D-Computers, Computer Networks & Broadband, Application Packages & Web Based Services.

Data Communication

Internet Protocols, Net Components and Architecture, OSI Model & TCP/IP Models, Physical Layer Standards. V.35, V.24703, MSIN etc. Data Link Layer Protocols (DLC), HDLC, PPP Etc. PAP, CHAP, LANs & VLANs. Ethernet, Fast Ethernet & Gigabit Ethernet standards, CSMA-CD & Switched Ethernet network, Collision Domain & Broadband Domain. Switched Ethernet Backbone.

Network Layer Protocols (IP, RARP, ARP, ICMP, IGMP, IP, addressing. VLSM, CIDR-Router & Routed network, IP Routing principles, Static routing,, Default routing & Dynamic routing, Dynamic Routing Protocols-RIP, OSPF, BGP etc. Transport Layer Protocols TCP, UDP, IP Addressing and subnetting. Network Operating system, Active Directory, DHCP, WLAN, Proxy Server, Firewall, Network Security issue, various type of attacks & their counter measures, various security products like antivirus software, IDS, vulnerability assessment & Penetration testing.

MPLS: MPLS, Label Distribution Protocol (LDP), QuS in MPLS Network, Traffic Engineering in MPLS Network, RSVP MPLS Based VPNs, Virtual Private Network (VPNs) MPLS based layer 3 VPNs, MPLS based layer 2 VPNs.

Data Communication

S N	Chapter	Page
1	What is Data Communication	02-09
2	A Basic LAN Network Architecture	10-12
3	What is Protocols	12-13
4	OSI Model	13-17
5	TCP/IP Model	17-21
6	Physical Layer Standards V.35, V.24,	21-24
7	Data Link Layer Protocols (DLC), HDLC, PPP	24-30
8	PAP, CHAP, LANs & VLANs.	30-32
9	Ethernet, Fast Ethernet & Gigabit Ethernet standards	32-34
10	CSMA-CD & Switched Ethernet network,	34-40
11	Collision Domain & Broadband Domain	40-41
12	Switched Ethernet Backbone	41-42
13	Network Layer Protocols (IP, RARP, ARP, ICMP, IGMP)	43-44
14	VLSM, CIDR-Router & Routed network,	44-49
15	IP Routing principles, Static routing,, Default routing & Dynamic routing, Dynamic Routing Protocols-RIP, OSPF, BGP etc	49-63
16	Transport Layer Protocols TCP, UDP, IP Addressing and subnetting	63-72
17	Network Operating system, Active Directory, DHCP, WLAN, Proxy Server	72-78
18	Firewall, Network Security issue, various type of attacks & their counter measures, various security products like antivirus software, IDS, vulnerability assessment & Penetration testing	78-90
19	MPLS: MPLS, Label Distribution Protocol (LDP),	90-96
20	QuS in MPLS Network	96-96
21	Traffic Engineering in MPLS Network,	97-98
22	RSVP MPLS Based VPNs	98-101
23	What is Virtual Private Network	101-103
24	MPLS Based Layer 2 VPNs	103-107
25	MPLS Based Layer 3 VPNs	107-108

Data Communications

The fundamental purpose of a communications system is the exchange of data between two parties.
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).
The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.
1. ***Delivery***. The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. ***Accuracy***. The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. ***Timeliness***. The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
4. ***Jitter***. Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the

Data Communication and Networking Introduction

Today computer is available in many offices and homes and therefore there is a need to share data and programs among various computers. With the advancement of data communication facilities the communication between computers has increased and thus it has extended the power of computer beyond the computer room. Now a user sitting at one place can communicate with computers of any remote site through communication channel. The aim of this lesson is to introduce you the various aspects of computer network.

Objectives

After going through this lesson, you will be in a position to learn the basic elements of data communication system describe communication protocols and data transmission modes explain the use of computer network describe different components of computer network identify different types of network understand what is internet and e-mail and its uses in modern communication appreciate the use of satellite communication.

Data Communication

We all are acquainted with some sorts of communication in our day to day life. For communication of information and messages we use telephone and postal communication systems. Similarly data and information from one computer system can be transmitted to other systems across geographical areas. Thus data transmission is the movement of information using some standard methods. These methods include electrical signals carried along a conductor, optical signals along an optical fibers and electromagnetic areas.
Suppose a manager has to write several letters to various clients. First he has to use his PC and Word Processing package to prepare the letter, if the PC is connected to all the client's PC through networking, he can send the letters to all the clients within minutes. Thus irrespective of geographical areas, if PCs are connected through communication channel, the data and information,

computer files and any other programs can be transmitted to other computer systems within seconds. The modern form of communication like e-mail and Internet is possible only because of computer networking.

Basic Elements of a Communication System
The following are the basic requirements for working of a communication system.
1. The sender (source) who creates the message to be transmitted
2. A medium that carries the message
3. The receiver (sink) who receives the message

In data communication four basic terms are frequently used. They are:
Data : A collection of facts in raw forms that become information after processing.
Signals : Electric or electromagnetic encoding of data.
Signaling : Propagation of signals across a communication medium.
Transmission : Communication of data achieved by the processing of signals.

The Five Main Components of Data Communication

The **five** main components of data communication system are:
1. **Message** - It is the information to be communicated. Popular forms of information include text, pictures, audio, video etc.
2. **Sender** - It is the device which sends the data messages. It can be a computer, workstation, telephone handset etc.
3. **Receiver** - It is the device which receives the data messages. It can be a computer, workstation, telephone handset etc.
4. **Transmission Medium** - It is the physical path by which a message travels from sender to receiver. Some examples include twisted-pair wire, coaxial cable, radiowaves etc.
5. **Protocol** - It is a set of rules that governs the data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating.

Communication Protocols

You may be wondering how computers send and receive data across communication links. The answer is data communication software. It is this software that enables us to communicate with other systems. The data communication software instructs computer systems and devices as to how exactly data is to be transferred from one place to another. The procedure of data transformation in the form of software is commonly known as protocol. The data transmission software or protocols perform the following functions for the efficient and error free transmission of data.

1. **Data sequencing** : A long message to be transmitted is broken into smaller packets of fixed size for error free data transmission.
2. **Data Routing** : It is the process of finding the most efficient route between source and destination before sending the data.
3. **Flow control** : All machines are not equally efficient in terms of speed. Hence the flow control regulates the process of sending data between fast sender and slow receiver.
4. **Error Control** : Error detecting and recovering is the one of the main functions of communication software. It ensures that data are transmitted without any error.

Data Transmission Modes

There are three ways for transmitting data from one point to another.

1. **Simplex** : In simplex mode the communication can take place in one direction. The receiver receives the signal from the transmitting device. In this mode the flow of information is Uni-directional. Hence it is rarely used for data communication.
2. **Half-duplex** : In half-duplex mode the communication channel is used in both directions, but only in one direction at a time. Thus a half-duplex line can alternately send and receive data.
3. **Full-duplex** : In full duplex the communication channel is used in both directions at the same time. Use of full-duplex line improves the efficiency as the line turnaround time required in half-duplex arrangement is eliminated. Example of this mode of transmission is the telephone line.

A B
Simplex A to B only
A B
Half-Duplex A to B or B to A
A B
Full-Duplex A to B and B to A

Digital and Analog Transmission

Data is transmitted from one point to another point by means of electrical signals that may be in digital and analog form. So one should know the fundamental difference between analog and digital signals. In analog signal the transmission power varies over a continuous range with respect to sound, light and radio waves.

On the other hand, a digital signal may assume only discrete set of values within a given range. (see fig. 5.2 and 5.3) Examples are computer and computer related equipment. Analog signal is measured in Volts and its frequency is in Hertz (Hz).

A digital signal is a sequence of voltage represented in binary form. When digital data are to be sent over an analog form the digital signal must be converted to analog form. So the technique by which a digital signal is converted to analog form is known as modulation. And the reverse process, that is the conversion Digital Signals of analog signal to its digital form, is known as demodulation. The device, which converts digital signal into analog, and the reverse, is known as modem.
1 0 0 0 0 0 0 1

Asynchronous and Synchronous Transmission

Data transmission through a medium can be either asynchronous or synchronous. In asynchronous transmission data is transmitted character by character as you go on typing on a keyboard. Hence there is irregular gaps between characters.

However, it is cheaper to implement, as you do not have to save the data before sending. On the other hand, in the synchronous mode, the saved data is transmitted block by block. Each block can contain many characters. Synchronous transmission is well suited for remote communication between a computer and related devices like card reader and printers.

Types of Communication Services

A term used to describe the data-handling capacity of a communication service is bandwidth. Bandwidth is the range of frequencies that is available for the transmission of data. A narrow range of frequencies in a communication system

is analogous to a garden hose with a small diameter. The flow of information in such a system its data rate is restricted, just as is the flow of water in the narrow hose. Wider bandwiths permit more rapid information flow. The communication data transfer rate is measured in a unit called baud. Baud is identical to bits per second. Therefore, a rate of 300 baud is 300 bits per second.

Communication companies such as American Telephone and Telegraph (AT&T) and Western Union are called common carriers, and they provide three general classes of service for both voice and data communication:

1. Narrowband handles low data volumes. Data transmission rates are from 45 to 300 baud. The low-speed devices might use narrow band communications.
2. Voiceband handles moderate data transmission volumes between 300 and 9600 baud. They are used for applications ranging from operating a CRT to running a line printer. Their major application is for telephone voice communication hence, the term voiceband.
3. Broadband handles very large volumes of data. These systems provide data transmission rates of 1 million baud or more. High-speed data analysis and satellite communications are examples of broadband communication systems.

Communication Media

Following are the major communication devices which are frequently used :
1. **Wire Pairs** : Wire pairs are commonly used in local telephone communication and for short distance digital data communication. They are usually made up of copper and the pair of wires is twisted together. Data transmission speed is normally 9600 bits per second in a distance of 100 meter.
2. **Coaxial Cables** : Coaxial cable is groups of specially wrapped and insulated wires that are able to transfer data at higher rate. They consist of a central copper wire surrounded by an insulation over which copper mesh is placed. They are used for long distance telephone lines and local area network for their noise immunity and faster data transfer.
3. **Microwave** : Microwave system uses very high frequency radio signals to transmit data through space. The transmitter and receiver of a microwave system should be in line-of-sight because the radio signal cannot bend. With microwave very long distance transmission is not possible. In order to overcome the problems of line of sight and power amplification of weak signal, repeaters are used at intervals of 25 to 30 kilometers between the transmitting and receiving end.
4. **Communication Satellite** : The problem of line-sight and repeaters are overcome by using satellites which are the most widely used data transmission media in modern days. A communication satellite is a microwave relay station placed in outer space. INSAT-1 B is such a satellite that can be accessible from anywhere in India. In satellite communication, microwave signal is transmitted from a transmitter on earth to the satellite at space. The satellite amplifies the weak signal and transmits it back to the receiver. The main advantage of satellite communication is that it is a single microwave relay station visible from any point of a very large area. In microwave the data transmission rate is 16 giga bits per second. They are mostly used to link big metropolitan cities.

Computer Network

A computer network is interconnection of various computer systems located at different places. In computer network two or more computers are linked together with a medium and data communication devices for the purpose of communication data and sharing resources. The computer that provides resources to other computers on a network is known as server. In the network the individual computers, which access shared network resources, are known as nodes.

Types of Networks

There are many different types of networks. However, from an end user's point of view there are two basic types:

Local-Area Networks (LANs)

The computers are geographically close together (that is, in the same building).

Wide-Area Networks (WANs)

The computers are farther apart and are connected by telephone lines or radio waves.

In addition to these types, the following characteristics are also used to categorize different types of networks.

Topology

The geometric arrangement of a computer system. Common topologies include bus, star, and ring.

Protocol

The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular protocols for LANs is called Ethernet. Another popular LAN protocol for PCs is the IBM token-ring network.

Architecture

Networks can be broadly classified as using either peer-to-peer or client/ server architecture.

Computers on a network are sometimes called nodes. Computers and devices that allocate resources for a network are called servers.

Local Area Network (LAN)

LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANS over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

Most LANs as shown in Fig. 5.4 connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it is also able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chart sessions.

There are many different types of LANs-token-ring networks, Ethernents, and ARCnets being the most common for PCs.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distance are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

Wide Area Network (WAN)

A WAN is a computer network that spans a relatively large geographical area. Typically, A WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet.
A typical WAN set up is shown in Fig. 5.5

Network Topologies
As we have seen earlier, topology is the geometric arrangement of the computers in a network. Common topologies include star, ring and bus.
Star Network
The star network as shown in Fig 5.6 is frequently used to connect one or more small computers or peripheral devices to a large host computer or CPU. Many organizations use the star network or a variation of it in a time-sharing system, in which several users are able to share a central processor.
Star Topology
In a time-sharing setup, each terminal receives a fixed amount of the CPU's time, called a time slice. If you are sitting at a terminal and cannot complete your task during the time slice, the computer will come back to you to allow you to do so. Actually, because the CPU operates so much faster than terminals, you will probably not even notice that the CPU is away.
By establishing time-sharing, many people in a large organization can use a centralized computing facility. Time-sharing can also be purchased from an outside service, which is an economical way to operate for a small company that cannot afford its own large computer.
Star network is frequently used in a LAN to connect several microcomputers to a central unit that works as a communications controller. If the user of one microcomputer wants to send a document or message to a user at another computer, the message is routed through the central communications controller. Another common use of the star network is the feasibility of connecting several microcomputers to a mainframe computer that allows access to an organization's database.
Access and control of star network typically is maintained by a polling system. Polling means that the central computer, or communications controller "polls" or asks each device in the network if it has a message to send and then allows each in turn to transmit data.

Ring Network
The ring network (see Fig. 5.7) is a Local Area Network (LAN) whose topology is a ring - can be as simple as a circle or point-to-point connections of computers at dispersed locations, with no central host computer or communications controller. That is, all of the nodes are connected in a closed loop. Messages travel around the ring, with each node reading those messages addressed to it. One of the advantages of ring networks is that they can span larger distance than other types of networks, such as bus networks, because each node regenerates messages as they pass through it.
Ring Topology
Access and control of ring networks are typically maintained by a "token-passing" system. IBM's Token-Ring network is thought by some observers to be a watershed event comparable to the development of the IBM PCV itself, because the Token-Ring network is designed to link all types of computers together, including not only personal computers but also possible mini computes and mainframes.
A Token-Ring network as shown in Fig. 5.7 resembles a merry-go-round. To deliver a message, you would hand over your addressed note to a rider (the token)

on the merry-go-round, who would drop it off at the appropriate place.

Bus Network

Bus networks (see Fig. 5.8) are similar to ring network that the ends are not connected. All communications are carried on a common cable or bus and are available to each device on the network.

Access and control of bus networks are typically maintained by a method called contention, whereby if a line is unused, a terminal or device can transmit its message at will, but if two or more terminals initiate messages simultaneously, they must stop and transmit again at different intervals.

Network Architecture

The term architecture can refer to either hardware or software, or a combination of hardware and software. The architecture of a system always defines its broad outlines, and may define precise mechanisms as well.

An open architecture allows the system to be connected easily to devices and programs made by other manufacturers. Open architectures use off-the-shelf components and conform to approved standards. A system with a closed architecture, on the other hand, is one whose design is proprietary, making it difficult to connect the system to other systems. As we have seen before, network architectures can be broadly classified as using either peer-to-peer or client/server architecture.

Peer-to-peer Architecture

This is a type of network in which each workstation has equivalent capabilities and responsibilities. This differs from client/server architecture, in which some workstations are dedicated to serving the others. Peer-to-peer networks are generally simpler and less expensive, but they usually do not offer the same performance under heavy loads.

Client/Server Architecture

This is a network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processors dedicated to managing disk drives (file servers), printers (print servers), or network traffic (network servers). Clients are less powerful PCs workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.

Important terms used in Networking

(a) Internet

The newest type of network to be used within an organisation is an internet or internet web. Such networks enable computers (or network) of any type to communicate easily. The hardware and software needs are the same as for the internet, specifically TCP/IP, server and browser software used for the World Wide Web. Because most organisations have a need for more dynamic ways to link people and information, the internet market is expanding day by day. Moreover, there is no need to adjust the network when a new user joins in. With the help of Internet, all computers of an organisation can work as stand-alone systems, connected to a mainframe, or part of a LAN or WAN.

(b) E-Mail

E-mail stands for electronic mail. This is one of the most widely used features of Internet. Mails are regularly used today where without the help of postage stamp we can transfer mails anywhere in the world. With electronic mail the service is similar. But here data is transmitted through Internet and therefore within minutes the message reaches the destination may it be anywhere in the world. Therefore the mailing system through e-mail is excessively fast and is being used widely for mail transfer.

(c) Voice Messaging

It is a new communication approach which is similar to electronic mail except that it is audio message rather than text messages that are processed. A sender speaks into a telephone rather than typing, giving the name of the recipient and the message. That sender's voice signal is then digitised and stored. The system can then either deliver the message at a specified time in future or it can be retrieved from a database by the recipient. The message is reconverted back into its analog format when it is delivered or retrieved so that the recipient hears it as the original sender's voice on a telephone. Voice messaging requires a computer with an ability to store the audio messages in digital form and then convert them back in an audio form upon verification. Each user has a voice mailbox in secondary storage and special equipment converts the audio message to and from the digital form. The main advantage of voice mail over electronic mail is that the sender does not have to type. Voice mail also makes it easy to include people in the firm's environment in an communication network.

(d) E-Commerce

Electronic commerce or e-commerce as it is popularly known refers to the paperless exchange of business information using Electronic Data Interchange, Electronic mail, Electronic Bulletin Boards, Electronic Fund Transfer and other network based technologies. Electronic Commerce (EC) not only automates manual process and paper transactions, but it also helps organisations to move into a fully electronic environment and change the way they usually operate. Few organisations have recently started conducting EC over Internet, the network of networks. Internet has also helped EC to boost up because it is a low cost alternative to the proprietary networks. EC standards are however under development. Electronic Data Interchange (EDI) is still the dominant part of EC.

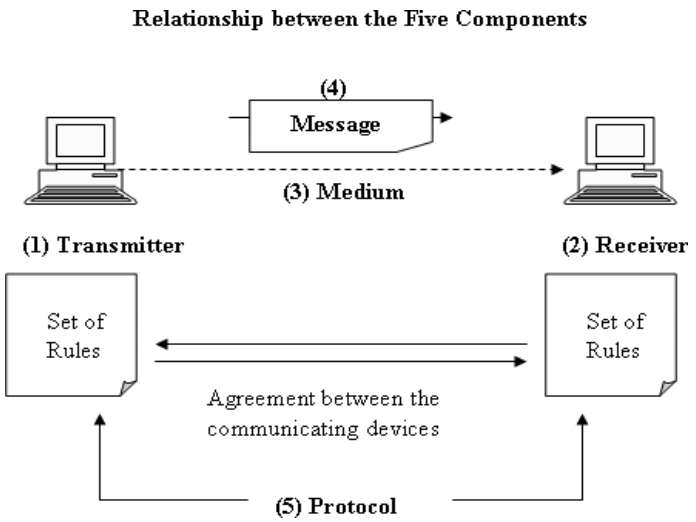
Information Technology has transformed the way people work. Electronic Commerce (EC) has unearthed yet another revolution which is changing the way business houses buy and sell products and services. EC is associated with buying and selling of products and services over computer communication networks. EC transfers information electronically from computer to computer in autonomous way. EC has, in fact, transformed the way organisations operate.

(e) Electronic Data Interchange (EDI)

EDI is the computer-to-computer exchange of business documents in a standard format. These formats look much like standard forms and are highly structured.

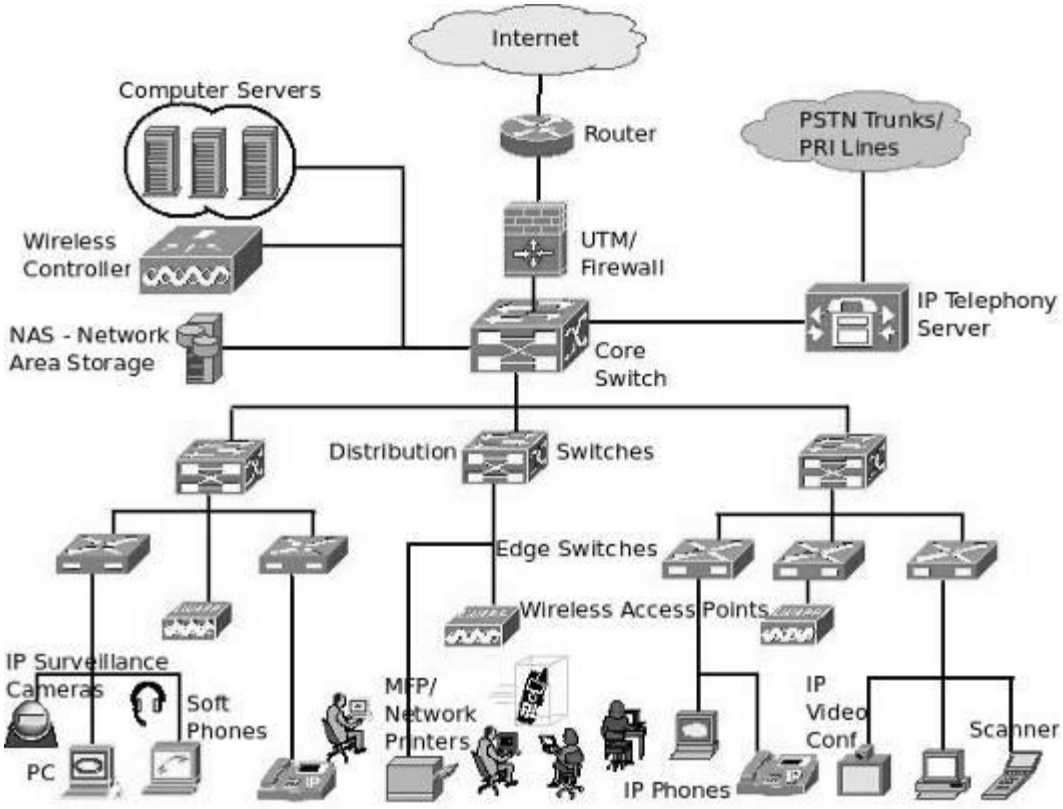
(f) Teleconferencing

It refers to electronic meetings that involve people who are at physically different sites. Telecommunication technology allows participants to interact with one another without travelling to the same location.



A Basic LAN Network Architecture

Block Diagram and Components



Have you ever wondered about what could be the various networking components that make an enterprise LAN (Computer Network / Local Area Network)? The above diagram shows you the connectivity architecture of the major components that form a network.

Brief description of the individual components below:

Internet: The Internet cloud refers to the source of the Internet to an organization. The organization could be connected to the Internet via Internet Leased Lines/ Broadband/ 3G etc. For connectivity to other branches, a VPN Network over the Internet could be used (or) A Managed Leased Line/ MPLS circuit could be used as well.

Router: The Enterprise Router is basically a Layer-3 Network device that connects disparate networks. It acts as a gateway between the LAN and the WAN networks and the Internet Leased Lines/ MPLS Circuits/ Managed Leased Lines/ Broadband networks are all terminated on the router. Some Routers support additional modules for secure connectivity to other branches through VPN, Intrusion Prevention and Content Filtering etc. Routers have WAN ports and LAN ports to connect WAN and LAN connections respectively, and some of them have built in Wireless/ VOIP capabilities.

UTM / Firewall: The Unified Threat Management Appliance (or software) is for providing gateway level network security for the various end points used in the organization. The UTM Devices provide the following network security options: Firewall, Anti-Spam, Anti-Virus, Content Filtering, URL Filtering, Intrusion Prevention (IPS), Virtual Private Network (VPN), Protection from Internet threats like Phishing etc.

Core Switch: A Core Switch is generally a Layer-3 based Network Switch that connects to the various distribution switches, edge switches (through distribution switches / directly) using Optical Fiber Networks or UTP Copper cabling. They generally also connect to the computer servers (ERP, Web Server, Mail Server, Database Server, Application Servers, etc). The core switch is in the center of an enterprise network and it also provides Inter-VLAN routing. They are either stand-alone switches (24/48 Ports Copper, 4/24 Port Fiber) or Chassi-based where there is processing unit and number of blade modules(For connecting fiber/copper) that go in to empty slots allowing for a flexible configuration.

NAS Device: A NAS Device refers to a Network Area Storage Appliance (This could also be a Storage Area Network, depending upon the storage requirements) where bulk of the files/ data are stored for the servers and individual users (PC's) to access them over the network whenever required. These appliances are mostly disk based and can be connected anywhere on the network (preferably to a core switch). They come in sizes ranging from 1 TB(Tera Byte) to multiple Tera Byte configurations.

Wireless Controller: There are many access points to provide wireless (Wi-Fi) access to the PC's/ Laptops/ Wi-Fi Phones in the enterprise. All these Access Points are managed/ controlled by an appliance called 'Wireless Controller'. Basically a wireless controller provides centralized authentication, encryption, network policies, radio frequency management, failover, load balancing, wireless intrusion scanning and other functionalities required for the wireless users across the network.

IP Telephony Server: The IP Telephony Server provides the call control functions (voice switching) for the telephony operations in an enterprise network. Since the IP Phones connect to the computer networks, these IP Telephony Servers provide centralized administration and connectivity to PSTN Lines to all the IP Phones/ VOIP devices over the network including the assigning of extension/ DID numbers and IVR (Interactive Voice Response).

Distribution Switches: Distribution Switches provide an aggregation layer for network switching. The distribution switches connect to both copper UTP cable network as well as optical fiber networks. The distribution switches are connected to the core switch on one end and to the edge switches on the other. Generally, there may be one distribution switch for

each department and a network is sometimes formed without the distribution/ aggregation layer by connecting the network endpoints directly to them.

Edge Switches: The Edge/ endpoint switches are basically Layer-2 switches that provide direct connectivity to the various network devices like PC's, laptops, Wireless Access Points etc using the Copper UTP cables. They come in various configurations including 8 Port/ 16 Port, 24 Port, 48 Port etc. They support 10/100 Mbps as well as 10/100/1000 Mbps connectivity to the various network devices. Some of them even support POE (Power Over Ethernet) for electrical power required for operation of certain network devices (like Wireless Access Points, IP Phones etc) and some of them could be stacked to each other for providing a single management interface/ combined backplane for multiple such edge switches.

Wireless Access Points: The Wireless Access Points contain built in radios which provide wireless signals for connecting certain network devices that has an in-built wireless adapter. Basically these access points send wireless signals that can be interpreted by the wireless enabled network clients for communicating the data/ information over the wireless medium. Their job is just to collect these signals, convert them in to wired signals and send it over the LAN network for the wireless controller to interpret them and take appropriate action. They generally have a coverage range of 20-30 meters indoor and 80-100 meters outdoor and each device can connect to more than 15 wireless devices within their coverage area. They operate in the 2.4 and 5 Ghz frequency spectrum.

Network Endpoints/ Devices: There are various network devices/ endpoints connecting to the LAN via edge switches/ wireless access points. Some of them include PC/ Laptop/ PDA etc for data connectivity, IP Phones, Cell Phones/Wi-Fi Phones, Soft Phones for voice connectivity, IP Surveillance Cameras/ IP Video Conferencing devices for video over IP. There are also network based accessories like network printers, MFP's (Multi-Function Printers), Scanners etc. connecting to the enterprise computer network.

What is a Protocol?

- When data is transmitted between two devices, something needs to govern the controls that keep the data intact.
- Protocol is a formal description of message formats and the rules two computers must follow to exchange those messages.
- Protocol describes low level details of machine to machine interfaces or high level exchanges between application programs.

What is Internet Protocol?

IP (Internet Protocol) is the primary network protocol used on the Internet, developed in the 1970s. On the Internet and many other networks, IP is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP.

IP supports unique addressing for computers on a network. Most networks use the Internet Protocol version 4 (IPv4) standards that features IP addresses four bytes (32 bits) in length. The newer Internet Protocol version 6 (IPv6) standard features addresses 16 bytes (128 bits) in length.

Data on an Internet Protocol network is organized into packets. Each IP packet includes both a header (that specifies source, destination, and other information about the data) and the message data itself.

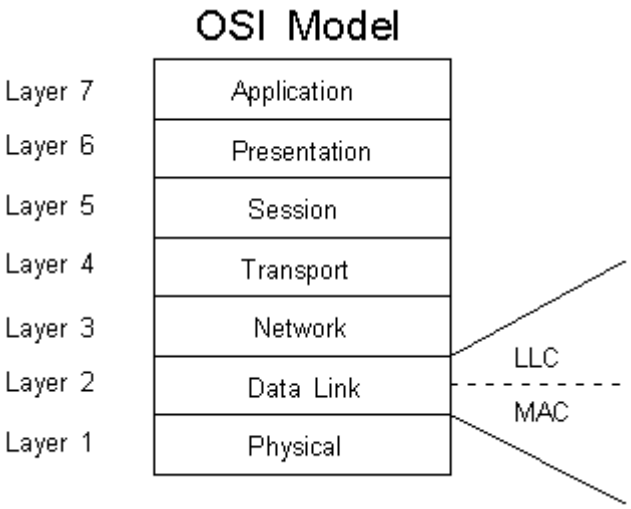
IP functions at layer 3 of the OSI model. It can therefore run on top of different data link interfaces including Ethernet and Wi-Fi.

