

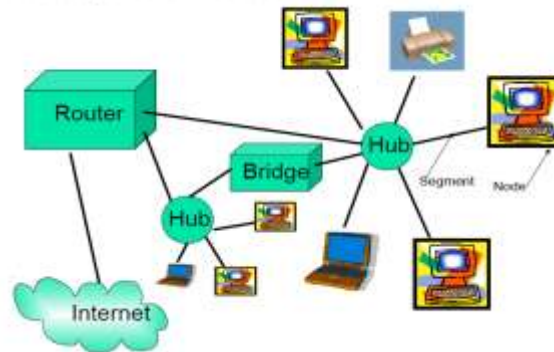
Chapter 1: Introduction

Introduction to Computer Network

What is computer Network?

Computer Network is a collection of computing devices. Devices are connected in various ways in order to communicate and share resources. Usually, the connections between computers in a network are made using physical wires or cables. Sometime connections are wireless, using radio waves or infrared signals. Example, a computer network can consists of a collection of computers, printers and other equipment like router, switch and servers that is connected together so that they can communicate with each other.

An example of a network



Uses/Application of Computer Network

Computer network has a broad range of application. It can be summarized in following points:

1. Business Application
2. Home Application
3. Mobile Users
4. Social Issues

Business Application

Resource sharing

The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource or the user. An obvious and widespread example is having a group of office workers share a common printer.

Telephone calls between employees may be carried by the computer network instead of the phone company. This technology is called IP telephony or Voice over IP (VoIP) when Internet technology is used.

Desktop sharing lets remote workers see and interact with a graphical computer screen. This makes it easy for two or more people who work far apart to write a report together.

Many companies are doing business electronically, especially with customers and suppliers. This new model is called e-commerce (electronic commerce) and it has grown rapidly in recent years. Airlines, bookstores, and other retailers have discovered that many customers like the convenience of shopping from home.

Home Application

The biggest reason to buy a home computer was probably for Internet access. Internet access provides home users with connectivity to remote computers. As with companies, home users can access information, communicate with other people, and buy products and services with e-commerce. Access to remote information comes in many forms. It can be surfing the World Wide Web for information or just

for fun. Information available includes the arts, business, cooking, government, health, history, hobbies, recreation, science, sports, travel, and many others.

Mobile Users

Mobile computers, such as laptop and handheld computers are one of the fastest-growing segments of the computer industry. People on the go often want to use their mobile devices to read and send email, tweet, watch movies, download music, play games, or simply to surf the Web for information. They want to do all of the things they do at home and in the office. Naturally, they want to do them from anywhere on land, sea or in the air.

Wireless networks are of great value to fleets of trucks, taxis, delivery vehicles, and repairpersons for keeping in contact with their home base. Perhaps the key driver of mobile, wireless applications is the mobile phone.

Text messaging or texting is tremendously popular. It lets a mobile phone user type a short message that is then delivered by the cellular network to another mobile subscriber. Since mobile phones know their locations, often because they are equipped with GPS (Global Positioning System) receivers, some services are intentionally location dependent. Mobile maps and directions are an obvious candidate as your GPS-enabled phone and car probably have a better idea of where you are than you do.

Social Issues

Social networks, message boards, content sharing sites, and a host of other applications allow people to share their views with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise. The trouble comes with topics that people actually care about, like politics, religion, or sex. Views that are publicly posted may be deeply offensive to some people. Furthermore, opinions need not be limited to text; high-resolution color photographs and video clips are easily shared over computer networks.

Computer networks make it very easy to communicate. They also make it easy for the people who run the network to snoop on the traffic.

There are multi-person messaging services too, such as the Twitter service that lets people send short text messages called “tweets” to their circle of friends or other willing audiences. The Internet can be used by applications to carry audio (e.g., Internet radio stations) and video (e.g., YouTube). One of the most popular social networking sites is Facebook. It lets people update their personal profiles and shares the updates with other people who they have declared to be their friends.

Advantages and Disadvantages of Computer Network

Advantages

- File Sharing
- Resource Sharing
 - Device sharing(Printers)
- In-expensive setup
 - Sharing Resource reduce Cost
- Flexible Handling
 - Easy For Network Admin to Manage Resource
 - User can login from any Host and access his/her files
- Increased Resource Capacity
 - By Sharing Resource

Disadvantages

- Security Concerns
 - Computer within a Network can be Vulnerable

- Malware (Malicious software)
 - Malicious software (worms, viruses, Trojan Horse, Logic bomb, zombie)
- Lack of Robustness
 - Break down of Central System disrupt the Entire System
- Needs An Efficient Handler
 - Required Technically qualified Candidate to maintain the system

Overview of Network Types

- **LAN (Local Area Network)**
A LAN is a network that is used for communicating among computer devices, usually within an office building or home. LAN's enable the sharing of resources such as files or hardware devices that may be needed by multiple users
- **PAN (Personal Area Network)**
PAN network is a computer network that allows devices to communicate around a single person. The network is structured for a single entity which can be in a small office, a building or apartment. PAN network connects different peripherals such as computers, telephones, video game consoles.
- **CAN (Campus Area Network)**
It is a type of network built upon connection of various LAN networks within restricted geographical area. It is also known as corporate network. These are interconnected with high speed Ethernet using optical fiber. The range of CAN varies from 1 km to 5 km.
- **MAN (Metropolitan Area Network)**
It is a large computer network that usually spans a city or a large campus. A MAN is optimized for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. Examples of MAN: Telephone company network that provides a high speed DSL to customers and cable TV network.
- **WAN (Wide Area Network)**
WAN covers a large geographic area such as country, continent or even whole of the world. A WAN is two or more LANs connected together. Multiple LANs can be connected together using devices such as bridges, routers, or gateways, which enable them to share data. The world's most popular WAN is the Internet.
- **GAN (Global Area Network)**
A **global network**, such as the internet, is referred to as the Global Area Network (GAN). The internet is, however, not the only computer network of its kind. Internationally operating companies also support local networks that comprise of several WANs and connect company computers across the world. GANs use the fiber optic infrastructure from wide area networks and combine these with **international undersea cables** or **satellite transmissions**.

Overview of Network Topologies

Topology - Physical and logical network layout

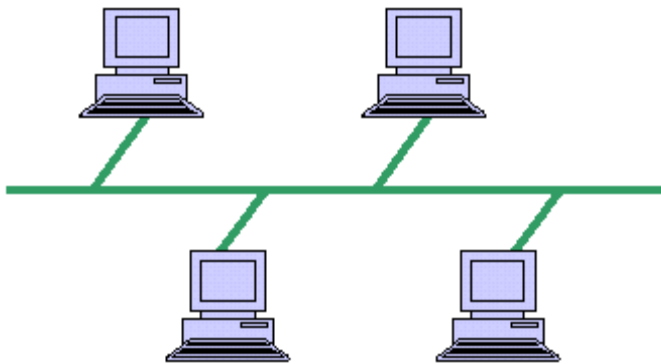
- Physical – actual layout of the computer cables and other network devices
- Logical – the way in which the network appears to the devices that use it

Bus Topology

Bus consists of a single linear cable called a trunk.

Data is sent to all computers on the trunk.

Each computer examines EVERY packet on the wire to determine who the packet is for and accepts only messages addressed to them.



Advantages	Disadvantages
Cheap and easy to implement	Network disrupts when computer are added or removed
Require less cable	A break in the cable will affect all the networks

Distributed Bus

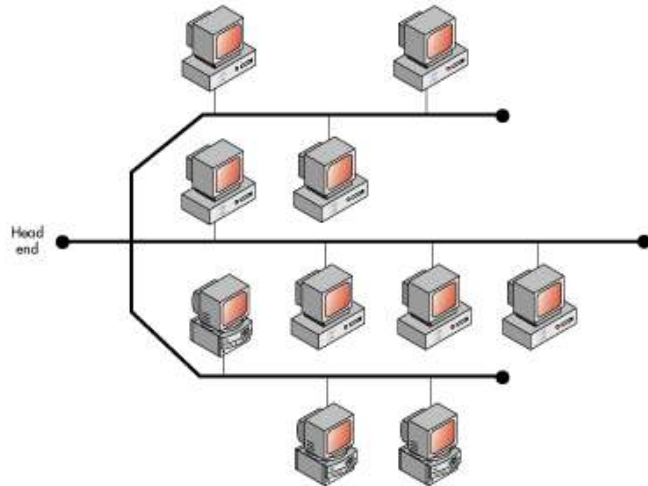
A more complex form of the physical bus topology is the distributed bus.

In the distributed bus, the trunk cable starts at what is called a "root" or "head end", and branches at various points along the way.

Unlike the simple bus topology, this variation uses a trunk cable with more than two end points.

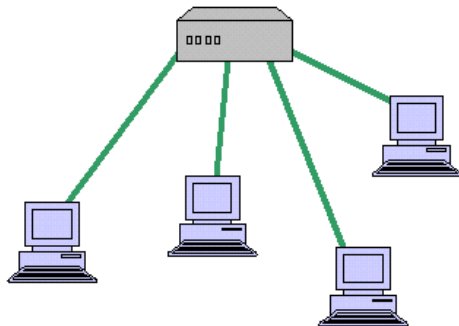
Where the trunk cable branches, the division is made by means of a simple connector.

This topology is susceptible to bottlenecking and single-point failure.



Star Topology

- All computers/devices connect to a central device called hub or switch.
- Each device requires a single cable
- Point-to-point connection between the device and hub.
- Most widely implemented

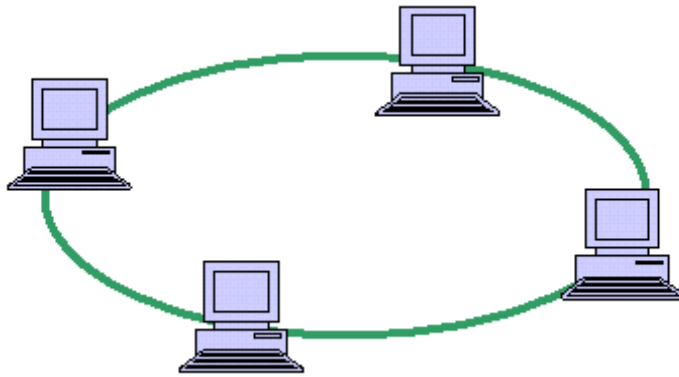


Advantages	Disadvantages
Easily expanded without disruption to the network	Requires more cable
Cable failure affects only a single user	Centralized device-Single point of failure

Ring Topology

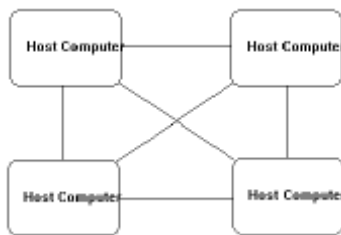
- Computers are connected on a single circle of cable.
- Usually seen in a Token Ring or FDDI (fiber optic) network.

Advantages	Disadvantages
Cable fault are easily located making troubleshooting easier	Expansion to the network can cause network disruption
Easy to install	A single break in the cable can disrupt entire network



Mesh Topology

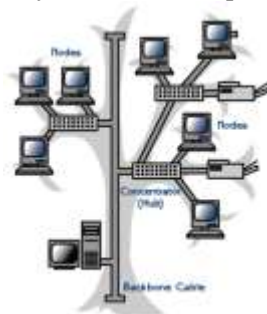
- Each computer connects to every other.
- High level of redundancy.



Advantages	Disadvantages
Provide redundant path between devices	Require more cable than the other LAN topologies
Network can be expanded without disruption	Complicated implementation

Tree Topology

- A tree topology (hierarchical topology) can be viewed as a collection of star networks arranged in a hierarchy.
- This tree has individual peripheral nodes which are required to transmit to and receive from one other only and are not required to act as repeaters or regenerators.



Advantages	Disadvantages
Expansion of network is easy	Relies on main bus cable, if it breaks entire system fails
Easy error detection and correction	Slow as number of devices increases
If one segment is affected other are not affected	

Hybrid Topology

- A combination of any two or more network topologies.
- A hybrid topology always accrues when two different basic network topologies are connected.

CLIENT SERVER MODEL

A client-server network consists of a number of devices called clients who acquire services from the relatively powerful devices called servers. Client devices are typically PCs or mobile devices with network software applications installed. Server device typically stores files, databases and applications like Web sites. The client-server model can be used on the Internet as well as local area networks (LANs). Examples of client-server systems on the Internet include Web browsers and Web servers, FTP clients and servers, and DNS.

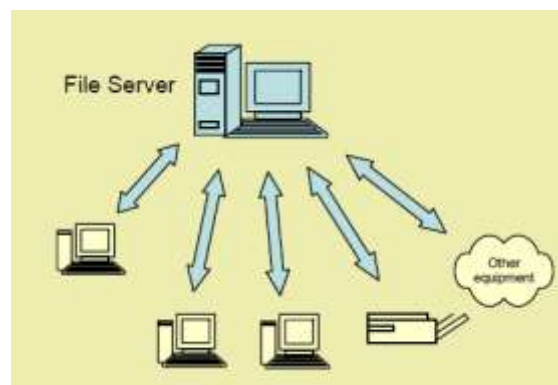


Figure: Client Server model

If we look at the client-server model in detail, we see that two processes (i.e., running programs) are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. These messages are shown in figure below.

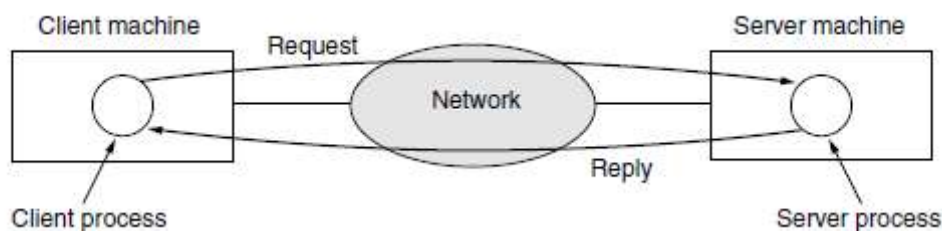


Figure: request and replies in client server model

Client and its function

Thin client– a personal computer that does not have to be very powerful because it only presents the user interface to the user. It is largely used for interaction with processing layers. Example: Increasingly PDA's, Handhelds or Smart phones

Fat client–a typically powerful personal computer capable of independent application processes. Also notebook computer or workstation

Different types of server and function

Database server– a server that hosts one or more databases, (Executing all data manipulation commands at the server)

Transaction server– a server that hosts services which ensure that all database updates for a transaction succeed or fail as a whole. (Crucial in banking contexts –cash machines; online shopping ...)

Application server–a server that hosts application logic and services for an information system. (between interface & database)

Messaging or groupware server– a server that hosts services for e-mail, calendaring, and other work group functionality.

Web server– a server that hosts Internet or intranet websites, (sends data (XML) and documents (HTML) to clients)

PEER-TO-PEER NETWORK

P2P is a distributed network architecture, which consists of devices known as peers that share their own resources (disk storage, processing power or network bandwidth) directly, without the need for central server. Peer-to-peer is popular for file sharing on the Internet. Peer-to-peer systems often implement an Application Layer overlay network on top of the native or physical network topology.

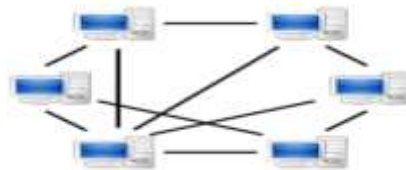


Figure: Peer-to-Peer Network

Peer-to-Peer computing is inspired by the controversial music-sharing service Napster. Instead of Internet information being held in a few central locations, Peer-to-Peer computing makes it theoretically possible to access the files and data residing on every personal computer connected to the Internet.

Problem with Server-Client Model

- **Scalability**

As the number of users increases, there is a higher demand for computing power, storage space, and bandwidth associated with the server-side

- **Reliability**

The whole network will depend on the highly loaded server to function properly

Advantage of P2P model

- The system is based on the direct communication between peers
- There is zero reliance on centralized service or resources for operations
- The system can survive extreme changes in network composition
- They thrive in a network with heterogeneous environment
- This model is highly scalable

Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	Client/Server Networks
• Easy to set up	• More difficult to set up
• Less expensive to install	• More expensive to install
• Can be implemented on a wide range of operating systems	• A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
• More time consuming to maintain the software being used (as computers must be managed individually)	• Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
• Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	• High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings
• Ideal for networks with less than 10 computers	• No limit to the number of computers that can be supported by the network
• Does not require a server	• Requires a server running a server operating system
• Demands a moderate level of skill to administer the network	• Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

ACTIVE NETWORK

An active network is a network in which the nodes are programmed to perform custom operations on the messages that pass through the node. For example, a node could be programmed or customized to handle packets on an individual user basis or to handle multicast packets differently than other packets. Active network approaches are expected to be especially important in networks of mobile users. Smart packets will use a special self-describing language that allows new kinds of information to be carried within a packet and operated on by a node. The architecture to implement an active network is composed of an execution environment that can execute active packets and a node operating system capable of supporting one or more execution environments. It also consists of active hardware, capable of routing or switching as well as executing code within active packets. Network processors are one means of implementing active networking concepts.

Advantages of Active Network

- Adaptive monitoring and predictive control
- Enables on-the-fly experimentation
- Minimizes global agreement overhead
- Enables more flexible network
- Reduces protocol deployment time from years to months
- Enables faster development of new services

Chapter 2: Reference Model

Protocols and Standards

Protocol is defined as a set of rules that governs any task. In computer network, it is a set of rules that governs the communication between two ends of communication. Different protocols exist at different levels during communication. eg. In OSI model, there are 7 layers and each layer has certain protocols to perform one or more task. Some network protocols are HTTP (Hyper Text Transfer Protocol), FTP (File Transfer protocol), etc

Standards are guidelines that are common to all the stakeholders. It explains how a particular protocol should operate.

De facto standards are that which are not approved by an organized body but are adopted as standards through widespread use. eg., MS Office

De jure are standards that have been legislated by an officially recognized body.

Some standards organizations are ISO (International Standards Organization), ANSI (American National Standards Institute), IEEE (Institute of Electrical and Electronics Engineers), EIA (Electronic Industries Alliance), etc

Interfaces and Services

In layered network architecture, there are a set of layers and protocols. The layers are organized as a stack, with each one built upon the one below it. A layered architecture with four layers is shown in following figure.

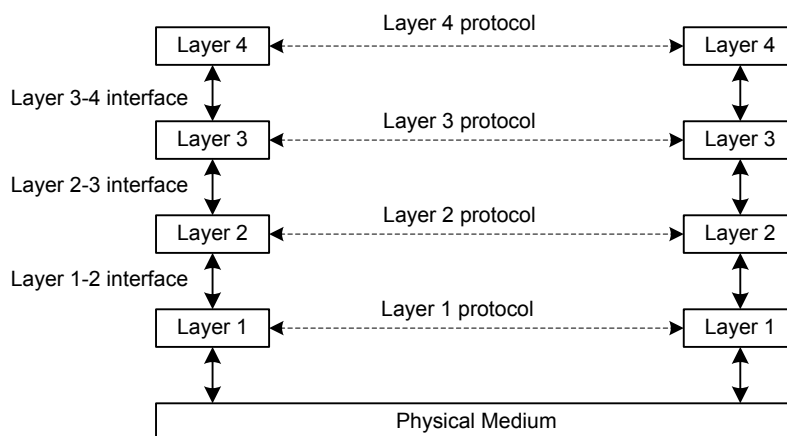


Fig: layer, protocol and interfaces

Each layer defines a family of functions distinct from those of the other layers. By defining and localizing functionality in this fashion, the designers created an architecture that is both comprehensive and flexible.

Interfaces

There is a well defined interface between each pair of adjacent layers that make it possible for the data to pass down through the layers at the sending host and back up through the same set of layers at the receiving host. Each interface defines the information, operation and services a layer must provide for the layer above it. Well-defined interface and layer functions provide greater modularity to a network. As long as a layer provides the expected services to the layers above it a completely different one can replace the implementation.

Services

Within a host, each layer calls upon the services of the layer just below it. For example, Layer 3 uses the service provided by layer 2 and provides its own services for layer 4. Between machines, layer x on one communicates with the corresponding layer x on another machine. This communication is governed by agreed rules of services called protocols. In reality no data are directly transferred from layer x on one machine to the same layer on another machine. Instead, each layer passed data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occur.

Importance of layered architecture

1. Layering reduces the design complexity.

It enables peer process abstraction which makes the unmanageable task of designing the complete network possible to be broken into several smaller manageable design problems, that is, the design of individual layers.

2. Provision of localized services strengthens modularity.

Each layer offers certain services to the higher layers and thus shields those layers from the details of how the offered services are actually implemented. Interfaces on all machines in a network need not be the same, if each machine correctly uses all the protocols.

3. They allow complete interoperability between incompatible systems

By defining the complete layered network model with all the interface details, the services and the protocols it is possible to ensure interoperability among various systems. There can be a seamless operation without considering the operating system or the computer hardware. For example, the OSI model has been developed with this aim.

4. Hardware and software vendor independence.

As long as correct layer functionality is ensured a network can be set up using products from different vendors and still the operation is guaranteed. For example, repeaters, hubs in the physical layer and web browser in the application layer.

OSI MODEL

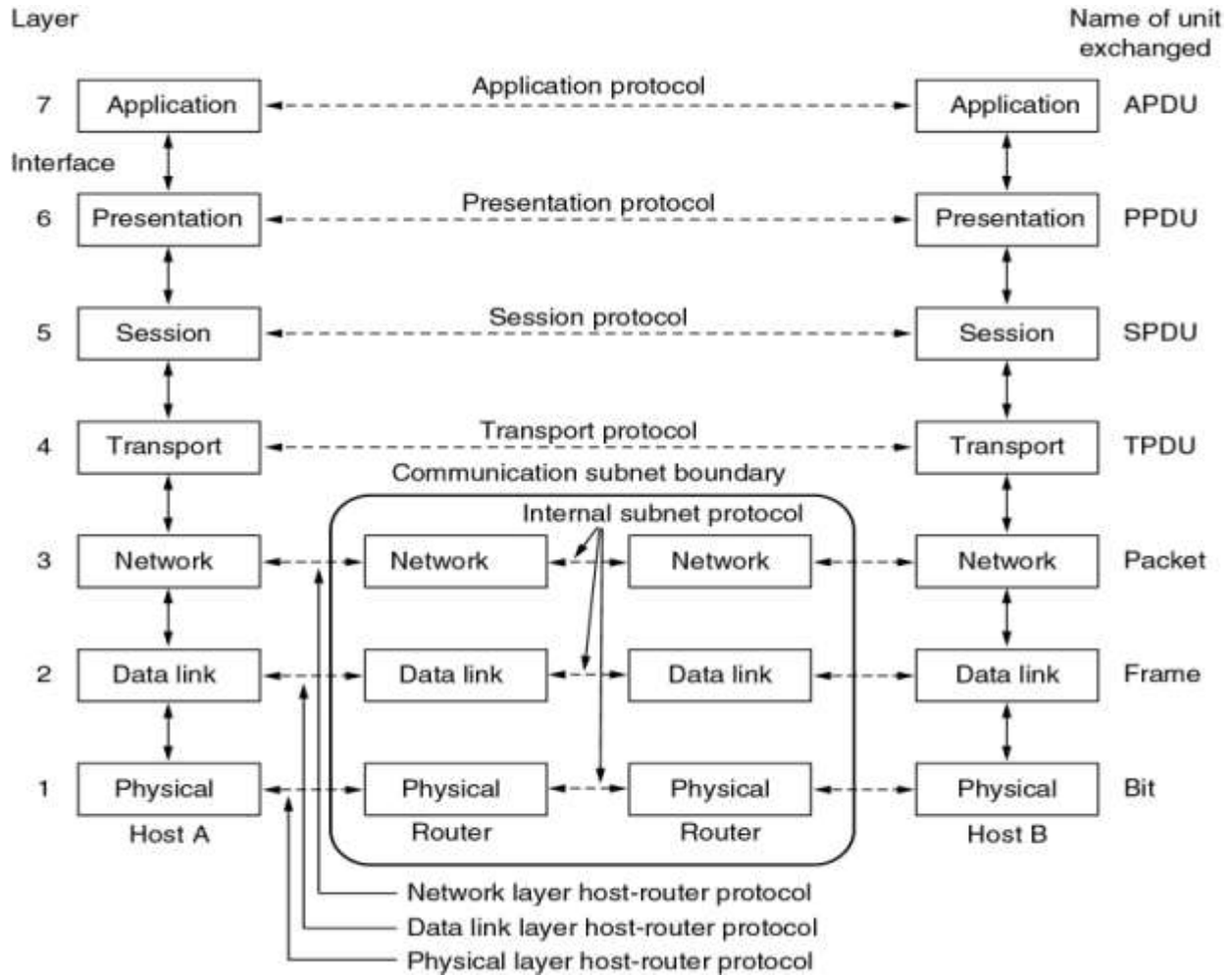


Figure: OSI model

The Physical Layer

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues largely deal with mechanical, electrical, and timing interfaces, as well as the physical transmission medium.

