جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

توضیح مهم :

با توجه به اینکه دروس و امتحانات مهندسی شبکه در سایر نقاط دنیا تماما به زبان انگلیسی برگزار می شود و در ایران به دلیل عدم تسلط به زبان انگلیسی اکثر دانشجویان با مشکل روبرو هستند استفاده از جزوه فارسی می تواند تا حد زیادی به روند آموزش این رشته کمک نماید اما قابل ذکر است مطالعه کتابهای انگلیسی (اصلی) الزامی بوده و در غیر اینصورت دانشجویان در امتحانات کلاسی و خصوصا امتحانات بین المللی دچار مشکل خواهند شد.

به همین دلیل در این جزوه و سری جزوات بعدی در قسمتهایی که مطالعه آنها اهمیت بیشتری داشته اند ، گزیده ای از کتابهای معتبر و مورد تائید که به زبان اصلی موجود بوده به جزوات اضافه شده است که میتواند در مطالعه متمرکز مطالب مفید واقع شود.

شناخت دوره هایی که در پیش داریم و امتحانات مربوطه :

	Course Group	Course Name	Exam #
1	Pre MCSE	Network+	------
2	CLIENT	Microsoft Windows XP Professional	070-270
3	CORE 1	Microsoft Windows Server 2003	070-290
4	CORE 2	Microsoft Windows 2003 Network Infrastructure 1 (Infra 1)	070-291
5	CORE 3	Microsoft Windows 2003 Network Infrastructure 2 (Infra 2)	070-293
6	CORE 4	Microsoft Windows 2003 Directory Service (Active Directory)	070-294
7	CORE - DESIGN	Active Directory and Network Infrastructure Design	070-297
8	ELECTIVE	درس انتخابی برای تعیین گرایش	-------

جلسه اول:

- محیط های غیر شبکه ای و مشکلات و مسائل موجود
- شبکه و هدف از تشکیل آن
- اجزاء تشکیل دهنده شبکه
- انواع شبکه
  - از نظرگستردگی و محدوده فیزیکی و جغرافیایی
  - از نظر روش عملکرد و ساختار کنترل و امنیت
  - از نظر روش اتصال فیزیکی
- انواع Server
- کمی بیشتر بدانیم !
- گزیده مطالب درسی به زبان اصلی

✸ شبکه چیست ؟

قبل از به وجود امدن شبکه بزرگترین مشکل کاربران کامپیوتر ، جابجا کردن اطلاعات بود .

در محیط های غیر شبکه ای که اصطلاحا آن را **Stand Alone Environment** می نامند در صورتی که کاربر تصمیم به انتقال اطلاعات به دستگاه دیگری می گرفت ، مجبور بود از ابزاری مانند دیسکت و کارت پانچ استفاده کرده و پس از کپی کردن اطلاعات بر روی آن به طور فیزیکی اقدام به ارسال دیسکت و یا پانچ کارد می کرد.

مشکلات اصلی این کار اولا هزینه ای است که جهت خریداری رسانه ای مثل دیسکت و سی دی و ... صرف می شود. ثانیا به دلیل نیاز به انتقال فیزیکی زمان بسیاری صرف می شود و ضمنا در صورت تعدد مقصد به ناچار نسخه های زیادی از اطلاعات می بایست به صورت فیزیکی تکثیر گردد که هم هزینه را بسیار افزایش می دهد و هم زمان بیشتری برای تکثیر و انتقال آن صرف می شود. ثانیا ابزار فیزیکی که برای انتقال کاربرد دارند دارای محدودیت در حجم ذخیره سازی اطلاعات و فرسایش تدریجی می باشند.

شبکه با اتصال کامپیوتر ها به روشهای گوناگون شرایطی را فراهم می آورد که برای انتقال اطلاعات هزینه ها کاهش یافته و سرعت و ریسک انتقال نیز پائین بیاید و نتیجتا امکانات و تسهیلاتی در اختیار بشر قرار می گیرد که به واسطه ان پیشرفت چشمگیری در کامپیوتر و علوم وابسطه پدید می آید.

شبکه به حد اقل دو کامپیوتر که به طریقی به یکدیگر اتصال یافته باشند تا از منابع و امکانات یکدیگر به صورت مشترک استفاده کنند ، گفته می شود. این منابع قابل اشتراک شامل : فایل ها ، پرینتر ها ، **CD - ROM** و ...

✸ اجزای اصلی موجود در شبکه شامل:

1- **Clients**: کامپیوتر سرویس گیرنده می باشد که از خدمات موجود در شبکه استفاده می کند.

2- **Servers**: کامپیوتر سرویس دهنده می باشد که خدمات متفاوت را در اختیار دیگر کامپیوتر ها قرار می دهد.

3- **Media**: تمامی موارد ارتباط دهنده بین کامپیو ترها می باشد که شامل : کابل ، کانکتور و تجهیزات ارتباطی

4- **Shared Data**: شامل تمام منابع موجود در شبکه مانند : به اطلاعاتی که به اشتراک گذاشته می شوند گفته می شود.

5- **Shared Peripherals and Hardware Resources**: به منابع به اشتراک گذاشته شده می گویند.

✸ انواع شبکه – از نظر گستردگی و موقعیت فیزیکی و جغرافیایی

Local Area Network (LAN)

به شبکه ای که از لحاظ موقعیت جغرافیایی محدود بوده و کامپیوتر های آن در موقعیتی شبیه به یک ساختمان با هم ارتباط دارند گفته می شود.

گفته می شود که از لحاظ فیزیکی محدود می باشند مانند شبکه موجود در یک ساختمان.

Wide Area Network (WAN)

به شبکه هایی گفته می شود که معمولا از اتصال دو یا چند **LAN** به وجود می آیند، البته قابل ذکر است این تعریف فقط به ارتباط **LAN** ها با یکدیگر گفته نمی شود وحتی اتصال حداقل دو کامپیوتر که فاصله زیادی از هم داشته باشند را نیز شامل می شود که بزرگترین آنها **Internet** می باشد.

تعاریف دیگری نیز مانند **PAN,MAN** وجود دارد که از محدوده این درس خارج است و نیازی به توضیح آنها وجود ندارد.

✸انواع شبکه - از نظر روش عملکرد و ساختار کنترل و امنیت

(WorkGroup) Peer To Peer

این شبکه ها به طور استاندارد حد اکثر **10** کامپیوتر تشکیل می شوند . البته می توانند بیشتر از این تعداد نیز باشند ولی به دلیل مشکلاتی که در مدیریت آنها ایجاد می شود افزایش تعداد کامپیوتر در این محیط پیشنهاد نمی گردد. در شبکه های **Workgroup** بررسی صحت نام کاربری و میزان دسترسی کاربر **(Authentication)** به صورت گسسته در کامپیوتر ها انجام می شود.

باید قبل از درک این مورد به بررسی موضوع کوچک دیگری بپردازیم ، یکی از کارهایی که در شبکه انجام می شود **Authentication** است. با توجه به اینکه هر کاربری برای کار کردن در شبکه باید خود را به سیستم معرفی نماید ، کامپیوتر در هنگام ورود هر شخص نام و رمز عبور ان کاربر را می پرسد و پس از بررسی آن ، در صورتی که آن فرد در شبکه شناخته شده و تعریف شده باشد درخواست راه یافتن او به شبکه توسط سیستم پذیرفته می شود که به این کار **Authentication** می گوئیم.در واقع کامپیوتر با انجام بررسی مشخصات فرد عمل **Authentication** را انجام می دهد. این کار در حقیقت همان **Login** کردن در شبکه است. موضوع این است که بدانیم صحت نام کاربری و رمز مربوطه و میزان دسترسی افراد به شبکه در کجا ثبت و نگهداری می شود و **(Authentication)** در کجای شبکه انجام می پذیرد؟

در شبکه های **Workgroup** هر کامپیوتر دارای **Local Security Database** می باشد و هرگاه یک کاربر تلاش می کند در شبکه **Login** نماید بررسی نام کاربری بر روی همان کامپیوتر انجام می شود و نکته مهم اینکه اگر تلاش کنیم به اطلاعات یا امکانات موجود در کامپیوتر دیگری از شبکه دسترسی بیابیم باید نام کاربری ما بر روی کامپیوتر میزبان به طور جدا ثبت شده باشد.

پس به همین دلیل اگر به تعداد ده کامپیوتر در یک **Workgroup** موجود باشد و یک **User** را بخواهیم در شبکه معرفی کنیم باید آن کاربر را به طور مجزا در هر ده سیستم بشناسانیم. دلیل محدودیت در تعداد کامپیوتر های **Workgroup** همین موضوع می باشد.

از ضعف های دیگر این روش عدم امکان کنترل مرکزی دسترسی افراد به اطلاعات و امکانات می باشد و مسلما همین امر باعث کاهش امنیت شبکه های **Workgroup** نسبت به **Domain** می باشد. در چنین محیطی امکان گسترش شبکه و افزایش تعداد کاربر ها و کامپیوتر ها وجود ندارد.

اما هزینه راه اندازی شبکه های **Workgroup** پائین بوده و هزینه نگهداری و مدیریت آن نیز کم است و راه اندازی ان نیز بسیار ساده است.

(Domain) Server Based

همانگونه که در قسمت قبلی نیز ذکر شد به واسطه انجام **Authentication** در شبکه ، میزان دسترسی افراد به منابع اطلاعاتی و امکانات تعیین می گردد. در شبکه های **Domain** این عمل که به آن **Authentication** می گویند به صورت متمرکز توسط یک **Server** که برای ایـن منظـور در نظر گرفته شده است انجام می گیرد. به **Server** ای که برای این منظور اختصاص داده می شود اصطلاحا **Domain Controller** می گویند.

این شبکه ها باید دارای حد اقل یک **Domain Controller** باشند که تمامی **User Account** ها بر روی آن تعریف گردد. بدین معنی کـه اگر کاربری بخواهد بر روی کامپیوتری **Login** کند ،مشخصات او از طریق کامپیوتر خودش برای **Domain Controller** ارسال می شـود و در صورت دریافت تائید ، کاربر می تواند در حدود تعریف شده به منابع شبکه دسترسی یابد.

به دلیل مرکزیت یافتن کنترل کاربران امنیت این نوع شبکه بیشتر می باشد و امکان گسترش ان نیز فراهم می گردد. البته مسلما هزینه راه انـدازی و نگهداری این نوع شبکه ها بیشتر می باشد.

برای تصمیم گیری در مورد روش راه اندازی شبکه و انتخاب **workgroup** و یا **Domain** به موارد زیر توجه می نمایند:

- اندازه شرکت یا سازمان مورد نظر
- میزان امنیت مورد نیاز
- میزان بودجه
- سطح مدیریت در دسترسی به اطلاعات و امکانات

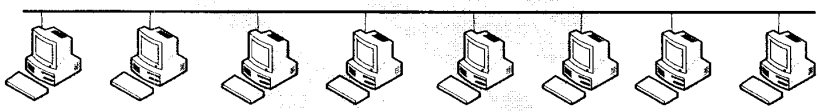
✸انواع شبکه - از نظر روش اتصال فیزیکی

شبکه ها از نظر روش اتصال و شکل و ظاهر اتصالات و کابل کشی نیز دارای انواع متفاوتی هستند. با توجه به اینکه روش های بدون سیم نیز برای اتصال کامپیوتر ها وجود دارد مسلما روش اتصال به صورت بی سیم (Wireless) نیز در موضوعات شبکه قابل بحث است. اما با توجه به گستردگی ان فعلا در این قسمت به ان پرداخته نمی شود. به ظاهر اتصالات شبکه یا مدیای اتصال دهنده کامپیوتر ها Topology نیز میگویند.

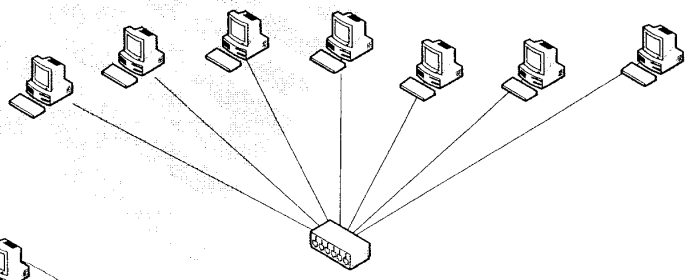
انواع توپولوژی:

- روش خطی یا سری (Bus)
- روش ستاره ای یا متمرکز (Star)
- روش حلقه ای (Ring)
- روش پوششی (Mesh)
- روش ترکیبی (Hybrid)

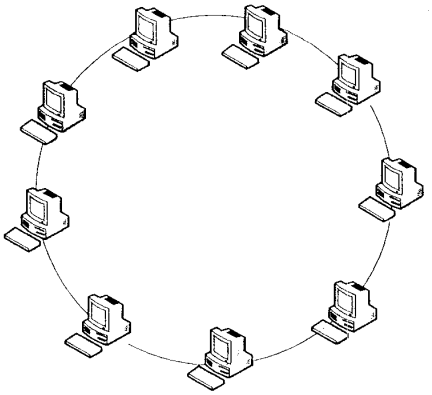
- در روش خطی (Bus) کامپیوتر ها به صورت انشعابی به کابل متصل می گردند و سیگنالهای اطلاعات در طول مسیر کابل ارسال می شود و تمام کامپیوتر هایی که به آن متصل هستند سیگنال ها را دریافت می نمایند.

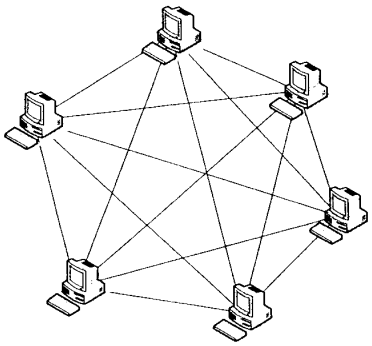


- در روش ستاره ای(Star) از یک دستگاه Hub و یا Switch برای اتصال کابل ها به هم استفاده می نمایند که در حقیقت این دستگاه نقطه مرکزی اتصال کامپیوتر ها با یکدیگر می گردد. به دلیل ساختار ستاره ای شکل به ان Star می گویند.



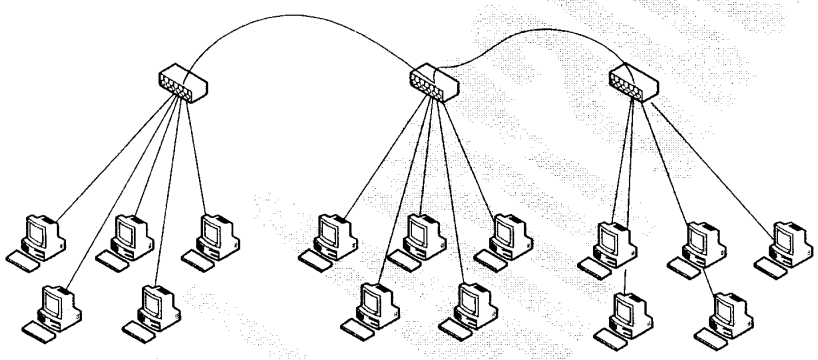
- در روش حلقه ای (Ring) کامپیوتر ها یا به صورت کاملا حلقه ای از طریق کابل به یکدیگر متصل می گردند و یا ساختار ارتباطی و ارسال اطلاعات توسط کامپیوتر ها گردشی می باشند که نتیجتا به آن Ring می گویند.





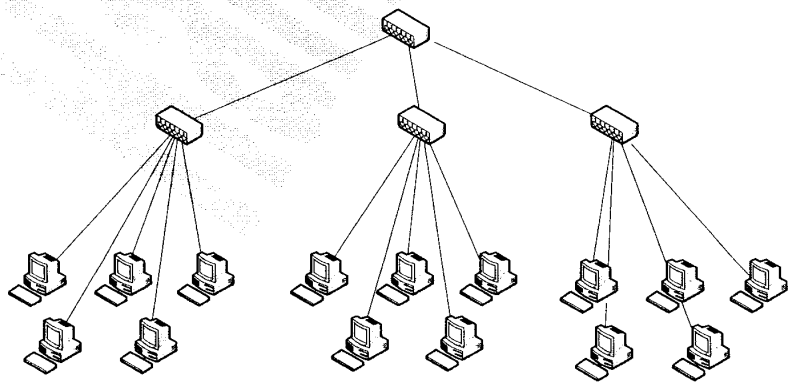
در روش پوششی **(Mesh)** تمام کامپیوتر ها با اتصالات مجزا به یکدیگر متصل می شوند ساختار نودرتو و پیچیده ای از کابل کشی ایجاد می شود. این روش به دلیل پیچیدگی زیاد ر ساختار های عادی و بزرگ استفاده نمی شود و برای تعداد بسیار کم کامپیوتر در شرایط ویژه کاربرد دارد.

در روشهای ترکیبی **(Hybrid)** از ترکیب روش های کابل کشی موجود برای گسترش و توسعه شبکه و افزایش تعداد کامپیوتر ها استفاده می کنند. در شکل زیر روش **Hybrid** از نوع **Star-Bus** نمایش داده شده است.



Star – Bus

در شکل زیر مدل **Hybrid** از نوع **Cascade Star** نمایش داده شده است. همانگونه که در شکل مشخص شده یک دستگاه **Hub** به عنوان اتصال دهنده اصلی **Hub** های دیگر را به هم وصل کرده است و از طریق **Hub** های لایه پائین کامپیوتر ها به یکدیگر متصل شده اند.



Cascade Star

قابل ذکر است متد پیچیده تر نیز وجود دارد که در درس های بعدی مورد تحلیل قرار می گیرد.

✸ انواع Server

سرویس دهنده Domain Controller تنها نوع Server شبکه نیست. برای خدمات متفاوت ، سرویس دهنده های متفاوتی نیز وجود دارند که هر یک برای منظوری خاص در شبکه نصب و راه اندازی می گردند.

انواع سرویس دهنده های شبکه عبارتند از:

- Directory Services Server (Domain Controller)
- File Server
- Print Server
- Fax Server
- Mail Server
- Web Server
- Database Server
- Cache Server
- Name Server
- Remote Access Server

کمی بیشتر بدانیم!

تصور کردن یک فروشگاه بزرگ که مشتریان در حال خرید کردن در آن موج می زنند کار سختی نیست ! اگر دقت کرده باشید در چنین موقعیتی فروشندگان به سختی مشغول رسیدگی به ارباب رجوع هستند و بعضا فرصت یک احوال پرسی ساده را هم ندارند ! در این شرایط با این تعداد زیاد رجوع کننده اگر قرار باشد یک نفر به عنوان فروشنده به تنهایی کار کند مسلما نمی تواند پاسخگو باشد و قطعا رضایت خاطر مشتریان نیز کسب نخواهد شد. در حقیقت با افزایش تعداد فروشندگان که معمولا همه آنها از نظر توانائی مشابه هم هستند و دانسته های کاری شبیه به هم نیز دارند ، فشار کاری را تقسیم کرده و به کیفیت و سرعت ارائه خدمات می افزایند. این کار در مورد **Server** های شبکه نیز انجام می شود . چرا که اگر مثلا یک **Domain Controller** بخواهد محدوده یک شبکه بسیار بزرگ را از نظر **Authentication** پشتیبانی کند ، از نظر فیزیکی توانائی نخواهد داشت و کامپیوترها زمان زیادی را باید در انتظار خدمات منتظر بمانند. نتیجتا به تعداد **Domain Controller** های شبکه می افزایند و به این شکل به جای یک **Server** ، چند دستگاه **Server** به انجام این کار مشغول می شوند و فشار کار **Authentication** در شبکه بین سرویس دهنده های مخصوص آن تعدیل می گردد. قابل ذکر است بسیاری از **Server** ها را می توان با انواع همنوع خودشان **Load Balance** کرده و در شبکه نصب و راه اندازی کرد.

در عین حال خاصیت دیگری که در شبکه ما به واسطه افزودن تعداد سرویس دهنده های همنوع ایجاد می شود ، افزونگی **(Redundancy)** می باشد. بدین معنی که می توان اطمینان داشت در صورت از کار افتادن یکی از سرویس دهنده ها ، **Server** کمکی آن به جایش کار کرده و اجازه توقف کامل ارائه خدمات را حتی برای لحظه ای نمی دهد.

البته برای اینکه دو سرویس دهنده بتوانند به طور موازی کار کنند باید اطلاعات آنها نیز همواره مشابه هم باشد که با همسان سازی اطلاعات که به آن **Replication** نیز می گویند این امکان فراهم می گردد.

Local Area Networks and Wide Area Networks

A LAN is a group of computers located in a relatively small area and connected by a common medium. Each of the computers and other communicating devices on the LAN is called a *node*. A LAN is characterized by three primary attributes: its topology, its medium, and its protocols. The *topology* is the pattern used to connect the computers together. With a *bus* topology, a network cable connects each computer to the next one, forming a chain. With a *star* topology, each of the computers is connected to a central nexus called a hub or switch. A *ring* topology is essentially a bus network with the two ends joined together.

The network medium, as defined earlier, is the actual physical connection between the networked computers. The topology and the medium used on a particular network are specified by the protocol operating at the data-link layer of the OSI model, such as Ethernet or Token Ring. Ethernet, for example, supports several different topologies and media. When you select one combination of topology and medium for a LAN, such as unshielded twisted pair (UTP) cable in a star topology, you must (in most cases) use the same topology and medium for all of the computers on that LAN. There are some hardware products that enable you to connect computers to the same LAN with different media, but this is only true for closely related technologies. You can't connect a bus Ethernet computer to a star Ethernet computer and have both systems be part of the same LAN.

In the same way, all of the computers on a LAN must share common protocols. You can't connect an Ethernet computer to a Token Ring computer on the same LAN, for example. The same is true for the protocols operating at the other layers of the OSI model. If the systems on the LAN don't have common protocols at every layer of the stack, communication among them is not possible.

In most cases, a LAN is confined to a room, a floor, or perhaps a building. To expand the network beyond these limits, you can connect multiple LANs together using devices called *routers*. This forms an *internetwork*, which is essentially a network of networks. A computer on one LAN can communicate with the systems on another LAN because they are all interconnected. By connecting LANs in this way, you can build an internetwork as large as you need. Many sources use the term *network* when describing a LAN, but just as many use the same term when referring to an internetwork.

Client/Server and Peer-to-Peer Networking

Computers can interact with each other on a network in different ways and fulfill different roles. There are two primary networking models used to define this interaction, called client/server and peer-to-peer. On a *client/server network*, certain computers act as servers and others act as clients. A *server* is simply a computer (or more precisely, an application running on a computer) that provides a service to other computers. The most basic network functions are the sharing of files and the sharing of printers; the machines that do this are called file servers and print servers. There are many other types of servers as well: application servers, e-mail servers, Web servers, database servers, and so on. A *client* is a computer that avails itself of the services provided by servers.

NOTE

Although servers are often thought of as computers, they are actually applications. A single computer can conceivably run several different server applications at the same time and, in most cases, perform client operations as well.

At one time, it was common for computers to be limited to either client or server roles. Novell NetWare, which was the most popular network operating system for many years, consists of a separate server operating system and clients that run on DOS and Microsoft Windows workstations. The server computer functions only as a server and the clients only as clients. The most popular network operating systems today, however, include both client and server functions. All of the current versions of Windows (Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, and windows 2003), for example, can function as both clients and servers. How to utilize each system is up to the network administrator.

You can construct a client/server network by designating one or more of the networked computers as a server and the rest as clients, even when all of the computers can perform both functions. In most cases, servers are better equipped systems, and on a large network many administrators connect them to the backbone so that all of the segments have equal access to them. A client/server network typically uses a directory service to store information about the network and its users. Users log on to the directory service instead of logging on to individual computers, and administrators can control access to the entire network using the directory service as a central resource.

On a *peer-to-peer network,* every computer is an equal and functions as both a client and a server. This means that any computer can share its resources with the network and access the shared resources on other computers. You can therefore use any of the Windows versions mentioned earlier for this type of network, but you cannot use a dedicated client/server operating system like NetWare. Peer-to-peer networks should be generally limited to 10 or 15 nodes or fewer on a single LAN, because each system has to maintain its own user accounts and other security settings.

Network Cables

Most LANs use some form of cable as their network medium. Although there are many types of wireless media, cables are more reliable and generally provide faster transmission speeds than other media. Data-link layer protocols often provide more than one cable specification to choose from. Each specification includes the type of cable to use, the cable grade, and the basic guidelines for installing it. The type of cable you choose should be based on the requirements of your installation, the nature of the site where your network is to be installed, and, of course, your budget.

The Bus Topology

A network that uses the *bus topology* is one in which the computers are connected in a single line, with each system cabled to the next system. Bus networks are illustrated in Figure 2.1. Early Ethernet systems used the bus topology with coaxial cable, a type of network that is rarely seen today. The cabling of a bus network can take two forms: *thick* and *thin*. Thick Ethernet networks use a single length of coaxial cable with computers connected to it using smaller individual cables called Attachment Unit Interface (AUI) cables (sometimes called transceiver cables), as shown on the top half of Figure 2.1. Thin Ethernet networks use separate lengths of a narrower type of coaxial cable, and each length of cable connects one computer to the next, as shown in the bottom half of Figure 2.1.

NOTE

The *transceiver* is an integral component of the network interface responsible for both transmitting and receiving data over the network medium. Thick Ethernet is the only form of Ethernet network that uses a transceiver that's separate from the network interface adapter. The transceiver itself connects to the coaxial cable using a device called a *vampire tap,* named for the metal teeth with which it penetrates the cable sheath to make a connection with the copper conductor inside. The transceiver is then connected to the network interface adapter in the computer using an AUI (transceiver) cable. All of the other Ethernet physical layer standards have their transceivers integrated into the network interface adapter card and do not require separate AUI cables.

