# Networking Basics

Computer networking has become an integral part of business today. Individuals, professionals and academics have also learned to rely on computer networks for capabilities such as electronic mail and access to remote databases for research and communication purposes. Networking has thus become an increasingly pervasive, worldwide reality because it is fast, efficient, reliable and effective. Just how all this information is transmitted, stored, categorized and accessed remains a mystery to the average computer user.

This tutorial will explain the basics of some of the most popular technologies used in networking, and will include the following:

- Types of Networks - including LANs, WANs and WLANs
- The Internet and Beyond - The Internet and its contributions to intranets and extranets
- Types of LAN Technology - including Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet,
  ATM, PoE and Token Ring
- Networking and Ethernet Basics - including standard code, media, topographies, collisions and CSMA/CD
- Ethernet Products - including transceivers, network interface cards, hubs and repeaters

## Types of Networks

In describing the basics of networking technology, it will be helpful to explain the different types of networks in use.

### Local Area Networks (LANs)

A network is any collection of independent computers that exchange information with each other over a shared communication medium. Local Area Networks or LANs are usually confined to a limited geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but can often link hundreds of computers used by thousands of people. The development of standard networking protocols and media has resulted in worldwide proliferation of LANs throughout business and educational organizations.

### Wide Area Networks (WANs)

Often elements of a network are widely separated physically. Wide area networking combines multiple LANs that are geographically separate. This is accomplished by connecting the several LANs with dedicated leased lines such as a T1 or a T3, by dial-up phone lines (both synchronous and asynchronous), by satellite links and by data packet carrier services. WANs can be as simple as a modem and a remote access server for employees to dial into, or it can be as complex as hundreds of branch offices globally linked. Special routing protocols and filters minimize the expense of sending data over vast distances.

### Wireless Local Area Networks (WLANs)

Wireless LANs, or WLANs, use radio frequency (RF) technology to transmit and receive data over the air. This minimizes the need for wired connections. WLANs give users mobility as they allow connection to a local area network without having to be physically connected by a cable. This freedom means users can access shared resources without looking for a place to plug in cables, provided that their terminals are mobile and within the designated network coverage area. With mobility, WLANs give flexibility and increased productivity, appealing to both entrepreneurs and to home users. WLANs may also enable network administrators to connect devices that may be physically difficult to reach with a cable.

The Institute for Electrical and Electronic Engineers (IEEE) developed the 802.11 specification for wireless LAN technology. 802.11 specifies over-the-air interface between a wireless client and a base station, or between two wireless clients. WLAN 802.11 standards also have security protocols that were developed to provide the same level of security as that of a wired LAN.
The first of these protocols is Wired Equivalent Privacy (WEP). WEP provides security by encrypting data sent over radio waves from end point to end point.

The second WLAN security protocol is Wi-Fi Protected Access (WPA). WPA was developed as an upgrade to the security features of WEP. It works with existing products that are WEP-enabled but provides two key improvements: improved data encryption through the temporal key integrity protocol (TKIP) which scrambles the keys using a hashing algorithm. It has means for integrity-checking to ensure that keys have not been tampered with. WPA also provides user authentication with the extensible authentication protocol (EAP).

**Wireless Protocols**

| **Specification** | **Data Rate** | **Modulation Scheme** | **Security** |
|---|---|---|---|
| 802.11 | 1 or 2 Mbps in the 2.4 GHz band | FHSS, DSSS | WEP and WPA |
| 802.11a | 54 Mbps in the 5 GHz band | OFDM | WEP and WPA |
| 802.11b/High Rate/Wi-Fi | 11 Mbps (with a fallback to 5.5, 2, and 1 Mbps) in the 2.4 GHz band | DSSS with CCK | WEP and WPA |
| 802.11g/Wi-Fi | 54 Mbps in the 2.4 GHz band | OFDM when above 20Mbps, DSSS with CCK when below 20Mbps | WEP and WPA |

# Types of LAN Technology

## Ethernet

Ethernet is the most popular physical layer LAN technology in use today. It defines the number of conductors that are required for a connection, the performance thresholds that can be expected, and provides the framework for data transmission. A standard Ethernet network can transmit data at a rate up to 10 Megabits per second (10 Mbps). Other LAN types include Token Ring, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk.

Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. These benefits, combined with wide acceptance in the computer marketplace and the ability to support virtually all popular network protocols, make Ethernet an ideal networking technology for most computer users today.

