IEEE 802 Series Specifications

The ISO Reference Model does not make explicit the actual specification of the 7 layers. The lower layers of the model have been "standardized" by organizations such as the Institute of Electrical and Electronic Engineers (IEEE) committee, which has published a series of specifications for the OSI layers 1 and 2 (Physical and Data Link).

These specs define the physical media popularly known as:

802.3	CSMA/CD (Ethernet)
802.4	Token Bus
802.5	Token Ring

Other IEEE Project Groups include:

802.0	Executive committee
802.1	Higher Layer Interfaces
802.2	Logical Link Control (LLC)
802.6	Metropolitan Area Network (MAN)
802.7	Broadband LAN
802.8	Fiber Optic LAN
802.9	Integrated Voice and Data LAN
802.10	Standards for Interoperable LAN Security
802.11	Wireless Networks
802.12	Demand Priority Access LAN, 100BaseVG-AnyLAN

Channel Access Methods

Once the cable is in place, you need specifications to define how systems will *talk* to each other.

There are three basic channel access methods:

Contention

Any network device may transmit whenever they want.

Protocol Example: CSMA

Carrier sense multiple Access

Contention

Polling

Polling

A primary or master device queries each of the other devices (referred to as secondaries) in a predetermined order. Secondaries can access the channel only after receiving a request from the primary. Polling is not commonly used in local area networks.

Protocol Example: SDLC

Synchronous Data link control

IP Addressing with Class Structure

1. Short for Internet Protocol address, an IP or IP address is an address of a computer or other network device on a network using TCP/IP. For example, the number "69.72.169.241" is an example of such an address. These addresses are similar to an addresses used on a house and is what allows data to reach the appropriate destination on a network and the Internet.
There are five classes of available IP ranges: Class A, Class B, Class C, Class D and Class E, while only A, B, and C are commonly used. Each class allows for a range of valid IP addresses. Below is a listing of these addresses.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved for future use, or Research and Development Purposes.

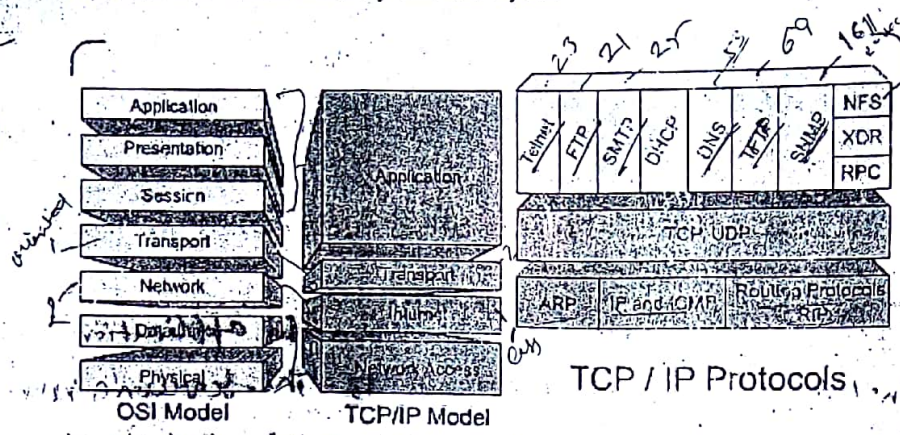
Automatically assigned addresses

There are several IP addresses that are automatically assigned when you setup a home network. These default addresses are what allow your computer and other network devices to communicate and broadcast information over your network. Below is the most commonly assigned network addresses in a home network.

192.168.1.0	0 is the automatically assigned network address.
192.168.1.1	1 is the commonly used address used as the gateway.
192.168.1.2	2 is also a commonly used address used for a gateway.
192.168.1.3 - 254	Addresses beyond 3 are assigned to computers and devices on the network.
192.168.1.255	255 is automatically assigned on most networks as the broadcast address.

If you have ever connected to your home network, you should be familiar with the gateway address or 192.168.1.1, which is the address you use to connect to your home network router and change its settings.

The Department of Defense created TCP/IP to ensure and preserve data integrity. This model is a condensed version of the OSI model and only has four layers.



Application Layer

This Layer
Defines protocols for node-to-node application communication and also controls user interface specifications. Consists of a set of services that provide ubiquitous access to all types of networks. Applications utilise the services to communicate with other devices and remote applications

Protocols and Applications

Port	Protocol	Discription
23	Telnet	Terminal Emulation (Telephone network)
21	FTP	ws file transfers between computers (File Transfer Protocol)
69	TFTP	Have to know what you want and where it is on the server, no directory browsing, no user authentication (Trivial File
2049	NFS	Allows remote file systems to be mounted as local (Network File System)
25	SMTP	Used to send mail between mail servers (Simple Mail Transfer Protocol)
515	LPD	Used for print sharing of network printers with TCP/IP (Line Printer Daemon)
161	SNMP	Collect and manipulates network information (Simple Network Management Protocol)
53	DNS	Resolves FQDN to IP addresses (Domain Name Service)
67	BootP	Used by diskless workstations to receive boot file and other information via TFTP
	DHCP	Assigns IP addresses to hosts from a pool. Can send IP address, Subnet mask, Domain Name, Default Gateway, DNS IP, WINS info. (Dynamic Host Configuration Protocol)

Transport Layer

http://www.dnicormick.org/tcpip.htm

TCP/IP Model
3/11/2008
Application layer
define Protocol for node to node application communication and User Provide user interface
Transport layer :- build above layer from sending packet
Provide end to end connection. Provide acknowledgment, sequencing, checksum, flow control
Provide TCP & UDP protocol
Internet layer Provide routing function IP also provide network interface to the upper layer
Network Access layer :- It monitor the data exchange between the host and the network

This layer shields the upper layers from the process of sending data. Also provides an end-to-end connection between two devices during communication by performing sequencing, acknowledgments, checksums, and flow control. Applications using services at this layer can use two different protocols: TCP and UDP.

Protocols at the Treansport Layer are:

TCP (Transmission Control Protocol)
TCP provides a connection-oriented, reliable services to the applications that use its services.

Main Functions of TCP

Segments application layer data stream--

TCP accepts data from applications and segments it into a desirable size for transmission between itself and the remote devices. The segment size is determined while TCP is negotiating the connection between the two devices. Either device can dictate the segment size.

Provides acknowledgment times--

TCP maintains timers to identify when packets have taken too long to get to their destination. When an acknowledgment is not received for a packet and the timer expires, TCP will resend the packet to the destination.

Enables sequence number checking--

TCP/IP uses sequence numbers to ensure that all packets sent by an application on one device are read in the correct order by an application on another device. The packets might not be received at the transport layer in the correct order, but TCP sequences them in their original order before passing them to the application layer.

Provides buffer management--

Any time two devices are communicating, the possibility exists that one device can send data faster than the other can accept it. If this happens, the receiving device puts the extra packets into a buffer to be read at the first chance it gets. When this data overflow persists, however, the buffer is eventually filled and packets begin to drop. TCP performs some preventive maintenance called flow control to avoid the problem.

Initiates connections with 3-way handshake--

TCP uses the concept of the three-way handshake to initiate a connection between two devices. A TCP connection begins with a device sending a request to synchronize sequence numbers (a SYN packet) and initiate a connection. The other device receives the message and responds with a SYN message and the sequence number increased by one. The first device responds by sending an acknowledgment message (an ACK) to the second device, indicating that the device received the sequence number it expected.

Performs error and duplication checking--

TCP uses a checksum to identify packets that have changed during transport. If a device receives a packet with a bad checksum, it drops the packet and does not send an acknowledgment for the packet. So the sending device will resend the packet. Any time TCP receives a duplicate packet it will drop the duplicate.

Any time a TCP device sends data to another device, it must wait for the acknowledgment that this data was received. To increase the bandwidth utilization, TCP can change the window size. Whatever the window size is negotiated to be, acknowledgments will only be sent after that many packets have been received at the receiving device. TCP sets the window size dynamically during a connection, allowing either device involved in the communication to slow down the sending data rate based on the other devices capacity. This process is known as sliding window because of TCP's ability to change the window size dynamically.