When any one of the computers on the network transmits data, the signals travel down the cable in both directions, reaching all of the other systems. A bus network always has two open ends, which must be terminated. *Termination* is the process of installing a resistor pack at each end of the bus to negate the signals that arrive there. Without terminators, the signals reaching the end of the bus would reflect back in the other direction and interfere with the newer signals being transmitted.

The main problem with the bus topology is that a single faulty connector, faulty terminator, or break in the cable affects the functionality of the entire network. Signals that cannot pass beyond a certain point on the cable cannot reach all of the computers beyond that point. In addition, when a component failure splits the network into two segments, each half of the cable is also not terminated. On the half of the network that does receive the signals transmitted by each computer, signal reflection garbles the data. This is one of the primary reasons that bus networks are rarely used now.

The Star Topology

Whereas the bus topology has the computers in a network connected directly to each other, the *star topology* uses a central cabling nexus called a *hub* or *concentrator*. In a star network, each computer is connected to the hub using a separate cable, as shown in Figure 2.2. Most of the Ethernet LANs installed today, and many LANs using other protocols as well, use the star topology. Star LANs can use several different cable types, including various types of twisted-pair and fiber optic cable.

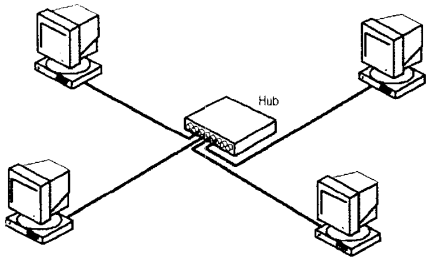


Figure 2.2

The unshielded twisted pair (UTP) cables used on most Ethernet LANs are usually installed using a star topology. Functionally, a star network uses a shared network medium, just as a bus network does. Despite the fact that each computer connects to the hub with its own cable, the hub propagates all signals entering through its ports out through all of its other ports. Signals transmitted by one computer are therefore received by all other computers on the LAN.

The main advantage of the star topology is that each computer has its own dedicated connection to the hub, providing the network with a measure of fault tolerance. If a single cable or connector should fail, only the computer connected to the hub by that cable is affected. The disadvantage of the star topology is that an additional piece of hardware, the hub, is required to implement it. If the hub should fail, the entire network goes down. However, this is a relatively rare occurrence because hubs are relatively simple devices that are usually found in a protected environment, such as a data center or server closet.

The Ring Topology

In terms of signal transmissions, a *ring network* is like a bus in that each computer is logically connected to the next. However, in a ring network, the two ends are connected instead of being terminated, thus forming an endless loop. This enables a signal originating on one computer to travel around the ring to all of the other computers and eventually back to its point of origin. Networks such as Token Ring, which use token passing for their Media Access Control (MAC) mechanism, are wired using a ring topology. The most important thing to understand about the ring topology is that, in most cases, it is strictly a logical construction, not a physical one. To be more precise, the ring exists in the wiring of the network, but not in the cabling.

NOTE

A *cable* is a device that contains a number of signal conductors, usually in the form of separate wires. A twisted-pair cable, for example, contains eight individual wires within a single sheath.

When you look at a network that uses the ring topology, you may be puzzled to see what looks like a star. In fact, the cables for a ring network connect to a hub and take the form of a star. The ring topology is actually implemented logically, using the wiring inside the cables (see Figure 2.4). Ring networks use a special type of hub, called a *multi station access unit* (MAU), which receives data through one port and transmits it out through each of the others in turn (not simultaneously, as with an Ethernet hub). For example, when the computer connected to port number 3 in an eight-port MAU transmits a data packet, the MAU receives the packet and transmits it out through port number 4 only. When the computer connected to port number 4 receives the packet, it immediately returns it to the MAU, which then transmits it out through port number 5, and so on. This process continues until the MAU has transmitted the packet to each computer on the ring. Finally, the computer that generated the packet receives it back again and is then responsible for removing it from the ring. If you were to remove the wire pairs from the sheaths of the cables that make up a ring network, you would have a circuit that runs from the MAU to each computer and back to the MAU.

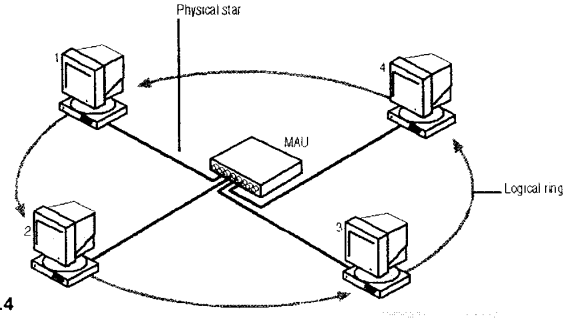


Figure 2.4

The design of the physical star topology used by the ring makes it possible for the network to function even when a cable or connector fails. The MAU contains special circuitry that removes a malfunctioning workstation from the ring, but still preserves the logical topology. By comparison, a network that is literally cabled as a ring would have no MAU, but a cable break or connector failure would cause the network to stop functioning completely. The one commonly used protocol that does include an option for a physical ring topology, Fiber Distributed Data Interface (FDDI), defines the use of a double ring, which consists of two separate physical rings with traffic flowing in opposite directions. When computers are connected to both rings, the network can still function despite a cable failure.

The Mesh Topology

The *mesh topology,* in the context of local area networking, is more of a theoretical concept than an actual real-world solution. On a mesh LAN, each computer has a dedicated connection to every other computer, as shown in Figure 2.5. In reality, this topology only exists on a two-node network. For a mesh network with three computers or more, it would be necessary to equip each computer with a separate network interface for every other computer on the network. Thus, for a five-node network, each computer would require four network interface adapters, which is certainly not practical. A mesh LAN provides excellent fault tolerance, however, as there is no single point of failure that can affect more than one computer.

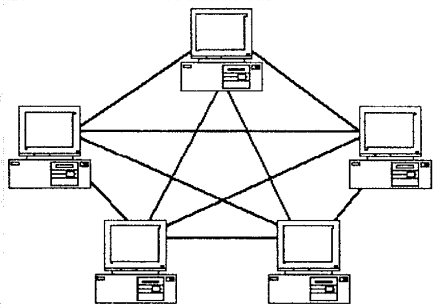


Figure2.5

In internetworking, the mesh topology is a cabling arrangement that you can actually use. A mesh internetwork has multiple paths between two destinations, made possible by the use of redundant routers, as shown in Figure 2.6. This topology is very common on large enterprise networks because it enables the network to tolerate numerous possible malfunctions, including router, hub, and cable failures. In most cases, when you see a reference to a mesh topology, this is the application being cited.

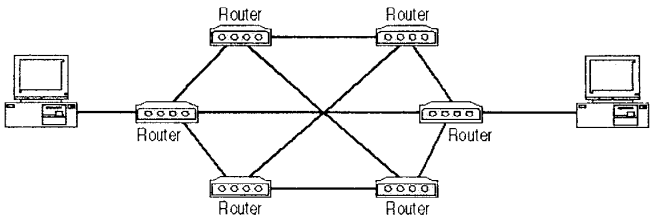


Figure 2.6

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه دوم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه دوم:

- کابل کشی در توپولوژی های متفاوت
  - کابلهای Coaxial و توپولوژی Bus
  - کابلهای Twisted Pair
- گزیده مطالب درسی به زبان اصلی

✸ کابل کشی در توپولوژی های متفاوت :

همانگونه که قبلا دیدیم توپولوژی ها با توجه به روشهای متفاوتی که در کابل کشی و اتصالات کامپیوتر ها در شبکه وجود دارد معنی پیدا می کنند. مسلما برای هر روش کابل کشی باید از کابل مناسب آن توپولوژی استفاده نمود.

در روش خطی یا سری (Bus) از کابل Coaxial استفاده می شود. به همین جهت با توجه به نوع کابل Coaxial مورد استفاده در شبکه می توان شبکه Bus را به دو دسته تقسیم کرد.

- Thin Net
- Thick Net

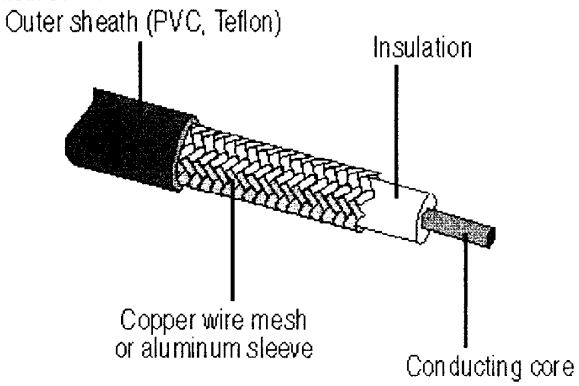
همانطور که قبلا هم اشاره شد روش Bus کامپیوترها از یک کابل انشعاب گرفته اند و در حقیقت سیگنال ها توسط هر کامپیوتر بر روی کابل فرستاده می شود. تمام سیگنالهای ارسالی بر روی کابل در هر جهت انتشار می یابد و عملا تمام کامپیوتر ها سیگنالها را می شنوند.

در درسهای بعدی خواهیم آموخت که چگونه در ساختار Packet های ارسالی شبکه معین می گردد که مبداء و مقصد کدام کامپیوتر ها هستند.

کابلهای Coaxial انواع و استفاده های گوناگونی دارند. مدل هائی که برای شبکه به کار می روند سیگنالها را به صورت دیجیتال جابجا می کنند و مهمتر از همه اینکه این نوع کابل صرفا برای انتقال اطلاعات به صورت Half Duplex قابل استفاده است. وقتی می گوئیم روش انتقال Half Duplex است منظور این است که در هر زمان صرفا امکان ارسال سیگنال از طریق یک کامپیوتر وجود دارد و اگر کامپیوتری در حال ارسال سیگنال باشد , کامپیوتر های دیگر باید صبر کنند. مثل دستگاه بی سیم که پلیس از آن استفاده می کند و در صورتی که توجه کرده باشید وقتی یک نفر صحبت می کند دیگران صرفا می توانند گوش کنند.

هر گاه در یک زمان دو کامپیوتر اقدام به ارسال سیگنال نمایند سیگنالها با هم تداخل پیدا کرده و از بین می روند که به این پدیده Collision می گویند. در شبکه هر چه تعداد Collision زیاد شود زمان بیشتری در انتقال اطلاعات تلف می شود , چرا که هر گاه یک سیگنال ایجاد Collision نماید به دلیل از دست دادن ماهیت اطلاعاتی خود باید دوباره توسط کامپیوتر مبداء ارسال شود.

در شبکه Thin Net همانطور که از اسم آن پیداست از کابل باریکتری به نسبت Thick Net استفاده می شود. ساختار کابل Coaxial در شکل سمت زیر نمایش داده شده است.



هسته مرکزی این کابل برای انتقال سیگنالهای اطلاعات استفاده می شود. یک روکش نارسانا از آن حفاظت مـی کنـد و سـپس یـک لایـه از آلیـاژ آلومینیوم به صورت بافته شده از ان حفاظت می کند. تمام این لایه ها در نهایت در روکش پلاستیکی محکمی قرار گرفته اند که در مجموع قطر کابل بین 0.25 اینچ تا 0.60 اینچ متغیر است . در شبکه Thin از کابل با قطر حدودی 0.25 و در شبکه Thick از کابل با قطر حدودی 0.5 استفاده می شود. با توجه به اینکه سلگنالها در هنگام عبور در طول کابل تضعیف می شوند و توان آنها کاهش می یابد , همواره برای انتقال سـیگنالها در مـسیر های بلند تر از تجهیزاتی به نام Repeater استفاده می شود.

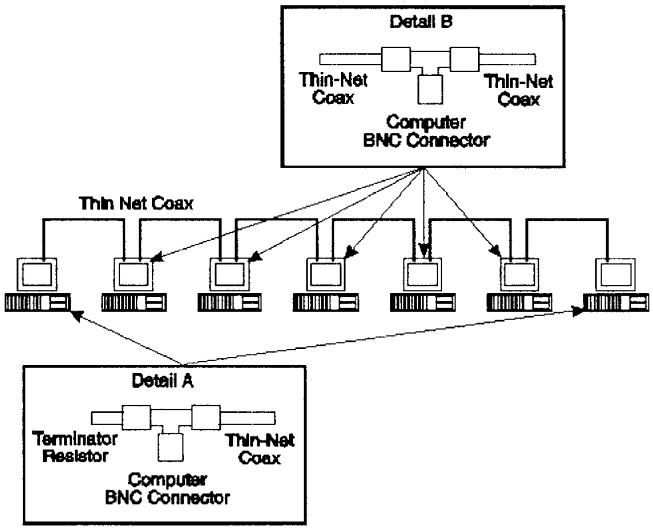
به کاهش توانائی سیگنال , وقتی در حال عبور از کابل می باشد Attenuation گفته می شود. هر چه کابل ضخیم تـر باشـد مقـدار کـاهش تـوان سیگنال در آن کمتر است و نتیجتا می توان در کابلهای با قطر بیشتر , سیگنال را در مسافت های دورتری انتقال داد.

مثلا در کابل Thin هر 185 متر نیاز به تقویت سیگنال وجود دارد اما در کابل Thick هر 500 متر باید سیگنال را توسط Repeater تقویت کرد.

برای اتصال کابلهای Coaxial به کامپیوتر ها و تجهیزات شبکه از Connector های با نام British Naval Connectors (BNC) استفاده می نمایند.

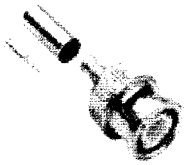
در شبکه های Thin Net کانکتورها همانگونه که در شکل زیر معین شده به کامپیوتر متصل می شوند. در قـسمت Detail B از شـکل زیـر ایـن موضوع به تصویر کشیده شده است که چگونه کابل پس از منشعب شدن برای اتصال یک کامپیوتر ادامه یافته و به کامپیوتر بعدی می رسد.

در Detail A از شکل زیر این موضوع بیان شده که در انتهای کابل برای جلوگیری از Signal Bounce که همـان بازگـشت سـیگنال اسـت , از BNC Terminator استفاده می شود. لازم به ذکر است اگر سیگنال ها در انتهای کابل Terminate نشوند شبکه کلا مختل شده و از کـار بـاز می ایستد. برای همین از یک مقاومت الکتریکی که توان آن 50Ω و یا 75Ω باشد , استفاده می گردد. اندازه این مقاومت به نوع کابل بستگی دارد.

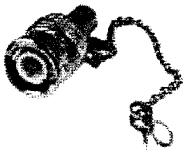


به شکلهای زیر توجه نمائید:

شکل (الف) معرف یک BNC Connector است



شکل (ب) معرف یک BNC Terminator است



شکل (ج) معرف یکBNC T Connector می باشد

شکل(د) معرف یک BNC Barrel Connector است

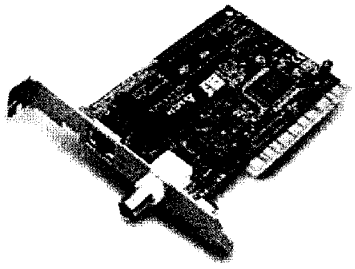
در شبکه های Thick Net با توجه به اینکه از کابل ضخیم تری استفاده می گردد استفاده از کانکتورهای معمولی BNC که در Thin Net استفاده می شد وجود ندارد. کابلهای ضخیم تر انعطاف پذیری کمتری نیز دارند و مسلما برای محیط های داخلی ساختمان که نیاز به انعطاف بیشتر برای عبور از کنار دیوارها داریم , مناسب نخواهند بود. معمولا برای مسافت های بیشتر که حد فاصل بین ساختمانهای نزدیک به هم می باشد و عموما در مخیط های بیرونی از این نوع کابل استفاده می شود.

برای اتصال این نوع کابل به کامپیوتر و یا تجهیزات شبکه از ابزاری به نام Vampire Tap استفاده می کنند که این ابزار با ایجاد سوراخ بر روی بدنه کابل به هسته مرکزی آن متصل می شود. ابزار دیگری به نام External Transceiver به Vampire Tap وصل می شود و از آن کابل دیگری از نوع 15 رشته ای که به کانکتور AUI-DIX DB-15 متصل می گردد , خارج می گردد. این کابل به عنوان یک انشعاب از شبکه می تواند به کامپیوتر متصل گردد.

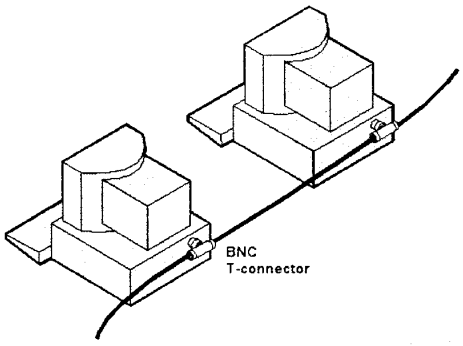
مسلما با توجه به تفاوت بین نوع کابل شبکه و ابزار اتصالی آن , کابل شبکه مورد استفاده در Thin Net و Thick Net نیز از نظر نوع پورت با هم تفاوت دارند.

به شکل زیر توجه فرمائید:

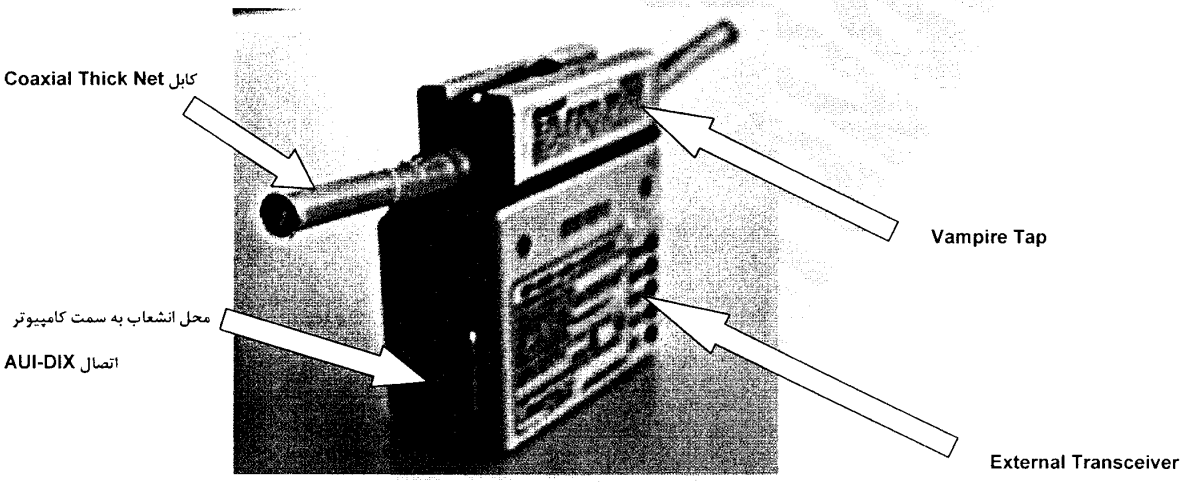
در این شکل کارت شبکه های مورد استفاده در Thin Netو Thick Net با هم مقایسه شده اند.



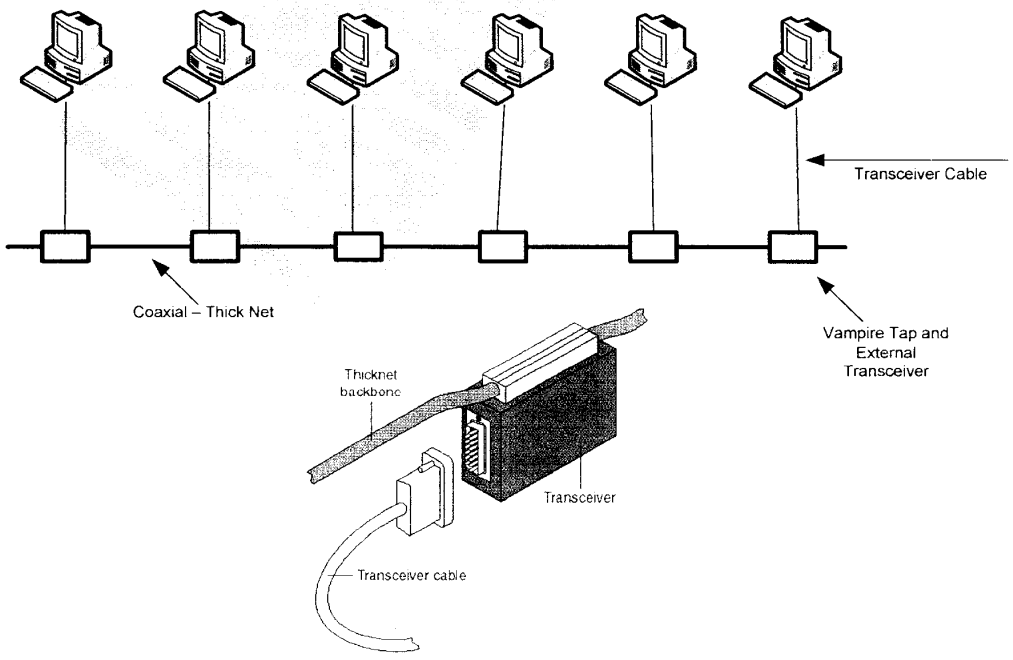
در شکل زیر روش اتصال کامپیوتر ها در شبکه **Thin Net** مشخص شده است:



و در شکل زیر یک **Vampire Tap** همراه با **External Transceiver** آن نمایش داده شده است.



در این شکل روش اتصال و محل استفاده از کابلها و تجهیزات اتصال دهنده معین شده است



جدول زیر هر دو نوع کابل را به صورت ساده با یکدیگر مقایسه می کند.

نوع کابل	Attenuation	نوع سیگنال	فرکانس	پهنای باند	Topology
Thin Net	185	Digital	10 Mhz	10 Mbps	Bus
Thick Net	500	Digital	10 Mhz	10 Mbps	Bus

دسته بندی دیگری که در مورد کابلهای Coaxial وجود دارد , از جهت مواد تشکیل دهنده آن است. در صورتی که بخواهیم برای محیطهای درون اتاق و نزدیک به کف زمین کابل کشی نمائیم از نوع PVC استفاده می کنیم. این نوع کابل در صورت بروز آتش سوزی به سادگی می شوزد و گاز بسیار سمی و کشنده ایجاد می کند.
مدل Plenum برای محیط های داخل سقف و زمین کاذب و کانال های هوا و رایزر کاربرد دارد. این نوع در صورت سوختن گاز سمی ایجاد نمی کند و بی خطر است.

کابلهای Coaxial از نظر مدل بسیار متعدد هستند ولی در این درس باید تعدادی از انها را بشناسیم که عبارتند از:

مدل	کاربرد	نوع سیگنال
RG58 U	شبکه Thin Net – هسته مرکزی یکپارچه Solid Copper Core	Digital
RG58 A/U	شبکه Thin Net – هسته مرکزی رشته Stranded Core	Digital
RG58 C/U	شبکه Thin Net – هسته مرکزی رشته Stranded Core - حفاظت شده در مقابل sniff	Digital
RG 8	شبکه Thick Net	Digital
RG 59	آنتن تلویزیون	Analog
RG 6	دوربین های فیلم برداری حرفه ای	Analog
RG 62	Arc Net	

نکته مهم اینکه در کابل Coaxial حتما باید نقطه انتهائی کابل توسط اتصال به زمین Ground Link از نظر انتقال جریانهای القائی و تشکیل مدار الکتریکی مورد تنظیم قرار گیرد.