The Data Link Layer

The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors. It break up the input data into **data frames** (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data (i.e., flow control).

The Network Layer

The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. If too many packets are present in the subnet at the same time, they will get in one another's way, forming bottlenecks. Handling congestion is also a responsibility of the network layer, in conjunction with higher layers.

The Transport Layer

The basic function of the transport layer is to accept data from above it, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end. The transport layer also determines what type of service to provide to the session layer, and, ultimately, to the users of the network.

The Session Layer

The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including **dialog control** (keeping track of whose turn it is to transmit), **token management** (preventing two parties from attempting the same critical operation simultaneously), and **synchronization** (check-pointing long transmissions to allow them to pick up from where they left off in the event of a crash and subsequent recovery).

The Presentation Layer

Unlike the lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted.

The Application Layer

The application layer contains a variety of protocols that are commonly needed by users. One widely used application protocol is **HTTP (HyperText Transfer Protocol)**, which is the basis for the World Wide Web.

TCP/IP MODEL

There are 4 layers in the TCP/IP model

Layer 4: Application

Layer 3: Transport

Layer 2: Internet

Layer 1: Network access (Host to Network)

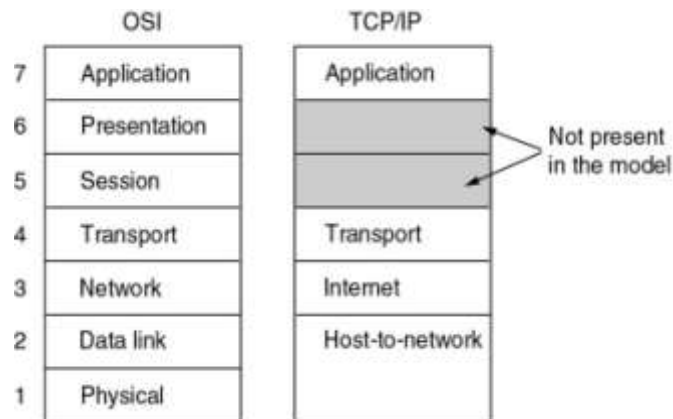


Fig: OSI and TCP/IP model

The network access layer (Host to Network)

Concerned with all of the issues that an IP packet requires to actually make the physical link. It includes all the details in the OSI physical and data link layers.

- Electrical, mechanical, procedural and functional specifications
- Data rate, Distances, Physical connector
- Frames
- Synchronization, flow control, error control

The Internet Layer

It is concerned with Packet Addressing. It sends source packets from any network and have them arrive at the destination independent of the path and networks they took to get there. Packet may arrive in different order to destination. It is job of higher layer to arrange them. It is also important to avoid congestion while packet routing.

The Transport Layer

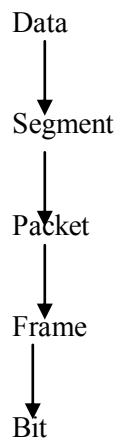
The transport layer deals with the quality-of-service issues of reliability, flow control, and error correction. Two end-to-end transport protocols have been defined here. The first one, **TCP (Transmission Control Protocol)**, is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. The second protocol in this layer, **UDP (User Datagram Protocol)**, is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own.

The Application Layer

The TCP/IP model does not have session or presentation layers. Instead, applications simply include any session and presentation functions that they require. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP).

How data encapsulation and de-encapsulation occurs in OSI model?

Data Encapsulation



Data De-encapsulation

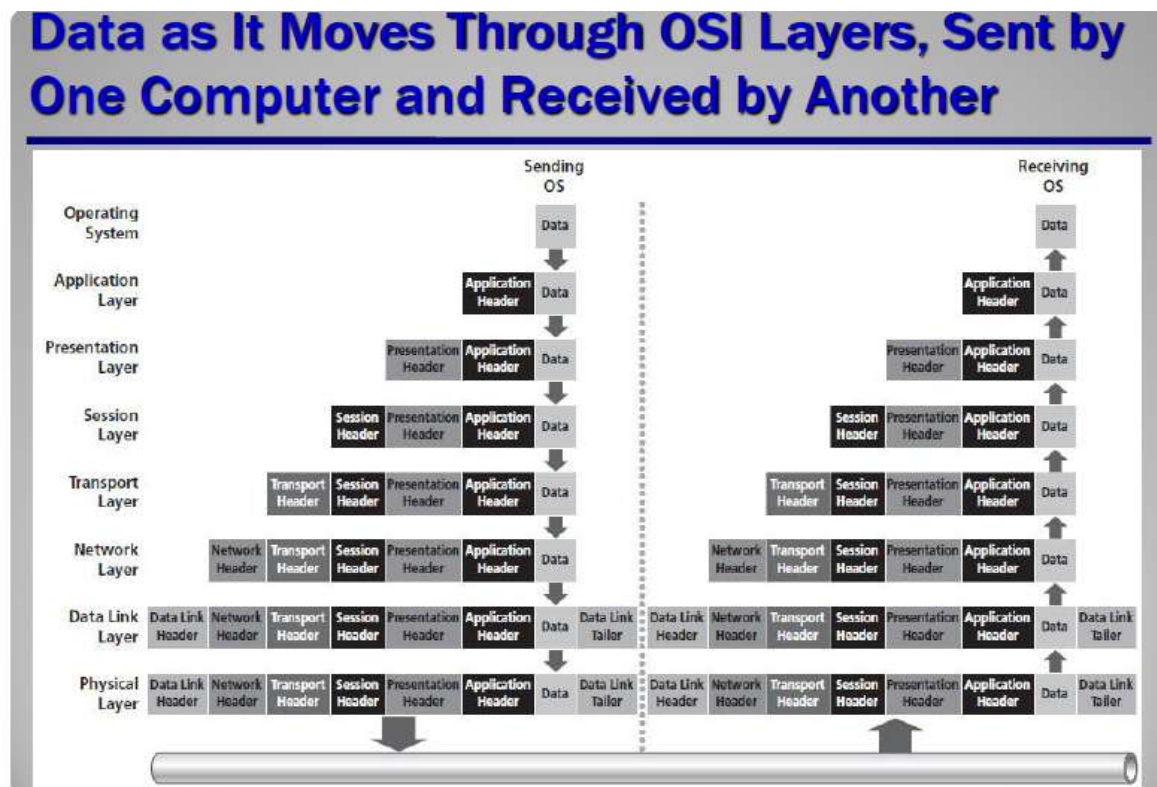
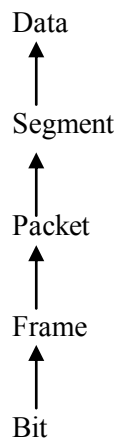


Fig: Data encapsulation and De-encapsulation

Comparison of OSI and TCP/IP

S.N	OSI	TCP/IP
1	It has 7 layers	It has 4 layers
2	OSI model has separate session layer and presentation layer	TCP/IP does not have separate session or presentation layer
3	Transport layer is connection oriented	Transport layer is both connection oriented and connectionless
4	Network layer is both connection oriented and connectionless	Network layer is connectionless
5	OSI is a reference model around which network are built. Generally used as guidance tool	TCP/IP is implementation model around which internet is based.
6	OSI model has a problem of fitting the protocol into the model	TCP/IP model does not fit any protocol
7	Protocols are hidden in OSI model and are easily replaced as the technology changes	In TCP/Ip model, replacing protocol is not easy
8	Concepts central to the OSI model are Services, Interfaces and Protocols	TCP/IP did not originally distinguish between services, interface and protocols.

Networking Hardware: NIC, Hub, Repeaters, Switches, Bridge, Router

NIC (Network Interface Card)

It is a circuit board or card that allows computers to communicate over a network via cables or wirelessly. It is also called network adaptor or network card. It enables clients, servers, printers and other devices to transmit and receive data over the network.

Hub

It is also called An Ethernet hub, active hub, network hub, repeater hub, multiport repeater or hub. It has multiple input/output (I/O) ports. In hub, a signal introduced at the input of any port appears at the output of every port except the original incoming. A HUB works at the physical layer (layer 1) of the OSI model. Hubs are now largely obsolete, having been replaced by network switches except in very old installations or specialized applications.

Repeaters

- Regenerate the signal
- Provide more flexibility in network design

- Extend the distance over which a signal may travel down a cable
- Example → Ethernet HUB
- Connect together one or more Ethernet cable segments of any media type
- Works at Layer 1 of OSI model
- Forwards every frames; has no filtering capability

Bridge

- Join two LAN segments (A,B), constructing a larger LAN
- Filter traffic passing between the two LANs and may enforce a security policy separating different work groups located on each of the LANs.
- Bridges work at the Media Access Control Sub-layer of the OSI model
- A bridge stores the hardware addresses observed from frames received by each interface
- Uses this information to learn which frames need to be forwarded by the bridge.
- Each bridge has two connections (ports) and there is a table associated with each port.
 - A bridge observes each frame that arrives at a port
 - extracts the source address from the frame
 - and places that address in the port's routing table

Switch

- Typically connects individual computers
- A switch is essentially the same as a bridge though typically used to connect hosts, not LANs
- Richer management capability.
- Logically partition the traffic to travel only over the network segments on the path between the source and the destination (reduces the wastage of bandwidth)

Benefits/Advantages

- Improved security
- users are less able to tap-in into other user's data
- Better management
- control who receives what information (i.e. Virtual LANs)
- limit the impact of network problems
- Dedicated access
- Host has direct connection to the switch
- rather than a shared LAN connection

Cut-Through Switching

- Start transmitting as soon as it reads destination address.
- Transmit the head of the packet via the outgoing link while still receiving the tail via the incoming link

- Much faster
- Cannot detect corrupt packets
- Destination is responsible for detecting corrupt packets
- Can propagate the corrupt packets to the network

Store and Forward switching

- Read the whole packet before transmit
- Slower than the cut-through mode
- More accurate since corrupt packets can be detected using the FCS
- More suit to large LAN since they will not propagate error packets

Router

- Layer 3 Devices
- Network Layer in OSI and Internet layer in TCP/IP protocol stack
- Main Function
 - Routing of Packets (Based on Routing Table)
 - Path Selection(Best Path) to forward the packets
 - Internetwork Communications
- Only packets with known network addresses will be passed - hence reduce traffic
- Routers can listen to a network and identify its busiest part
- Will select the most cost effective path for transmitting packets
- Routing table is formed based on communications between routers using “Routing Protocols”
- Routing Protocols collect data about current network status and contribute to selection of the best path

Comparison of hub, switch and Router

	Hub/ Repeater	Bridge/ Switch	Router
Traffic isolation	no	yes	yes
Plug and Play	yes	yes	no
Efficient routing	no	no	yes
Cut through	yes	yes	no

Chapter 3: Physical Layer

Transmission Medium

In a data transmission system, transmission media is anything that can carry information from a source to a destination. The transmission media that are used to convey information can be classified as guided or unguided. Guided media provide a physical path along which the signals are propagated; these include twisted pair, coaxial cable, and optical fiber. Unguided media employ an antenna for transmitting through air, vacuum, or water.

Guided Transmission media

Twisted Pair Cable

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The purpose of twisting the wire is to eliminate electrical interference from other wires and outside sources such as motors. Twisting the wires cancels any electrical noise from the adjacent pair. The more twists per linear foot, the greater the effect. Compared to other commonly used guided transmission media (coaxial cable, optical fiber), twisted pair is limited in distance, bandwidth, and data rate.

- A straight-through cable has identical ends. A crossover cable has different ends.
- A straight through is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.
- Odd numbered pins are always striped; even numbered pins are always solid colored.

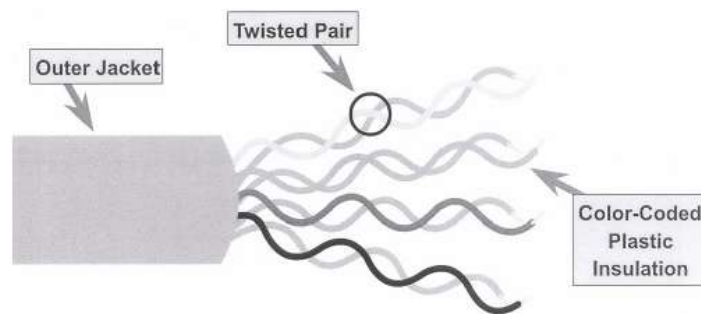


Fig: Twisted pair cable

There are two types of twisted pair cable: STP and UTP

UTP (Unshielded Twisted Pair): It is the most common medium used in telephone network, between house and local exchange (subscriber loop), within a company's buildings to private

branch exchange (PBX) and for local area networks (LAN). Because it lacks shielding UTP is not as good as STP in blocking noise and interference. The categories of UTP into 7 classes are:

- **Category 1:** Used for telephone communications. It is not suitable for transmitting data.
- **Category 2:** Capable of transmitting data at speeds up to 4 megabits per second (Mbps).
- **Category 3:** Used in 10BASE-T networks. It can transmit data at speeds up to 10 Mbps.
- **Category 4:** Used in Token Ring networks. It can transmit data at speeds up to 16 Mbps.
- **Category 5:** a tighter twist, same number of wires, just less crosstalk and higher speeds (100 Mbps)
- **Category 6 (250 MHz):** 4 pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cable is currently the fastest standard for UTP.
- **Category 7 (600 MHz)** is upcoming.

STP (Shielded Twisted Pair): It is covered with a foil shield to reduce cross talk and interference. It provides better performance but more expensive and difficult to work than UTP. STP can handle high-speed transmission and used in token ring network.

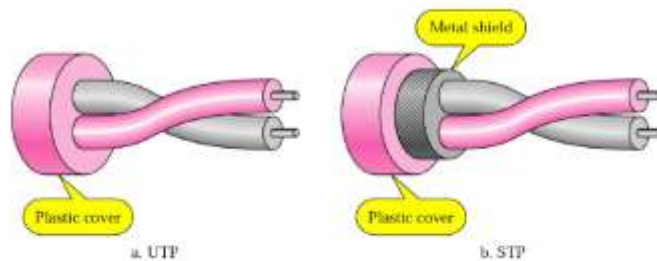


Figure: UTP and STP

Advantages

- Protect against cross talk & interference
- Easy to add computers to network
- Well understood technology
- Less expensive

Disadvantages

- Susceptibility to noise
- Least secure
- Distance limitations
- Requires more expensive hubs

Coaxial Cable

Coaxial cable, like twisted pair, consists of two conductors, but is constructed differently to permit it to operate over a wider range of frequencies. It consists of a hollow outer cylindrical conductor that surrounds a single inner wire conductor (Figure). The inner conductor is held in place by either regularly spaced insulating rings or a solid dielectric material. The outer conductor is covered with a jacket or shield. A single coaxial cable has a diameter of from 1 to 2.5 cm. Coaxial cable can be used over longer distances and support more stations on a shared line than twisted pair.

Applications

- Television distribution
- Long-distance telephone transmission
- Short-run computer system links
- Local area networks

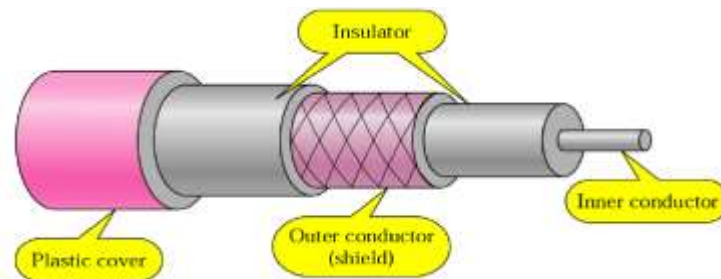


Figure: Coaxial cable

Advantages

- Transmits up to 10Mbps over 500m
- Easy to install
- Low maintenance
- Good resistance to noise over long distances

Disadvantages

- Inflexible
- Low security
- Limited distance

Optical Fiber

An optical fiber cable has a cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket (Figure). The **core** is the innermost section and consists of one or more very thin strands, or fibers, made of glass or plastic. Its own cladding, a glass or plastic coating that has optical properties different from those of the core surrounds each fiber. The interface between the core and cladding acts as a reflector to confine light that would otherwise escape the core. The outermost layer, surrounding one or a bundle of cladded fibers, is the **jacket**. The jacket is composed of plastic and other material layered to protect against moisture, abrasion, crushing, and other environmental dangers.

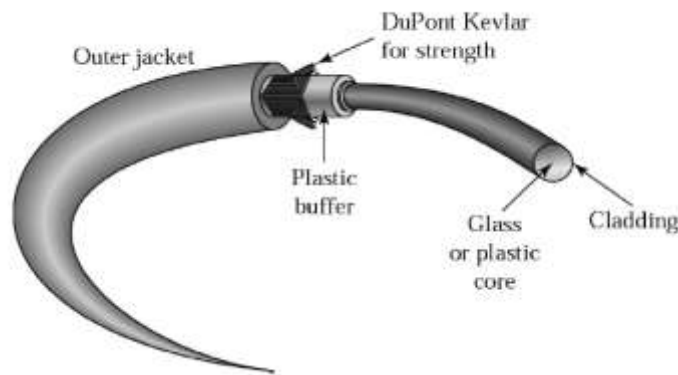


Figure: Optical Fiber

We must have a light source in order to send the data. It sends a ray of light for each 1 bit, and no light for a 0 bit. We must have a detector to detect the light signal. The detector emits an electric pulse for each light ray it detects. The slowest part of the system is the conversion that happens at either end.



Figure: Transmission

Light propagation modes

Step-index multimode: It's refraction index is constant for the fibre core, distance to core's centre does not matter that implies different path lengths for light rays, making reception difficult. It present a thicker core (hundreds of μm) so cheaper fiber.

Graded-index multimode: It's refraction index decreases from the core centre to edges that offer a better focusing of the rays, so a lower attenuation and easier reception.

Single mode (mono-mode): It has direct path for light ray, no loss, no attenuation, but more expensive

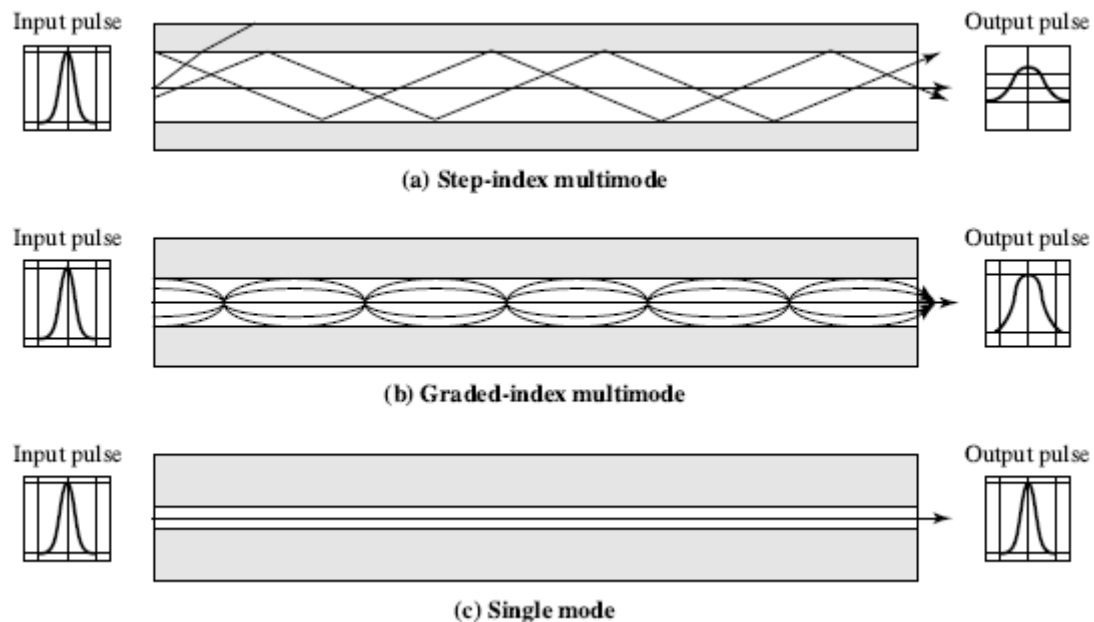


Figure: Optical fiber transmission mode

Advantages

- High data rate and wide bandwidth
- Low attenuation (data loss)
- Longer distance –up to 5 km with Multimode fiber or over 25 km with Single Mode fiber
- Small cable diameter fits anywhere
- No sparks if cut and no shock hazard
- Secure communications
- Longer life expectancy than copper or coaxial cable
- Cabling of the future

Disadvantages

- Expensive
- Difficult to install
- Require two cables to transmit & receive data
- Require special connections

Unguided Transmission Media

Bluetooth

- Developed by SIG (Special Interest Group)
- The IEEE 802.15 Standard defines Bluetooth.
- It defines Wireless PAN operable in an area of room or a hall.
- Used Technology Called FHSS (Frequency Hopping Spread Spectrum)
- When two Bluetooth devices notice each other they create a network called a Piconet

Bluetooth Architecture

- Piconet
- Scatternet

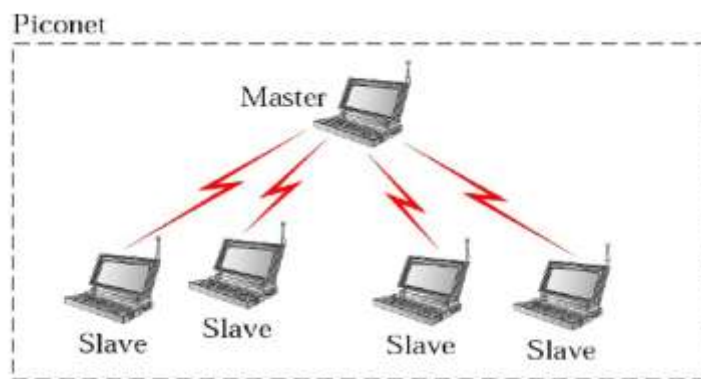


Figure: Piconet

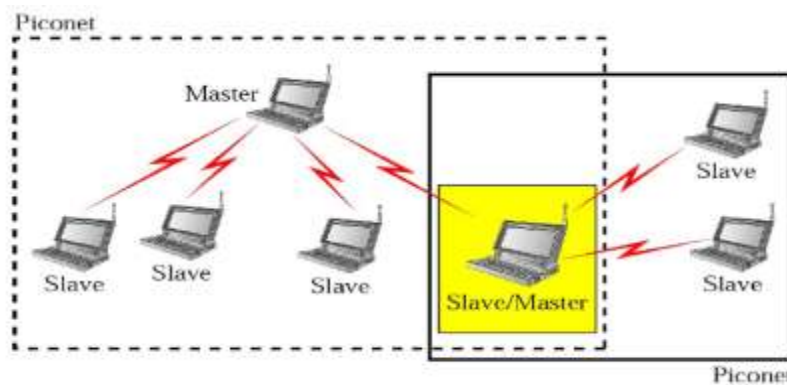


Figure: Scatternet

Radio wave

Radio waves are a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared light.

The principal difference between broadcast radio and microwave is that the former is omnidirectional and the latter is directional. Thus broadcast radio does not require dish-shaped antennas, and the antennas need not be rigidly mounted to a precise alignment.