TCP Overview

Before data is sent, the transmitting host contacts the receiving host to set up a connection known as a virtual circuit. This makes TCP connection-oriented. During the handshake the two hosts agree upon the amount of information to be sent before an acknowledgment is needed (Windowing). TCP takes the large blocks of data from the upper layers and breaks them up into segments that it numbers and sequences. TCP will the pass the segments to the network layer, which will route them through the Internetwork. The receiving TCP can put the segments back into order. After packets are sent, TCP waits for an acknowledgment from the receiving end of the virtual circuit. If no acknowledgment is received then the sending host will retransmit the segment.

TCP Header Information			
Source Port Number 16 bits (Number of calling port)			Destination Port Number 16 bits (Number of called port)
Sequence Number 32 bits **(Number to ensure proper sequence of data.)**			
Acknowledgment Number 32-bits **(Identifies next segment expected)**			
Header Length 4 bits **(Number of 32 bit words in header)**	Reserved 6 bits **(Always 0)**	Code bits 6 bits **(Identifies type of segment, setup/termination of session)**	Window size 16 bits **(Number of octets the device is willing to accept)**
TCP Checksum 16 bits **(Used to ensure data integrity)**			Urgent Pointer 16 bits **(Indicates end of urgent data)**
Options 0 or 32 bits **(Identifies maximum segment size)**			
Data			

UDP (User Datagram Protocol)

UDP transports information that doesn't require reliable delivery; therefore it can have less overhead than TCP as no sequencing or acknowledgments are used. NFS and SNMP use UDP for their sessions, the applications have their own methods to ensure reliability. UDP receives blocks of information from the upper layers, which it breaks into segments. It gives each segment a number, sends it, and then forgets about it. No acknowledgments, no virtual circuits, connectionless protocol.

UDP Header Format

The UDP is the simplest of the two standard TCP/IP transport protocol. It is an end-to-end transport level protocol that add 3/11/2008 only source port address, checksum error control, and length information for the data from the upper layer. The packet produced by UDP is called a user datagram. A brief description of its fields is in order—

→ Source port address - is the address of the application program that has created the message.

→ Destination port address:- is the address of the application program that will receive the message.

→ Total length:- This field defines the total length of the user datagram in byte.

→ Checksum:- is a 16 bit field used in error detection.

Source Port Number 16 bits (Number of calling port)	Destination Port Number 16 bits (Number of called port)
UDP Length 16 bits (Length of UDP in bytes)	UDP Checksum 16 bits (Used to ensure data integrity)
8 byte (variable size) Header	Data

Differences between TCP and UDP

TCP	UDP
Sequenced	Unsequenced
Reliable -sequence numbers, acknowledgments, and 3-way handshake	Unreliable -best effort only
Connection Oriented	Connectionless
Virtual Circuits	Low Overhead
Checksum for Error Checking	Checksum for Error Checking
Uses buffer management to avoid overflow, uses sliding window to maximize bandwidth efficiency	No flow control
Assigns datagram size dynamically for efficiency	Every datagram segment is the same size

TCP and UDP Port Numbers

TCP and UDP use port numbers to communicate with the upper layers. Port numbers keep track of different sessions across the network. The source port will be above 1024 (unprivileged). 1023 and below (privileged) are known as well known ports and are assigned to common protocols. TCP and upper layer don't use hardware (MAC) and logical (IP) addresses to see the host's address; instead they use port numbers.

Internet Layer

The Internet Layer exists for routing and providing a single network interface to the upper layers. IP provides the single network interface for the upper layers.

Protocols at the Internet Layer are:

IP (Internet Protocol)

The Internet Protocol (IP) is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams through an internetwork; and providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit (MTU) sizes.

All machines on a TCP/IP network have a unique logical address, an IP address. The Internet Layer (IP) has a complete picture of the entire network and is responsible for path determination and packet switching. IP is the transport for TCP, UDP, and ICMP and provides an unreliable service. It lets the upper layer protocols that use it worry about reliability. IP will perform as a connectionless service because it handles each datagram as an independent entity. IP performs packet switching and path determination by maintaining

tables that indicate where to send a packet based on its IP address. IP gets the destination address from the packet. IP receives segments from the Host-to-Host layer and fragments them into packets. IP will then reassemble the packets into segments on the receiving end to send to the Host-to-Host layer. Each packet has the source and destination IP address. Each router will make path determinations based on the destination IP address.

ICMP (Internet Control Message Protocol)

The Internet Control Message Protocol (ICMP) is a network-layer Internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. ICMP utilizes IP to carry the ICMP data within it through a network.

ICMP Messages

ICMPs generate several kinds of useful messages, including Destination Unreachable, Echo Request and Reply, Redirect, Time Exceeded, and Router Advertisement and Router Solicitation. If an ICMP message cannot be delivered, no second one is generated. This is to avoid an endless flood of ICMP messages.

When an ICMP destination-unreachable message is sent by a router, it means that the router is unable to send the package to its final destination. The router then discards the original packet. Destination-unreachable messages include four basic types: network unreachable, host unreachable, protocol unreachable, and port unreachable.

Network-unreachable messages usually mean that a failure has occurred in the routing or addressing of a packet.
Host-unreachable messages usually indicates delivery failure, such as a wrong subnet mask.
Protocol-unreachable messages generally mean that the destination does not support the upper-layer protocol specified in the packet.
Port-unreachable messages imply that the TCP socket or port is not available.
An ICMP echo-request message, which is generated by the ping command, is sent by any host to test node reachability across an internetwork. The ICMP echo-reply message indicates that the node can be successfully reached. PING - Packet Internet Gropher, uses echo message to test physical connectivity.

An ICMP Redirect message is sent by the router to the source host to stimulate more efficient routing. The router still forwards the original packet to the destination. ICMP redirects allow host routing tables to remain small because it is necessary to know the address of only one router, even if that router does not provide the best path. Even after receiving an ICMP Redirect message, some devices might continue using the less-efficient route.

An ICMP Time-exceeded message is sent by the router if an IP packet's Time-to-Live field (expressed in hops or seconds) reaches zero. The Time-to-Live field prevents packets from continuously circulating the internetwork if the internetwork contains a routing loop. Routers discard packets that have reached their maximum hop count and tell the source machine that the packet is expired. Traceroute - uses ICMP timeouts to find the path a packet takes through the internetwork.

ARP (Address Resolution Protocol)

Used to find the MAC address from the known IP address. ARP sends a broadcast asking for the machine with the specified IP address to respond with its MAC address. If two devices want to communicate, the first device can send a broadcast ARP message requesting the physical address for a specified IP address. The receiving device responds with its IP address and the first device maintains the entry in its ARP cache. If a device doesn't exist on the same subnet, the sending device addresses the the default gateway's physical address and sends the packet to the default gateway.

RARP Reverse Address Resolution Protocol)

This protocol is used to find an IP address when the MAC address is known. A machine sends a broadcast with its MAC address and requests its IP address. An example of a device that uses RARP is a diskless workstation. Since it can't store its logical network address, it sends its MAC address to a RARP server to requests its IP address. A RARP server responds to the RARP request with the device's IP address.

Network Access Layer

The Network Access Layer monitors the data exchange between the host and the network. Oversees MAC addressing and defines protocols for the physical transmission of data.

Close browser

Wi-Fi Network

Definition: Wi-Fi is a wireless networking protocol that allows devices to communicate without internet cords. It's technically an industry term that represents a type of wireless local area network (LAN) protocol based on the 802.11 IEEE network standard.

Wi-Fi is the most popular means of communicating data wirelessly, within a fixed location. It's a trademark of the Wi-Fi Alliance, an international association of companies involved with wireless LAN technologies and products.

Note: Wi-Fi is commonly mistaken as an acronym for "wireless fidelity." It's also sometimes spelled as wifi, Wifi, WIFI or WiFi, but none of these are officially approved by the Wi-Fi Alliance. Wi-Fi is also used synonymously with the word "wireless," but wireless is actually much broader.

Wi-Fi Example and How It Works

The easiest way to understand Wi-Fi is to consider an average home or business since most of them support Wi-Fi access. The main requirement for Wi-Fi is that there's a device that can transmit the wireless signal, like a router, phone or computer.