RG Number	Cable Description	Size and Strand Nom. D.C.R.	Dielectric O.D. INCHES	Shielding	Jacket Nom. O.D.	Approx. Wgt./M' Lbs.	Nom. IMP. Ohms
RG-6/U Type	Non-Plenum	#18 Solid 7.5 ohm/M'	Foam PE .180	Foil & 60% TC Braid	PVC .270	30	75
RG-6/U Type	CATV Drop Cable	#18 Solid 6.4 ohm/M'	Foam PE .183	Foil & 45% AL Braid	PVC .269	29	75
RG-6/U Type	CATV Drop Cable	#18 Solid 16.3 ohm/M'	Foam PE .180	Foil & 60% AL Braid	PVC .270	29	75
RG-6/U Type	Precision Video Cable	#18 Solid 7.5 ohm/M'	Foam PE .180	Double BC 98% Braid	PVC .288	60	75
RG-6/U Type Plenum	Precision Video Cable	#18 Solid 6.4 ohm/M'	Foam FEP .170	Foil & 63% TC Braid	PRPVC .226	35	75
RG-6/U Type Plenum	Precision Video Cable	#18 Solid 6.4 ohm/M'	Foam FEP .170	Foil & 63% TC Braid	FEP .222	70	75
RG-6A/U Type	Non-Plenum	#21 Solid 32.0 ohm/M'	PE .185	Double BC 97% Braids	PVC .332	79	75
RG-8/U Type Thick-Net®	Computer-Lan DEC 17-00451-00	#12 Solid 1.42 ohm/M'	Foam PE .247	Foil & Double 94%,90% TC Braids	PVC .405	121	50
RG-8/U Type	Non-Plenum	#11 (7/19) 12.0 ohm/M'	Foam PE .280	BC 95% Braid	PVC .398	97	50
RG-8/U Type Plenum Thick-Net®	Computer-Lan DEC 17-00324-00	#12 Solid 1.42 ohm/M'	Foam FEP .247	Double Foil & Double 92% TC Braids	FEP .375	156	50
RG-8A/U Type	Non-Plenum	#11 (7/21) 19.0 ohm/M'	PE .285	BC 97% Braid	PVC .405	108	52
RG-11/U Type	Non-Plenum	#18 (7/26) 6.06 ohm/M'	PE .285	BC 95% Braid	PVC .405	103	75
RG-11/U Type	Non-Plenum	#14 Solid 2.6 ohm/M'	Foam PE .285	BC 97% Braid	PE .405	90	75
RG-11/U Type	Precision Video Cable	#14 Solid 2.6 ohm/M'	Foam PE .285	Foil & 61% TC Braid	PVC .405	76	75
RG-11/U Type	Precision Video Cable	#18 (7/30) 8.1 ohm/M'	PE .285	BC 97% Braid	PVC .405	108	75
RG-11/U Type Plenum	Plenum	#14 Solid 25.0 ohm/M'	Foam FEP .280	Foil & 96% TC Braid	PRPVC .346	79	75
RG-11/U Type Plenum	Precision Video Cable	#14 Solid 2.5 ohm/M'	Foam FEP .274	Foil & 63% TC Braid	FEP .348	80	75
RG-11A/U Type	Non-Plenum	#18 (7/26) 6.06 ohm/M'	PE .285	BC 97% Braid	PVC .405	103	75
RG-22B/U Type	Computer-Lan Twinaxial Cable	#18 (7/26) 2 Cond. 66.0 ohm/M'	PE .285	Double TC 95% Braids	PVC .420	128	95
RG-58/U Type	Non-Plenum	#20 Solid 10.0 ohm/M'	PE .116	TC 95% Braid	PVC .196	26	52
RG-58/U Type Plenum	Plenum	#19 Solid 81.0 ohm/M'	FEP .100	TC 95% Braid	PRPVC .156	21	50
RG-58A/U Type Thin-Net®	Computer-Lan DEC 17-01248-00	#20 (19/32) 8.8 ohm/M'	Foam PE .101	Foil & 95% TC Braid	PVC .183	22	50
RG-58A/U Type	Non-Plenum	#20 (19/32) 8.8 ohm/M"	Foam PE .114	TC 95% Braid	PVC .195	27	50
RG-58A/U Type	Non-Plenum	#20 (19/.0071) 10.8 ohm/M'	PE .116	TC 95% Braid	PVC .195	26	50
RG-58C/U Type	Non-Plenum	#20 (19/.0071) 10.8 ohm/M'	PE .116	TC 95% Braid	NCPVC .195	27	50
RG-58C/U Type Plenum Thin-Net®	Computer-Lan DEC 17-0124-00	#20 (19/32) 8.8 ohm/M'	Foam FEP .095	Foil & 95% TC Braid	FLC .160	25	50
RG-59/U Type	Non-Plenum	#22 Solid 50.0 ohm/M'	PE .146	BC 85% Braid	PVC .242	33	75
RG-59/U Type	Non-Plenum	#22 Solid 50.5 ohm/M	Foam PE .146	BC 95% Braid	PVC .242	34	80
RG-59/U Type	Non-Plenum	#22 (7/30) 15.0 ohm/M'	Foam PE .146	BC 95% Braid	PVC .242	35	75
RG-59/U Type	Precision Video Cable	#23 Solid 47.0 ohm/M'	PE .146	BC 95% Braid	PVC .242	39	75
RG-59/U Type	Precision Video Cable	#20 Solid 10.0 ohm/M'	PE .200	Double TC 98% Braids	PE .304	141	75
RG-59/U Type	Precision Video Cable	#23 Solid 47.0 ohm/M'	Foam PE .146	BC 95% Braid	PVC .242	41	75
RG-59/U Type	Precision Video Cable	#22 (7/30) 15.0 ohm/M'	Foam PE .146	BC 95% Braid	PVC .242	34	75
RG-59/U Type	Precision Video Cable	#20 Solid	Foam PE	BC 95%	PVC	36	75

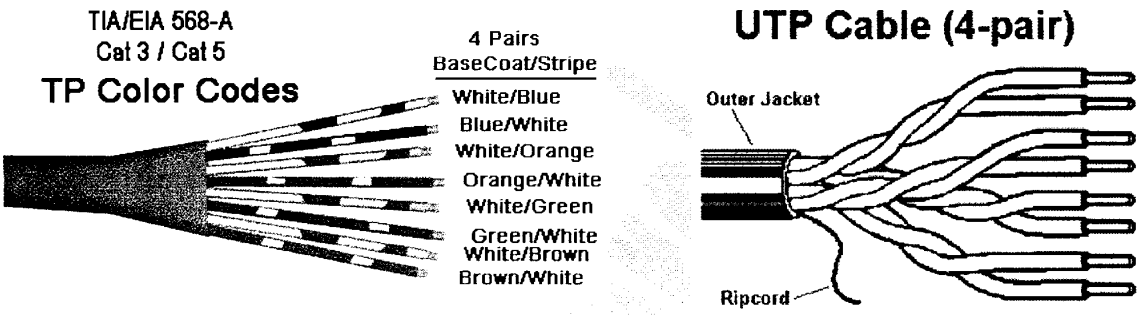
		10.0 ohm/M'	.146	Braid	.242		
RG-59/U Type	Precision Video Cable	#20 Solid 10.0 ohm/M'	Foam PE .143	BC 95% Braid	PE .242	30	75
RG-59/U Type	Precision Video Cable	#20 Solid 10.0 ohm/M'	Foam PE .143	BC 95% Braid	PVC .242	32	75
RG-59/U Type	Precision Video Cable	#20 Solid 10.0 ohm/M	Foam PE .146	BC 95% Braid	PVC .242	32	75
RG-59/U Type	Computer-Lan Duplex-Coax Cable	#23 Solid 2/C Parallel 47.0 ohm/M'	Foam PE .146	BC 95% Braid	PVC .242	81	75
RG-59/U Type	CATV Drop Cable	#20 Solid 25.9 ohm/M'	Foam PE .146	Foil & 40% AL Braid	PVC .242	24	75
RG-59/U Type	CATV Drop Cable	#20 Solid 25.9 ohm/M'	Foam PE .146	Foil & 67% AL Braid	PVC .242	24	75
RG-59/U Type Plenum	Plenum	#20 Solid 26.0 ohm/M'	Foam FEP .140	Foil & 95% TC Braid	PRPVC .198	33	75
RG-59/U Type Plenum	Precision Video Cable	#22 (7/30) 15.0 ohm/M'	Foam FEP .135	BC 95% Braid	FEP .193	42	75
RG-59/U Type Plenum	Precision Video Cable	#20 Solid 10.0 ohm/M'	Foam FEP .135	Foil & 95% TC Braid	PRPVC .199	30	75
RG-59/U Type Plenum	Precision Video Cable	#20 Solid 10.0 ohm/M'	FEP .185	Double TC 98% Braids	FLC .271	33	75
RG-59/U Type Plenum	Precision Video Cable	#20 Solid 34.5 ohm/M'	Foam FEP .140	Double BC 95% Braids	FLC .246	33	75
RG-59B/U Type	Non-Plenum	#23 Solid 50.5 ohm/M'	Foam PE .146	BC 95% Braid	PVC .242	35	75
RG-62/U Type Plenum	Plenum	#22 Solid 41.2 ohm/M'	FEP .146	BC 95% Braid	PRPVC .202	30	93
RG-62A/U Type	Computer-Lan IBM 323921	#22 Solid 41.2 ohm/M'	PE .146	BC 95% Braid	PVC .240	37	93
RG-62A/U Type Plenum	Plenum	#22 Solid 41.2 ohm/M'	Foam FEP .142	Foil & 96% TC Braid	PRPVC .197	40	93
RG-108A/U MIL-C-17D	Twinaxial Cable MIL-C-17D	#20 (7/28) 2 Cond. 9.5 ohm/M'	PE .078	TC 90% Braid	PVC .235	36	78
RG-142B/U MIL-C-17D	High Temperature MIL-C-17D	.037 Solid 19.5 ohm/M	PTFE .116	SPC 95% Braid	FEP .071	50	50
RG-174/U Type	Non-Plenum	#26 (7/34) 9.7 ohm/M'	PE .060	BC 90% Braid	PVC .110	9	50
RG-178B/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .033	SPC 95% Braid	FEP .071	6	50
RG-179B/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .063	SPC 95% Braid	FEP .100	10	75
RG-180B/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .102	SPC 95% Braid	FEP .142	2	95
RG-187B/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .063	SPC 95% Braid	TFE (TW) .111	11	75
RG-188A/U MIL-C-17D	High Temperature MIL-C-17D	.020 (7/.0067) 84.1 ohm/M'	PTFE .058	SPC 95% Braid	TFE (TW) .108	13	50
RG-195A/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .102	SPC 95% Braid	TFE (TW) .155	6	95
RG-196A/U MIL-C-17D	High Temperature MIL-C-17D	.012 (7/38) 245.0 ohm/M'	PTFE .034	SPC 95% Braid	TFE (TW) .080	10	50
RG-213/U Type	Non-Plenum	#13 (7/21) 1.73 ohm/M'	PE .285	BC 96% Braid	PVC .405	105	50
RG-214/U Type	Non-Plenum	#13 (7/21) 1.73 ohm/M'	PE .285	Double SPC 96%Braids	PVC .425	141	50
RG-223/U Type MIL-C-17D	Mil-Spec	#19 Solid 8.05 ohm/M'	PE .116	Double SPC 96%Braids	NCPVC .210	39	50
RG-316/U MIL-C-17D	High Temperature MIL-C-17D	.020 (7/.0067) 84.1 ohm/M'	PTFE .060	SPC 95% Braid	FEP .098	11	50

Key Insulations:
PVC = Polyvinyl Chloride
NCPVC = Non-Contaminating Polyvinyl Chloride
PRPVC = Plenum Rated Polyvinyl Chloride
PE = Polyethylene
Foamed PE = Gas Injected Polyethylene
FLC = Fluorocopolymer
FEP = Teflon® FEP
Foamed FEP = Gas Injected Teflon® FEP
PTFE = Teflon® PTFE
TFE = Teflon® TFE
TFE (TW) = Tape Wraped Teflon® TFE

کابل کشی توسط کابل **Twisted Pair**

کابلهای **TP** یا **Twisted Pair** از نظر ساختار کاملا متفاوت از کابلهای دیگر می باشند و در آن به جای انتقال اطلاعات بر روی یک سیم ، از چند رشته سیم استفاده شده است.

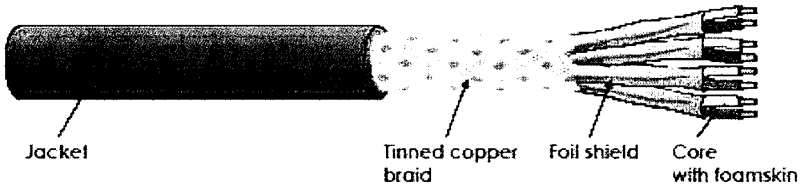
همانگونه که در شکل نیز معین شده است هر رشته سیم دارای یک روکش رنگی نازک است و تمام رشته به همراه هم در پوششی از جنس پلاستیک محافظت می شود. البته بعضا در مدل های متفاوت این کابل از لایه های محافظ اضافه تری نیز استفاده می شود.



کابلهای **Twisted Pair** دارای انواع متفاوتی هستند که عبارتند از:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**
- **Shielded Foiled Twisted Pair (SFTP)**
- **Foiled Twisted Pair (FTP)**

در شکل زیر نمائی از کابل **STP** نمایش داده شده است. کابل **STP** زیر لایه پلاستیکی دارای یک لایه بافته شده **Shield** است که جهت جذب سیگنالهای نویز و انتقال آن به زمین کاربرد دارد.

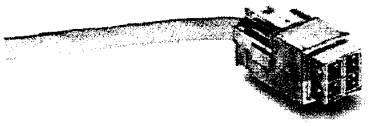


در عین حال کابلهای **Twisted Pair** بر اساس توان انتقال سیگنال و فرکانس و پهنای باند نیز تقسیم بندی می شوند کـه اینگونـه دسـته بنـدی اصطلاحا **Category** کابل نامیده می شود.

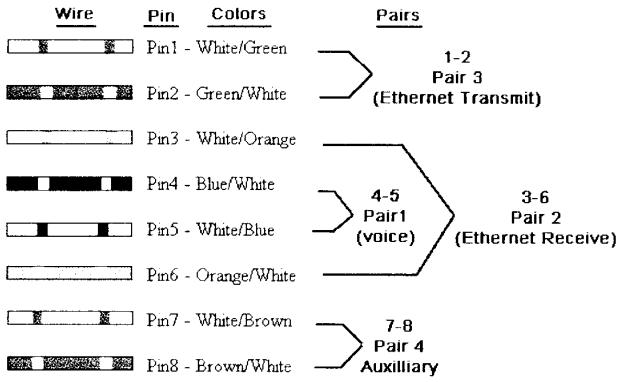
Category	Frequency	Bandwidth	Wire Pairs	شرح مختصر	Connector type
Cat 1	1 Mhz	---------	2	PSTN and ISDN BRI	RJ-11
Cat 2	1 Mhz	4Mbps	4	IBM Token Ring	RJ-45
Cat 3	16 Mhz	10Mbps	4	Ethernet Network , 3 twists per feet	RJ-45
Cat 4	20 Mhz	16Mbps	4	Ethernet Network	RJ-45
Cat 5	100 Mhz	100 Mbps	4	Ethernet Network	RJ-45
Cat 5 e	Up to 250 Mhz	100/1000 Mbps	4	Ethernet Network	RJ-45
Cat 6	Up to 400 Mhz	100/1000/10000 Mbps	4	Ethernet Network	RJ-45
Cat 7	600 – 700 Mhz	100/1000/10000 Mbps	4	Ethernet Network	RJ-45

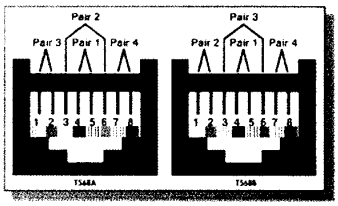
در این شکل نمائی از کانکتور **RJ-45** مشخص شده است .

در کابلهای **Cat 7** مدل کانکتور مقداری تغییر کرده که در شکل زیر مشخص گردیده.



ترتیب رنگ بندی کابلهای **TP** به صورت زیر می باشد.





Cable Types

There are three primary types of cable used to build LANs: coaxial, twisted-pair, and fiber optic. Coaxial and twisted-pair cables are copper-based and carry electrical signals and fiber optic cables use glass or plastic fibers to carry light signals.

Coaxial Cable

Coaxial cable is so named because it contains two conductors within the sheath. Unlike other two-conductor cables, however, coaxial cable has one conductor inside the other, as illustrated in Figure 2.7. At the center of the cable is the copper core that actually carries the electrical signals. The core can be solid copper or braided strands of copper. Surrounding the core is a layer of insulation, and surrounding that is the second conductor, which is typically made of braided copper mesh. This second conductor functions as the cable's ground. Finally, the entire assembly is encased in an insulating sheath made of PVC or Teflon.

CAUTION

The outer sheath—also called a casing—of electrical cables can be made of different types of materials, and the sheath you use should depend on local building codes and the location of the cables in the network's site. Cables that run through a building's air spaces (called *plenums*) usually must have a sheath made of a material that doesn't generate toxic gases when it burns. Plenum cable costs more than standard PVC-sheathed cable and is somewhat more difficult to install, but it's an important feature that should not be overlooked when you are purchasing cable.

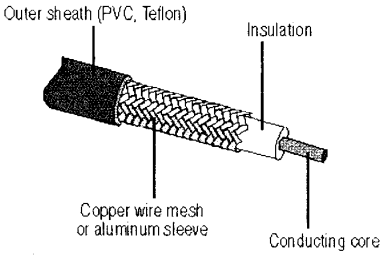


Figure 2.7 - Coaxial *cable consists of two electrical conductors sharing the same axis, with insulation in between and encased in a protective sheath*

There are two types of coaxial cable that have been used in local area networking: RG-8, also known as thick Ethernet, and RG-58, which is known as thin Ethernet. These two cables are similar in construction but differ primarily in thickness (0.405 inches for RG-8 versus 0.195 inches for RG-58) and in the types of connectors they use (N connectors for RG-8 and bayonet-Neill-Concel man [BNC] connectors for RG-58). Both cable types are wired using the bus topology.

Because of their differences in size and flexibility, thick and thin Ethernet cables are installed differently. On a thick Ethernet network, the RG-8 cable usually runs along a floor, and separate AUI cables run from the RG-8 trunk to the network interface adapter in the computer. The RG-58 cable used for thin Ethernet networks is thinner and much more flexible, so it's possible to run it right up to the computer's network interface, where it attaches using a T fitting with a BNC connector to preserve the bus topology.

NOTE

Thick Ethernet and thin Ethernet are also known as *10Base5* and *10Base2,* respectively. These abbreviations indicate that the networks on which they are used run at 10 Mbps, use baseband transmissions, and are limited to maximum cable segment lengths of 500 and 200 (actually 185) meters, respectively.

Coaxial cable is used today for many applications, most noticeably cable television networks. It has fallen out of favor as a LAN medium due to the bus topology's fault-tolerance problems and the size and relative inflexibility of the cables, which make them difficult to install and maintain.

Twisted-Pair Cable

Twisted-pair cable wired in a star topology is the most common type of network medium used in LANs today. Most new LANs use UTP cable, but there is also a shielded twisted pair (STP) variety for use in environments more prone to electromagnetic interference. Unshielded twisted pair cable contains eight separate copper conductors, as opposed to the two used in coaxial cable. Each conductor is a separate insulated wire, and the eight wires are arranged in four pairs, twisted at different rates. The twists prevent the signals on the different wire pairs from interfering with each other (called *crosstalk*) and also provide resistance to outside interference. The four wire pairs are then encased in a single sheath, as shown in Figure 2.8. The connectors used for twisted-pair cables are called RJ45s; they are the same as the RJ11 connectors used on standard telephone cables, except that they have eight electrical contacts instead of four or six.

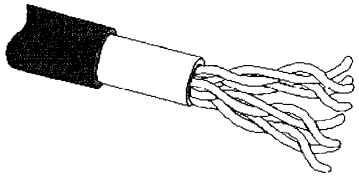


Figure 2.8 UTP *cable has four separate wire pairs, each individually twisted, enclosed in a protective sheath*

Twisted-pair cable has been used for telephone installations for decades; its adaptation to LAN use is relatively recent. Twisted-pair cable has replaced coaxial cable in the data networking world because it has several distinct advantages. First, because it contains eight separate wires, the cable is more flexible than the more solidly constructed coaxial cable. This makes it easier to bend, which simplifies installation. The second major advantage is that there are thousands of qualified telephone cable installers who can easily adapt to installing LAN cables as well. In new construction, the same contractor often installs telephone and LAN cables simultaneously.

UTP Cable Grades

Unshielded twisted pair cable comes in a variety of different grades, called *categories* by the Electronics Industry Association (EIA) and the Telecommunications Industry Association (TIA), the combination being referred to as EIA/TIA. These categories are listed in Table 2.1. The two most significant UTP grades for LAN use are Category 3 and Category 5. Category 3 cable was designed for voice-grade telephone networks and eventually came to be used for Ethernet. Category 3 cable is sufficient for 10-Mbps Ethernet networks (where it is called 10Base-T), but it is generally not used for Fast Ethernet (except with special equipment). If you have an existing Category 3 cable installation, you can use it to build a standard Ethernet network, but virtually all new UTP cable installations today use at least Category 5 cable.

CAUTION

Most Ethernet networks use only two of the four wire pairs in the UTP cable, one for transmitting data and one for receiving it. However, this does not mean that you are free to utilize the other two pairs for another application, such as voice telephone traffic. The presence of signals on the other two wire pairs is almost certain to increase the amount of crosstalk on the cable, which could lead to signal damage and data loss.

Table 2.1 EIA/*TIA UTP Cable Categories*

Category	Use
1	Voice-grade telephone networks only; not for data transmissions
2	Voice-grade telephone networks, as well as IBM dumb-terminal connections to mainframe computers
3	Voice-grade telephone networks, 10-Mbps Ethernet, 4-Mbps Token Ring, 100Base-T4 Fast Ethernet, and 100Base-VG-AnyLAN
4	16-Mbps Token Ring networks
5	100Base-TX Fast Ethernet, Synchronous Optical Network (SONET), and Optical Carrier (OC3) Asynchronous Transfer Mode (ATM)
5e	1000Base-T (Gigabit Ethernet) networks

TIP

When you install a network with a particular grade of cable, you must be aware of more than the category of the cable. You must also be sure that all of the connectors, wall plates, and patch panels you use are rated for the same category as the cable. A network connection is only as strong as its weakest link.

Category 5 UTP is suitable for 100Base-TX Fast Ethernet networks running at 100 Mbps, as well as for slower protocols. The standard for Category 5e UTP cable was ratified in 1999 and is intended for use on 1000Base-T networks. 1000Base-T is the Gigabit Ethernet standard designed to run on UTP cable with 100-meter segments, making it a suitable upgrade path from Fast Ethernet. The Category 5e standard does not call for an increase in the frequency supported by the cable over that of Category 5 (both are 100 MHz), but it does elevate the requirements for some of the other Category 5 testing parameters and adds other new parameters. In addition to the officially ratified EIA/TIA categories, there are other UTP cable grades available that have not yet been standardized. A series of numbered cable standards (called levels) from Anixter, Inc. is currently being used as the basis for UTP cables that go beyond the performance levels of Category 5e.

NOTE

There is a Fast Ethernet protocol called 100Base-T4 that is designed to use Category 3 UTP cable and run at 100 Mbps. This is possible because 100Base-T4 uses all four wire pairs in the cable, whereas 100Base-TX uses only two pairs..

STP Cable Grades

Shielded twisted pair cable is similar in construction to UTP, except that it has only two pairs of wires and it also has additional foil or mesh shielding around each pair. The additional shielding in STP cable makes it preferable to UTP in installations where electromagnetic interference is a problem, often due to the proximity of electrical equipment. IBM, which developed the Token Ring protocol that originally used them, standardized the various types of STP cable. STP networks use Type 1A cables for longer runs and Type 6A cables for patch cables. Type 1A contains two pairs of 22 gauge solid wires with foil shielding, and Type 6A contains two pairs of 26 gauge stranded wires with foil or mesh shielding. Token Ring STP networks also use large, bulky connectors called IBM data connectors (IDCs). However, most Token Ring LANs today use UTP cable.

Wireless Topologies

The term *topology* usually refers to the arrangement of cables that forms a network, but it doesn't have to. Although wireless networks use what are called *unbounded media,* the computers still have specific patterns they use to communicate with each other. Wireless LANs have two basic topologies, the ad hoc topology and the infrastructure topology. In the *ad hoc topology,* a group of computers are all equipped with wireless network interface adapters and are able to communicate freely with each other. This provides complete freedom of movement for all of the computers on the network, as long as they remain inside the communication range of the wireless technology. This topology is useful for a home or small business network that consists of only a handful of computers, and for which the installation of cables is inconvenient, impractical, or impossible.

An infrastructure network consists of wireless-equipped computers that communicate with a network using wireless transceivers connected to the LAN by standard cables. These transceivers are called *network access points.* In this arrangement, the wireless computers do not communicate directly with each other. Instead, they communicate only with the cabled network via the network access points. This topology is better suited to a larger network that has only a few wireless computers, such as laptops belonging to traveling users. These users have no need to communicate with each other; instead, they use the wireless connection to access servers and other resources on the corporate network.

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه سوم

نام استاد : مهندس امرآبادی

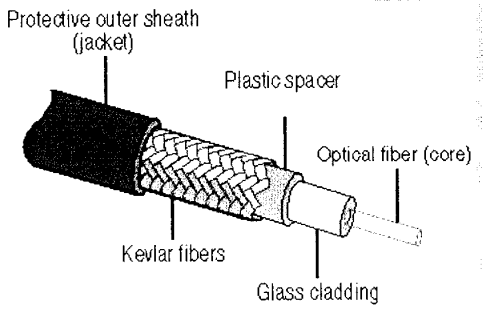
MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه سوم :

- ادامه بحث کابل
  - کابلهای فیبر نوری
- ساختار ارسال اطلاعات در شبکه
- گزیده مطالب درسی به زبان اصلی

✸فیبر نوری

در ادامه بحث کابل و کابل کشی در حد ساده با فیبرهای نوری آشنا می شویم. فیبرهای نوری از تکنولوژی کاملا متفاوت استفاده می کنند . در کابلهای عادی از سیگنالهای **Electromagnetic** استفاده می شود. اما در فیبرهای نوری از نور و لیزر برای انتقال اطلاعات در طول کابل استفاده می شود. مسلما جنس ماده انتقال دهنده سیگنال در کابل عادی فلزی است . اما در فیبر نوری از چیزی شبیه به شیشه که شفاف و نارسانا است استفاده می شود. با توجه به اینکه سیگنال های نور و یا لیزر نیاز به رسانا بودن ندارند و به شفافیت جنس هادی نیاز دارند جنس شیشه برای این موضوع مناسب است.



با توجه به شکننده بودن و باریک بودن هسته مرکزی فیبر ، از لایه های محافظ با خواص متفاوت برای آن استفاده می شود.

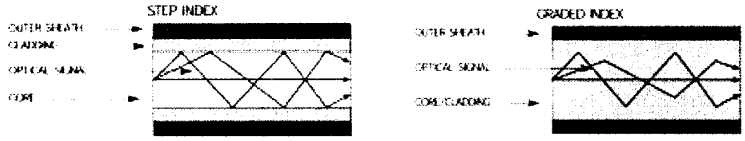
محافظت در مقابل خمش ، فشار ، برش ، رطوبت ، موجودات جونده و ... در مورد فیبر نوری اعمال می شود زیرا که به دلیل امکان استفاده از فیبر نوری در فواصل طولانی و زیر زمین و آب دریا و... معمولا این نوع کابل از محیط های متفاوتی عبور می کند و با خطرات متفاوتی روبرو است.

فیبر نوری در دو نوع وجود دارد:

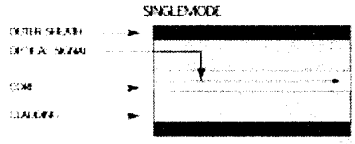
- **Multi Mode**
  - **50 /125 µm**
  - **62.5/125 µm**
- **Single Mode**
  - **9/125 µm**

با توجه به روش **Distribution** نور در داخل فیبر نوری که در فیبرهای **Single Mode** به صورت مستقیم انجام می پذیرد نیاز است فیبر های از این نوع بیشتر از اندازه استاندارد تعیین شده برای کابل خمش پیدا نکنند.