The Institute for Electrical and Electronic Engineers developed an Ethernet standard known as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network and also specifies how the elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

## Fast Ethernet

The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds. This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure. Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.

There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable; 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable. The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.

Network managers who want to incorporate Fast Ethernet into an existing configuration are required to make many decisions. The number of users in each site on the network that need the higher throughput must be determined; which segments of the backbone need to be reconfigured specifically for 100BASE-T; plus what hardware is necessary in order to connect the 100BASE-T segments with existing 10BASE-T segments. Gigabit Ethernet is a future technology that promises a migration path beyond Fast Ethernet so the next generation of networks will support even higher data transfer speeds.

## Gigabit Ethernet

Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP). Also known as "gigabit-Ethernet-over-copper" or 1000Base-T, GigE is a version of Ethernet that runs at speeds 10 times faster than 100Base-T. It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone. Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.

From the data link layer of the OSI model upward, the look and implementation of Gigabit Ethernet is identical to that of Ethernet. The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

## 10 Gigabit Ethernet

10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards. IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.

Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections. This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing. As it is still very new, which of the standards will gain commercial acceptance has yet to be determined.

### Asynchronous Transfer Mode (ATM)

ATM is a cell-based fast-packet communication technique that can support data-transfer rates from sub-T1 speeds to 10 Gbps. ATM achieves its high speeds in part by transmitting data in fixed-size cells and dispensing with error-correction protocols. It relies on the inherent integrity of digital lines to ensure data integrity.

ATM can be integrated into an existing network as needed without having to update the entire network. Its fixed-length cell-relay operation is the signaling technology of the future and offers more predictable performance than variable length frames. Networks are extremely versatile and an ATM network can connect points in a building, or across the country, and still be treated as a single network.

**LAN Technology Specifications**

| Name | IEEE Standard | Data Rate | Media Type | Maximum Distance |
|---|---|---|---|---|
| Ethernet | 802.3 | 10 Mbps | 10Base-T | 100 meters |
| Fast Ethernet/ 100Base-T | 802.3u | 100 Mbps | 100Base-TX<br>100Base-FX | 100 meters<br>2000 meters |
| Gigabit Ethernet/ GigE | 802.3z | 1000 Mbps | 1000Base-T<br>1000Base-SX<br>1000Base-LX | 100 meters<br>275/550 meters<br>550/5000 meters |
| 10 Gigabit Ethernet | IEEE 802.3ae | 10 Gbps | 10GBase-SR<br>10GBase-LX4<br>10GBase-LR/ER<br>10GBase-SW/LW/EW | 300 meters<br>300m MMF/ 10km SMF<br>10km/40km<br>300m/10km/40km |

### Token Ring

Token Ring is another form of network configuration. It differs from Ethernet in that all messages are transferred in one direction along the ring at all times. Token Ring networks sequentially pass a “token” to each connected device. When the token arrives at a particular computer (or device), the recipient is allowed to transmit data onto the network. Since only one device may be transmitting at any given time, no data collisions occur. Access to the network is guaranteed, and time-sensitive applications can be supported. However, these benefits come at a price. Component costs are usually higher, and the networks themselves are considered to be more complex and difficult to implement. Various PC vendors have been proponents of Token Ring networks.

## Networking and Ethernet Basics

### Protocols

After a physical connection has been established, network protocols define the standards that allow computers to communicate. A protocol establishes the rules and encoding specifications for sending data. This defines how computers identify one another on a network, the form that the data should take in transit, and how this information is processed once it reaches its final destination. Protocols also define procedures for determining the type of error checking that will be used, the data compression method, if one is needed, how the sending device will indicate that it has finished sending a message, how the receiving device will indicate that it has received a message, and the handling of lost or damaged transmissions or "packets".

The main types of network protocols in use today are: TCP/IP (for UNIX, Windows NT, Windows 95 and other platforms); IPX (for Novell NetWare); DECnet (for networking Digital Equipment Corp. computers); AppleTalk (for Macintosh computers), and NetBIOS/NetBEUI (for LAN Manager and Windows NT networks).

Although each network protocol is different, they all share the same physical cabling. This common method of accessing the physical network allows multiple protocols to peacefully coexist over the network media, and allows the builder of a network to use common hardware for a variety of protocols. This concept is known as "protocol independence," which means that devices which are compatible at the physical and data link layers allow the user to run many different protocols over the same medium.

