلیک بر روی OK، در زیر گروه Talif.com پوشه Customer1 که به عنوان یک OU می‌باشد اضافه شده است. حال می‌توانید برای این OU کاربر جدید، گروه جدید، رایانه جدید، چاپگر جدید و . . . اضافه نمایید. برای زمانی که مشخصات دسترسی کاربران یک OU شبیه هم بود شما می‌توانید بعد از ایجاد کاربر آن را تکثیر نمایید. مراحل کپی کردن یک کاربر روی کاربر مورد نظر Mojtaba) (Karimi کلیک راست نموده سپس گزینه Copy... را انتخاب نمایید. در کادر Copy Object User مشخصات کاربر جدید را وارد کنید (شکل ۴۱ـ۱۲).

شکل ۴۱ـ۱۲

با کلیک بر روی Next کادر دریافت کلمه عبور ظاهر می‌گردد، بعد از ورود کلمه عبور و کلیک بر روی دکمه Next گزارش ایجاد کاربر ظاهر می‌گردد که در آن مشخص شده که کاربر جدید از روی کاربر Mojtaba Karimi ایجاد شده است.



شکل ۴۲ـ۱۲

توجه داشته باشید با کپی کردن یک کاربر، پارامترهایی چون نام کشور ـ استان و شهر تنظیماتی چون Log on To Hours و Logon Account Expire از کاربر قبلی بر روی کاربر جدید نیز اعمال می‌شود.

۸ـ۱۲ـ Computer Account

یکی دیگر از اجزای AD، Computers می‌باشد. Computer Account فقط برای سیستم عامل‌هایی که دارای تکنولوژی NT هستند استفاده می‌شود (مانند Windows NT,2000,XP,2003,Vista,7,2008).

وقتی با ویندوزهای با تکنولوژی NT به دامنه (Domain) ویندوز سرور متصل می‌شوید یک حساب رایانه‌ای (Computer Account) به فهرست Computers اضافه می‌شود. شما می‌توانید حساب‌های کاربری و رایانه‌ای را غیر فعال (Disable)، تنظیم مجدد (Reset) و حذف نمایید.

به دو طریق می‌توان یک حساب رایانه‌ای برای اتصال به Domain ایجاد نمود.

۱ــ کلیک راست بر روی Computers در Active Directory User and Computer و انتخاب گزینه New و زیر گزینه Computers که کادر Newobjet Computer را برای ورود اطلاعات Computer Account نمایش می‌دهد.

شکل ۴۳ــ۱۲

کافی است در کادر Computer name نام رایانه را وارد کنید.

۲ــ از روی یک رایانه‌ای موجود در شبکه می‌توان یک حساب رایانه‌ای برای اتصال به Domain ایجاد نمود.

۹ــ۱۲ــ مراحل اتصال یک کلاینت به Domain

الف) در رایانه سرویس گیرنده (کلاینت) که دارای یکی از ویندوزهای XP، Vista و 7 می‌باشد ابتدا بر روی My Computer کلیک راست نموده سپس گزینه Properties را انتخاب نمایید.(در Windows XP[1])

۱ــ در W ndows V sta یا W ndows 7 بعد از انتخاب Propert es باید بر روی گزینه Change Sett ngsکلیک نمایید تا به زبانه Computer Nameدسترسی پیدا کنید.

ب) زبانه Computer Name را انتخاب نمایید و بر روی دکمه Change... کلیک نمایید.

ج) ابتدا در بخش Member of گزینه Domain را انتخاب نموده سپس نام دامنه (Talif.com) را وارد کنید. سپس بر روی OK کلیک کنید.

د) اگر ارتباط با دامنه Talif.com بر قرار شد کادر زیر برای دریافت نام کاربر و کلمه ورود نمایش داده می‌شود.

شکل ۴۴ــ۱۲

هـ) توجه داشته باشید که باید نام و کلمه عبور کاربر Administrator در ویندوز سرور ۲۰۰۸ که یک Domain می‌باشد را وارد کنید. در صورتی کلمه عبور و نام کاربر را درست وارد نمودید پیغام خوش آمدگویی به دامنه Talif.com ظاهر می‌گردد.

شکل ۴۵ــ۱۲

و) همچنین صفحه مشخصات رایانه با تعاریف جدید نمایش داده می‌شود.

شکل ۴۶ــ۱۲

ز) با کلیک کردن بر روی دکمه OK کادر پیغام زیرمبنی بر راه‌اندازی مجدد سیستم ظاهر می‌گردد.

شکل ۴۷ــ۱۲

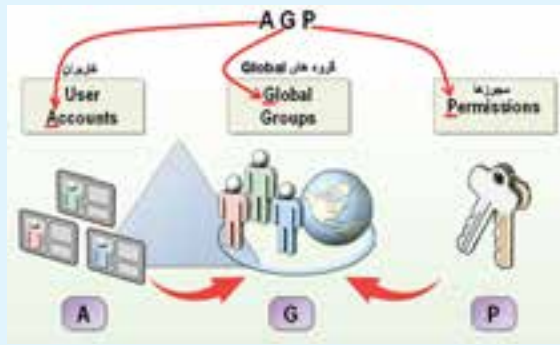
ح) بعد از انجام تنظیمات فوق، رایانه سرویس گیرنده باید مجدداً راه اندازی شود. به طوری که بعد از بالا آمدن سیستم عامل صفحه Logon ویندوز به صورت منوی کشویی برای نام کاربر جهت اتصال به Domain ظاهر می‌گردد.

۱۰ـ۱۲ـ روش‌های اعطای مجوز به کاربران

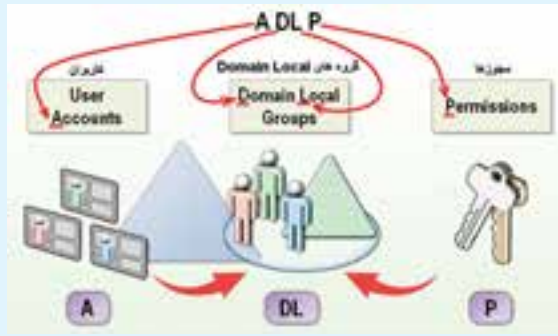
از روش‌های مختلفی برای اعطای مجوز به کاربران به کمک گروه‌ها می‌توان استفاده نمود. در این‌جا به چند روش اشاره می‌شود.

۱ـ۱۰ـ۱۲ـ روش AGP : در این روش کاربران (Account)ها در گروه‌های مختلف از نوع Global دسته‌بندی می‌شوند. همان‌طوری که قبلاً هم بیان شد، این دسته‌بندی از نظر نوع کار و محل جغرافیایی کاربران انجام می‌شود. سپس مجوز (permission) لازم به گروه‌ها اعطا می‌شود. از این روش در شبکه‌هایی که تعداد objectها زیاد نیست می‌توان استفاده کرد.

۲ـ۱۰ـ۱۲ـ روش ADLP : دراین روش می‌توانید کاربران (Account)ها را در گروه‌های مختلف از نوع Domain Local دسته‌بندی کنید. سپس به گروه‌های مورد نظر مجوز لازم اعطا کنید (شکل ۴۸ـ۱۲).

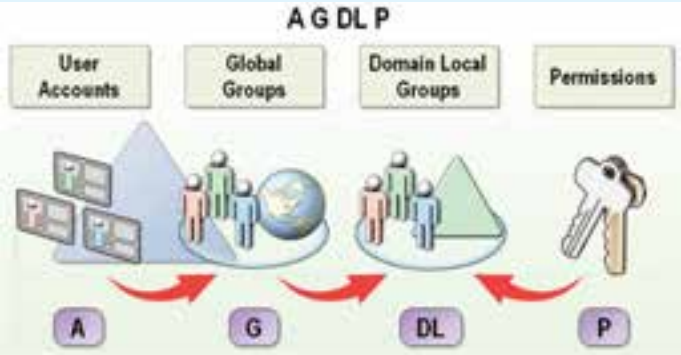


شکل ۴۸ـ۱۲



شکل ۴۹ـ۱۲

۳ـ۱۰ـ۱۲ـ AGDLP : در این روش کاربران (Account)ها را در گروه‌های مختلف از نوع Global دسته‌بندی کنید. سپس گروه‌های از نوع Domain Local ایجاد کرده و به آن‌ها مجوز (Permission) لازم را اعطا کنید. حال تمامی گروه‌های Global که لازم است مجوزهای مربوطه را داشته باشند، به عضویت گروه‌های Domain Local درآورید.



شکل ۱۲ـ۵۰

از این روش در شبکه‌هایی که تعداد object های زیادی دارند و یا شبکه‌هایی که از چندین Domain تشکیل شده‌اند می‌توان استفاده کرد.

۱۱ـ۱۲ـ آشنایی با گروه‌های Built-in

گروه‌های Built in گروه‌هایی هستند که زمان نصب Active Directory به صورت اتوماتیک ایجاد می‌شوند. این گروه‌ها را در ابزار Active Directory Users and Computers در پوشه‌های Built in و Users می‌توان مشاهده نمود.

۱ـ۱۱ـ۱۲ـ گروه‌های Built in Global : این گروه‌ها در پوشهٔ Users در ابزار Active Directory Users and Computer قرار دارند و عبارتند از :

■ **Domain users** : این گروه شامل تمامی کاربران Domain می‌شود. هر کاربری که در Domain ایجاد می‌شود، به صورت اتوماتیک به عضویت این گروه درمی‌آید.

■ **Domain Admins** : اعضای این گروه می‌توانند Domain را مدیریت کنند و به عنوان مدیر Domain شناخته می‌شوند. فقط Administrator همان Domain به

صورت پیش‌فرض عضو این گروه می‌باشد.

■ **Enterprise Admins** : اعضای این گروه می‌توانند Forest را مدیریت کنند. یعنی توان مدیریت در تمامی Domainهای Forest را خواهند داشت. به صورت پیش‌فرض Administrator اولین Domain عضو این گروه می‌باشد. این گروه به صورت پیش‌فرض از نوع Global می‌باشد. اما اگر سطح کارکرد Domain را به Native ۲۰۰۰ یا به Server ۲۰۰۳ تغییر دهید، این گروه به صورت اتوماتیک به نوع Universal تبدیل خواهد شد.

شکل ۱۲ــ۵۱

شکل ۱۲ــ۵۲

شکل ۱۲ــ۵۳

۲ــ۱۱ــ۱۲ــ گروه‌های Built in Domain Local : این گروه‌ها در پوشه Built in در ابزار Active Directory Users and Computers قرار دارند عبارتند از :

■ **Administrators** : اعضای این گروه می‌توانند DCها را مدیریت کنند و

تمامی مجوزها روی این رایانه‌ها قرار خواهند داشت.

■ **Server operators** : اعضای این گروه می‌توانند در انجام بعضی ازکارهای مدیریتی به مدیر شبکه کمک کنند به‌عنوان مثال می‌توانند عملیات زیر را روی DCها انجام دهند.

- Log on کردن
- Shut down کردن
- قالب‌بندی کردن درایوها
- تغییرساعت

■ **Account operators** : اعضای این گروه می‌توانند عملیات مدیریتی همچون ایجاد، حذف و ... را روی Accountها (شامل : کاربران، گروه‌ها و رایانه) انجام دهند. به‌عنوان مثال اعضای این گروه می‌توانند یک کاربر و یک گروه ایجاد کرده و آن کاربر را به عضویت آن گروه درآورند.

■ **Print operators** : اعضای این گروه می‌توانند چاپگرهای Domain را مدیریت نمایند.

● **Backup operators** : اعضای این گروه می‌توانند عملیات Backup گرفتن از اطلاعات و برگرداندن اطلاعات (Restore کردن) را انجام دهند.

■ **Network configuration operators** : اعضای این گروه می‌توانند تنظیمات شبکه را تغییر دهند. به عنوان مثال این اعضا می‌توانند آدرس IP را روی کارت شبکه DC تغییر دهند.

۳ــ۱۱ــ۱۲ــ گروه‌های Built in system : این گروه‌ها، گروه‌هایی هستند که لیست اعضای آن‌ها را نمی‌توان دید و یا تغییر داد. اما می‌توانید از آن‌ها برای انجام کارهای مدیریتی استفاده کنید، به عنوان مثال می‌توانید به این گروه‌ها مجوز اعطا کنید. این گروه‌ها عبارتند از :

■ **Every one** : این گروه شامل تمامی کاربرانی می‌شود که به یک رایانه متصل می‌باشند (تمامی کاربران شناخته شده و یا ناشناخته).

■ **Authenticated users** : تمامی کاربران که عمل authentication برای

آن‌ها اتفاق می‌افتد یا به عبارت دیگر دارای account می‌باشند.

■ **Anonymous Logon** : این گروه شامل کاربرانی است که به صورت ناشناس به یک رایانه متصل می‌شوند.

■ **Dialup** : این گروه شامل کاربرانی است که از طریق Dialup به رایانه متصل می‌شوند.

■ **Network** : شامل کاربرانی است که از طریق شبکه به یک رایانه متصل می‌شوند.

زمانی که به کاربران مجوز اعطا می‌کنید در لیستی که کاربران و گروه‌ها نمایش داده می‌شوند، می‌توانید گروه‌های سیستمی را مشاهده کنید.

۱۲ـ۱۲ـ پیاده‌سازی روش‌های مختلف اعطای مجوز به کاربران

۱ـ ۱۲ـ۱۲ـ پیاده‌سازی روش AGP : در این روش ابتدا یك گروه از نوع Global به همان شیوه‌ای که در مراحل قبل یاد گرفتید با نام G sale ایجاد کنید.

سپس مطابق شکل ۱۲ـ۵۴ از این گروه Properties گرفته و در زبانه Members لیست اعضای این گروه را مشاهده می‌کنید.

شکل ۱۲ـ۵۴

حال اگر روی کلید Add کلیک کنید پنجرهٔ شکل ۵۰ـ۱۲ نمایش داده خواهد شد. در این پنجره می‌توانید اسامی کاربران را تایپ کرده و به لیست اضافه نمایید و یا برای انتخاب کاربران از لیست روی کلید Advanced کلیک کرده و سپس روی گزینهٔ Find Now کلیک نمایید تا لیستی از کاربران و گروه‌ها نمایش داده شوند.

شکل ۵۵ـ۱۲

حال کاربران مورد نظر را به کمک کلیدهای Ctrl و یا Shift انتخاب کرده و به لیست اضافه نمایید. مشاهده خواهید کرد که این کاربران در زبانه Members لیست شده‌اند. روی گزینه OK کلیک کنید.