In a typical home, a router transmits an internet connection coming from outside the network, like an ISP, and delivers that service to nearby devices that can reach the wireless signal. Another way to use Wi-Fi is a Wi-Fi hotspot so that a phone or computer can share its wireless or wired internet connection, similar to how a router works.

No matter how the Wi-Fi is being used or what its source of connection is, the result is always the same: a wireless signal that lets other devices connect to the main transmitter for communication, like to transfer files or carry voice messages.

Wi-Fi, from the user's perspective, is just internet access from a wireless capable device like a phone, tablet or laptop. Most modern devices support Wi-Fi so that it can access a network to get internet access and share network resources.

Is Wi-Fi Always Free?

There are tons of places to get free Wi-Fi access, like in restaurants and hotels, but Wi-Fi isn't free just because it's Wi-Fi. What determines the cost is whether or not the service has a data cap.

For Wi-Fi to work, the device transmitting the signal has to have an internet connection, which is not free. For example, if you have the internet at your house, you're probably paying a monthly a fee to keep it coming. If you use Wi-Fi so that your iPad and Smart TV can connect to the internet, those devices don't have to pay for the internet individually but the incoming line to the home still costs regardless of whether or not Wi-Fi is used.

However, most home internet connections don't have data caps, which is why it's not a problem to download hundred of gigabytes of data each month. However, phones usually do have data caps, which is why Wi-Fi hotspots are something to look for and use when you can.

If your phone can only use 10 GB of data in a month and you have a Wi-Fi hotspot set up, while it's true that other devices can connect to your phone and use the internet as much as they want, the data cap is still set at 10 GB and it applies to any data moving through the main device. In that case, anything over 10 GB used between the Wi-Fi devices will push the plan over its limit and accrue extra fees.

Use a free Wi-Fi hotspot locator to find free Wi-Fi access around your location.

Setting up Wi-Fi Access

If you're wanting to set up your own Wi-Fi at home, you need a wireless router and access to the router's admin management pages to configure the right settings like the Wi-Fi channel, password, network name, etc.

It's usually pretty simple to configure a wireless device to connect to a Wi-Fi network. The steps include ensuring that the Wi-Fi connection is enabled and then searching for a nearby network to provide the proper SSID and password to make the connection.

Some devices don't have a wireless adapter built-in, in which case you can buy your own Wi-Fi USB adapter.

You can also share your internet connection with other devices to create a wireless hotspot from your computer. The same can be done from mobile devices, such as with the Hotspotio Android app.

Bluetooth

Bluetooth is, with the infrared, one of the major wireless technologies developed to achieve WPAN. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on.

• Bluetooth project was started by SIG (Special Interest Group) formed by four companies IBM, Intel, Nokia and Toshiba for interconnecting computing and communicating devices using short-range, lower-power, inexpensive wireless radios.

• The project was named Bluetooth after the name of Viking king – Harald Blaatand who unified Denmark and Norway in 10th century.

• Nowadays, Bluetooth technology is used for several computer and non computer application:

1. It is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.

2. It is used by modern healthcare devices to send signals to monitors.

3. It is used by modern communicating devices like mobile phone, PDAs, palmtops etc to transfer data rapidly.

4. It is used for dial up networking. Thus allowing a notebook computer to call via a mobile phone.

5. It is used for cordless telephoning to connect a handset and its local base station.

6. It also allows hands-free voice communication with headset.

7. It also enables a mobile computer to connect to a fixed LAN.

Formatted: Font: 16 pt, Bold

Formatted: Font: 14 pt

Formatted: Font: 14 pt

Formatted: Font: 14 pt

Formatted: Font: 14 pt

8. It can also be used for file transfer operations from one mobile phone to another.

9. Bluetoothusesomnidirectionalradio waves that can through wallsor othernon-metalbarriers.

Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.

Bluetooth is that when the device is with in the scope of a other devices automatically start the transfer information without the user noticing. a small network between the devices is created and the user can accessed as if there were cables.

Formatted: Font: 14 pt

Formatted: Font: 14 pt

Bluetooth Architecture

Bluetooth architecture defines two types of networks:

1. Piconet

2. Scattemet

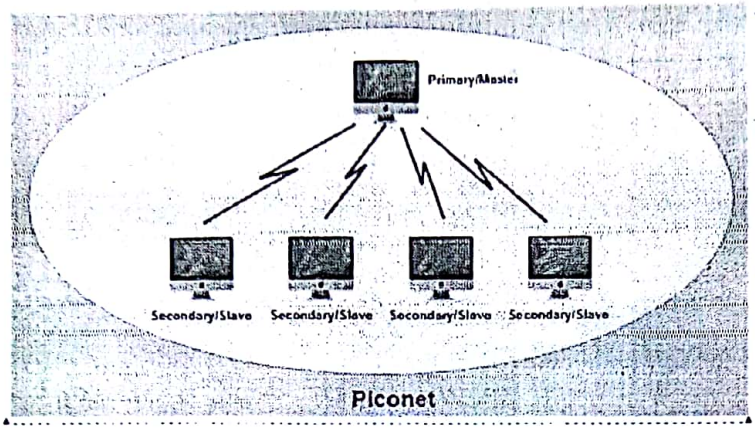
1. Piconet

• Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.

• Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.

• There can be only one primary or master station in each piconet.

• The communication between the primary and the secondary can be one-to-one or one-to-many.



Formatted: Justified

Formatted: Font: 14 pt, Font color: Auto

Formatted: Font: 14 pt

• All communication is between master and a slave. Salve-slave communication is not possible.

• In addition to seven active slave station, a piconet can have upto 255 parked nodes. These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.

2. Scatternet

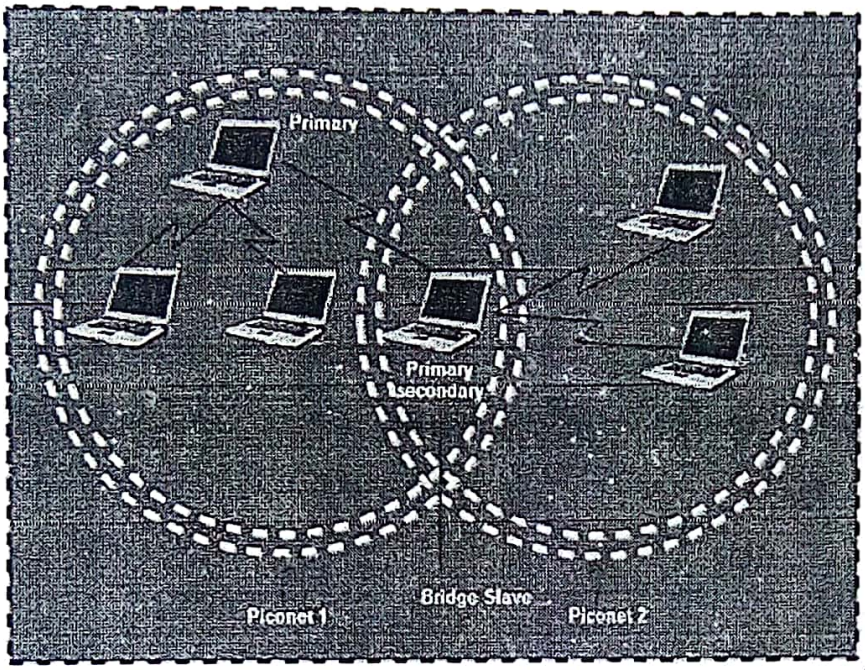
• Scattemet is formed by combining various piconets.

• A slave in one piconet can act as a master or primary in other piconet.

• Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.

• Thus a station can be a member of two piconets.

• A station cannot be a master in two piconets.



Formatted: Font: 14 pt

Formatted: Font: 14 pt

DHCP

You will likely find it more convenient to use Dynamic Host Configuration Protocol (DHCP) to manage IP addressing parameters for the majority of your network stations. With DHCP, a system is issued an address for a specified period of time. Before this lease period expires, the system will attempt to renew for the same period. If the system does not attempt to renew its lease, the DHCP server assumes that the IP address is available for reassignment to another system.