## The Open System Interconnection Model

The Open System Interconnection (OSI) model specifies how dissimilar computing devices such as Network Interface Cards (NICs), bridges and routers exchange data over a network by offering a networking framework for implementing protocols in seven layers. Beginning at the application layer, control is passed from one layer to the next. The following describes the seven layers as defined by the OSI model, shown in the order they occur whenever a user transmits information.

**Layer 7: Application**

This layer supports the application and end-user processes. Within this layer, user privacy is considered and communication partners, service and constraints are all identified. File transfers, email, Telnet and FTP applications are all provided within this layer.

**Layer 6: Presentation (Syntax)**

Within this layer, information is translated back and forth between application and network formats. This translation transforms the information into data the application layer and network recognize regardless of encryption and formatting.

**Layer 5: Session**

Within this layer, connections between applications are made, managed and terminated as needed to allow for data exchanges between applications at each end of a dialogue.

**Layer 4: Transport**

Complete data transfer is ensured as information is transferred transparently between systems in this layer. The transport layer also assures appropriate flow control and end-to-end error recovery.

**Layer 3: Network**

Using switching and routing technologies, this layer is responsible for creating virtual circuits to transmit information from node to node. Other functions include routing, forwarding, addressing, internetworking, error and congestion control, and packet sequencing.

**Layer 2: Data Link**

Information in data packets are encoded and decoded into bits within this layer. Errors from the physical layer flow control and frame synchronization are corrected here utilizing transmission protocol knowledge and management. This layer consists of two sub layers: the Media Access Control (MAC) layer, which controls the way networked computers gain access to data and transmit it, and the Logical Link Control (LLC) layer, which controls frame synchronization, flow control and error checking.

**Layer 1: Physical**

This layer enables hardware to send and receive data over a carrier such as cabling, a card or other physical means. It conveys the bitstream through the network at the electrical and mechanical level. Fast Ethernet, RS232, and ATM are all protocols with physical layer components.

This order is then reversed as information is received, so that the physical layer is the first and application layer is the final layer that information passes through.

## Standard Ethernet Code

In order to understand standard Ethernet code, one must understand what each digit means. Following is a guide:

## Media

An important part of designing and installing an Ethernet is selecting the appropriate Ethernet medium. There are four major types of media in use today: Thickwire for 10BASE5 networks; thin coax for 10BASE2 networks; unshielded twisted pair (UTP) for 10BASE-T networks; and fiber optic for 10BASE-FL or Fiber-Optic Inter-Repeater Link (FOIRL) networks. This wide variety of media reflects the evolution of Ethernet and also points to the technology's flexibility. Thickwire was one of the first cabling systems used in Ethernet, but it was expensive and difficult to use. This evolved to thin coax, which is easier to work with and less expensive. It is important to note that each type of Ethernet, Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet, has its own preferred media types.

The most popular wiring schemes are 10BASE-T and 100BASE-TX, which use unshielded twisted pair (UTP) cable. This is similar to telephone cable and comes in a variety of grades, with each higher grade offering better performance. Level 5 cable is the highest, most expensive grade, offering support for transmission rates of up to 100 Mbps. Level 4 and level 3 cable are less expensive, but cannot support the same data throughput speeds; level 4 cable can support speeds of up to 20 Mbps; level 3 up to 16 Mbps. The 100BASE-T4 standard allows for support of 100 Mbps Ethernet over level 3 cables, but at the expense of adding another pair of wires (4 pair instead of the 2 pair used for 10BASE-T). For most users, this is an awkward scheme and therefore 100BASE-T4 has seen little popularity. Level 2 and level 1 cables are not used in the design of 10BASE-T networks.

For specialized applications, fiber-optic, or 10BASE-FL, Ethernet segments are popular. Fiber-optic cable is more expensive, but it is invaluable in situations where electronic emissions and environmental hazards are a concern. Fiber-optic cable is often used in inter-building applications to insulate networking equipment from electrical damage caused by lightning. Because it does not conduct electricity, fiber-optic cable can also be useful in areas where heavy electromagnetic interference is present, such as on a factory floor. The Ethernet standard allows for fiber-optic cable segments up to two kilometers long, making fiber-optic

Ethernet perfect for connecting nodes and buildings that are otherwise not reachable with copper media.

