What is a computer Network?

A network is any collection of independent computers that communicate with one another over a shared network medium. A computer network is a collection of two or more connected computers. When these computers are joined in a network, people can share files and peripherals such as modems, printers, tape backup drives, or CD-ROM drives. When networks at multiple locations are connected using services available from phone companies, people can send e-mail, share links to the global Internet, or conduct video conferences in real time with other remote users. When a network becomes open sourced it can be managed properly with online collaboration software. As companies rely on applications like electronic mail and database management for core business operations, computer networking becomes increasingly more important.

Every network includes:

- At least two computers Server or Client workstation.
- Networking Interface Card's (NIC)
- A connection medium, usually a wire or cable, although wireless communication between networked computers and peripherals is also possible.
- Network Operating system software, such as Microsoft Windows NT or 2000, Novell NetWare, Unix and Linux.

Types of Networks:

LANs (Local Area Networks)

A network is any collection of independent computers that communicate with one another over a shared network medium. LANs are networks usually confined to a geographic area, such as a single building or a college campus. LANs can be small, linking as few as three computers, but 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.

WANs (Wide Area Networks)

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

Internet

The Internet is a system of linked networks that are worldwide in scope and facilitate data communication services such as remote login, file transfer, electronic mail, the World Wide Web and newsgroups.

With the meteoric rise in demand for connectivity, the Internet has become a communications highway for millions of users. The Internet was initially restricted to military and academic institutions, but now it is a full-fledged conduit for any and all forms of information and commerce. Internet websites now provide personal, educational, political and economic resources to every corner of the planet.

Intranet

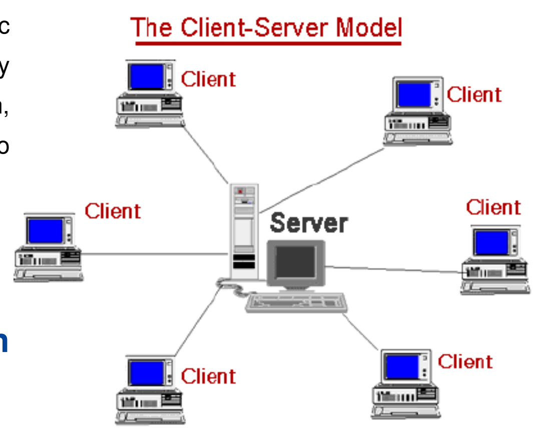
With the advancements made in browser-based software for the Internet, many private organizations are implementing intranets. An intranet is a private network utilizing Internet-type tools, but available only within that organization. For large organizations, an intranet provides an easy access mode to corporate information for employees.

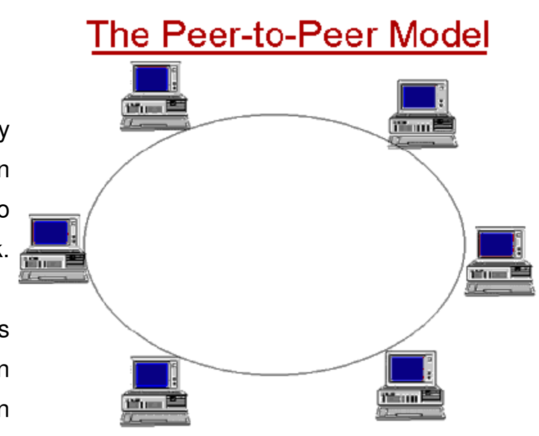
MANs (Metropolitan area Networks)

The refers to a network of computers with in a City.

VPN (Virtual Private Network)

VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access server on your workplace network. Using a VPN helps you save money by using the public Internet instead of making long–distance phone calls to connect securely with your private network. There are two ways to create a VPN connection, by dialing an Internet service provider (ISP), or connecting directly to Internet.





Categories of Network:

Network can be divided in to two main categories:

- Peer-to-peer.
- Server – based.

In peer-to-peer networking there are no dedicated servers or hierarchy among the computers. All of the computers are equal and therefore known as peers. Normally each computer serves as Client/Server and there is no one assigned to be an administrator responsible for the entire network.

Peer-to-peer networks are good choices for needs of small organizations where the users are allocated in the same general area, security is not an issue and the organization and the network will have limited growth within the foreseeable future.

The term Client/server refers to the concept of sharing the work involved in processing data between the client computer and the most powerful server computer.