در صورتی که به شکل زیر توجه فرمائید می بینید که پایه انتقال اطلاعات در فیبر نوری شکست نور در داخل هسته شیشه ای یا پلاستیکی شفاف درون کابل است. این شکل شکست نور را در مدل **Multi Mode** نمایش می دهد.



در مدل **Single Mode** نور به صورت مستقیم به درون هسته مرکزی تابانده می شود. به شکل زیر توجه کنید :

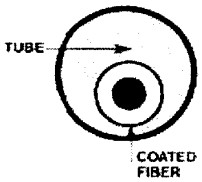


کاربرد های فیبرهای نوری از نظر محیطی به صورت زیر می باشد :

- **Outdoor**
- **Indoor**
- **Indoor/Outdoor**

تعریف لایه محافظ **Loose-Tube** :

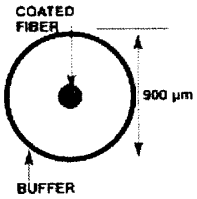
در برخی از انواع فیبر نوری با توجه به اینکه تا حد امکان باید از خمیدگی بیش از حد هسته مرکزی فیبر جلوگیری نمائیم در لایه های محافظ فیبر از یک پوسته که درون آن یک نوع ژل مایع وجود دارد استفاده می شود. این لایه اجازه می دهد که هسته مرکزی حد فاصل جدار در برگیرنده ژل معلق باشد و در هنگام خمش یا حرکت دادن کابل از فشار به هسته مرکزی جلوگیری می کند.



تعریف لایه محافظ **Tight Buffered** :

درون برخی مدل های فیبر نوری از یک لایه محافظ که رشته های باریک نخ نایلونی است استفاده می شود . این نخ های بسیار باریک نایلونی نیز محیطی مناسب را برای هسته مرکزی فیبر فراهم می کنند که امکان خمش فیبر بدون آسیب دیدن هسته مرکزی , در این محدوده بیشتر باشد.

در عین در صورت فشار آمدن به فیبر محدوده تحمل فشار فیبر بیشتر می گردد.

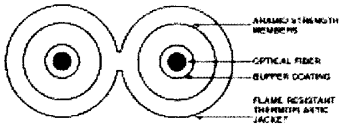


به طور کلی فیبرهای نوری به سه دسته اصلی تقسیم می شوند که عبارتند از:

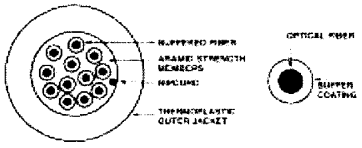
- **Interconnect Cables**
- **Distribution Cables**
- **Breakout Cables**

کابلهای **Interconnect** برای ارتباط تجهیزات به یکدیگر کاربرد دارد. امکان خمش آن بسیار زیاد و رویه آن پلاستیک نرم می باشد. این کابلها معمولا در **Rack** برای ارتباط **Patch Panel** با **Switch** کاربرد دارد و یا برای اتصال کامپیوترهای مجهز به کارت شبکه فیبر نوری با تجهیزات شبکه بکار میرود.این نوع فیبر دارای دو رشته کنار هم می باشد که یکی برای ارسال و دیگری برای دریافت کاربرد دارد.

به شکل روبرو توجه فرمائید:



کابلهای **Distribution** برای ارتباطات درون ساختمان ,از محل ورود کابل های **Backbone** به ساختمان تا محل قرار گرفتن تجهیزات اتصال مانند **Switch** ها در **Rack** استفاده می شوند. این نوع فیبر دارای توانائی خمش کمتری به نسبت کابلهای نوع قبل می باشو و تعداد زوج فیبرهای درون آن زیاد است. به شکل زیر توجه فرمائید:

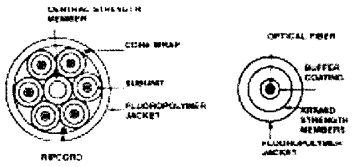


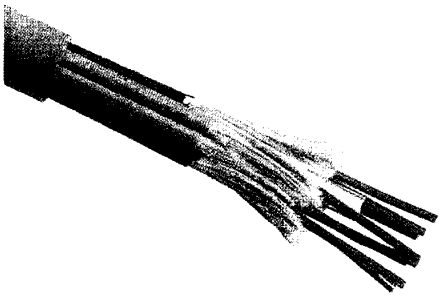
فیبرهای نوع **Breakout** :

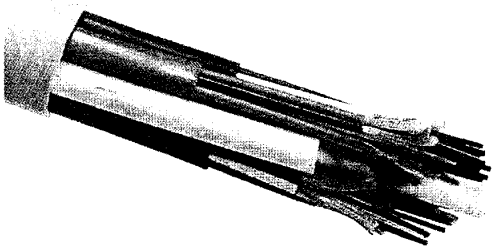
در این نوع فیبر که مدل ها و تعداد هسته فیبرهای درونی آن متفاوت هستند امکان خم کردن کابل وجود ندارد. این نوع کابل دارای تعداد زیادی زوج فیبر می باشد که برای مسیرهای طولانی و ارتباط بین مجموعه های اطلاعاتی کاربرد دارد. مدل های مختلف آن برای زیر خاک و یا زیر آب دریا و دریاچه ها طراحی و ساخته می شوند. رویه ضخیم و مقاوم و لایه های متعدد , از مشخصات اصلی این نوع کابل است.

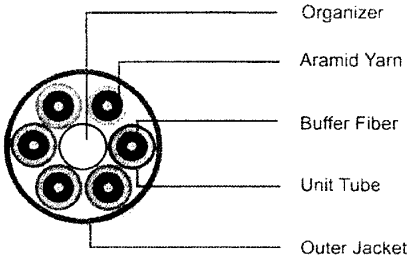
در قسمت وسطی کابل یک هسته غیر قابل انعطاف وجود دارد که فیبرهای انتقال اطلاعات در پوشش های جدا از هم به صورت موازی کنار آن قرار دارند. این قسمت جلوی خمش کابل را می گیرد و از ایجاد شکستگی در آن جلوگیری می کند.

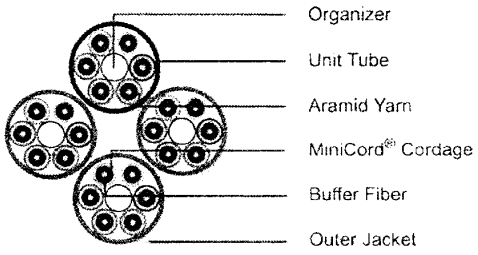
زیر پوشش پلاستیکی روئی کابل یک قسمت فلزی بسیار سخت قرار دارد که به آن **Mechanical** می گویند. مشخصات این قسمت که گویای مقدار مقاومت آن در مقابل فشارهای جانبی به کابل است متنوع بوده و از این بابت بسته به کارائی که هر نوع کابل دارد از پوشش های قوی تر یا ضعیف تر استفاده می شود. به شکل زیر توجه فرمائید:





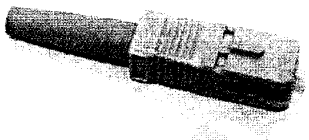


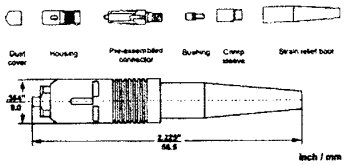




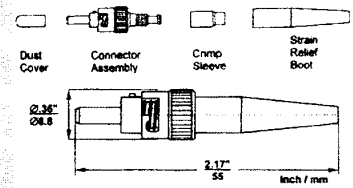
به شکلهای زیر توجه نمائید. تعدادی از کانکتورهای فیبر نوری که بیشتر مورد استفاده قرار می گیرند در شکل نمایش داده شده است.

- **SC** (subscriber connector)



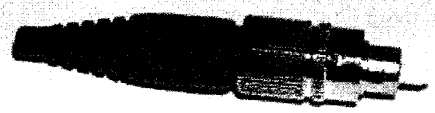


- **ST** (Straight Tip)



- **LC**

- **FC**



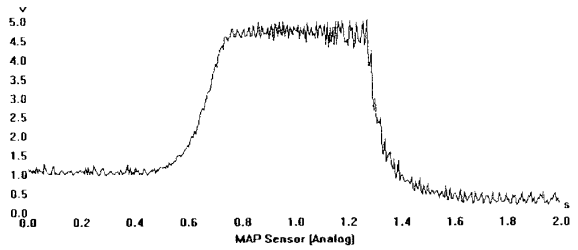
✹ساختار ارسال اطلاعات در شبکه

همانگونه که می دانید در شبکه اطلاعات به صورت سیگنال ارسال و دریافت می شود. یک سیگنال می تواند دارای ارزش باینری صفر ویا یک باشد و به همین دلیل نمی توان انتظار داشت که مبداء و مقصد یک سیگنال معلوم باشد. هر سیگنال بر روی **Media** که انتقال دهنده آن فرض می شود به همه جهت و برای تمام **Node** های دیگری که به آن **Media** متصل هستند ارسال می شود. اما اگر قرار بر این باشد که بر این اساس شنونده در یابد که چه کسی آن سیگنال را فرستاده است , مسلما امکان این کار وجود ندارد و نتیجتا سیگنال به صورت واحد ارزشی ندارد.

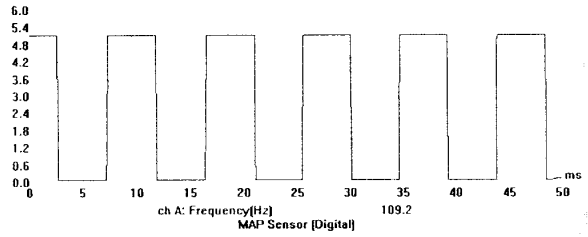
سلگنالها به دو صورت کلی تقسیم می شوند که عبارتند از :

- **Analog (Broadband)**
- **Digital (Base band)**

سیگنالهای آنالوگ شکل مشابه مثال زیر دارند:



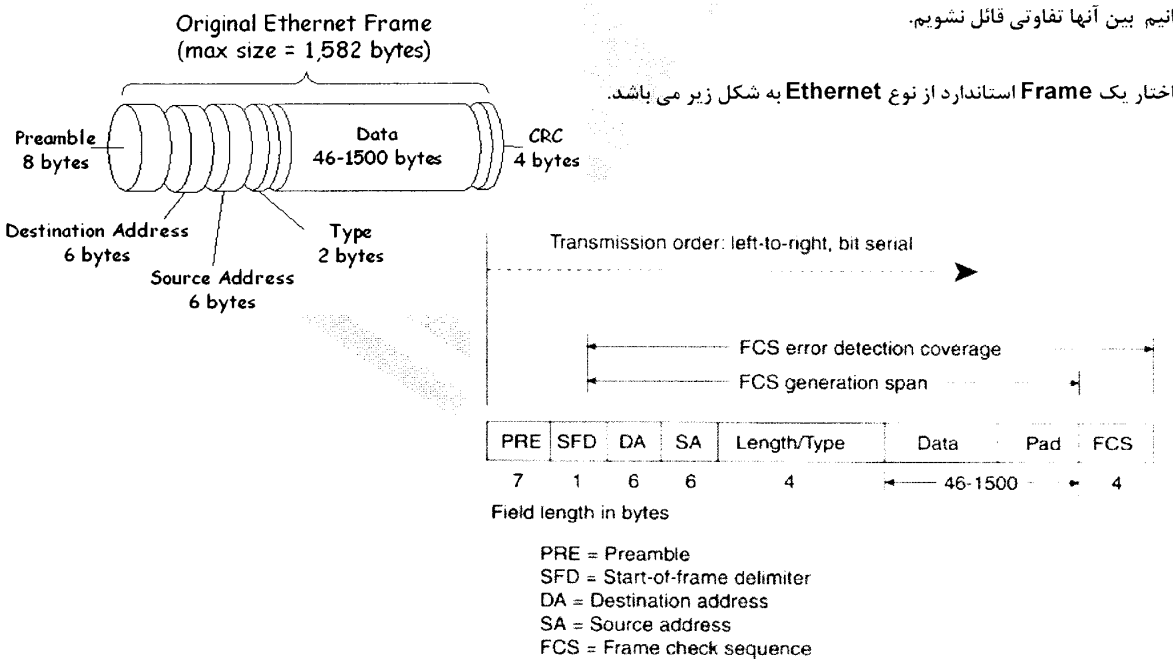
سیگنالهای دیجیتال به صورت زیر می باشند:



برای ارسال اطلاعات سیگنالها در فرم و قالب تعریف شده ای طبق استاندارد توسط کامپیوتر ارسال کننده مرتب می شوند به صورت پشت سر هم ارسال می شوند . در نتیجه کامپیوتر های شنونده با واقف بودن به ترتیب ارسال اطلاعات و درک اینکه چه ساختاری در سیگنالهای مرتب شده دریافتی , وجود دارد می توانندآنرا ارزش دهی نمایند و پس از معین شدن مبداء ومقصد به تحلیل اطلاعات موجود درآن بپردازند.

به این ساختار **Packet** ویا **Frame** گفته می شود . البته قابل ذکر است **Packet** و **Frame** با هم تفاوت دارند ولی فعلا در حد این درس می توانیم بین آنها تفاوتی قائل نشویم.

ساختار یک **Frame** استاندارد از نوع **Ethernet** به شکل زیر می باشد.



آدرس دهی در کامپوترهای شبکه:

هر کامپیوتر که دارای کارت شبکه می باشد برای ارسال اطلاعات در شبکه از آدرسی که شناسه آن کامپیوتر در شبکه است استفاده می نماید. این آدرس توسط کارخانه سازنده کارت شبکه در Firmware آن کارت شبکه ثبت شده است و قابل تغییر نمی باشد. هر کامپیوتر در هنگام ارسال اطلاعات در شبکه آدرس مبداء و مقصد را بر طبق این روش آدرس دهی بر روی Frame قرار می دهد. این آدرس MAC Address نامیده می شود که 48 بیتی است و به صورت 12 رقمی در مبنای 16 نوشته می شود. مثل : 00-E0-4C-BB-07-37

همانگونه در مثال مشاهده کردید هر دو رقم از MAC Address توسط یک خط تیره از ارقام قبل و بعد جدا شده. ارزش هر تک رقم در مبنای 16 بین 0 تا F تغییر می کند.

هر Frame در شبکه می توان به یکی از سه روش زیر ارسال گردد.

الف) Unicast :

در این روش هر Packet از مبداء به یک مقصد مشخص ارسال می گردد. در حقیقت در این روش مبداء اطلاعات را برای یک مقصد خاص ارسال می کند و نمی خواهد این اطلاعات را کامپیوتر دیگری غیر از مقصد در شبکه دریافت کند.

ب) Broadcast :

در این روش هر Packet از مبداء به مقصد همه node های شبکه ارسال می گردد. هر گاه کامپیوتری در شبکه بخواهد اطلاعاتی را برای همه ارسال کند اقدام به ارسال Packet های Broadcast می نماید.

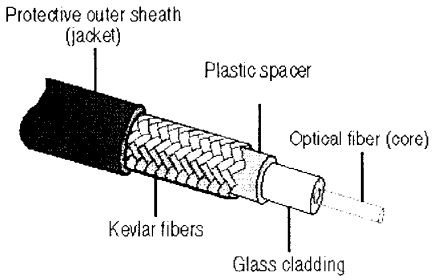
ج) Multicast :

در این روش مبداء Packet را به روشی آدرس دهی می کند که برای گروهی از کل کامپیوتر ها ارسال گردد. اصطلاحا این نوع Packet از یک مبداء به تعدادی از کل (یک گروه) ارسال می شود.

Fiber Optic Cable

Fiber optic cable is a completely different type of network medium than twisted-pair or coaxial cable. Instead of carrying signals over copper conductors in the form of electrical voltages, fiber optic cables transmit pulses of light over a glass or plastic filament. Fiber optic cable is completely resistant to the electromagnetic interference that so easily affects copper-based cables. Fiber optic cables are also much less subject to *attenuation*—the tendency of a signal to weaken as it travels over a cable—than are copper cables. On copper cables, signals weaken to the point of unreadability after 100 to 500 meters (depending on the type of cable). Some fiber optic cables, by contrast, can span distances up to 120 kilometers without excessive signal degradation. Fiber optic cable is thus the medium of choice for installations that span long distances or connect buildings on a campus. Fiber optic cable is also inherently more secure than copper because it is impossible to tap into a fiber optic link without affecting normal communication over that link.

A fiber optic cable, illustrated in Figure 2.9, consists of a clear glass or a clear plastic core that actually carries the light pulses, surrounded by a reflective layer called the *cladding.* Surrounding the cladding is a plastic spacer layer, a protective layer of woven Kevlar fibers, and an outer sheath.



There are two primary types of fiber optic cable, single mode and multimode, with the thickness of the core and the cladding being the main difference between them. The measurements of these two thicknesses are the primary specifications used to identify each type of cable. Single mode fiber typically has a core diameter of 8.3 microns, and the thickness of the core and cladding together is 125 microns. This is generally referred to as 8.3/125 single mode fiber. Most of the multimode fiber used in data networking is rated as 62.5/125.

Single mode fiber uses a single-wavelength laser as a light source, and as a result, it can carry signals for extremely long distances. For this reason, single mode fiber is more commonly found in outdoor installations that span long distances, such as telephone and cable television networks. This type of cable is less suited to LAN installations because it is much more expensive than multimode cable and it has a higher bend radius, meaning that it cannot be bent around corners as tightly. Multimode fiber, by contrast, uses a light-emitting diode (LED) as a light source instead of a laser and carries multiple wavelengths. Multimode fiber cannot span distances as long as single mode, but it bends around corners better and is much cheaper. Fiber optic cables use one of two connectors, the straight tip (ST) connector or the subscriber connector (SC), as shown in Figure 2.10.

Installing fiber optic cable is very different from copper cable installation. The tools and testing equipment required for installation are different, as are the cabling guidelines. Generally speaking, fiber optic cable is more expensive than twisted-pair or coaxial cable in every way, although prices have come down in recent years.

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه چهارم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه چهارم :

- روش ارسال و دریافت اطلاعات در شبکه
- موسسه استاندارد جهانی (ISO)
- استاندارد تعیین شده برای ارتباطات شبکه ای

✸روش ارسال و دریافت اطلاعات در شبکه

همانگونه که قبلا نیز بیان شد ، اطلاعات در مدیا به صورت سیگنال و بیت به بیت ارسال می شوند . با توجه به اینکه یک بیت به تنهائی ارزش اطلاعاتی نخواهد داشت و مبداء و مقصد آن نیز معلوم نمی گردد ، ساختاری به عنوان **Packet** تعریف گریده است که ترکیبی از بیت های ارسالی به صورت پشت سر هم می باشد. در این ساختار طبق توضیحاتی که در قسمتهای قبلی نیز ارائه شد آدرس مبداء و مقصد و اطلاعات و ... موجود می باشد که با توجه به مبتنی بودن این ساختار به استاندارد های جهانی تمام کامپیوتر های عضو شبکه طبق این مند رفتار می کنند و نتیجتا می توانند با یکدیگر ارتباط برقرار گرده و به ارسال و دریافت اطلاعات بپردازند.

با توجه به اینکه اطلاعات در قالبهای متفاوتی مثل فایل و ... وجود دارد و فایلها نیز معمولا دارای حجم بالائی هستند نمی توان انتظار داشت که یک فایل در شبکه به صورت یکپارچه ارسال شود. همانگونه که می دانید شبکه محیط دسترسی تعدادی کامپیوتر را برای ارسال و دریافت اطلاعات ایجاد می نماید. نتیجتا اگر قرار باشد یک فایل بزرگ در شبکه از یک کامپیوتر به کامپیوتر دیگر ارسال شود به دلیل مشترک بودن مدیای ارتباطی ، تا لحظه ای که ارسال آن فایل به اتمام نرسد کامپیوترهای دیگر امکان استفاده از مدیای شبکه را نخواهند داشت که این موضوع صحیح نیست و نباید اتفاق بیافتد. ضمنا اگر حتی قسمت کوچکی از این اطلاعات مثلا به دلیل تاثیر نویز آسیب ببیند و مورد تائید دریافت کننده واقع نشود ، کامپیوتر مبداء باید دوباره کل آن اطلاعات را ارسال نماید. به همین دلیل روش ارسال اطلاعات در شبکه اینگونه است که هر قالب اطلاعاتی ابتدا بر روی کامپیوتر مبدا به قطعات کوچک تبدیل شده و هر قطعه به صورت جدا آدرس دهی شده و ارسال می گردد. نتیجتا در فواصل ارسال هر قطعه از اطلاعات توسط یک کامپیوتر به دیگری ، نود های دیگر شبکه نیز این فرصت را پیدا می کنند که به ارسال یک قطعه از اطلاعات مورد نظر خود بپردازند. در حقیقت با تقسیم حداکثر توانایی ارسال اطلاعات در واحد زمان بین نودهای شبکه همگی بصورت مشترک از آن استفاده مینمایند. این حداکثر توانایی ارسال اطلاعات در مدیا ها با یکدیگر تفاوت دارد و به آن **Bandwidth** میگویند. واحد آن **bps** یعنی **bit per second** می باشد. که در واحد های کلان تر **Kbps** یعنی **Kilobit per second** و **Mbps** یعنی **Megabit per second** می باشد.

تعریف CRC :

با توجه به اینکه برای اطمینان از سالم دریافت شدن اطلاعات در کامپیوتر مقصد نیاز به یک راهکار مناسب بوده است در ساختار Frame قسمتی تحت عنوان Cyclical Redundancy Check یا CRC وجود دارد که به وسیله آن کامپیوتر مقصد در می یابد که آیا اطلاعات دریافتی را صحیح و سالم دریافت کرده یا خیر.

کامپیوتر مبداء در لایه Data link (در مورد لایه ها در قسمت های بعدی بحث خواهد شد) با انجام یک محاسبه منطقی و ریاضی بر روی داده ها حاصل به دست آمده را به انتهای Frame اضافه می کند. Frame در کامپیوتر دریافت کننده مجددا مورد محاسبه CRC واقع می شود و در صورت برابر بودن حاصل محاسبه مجدد با حاصل دریافتی Frame مذکور سالم فرض می شود. خاصیت CRC این است که در صورت تغییر حتی یک بیت اطلاعات در طول مسیر انتقال ، در مقصد حاصل متفاوتی ایجاد شده و تغییر مذکور معیین می گردد.

ارتباط Connection Oriented :

به ارتباطی Connection Oriented می گویند که پس از ارسال اطلاعات ، کامپیوتر مبداء انتظار دریافت Acknowledge داشته باشد و در صورت عدم دریافت Acknowledge مربوط به یک Frame پس از مدت زمان تعریفی معین ، با فرض عدم دریافت صحیح Frame مذکور ، اقدام به ارسال مجدد آن Frame نماید. مسلما در صورتی که در زمان تعیین شده Acknowledge مربوطه دریافت شود ، کامپیوتر مبداء از دریافت صحیح آن Frame در مقصد اطمینان حاصل میکند.این روش ارتباط برای ارسال فایل و اطلاعات مهم کاربرد دارد.

ارتباط Connection Less:

در این روش پس از ارسال اطلاعات ، کامپیوتر مقصد مبادرت به ارسال Acknowledge نمی کند. در این متد اطلاعات ارسال شده نیازی به تائید دریافت کننده ندارند. با توجه به یک طرفه بودن این نوع ارتباط سرعت ارسال می تواند تا حدودی بالا تر باشد. این روش برای ارسال اطلاعات صوتی به صورت real کاربرد زیادی دارد. مثل Voice Chat و البته برای پخش فیلم در شبکه و ارتباطات Multicast استفاده می شود.

✸موسسه استاندارد جهانی (ISO)

نظم و ترتیب جائی برقرار می شود که قانون باشد و هر جا رفتارها طبق قانون و در چهاچوب های تعریف شده باشد با توجه به اینکه روش و محل و زمان انجام هر کار معیین می گردد می توان اطمینان داشت که تمامی موجودیت های آن محیط می توانند به راحتی به صورت مرتبط با هم کار کنند. موسسه استاندارد جهانی مسئولیت قانون گذاری و نظارت بر رعایت قانون را در زمینه های متفاوت به عهده دارد. از جمله استاندارد های تعیین شده این شرکت ISO 9001 و ISO 9002 می باشد. دارندگان مدرک استاندارد ISO می توانند ادعا نمایند که برای انجام کارهای خود طبق یک سلسله قوانین تعیین شده از سوی موسسه استاندارد رفتار می کنند . بر این اساس شرکت هایی که پس از ارزیابی موسسه ISO مدرک مربوط به آن را دریافت می کنند باید برای حفظ مدرک خود از آن پس طبق چهارچوبهای استاندارد مربوط به آن مدرک رفتار نمایند و در صورت تخطی مدرک آنها لغو می شود. این امر باعث می شود که در درجه اول نظم در محیط حکم فرما گردد و در درجه دوم تمام شرکتهای دارنده این مدرک از نظر رفتار کاری محیط به هم تشابه خواهند داشت و نتیجتا در صورت نیاز اگر بخواهیم بین این مجموعه ها ارتباط کاری بوجود بیاوریم امکان پذیر خواهد بود.

(OSI) Open System Interconnection

موسسه استاندارد جهانی ISO برای شبکه نیز به طراحی یک استاندارد پرداخته است که این استاندارد پایه و اساس تمامی پروتکل های شبکه می باشد. هر شرکت تولید کننده نرم افزار یا سخت افزار ملزم است در تولیدات خود در صورتی که از شبکه استفاده می کند ، این چهارچوب ها و قوانین را رعایت نموده و بر اساس آن عمل کند. نتیجتا این اطمینان حاصل شده است که تمامی تجهیزات شبکه و نرم افزار های مرتبط می توانند با یکدیگر ارتباط برقرار نمایند.