Applications

- TV & radio broadcasting
- Cordless phones

Infrared

Infrared communications is achieved using transmitters/receivers (transceivers) that modulate non-coherent infrared light. Transceivers must be within the line of sight of each other either directly or via reflection from a light-colored surface such as the ceiling of a room. One important difference between infrared and microwave transmission is that the former does not penetrate walls. Thus the security and interference problems encountered in microwave systems are not present. Furthermore, there is no frequency allocation issue with infrared, because no licensing is required. Unguided infrared waves are widely used for short-range communication. The remote controls used for televisions, VCRs, and stereos all use infrared communication. They are relatively directional, cheap, and easy to build. They have a major drawback that they do not pass through solid objects.

Microwave

Microwave links are widely used to provide communication links when it is impractical or too expensive to install physical transmission media. Two properties of microwave transmission restrict its use. First, microwave travels in straight path and will not follow earth's curvature. Second atmospheric condition and solid objects interfere with microwave. For example, they cannot travel through buildings.

Applications

- Long-distance telephone communication
- Mobile phones
- Television broadcast

Satellite Communication

Satellite transmission is a microwave transmission in which one of the stations is the satellite orbiting the earth. A microwave beam is transmitted to the satellite from the ground. The two stations can use a satellite as a relay station for their communication. Receiver and transmitter in satellite is known as transponder. One Earth Station sends a transmission to the satellite. This is called a Uplink. The satellite Transponder converts the signal and sends it down to the second earth station. This is called a Downlink.

The advantages of satellite communication over terrestrial communication are:

- The coverage area of a satellite greatly exceeds that of a terrestrial system.
- Transmission cost of a satellite is independent of the distance from the center of the coverage area.
- Satellite-to-Satellite communication is very precise.
- Higher Bandwidths are available for use.

The disadvantages of satellite communication are:

- Launching satellites into orbit is costly.
- Satellite bandwidth is gradually being used up.
- There is a larger propagation delay in satellite communication than in terrestrial communication.

Wireless Propagation

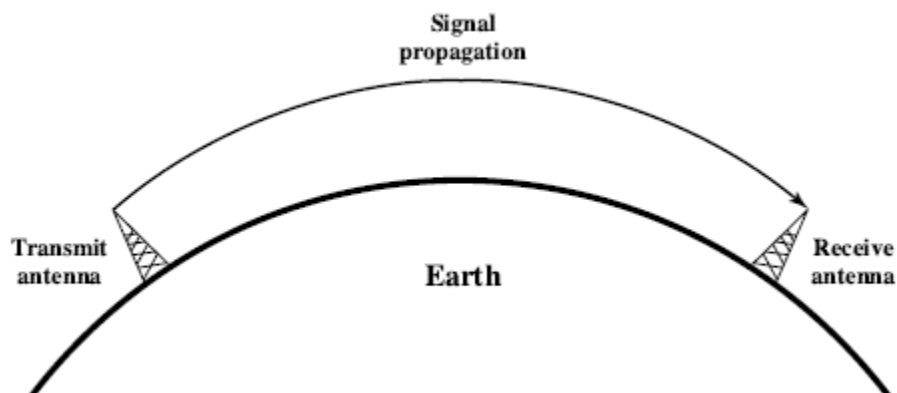


Figure: Ground wave propagation

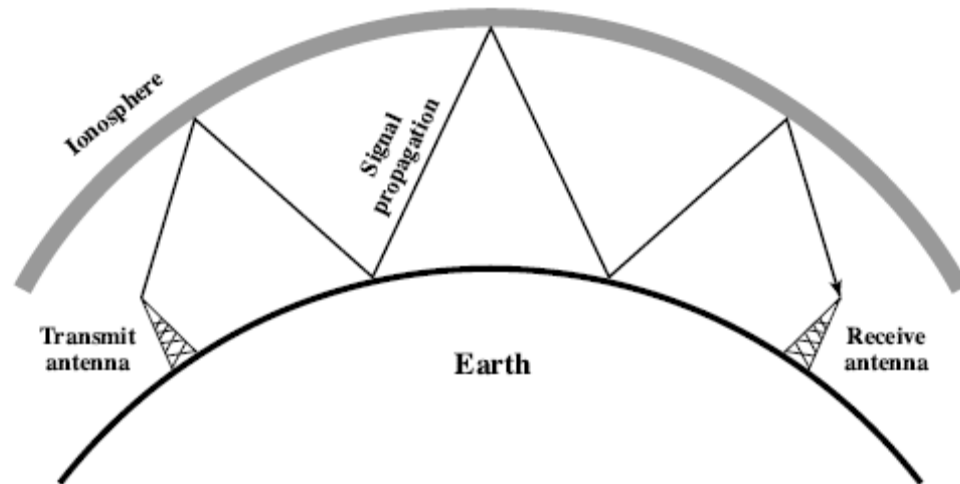


Figure: Sky wave propagation

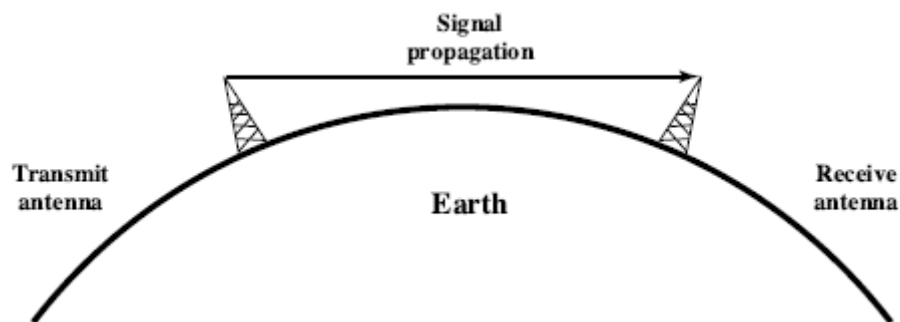


Figure: Line of Sight Propagation

Switching

Every time in computer network you access the internet or another computer network outside your immediate location, your messages are sent through a maze of transmission media and connection devices. The mechanism for moving information between different computer network and network segment is called switching in computer network.

There are three different types of switching:

- Message switching
- Circuit switching
- Packet switching

Message switching

It does not need physical path to set up between the sender and receiver. The whole message (or block of data) is sent to the switching office. Once it has been received, it is inspected for errors and is then sent to the next switching office. This method is not used anymore.

Circuit switching

Conceptually, when you or your computer places a telephone call, the switching equipment within the telephone system seeks out a physical path all the way from your telephone to the receiver's telephone. This technique is called **circuit switching**. This used to be done by a person at a switchboard. Now it is done automatically. Setting up the circuit can still take time, depending on how far the call is going and how many switches it passes through.

An important property of circuit switching is the need to set up an end-to-end path *before* any data can be sent. The elapsed time between the end of dialing and the start of ringing can easily be 10 sec, more on long-distance or international calls. During this time interval, the telephone system is hunting for a path, as shown in Fig. 2.16(a). Note that before data transmission can even begin, the call request signal must propagate all the way to the destination and be acknowledged.

Packet switching

With this technology, packets are sent as soon as they are available. There is no need to set up a dedicated path in advance. It is up to routers to use store-and-forward transmission to send each packet on its way to the destination on its own. This procedure is unlike circuit switching, in which the result of the connection setup is the reservation of bandwidth all the way from the sender to the receiver. All data on the circuit follows this path. Among other properties, having all the data follow the same path means that it cannot arrive out of order. With packet switching there is no fixed path, so different packets can follow different paths, depending on network conditions at the time they are sent, and they may arrive out of order.

Two Types of Packet Switching

- Datagram Packet Switching
- Virtual Circuit Packet Switching

Packet Switching: Datagram Packet Switching

- No need to establish the connection between the source and destination
- Route chosen on packet by packet basis.
- Packets may be stored until delivered => (Store and Forward)
- Different packets may follow different routes.
- Packets may arrive out of order at the destination.

Packet Switching: Virtual Circuit Switching

- Route is chosen at the start of session and it is only a logical connection.
- All Packets associated with a session follow the same path.
- Packets are labeled with a virtual circuit identifier designated the route.
- The VC number must be unique on a given link.
- Packets are forwarded more quickly. (No Routing Decisions)
- Example : Asynchronous Transfer Mode

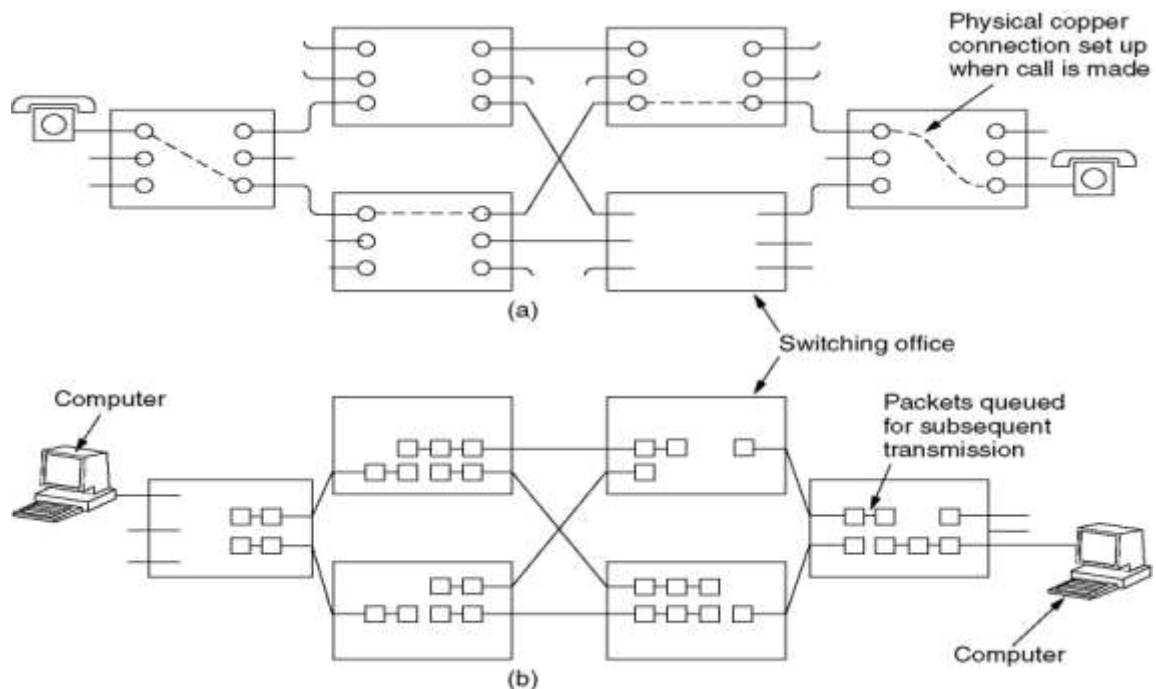


Figure: a) circuit switching b) packet switching

Comparison of Circuit and Packet switching

Item	Circuit-switched	Packet-switched
Call setup	Required	Not needed
Dedicated physical path	Yes	No
Each packet follows the same route	Yes	No
Packets arrive in order	Yes	No
Is a switch crash fatal	Yes	No
Bandwidth available	Fixed	Dynamic
When can congestion occur	At setup time	On every packet
Potentially wasted bandwidth	Yes	No
Store-and-forward transmission	No	Yes
Transparency	Yes	No
Charging	Per minute	Per packet

ISDN

The evolution to the existing telecommunications networks and specialized carrier facilities to integrated digital networks is based on two technological developments:

- Digital switching
- Digital transmission

Both technologies are well established. But IDN provided a revolutionary idea of integrating the functions of these two. As the use of distributed processing and data communications has grown, the evolution of an all-digital network has been pulled by the need to provide a framework for ISDN (Integrated Service Digital Network). It is ITU Standard For global Digital Communication. It allows the complete integration of both Voice, Video and Data within a single system.

Principles of ISDN

- Support of voice and non-voice applications using a limited set of standardized facilities
- Support for switched and non-switched applications
 - both circuit-switched and packet-switched connections
 - also supports non-switched services in the form of dedicated lines

- Reliance on 64-kbps connections
 - fundamental block of ISDN
 - chosen because it was the standard rate for digitized voice
- Intelligence in the network
 - sophisticated network management and maintenance capabilities
- Layered protocol architecture
 - Already developed standards for OSI may be used for ISDN (e.g. X.25)
 - New ISDN standard can be based on existing ones (LAPD based on LAPB)
- Variety of configurations
 - More than one physical configuration is possible for implementing ISDN

ISDN Channels

B-channel

- 64 kbps
- basic user channel
- can carry digital data, PCM-encoded digital voice, or a mixture of lower-rate traffic
- supports circuit-switched and packet-switched

D-channel

- 16 or 64 kbps
- carries signaling information to control circuit switched calls on B-channel such as who is calling, type of call and calling what number

H-channel

- 384 (H0), 1536 (H11), 1920 (H12) kbps
- is a high-speed channel
- can be used as a single trunk or subdivided by the user fast fax, video, high-speed data, high-quality audio and multiplexed information streams at lower data rates

ISDN Services Types

Also called ISDN Interface

- Basic Rate Interface(BRI)
 - Connection from ISDN office to the user location provides for access to 3 channels.
 - 2B channels + 1 D channel
 - $2 \times 64 + 16 = 144$ kbps (192 kbps total)



- Primary Rate Interface(PRI)
 - Especially for LAN
 - T1 connection: 23B+D
 - American Standards
 - Data rate $23 \times 64\text{Kbps} + 64\text{Kbs} + 8\text{bits header}$
 - Information = $1544\text{kbs} = 1.544\text{Mbps}$
 - E1 Connection: 30B+D
 - European Standards
 - $30 \times 64\text{Kbps} + 64\text{Kbps} + 64\text{Kbps}$
 - $2048\text{Kbps} = 2.048\text{Mbps}$
 - Last D channel for Framing and Synchronization in E1 Connections

ISDN Architecture

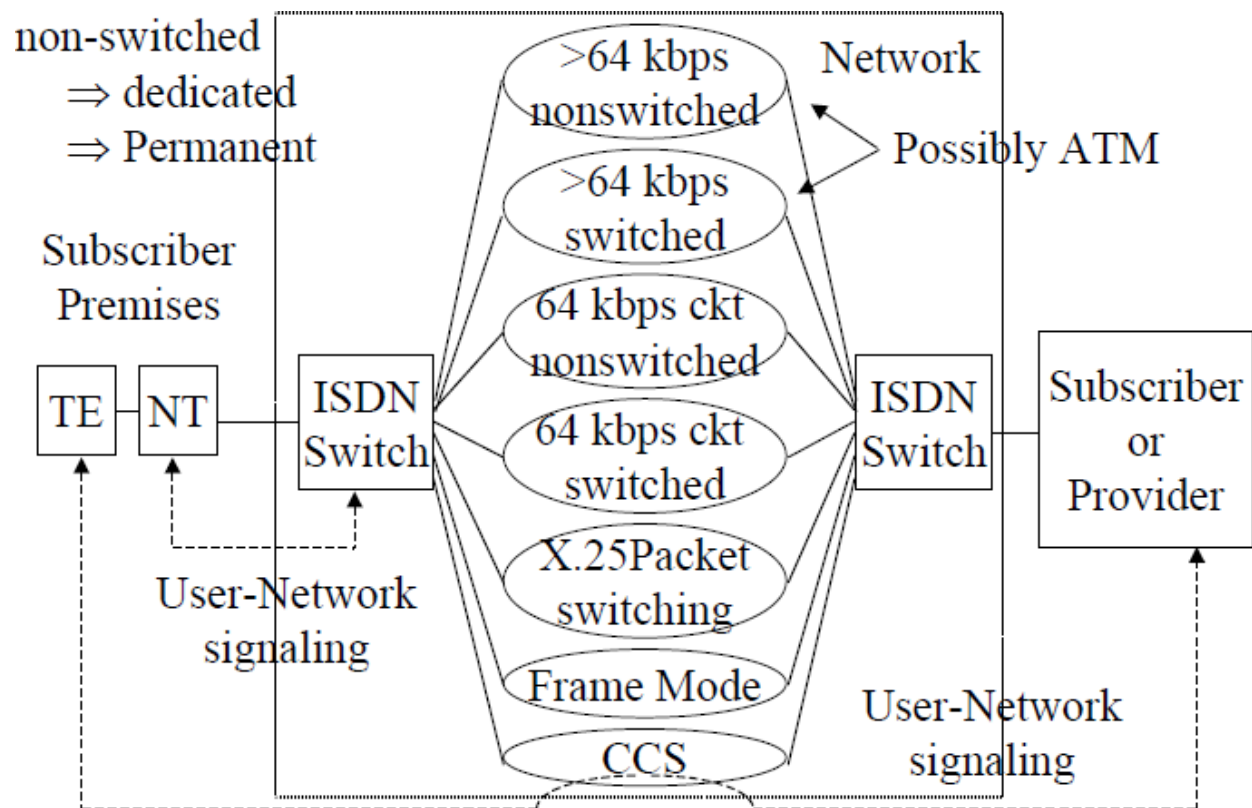


Figure: ISDN Architecture

ISDN supports a new physical connector for users, a digital subscriber line, and a variety of transmission services. Physical interface provides a standardized means of attaching to the

network. The interface supports a *basic* service consisting of three times multiplexed channels, two at 64 kbps and one at 16 kbps. In addition, there is a *primary* service that provides multiple 64- kbps channels. For both basic and primary service, an interface is defined between the customer's equipment (TE) and a device on the customer's premises, known as a network termination (NT). The subscriber line is the physical path from the subscriber's NT to the ISDN central office. ISDN central office connects subscriber lines to the digital network, providing access to lower-layer transmission facilities.

- Circuit-switched capabilities
 - Same facility provided by other digital-switched telecom. net's (64 kbps)
- Non-switched capabilities
 - 64 kbps dedicated link, higher rates in B-ISDN using PVC in ATM tx
- Switched capabilities
 - high speed (>64 kbps) switched connections using ATM in B-ISDN
- Packet-switched capabilities
 - resembles packet-switched service provided by other data networks
- Frame-mode capabilities
 - a service that supports frame relay
- Common-channel signaling capabilities
 - used to control the network and provide call management

ISDN Signaling

The signaling method will be Common Channel Signaling (CCS).

- The signaling information relating to a multiplicity of channels or functions or for network management is conveyed over a single channel by addressed messages.
- CCS will be able to operate in two modes:
 - **associated mode** (i.e. signaling points, that are the origin and destination points of the messages are directly interconnected by a link)
 - **quasi-associated mode** (i.e. messages pass through one or more signaling points other than those which are the origin or destination of the messages. The path is pre-determined).

Bandwidth

Bandwidth is the maximum amount of data that can be carried from one point to another in a given time period (usually in second). For Digital Devices, it refers to channel capacity. Bandwidth is expressed in bits per second (bps).

For Analog Devices, it refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass. Bandwidth is expressed in cycle per sec OR Hz.

Throughput

Throughput is the rate of successful message delivery over a communication channel. It is usually measured in bits per second.

Example:

A network with bandwidth of 10 Mbps can pass only an average of 12,000 frames per minute with each frame carrying an average of 10,000 bits. What is the throughput of this network?

Solution,

We can calculate the throughput as

$$\text{Throughput} = \frac{12,000 \times 10,000}{60} = 2 \text{ Mbps}$$

The throughput is almost one-fifth of the bandwidth in this case.

Bandwidth versus throughput

Bandwidth is the theoretical capability of the connection; the throughput is the actual data rate of a specific application.

Delay

Delay is the time required for a signal to traverse the network.

Propagation Delay

Propagation speed: speed at which a bit travels through the medium from source to destination

Propagation delay: Time taken for the first bit to travel from the sender to the receiver

$$\text{Propagation delay} = \text{Distance (Link Length)} / \text{Propagation speed}$$

Transmission Delay

Transmission speed: The amount of time from the beginning until the end of a message transmission

Transmission delay: Amount of time required to push all of the packet's bits into the wire

$$\text{Transmission Delay} = \text{Message size} / \text{bandwidth}$$

It is also called Store and Forward Delay. It is function of Packet Length, nothing to do with distance between the nodes.

Example

What are the propagation time and the transmission time for a 2.5-kbyte message (an e-mail) if the bandwidth of the network is 1 Gbps? Assume that the distance between the sender and the receiver is 12,000 km and that light travels at 2.4×10^8 m/s.

Solution

We can calculate the propagation and transmission time as

$$\text{Propagation time} = \text{Distance} / \text{Speed}$$

$$\text{Transmission time} = \text{Packet Size} / \text{bandwidth of link}$$

$$\begin{aligned}\text{Propagation time} &= \frac{12,000 \times 1000}{2.4 \times 10^8} = 50 \text{ ms} \\ \text{Transmission time} &= \frac{2500 \times 8}{10^9} = 0.020 \text{ ms}\end{aligned}$$

Latency

Network latency is the delay that is introduced by the network

$$\text{Latency} = \text{Propagation delay} + \text{Transmission delay} + \text{Queuing time} + \text{Processing time}$$

Low Latency: Network that experiences Low Delay

High Latency: Network that experience High Delay

Jitter

Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift, or route changes. The causes of jitter are electromagnetic interference (EMI) and crosstalk with other signals.

Bandwidth Delay Product

Product of a data link's capacity (in bits per second) and its round-trip delay time (in seconds).

A network with a large bandwidth-delay product $> 10^5$ bits is commonly known as a long fat network.

Baseband and Broadband

Baseband: digital signals sent through direct current (DC) pulses applied to a wire. It requires exclusive use of wire's capacity. Baseband systems can transmit one signal at a time.

Broadband: signals modulated as radiofrequency (RF) analog waves that use different frequency ranges. It does not encode information as digital pulses.

Chapter 4: Data Link Layer

The data link layer has a number of specific functions it can carry out. These functions include

- Provide a well-defined service interface to the network layer.
- Deal with transmission errors.
- Regulate the flow of data so that fast senders do not swamp slow receivers.

Services Provided to the Network Layer

The function of the data link layer is to provide services to the network layer.

The actual services offered can vary from system to system. Three reasonable possibilities that are we will consider in turn are:

- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection-oriented service

Data Link layer is divided into two sub layers:

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

Logical Link Control (LLC)

LCC is responsible for error control & flow control. It is defined by IEEE 802.2 Standard. The LLC sub-layer acts as an interface between the media access control (MAC) sub-layer and the network layer

Medium Access Control (MAC)

MAC is responsible for multiple access resolutions. It provides addressing and channel access control mechanisms. It also provides End Devices Addressing Mechanism using physical address

Physical (MAC) addressing Overview

It is also called Physical Address OR Hardware Address. It is 48-bit address represented in Hexadecimal number. Example:

01:23:45:67:89:ab

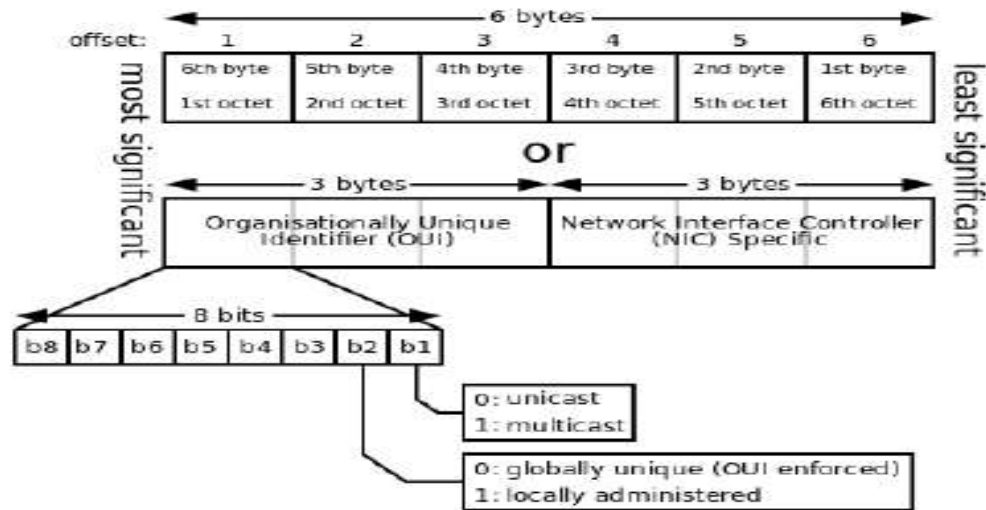


Figure: MAC Address

Upper 3 bytes represents the OUI (Organization Unique Identifier) also called Manufacturer ID and lower 3 bytes represent the Device ID

Framing

Data link layer translates the physical layer's raw bit stream into discrete units called *frames* and encapsulates a network layer datagram into frame. The Process of creating Frames by the Data Link Layer is known as Framing.