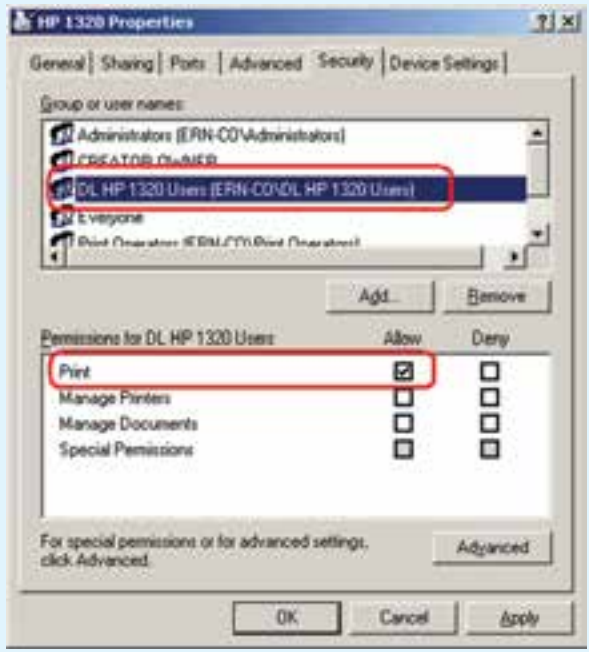
شکل ۵۶ـ۱۲

حال در هر جایی که منابع قرار دارند به این گروه مجوز می‌دهید. به عنوان مثال فرض کنید که یک پوشه به اشتراک گذاشته شده به‌نام Sale Data وجود دارد. روی این پوشه کلیک راست کرده و گزینه Sharing and security را انتخاب کنید، در پنجره ظاهر شده روی Permissions کلیک کنید تا پنجره شکل ۵۶ـ۱۲ ظاهر شود.

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.

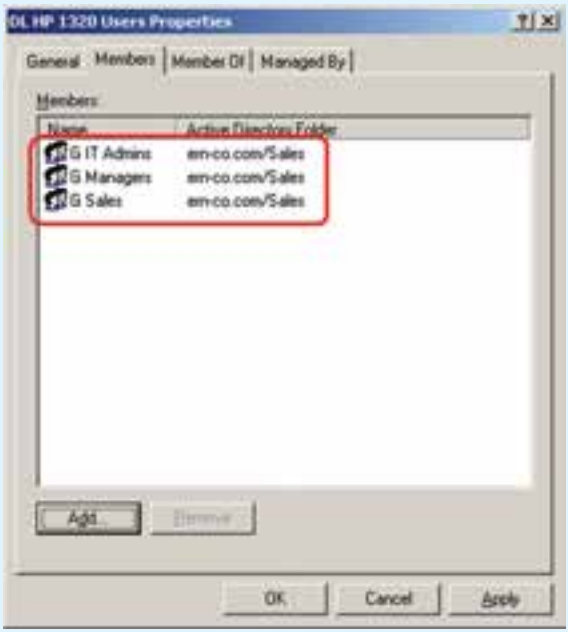
۲ــ ۱۲ ــ۱۲ــ پیاده‌سازی روش ADLP : این روش مشابه روش قبلی می‌باشد با این تفاوت که گروه را با نام DL Sales ایجاد کرده و نوع آن را Domain Local انتخاب کنید. بقیه مراحل مشابه مثال قبل می‌باشد.

۳ــ ۱۲ ــ۱۲ــ پیاده‌سازی روش AGDLP : دراین روش ابتدا یک دسته‌بندی منطقی برای کاربران درنظر گرفته و سپس گروه‌هایی از نوع Global را ایجاد کنید و کاربران را براساس آن دسته‌بندی به عضویت گروه‌های مختلف درآورید. سپس یک گروه از نوع Domain Local ایجاد نمایید و مجوزهای لازم روی منبع موردنظر را به آن اعطا نمایید. به عنوان مثال یک گروه با نام DL HP ۱۳۲۰ Users از نوع Domain Local ایجاد نموده و مجوز Print را روی یک چاپگر به اشتراک گذاشته شده به آن اعطا کنید (شکل ۵۷ــ۱۲).



شکل ۵۷ــ۱۲

حال تمامی گروه‌های از نوع Global را که قرار است مجوز Print روی این چاپگر داشته باشند، به عضویت گروه DL HP ۱۳۲۰ users درآورید (شکل ۵۸ـ۱۲).



شکل ۵۸ـ۱۲

خودآزمایی و پژوهش

۱ـ Domain Controller چیست؟ وظایف و ویژگی‌های آن‌ها را شرح دهید.

۲ـ Forest چیست؟

۳ـ Child Domain را با ذکر مثال تعریف کنید.

۴ـ آیا یک رایانه می‌تواند به طور همزمان عضو چند Domain باشد؟

۵ـ بررسی کنید که چه روش دیگری برای نصب Active Directory وجود دارد؟

۶ـ تفاوت Security Group و Distribution در چیست؟

۷ــ چطور می‌توان در یک سطح وزارتخانه برای کاربران مجوزهای لازم را صادر کرد؟

۸ــ اگر بخواهیم برای یک مدرسه، شبکه‌ای ایجاد کنیم که شامل کلیه دانش‌آموزان و معلمان و مدیران باشند از کدام روش باید برای اعطای مجوز به کاربران استفاده کنیم؟ توضیح دهید.

۹ــ انواع Account را نام ببرید.

۱۰ــ کاربرد Account Expires چیست و رابطه آن را Password never expires بنویسید.

۱۱ــ یک کاربر به عنوان Student ایجاد کرده که دارای ویژگی‌های زیر باشد.

الف) فقط روزهای زوج از ساعت ۱۰ الی ۱۴ بتواند Log on کند.

ب) فقط روی ۳ عدد از سرویس گیرنده‌ها بتوانند Log on کند.

ج) بتواند چاپگر را مدیریت کند.

د) بتواند تنظیمات شبکه، IP سیستم‌ها را عوض کند.

هـ) بتواند از طریق Dial up به شبکه متصل شود.

فصل سیزدهم

DNS و روش‌های تبدیل اسم به IP

هدف‌های رفتاری: هنرجو پس از پایان این فصل می‌تواند:

- کاربردهای DNS را بیان کند.
- اسامی اینترنتی و Host Name را شناسایی کند.
- اجزای DNS را توضیح دهد.
- مراحل تبدیل اسم به IP را در اینترنت شرح دهد.
- یک سرویس DNS را نصب و راه اندازی کند.
- سرویس DNS را برای انجام عمل Name Resolution آزمایش کند.

۱ـ۱۳ـ کاربردهای DNS

سرویس Domain Name System یا سیستم نام دامنه، به اختصار DNS نامیده می‌شود. همانطور که قبلاً اشاره شد، برای دسترسی به یک رایانه در یک شبکه محلی هم می‌توان از نام رایانه استفاده نمود و هم امکان استفاده از آدرس IP آن رایانه وجود دارد. برای ورود به وب سایت‌های اینترنتی هم این شرایط صادق است، یعنی هم می‌توان آدرس سایت (نام سایت) را در مرورگر وب[۱] وارد کرد و هم می‌توان با دانستن آدرس IP وب سرور، به سایت مورد نظر دسترسی پیدا نمود، ولی اکثر کاربرها ترجیح می‌دهند به جای استفاده از اعداد و ارقام آدرس IP، از نام آن سایت استفاده کنند، چرا که به خاطر سپردن نام به مراتب راحت تر از آدرس IP می‌باشد. (توجه داشته باشید که به خاطر سپردن IPv6 به مراتب سخت تر خواهد شد)

به عنوان مثال با استفاده از آدرس IPv4 مربوط به سازمان سنجش آموزش کشور (که برابر

۱ـ Web Browser

92.242.195.1 می‌باشد)و وارد کردن این آدرس IP در مرورگر وب، می‌توان وب سایت سازمان سنجش را مشاهده نمود، ولی با استفاده از آدرس www.sanjesh.org هم می‌توان به آن دسترسی پیدا کرد. با توجه به مطالب فوق باید مکانیزمی برای تطبیق نام و آدرس IP وجود داشته باشد تا از بروز خطا جلوگیری شود که به آن مکانیزم در شبکه‌های رایانه ای سرویس DNS می‌گویند. بنابراین سرویس DNS عمل تطبیق نام با آدرس IP را انجام می‌دهد (در حقیقت DNS، یک سیستم پایگاه داده‌ای است که نام FQDN را به آدرس IP ترجمه می‌کند)

سرویس Domain Name System (DNS) در اینترنت و بسیاری از شبکه‌های خصوصی استفاده می‌شود و نقش کلیدی در ویندوز ۲۰۰۸ سرور دارد و یکی از کارهای اصلی آن تبدیل اسم به IP و بالعکس می‌باشد. لازم به ذکر است که اکتیودایرکتوری(AD) به کمک DNS تحلیل نام رایانه و پیدا کردن آن‌ها در شبکه را انجام می‌دهد.

می‌توان گفت که استفاده از DNS شبیه برقراری یک تماس تلفنی با گوشی تلفن همراه می‌باشد، وقتی که شما نام مخاطب را تعیین می‌کنید، به طور خودکار شماره مخاطب مورد نظر در دسترس قرار خواهد گرفت.

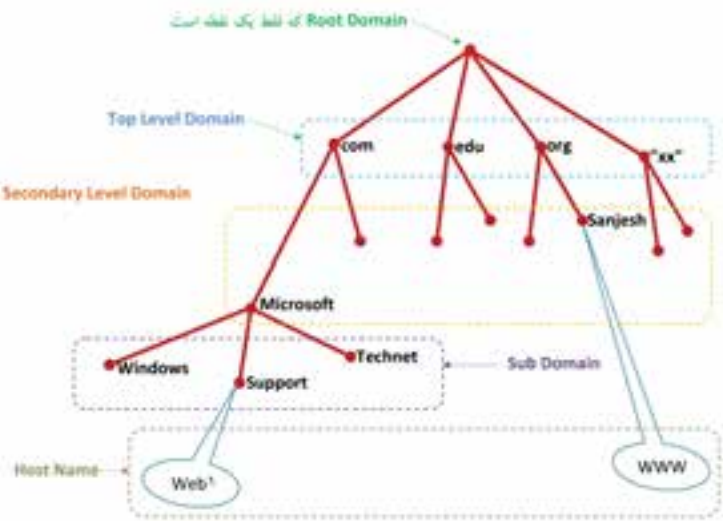
> **نکته:** قبل از DNS، تطبیق نام با آدرس IP با استفاده از پرونده‌های متنی به نام پرونده میزبان (Host File) انجام می‌گرفت که به صورت محلی بر روی هر رایانه ذخیره شده بود. پرونده میزبان حاوی اسامی و آدرس‌های IP متناظر با آن اسامی می‌باشد. هر گاه یک میزبان جدید بـه شبکه اضافه می‌شد، مدیر شبکه به صورت دستی نام میزبان جدید و آدرس IP آن را به پرونده میزبان اضافه و آن را به روز رسانی می‌کرد.

۲ـ۱۳ـ انواع اسامی‌دامنه DNS

سرویس DNS از نام گذاری سلسله مراتبی پشتیبانی می‌کند و به عنوان یک پایگاه داده سلسله مراتبی و توزیع شده می‌باشد که حاوی انواع داده‌ها، اسامی‌دامنه و اسامی‌میزبان می‌باشد.

اسامی در DNS از ساختار درختی سلسله مراتبی به نام فضای نام دامنه یا Domain Namespace تشکیل شده است و از پنج مجموعه برای تشریح فضای نام دامنه (Domain Namespace) استفاده می‌شود.

الف) Root Domain : در بالاترین محل ساختار درختی دامنه ریشه(Root Domain) قرار دارد و به صورت یک نقطه "." می‌باشد یعنی تمام اسامی‌اینترنتی به یک نقطه ختم می‌شوند البته در موقع درج یک آدرس استفاده از نقطه الزامی‌نیست و معمولاً در معرفی یک آدرس اینترنتی آن را نمی‌نویسند، ولی باید توجه داشته باشید که این نقطه بخشی از نام آدرس اینترنتی می‌باشد (برخلاف نقطه‌های دیگر آدرس که به عنوان جداکننده استفاده می‌شود).



شکل ۱ــ۱۳ــ ساختار درختی آدرس اینترنتی

با توجه ساختار درختی ۱ــ۱۳ می‌توان FQDNهای زیر را نوشت

Web1.support.Microsoft.com.

www.sanjesh.org.

ب) Top Level Domain یا TLD : دومین بخش از ساختار درختی یک آدرس می‌باشد که تعیین کننده حوزه فعالیت می‌باشد و به دو بخش تجزیه می‌شود :

● ***Generic TLD یا gTLD*** : به مفهوم حوزه عمومی‌فعالیت و تعیین کننده نوع سازمان بوده و شامل پسوندهایی نظیر com، edu، net، org، sch و ac ... می‌باشد.

● ***ccTLD یا Country Code*** : از یک استاندارد دو حرفی برای تعیین کشور (حوزه جغرافیایی) استفاده می‌شود مانند ir، tw، ip، jp، uk، us و ... که به ترتیب مشخص کننده کشورهای ایران، تایوان، عراق، ژاپن، انگلیس و آمریکا و... می‌باشد.

به عنوان مثال آدرس www.bmi.ir، آدرس اینترنتی بانک ملی جمهوری اسلامی ایران می‌باشد.

در بعضی از مواقع gTLD و ccTLD به صورت ترکیبی مورد استفاده قرار می‌گیرند به طوری که ابتدا gTLD وسپس ccTLD قرار می‌گیرد

gTLD.ccTLD

به عنوان مثال در ایران gov.ir برای وزارتخانه‌ها و فرمانداری‌ها و سایر مؤسسات دولتی استفاده می‌شود.

www.refah.gov.ir (وزارت رفاه)، www.mfa.gov.ir (وزارت امورخارجه) و www.kashan.gov.ir (فرمانداری کاشان) و www.gilan.mim.gov.ir (سازمان صنایع و معادن استان گیلان) و www.oil.gov.iq (وزارت نفت عراق)

به عنوان نمونه دیگر برای مدارس و سازمان‌های وابسته به آن در کشور ما، از sch.ir استفاده می‌شود.

مانند www.chap.sch.ir (پایگاه کتاب‌های درسی)، www.talif.sch.ir (دفتر برنامه‌ریزی و تألیف کتب درسی) و www.jafari.sch.ir (هنرستان علامه جعفری)

همچنین برای دانشگاه‌های ایران از پسوند ac.ir استفاده می‌شود :

مانند www.tvu.ac.ir (دانشگاه فنی و حرفه‌ای کشور)، www.pnu.ac.ir (دانشگاه پیام نور) و www.nit.ac.ir (دانشگاه صنعتی نوشیروانی بابل)

ج) ***Secondary Level Domain یا SLD*** : دومین سطح دامنه می‌باشد که به صورت منحصر به فرد بوده و می‌توان آن را به صورت حقیقی[1] یا حقوقی[2] به ثبت رساند.

مطالعه آزاد

مدیریت Domain Root در اختیار شرکت بین‌المللی غیرانتفاعی ICANN[3] می‌باشد (آدرس سایت شرکت www.icann.org می‌باشد) که ابتدا این مدیریت قبل از سال ۱۹۹۸ در اختیار دولت آمریکا بود. ضمناً gTLD نیز توسط ICANN

۱ــ ثبت به نام شخص

۲ــ ثبت به نام شرکت یا مؤسسه

۳ــ Internet Corporat on for Ass gned Numbers and Names

مدیریت می‌شود و به یک سری از ثبات‌های معتبر واگذار شده است. اینترنیک InterNIC[1](زیرمجموع ICANN است) سازمانی است که domain name ها را صادر می‌کند، ولی مدیریت ccTLD به کشورهای مربوطه واگذار شده است(مانند ir که به ایران واگذار شده است.) در ایران امتیاز و مسئولیت دامنه‌ها برعهده پژوهشگاه دانش‌های بنیادی است. لازم به ذکر است شرکت ICANN محتوای اینترنت را کنترل نمی‌کند، بلکه فقط آدرس‌های اینترنتی را کنترل می‌نماید.