Internet Protocols contains a set of related most widely used network protocols besides Internet Protocol (IP) itself, that is higher-level protocols like TCP, UDP, HTTP, and FTP all integrate with IP to provide additional capabilities. Similarly, lower-level Internet Protocols like ARP. RARP,IGMP, and ICMP also co-exist with IP. These higher level protocols interact more closely with applications like Web browsers while lower-level protocols interact with network adapters and other computer hardware.

Some features of IP.

- Receives the data segments from the upper layer and converts them to IP packets.
- Provides basic delivery mechanism for packets sent between all systems on Internet.
- Provides best-effort or connection-less delivery service & No error checking or tracking.
- Transports blocks of data called datagrams each of which is transported separately.
- Each datagram is identified by identification number set by the source. Identification number is incremented by 1 for each datagram sent.
- Distribute network information via routing protocols like RIP,OSPF etc.
- Responsible for addressing IPv4 or IPv6
- IP is responsible for fragmentation of the IP datagram.
- If the original packet length exceeds the MTU of a data link fragmentation occurs at the routers that cannot send IP datagram to the next interface.
- If not all fragments were received, then hosts discard the packets and sends a time exceeded ICMP message to the source machine.
- If a single fragment is lost the entire packet is resent.

OSI model



Introduction

In the late 1970s the **International Organization for Standardization (ISO)** worked on a seven layer model for LAN architectures by defining the **Open Systems Interconnection Basic Reference Model (OSI)**. Alongside this The ISO developed a set of protocols that fit within this model. Since then, other models such as the 5 layer TCP/IP model were developed, however the OSI model is still used to map and categorize protocols because of its concise and clear way of representing network functions.

The IEEE formed the 802 committee in February 1980 with the aim of standardizing LAN protocols. This resulted in the IEEE 802 series of committees that sit to develop worldwide standards for communications.

Within the OSI model, the Data Link layer was split into two, the Media Access Control (MAC) sub-layer and the 802.2 Logical Link Control (LLC) sub-layer.

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

The seven layers of the OSI model can be divided into two groups: upper layers (layers 7, 6 & 5) and lower layers (layers 4, 3, 2, 1). The upper layers of the OSI model deal with application issues and generally are implemented only in software. The highest layer, the application layer, is closest to the end user. The lower layers of the OSI model handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium (the wires, for example) and is responsible for placing data on the medium.

Network operation at all seven 7 layers of the OSI model includes.
• Network management stations (NMS)
• Web and application servers
• Gateways
• Host

Application Layer 7

It is employed in software packages which implement client-server software. When an application on one computer starts communicating with another computer, then the Application layer is used. The header contains parameters that are agreed between applications. This header is often only sent at the beginning of an application operation. Examples of services within the application layer include:

- FTP
- DNS
- SNMP
- SMTP gateways
- Web browser
- Network File System (NFS)
- Telnet and Remote Login (rlogin)
- X.400
- FTAM
- Database software

- Print Server Software

1. Defines interface to user processes for communication and data transfer in network
2. Provides standardized services such as virtual terminal, file and job transfer and operations

Presentation Layer 6

This provides function call exchange between host operating systems and software layers. It defines the format of data being sent and any encryption that may be used, and makes it presentable to the Application layer. Examples of services used are listed below:

- MIDI
- HTML
- GIF
- TIFF
- JPEG
- ASCII
- EBCDIC

1. Masks the differences of data formats between dissimilar systems
2. Specifies architecture-independent data transfer format
3. Encodes and decodes data; Encrypts and decrypts data; Compresses and decompresses data

Session Layer 5

The Session layer defines how data conversations are started, controlled and finished. The Session layer manages the transaction sequencing and in some cases authorisation. The messages may be bidirectional and there may be many of them, the session layer manages these conversations and creates notifications if some messages fail. Indications show whether a packet is in the middle of a conversation flow or at the end. Only after a completed conversation will the data be passed up to layer 6. Examples of Session layer protocols are listed below:

- RPC
- SQL
- NetBIOS names
- Appletalk ASP
- DECnet SCP

1. Manages user sessions and dialogues
2. Controls establishment and termination of logic links between users
3. Reports upper layer errors

Transport Layer 4

This layer is resonsible for the ordering and reassembly of packets that may have been broken up to travel across certain media. Some protocols in this layer also perform error recovery. After error recovery and reordering the data part is passed up to layer 5. Examples are:

- TCP
- UDP

- SPX

1. Manages end-to-end message delivery in network
2. Provides reliable and sequential packet delivery through error recovery and flow control mechanisms
3. Provides connectionless oriented packet delivery

Network Layer 3

This layer is responsible for the delivery of packets end to end and implements a logical addressing scheme to help accomplish this. This can be connectionless or connection-oriented and is independent of the topology or path that the data packets travel. Routing packets through a network is also defined at this layer plus a method to fragment large packets into smaller ones depending on MTUs for different media (Packet Switching). Once the data from layer 2 has been received, layer 3 examines the destination address and if it is the address of its own end station, it passes the data after the layer 3 header to layer 4. Examples of Layer 3 protocols include:

- Appletalk DDP
- IP
- IPX
- DECnet

1. Determines how data are transferred between network devices
2. Routes packets according to unique network device addresses
3. Provides flow and congestion control to prevent network resource depletion

Data Link Layer 2

This layer deals with getting data across a specific medium and individual links by providing one or more data link connections between two network entities. End points are specifically identified, if required by the Network layer Sequencing. The frames are maintained in the correct sequence and there are facilities for Flow control and Quality of Service parameters such as Throughput, Service Availability and Transit Delay.

Examples include:

- IEEE 802.2
- IEEE 802.3
- 802.5 - Token Ring
- HDLC
- Frame Relay
- FDDI
- ATM
- PPP

The Data link layer performs the error check using the Frame Check Sequence (FCS) in the trailer and discards the frame if an error is detected. It then looks at the addresses to see if it needs to process the rest of the frame itself or whether to pass it on to another host. The data between the header and the trailer is passed to layer 3. The MAC layer concerns itself with the access control method and determines how use of the physical transmission is controlled and provides the token ring protocols that define how a token ring operates. The LLC shields the higher level layers from concerns with the specific LAN implementation.

1. Defines procedures for operating the communication links

2. Frames packets
3. Detects and corrects packets transmit errors

Physical Layer 1

This layer deals with the physical aspects of the media being used to transmit the data. The electrical, mechanical, procedural and functional means This defines things like pinouts, electrical characteristics, modulation and encoding of data bits on carrier signals. It ensures bit synchronisation and places the binary pattern that it receives into a receive buffer. Once it decodes the bit stream, the physical layer notifies the data link layer that a frame has been received and passes it up. Examples of specifications include:

- V.24
- V.35
- EIA/TIA-232
- EIA/TIA-449
- FDDI
- 802.3
- 802.5
- Ethernet
- RJ45
- NRZ
- NRZI

You will notice that some protocols span a number of layers (e.g. NFS, 802.3 etc.). A benefit of the seven layer model is that software can be written in a modular way to deal specifically with one or two layers only, this is often called *Modular Engineering*.

Each layer has its own header containing information relevant to its role. This header is passed down to the layer below which in turn adds its own header (encapsulates) until eventually the Physical layer adds the layer 2 information for passage to the next device which understands the layer 2 information and can then strip each of the layers' headers in turn to get at the data in the right location. Each layer within an end station communicates at the same layer within another end station.

1. Defines physical means of sending data over network devices
2. Interfaces between network medium and devices
3. Defines optical, electrical and mechanical characteristics

The OSI protocol set is rarely used today, however the model that was developed serves as a useful guide when referencing other protocol stacks such as ATM, TCP/IP and SPX/IPX.

TCP/IP MODEL

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) is a descriptive framework for the Internet Protocol Suite of computer network protocols created in the 1970s by DARPA, an agency of the United States Department of Defense. It evolved from ARPANET, which were an early wide area network and a predecessor of the Internet. The TCP/IP Model is sometimes called the Internet Model or less often the DoD Model.

The TCP/IP model describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP

provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination. Protocols exist for a variety of different types of communication services between computers.

TCP/IP has four abstraction layers as defined in RFC 1122. This layer architecture is often compared with the seven-layer OSI Reference Model; using terms such as *Internet reference model*, incorrectly, however, because it is descriptive while the OSI Reference Model was intended to be prescriptive, hence being a reference model.

The TCP/IP model and related protocols are maintained by the Internet Engineering Task Force (IETF).

TCP/IP was developed on the lines of the OSI model, also referred to as the DoD or ARPANET protocol, as the early developments were funded by Advanced Research Projects Agency (ARPA). ARPA is a part of the US Department of Defense (DoD). The OSI model has seven layers and in 1974, the TCP/IP reference model was drawn on the lines of the OSI model. There are many similarities as well as differences between the OSI and TCP/IP reference model. The seven layers of the OSI reference model are as follows:

- Physical layer
- Data link layer
- Network Layer
- Transport Layer
- Session Layer
- Presentation Layer
- Application Layer

TCP/IP protocol stack requires very less central management and can easily recover from node or phone line failures. It is called the protocol stack, as usually, stack is referred to the software related to the protocol. TCP is transmission control protocol and is responsible for transmitting packets of data from client to the server. The TCP retransmits data if the data is lost or if erroneous data is received at the endpoints. The data is retransmitted until it is completely received without any error by the server or any endpoint that had requested for that data.

The IP, i.e. the Internet Protocol, is operated on the network gateways and is responsible for transmitting packets from node to node. Internet Protocol uses the IP address of the node for transmission of data. The TCP/IP protocol stack usually consists of four layers which can be described as follows:

Network Interface Layer

The network interface is between the host computer and the network. It refers to the physical network and all related physical components which are responsible for the transmission of data. This layer uses protocol to send packets of information over the network. This protocol is not the same everywhere and varies from network to network. The functionalities of this layer can be seen by the internet user because they are carried out by the operating system and the hardware drivers (network drivers) allow the connection with the computer network. The main functions of network interface layer are routing and synchronizing data over the

network, checking the data format, converting signals (analog to digital), error detection in the transmitted data.

Internet Layer
This the most crucial layer amongst the four layers of the TCP/IP model that follows five different protocols viz. IP protocol, ARP protocol, ICMP protocol, RARP protocol and IGMP protocol. This protocol enables the routing of data packets to remote computers and manages the data received at these machines. The data packets are sent from the host machine in any random order across the network. The IP protocol is responsible for receiving the data packets in an ordered fashion at the receiver end.

Transport Layer
The transport layer is the third layer of the TCP/IP protocol stack. As the name suggests, the transport layer is responsible for the transport of the data. The transmission and reception of data is handled by the transport layer. This layer is also functions for detecting the errors in the transmitted data. Basically, the transport layer communicates data between the applications running on the computers. The applications and the operating system used are different on different computers. To identify the applications along with the operating systems, the transport layer uses a numbering system. These numbers assigned are associated with the application used and are called port numbers. The transport layer uses two protocols which are :

TCP (Transmission Control Protocol): This a connection-oriented protocol.

UDP (User Datagram Protocol): This is a connectionless protocol.

Application Layer
This layer is the topmost layer of the TCP/IP protocol stack. The application layer deals with the actual applications running on the computers that want to communicate. These applications perform the functions like network connection, internet utilities, remote connection services and various other internet services. The application running on the host computer provides a communication between the operating system and the network services.

TCP/IP Reference Model

The TCP/IP model does not same as OSI model. There is no universal agreement regarding how to define TCP/IP with a layered model but it is generally agreed that there are fewer layers than the seven layers of the OSI model.

TCP/IP model define 4 layers that are as follows:

1) Internet layer :
Packet switching network depends upon a connectionless internetwork layer. This layer is known as internet layer, is the linchpin that holds the whole design together. Its job is to allow hosts to insert packets into any network and have them to deliver independently to the destination. They may appear in a different order than they were sent in each case it is a job of higher layers to rearrange them in order to deliver them to proper destination.

The internet layer specifies an official packet format and protocol known as internet protocol. The job of internet layer is to transport IP packets to appropriate destination. Packet routing is very essential task in order to avoid congestion. For these reason it is said that TCP/IP internet layer perform same function as that of OSI network layer.

2) Transport layer :

In the TCP/IP model, the layer above the internet layer is known as transport layer. It is developed to permit entities on the source and destination hosts to carry on a conversation. It specifies 2 end-to-end protocols
1)TCP (Transmission Control Protocol)
2)UDP (User Datagram Protocol)

1) TCP

It is a reliable connection-oriented protocol that permits a byte stream originating on one machine to be transported without error on any machine in the internet. It divides the incoming byte stream into discrete message and passes each one onto the internet layer. At the destination, the receiving TCP process collects the received message into the output stream. TCP deals with flow control to make sure a fast sender cannot swamp a slow receiver with more message than it can handle.

2) UDP

It is an unreliable, connectionless protocol for applications that do not want TCP's sequencing on flow control and wish to offer their own. It is also used for client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery such as transmitting speech or video.

Application Layer :

In TCP/IP model, session or presentation layer are not present. Application layer is present on the top of the Transport layer. It includes all the higher-level protocols which are virtual terminal (TELNET), file transfer (FTP) and electronic mail (SMTP).

The virtual terminal protocol permits a user on one machine to log into a distant machine and work there. The file transfer protocol offers a way to move data efficiently from one machine to another. Electronic mail was used for file transfer purpose but later a specialized protocol was developed for it.

The Application Layer defines following protocols

File Transfer Protocol (FTP)

It was designed to permit reliable transfer of files over different platforms. At the transport layer to ensure reliability, FTP uses TCP. FTP offers simple commands and makes the differences in storage methods across networks transparent to the user. The FTP client is able to interact with any FTP server; therefore the FTP server must also be able to interact with any FTP client. FTP does not offer a user interface, but it does offer an application program interface for file transfer. The client part of the protocol is called FTP and the server part of the protocol is known as FTPd. The suffix "d" means Daemon this is a legacy from Unix computing where a daemon is a piece of software running on a server that offers a service.

Hyper Text Transfer Protocol

HTTP permits applications such as browsers to upload and download web pages. It makes use of TCP at the transport layer again to check reliability. HTTP is a connectionless protocol that sends a request, receives a response and then disconnects the connection. HTTP delivers HTML documents plus all the other components supported within HTML such as JavaScript, Visual script and applets.

Simple Mail Transfer Protocol

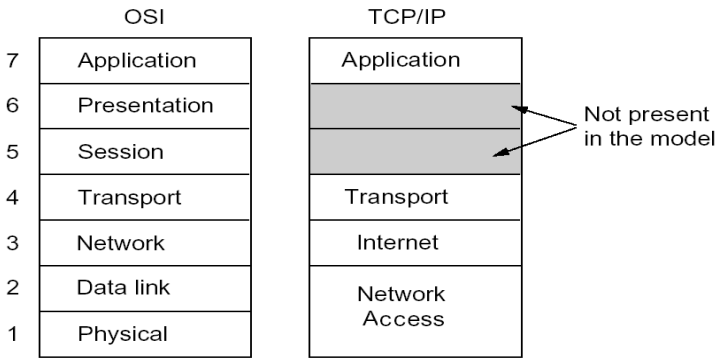
By using TCP, SMTP sends email to other computers that support the TCP/IP protocol suite. SMTP provides an

extension to the local mail services that existed in the early years of LANs. It supervises the email sending from the local mail host to a remote mail host. It is not reliable for accepting mail from local users or distributing received mail to recipients this is the responsibility of the local mail system.

SMTP makes use of TCP to establish a connection to the remote mail host, the mail is sent, any waiting mail is requested and then the connection is disconnected. It can also return a forwarding address if the intended recipient no longer receives email at that destination. To enable mail to be delivered across differing systems, a mail gateway is used.

Simple Network Management Protocol
For the transport of network management information, SNMP is used as standardized protocol. Managed network devices can be cross-examined by a computer running to return details about their status and level of activity. Observing software can also trigger alarms if certain performance criteria drop below acceptable restrictions. At the transport layer SNMP protocol uses UDP. The use of UDP results in decreasing network traffic overheads.

4) The Host to Network Layer:
Below the internet layer is great void. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has connect to the network using some protocol so it can transmit IP packets over it. This protocol is not specified and varies from host to host and network to network



Physical Layer

Physical layer is lowest layer of the OSI Reference Model. Which works at the very lowest level and deal with the actual ones and zeroes that are sent over the network. For example, when considering network interconnection devices, the simplest ones operate at the physical layer: repeaters, conventional hubs and transceivers. These devices have absolutely no knowledge of the contents of a message. They just take input bits and send them as output. Devices like switches and routers operate at higher layers and look at the data they receive as being more than voltage or light pulses that represent one or zero.

Physical Layer Functions

The following are the main responsibilities of the physical layer.

- **Definition of Hardware Specifications:** The details of operation of cables, connectors, wireless radio transceivers, network interface cards and other hardware devices are generally a function of the physical layer.

- **Encoding and Signalling:** The physical layer is responsible for various encoding and signalling functions that transform the data from bits that reside within a computer or other device into signals that can be sent over the network.
- **Data Transmission and Reception:** After encoding the data appropriately, the physical layer actually transmits the data, and of course, receives it. Note that this applies equally to wired and wireless networks.
- **Topology and Physical Network Design:** The physical layer is also considered the domain of many hardware-related network design issues, such as LAN and WAN topology.

V.35

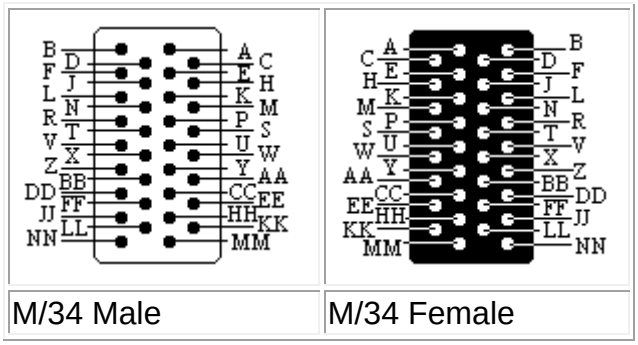
V.35 is a partially balanced, partially single-ended interface specification. The data leads and clock leads are balanced; the handshake leads are single-ended. Most commonly used for 56kbps and 64kbps data rates.

	DATA LEADS		CONTROL LEADS	
Vdc	**B > A**	**A > B**	**-3 to -25**	**+3 to +25**
binary	1	0	1	0
signal	MARK	SPACE	MARK	SPACE
function	off	on	off	on

Transmitter output voltage from a balanced tranmitter indicating a MARK is +0.35Vdc for the B line, -0.2Vdc for the A line. Indication of a SPACE condition is +0.35Vdc for the A line, -0.2Vdc for the B line. Output voltage difference is 0.55Vdc. To make sense to the receiver it must be at least 0.01Vdc difference between the A line and B line. Maximum cable length depends on required speed and cable capacitance. The extremes specified are 2000ft/600m to 4000ft/1200m @ 100kbps, 300ft/90m at 10Mbps. Sync applications only, no async V.35 equipment around.

More speed/distance equations: 610m @ 64 kbps.

Pinning



M/34 Male | M/34 Female

Pin	Signal	Abbr.	DTE	DCE
A	Chassis Ground		-	-
B	Signal Ground		-	-
C	Request To Send	RTS	Out	In
D	Clear To Send	CTS	In	Out
E	Data Set Ready	DSR	In	Out
F	Data Carrier Detect	DCD	In	Out
H	Data Terminal Ready	DTR	Out	In
J	Local Loopback	LL	In	Out
K	Local Test		Out	In
L	Unassigned			
M	Unassigned			
N	Unassigned			
P	Send Data A	TxD-	Out	In
R	Receive Data A	RxD-	In	Out
S	Send Data B	TxD+	Out	In
T	Receive Data B	RxD+	In	Out
U	Terminal Timing A		Out	In
V	Receive Timing A		In	Out
W	Terminal Timing B		Out	In
X	Receive Timing B		In	Out
Y	Send Timing A		In	Out
Z	Unassigned			
AA	Send Timing B		In	Out
BB	Unassigned			
CC	Unassigned			
DD	Unassigned			
EE	Unassigned			
FF	Unassigned			
HH	Unassigned			
JJ	Unassigned			
KK	Unassigned			
LL	Unassigned			
MM	Unassigned			
NN	Unassigned			

There are two versions of V.35 screw locks. The US-version measures 16/10 mm (the large one), the French version measures 10/10 mm (the small one). The US-version is also known as domestic and the French version is also called International.

V.35 Cross Cable		
A	-	A
B	-	B
C	-	F

F	-	C
E	-	H
H	-	E
R	-	P
T	-	S
P	-	R
S	-	T
V	-	U
X	-	W
U	-	V
W	-	X

V.24

V.24 is a specification for single-ended communications that includes the definition of connector pin allocations. It is used together with V.28 to define a specification for serial asynchronous or synchronous communications.

V.28 is a specification for single-ended communications that defines signal electrical characteristics. It is used together with V.24 to define a serial communications specification used for asynchronous or synchronous communications. V.28 signals are used in V.24 and part of V.35 interfaces.

RS-232C is essentially equivalent to a combination of V.24 and V.28. Note that the EIA standards have effectively replaced the RS standards.

X.21bis is a standard that incorporates a subset of V.24 but its use is in decline.

INTERFACE CHARACTERISTICS

V.24 is a single-ended interface, typically limited to a maximum throughput of 115Kbps. Communications distance is typically limited to 6m, the actual performance being mostly dependent on cable specification. Note that some examples of these interfaces are capable of higher ('non-standard') performance due to technological advances that enable interface integrated circuits to support bit rates exceeding 230Kbps. In synchronous mode, both receive and transmit clocks are used to transfer data (both clocks are driven by one end of a connection).

INTERFACE APPLICATIONS

One of the most common applications of V.24 interfaces is for the ubiquitous COM port and the matching serial ports of the many types of peripheral devices that can be attached to them. These implementations use the asynchronous mode of communications (ASYNC).

V.24 is also used for interfaces operating in synchronous mode, for example to connect a synchronous modem on a leased-line to a synchronous communications adapter installed in a host computer system. Typical protocols used over synchronous V.24 interfaces are HDLC, X.25, SNA and PPP.

DATA-LINK LAYER

The Data-Link layer is the protocol layer in a program that handles the moving of data in and out across a physical link in a network. The Data-Link layer is layer 2 in the Open Systems Interconnect (OSI) model for a set of telecommunication protocols.

The Data-Link layer contains two sub layers that are described in the IEEE-802 LAN standards:

- Media Access Control (MAC)
- Logical Link Control (LLC)

The Data-Link layer ensures that an initial connection has been set up, divides output data into data frames, and handles the acknowledgements from a receiver that the data arrived successfully. It also ensures that incoming data has been received successfully by analyzing bit patterns at special places in the frames.

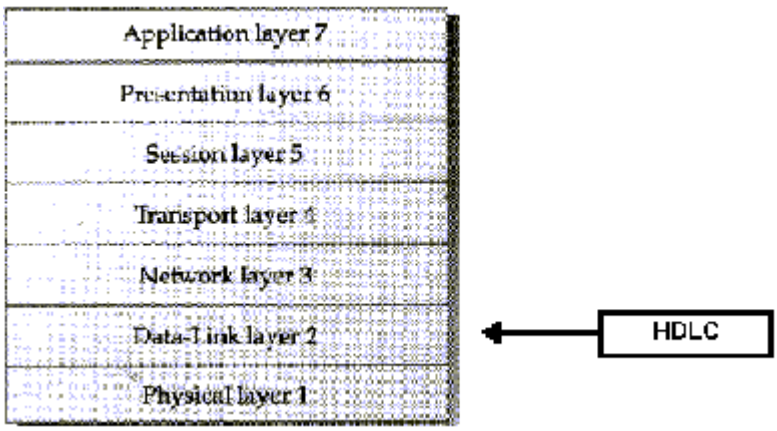
DLC - DATA LINK CONTROL

In the OSI networking model, **Data Link Control** (**DLC**) is the service provided by the data link layer. Network interface cards have a DLC address that identifies each card; for instance, Ethernet and other types of cards have a 48-bit MAC address built into the cards' firmware when they are manufactured.

There is also a network protocol with the name Data Link Control. It is comparable to better-known protocols such as TCP/IP or AppleTalk. DLC is a transport protocol used by IBM SNA mainframe computers and peripherals and compatible equipment. In computer networking, it is typically used for communications between network-attached printers, computers and servers, for example by HP in their JetDirect print servers. While it was widely used up until the time of Windows 2000, the DLC protocol is no longer included in Windows XP. It is currently available for download.

What is HDLC? (High Level Data Link Control)

High-Level Data Link Control, also known as HDLC, is a bit oriented, switched and non-switched protocol. It is a data link control protocol, and falls within layer 2, the Data Link Layer, of the Open Systems Interface (OSI) model as shown.



HDLC is a protocol developed by the International Organization for Standardization (ISO. It has been so widely implemented because it supports both half duplex and full duplex communication lines, point to point (peer to peer) and multi-point networks, and switched or non-switched channels. The procedures outlined in HDLC are designed to permit synchronous, code-transparent data transmission. Other benefits of HDLC are that the control information is always in the same position, and specific bit patterns used for control differ dramatically from those in representing data, which reduces the chance of errors.

It has also led to many subsets. Two subsets widely in use are Synchronous Data Link Control (**SDLC**) and Link Access Procedure-Balanced (**LAP-B**).

This technical overview will be concerned with the following aspects of HDLC:

- Stations and Configurations
- Operational Modes
- Non-Operational Modes
- Frame Structure
- Commands and Responses
- HDLC Subsets(SDLC and LAPB)

HDLC STATIONS AND CONFIGURATIONS

HDLC specifies the following three types of stations for data link control:

- Primary Station
- Secondary Station
- Combined Station

PRIMARY STATION

Within a network using HDLC as it's data link protocol, if a configuration is used in which there is a primary station, it is used as the controlling station on the link. It has the responsibility of controlling all other stations on the link(usually secondary stations). Despite this important aspect of being on the link, the primary station is also responsible for the organization of data flow on the link. It also takes care of error recovery at the data link level(layer 2 of the OSI model).

SECONDARY STATION

If the data link protocol being used is HDLC, and a primary station is present, a secondary station must also be present on the data link. The secondary station is under the control of the primary station. It has no ability, or direct responsibility for controlling the link. It is only activated when requested by the primary station. It only responds to the primary station. The secondary station's frames are called responses. It can only send response frames when requested by the primary station.

COMBINED STATION

A combined station is a combination of a primary and secondary station. On the link, all combined stations are able to send and receive commands and responses without any permission from any other stations on the link. Each combined station is in full control of itself, and does not rely on any other stations on the link. No other stations can control any combined station.

HDLC also defines three types of configurations for the three types of stations:

- Unbalanced Configuration
- Balanced Configuration
- Symmetrical Configuration

UNBALANCED CONFIGURATION

The unbalanced configuration in an HDLC link consists of a primary station and one or more secondary stations. The unbalanced occurs because one stations controls the other stations. In a unbalanced configurations, any of the following can be used:

- Full - Duplex or Half - Duplex operation
- Point to Point or Multi-point networks

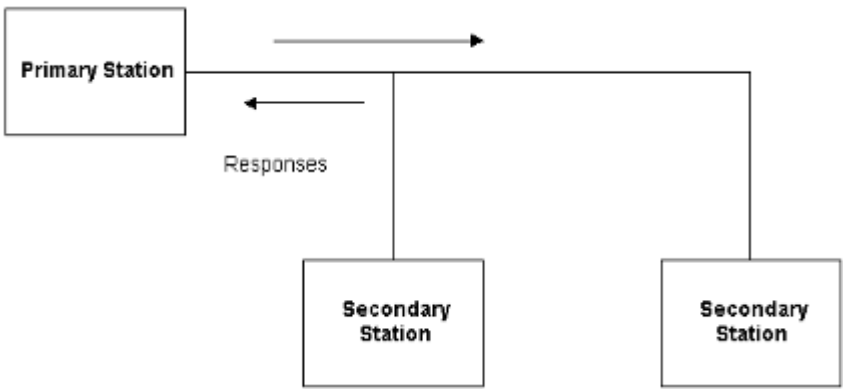
An example of an unbalanced configuration can be found below in figure 2.a

BALANCED CONFIGURATION

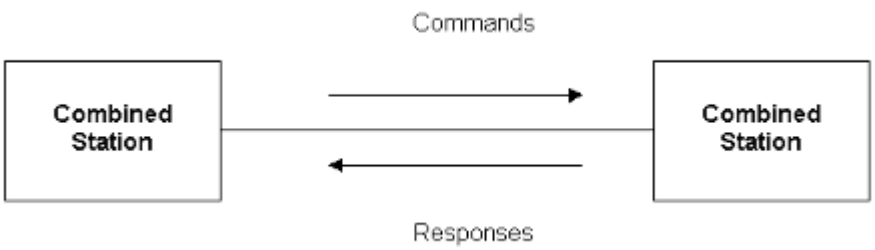
The balanced configuration in an HDLC link consists of two or more combined stations. Each of the stations have equal and complimentary responsibility compared to each other. Balanced configurations can used only the following:

- Full - Duplex or Half - Duplex operation
- Point to Point networks

An unbalanced configuration



A balanced configuration



SYMMETRICAL CONFIGURATION

This third type of configuration is not widely in use today. It consists of two independent point to point, unbalanced station configurations. In this configurations, each station has a primary and secondary status. Each station is logically considered as two stations.