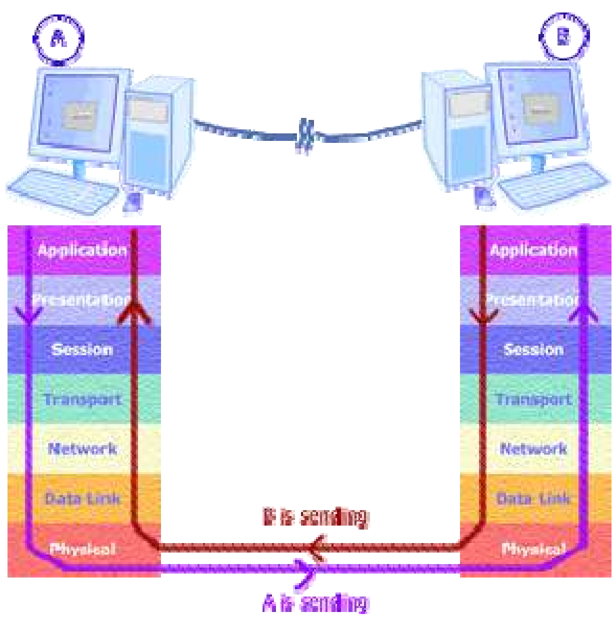
The client/server network is the most efficient way to provide:

- Databases and management of applications such as Spreadsheets, Accounting, Communications and Document management.
- Network management.
- Centralized file storage.

The client/server model is basically an implementation of distributed or cooperative processing. At the heart of the model is the concept of splitting application functions between a client and a server processor. The division of labor between the different processors enables the application designer to place an application function on the processor that is most appropriate for that function. This lets the software designer optimize the use of processors--providing the greatest possible return on investment for the hardware.

Client/server application design also lets the application provider mask the actual location of application function. The user often does not know where a specific operation is executing. The entire function may execute in either the PC or server, or the function may be split between them. This masking of application function locations enables system implementers to upgrade portions of a system over time with a minimum disruption of application operations, while protecting the investment in existing hardware and software.

The OSI Model:



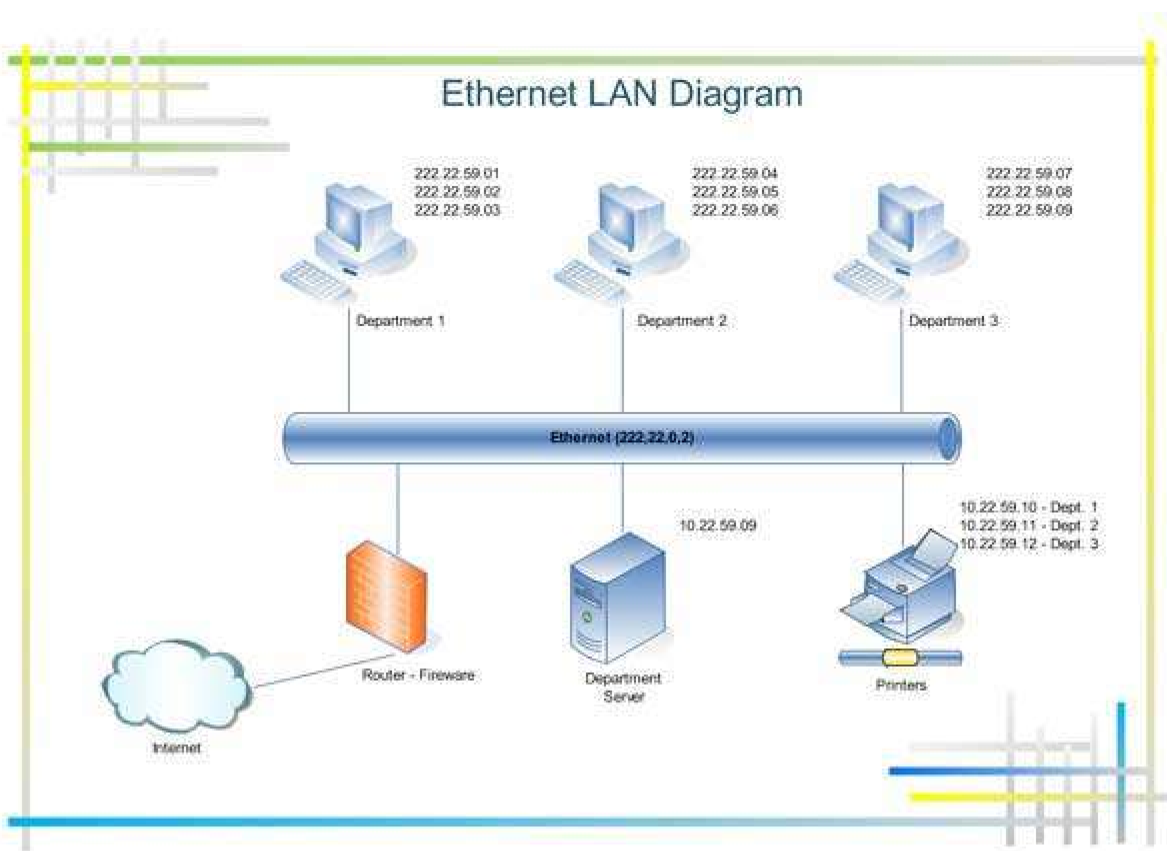
Open System Interconnection (OSI) reference model has become an International standard and serves as a guide for networking. This model is the best known and most widely used guide to describe networking environments. Vendors design network products based on the specifications of the OSI model. It provides a description of how network hardware and software work together in a layered fashion to make communications possible. It also helps with trouble shooting by providing a frame of reference that describes how components are supposed to function.