د) **Sub Domain** : زیر دامنه که به شرکت‌های مربوطه واگذار می‌شود (در واقع به SLD واگذار می‌شود) برای مثال شرکت Microsoft می‌تواند زیر دامنه Support یا هر زیر دامنه دلخواه دیگر را ایجاد نماید و کنترل نام زیر دامنه بر عهده شرکت Microsoft خواهد بود.

هـ) **Host Name** : می‌توان نام میزبان را مانند برگ در درخت دانست که برای شناسایی یک منبع خاص استفاده می‌شود.

با توجه به ساختار درختی فوق می‌توان آدرس کامل یک سایت یا FQDN یک سایت را به صورت زیر نوشت :

www.support.microsoft.com

FQDN یک نام منحصر به فرد برای شناسایی موقعیت میزبان درون درخت سلسله مراتبی DNS می‌باشد. به عبارت دیگرFQDN،محل دقیق قرارگیری یک کامپیوتر در دامنه را توصیف می‌کند. حال با توجه به مطالب فوق می‌توان فرم کلی اسامی‌اینترنتی را به صورت زیر نوشت :

Host.subdomain.SLD.TLD.

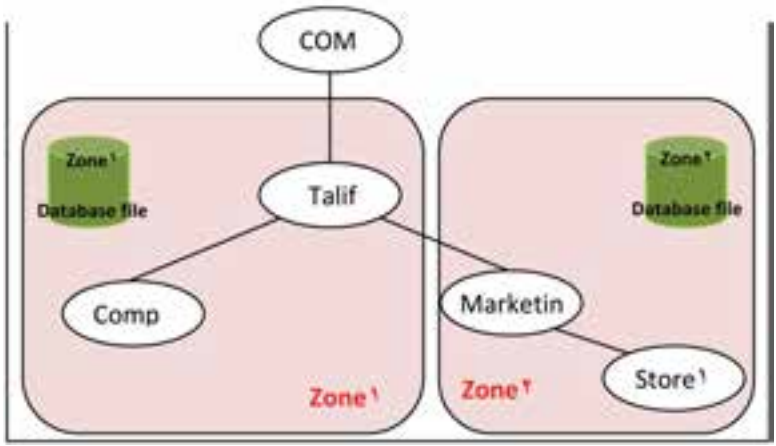
۳ـ۱۳ـ اجزای DNS

۱ـ۳ـ۱۳ـ Zone : بخشی از فضای نام دامنه (Domain namespace) در DNS می‌باشد. یکZone فضای نام دامنه را به چند بخش تقسیم می‌کند تا مدیریت آنها برای مدیران راحت‌تر شود. باید توجه داشت که Zone معادل Domain نیست بلکه از یک یا چند Domain مجاور هم تشکیل شده است. (چند Domain غیرمجاور نمی‌توانند یک Zone را تشکیل دهند) بنابراین Zoneها

۱ـ Internet Network Informat on Center

شامل رکوردهای منابع برای اسامی‌یک منطقه خاص می‌باشد. در یک سرور DNS، پرونده‌های Zone شامل رکوردهای بانک اطلاعاتی DNS Server می‌باشد ولی زمانی که AD با DNS به صورت مجتمع نصب می‌شوند داده‌های DNS داخل AD ذخیره خواهند شد.

به عنوان مثال، در شکل ۲ــ۱۳، قلمروی Talif.com به دو Zone تقسیم شده است. این Zoneها به یک مدیر اجازه می‌دهند قلمروی Talif و Comp را مدیریت کند و به مدیر دیگر، مدیریت قلمرو marketing و Storel را واگذار می‌کند.



شکل ۲ــ۱۳

هرZone شامل یک بانک اطلاعاتی مخصوص به خود است که تمامی‌اطلاعات مربوط به زیر دامنه‌های خود را در آن نگهداری می‌کند.

۲ــ۳ــ۱۳ــName Server : به کامپیوتری گفته می‌شود که سرویس DNS بر روی آن نصب شده باشد و داده‌های مربوط به یک Zone یاچندین Zone را در خود نگهداری کند. در واقع Name Server دارای یک فایل بانک اطلاعاتی اصلی است که به بانک اطلاعاتی Zoneها اشاره دارد.

۳ــ۳ــ۱۳ــName Resolution : فرآیندی است که توسط Name Server جهت پیدا کردن کامپیوتر در یک دامنه، با تبدیل اسم به IP و یا بالعکس، انجام می‌گیرد.

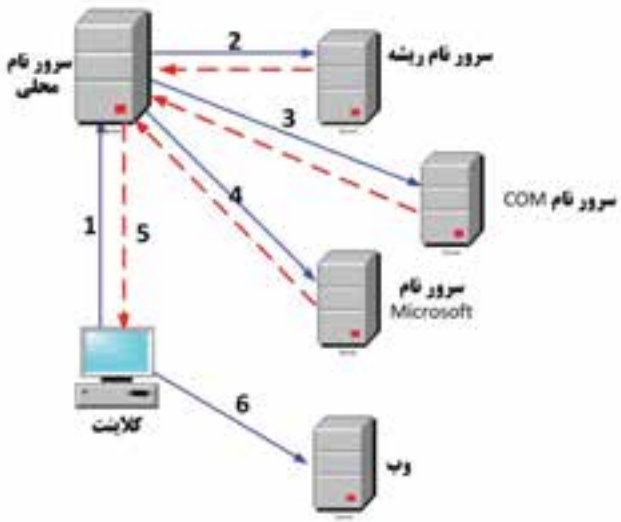
DNS دو نوع در خواست را بررسی می‌کند :

● ***Forward Lookup Query*** : درخواست‌های Forward، نام را به IP تبدیل می‌کنند.

Client درخواست خود را به Name Server محلی خود ارسال می‌کند. Name Server اگر پاسخ در خواست را داشته باشد به Client جواب می‌دهد، در غیر این صورت در خواست Client

را به یک Name Server دیگر می‌فرستد.

مراحل تحلیل این درخواست، در شکل ۳ـ۱۳ برای پیدا کردنIP آدرس www.microsoft.com نشان داده شده است.



شکل ۳ـ۱۳

مراحل شکل۳ـ۱۳ ، عملیات زیر را به تصویر کشیده‌اند :

۱ـ کلاینت(Client) درخواست forward برای www.microsoft.com را به سرور محلی خود ارسال می‌کند.

۲ـ سرور محلی ، درخواست را با بانک اطلاعاتی خود مقایسه می‌کند در صورتی که این درخواست قبلاً ثبت شده باشد و IP آن را یک بار جستجو کرده باشد، IP را به کلاینت بازمی‌گرداند اما اگر قبلاً این آدرس درخواست نشده باشد برای شناسایی قلمروی Top_level آن، درخواست را برای سرور ریشه (Root Server) ارسال می‌کند. بعد از بازگشت مشخص می‌کند قلمروی آن com.* است.

۳ـ سرور محلی، درخواست را به سرور com می‌فرستد. آدرس تحلیل و در پاسخ، Second_level، microsoft را برمی‌گرداند.

۴ـ سرور محلی این بار درخواست را به سرور microsoft ارسال می‌کند. با توجه به این که این آدرس در سرور microsoft ثبت گردیده، این سرور IP آن را برای سرور محلی برمی‌گرداند.

۵ ـ سرور محلی، IP را به کلاینت می‌فرستد.

۶ ــ Client، IP را دریافت کرده و در اختیار مرورگر خود قرار می‌دهد تا کاربر توسط آن به سایت مورد درخواست خود دسترسی پیدا کند.

نکته: Name Server Caching : وقتی که Name Server فرآیند جست‌وجو را انجام می‌دهد برای گرفتن پاسخ به چندین پرس و جو نیاز دارد به همین دلیل برای کاهش بار ترافیک شبکه، نتایج آنها را Cache می‌کند. این نتایج برای مدت زمان معینی با عنوان TTL (Time To live) نگهداری می‌شوند.

● ***Reverse lookup Query*** : درخواست‌های Reverse، IP را به نام تبدیل می‌کنند. معمولاً ابزارهای عیب‌یابی مانند دستور NSlookup از این سرویس برای برگشت گزارش به Client استفاده می‌کنند که در ادامه تشریح خواهد شد.

۴ــ۳ــ۱۳ــ Resource Records : بانک اطلاعاتی Zone، اطلاعات خود را به صورت رکورد ذخیره می‌کند. این رکوردها به صورت‌های متفاوتی، اطلاعاتی را نگه داری می‌کنند که مهمترین آنها عبارتند از :

● ***رکورد Host (A or AAAA)*** : رکورد نوع A بیشترین نوع رکوردی است که در DNS و برای اختصاص نام دامنهٔ یک کامپیوتر به آدرس IPv4 استفاده می‌شود. AAAA (خوانده شود quad ــ A) جهت تعریف رکورد برای کامپیوتر دارای آدرس IPv6 به کار می‌رود.

● ***رکورد Alias (CNAME)*** : به شما امکان می‌دهد که چندین نام را برای یک کامپیوتر خاص استفاده کنید. برای مثال سرورهای معروفی که به نام www نام گذاری شده‌اند اغلب از نوع CNAME هستند.

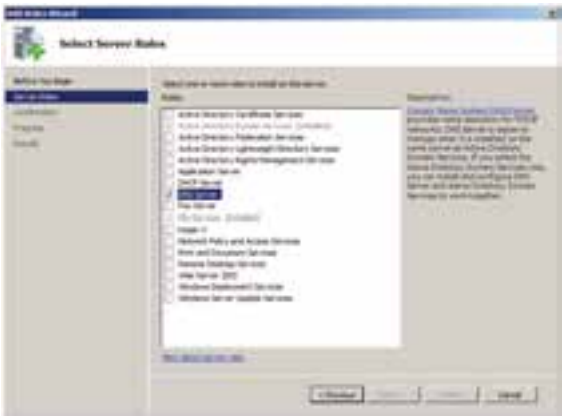
● ***رکورد Pointer(PTR)*** : رکورد نوع PTR در بخش Reverse استفاده می‌شود و به منظور اختصاص IP به نام دامنه یک کامپیوتر به کار می‌رود.

● ***رکورد Service location (SRV)*** : رکوردهای SRV برای پیدا کردن محل یک سرویس مشخص در دامنه مورد استفاده قرار می‌گیرد. برنامه‌های کاربردی مثل AD، توسط این نوع رکورد آدرس سرورهای مرتبط با خود را پیدا می‌کنند.

● ***رکورد NS*** : از این رکورد برای معرفی Name Server استفاده می‌شود. این رکورد قابل ایجاد به صورت دستی نمی‌باشد.

۴ـ۱۳ـ نصب و راه‌اندازی سرویس DNS

۱ـ۴ـ۱۳ـ نصب سرویس DNS : این سرویس به طور پیش فرض هنگام نصب AD، بر روی سرور نصب می‌شود این سرویس مخصوص AD نیست و برای DHCP و WINS نیز استفاده می‌شود و همچنین می‌توان آن را بر روی سرویس دهنده‌های Stand alone نیز نصب کرد. برای نصب مجزای این سرویس از ابزار Server Manager استفاده می‌شود. با انتخاب گزینه Add Roles دربخش Roles این برنامه، پنجره‌ای مطابق با شکل ۴ـ۱۳ ظاهر می‌شود.



شکل ۴ـ۱۳

گزینهٔ DNS Server را فعال و دکمهٔ Next را انتخاب کنید.

در پنجرهٔ بعدی توضیحاتی در مورد DNS و مفاهیم آن نمایش داده می‌شود. دکمهٔ Next را کلیک کنید.

در پنجرهٔ بعدی (شکل ۵ـ۱۳) با انتخاب دکمهٔ Install، فرآیند نصب DNS شروع می‌شود.

شکل ۵ـ۱۳

پس از پایان این فرآیند، ابزار DNS در مسیر Start→Administrative Tools قرار می‌گیرد. به این ترتیب سرور شما تبدیل به یک DNS Server (Name Server) شده است و می‌تواند به سرویس گیرنده‌ها برای اتصال به اینترنت و شبکه‌های دیگر سرویس دهی کند.

نکته: برای حذف DNS Server در پنجره Server Manager از منوی Action گزینه Remove Roles را انتخاب نموده و در ویزارد نمایش داده شده سرویس DNS را برای حذف انتخاب نمایید.

۲ـ۴ـ۱۳ـ ایجاد کردن Zone

: می‌خواهیم یک Zone به نام test.com ایجاد کنیم. مطابق با شکل ۶ـ۱۳، بر روی گزینه Forward Lookup zones کلیک راست کرده و گزینه New Zone را انتخاب کنید.

شکل ۶ـ۱۳

پنجره welcome ظاهر می‌شود دکمهٔ Next را کلیک کنید.

شکل ۷ـ۱۳

پنجرهٔ شکل ۸ــ۱۳ به نمایش درمی‌آید.

شکل ۸ــ۱۳

در این پنجره نوع Zone و نحوه ارتباط Zone با AD از ما سؤال می‌شود و چون از بحث این کتاب خارج است، حالت پیش فرض را انتخاب و گزینه ... Store the zone را غیر فعال کنید. سپس روی Next کلیک کنید.

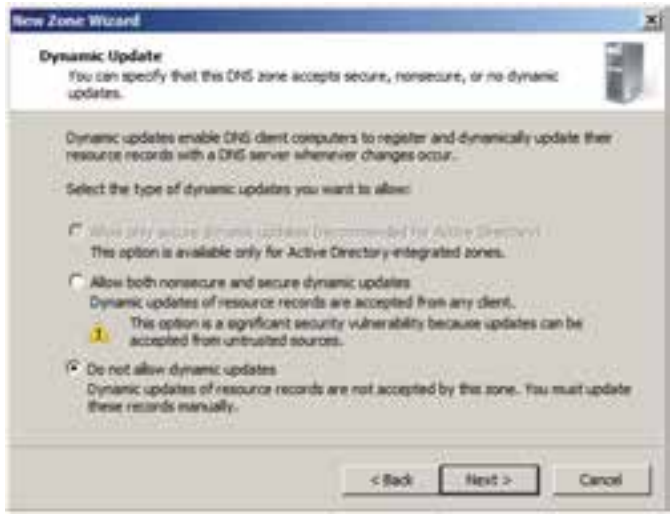
در پنجرهٔ بعد نام Zone از شما سؤال می‌شود، test.com را در کادر Zone name وارد کنید و روی دکمهٔ Next کلیک کنید. (شکل ۹ــ۱۳)

شکل ۹ــ۱۳

پنجرهٔ شکل ۱۰ــ۱۳ ظاهر می‌شود. در این پنجره نام پروندهٔ Zone، جهت ذخیرهٔ اطلاعات مربوط به آن از شما سؤال می‌شود. نام پیش فرض را قبول کرده و روی گزینه Next کلیک کنید.