**Cable Grade Capabilities**

| **Cable Name** | **Makeup** | **Frequency Support** | **Data Rate** | **Network Compatibility** |
|---|---|---|---|---|
| Cat-5 | 4 twisted pairs of copper wire -- terminated by RJ45 connectors | 100 MHz | Up to 1000Mbps | ATM, Token Ring,1000Base-T, 100Base-TX, 10Base-T |
| Cat-5e | 4 twisted pairs of copper wire -- terminated by RJ45 connectors | 100 MHz | Up to 1000Mbps | 10Base-T, 100Base-TX, 1000Base-T |
| Cat-6 | 4 twisted pairs of copper wire -- terminated by RJ45 connectors | 250 MHz | 1000Mbps | 10Base-T, 100Base-TX, 1000Base-T |

## Topologies

Network topology is the geometric arrangement of nodes and cable links in a LAN. Two general configurations are used, bus and star. These two topologies define how nodes are connected to one another in a communication network. A node is an active device connected to the network, such as a computer or a printer. A node can also be a piece of networking equipment such as a hub, switch or a router.

## LAN TOPOLOGY

Common LAN topologies are Bus, Ring and Star, Network requirements of these topologies are:

- Flexible to accommodate
  - Changes in physical location of the stations
  - Increase in number of stations.
  - Increase in LAN coverage.
- Consistent with the media access method
- Minimum cost of physical media.

**Bus Topology**

In bus topology, a single transmission medium interconnects all the stations (Fig.3.1) All stations share this medium for transmission to any other station. Every stations listens to all the transmissions on the bus. Every transmission has source and destination address so that stations can pick the messages meant for them and identify their senders.

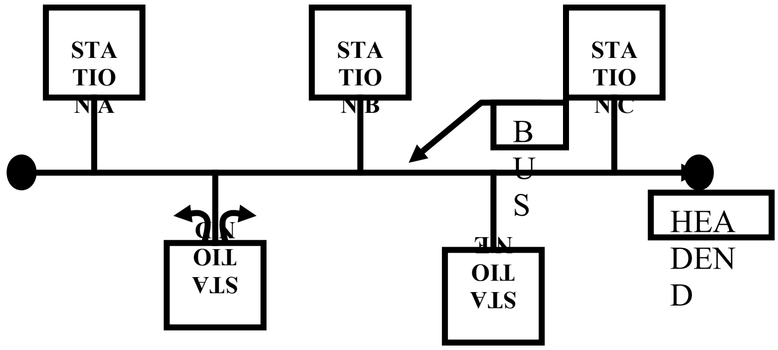
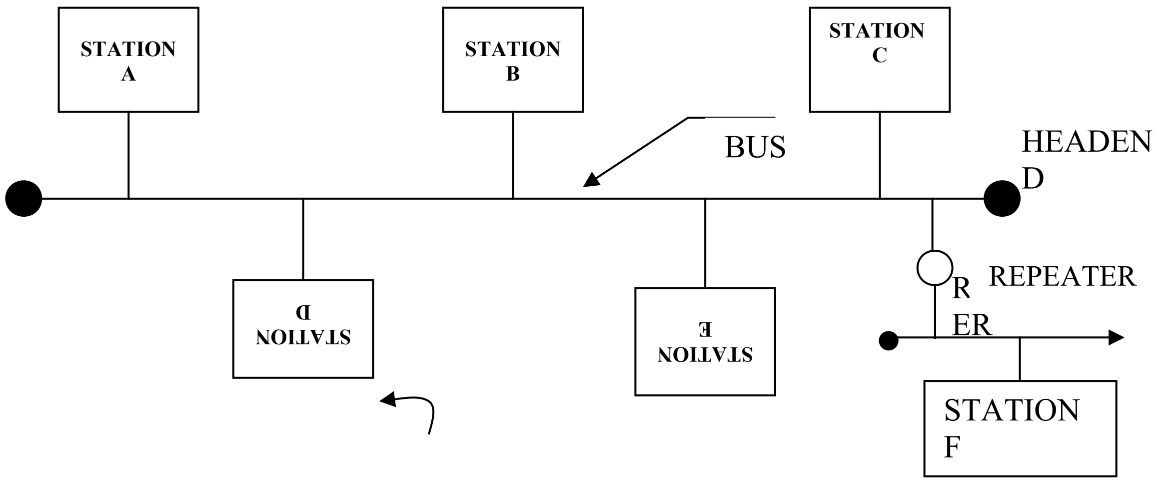



Fig.3.1 shows a two-way bus. Each station injects its signals on the bus, which flow in both the directions. To avoid signal reflection at the ends of the bus, the bus is terminated by appropriate impedance (characteristic impedance) called head end. Note that signal flow is bi-directional, therefore amplifiers can not be used to compensate for bus attenuation. Repeaters which interconnect two buses are used for extending the physical coverage of the network (fig. 3.2). A repeater is transparent to rest of the system in the sense that it does not have buffer and interconnects the two sections to make them virtually one section.