There are seven to get familiar with and these are the physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and the application layer.

- Physical Layer, is just that the physical parts of the network such as wires, cables, and there media along with the length. Also this layer takes note of the electrical signals that transmit data throughout system.
- Data Link Layer, this layer is where we actually assign meaning to the electrical signals in the network. The layer also determines the size and format of data sent to printers, and other devices. Also I don't want to forget that these are also called nodes in the network. Another thing to consider in this layer is will also allow and define the error detection and correction schemes that insure data was sent and received.
- Network Layer, this layer provides the definition for the connection of two dissimilar networks.
- Transport Layer, this layer allows data to be broken into smaller packages for data to be distributed and addressed to other nodes (workstations).
- Session Layer, this layer helps out with the task to carry information from one node (workstation) to another node (workstation). A session has to be made before we can transport information to another computer.
- Presentation Layer, this layer is responsible to code and decode data sent to the node.
- Application Layer, this layer allows you to use an application that will communicate with say the operation system of a server. A good example would be using your web browser to interact with the operating system on a server such as Windows NT, which in turn gets the data you requested.

Network Architectures:

Ethernet

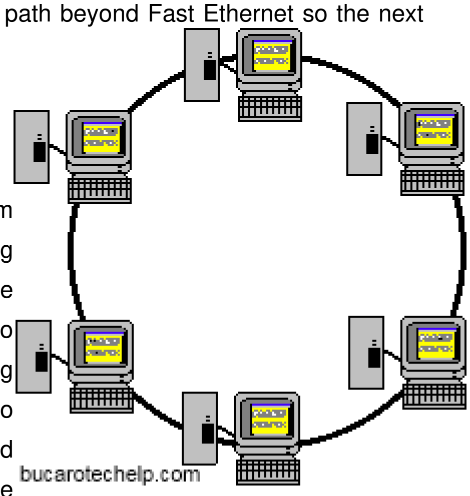


Ethernet is the most popular physical layer LAN technology in use today. Other LAN types include Token Ring, Fast Ethernet, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and LocalTalk. Ethernet is popular because it strikes a good balance between speed, cost and ease of installation. 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 (IEEE) defines the Ethernet standard as IEEE Standard 802.3. This standard defines rules for configuring an Ethernet network as well as specifying how elements in an Ethernet network interact with one another. By adhering to the IEEE standard, network equipment and network protocols can communicate efficiently.

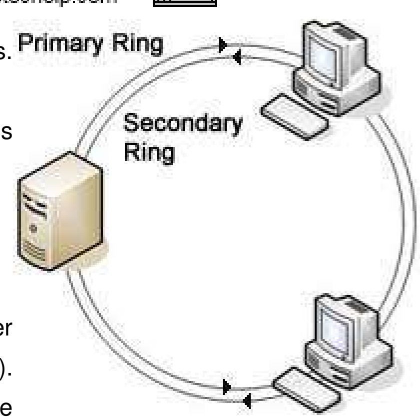
Fast Ethernet

For Ethernet networks that need higher transmission speeds, the Fast Ethernet standard (IEEE 802.3u) has been established. This standard raises the Ethernet speed limit from 10 Megabits per second (Mbps) to 100 Mbps with only minimal changes to the existing cable structure. 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. For the network manager, the incorporation of Fast Ethernet into an existing configuration presents a host of decisions. Managers must determine the number of users in each site on the network that need the higher throughput, decide which segments of the backbone need to be reconfigured specifically for 100BASE-T and then choose the necessary hardware 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.

Token Ring



Token Ring is another form of network configuration which differs from Ethernet in that all messages are transferred in a unidirectional manner along the ring at all times. Data is transmitted in tokens, which are passed along the ring and viewed by each device. When a device sees a message addressed to it, that device copies the message and then marks that message as being read. As the message makes its way along the ring, it eventually gets back to the sender who now notes that the message was received by the intended device. The sender can then remove the message and free that token for use by others.



Various PC vendors have been proponents of Token Ring networks at different times and thus these types of networks have been implemented in many organizations.

FDDI

FDDI (Fiber-Distributed Data Interface) is a standard for data transmission on fiber optic lines in a local area network that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users.

Protocols:

Network protocols are standards that allow computers to communicate. A protocol 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 handling lost or damaged transmissions or "packets." 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) are the main types of network protocols in use today.

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,"

Some Important Protocols and their job:

Protocol	**Acronym**	**Its Job**
Point-To-Point	TCP/IP	The backbone protocol of the internet. Popular also for intranets using the internet
Transmission Control Protocol/internet Protocol	TCP/IP	The backbone protocol of the internet. Popular also for intranets using the internet
Internetwork Package Exchange/Sequenced Packet Exchange	IPX/SPX	This is a standard protocol for Novell Network Operating System
NetBIOS Extended User Interface	NetBEUI	This is a Microsoft protocol that doesn't support routing to other networks
File Transfer Protocol	FTP	Used to send and receive files from a remote host
Hyper Text Transfer Protocol	HTTP	Used for the web to send documents that are encoded in HTML.
Network File Services	NFS	Allows network nodes or workstations to access files and drives as if they were their own.
Simple Mail Transfer Protocol	SMTP	Used to send Email over a

		network
Telnet		Used to connect to a host and emulate a terminal that the remote server can recognize

Introduction to TCP/IP Networks:

TCP/IP-based networks play an increasingly important role in computer networks. Perhaps one reason for their appeal is that they are based on an open specification that is not controlled by any vendor.