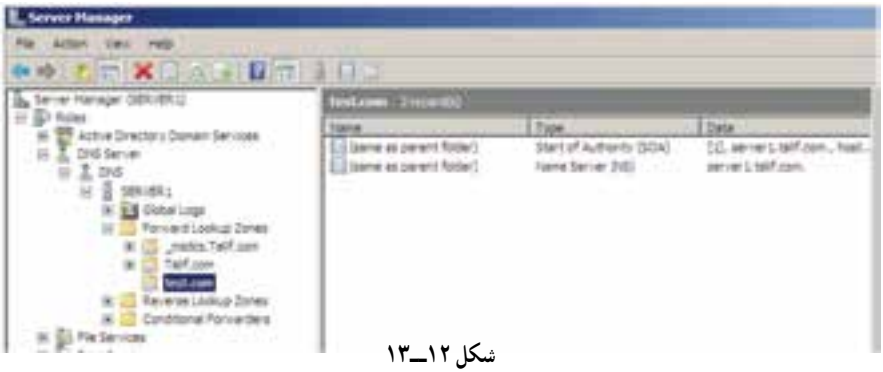
شکل ۱۰ــ۱۳

در پنجرهٔ بعدی نوع به روز رسانی اطلاعات مربوط به رکوردها سؤال می‌شود. حالت پیش فرض را تأیید کنید. (شکل ۱۱ــ۱۳)



شکل ۱۱ــ۱۳

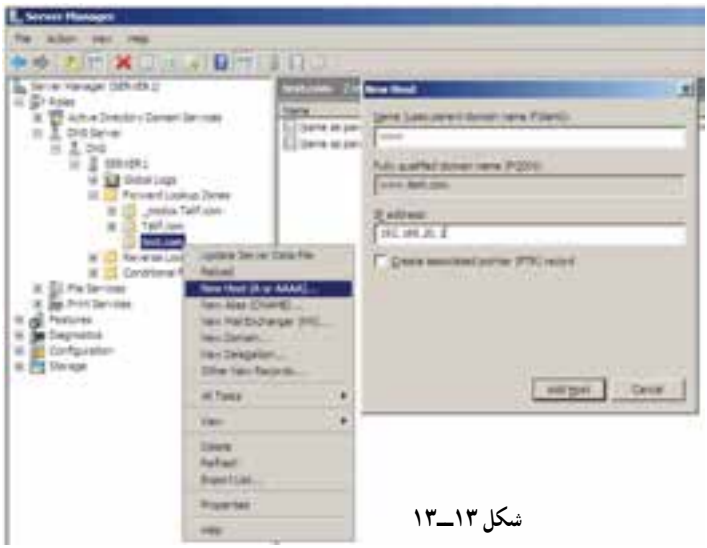
در پنجرهٔ آخر، خلاصه‌ای از مشخصات Zone تعریف شده نمایش می‌یابد. با تأیید آن، Zone به لیست بخش Forward Lookup Zones اضافه می‌شود. (شکل ۱۲ــ۱۳)



شکل ۱۲ــ۱۳

۳ــ۴ــ۱۳ــ ایجاد کردن Resource Record : برای ایجاد رکورد، بر روی Zone، test.com کلیک راست کرده و از منویی که ظاهر می‌شود گزینه New Host (A or AAAA) را انتخاب کنید.

در پنجره‌ای که باز می‌شود در قسمت Name، www و در قسمت IP address، IP سرویس دهندهٔ مورد نظر را وارد کنید. اگر می‌خواهید که برای این رکورد، یک رکورد PTR نیز به طور خودکار ایجاد شود گزینهٔ Cre ate associated pointer (PTR) record را فعال کنید. سپس دکمه‌ی Add Host را انتخاب کنید (شکل ۱۳ــ۱۳).

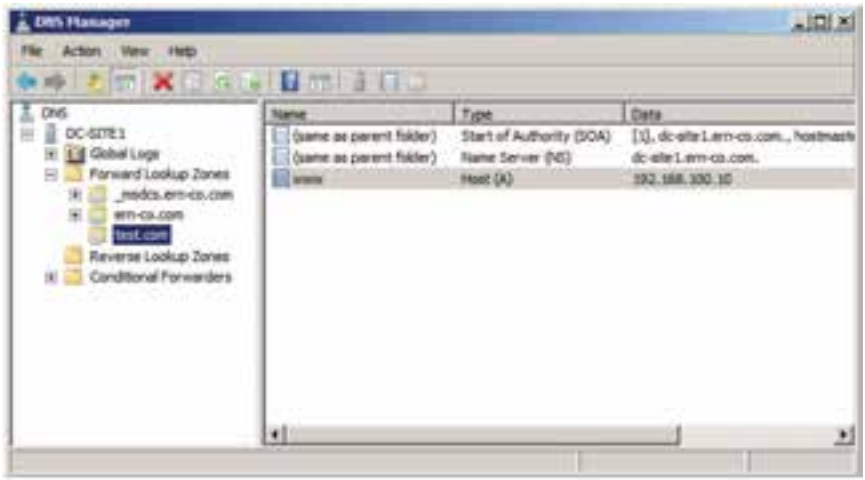


شکل ۱۳ــ۱۳

بعد از کلیک بر روی Add Host کادر تأیید شکل ۱۴ــ۱۳ ظاهر می‌گردد.

شکل ۱۴ــ۱۳

همان‌طور که درشکل ۱۵ــ۱۳ مشاهده می‌کنید، یک‌رکورد از نوع Host(A) با نام www در Zone، test.com ایجاد شده است.

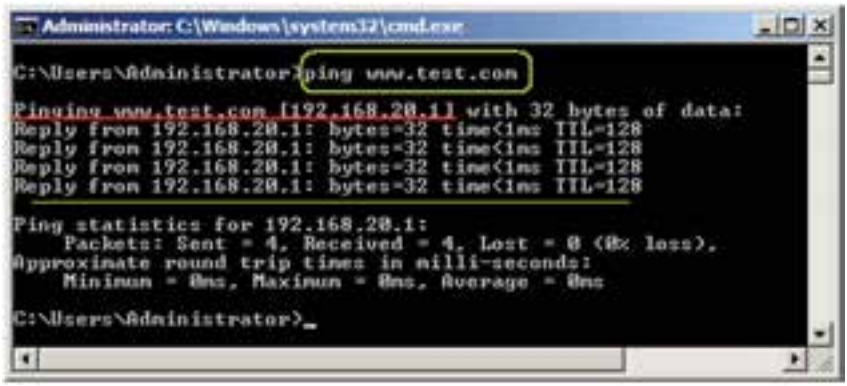


شکل ۱۵ــ۱۳

۴ــ۴ــ۱۳ــ تست کردن DNS برای انجام عمل Name Resolution :

می‌خواهیم یک درخواست (Query) به سرور DNS ارسال کنیم تا IP رکوردهای تعریف شده در بانک اطلاعاتی Zoneها را ببینیم. برای انجام این کار می‌توان از یکی از دو دستور زیر استفاده کرد :

□ **دستور ping** : با اجرای دستور ping www.test.com مطابق با شکل ۱۶ــ۱۳، مشاهده خواهید کرد که IP رکورد درخواست شده به شما نشان داده می‌شود.



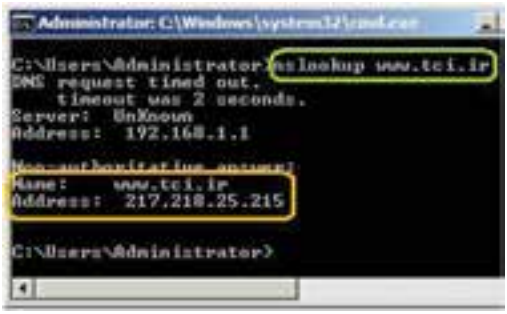
شکل ۱۶ــ۱۳

بعد از اجرای فرمان Ping اگر ارتباط بر قرار نباشد، پیغام خطای Ping request could find not host ظاهر می‌گردد.

□ **دستور nslookup** : فرمان nslookup را به دو صورت می‌توانید مورد استفاده قرار دهید.

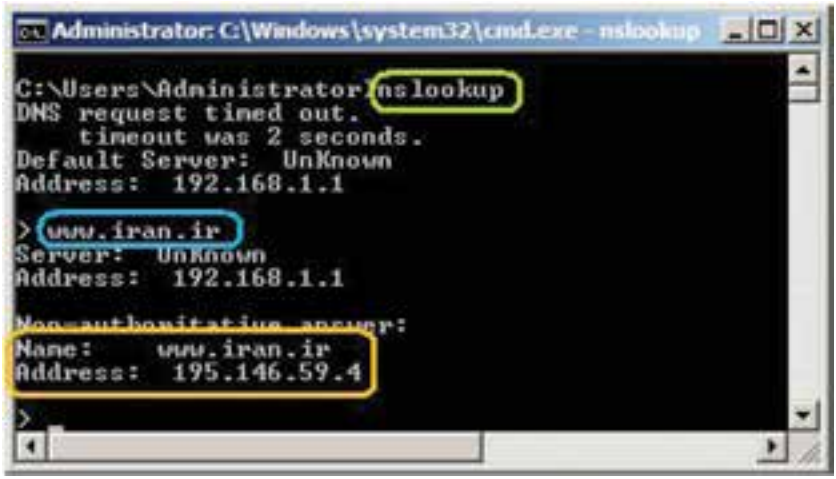
- ***Nslookup SiteName*** : مانند nslookup www.tci.ir

(البته زمانی می‌توانیدIP سایت‌های اینترنتی را پیدا کنید که به اینترنت متصل باشید.)



شکل ۱۷ــ۱۳

اجرای nslookup بدون پارامتر: پس از اجرای دستور nslookup اعلان فرمان به > تغییر می‌یابد. در این قسمت هر نامی‌را که وارد می‌کنید به سرور DNS پیش فرض ارسال می‌شود و IP آن را درخواست می‌کند. در صورت پیدا کردن رکورد معادل نام درخواستی، IP آن را نمایش می‌دهد (شکل ۱۸ــ۱۳).



شکل ۱۸ــ۱۳

خودآزمایی و پژوهش

۱ــ کاربرد سرویس DNS در شبکه را توضیح دهید.

۲ــ مفهوم هر یک از اجزای آدرس اینترنتی http://www.tvoccd.sch.ir را بنویسید.

۳ــ انواع Zone را نام برده و وظیفه هر یک را توضیح دهید.

۴ــ زمانی که سرویس‌دهنده IP,Local درخواست شده سرویس‌گیرنده را پیدا کرد به چه دلیل آن اسم و IP را در Cache کپی می‌کند؟

۵ــ فرمانی بنویسید که به وسیلهٔ آن بتوان Host,IP با نام http://www.tvoccd.sch.ir به‌دست آورد.

فصل چهاردهم

ابزارهای خط فرمان در ویندوز

هدف‌های رفتاری: هنرجو پس از پایان این فصل می تواند:

- فواید دستورات خط فرمان را بیان کند.
- کاربردهای دستورات خط فرمان را توضیح دهد.
- نصب Window's support tools را انجام دهد.
- بتواند با استفاده از Window's support tools روش استفاده از دستورات را پیدا کند.

فعالیت کارگاهی

۱ـ۱۴ـ دستورات خط فرمان

سیستم‌عامل ویندوز معمولاً درخواست‌ها و فرمان‌های کاربر را از طریق رابط گرافیکی یا GUI انجام می‌دهد. اما برخی ازاین دستورات را کاربران می‌توانند در بخش Start/Run یا محیط شبیه‌ساز DOS انجام دهند.

یکی از نکاتی که باید در مورد ابزارهای خط فرمان به آن توجه کرد این است که برخی از دستورات خط فرمان وجود دارد که دارای معادل گرافیکی نمی‌باشد. و تنها کاربر باید از طریق خط فرمان آنرا اجرا کند. دستورات خط فرمان با توجه به نوع عملکرد آن به چند بخش کلی تقسیم می‌شود. از بخش‌های عمده و اصلی آن می‌توان به ابزارهای مدیریت پرونده و پوشه، ابزارهای مدیریت سخت‌افزار، ابزارهای مدیریت اینترنت و شبکه، ابزارهای مدیریت سیستم و سرویس‌ها اشاره کرد.

نکته: برای مشاهده طبقه‌بندی تمامی دستورات خط فرمان به بخش Tools by Category برنامه Window's support tools مراجعه نمایید.

۲ـ۱۴ـ ابزارهای خط فرمان در TCP/IP

پس از پیاده‌سازی و برقراری ارتباط شبکه مابین سرویس‌گیرنده‌ها و سرور در ویندوز ایکس‌پی و سرور ابزارهای خط فرمان و برنامه‌های کمکی وجود دارند که کاربران و مدیران شبکه به‌وسیله آن می‌توانند بر شبکه نظارت داشته باشند و در صورت لزوم نسبت به رفع اشکال آن اقدام کنند. معمولاً در ویندوز سرور دستوراتی عمومی وجود دارند، که به‌راحتی قابل اجرا می‌باشد. اما برای نصب تمامی دستورات خط فرمان می‌توانیم برنامه Window's support tools را از روی سی‌دی ویندوز سرور پوشه Support نصب نماییم. بعد از نصب این برنامه تمامی دستورات خط فرمان به‌همراه راهنمای استفاده از آن بر روی سیستم‌عامل نصب می‌شود.

۱ـ۲ـ۱۴ـ Ping : از اصلی‌ترین و متداول‌ترین دستورات کمکی می‌باشد. با استفاده از این دستور می‌توان فعال بودن پروتکل TCP/IP را در شبکه بررسی نماییم. همچنین این امکان وجود دارد که وضعیت ارتباطی رایانه را با سایر رایانه‌های شبکه بررسی نماییم. از دیگر قابلیت‌های این دستور مشاهده آدرس IP و نام میزبان است. عملکرد برنامه Ping به این شکل است که ابتدا بسته داده‌ای به نام Echo request با استفاده از ICMP (Internet Control Message Protocol) به مقصد تعیین شده ارسال می‌کند. رایانه مقصد نیز به‌ازای هر درخواست دریافتی بسته داده‌ای به نام Echo Response را باز می‌گرداند. در این دستور اندازه هر بسته ارسالی برحسب بایت و زمان رفت و برگشت بسته برحسب ثانیه می‌باشد.