If signals are amplified along the bus, the bus becomes unidirectional. Therefore two separate channels are required. Every station injects signal on one bus and listens to the other bus. At one end of the LAN, the buses are looped. These two channels can be provided on a signal bus also using frequency division multiplexing. In this case. the head-end contains a frequency translator. Stations transmit on one frequency and listen to other frequency.

**Advantages of bus topology:**

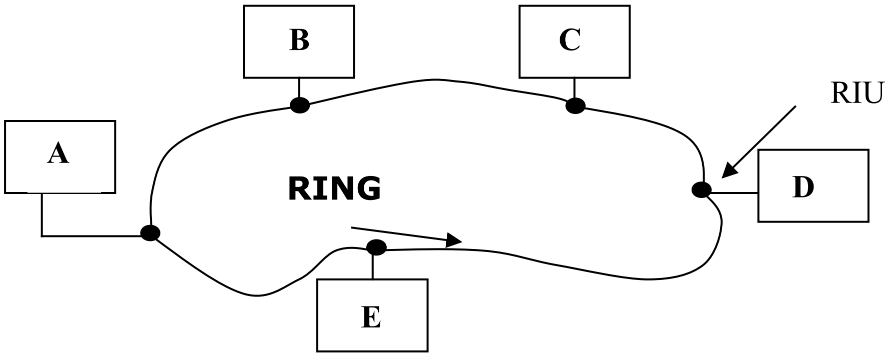
- Stations are connected to the bus using a passive tap.
- Least amount of media is used.
- Coverage can be increased by extending the bus using repeaters.
- New stations are easily added by tapping working bus.

**Disadvantages of bus topology :**

- Fault diagnostics is difficult
- Fault isolation is difficult
- Nodes must be intelligent

**Ring Topology**

A ring network consists of a number of transmission links joined together in form of a ring through repeaters called Ring interface Units (RIU). The transmission is usually unidirectional on the ring Thus each repeater receives the signals at its input and after regeneration, sends it to the repeater of the next station. If the frame belongs to the station, a copy of the incoming frame is retained. Each frame contains source and destination addresses. Fig. 3.3 shows a ring network.




Unlike a bus, signals on the ring never reach an end. They will keep circulating in the ring unless removed. This responsibility is usually given to the source because the destination may not be available. Possibility of source going down after transmitting a frame cannot be ruled out. Therefore a monitoring station is required to remove continuously circulating frames. Rings are not as flexible as bus because to add a station means breaking the ring and adding an RIU. Another possible problem can be an RIU may fail resulting in total network failure. A "Dead Man Relay" is usually provided to bypass a failed RIU. Wire centers are provided to improve flexibility of removing or adding a station and to isolate a faulty section To add a new station, cables are laid to the wire center. The bypass relays are also moved to the wire center. Wire centers can be connected together to increase geographic coverage of the network. A ring network does not economize on cables.

**Advantages of Ring topology:**

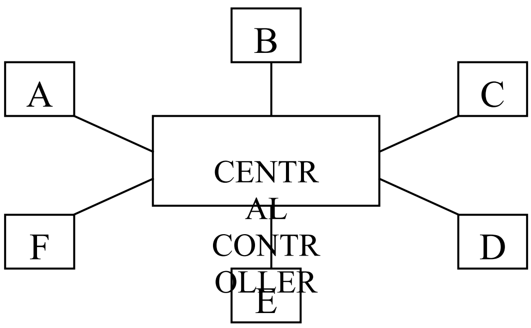
- Short cable length
- Suitable for optical fiber

**Disadvantages of Ring:**

- Node failure cause network failure
- Difficult to diagnose fault
- Network reconfiguration is difficult

**Star Topology**

A star network consists of dedicated links from the stations to the central controller (fig.3.4). Each interconnection supports two-way communication. The central controller acts as a switch to route the frames from source to the destination unlike ring or bus topologies where communication is in broadcast mode.