DHCP is especially well suited to PC-based network environments, given the inherently mobile nature of PCs. Even for a desktop system, it is not that difficult to move the machine to another office. This could mean that the machine has moved to a different subnetwork, which would require assignment of a new IP address. Manual address assignment and tracking could quickly become tedious.

Not all systems can be configured as DHCP clients, however. Machines that need a static, known address, must be configured manually. These include:

- DHCP servers
- WINS servers
- DNS servers
- Gateways (routers)

This is not a complete list of all machines and situations that may require a static IP address.

Domain Name System (DNS)

The Domain Name System, or DNS, allows users to access information across UNIX-based systems, the Internet, and intranet. Administrators can easily configure and manage name-to-IP address mapping by using a graphical administration tool. Before the GUI utility, administrators would manually edit an ASCII file named HOSTS to resolve IP addresses. The HOSTS file is an ASCII text file that is created to allow a host to query and resolve an IP to a domain name for routing information. HOSTS files were designed for use before DNS server became an alternative name resolver and for non-standard systems. This was tedious and error prone. A DNS name server is a subtree of a DNS database that is administered as a single separate entity, also called a zone. A zone can consist of a single domain or a domain with subdomains. One or more name servers can be set up for the zone. While troubleshooting name resolution, if you are able to ping an IP address but not a domain name, check your DNS server configuration or HOSTS file.

SLIP

- Established protocol
- Requires minimal overhead
- No compression
- No error checking or flow control
- No security provided by the protocol
- Supports TCP/IP only

Once considered the de facto standard for serial (dial-up) connections, SLIP has lost popularity in recent years.

PPP

- Newer protocol
- Requires a small amount of overhead, even less than SLIP
- Supports compression
- Error checking and flow control are provided
- Security supports the use of encrypted passwords
- Supports TCP/IP, NWLink (IPX/SPX), and NetBIOS
- Supported by DHCP

PPTP

- Provides secure client connections over the Internet
- Supports multiprotocol virtual private networks (VPNs)
- Allows Packet filtering
- Works with any protocol, including IP, IPX, and NetBEUI
- Supports RAS over switched connections or virtual WANS
- Supports the outsourcing of a dial-up network

Your protocol selections will be determined by application requirements and client capabilities.

FTP

The File Transfer Protocol (FTP) is a standard network protocol used for the transfer of computer files between a client and server on a computer network.

FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.[1] FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). SSH File Transfer Protocol (SFTP) is sometimes also used instead; it is technologically different.

The first FTP client applications were command-line programs developed before operating systems had graphical user interfaces, and are still shipped with most Windows, Unix, and Linux operating systems.[2][3] Many FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware, and FTP has been incorporated into productivity applications, such as web page editors.

Telnet

Telnet is a protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 854, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards. The name stands for "teletype network".

Historically, Telnet provided access to a command-line interface (usually, of an operating system) on a remote host, including most network equipment and operating systems with a configuration utility (including systems based on Windows NT). However, because of serious security concerns when using Telnet

over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH.

The term telnet is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. Telnet is also used as a verb. To telnet means to establish a connection using the Telnet protocol, either with command line client or with a programmatic interface. For example, a common directive might be: "To change your password, telnet into the server, log in and run the passwd command." Most often, a user will be telnetting to a Unix-like server system or a network device (such as a router) and obtaining a login prompt to a command line text interface or a character-based full-screen manager.

E-mail Protocols are set of rules that help the client to properly transmit the information to or from the mail server. Here in this tutorial, we will discuss various protocols such as **SMTP, POP,** and **IMAP.**

SMTP

SMTP stands for **Simple Mail Transfer Protocol.** It was first proposed in 1982. It is a standard protocol used for sending e-mail efficiently and reliably over the internet.

Key Points:

- SMTP is application level protocol.
- SMTP is connection oriented protocol.
- SMTP is text based protocol.
- It handles exchange of messages between e-mail servers over TCP/IP network.
- Apart from transferring e-mail, SMPT also provides notification regarding incoming mail.
- When you send e-mail, your e-mail client sends it to your e-mail server which further contacts the recipient mail server using SMTP client.
- These SMTP commands specify the sender's and receiver's e-mail address, along with the message to be send.
- The exchange of commands between servers is carried out without intervention of any user.
- In case, message cannot be delivered, an error report is sent to the sender which makes SMTP a reliable protocol.

SMTP Commands

The following table describes some of the SMTP commands:

S.N.	Command Description
1	**HELLO** This command initiates the SMTP conversation.
2	**EHELLO** This is an alternative command to initiate the conversation. ESMTP indicates that the sender server wants to use extended SMTP protocol.
3	**MAIL FROM** This indicates the sender's address.
4	**RCPT TO** It identifies the recipient of the mail. In order to deliver similar message to multiple users this command can be repeated multiple times.
5	**SIZE** This command let the server know the size of attached message in bytes.
6	**DATA** The **DATA** command signifies that a stream of data will follow. Here stream of data refers to the body of the message.
7	**QUIT** This commands is used to terminate the SMTP connection.
8	**VERFY** This command is used by the receiving server in order to verify whether the given username is valid or not.
9	**EXPN** It is same as VRFY, except it will list all the users name when it used with a distribution list.

IMAP

IMAP stands for **Internet Mail Access Protocol.** It was first proposed in 1986. There exist five versions of IMAP as follows:

1. Original IMAP
2. IMAP2
3. IMAP3
4. IMAP2bis
5. IMAP4

Key Points:

- IMAP allows the client program to manipulate the e-mail message on the server without downloading them on the local computer.
- The e-mail is hold and maintained by the remote server.
- It enables us to take any action such as downloading, delete the mail without reading the mail.It enables us to create, manipulate and delete remote message folders called mail boxes.
- IMAP enables the users to search the e-mails.
- It allows concurrent access to multiple mailboxes on multiple mail servers.

IMAP Commands

The following table describes some of the IMAP commands:

S.N.	Command Description
1	**IMAP_LOGIN** This command opens the connection.
2	**CAPABILITY** This command requests for listing the capabilities that the server supports.
3	**NOOP** This command is used as a periodic poll for new messages or message status updates during a period of inactivity.
4	**SELECT** This command helps to select a mailbox to access the messages.
5	**EXAMINE** It is same as SELECT command except no change to the mailbox is permitted.
6	**CREATE** It is used to create mailbox with a specified name.
7	**DELETE** It is used to permanently delete a mailbox with a given name.
8	**RENAME** It is used to change the name of a mailbox.
9	**LOGOUT** This command informs the server that client is done with the session. The server must send BYE untagged response before the OK response and then close the network connection.

POP

POP stands for Post Office Protocol. It is generally used to support a single client. There are several versions of POP but the POP 3 is the current standard.

Key Points

- POP is an application layer internet standard protocol.

- Since POP supports offline access to the messages, thus requires less internet usage time.
- POP does not allow search facility.
- In order to access the messaged, it is necessary to download them.
- It allows only one mailbox to be created on server.
- It is not suitable for accessing non mail data.
- POP commands are generally abbreviated into codes of three or four letters. Eg. STAT.

POP Commands

The following table describes some of the POP commands:

S.N.	Command Description
1	**LOGIN** This command opens the connection.
2	**STAT** It is used to display number of messages currently in the mailbox.
3	**LIST** It is used to get the summary of messages where each message summary is shown.
4	**RETR** This command helps to select a mailbox to access the messages.
5	**DELE** It is used to delete a message.
6	**RSET** It is used to reset the session to its initial state.
7	**QUIT** It is used to log off the session.

Comparison between POP and IMAP

S.N.	POP	IMAP
1	Generally used to support single client.	Designed to handle multiple clients.
2	Messages are accessed offline.	Messages are accessed online although it also supports offline mode.
3	POP does not allow search facility.	It offers ability to search emails.
4	All the messages have to be downloaded.	It allows selective transfer of messages to the client.
5	Only one mailbox can be created on the server.	Multiple mailboxes can be created on the server.
6	Not suitable for accessing non-mail data.	Suitable for accessing non-mail data i.e. attachment.
7	POP commands are generally abbreviated into	IMAP commands are not abbreviated, they

	codes of three or four letters. Eg. STAT.	are full. Eg. STATUS.
8	It requires minimum use of server resources.	Clients are totally dependent on server.
9	Mails once downloaded cannot be accessed from some other location.	Allows mails to be accessed from multiple locations.
10	The e-mails are not downloaded automatically.	Users can view the headings and sender of e-mails and then decide to download.
10	POP requires less internet usage time.	IMAP requires more internet usage time.