HDLC Operational Modes

HDLC offers three different modes of operation. These three modes of operations are:

- Normal Response Mode(NRM)
- Asynchronous Response Mode(ARM)
- Asynchronous Balanced Mode(ABM)

Normal Response Mode

This is the mode in which the primary station initiates transfers to the secondary station. The secondary station can only transmit a response when, and only when, it is instructed to do so by the primary station. After receiving permission from the primary station, the secondary station initiates its transmission. This transmission from the secondary station to the primary station may be much more than just an acknowledgment of a frame. Once the last frame is transmitted by the secondary station, it must wait once again from explicit permission to transfer anything, from the primary station. Normal Response Mode is only used within an unbalanced configuration.

Asynchronous Response Mode

In this mode, the primary station doesn't initiate transfers to the secondary station. In fact, the secondary station does not have to wait to receive explicit permission from the primary station to transfer any frames. The frames may be more than just acknowledgment frames. They may contain data, or control information regarding the status of the secondary station. This mode can reduce overhead on the link, as no frames need to be transferred in order to give the secondary station permission to initiate a transfer. However some limitations do exist. Due to the fact that this mode is Asynchronous, the secondary station must wait until it detects and idle channel before it can transfer any frames.

Asynchronous Balanced Mode

This mode uses combined stations. There is no need for permission on the part of any station in this mode. This is because combined stations do not require any sort of instructions to perform any task on the link.

Normal Response Mode is used most frequently in multi-point lines, where the primary station controls the link. Asynchronous Response Mode is better for point to point links, as it reduces overhead. Asynchronous Balanced Mode is not used widely today.

The "asynchronous" in both ARM and ABM does not refer to the format of the data on the link. It refers to the fact that any given station can transfer frames without explicit permission or instruction from any other station.

HDLC Non-Operational Modes

HDLC also defines three non-operational modes. These three non-operational modes are:

- Normal Disconnected Mode (NDM)

- Asynchronous Disconnected Mode(ADM)
- Initialization Mode (IM)

The two disconnected modes (NDM and ADM) differ from the operational modes in that the secondary station is logically disconnected from the link (note the secondary station is not physically disconnected from the link). The IM mode is different from the operations modes in that the secondary station's data link control program is in need of regeneration or it is in need of an exchange of parameters to be used in an operational mode.

HDLC Frame Structure

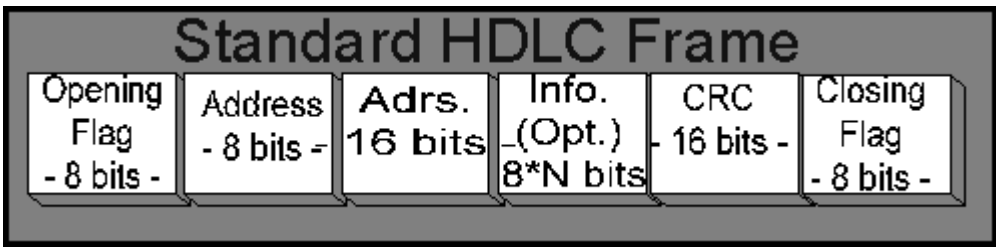
HDLC uses the term "frame" to indicate an entity of data(or a protocol data unit) transmitted from one station to another. Figure 3 below is a graphical representation of a HDLC frame with an information field.

HDLC frame with an information field.

Field Name	Size(in bits)
Flag Field(F)	8 bits
Address Field(A)	8 bits
Control Field(C)	8 or 16 bits
Information Field(I)	Variable; Not used in some frames
Frame Check Sequence(FCS)	16 or 32 bits
Closing Flag Field(F)	8 bits

Frame Formats:

The standard frames of the HDLC protocol handles both data and control messages. It has the following format:



The length of the address field is commonly 0,8 or 16 bits, depending on the data link layer protocol.
For instance the SDLC use only 8 bit address, while SS#7 has no address field at all because it is always used in point to point links.

The 8 or 16 bit control field provides a flow control number and defines the frame type (control or data). The exact use and structure of this field depends upon the protocol using the frame.

Data is transmitted in the data field, which can vary in length depending upon the protocol using the frame. Layer 3 frames are carried in the data field.

Error Control is implemented by appending a cyclic redundancy check (CRC- The Frame Control Sequence (FCS) is the HDLC frame is in most cases - 16 bit wide , the generator polynomial used is normally CRC-CCITT: x^16+x^12+x^5+1) to the frame, which is 16 bits long in most protocols.

Frame Classes:

In the HDLC protocol, three classes of frames are used:

1. **Unnumbered frames** - (Unnumbered frames are used for link management, for example they are used to set up the logical link between the primary station and a secondary station, and to inform the secondary station about the mode of operation which is used.) are used for link management.
2. **Information frames** - (Information frames are those who carry the actual data. The Information frames can be used to piggyback acknowledgment information relating to the flow of Information frames in the reverse direction when the link is being operated in ABM or ARM.) are used to carry the actual data.
3. **Supervisory frames** - are used for error and flow control.

PPP

- In networking, the **Point-to-Point Protocol** (**PPP**) is a data link protocol commonly used in establishing a direct connection between two networking nodes. It can provide connection authentication, transmission encryption, and compression.
- PPP is used over many types of physical networks including serial cable, phone line, trunk line, cellular telephone, specialized radio links, and fiber optic links such as SONET. PPP is also used over Internet access connections (now marketed as "broadband"). Internet service providers (ISPs) have used PPP for customer dial-up access to the Internet, since IP packets cannot be transmitted over a modem line on their own, without some data link protocol. Two encapsulated forms of PPP, Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over ATM (PPPoA), are used most commonly by Internet Service Providers (ISPs) to establish a Digital Subscriber Line (DSL) Internet service connection with customers.
- PPP is commonly used as a data link layer protocol for connection over synchronous and asynchronous circuits, where it has largely superseded the older Serial Line Internet Protocol (SLIP) and telephone company mandated standards (such as Link Access Protocol, Balanced (LAPB) in the X.25 protocol suite). PPP was designed to work with numerous network layer protocols, including Internet Protocol (IP), TRILL, Novell's Internetwork Packet Exchange (IPX), NBF and AppleTalk.

- PPP was designed somewhat after the original HDLC specifications. The designers of PPP included many additional features that had been seen only in proprietary data-link protocols up to that time.
- RFC 2516 describes Point-to-Point Protocol over Ethernet (PPPoE) as a method for transmitting PPP over Ethernet that is sometimes used with DSL. RFC 2364 describes Point-to-Point Protocol over ATM (PPPoA) as a method for transmitting PPP over ATM Adaptation Layer 5 (AAL5), which is also a common alternative to PPPoE used with DSL.

CHAP

CHAP is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client user's password).

1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
4. At random intervals the authenticator sends a new challenge to the peer and repeats steps 1 through 3.

CHAP PACKETS

Description	1 byte	1 byte	2 bytes	1 byte	Variable	variable
Challenge	Code = 1	ID	Length	Challenge length	Challenge value	Name
Response	Code = 2	ID	Length	Response Length	Response value	Name
Success	Code = 4	ID	Length		Message	
Failure	Code = 4	ID	Length		Message	

The ID chosen for the random challenge is also used in the corresponding response, success, and failure packets. A new challenge with a new ID must be different from the last challenge with another ID. If the success or failure is lost the same response can be sent again, and triggers the same success or failure indication.

LAN

A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a **wide-area network (WAN)**.

Most LANs connect workstations and personal computers. Each **node** (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

There are many different types of LANs **Ethernets** being the most common for PCs. Most Apple Macintosh networks are based on Apple's AppleTalk network system, which is built into Macintosh computers.

The following characteristics differentiate one LAN from another:

topology : The geometric arrangement of devices on the network. For example, devices can be arranged in a ring or in a straight line.
protocols : The rules and encoding specifications for sending data. The protocols also determine whether the network uses a peer-to-peer or client/server architecture.

media : Devices can be connected by twisted-pair wire, coaxial cables, or fiber optic cables. Some networks do without connecting media altogether, communicating instead via radio waves.

LANs are capable of transmitting data at very fast rates, much faster than data can be transmitted over a telephone line; but the distances are limited, and there is also a limit on the number of computers that can be attached to a single LAN.

VLAN

A VLAN is a grouping of computers that is logically segmented by functions, project teams, or applications without regard to the physical location of users. For example, several end stations might be grouped as a department, such as Engineering or Accounting, having the same attributes as a LAN even though they are not all on the same physical LAN segment. To accomplish this logical grouping, a VLAN-capable switching device must be used. Each switch port can be assigned to a VLAN. Ports in a VLAN share broadcast traffic and belong to the same broadcast domain. Broadcast traffic in one VLAN is not transmitted outside that VLAN. This segmentation improves the overall performance of the network.

Benefits

VLANs provide the following benefits:

- Reduced administration costs associated with moves, adds, and changes
- Controlled broadcast activity and better network security
- Leveraging existing investments
- Flexible and scalable segmentation

Types of VLANS

Each VLAN is of a particular type, and has its own maximum transmission unit (MTU) size. Two types of VLANs are defined:

- Ethernet/802.3 VLANs

- Token Ring/802.5 VLANs

Switches will allow a VLAN of one of these types to be assigned to a static/dynamic port for which the physical MAC layer is of the corresponding type; for example, allow a VLAN of type Ethernet/802.3 to be assigned to a physical 10BaseT port.

Ethernet

Ethernet was originally developed by Digital, Intel and Xerox (DIX) in the early 1970's and has been designed as a 'broadcast' system, i.e. stations on the network can send messages whenever and wherever it wants. All stations may receive the messages, however only the specific station to which the message is directed will respond.

The original format for Ethernet was developed in Xerox Palo Alto Research Centre (PARC), California in 1972. Using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) it had a transmission rate of 2.94Mb/s and could support 256 devices over cable stretching for 1km. The two inventors were Robert Metcalf and David Boggs.

Ethernet is most widely used device in LAN for networking. 10BASE-T, one of several physical media specified in the IEEE 802.3standard for Ethernet local area networks (LANs), is ordinary telephone twisted pair wire. 10BASE-T supports Ethernet's 10 Mbps transmission speed.

In addition to 10BASE-T, 10 megabit Ethernet can be implemented with these media types:

- 10BASE-2 (Thin wire coaxial cable with a maximum segment length of 185 meters)
- 10BASE-5 (Thick wire coaxial cable with a maximum segment length of 500 meters)
- 10BASE-F (optical fiber cable)
- 10BASE-36 (broadband coaxial cable carrying multiple baseband channels for a maximum length of 3,600 meters)

This designation is an Institute of Electrical and Electronics Engineers (IEEE) shorthand identifier. The "10" in the media type designation refers to the transmission speed of 10 Mbps. The "BASE" refers to baseband signaling, which means that only Ethernet signals are carried on the medium. The "T" represents twisted-pair; the "F" represents fiber optic cable; and the "2", "5", and "36" refer to the coaxial cable segment length (the 185 meter length has been rounded up to "2" for 200).

Fast Ethernet

Fast Ethernet is a local area network (LAN) transmission standard that provides a data rate of 100 megabits per second (referred to as "100BASE-T"). Workstations with existing 10 megabit per second (10BASE-T) Ethernet card can be connected to a Fast Ethernet network. (The 100 megabits per second is a shared data rate; input to each workstation is constrained by the 10 Mbps card.)

Gigabit Ethernet

The functional principles of Gigabit Ethernet are the same as Ethernet and Fast Ethernet i.e. CSMA/CD and the Framing format, the physical outworking is very different. One difference is the slot time. The standard Ethernet slot time required in CSMA/CD half-duplex mode is

not long enough for running over 100m of copper, so **Carrier Extension** is used to guarantee a 512-bit slot time.

1000BaseX (802.3z)

802.3z is the committee responsible for formalizing the standard for **Gigabit Ethernet**. The 1000 refers to 1Gb/s data speed. The existing Fiber Channel interface standard (ANSI X3T11) is used and allows up to 4.268Gbps speeds. The Fiber Channel encoding scheme is 8B/10B.

Gigabit Ethernet can operate in half or full duplex modes and there is also a standard 802.3x which manages XON/XOFF flow control in full duplex mode. With 802.3x, a receiving station can send a packet to a sending station to stop it sending data until a specified time interval has passed.

There are three media types for 1000BaseX. 1000BaseLX, 1000BaseSX and 1000BaseCX. With 1000BaseSX, 'S' is for Short Haul, and this uses short-wavelength laser (850nm) over multi-mode fiber. 1000BaseSX can run up to 300m on 62.5/125um multimode fiber and up to 550m on 50/125um multimode fiber.

Using 1300nm wavelength, Gigabit Ethernet (1000BaseLX where the 'L' is for Long wavelength laser, or Long Haul) can run up to 550m on 62.5/125um multi-mode fiber or 50/125um multi-mode fiber. In addition, 1000BaseLX can run up to 5km (originally 3km) on single-mode fiber using 1310nm wavelength laser.

1000BaseCX is a standard for STP copper cable and allows Gigabit Ethernet to run up to 25m over STP cable.

There is currently an issue as many multimode fibre installations using 62.5/125um fibre and so 220m is often the limit for the backbone when it should be 500m to satisfy ISO 11801 and EIA/TIA 568A.

1000BaseT (802.3ab)

Many cable manufacturers are enhancing their cable systems to 'enhanced Category 5' standards in order to allow Gigabit Ethernet to run at up to 100m on copper. The Category 6 standard has yet to be ratified, and is not likely to be due for a while.

In order to obtain the 1000Mbps data bit rate across the UTP cable without breaking the FCC rules for emission, all 4 pairs of the cable are used. Hybrid circuits at each end of each pair are used to allow simultaneous transmission and reception of data (full-duplex) by separating the transmission signal from the receiving signal. Because some transmission signal still manages to couple itself to the receiving side there is an additional echo canceller built in, this is called a NEXT canceller. This system minimizes the symbol rate.

Gigabit Ethernet, a transmission technology based on the Ethernet frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one gigabit). Gigabit Ethernet is defined in the IEEE 802.3standard and is currently being used as the backbone in many enterprise networks.

Gigabit Ethernet is carried primarily on optical fiber (with very short distances possible on copper media). Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone. An alternative technology that competes with Gigabit Ethernet is ATM. A newer standard, 10-Gigabit Ethernet, is also becoming available.

CSMA/CD & Switched Ethernet network.

In computer networks, the collision domain is a logical area where the data packets collide with each other. In network, when devices compete with each other a collision occurs. When two or more devices access the network, a collision occurs.

Collision domain mainly occurs in the Ethernet and it can mainly be a part of the segment cable, Ethernet hub or the whole network of switches, hubs and other devices.

In the collision domain, only one device is able to transmit the data. When a collision occurs then the devices retransmits the data signals at the later time. The following disadvantages are caused by the data collisions.

- Decreased network efficiency
- Latency
- Packet Loss.
- Slow Performance of the network.
- More bandwidth utilization
- Network Congestion
- Signals Distortions.

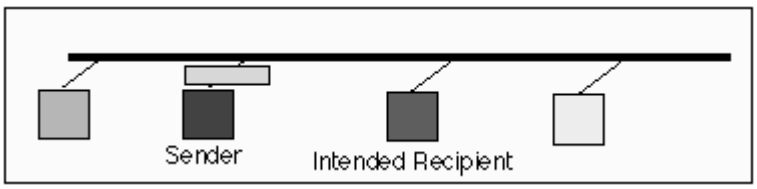
CSMA/CD is an efficient way to avoid the collisions in the network. It is a set of rules that tells each network devices like hub, switch and router that when to send the data and when to stop the data transmission. When a computer or network device wants to transmit the data in the network it first listen to the network and see if any other device is using the channel or not.

When the transmission channel is free the data is transmitted. More collisions results in more decreased efficiency in the network. Collision domain main occur in the Ethernet network that is using hubs and it is confined to one subnet.

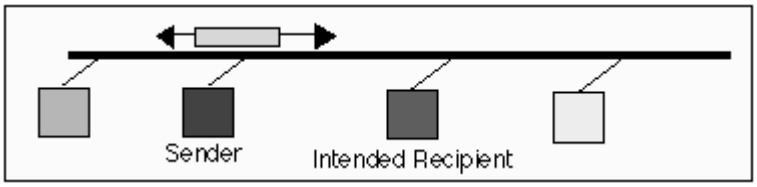
(CSMA/CD) Carrier Sense Multiple Access with Collision Detection

The Ethernet network may be used to provide shared access by a group of attached nodes to the physical medium which connects the nodes. These nodes are said to form a Collision Domain. All frames sent on the medium are physically received by all receivers, however the Medium Access Control (MAC) header contains a MAC destination address which ensures only the specified destination actually forwards the received frame (the other computers all discard the frames which are not addressed to them).

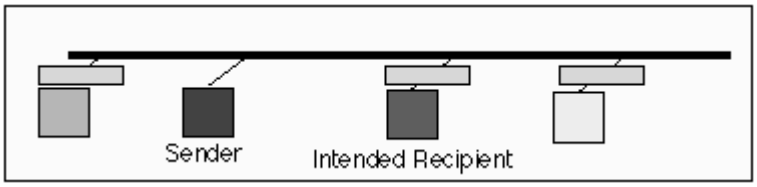
Consider a LAN with four computers each with a Network Interface Card (NIC) connected by a common Ethernet cable:



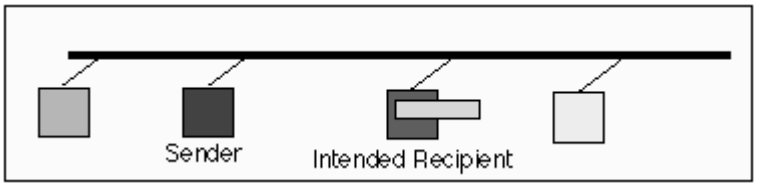
One computer (Blue) uses a NIC to send a frame to the shared medium, which has a destination address corresponding to the source address of the NIC in the red computer.



The cable propagates the signal in both directions, so that the signal (eventually) reaches the NICs in all four of the computers. Termination resistors at the ends of the cable absorb the frame energy, preventing reflection of the signal back along the cable.



All the NICs receive the frame and each examines it to check its length and checksum. The header destination MAC address is next examined, to see if the frame should be accepted, and forwarded to the network-layer software in the computer.



Only the NIC in the red computer recognizes the frame destination address as valid, and therefore this NIC alone forwards the contents of the frame to the network layer. The NICs in the other computers discard the unwanted frame.

The shared cable allows any NIC to send whenever it wishes, but if two NICs happen to transmit at the same time, a collision will occur, resulting in the data being corrupted.

ALOHA & COLLISIONS

To control which NICs are allowed to transmit at any given time, a protocol is required. The simplest protocol is known as ALOHA (this is actually an Hawaiian word, meaning "hello"). ALOHA allows any NIC to transmit at any time, but states that each NIC must add a checksum/CRC at the end of its transmission to allow the receiver(s) to identify whether the frame was correctly received.

ALOHA is therefore a best effort service, and does not guarantee that the frame of data will actually reach the remote recipient without corruption. It therefore relies on ARQ protocols to retransmit any data which is corrupted. An ALOHA network only works well when the medium has a low utilization, since this leads to a low probability of the transmission colliding with that of another computer, and hence a reasonable chance that the data is not corrupted.

CARRIER SENSE MULTIPLE ACCESS (CSMA)

Ethernet uses a refinement of ALOHA, known as Carrier Sense Multiple Access (CSMA), which improves performance when there is a higher medium utilization. When a NIC has data to transmit, the NIC **first** listens to the cable (using a transceiver) to see if a carrier (signal) is being transmitted by another node. This may be achieved by monitoring whether a current is flowing in the cable (each bit corresponds to 18-20 milliAmps (mA)). The individual bits are sent by encoding them with a 10 (or 100 MHz for Fast Ethernet) clock using Manchester encoding. Data is only sent when no carrier is observed (i.e. no current present) and the physical medium is therefore idle. Any NIC which does not need to transmit, listens to see if other NICs have started to transmit information to it.

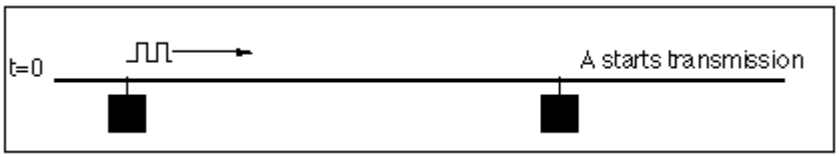
However, this alone is unable to prevent two NICs transmitting at the same time. If two NICs *simultaneously* try transmit, then both could see an idle physical medium (i.e. neither will see the other's carrier signal), and both will conclude that no other NIC is currently using the medium. In this case, both will then decide to transmit and a *collision* will occur. The collision will result in the corruption of the frame being sent, which will subsequently be discarded by the receiver since a corrupted Ethernet frame will (with a very high probability) not have a valid 32-bit MAC CRC at the end.

COLLISION DETECTION (CD)

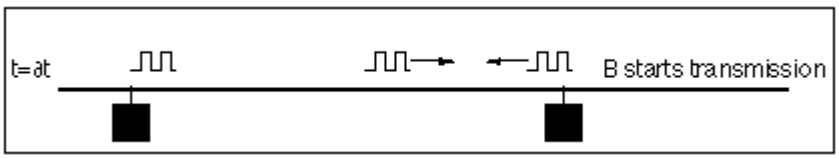
A second element to the Ethernet access protocol is used to detect when a collision occurs. When there is data waiting to be sent, each transmitting NIC also monitors its own transmission. If it observes a collision (excess current above what it is generating, i.e. > 24 mA for coaxial Ethernet), it stops transmission immediately and instead transmits a 32-bit jam sequence. The purpose of this sequence is to ensure that any other node which may currently be receiving this frame will receive the jam signal in place of the correct 32-bit MAC CRC, this causes the other receivers to discard the frame due to a CRC error.

To ensure that all NICs start to receive a frame before the transmitting NIC has finished sending it, Ethernet defines a minimum frame size (i.e. no frame may have less than 46 bytes of payload). The minimum frame size is related to the distance which the network spans, the type of media being used and the number of repeaters which the signal may have to pass through to reach the furthest part of the LAN. Together these define a value known as the *Ethernet Slot Time*, corresponding to 512 bit times at 10 Mbps.

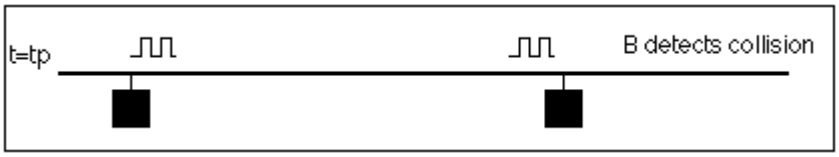
When two or more transmitting NICs each detect a corruption of their own data (i.e. a collision), each responds in the same way by transmitting the jam sequence. The following sequence depicts a collision:



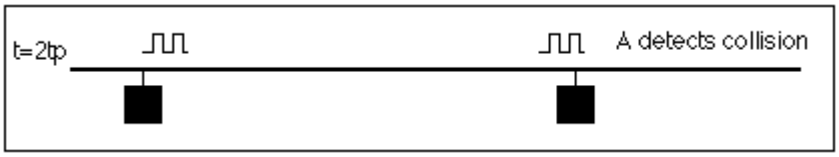
At time t=0, a frame is sent on the idle medium by NIC A.



A short time later, NIC B also transmits. (In this case, the medium, as observed by the NIC at B happens to be idle too).



After a period, equal to the propagation delay of the network, the NIC at B detects the other transmission from A, and is aware of a collision, but NIC A has not yet observed that NIC B was also transmitting. B continues to transmit, sending the Ethernet Jam sequence (32 bits).



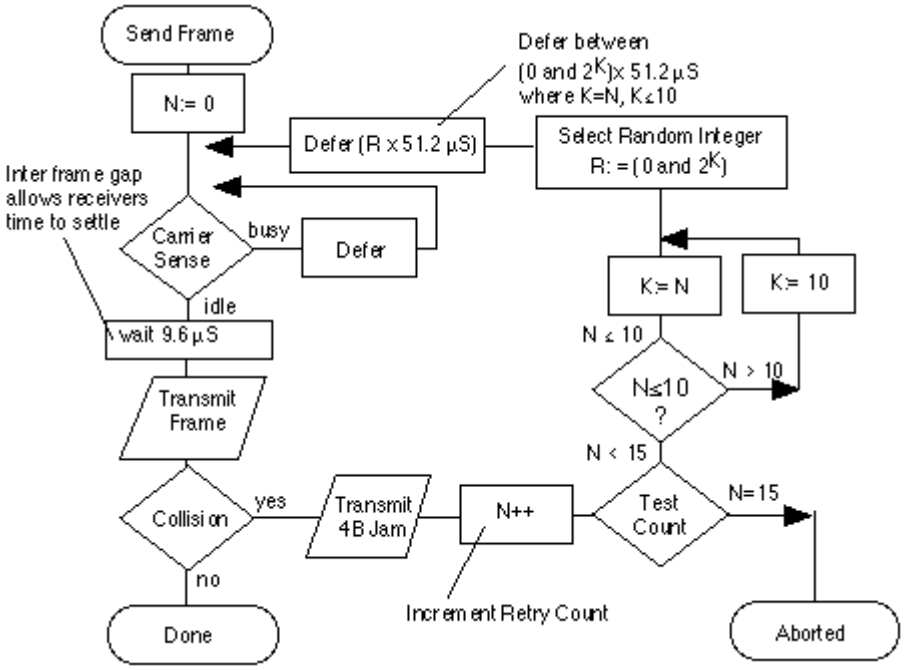
After one complete round trip propagation time (twice the one way propagation delay), both NICs are aware of the collision. B will shortly cease transmission of the Jam Sequence; however A will continue to transmit a complete Jam Sequence. Finally the cable becomes idle.

RETRANSMISSION BACK-OFF

An overview of the transmit procedure is shown below. The transmitter initializes the number of transmissions of the current frame (n) to zero, and starts listening to the cable (using the carrier sense logic (CS) - e.g., by observing the Rx signal at transceiver to see if any bits are being sent). If the cable is not idle, it waits (defers) until the cable is idle. It then waits for a small Inter-Frame Gap (IFG) (e.g., 9.6 microseconds) to allow to time for all receiving nodes to return to prepare themselves for the next transmission.

Transmission then starts with the preamble, followed by the frame data and finally the CRC-32. After this time, the transceiver Tx logic is turned off and the transceiver returns to passively monitoring the cable for other transmissions.

During this process, a transmitter must also continuously monitor the collision detection logic (CD) in the transceiver to detect if a collision occurs. If it does, the transmitter aborts the transmission (stops sending bits) within a few bit periods, and starts the collision procedure, by sending a Jam Signal to the transceiver Tx logic. It then calculates a retransmission time.



If all NICs attempted to retransmit immediately following a collision, then this would certainly result in another collision. Therefore a procedure is required to ensure that there is only a low probability of simultaneous retransmission. The scheme adopted by Ethernet uses a random back-off period, where each node selects a random number, multiplies this by the slot time (minimum frame period, 51.2 µS) and waits for this random period before attempting retransmission. The small Inter-Frame Gap (IFG) (e.g., 9.6 microseconds) is also added.

On a busy network, a retransmission may still collide with another retransmission (or possibly new frames being sent for the first time by another NIC). The protocol therefore counts the number of retransmission attempts (using a variable N in the above figure) and attempts to retransmit the same frame up to 15 times.

For each retransmission, the transmitter constructs a set of numbers:

{0, 1, 2, 3, 4, 5, L} where L is ([2 to the power (K)]-1) and where K=N; K<= 10;

A random value R is picked from this set, and the transmitter waits (defers) for a period

R x (slot time) i.e. R x 51.2 Micro Seconds

For example, after two collisions, N=2, therefore K=2, and the set is {0, 1, 2, 3} giving a one in four chance of collision. This corresponds to a wait selected from {0, 51.2, 102.4, 153.6} micro seconds.

After 3 collisions, N = 3, and the set is {0, 1, 2, 3, 4, 5, 6, 7}, that is a one in eight chance of collision.

But after 4 collisions, N=4, the set becomes {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15}, that is a one in 16 chance of collision.