**Advantages of star topology:**

- Control/fault diagnostics is centralized.
- Simple access protocols are employed.
- Ease of service
- One device per connection

**Disadvantages of star topology:**

While star topology is well understood and is based on prove technology (telephone network), its disadvantages are

- Single point of failure.
- No sharing of transmission
- Long cable lengths involved
- Difficult to expand
- Central node dependency

## 3.1 TRANSMISSION MEDIA FOR LAN

In a local area network, stations are interconnected using transmission media which can be a twisted pair, cable or a coaxial cable or even an optical fiber cable, Choice of transmission media depends on several factors. While data rate and cost are prime considerations, physical and electrical characteristics of the media need also to be taken into account because they determine ease of installation, noise immunity, geographical coverage etc. In this chapter, popular physical transmission media are discussed. They are twisted pair, base-band and broadband coaxial cables and optical fibers. Their physical construction, characteristics and applicability to various medium access methods are described.

### 3.1.1 Considerations for Choice of Transmission Media

The following features of the transmission media must be taken into consideration while choosing suitable media for local area networks.

**Bandwidth**

Bandwidth of the transmission media determines the maximum data rates which can be handled by the media Data rates are, of course, determined by the stations but the transmission medium should not become bottleneck in achieving the required data rate it must be kept in mind that bandwidth of transmission media is function of the length of the media e.g. it may be possible to achieve very high data rates on a low cost twisted pair but then maximum length of one transmission segment is limited to not more than a few meters.

**Connectivity**

Some transmission media are suitable for broadcast mode of operation and point to multi-point links, while others are better suited for point to point links. For example, the present status of technology, Optical fiber is suited for point to point links only.

**Geographic Coverage**

In a LAN operating in broadcast mode on a bus, the electrical signals should reach from one end to the other without degradation in quality of the signals below the required limits. Attenuation and group delay characteristics of the medium determine overall distortion in the signals. These characteristics are function of distance and therefore determine the geographic coverage of the LAN. Propagation time, which is also dependent on the media characteristics, is an important consideration in that access mechanism where propagation delay determines the length of one segment of the media.

**Noise immunity**

Ideally the transmission media chosen for LAN should be free from interference from outside sources practically it is not possible. Degree of immunity to interference varies from media to media, Susceptibility to interference is because LAN cabling is usually done in the same ducts which carry power cables also. Degree of noise immunity required depends on environment where a LAN is installed.

**Security**

In some of the LAN topologies and access methods it is very easy to tap on the LAN & pick up the messages without generating any alarm. For considerations of data security, the transmission medium is to be so chosen that it may not be easily tapped.

**Cost.**

At present state of technology, cost of different media are different and are changing continuously. Metallic media is becoming costlier and optical fiber costs are going down. Cost of media is also related to the cost of equipment associated with the media. Therefore an overall view of cost structure is more important than media alone

In most of the instances, the LAN vendors specify the medium for which their products are designed. A look into the characteristics of media do help the user in becoming aware of the limitations of the transmission medium being supplied by the vendor. A comparison of various transmission media is given in Tables 1, 2 and 3 the end.

10BASE-T Ethernet and Fast Ethernet use a star topology where access is controlled by a central computer. Generally a computer is located at one end of the segment, and the other end is terminated in central location with a hub or a switch. Because UTP is often run in conjunction with telephone cabling, this central location can be a telephone closet or other area where it is convenient to connect the UTP segment to a backbone. The primary advantage of this type of network is reliability, for if one of these 'point-to-point' segments has a break; it will only affect the two nodes on that link. Other computer users on the network continue to operate as if that segment were non-existent.

## Collisions

Ethernet is a shared medium, so there are rules for sending packets of data to avoid conflicts and to protect data integrity. Nodes determine when the network is available for sending packets. It is possible that two or more nodes at different locations will attempt to send data at the same time. When this happens, a packet collision occurs.

Minimizing collisions is a crucial element in the design and operation of networks. Increased collisions are often the result of too many users on the network. This leads to competition for network bandwidth and can slow the performance of the network from the user's point of view. Segmenting the network is one way of reducing an overcrowded network, i.e., by dividing it into different pieces logically joined together with a bridge or switch.

**CSMA/CD**

In order to manage collisions Ethernet uses a protocol called Carrier Sense Multiple Access/Collision Detection (CSMA/CD). CSMA/CD is a type of contention protocol that defines how to respond when a collision is detected, or when two devices attempt to transmit packages simultaneously. Ethernet allows each device to send messages at any time without having to wait for network permission; thus, there is a high possibility that devices may try to send messages at the same time.

After detecting a collision, each device that was transmitting a packet delays a random amount of time before re-transmitting the packet. If another collision occurs, the device waits twice as long before trying to re-transmit.