شکل دستور :

ping[-t] [-a] [-n Count] [-L Size] target- name

مثال : Ping 10.10.1.3

```
Pinging 10.10.1.3 with 32 bytes of data:
Reply from 10.10.1.3: bytes=32 time = 1ms TTL=255
Reply from 10.10.1.3: bytes=32 time = 1ms TTL=255
```

Reply from 10.10.1.3: bytes=32 time = 1ms TTL=255
Reply from 10.10.1.3: bytes=32 time = 1ms TTL=255
Ping statistics for 10.10.1.3:
Packets: Sent = 4, Received = 4, Lost = 0 (0%loss),
Approximate round trip times in milli - seconds:

با اجرای فرمان فوق ۴ بسته داده (Packet) با حجم ۳۲ بایت به‌طور متوالی به رایانه مقصد (target - name) ارسال می‌شود. و پاسخ آن دریافت می‌شود در مثال فوق زمان رفت و برگشت بسته داده ۱ میلی ثانیه می‌باشد. سپس گزارش این ارسال و دریافت اعلام می‌شود. در سه خط آخر این گزارش تعداد بسته‌های ارسالی و دریافتی به همراه بسته‌های اطلاعاتی که ارسال شده ولی دریافت نشده نشان داده می‌شود. اگر ارتباط مابین دو رایانه در شبکه بطور کامل برقرار باشد مقدار Packet Lost باید صفر باشد. (Lost =0 (0% loss در غیر اینصورت یک اشکال در ارتباط وجود دارد. همچنین در یک شبکه LAN ایده‌آل باید زمان رفت و برگشت بسته داده ۱ میلی ثانیه باشد.

پارامترها

t- : معمولاً ارسال بسته داده به مقصد چهار مرتبه انجام می گیرد اما اگر از پارامتر t استفاده نماییم عملیات ارسال بطور متوالی تکرار می‌شود. تا لحظه‌ای که کاربر آن‌را متوقف کند. اگر کاربر توسط کلیدهای CTRL + BREAK این کار را انجام دهد. آمار ارسال و دریافت نشان داده شده و مجدداً عملیات آغاز می‌شود. اما اگر توسط CTRL + C عملیات را متوقف کنیم. از برنامه Ping خارج می‌شویم.

a- : برای یافتن نام میزبان از روی آدرس آی پی استفاده می‌شود.

n- : برای مشخص کردن تعداد دفعات ارسال بسته داده

l- : برای تعیین کردن حجم بسته داده ارسالی برحسب بایت حداکثر این حجم می‌تواند ۶۵,۵۲۷ بایت باشد.

برای شناسایی وضعیت ارتباطی شبکه و رفع اشکال آن می‌توانیم از مراحل زیر استفاده کنیم :

۱ــ به آدرس میزبان محلی 127.0.0.1 بسته اطلاعاتی ارسال می کنیم. اگر پاسخ دریافت شد بدین معنی است که پروتکل TCP/IP بدرستی کار می کند.

۲ــ به آدرس IP تنظیم شده در کارت شبکه خود پینگ می‌نماییم. اگر پاسخی

دریافت نشد بدین معنا است که پیکربندی و TCP/IP مشکلی دارد.

۳ـ حال باید به یک آدرس IP محلی پینگ نماییم. اگر پاسخی دریافت شد به این معنی است که حداقل ارتباط لازم در شبکه وجود دارد. اما اگر این مرحله از آزمایش جواب نداد امکان دارد که مشکل سخت‌افزاری بین شما و شبکه (مثل کابلها یا پورت‌های سوئیچ) باشد. معمولاً در چنین شرایطی پیام Destination host unreachable ظاهر می‌شود. اما اگر پیکربندی آدرس‌ها اشکال داشته باشد. پیام Request time out ظاهر می‌شود.

۲ـ۲ـ۱۴ـ IPConfig : برای بررسی پیکربندی پروتکل TCP/IP از این دستور استفاده می‌شود. این دستور همه اطلاعات مربوط به پیکربندی کارت شبکه را در اختیار ما قرار می‌دهد. این اطلاعات شامل نام میزبان نام سرویس‌دهنده اولیه و ثانویه WINS و DNS و آدرس IP کارت شبکه و الگوی زیر شبکه Subnet Mask و آدرس دروازه اینترنت Default Gateway و آدرس فیزیکی کارت شبکه Mac Address و نام درایور کارت شبکه نشان داده می‌شود. در دستور زیر منظور از Adapter نام کارتی است که در Ipconfig نشان داده می‌شود.

ipconfig [/all] [/renew [Adapter]] [/release [Adapter]]

پارامترها

All : نام میزبان، نام کارت شبکه و آدرس فیزیکی به همراه وضعیت فعال یا غیرفعال بودن DHCP و آدرس DNS نمایش داده می‌شود.

Renew : با اجرای این فرمان آی پی دریافت شده از DHCP تجدید شده و آی‌پی جدید دریافت می‌شود.

Release : با اجرای این دستور آدرس آی پی پاک می‌شود.

مثال :

```
C:\>ipconfig
Windows IP Configuration
Host Name .....: My PC
Primary Dns Suffix .....:
Node Type .....: Unknown
IP Routing Enabled ..... : No
```

WINS Proxy Enabled .....: No

Ethernet adapter Local Area Connection 1:

. Connection - specific DNS Suffix:

Description .....: MyLan

Physical Address .....: 00-1A-4D-7C-F8-35

DHCP Enabled .....: No

IP Address .....: 192. 168.0.10

Subnet Mask .....:255.255.255.0

Default Gateway .....: 192.168.0.1

DNS servers.....: 192.168.0.1

۳ـ۲ـ۱۴ـ Tracert (Trace Route) : یکی دیگر از برنامه‌های مهم برای بررسی ارتباط با شبکه اینترنت می‌باشد. به این ترتیب که پس از اجرای این دستور می‌توان به هر دروازه Gateway مابین خودمان و یک آدرس IP پینگ نماییم. وقتی از این دستور استفاده می‌کنیم که با شبکه محلی ارتباط داشته باشیم، ولی با یک میزبان راه دور متصل نباشیم. به این وسیله می‌توانیم، مسیر را چک نماییم و ببینیم که کدام میزبان در طول مسیر به ما پاسخگو نیست. مورد استفاده دیگر این دستور برای بررسی کندی ارتباطات در شبکه است. زیرا این دستور زمان لازم برای دریافت پاسخ از هر دروازه را لیست می‌کند.

C:\>tracert 4.2.2.2

Tracing route to vnsc-bak. sys. gtei. net [4.2.2.2]

over a maximum of 30 hops :

1	ms <1 ms	< 1ms	[217.11.22.82]	
2	2ms	2ms	3ms	[172.16.25.1]
3	2ms	3ms	3ms	[80.75.1.25]
4	*	*	*	Request time out.
5	*	*	*	Request time out.
6	*	*	*	Request time out.
7	*	*	*	Request time out.

در مثال بالا آدرس 4.2.2.2 نام یکی از سرورهای اینترنت است. ارتباط ما تا مرحله سوم یعنی آدرس 80.75.1.25 برقرار است اما از آن به بعد ارتباط قطع می‌باشد. و بسته اطلاعاتی به آدرس 4.2.2.2 نمی‌رسد.

۴ــ۲ــ۱۴ــ Net : یکی از پرکاربردترین فرمان‌ها در شبکه می‌باشد. این فرمان در شبکه دارای سوئیچ‌های متعددی می‌باشد که به توضیح برخی از آنها می‌پردازیم :

Net Session *:* نام و IP رایانه‌هایی را که به سرور متصل هستند و از منابع اشتراکی سرور استفاده می‌کنند را نمایش می‌دهند.

net session [\\Computer Name] [/delete]

سوئیچ

Delete *:* اگر رایانه‌ای درحال خواندن اطلاعات از روی سرور باشد، با این فرمان ارتباط رایانه به سرور قطع می‌شود.

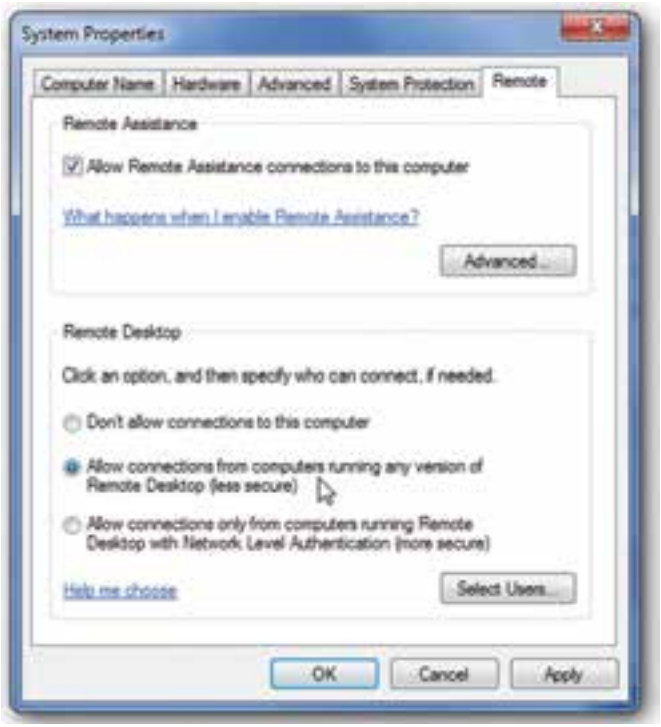
Net share *:* برای دیدن کلیه منابع اشتراک شده روی رایانه از این دستور استفاده می‌شود.

Net view *:* لیست کلیه رایانه‌های موجود در Domain را نشان می‌دهد.

۵ــ۲ــ۱۴ــ Mstsc (Remote desktop connection) : برای ایجاد ارتباط با میز کار یک ترمینال سرور یا رایانه راه دور از این دستور استفاده می‌کنیم. این دستور تصویری از محیط کار یک رایانه را در اختیار ما قرار می‌دهد. معمولاً مدیران شبکه برای تنظیم یا رفع اشکال سرورها از طریق شبکه اینترنت به آن‌ها متصل می‌شوند و تنظیمات موردنظر خود را انجام می‌دهند. به‌جای این‌که مستقیماً این کار را روی خود سرور انجام دهند. این دستور فقط بر روی سیستم عامل‌های ویندوز ۲۰۰۰ به بالا سازگار است. قبل از این‌که بخواهیم به رایانه راه دور متصل شویم باید تنظیمات زیر را انجام دهیم.

۱ــ ابتدا از بخش Remote desktop با توجه به امنیت مورد نیاز گزینه دوم یا سوم را فعال می‌نماییم (شکل ۱ــ ۱۴).

حال برای مجوز دادن به کاربرانی که می‌خواهیم از راه دور به این رایانه متصل شوند گزینه Select Users را انتخاب می‌کنیم (شکل ۲ــ ۱۴).



شکل ۱ــ۱۴

شکل ۲ــ۱۴

لازم به ذکر است که کاربر Administrator به طور پیش‌فرض انتخاب شده است و برای اضافه کردن نام سایر کاربران می‌توانیم گزینه Add را انتخاب کنیم.

mstsc.exe [/v:ServerName[:Port]] [/console] [/f] [/w:Width /h:Height]

نکته: پورت پیش‌فرض برای این سرویس ۳۳۸۹ می‌باشد. درصورتی که در فرمان مشخص نشود سیستم عامل از این پورت استفاده می‌کند.

mstsc.exe /v:192.168.0.1

سوئیچ‌ها

consol/ : اگر فرمان را بدون این سوئیچ استفاده نماییم، در هنگام ورود به ویندوز میز کار جدیدی برای ما باز می‌شود. اما با استفاده از این فرمان می‌توانیم آخرین میز کاری که از قبل اجرا شده است را ببینیم.

f/ : برای اجرای برنامه به صورت Full Screen از این سوئیچ استفاده می‌کنیم.

H/ و **w/** : ابعاد پنجره میز کار ویندوز را مشخص می‌کند W نشانگر عرض و H بیانگر طول صفحه نمایش می‌باشد.

پژوهش

۱ــ برنامه دیوار آتش ویندوز را برای این برنامه فعال نمایید.

۲ــ تفاوت دستور mstsc.exe با دستور tsmmc.msc در چیست؟ (در ویندوز سرور)

۶ــ۲ــ۱۴ــ Whoami (Who am I?) : این دستور نام دامنه، نام رایانه، نام کاربر، نام گروه‌هایی را که کاربر عضو آن‌ها می‌باشد نشان می‌دهد.

whoami [{/user | /groups | /priv} / all]

سوئیچ‌ها

User : برای نشان دادن نام کاربر به همراه نام دامنه

Groups : نام گروه‌هایی را که کاربر عضو آن می‌باشد نشان می‌دهد.

priv : مجوزهایی را که به کاربر داده شده است نشان می‌دهد. به‌عنوان مثال تغییر ساعت ویندوز، نصب و حذف برنامه‌ها، تغییرات در تنظیمات شبکه

۷ــ۲ــ ۱۴ــ Getmac : برای نشان دادن آدرس فیزیکی کارت شبکه به همراه لیستی از پروتکل‌های شبکه‌ای که به کارت شبکه مربوط می‌شود. آدرس فیزیکی ۱۲ طول دارد که کارکتر بر مبنای هگزا دسیمال می‌باشد که توسط خط تیره از هم جدا می‌شوند (00-15-18-00-04-F9). آدرس فیزیکی تجهیزات شبکه منحصر به فرد بوده و تکراری نیست.

getmac.exe [/***s*** Computer [/***u*** Domain\ User [/***p*** Password]]]

مثال getmac

Physical Address Transport Name

Disabled Disconnected

00-15-18-00-04-F9 \Device\ Tcpip_{2B3BABC4-80CA-411B-846C-23868F2685F2}

سوئیچ‌ها

/s : برای مشخص کردن نام رایانه یا آدرس آی‌پی

/u : برای مشخص کردن نام کاربر به همراه نام دامنه

/p : برای مشخص کردن کلمه عبور معمولاً این سوئیچ به همراه سوئیچ u استفاده می‌شود و مورد استفاده آن زمانی می‌باشد که بخواهیم آدرس فیزیکی یک رایانه راه دور را ببینیم. به همین دلیل باید نام کاربری و کلمه عبور رایانه راه دور را داشته باشیم.

پژوهش

آیا آدرس فیزیکی قابل تغییر است؟ چگونه؟

۳ــ۱۴ــ ابزارهای خط فرمان برای مدیریت ویندوز سرور

۱ــ۳ــ۱۴ــ System File Checker (sfc): این دستور نسخه و صحت کلیه پرونده‌های سیستمی ویندوز را از روی سی‌دی ویندوز بررسی می‌کند و اگر مغایرتی بین این پرونده‌ها پیدا کند آن‌را مجدداً از روی سی‌دی کپی می‌کند و آن‌را اصلاح می‌کند.

sfc [/scannow]

سوئیچ scannow/ : این دستور تمامی پرونده‌هایی را که توسط ویندوز محافظت می‌شود بلافاصله اسکن می‌نماید.

۲ــ۳ــ۱۴ــ Systeminfo : گزارش کاملی از کلیه تجهیزات سخت‌افزاری و سیستم عامل نشان می‌دهد.

خودآزمایی و پژوهش

۱ــ فرمانی Ping را به‌نحوی اجرا کنید که حجم بسته اطلاعاتی که به مقصد ارسال می‌شود ۳۰۰۰ بایت باشد. و فقط ۱۰ مرتبه این عمل را انجام دهد.

۲ــ به‌طور همزمان چند کاربر می‌توانند به‌صورت Remote به ویندوز ایکس پی یا سرور متصل شوند.