One of the method of framing is fixed size Framing that have Fixed Length and no need to define boundaries for Frames. Example, ATM Frames (54 byte cells)

Other method of framing is variable size framing. Its types are:

- Character count
- Flag bytes with byte stuffing
- Starting and ending flags, with bit stuffing.
- Physical layer coding violations

Character Count

The first framing method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is. This technique is shown in figure for four small example frames of sizes 5, 5, 8, and 8 bytes, respectively.

The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the byte count of 5 in the second frame of figure becomes a 7 due to a single bit flip,

the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.

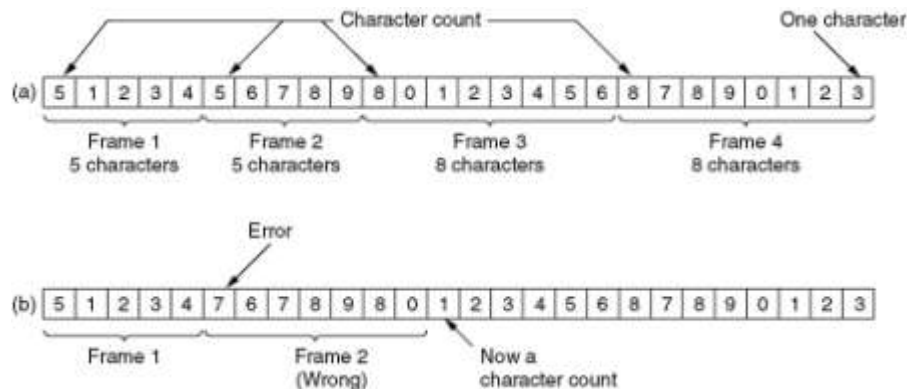


Figure: A byte stream a) Without errors b) With one error

Flag bytes with byte stuffing

Often the same byte, called a **flag byte**, is used as both the starting and ending delimiter. This byte is shown in Figure as FLAG. Two consecutive flag bytes indicate the end of one frame and the start of the next. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.

However, there is still a problem we have to solve. It may happen that the flag byte occurs in the data. One way to solve this problem is to have the sender's data link layer insert a special escape byte (ESC) just before each "accidental" flag byte in the data. The data link layer on the receiving end removes the escape bytes before giving the data to the network layer. This technique is called **byte stuffing**.

Of course, the next question is: what happens if an escape byte occurs in the middle of the data? The answer is that it, too, is stuffed with an escape byte. At the receiver, the first escape byte is removed, leaving the data byte that follows it. Some examples are shown in Figure.

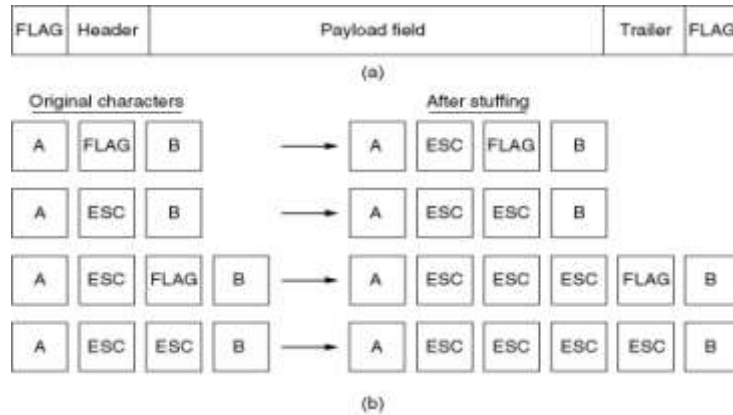


Figure : a) A frame delimited by flag bytes. b) Four examples of byte sequences before and after byte stuffing

Starting and ending flags, with bit stuffing

The new technique allows data frames to contain an arbitrary number of bits and allows character codes with an arbitrary number of bits per character. It works like this. Each frame begins and ends with a special bit pattern, 01111110 (in fact, a flag byte). Whenever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream. This bit stuffing is analogous to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110, this flag is transmitted as 0111111010 but stored in the receiver's memory as 01111110. Figure gives an example of bit stuffing.

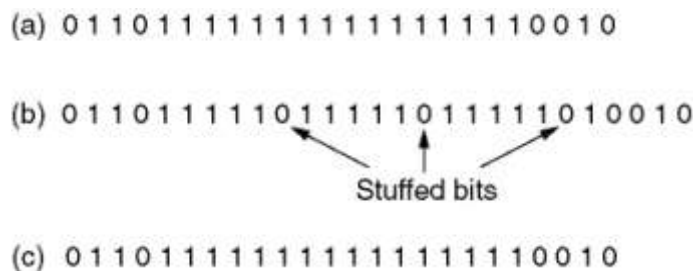


Figure: Bit stuffing. a) The original data b) The data as they appear on the line. c) The data as they are stored in the receiver's memory after de-stuffing.

Physical layer coding violations

The last method of framing is only applicable to networks in which the encoding on the physical medium contains some redundancy. For example, some LANs encode 1 bit of data by using 2 physical bits. Normally, a 1 bit is a high-low pair and a 0 bit is a low-high pair. The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.

Flow Control

Another important design issue that occurs in the data link layer (and higher layers as well) is what to do with a sender that systematically wants to transmit frames faster than the receiver can accept them. This situation can easily occur when the sender is running on a fast (or lightly loaded) computer and the receiver is running on a slow (or heavily loaded) machine. The sender keeps pumping the frames out at a high rate until the receiver is completely swamped.

Two approaches are commonly used. In the first one, feedback-based flow control, the receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing. In the second one, rate-based flow control, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver. Here, we will study feedback-based flow control schemes because rate-based schemes are never used in the data link layer.

Stop and Wait protocol

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent this, we somehow need to tell the sender to slow down i.e., stop to transmit and wait for receiver acknowledgement signals

Stop and Wait: Normal Operation

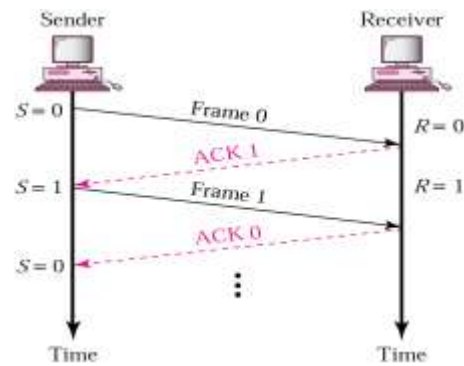


Figure (a): Stop and Wait: Normal Operation

Sender keeps a copy of the last frame until it receives an acknowledgement. For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1. Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1). Receiver has a control variable (R) that holds the number of the next frame expected (0 or 1). Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it. Receiver send only positive ACK if the frame is intact. ACK number always defines the number of the next expected frame.

Stop-and-Wait, lost frame

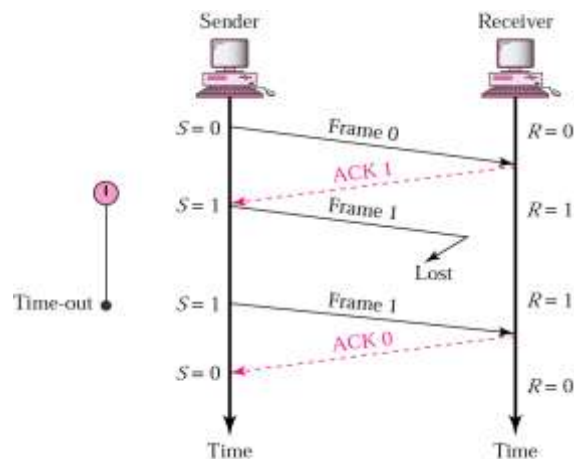


Figure (b): Stop-and-Wait ARQ, lost frame

When a receiver receives a damaged frame, it discards it and keeps its value of R. After the timer at the sender expires, another copy of frame 1 is sent.

Stop and wait ,Lost ACK

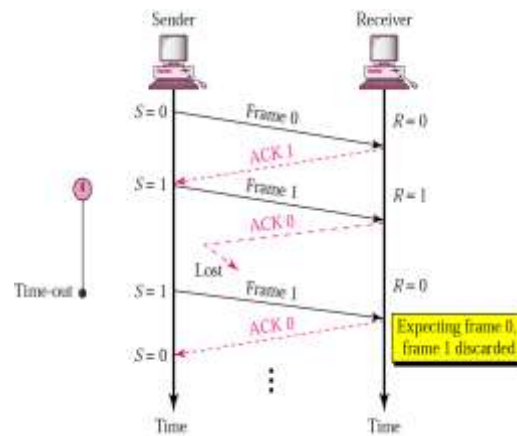


Figure (c): Stop and wait ,Lost ACK

If the sender receives a damaged ACK, it discards it. When the timer of the sender expires, the sender retransmits frame 1. Receiver has already received frame 1 and expecting to receive frame 0 ($R=0$). Therefore it discards the second copy of frame 1.

Stop-and-Wait, delayed ACK

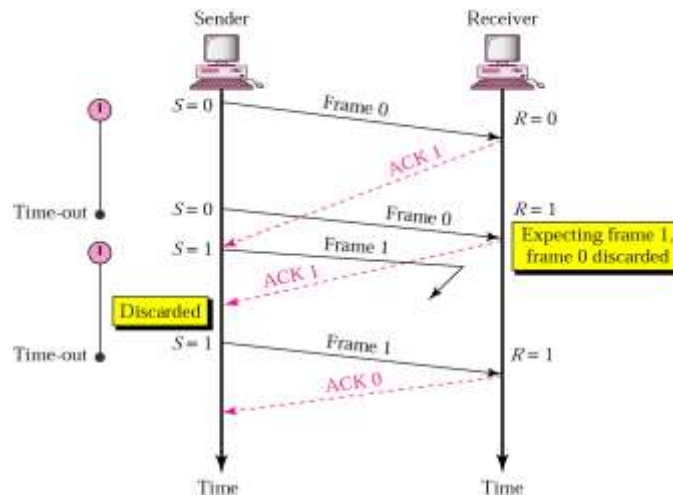


Figure (d): Stop-and-Wait ARQ, delayed ACK

The ACK can be delayed at the receiver or due to some problem. It is received after the timer for frame 0 has expired. Sender retransmitted a copy of frame 0. However, $R = 1$ means receiver expects to see frame 1. Receiver discards the duplicate frame 0. Sender receives 2 ACKs, it discards the second ACK.

Disadvantage of Stop-and-Wait

In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged. This is not a good use of transmission medium. To improve efficiency, multiple frames should be in transition while waiting for ACK.

A Protocol Using Go-Back-N

Allowing the sender to transmit up to w frames before blocking, instead of just 1. With a large enough choice of w the sender will be able to continuously transmit frames since the acknowledgements will arrive for previous frames before the window becomes full, preventing the sender from blocking.

To find an appropriate value for w we need to know how many frames can fit inside the channel as they propagate from sender to receiver. This procedure requires additional features to be added to Stop-and-Wait ARQ. It uses Sequence Numbering Techniques to track the Frames. It can send one cumulative acknowledgment for several frames.

Sequence Number

- Frames from a sender are numbered sequentially
- We need to set a limit since we need to include the sequence number of each frame in the header
- If the header of the frame allows m bits for sequence number, the sequence numbers range from 0 to $2^m - 1$.
- for $m = 3$, sequence numbers are: 0, 1, 2, 3, 4, 5, 6, 7.
- We can repeat the sequence number.
- Sequence numbers are:
 - 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, 2, 3, 4, 5, 6, 7, 0, 1, ...
- Sliding window define the range of Sequences Number
- Here Sender Sliding window define the window size=7
- Total Number of Frames that can be sent without receiving ACKs is 7

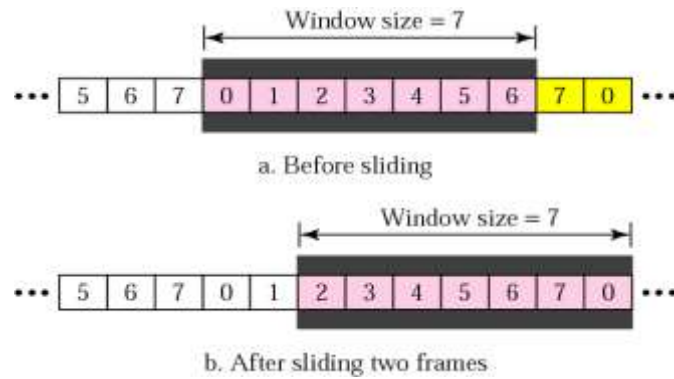


Figure: Go-Back-N ARQ: Sender sliding window

Control Variables

- Sender has 3 variables: S, SF, and SL
- S holds the sequence number of recently sent frame
- SF holds the sequence number of the first frame
- SL holds the sequence number of the last frame
- Receiver only has the one variable, R, that holds the sequence number of the frame it expects to receive. If the seq. no. is the same as the value of R, the frame is accepted, otherwise rejected.

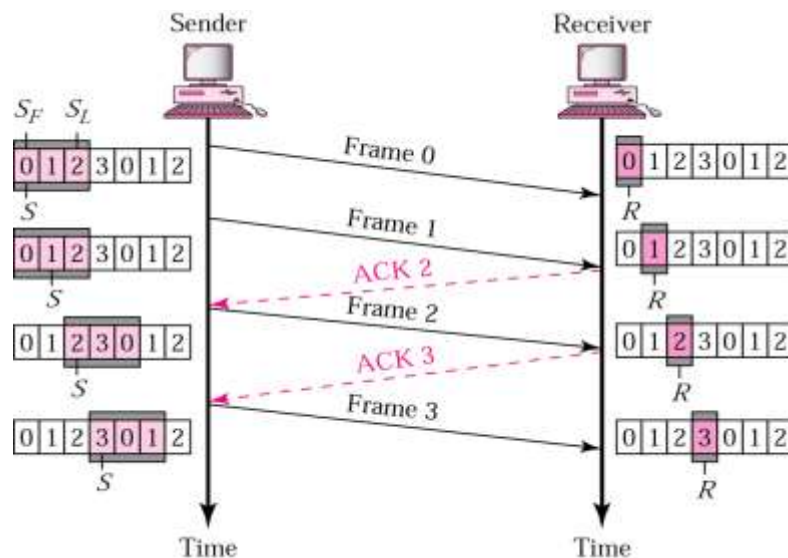


Figure: Go-Back-N ARQ : Normal Operation

Selective Repeat

The other general strategy for handling errors when frames are pipelined is called **selective repeat**. When it is used, a bad frame that is received is discarded, but any good frames received after it are accepted and buffered. When the sender times out, only the oldest unacknowledged frame is retransmitted. If that frame arrives correctly, the receiver can deliver to the network layer, in sequence, all the frames it has buffered. Selective repeat corresponds to a receiver window larger than 1. This approach can require large amounts of data link layer memory if the window is large.

Selective repeat is often combined with having the receiver send a negative acknowledgement (NAK) when it detects an error, for example, when it receives a checksum error or a frame out of sequence. NAKs stimulate retransmission before the corresponding timer expires and thus improve performance.

It is more efficient for noisy links. The Selective Repeat Protocol also uses two windows: a send window and a receive window. Size of the Send window and Receive window are same.

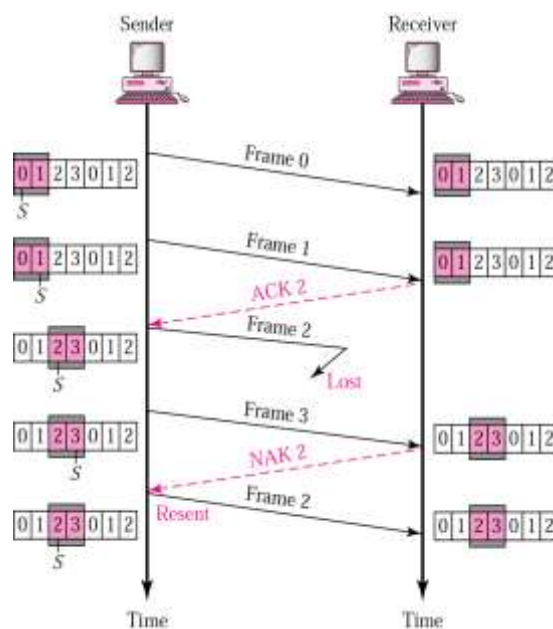


Figure: *Selective Repeat Request, lost frame*

What happens when we get a bad frame?

- **Go back N** – Ask the sender to go back and start retransmitting from the lost frame.
- **Selective repeat** – Ask the sender to repeat the particular frames that were lost.

Error Control

Suppose that the sender just kept outputting frames without regard to whether they were arriving properly. This might be fine for unacknowledged connectionless service, but would most certainly not be fine for reliable, connection-oriented service.

Typically, the protocol calls for the receiver to send back special control frames bearing positive or negative acknowledgements about the incoming frames. If the sender receives a positive acknowledgement, it knows the frame has arrived safely and, a negative acknowledgement means that something has gone wrong, and the frame must be transmitted again.

An additional complication comes from the possibility that hardware troubles may cause a frame to vanish completely (e.g., in a noise burst). This possibility is dealt with by introducing timers into the data link layer. The timer is set to expire after an interval long enough for the frame to reach the destination, be processed there, and have the acknowledgement propagate back to the sender.

However, if either the frame or the acknowledgement is lost, the timer will go off, alerting the sender to a potential problem. The obvious solution is to just transmit the frame again. However, when frames may be transmitted multiple times there is a danger that the receiver will accept the same frame two or more times and pass it to the network layer more than once. To prevent this from happening, it is generally necessary to assign sequence numbers to outgoing frames, so that the receiver can distinguish retransmissions from originals.

Error control includes both error detection and error correction.

Error Detection

- CRC (Cyclic Redundancy Check)
- Parity Check
- CheckSum

CRC (Cyclic Redundancy Check)

Given a k -bit frame or message, the transmitter generates an n -bit sequence, known as a frame check sequence (FCS), so that the resulting frame, consisting of $(k+n)$ bits, is exactly divisible by some predetermined number. The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

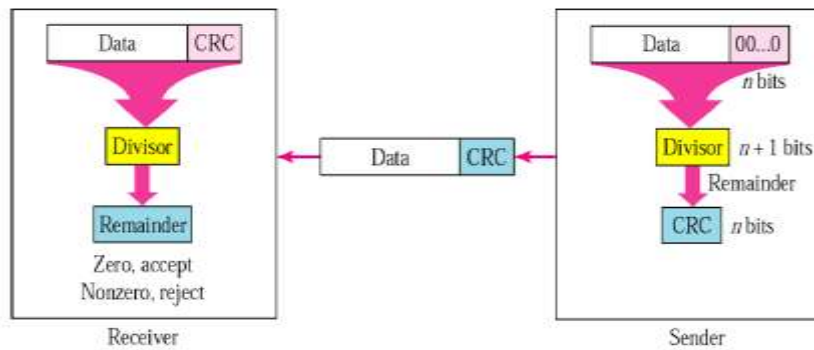


Figure (a): CRC

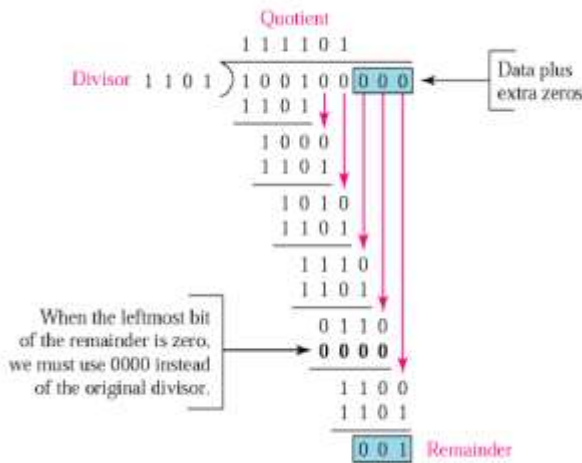


Figure (b): CRC Encoding

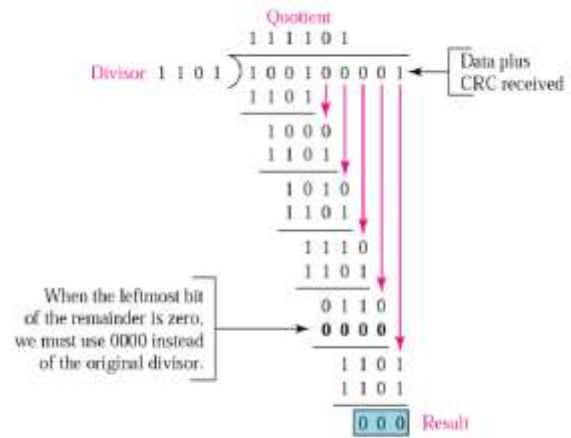


Figure (c): CRC Decoding

Parity Check

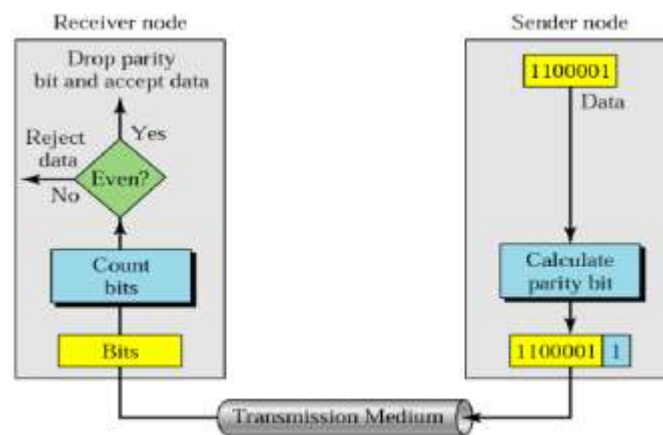


Figure (a): Parity Check (Even Parity)

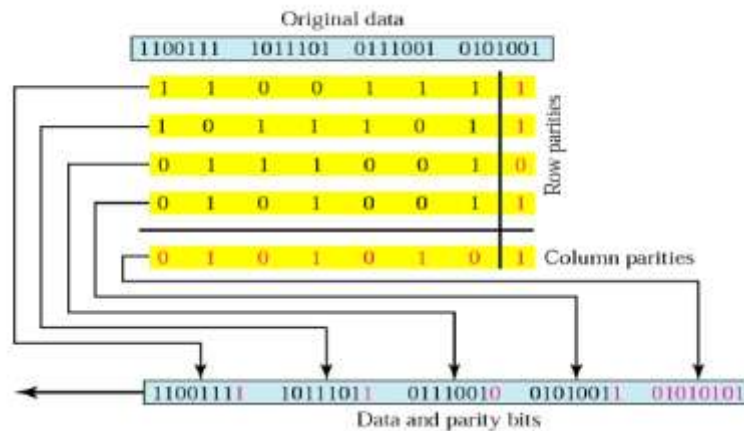


Figure (b): Two dimensional Parity check

Error Correction

Forward Error Control (FEC)

Each block transmitted contains extra information which can be used to detect the presence of errors and determine the position in the bit stream of the errors.

Backward (Feedback) Error Control (BEC)

Extra information is sufficient to only detect the presence of errors. If necessary, a retransmission control scheme is used to request that another copy of the erroneous information be sent.

Hamming codes

Given any two code words that may be transmitted or received—say, 10001001 and 10110001. It is possible to determine how many corresponding bits differ. In this case, 3 bits differ.

For example: 10001001 and 10110001 differs in third, fourth and fifth bit position.