SMNP

Networks have a bad habit of failing. This makes network management an extremely important task. Because protocols (such as TCP) will correct lost or damaged frames, intermittent hardware or software failures can be difficult to detect. While the system may continue to operate despite failures, performance can suffer.

Most networks are heterogeneous, composed of equipment from many different vendors. A network management system has to be standardized and supported by a wide variety of equipment to be useful. The Simple Network Management Protocol is a system for communicating with network components that is useful in locating network problems. SNMP is an application layer protocol. It uses the well-known client server model although it calls the clients "managers" and the servers are "agents". SNMP data travels the network just like any other user data. The Internet Protocol does not have any network management functionality built into it.

All sorts of network components (such as hubs, switches, routers, repeaters and bridges) support SNMP agents. These programs maintain a set of variables (called objects) that describe the status of the device. The agents are programmed to record interesting values and counters in these variables. Some variables might count the number of incorrect CRCs received or the number of packets sent.

SNMP uses a fetch-store paradigm. Management software on a host computer can fetch statistical counters from managed devices. Management software can reset the counters by storing a zero in the object. Storing values in certain objects can direct the device to take certain actions, such as disable a line or reboot.

In order to receive an SNMP message, which is sent using the Internet Protocol, a device must have a hardware address and an Internet address. This is normal for devices such as gateways and routers, but throughout the semester we have stated

that repeaters and bridges do not have Internet addresses. In actuality, managed devices have IP addresses for the sole purpose of network management. Messages sent to the IP address of a bridge are intended for the bridge SNMP agent and are not intended to be sent to another network segment.

Data items are encoded according to the Abstract Syntax Notation.1 (ASN.1) standard.

The collection of all data objects that an SNMP manager can access is known as a Management Information Base. SNMP does not define the database. It only defines the message format and how messages are encoded. ASN.1 defines long hierarchical names for the data objects which are translated to a more compact numeric representation for transmission.

Introduction

During this chapter we will look at various communications devices. Our investigation of these devices will include both what they do and examples of situations where they are used.

These devices include:

- Repeaters
- Bridges
- Routers
- Brouters
- Gateways

Each device plays an important role in network management.

Internet Devices

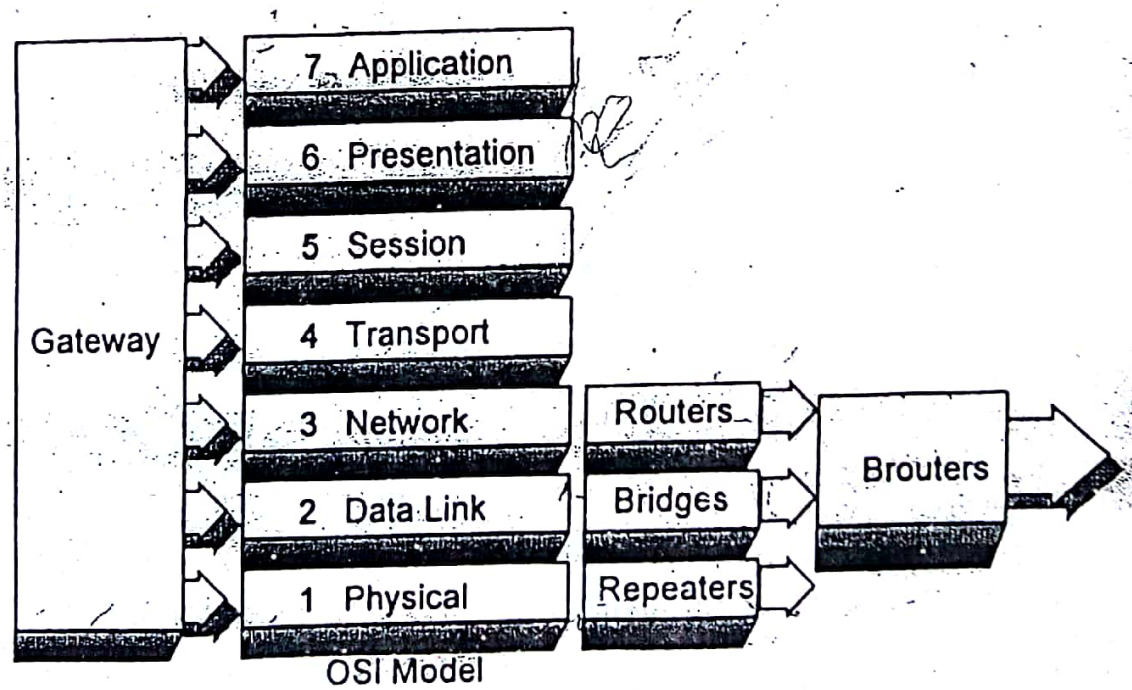
There are four different types of devices typically used to form internetworks:

- Repeaters
- Bridges
- Routers
- Gateways

On a technical level, these devices are distinguished by the OSI level at which they function:

Gateways	Level 1-7	All Layers
Routers	Level 3	Network
Bridges	Level 2	Data Link
Repeaters	Level 1	Physical

Another device, known as a Brouter, combines the characteristics of a Bridge and a Router.



Switch

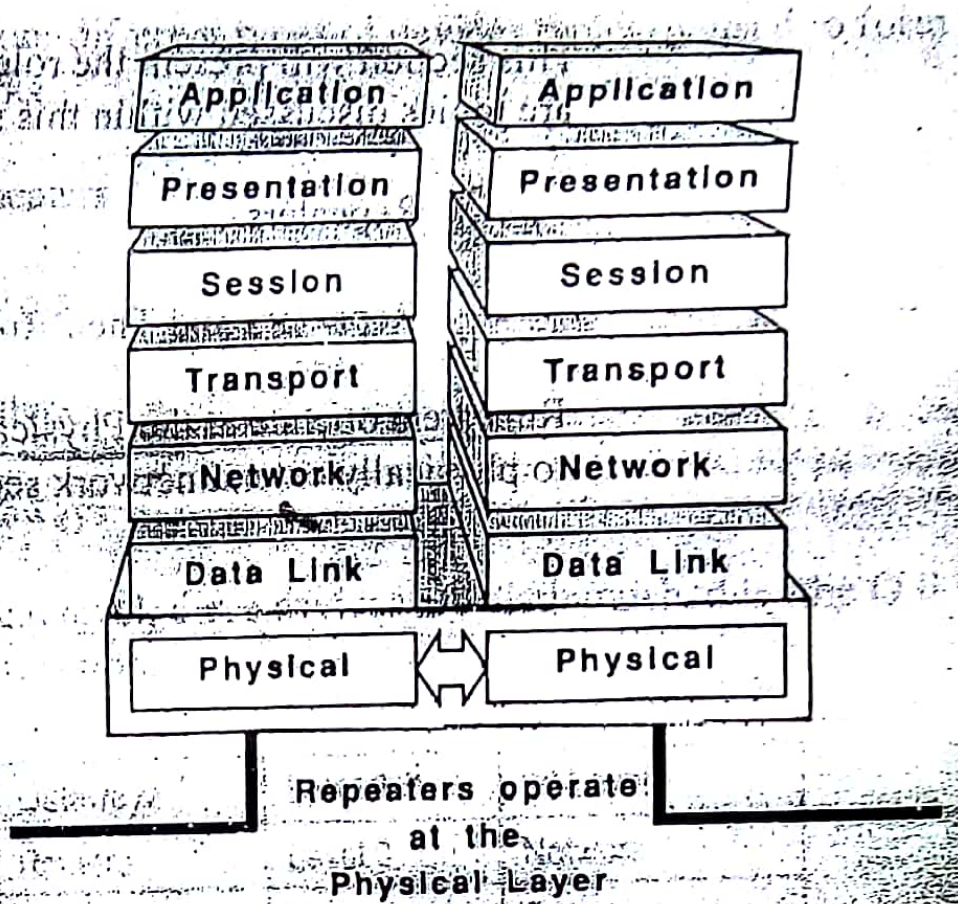
A **network switch** (also called **switching hub**, **bridging hub**, officially **MAC bridge**) is a computer networking device that connects devices together on a computer network by using packet switching to receive, process, and forward data to the destination device.