این استانداردOSI نام دارد و در آن هفت لایه عملکرد تعریف شده است. عملیاتی که باید در هر لایه انجام شود مشخص گردیده و در حقیقت تمام کامپوتر ها در شبکه باید طبق این سلسله مراتب عمل نمایند تا بتوانند در شبکه به ارسال و دریافت اطلاعات بپردازند. لایه های بالائی نرم افزاری هستند و هر چه به سمت لایه های پائینی پیش می رویم به سخت افزار نزدیک می شویم. به صورتی که لایه پائینی از این لایه ها تماما سخت افزاری بوده و عملیاتی که در آن تعریف می شود کاملا در حد تجهیزات سخت افزاری است.

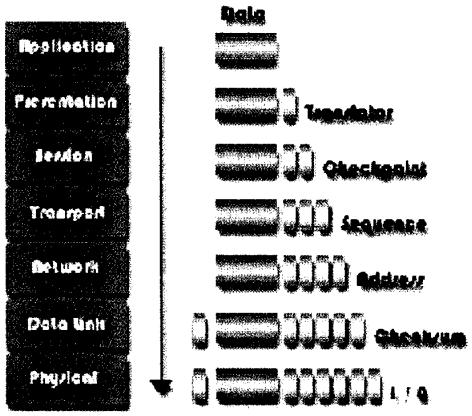
در لایه بالائی اطلاعات مورد نظر برای ارسال قطعه قطعه شده و هر **Chunk** اطلاعاتی به طور مجزا وارد **OSI** می گردد. در هر لایه یک سری اعمال بر روی آن **Chunk** انجام می شود و نتیجه آن عملیات در همان لایه به آن **Chunk** افزوده می شود. به این قطعات که در هر لایه به **Chunk** افزوده می شود **Header** می گویند. هر ژیزی که در یک لایه به **Frame** اضافه شده در لایه متناظر آن در کامپیوتر دریافت کننده تحلیل شده و از **Frame** جدا می شود. پس در حقیقت هر لایه از کامپیوتر ارسال کننده اطلاعات با لایه متناظر خود در کامپیوتر دریافت کننده به صورت غیر مستقیم در ارتباط است.

هر لایه با لایه های بالاتر و پائین تر توسط یک **Interface** در ارتباط است. با توجه به اینکه سیگنال های اطلاعات توسط یک **Media** انتقال می یابند و مدیا یک ابزار سخت افزاری و فیزیکی برای انتقال است ، نتیجتا هر کامپیوتر از طریق لایه **Physical** که پائین ترین لایه از **OSI** است با کامپیوتر طرف مقابل ارتباط دارد.

لایه ها از پائین به بالا شماره گذاری شده اند و نام و ترتیب آنها در شکل زیر معین شده است.

The OSI Layer Model

OSI	TCP/IP
Layer 7 Application	**Application** Telnet, FTP, NFS, NIS
Layer 6 Presentation	**Session** e.g. RPC
Layer 5 Session	**Transport** Sockets/Streams - TLI
Layer 4 Transport	TCP UDP
Layer 3 Network	**Network** IP + ARP/RARP/ICMP
Layer 2 Data Link	**Physical Protocol** Ethernet/TR/FDDI/PPP
Layer 1 Physical	**Transmission medium** Coax, Fiber, 10baseT..



Application Layer:

این لایه اطلاعات مورد نظر برای ارسال در شبکه را قطعه قطعه وارد لایه های پائینی می نماید تا سلسله مراتب لازم در مورد اطلاعات ارسالی در لایه ها به ترتیب انجام پذیرد و ارسال داده ها انجام شود. از طرفی در کامپیوتر دریافت کننده این لایه آنچه که از لایه پائینی یعنی **Presentation** دریافت می کند را به ترتیب به هم متصل می کند تا اصل اطلاعات ارسال شده از مبداء ، در مقصد به وجود آید.

در عین حال نظارت بر **Error Recovery** و **Flow Control** در هنگام ارسال و دریافت اطلاعات به عهده این لایه می باشد.

Presentation Layer:

در این لایه عمل **Compression** و در مقابل آن **Decompression** و از طرفی **Encryption** و **Decryption** انجام می شود. در این لایه عملگری با عنوان**Redirector** یا **RDR** وجود دارد که بر اطلاعاتی ارسالی نظارت می کند و در صورتی که مقصد ارسال اطلاعات و یا درخواستی ، خود همان کامپیوتر بود ، جلوی ارسال آن به لایه های بعدی را گرفته و آنرا به سیستم خودش **Redirect** میکند.

مفهوم **Compression** فشرده سازی اطلاعات است و منظور از **Encryption** به رمز درآوردن اطلاعات است که برای حفاظت از اطلاعات کاربرد دارد.

Session Layer:

برقراری هر ارتباط بین دو کامپیوتر نیازمند تعریف نوع و دلیل ارتباط بین دو کامپیوتر است. در حقیقت با توجه به اینکه دو کامپیوتر در یک زمان تحت یک **Connection** می توانند تعدادی بیش از یک موضوع ارتباط داشته باشند باید بدانند که چه **Packet** هایی که ارسال و یا دریافت می کنند مربوط به کدام موضوع صحبت یا **Session** است. در این لایه تعریف ارتباط کامپیوتر ها با هم انجام می شود. هر دو کامپیوتر قبل از آغاز ارسال و دریافت اطلاعات با انجام **3 Way Handshaking** در مورد موضوع صحبت با هم به تفاهم می رسند. تصمیم گیری در مورد آغاز و ادامه یافتن و پایان **Session** ها در این لایه انجام می شود.

Transport Layer:

همانگونه که قبلا بیان شده ارتباط کامپیوتر ها به دو صورت **Connection Oriented** و **Connection Less** امکان پذیر است . در این لایه در مورد اینکه هر ارتباط در حال برقرار شدن از کدام نوع باشد ، تصمیم گیری می شود. در حقیقت در این لایه عمل **Error Recovery** صورت می پذیرد. نظارت بر این عمل در لایه **Application** انجام می شد.

Acknowledge که تائیدیه دریافت اطلاعات به صورت صحیح می باشد توسط این لایه ایجاد و به کامپیوتر ارسال کننده اطلاعات ارسال می شود.

Network Layer:

آدرس دهی در شبکه یکی از اصلی ترین کارهاست. این کار به دو صورت انجام می شود :

الف) آدرس دهی فیزیکی که توسط **MAC Address** انجام می شود.

ب) آدرس دهی لاجیکال که توسط **IP** ویا **IPX** و ... در پروتکل های متفاوت انجام می شود.

آدرس لاجیکال که قابل تغییر و تعیین بر روی هر کامپیوتر عضو شبکه است دارای خاصیت**Arrange able** بودن است و نتیجتا برای کنترل ترافیک در محدوده های بزرگ مثل اینترنت کاربرد دارد. این نوع آدرس دهی در این لایه انجام می پذیرد. یعنی در لایه **Network** آدرس مبداء و مقصد از نوع لاجیکال به **Frame** اضافه می شود.

آدرس دهی **Physical** در این لایه انجام نمی شود.

DataLink Layer:

آدرس دهی **MAC** در این لایه انجام می شود. این نوع آدرس غیر قابل تغییر است و در **Firmware** کارت شبکه توسط شرکت سازنده ثبت شده است. هر کامپیوتر در محیط **LAN** مثلا در محیط شبکه ای از نوع **Ethernet** باید از این آدرس برای ارسال اطلاعات استفاده کند.

در عین حال **CRC** که در قسمت های قبلی توضیح داده شد در این لایه به **Frame** اضافه می شود. مسلما در طرف دریافت کننده اطلاعات نیز بررسی **CRC** جهت اطمینان از سالم بودن **Frame** دریافت شده ، انجام می شود.

Physical Layer:

این لایه مسئولیت ارسال و دریافت سیگنال را در قالب های تعریف شده به عهده دارد. کابل از جمله مواردی است که عملکرد آن در این لایه تعریف شده است.

در صورتی که به شکل زیر توجه نمائید سلسله مراتبی که برای ارسال و دریافت اطلاعات وجود دارد را درک خواهید نمود.

The OSI, or Open System Interconnection, model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.
Presentation (Layer 6)	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the *syntax layer*.
Session (Layer 5)	This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.
Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.
Physical (Layer 1)	This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.

Purpose

The OSI model divides the functions of a protocol into a series of layers. Each layer has the property that it only uses the functions of the layer below, and only exports functionality to the layer above. A system that implements protocol behavior consisting of a series of these layers is known as a 'protocol stack' or 'stack'. Protocol stacks can be implemented either in hardware or software, or a mixture of both. Typically, only the lower layers are implemented in hardware, with the higher layers being implemented in software.

This OSI model is roughly adhered to in the computing and networking industry. Its main feature is in the interface between layers which dictates the specifications on how one layer interacts with another. This means that a layer written by one manufacturer can operate with a layer from another (assuming that the specification is interpreted correctly.) These specifications are typically known as Request for Comments or "RFC"s in the TCP/IP community. They are ISO standards in the OSI community.

Usually, the implementation of a protocol is layered in a similar way to the protocol design, with the possible exception of a 'fast path' where the most common transaction allowed by the system may be implemented as a single component encompassing aspects of several layers.

This logical separation of layers makes reasoning about the behaviour of protocol stacks much easier, allowing the design of elaborate but highly reliable protocol stacks. Each layer performs services for the next higher layer, and makes requests of the next lower layer. An implementation of several OSI layers is often referred to as a *stack* (as in TCP/IP stack).

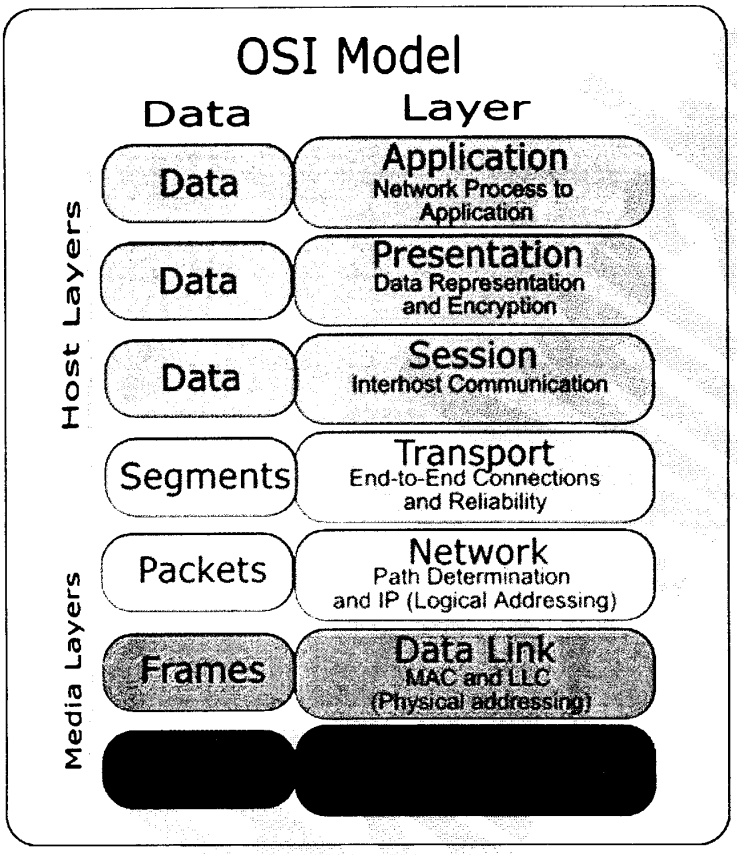
The OSI reference model is a hierarchical structure of seven layers that defines the requirements for communications between two computers. The model was defined by the International Standards Organization. It was conceived to allow interoperability across the various platforms offered by vendors. The model allows all network elements to operate together, regardless of who built them. By the late 1970's, ISO was recommending the implementation of the OSI model as a networking standard.

Of course, by that time, TCP/IP had been in use for years. TCP/IP was fundamental to ARPANET and the other networks that evolved into the Internet. It had its own quite different model, see RFC 871.

Only a subset of the whole OSI model is used today. It is widely believed that much of the specification is too complicated and its full functionality has taken too long to implement, although there are many people that strongly support the OSI model.

On the other hand, many feel that the best thing about the whole ISO networking effort is that it failed before it could do too much damage.

Description of layers



- **Physical layer** Layer 1: The physical layer defines all electrical and physical specifications for devices. This includes the layout of pins, voltages, and cable specifications. Hubs and repeaters are physical-layer devices. The major functions and services performed by the physical layer are:
  - Establishment and termination of a connection to a communications medium.
  - Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
  - modulation, or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling -- copper and fiber optic, for example. SCSI operates at this level.

- **Data link layer** Layer 2: The Data link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer. The addressing scheme is physical which means that the addresses (MAC address) are hard-coded into the network cards at the time of manufacture. The addressing scheme is flat. *Note:* The best known example of this is Ethernet. Other examples of data link protocols are HDLC and ADCCP for point-to-point or packet-switched networks and LLC and Aloha for local area networks. This is the layer at which bridges and switches operate. Connectivity is provided only among locally attached network nodes.

- **Network layer** Layer 3: The Network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport layer. The Network layer performs network routing, flow control, segmentation/documentation, and error control functions. The router operates at this layer -- sending data throughout the extended network and making the Internet possible, although there are layer 3 (or IP) switches. This is a logical addressing scheme - values are chosen by the network engineer. The addressing scheme is hierarchical.

- **Transport layer** Layer 4: The purpose of the Transport layer is to provide transparent transfer of data between end users, thus relieving the upper layers from any concern with providing reliable and cost-effective data transfer. The transport layer controls the reliability of a given link. Some protocols are stateful and connection oriented. This means that the transport layer can keep track of the packets and retransmit those that fail. The best known example of a layer 4 protocol is TCP.

- **Session layer** Layer 5: The Session layer provides the mechanism for managing the dialogue between end-user application processes. It provides for either duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures. This layer is responsible for setting up and tearing down TCP/IP sessions.

- **Presentation layer** Layer 6: The Presentation layer relieves the Application layer of concern regarding syntactical differences in data representation within the end-user systems. MIME encoding, encryption and similar manipulation of the presentation of data is done at this layer. An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file.

- **Application layer** Layer 7, the highest layer: This layer interfaces directly to and performs common application services for the application processes. The common application services provide semantic conversion between associated application processes. Examples of common application services include the virtual file, virtual terminal (for example, Telnet), and "Job transfer and Manipulation protocol" (JTM, standard ISO/IEC 8832).

The OSI model in the real world

Real-world protocol suites often do not strictly match the seven-layer model. There can be some argument as to where the distinctions between layers are drawn; there is no one correct answer. However, most protocol suites share the concept of three general sections: media, covering layers 1 and 2; transport, covering layers 3 and 4, and application, covering layers 5 through 7.

The DoD model, developed in the 1970s for DARPA, is a 4-layer model that maps closely to current common internet protocols. It is based on a more "pragmatic" approach to networking than OSI.

Strict conformance to the OSI model has not been a common goal in real-world networks, in part because of the negative view of the OSI protocol suite. Andrew Tanenbaum argues in his popular textbook *Computer Networks* ISBN 0130661023 that the failure of the OSI suite to become popular was due to bad timing, bad technology, bad implementations, and bad politics. The timing was bad because the model was finished only after a significant amount of research time and money had been spent on the TCP/IP model. The technology is "bad" because the session and presentation layers are nearly empty, whereas the data link layer is overfilled. Early implementations were notoriously buggy and in the early days, OSI became synonymous with poor quality, whereas early implementations of TCP/IP were

More reliable. Finally, the politics were bad because TCP/IP was closely associated with Unix, making it popular in academia, whereas OSI did not have this association.

An early implementation of the TP4 transport protocol was so inefficient that packet transmission took longer than the connection time-out used by TCP/IP. The X.400 email protocols were stupendously complex, and independent implementations of the standard were unable to actually send email to each other. Ultimately, the biggest cost of OSI's failure was the delay it caused in the adoption of internet infrastructure in Europe and Japan, a cost that no one today would dare to calculate. (Finland opted to install TCP/IP instead of investing in OSI).

Having said all that, the model is still the general reference standard for nearly all networking documentation. All networking phrases referring to numbered layers, such as "layer 3 switching", refer to this OSI model.

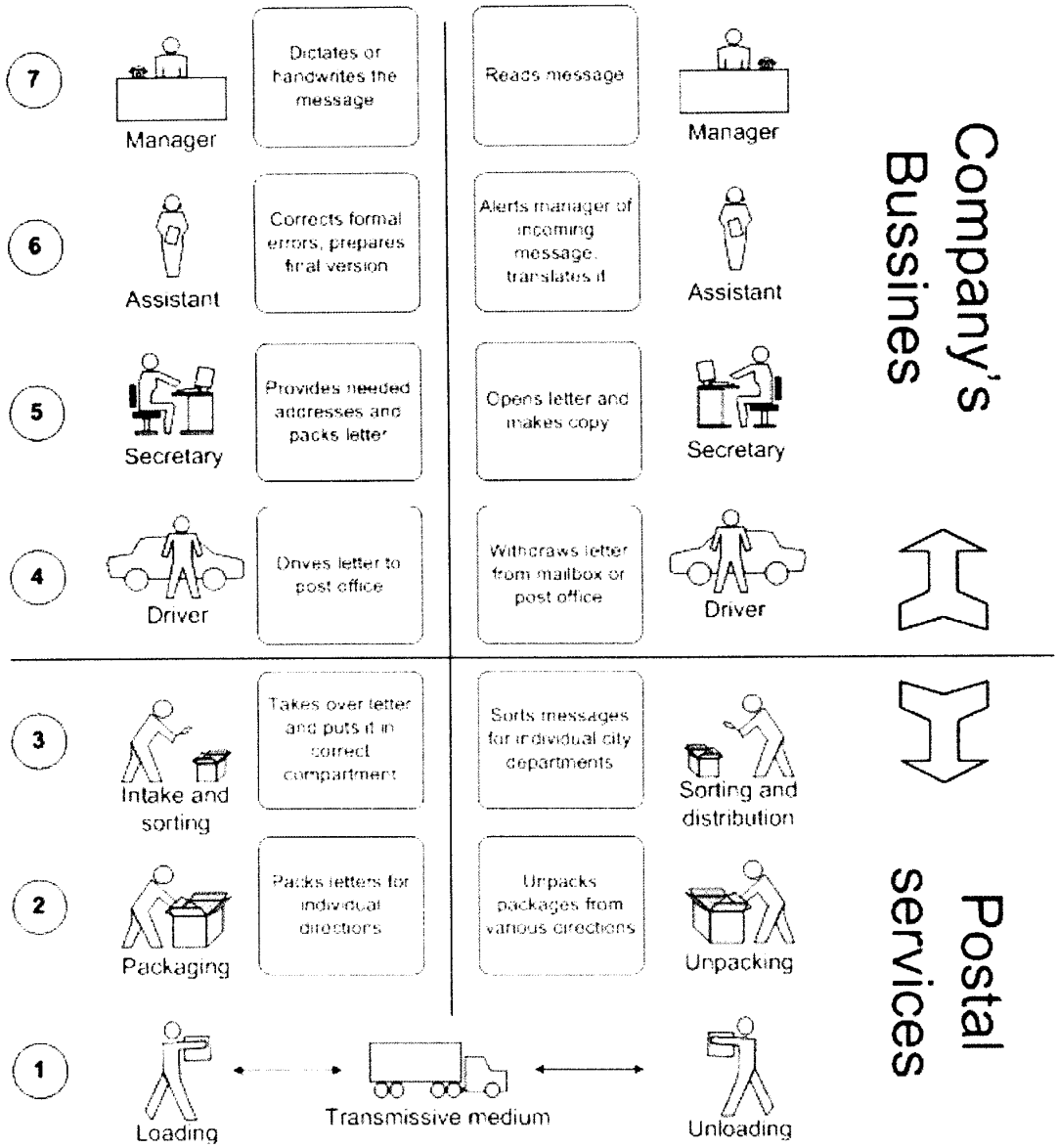
Interfaces

In addition to standards for individual protocols in transmission, there are also interface standards for different layers to talk to the ones above or below (usually operating-system-specific). For example, Microsoft Windows' Winsock and Unix's Berkeley sockets and System V Streams are interfaces between applications (layers 5 and above) and the transport (layer 4). NDIS and ODI are interfaces between the media (layer 2) and the network protocol (layer 3).

Table of examples

Layer	Misc. examples	TCP/IP suite	SS7	AppleTalk suite	OSI suite	IPX suite	SNA	UMTS
7 - Application	HL7, Modbus, SIP	HTTP, SMTP, SNMP, FTP, Telnet, NFS, NTP	ISUP, INAP, MAP, TUP, TCAP	AFP, PAP	FTAM, X.400, X.500, DAP		APPC	
6 - Presentation	TDI, ASCII, EBCDIC, MIDI, MPEG	XDR, SSL, TLS		AFP, PAP				
5 - Session	Named Pipes, NetBIOS, SAP, SDP	Session establishment for TCP		ASP, ADSP, ZIP		NWLink	DLC?	
4 - Transport	NetBEUI	TCP, UDP, RTP, SCTP		ATP, NBP, AEP, RTMP	TP0, TP1, TP2, TP3, TP4	SPX, RIP		
3 - Network	NetBEUI, Q.931	IP, ICMP, IPsec, ARP, RIP, OSPF, BGP	MTP-3, SCCP	DDP	X.25 (PLP), CLNP	IPX		RRC (Radio Resource Control)
2 - Data Link	Ethernet, Token Ring, FDDI, PPP, HDLC, Q.921, Frame Relay, ATM, Fibre Channel		MTP-2	LocalTalk, TokenTalk, EtherTalk, Apple Remote Access, PPP	X.25 (LAPB), Token Bus	802.3 framing, Ethernet II framing	SDLC	MAC (Media Access Control)
1 - Physical	RS-232, V.35, V.34, Q.911, T1, E1, 10BASE-T, 100BASE-TX, ISDN, SONET, DSL		MTP-1	Localtalk on shielded, Localtalk on unshielded (PhoneNet)	X.25 (X.21bis, EIA/TIA-232, EIA/TIA-449, EIA-530, G.703)		Twinax	PHY (Physical Layer)

Parallel



This is parallel of OSI and standard letter communication between two company managers.

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه پنجم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه پنجم:

- تقسیم بندی لایه ها به سطوح مختلف و تعریف پروتکل
- معرفی تعدادی از پروتکل ها
- تعریف Protocol Stack
- تجهیزات شبکه و حدود عملکرد آنها

✸تقسیم بندی لایه ها به سطوح مختلف و تعریف پروتکل

همانگونه که در مباحث قبلی بیان شد در لایه های **OSI** ، کارهای متفاوتی انجام می پذیرد تا یک **Packet** اطلاعاتی از یک کامپیوتر به کامپیوتر دیگر منتقل شود. این لایه ها با توجه به یک سری وجوه تشابه خاص به سه ناحیه تقسیم میشوند .

Application Level: که شامل سه لایه بالایی از لایه های **OSI** می باشد.

Transport Level: که شامل صرفا لایه **Transport** می باشد.

Network Level: که شامل سه لایه پائینی از لایه های **OSI** می باشد.

✸تعریف **Protocol** :

پروتکل به مجموعه ای از قوانین و توابع مربوط به آن گفته می شود که برای انجام یک کار خاص طراحی شده و محدوده عملکرد هر پروتکل یکی از سه ناحیه می باشد. تعدادی از پروتکل ها به قرار زیر می باشند:

FTP (File Transfer Protocol)

این پروتکل برای ارسال و دریافت فایل در شبکه کاربرد دارد.

SMTP (Simple Mail Transfer Protocol)

این پروتکل برای انتقال نامه های الکترونیکی کاربرد دارد.

SNMP (Simple Network Management Protocol)

برای مدیریت تجهیزات و کنترل آنها در شبکه می توان از پروتکل **SNMP** استفاده کرد

IP (Internet Protocol)

آدرس دهی **Frame** های مورد نظر برای انتقال در شبکه توسط این پروتکل انجام می شود . این پروتکل زیر مجموعه **TCP/IP** می باشد.

TCP (Transmission Control Protocol)

برای انتقال اطلاعات به صورت **Connection Oriented** در شبکه توسط **TCP/IP Stack** از این پروتکل استفاده می شود.

UDP (User Datagram Protocol)

برای انتقال اطلاعات به صورت **Connection Less** در شبکه توسط **TCP/IP Stack** از این پروتکل استفاده می شود.

تعدادی دیگر از Protocol ها در این قسمت ذکر شده اند. نکته مورد توجه این است که هر یک پروتکل برای یک کار خاص طراحی شده و برای انجام آن کار نیز باید با پروتکل های دیگری که مکمل انجام کارهایش هستند همکاری نماید و هیچ پروتکلی به تنهایی در شبکه کارایی ندارد.

HTTP (Hyper Text Transfer Protocol)

POP (Post Office Protocol)

NNTP (Network News Transport Protocol)

IGMP (Internet Group Management Protocol)

ICMP (Internet Control Message Protocol)

ARP (Address Resolution Protocol)

SPX (Sequenced Packet Exchanged)

IPX (Internetwork Packet Exchange)

✸تعریف Stack Protocol:

نکته مهم و قابل توجه در پروتکل ها این است که هر پروتکل صرفا در یکی از سه ناحیه عمل می کند و با توجه به اینکه برای ارسال هر گونه اطلاعات باید مجموعه عملیاتی در سطح هفت لایه انجام شود ، پس یک پروتکل نمی تواند تمام کارهای مربوط به ارسال اطلاعات را انجام دهد. این بدین معنی است که پروتکل ها با یکدیگر همکاری می کنند تا اطلاعات ارسال و دریافت شود و هر مرحله از امور مربوط به ارسال و دریافت اطلاعات توسط پروتکل خاص آن انجام و کنترل می شود.