۳ــ دو روش برای خواندن آدرس فیزیکی بنویسید.

۴ــ تحقیق کنید تفاوت Remote Assistance با Remote Desktop در چیست؟

فصل پانزدهم

DHCP Server مقدماتی

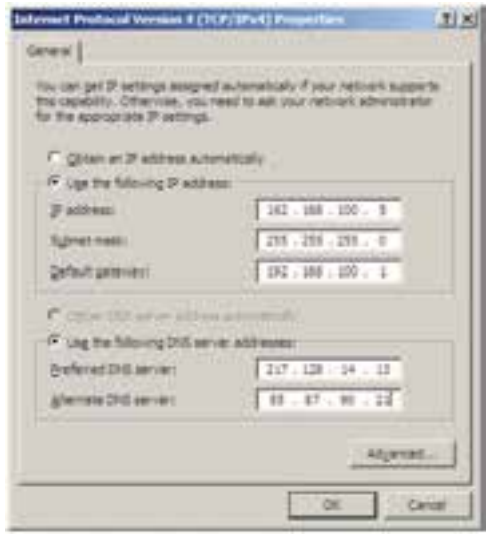
هدف‌های رفتاری: هنرجو پس از پایان این فصل می تواند:

- فواید DHCP Server را بیان کند.
- اجزای DHCP را توضیح دهد.
- حالت‌های مختلف قرارگیری DHCP Server در شبکه را شرح دهد.
- نصب DHCP Server را انجام دهد.
- پیکربندی DHCP Server را شرح دهد.
- پیکربندی DHCP Server را انجام دهد.
- Backup/Restore از اطلاعات DHCP Server نسخه پشتیبان گرفته و جایگزین نماید.
- عیب یابی DHCP را انجام دهد.

۱ـ۱۵ـ کاربرد DHCP Server[۱]

زمانی که شما می‌خواهید به یک شبکه محلی Workgroup متصل شوید، باید آدرس IP رایانه شما با آدرس IP شبکه در یک کلاس باشد. یعنی باید IP Address و Subnet Mask متناسب با رایانه‌های دیگر شبکه تنظیم شده باشد و یا اگر بخواهید با استفاده روتر(مانند مودم ADSL) به شبکه دیگری (مانند اینترنت) متصل شوید، باید Default Gateway که همان آدرس IP روتر می‌باشد را نیز تنظیم نمایید و برای متصل شدن به یک Domain باید آدرس IP سرور DNS را نیز تنظیم نمایید.(مانند شکل ۱ـ ۱۵ که برای تنظیمات IPv4 می‌باشد).

۱ـ Host Conf gurat on Protoco Dynam c



شکل ۱ــ۱۵

همانطور که در شکل ۱ــ۱۵ ملاحظه می‌کنید، انجام تنظیمات فوق به صورت دستی، به دقت و زمان زیادی نیاز دارد. لازم به ذکر است تنظیمات فوق برای تک تک رایانه‌های موجود در شبکه باید انجام بگیرد که کار طاقت فرسایی است. در صورت کوچک‌ترین اشتباه، امکان تداخل و عدم اتصال به شبکه به وجود خواهد آمد. برای حل مشکل مطرح شده از سرویس DHCP (پروتکل پیکربندی پویا یا دینامیکی میزبان) می‌توان استفاده نمود. سرویس DHCP پروتکلی است که اجازه می‌دهد به صورت متمرکز پیکربندی آدرس IP و دیگر تنظیمات TCP/IP میزبان‌های(Host) شبکه به صورت خودکار و پویا انجام شده و کاربران شبکه را از پیکربندی دستی آدرس‌های IP بی نیاز می‌کند. با استفاده از DHCP شما آدرس IP را به یک یا چند میزبان شبکه برای مدت زمانی خاص اجاره می‌دهید.

مزایای DHCP در ویندوز ۲۰۰۸ سرور

- قابل پیکربندی است، یعنی با استفاده از DHCP مشکل تداخل[۱] IPها به وجود نمی‌آید.
- کاهش زمان مدیریت پیکربندی و امکان تنظیم مجدد آدرس‌های IP
- استفاده مجدد از آدرس‌های IP پس از اتمام زمان مشخص شده
- کلاینت‌ها برای استفاده از تنظیمات جدید DHCP سرور نیازی به راه‌اندازی دوباره ندارند.
- علاوه بر آدرس Unicast از آدرس Multicast نیز پشتیبانی می‌کند.

۱ــ IP Conf ct

معایب استفاده از DHCP

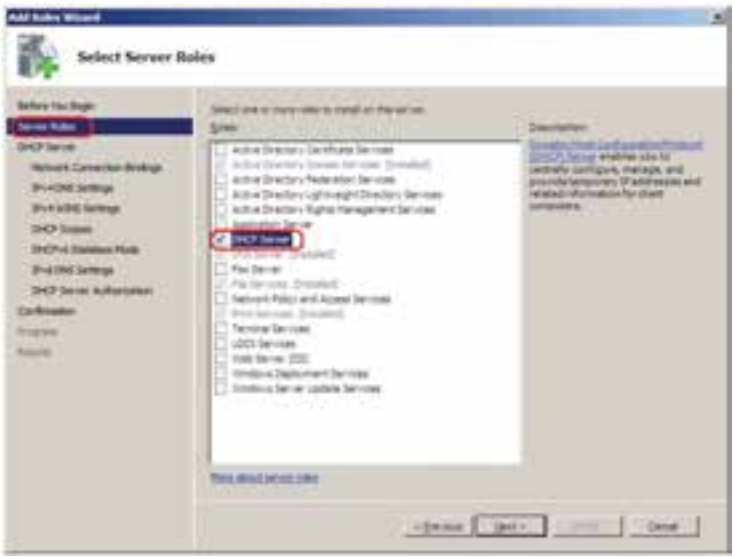
- مشکل امنیتی (رایانه غیر مجاز هم می‌تواند از سرور درخواست IP داشته باشد[1]).
- در صورت خرابی سرویس DHCP تخصیص آدرس IP به کلاینت‌ها با شکست مواجه خواهد شد.
- افزایش ترافیک شبکه به خاطر ارتباط کلاینت با سرویس دهنده DHCP اتفاق خواهد افتاد.

فعالیت کارگاهی

۲ـ۱۵ـ نصب سرویس DHCP Server

قبل از شروع به نصب باید کارت شبکه‌ای را که قرار است برای سرویس دهنده DHCP استفاده کنید با یک آدرس IP دستی یا استاتیک تنظیم نمایید.

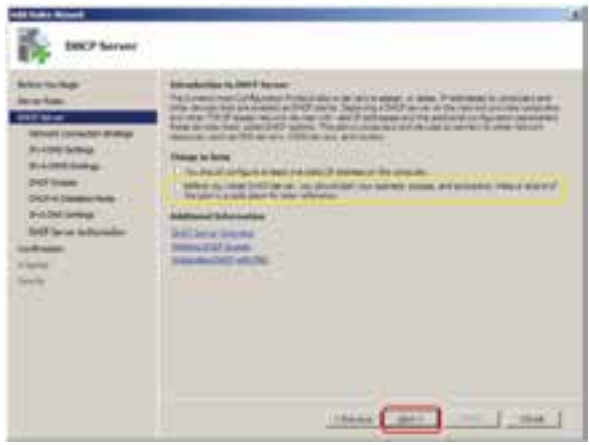
برای نصب این سرویس، از ابزار Server Manager استفاده می‌شود. با انتخاب گزینهٔ Add Roles دربخش Roles این برنامه، پنجره‌ای مطابق با شکل ۲ـ۱۵ ظاهر می‌شود. گزینه DHCP Server را فعال و دکمهٔ Next را انتخاب کنید.



شکل ۲ـ۱۵

۱ـ البته برای حل این مشکل ابزاری به نام DHCP Se ver Ca out DLL برای فیلتر کردن درخواست‌ها وجود دارد که توسط شرکت مایکروسافت در سال ۲۰۰۷ ارائه شده است. البته در W ndows Se ver 2008 R2 به طور پیش فرض نصب می‌شود.

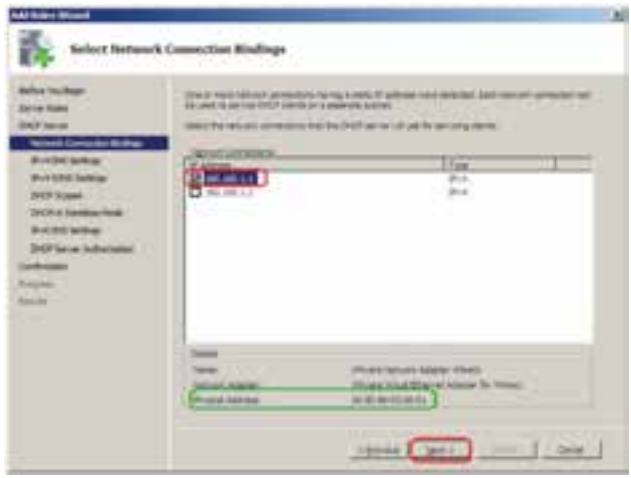
پنجرهٔ بعدی DHCP Server را معرفی می‌کند و تأکید شده است که قبل از نصب باید برای کارت شبکه آدرس IP استاتیک (دستی) در نظر بگیرید (شکل ۳ــ۱۵ کادر زرد رنگ).



شکل ۳ــ۱۵

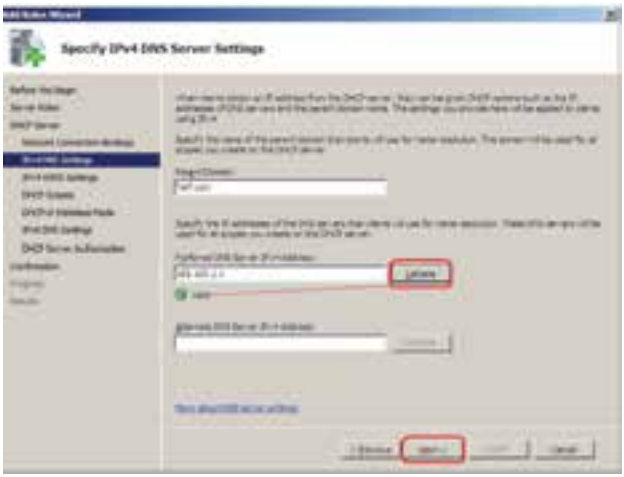
برای ادامه نصب دکمهٔ Next را انتخاب کنید.

در پنجرهٔ بعدی (شکل ۴ــ۱۵) IP کارت شبکه‌ای را انتخاب کنید که می‌خواهید سرور DHCP برای سرویس دهی به سرویس گیرنده‌ها از آن استفاده کند. پس از انتخاب آن، دکمهٔ Next را کلیک کنید. ضمناً در این پنجره آدرس فیزیکی کارت شبکه(MAC Address) نمایش داده می‌شود (کادر سبز رنگ در شکل ۴ــ۱۵).



شکل ۴ــ۱۵

در پنجرهٔ شکل ۵ــ۱۵، نام دامنه یا Domain و IP سرور DNS را تعیین کنید. ضمناً برای مطمئن شدن از درست بودن آدرس DNS بر روی دکمه Validate کلیک کنید تا کلمه Valid ظاهر شود.

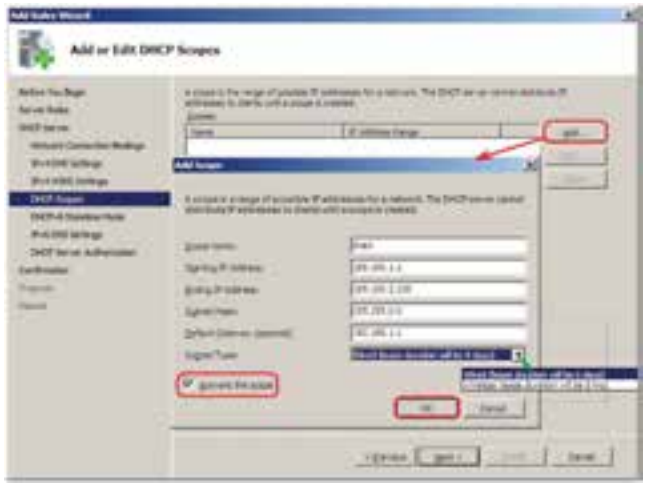


شکل ۵ــ۱۵

سپس روی دکمهٔ Next کلیک کنید. در پنجره‌های بعدی تنظیمات مربوط به WINS Server را می‌توان انجام داد. WINS Server جهت پشتیبانی از سرویس گیرنده‌های دارای سیستم عامل‌های قبل از ۲۰۰۰ به کار می‌رود. حالت پیش فرض را تأیید نمایید. (عدم استفاده از WINS Server)

شکل ۶ــ۱۵

در پنجره شکل ۷ــ۱۵ باید محدودهٔ (Scope) آدرس‌دهی IP مربوط به شبکه خود را تعیین کنید. با زدن دکمهٔ Add، پنجرهٔ جدیدی باز می‌شود که تنظیمات زیر را مطابق با شکل ۷ــ۱۵ می‌توان در آن پیکربندی کرد.



شکل ۷ــ۱۵

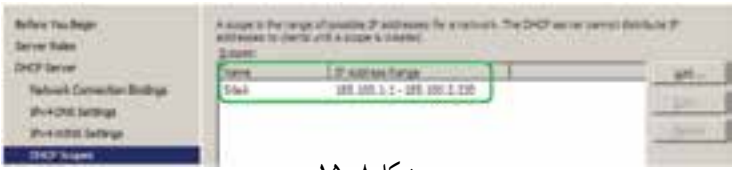
اجزای کادر Add Scope عبارت‌اند از :

- **Scope Name** : نام محدوده IP، که می‌تواند یک عبارت توصیفی کوتاه برای محدودهٔ قابل تعریف باشد و نوشتن آن الزامی‌است.(مثلاً SiteA)
- **Starting IP address** : شروع محدودهٔ آدرس IP برای DHCP
- **Ending IP address** : پایان محدودهٔ آدرس IP برای DHCP
- **Subnet mask** : این کادر بر اساس کلاس IP وارد شده، به طور خودکار تنظیم می‌شود. چون محدوده آدرسی که وارد شده است کلاس B می‌باشد Subnet Mask نیز برابر 255.255.0.0 خواهد بود.
- **Default gateway** : در صورت وجود دستگاهی مثل روتر در شبکه، که سرویس گیرنده‌ها به واسطهٔ آن با شبکه‌های دیگر، ارتباط پیدا می‌کنند، IP آن را در این کادر وارد کنید.
- **Subnet type** : بر اساس نوع شبکه (سیمی یا بی‌سیم) تنظیم می‌شود و مدت زمان اجاره (Lease Duration) IP به یک میزبان را تعیین می‌کند. این زمان برای شبکه بی‌سیم ۸ روز و برای شبکه سیمی ۵ روز می‌باشد.