The scaling is performed by multiplication and is known as exponential back-off. This is what lets CSMA/CD scale to large numbers of NICs - even when collisions may occur. The first ten times, the back-off waiting time for the transmitter suffering collision is scaled to a larger

value. The algorithm includes a threshold of 1024. The reasoning is that the more attempts that are required, the more greater the number of NICs which are trying to send at the same time, and therefore the longer the period which needs to be deferred. Since a set of numbers {0,1,...,1023} is a large set of numbers, there is very little advantage from further increasing the set size.

LATE COLLISIONS

In a proper functioning Ethernet network, a NIC may experience collision within the first slot time after it starts transmission. This is the reason why an Ethernet NIC monitors the CD signal during this time and use CSMA/CD. A faulty CD circuit, or misbehaving NIC or transceiver may lead to a late collision (i.e. after one slot time). Most Ethernet NICs therefore continue to monitor the CD signal during the entire transmission. If they observe a late collision, they will normally inform the sender of the error condition.

ETHERNET CAPTURE

A drawback of sharing a medium using CSMA/CD, is that the sharing is not necessarily fair. When each computer connected to the LAN has little data to send, the network exhibits almost equal access time for each NIC. However, if one NIC starts sending an excessive number of frames, it may dominate the LAN. Such conditions may occur, for instance, when one NIC in a LAN acts as a source of high quality packetised video. The effect is known as "Ethernet Capture".

Ethernet Capture by Node

The figure above illustrates Ethernet Capture. Computer A dominates computer B. Originally both computers have data to transmit. A transmits first. A and B then both simultaneously try to transmit. B picks a larger retransmission interval than A (shown in red) and defers. A sends, then sends again. There is a short pause, and then both A and B attempt to resume transmission. A and B both back-off, however, since B was already in back-off (it failed to retransmit), it chooses from a larger range of back-off times (using the exponential back-off algorithm). A is therefore more likely to succeed, which it does in the example. The next pause in transmission, A and B both attempt to send, however, since this fails in this case, B further increases its back-off and is now unable to fairly compete with A.

Ethernet Capture may also arise when many sources compete with one source which has much more data to send. Under these situations some nodes may be "locked out" of using the medium for a period of time. The use of higher speed transmission (e.g. 100 Mbps) significantly reduces the probability of Capture, and the use full duplex cabling eliminates the effect.

Collision domain:

Basically, a collision domain is a network segment that allows normal network traffic to flow back and forth. In the old days of hubs, this meant you had a lot of collisions, and the old CSMA/CD would be working overtime to try to get those packets re-sent every time there was a collision on the wire (since ethernet allows only one host to be transmitting at once without there being a traffic jam). With switches, you break up collision domains by switching packets bound for other collision domains. These days, since we mostly use switches to connect computers to the network, you generally have one collision domain to a PC.

A **Collision** Domain in which collisions can take place (usually in Ethernet networks). If there is more traffic in on a collision domain, the chances of collisions are also more. Increased collisions will result in low quality network where hosts spending more and more time for packet retransmission. Usually switches are used to segment a collision domain.

In a half-duplex CSMA/CD Ethernet network (typically a hub-based network), the bandwidth is shared (a bus topology, all devices share the same segment, only one can transmit at any time). CSMA/CD stands for Carrier Sense Multiple Access with Collision Detect. It's Multiple Access because there are multiple hosts with access to one network segment. Before a host transmits it will "sense the carrier" if it's free. If more than one device transmits at the same time, collisions will occur, and the frames transmitted will be destroyed. The hosts will detect the collision, and use a random back-off timer before trying to retransmit. (That should explain all the letters in CSMA/CD).

What's important to know is that in a modern Ethernet (a switched Ethernet) you'll typically run in full-duplex mode, where the CSMA/CD is switched off. There are no collisions at all, as there are dedicated transmit/receive "paths". Collision domains are also found in **wireless networks** such as **Wi-Fi**.

Broadcast domain:

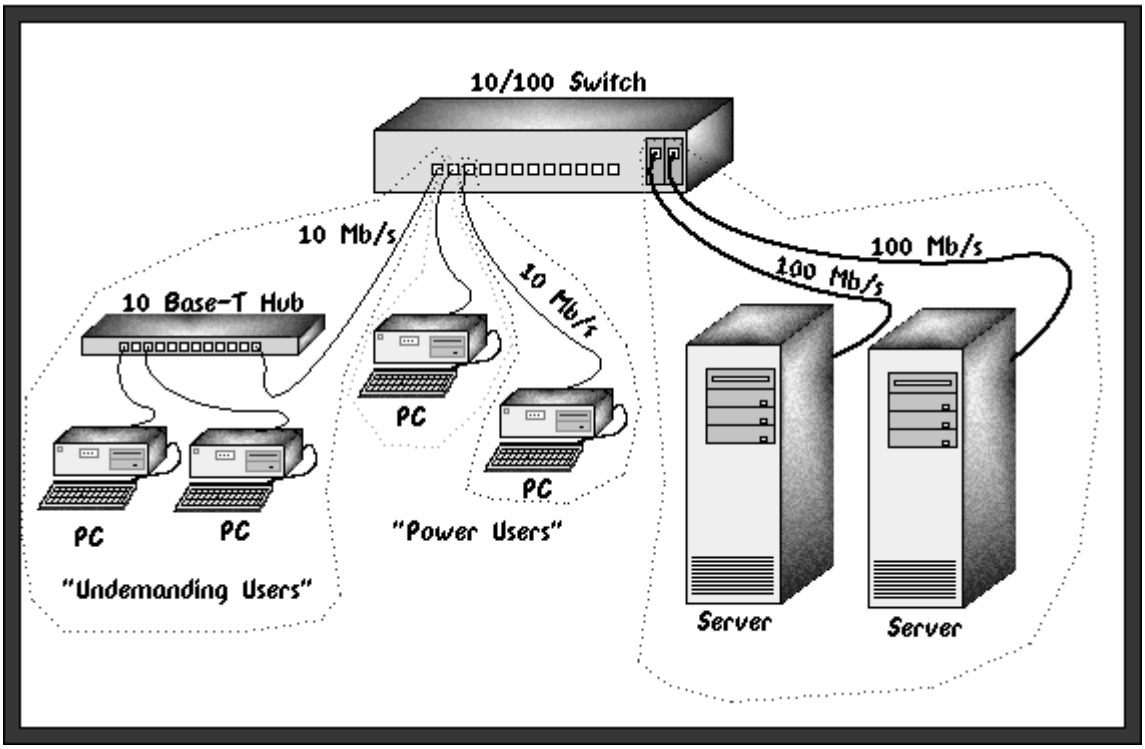
A Broadcast Domain is all devices that will receive any broadcast packet originating from any device within the group. In Collision domain, any type of data packet can encounter a collision, while in Broadcast Domain, we refer broadcast packets. Usually Routers are used to segment broadcast domain.

Typically equals your IP subnet. If you are on 10.1.1.0/24, your broadcast domain is that network. Your broadcast will be heard by all hosts in that network, but it won't traverse any router, so hosts in the next network won't see your broadcast. This is in some cases a problem (for example with DHCP, if your client is in one network and the server is in another), so there are ways to forward broadcasts to a different network (but as unicast traffic). With Cisco, this is done with the "ip helper-address", all broadcast on a given port will be forwarded as unicast to one or more hosts.

Broadcast domains are exactly what they imply: they are network segments that allow broadcasts to be sent across them. Since switches and bridges allow for broadcast traffic to go unswitched, broadcasts can traverse collision domains freely. Routers, however, don't allow broadcasts through by default, so when a broadcast hits a router (or the perimeter of a VLAN), it doesn't get forwarded. The simple way to look at it is this way: switches break up collision domains, while routers (and VLANs) break up collision domains and broadcast domains. Also, a broadcast domain can contain multiple collision domains, but a collision domain can never have more than one broadcast domain associated with it.

Switched Ethernet backbone network

A high speed backbone network is usually run at a speed of 100 Mbps, and is used to interconnect all of the servers and switches on the network. A diagram of such a setup is shown in Figure.



This layout is splitting our overall network into four sub networks. From left to right these sub networks are outlined in Red, Green, Blue, and Violet. The Red sub network is a shared 10 Mbps setup, with all of the "Undemanding Users" sharing 10 Mbps of bandwidth.

TYPES OF SWITCHES

There are three basic types of switches on the market at this time. They all perform the same basic function of dividing a large network into smaller sub networks, however the manner in which they work internally is different. The types are known as Store and Forward, Cut Through, and Hybrid.

Store and Forward

A Store and Forward switch operates much as its name implies; first it stores each incoming frame in a buffer, checks it for errors, and if the frame is good it then forwards it to its destination port. The advantage of this type of switch is that it prevents wasting bandwidth on the destination network by invalid or damaged frames. The disadvantage is that it increases the latency of the switch slightly. In a network with few errors, this results in lower overall throughput through the switch. Store and forward is most useful in networks which may experience high error rates.

Cut Through

A Cut Through switch operates differently than a Store and Forward type. In a Cut Through switch, the switch begins forwarding the frame immediately upon receiving the Destination Address. This results in a very low latency and is somewhat faster than a Store and Forward switch, as each frame is in the switch for less time. However, this scheme can propagate errors from one sub network to another, which

can result in bandwidth being wasted in the forwarding of invalid or damaged frames. Cut Through switches work best in networks which experience few errors.

Hybrid

A Hybrid switch is an attempt to get the best of both Store and Forward switches and Cut Through switches. A Hybrid switch normally operates in Cut Through mode, but constantly monitors the rate at which invalid or damaged frames are forwarded. If these errors occur at a frequency higher than a certain threshold value, the switch then stops operating as a Cut Through switch and begins operating like a Store and Forward unit. If the error rate drops back below the threshold, then the switch will again go into a Cut Through mode. This gives the performance advantage of Cut Through switches when error rates are low and the error trapping of Store and Forward switches when error rates are high.

DESIGNING A SWITCHED ETHERNET NETWORK

Designing a switched Ethernet network is actually a fairly straight forward process. The first step is to evaluate the traffic flow through you expect each user or group of users to generate. For example, if all of your application programs will reside on the file servers, then the network will experience a very heavy load as users start, use, and quit various programs. In such a case, you should limit as much as possible the number of users per switch port, and possibly consider connecting each user directly to a switch port.

Analysis of the network will most likely find that you have a large number of users who are not going to place a heavy load on the network, and a smaller number of users who will place a large load on the network. We now group the Undemanding Users together on a hub and connect each hub to a switch port. Our more demanding users will usually be either directly connected to the switch, or if they are on hubs, fewer of them will be sharing each switch port than on the Undemanding User portion.

Network Layer Protocols

The most significant protocol at layer 3 (also called the network layer) is the Internet Protocol, or IP. IP is the standard for routing packets across interconnected networks--hence, the name internet. It is an encapsulating protocol similar to the way Ethernet is an encapsulating protocol. If we view the original check as a unit of data needed to be sent, we now have two envelopes required to do the transmission--the check first goes into an IP envelope, and then the entire IP envelope (known as a *packet*) is placed into an Ethernet frame.

The most significant aspect of the IP protocol is the addressing: every IP packet includes the IP source address (where the packet is coming from) and the IP destination address (where the packet is heading to).

The network layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different

network, while maintaining the quality of service requested by the transport layer (in contrast to the data link layer which connects hosts within the same network). The network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer, sending data throughout the extended network and making the Internet possible.

The network layer may be divided into three sub layers:

1. Sub network access – that considers protocols that deal with the interface to networks, such as X.25;
2. Sub network-dependent convergence – when it is necessary to bring the level of a transit network up to the level of networks on either side
3. Sub network-independent convergence – handles transfer across multiple networks.

A number of layer-management protocols belong to the network layer. These include routing protocols. as follows.

ICMP

Internet Control Message Protocol

- A mechanism used by hosts and routers to send notification of datagram problems back to the sender.
- Sends error messages only to the source and not to intermediate routers.
- Sole function is to report problems not to correct them.
- An important use of ICMP is echo/reply to test whether a destination is reachable and responding
- Echo request/reply (PING- Packet Internet Gropher) Destination unreachable

IGMP

Internet Group Message Protocol

- Allows multi-cast operation- a message can be simultaneously received by a group of hosts
- Special type of Class-D IP addresses starting with 1110 are reserved as multicast addresses

ARP
Address Resolution Protocol

- Used to translate 32 bit IP address to 48 bit Ethernet Address (MAC Address)
- MAC(Media Access Control) address is the physical address of an Ethernet Interface which is unique
- The machine with matching IP address in broadcast message sends its hardware address to the machine originating broadcast

RARP
Reverse Address Resolution Protocol

- It is reverse of ARP

- Used to get the IP address corresponding to the 48 bit MAC address
- A diskless workstation broadcasts RARP request to find its IP address at the time of boot up

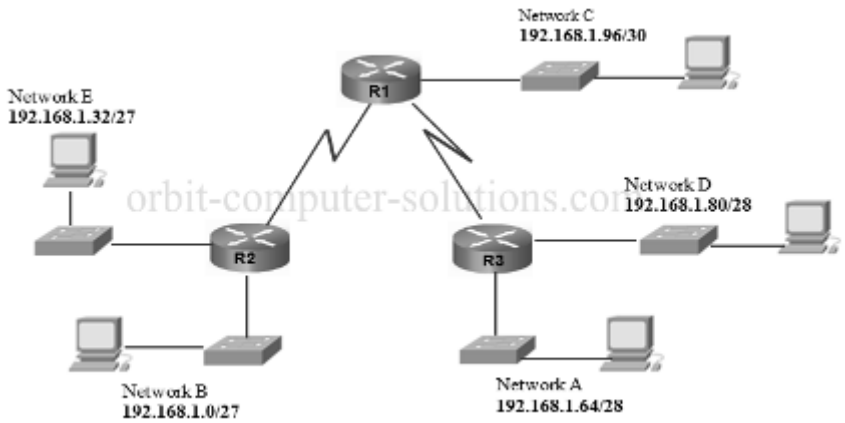
VLSM

VARIABLE LENGTH SUBNET MASK

Variable Length Subnet Masking - VLSM - is a technique that allows network administrators to divide an IP address space into subnets of different sizes, unlike simple same-size Subnetting.

Variable Length Subnet Mask (VLSM) in a way, means subnetting a subnet. To simplify further, VLSM is the breaking down of IP addresses into subnets (multiple levels) and allocating it according to the individual need on a network. It can also be called a classless IP addressing. A classful addressing follows the general rule that has been proven to amount to IP address wastage.

Before you can understand VLSM, you have to be very familiar with IP address structure. The best way you can learn how to subnet a subnet (VLSM) is with examples. Lets work with the diagram below:



Looking at the diagram, we have three LANs connected to each other with two WAN links. The first thing to look out for is the number of subnets and number of hosts. In this case, an ISP allocated 192.168.1.0/24. Class C

HQ = 50 host
RO1 = 30 hosts
RO2 = 10 hosts
2 WAN links

We will try and subnet 192.168.1.0 /24 to sooth this network which allows a total number of 254 hosts I recommend you get familiar with this table below. I never leave home without it!

Bit Value	128	64	32	16	8	4	2	1
Bits Borrowed	1	2	3	4	5	6	7	8
Subnet mask	128	192	224	240	248	252	254	255
Subnet Prefix /CIDR	/25	/26	/27	**/28**	/29	/30		

Let's begin with **HQ** with 50 hosts, using the table above:

We are borrowing 2 bits with value of 64. This is the closest we can get for 50 hosts.
HQ - 192.168.1.0 /26 Network address
HQ = **192.168.1.1** Gateway address
192.168.1.2, First usable address
192.168.1.62- Last usable address. Total address space -192.168.1.2 to 192.168.1.62
192.168.1.63 will be the broadcast address (remember to reserve the first and last address for the Network and Broadcast)
HQ **Network Mask 255.255.255.192** - we got the **192** by adding the bit value from the left to the value we borrowed = 128+64=192
HQ address will look like this 192.168.1.0 /26
RO1 = 30 hosts
We are borrowing 3 bits with value of 32; this again is the closest we can get to the number of host needed.
RO1 address will start from **192.168.1.64** - Network address
Now we add the 32 to the 64 we borrowed earlier = 32+64 = 96
RO1 = 192.168.1.65 Gateway address
192.168.1.66 - First usable IP address
192.168.1.94 - Last usable IP address
192.168.1.95 Broadcast address – total address space – 192.168.1.66 –192.168.1. 94
Network Mask 255.255.255.224 I.e. 128+64+32=224 or 192.168.1.64/27
RO2 = 192.168.1.96 Network address
We borrow 4 bits with the value of 16. That's the closest we can go.
96+16= 112
So, 192.168.1.97- Gateway address
192.168.1.98 - First usable address
192.168.1.110 - Last usable address
192.168.1.111 broadcast
Total host address space – 192.168.1.98 to 192.168.1.110
Network Mask 255.255.255.**240** or 192.168.1.96 /28
WAN links = we are borrowing 6 bit with value of 4
=**112 + 4 =116**
WAN links from HQ to RO1 Network address will be 192.168.1.112 /30 :
HQ se0/0 = 192.168.1.113
RO1 se0/0= 192.168.1.114
Mask for both links= 255.255.255.**252** (we got 252 by adding the bits value we borrowed i.e 124 +64 +32 +16+ 8 +4=252
WAN Link 2= 112+4=116
WAN Link from HQ to RO2 Network address = 192.168.1.116 /30
HQ = 192.168.1.117 subnet mask 255.255.255.252
RO2 = 192.168.1.118 Subnet mask 255.255.255.252

Subnet Prefix / CIDR	Subnet mask	Usable IP address/hosts	Usable IP addresses + Network and Broadcast address
26	255.255.255.192	62	64
27	255.255.255.224	30	32
28	255.255.255.240	14	16
29	255.255.255.248	6	8
30	255.255.255.252	2	4

As I mentioned earlier, having this table will prove very helpful. For example, if you have a subnet with 50 hosts then you can easily see from the table that you will need a block size of 64. For a subnet of 30 hosts you will need a block size of 32.

What is CIDR?

CIDR is a new addressing scheme for the Internet which allows for more efficient allocation of IP addresses than the old Class A, B, and C address scheme.

Why Do We Need CIDR?

With a new network being connected to the Internet every 30 minutes the Internet was faced with two critical problems:

- Running out of IP addresses
- Running out of capacity in the global routing tables

The mask of 255.255.255.224 can also be denoted as / 27 as there are 27 bit s that are set in the mask.
204.15.5.0/ 27

- This method is used with CIDR (Classless Inter domain Routing) protocol
- CIDR is a method to manage the available IP address space efficiently by eliminating the Classful IP addressing.
- Subnetting also reduces the load on a single router and its WAN link since different subnets are managed by different routers with their corresponding routing tables.
- This also lessens the burden of updating the external routing, saves routing table space in all backbone routers.

Running Out of IP Addresses
There is a maximum number of networks and hosts that can be assigned unique addresses using the Internet's 32-bit long addresses. Traditionally, the Internet assigned "classes" of addresses: Class A, Class B and Class C were the most common. Each address had two parts: one part to identify a unique network and the second part to identify a unique host in that network. Another way the old Class A, B, and C addresses were identified was by looking at the first 8 bits of the address and converting it to its decimal equivalent.

Address Class	# Network Bits	# Hosts Bits	Decimal Address Range
Class A	8 bits	24 bits	1-126
Class B	16 bits	16 bits	128-191
Class C	24 bits	8 bits	192-223

Using the old Class A, B, and C addressing scheme the Internet could support the following:

- 126 Class A networks that could include up to 16,777,214 hosts each
- Plus 65,000 Class B networks that could include up to 65,534 hosts each
- Plus over 2 million Class C networks that could include up to 254 hosts each

(Some addresses are reserved for broadcast messages, etc.). Because Internet addresses were generally only assigned in these three sizes, there was a lot of wasted addresses. For example, if you needed 100 addresses you would be assigned the smallest address (Class C), but that still meant 154 unused addresses. The overall result was that while the Internet was running out of unassigned addresses, only 3% of the assigned addresses were actually being used. CIDR was developed to be a much more efficient method of assigning addresses.

Restructuring IP Address Assignments

Classless Inter-Domain Routing (CIDR) is a replacement for the old process of assigning Class A, B and C addresses with a generalized network "prefix". Instead of being limited to network identifiers (or "prefixes") of 8, 16 or 24 bits, CIDR currently uses prefixes anywhere from 13 to 27 bits. Thus, blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts. This allows for address assignments that much more closely fit an organization's specific needs.

A CIDR address includes the standard 32-bit IP address and also information on how many bits are used for the network prefix. For example, in the CIDR address 206.13.01.48/25, the "/25" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.

CIDR Block Prefix	# Equivalent Class C	# of Host Addresses
/27	1/8th of a Class C	32 hosts
/26	1/4th of a Class C	64 hosts
/25	1/2 of a Class C	128 hosts
/24	1 Class C	256 hosts
/23	2 Class C	512 hosts
/22	4 Class C	1,024 hosts
/21	8 Class C	2,048 hosts
/20	16 Class C	4,096 hosts
/19	32 Class C	8,192 hosts
/18	64 Class C	16,384 hosts
/17	128 Class C	32,768 hosts
/16	256 Class C (= 1 Class B)	65,536 hosts
/15	512 Class C	131,072 hosts
/14	1,024 Class C	262,144 hosts
/13	2,048 Class C	524,288 hosts

Superneting is nothing but CIDR

• is just the reverse of subnets (which divides one single network into smaller networks. I .e. Sub networks)
• is an aggregation of IP network addresses advertised as a single classless network address
• enables optimum utilisation of IP address space
• while subnetting makes use of the host part of the IP address to create more subnets, Supernetting makes use of the network part of the IP address to aggregation. Supernetting allows use of multiple IP network on the same Interface.

Example of Supernetting

Consider the following four Class C network with IP nos.
220.78.168.0 11011100 01001110 10101000 00000000

220.78.169.0 11011100 01001110 10101001 00000000
220.78.170.0 11011100 01001110 10101010 00000000
220.78.171.0 11011100 01001110 10101011 00000000

- 22 bits of the network portion for all the above class C networks are the same which can be used for advertising through an aggregated network address viz. 220.78.168.0/ 22.
- The CIDR entry in the routing tables of the Internet routers becomes: 220.78.168.0 / 255.255.252.0

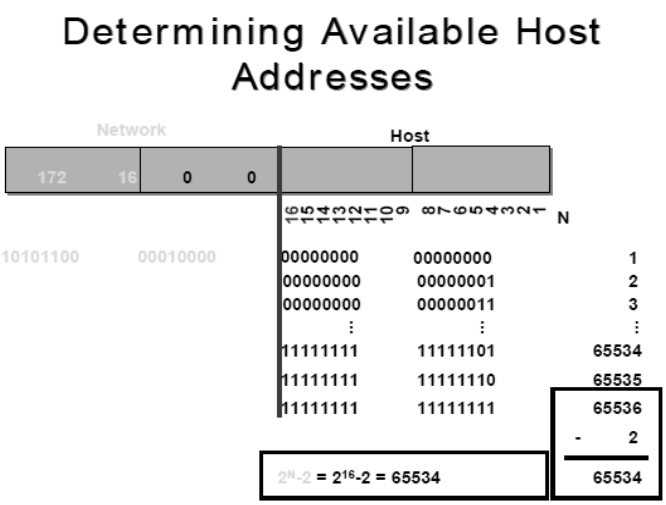
Decimal Equivalents of Bit Pat terns

128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	=0
1	0	0	0	0	0	0	0	=128
1	1	0	0	0	0	0	0	=192
1	1	1	0	0	0	0	0	=224
1	1	1	1	0	0	0	0	=240
1	1	1	1	1	0	0	0	=248
1	1	1	1	1	1	0	0	=252
1	1	1	1	1	1	1	0	=254
1	1	1	1	1	1	1	1	=255

Subnet Mask without Subnets

	Network		Host	
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000

Network Number	172	16	0	0



What is routing?

Routing is a core concept of the Internet and many other networks. Routing provides the means of forwarding logically addressed packets from their local sub network toward their ultimate destination. In large networks, packets may pass through many intermediary destinations before reaching their destination. Routing occurs at layer 3 of the OSI seven layer model.

Types of Routing

- **Static**
- **Dynamic**

Static Routing

- The router is configured manually
- The routing table is also updated manually

Dynamic routing

- Only the initial configuration is done manually for the directly connected links
- The routing protocol updates the routing table automatically.

Routing protocols

IGP (Interior Gateway Protocol)
IGRP/ EI GRP (Enhanced Interior Gateway Routing Protocol)
BGP (Border Gateway Protocol)

Routed versus Routing protocol

- **Routed protocol:** Any network protocol that provides enough information in it s network layer address to allow a packet to be forwarded from host to host ,based on the addressing scheme. Routed protocols define the format and use of the fields within a packet . Packet s generally are conveyed from end system to end system. IP is an example of a routed protocol.

- **Routing protocols:** facilitate the exchange of **routing information** between networks, allowing routers to build routing tables dynamically. Traditional IP routing stays simple because it uses **next -hop rout ing** where the router only needs to consider where it sends the packet , and does not need to consider the subsequent path of the packet on the remaining hops

BGP

- The Border Gateway Protocol (BGP) is an inter- Autonomous System routing protocol
- Border Gateway Protocol, a standard routing protocol, used primarily for routing between large, heterogenous networks with multiple gateways. BGB is defined in RFC 1771

IGP

- An IGP (Interior Gateway Protocol) is a protocol for exchanging routing information between gateway (hosts with routers) within an autonomous network (for example, a system of corporate local area networks) . The routing information can then be used by the Internet Protocol or other network protocols to specify how to route transmissions.
- There are two commonly used IGPs:
- the Routing Information Protocol (RIP) and
- The Open Shortest Path First (OSPF) protocol.

RIP (Routing Information Protocol)

The Routing Information Protocol, or RIP, as it is more commonly called, is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP- like routing protocols proliferated, some of which even used RIP and the myriad RIP- like protocols were based
on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address

OSPF (Open Shortest Path First)

OSPF is an internal gateway protocol; it is designed to be used internal to a single Autonomous System. OSPF uses link-state or SPF-based technology

Introduction

Open Shortest Path First (OSPF) routing protocol is a Link State protocol based on cost rather than hops or ticks (i.e. it is not a vector based routing protocol). As with RIPv2 different sized subnet masks can be used within the same network thereby allowing more efficient utilization of available address space. Also, OSPF supports unnumbered point to point links and equal cost multipath (or load balancing for up to 6 paths; meaning balancing the distribution of IP datagram's down parallel routes to the same destination router using a round robin or a direct addressing option).

Link State Advertisements

Because only link state advertisements are exchanged rather than complete network information (as in RIP), OSPF networks converge far more quickly than RIP networks. In

addition, Link State Advertisements are triggered by network changes (like the triggered updates in RIP). The Dijkstra's algorithm used to calculate the SPF tree is CPU intensive, therefore it is advisable to run it (the Soloist) on a router slot that either has a slow speed network attached or none at all.

The OSPF Process

The Link State Database (LSDB) contains the link state advertisements sent around the 'Area' and each router holds an identical copy of this LSDB. The router then creates a Shortest Path First (SPF) tree using Dijkstra's algorithm on the LSDB and a routing table can be derived from the SPF tree which now contains the best route to each router.

OSPF Networks

Within OSPF there can be Point-to-Point networks or Multi-Access networks. The Multi-Access networks could be one of the following:

Broadcast Network: A single message can be sent to all routers

Non-Broadcast Multi-Access (NBMA) Network: Has no broadcast ability, ISDN, ATM, Frame Relay and X.25 are examples of NBMA networks.

Point to Multipoint Network: Used in group mode Frame Relay networks.

Forming Adjacencies

Each router within an Area maintains an identical LSDB by maintaining communications with other routers by way of adjacencies. The formation of an adjacency occurs between two routers A and B that are in the initial **Down** state as follows:

1. **Init state:** Hello packets are exchanged between routers A and B, in order to form a **Neighbour Relationship**. Then based on these packets they decide whether or not to become adjacent. The Hello packet contains the router ID and the hello and dead intervals and is sent to the multicast address 224.0.0.5. In multi-access networks the hellos are sent every 10 seconds. The **Dead Interval** is normally 4 times the Hello interval and is the time waited before the router declares the neighbour to be down. The Hello packet also contains the router ID is 32 bits and is normally the highest IP on the interface of the router or the loopback address if that is configured. Bi-directional communication is confirmed when the routers see each other in each other's hello packet. The **Router Priority** and the DR/BDR addresses are also included and the routers have to agree the **Stub Area Flag** and the **Authentication Password**.

2. **Two-way state:** The routers add each other to their Neighbour (Adjacencies) database and they become neighbours.

3. **DR and BDR Election:**

Initially, on forming an adjacency, the router with the highest **Router Priority** (information held within the 'hello' packet) becomes the DR, or the router with the highest router ID (highest IP address or the loopback interface address). The router with the next highest ID becomes the BDR. The BDR just receives the same information as the DR but only performs

the task of a DR when the DR fails. The BDR still maintains adjacencies with all routers. In a hub and spoke environment it is necessary to set all the spoke router priorities to '0' so that they never can become the DR or BDR and therefore become isolated from the other routers.