The number of bit positions in which two code words differ is called the **Hamming Distance (d)**

Example:

$W1=10001001$, $W2=10110001$, then $d(W1, W2) = 3$

The minimum Hamming distance (or “minimum distance”) of the scheme is the smallest number of bit errors that changes one valid codeword into another.

This scheme can detect any combination of $\leq D-1$ bit errors and correct any combination of strictly less than $D/2$ bit errors.

Suppose only 4 valid code words are:

00000 00000, 00000 11111, 11111 00000, and 11111 11111

Minimum distance is $D=5$, so any combination of ≤ 4 bit errors can be detected and any combination of ≤ 2 bit errors can be corrected, but 3 bit errors can't be properly corrected.

If 00000 00000 transmitted, $W=00000\ 00011$ received: $d(W, C1)=2$, $d(W, C2)=3$, $d(W, C3)=7$, and $d(W, C4)=8$ receiver takes $C1=00000\ 00000$ as transmitted codeword (errors corrected)

If 00000 00000 transmitted, $X=00000\ 00111$ received: $d(X, C1)=3$, $d(X, C2)=2$, $d(X, C3)=8$, and $d(X, C4)=7$ receiver takes $C2=00000\ 11111$ as transmitted codeword (in this case, error correction fails)

Random Access Protocols

In this method, there is no control station. Any station can send the data. There is no scheduled time for a stations to transmit. They can transmit in random order. The various random access methods are:

- ALOHA
- CSMA (Carrier Sense Multiple Access)
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection)
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

ALOHA

Any terminal is allowed to transmit without considering whether channel is idle or busy. If packet is received correctly, the base station transmits an acknowledgement. If no acknowledgement is received, it assumes the packet to be lost and it retransmits the packet after waiting a *random time*. There are two different versions of ALOHA:

- Pure ALOHA
- Slotted ALOHA

Pure ALOHA

In pure ALOHA, stations transmit frames whenever they have data to send. When two stations transmit simultaneously, there is collision and frames are lost. In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver. If acknowledgement is not received within specified time, the station assumes that the frame has been lost. If the

frame is lost, station waits for a random amount of time and sends it again. This waiting time must be random, otherwise, same frames will collide again and again. Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost. If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.

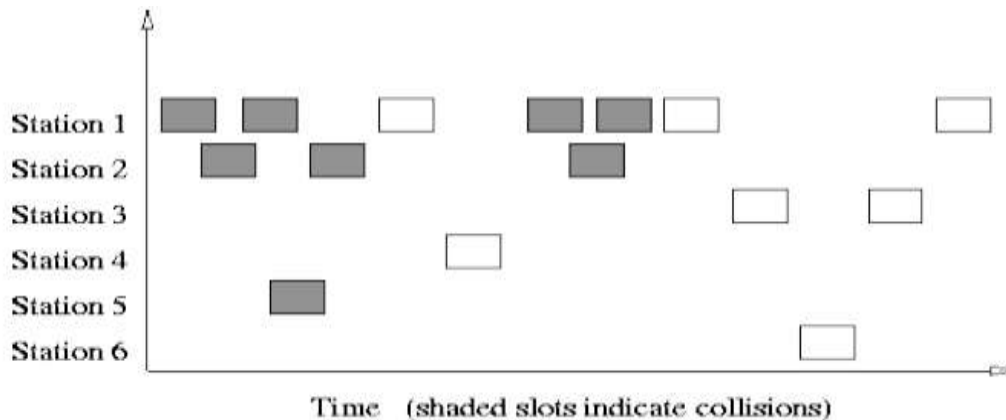


Figure: Pure ALOHA

Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA, time of the channel is divided into intervals called slots. The station can send a frame only at the beginning of the slot and only one frame is sent in each slot. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot. There is still a possibility of collision if two stations try to send at the beginning of the same time slot.

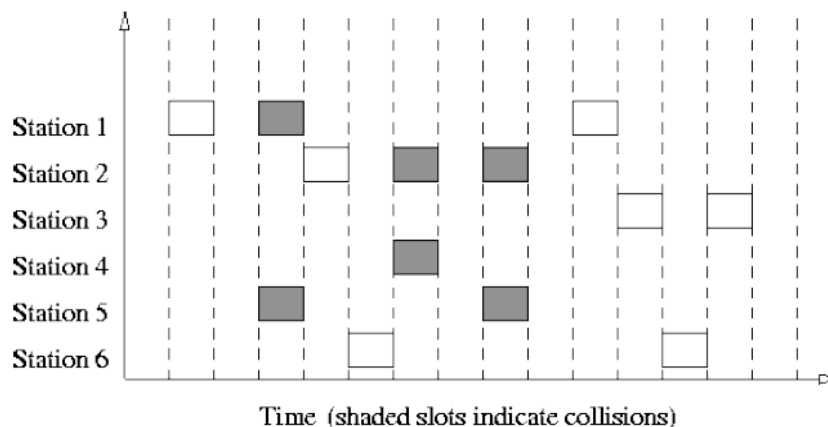


Figure: Slotted ALOHA

CSMA

CSMA was developed to overcome the problems of ALOHA i.e. to minimize the chances of collision. It is based on the principle "sense before transmit" or "listen before talk." In CSMA, node verifies the absence of other traffic before transmitting on a shared transmission medium. Multiple access means that multiple stations send and receive on the medium. Each station first listen to the medium before Sending.

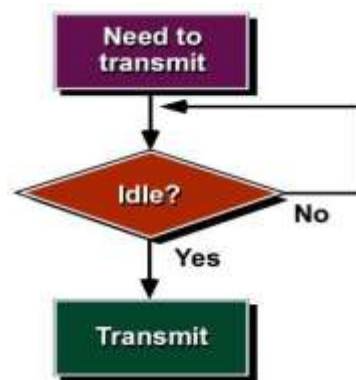


Figure (a): CSMA

The chances of collision still exist because of propagation delay. There are three different types of CSMA protocols:

- 1-Persistent CSMA
- Non-Persistent CSMA
- P-Persistent CSMA

1-Persistent CSMA

In this method, station that wants to transmit data, continuously senses the channel to check whether the channel is idle or busy. If the channel is busy, station waits until it becomes idle. When the station detects an idle channel, it immediately transmits the frame. This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.

Non-Persistent CSMA

A station that has a frame to send senses the channel. If the channel is idle, it sends immediately. If the channel is busy, it waits a random amount of time and then senses the channel again. It reduces the chance of collision because the stations wait for a random amount of time. It is unlikely that two or more stations will wait for the same amount of time and will retransmit at the same time.

P-Persistent CSMA

In this method, the channel has time slots such that the time slot duration is equal to or greater than the maximum propagation delay time. When a station is ready to send, it senses the channel. If the channel is busy, station waits until next slot. If the channel is idle, it transmits the frame.

CSMA/CD (CSMA with Collision Detection)

In this protocol, the station senses the channel before transmitting the frame. If the channel is busy, the station waits. Additional feature in CSMA/CD is that the stations can detect collisions. The stations abort their transmission as soon as they detect collision. In CSMA/CD, the station that sends its data on the channel, continues to sense the channel even after data transmission. If collision is detected, the station aborts its transmission and waits for a random amount of time & sends its data again. As soon as a collision is detected, the transmitting station release a *jam signal*. Jam signal alerts other stations. Stations are not supposed to transmit immediately after the collision has occurred.

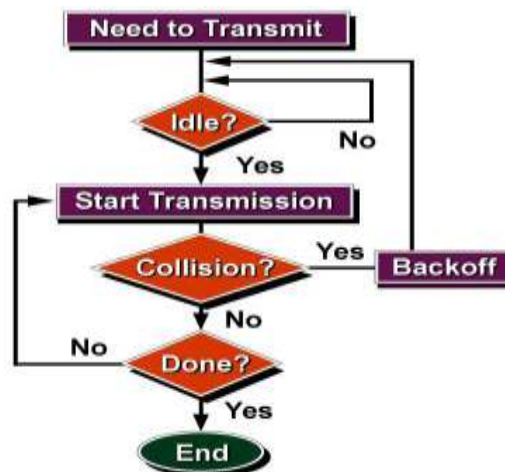


Figure: CSMA/CD

IEEE 802.3: Ethernet

The IEEE standard for Ethernet is 802.3. Ethernet operates in two areas of the OSI model: the lower half of the data link layer, which is known as the MAC sub layer, and the physical layer.

The CSMA/CD is the access method used in Ethernet to detect and avoid collision in network. Beside carrier sensing, collision detection and the binary exponential back-off algorithm, the

standard also describes the format of the frames and the type of encoding used for transmitting frames. The minimum length of frames can be varied from network to network.

The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. **Fast Ethernet** or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASE-T cards. **Gigabit Ethernet** provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.

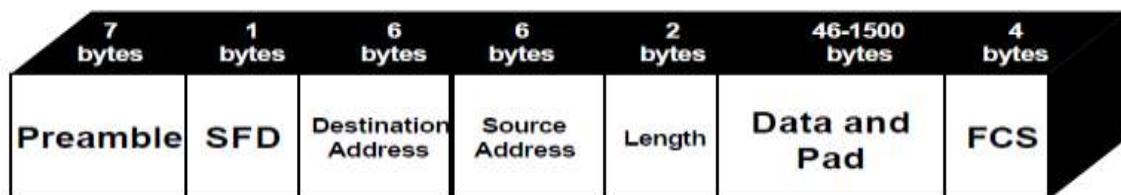


Figure: Ethernet Frame Format

IEEE 802.4: Token Bus

802.3 suffer from the difficulty of large delay in getting the access and at the same time poor performance under heavy load. There are also no priorities in 802.3, making them unsuited for real time systems. Token passing protocols were proposed and were found to be very attractive for situations with heavy load. The basic idea is to generate a token in the network. Only the holder of the token can transmit. Thus with one token, only one station can transmit at a time, eliminating collisions totally. Normally a token can be held by a user for a prescribed time only after which it has to be passed to the next station. If the user finishes his transmission before his token holding time is over, he passes the token to the next user.

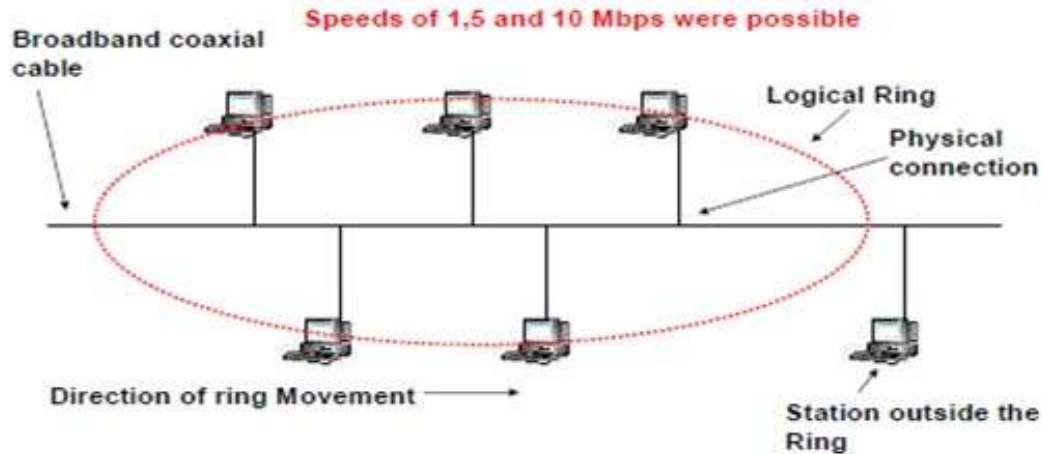


Figure (a): Token bus layout

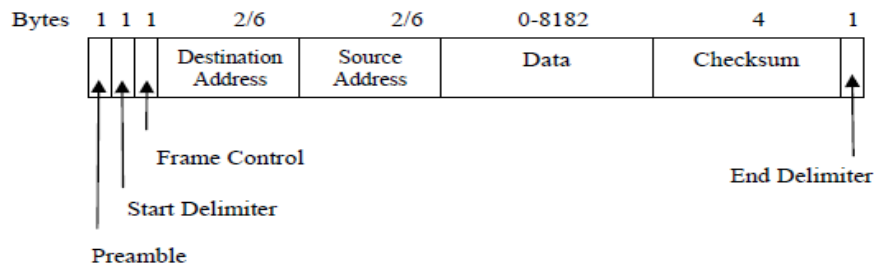


Figure (b): IEEE 802.4 Frame format

IEEE 802.5: Token Ring

Ring is not a broadcast medium but a collection of point-to-point links forming a circle. Rings can be based on twisted pair, coaxial or a fiber optics cable. Channel access problem is solved with the help of a special frame called a “Token”. A free token circulates the ring when all stations are idle. A station wishing to transmit must wait until it detects a free token passing by. It then seizes the token by changing the token bit to transform it into the start-of-frame sequence for a data frame. The data to be transmitted is then appended. The frame on the ring will make a round trip and then removed by the transmitting station.

Use of wire centers

Cable breaks can lead to ring failure. This problem can be resolved with the help of a Wire Center. A wire center has bypass relays which draw current from the station. If a station is powered down the relays close thereby removing the station from the ring and maintaining the

ring. Relays can be operated by software for network management. The wire centers make the ring a star-shaped ring.

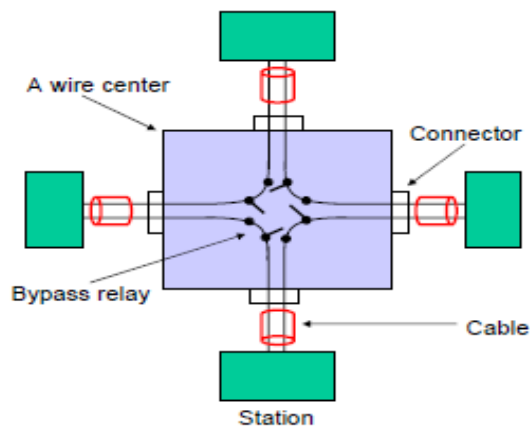


Figure (a): Four stations connected to a wire center

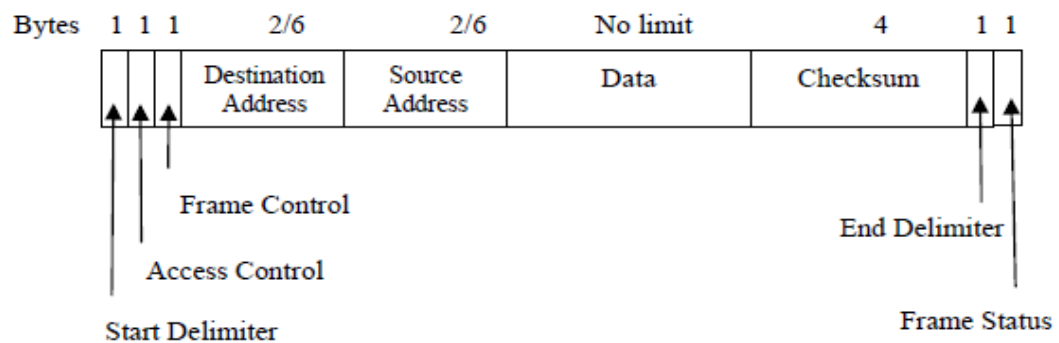
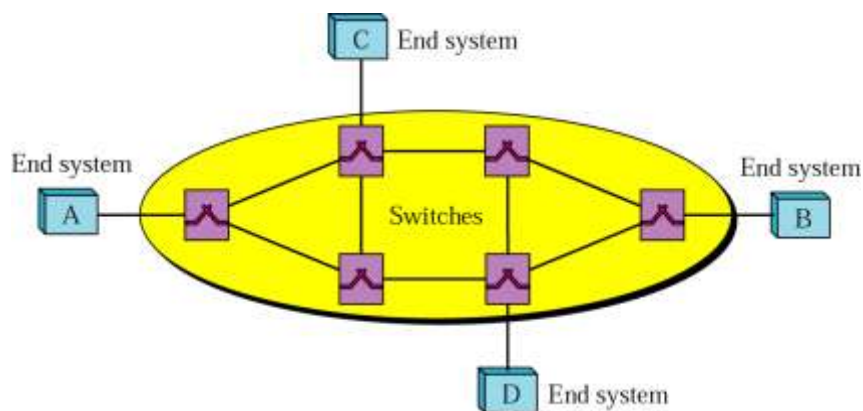
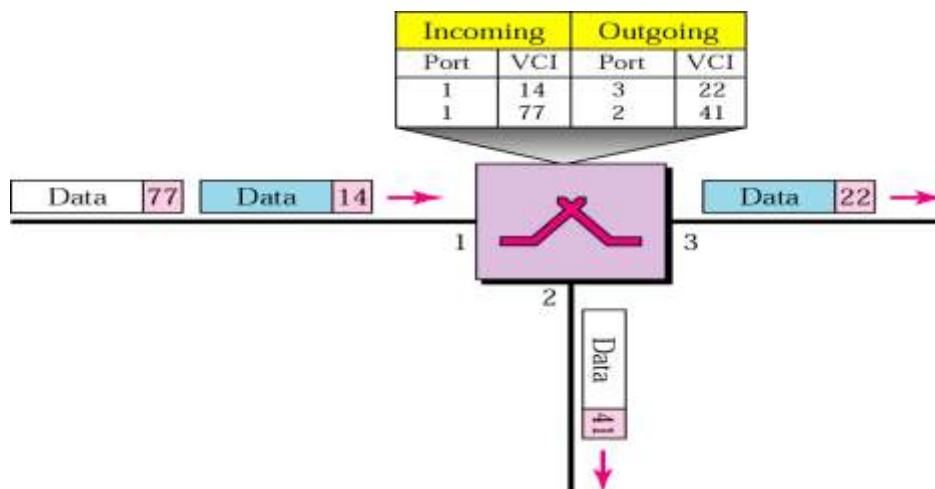
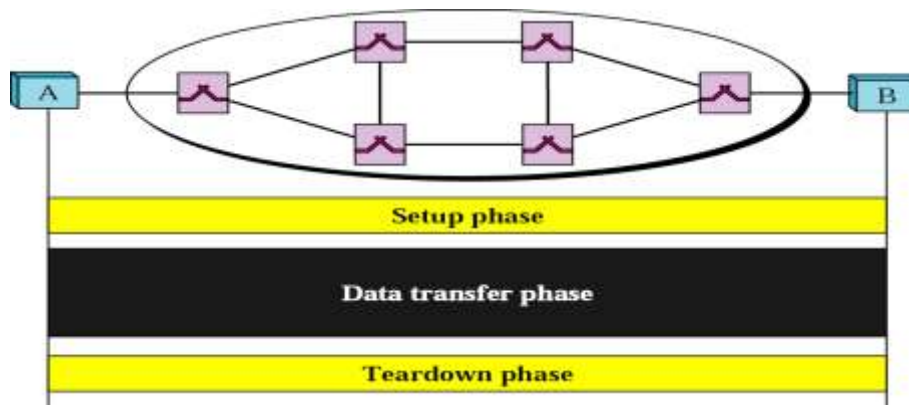
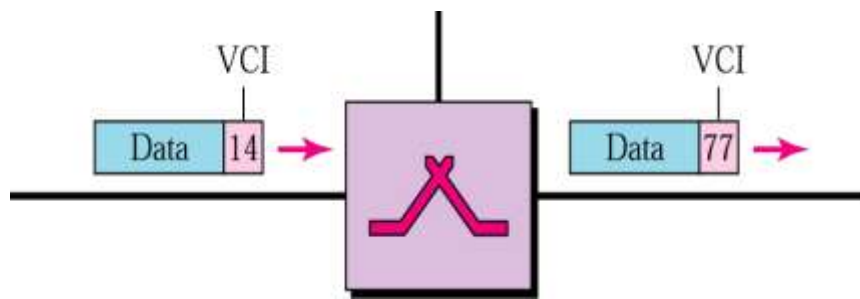
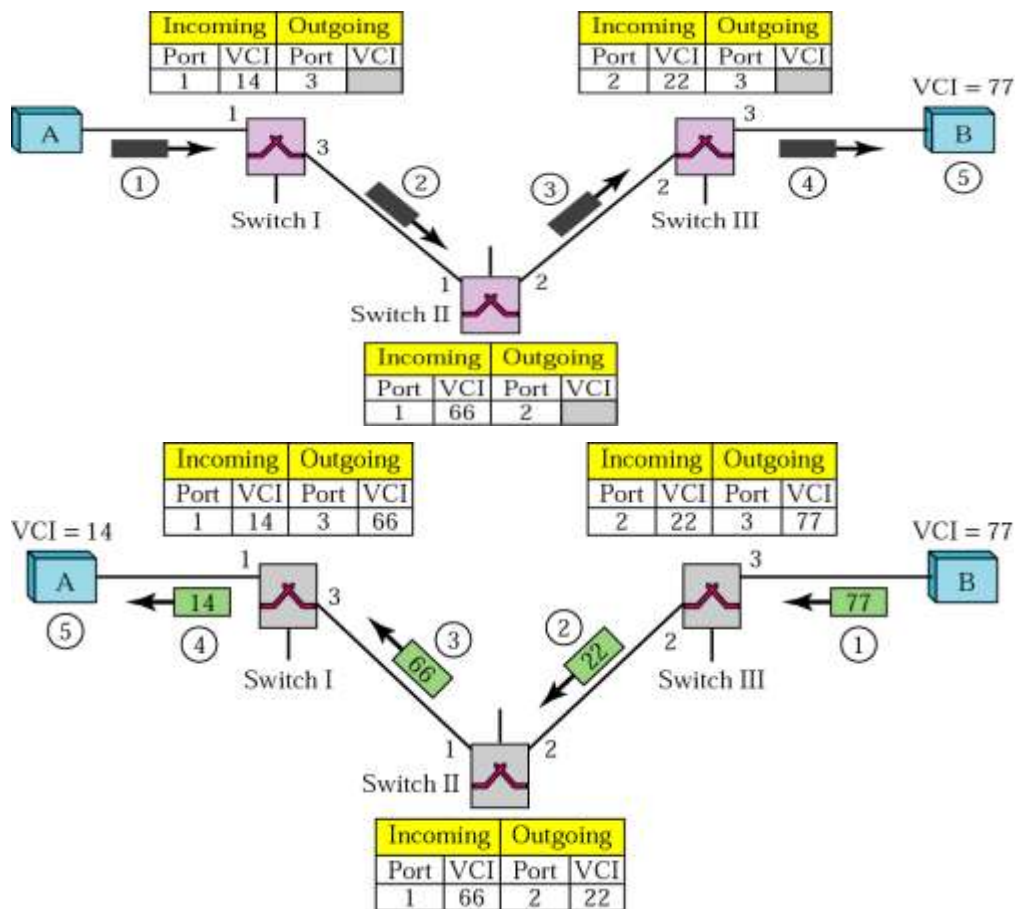
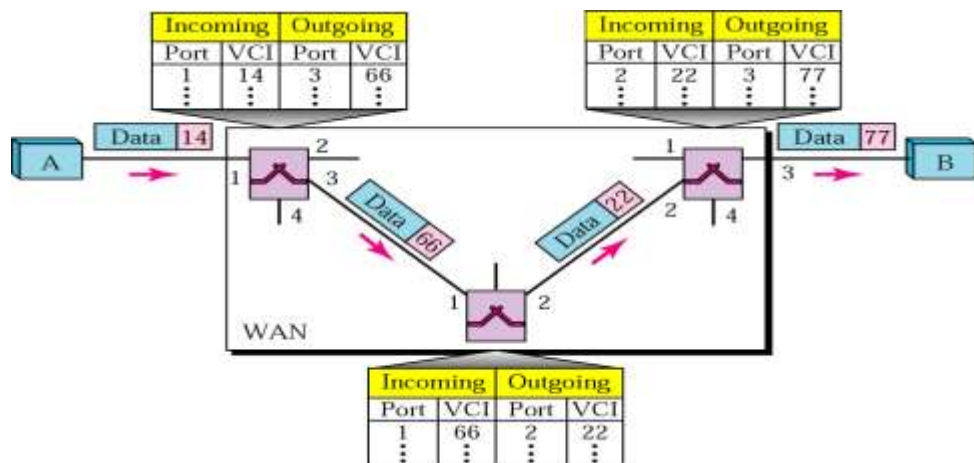


Figure (b): IEEE 802.5 Frame Format

Virtual Circuit Switching







Frame Relay

Frame Relay is a virtual-circuit wide-area network. It is connection-oriented network with no error control and no flow control. Therefore, packets are always delivered in the same order they were sent. It does not have a retransmission policy if a frame is damaged which is simply dropped. Frame relay was designed in this way to provide fast transmission capability for more reliable media and for those protocols that have flow and error control at the higher layers. Like any other connection-oriented systems, Frame Relay involves three phases, namely, connection establishment phase, data transmission phase and connection termination phase. Frame Relay is used for interconnecting LANs at multiple company offices, and can also be used as a backbone network.