A network switch is a multiport network bridge that uses hardware addresses to process and forward data at the data link layer (layer 2) of the OSI model. Some switches can also process data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.

Switches for Ethernet are the most common form of network switch. The first Ethernet switch was introduced by Kalpana in 1990.[3] Switches also exist for other types of networks including Fibre Channel, Asynchronous Transfer Mode, and InfiniBand.

Unlike less advanced repeater hubs, which broadcast the same data out of each of its ports and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.

Repeaters



In simple terms, a repeater amplifies the electronic signal from one network cable segment and passes it to another. As an amplifier, a repeater connects network segments of similar media. It is not sensitive higher-layer protocol attributes since it simply takes a signal from one and amplifies it on the other side.

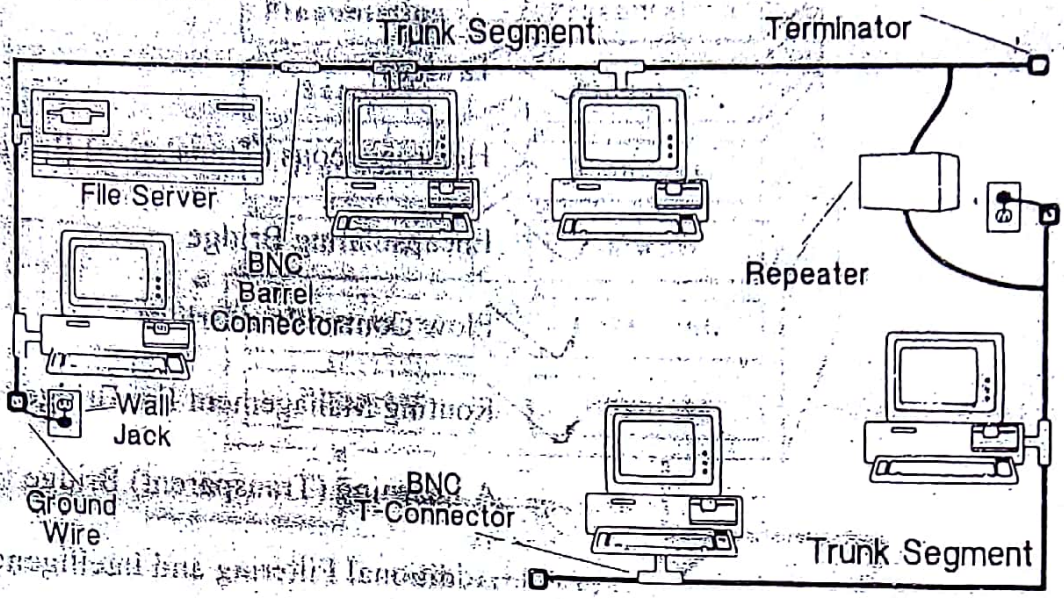
In addition to amplifying the signal, a repeater also amplifies noise result, there will be a limit to the number of repeaters that may be given network segment.

"Intelligent" repeaters regenerate the digital signal and are immune limitations of increasing attenuation over distance.

Repeaters extend Baseband networks that use one signal. Broadband networks support multiple signal transmissions simultaneously example of cable TV. Broadbase networks use amplifiers to extend signal transmissions.

Repeaters and Their Role

The earliest functional role of repeaters was to simply extend the physical length of a LAN. This is still one of the primary benefits of a repeater.



There are, however, several potential problem areas that are not addressed by repeaters. These include:

- Signal quality

  Most repeaters do nothing to filter noise out of the line, so it is amplified and sent on with the signal.

- Time delays

  Time delays can occur as signals are generated over greater distances. These delays may eventually generate timeout errors, which keeps repeaters from being used for remote links.

- Network traffic

  Because they do not have any capacity for filtering traffic, repeaters do nothing to reduce the network traffic load.

- Node limitations

  Repeaters are "invisible" to access protocols. All nodes added through a repeater count toward the total that can be supported in a subnet.

Repeaters are typically used on bus networks. To get the best signal quality, place a repeater so that the two segments connected are approximately the same length.

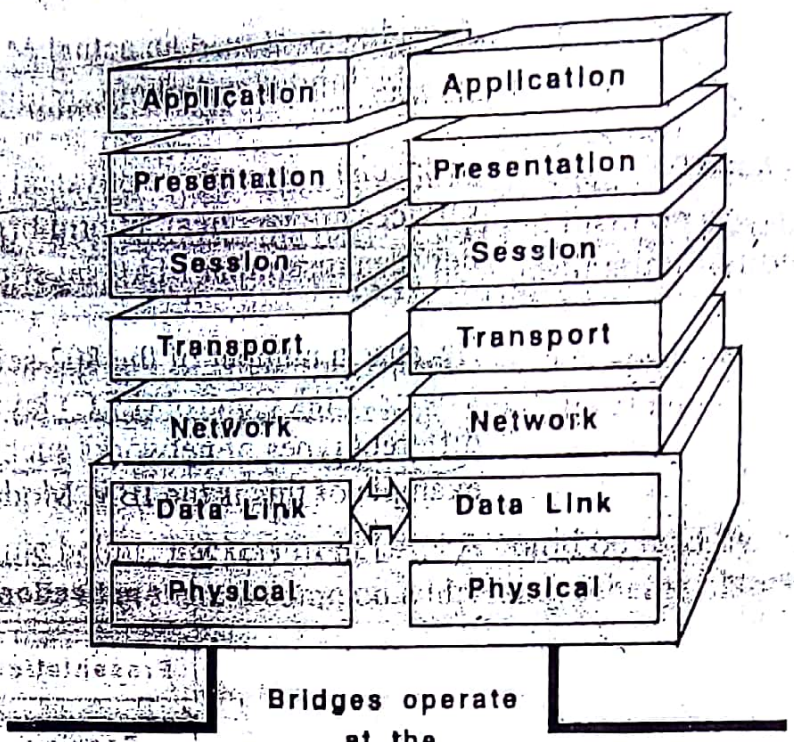
Introduction to Bridges

This section introduces bridges. This includes a look at bridge functions and available options when implementing bridges. The following are topics discussed within this section:

- Bridges
- Heterogeneous (Translating) Bridges
- Encapsulating Bridge
- Flow Control In a Bridge
- Routing Management For Bridges
- A Learning (Transparent) Bridge
- Additional Filtering and Intelligence
- Local and Remote Bridges
- Data Switches

It is important that you understand each of the network connection devi including bridges, to be able to select the correct device to meet you network requirements. Bridges provide a way of segmenting network traffic and connecting different LAN types.

Bridges



Bridges are more intelligent than repeaters. They can read the specific physical address of devices on one network and filter information before passing it on to another network segment.

Bridges operate at the Data Link layer, or more precisely, at the Media Access Control (MAC) sublayer. They go beyond simply amplifying the signal and are able to regenerate the signal. Rather than passing on line noise, a clean signal is sent out. This allows bridges to expand a network beyond what is normally allowed with repeaters.

In general, bridges:

- Are transparent to higher-level protocols.

  Segments connected through a bridge remain part of the same logical network.

- Can filter traffic based on addresses.

  This allows a bridge to reduce traffic between segments. This feature can also be used to improve security by selecting the packets that can be passed.