If a router with a higher priority is added to the network later on it does NOT take over the DR and no re-election takes place. It is possible for a router to be a DR in one network and a normal router in another at the same time.

4. After election the routers are in the **Exstart** state as the DR and BDR create an adjacency with each other and the router with the highest priority acts as the master and they begin creating their link-state databases using Database Description Packets.

5. The process of discovering routes by exchanging **Database Description Packets (DBD)** is known as **Exchange**. These packets contain details such as the link-state type, the address of the advertising router, the cost of the link and the sequence number that identifies how recent the link information is. Unicasts are used to compare LSDBs to see which Link State Advertisements (LSAs) are missing or out of date.

6. **Link State ACK:** Once a DBD has been received a Link State ACK is sent containing the link-state entry sequence number. The slave router compares the information and if it is newer it sends a request to update.

7. **Link State Request:** In order to update its LSDB the slave router sends a Link State Request. This is known as the **Loading** state.

8. **Link State Update:** A Link State Update is sent in response to a Link State Request and it contains the requested LSAs.

9. **Link State ACK:** Once a Link State Update has been received a Link State ACK is sent again and the adjacency has been formed. At this point the databases are considered to be synchronous.

10. **Full:** In the Full state the routers can route traffic and the routers continue sending each other hello packets in order to maintain the adjacency and the routing information.

Maintaining the Routing Tables

Point-to-Point and Point-to-Multipoint links do not require a Designated Router (DR) or a Backup Designated Router (BDR) because adjacencies have to form with each other anyway. On a Point-to-Point and Point-to-Multipoint networks adjacencies are always formed between the two routers so there is no requirement for a DR or BDR, whilst on a multi-access network a router will form an adjacency with the Designated Router (DR) and the Backup Designated Router (BDR). In a broadcast or NBMA network it is not feasible for every router to form a full mesh of adjacencies with all the other routers. The Designated Router forms adjacencies with each of the other routers and performs the link-state information exchange thereby minimising the traffic load and making sure that the information is consistent across the network.

On detection of a link state, the OSPF router sends a Link State Update (LSU) to the multicast address 224.0.0.6 which is all the OSPF DR/BDRs. The LSU contains several

LSAs. After acknowledging the LSU the DR **Floods** link-state information to all the OSPF routers on the OSPF multicast address 224.0.0.5. Each LSA is acknowledged separately with a **LSAck** if the LSA is new and therefore added to the Link State Database, otherwise the LSA is ignored. Rather than each router having to form an adjacency with each other router this significantly cuts down on the amount of traffic. DRs in other networks that are connected also receive the LSUs. On receipt of the new LSA the routers recalculate their routing tables.

The LSA has a 30 minute timer that causes the router to send an LSU to everyone on the network once it ages out. This verifies that the link is still valid. If a router receives an LSA with old information then it will send a LSU to the sender to update the sender with the newer information.

Important Parameters

The **Retransmit Interval** is the number of seconds between LSAs across an adjacency. The following settings are often recommended:

Broadcast network	5 seconds
Point-to-Point network	10 seconds
NBMA network	10 seconds
Point-to Multipoint network	10 seconds

The **Hello Interval** must be the same on each end of the adjacency otherwise the adjacency will not form. In a Point-to-Point network this value is 10 seconds whereas in a Non Broadcast Multiaccess Network (NBMA) the Hello Interval is 30 seconds.

The **Dead Interval** is 40 seconds in a Point-to-Point network and 120 seconds in a Non Broadcast Multiaccess Network (NBMA).

The **Metric Cost** can be related to line speed by using the formula **10^8 / line speed (bps)**

The following table gives some guidelines for costs:

Network Type	**Cost**
FDDI/Fast Ethernet	1

Token Ring (16Mbps)	6
Ethernet	10
E1	48
T1	64
64 kb/s	1562
56 kb/s	1785

These costs are used to calculate the metric for a line and thus determine the best route for traffic. The lowest cost to a destination is calculated using **Dijkstras Algorithm**. The lowest cost link is used unless there are multiple equally low cost links in which case load balancing takes place between up to 6 route entries.

RFC 2328 describes Dijkstras Algorithm (also called the **Shortest Path First (SPF)** algorithm.

OSPF has a 5 second damper in case a link flaps. A link change will cause an update to be sent only after 5 seconds has elapsed so preventing routers locking up due to continually running the SPF algorithm and never allowing OSPF to converge. There is also a timer that determines the minimum time between SPF calculations, the default for this is often 10 seconds.

A **Password** can be enabled on a per Area basis so providing some form of security and consistency in route information.

Types of Multi-access networks

As mentioned earlier these are typically Frame Relay, ATM or X.25 networks that have no broadcast capability but have many routers connected. There are three types:

Hub and Spoke - a central router has links to other routers in a star arrangement. A spoke can only talk to other spokes via the hub.

Full Mesh - each router has a link to every other router providing full resilience.

Partial Mesh - not all routers have links to the central site.

Point-to-Point and **Multipoint-to-Point** networks have no need for DR/BDRs and form adjacencies with their neighbours automatically and quickly without the need for static neighbours being configured.

In a hub-spoke network operating in **Broadcast mode** the DR really needs to be the hub router in order for it to maintain contact with all the routers. It is therefore important to make sure that none of the other routers can become the DR by setting their interface priorities to 0 or raising the hub router's interface priority to be the highest.

The **Non-Broadcast Multi-Access (NBMA)** network has all the router interfaces in the same subnet, in addition the neighbours have to be statically defined because there is no facility for broadcasts. You can also configure sub-interfaces to allow separate subnets and therefore separate NBMA networks to exist.

Rather than use a NBMA network where you have to statically configure the neighbours you can configure a Point-to-Multipoint network for Partial Mesh networks. In this case there is no DR and each link is treated as a separate Point-to-Point. A Point-to-Multipoint network can exist in one subnet.

There are some Point-to-Multipoint networks such as **Classic IP over ATM** that do not support broadcasts. For these networks you can configure a **Point-to-Multipoint Non-broadcast mode** that requires the configuration of static neighbours since they cannot be discovered dynamically.

OSPF Packet Types

Within the OSPF header the packet type is indicated by way of a type code as follows:

Type Code	Packet Type
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

OSPF Areas

Within a network multiple Areas can be created to help ease CPU use in SPF calculations, memory use and the number of LSAs being transmitted. 60-80 routers are considered to be the maximum to have in one area. The Areas are defined on the routers and then interfaces are assigned to the areas. The default area is 0.0.0.0 and should exist even if there is only one area in the whole network (which is the default situation). As more areas are added,

0.0.0.0 becomes the 'backbone area'. In fact, if you have one area on its own then it could be configured with a different area number than 0 and OSPF will still operate correctly, but this should really be a temporary arrangement. You may for instance, want to set up separate areas initially that are to be joined at a later date. Separate LSDBs are maintained one per area and networks outside of an area are advertised into that area, routers internal to an area have less work to do as only topology changes within an area affect a modification of the SPF specific to that area. Another benefit of implementing areas is that networks within an area can be advertised as a summary so reducing the size of the routing table and the processing on routers external to this area. Creating summaries is made easier if addresses within an area are contiguous.

In a multiple area environment there are four types of router:

Internal router: All its directly connected networks are within the same area as itself. It is only concerned with the LSDB for that area.

Area Border Router: This has interfaces in multiple areas and so has to maintain multiple LSDBs as well as be connected to the backbone. It sends and receives Summary Links Advertisements from the backbone area and they describe one network or a range of networks within the area.

Backbone Router: This has an interface connected to the backbone.

AS Boundary Routers: This has an interface connected to a non-OSPF network which is considered to be outside its Autonomous System (AS). The router holds AS external routes which are advertised throughout the OSPF network and each router within the OSPF network knows the path to each ASBR.

A RIP network will look at any IP address within an OSPF network as only one hop away.

When configuring an area, **authentication** can be configured with a password which must be the same on a given network but (as in RIPv2) can be different for different interfaces on the same router.

There are seven types of Link State Advertisements (LSAs):

Type 1: Router Links Advertisements are passed within an area by all OSPF routers and describe the router links to the network. These are only flooded within a particular area.

Type 2: Network Links Advertisements are flooded within an area by the DR and describes a multi-access network, i.e. the routers attached to particular networks.

Type 3: Summary Link Advertisements are passed between areas by ABRs and describes networks within an area.

Type 4: AS (Autonomous System) Summary Link Advertisements are passed between areas and describe the path to the AS Boundary Router (ASBR). These do not get flooded into Totally Stubby Areas.

Type 5: AS External Link Advertisements are passed between and flooded into areas by ASBRs and describe external destinations outside the Autonomous System. The areas that do not receive these are Stub, Totally Stubby and Not So Stubby areas. There are two types of External Link Advertisements, Type 1 and Type 2. Type 1 packets add the external cost to the internal cost of each link passed. This is useful when there are multiple ASBRs advertising the same route into an area as you can decide a preferred route. Type 2 packets only have an external cost assigned so is fine for a single ASBR advertising an external route.

Type 6: Multicast OSPF routers flood this Group Membership Link Entry.

Type 7: NSSA AS external routes flooded by the ASBR. The ABR converts these into Type 5 LSAs before flooding them into the Backbone. The difference between Type 7 and Type 5 LSAs is that Type 5s are flooded into multiple areas whereas Type 7s are only flooded into NSSAs.

Stub Area

A stub area is an area which is out on a limb with no routers or areas beyond it. A stub area is configured to prevent AS External Link Advertisements (Type 5) being flooded into the Stub area. The benefits of configuring a Stub area are that the size of the LSDB is reduced along with the routing table and less CPU cycles are used to process LSA's. Any router wanting access to a network outside the area sends the packets to the default route (0.0.0.0).

Totally Stubby Area

This is a Stub Area with the addition that Summary Link Advertisements (Type 3/4) are not sent into the area, as well as External routes, a default route is advertised instead.

Not So Stubby Area (NSSA)

This area accepts Type 7 LSAs which are external route advertisements like Type 5s but they are only flooded within the NSSA. This is used by an ISP when connecting to a branch office running an IGP. Normally this would have to be a standard area since a stub area would not import the external routes. If it was a standard area linking the ISP to the branch office then the ISP would receive all the Type 5 LSAs from the branch which it does not want. Because Type 7 LSAs are only flooded to the NSSA the ISP is saved from the external routes whereas the NSSA can still receive them.

The NSSA is effectively a 'No-Mans Land' between two politically disparate organisations and is a hybrid stubby area. Over a slow link between the two organisations you would not normally configure OSPF because the Type 5 LSAs would overwhelm the link, so redistribution across RIP would be common. With NSSA, OSPF can still be maintained but by using less intensive Type 7 LSAs.

RFC 1587 describes the Not So Stubby Area.

Virtual Links

If an area has been added to an OSPF network and it is not possible to connect it directly to the backbone or two organisations that both have a backbone area have merged, then a virtual link is required. The link must connect two routers within a common area called a **Transit Area** and one of these routers must be connected to the backbone. A good example of its use could be when two organisations merge and two Area 0s must be connected i.e. 'patching the backbone'.

Virtual links cannot be used to patch together a split area that is not the backbone area. Instead a tunnel must be used, the IP address of which is in one of the areas.

External Routes

In order to make non-OSPF networks available to routers within an OSPF network, the router connected to the non-OSPF network needs to be configured as an AS Boundary Router (ASBR). As described earlier AS External Link Advertisements (one for each external route) are flooded into the OSPF network (except Stub networks). There are two types of metric for external detinations:

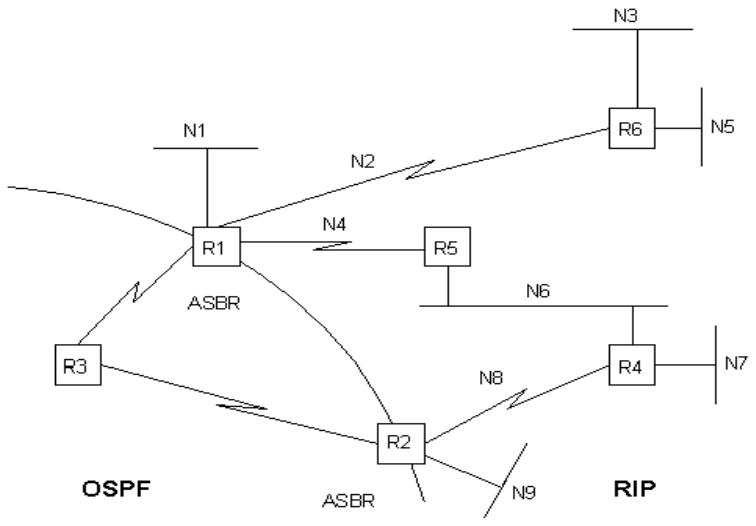
Type-1 destination networks: The cost to an external network directly connected to the ASBR (close) plus the internal path cost within the OSPF network gives the total cost.

Type-2 destination networks: The cost to a 'far away' network (i.e. not directly connected to the ASBR) is merely the number of hops from the ASBR to the external network.

If a number of routes to a network are advertised to an internal OSPF router, then the router picks the Type-1 route rather than the Type-2 route. If this router learns the route via different protocols then it decides which route to use based on firstly the **preference value** (configurable) and then on **route weight** (non-configurable).

OSPF Accept Policies

These can only be configured for external routes (Type-1 and Type-2) and can be set up on any router. Consider the following network:



An OSPF Accept Policy can be configured on R3 to prohibit R3 from forwarding IP datagrams to N1. N1 is learned as a Type-1 external route from R1 (since N1 is directly connected to R1 which is an ASBR) but N1 is also learned as a Type-2 external route from R2 (since N1 is now several networks away from R2). Because the routing table in R3 sees N1 as a Type-1 or Type-2 external route, an Accept Policy can be created to exclude these networks from R3's routing table, however other routers within the OSPF domain can still learn about N1 unless Accept Policies are also configured on these.

OSPF Announce Policies

Unlike OSPF Accept Policies, the OSPF Announce Policies can only be configured on an ASBR since they determine which Type-1 and Type-2 external routes are advertised into the OSPF domain. Referring to Fig. 25c:

We want traffic from R3 to N6 to be routed via R2, and if R2 goes down then the traffic to go via R1. R3 learns about N6 after receiving Type-2 external LSAs from R2 and R1, the metric being 2. To force traffic through R2 we can create an announce policy on R1 that advertises N6 with a metric of 3.

Important parameters for both Accept and Announce Policies are **Name** (of Policy - this needs to describe what it actually does), **precedence** (out of a number of policies created, the one with the highest metric takes precedence) and **route source** (hexadecimal values indicating the non-OSPF protocols contributing to the route).

Just a final note to say that some items shown on the OSPF Announce Policy screen only actually apply to RIP Policies, the software has been lazily written.

The achilles heel of OSPF is that all areas are connected to the backbone area. This limits the number of routers that can take part in OSPF to about 1000. The protocol Intermediate System to Intermediate System (IS-IS) is designed to be more scalable than OSPF.

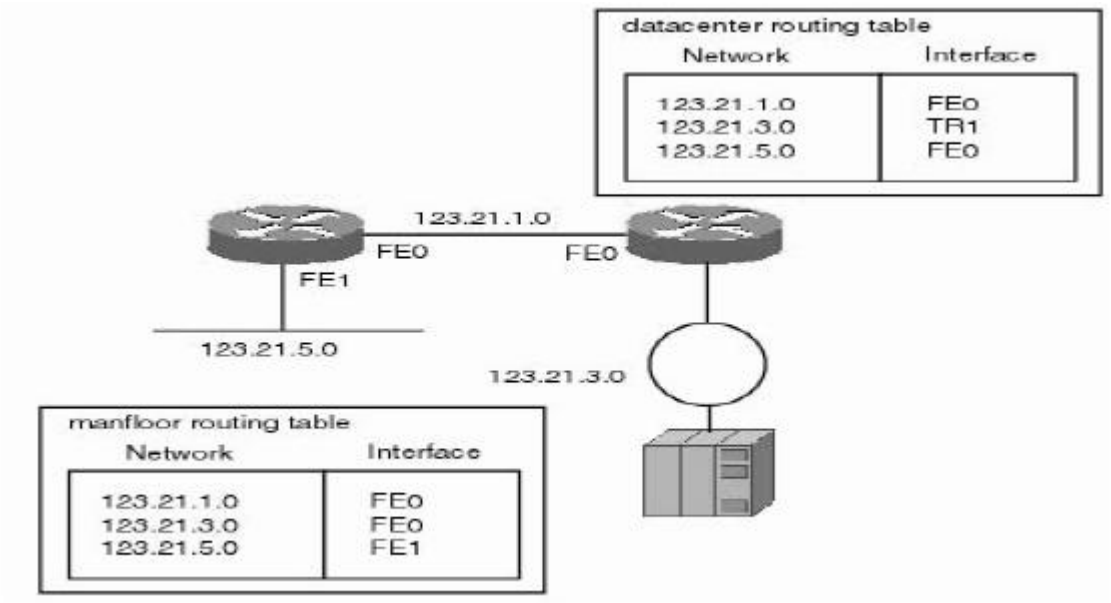
I GRP/ EI GRP

I GRP (Interior Gateway Routing Protocol)
A proprietary IGP used by Cisco Systems' routers.
EI GRP (Enhanced Interior Gateway Routing Protocol)
Advanced version of IGRP developed by Cisco

TCP/ IP Routed Protocols

- TCP/ IP Routed Protocols include information on ICMP (Internet Control Message Protocol) , IP(Internet Protocol v4) ,
- TCP(Transport Cont rol Protocol) , UDP(User Datagram Protocol) , Telnet , etc.

Routing Tables



IANA

(Internet Assigned Number Authority)

The IANA's role is to allocate IP addresses from the pools of unallocated addresses to the four RIRs (Regional Internet Registry) according to their established needs. When an RIR requires more IP addresses for allocation or assignment within its region, the IANA makes an additional allocation to the RIR.

RIRs

1.APNIC (Asia Pacific Network Information Cent re) - Asia/ Pacific Region
2.ARIN (American Registry for Internet Numbers) -North America and Sub-Sahara Africa
3.LACNIC (Regional Lat in-American and Caribbean IP Address Registry)
–Lat in America and some Caribbean Islands
4.RIPE NCC (Réseaux IP Européens)
-Europe, the Middle East , Cent ral Asia, and African countries located north of the equator

How to obtain IP number

Users are assigned IP addresses by Internet service providers (ISPs) .
ISPs obtain allocations of IP addresses from a local Internet registry (LIR) or national Internet registry (NIR) , or from their appropriate Regional Internet Registry (RIR) :

Sharing of Network resource

In computing, a **shared resource** or **network share** is a device or piece of information on a computer that can be remotely accessed from another computer, typically via a local area network or an enterprise Intranet, transparently as if it were a resource in the local machine.

Examples are **shared file access** (also known as *disk sharing* and *folder sharing*), **shared printer access** (*printer sharing*), **shared scanner access**, etc. The shared resource is called a *shared disk* (also known as mounted disk), *shared drive volume*, *shared folder*, *shared file*, *shared document*, *shared printer* or *shared scanner*.

The term **file sharing** traditionally means shared file access, especially in the context of operating systems and LAN and Intranet services, for example in Microsoft Windows

documentation. Though, as BitTorrent and similar applications became available in the early 2000's, the term **file sharing** increasingly has become associated with peer-to-peer file sharing over the Internet.

Contents

1 Common file systems and protocols
2 Naming convention and mapping
3 Security issues
4 Workgroup topology or centralized server
5 Difference from file transfer

Common file systems and protocols

Shared file and printer access require an operating system on the client that supports access to resources on a server, an operating system on the server that supports access to its resources from a client, and an application layer (in the four or five layer TCP/IP reference model) file sharing protocol and transport layer protocol to provide that shared access. Modern operating systems for personal computers include distributed file systems that support file sharing, while hand-held computing devices sometimes require additional software for shared file access.

The most common such file systems and protocols are:

Primary operating system	Application protocol	Transport protocol
Mac OS	Apple Filing Protocol	• TCP, • UDP or • AppleTalk
Unix-like systems	Network File System (NFS), SMB	• TCP or • UDP
MS-DOS, Windows	SMB, also known as CIFS	• TCP, • NBT (includes UDP), • NBF, or • other NetBIOS transports
Novell NetWare (server) MS-DOS, Windows (client)	• NCP and • SAP	• SPX (over IPX), or • TCP

The "primary operating system" is the operating system on which the file sharing protocol in question is most commonly used.

On Microsoft Windows, a network share is provided by the Windows network component "File and Printer Sharing for Microsoft Networks", using Microsoft's SMB (Server Message Block) protocol. Other operating systems might also implement that protocol; for example, Samba is an SMB server running on Unix-like operating systems and some other non-MS-DOS/non-Windows operating systems such as OpenVMS. Samba can be used to create

network shares which can be accessed, using SMB, from computers running Microsoft Windows. An alternative approach is a shared disk file system, where each computer has access to the "native" filesystem on a shared disk drive.

Shared resource access can also be implemented with Web-based Distributed Authoring and Versioning (WebDAV).

Naming convention and mapping

The share can be accessed by client computers through some naming convention, such as UNC (Universal Naming Convention) used on DOS and Windows PC computers. This implies that a network share can be addressed according to the following:

\\ServerComputerName\ShareName

Where Server Computer Name is the WINS name, DNS name or IP address of the server computer, and Share Name may be a folder or file name, or its path. The shared folder can also be given a Share Name that is different from the folder local name at the server side. For example \\server\c$ usually denotes a drive with drive letter C: on a Windows machine.

A shared drive or folder is often mapped at the client PC computer, meaning that it is assigned a drive letter on the local PC computer. For example, the drive letter H: is typically used for the user home directory on a central file server.

Security issues

A network share can become a security liability when access to the shared files is gained (often by devious means) by those who should not have access to them. Many computer worms have spread through network shares. Network shares would consume extensive communication capacity in non-broadband network access. Because of that, shared printer and file access is normally prohibited in firewalls from computers outside the local area network or enterprise Intranet. However, by means of virtual private networks (VPN), shared resources can securely be made available for certified users outside the local network.

A network share is typically made accessible to other users by marking any folder or file as shared, or by changing the file system permissions or access rights in the properties of the folder. For example, a file or folder may be accessible only to one user (the owner), to system administrators, to a certain group of users to public, i.e. to all logged in users. The exact procedure varies by platform.

In operating system editions for homes and small offices, there may be a special *pre-shared folder* that is accessible to all users with a user account and password on the local computer. Network access to the pre-shared folder can be turned on. In the Windows XP Home Edition operating system, english version, the pre shared folder is named *Shared documents*, typically with the path C:\Documents and Settings\All users\Shared documents. In Windows Vista and Windows 7, the pre-shared folder is named public documents, typically with the path C:\Users\Public\Public documents.

Workgroup topology or centralized server

In home and small office networks, a decentralized approach is often used, where every user may make their local folders and printers available to others. This approach is sometimes denoted a Workgroup or peer-to-peer network topology, since the same computer may be used as client as well as server.

In large enterprise networks, a centralized file server or print server, sometimes denoted client–server paradigm, is typically used. A client process on the local user computer takes the initiative to start the communication, while a server process on the file server or print server remote computer passively waits for requests to start a communication session

In very large networks, a Storage Area Network (SAN) approach may be used.

Online storage on a server outside the local network is currently an option, especialy for homes and small office networks.

Transport Layer Protocol

WHAT IS TCP? (Transmission Control Protocol)

- Receives data from the upper layers (application layers)
- Segments the data and sends it to the lower layer (Network layer)
- Responsible for Connection oriented reliable host to host transmission.

TCP Functions

- Provides application programs access to the network using a reliable connection-oriented transport layer service
- It is a byte oriented protocol. Every byte in each packet is assigned a sequence number
- Sequence numbers are used to determine the ordering or data in the packet and to find the missing packets.
- TCP divides the data stream into segments for transmission to remote network.
- Segment size can go up to 65535 bytes
- Originating TCP retains a copy of the transmitted data until it receives an acknowledgement from the destination TCP.
- If no acknowledgement is received within a specified time, data is retransmitted.
- TCP will time out after a number of unsuccessful retransmissions.
- Establish a connection, 3-way handshake between both ends before transmitting data
- Once transmission is established TCP's main job is to transfer data by maintaining the connection by exchanging sequence numbers and acknowledgements.
- Ends transmission by smoothly terminating the connection.
- Flow control of data using window size in TCP header.
- Can run a number of applications using the same transport by multiplexing through port numbers

Protocols at various layers of a TCP / IP Network

Application	HTTP,FTP,POP3,SPTP,SNMP,DNS,TELNET
Transport	TCP,UDP
Network	IP,ICMP,IGMP
Data Link	ETHERNET,TOKEN RING
Physical	T1/E1

Upper layer protocols of TCP

•**FTP** File Transfer Protocol which enables uploading and downloading of files between hosts on the network

• **HTTP** Hyper Text Transfer Protocol enables transfer of web pages from Web Server to Web Clients

• **SMTP** -Simple Mail Transfer Protocol enables to send mail between user in the network

• **Telnet**- Enables to login into a remote server on the network

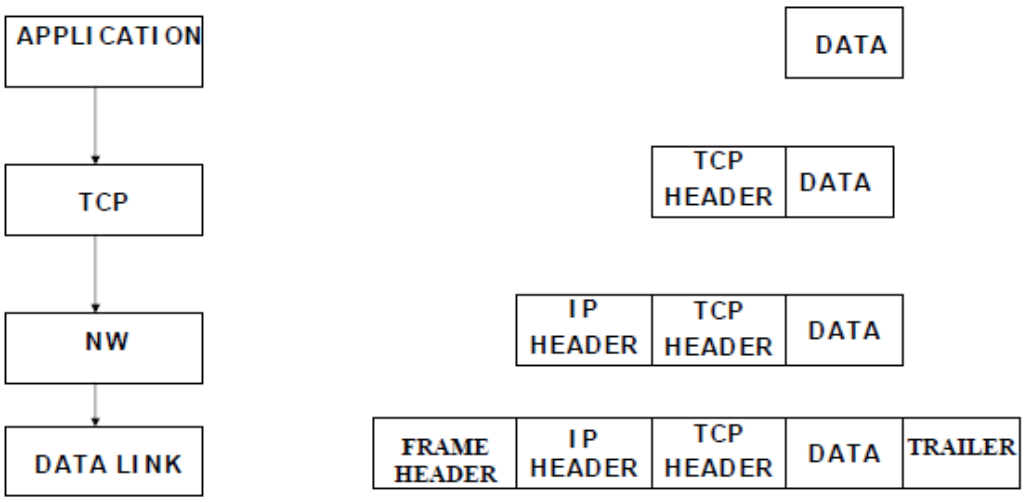
UDP (User Datagram Protocol)

- User Datagram Protocol
- A transport layer protocol
- An unreliable connection-less protocol
- Transfers data without establishing a session
- Used for services that have in-built reliability
- Does not use end to end error checking and correction
- Does not order the packets
- May loose or duplicate a packet
- Runs faster than TCP due to less overheads

Upper Layer protocols of UDP

- **TFTP**-Trivial File Transfer Protocol provides simplex file transfer for network booting devices.
- **NFS**-Network File System enables sharing directories between hosts on the network.
- **DNS**-Domain Name Service provides mapping between domain name and IP address and vice versa
- **SNMP**-Simple Network Management Protocol provides network management services

TCP/IP DATA ENCAPSULATION



Port Numbers

- TCP & UDP provides a concept of ports to identify a unique application in the machine
- Source port is randomly generated by the source machine
- Numbers ranging from 0 to 65535 can be defined for port numbers
- The first 1024 ports (0 to 1023) are assigned for standard applications by IANA

TCP Ports

Port Number Description

1. File Transfer Protocol
2. File Transfer Control

- 23 Telnet
- 25 SMTP
- 53 DNS
- 69 TFTP
- 80 WWW(HTTP)
- 110 POP3

TCP DATA TRANSFER

- For each byte of data sent, the sequence number increments by one
- Each sequence sent must be acknowledged
- Multiple sequence can be acknowledged
- Acknowledgment number= Sequence number+ Number of bytes successfully received+ 1
- Process is full duplex for each end of communication maintains its own sequence numbers for the other side

Information formats

Common information formats include

Format	Source & Destination Entities

- Frame : Data Link Layer
- Packet : Network Layer using Connection oriented Service
- Datagram : Network Layer using Connectionless service
- Segment : Tran sport Layer
- Message : Above Network Layer(Often Application)
- Cell : Data Link Layer in ATM

IP ADDRESSING & SUBNETTING

Why addressing?