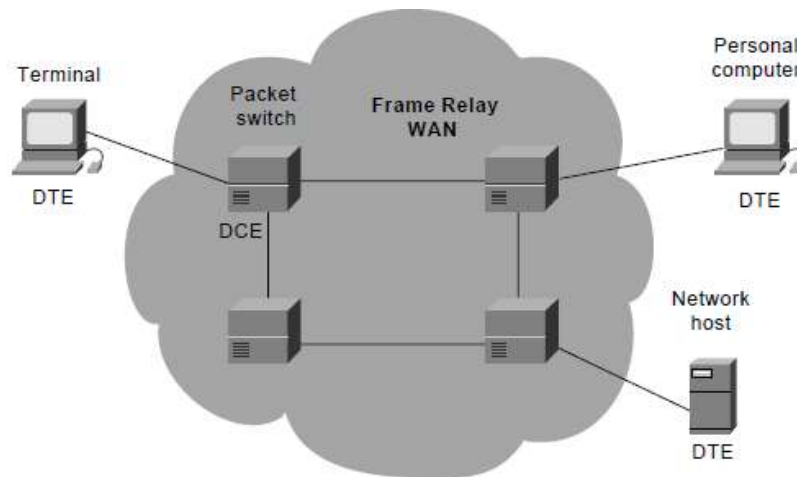


Figure: Basic frame relay setup

A Frame Relay network may be considered as a cloud that consists of switches, and customer nodes. The switch acts as Data Communication Equipment (DCE) and the customer equipment works as Data Terminal Equipment (DTE). A virtual circuit is established between the DTE and corresponding DCE. A virtual circuit is identified by a DLCI (Data Link Connection Identifier) number. On a given physical channel, there cannot be two DLCIs which are identical.

Permanent Virtual Circuit (PVC) and Switched Virtual Circuit (SVC)

In PVC, a permanent connection is established between two distant hosts that communicate frequently, and the process involves recording corresponding table entry for all the switches by the administrator. An outgoing DLCI is given to the source and an incoming DLCI is given to the destination. One of the drawbacks of PVC is that it is costly because the connection needs to

be kept connected all the time even when it is idle. Another drawback is that separate PVC is needed if a hosts needs to be connected to multiple hosts.

In a SVC, a temporary connection is established between the two distant hosts whenever data transfer is required, that is dynamically and is soon disconnected when the job is done. Thus SVC overcomes the shortcomings of the PVC. In an SVC three steps are required: (1) establish a connection, (2) transfer data and (3) terminate the connection.

Asynchronous Transfer Mode (ATM)

It is a switching technique used by telecommunication networks that uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. This is different from Ethernet or Internet, which use variable packet sizes for data or frames. *ATM* (also called *cell relay*) was originally designed to carry both voice and data traffic over WANs. ATM is the core protocol used over the synchronous optical network (SONET) backbone of the integrated digital services network (ISDN).

Characteristics of ATM

- ATM was designed with fixed cell structure in mind.
- ATM creates fixed routes between two points before data transfer begins
- ATM uses a mesh topology
 - This mesh is made up of point-to-point, full duplex circuits that interconnect ATM switches.
- ATM addressing uses *virtual channels (VCs)*.
- VCs can be set up in one of two ways:
 - Permanent Virtual Circuits (PVCs): permanent virtual circuits set up for long periods.
 - Switched Virtual Circuits (SVCs) : temporary virtual circuits set up for one transmission and deleted when the transmission is completed.

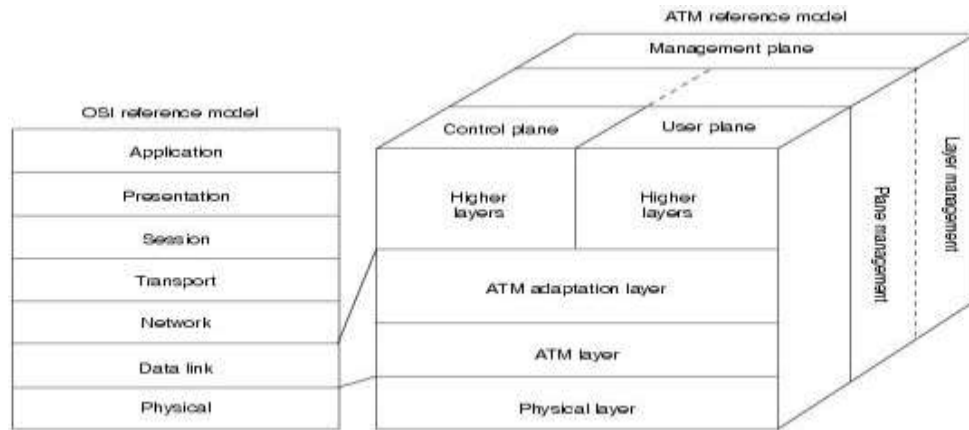


Figure: ATM

- ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model.
- The ATM reference model, as shown in Figure, consists of the following planes:
 - Control: This plane is responsible for generating and managing signaling requests.
 - User: This plane is responsible for managing the transfer of data.
 - Management: This plane contains two components:
 - Layer management manages layer-specific functions, such as the detection of failures and protocol problems.
 - Plane management manages and coordinates functions related to the complete system.
- The ATM reference model consists of the following ATM layers:
 - Physical layer: Analogous to the physical layer of the OSI reference model, the main functions of the ATM physical layer are as follows:
 - Cells are converted into a bit stream
 - The transmission and receipt of bits on the physical medium are controlled
 - ATM layer: Combined with the ATM adaptation layer, the ATM layer is roughly analogous to the data link layer of the OSI reference model.
 - The ATM layer provides routing, traffic management, switching and multiplexing services.

- It processes outgoing traffic by accepting 48-byte segment from the AAL sub-layers and transforming them into 53-byte cell by addition of a 5-byte header.
- ATM adaptation layer (AAL): Combined with the ATM layer, the AAL is roughly analogous to the data link layer of the OSI model.
 - The AAL is responsible for isolating higher-layer protocols from the details of the ATM processes.
 - AAL Protocol accepts transmission from upper layer services (e.g.: packet data) and map them into fixed-sized ATM cells.
 - There are four types of data streams that are identified: Constant-bit rate, variable bit-rate, connection oriented packet data transfer, connectionless packet data transfer.

X.25

X.25 is an International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) protocol standard for WAN communications that defines how connections between user devices and network devices are established and maintained. It is typically used in the packet-switched networks (PSNs) of common carriers, such as the telephone companies. Subscribers are charged based on their use of the network. The development of the X.25 standard was initiated by the common carriers in the 1970s. At that time, there was a need for WAN protocols capable of providing connectivity across public data networks (PDNs). X.25 is now administered as an international standard by the ITU-T.

X.25 Devices and Protocol Operation

X.25 network devices fall into three general categories: data terminal equipment (DTE), data circuit-terminating equipment (DCE), and packet-switching exchange (PSE). Data terminal equipment devices are end systems that communicate across the X.25 network. They are usually terminals, personal computers, or network hosts, and are located on the premises of individual subscribers. DCE devices are communications devices, such as modems and packet switches, that provide the interface between DTE devices and a PSE, and are generally located in the carrier's facilities. PSEs are switches that compose the bulk of the carrier's network. They

transfer data from one DTE device to another through the X.25 PSN. Figure 1.7 illustrates the relationships among the three types of X.25 network devices.

Figure below shows DTEs, DCEs, and PSEs that make up an X.25 Network

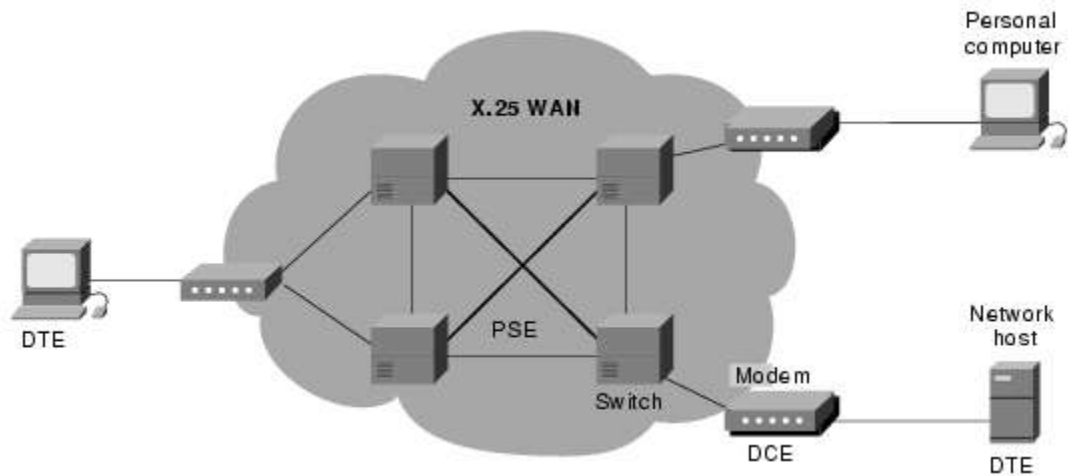


Figure: X.25 Network

Chapter 5: Network Layer

Introduction

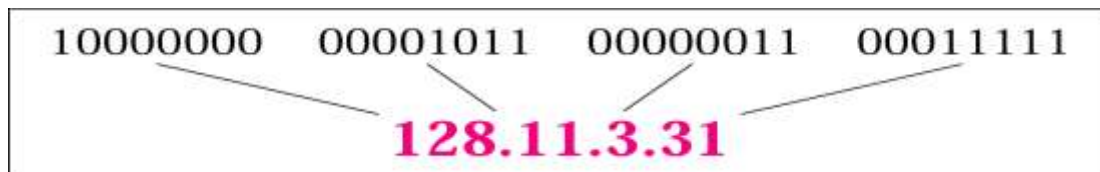
- Layer 3 or Network Layer is backbone of the OSI model
- It finds the best path for data transfer between nodes
- It manages device addressing

A routed protocol is a Layer 3 protocol that applies logical addresses to devices and routes data between networks (such as IP)

A routing protocol dynamically builds the network, topology, and next hop information in routing tables (such as RIP, EIGRP, etc.)

IPV4 address

- 32 bit address
- Total unique address equals to 2^{32}
 - Around 4.2 billion address
- Represented in dotted Decimal Format
- IANA has authority for IP address management



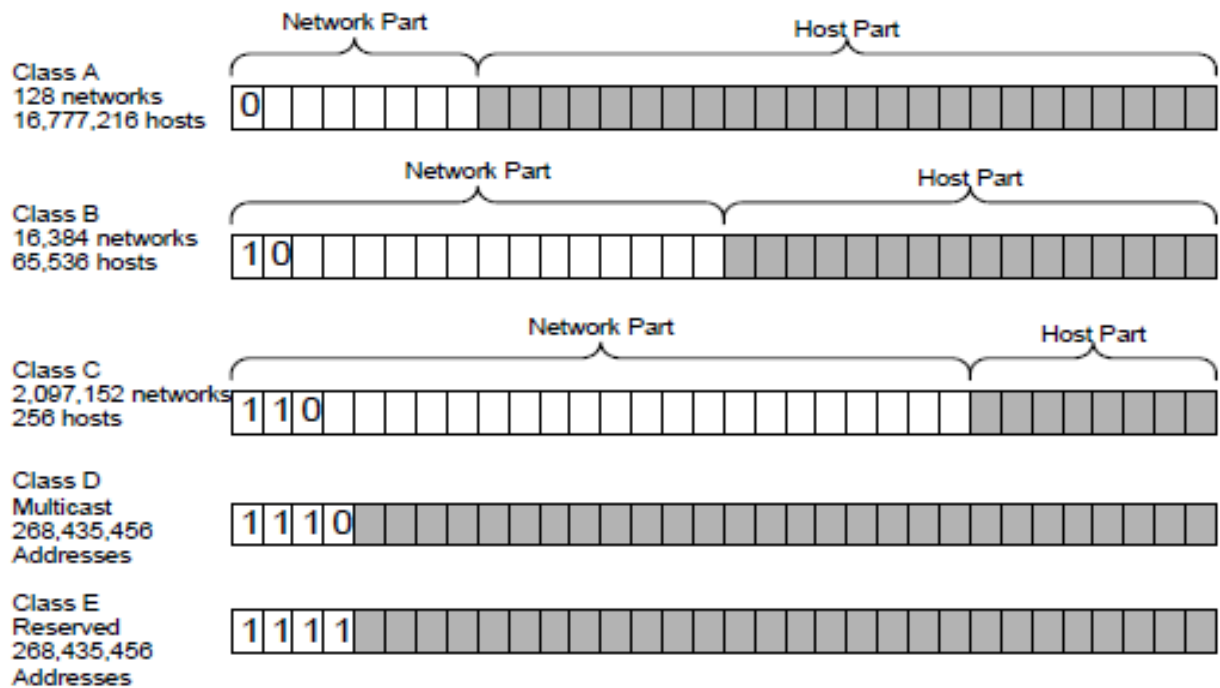
Example of IPV4 address

RIR-Regional Internet Registry manages allocation and registration of internet

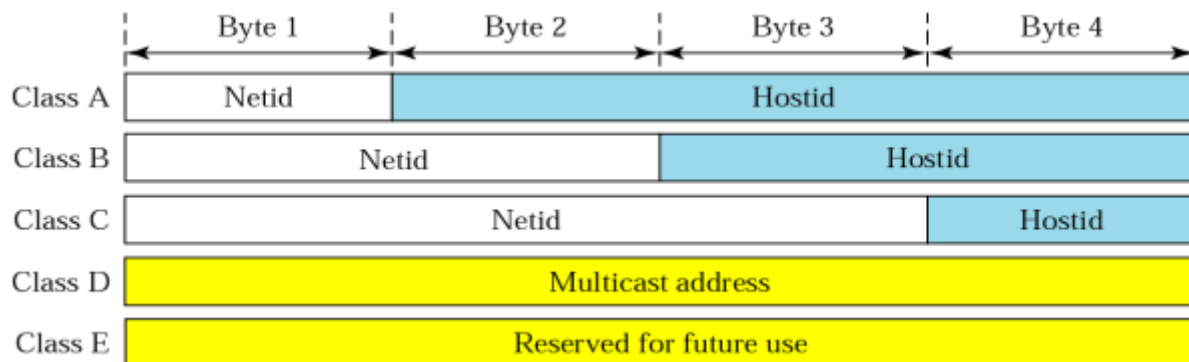
5 RIR are:

- APNIC(Asia Pacific Network Information Centre)
- ARIN (American Registry for Internet Numbers)
- LACNIC (Latin America and Caribbean Network Information Centre)
- AFRINIC (Africa Network Information Centre)
- RIPE NCC (Reseaux IP Europeans Network Coordination Centre)

Classful Addressing



Network Id and Host Id in Classful addressing



Default subnet mask for Classful address

Class	In Binary	In Dotted-Decimal	Using Slash
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Logical Address

- IP address at the Network Layer
- Used to Communicate with the different subnets
- Netid: Identify network
- Hostid: Identify End devices
- Mask: Used to find netid and hostid
- CIDR: Classless interdomain routing
 - Used in classless addressing
 - Defined by slash notation /n
 - Example: /8, /16, /24

Subnetting and Supernetting

- Subnetting
 - Method used to divide the addresses into several contiguous groups (network)
- Supernetting:
 - Several Network are combined to create a SuperNetwork
 - Mainly used to combine several class C blocks to create a large range of address
 - Supernetting decrease the number of 1s in the mask

Classless Addressing

- To overcome address depletion, classless concept is used
- For classless addressing
 - The address in a block must be contiguous
 - The number of address in a block must be power of 2

Private IP Address

- Range of IP address, which are not routable to internet commonly used for home, office, and enterprise local area networks (LANs)
- If such a private network needs to connect to the Internet, it must use either a network address translator (NAT) gateway, or a proxy server.

Class A	10.0.0.0 – 10.255.255.255
Class B	172.16.0.0 – 172.31.255.255
Class C	192.168.0.0 – 192.168.255.255

Introduction to IPV6

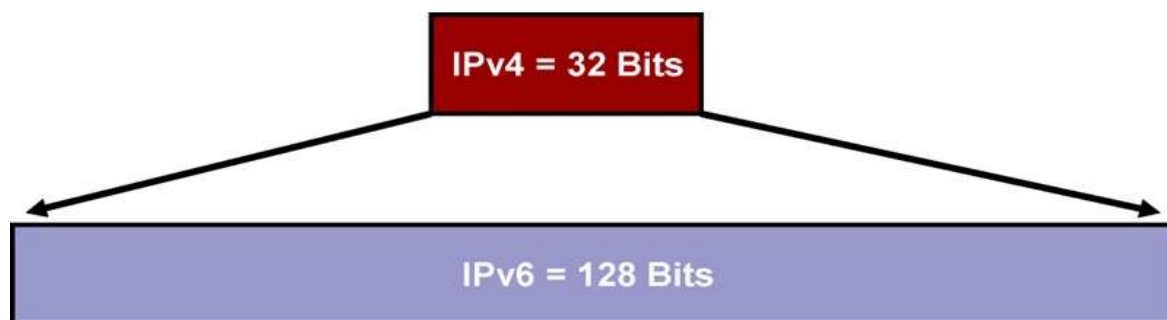
- Major points that played a key role in the birth of IPv6 (drawback of IPv4):
 - address space allowed by IPv4 is saturating.
 - IPv4 on its own does not provide any security features.
 - Data has to be encrypted with some other security application before being sent on the Internet.
 - IPv4 enabled clients can be configured manually or they need some address configuration mechanism.
 - It does not have a mechanism to configure a device to have globally unique IP address.

Features

- Larger Address Space (128 Bit Address Space).
- Supports Resource Allocation via Flow Control Field.
- Supports More Security
- Better Header Format (Base Header and Extension Header)

IPv6 Address

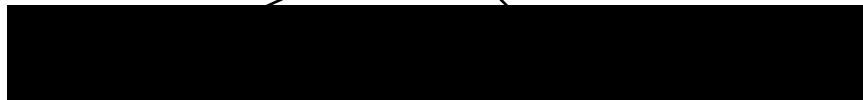
- IPv6: 128 bits or 16 bytes
 - $3.4 * 10^{38}$ possible addressable nodes
 - 340,282,366,920,938,463,374,607,432,768,211,456