What Is TCP/IP?

TCP stands for Transmission Control Protocol and IP stands for Internet Protocol. The term TCP/IP is not limited just to these two protocols, however. Frequently, the term TCP/IP is used to refer to a group of protocols related to the TCP and IP protocols such as the User Datagram Protocol (UDP), File Transfer Protocol (FTP), Terminal Emulation Protocol (TELNET), and so on.

The Origins of TCP/IP

In the late 1960s, DARPA (the Defense Advanced Research Project Agency), in the United States, noticed that there was a rapid proliferation of computers in military communications. Computers, because they can be easily programmed, provide flexibility in achieving network functions that is not available with other types of communications equipment. The computers then used in military communications were manufactured by different vendors and were designed to interoperate with computers from that vendor only. Vendors used proprietary protocols in their communications equipment. The military had a multi vendor network but no common protocol to support the heterogeneous equipment from different vendors

Net work Cables and Stuff:

In the network you will commonly find three types of cables used these are the, coaxial cable, fiber optic and twisted pair.

Thick Coaxial Cable

This type cable is usually yellow in color and used in what is called thicknets, and has two conductors. This coax can be used in 500-meter lengths. The cable itself is made up of a solid center wire with a braided metal shield and plastic sheathing protecting the rest of the wire.

Thin Coaxial Cable

As with the thick coaxial cable is used in thicknets the thin version is used in thinnets. This type cable is also used called or referred to as RG-58. The cable is really just a cheaper version of the thick cable.

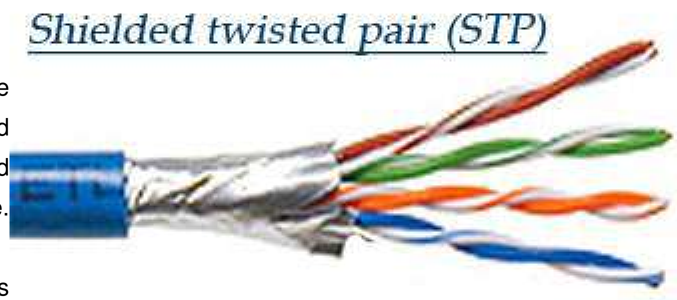
Fiber Optic Cable

As we all know fiber optics are pretty darn cool and not cheap. This cable is smaller and can carry a vast amount of information fast and over long distances.

Twisted Pair Cables

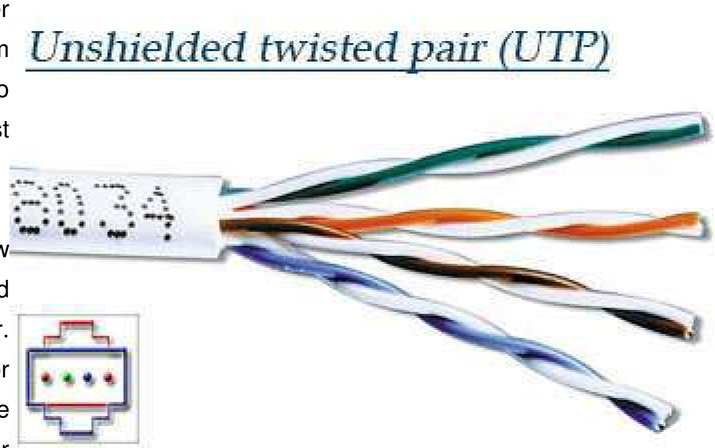
These come in two flavors of unshielded and shielded.

Shielded Twisted Pair (STP)



Is more common in high-speed networks. The biggest difference you will see in the UTP and STP is that the STP use's metallic shield wrapping to protect the wire from interference.

-Something else to note about these cables is that they are defined in numbers also. The bigger the number the better the protection from interference. Most networks should go with no less than a CAT 3 and CAT 5 is most recommended.



-Now you know about cables we need to know about connectors. This is pretty important and you will most likely need the RJ-45 connector. This is the cousin of the phone jack connector and looks real similar with the exception that the RJ-45 is bigger. Most commonly your connector are in two flavors and this is BNC (Bayonet Naur Connector) used in thicknets and the RJ-45 used in smaller networks using UTP/STP.

Unshielded Twisted Pair (UTP)

This is the most popular form of cables in the network and the cheapest form that you can go with. The UTP has four pairs of wires and all inside plastic sheathing. The biggest reason that we call it Twisted Pair is to protect the wires from interference from themselves. Each wire is only protected with a thin plastic sheath.