# Ethernet Products

The standards and technology just discussed will help define the specific products that network managers use to build Ethernet networks. The following presents the key products needed to build an Ethernet LAN.

## Transceivers

Transceivers are also referred to as Medium Access Units (MAUs). They are used to connect nodes to the various Ethernet media. Most computers and network interface cards contain a built-in 10BASE-T or 10BASE2 transceiver which allows them to be connected directly to Ethernet without the need for an external transceiver.

Many Ethernet devices provide an attachment unit interface (AUI) connector to allow the user to connect to any type of medium via an external transceiver. The AUI connector consists of a 15-pin D-shell type connector, female on the computer side, male on the transceiver side.

For Fast Ethernet networks, a new interface called the MII (Media Independent Interface) was developed to offer a flexible way to support 100 Mbps connections. The MII is a popular way to connect 100BASE-FX links to copper-based Fast Ethernet devices.

## Network Interface Cards

Network Interface Cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus. Different computers have different bus architectures. PCI bus slots are most commonly found on 486/Pentium PCs and ISA expansion slots are commonly found on 386 and older PCs. NICs come in three basic varieties: 8-bit, 16-bit, and 32-bit. The larger the number of bits that can be transferred to the NIC, the faster the NIC can transfer data to the network cable. Most NICs are designed for a particular type of network, protocol, and medium, though some can serve multiple networks.

Many NIC adapters comply with plug-and-play specifications. On these systems, NICs are automatically configured without user intervention, while on non-plug-and-play systems, configuration is done manually through a set-up program and/or DIP switches.

Cards are available to support almost all networking standards. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate speed. Gigabit Ethernet NICs are 10/100/1000 capable with auto negotiation depending on the user’s Ethernet speed. Full duplex networking is another option where a dedicated connection to a switch allows a NIC to operate at twice the speed.

## Hubs/Repeaters

Hubs/repeaters are used to connect together two or more Ethernet segments of any type of medium. In larger designs, signal quality begins to deteriorate as segments exceed their maximum length. Hubs provide the signal amplification required to allow a segment to be extended a greater distance. A hub repeats any incoming signal to all ports.

Ethernet hubs are necessary in star topologies such as 10BASE-T. A multi-port twisted pair hub allows several point-to-point segments to be joined into one network. One end of the point-to-point link is attached to the hub and the other is attached to the computer. If the hub is attached to a backbone, then all computers at the end of the twisted pair segments can communicate with all the hosts on the backbone. The number and type of hubs in any one-collision domain is limited by the Ethernet rules. These repeater rules are discussed in more detail later.

A very important fact to note about hubs is that they only allow users to share Ethernet. A network of hubs/repeaters is termed a "shared Ethernet," meaning that all members of the network are contending for transmission of data onto a single network (collision domain). A hub/repeater propagates all electrical signals including the invalid ones. Therefore, if a collision or electrical interference occurs on one segment, repeaters make it appear on all others as well. This means that individual members of a shared network will only get a percentage of the available network bandwidth.

Basically, the number and type of hubs in any one collision domain for 10Mbps Ethernet is limited by the following rules:

| Network Type | Max Nodes Per Segment | Max Distance Per Segment |
|---|---|---|
| 10BASE-T | 2 | 100m |
| 10BASE-FL | 2 | 2000m |

# Bridges

Bridges connect two LAN segments of similar or dissimilar types, such as Ethernet and Token Ring. This allows two Ethernet segments to behave like a single Ethernet allowing any pair of computers on the extended Ethernet to communicate. Bridges are transparent therefore computers don't know whether a bridge separates them.

Bridges map the Ethernet addresses of the nodes residing on each network segment and allow only necessary traffic to pass through the bridge. When a packet is received by the bridge, the bridge determines the destination and source segments. If the segments are the same, the packet is dropped or also referred to as "filtered"; if the segments are different, then the packet is "forwarded" to the correct segment. Additionally, bridges do not forward bad or misaligned packets.

Bridges are also called "store-and-forward" devices because they look at the whole Ethernet packet before making filtering or forwarding decisions. Filtering packets and regenerating forwarded packets enables bridging technology to split a network into separate collision domains. Bridges are able to isolate network problems; if interference occurs on one of two segments, the bridge will receive and discard an invalid frame keeping the problem from affecting the other segment. This allows for greater distances and more repeaters to be used in the total network design.