128-bit IPv6 Address



Leading Zeros can be removed



Unabbreviated

FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF



FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF

Abbreviated

Abbreviated

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF



FDEC : : BBFF : 0 : FFFF

More Abbreviated

Transition from IPv4 to IPv6

- ☐ Tunneling
- ☐ Dual Stack
- ☐ Header Translation

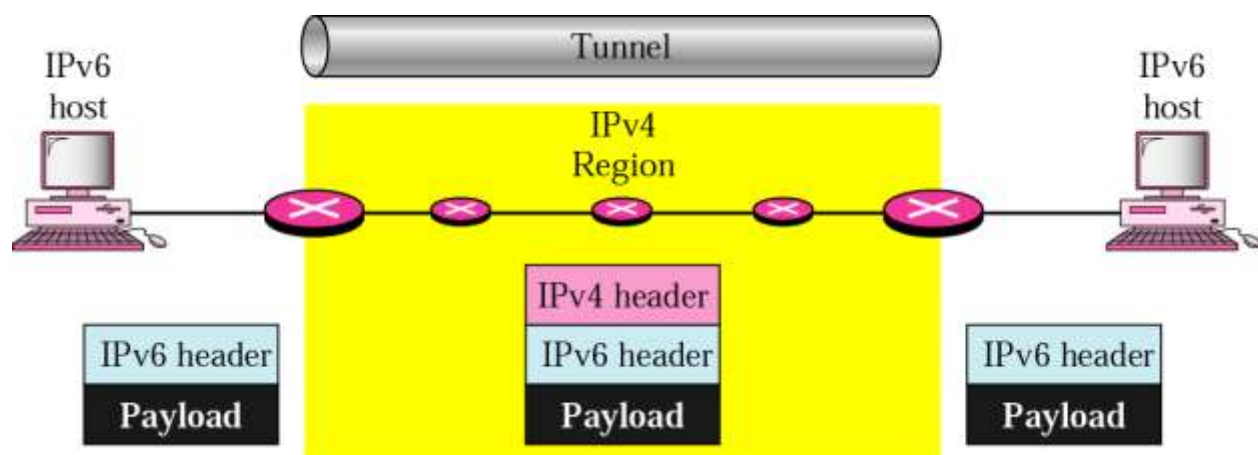


Figure: Tunnelling

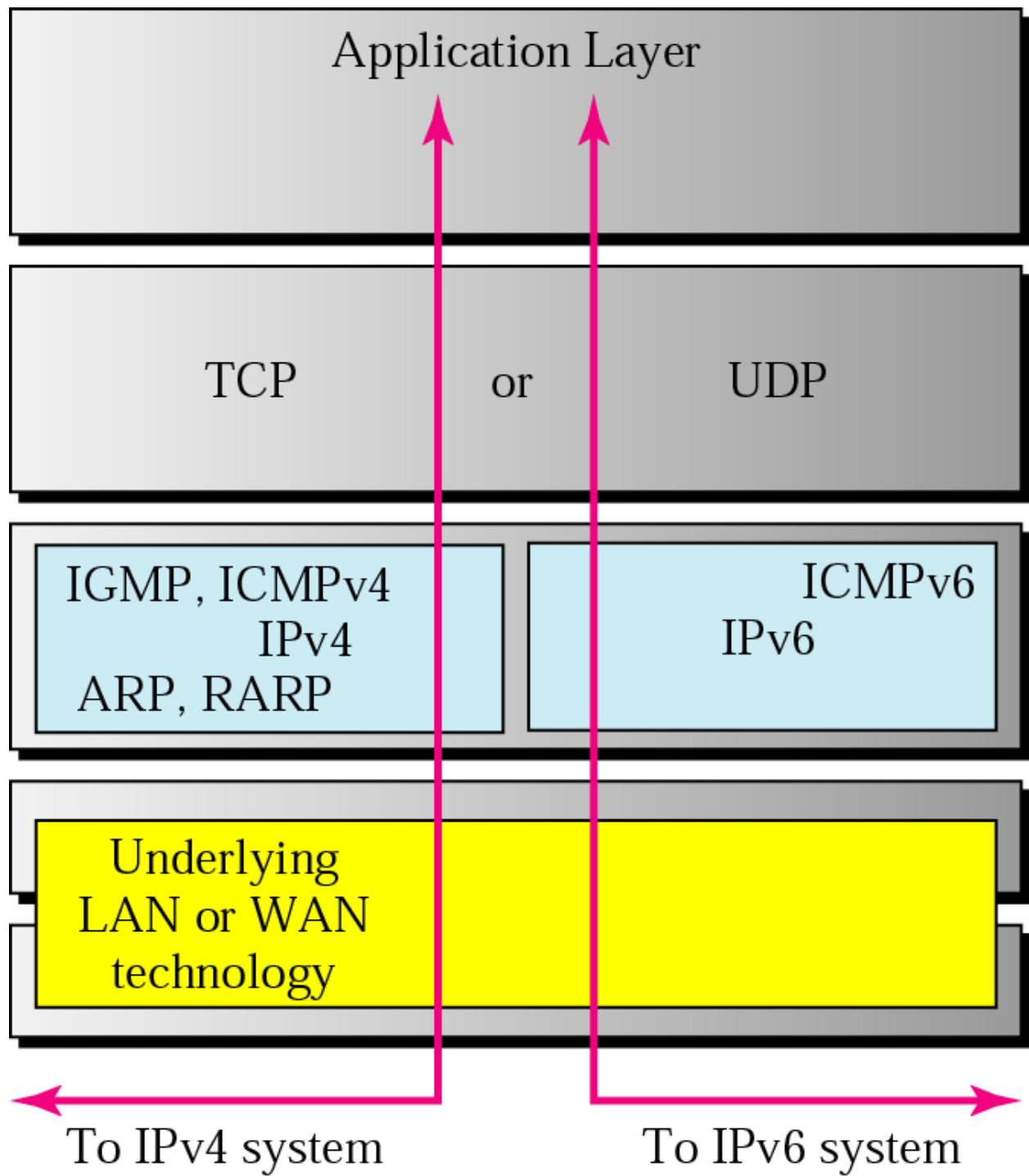


Figure: Dual Stack

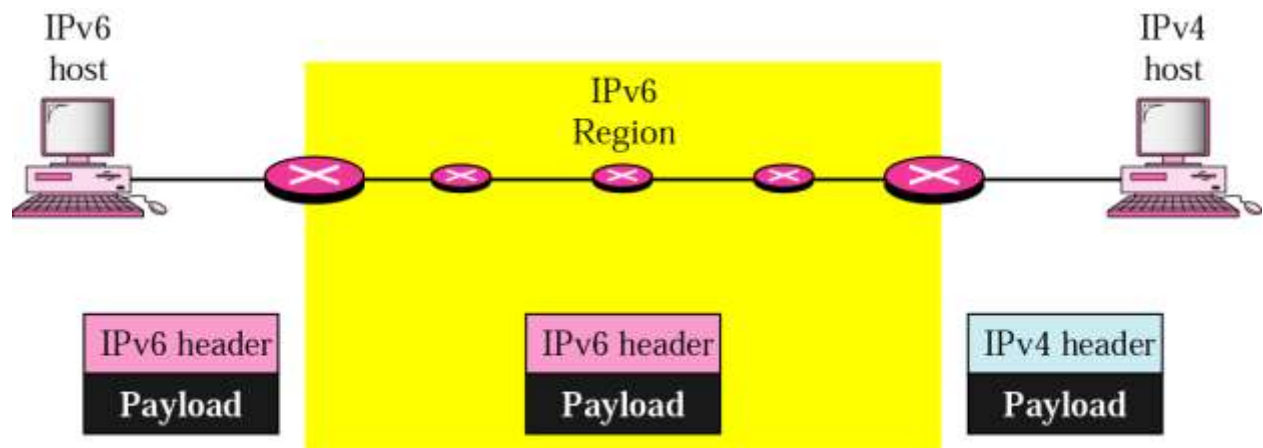


Figure: Header Translation

IPv4 & IPv6 Header Comparison

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

Figure: IPV4 Header

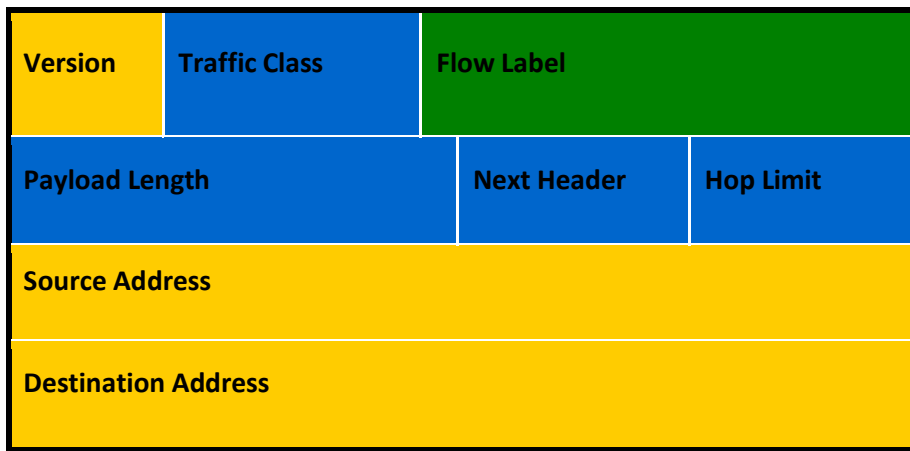






Figure: IPV6 Header

-  Field's name kept from IPV4 to IPV6
-  Field's name not in IPV6
-  Name and position changed in IPV6
-  New field in IPV6

Comparison of IPV4 and IPV6 Addressing

IPV4	IPV6
IPV4 addresses are 32 bit	IPV6 addresses are 128 bit
IPV4 are represented in dotted decimal format	IPV6 addresses are represented in hexadecimal format separated by colon(:)
IPSec support is only optional	Inbuilt IPSec support
Fragmentation is done by senders and forwarding routers	Fragmentation is done by sender
No packet flow identification	Packet Flow identification is available using Flow Label field
Checksum field is available in IPV4 header	No checksum field in IPV6 header
IPV4 configuration is done manually or using DHCP	Auto-configuration addresses is available

Options field is available	No options field but IPV6 extension header are available
Limited address space	Large addressing space
Broadcast address are available	No broadcast, its function is superseded by multicast address

Routing Algorithm Overview

Classful Routing

- Classful routing protocols do not send the subnet mask along with their updates
- Examples of Classful routing protocol is RIP version 1

Classless Routing Protocols

- Classless Routing Protocols send the Subnet mask along with their updates
- Benefits for using Classless routing protocols
 - We can save lot of IP address using VLSM techniques in classless routing protocols
 - Examples: OSPF, EIGRP, RIPV2

Adaptive Routing Protocols

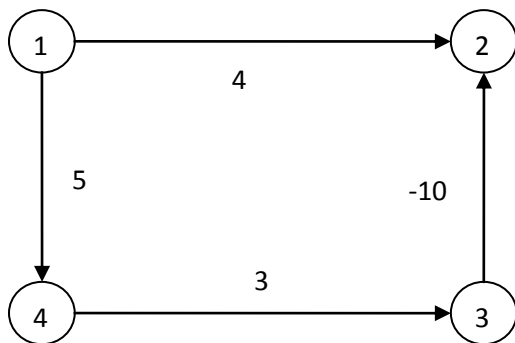
- Adaptive routing protocols can easily adapt to network changes.
- Routing protocols are used by routers to inform one another of the IP networks accessible to them.
- Adaptive Routing protocols are also called Dynamic routing Protocols
- Examples of Adaptive routing Protocols are: OSPF, EIGRP, RIP, BGP, IGRP

Non-Adaptive Routing Protocols

- Non Adaptive Routing Protocols doesn't respond to change in topology
- Non-Adaptive Routing Protocols are also called as Static routing Protocols
- Non-Adaptive Routing protocols are more secure than Adaptive Routing protocols as they don't advertise the routing update unnecessarily
- Network Administrator is responsible for configuring the static routing in the router
- Static routes are fixed and do not change if the network is changed or reconfigured

Distance Vector Routing

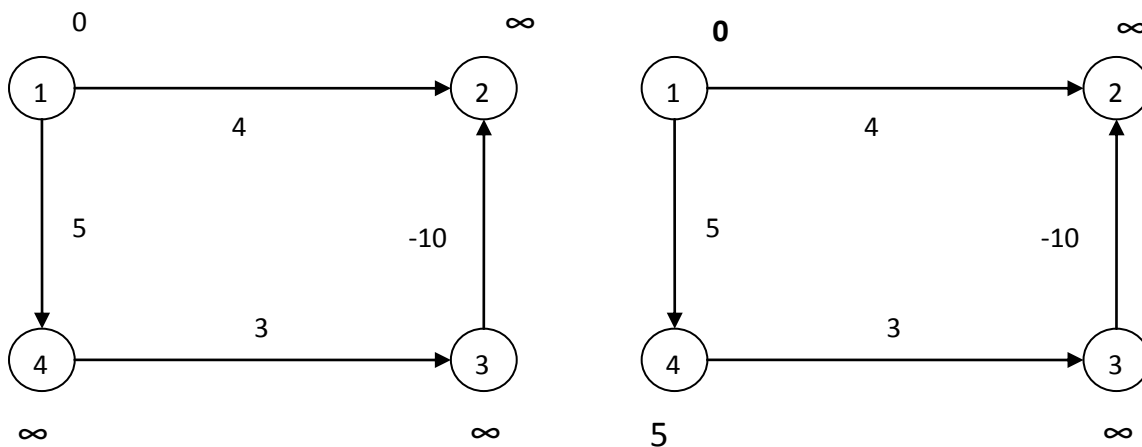
It is a dynamic routing algorithm. Distance vector routing algorithms operate by having each router maintain a table (i.e, a vector) giving the best known distance to each destination and which line to use to get there. These tables are updated by exchanging information with the neighbors. It is also called Bellman-Ford routing algorithm.



Let us consider source vertex 1, then we need to find the shortest path to all other vertices or nodes. For n vertices, n-1 iteration gives the shortest path, but we may get result in less than n-1 as well. Since there are 4 vertices we need 3 iteration to find the shortest path.

Edges-> (3,2),(4,3),(1,4),(1,2)

Iteration 1



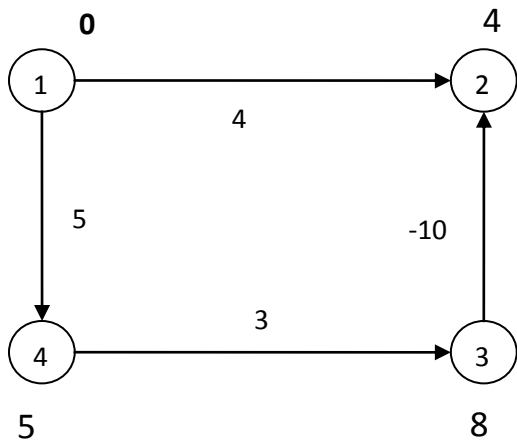
Initially the initial vertex is marked as 0 and other as infinity, then we find the cost to every vertex according to edges as: (3, 2) -> $\infty - 10 = \infty$

(4, 3) -> $\infty + 3 = \infty$

(1, 4) -> $0 + 5 = 5$ (less than infinity so take this value)

(1,2) -> $0 + 4 = 4$ (less than infinity so take this value) [take value if less than given value]

Iteration 2



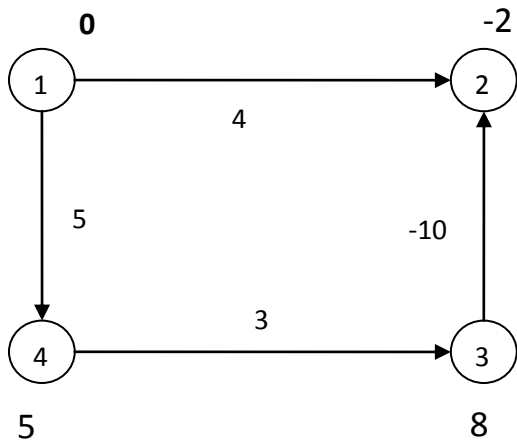
$$(3,2) \rightarrow \infty - 10 = \infty$$

$$(4,3) \rightarrow 5 + 3 = 8$$

$$(1,4) \rightarrow 0 + 5 = 5$$

$$(1,2) \rightarrow 0 + 4 = 4$$

Iteration 3



$$(3,2) \rightarrow 8 - 10 = -2$$

$$(4,3) \rightarrow 5 + 3 = 8$$

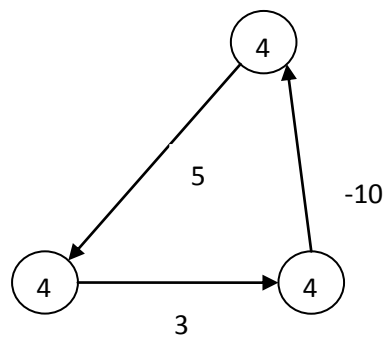
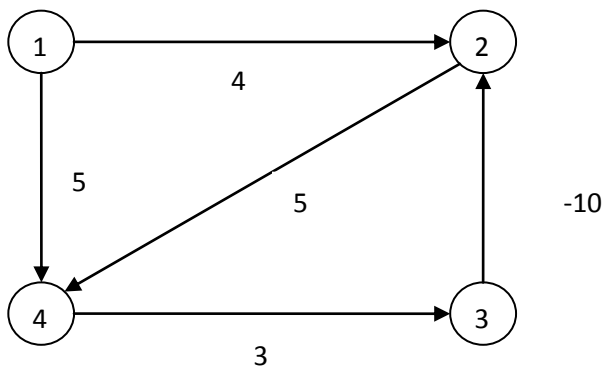
$$(1,4) \rightarrow 0 + 5 = 5$$

$$(1,2) \rightarrow 0 + 4 = -2$$

Change value only if you get lesser value in the iterations.

So shortest path from 1 to other vertices are: 1=0, 2=-2, 3=8 and 4=5

Drawbacks



If there is negative weight with cycle, then we don't get result in n-1 iteration it could go on and we can see in above example, but it works with positive result.

Link State Routing

- Distance vector routing algorithm such as rip has limitations that they don't work for longer network
- Convergence and scalability problem for topology changes
- Link state routing is used to overcome those limitations
 - Link state routing has full knowledge of network.
 - Each node maintains the full graph by collecting the updates from all other nodes
 - Each node then independently calculates the next best logical *path* from it to every possible destination in the network
 - Router's receive topology information from their neighbor router via link state advertisements(LSA)
 - Use Dijkstra's shortest path first algorithm to find out optimal paths
 - Link state protocols don't have to constantly resend their entire LSAs instead they can send small hello LSAs to let their neighbor routers know they are still alive
- The idea behind link state routing is fairly simple and can be stated as five parts. Each router must do the following:
 - Discover its neighbors, learn their network address.
 - Measure the delay or cost to each of its neighbors.
 - Construct a packet telling all it has just learned.
 - Send this packet to all other routers.
 - Compute the shortest path to every other router.

Interior Routing Protocols

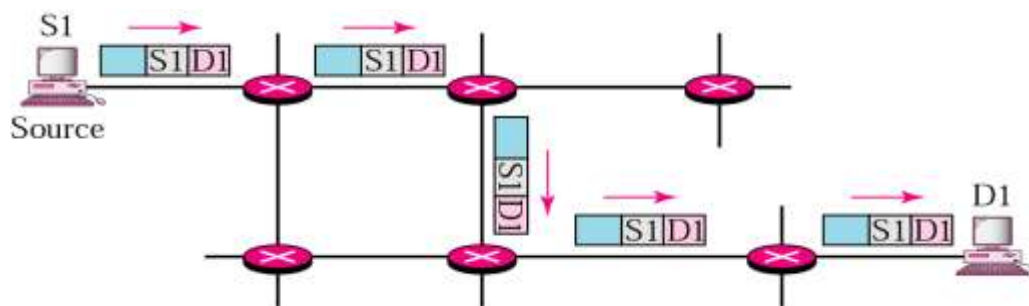
- Used for Routing Inside an Autonomous System (AS).
- Used within the Organization
- AS => Network under Common Administration.
- Router having Same AS, share their routing tables
- Examples => RIP, EIGRP and OSPF, IGRP

Exterior Routing Protocols

- Used for Routing between Autonomous System (AS)
- Border Gateway Routing Protocols (BGP)
- Used between the organization (ISPs to ISPs)

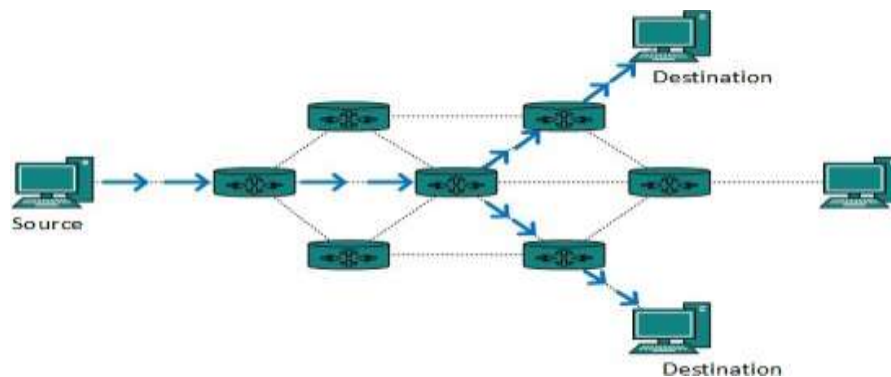
Unicast Routing

- In unicasting there is a single sender (source) and a single receiver (destination)
- In unicast routing, the router forwards the received packet through only one of its interfaces
- Examples of Unicast Routing are: OSPF, RIP and BGP



MultiCast Routing

- In multicasting there is at least one sender and several receivers (group of receivers called multicast group)
- In multicast routing, the router may forward the received packet through several of its interfaces.
- M-cast group address “delivered” to all receivers in the group
- Internet uses Class D for m-cast
- M-cast address distribution, etc. managed by IGMP Protocol



RIP (Routing Information Protocol)

RIP is a routing protocol for exchanging routing table information between routers. Routing updates must be passed between routers so that they can make the proper choice on how to route a packet. It is oldest Distance Vector Routing Protocol. It update routing table every 30 sec. It uses Hop count as Metric to find best path to the destination. RIP has a maximum hop count of 15. A route with a hop count greater than 15 is considered unreachable. It has two version:RIP Version 1 and RIP Version 2. RIP version 1 is the classful routing protocol. RIP Version 2 is classless routing protocol. In fact, most DSL/cable modem routers such as the ones from Linksys come bundled with RIP.

OSPF (Open Shortest Path First)

It is a Classless routing protocol. It uses a link state routing algorithm and falls into the group of interior routing protocols. OSPF was developed as a replacement for the distance vector routing protocol RIP. It uses cost to find the best route to find the destination

Every intra-domain must have a core area

- It is referred to as a *backbone area*
- This is identified with Area ID 0
- Areas are identified through a 32-bit area field
- Thus Area ID 0 is the same as 0.0.0.0

Areas (other than the backbone) are sequentially numbered as Area 1 (i.e., 0.0.0.1), Area 2, and so on

BGP (Border Gateway Routing Protocols)

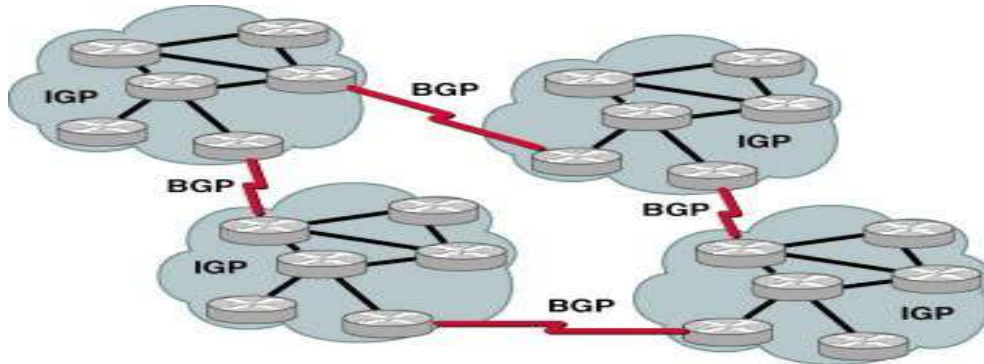
It is designed to exchange routing and reach-ability information between autonomous systems (AS) on the Internet. It is of two types: Internal BGP and External BGP. Internal BGP has the Administrative Distance of 200 while external BGP has the Administrative Distance of 20. The protocol is often classified as a path vector protocol, but is sometimes also classed as a distance-vector routing protocol.

PATH VECTOR PROTOCOL

It is a routing protocol which maintains the path information that gets updated dynamically.

Updates which have looped through the network and returned to the same node are easily detected and discarded. Peers exchange BGP messages using TCP. BGP defines 4 types of messages:

- OPEN: opens a TCP connection to peer and authenticates sender
- UPDATE: advertises new path (or withdraws old)
- KEEPALIVE: keeps connection alive in absence of UPDATES; also serves as ACK to an OPEN request
- NOTIFICATION: reports errors in previous message; also used to close a connection



Chapter 6: Transport layer and protocols

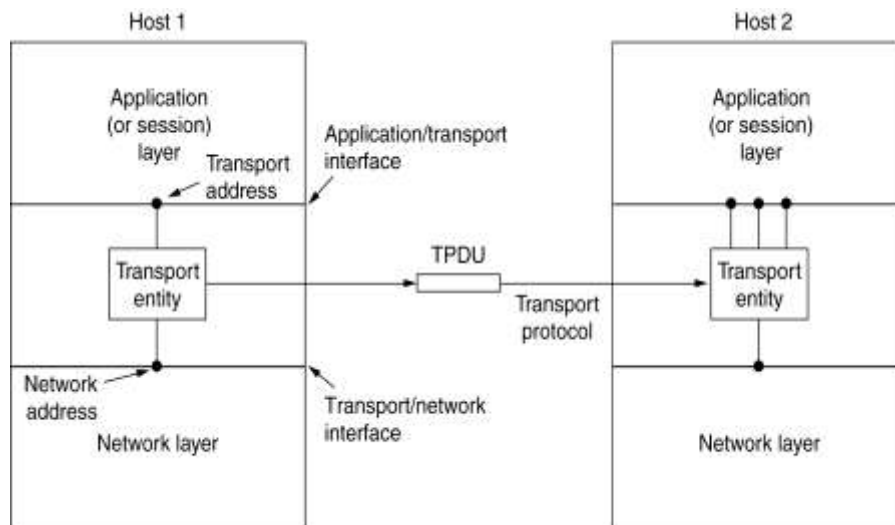
Why do we need a Transport Layer?

With a Network Service Provider you can exchange packets between hosts (e.g. PCs), these hosts are uniquely identified by their network address (e.g. IP address). As a user you may want to send and receive email, browse the web, logon to another host. So, you may want to run several programs or processes. The transport layer allows for processes or applications to communicate with each other. Networks (and the network layer) is under control of a network operator. The network service users have no control over it. So, if something goes wrong, a user can do nothing.

The transport service is what users can add to improve the reliability of the service provided by the network. Functions that you can encounter in the Transport Layer are:

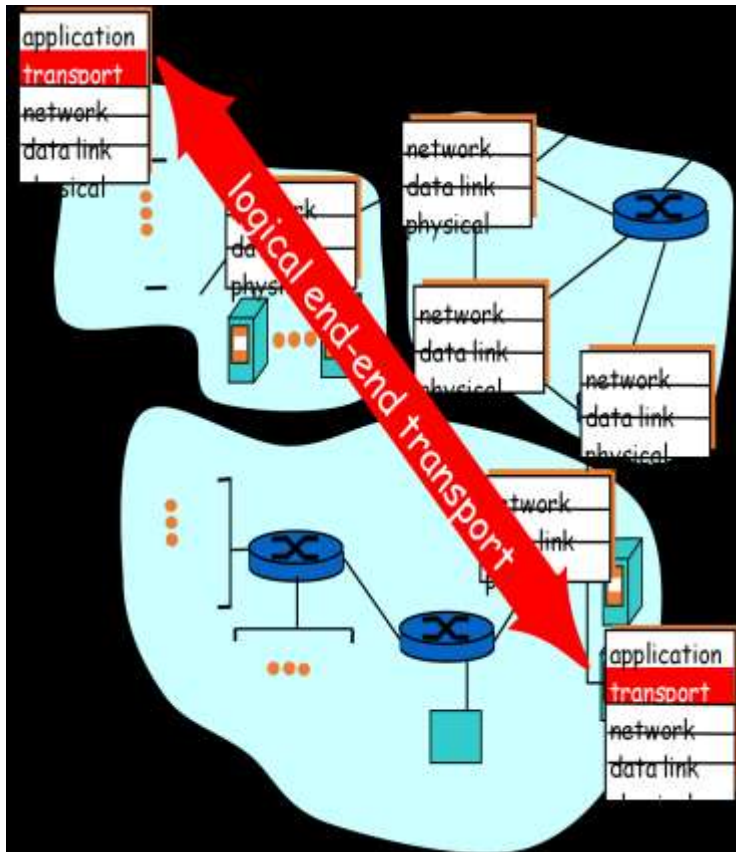
- Error Handling
- Flow Control
- Multiplexing
- Connection Set-up and Release
- Congestion Handling
- Segmentation and Reassembly
- Addressing

Services Provided to the Upper Layers



- The ultimate goal of the transport layer is to provide efficient, reliable, and cost-effective data transmission service to its users, normally processes in the application layer.
- The software and/or hardware within the transport layer that does the work is called the transport entity.