با توجه به همین موضوع به مجموعه ای از پروتکل ها که با یکدیگر به صورت وابسته همکاری می کنند تا هر گونه اطلاعات ارسال و دریافت شوند Stack Protocol می گویند. نمونه ای از این Stack Protocol ها TCP/IP می باشد که کاربردی ترین و مشهورترین Stack بوده و رکن اصلی ارتباطات در اینترنت می باشد. ممکن است اینگونه به نظر برسد که TCP/IP صرفا دارای دو پروتکل TCP و IP است . اما اینگونه نیست و این Stack Protocol دارای تعداد زیادی پروتکل است که به صورت مجموعه ای متحد هدف واحدی با عنوان Communication یعنی ارتباطات را دنبال می کنند.

تعدادی از Stack Protocol ها به قرار زیر می باشند:

- TCP/IP (Transmission Control Protocol / Internet Protocol)
- IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchanged)
- Apple Talk
- BetBEUI
- Nwlink IPX/SPX

در عین حال TCP/IP به عنوان یکی از کاربردی ترین پروتکلها داری حجم زیاد از نظر نرم افزاری و استفاده از توانایی های سخت افزاری سیستم در حد متوسط می باشد. این Stack پایه و اساس ارتباطات در اینترنت بوده و اصطلاحا امکان Route دارد.

پروتکل IPX/SPX مخصوص شبکه های Netware بوده و توسط سیستم عامل Novell Netware در شبکه استفاده می شود. با توجه به اینکه این Stack برای ارتباط با شبکه های از انواع دیگر کارآیی ندارد کم کم Novell Netware نیز از TCP/IP به عنوان راهکار ارتباط با شبکه های دیگر استفاده می کند.

NetBEUI یک Stack کاملا مایکروسافتی است که سرعت بسیار بالایی در انتقال اطلاعات دارد . اما امکان Route نداشته و به درد شبکه های کوچک که تعداد کمی کامپیوتر دارند می خورد.

AppleTalk نیز به عنوان یک Stack در شبکه های Apple Macintosh استفاده می شود و امکان Route نیز دارد.

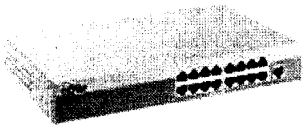
با توجه به اینکه سیستم عامل Windows که توسط شرکت مایکروسافت ساخته شده ، پر طرفدار ترین سیستم عامل در جهان می باشد ، مایکروسافت این امکان را در ویندوز ایجاد کرده که این سیستم عامل بتواند توسط تمام Stack های ذکر شده در شبکه کار کند.

✸ تجهیزات شبکه و حدود عملکرد آنها

- Hub:

در این دستگاه که در حد لایه **Physical** عمل می کند سیگنالها پس از دریافت بدون هیچگونه تحلیلی سریعا ارسال می شوند. این دستگاه به عنوان یک واسط برای ارتباط بین دستگاها در شبکه **Star** کاربرد دارد . در این دستگاه هر سیگنال پس از دریافت به تمام پورت ها غیر از پورت مبداء ارسال می گردد. روش عملکرد **Hub** همواره **Half Duplex** می باشد.

به شکل زیر توجه نمائید:



- Switch:

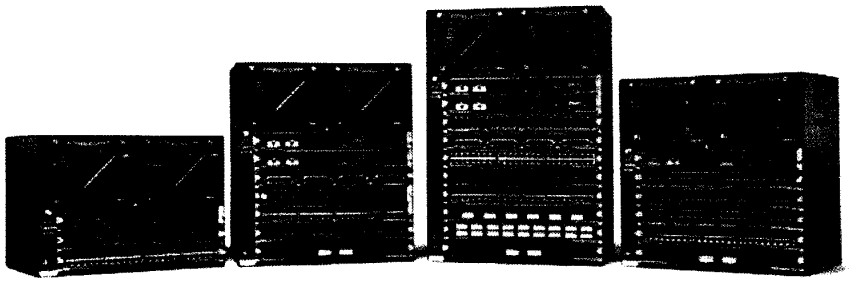
در این دستگاه علاوه بر دریافت و ارسال سیگنال کارهای دیگری نیز انجام می شود. در حقیقت حدود عملیاتی که در **Switch** انجام می شوند لایه **Datalink** می باشد. یعنی سوییچ در دو لایه پائینی **OSI** کار می کند.

سویچ سیگنالها را دریافت کرده و پس از دریافت سیگنالهای یک **Frame** به صورت کامل ، ابتدا اقدام به کنترل **CRC** می نماید. در صورتی که **CRC** نشان دهنده سالم بودن **Frame** باشد ، در مرحله بعد آدرس مبداء و مقصد **(MAC Address)** آن کنترل می شود . با کنترل آدرس مبداء ، شماره پورت و **MAC Address** مربوط به کامپیوتر ارسال کننده در جدول **Filter/Forward Table** ثبت می گردد و سپس در صورتی که مقصد نیز در جدول مذکور شناخته شده بود ، اطلاعات صرفا به همان پورتی که مقصد به آن متصل است ارسال می شود.

در صورت وجود نداشتن آدرس کامپیوتر مقصد در جدول مذکور با توجه به اینکه معلوم نیست مقصد بر روی کدام پورت است **Frame** دریافت شده توسط **Switch** به تمام پورت ها ارسال شده یا اصطلاحا **Flood** می شود. ضمنا در صورتی که یک **Frame** از نوع **Broadcast** به **Switch** برسد به تمام پورت ها **Flood** می شود.

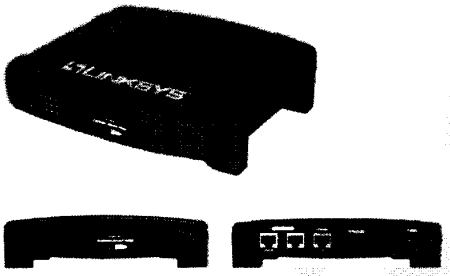
تعداد پورت های **Switch** در برخی مدل ها بیش از **48** عدد می باشد. و دارای کاربرد ها و مدل های بسیار متفاوتی است.

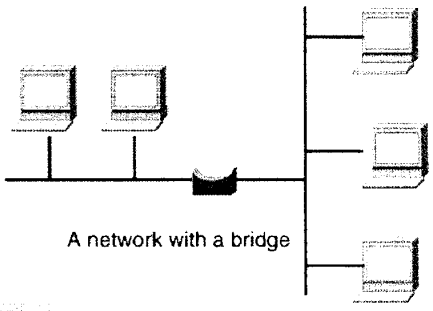
به شکل های زیر توجه کنید: قابل ذکر است با توجه به کاربرد های متفاوت از سویچ های متفاوت با ابعاد و توانائی های گوناگون استفاده می شود.



- **Bridge**:

این دستگاه نیز بسیار به **Switch** شباهت دارد و از نظر لایه های کاری نیز در دو لایه پائینی شبکه کار می کند. تمام موارد کاری آن شبیه **Switch** است با این تفاوت که تعداد پورت های آن معمولا دو تا و در برخی موارد چهار تا می باشد. و برای اتصال شبکه های **Bus** به یکدیگر طراحی شده است.

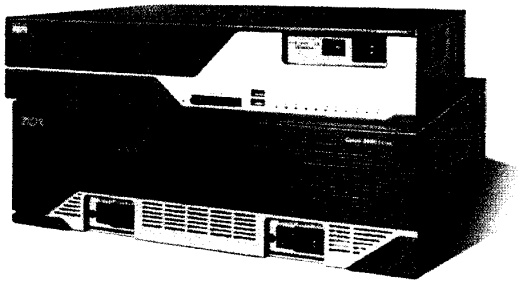




- **Router**:

این دستگاه یک لایه بالاتر از **Switch** کار می کند. در حقیقت این دستگاه در سه لایه پائینی از **OSI** کار می کند و از آدرس های لاجیکال برای تشخیص مسیر ارسال **Frame** استفاده می کنند.

بر خلاف **Switch** که در صورت دریافت **Frame** های از نوع **Broadcast** آنرا **Flood** میکند، **Router** در صورت دریافت **Broadcast** اجازه عبور ان را نمی دهد.



جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه ششم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

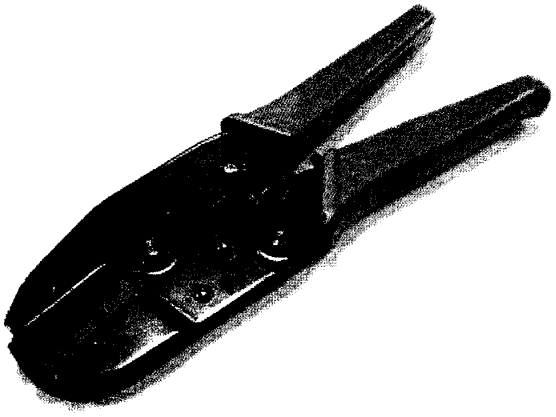
جلسه ششم:

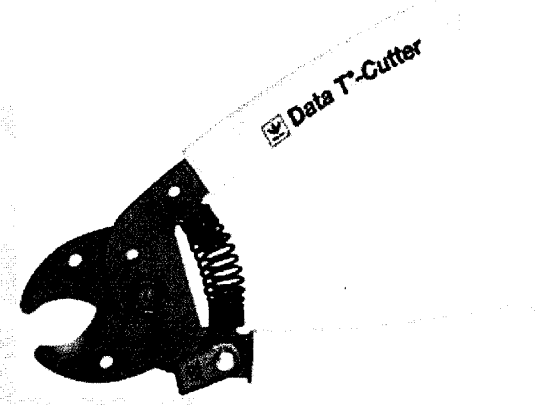
- معرفی تجهیزات کار با کابل
- تجهیزات مرکزی اتصالات شبکه

- معرفی تجهیزات ابزار کار با کابل

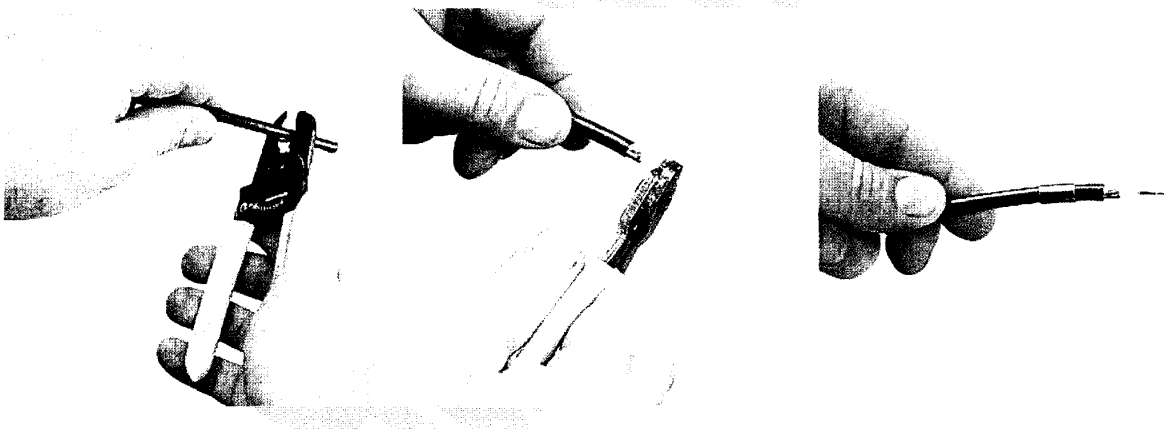
برای اتصال دادن کابل های Coaxial از ابزار نمایش داده شده در شکل زیر استفاده می شود:

شکل سمت راست نمایش دهنده ابزار روکش برداری از کابل است و شکل سمت چپ نقاط اتصال را با دندانه مخصوص خود فشار می دهد و به کابل متصل می کند.کانکتور را به کابل متصل می کند.

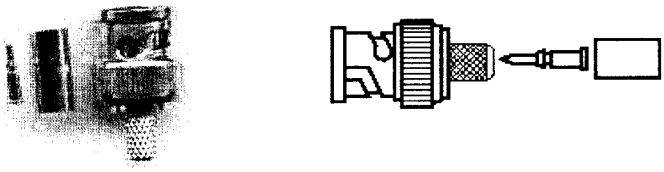


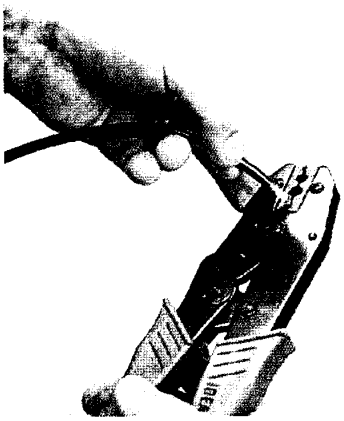


با استفاده از ابزار مخصوص روکش برداری یا وسیله ای مشابه تیغ کاتر باید کابل را مشابه شکل زیر روکش برداری کرد.



قسمتهای متفاوت یک کانکتور BNC در شکل زیر مشخص شده و ترتیب اتصال آنها به صورت زیر است:

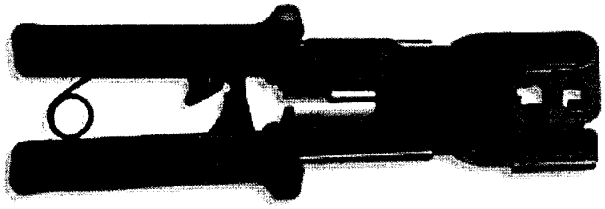




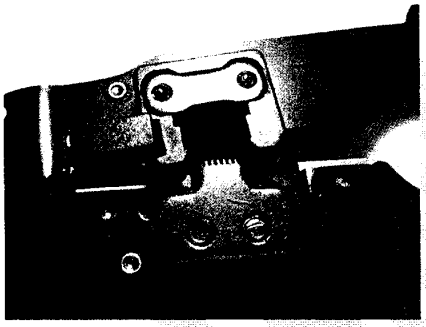
برای اتصال کانکتور مانند شکل زیر از ابزار استفاده می شود:

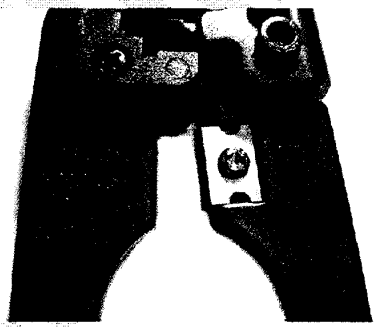
در مورد کابلهای **Twisted Pair** ابزار و روش کار کاملا متفاوت است

شکل زیر یک دستگاه **Crimp** مخصوص کابلهای **Twisted Pair** را نمایش می دهد.



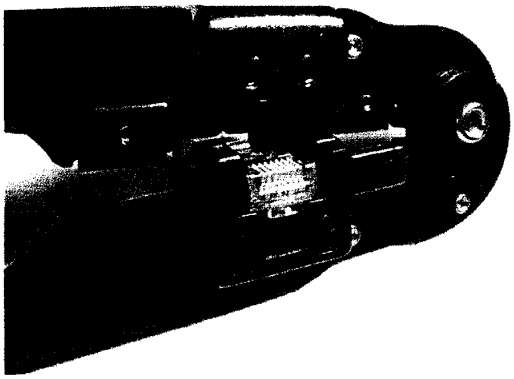
شکل سمت راست تیغه برش کابل را نمایش می دهدو شکل سمت چپ قسمت پرس کننده کانکتور را نشان می دهد.



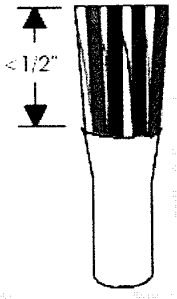


در این شکل همانگونه که مشاهده می کنید یک کانکتور **RJ45** توسط

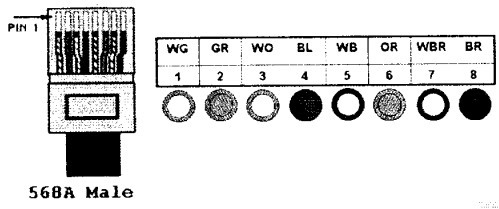
ابزار در حال پرس شدن است.

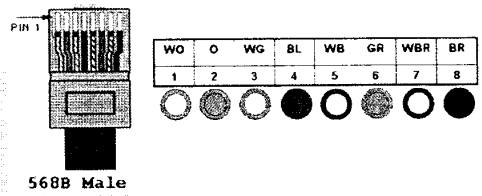


برای اتصال کانکتور می بایست ابتدا کابل را روکش برداری کرد و سپس پیچش سیم ها را باز کرده و به ترتیب رنگ تعیین شده مرتب و در کانکتور جا سازی کرد.

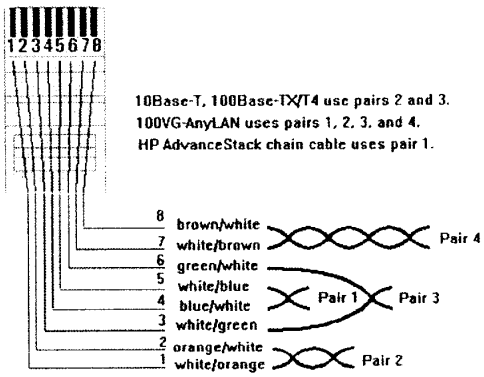


ترتیب رنگ در دو استاندارد **EIA/TIA 568A** و **EIA/TIA 568B** به صورت زیر می باشند.



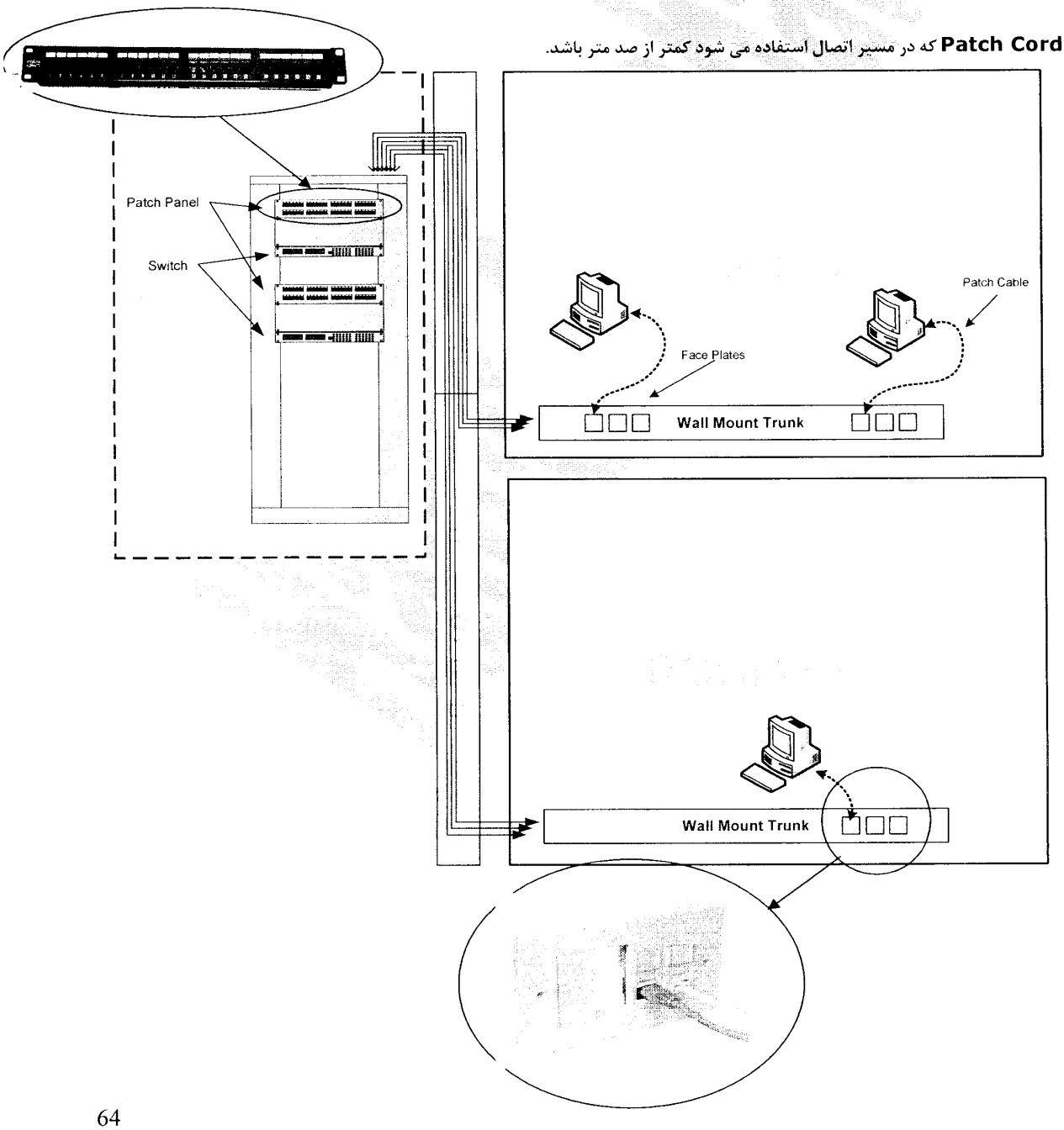


این شکل نیز راهنمای دیگری برای اتصال کانکتور به کابل **Twisted Pair** می باشد.



- تجهیزات مرکزی اتصالات شبکه

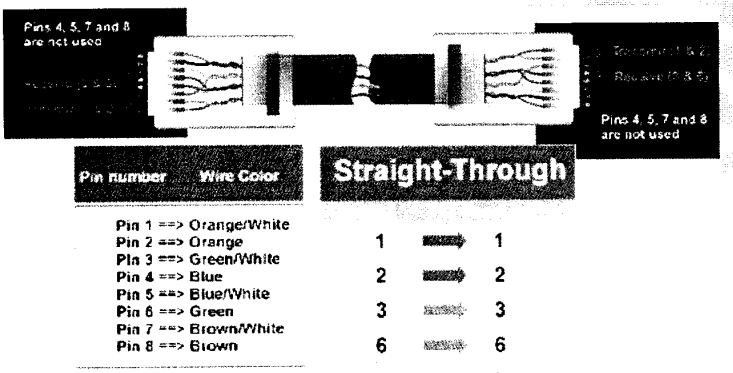
فاصله هر کامپیوتر در شبکه ای از نوع **Star** ، از محل **Hub** ویا **Switch** تا کارت شبکه کامپیوتر **Link** نامیده می شود. روش توزیع شبکه در ساختمان شباهت بسیار زیادی به توزیع برق دارد. در حقیقت هر وسیله ای که بخواهد به شبکه وصل شود توسط یک کابل که دو طرف آن **Connector** دارد **(Patch Cord)** به پریز شبکه نزدیک خود متصل می شود. پریز های اتاق توسط کابل های شبکه به اتاق مرکزی سایت متصل هستند. در واقع هر پریز به صفحه اتصالات **(Patch Panel)** متصل است و **Patch Panel** نیز توسط **Patch cord** به هاب و یا سویچ متصل می شود. فاصله بین پریز تا **Patch Panel** را **Horizontal** می گویند. با توجه به اینکه کابلهای **T.P.** حداکثر مسافت **100** متر را از نظر **Attenuation** پشتیبانی میکند ، **Horizontal** باید حداکثر **90** متر باشد که به انضمام کابلهای **Patch Cord** که در مسیر اتصال استفاده می شود کمتر از صد متر باشد.



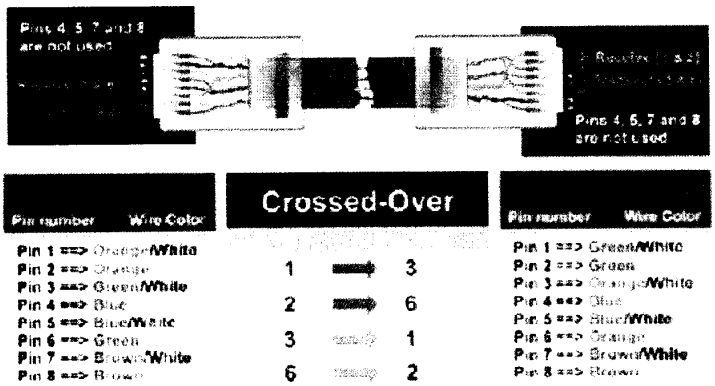
به تجهیزات داخل پریز های اتصال شبکه **Key Stone Jack** می گویند . کابل ها از پشت **Patch Panel** که در سایت مرکزی در داخل **Rack** قرار دارد به درون کانالهای دیوار منتقل می شوند و از درون کانالها به اتاق ها می رسد و به پریز ها متصل می شود. به شکل زیر توجه کنید:

قابل ذکر است **Patch Cord** ها که برای اتصال کامپیوتر ها به **Key Stone Jack** موجود درون پریز شبکه **(Face Plate)**

استفاده می شوند در هر دو سر کابل با یک ترتیب رنگ بندی به کانکتور متصل می شوند. به این کابل **Straight Through** می گویند.