- Addressing is the prime requirement of communication.
- Host machines of the Internet is identified by the users by their URL(Uniform Resource Locator) Eg: http://www.microsoft.com
- But routers can understand only numbers (that too binary) expressed as IP(Internet Protocol) address.
- Like 207.46.130.108 (Corresponding to microsoft.com)

IP Numbers

An IP address is a 32-bit identifier assigned to a host that uses the Internet Protocol. The I P address is represented by four octets (8bit fields). In decimal form, an IP address consists of four fields separated by dots, where each field contains a value in the range 0 - 255. This is called dotted decimal notation

Binary v/s Dotted decimal

An Internet Protocol version 4 address consists of four bytes (32 bits). These bytes are also known as octets. For readability purposes, humans typically work with IP addresses in a decimal notation that uses periods to separate each octet. For example, the IP address
00001010 00000000 00000000 00000001
usually appears in the equivalent **dotted decimal** representation
10.0.0.1

IP Address Space

Because each byte is 8 bits in length, each octet in an IP address ranges in value from a minimum of 0 to a maximum of 255.
Therefore, the full range of IP addresses is from
through 255.255.255.255.
That represents a total of 4,294,967,296 possible IP addresses.
This entire range of IP addresses is known as IP address space.

Loop Back Address

As with broadcast, I P officially reserves the entire range from **127.0.0.0** through **127.255.255.255** for loopback purposes.
1 27.0.0.1 is the **loopback** address in IP.
Loopback is a test mechanism of network adapters.
Messages sent to 127.0.0.1 do not get delivered to the network. Instead, the adapter intercepts all loopback messages and returns them to the sending application.
I P applications often use this feature to test the behavior of their network interface.

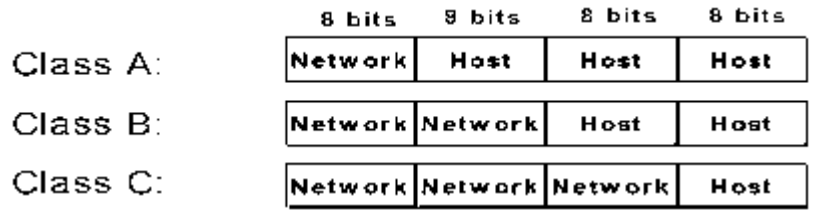
IP Version 6

IP addressing changes significantly with IPv6. IPv6 addresses are 16 bytes (128 bits) long rather than four bytes (32 bits). That represents m ore than
300,000,000,000,000,000,000,000,000,000,0
00,0 0 0,0 0 0 ($3x10^{38}$)
possible addresses! In the coming years, as an increasing number of cell phones, PDAs, and other network appliances expand their networking capability, this much larger IPv6 address space will probably be necessary.
IPv6 addresses are generally written in the following form:
-hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh
Each h in hexadecimals
In this notation, pairs of IPv6 bytes are separated by a colon and each byte in turns is represented as an equivalent pair of **hexadecimal** numbers. Eg.
E3D7:0000:0000:0000:51F4:9BC8:C0A8:6420
IPv6 does not use classes
IPv6 reserves just two special addresses: 0:0:0:0:0:0:0:0 and 0:0:0:0:0:0:0:1.
IPv6 uses 0:0:0:0:0:0:0:0 internal to the protocol implementation, so nodes cannot use it for their own communication purposes. IPv6 uses 0: 0: 0: 0: 0: 0: 0: 1 as its loopback address, equivalent to 127.0.0.1 in IPv4.

Unique Identity

Each host ID must be unique within a given network, and each network number must be u n iqu e with in a given in tern et. Host I Ds are assigned by the network administrator. The network number is assigned by the inter-network administrator. For a public network on the I nternet, you must obtain a network number assigned by the Network Information Center (NI C).
An IP address consists of two parts. The first part of the address, called the network number, identifies a network on the internet; the remainder, called the host ID, identifies an individual host on that network

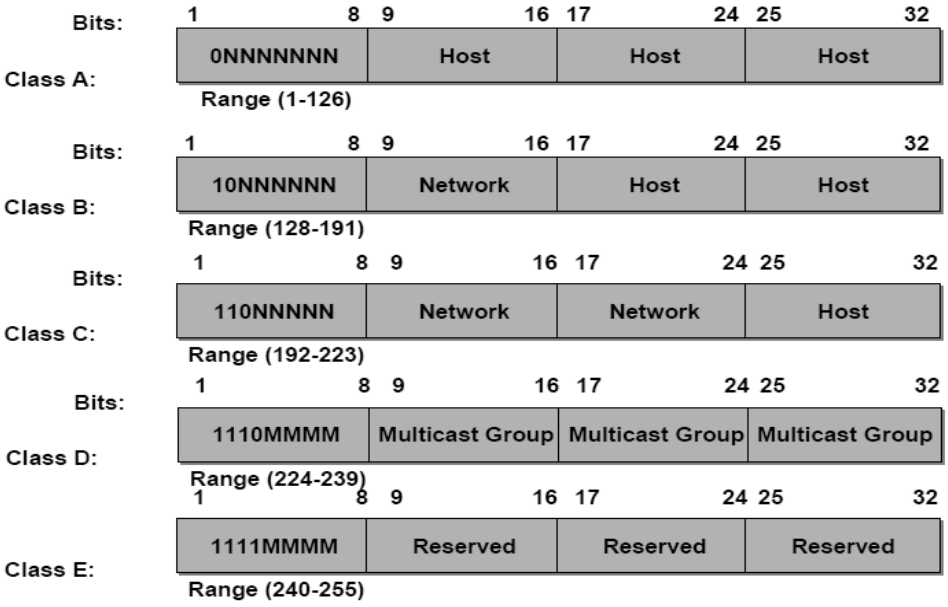
IP Address Classes



Class D: Multicast

Class E: Research

IP Address Classes



Some Examples

Class A
26.4.0.1, for host 4.0.1 on net number 26.
Class B
128.89.0.26, for host 0.26 on net 128.89.
Class C
192.15.28.16, for host 16 on net 192.15.28

Private IP addresses

The IP standard defines specific address ranges within Class A, Class B, and Class C reserved for use by pr ivate networks (int ranets).The table below lists these reserved ranges of the IP address space.

Class	Private start address	Private finish address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

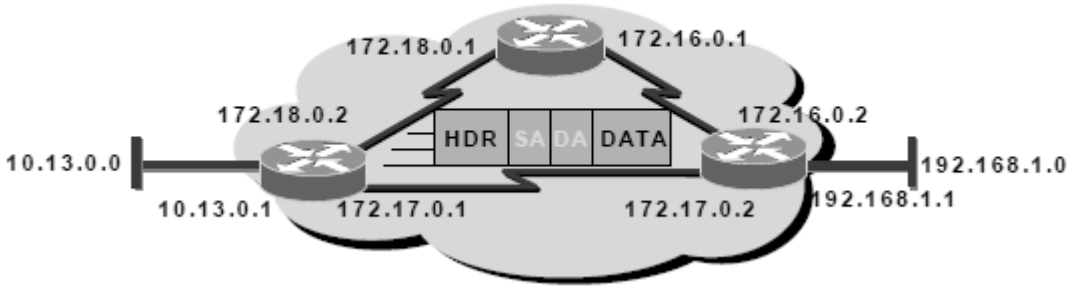
Address Masks

An address mask determines which port ion of an IP address ident ifies the network and which portion identifies the host . Like the IP address, the mask is represented by four octets.
Eg: For a Class C network the mask is
255.255.255.0
This means that the first three octets represent Network address the last one represent the host .
Mask is used to mask (hide) the host address i.e. the last octet.

Network ID using subnet mask

• When the IP address is ANDed with the mask the last octet disappears since it is all 0s.Thus the network address can be obtained
• 192.168.202.12 IP address of Host
• 255.255.255.0 Subnet Mask of Host
• 192.168.202.0 Network ID

IP Addresses



–Unique addressing allows communication between end stat ions
–Path choice is based on destination address

Network Masks

A network mask helps you know which port ion of the address identifies the network and which port ion of the address identifies the node. Class A, B, and C networks have default masks, also known as natural masks, as shown here:
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

- By using a mask the router can ignore the part of the host address. It needs to work only in network address.
- An IP address on a Class A network that has not been would have an address/mask pair similar to: 8.20.15.1/ 255.0.0.0.

The binary representation is as given below

8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
- -
net id | host id

when the IP address is 'AND' operated to the Mask the result is the network address. The remaining 3 octets form the host address
net id = 00001000 = 8
host id = 00010100.00001111.00000001 = 20.15.1

Broadcast domain

A **broadcast domain** is a logical area in a computer network where any computer connected to the computer network can direct ly t ransmit to any other in the domain without having to go through a rout ing device.

- Class A networks have a broadcast domain of 16million (224) hosts
- Class B networks have a broadcast domain of 64K(216) hosts

Problems with the Classful IP address

- A range of bits is applied to an address , most of which are wasted
- Having 16777214 hosts for Class-A and 254 hosts for Class-C were not working well

- Every IP address requires one entry in the routing table Addresses were arbitrarily handed out without regard to geographic location
- Class C addresses were overtaxing the internet routing tables.
- Class stopped being handed out and Class-B was exhausted

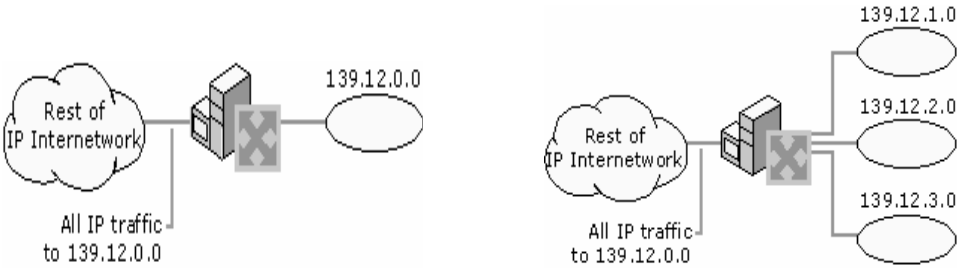
Solution to optimum use of IP address space

- Creation of subnets by allowing to use some of the bits normally used by the host portion of the address to the network portion of the address.
- The format of the subnet ted IP address would be < Network Number, Subnet Number ,Host Number>
- This method uses the full network address efficiently
- Provides for another hierarchy of rout ing
- Subnet is a real network under a network
- Any of the classes can be subnetted

Subnets

I n an effort to create smaller broadcast domains and to better utilize the bits in the host ID, an IP network can be subdivided into smaller networks, each bounded by an IP router and assigned a new subnet ted network ID, which is a subset of the original class-based network ID.
Example: A network identified by IP address 139.12.0.0
is divided into 3 subnets with IP addresses
139.12.1.0,139.12.2.0 & 139.12.3.0

Before subnetting **After subnetting**



Subnetting

Subnetting allows you to create multiple logical networks that exist within a single Class A, B, or C network.
To subnet a network, extend the natural mask using some of the bits from the host ID port ion of the address to create a subnetwork ID.

For example, given a Class C network of 204.15.5.0
which has a natural mask of 255.255.255.0, you can create subnets in this manner:

204.15.5.0 - 11001100.00001111.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
- | sub| - - - -

By extending the mask to be 255.255.255.224, you we have taken three bits (indicated by "sub") from the original host portion of the address and used them to make subnets.
With these three bits, it is possible to create eight subnets.

With the remaining five host ID bits, each subnet can have up to 32 host addresses, 30 of which can actually be assigned to a device *since host ids of all zeros or all ones are not allowed* (it is very impor tant to remember this) .

So, with this in mind, these subnets have been created.

The following 8 subnets can be created out of the 3 bits borrowed from the host portion of the net

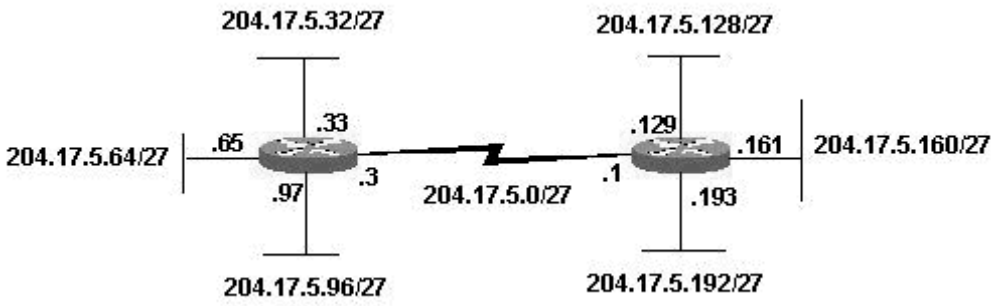
204.15.5.0	255.255.255.224	host address 1 to 30
204.15.5.32	255.255.255.224	host address 33 to 62
204.15.5.64	255.255.255.224	host address 65 to 94
204.15.5.96	255.255.255.224	host address 97 to 126
204.15.5.128	255.255.255.224	host address 129 to 158
204.15.5.160	255.255.255.224	host address 161 to 190
204.15.5.192	255.255.255.224	host address 193 to 222
204.15.5.224	255.255.255.224	host address 225 to 254

Subnet Mask

After subnetting, the default subnet mask of the IP address is changed according to the number of subnets created.

In the earlier example the default subnet mask of IP address
204.15.5.0 was
255.255.255.0
After subnetting its subnet mask is changed to
255.255.224.0

Subnetting the Network



What is Network Operating System

Unlike operating systems, such as Windows, that are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

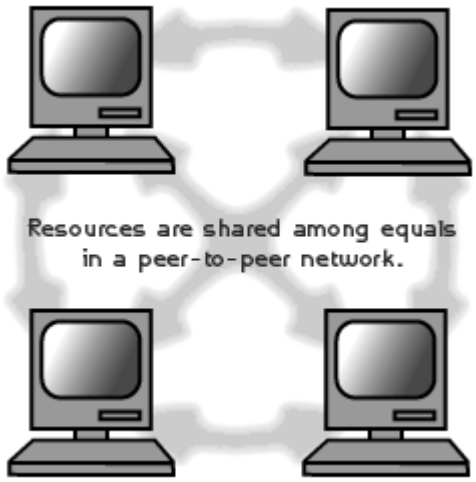
The two major types of network operating systems are:

- Peer-to-Peer
- Client/Server

Nearly all modern networks are a combination of both. The networking design can be considered independent of the servers and workstations that will share it.

PEER-TO-PEER

Peer-to-peer network operating systems allow users to share resources and files located on their computers and to access shared resources found on other computers. However, they do not have a file server or a centralized management source (See fig. 1). In a peer-to-peer network, all computers are considered equal; they all have the same abilities to use the resources available on the network. Peer-to-peer networks are designed primarily for small to medium local area networks. Nearly all modern desktop operating systems, such as Macintosh OSX, Linux, and Windows, can function as peer-to-peer network operating systems.



ADVANTAGES OF A PEER-TO-PEER NETWORK:

- Less initial expense - No need for a dedicated server.
- Setup - An operating system (such as Windows XP) already in place may only need to be reconfigured for peer-to-peer operations.

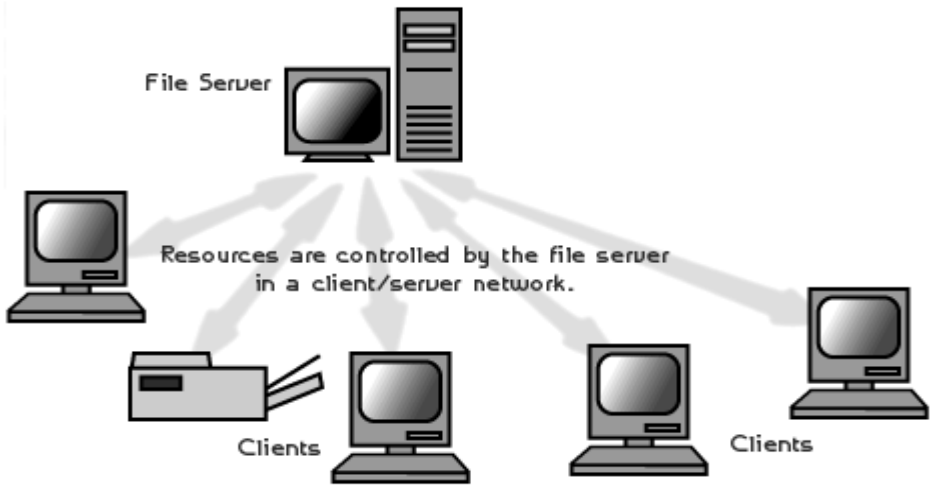
DISADVANTAGES OF A PEER-TO-PEER NETWORK:

- Decentralized - No central repository for files and applications.
- Security - Does not provide the security available on a client/server network.

CLIENT/SERVER

Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers (See fig. 2). The file servers become the heart of the system, providing access to resources and providing security. Individual workstations (clients) have access to the resources available on the file servers. The network operating system provides the mechanism to integrate all the components of the network and allow multiple users to simultaneously share the same resources irrespective of physical

location. UNIX/Linux and the Microsoft family of Windows Servers are examples of client/server network operating systems.



ADVANTAGES OF A CLIENT/SERVER NETWORK:

- Centralized - Resources and data security are controlled through the server.
- Scalability - Any or all elements can be replaced individually as needs increase.
- Flexibility - New technology can be easily integrated into system.
- Interoperability - All components (client/network/server) work together.
- Accessibility - Server can be accessed remotely and across multiple platforms.

DISADVANTAGES OF A CLIENT/SERVER NETWORK:

- Expense - Requires initial investment in dedicated server.
- Maintenance - Large networks will require a staff to ensure efficient operation.
- Dependence - When server goes down, operations will cease across the network.

NETWORK OPERATING SYSTEM SOFTWARE

The following links include some of the more popular peer-to-peer and client/server network operating systems.

- Macintosh OS X
- Microsoft Windows Server
- UNIX/Linux

WHAT IS ACTIVE DIRECTORY?

Active Directory is a database that keeps track of all the user accounts and passwords in your organization. It allows you to store your user accounts and passwords in one protected location, improving your organization's security.

Active Directory is subdivided into one or more **domains**. A domain is a security boundary. Each domain is hosted by a server computer called a **domain controller** (DC). A domain controller manages all of the user accounts and passwords for a domain.

Domains and the Domain Name System (DNS)

Domains are named using the Domain Name System (DNS). If your company is called ACME Corporation your DNS name would be (for example) acme.com. This is the **top-level domain name** for your company. The security domain in Active Directory maps directly to the DNS domain name.

For larger organizations you can subdivide Active Directory into child domains (based on geography for example). If ACME Corporation has three divisions named West, Central, and East, the sub-domains can have the DNS nameswest.acme.com, central.acme.com, and east.acme.com.

Each domain requires a server computer. In the above scenario you would need at least four servers to host Active Directory as follows:

- acme.com
- west.acme.com
- central.acme.com
- east.acme.com

Active Directory features include:

- Support for the X.500standard for global directories
- The capability for secure extension of network operations to the Web
- A hierarchical organization that provides a single point of access for system administration (management of user accounts, clients, servers, and applications, for example) to reduce redundancy and errors
- An object-oriented storage organization, which allows easier access to information
- Support for the Lightweight Directory Access Protocol (LDAP) to enable inter-directory operability
- Designed to be both backward compatible and forward compatible

DHCP

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.
DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.
The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.
- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.
- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.

- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.
- A DHCP-enabled client, upon accepting a lease offer, receives:
- A valid IP address for the subnet to which it is connecting.

Requested DHCP options, which are additional parameters that a DHCP server is configured to assign to clients.

WLAN

Also Known As: Wireless LAN

Definition:

WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter through a wireless (radio) connection.
Using technology from the Symbionics Networks, Ltd., a wireless LAN adapter can be made to fit on a Personal Computer Memory Card Industry Association (PCMCIA) card for a laptop or notebook computer.
Network security remains an important issue for WLANs. Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks. The IEEE 802.11 group of standards specifies the technologies for wireless LANs. 802.11 standards use the Ethernet Mobile Basics Protocol and CSMA/CA (carrier sense multiple access with collision avoidance) for path sharing and include an encryption method, the Wired Equivalent Privacy algorithm.
High-bandwidth allocation for wireless will make possible a relatively low-cost wiring of classrooms in the United States. A similar frequency allocation has been made in Europe. Hospitals and businesses are also expected to install wireless LAN systems where existing LANs are not already in place.

Disk Quotas

Disk space can be restricted by implementing disk quotas which alert a system administrator before a user consumes too much disk space or a partition becomes full.

Disk quotas can be configured for individual users as well as user groups. This makes it possible to manage the space allocated for user-specific files (such as email) separately from the space allocated to the projects a user works on (assuming the projects are given their own groups).

In addition, quotas can be set not just to control the number of disk blocks consumed but to control the number of inodes (data structures that contain information about files in UNIX file systems). Because inodes are used to contain file-related information, this allows control over the number of files that can be created.

The **quota** RPM must be installed to implement disk quotas.

Configuring Disk Quotas

To implement disk quotas, use the following steps:

- Enable quotas per file system by modifying the **/etc/fstab** file.
- Remount the file system(s).
- Create the quota database files and generate the disk usage table.
- Assign quota policies.

Each of these steps is discussed in detail in the following sections.

Enabling Quotas

As root, using a text editor, edit the **/etc/fstab** file.
Example Edit /etc/fstab
For example, to use the text editor **vim** types the following:
vim /etc/fstab
Add the **usrquota** and/or **grpquota** options to the file systems that require quotas:
Example Add quotas

```
/dev/VolGroup00/LogVol00                /                       ext3    defaults            1 1
LABEL=/boot                             /boot                           ext3    defaults            1 2
none                                    /dev/pts                devpts  gid=5,mode=620  0 0
none                                    /dev/shm                tmpfs   defaults            0 0
none                                    /proc                           proc    defaults            0 0
none                                    /sys                    sysfs   defaults            0 0
/dev/VolGroup00/LogVol02                /home                   ext3    defaults,usrquota,grpquota  1 2
/dev/VolGroup00/LogVol01                swap                            swap    defaults            0 0 . . .
```

In this example, the **/home** file system has both user and group quotas enabled.

Remounting the File Systems

After adding the **usrquota** and/or **grpquota** options, remount each file system whose **fstab** entry has been modified. If the file system is not in use by any process, use one of the following methods:

Issue the **umount** command followed by the **mount** command to remount the file system. Refer to the **man** page for both **umount** and **mount** for the specific syntax for mounting and unmounting various file system types.

Issue the **mount -o remount *file-system*** command (where ***file-system*** is the name of the file system) to remount the file system. For example, to remount the **/home** file system, the command to issue is **mount -o remount /home**.

If the file system is currently in use, the easiest method for remounting the file system is to reboot the system.

Creating the Quota Database Files

After each quota-enabled file system is remounted run the **quotacheck** command.

The **quotacheck** command examines quota-enabled file systems and builds a table of the current disk usage per file system. The table is then used to update the operating system's copy of disk usage. In addition, the file system's disk quota files are updated.

To create the quota files (**aquota.user** and **aquota.group**) on the file system, use the **-c** option of the **quotacheck** command.

Example. Create quota files

For example, if user and group quotas are enabled for the **/home** file system, create the files in the **/home** directory:
quotacheck -cug /home

The **-c** option specifies that the quota files should be created for each file system with quotas enabled, the **-u** option specifies to check for user quotas, and the **-g** option specifies to check for group quotas.
If neither the **-u** or **-g** options are specified, only the user quota file is created. If only **-g** is specified, only the group quota file is created.
After the files are created, run the following command to generate the table of current disk usage per file system with quotas enabled:
quotacheck -avug
The options used are as follows:
a
Check all quota-enabled, locally-mounted file systems
v
Display verbose status information as the quota check proceeds
u
Check user disk quota information
g
Check group disk quota information
After **quotacheck** has finished running, the quota files corresponding to the enabled quotas (user and/or group) are populated with data for each quota-enabled locally-mounted file system such as **/home**.

Assigning Quotas per User

The last step is assigning the disk quotas with the edquota command.
To configure the quota for a user, as root in a shell prompt, execute the command:
edquota *username*

Perform this step for each user who needs a quota. For example, if a quota is enabled in /etc/fstab for the /home partition (/dev/VolGroup00/LogVol02 in the example below) and the command edquota testuser is executed, the following is shown in the editor configured as the default for the system:

Disk quotas for user testuser (uid 501):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/VolGroup00/LogVol02	440436	0	0	37418	0	0

Assigning Quotas per Group

Quotas can also be assigned on a per-group basis. For example, to set a group quota for the devel group (the group must exist prior to setting the group quota), use the command:
edquota -g devel
This command displays the existing quota for the group in the text editor:
Disk quotas for group devel (gid 505):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/VolGroup00/LogVol02	440400	0	0	37418	0	0

Modify the limits, then save the file.
To verify that the group quota has been set, use the command:
quota -g devel

Internet Security (Proxy, Firewall, Virus solutions)

Proxy Concepts

Data networking is growing at a dizzying rate. More than 80% of Fortune 500 companies have web sites. More than half of these companies have implemented intranets and are putting graphically rich data on to the corporate WANs. The number of web users is expected to increase by a factor of five by the next 3 years.
The resulting uncontrolled growth of Web access requirements is straining all attempts to meet the bandwidth demand.

Caching is the technique of keeping frequently accessed information in a location close to the requester.
A Web cache stores web pages and contents on a storage device that is physically or logically closer to the user-this is closer and faster than a web look-up.
By reducing the amount of traffic on WAN links and on overburdened Web Servers, caching provides significant benefits to ISPs, Enterprise Networks and end users.

Web Caching

There are two key benefits

- Cost savings due to WAN bandwidth reduction.
- Improved productivity for end users-reduced response time.

Web Caching works as follows

1. A user accesses a web page
2. While the page is being transmitted to the user, the caching system saves the page and its entire associated graphics on a local storage device. That content is now cached
3. Another user (or the original user) accesses that web page later in the day.
4. Instead of sending the request over the internet, the web cache system delivers the web page from local storage. This process speeds download time for the user and reduces bandwidth demand on the WAN link.
5. The im portant task of ensuring that data is up-to-date is addressed in a variety of ways depending on the design of the system

Browser based client caching

- Internet Browser application allows an individual user to cache web pages (i.e. images and HTML texts) on users local Hard Disks.
- A user can configure the amount of disk space devoted to caching

Caching solutions on the network level:

The proxy server and network cache concepts

- To limit bandwidth demand caused by the uncontrolled growth of internet use, vendors have developed applications that extend local caching to the network level

- The two current types of network level caching products are proxy servers & network caches

Cisco's network based shared caching

- The cache engine solutions comprise of the web cache control protocol (A standard feature of Cisco IOS software) and one or more Cisco cache engines that stores the data in the local network.
- The Cisco cache engine is a single purpose network appliance that stores and retrieves content using highly optimised caching and retrieval algorithms.

- The web cache control protocol defines the communication between the cache engine and the router
- Using the web cache control protocol the router directs only web requests to the cache engines (rather than to the intended server)
- The router also determines cache engine availability and redirects requests to new cache engines as they are added to an installation

Cache engine operation

Using the web cache control protocol, the Cisco IOS router routes requests for TCP port 80 (HTTP traffic) over a local subnet to the cache engine. The cache engine is dedicated solely to content management and delivery. Because only web requests are routed to the cache engines no other user traffic is affected by the caching process-web caching is done "off to the side" . For non web traffic the router functions entirely in its traditional role.

The cache engine works as follows.

- A client requests web content in the normal fashion.
- The router running the web cache control protocol intercepts TCP port 80 web traffic and routes it to the cache engine.
- The Client is not involved in this transaction and no changes to the client or browser are required

- If the cache engine does not have the requested content, it sends the requests to the internet or intranet in the normal fashion
- The content returns to and is stored at the cache engine.
- The cache engine returns the contents to the clients.
- Upon subsequent requests for the same content, the cache engine fulfills the request from local storage.

Cache Engine Operation Transparency

Because the router redirects packets destined for web server to the cache engine, the cache engine operates transparently to the clients.

Clients do not need to configure their browsers to be in proxy server mode. I n addition the operation of cache engine is transparent to the network- the router operates entirely in its normal role for non web traffic. This transparent design is the requirement for a system to offer network wide scalability, fault tolerance and failsafe operation

Proxy Servers

- A server that sits between a client application, such as a Web browser, and a real server.
- I t intercepts all requests to the real server to see if it can fulfill the requests itself.
- If not, it forwards the request to the real server.

Proxy servers -two main purposes

- **Improve Performance:** Proxy servers can dramatically improve performance for groups of users. This is because it saves the results of all requests for a certain amount of time
- **Filter Requests:** Proxy servers can also be used to filter requests. For example, a company might use a proxy server to prevent its employees from accessing a specific set of Web sites.

Proxy Settings in Internet Explorer 6.X

- Click "Service" \ "Internet Options"; Click "Connections";
- If you use Dial-Up connection, choose your connection and click "Settings" button. if you use LAN connection, click "LAN Settings" button in the "Local Area Network (LAN) Settings" group box;
- Enable "use a proxy server";
- I n fields "Address" and "port", type proxy name and proxy port number;
- If nessesary, enable "bypass proxy server for local addresses";
- Click "OK";
- Click "OK" to close IE settings.

Proxy Settings in Netscape Navigator 6.x

- Click "Edit" \ "Preferences";
- Click "Category" \ "Advanced" \ "Proxies";
- Set "Manual proxy configuration";
- Click "View" at "Manual proxy configuration";
- Set proxies for following protocols: HTTP, FTP, etc.