Lease Duration مدت زمان اجاره آدرس IP به یک سرویس گیرنده از طرف سرویس دهنده DHCP می‌باشد به طوری که بعد از گذشت نصف زمان تعیین شده، درخواست مجددی از طرف سرویس گیرنده به سرویس دهنده DHCP برای تمدید مدت اجاره ارسال می‌شود چنانچه بعد از گذشت زمان تعیین شده، درخواستی از طرف سرویس گیرنده ارسال نشود، آن آدرس IP به سرویس گیرنده دیگری واگذار می‌شود.

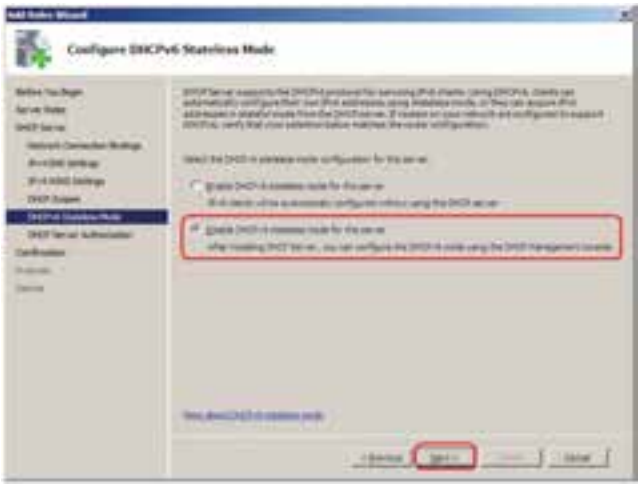
- **Active this scope** : درصورت فعال بودن این گزینه، پس از نصب DHCP، محدوده تعیین شده IP فعال خواهد شد.

تنظیمات را انجام داده و دکمهٔ OK را کلیک کنید. مشخصات Scope تعریف شده در لیست نمایش می‌یابد (شکل ۸ــ۱۵).



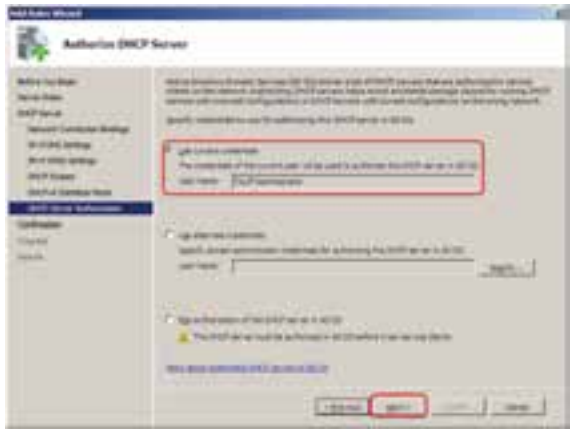
شکل ۸ــ۱۵

دکمهٔ Next را کلیک نمایید. در پنجرهٔ بعدی تنظیمات مربوط به IPv6 سؤال می‌شود. می‌توانید آن را فعال(Enable) یا غیر فعال (Disable) کنید البته بعد از نصب هم با توجه به ضرورت می‌توانید آن را تغییر دهید برای ادامه کار گزینه ... Disable را انتخاب کرده و دکمه Next را کلیک کنید.



شکل ۹ــ۱۵

در پنجره شکل ۱۰ــ ۱۵، باید نام کاربری را مشخص کنیم که برای مجاز کردن سرویس‌دهی DHCP در محیط AD مجوز لازم را دارد. این عمل را اصطلاحاً Authorize می‌گویند.



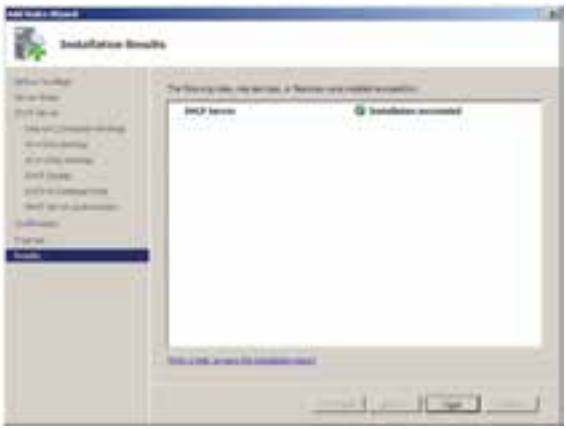
شکل ۱۰ــ۱۵

نکته۱: عمل Authorize را وقتی انجام می‌دهیم که DHCP Server در محیط AD قرار داشته باشد. این عمل را می‌توان بعد از نصب DCHP نیز انجام داد. برای این کار بر روی نام سرور در برنامهٔ DHCP کلیک راست کرده و سپس گزینه Authorize را انتخاب کنید.

با کلیک دکمه Next، پنجرهٔ شکل ۱۱ــ۱۵ ظاهر می‌شود که تنظیمات انجام گرفته در حین نصب سرویس DHCP را نمایش می‌دهد. با انتخاب دکمهٔ Install، این سرویس نصب می‌شود.

شکل ۱۱ــ۱۵

در پایان نصب شکل ۱۲ــ۱۵ ظاهر می‌گردد. بر روی دکمه Close کلیک نمایید.

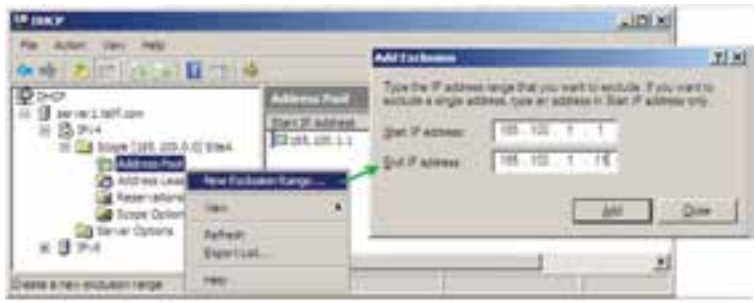


شکل ۱۲ــ۱۵

با انتخاب گزینهٔ DHCP از طریق مسیر Start→Administrative Tools، کنسول DCHP مطابق با شکل ۱۳ــ۱۵ باز می‌شود که می‌توان Scope تعریف شده را به همراه تنظیمات آن مشاهده کرد.

شکل ۱۳ــ۱۵

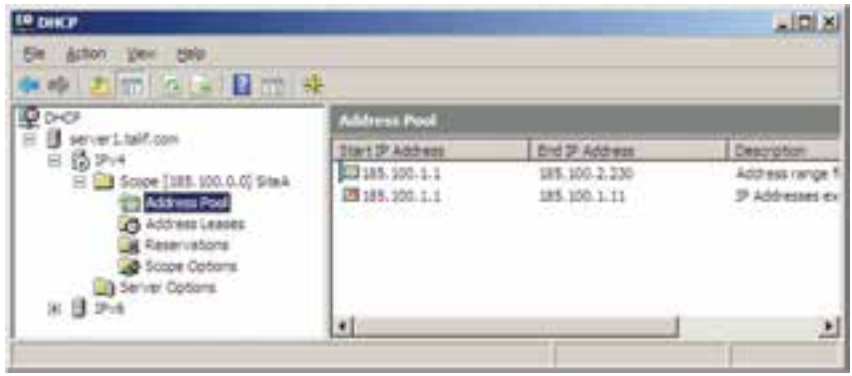
نکته۲: در صورتیکه بخواهید یک یا چند آدرس IP را که در محدودهٔ آدرس‌های DCHP تعریف شده است را برای کاربردهای خاص، به سرویس گیرنده‌ها اختصاص ندهید، باید آنها را فیلتر کنید. برای این کار برروی گزینهٔ Address Pool کلیک راست کرده و گزینهٔ New Exclusion Range را انتخاب کنید. سپس در پنجره ای که باز می‌شود IP یا محدودهٔ IP مورد نظر را خود وارد کنید. در شکل ۱۴ــ۱۵ فرض شده است ما می‌خواهیم ۱۰ آدرس اول را به سرویس گیرنده‌ها اختصاص ندهیم.



شکل ۱۴ــ۱۵

در Scope تعریف شده موارد زیر قابل مشاهده است :

■ **Address Pool** : محدودهٔ آدرس‌هایی که می‌تواند به سرویس گیرنده‌ها داده شود و همچنین آدرس‌هایی که نباید داده شود را نمایش می‌دهد (شکل ۱۵ــ۱۵).



شکل ۱۵ــ۱۵

■ **Address Leases** : آدرس‌هایی را که تاکنون سرویس گیرنده‌ها از سرویس دهنده گرفته‌اند را به همراه مشخصات سرویس گیرنده نمایش می‌دهد.

■ **Reservations** : اگر می‌خواهید آدرس مشخصی را برای یک سرویس گیرنده به طور دائمی‌اختصاص دهید می‌توانید از این ویژگی استفاده کنید. برای این کار، IP مشخصی از محدودهٔ تعریف شده را برای یک کارت شبکه تعریف کنید. برای مثال ما می‌خواهیم آدرس IP، 180.100.100.100 را به رایانه‌ای که آدرس فیزیکی[1] (Mac Address) آن برابر 00ــ3Eــ4Aــ01ــD4ــB8 می‌باشد.

۱ــ برای پیدا کردن آدرس فیزیکی کارت می‌توانید از دستور pconf g /a در Command Prompt استفاده نمایید.

بدین صورت که بر روی گزینه Reservation کلیک راست کرده و سپس گزینه New Reservation ... را انتخاب کنید. در پنجره ای که مطابق شکل ۱۶ــ۱۵ باز می‌شود، IP و Physical Address کارت شبکهٔ مورد نظر را وارد کنید.

شکل ۱۶ــ۱۵

نکته۳: ویژگی ذخیرهٔ IP، نمی‌تواند به عنوان روش جایگزین آدرس‌دهی ثابت برای رایانه‌های سرویس دهنده مثل سرویس دهنده DNS باشد بلکه بهتر است برای رایانه‌هایی استفاده شود که حضورشان در شبکه الزامی نیست.

اگر بخواهید تغییراتی را در Scope تعریف شده، اعمال کنید، بر روی آن کلیک راست کرده و گزینهٔ Properties را انتخاب کنید. سپس مطابق با شکل ۱۷ــ۱۵ پارامترهای آن را تغییر دهید.

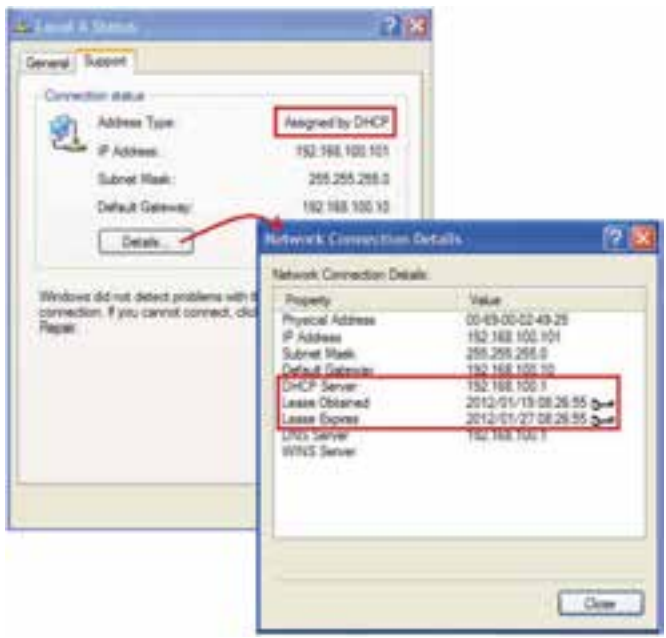
شکل ۱۷ــ۱۵

در پنجره ۱۷ـ۱۵ می‌توان محدودیت زمانی را کم یا زیاد نمود و یا این که با انتخاب گزینه Unlimited محدودیت زمانی را از محدوده تعیین شده حذف نمایید.

در صورتی که بخواهید Scope جدیدی در کنسول DHCP بسازید، بر روی گزینه IPv4 کلیک راست نمایید و گزینهٔ New Scope را انتخاب کنید. سپس در پنجره‌ای که ظاهر می‌شود تنظیمات مورد نظر را انجام دهید.

۳ـ۱۵ـ تنظیم سرویس گیرنده

برای تنظیم سرویس گیرنده، جهت دریافت اطلاعات آدرس IP از سرویس دهنده DHCP، باید در کادر محاوره ای Internet Protocol (TCP/IP) Properties مربوط به کارت شبکه، گزینهٔ Obtain an IP address automatically را انتخاب کنید. همچنین جهت دریافت اطلاعات مربوط به سرور DNS، گزینهٔ Obtain DNS server address automatically را فعال نمایید. پس از تأیید می‌توان تنظیمات دریافتی را مطابق با شکل ۱۸ـ۱۵ مشاهده کرد.



شکل ۱۸ـ۱۵

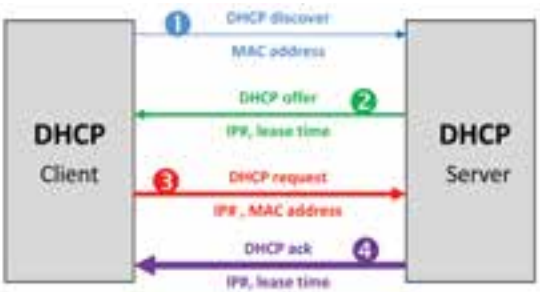
اگر سرویس گیرنده، قبل از نصب DHCP به روی حالت خودکار تنظیم شده باشد، از IP ، APIPA[1] استفاده می کند بنابراین برای دریافت تنظیمات از سرور DHCP جدید فقط کافی است مجدداً، تنظیمات را دریافت کند . برای این کار می‌توانید از دستور IPConfig /Renew استفاده کنید و یا سیستم را مجدداً راه اندازی نمایید.

نکته: عمل دریافت تنظیمات IP از سرور DHCP توسط سرویسی به نام DHCP Client انجام می گیرد. بدیهی است که این سرویس باید بر روی سرویس گیرنده‌ها فعال باشد . این سرویس به‌طور پیش فرض در حالت Started قرار دارد و جهت دسترسی به آن می‌توان از کنسول سرویس‌ها (Services.msc) استفاده کرد.

۴ـ۱۵ـ تشریح عملکرد DHCP

وقتی که یک کاربر رایانه خود را راه اندازی می کند سیستم عامل آن بعد از بالا آمدن در خواست IP می‌کند و آن را از سرویس دهنده DHCP دریافت می‌کند . به طوری که این درخواست و دریافت به ترتیب در طی چهار مرحله تکمیل می‌شود :

- **DHCP Discover** : در این مرحله کلاینت پیغام DHCP Discover خود را جهت دریافت IP در شبکه Broadcast می کند. در این حالت آدرس IP کلاینت به صورت 0.0.0.0 خواهد بود.
- **پیشنهاد IP از طرف سرور DHCP یا DHCP Offer** : در این مرحله تمام سرویس‌دهنده‌های DHCP از محدوده آدرس IP تعریف شده بر روی خود یک IP انتخاب نموده و به



شکل ۱۹ـ۱۵

۱ـ Automat c Pr vate Ip Address ng به تخصیص Ip address به طور خودکار و تصادفی در محدوده 69.254.x.y گفته می‌شود.