Ethernet Cabling

Now to familiarize you with more on the Ethernet and it's cabling we need to look at the 10's. 10Base2, is considered the thin Ethernet, thinnet, and thinwire which uses light coaxial cable to create a 10 Mbps network. The cable segments in this network can't be over 185 meters in length. These cables connect with the BNC connector. Also as a note these unused connection must have a terminator, which will be a 50-ohm terminator.

10Base5, this is considered a thicknet and is used with coaxial cable arrangement such as the BNC connector. The good side to the coaxial cable is the high-speed transfer and cable segments can be up to 500 meters between nodes/workstations. You will typically see the same speed as the 10Base2 but larger cable lengths for more versatility.

10BaseT, the “T” stands for twisted as in UTP (Unshielded Twisted Pair) and uses this for 10Mbps of transfer. The down side to this is you can only have cable lengths of 100 meters between nodes/workstations. The good side to this network is they are easy to set up and cheap! This is why they are so common an ideal for small offices or homes.

100BaseT, is considered Fast Ethernet uses STP (Shielded Twisted Pair) reaching data transfer of 100Mbps. This system is a little more expensive but still remains popular as the 10BaseT and cheaper than most other type networks. This on of course would be the cheap fast version.

10BaseF, this little guy has the advantage of fiber optics and the F stands for just that. This arrangement is a little more complicated and uses special connectors and NIC's along with hubs to create its network. Pretty darn neat and not to cheap on the wallet.

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 was expensive and difficult to use. This evolved to thin coax, which is easier to work with and less expensive.

Network Topologies:

What is a Network topology?

A network topology is the geometric arrangement of nodes and cable links in a LAN,

There are three topology's to think about when you get into networks. These are the star, rind, and the bus.

Star, in a star topology each node has a dedicated set of wires connecting it to a central network hub. Since all traffic passes through the hub, the hub becomes a central point for isolating network problems and gathering network statistics.

Ring, a ring topology features a logically closed loop. Data packets travel in a single direction around the ring from one network device to the next. Each network device acts as a repeater, meaning it regenerates the signal

Bus, the bus topology, each node (computer, server, peripheral etc.) attaches directly to a common cable. This topology most often serves as the backbone for a network. In some instances, such as in classrooms or labs, a bus will connect small workgroups

Collisions:

Ethernet is a shared media, so there are rules for sending packets of data to avoid conflicts and protect data integrity. Nodes determine when the network is available for sending packets. It is possible that two nodes at different locations attempt to send data at the same time. When both PCs are transferring a packet to the network at the same time, a collision will result.

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, which results in a lot of contention for network bandwidth. This can slow the performance of the network from the user's point of view. Segmenting the network, where a network is divided into different pieces joined together logically with a bridge or switch, is one way of reducing an overcrowded network.

Ethernet Products:

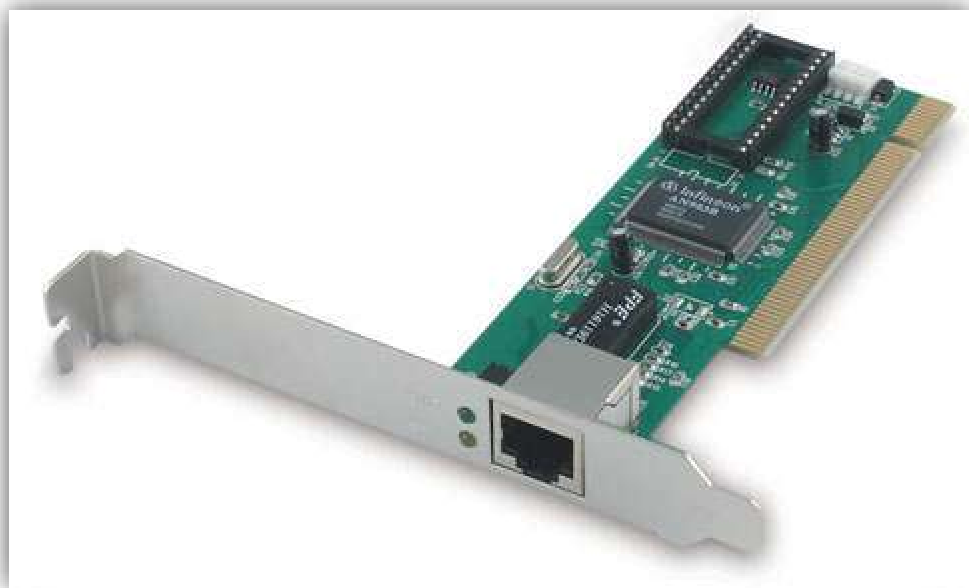
The standards and technology that have just been discussed help define the specific products that network managers use to build Ethernet networks. The following text discusses the key products needed to build an Ethernet LAN.

Transceivers

Transceivers 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, allowing them to be connected directly to Ethernet without requiring an external transceiver. Many Ethernet devices provide an AUI connector to allow the user to connect to any media type 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. Thickwire (10BASE5) cables also use transceivers to allow connections.

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, and 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 master 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.