Free Proxy Servers

CC Proxy - Proxy Server Download

FIREWALL

- A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both.
- Firewalls are frequently used to prevent unauthorized I nternet users from accessing private networks connected to the Internet, especially *intranets.*
- All m essages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.
- A firewall is considered a first line of defense in protecting private information

Types of Firewall techniques

- Packet filter Application gateway Circuit-level gateway Proxy server
- In practice, many firewalls use two or m ore of these techniques in concert.

Packet filter

- Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules.
- Packet filtering is fairly effective and transparent to users, but it is difficult to configure.
- I n addition, it is susceptible to IP spoofing
- (IP spoofing :An attack whereby a system attempts to illicitly impersonate another system by using IP network address)

Application gateway

- Applies security mechanisms to specific applications, such as FTP and Telnet servers.
- This is very effective, but can impose a performance degradation

Circuit-level gateway

- Applies security mechanisms when a TCP or UDP connection is established.
- Once the connection has been made, packets can flow between the hosts without further checking

Proxy server

- Intercepts all messages entering and leaving the network.
- The proxy server effectively hides the true n et w or k addresses.

Making the Firewall Fit

Firewalls are customizable.

This means that filters can be added or remove based on several conditions

- 1. **IP ADDRESS**: Each machine on the Internet is assigned a unique address called an **I P address**. IP addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical IP address looks like this: 216.27.61.137. For example, if a certain IP address outside the company is reading too m any files from a server, the firewall can block all traffic to or from that IP address.

- DOMAIN NAMES Because it is hard to remember the string of numbers that make up an IP address, and because IP addresses sometimes need to change, all servers on the I nternet also have human-readable names, called **domain names**.
- For example, it is easier to remember www.howstuffworks.com than it is to remember 216.27.61.137. A company might block all access to certain domain names, or allow access only to specific domain names.

- PROTOCOL The **protocol** is the pre-defined way that som eone who wants to use a service talks with that service. The "someone" could be a person, but more often it is

a computer program like a Web browser. Protocols are often text, and simply describe how the client and server will have their conversation. The **http** in the Web's protocol.

- Some common protocols that you can set firewall filters for include:
- **I P,TCP,HTTP,FTP,UDP,I CMP,SMTP, SNMP, Tel net**
- A company might set up only one or two machines to handle a specific protocol and ban
- That protocol on all other machines.

- 4.Ports:Any server machine makes its services available to the Internet using numbered **ports**, one for each service that is available on the server
- For example, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21 . A company might block port 21 access on all machines but one inside the com pany.

- Specific words and phrases -
- This can be anything. The firewall will **sniff** (search through) each packet of information for an exact m atch of the text listed in the filter. For exam ple, you could instruct the firewall to block any packet with the word "X-rated" in it. The key here is that it has to be an exact match. The
- "X-rated" filter would not catch "X rated" (no
- hyphen). But you can include as many words, phrases and variations of them as you need.

FIREWALL CATEGORI ES

1. Software Firewall
2. Hardware Firewall

Software Firewall

- A software firewall can be installed on the computer in home that has an Internet connection. This computer is considered a **gateway** because it provides the only point of access between your home network and the Internet.
- In case of LAN, it has to be installed on each machine.
- A few examples of shareware/freeware firewalls are
- Tiny Firewall ZoneAlarm Sysgate Kerio Firewall
- Windows XP has a built-in firewall

Hardware Firewall

- Hardware firewalls are incredibly secure and not very expensive. Home versions that include a router, firewall and Ethernet hub for broadband connections.
- Hardware firewall unit itself is normally the gateway.
- A good example is the Linksys Cable/DSL router. It has a built-in Ethernet card and hub. Computers in home network connect to the router, which in turn is connected to either a cable or DSL modem. The router can be configured via a Web-based interface that you reach through the browser on your computer. You can then set any filters or additional information.

What Firewall protects from

Remote login - When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer

Application backdoors - Some programs have special features that allow for remote access. Others contain bugs that provide a **backdoor**, or hidden access, that provides some level of control of the program.

SMTP session hijacking - SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk email (**spam**) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace

Operating system bugs - Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

Denial of service - You have probably heard this phrase used in news reports on the attacks on m ajor Web sites. This type of attack is nearly impossible to counter. What happens is that the hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.

E-mail bombs - An e-mail bomb is usually a personal attack. Someone sends you the same email hundreds or thousands of times until your email system cannot accept any more messages.

Macros - To simplify complicated procedures, m any applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

Viruses - Probably the most well-known threat is computer viruses. A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.

Spam - Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

Redirect bombs -Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router. This is one of the ways that a denial of service attack is set up.

Source routing -In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel. Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.

Cyber threats

- A survey conducted by Internet service provider America Online Inc. found that 20% of home com puters were infected by a virus, worm or trojans and that various forms of snooping programs such as spyware, adware and spam are on a whopping 80% of systems.
- Even so, more than two-thirds of home users think they are safe from online threats.

Threats

- **Destructive**
- **Non-destructive**
- Malware
- Adware
- Spam
- Virus
- Worm
- Trojan
- Spyware

Malware

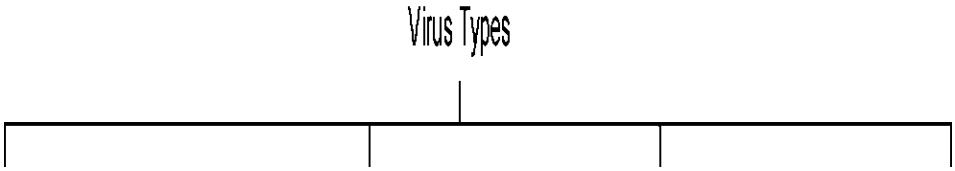
- **Malware** (a contraction of "malicious software") is any software developed for the purpose of doing harm to a computer system.
- Malware can be classified based on how it gets executed, how it spreads, and/or what it does
- Two common types of malware are viruses and worms. These types of programs have in com m on that they are both able to self-replicate; they can spread (possibly modified) copies of themselves.
- Trojans, spyware are also falling under the category of malware

Virus- Definition

- A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can also replicate themselves.
- All computer viruses are manmade.
- A simple virus that can make a copy of itself over and over again is relatively easy to produce.
- Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt.
- An even m ore dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

- A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes.
- Viruses can also replicate themselves.
- All computer viruses are manmade.
- A simple virus that can make a copy of itself over and over again is relatively easy to produce.
- Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt.
- An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

VIRUS CATEGORIES



File infector		**System 1 Boot Record Infector[1]**	**[1] File system or Cluster Virus**	**Kernel Virus**

Direct Action

Resident

Boot Sector Virus

Boot & File Virus

File Infectors

Virus attaches itself to ordinary program files viz com, exe, bat, sys, ovl, obj, prj, mnu

Classified into two types

•Direct action (Non Resident): Virus selects one or more program to infect each time a program infected by it is executed. Eg:

• Resident: Installs itself some where in the memory the first time an infected program is executed and thereafter infects other programs when they are executed. Eg: jerusalem virus

System / Boot Infector

Boot Sector Virus

- These viruses infect executable code found in certain system areas on a disk. On PCs there are ordinary boot sector viruses which infect only DOS boot sector and MBR(Master Boot Record) viruses which infect MBR on fixed Disks and DOS Boot sector on diskettes.
- E.g.: Brain, Stoned, Empire
- All com m on boot sector /MBR viruses are memory resident.

Boot & File Virus

- Viruses which are able to infect both files and boot sectors.
- Also called Multi-partite viruses. Eg. Tequila

File system or Cluster Virus

- These viruses modify directory table entries so that the virus is loaded and executed before the desired program is loaded.
- The program itself is not physically altered, only the directory entry of the program file is altered.
- Also referred as Link Virus

Kernel Virus

- Target specific features of programs that contain the core of an operating system
- Eg: 3APA3A is a DOS kernel virus and also a m u lti-partite virus

TOP 10 VIRUS / WORM/ TROJAN

- Backdoor.Win32.Surila.k
- Worm .P2P.Krepper.c
- TrojanDropper.Win32.Small.kv
- I-Worm.Mydoom.y
- Backdoor.SdBot.gen
- TrojanDropper.VBS.Zerolin
- I-Worm.NetSky.aa
- Backdoor.Rbot.gen
- Trojan.Win32.Defacer.a
- Win32.Parite.a

Virus-Prevention

Anti Virus Software

- A utility that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered.
- The antivirus software installed should be enabled always.

Some popular antivirus utilities

- Norton
- F-Prot
- AVG
- Panda
- eZ
- Dr. Solomon's

Worm- definition

- A computer worm is a self-replicating computer program, similar to a computer virus.
- A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself.
- Worm spreads itself to the other computers through their own SMTP engine by using information in users address books. Worms are very dangerous, hard to find and delete programs. They are able to mutuate (replace their code by themselves).
- That m akes them very hard to find for antivirus programs.
- In addition to replication, a worm may be designed to do any number of things, such as delete files on a host system or send documents via email

Worm Prevention

- Update the o/s by downloading the latest patches which provides necessary security.

- Do not open email attachments from unknown sources
- Using appropriate antivirus tools or using a Firewall
- Configure the firewall to block entry of worms

- For eg: To prevent Blaster.exe worm
- Block access to TCP port 4444 at the firewall level, and then block the following ports, if they do not use the applications listed:

Trojans - Definition

- A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.
- One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your com puter

Examples- Trojans

- A simple example of a Trojan horse would be a program named "SEXY.EXE" that is posted on a website with a promise of "hot pix"; but, when run, it instead erases all the files on the computer and displays a taunting message.
- On the Microsoft Windows platform, an attacker m ight attach a Trojan with an innocent-looking filename to an email message which entices the recipient into opening the file.
- The Trojan itself would typically be a Windows executable program file, and thus must have an executable filename extension such as .exe, .scr, .bat, or .pif.
- Since Windows is sometimes configured by default to hide filename extensions from a user, the Trojan horse's extension might be "masked" by giving it a name such as 'Readme.txt.exe'.
- With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file.
- Icons can also be chosen to imitate a different file type. When the recipient double-clicks on the attachment, the trojan might superficially do what the user expects it to do (open a text file, for example), so as to keep the victim unaware of its malicious purpose.
- Meanwhile, it might discreetly modify or delete files, change the configuration of the computer, or even use the computer as a base from which to attack local or other networks.

Precautions against Trojans

- Do not open unusual attachments that arrive unexpectedly, any unopened Trojans will not affect the computer.
- This is true even if you know the sender or recognize the source's address.
- Even if one expects an attachment, scanning it with updated antivirus software before opening it is prudent.
- Files downloaded from file-sharing services such as Kazaa or Gnutella are particularly suspect, because file-sharing services are regularly used to spread Trojan programs.

Spyware

Spyware consists of computer software that gathers information about a computer user and then transmits this information to an external entity without the knowledge or informed consent of the user.

Solutions to spyware

Use of automatic updates (on Windows systems), antivirus, and other software upgrades will help to protect systems.

Software bugs and exploits remaining in older software leave one vulnerable, because the public rapidly learns over time how to exploit unpatched systems

Adware

Adware or **advertising-supported software** is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen

Examples of Shareware that contains adware

•Eudora—Email client •Opera—Web browser •DivX—Video codec

•Kazaa—Filesharing program, also contains spyware

•iMesh—Filesharing program, also contains spyware

•Grokster —Filesharing program, contains spyware that may seriously impact performance of Microsoft Windows.

SPAM

- **Spamming** is the act of sending unsolicited electronic messages in bulk.
- In the popular eye, the most common form of spam is that delivered in e-mail as a form of com m ercial advertising.
- However, over the short history of electronic media, people have done things comparable to spamming for many purposes other than the commercial, and in many media other than em ail.
- I n this article and those related, the term *spamming* is used broadly to refer to all of these behaviors, regardless of medium and commercial intent.

Types of SPAMs

- E-mail spam Messaging spam Newsgroup spam
- Spamdexing (search engine spam)
- Blog spam
- Mobile phone spam
- Internet telephony spam

Messaging spam

Messaging spam, often termed *spim,* is a type of spamming where the target of the spamming is instant messaging (IM). Many IM systems offer a directory of users, including demographic information such as age and sex. Advertisers can gather this information, sign on to the system, and send unsolicited messages

Newsgroup spam

Newsgroup spam is a type of spamming where the target of the spamming are Usenet newsgroups. Spamming of Usenet newsgroups actually pre-dates e-mail spam. Old Usenet convention defines spamming as *excessive multiple posting,* that is, the repeated posting of a message (or substantially similar messages). Since posting to newsgroups is nearly as easy as sending e-mails, newsgroups are a popular target of spammers.

Spamdexing (search engine spam)

Spamdexing (a combination of *spamming* and *indexing)* refers to the practice on the World Wide Web of deliberately modifying HTML pages to increase the chance of them being placed high on search engine relevancy lists. People who do this are called search engine spammers.

Blog spam

In blog spam the targets are weblogs. In 2003, this type of spam took advantage of the open nature of comments in the blogging software Movable Type by repeatedly placing com m ents to various blog posts that provided nothing more than a link to the spammer's com m ercial web site. These link would in theory enhance the ranking of the target page in search engine indexes

Mobile phone spam

Mobile phone spam is a form of spamming directed at the text messaging service of a m obile phone. This can be especially irritating to consumers not only for the inconvenience but also because they sometimes have to pay to receive the text message.

Internet telephony spam

It has been predicted that voice over IP (VoIP) communications will be vulnerable to being spammed by pre-recorded messages. Although there have been few reported incidents, some com panies have already developed technology to broadcast messages via VoIP. This form of spamming has been dubbed SPIT (SPam over Internet Telephony). VoIP providers have acknowledged that SPIT will "happen, just as spam e-mail did" and are trying to "get ahead of the game" by putting in place security measures against it.

How to prevent SPAM

By using

- Anti-spam Software Anti-spam Firewall (Hardware)
- A Presentation by IT Faculty
- Centre for Excellence in Telecom Technology & Management MTNL,

Introduction to MPLS LDP

What is MPLS?

MPLS stands for Multi-protocol Label Switching. MPLS is a packet forwarding technology that is capable of carrying any L3 protocol and here comes the word multi-protocol. MPLS is capable of tunneling L3 packets inside the MPLS network using MPLS labels. The MPLS label is pushed into the packet between the layer two header and the layer three header of the packet at the ingress router and is used to switch the packets across the network to its destination.

Multi-Protocol Label Switching (MPLS) provides a mechanism for forwarding packets for any network protocol. It was originally developed in the late 1990s to provide faster packet forwarding for IP routers (see RFC 3031). Since then its capabilities have expanded massively, for example to support service creation (VPNs), traffic engineering, network convergence, and increased resiliency

Traditional IP networks are connectionless: when a packet is received, the router determines the next hop using the destination IP address on the packet alongside information from its own forwarding table. The router's forwarding tables contain information on the network topology, obtained via an IP routing protocol, such as OSPF, IS-IS, BGP, RIP or static configuration, which keeps that information synchronized with changes in the network.

MPLS similarly uses IP addresses, either IPv4 or IPv6, to identify end points and intermediate switches and routers. This makes MPLS networks IP-compatible and easily integrated with traditional IP networks. However, unlike traditional IP, MPLS flows are connection-oriented and packets are routed along pre-configured Label Switched Paths (LSPs).

The evident power of the basic MPLS concepts led the industry to define generalized extensions to MPLS, or Generalized MPLS (GMPLS). This work extended the MPLS concept of a label to include implicit values defined by the medium that is being provisioned, for example a wavelength for a DWDM system or a timeslot for a SONET/SDH device. So with GMPLS, there is no need for a switch to "read" the label in each packet header. The label is an inherent part of the switch fabric and the switching operations depend on wavelength, or timeslot etc. This permits the benefits of MPLS to be shared by many different types of switching platform

MPLS LDP provides the means for LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of routers communicate the LDP parameters, they establish a label-switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is also called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router the router looks at the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router the router looks at the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

Function of MPLS LDP

MPLS LDP provides the building blocks for MPLS-enabled applications, such as MPS Virtual Private Networks (VPNs).

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labelled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

From an historical and functional standpoint, LDP is a superset of the Cisco prestandard Tag Distribution Protocol (TDP), which also supports MPLS forwarding along normally routed paths. For those features that LDP and TDP share in common, the pattern of protocol

exchanges between network routing platforms is identical. The differences between LDP and TDP for those features supported by both protocols are largely embedded in their respective implementation details, such as the encoding of protocol messages.

This release of LDP, which supports both the LDP and TDP protocols, provides the means for transitioning an existing network from a TDP environment to an LDP environment. Thus, you can run LDP and TDP simultaneously on any router platform. The label distribution protocol that you select can be configured on a per-interface basis for directly connected neighbours and on a per-session basis for non directly connected (targeted) neighbours. In addition, an LSP across an MPLS network can be supported by LDP on some hops and by TDP on other hops.

Introduction to LDP Sessions

When you enable MPLS LDP, the LSRs send out messages to try to find other LSRs with which they can create LDP sessions. The following sections explain the differences between directly connected LDP sessions and non directly connected LDP sessions.

Directly Connected MPLS LDP Sessions

If an LSR is one hop from its neighbour, it is directly connected to its neighbour. The LSR sends out LDP link Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet (multicast). A neighbouring LSR may respond to the link Hello message, allowing the two routers to establish an LDP session. This is called basic discovery.

To initiate an LDP session between routers, the routers determine which router will take the active role and which router will take the passive role. The router that takes the active role establishes the LDP TCP connection session and initiates the negotiation of the LDP session parameters. To determine the roles, the two routers compare their transport addresses. The router with the higher IP address takes the active role and establishes the session.

After the LDP TCP connection session is established, the LSRs negotiate the session parameters, including the method of label distribution to be used. Two methods are available:

- Downstream Unsolicited: An LSR advertises label mappings to peers without being asked to.

- Downstream on Demand: An LSR advertises label mappings to a peer only when the peer asks for them.

Non directly Connected MPLS LDP Sessions

If the LSR is more than one hop from its neighbour, it is non directly connected to its neighbour. For these non directly connected neighbours, the LSR sends out a targeted Hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The non directly connected LSR responds to the Hello message and the two routers begin to establish an LDP session. This is called extended discovery.

An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need

to establish a label distribution session between the tunnel head end and the tail end routers. You establish non directly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

You can use the **MPLS LDP neighbour targeted** command to set up a targeted session when other means of establishing targeted sessions do not apply, such as configuring **MPLS IP** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you can use this command to create a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **LDP neighbour targeted** command can improve label convergence time for directly connected neighbour LSRs when the link(s) directly connecting them are down. When the links between the neighbour LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbour LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to re establish their LDP session and exchange labels.

The exchange of targeted Hello messages between two non directly connected neighbours can occur in several ways, including the following:

- Router 1 sends targeted Hello messages carrying a response request to Router 2. Router 2 sends targeted Hello messages in response if its configuration permits. In this situation, Router 1 is considered to be *active* and Router 2 is considered to be *passive*.

- Router 1 and Router 2 both send targeted Hello messages to each other. Both routers are considered to be *active*. Both, one, or neither router can also be *passive*, if they have been configured to respond to requests for targeted Hello messages from each other.

The default behavior of an LSR is to ignore requests from other LSRs that send targeted Hello messages. You can configure an LSR to respond to requests for targeted Hello messages by issuing the **MPLS LDP discovery targeted-hello accept** command.

The active LSR mandates the protocol that is used for a targeted session. The passive LSR uses the protocol of the received targeted Hello messages.

Introduction to LDP Label Bindings, Label Spaces, and LDP Identifiers

An LDP label binding is an association between a destination prefix and a label. The label used in a label binding is allocated from a set of possible labels called a label space.

LDP supports two types of label spaces:

- **Interface-specific**—An interface-specific label space uses interface resources for labels. For example, label-controlled ATM (LC-ATM) interfaces use virtual path identifiers/virtual circuit identifiers (VPIs/VCIs) for labels. Depending on its configuration, an LDP platform may support zero, one, or more interface-specific label spaces.

- **Platform-wide**—An LDP platform supports a single platform-wide label space for use by interfaces that can share the same labels. For Cisco platforms, all interface types, except LC-ATM, use the platform-wide label space.

LDP uses a 6-byte quantity called an LDP Identifier (or LDP ID) to name label spaces. The LDP ID is made up of the following components:

- The first four bytes, called the LPD router ID, identify the LSR that owns the label space.
- The last two bytes, called the local label space ID, identify the label space within the LSR. For the platform-wide label space, the last two bytes of the LDP ID are always both 0.

The LDP ID takes the following form:
< LDP router ID> : <local label space ID>
The following are examples of LPD IDs:

- 172.16.0.0:0
- 192.168.0.0:3

The router determines the LDP router ID as follows, if the **MPLS LDP router-id** command is not executed,

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

The normal (default) method for determining the LDP router ID may result in a router ID that is not usable in certain situations. For example, the router might select an IP address as the LDP router ID that the routing protocol cannot advertise to a neighbouring router. The **MPLS LDP router-id** command allows you to specify the IP address of an interface as the LDP router ID. Make sure the specified interface is operational so that its IP address can be used as the LDP router ID.

When you issue the **MPLS LDP router-id** command without the **force** keyword, the router select selects the IP address of the specified interface (provided that the interface is operational) the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is configured.

When you issue the **MPLS LDP router-id** command with the **force** keyword, the effect of the **mpls ldp router-id** command depends on the current state of the specified interface:

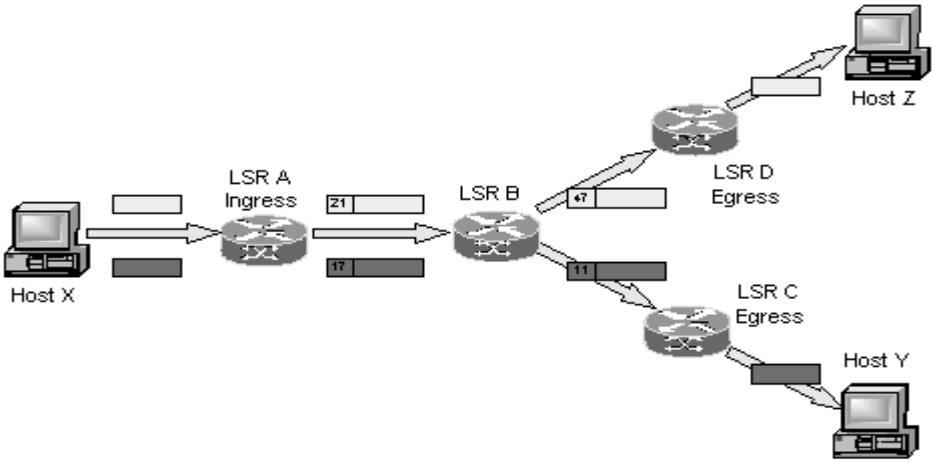
- If the interface is up (operational) and if its IP address is not currently the LDP router ID, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down (not operational) when the **MPLS LDP router-id force** command is issued, when the interface transitions to up, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

HOW DOES MPLS WORK?

MPLS works by tagging the traffic, in this example packets, with an identifier (a label) to distinguish the LSPs. When a packet is received, the router uses this label (and sometimes also the link over which it was received) to identify the LSP. It then looks up the LSP in its own forwarding table to determine the best link over which to forward the packet, and the label to use on this next hop.

A different label is used for each hop, and it is chosen by the router or switch performing the forwarding operation. This allows the use of very fast and simple forwarding engines, which are often implemented in hardware.

Ingress routers at the edge of the MPLS network classify each packet potentially using a range of attributes, not just the packet's destination address, to determine which LSP to use. Inside the network, the MPLS routers use only the LSP labels to forward the packet to the egress router.



The diagram above shows a simple example of forwarding IP packets using MPLS, where the forwarding is based only on packet destination IP address. LSR (Label Switched Router) A uses the destination IP address on each packet to select the LSP, which determines the next hop and initial label for each packet (21 and 17). When LSR B receives the packets, it uses these labels to identify the LSPs, from which it determines the next hops (LSRs D and C) and labels (47 and 11). The egress routers (LSRs D and C) strip off the final label and route the packet out of the network.

The above is only one use of MPLS. Since MPLS uses only the label to forward packets, it is protocol-independent, hence the term "Multi-Protocol" in MPLS. It can be used to carry any content (not only packets) over any link technology (using different label encoding for each layer 2 link type)

What is the MPLS Label and How is it used?

The MPLS label is a fixed 4 byte identifier added to the packet by the ingress router between the data-link layer (Layer2) and the network layer (Layer3) and is used by all middle routers to switch the packet to its destination without the need for any routing table (Layer3) look-ups. MPLS is considered a **layer 2.5** technology and the MPLS header is called the shim header.

The diagram below illustrates the structure of the label. One or more labels are pushed on the packet at the ingress router forming a label stack. The first label is called the top label or the transport label, other labels are used by different MPLS applications if needed.

MPLS Label Structure

- **Label**: label value, 20 bits.
- **EXP**: Experimental bits, Name is currently changed to Traffic class, 3 bits.
- **S**: bottom of stack, 1 bit.
- **TTL**: Time to live, 8 bits.

A couple of definitions are important before moving to MPLS operation:

- **Downstream router**: This is the router which advertises the prefix. In other words the router that is the next hop to a specific prefix is the downstream.
- **Upstream router**: This router receives the routing information from its downstream router.
- **Label Edge Router (LER)**: Operates at the edge of the MPLS network (ingress/egress) and make forwarding decisions based on the IP header information of the packet.
- **Label Switch router (LSR)**: the routers in the middle of the MPLS network which forwards MPLS packets based on label information.
-

QoS in IP/MPLS

QoS in IP/MPLS networks using Cisco IOS and Cisco IOS XR Software

- Understand IP QoS architectures and how they apply to MPLS
- Take a detailed look at traffic management using policing, shaping, scheduling, and active queue management
- Study Cisco QoS behavioral model and the modular QoS command-line interface (MQC)
- Learn the operation of MPLS TE with its DiffServ extensions and applicability as a traffic-protection alternative
- Find multiple configuration and verification examples illustrating the implementation of MPLS TE, DS-TE, and FRR
- Review the different designs, ranging from a best-effort backbone to the most elaborate scenarios combining DiffServ, DS-TE, and FRR

Quality of service (QoS) plays a key role in the implementation of IP and MPLS networks today. However, QoS can be one of the most complex aspects of networking. The industry efforts to achieve convergence have generated a need for increased levels of traffic differentiation. Today's networks need to meet an array of QoS requirements to support distinct applications (such as voice, video, and data) and multiple network services (such as IP, Ethernet, and ATM) on a single converged, multiservice network. QoS has therefore has become an integral part of network design, implementation, and operation.

QoS for IP/MPLS Networks is a practical guide that will help you facilitate the design, deployment, and operation of QoS using Cisco® IOS® Software and Cisco IOS XR Software. The book provides a thorough explanation of the technology behind MPLS QoS and related technologies, including the different design options you can use to build an MPLS network with strict performance requirements. This book discusses MPLS Traffic Engineering (MPLS TE) as a tool to complement MPLS QoS and enhance the performance characteristics of the network. You'll learn technology, configuration, and operational details, including the essentials facts about the behavior and configuration of the rich MPLS QoS and related MPLS TE functionality. To get the most out of this book, you should have a basic understanding of both IP and MPLS, including the basics of IP addressing and routing and the basics of MPLS forwarding.

MPLS Traffic Engineering Theory

MPLS TE Overview

In a traditional IP forwarding paradigm, packets are forwarded on a per-hop basis where a route lookup is performed on each router from source to destination. As cited earlier, the destination-based forwarding paradigm leads to suboptimal use of available bandwidth between a pair of routers in the service provider network. Predominantly, the suboptimal paths are under-utilized in IP networks. To avoid packet drops due to inefficient use of available bandwidth and to provide better performance, TE is employed to steer some of the traffic destined to follow the optimal path to a suboptimal path to enable better bandwidth management and utilization between a pair of routers. TE, hence, relieves temporary congestion in the core of the network on the primary or optimal cost links. TE maps flows between two routers appropriately to enable efficient use of already available bandwidth in the core of the network. The key to implementing a scalable and efficient TE methodology in the core of the network is to gather information on the traffic patterns as they traverse the core of the network so that bandwidth guarantees can be established, TE tunnels, ***Tunnel1 and Tunnel2,*** can be configured on PE1-AS1 that can map to separate paths ***(PATH1, PATH2),*** enabling efficient bandwidth utilization.

TE tunnels configured on routers are unidirectional. Therefore, to implement bidirectional TE deployment between routers PE1-AS1 and PE2-AS1 in a pair of tunnels must also be configured on PE2-AS1 in addition to ***Tunnel1 and Tunnel2*** configured on PE1-AS1. In an MPLS network, all pertinent tunnel configurations are always performed or provider edge (PE) routers. The TE tunnels or LSPs will be used to link the edge routers across the core of the service provider network.