همراه مدت زمانی که قرار است آن IP را در اختیار کلاینت قرار دهد (پیغام DHCP Offer) و آن را به صورت شکل ۱۹ـ۱۵ ارسال می‌کند.

که در آن IP# : شماره آدرس IP می‌باشد.

■ **درخواست برای تأیید IP پیشنهادی یا DHCP Request** :کلاینت درخواست کننده پس از دریافت IP های پیشنهادی، اولین IP پیشنهادی را انتخاب نموده و آن را توسط یکPacket در شبکه Broadcast می‌کند و در آن Packet آدرس سرویس دهنده DHCP را که پیشنهاد او قبول شده است مشخص می‌نماید.

■ **تأیید درخواست IP با پیغام DHCP Ack** : پس از آنکه سرویس گیرنده بهDHCP Serverکه پیشنهاد او قبول شده DHCP Request را فرستاد در صورتیکه هنوز IPکه پیشنهاد شده در محدوده یا رنج IPهای سرویس دهنده DHCP وجود داشته باشد و توسط Admin حذف نشده باشد DHCP Server تأیید خود را مبنی بر اختصاص IP به سرویس گیرنده با پیامDHCP ack اعلام می‌کند. ولی اگر IP توسط Admin از محدوده مربوطه حذف شده باشد سرویس دهنده DHCP به کلاینت درخواست کننده پیغام DHCP Nack را ارسال می‌کند و Client مجبور می‌شود که تمام مراحل را دوباره طی کند.

خودآزمایی و پژوهش

تمرین ۱ : DHCP را روی سرویس دهنده نصب و راه اندازی کرده و آدرس IP را از کلیه رایانه‌های سرویس‌گیرنده پاک کرده و آن را به صورت اتوماتیک فعال کنید. سپس آزمایش کنید که آیا رایانه از سرویس دهنده IP دریافت کرده یا نه ؟

به دو روش یکی به صورت Command line دوم : از طریق نشانه شبکه روی نوار وظیفه

پژوهش : چگونه می‌توان یک IP خصوصی را برای یک سرویس‌گیرنده رزرو نمود؟

تمرین ۲ : چگونه می‌توان از روی سرویس دهنده IP و Mac Address یک سرویس گیرنده را پیدا کرد؟

پیوست‌ها

پیوست ۱ــ سیاست‌های امنیتی کاربران

معمولاً بعد از نصب Active Directory سیستم عامل سیاست‌های امنیتی خاصی را برای حساب‌های کاربران و گذرواژه آن‌ها تعریف می‌کند. که در بخش Administrative Tools/Security Setting/Account policies قرار دارد. که در این تعریف چگونگی تعامل کاربران با رایانه‌ها و دامین مشخص می‌شود. در ضمن باید برای ثبت تغییرات policyدر سیستم عامل، رایانه را راه‌اندازی مجدد نمایید یا در خط فرمان دستور gpupdateرا بنویسید و اجرا کنید.

۱ــ۱ــ سیاست‌های گذرواژه Password policy

سیاست‌های گذرواژه برای حساب‌های کاربران دامین یا کاربران محلی استفاده می‌شود. این سیاست‌ها وظیفه تصمیم‌گیری تنظیمات گذرواژه مانند طول عمر و چگونگی عملکرد آن برروی کاربران را دارند.

۱ــ۱ــ۱ــ Enforce password history : این بخش کاربران را مجبور می‌کند که در هنگام تعویض کلمه عبور حتماً گذرواژه جدید و منحصر وارد نمایند. یعنی کاربران اجازه ندارند کلمه عبورهای قبلی خود را استفاده نمایند. تعداد گذرواژه‌هایی که می‌توان در این بخش تعریف نمود، حداکثر ۲۴ می‌باشد.

۲ــ۱ــ۱ــ Maximum password age : در این بخش طول عمر یا حداکثر زمان اعتبار کلمه‌های عبور را می‌توان برحسب روز تعریف کرد. یا به عبارت دیگر اگر مقدار این قسمت ۵ روز باشد. همه کاربران باید بعد از ۵ روز کلمه عبور خود را تغییر دهند. حداکثر مقدار تعریف شده در این قسمت می‌تواند ۹۹۸ روز باشد.

۳ــ۱ــ۱ــ Minimum password age : در این بخش حداقل طول عمر یا زمان اعتبار کلمه‌های عبور را می‌توان برحسب روز تعریف کرد. یا به عبارت دیگر اگر مقدار این قسمت ۵ روز باشد. هیچ کاربری اجازه ندارد زودتر از ۵ روز کلمه عبور خود را تغییر دهد. در هنگام تنظیم این بخش باید توجه داشت که این مقدار باید کمتر از حداکثر طول عمر کلمه عبور باشد. حداقل مقدار تعریف شده

در این قسمت می‌تواند ۹۹۸ روز باشد.

۴ــ۱ــ۱ــ Minimum password length : در این بخش حداقل طول کلمه عبور تعیین می‌شود این مقدار حداکثر ۱۴ می‌تواند باشد.

۵ــ۱ــ۱ــ passwords must meet complexity requirements : در این بخش می‌توانیم پیچیدگی کلمه عبور را فعال یا غیرفعال نماییم. پیچیدگی در کلمه عبور به این معنا می‌باشد که کاربر نمی‌تواند از حروف ساده یا اعداد برای کلمه عبور استفاده کند. مانند abcd – 123456 با فعال شدن این بخش باید موارد زیر را در تعیین کلمه عبور درنظر داشته باشیم :

کلمه عبور نباید همان نام کاربری یا بخشی از آن باشد.

باید حداقل ۶ حرف طول داشته باشد.

باید ترکیبی از حروف بزرگ انگلیسی حروف کوچک انگلیسی اعداد و علائم مانند !، $, #, باشد.

۶ ــ۱ــ۱ــ Store passwords using reversible encryption : فعال شدن این بخش باعث می‌شود که کلمه‌های عبور به‌صورت الگوریتم‌های رمزگذاری بازگشتی ذخیره شود.

پیوست ۲ــ تجهیزات سخت افزاری مورد نیاز برای نصب ویندوز ۲۰۰۸ سرور

ــ پردازنده حداقل 1GHz برای ۳۲ بیتی 1.4GHz برای ۶۴ بیتی ولی بهتر است از پردازنده با سرعت 2GHz بالاتر استفاده شود.

ــ حافظه اصلی RAM حداقل 512MB و توصیه می‌شود که 2GB یا بیشتر باشد. حداکثر میزان RAM برای سیستم‌عالم ۳۲ بیتی ۴ گیگابایت می‌باشد (برای ویرایش مؤسسات[1] و داده‌های مرکزی[2])

در ویندوز ۲۰۰۸ سرور ویرایش استاندارد ۶۴ بیتی 32GB بایت و برای ویرایش مؤسسات و داده مرکزی ۶۴ بیتی تا ۲ TB[3] حافظه اصلی پشتیبانی می‌شود.

ــ فضای خالی دیسک سخت حداقل ۱۰ گیگابایت ولی بهتر است از ۴۰ گیگابایت بیشتر باشد.

توجه : رایانه‌هایی که دارای RAM بالای ۱۶ گیگابایت هستند باید فضای بیشتری از دیسک سخت را در نظر بگیرید (به خاطر وجود pagefile در درایو نصب ویندوز)

ــ DVD ROM

ــ ماوس و صفحه کلید

ــ کارت گرافیک Super VGA که از ۶۰۰*۸۰۰ پشتیبانی کند.

مراحل نصب :

۱ــ DVD را داخل درایو قرار دهید.

۲ــ در محیط گرافیکی بر روی Install Now کلیک کنید.

۳ــ انتخاب نوع ویرایش سیستم‌عامل

۴ــ واردکردن سریال نصب

۵ــ پذیرش قواعد نصب

۶ــ انتخاب درایو نصب

۷ــ تأیید پیغام راه‌اندازی مجدد سیستم

۸ــ بعد از راه‌اندازی مجدد نام کاربر مدیر و رمز عبور را باید تعیین کنید.

۹ــ تنظیم ساعت و تاریخ و منطقه زمانی

۱ــ Enterpr se

۲ــ Data Center

۳ــ TB = 024 GB

۱۰ــ پیکربندی شبکه

۱۱ــ کلیدهای Alt Ctrl Delete را برای Log on شدن (ورود به ویندوز) فشار دهید.

۱۲ــ کلمه عبور کاربر مدیر را برای ورود به ویندوز وارد کنید.

ــ فعال کردن ویندوز بعد از نصب چون ویندوز شما ۳۰ روزه می‌باشد و شما باید با استفاده از Activation آن را فعال کنید.

پیوست ۳ــ برخی از اختصارات شبکه

سرنام	شرح
ADSL	Asymmetric Digital Subscriber Line
AP	Access point
AIPA	Automatic Private IP Addressing
AUI	Attachment Unit Interface
BA	Broadcast Address
Bps	Byte per Second
bps	Bit per second
CSMA/CD	Carrier Sense Mulitple Access with Collision Detection
COM	Communication
DC	Domain Controller
DNS	Domain Name Service
DRA	DHCP Relay
DHCP	Dynamic Host Control Protocol
DSL	Digital Subcarrier Line
Email	Electronic Mail
FDDI	Fiber Distributed Data Interface
FTP	File Transfer protocol
FO	Fiber Optic
FQDN	Full Qualified Domain Name
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

ICP	Internet Central Provider
IANA	Internet Assingned Numbers Authority
ICS	Internet Connection Sharing
ID	Idetifire
IE	Internet Explorer
IP	Internet Protocol
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Media Access Control
MAN	Metro Politan Area Network
MM	Multi Mode
NET	Network
NAS	Network Attached Storage
NAT	Network Address Translation
NIC	Network Interface Card
NNTP	Network News Transfer Protocol
ORG	Organization
OSI	Open System Interconnection
POP 3	Post Office Protocol (version 3)
PtP	Point to Point
SMTP	Simple Network

SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
URL	Universal Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network
WLANS	Wireless Local Area Networks
WMANS	Wireless Metropolitan Area Networks
WPANS	Wireless Personal Area Networks
WWANS	Wireless Wide Area Networks
WWW	World Wide Web

پیوست ۴ــ دستورات خط فرمان

دستورات خط فرمان برای اجرای برنامه‌های مرکز کنترل :

Command Name	Description
CONTROL	opens the control panel window
CONTROL ADMINTOOLS	opens the administrative tools
CONTROL KEYBOARD	opens keyboard properties
CONTROL COLOUR	opens display properties Appearance tab
CONTROL FOLDERS	opens folder option
CONTROL FONTS	opens font policy management
CONTROL INTERNATIONAL or INTL CPL	opens Regional and Language option
CONTROL MOUSE or MAIN CPL	opens mouse properties
CONTROL USERPASSWORDS	opens User Accounts editor
CONTROL USERPASSWORDS 2	user account access restrictions
CONTROL PRINTERS	opens faxes and printers available
APPWIZ CPL	opens Add or Remove programs utility tool
DESK CPL	opens display properties Themes tab
HDWWIZ CPL	opens add hardware wizard
JOY CP	opens game controllers settings
MMSYS CPL	Opens Sound and Audio device Properties Volume tab
SYSDM CPL	Opens System properties
TELEPHON CPL	Opens phone and Modem options
TIMEDATE CPL	Date and Time properties

دستورات خط فرمان برای اجرای برنامه‌های مرکز کنترل :

Command Name	Description
CONTROL	Opens the control panel window
CONTROL ADMINTOOLS	Opens the administrative tools
CONTROL KEYBOARD	Opens keyboard properties
CONTROL COLOUR	Opens display properties Appearance tab
CONTROL FOLDERS	Opens folder options
CONTROL FONTS	Opens font policy management
CONTROL INTERNATIONAL or INTL CPL	Opens Regional and Language option
CONTROL MOUSE or MAIN CPL	Opens mouse properties
CONTROL USERPASSWORDS	Opens User Accounts editor
CONTROL USERPASSWORDS 2	User account access restrictions
CONTROL PRINTERS	Opens faxes and printers available
APPWIZ CPL	Opens Add or Remove programs utility tool
DESK CPL	Opens display properties Themes tab
HDWWIZ CPL	Opens add hardware wizard
JOY CP	Opens game controllers settings
MMSYS CPL	Opens Sound and Audio device Properties Volume tab
SYSDM CPL	Opens System properties
TELEPHON CPL	Opens phone and Modem options
TIMEDATE CPL	Date and Time properties
ACCESS CPL	Opens Accessibility Options

WUAUCPL CPL	Opens Automatic Updates
POWERCFG CPL	Opens Power Options Properties
AZMAN MSC	Opens authorization management utility tool
COMPMGMT MSC	Opens the Computer management tool
COMEXP MSC or DCOMCNFG	Opens the Computer Services management tool
DEVMGMT MSC	Opens Device Manager
EVENTVWR or EVENTVWR MSC	Opens Event Viewer
FSMGMT MSC	Opens Shared Folders
NAPCLCFG MSC	NAP Client configuration utility tool
SERVICES MSC	Opens Service manager
GPEDIT MSC	Opens Group Policy utility tool
LUSRMGR MSC	Opens Local Users and Groups
SECPOL MSC	Opens local security settings
WMIMGMT MSC	Opens (WMI) Window Management Instrumentation
PERFMON or PERFMON MSC	Opens the Performance monitor
MMC	Opens empty Console
DXDIAG	Opens DirectX diagnostics tools
ODBCAD 32	Opens ODBC Data source Administrator
REGEDIT or REGEDT 32	Opens Registry Editor
DRWTSN 32	Opens Dr Watson
VERIFIER	Opens Driver Verifier Manager
CLICONFG	Opens SQL Server Client Network Utility
UTILMAN	Opens Utility Manager
MSCONFIG	Opens System Configuration Utility
SYSEDIT	Opens System Configuration Editor
SYSKEY	Windows Account Database Security management

دستورات خط فرمان برای اجرای برنامه‌های کاربردی :

Command Name	Description
EPLORER	Opens Windows Explorer
IEXPLORER	Opens Internet explorer
WAB	Opens Contacts
CHARMAP	Opens Character Map
WRITE	Opens WordPad
NOTEPAD	Opens Notepad
CALC	Opens Calculator
CLIPBRD	Opens Clipbook Viewer
WINCHAT	Opens Microsoft Chat Interface
SOUNDRECORDER	Opens sound recording tool
DVDPLAY	Run CD or DVD
WMPLAYER	Opens Windows Media Player
MOVIEMK	Opens untitled Windows Movie Maker
OSK	Opens on_screen Keyboard
MAGNIFY	Opens Magnifier
DIALER	Opens phone Dialer
WINCAL	Opens Calendar
EUDCEDIT	Opens Private Character Editor

دستورات خط فرمان برای اجرای برنامه‌های مدیریت دیسک :

Command Name	Description
DISKMGMT MSC	Opens disk management utility
CLEANMGR	Opens disk drive clean up utility
DFRG MSC	Opens disk defragmenter
CHKDSK	Complete analysis of disk partition
DISKPART	Disk partitioning tool