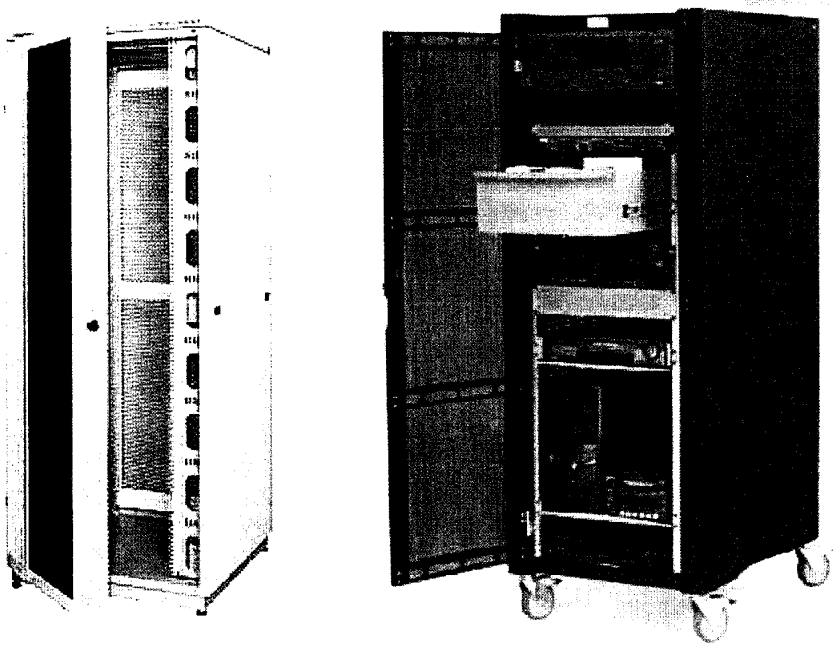


اما هرگاه دو کامپیوتر را بخواهیم مستقیما و بدون دخالت سویچ به هم وصل کنیم باید از **Cross Over** استفاده کنیم که ترتیب رنگ متفاوتی در دو سوی کابل دارد.



در صورتی که به تصویر زیر توجه نمائید نمائی از یک **Rack** را مشاهده می کنید. **Rack** به عنوان یک کابینت مخصوص برای حفظ تجهیزات شبکه کاربرد دارد. مثلا **Router** ها و **Switch** ها و برخی انواع **Server** ها در **Rack** نگهداری می شوند.

Rack مجهز به سیستم تهویه می باشد و جریان هوا درون آن کمک می کند که تجهیزات شبکه گرم نشوند.

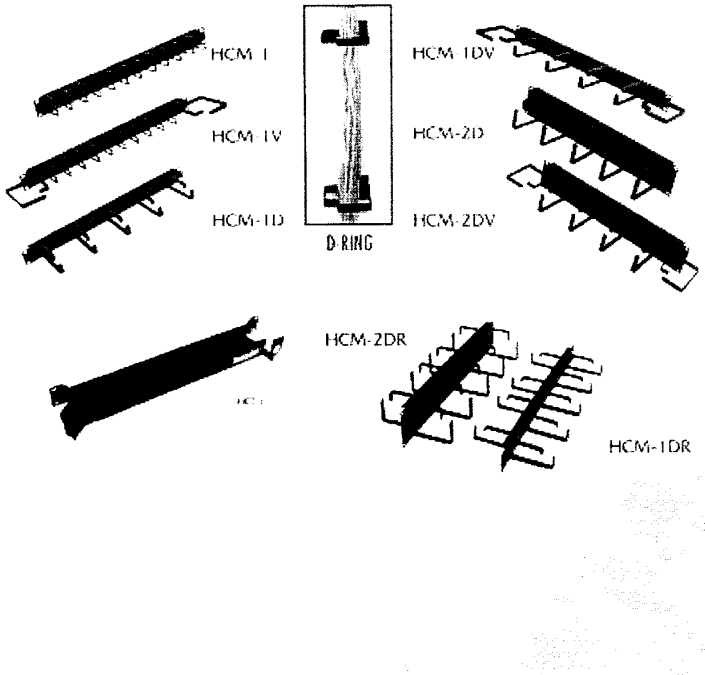


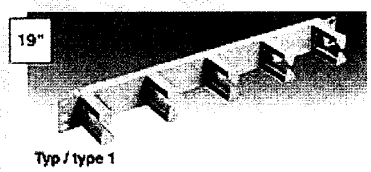
در یک قسمت مخصوص که پشت **Rack** در قسمت بالا ویا پائین قرار دارد کابلهای شبکه که به **Patch Panel** ها متصل شده اند از **Rack** خارج شده و وارد کانالهای **Trunk** می شوند و این کابلها در تمام نقاط ساختمان تا اتاق ها امتداد پیدا می کنند و به پریز ها متصل می شوند. به نقشه ای که در دو صفحه قبل نمایش داده شده توجه کنید.

درب رک به قفل مجهز است و معمولا شیشه ای است ، به گونه ای که بتوان از تجهیزات محافظت کرد و جریان هوای داخل **Rack** را نیز کنترل کرد. برای اینکه **Patch Cord** های استفاده شده برای اتصال **Patch Panel** به **Switch** باعث بی نظمی محیط داخل **Rack** نشوند از **Cable Manager** یا **Cable Guide** استفاده می شود.

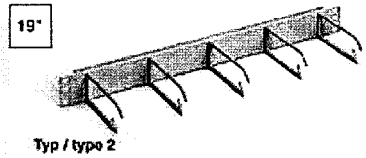
به شکل زیر توجه کنید :

در این شکل مدل های متفاوتی از **Cable Guide** نمایش داده شده است.



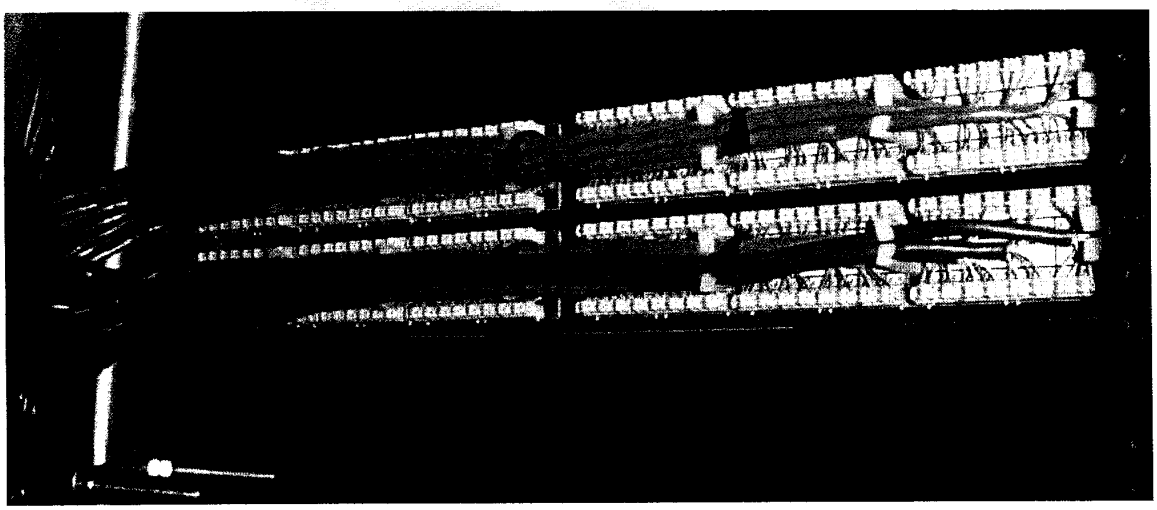


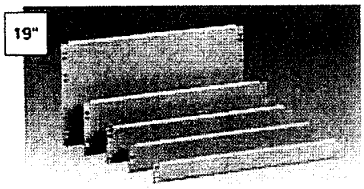
Typ / type 1



Typ / type 2

در شکل زیر روش اتصال کابلهائی که از اتاق ها و طبقات ساختمان یک شبکه ، توسط کانالهای **Trunk** به **Rack** هدایت شده اند ، به **Patch Panel** نمایش داده شده است.





برای پوشاندن فضاهای استفاده نشده در **Rack** از **Blank Unit** استفاده می کنند.

You will need a length of network cable (**UTP-Cat5**), preferably a factory assembled straight through cable that comfortabl reaches each computer. Be careful and measure accurately you would hate to find out that following the baseboard of the wal you end up two feet short. On the other hand you don't want to use a fifty foot cable to connect two computers ten feet apar Ethernet does not like coiled up excess cable. Consider making the cable with enough slack to allow servicing the compute without needing to unplug the cable.

The hardest part for most people will most likely be finding the **RJ45** cable connectors. Check with your local computer stor that do network installations, most techs will give you a couple if you ask. Otherwise you will have to buy a five or ten pack Make sure you get at least two, three is better. That way if you mess up you can just cut off the bad end and try again. Cut of the **RJ45** connector from one end of the cable and prepare the end for the new **RJ45** connector. I don't use measurements for stripping the cable end, I start by stripping at least 1 inch of the main cable insulation and then carefully trim the eight internal wires using the factory assembled end as a guide to the proper length. Just make sure that each wire is equal length and that the connector cable lock pinches the main cable insulation.

You don't need any fancy crimping tools to make one cable, just one normal size screw driver and one small screwdriver w a blade the same thickness' of the brass conductors in the **RJ45** connector. You may need a second pair of hands to help hol the cable and **RJ45** connector while you or your helper secures the connector cable lock. It's a little tricky to get all the wire into the proper holes but with a little patience anyone can do it. When it comes time to securing the connector cable lock use the normal size screwdriver that fits into the connector cable lock slot. It doesn't take a lot of pressure to seat the cable fo just tap lightly until the cable is secure.

Note: Make sure ALL wires are pushed completely into the connector before seating the connector cable lock.

Once the connector cable lock is secure it's time to move on to seating the brass wire conductors. This is probably the mo tricky part, each wire has a separate brass conductor that needs to be seated to make contact with the wire. Once again you will want a second pair of hands to hold the **RJ45** connector while you or your partner carefully seats each of the brass conductors. Lightly tap each conductor down with the small thin screwdriver to just below the plastic ridge, use the factory assembled end of the cable as a guide for how deep to seat the brass conductors.

Note: A pliers can be used to press down all the brass conductors at one time to the plastic ridges, then use the small thin blade screwdriver to finish seating to the proper recessed level.

That's it, if everything went well you now have an **Ethernet UTP Category 5 crossover cable**.

Note: The standard connector view shown is color-coded for a straight thru cable

Category 5 wiring standards:

EIA/TIA 568A/568B and **AT&T 258A** define the wiring standards and allow for two different wiring color codes.

Pin #	Signal	EIA/TIA 568A	AT&T 258A, or EIA/TIA 568B	Ethernet 10BASE-T 100BASE-T
1	Transmit+	White/Green	White/Orange	X
2	Transmit-	Green/White or Green	Orange/White or Orange	X
3	Receive+	White/Orange	White/Green	X
4	N/A	Blue/White or Blue	Blue/White or Blue	Not used *
5	N/A	White/Blue	White/Blue	Not used *
6	Receive-	Orange/White or Orange	Green/White or Green	X
7	N/A	White/Brown	White/Brown	Not used *
8	N/A	Brown/White or Brown	Brown/White or Brown	Not used *

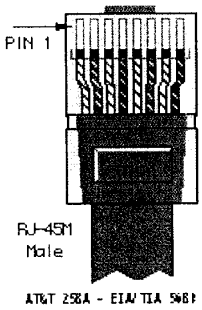
- Pairs may be solid colors and not have the stripe.
- Category 5 cable must use Category 5 rated connectors.

Only two pairs of wires in the eight-pin RJ-45 connector are used to carry Ethernet signals. Both **10BASE-T** and **100BASE-T** use the same pins, a **crossover cable** made for one will also work with the other.

Note: Even though pins 4,5,7, and 8 are not used, it is mandatory that they be present in the cable.

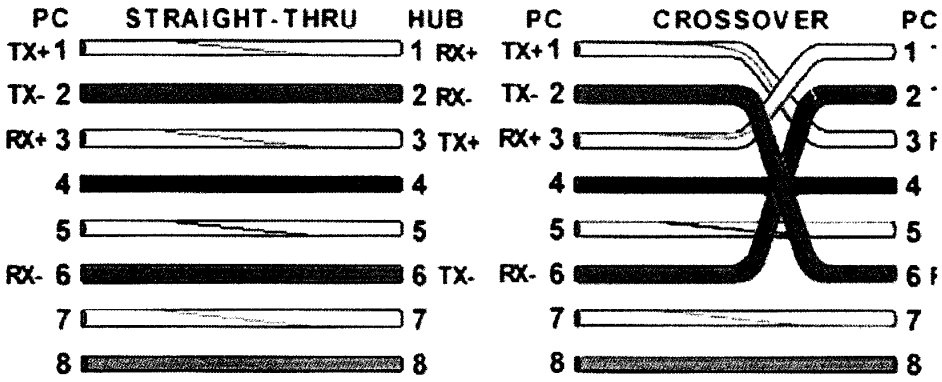
Crossover Cable

RJ-45 PIN	RJ-45 PIN
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-



Straight Through Cable

RJ-45 PIN	RJ-45 PIN
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-



جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه هفتم

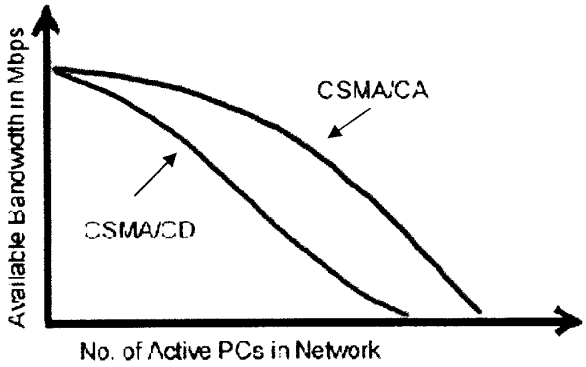
نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه هفتم:

- تعریف شیوه دسترسی و انواع آن (Access Method)
- تعریف Ethernet
- انواع Ethernet
- پروتکل TCP/IP و لایه های آن
- آدرس دهی در TCP/IP

در روش **CSMA/CA** دقیقا رفتار کامپیوتر ها مشابه روش قبلی است با این تفاوت که هر دستگاه عضو شبکه با ارسال یک پیغام خاص در شبکه مجوز استفاده از مدیا را به خود اختصاص می دهد و تا هنگام پایان نیافتن ارسال اطلاعات توسط یک دستگاه ، دیگر دستگاه ها اقدام به ارسال هیچگونه سیگنالی نمی کنند. در حقیقت منظور از **Collision Avoidance** این است که امکان پیش آمدن **Collision** وجود نخواهد داشت. هر کامپیوتر در این روش با ارسال یک سیگنال مخصوص کامپیوترهای دیگر را از اینکه قصد ارسال اطلاعات وجود دارد مطلع می سازد.



در روش **Token Passing** که در توپولوژی **Ring** استفاده می شود یک مجوز خاص به نام **Token** بین کامپیوتر ها در گردش است و هر کامپیوتری که می خواهد در شبکه چیزی ارسال کند باید صبر کند تا این **Token** به دست او برسد. پس از به دست آوردن **Token** ، کامپیوتر ارسال کننده آنرا نزد خود نگهداری کرده و اقدام به ارسال اطلاعات به صورت گردشی می کند و سپس **Token** را مجددا در شبکه به گردش می اندازد تا دستگاههای دیگر نیز به همین ترتیب بتوانند از آن استفاده کنند.

Ethernet چیست؟

اولین شبکه ای که با مشخصات یک شبکه **Ethernet** به وجود آمدن نتیجه تحقیقات تلاش انجام شده در دانشگاه **ALOHA** در هاوائی بود. این شبکه با تعداد **30** کامپیوتر در سال **1980** راه اندازی شد.

از آن پس به شبکه ای که دارای مشخصات زیر باشد **Ethernet** میگویند.

- **Access Method : CSMA/CD**
- **Signaling : Baseband – Digital**
- **Topology : Star or Bus**
- **Cable type : Coaxial – Twisted Pair – Fiber Optic**
- **Specification : 802.3**

انواع Ethernet عبارتند از :

- 10Base-2

این نوع از Ethernet از کابل Thin Net Coaxial استفاده می کند. سرعت انتقال اطلاعات آن حداکثر 10 Mbps است و دارای محدودیت 5-4-3 Rule می باشد.

- 10Base-5

این نوع از Ethernet از کابل Thick Net Coaxial استفاده می کند. سرعت انتقال اطلاعات حداکثر 10 Mbps است و دارای محدودیت 5-4-3 Rule می باشد.

- 10Base-T

در این نوع از کابل Twisted Pair استفاده می شود و سرعت آن 10 Mbps است. حداکثر تعداد کامپیوتر در چنین شبکه ای 1024 دستگاه می باشد.

- 10Base-F

در این روش از فیبر نوری استفاده می شود و با توجه به نوع فیبر، برای مسافت بیشتری می توان کابل کشی انجام داد.

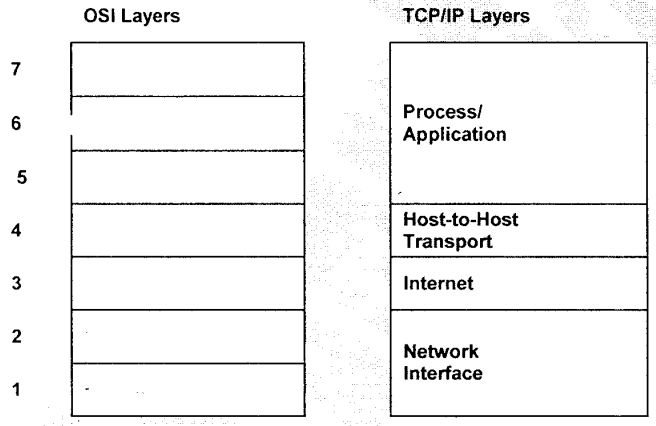
در مدل های دیگری از Ethernet که از کابلهای Twisted Pair و یا فیبر نوری جدیدتری استفاده می شود که با سرعت بیشتری امکان انتقال اطلاعات را دارند. به این انواع اصطلاحا Fast Ethernet نیز می گویند. تنوع این زیر مجموعه های Fast Ethernet زیاد است. تعدادی از آنها به قرار زیر می باشد:

- 100Base-TX
- 100Base-T4
- 100Base-FX

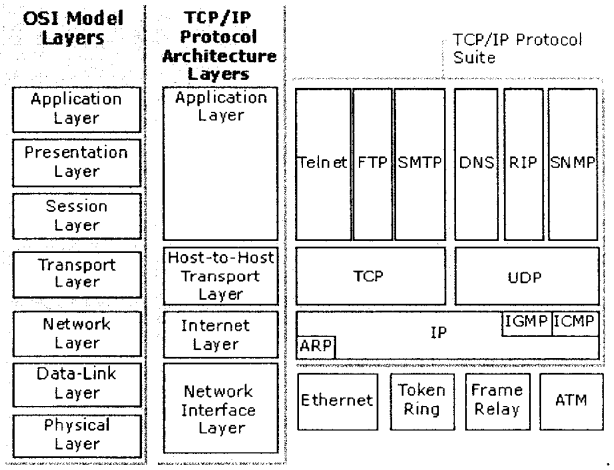
- پروتکل TCP/IP و لایه های آن

همانگونه که می دانید OSI به عنوان یک مرجع برای تمام سیستم های نرم افزار ی و سخت افزاری که بخواهند با شبکه ارتباط برقرار کنند اجباری است . نتیجتا TCP/IP نیز به عنوان یک Stack Protocol می بایست منطبق بر OSI عمل نماید.

TCP/IP به صورت چهار لایه ای تعریف شده است اما به گونه ای که تمام مراحل تعریف شده در OSI را انجام می دهد و کاملا بر OSI منطبق است. به شکل زیر توجه فرمائید



با کمی دقت در شکل بالا , این نکته را در می یابیم که TCP/IP کاملا منطبق بر OSI عمل می نماید و هر لایه آن به نوعی یک یا چند لایه از OSI را پوشش می دهد. شکل زیر ضمن نمایش این تطبیق, محل قرار گرفتن پروتکلهای زیر مجموعه TCP/IP را نیز نشان می دهد



پروتکلهای لایه Application که در مبحث شناخت پروتکل ها مورد بررسی قرار گرفتند در قسمت بالایی لایه های TCP/IP قرار دارند.

ارسال اطلاعات به دو روش Connection Oriented و Connectionless توسط دو پروتکلTCP و UDP انجام می پذیرد که در لایه Host to Host یا Transport قرار دارند.

ICMP (Internet Control Message Protocol) که در لایه Internet قرار دارد, مسئول انجام کارهای زیر می باشد:

- Echo Request و Echo Reply برای کنترل امکان ارتباط با یک دستگاه مرتبط با شبکه مبتنی بر IP
- Source Quench Message برای اطلاع دادن Buffer Over flow به کامپیوتر ارسال کننده اطلاعات.
- Destination Unreachable که نمایش دهنده عدم امکان ارتباط با مقصد مورد نظر می باشد.

تعدادی از کارهایی که ICMP مسئولیت انجام آنها را به عهده دارد در قسمت های بعدی مورد بررسی قرار می گیرند.

IGMP (Internet Group Management Protocol) برای انتقال اطلاعات به صورت Multicast در شبکه IP استفاده می شود.

ARP (Address Resolution Protocol) مسئولیت تبدیل IP Address به MAC Address را به عهده دارد. به این عمل اصطلاحا Name Resolve می گویند.

یکی از پروتکلهای مهم موجود در لایه Internet که مسئولیت آدرس دهی لاجیکال را به عهده دارد IP می باشد.

در لایه Network پروتکل هایی مثل Ethernet و Frame Relay و X.25 و موارد مشابه وجود دارند که مسئولیت آدرس دهی سخت افزاری و ارسال سیگنال به عهده آنهاست.

قبل از آغاز مبحث IP Addressing این نکته را باید یادآوری کرد که دانستن مفاهیم مربوط به مبنا ها و تبدیل آنها به یکدیگر از پیش نیاز های این بخش خواهد بود. مبناهای 2 و 10 و 16 در شبکه بسیار مورد استفاده قرار می گیرند و دانشجویان محترم می بایست به آن تسلط کافی داشته باشند. طی جلسات کلاسی از روش ساده ای برای تبدیل اعداد باینری به دسیمال , یعنی مبنای دو به ده و بالعکس استفاده می کنیم که جدول زیر برای محاسبات مذکور مورد استفاده قرار می گیرد.

7	6	5	4	3	2	1	0
128	64	32	16	8	4	2	1
128	192	224	240	248	252	254	255

- آدرس دهی در TCP/IP

هر کامپیوتری که بخواهد از TCP/IP استفاده کند باید برای معین کردن آدرس مبداء و مقصد، از آدرس IP که در لایه Network از OSI و در لایه Internet از TCP/IP تعریف شده است استفاده نماید.

این آدرس 32 بیت طول دارد و به چهار قسمت 8 بیتی که Octet نامیده می شوند تقسیم می شود. بین هر دو Octet یک نقطه وجود دارد.

هر عدد 8 بیتی در مبنای 10 از 0 تا 255 قابل تغییر خواهد بود و به همین علت IP Address به صورت نمایش باینری از چهار قسمت تشکیل می شود که در هر قسمت عددی بین 0 تا 255 نوشته شده است. مانند :

192.168.231.17

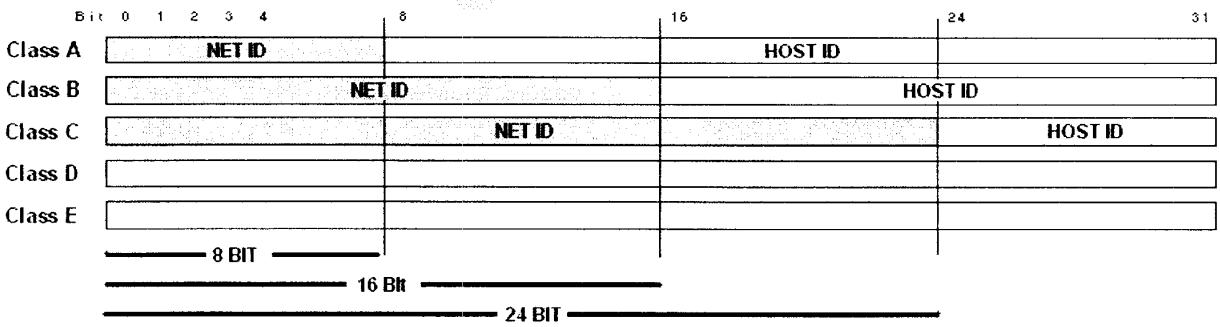
در صورتی که IP آدرس بالا را به صورت باینری بنویسیم به صورت زیر خواهد بود:

11000000.10101000.11100111.00010001

IP Address به دو قسمت اصلی تقسیم می شود که عبارتند از:

- مشخصه شبکه ای NET ID
- مشخصه میزبان HOST ID

تمام کامپیوتر های یک شبکه IP باید دارای NET ID مشابه باشند و HOST ID آنها با یکدیگر تفاوت داشته باشد. NET ID می تواند 8 بیت اول ویا 16 بیت اول و یا 24 بیت اول از سمت چپ IP Address باشد. البته در Class Less IP Addressing از NET ID با اندازه غیر از 8 یا 16 یا 24 بیت نیز استفاده می شود.



IP Address دارای پنج کلاس می باشد

در CLASS A تمام کامپیوتر ها 8 بیت مشترک دارند . یعنی NET ID هشت بیت سمت چپ و HOST ID بیست و چهار بیت می باشد.

در CLASS B تمام کامپیوتر ها 16 بیت مشترک دارند. یعنی NET ID شانزده بیت سمت چپ و HOST ID شانزده بیت می باشد.

در CLASS C تمام کامپیوتر ها 24 بیت مشترک دارند. یعنی NET ID بیست و چهار بیت سمت چپ و HOST ID هشت بیت می باشد.

وضعیت CLASS D , CLASS E در درسهای بعدی مورد بررسی قرار می گیرد.

CLASS	BIT Arrangement	Left Octet Value Range	Left Octet Useful Range	Host Per Subnet Formula	Host Per Subnet
A	0xxxxxxx	0-127	1-126	(2^24)-2	16777214
B	10xxxxxx	128-191	128-191	(2^16)-2	65534
C	110xxxxx	192-223	192-223	(2^8)-2	254
D	1110xxxx	224-239	224-239		
E	1111xxxx	240-255			

متن زیر را مطالعه بفرمائید:

TCP/IP Addressing

Each host on the TCP/1P network has a unique 32-bit network address-referred to as the IP address-that is unique for each host on the network. If the host will participate on the Internet, this address must also be unique to the Internet. For this reason, Internet IP addresses are controlled by an administrative agency, such as the InterNIC.