MPLS TE can also map to certain classes of traffic versus destinations. If Customer A CE routers are connected into the SP network using OC3 links versus Customer B connecting into the SP network using a 64 K dialup link, preferential treatment can be configured on TE tunnels so that TE ***Tunnel1*** can carry Customer A traffic and Tunnel2 can carry Customer B traffic. Tunnels configured on both PE1-AS1 and PE2-AS1.

TE tunnels are, thus, data flows between a specific source and destination that might have properties or attributes associated with them. The attributes associated with a tunnel, in addition to the ingress (headend) and egress (tailend) points of the network, can include the bandwidth requirements and the CoS for data that will be forwarded utilizing this tunnel.

Traffic is forwarded along the path defined as the TE tunnel by using MPLS label switching. Hence, TE tunnels are assigned specific label switched paths (LSPs) in the network from source to destination, which are usually PE routers. MPLS LSPs have a one-to-one mapping with TE tunnels, and TE tunnels are not bound to a specific path through the SP network to a destination PE router. Unless configured explicitly, TE tunnels can reroute packets via any path through the network associated with an MPLS LSP. This path might be defined by the IGP used in the core, which are discussed in the section on MPLS TE extensions.

The primary reason for the implementation of MPLS TE is to control paths along which traffic flows through a network. MPLS TE also lends itself to a resilient design in which a secondary path can be used when the primary path fails between two routers in a network. Data plane information is forwarded using label switching; a packet arriving on a PE from the CE router is applied labels and forwarded to the egress PE router. The labels are removed at the egress router and forwarded out to the appropriate destination as an IP packet.

OSPF or IS-IS with extensions for TE is used to carry information pertaining to the tunnel configured on a router. The extensions carry information on available resources for building a tunnel, like bandwidth on a link. As a result, a link that does not have the requested resources (like bandwidth) is not chosen to be a part of the LSP tunnel or TE tunnel. Signaling in an MPLS TE environment uses resource reservation protocol (RSVP) with extensions to support TE tunnel features.

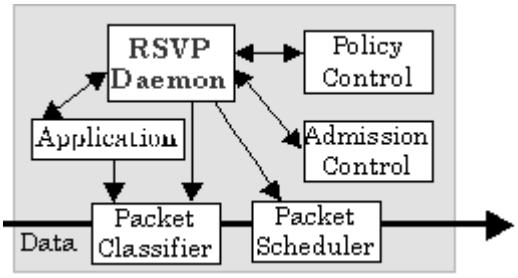
The data plane ingress (headend) router in the MPLS domain requires information pertaining to the resource availability on all links capable of being a part of the MPLS TE tunnel. This information is provided by IGPs like OSPF and IS-IS due to the inherent operation of flooding information about links to all routers in the IGP domain. In IS-IS, a new TLV (type 22) has been developed to transmit information pertaining to resource availability and link status in the LS-PDUs. In OSPF, the type 10 LSA provides resource and links status information. When this information is flooded in IGP updates, the ingress (headend) router gathers information on all the available resources in the network along with the topology, which defines tunnels through the network between a set of MPLS-enabled routers.

The inspiration behind MPLS TE is ***Constraint Based Routing (CBR)***, which takes into account the possibility of multiple paths between a specific source/destination pair in a network. With CBR, the operation of an IP network is enhanced so the least cost routing can be implemented as well as variables to find paths from a source to destination. CBR requires an IGP, like OSPF or IS-IS, for its operation. CBR is the backbone of the TE tunnel definition and is defined on the ingress routers to the MPLS domain when implementing MPLS TE. Resource availability and link status information are calculated using a ***constrained SPF*** calculation in which factors such as the bandwidth, policies, and topology are taken into consideration to define probable paths from a source to destination.

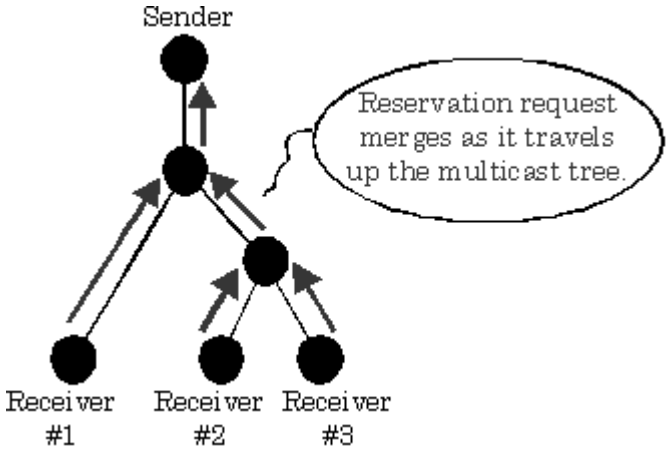
CSPF calculation results with an ordered set of IP addresses that map to next-hop IP addresses of routers forming an LSP, in turn mapping to the TE tunnel. This ordered set is defined by the headend router that is propagated to other routers in the LSP. The intermediate routers, thus, do not perform the function of path selection. RSVP with TE extensions is used to reserve resources in the LSP path as well as label association to the TE tunnel.

RSVP Protocol

A host uses RSVP to request a specific *Quality of Service* (QoS) from the network, on behalf of an application data stream. RSVP carries the request through the network, visiting each node the network uses to carry the stream. At each node, RSVP attempts to make a resource reservation for the stream.



To make a resource reservation at a node, the RSVP daemon communicates with two local decision modules, *admission control* and *policy control*. Admission control determines whether the node has sufficient available resources to supply the requested QoS. Policy control determines whether the user has administrative permission to make the reservation. If either check fails, the RSVP program returns an error notification to the application process that originated the request. If both checks succeed, the RSVP daemon sets parameters in a *packet classifier* and *packet scheduler* to obtain the desired QoS. The packet classifier determines the QoS class for each packet and the scheduler orders packet transmission to achieve the promised QoS for each stream.



A primary feature of RSVP is its scalability. RSVP scales to very large multicast groups because it uses receiver-oriented reservation requests that merge as they progress up the multicast tree. The reservation for a single receiver does not need to travel to the source of a multicast tree; rather it travels only until it reaches a reserved branch of the tree. While the RSVP protocol is designed specifically for multicast applications, it may also make unicast reservations.

RSVP is also designed to utilize the robustness of current Internet routing algorithms. RSVP does not perform its own routing; instead it uses underlying routing protocols to determine where it should carry reservation requests. As routing changes paths to adapt to topology changes, RSVP adapts its reservation to the new paths wherever reservations are in place. This modularity does not rule out RSVP from using other routing services. Current research within the RSVP project is focusing on designing RSVP to use routing services that provide alternate paths and fixed paths.

RSVP runs over IP, both IPv4 and IPv6. Among RSVP's other features, it provides opaque transport of traffic control and policy control messages, and provides transparent operation through non-supporting regions.

The Resource Reservation Protocol (RSVP) is a network-control protocol that enables Internet applications to obtain special qualities of service (QoSs) for their data flows. RSVP is not a routing protocol; instead, it works in conjunction with routing protocols and installs the equivalent of dynamic access lists along the routes that routing protocols calculate. RSVP occupies the place of a transport protocol in the OSI model seven-layer protocol stack. RSVP originally was conceived by researchers at the University of Southern California (USC) Information Sciences Institute (ISI) and Xerox Palo Alto Research Center. The Internet Engineering Task Force (IETF) is now working toward standardization through an RSVP working group. RSVP operational topics discussed in this chapter include data flows, quality of service, session startup, reservation style, and soft state implementation.

RSVP with TE Extensions: Signaling

RSVP reserves bandwidth along a path from a specific source to destination. RSVP messages are sent by the head end router in a network to identify resource availability along the path from a specific source to destination. The head end router is always the source of the MPLS TE tunnel, and the tail end router is the router that functions as the endpoint for the TE tunnel. After the RSVP messages are sent, the status of routers in the path (resource availability) information is stored in the path message as it traverses the network. RSVP, therefore, communicates the requirements of a specific traffic flow to the network and gathers information about whether the requirements can be fulfilled by the network.

The four main messages used in implementation of RSVP for TE are the ***RSVP PATH message,*** the ***RSVP RESERVATION message, RSVP error messages,*** and ***RSVP tear messages.***

In MPLS TE, RSVP is used to ensure and verify resource availability, as well as apply the MPLS labels to form the MPLS TE LSP through the routers in the network:

RSVP PATH message— Generated by the head end router and is forwarded through the network along the path of a future TE LSP. At each hop, the PATH message checks the availability of requested resources and stores this information. In our network the PATH message is generated by Router PE1-AS1, the head end router, and is forwarded downstream where it checks resource availability at each hop (P1-AS1 and PE2-AS1). The RSVP PATH message functions as a label request in MPLS TE domain. Because all TE domains function with downstream-on-demand label allocation mode, the request to assign a label is generated at the head end router and propagated downstream.

RSVP RESERVATION message— Created by the tail end router in the MPLS TE domain and used to confirm the reservation request that was sent earlier with the PATH messages. In the network, PE2-AS1 will generate the RSVP RESERVATION message in response to the PATH message. Therefore, PATH messages function as reservation requests and RESERVATION messages function as reservation confirmations for the availability of requested resources. The RSVP RESERVATION message performs the function of label assignment for a particular LSP mapping to the TE tunnel. As the MPLS domain label allocation and distribution is performed downstream-on-demand, the label mapping to a TE LSP is first generated by the tail end router or egress Edge LSR and then propagated upstream. This process is repeated at each hop upstream where local labels mapping to a TE tunnel are assigned and propagated upstream until the head end router is reached.

RSVP error messages— In the event of unavailability of the requested resources, the router generates RSVP error messages and sends them to the router from which the request or reply was received. If Router P1-AS1 is unable to accommodate requested resources as defined in the PATH message generated by PE1-AS1 (head end router), the router generates a PATH ERROR (PATHERR) message and sends it to its upstream LSR PE1-AS1.

If the RSVP PATH message successfully reaches the tail end router, the tail end Router PE2-AS1 generates a RESERVATION message. If in the time lapsed between P1-AS1 receiving the PATH message from PE1-AS1 to receiving the RESERVATION message from PE2-AS1, P1-AS1 identifies a lack of resources to confirm the request, P1-AS1 will send a RESERVATION ERROR (RESVERR) message to its downstream LSR PE2-AS1 denying the reservation.

RSVP tear messages— RSVP creates two types of tear messages, namely, the PATH tear message and the RESERVATION tear message. These tear messages clear the PATH or RESERVATION states on the router instantaneously. The process of clearing a PATH or RESERVATION state on a router using tear messages enables the reuse of resources on the router for other requests. The PATH tear messages are usually generated in inter-area LSP creation where the inter-area LSP is not configured to be fast reroutable, and if a link failure occurs within an area, the LSR to which the failed link is directly attached will generate an RSVP PATH error and an RESV tear message to the headend. The headend will then generate an RSVP PATH tear message. The corresponding path option will be marked as invalid for a certain amount of time and the next path option will be immediately evaluated if it exists.

RSVP Operation in MPLS TE

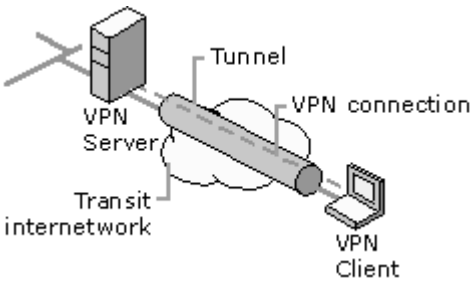
As mentioned earlier, the result of a CSPF or CBR calculation on the headend router is an ordered list of IP addresses that identifies the next hops along the path of the TE tunnel or LSP. This list of routers is computed and is known only to the headend router that is the source of the TE tunnel. Other routers in the domain do not perform a CBR calculation. The headend router provides information to the routers in the TE tunnel path via RSVP signaling to request and confirm resource availability for the tunnel. RSVP with extensions for TE reserves appropriate resources on each LSR in the path defined by the headend router and assigns labels mapping to the TE tunnel LSP.
The RSVP extensions to enable RSVP use for signaling in an MPLS environment to implement TE are defined in Table. The functions of each of these extensions/objects in the messages are also outlined.

In the implementation of RSVP for MPLS TE, RSVP with extensions for TE requests as well as confirms the LSP, reserves resources as requested on all LSP path routers, and applies MPLS labels to form the MPLS LSP through the network. Note that the routers store a copy of the PATH request as the request is forwarded to the next-hop LSR. This information identifies the interface as reservation messages are received on the same LSR to an egress interface to the headend router. In the next section, you will be introduced to the constraint-based SPF calculation process and the need for a link-state protocol to enable MPLS TE dynamically in a service provider core.

Introduction to VPN

A virtual private network (VPN) is the extension of a private network that encompasses links across shared or public networks like the Internet. A VPN enables you to send data between two computers across a shared or public internetwork in a manner that emulates the properties of a point-to-point private link. The act of configuring and creating a virtual private network is known as virtual private networking.

To emulate a point-to-point link, data is encapsulated, or wrapped, with a header that provides routing information allowing it to traverse the shared or public transit internetwork to reach its endpoint. To emulate a private link, the data being sent is encrypted for confidentiality. Packets that are intercepted on the shared or public network are indecipherable without the encryption keys. The portion of the connection in which the private data is encapsulated is known as the tunnel. The portion of the connection in which the private data is encrypted is known as the virtual private network (VPN) connection.



VPN connections allow users working at home or on the road to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public internetwork (such as the Internet). From the user's perspective, the VPN connection is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate internetwork is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.

VPN technology also allows a corporation to connect to branch offices or to other companies over a public internetwork (such as the Internet), while maintaining secure communications. The VPN connection across the Internet logically operates as a wide area network (WAN) link between the sites.

In both of these cases, the secure connection across the internetwork appears to the user as a private network communication—despite the fact that this communication occurs over a public internetwork—hence the name virtual private network.
VPN technology is designed to address issues surrounding the current business trend toward increased telecommuting and widely distributed global operations, where workers must be able to connect to central resources and must be able to communicate with each other.

To provide employees with the ability to connect to corporate computing resources, regardless of their location, a corporation must deploy a scalable remote access solution. Typically, corporations choose either an MIS department solution, where an internal information systems department is charged with buying, installing, and maintaining corporate modem pools and a private network infrastructure; or they choose a value-added network (VAN) solution, where they pay an outsourced company to buy, install, and maintain modem pools and a telecommunication infrastructure.

Neither of these solutions provides the necessary scalability, in terms of cost, flexible administration, and demand for connections. Therefore, it makes sense to replace the modem pools and private network infrastructure with a less expensive solution based on Internet technology so that the business can focus on its core competencies. With an Internet solution, a few Internet connections through Internet service providers (ISPs) and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients and branch offices.

Common Uses of VPNs

- Remote Access Over the Internet
- Connecting Networks Over the Internet
- Connecting Computers over an Intranet

Basic VPN Requirements

Therefore, a VPN solution should provide at least all of the following:

- **User Authentication**. The solution must verify the VPN client's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.
- **Address Management**. The solution must assign a VPN client's address on the intranet and ensure that private addresses are kept private.
- **Data Encryption**. Data carried on the public network must be rendered unreadable to unauthorized clients on the network.
- **Key Management**. The solution must generate and refresh encryption keys for the client and the server.
- **Multiprotocol Support**. The solution must handle common protocols used in the public network. These include IP, Internetwork Packet Exchange (IPX), and so on.
- **IPSec tunnel mode**. IPSec tunnel mode allows IP packets to be encrypted, and then encapsulated in an IP header to be sent across a corporate IP internetwork or a public IP internetwork such as the Internet.
-

Accounting, Auditing, and Alarming

To properly administer a VPN system, network administrators should be able to track who uses the system, how many connections are made, unusual activity, error conditions, and situations that may indicate equipment failure. This information can be used for billing, auditing, and alarm or error-notification purposes.

The RADIUS protocol defines a suite of call-accounting requests that are independent from the authentication requests discussed above. These messages from the NAS to the RADIUS server request the latter to generate accounting records at the start of a call, the end of a call, and at predetermined intervals during a call. The Routing and Remote Access service can be configured to generate these RADIUS accounting requests separately from connection requests (which could go to the domain controller or to a RADIUS server). This allows an administrator to configure an accounting RADIUS server, whether RADIUS is used for authentication or not. An accounting server can then collect records for every VPN connection for later analysis. A number of third-parties have already written billing

Introduction to Layer 2 VPNs

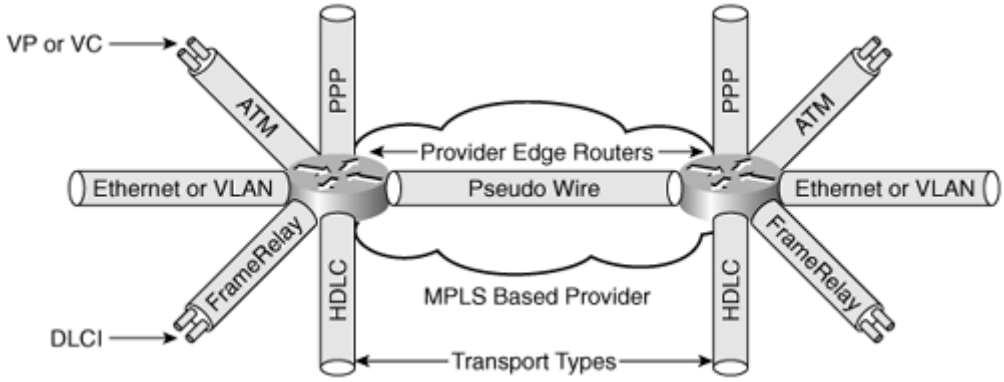
Layer 2 VPNs were originally implemented using Layer 2 technologies like Frame Relay and ATM. However, there has been a considerable shift in technology; service provider (SP) networks are transitioning from circuit-switched networks to packet-switched networks. This shift is primarily due to increased revenue generation opportunities and improved management of current network resources. Overall, Layer 2 VPNs help reduce the cost for the provider because the cost of managing separate networks (TDM, FR, ATM, IP) is much higher from both a CAPEX and OPEX perspective than managing one larger aggregate network.

SPs can support both Layer 2 VPNs and Layer 3 MPLS VPNs over a single infrastructure because MPLS-enabled networks allow seamless integration of Layer 2 and Layer 3 services. Layer 2 VPNS provide several benefits, such as

- Consolidation of multiple Layer 2 networks within enterprise or SP environments into one core network with Layer 2 services running over a common IP/MPLS core. This enables the SP to deliver transparent services to end customers.
- The ability to seamlessly extend LANs as private virtual LANs across a SP's network and to deliver multipoint Ethernet services.

A Layer 2 VPN is defined as a VPN comprising switched connections between subscriber endpoints over a shared network. shows an MPLS-based provider that offers Layer 2 VPN services.

Layer 2 VPNs



INTRODUCTION TO MPLS L2 VPN

Traditional VPN

Traditional VPNs based on Asynchronous Transfer Mode (ATM) or Frame Relay (FR) are quite popular. They share the network infrastructure of carriers. However, they have some inherent disadvantages:

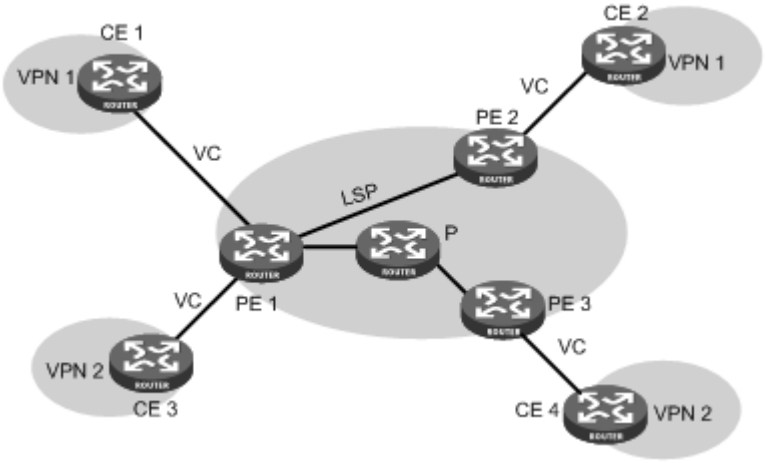
· Dependence on dedicated media: To provide both ATM-based and FR-based VPN services, carriers must establish two separate infrastructures across the whole service scope, one ATM infrastructure and one FR infrastructure. Apparently, the cost is very high and the infrastructures are not utilized efficiently.
· Complicated deployment: To add a site to an existing VPN, you have to modify the configurations of all edge nodes connected with the VPN site.
MPLS L2VPN is developed as a solution to address the above disadvantages.

MPLS L2 VPN

MPLS L2VPN provides Layer 2 VPN services on the MPLS network. It allows carriers to establish L2VPNs on different data link layer protocols, including ATM, FR, VLAN, Ethernet and PPP.

MPLS L2VPN transfers Layer 2 user data transparently on the MPLS network. For users, the MPLS network is a Layer 2 switched network and can be used to establish Layer 2 connections between nodes.

Consider ATM as an example. Each customer edge device (CE) can connect to the MPLS network through an ATM virtual circuit (VC) to communicate with another CE. This is similar to that on an ATM network.



Comparison with MPLS L3 VPN

Compared with MPLS L3VPN, MPLS L2VPN has the following advantages:

· High scalability: MPLS L2VPN establishes only Layer 2 connections. It does not involve the routing information of users. This greatly reduces the load of the PEs and even the load of the whole service provider network, enabling carriers to support more VPNs and to service more users.
· Guaranteed reliability and private routing information security: As no routing information of users is involved, MPLS L2VPN neither tries to obtain nor processes the routing information of users, guaranteeing the security of the user VPN routing information.
· Support for multiple network layer protocols, such as IP, IPX, and SNA.

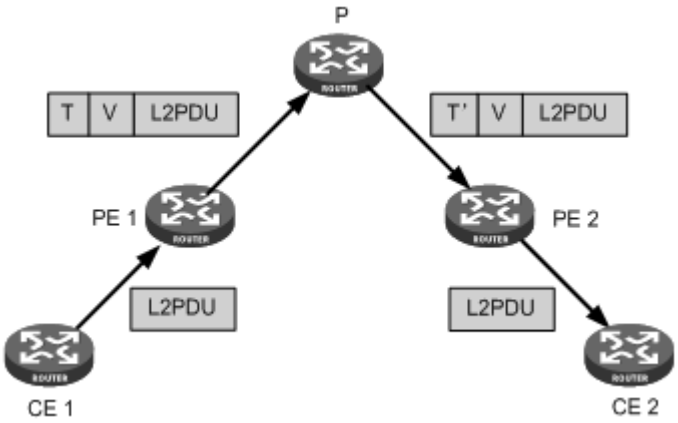
BASIC CONCEPTS OF MPLS L2VPN

In MPLS L2VPN, the concepts and principles of CE, PE and P are the same as those in MPLS L3VPN:

· Customer edge device (CE): A CE resides on a customer network and has one or more interfaces directly connected with service provider networks. It can be a router, a switch, or a host. It cannot "sense" the existence of any VPN, neither does it need to support MPLS.
· Provider edge router (PE): A PE resides on a service provider network and connects one or more CEs to the network. On an MPLS network, all VPN processing occurs on the PEs.
· Provider (P) router: A P router is a backbone router on a service provider network. It is not directly connected with any CE. It only needs to be equipped with basic MPLS forwarding capability.
MPLS L2VPN uses label stacks to implement the transparent transmission of user packets in the MPLS network.

· Outer label, also called tunnel label, is used to transfer packets from one PE to another.
· Inner label, also called VC label, is used to identify different connections between VPNs.
· Upon receiving packets, a PE determines to which CE the packets are to be forwarded according to the VC labels.
Figure 2 illustrates how the label stack changes in the MPLS L2VPN forwarding process.

Figure 2 MPLS L2VPN label stack processing



IMPLEMENTATION OF MPLS L2 VPN

MPLS L2VPN can be implemented in one of the following methods:

· Circuit Cross Connect (CCC) and Static Virtual Circuit (SVC)—Two methods of implementing MPLS L2VPN by configuring VC labels statically.
· Martini—A method for establishing point-to-point links to implement MPLS L2VPN. It uses Label Distribution Protocol (LDP) as a signaling protocol to transfer VC labels.
· Kompella—A CE-to-CE mode for implementing MPLS L2VPN on the MPLS network. It uses multiprotocol BGP as the signaling protocol to advertise Layer 2 reachability information and VC labels.
The switch supports only Martini MPLS L2VPN. The following section describes the characteristics of Martini MPLS L2VPN.

CONFIGURING MPLS L2 VPN

You can select any of the implementation methods for MPLS L2VPN as needed. However, no matter what method you select, you must complete the following tasks:

· Configure MPLS basic capability
· Enable L2VPN
· Enable MPLS L2VPN

Follow these steps to configure MPLS L2VPN:

To do…	Use the command…	Remarks
Enter system view	system-view	—
Configure the LSR ID	mpls lsr-id *lsr-id*	Required
Configure MPLS basic capability and enter MPLS view	mpls	Required
Return to system view	quit	—
Enable L2VPN and enter L2VPN view	l2vpn	Required Disabled by default
Enable MPLS L2VPN	mpls l2vpn	Required Disabled by default

CONFIGURING ETHERNET ENCAPSULATION FOR THE INTERFACE

· If the interface is a Layer 3 Ethernet interface, it uses Ethernet encapsulation. For configuration information about Layer 3 Ethernet interface,
· If the interface is an access-type VLAN interface, it uses Ethernet encapsulation. For configuration information about VLAN interface and link type, see the *Layer 2—LAN*

CONFIGURING VLAN ENCAPSULATION FOR THE INTERFACE

· If the interface is aLayer 3 Ethernet subinterface, it uses VLAN encapsulation. For configuration information about Layer 3 Ethernet subinterface, see the *Interface Configuration Guide*.
· If the interface is a trunk-type or hybrid-type VLAN interface, it uses VLAN encapsulation. The VLAN to which the interface belongs is the same as the VLAN of the CE. For configuration information about VLAN interface and link type, see the *Layer 2—LAN Switching Configuration Guide*.

L3 MPLS VPN

MPLS has gained increasing interest from service providers over the past few years. It was originally used for traffic engineering purposes. Now, the latest application of MPLS is implementing provider provisioned VPNs. Using MPLS for implementing VPNs is a viable alternative to using a pure layer-2 solution, a pure layer-3 solution, or any of the tunnelling methods commonly used for implementing VPNs.

Multiprotocol Label Switching (MPLS) is a mechanism in high-performance telecommunications networks which directs and carries data from one network node to the next. MPLS makes it easy to create "virtual links" between distant nodes. It can encapsulate packets of various network protocols.

L3 VPN is the most favourite application that is used on top of MPLS network. Due to its popularity, there is an active developer community trying to generate new ways to get advantage of the technique.

The layer-3 approach to creating MPLS-based VPNs offers a routed solution to the problem The de facto standard for implementing such VPNs is described in “RFC 2547”, with a new version, currently, under development referred to as 2547bis which is described in “draft-ietf-ppvpn-rfc2547bis-01.txt”. The approach is also referred to as BGP/MPLS VPNs.

Type of Traffic Supported
Comparing both approaches described above, it is clear that the layer-3 approach offers transport of IP traffic only. On the other hand, the layer-2 approach allows transporting any customer layer-3 protocol packets: IPv4, IPv6, IPX, DECNet, OSI, etc. Many enterprise customers still use other protocols than IP in their IT infrastructure, hence, a layer-2 service is less restricting for them. Also, with IPv6 on the horizon, some organizations are already experimenting with IPv6, and in the near future, many will be migrating to it. To continue providing connectivity for those organizations using a layer-3 solution would require some enhancement to the current standard – like creating a VPNIPv6 address family – and might require some upgrades to the provider’s routers. A layer-2 solution could continue to serve those organizations, even when the provider network has not yet been upgraded to use IPv6 internally. The mechanisms behind BGP/MPLS VPNs were designed to address some of the shortcomings of the pure layer-3 VPNs (without tunneling) that preceded it. Some of the main goals were: Supporting globally

unique IP addresses on the customer side, as well as private non unique and hence, overlapping – addresses.

Supporting overlapping VPNs, where one site could belong to more than one VPN. Since this type of VPNs relies on routing, achieving the above mentioned goals could be a challenge.

Possible Connectivity Scenarios
Several connectivity scenarios for customer sites could be implemented using both approaches. Both approaches could be used to implement the following connectivity scenarios:
1. Point-to-Point.
2. Hub and Spoke.
3. Partial Mesh.
4. Full Mesh.
5. Overlapping VPNs.

The layer-3 approach performs well at implementing scenarios 1, 4, and 5 in a manner that is transparent to the CE devices. However, the layer-3 approach could get a bit more complicated when implementing scenarios 2 and 3.

The approach relies on taking customer IP datagrams from a given site, looking up the destination IP address of the datagram in a forwarding table, then sending that datagram to its destination across the provider's network using an LSP.

Advantages
- Cost effective solution with QoS capabilities.
- Increased response time and improved application performance through reduced "hops" between network points.
- Less or no downtime as redundant paths are made available in the MPLS cloud.
- Allow quick traffic re-routing, providing continued application availability.