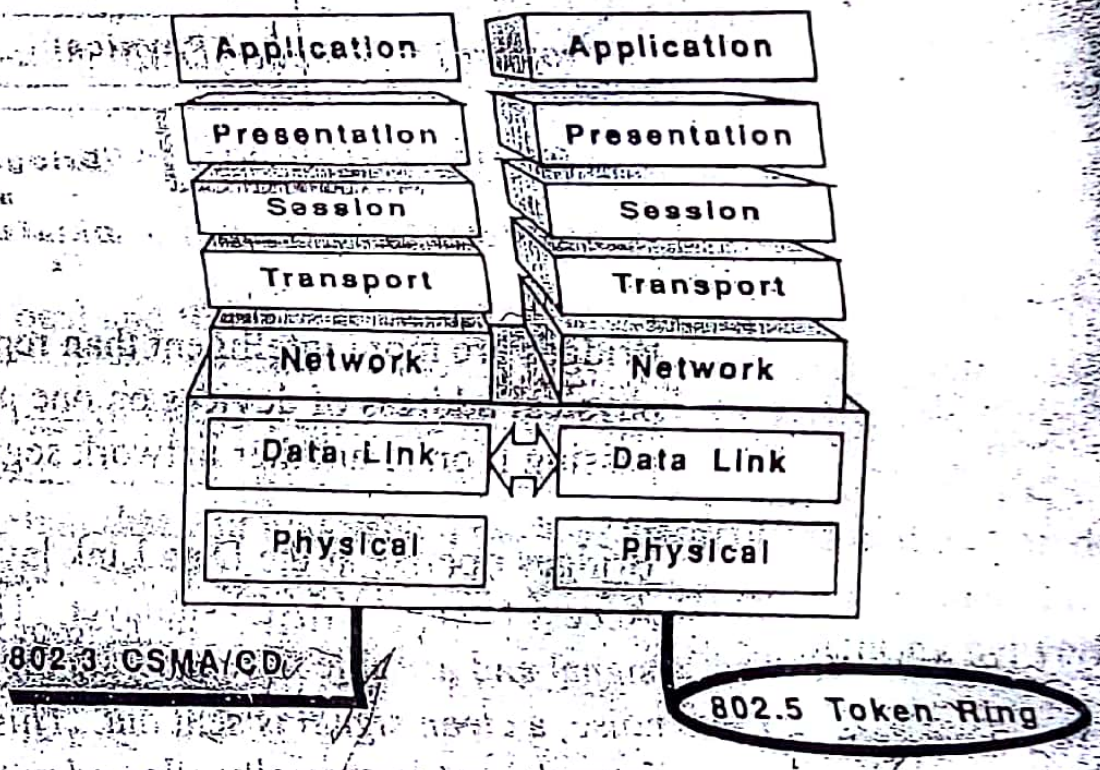
There are a number of other terms and concepts relating to bridges and how they operate. Let us take a closer look at some of these.

Heterogeneous (Translating) Bridges

A bridge must read an actual MAC layer frame. Therefore, some bridges may be limited to linking similar MAC layer protocols.

In special cases where physical addressing is similar and the logical link services are identical, hybrid bridges can be developed to allow linkages between dissimilar MAC layer protocols.

Because a number of the 802 series of protocols share the common 802.2 Logical Link Control (LLC) layer, it is possible for bridges to interconnect different types of networks such as Ethernet and Token Ring. One example of this is the IBM Model 8209 Ethernet to Token Ring Bridge.



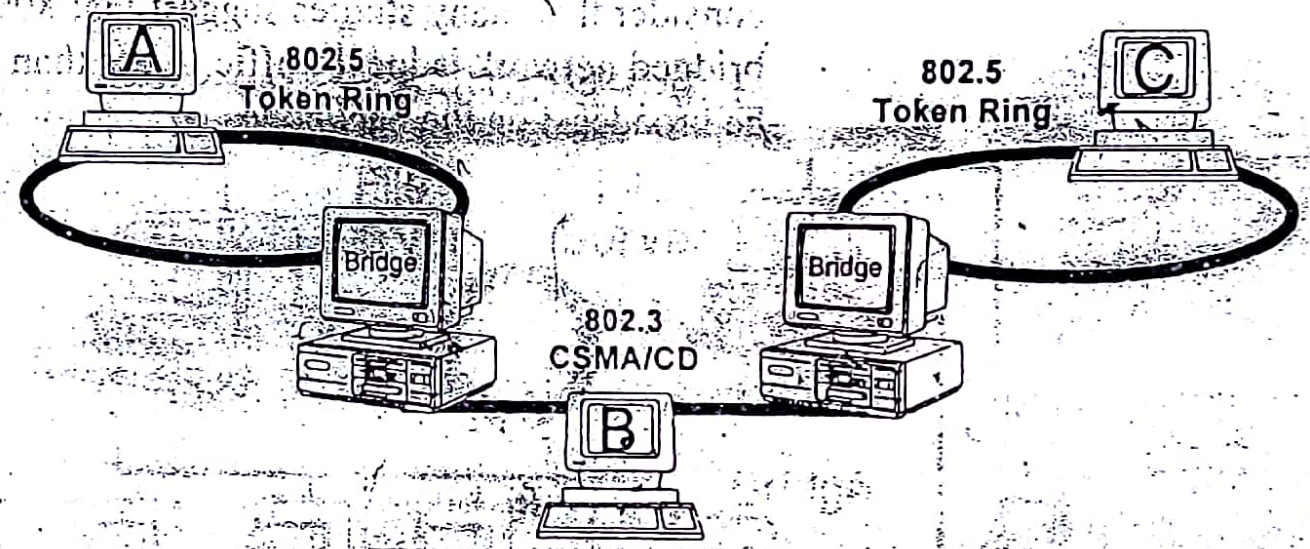
Bridges of this type are also called translating bridges.

Encapsulating Bridge

In encapsulating mode, a bridge packages frames of one format in the format of the other. For example, Token Ring frames may be "encapsulated" in Ethernet frames and passed out onto the Ethernet network. Presumably, there would be another Ethernet-Token bridge which would de-encapsulate the packets and put them on a second Token Ring network where they would be read by a destination station.

To stations on the intermediate Ethernet, these "encapsulated" frames would be unrecognizable since there is no lower level address translation being performed by the bridge.

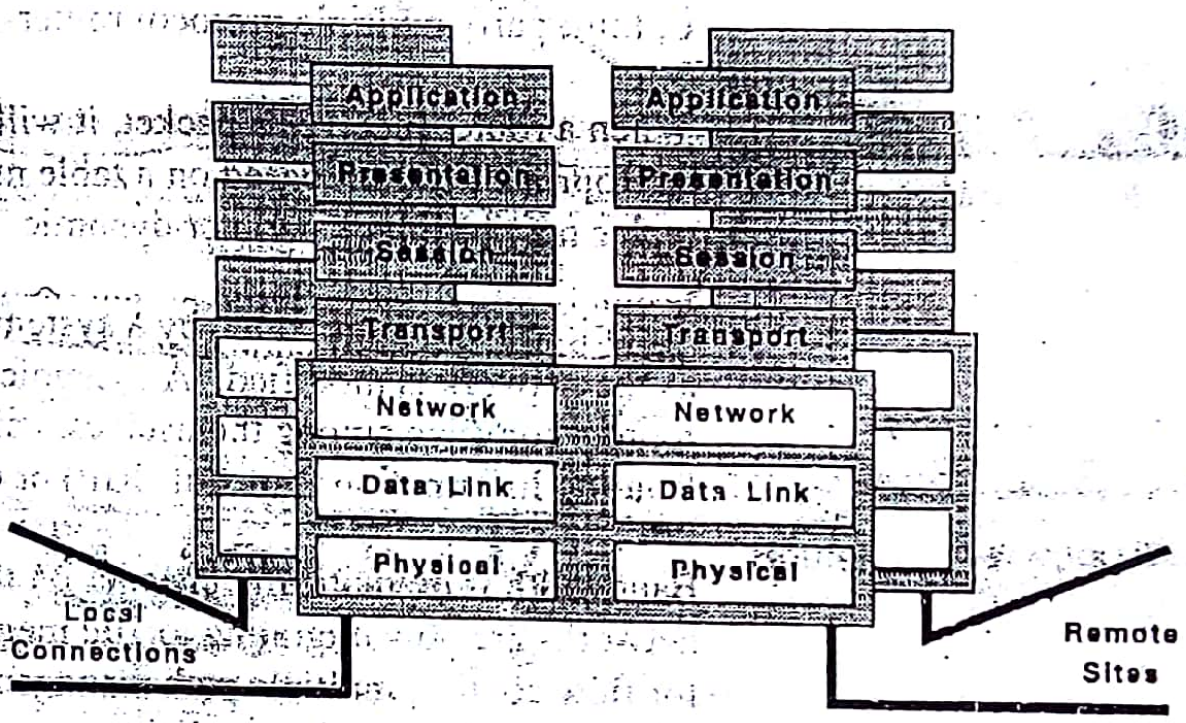
In the example below, Packets from LAN A could be read by nodes on LAN C because they share a common addressing scheme. Nodes on LAN B could not read the packets.