The IP address is a sequence of four bytes and is written in the form of four decimal integers separated by periods (for example, 0.0.0.0). Each integer is 8 bits long and ranges from 0 to 255. The IP address consists of two parts: a network ID assigned by the InterNIC administrative agency and the host ID assigned by the local administrator. The first integer of the address (0.0.0.0) determines the address type and is referred to as its class, There are five classes of IP addresses: A, B, C, D, andE. Without going into great detail, the following is a brief description of each class.

Class A Networks

Class A networks are used for very large networks with millions of hosts, such as the Internet. A class A network number uses the first 8 bits of the IP address as its network ID. The remaining 24 bits comprise the host part of the IP address. The values assigned to the first byte of class A network numbers fall within the range 0 to 127. For example, consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining 3 bytes is left to the discretion of the owner of the network number. Only 127 class A networks can exist; each of these networks can accommodate up to 16,777,214 hosts.

Class B Networks

Class B networks are medium-sized networks, such as universities and large businesses with many hosts. A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128 to 191. In the number 129.144.50.56, the first 2 bytes, 129.144, are assigned by the InterNIC and comprise the network address. The last 2 bytes, 50.56, make up the host address and are assigned at the discretion of the network's owner. A class B network can accommodate a maximum of 65,534 hosts.

Class C Networks

Class C networks are used for small networks containing fewer than 254 hosts. Class C network numbers use 24 bits for the network number and 8 bits for host numbers. A class C network number occupies the first 3 bytes of an IP address; only the fourth byte is assigned at the discretion of the network's owner. The first byte of a class C network number covers the range 192 to 223. The second and third bytes each cover the range I to 255. A typical class C address might be 192.5.2.5, with the first 3 bytes, 192.5.2, forn-iing the network number. The final byte in this example, 5, is the host number. A class C network can accommodate a maximum of 254 hosts.

Class D and E Networks

Class D addresses cover the range 224 to 239 and are used for IP multicasting as defined in RFC 988. Class E addresses cover the range 240 to 255 and are reserved for experimental use.

هر **IP Address** توسط یک **Subnet Mask** از نظر تعداد بیت های **NET ID** و **HOST ID** قابل تشخیص می گردد و در حقیقت **Subnet mask** از سمت چپ با بیت های ارزش دهی شده با مقدار یک تا مرز **Host ID** پیش می رود.

Subnet Mask در حالت **Class Full** یکی از سه حالت زیر می باشد:

255.0.0.0 **11111111.00000000.00000000.00000000**

255.255.0.0 **11111111.11111111.00000000.00000000**

255.255.255.0 **11111111.11111111.11111111.00000000**

برای مثال یک **IP Address** از نوع **CLASS A** با توجه به اینکه از هشت بیت اول از سمت چپ به عنوان **NET ID** استفاده می کند باید دارای **Subnet Mask** با مقدار زیر باشد.

```
IP Address      = 01000100 . 11000000 . 11111110 . 01100100   (68.192.254.100)
Subnet Mask     = 11111111 . 00000000 . 00000000 . 00000000   (255.0.0.0)
AND Operation   ------------------------------------------------------------
Network Number  = 01000100 . 00000000 . 00000000 . 00000000   (68.0.0.0)
```

طبق آنچه در مثال بالا نمایش داده شده است , در صورتی که IP Address را در Subnet Mask آن AND کنیم , ادرس شبکه که به آن Network Number می گویند بدست می آید.

جدول زیر تعدادی IP Address را همراه با مشخصات مرتبط به آنها به عنوان مثال در بر دارد.

CLASS	IP Address	Subnet Mask	Network Number	NET ID Bits	HOST ID Bits
A	10.32.213.21	255.0.0.0	10.0.0.0	8	24
A	65.123.30.254	255.0.0.0	65.0.0.0	8	24
A	126.0.1.2	255.0.0.0	126.0.0.0	8	24
A	1.250.9.7	255.0.0.0	1.0.0.0	8	24
B	162.67.43.21	255.255.0.0	162.67.0.0	16	16
B	153.19.72.120	255.255.0.0	153.19.0.0	16	16
B	129.76.34.50	255.255.0.0	129.76.0.0	16	16
B	190.200.210.254	255.255.0.0	190.200.0.0	16	16
C	200.200.200.1	255.255.255.0	200.200.200.0	24	8
C	220.190.21.38	255.255.255.0	220.190.21.0	24	8
C	192.168.0.1	255.255.255.0	192.168.0.0	24	8

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه هشتم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه هشتم:

- شناخت بیشتر TCP/IP Addressing
- Routing چیست و چه ارتباطی با IP Address دارد؟
- Routing Protocol چیست؟
- Collision Domain چیست؟

- شناخت بیشتر TCP/IP Addressing

- آدرس دهی در TCP/IP

با اشاره به مطالب قبلی اینگونه نتیجه گرفتیم که می توان به هر کارت شبکه IP Address ای از کلاس A و یا B و یا C نسبت داد و پس از این کار آن کارت شبکه از IP Address مذکور برای معرفی خود در شبکه استفاده می کند.

مشخصات کلاسهای متفاوت IP در جدول زیر ذکر شده است:

Network Number	Subnet Mask	Broadcast Add.	Start Add.	End Add.	
A.0.0.0	255.0.0.0	A.255.255.255	A.0.0.1	A.255.255.254	/8
B.x.0.0	255.255.0.0	B.x.255.255	B.x.0.1	B.x.255.254	/16
C.x.y.0	255.255.255.0	C.x.y.255	C.x.y.1	C.x.y.254	/24

توضیحات :

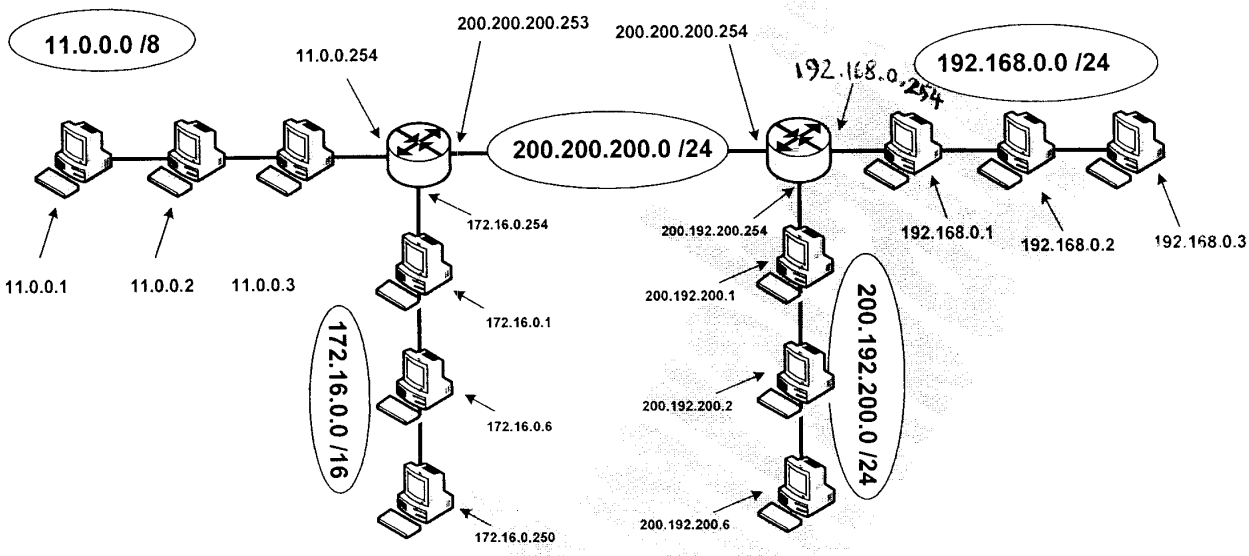
- A می تواند بین 1 تا 126 تغییر نماید
- B می تواند بین 128 تا 191 تغییر نماید
- C می تواند بین 192 تا 223 تغییر نماید.
- X و Y می تواند بین 0 تا 255 تغییر نماید
- آدرس Broadcast و Network Number قابل نسبت دادن به هیچ کارت شبکه ای نیست.
- هر آدرس Class C توانایی آدرس دهی به 254 کامپیوتر را دارد
- هر آدرس Class B توانایی آدرس دهی به 65534 کامپیوتر را دارد
- هر آدرس Class A توانایی آدرس دهی به 16777214 کامپیوتر را دارد.

قابل ذکر است هرگاه کامپیوتری در یک Subnet بخواهد یک Packet از نوع Broadcast برای دیگر کامپیوتر های شبکه خود ارسال کند از آدرس Broadcast استفاده می کند. آدرس Broadcast از پر کردن بیت های Host ID با مقدار 1 به دست می آید.

Net# in Dec Form	Net# in Bin Form	Broadcast in Dec Form	Broadcast in Bin Form
192.16.6.0	11000000.00010000.00000110.00000000	192.16.6.255	11000000.00010000.00000110.11111111

Routing چیست و چه ارتباطی با **IP Address** دارد؟

هر **Router** بر اساس **Network Number** مربوط به آدرس **Frame** های دریافتی تشخیص می دهد که آن **Frame** را به کدام سمت ارسال نماید. به شکل زیر توجه کنید:



کامپیوتر های هر **Subnet** در قسمت **Net ID** از **IP Address** هایشان با یکدیگر مشترک هستند و در هیچ **Subnet** ای دو کامپیوتر با **IP Address** های یکسان وجود ندارند. ضمنا تمام کامپیوتر ها **Subnet Mask** مشابه هم دارند.

هرگاه تمام بیت های قسمت **Host ID** از **IP Address** صفر شود **Network Number** به دست می آید.محاسبه **Network Number** مربوط به هر **IP Address** از طریق **AND** کردن **IP Address** در **Subnet Mask** آن انجام می پذیرد.

به نمونه ای از این محاسبه توجه کنید:

نمونه (الف)

```
IP Address      = 01000100 . 11000000 . 11111110 . 01100100   (68.192.254.100)
Subnet Mask     = 11111111 . 00000000 . 00000000 . 00000000   (255.0.0.0)
AND Operation   ------------------------------------------------------------
Network Number  = 01000100 . 00000000 . 00000000 . 00000000   (68.0.0.0)
```

نمونه (ب)

```
IP Address      = 01000100 . 00000010 . 00000101 . 00000001   (68.2.5.1)
Subnet Mask     = 11111111 . 00000000 . 00000000 . 00000000   (255.0.0.0)
AND Operation   ------------------------------------------------------------
Network Number  = 01000100 . 00000000 . 00000000 . 00000000   (68.0.0.0)
```

همانگونه که در مثال های صفحه قبل مشخص شده است هر دو **IP Address** دارای **Network Number** برابر هستند.

هر **router** با توجه به **Network Number** آدرس مقصد در هر **Packet** تشخیص می دهد که از چه راهی می تواند آنرا به مقصد برساند.

با توجه به اینکه **Router** اجازه عبور **Packet** های **Broadcast** را نمی دهد، هر محدوده که توسط **Router** از محدوده های دیگر جدا شده است را **Broadcast Domain** می نامند.

- **Routing Protocol** چیست؟

با توجه به اینکه هر **Router** به صورت عادی صرفا **Subnet** های متصل به خودش را می شناسد چگونه می تواند تشخیص دهد که یک **Packet** را از چه راهی باید به یک شبکه دوردست برساند؟

مسلما هر **Router** باید در مورد شبکه هایی که به آنها به صورت مستقیم متصل است و **Network Number** آنها اطلاعاتی را به **Router** های مجاور خود ارسال کنند و به این ترتیب با اطلاعاتی که دست به دست بین **Router** ها جا به جا می شود ، مسیر های متفاوت دسترسی به هر مقصد شناخته شده و در نتیجه **Router** می تواند اطلاعات را از مسیر های موجود به طرف مقصد راهنمایی کند.

این تنظیمات می تواند به صورت **Static** توسط **Administrator** در **Router** تنظیم شود. اما با توجه به اینکه این تنظیمات بسیار پیچیده هستند ، پروتکل هایی وجود دارند که به صورت اتوماتیک این تنظیمات را بر روی **router** انجام داده و اطلاعات مربوطه را نیز بین آنها جابجا می کنند. به این پروتکل ها **Routing Protocol** می گویند.

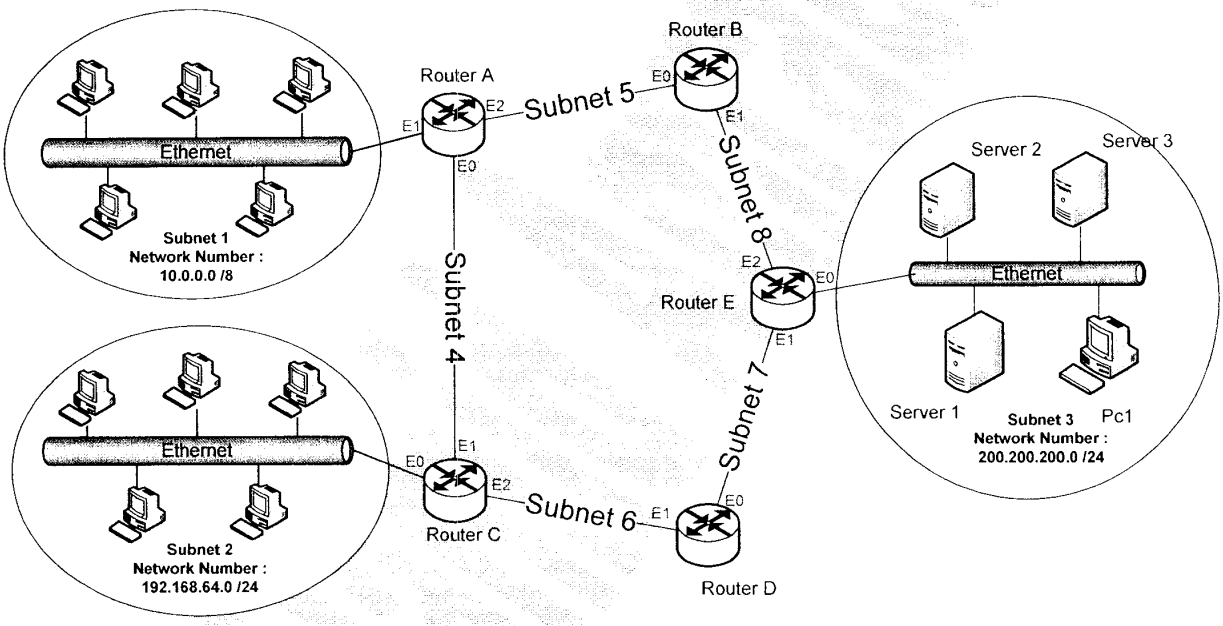
تعدادی از **Routing Protocol** ها به قرار زیر هستند:

- **RIP v1**
- **RIP v2**
- **OSPF**
- **NLSP**
- **IGRP**
- **EIGRP**
- **BGP**
- **EGP**

Routing چیست و **Routing Table** در آن چه نقشی دارد؟

همانگونه از توضیحات مشخص است هر **Router** باید بتواند بر اساس یک سری اطلاعات تصمیم بگیرد که یک **Packet** را در چه جهت راهنمائی و ارسال نماید که از کوتاه ترین راه به مقصد برسد. در این میان از **Routing Protocol** به عنوان یک ابزار یاد شد که می تواند به **Router**ها کمک کند تا به صورت اتوماتیک از **Subnet** های پیرامون خود اطلاعات کسب کنند و با رد و بدل کردن این اطلاعات با **Router** های همسایه خود به صورت مستمر آنرا تکمیل تر نمایند. این اطلاعات در جدولی که به آن **Routing Table** میگویند ثبت و نگهداری می شود و هر **Router** بر اساس این جدول نسبت به جهت یابی برای ارسال **Packet** ها اقدام می کند.

به شکل زیر توجه فرمائید:



هر پورت از هر **Router** را با یک معرفه شناسائی می کنند. مثلا برای پورت از نوع **Ethernet** از نام مشابه **E0** ویا **E1** استفاده می کنند. یا در مورد پورت های **Fast Ethernet** از نام های **FE0** ویا **FE2** و .. استفاده می کنند.در شکل بالا نیز هر هر پورت با یک معرفه معین گردیده است.

اگر کامپیوتری از **Subnet 1** بخواهد با **Server 2** در **Subnet 3** صحبت کند باید **Packet** ارسالی را به **Router A** بسپارد. **Router A** با توجه به مقادیر ثبت شده در **Routing Table** خود **Packet** مذکور را تحویل **Router B** می دهد. سپس **Router B** آن **Packet** را به **Router C** می فرستد و در نهایت اطلاعات ارسالی به مقصد در **Subnet 3** میرسد.

به Routing Table موجود در Router A توجه نمائید:

Network Destination	Subnet Mask	Gateway	Interface	Metric
10.0.0.0	255.0.0.0	Router A – E1	Router A – E1	1
Subnet 5	-	Router A – E2	Router A – E2	1
Subnet 4	-	Router A – E0	Router A – E0	1
Subnet 8	-	Router B – E0	Router A – E2	2
Subnet 8	-	Router C – E1	Router A – E0	4
Subnet 7	-	Router B – E0	Router A – E2	3
Subnet 7	-	Router C – E1	Router A – E0	3
192.168.64.0	255.255.255.0	Router C – E1	Router A – E0	2
192.168.64.0	255.255.255.0	Router B – E0	Router A – E2	5
200.200.200.0	255.255.255.0	Router B – E0	Router A – E2	3
200.200.200.0	255.255.255.0	Router C – E1	Router A – E0	4

- در ستون Metric هر چه عدد کوچکتر باشد نشانگر فاصله کوتاه تر می باشد.
- ستون Interface نمایش دهنده این است که برای ارسال Packet کدام پورت Router باید استفاده شود.
- Gateway نمایش دهنده این است که Router برای راهنمایی Packet به طرف مقصد باید آنرا به کدام Router همسایه ارسال کند.
- در ستون Network Destination شبکه های مقصد نام برده شده اند.

قابل توجه اینکه Router A توانسته Subnet هائی غیر از آنچه متصل به آن است را نیز شناسایی و در جدول خود اضافه نماید. این شناخت به دلیل وجود داشتن Routing Protocol ها امکان پذیر گشته و در غیر اینصورت باید به صورت دستی توسط Administrator به Router شناسانده شود که به این کار اصطلاحا تنظیم Static Route می گویند.

- Collision Domain چیست؟

همانطور که می دانید Bridge و Switch در لایه Datalink از OSI کار می کنند. هر تجهیزات انتقال دهنده اطلاعات که در لایه Datalink و یا بالاتر از آن کار کنند ، اجازه پیش آمدن Collision بین تجهیزاتی که از طریق آن با هم ارتباط یافته اند را نمی دهد.

در نتیجه اگر تعدادی کامپیوتر با Hub به هم وصل شوند در محدوده ای واقع می شوند که امکان تداخل سیگنال یا Collision با یکدیگر خواهند داشت. اما در صورتی که به جای Hub از Switch استفاده شود هر پورت از Switch یک محدوده جدا برای Collision ها ایجاد می کند و درنتیجا با توجه به قرار گرفتن کامپیوتر ها در محدوده های Collision مجزا ، امکان پیش آمدن تداخل سیگنال از بین می رود.

به این محدوده ها Collision Domain می گویند.

جزوه درسی

مهندسی شبکه

ترم پیش نیاز

درس Network+

جلسه نهم

نام استاد : مهندس امرآبادی

MCP, MCP+I, MCSE NT4.0, MCSA 2000, MCSE 2000, MCSA 2003, MCSE 2003, CCNA

جلسه نهم :

- Gateway چیست؟
- سیستم های ارتباطی بی سیم (Wireless) :

Gateway چیست؟

با توجه به اینکه نرم افزار های متفاوت در شبکه با روش های متفاوت ارائه خدمات می کنند و در خیلی از شبکه های گسترده نیاز است که از سرویس دهنده های متفاوت با Platform های گوناگون استفاده شود ، باید راه کاری وجود داشته باشد تا بتوان این انواع متفاوت Server ها را به یکدیگر ارتباط داد.

مثلا اگر سیستم عامل Novell Netware را به عنوان File Server در شبکه استفاده کنیم ، چگونه باید سیستم عامل Microsoft به عنوان Client با آن ارتباط برقرار کند؟

در حقیقت Gateway به نرم افزاری می گویند که ساختار ها و Platform های متفاوت را به یکدیگر مرتبط می سازد و در این ارتباط حکم یک ترجمه کننده را دارد. برای مثال می توان GSNW و CSNW و FPNW و SNA را نام برد.

با توجه به اینکه Netware از IPX/SPX به عنوان پروتکل ارتباطی استفاده می کند , باید بر روی Windows نیز NWLink IPX/SPX را نصب نمایند تا این دو بتوانند با هم ارتباط برقرار نمایند.انجام این لازم هست ولی کافی نیست! برای اینکه Microsoft Windows بتواند با Netware ارتباط برقرار کند علاوه بر پروتکل باید Client Service مناسب نیز بر روی آن نصب شود.

راه اندازی CSNW یا Client Services for NetWare بر روی Windows امکان ارتباط برقرار کردن Microsoft Client را با Netware Server فراهم می سازد.

Gateway Service های دیگری نیز وجود دارند که به دلایل مشابه در شبکه استفاده می شوند. مثلا اگر بخواهیم در شبکه Client های Microsoft Windows بدون نیاز به برقراری ارتباط با NetWare File Server از منابع share شده بر روی آن استفاده کنند , یک کامپیوتر Microsoft Windows Server را به عنوان واسط در نظر گرفته و بر روی آن (Gateway Services for NetWare) که به اختصار GSNW خوانده می شود را نصب می کنیم. از آن پس کامپیوتر های Client برای استفاده از منابع به این دستگاه Server مراجعه می کنند و به صورت غیر مستقیم از خدمات NetWare Server ای که در این میان از دید Client ها پنهان است استفاده می کنند.

سیستم های ارتباطی بی سیم (Wireless) :

با توجه به اینکه در برخی نقاط نمی توان از کابل برای انتقال اطلاعات استفاده کرد به مرور سیستم های جدید به تجهیزات ارسال و دریافت بی سیم مجهز شدند. برای انتقال اطلاعات در ای روش می توان از تکنولوژی های زیادی استفاده کرد که هر یک به نوعی اقدام به ارسال و دریافت سیگنال می کنند. مانند :

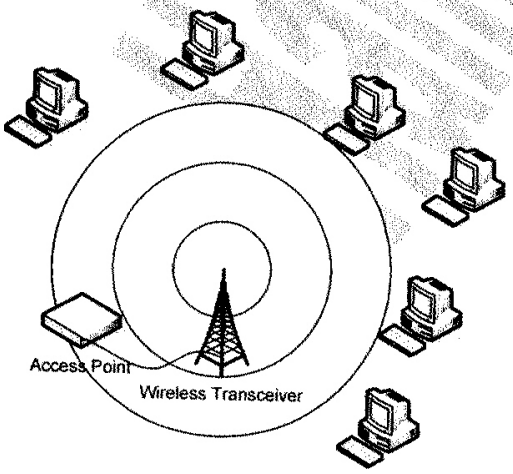
- اشعه لیزر
- اشعه مادون قرمز
- مایکرو ویو (Microwave)

هر تکنولوژی با توجه به نوع سیگنال از نظر پهنای باند و مسافت و... دارای مشخصات ویژه ای است.

Wireless با شماره استاندارد 802.11 شناسائی شده و دارای Category های مختلفی است. مانند: 802.11a , 802.11b , 802.11g

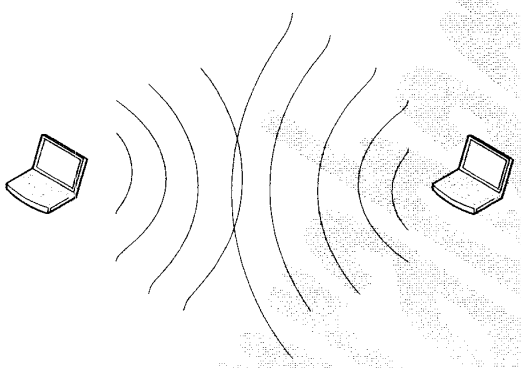
در مدل WLAN (Wireless Local Area Network) کامپیوتر های درون یک محیط مانند طبقات یک ساختمان از طریق ابزاری که مانند Hub عمل می کند به یکدیگر اتصال می یابند. این نوع hub با توجه به اینکه کابلی به آن وصل نیست و صرفا نقطه اتصال مرکزی سیستم ها به صورت بی سیم می باشد , Wireless Hub یا Access Point نامیده می شود. معمولا Access Point می تواند تعداد محدودی کامپیوتر را به هم وصل کند و باید به یک آنتن مجهز باشد.

به شکل زیر توجه کنید:



در مدل **adhoc** که برای اتصال دو دستگاه به صورت مستقیم به یکدیگر کاربرد دارد , دو کامپیوتر توسط آنتن های **wireless** از طریق کارتهای شبکه بی سیم خود اقدام به ارسال و دریافت مستقیم اطلاعات می نمایند. در روش های بی سیم سرعت قابل مقایسه با کابل نیست. مسلما کیفیت و سرعت و امنیت انتقال اطلاعات در هنگام استفاده از کابل به عنوان **Media** بسیار بالاتر است.

شکل زیر نمایش دهنده مدل **adhoc** است.



اما در عین حال **wireless** می تواند تکنولوژی مناسبی برای ارتباط دادن شبکه ها به یکدیگر باشد. با این هدف که شبکه ها را با استفاده از کابل ایجاد نمائیم و هر گاه موقعیت جغرافیایی آنها با یکدیگر متفاوت بود , از **Wireless** برای ایجاد ارتباط استفاده کنیم.