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

Cards are available to support almost all networking standards, including the latest Fast Ethernet environment. Fast Ethernet NICs are often 10/100 capable, and will automatically set to the appropriate 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 media type. 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 takes any incoming signal and repeats it out 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.

Network Type	Max Nodes Per Segment	Max Distance Per Segment
10BASE-T	2	100m
10BASE2	30	185m
10BASE5	100	500m
10BASE-FL	2	2000m

Adding Speed:

While repeaters allow LANs to extend beyond normal distance limitations, they still limit the number of nodes that can be supported. Bridges and switches, however, allow LANs to grow significantly larger by virtue of their ability to support full Ethernet segments on each port. Additionally, bridges and switches selectively filter network traffic to only those packets needed on each segment - this significantly increases throughput on each segment and on the overall network. By providing better performance and more flexibility for network topologies, bridges and switches will continue to gain popularity among network managers.

Bridges:

The function of a bridge is to connect separate networks together. Bridges connect different networks types (such as Ethernet and Fast Ethernet) or networks of the same type. 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 ("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 enable bridging technology to split a network into separate collision domains. This allows for greater distances and more repeaters to be used in the total network design.

Ethernet Switches:

Ethernet switches are an expansion of the concept in Ethernet bridging. LAN switches can link four, six, ten or more 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, on the other hand, accepts and analyzes the entire packet before forwarding it to its destination.

It takes more time to examine the entire packet, but it allows the switch to catch certain packet errors and keep them from propagating through the network. 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, FDDI, Fast 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:

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.

What is a network firewall?

A firewall is a system or group of systems that enforces an access control policy between two networks. The actual means by which this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic. Probably the most important thing to recognize about a firewall is that it implements an access control policy. If you don't have a good idea of what kind of access you want to allow or to deny, a firewall really won't help you. It's also important to recognize that the firewall's configuration, because it is a mechanism for enforcing policy, imposes its policy on everything behind it. Administrators for firewalls managing the connectivity for a large number of hosts therefore have a heavy responsibility.

Network Design Criteria:

Ethernets and Fast Ethernets have design rules that must be followed in order to function correctly. Maximum number of nodes, number of repeaters and maximum segment distances are defined by the electrical and mechanical design properties of each type of Ethernet and Fast Ethernet media.

A network using repeaters, for instance, functions with the timing constraints of Ethernet. Although electrical signals on the Ethernet media travel near the speed of light, it still takes a finite time for the signal to travel from one end of a large Ethernet to another. The Ethernet standard assumes it will take roughly 50 microseconds for a signal to reach its destination.

Ethernet is subject to the "5-4-3" rule of repeater placement: the network can only have five segments connected; it can only use four repeaters; and of the five segments, only three can have users attached to them; the other two must be inter-repeater links.

If the design of the network violates these repeater and placement rules, then timing guidelines will not be met and the sending station will resend that packet. This can lead to lost packets and excessive resent packets, which can slow network performance and create trouble for applications. Fast Ethernet has modified repeater rules, since the minimum packet size takes less time to transmit than regular Ethernet. The length of the network links allows for a fewer number of repeaters. In Fast Ethernet networks, there are two classes of repeaters. Class I repeaters have a latency of 0.7 microseconds or less and are limited to one repeater per network. Class II repeaters have a latency of 0.46 microseconds or less and are limited to two repeaters per network. The following are the distance (diameter) characteristics for these types of Fast Ethernet repeater combinations:

Fast Ethernet	**Copper**	**Fiber**
No Repeaters	100m	412m*
One Class I Repeater	200m	272m
One Class II Repeater	200m	272m
Two Class II Repeaters	205m	228m

* Full Duplex Mode 2 km

When conditions require greater distances or an increase in the number of nodes/repeaters, then a bridge, router or switch can be used to connect multiple networks together. These devices join two or more separate networks, allowing network design criteria to be restored. Switches allow network designers to build large networks that function well. The reduction in costs of bridges and switches reduces the impact of repeater rules on network design.

Each network connected via one of these devices is referred to as a separate collision domain in the overall network.

Types of Servers:

Device Servers

A device server is defined as a specialized, network-based hardware device designed to perform a single or specialized set of server functions. It is characterized by a minimal operating architecture that requires no per seat network operating system license, and client access that is independent of any operating system or proprietary protocol. In addition the device server is a "closed box," delivering extreme ease of installation, minimal maintenance, and can be managed by the client remotely via a Web browser.

Print servers, terminal servers, remote access servers and network time servers are examples of device servers which are specialized for particular functions. Each of these types of servers has unique configuration attributes in hardware or software that help them to perform best in their particular arena.

Print Servers

Print servers allow printers to be shared by other users on the network. Supporting either parallel and/or serial interfaces, a print server accepts print jobs from any person on the network using supported protocols and manages those jobs on each appropriate printer.

Print servers generally do not contain a large amount of memory; printers simply store information in a queue. When the desired printer becomes available, they allow the host to transmit the data to the appropriate printer port on the server. The print server can then simply queue and print each job in the order in which print requests are received, regardless of protocol used or the size of the job.