Encapsulation is faster than translation. It allows the LAN to pass data more quickly when the packets have to pass through multiple LANs.

Routers

As networks become more complex, simple bridging does not provide enough control of the flow of traffic. For example, broadcasts in a bridged network may propagate unnecessarily throughout the network. Routers allow for the segmentation of an extended internetwork into manageable, logical subnets.



Routers are fundamentally different from bridges, because they operate at the Network Layer. This means that a router opens the MAC (Media Access Control) layer envelope and looks at the contents of the packet delivered at the MAC layer. The contents of the MAC layer envelope are used to make routing decisions. This also means that protocols must have Network Layer addressing in order to be routable.

Routers may not match the throughput of bridges. Router activities require more processor time, more memory, and multiple network connections. Current routers are typically fast enough to handle Ethernet and Token Ring traffic without dropping packets.

About Routers

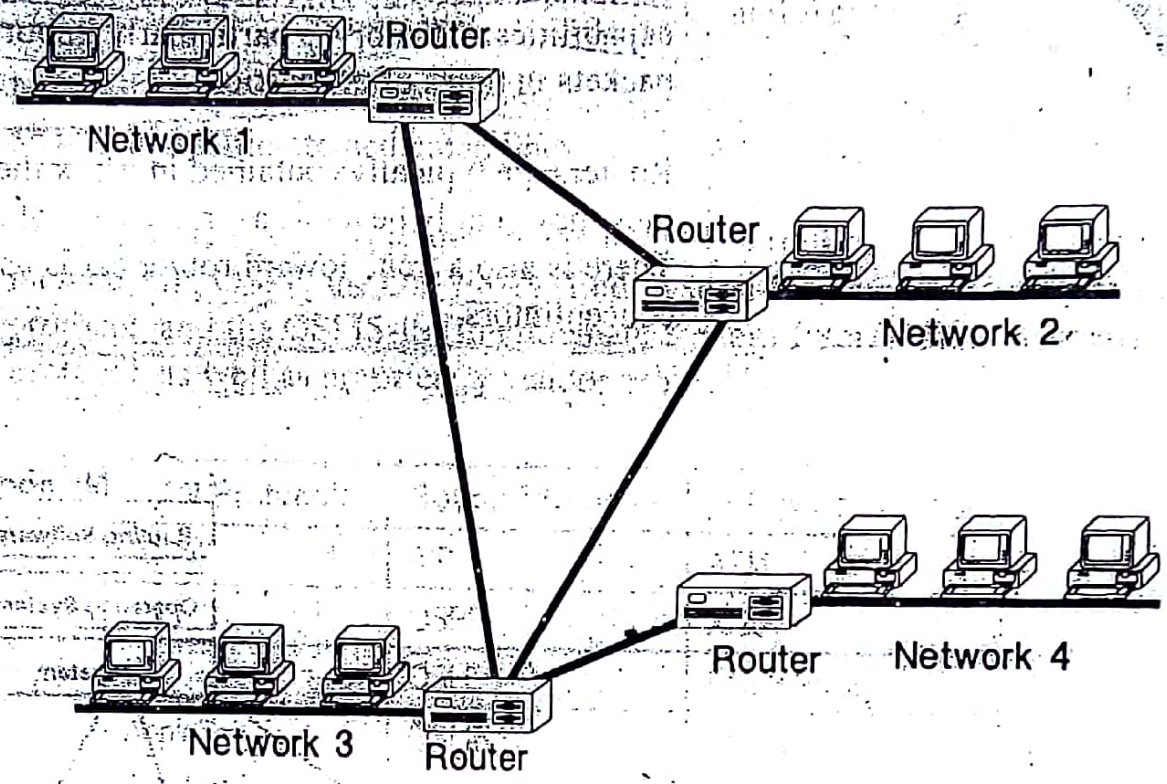
Early routers often supported a single protocol, such as TCP/IP or XNS. Today, multiple protocol routers may support 15 to 20 protocols simultaneously. In some cases, routers may be integrated with a LAN operating system such as Novell's NetWare IPX routing or Banyan VINE (both of which are derivations of XNS). However, the rise of networks running multiple protocols on the same wire is leading to the increased use of third party multiple protocol routers.

When a router receives a packet, it will generally forward it to the appropriate network based on a table maintained in the router. These tables may be either static or dynamic.

A static table is maintained by a system manager and is updated manually as the network is modified. A dynamic table is updated automatically as routers converse among themselves, using a common protocol such as Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

Bandwidth is dramatically cheaper on the LAN. Modern backbone networks are now migrating to 100 megabit speeds and above. The need for flow control, multiple path management, and routing decision rules arise primarily in wide area links.

Wide area connections generally require a routable protocol, such as TCP/IP or XNS. Each network segment is a separate logical network and may be administered independently. This also provides easier fault isolation.



The additional intelligence of routers allows for multiple (redundant) paths between locations, which provides both backup and the ability to do load balancing and makes full use of available bandwidth. With bridges, multiple paths have to be avoided. Spanning Tree, for example, shuts down redundant links until they are needed, which is a waste of bandwidth.

Offsetting the higher cost of managing and coordinating these more complex connections is the increased functionality that includes the ability to isolate individual workgroup networks as unique subnets. The router provides a port of entry that can control entrance and exit of traffic to and from the subnet. This segmentation is vital in organizations that rely on department-level network management. It also improves security and reduces congestion across the internetwork.

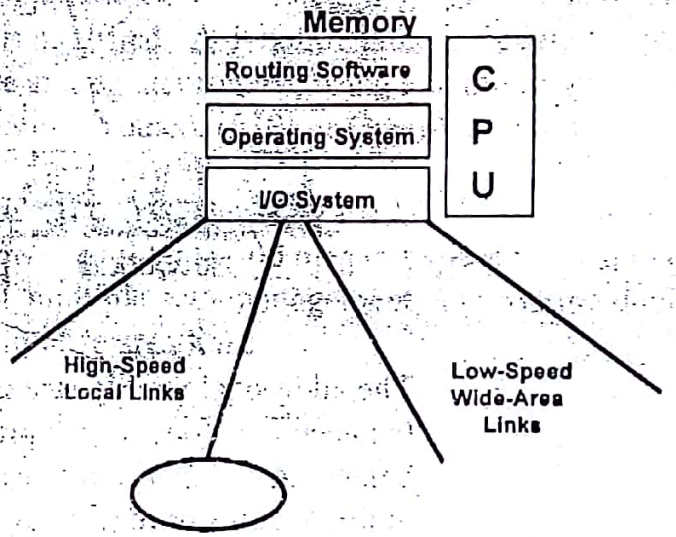
The programmable features of routers allow for effective management of remote links. Because these wide area connections are the most expensive components of the network, proper management and prioritization of traffic on these links is a vital concern for multi-site organizations.

Router Features

Processor/Memory/Storage

Routers are actually specialized microcomputers with highly tailored I/O capabilities. Memory is particularly important because it is used to buffer packets in times of congestion.

Routers are typically contained in a box the size of a PC. In some cases they may simply be a PC, as in the case of an external NetWare router. There is also a trend toward router cards used in hubs or wiring concentrators.



Router Components

Physical Interfaces (Ports) Supported

These may vary considerably from vendor to vendor. In some cases, the router may be a simple box with multiple ports from which two or three particular ports may be selected. Other boxes may be expanded through the addition of cards supporting particular interfaces.

On the LAN side, there may be the common Ethernet, Token Ring, or ARCnet interfaces. Connections to the wide area (telecommunications) network may include RS-232, V.35, and RS-442 interfaces. Other possible interfaces include FDDI and broadband.

Since hardware is similar for bridges, routers, and brouters, upgrades may simply require new software.