### Dealing with Loops

Most bridges are self-learning task bridges; they determine the user Ethernet addresses on the segment by building a table as packets that are passed through the network. However, this self-learning capability dramatically raises the potential of network loops in networks that have many bridges. A loop presents conflicting information on which segment a specific address is located and forces the device to forward all traffic. The Distributed Spanning Tree (DST) algorithm is a software standard (found in the IEEE 802.1d specification) that describes how switches and bridges can communicate to avoid network loops.

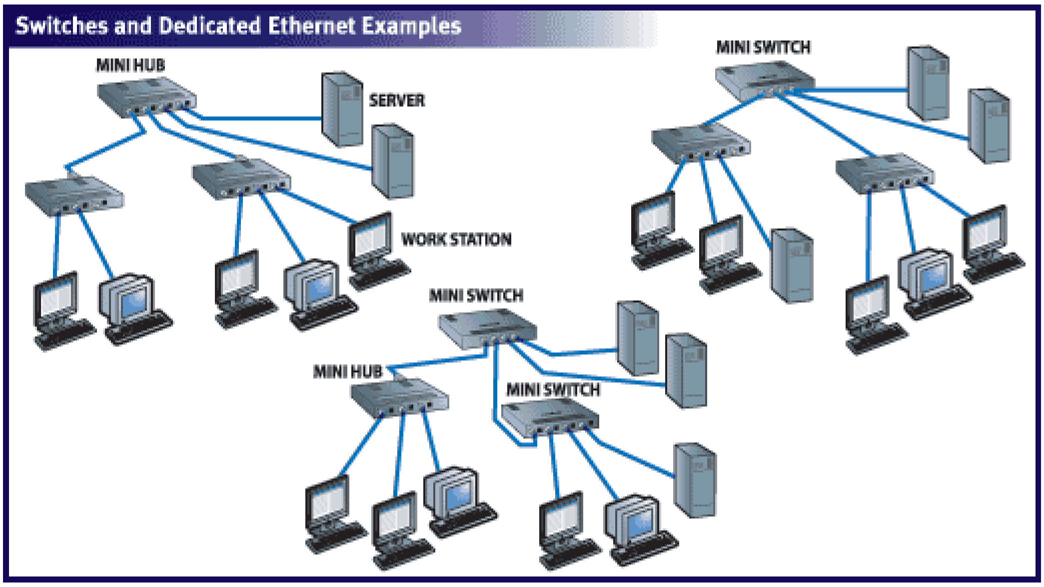
## Ethernet Switches

Ethernet switches are an expansion of the Ethernet bridging concept. The advantage of using a switched Ethernet is parallelism. Up to one-half of the computers connected to a switch can send data at the same time.

LAN switches link multiple networks together and have two basic architectures: cut-through and store-and-forward. In the past, cut-through switches were faster because they examined the packet destination address only before forwarding it on to its destination segment. A store-and-forward switch works like a bridge in that it accepts and analyzes the entire packet before forwarding it to its destination.

Historically, store-and-forward took more time to examine the entire packet, although one benefit was that it allowed the switch to catch certain packet errors and keep them from propagating through the network. Today, the speed of store-and-forward switches has caught up with cut-through switches so the difference between the two is minimal. Also, there are a large number of hybrid switches available that mix both cut-through and store-and-forward architectures.

Both cut-through and store-and-forward switches separate a network into collision domains, allowing network design rules to be extended. Each of the segments attached to an Ethernet switch has a full 10 Mbps of bandwidth shared by fewer users, which results in better performance (as opposed to hubs that only allow bandwidth sharing from a single Ethernet). Newer switches today offer high-speed links, either Fast Ethernet, Gigabit Ethernet, 10 Gigabit Ethernet or ATM. These are used to link switches together or give added bandwidth to high-traffic servers. A network composed of a number of switches linked together via uplinks is termed a "collapsed backbone" network.




# Routers

A router is a device that forwards data packets along networks, and determines which way to send each data packet based on its current understanding of the state of its connected networks. Routers are typically connected to at least two networks, commonly two LANs or WANs or a LAN and its Internet Service Provider's (ISPs) network. Routers are located at gateways, the places where two or more networks connect.

Routers filter out network traffic by specific protocol rather than by packet address. Routers also divide networks logically instead of physically. An IP router can divide a network into various subnets so that only traffic destined for particular IP addresses can pass between segments. Network speed often decreases due to this type of intelligent forwarding. Such filtering takes more time than that exercised in a switch or bridge, which only looks at the Ethernet address. However, in more complex networks, overall efficiency is improved by using routers.