Multiport Device Servers

Devices that are attached to a network through a multiport device server can be shared between terminals and hosts at both the local site and throughout the network. A single terminal may be connected to several hosts at the same time (in multiple concurrent sessions), and can switch between them. Multiport device servers are also used to network devices that have only serial outputs. A connection between serial ports on different servers is opened, allowing data to move between the two devices.

Given its natural translation ability, a multi-protocol multiport device server can perform conversions between the protocols it knows, like LAT and TCP/IP. While server bandwidth is not adequate for large file transfers, it can easily handle host-to-host inquiry/response applications, electronic mailbox checking, etc. And it is far more economical than the alternatives of acquiring expensive host software and special-purpose converters. Multiport device and print servers give their users greater flexibility in configuring and managing their networks.

Whether it is moving printers and other peripherals from one network to another, expanding the dimensions of interoperability or preparing for growth, multiport device servers can fulfill your needs, all without major rewiring.

Access Servers

While Ethernet is limited to a geographic area, remote users such as traveling sales people need access to network-based resources. Remote LAN access, or remote access, is a popular way to provide this connectivity. Access servers use telephone services to link a user or office with an office network. Dial-up remote access solutions such as ISDN or asynchronous dial introduce more flexibility. Dial-up remote access offers both the remote office and the remote user the economy and flexibility of "pay as you go" telephone services. ISDN is a special telephone service that offers three channels, two 64 Kbps "B" channels for user data and a "D" channel for setting up the connection. With ISDN, the B channels can be combined for double bandwidth or separated for different applications or users. With asynchronous remote access, regular telephone lines are combined with modems and remote access servers to allow users and networks to dial anywhere in the world and have data access. Remote access servers provide connection points for both dial-in and dial-out applications on the network to which they are attached. These hybrid devices route and filter protocols and offer other services such as modem pooling and terminal/printer services. For the remote PC user, one can connect from any available telephone jack (RJ45), including those in a hotel rooms or on most airplanes.

Network Time Servers

A network time server is a server specialized in the handling of timing information from sources such as satellites or radio broadcasts and is capable of providing this timing data to its attached network. Specialized protocols such as NTP or udp/time allow a time server to communicate to other network nodes ensuring that activities that must be coordinated according to their time of execution are synchronized correctly. GPS satellites are one source of information that can allow global installations to achieve constant timing.

IP Addressing:

An IP (Internet Protocol) address is a unique identifier for a node or host connection on an IP network. An IP address is a 32 bit binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points. This is known as "dotted decimal" notation.

Example: 140.179.220.200

It is sometimes useful to view the values in their binary form.

140 .179 .220 .200

10001100.10110011.11011100.11001000

Every IP address consists of two parts, one identifying the network and one identifying the node. The Class of the address and the subnet mask determine which part belongs to the network address and which part belongs to the node address.

Address Classes:

There are 5 different address classes. You can determine which class any IP address is in by examining the first 4 bits of the IP address.

Class A addresses begin with 0xxx, or 1 to 126 decimal.

Class B addresses begin with 10xx, or 128 to 191 decimal.

Class C addresses begin with 110x, or 192 to 223 decimal.

Class D addresses begin with 1110, or 224 to 239 decimal.

Class E addresses begin with 1111, or 240 to 254 decimal.

Addresses beginning with 01111111, or 127 decimal, are reserved for loopback and for internal testing on a local machine. [You can test this: you should always be able to ping 127.0.0.1, which points to yourself] Class D addresses are reserved for multicasting. Class E addresses are reserved for future use. They should not be used for host addresses.

Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the node (n).

Class A -- NNNNNNNN.nnnnnnnn.nnnnnnn.nnnnnnn

Class B -- NNNNNNNN.NNNNNNNN.nnnnnnnn.nnnnnnnn

Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN.nnnnnnnn

In the example, 140.179.220.200 is a Class B address so by default the Network part of the address (also known as the Network Address) is defined by the first two octets (140.179.x.x) and the node part is defined by the last 2 octets (x.x.220.200).

In order to specify the network address for a given IP address, the node section is set to all "0"s. In our example, 140.179.0.0 specifies the network address for 140.179.220.200. When the node section is set to all "1"s, it specifies a broadcast that is sent to all hosts on the network. 140.179.255.255 specifies the example broadcast address. Note that this is true regardless of the length of the node section.

Private Subnets:

There are three IP network addresses reserved for private networks. The addresses are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. They can be used by anyone setting up internal IP networks, such as a lab or home LAN behind a NAT or proxy server or a router. It is always safe to use these because routers on the Internet will never forward packets coming from these addresses

Subnetting an IP Network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN, etc.), preservation of address space, and security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Subnet Masking

Applying a subnet mask to an IP address allows you to identify the network and node parts of the address. The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s. Performing a bitwise logical AND operation between the IP address and the subnet mask results in the Network Address or Number.

For example, using our test IP address and the default Class B subnet mask, we get:

10001100.10110011.11110000.11001000 140.179.240.200 Class B IP Address

11111111.11111111.00000000.00000000 255.255.000.000 Default Class B Subnet Mask

10001100.10110011.00000000.00000000 140.179.000.000 Network Address

Default subnet masks:

Class A - 255.0.0.0 - 11111111.00000000.00000000.00000000

Class B - 255.255.0.0 - 11111111.11111111.00000000.00000000

Class C - 255.255.255.0 - 11111111.11111111.11111111.00000000

CIDR -- Classless InterDomain Routing.

CIDR was invented several years ago to keep the internet from running out of IP addresses. The "classful" system of allocating IP addresses can be very wasteful; anyone who could reasonably show a need for more that 254 host addresses was given a Class B address block of 65533 host addresses. Even more wasteful were companies and organizations that were allocated Class A address blocks, which contain over 16 Million host addresses! Only a tiny percentage of the allocated Class A and Class B address space has ever been actually assigned to a host computer on the Internet.

People realized that addresses could be conserved if the class system was eliminated. By accurately allocating only the amount of address space that was actually needed, the address space crisis could be avoided for many years. This was first proposed in 1992 as a scheme called Supernetting.

The use of a CIDR notated address is the same as for a Classful address. Classful addresses can easily be written in CIDR notation (Class A = /8, Class B = /16, and Class C = /24)

It is currently almost impossible for an individual or company to be allocated their own IP address blocks. You will simply be told to get them from your ISP. The reason for this is the ever-growing size of the internet routing table. Just 5 years ago, there were less than 5000 network routes in the entire Internet. Today, there are over 90,000. Using CIDR, the biggest ISPs are allocated large chunks of address space (usually with a subnet mask of /19 or even smaller); the ISP's customers (often other, smaller ISPs) are then allocated networks from the big ISP's pool. That way, all the big ISP's customers (and their customers, and so on) are accessible via 1 network route on the Internet.

It is expected that CIDR will keep the Internet happily in IP addresses for the next few years at least. After that, IPv6, with 128 bit addresses, will be needed. Under IPv6, even sloppy address allocation would comfortably allow a billion unique IP addresses for every person on earth

Examining your network with commands:

Ping

PING is used to check for a response from another computer on the network. It can tell you a great deal of information about the status of the network and the computers you are communicating with.

Ping returns different responses depending on the computer in question. The responses are similar depending on the options used.

Ping uses IP to request a response from the host. It does not use TCP

.It takes its name from a submarine sonar search - you send a short sound burst and listen for an echo - a ping - coming back.

In an IP network, `ping' sends a short data burst - a single packet - and listens for a single packet in reply. Since this tests the most basic function of an IP network (delivery of single packet), it's easy to see how you can learn a lot from some `pings'.

To stop ping, type control-c. This terminates the program and prints out a nice summary of the number of packets transmitted, the number received, and the percentage of packets lost, plus the minimum, average, and maximum round-trip times of the packets.

Sample ping session

PING localhost (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=7 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=8 ttl=255 time=2 ms
64 bytes from 127.0.0.1: icmp_seq=9 ttl=255 time=2 ms

localhost ping statistics

10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 2/2/2 ms
meikro$

The Time To Live (TTL) field can be interesting. The main purpose of this is so that a packet doesn't live forever on the network and will eventually die when it is deemed "lost." But for us, it provides additional information. We can use the TTL to determine approximately how many router hops the packet has gone through. In this case it's 255 minus N hops, where N is the TTL of the returning Echo Replies. If the TTL field varies in successive pings, it could indicate that the successive reply packets are going via different routes, which isn't a great thing.

The time field is an indication of the round-trip time to get a packet to the remote host. The reply is measured in milliseconds. In general, it's best if round-trip times are under 200 milliseconds. The time it takes a packet to reach its destination is called latency. If you see a large variance in the round-trip times (which is called "jitter"), you are going to see poor performance talking to the host

NSLOOKUP

NSLOOKUP is an application that facilitates looking up hostnames on the network. It can reveal the IP address of a host or, using the IP address, return the host name.

It is very important when troubleshooting problems on a network that you can verify the components of the networking process. Nslookup allows this by revealing details within the infrastructure.

NETSTAT

NETSTAT is used to look up the various active connections within a computer. It is helpful to understand what computers or networks you are connected to. This allows you to further investigate problems. One host may be responding well but another may be less responsive.

IPconfig

This is a Microsoft windows NT, 2000 command. It is very useful in determining what could be wrong with a network.

This command when used with the /all switch, reveal enormous amounts of troubleshooting information within the system.

Windows 2000 IP Configuration

Host Name . . . . : cowder
Primary DNS Suffix . . . . :
Node Type . . . . : Broadcast
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Connection-specific DNS Suffix . :
Description . . . . :
WAN (PPP/SLIP) Interface
Physical Address. . . . . : 00-53-45-00-00-00
DHCP Enabled. . . . . : No
IP Address. . . . . : 12.90.108.123
Subnet Mask . . . . : 255.255.255.255
Default Gateway . . . . : 12.90.108.125
DNS Servers . . . . : 12.102.244.2
204.127.129.2