- It provide *logical communication* between application processes running on different hosts
- Transport protocols run in end systems
 - send side: breaks application messages into segments, passes to network layer
 - receive side: reassembles segments into messages, passes to application layer
- more than one transport protocol available to apps
 - Internet: TCP and UDP



Port Addressing

- Ports are conceptual “points of entry” into a host computer.
- Usually a service is associated with a port (e.g. http on port 80).
- Servers “listen on a port” for connection attempts.
- Ports provide one level of internet security.
 - Each *process that wants to communicate with another process identifies itself to the TCP/IP protocol suite by one or more ports.*
- Popular applications have well-known ports.

- Ranges of Port Number
 - Server has a well-known port (e.g., port 80 for HTTP)
 - Between 0 and 1023 (requires root to use)
 - Allocated to server services by IANA
 - Registered Port
 - Between 1024 and 49151
 - Can be registered for services with the IANA
 - Client picks an unused ephemeral (i.e., temporary) port
 - Between 49152 and 65535
 - Used by client programs

Services	Listens on Port
HTTP	80
Telnet	23
SMTP	25
FTP Control	21
FTP Data	20
SSH	22
POP3	110
IMAP	143

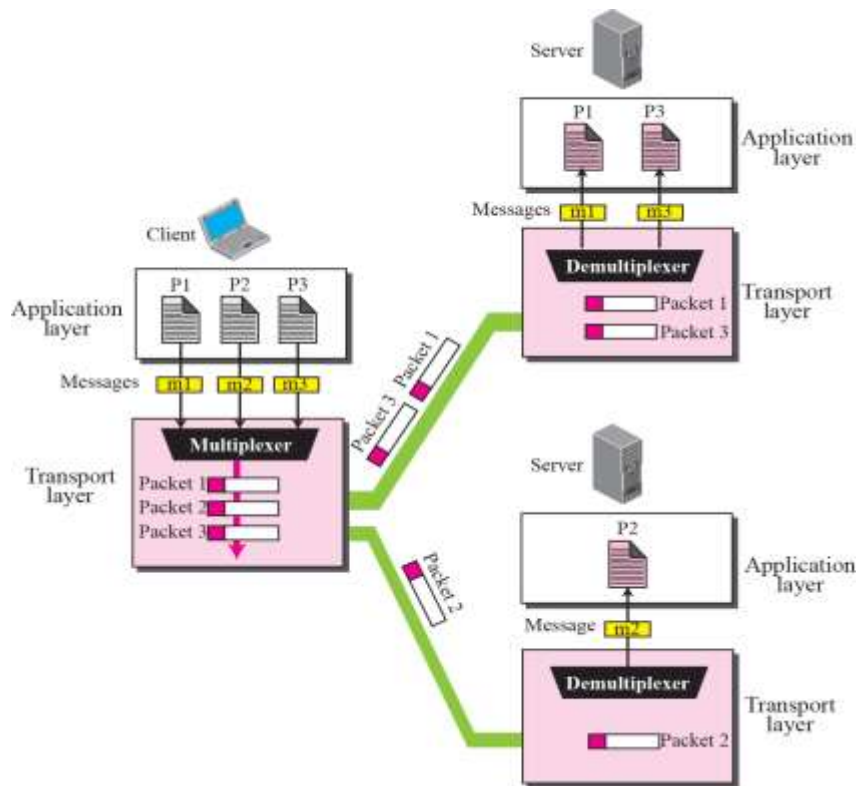
Multiplexing & De-multiplexing

De-multiplexing at rcv host:

It is associated with delivering received segments to correct socket

Multiplexing at send host:

It is concerned with gathering data from multiple sockets, enveloping data with header (later used for de-multiplexing)



Connectionless de-multiplexing

- UDP socket identified by two tuple:
 - (destination IP address, destination port number)
- When host receives UDP segment:
 - checks destination port number in segment
 - directs UDP segment to socket with that port number

Connection-oriented de-multiplexing

- TCP socket identified by 4- tuple:
 - source IP address
 - source port number
 - destination IP address
 - destination port number
- Receiving host uses all four values to direct segment to appropriate socket
- Server host may support many simultaneous TCP sockets:
 - each socket identified by its own 4-tuple

- Web servers have different sockets for each connecting Client
 - non-persistent HTTP will have different socket for each request

Transmission Control Protocol (TCP)

TCP Protocol Functions

- Multiplexing
- Error Handling
- Flow Control
- Congestion Handling
- Connection Set-up and release

TCP Transport Service

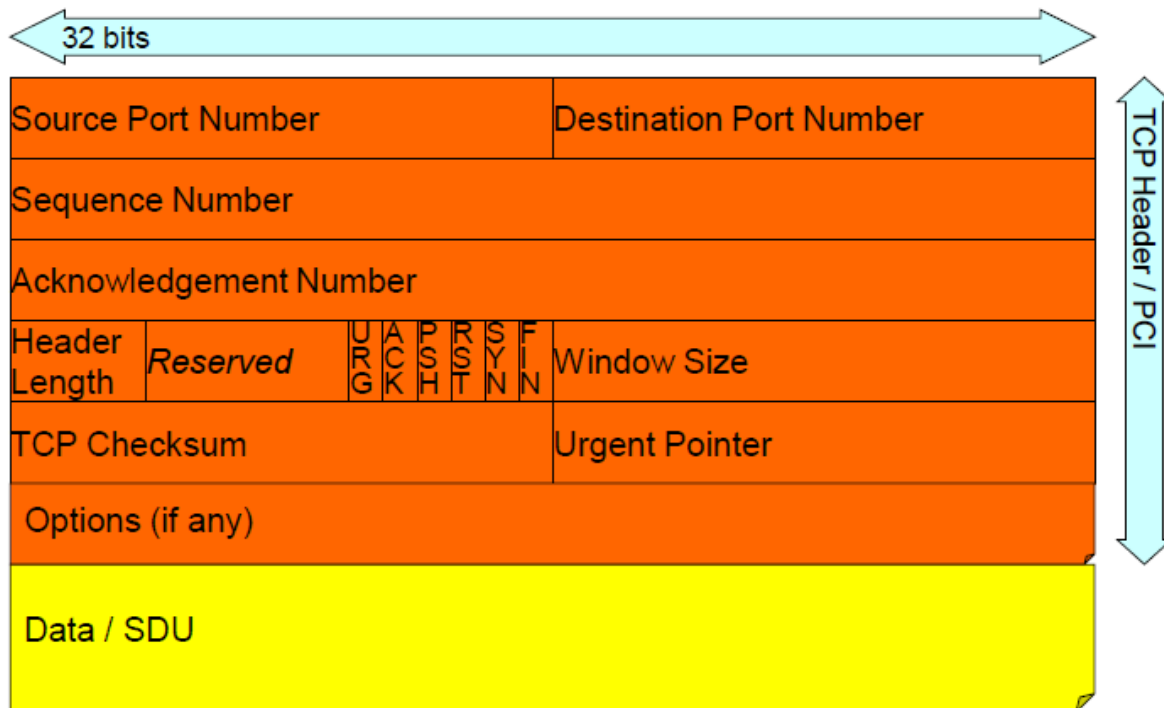
- Connection Oriented (full duplex point-to-point connection between processes).
- Reliable
- In-sequence segment delivery

Well-known TCP ports

Protocol	TCP port
HTTP	80
HTTPS	443
FTP	20,21
SMTP	25
Telnet	23
IMAP	143
POP3	110

TCP Segment

- ✓ Source Port: The 16-bit source port number, used by the receiver to reply.
- ✓ Destination Port : The 16-bit destination port number
- ✓ Sequence Number : The sequence number of the first data byte in this segment.
- ✓ Acknowledgment Number: If the ACK control bit is set, this field contains the value of the next sequence number that the receiver is expecting to receive.
- ✓ Header length: A 4-bit field that represents the header length in multiple of four bytes
- ✓ Reserved: Six bits reserved for future use; must be zero.
- ✓ URG: Indicates that the urgent pointer field is significant in this segment.



- ✓ ACK: Indicates that the acknowledgment field is significant in this segment.
- ✓ PSH: Push function.
- ✓ RST: Resets the connection
- ✓ SYN: Synchronizes the sequence numbers.
- ✓ FIN : No more data from sender.
- ✓ Window size: It specifies the number of data bytes that the receiver is willing to accept.
- ✓ Checksum : A 16-bit field used for error correction.
- ✓ Urgent Pointer : Points to the first data octet following the urgent data.

Opening a connection (3-way handshake):

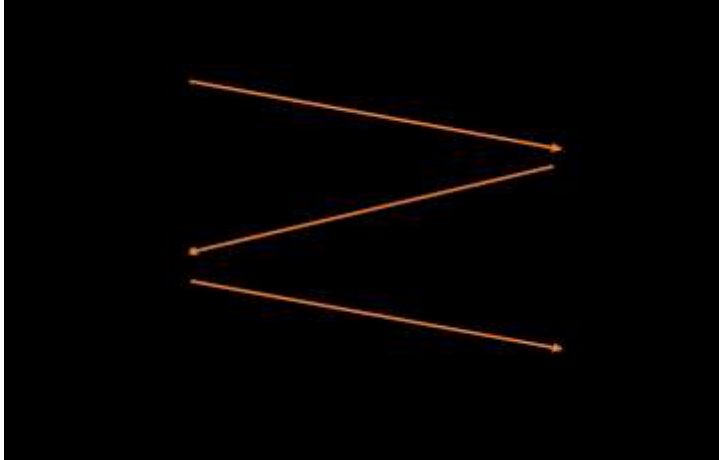
Step 1: client end system sends TCP SYN control segment to server

Step 2: server end system receives SYN, replies with SYN-ACK

- allocates buffers
- ACKs received SYN

Step 3: client receives SYN-ACK

- connection is now set up
- client starts the “real work”



Closing a connection:

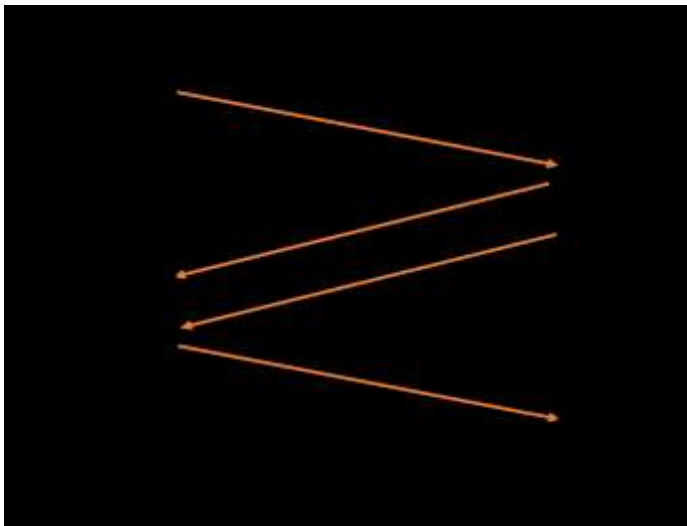
Step 1: client end system sends TCP FIN control segment to server

Step 2: server receives FIN, replies with ACK. Closes connection, sends FIN

Step 3: client receives FIN, replies with ACK.

- Enters “timed wait” - will respond with ACK to received FINs

Step 4: server, receives ACK. Connection closed.



UDP (User Datagram Protocol)

UDP protocol functions are:

- Multiplexing
- Error Detection

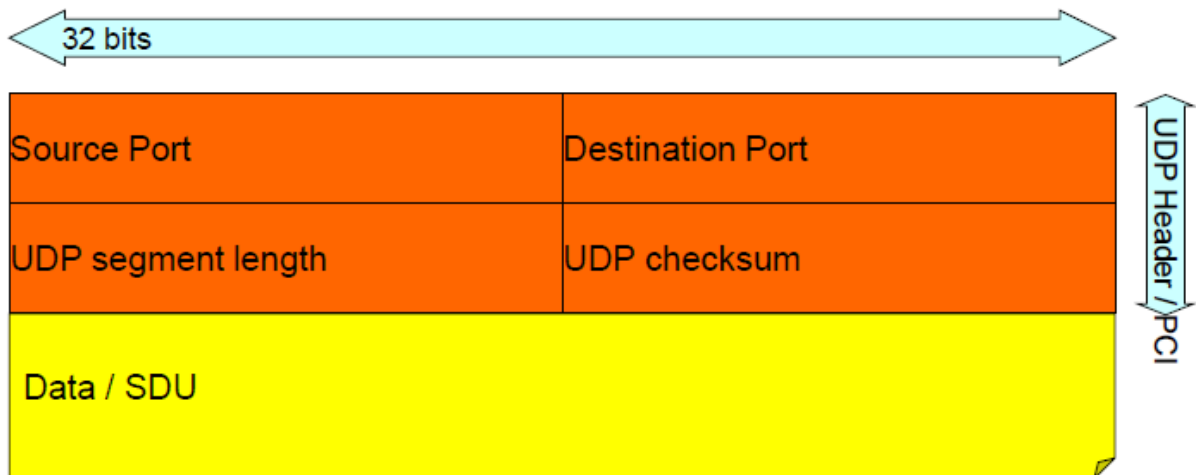
UDP Services:

- Is a connectionless service
- Is unreliable
- Has no in-sequence delivery guarantees

Well-known UDP ports

Protocols	UDP Ports
DNS	53
DHCP	67,68
SNMP	161,162

UDP Segment



Why would anyone use UDP?

- No delay for connection establishment
 - UDP just blasts away without any formal preliminaries
 - avoids introducing any unnecessary delays
- No connection state
 - No allocation of buffers, parameters, sequence numbers, etc.
 - easier to handle many active clients at once
- Small packet header overhead
 - UDP header is only eight-bytes long

Comparison of TCP and UDP

S.N	TCP	UDP
1	Stream Oriented	Datagram Oriented
2	Reliable, Connection-oriented	Unreliable, Connectionless
3	Complex	Simple
4	Only Unicast	Unicast and multicast
5	Uses Windows or Acks	No windows or Acks
6	Full Header	Small header, less overhead
7	Sequencing	No sequencing
8	Used for most internet applications	Useful for only few applications
9	Example: HTTP, FTP, SMTP	Example: DNS, SNMP

Socket

To the kernel, a socket is an endpoint of communication. To an application, a socket is a file descriptor that lets the application read/write from/to the network. All Unix I/O devices, including networks, are modeled as files. Sockets are UNIQUELY identified by Internet address, end-to-end protocol, and port number. Clients and servers communicate with each by reading from and writing to socket descriptors.

Socket programming with TCP

Client must contact server

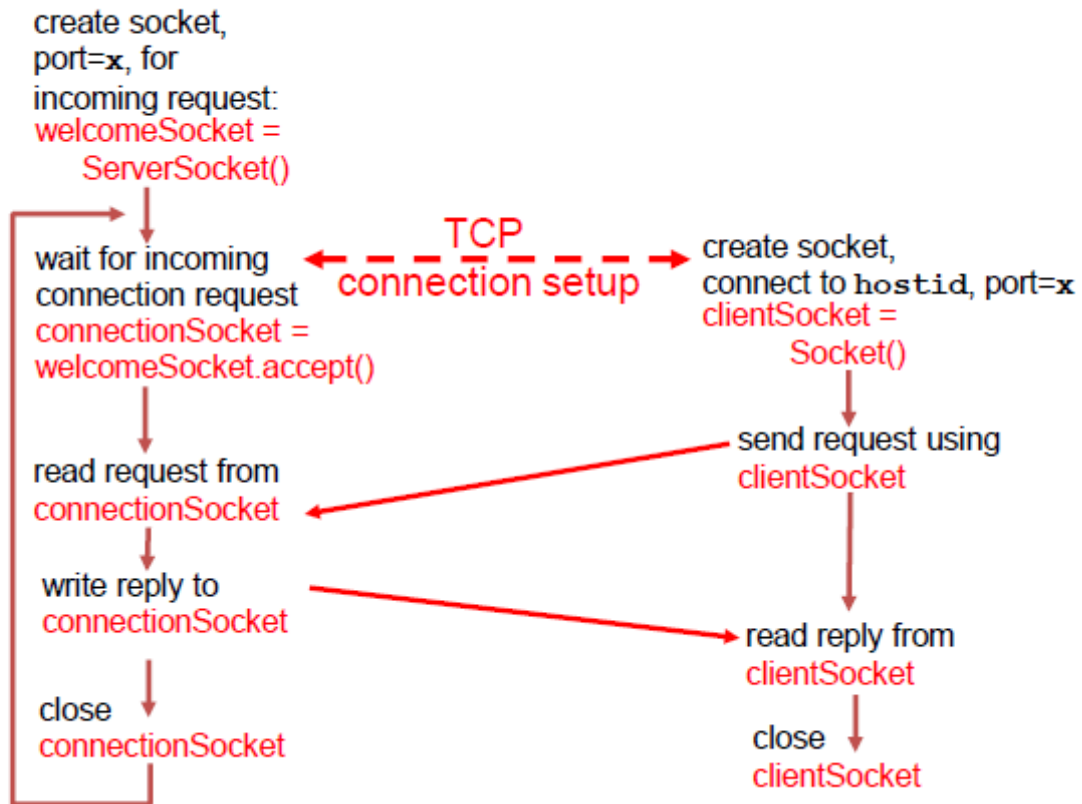
- server process must first be running
- server must have created socket (door) that welcomes client's contact

Client contacts server by:

- creating client-local TCP socket
- specifying IP address, port number of server process
- client establishes TCP connection to server

Server (running on `hostid`)

Client



Socket programming with UDP

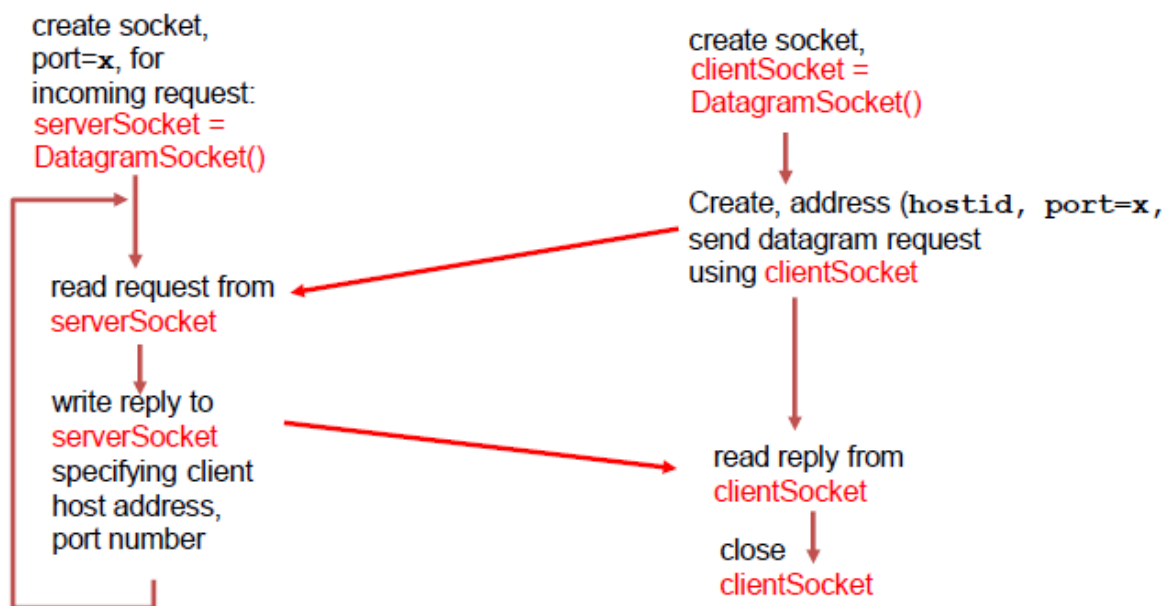
No "connection" between client and server

- no handshaking
- sender explicitly attaches IP address and port of destination to each packet
- server must extract IP address, port of sender from received packet to return uppercase sentence to sender

Transmitted data may be received out of order, or lost

Server (running on `hostid`)

Client



Chapter 7: Congestion Control and Quality of Services

Some of the Causes of Congestion

- Too many host in broadcast domain
- Low bandwidth
- Outdated hardware
- Bad configuration management
- Poor network design

Congestion Control

Open Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination

Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens.

Open Loop Congestion Control

Retransmission Policy

If a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion.

Window Policy

The Selective Repeat window is better than the Go-Back-N window for congestion control. In the Go-Back-N window, sends from last lost frame that may cause duplication and congestion. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only N packets at a time. Sending fewer acknowledgments means imposing less load on the network.

Discarding Policy

A good discarding policy by the routers may prevent congestion. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

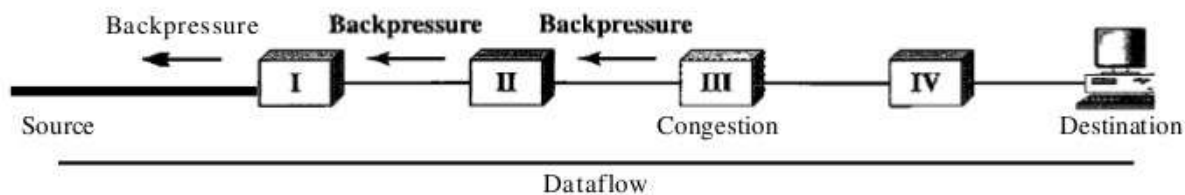
Admission Policy

Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual- circuit connection if there is congestion in the network or if there is a possibility of future congestion.

Closed-Loop Congestion Control

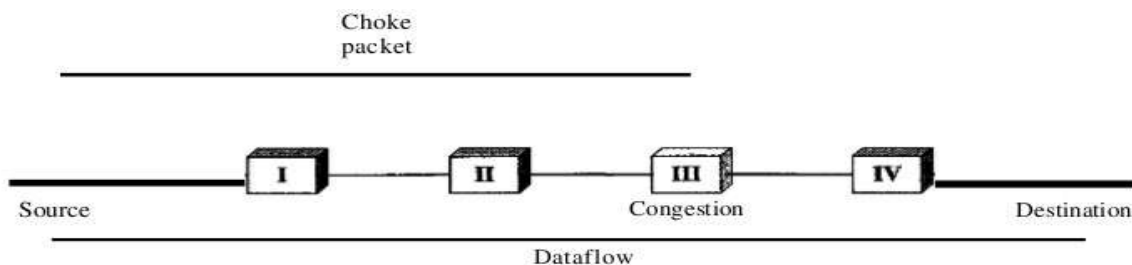
Back-pressure

The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes and so on.



Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion. Difference from backpressure - the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has traveled are not warned.



Implicit Signaling

In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is a congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down.

Explicit Signaling

In the choke packet method, a separate packet is used ; in the explicit signaling method, the signal is included in the packets that carry data.

Backward Signaling

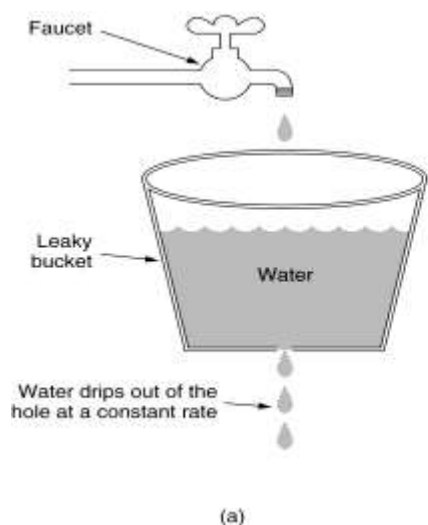
A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets.

Forward Signaling

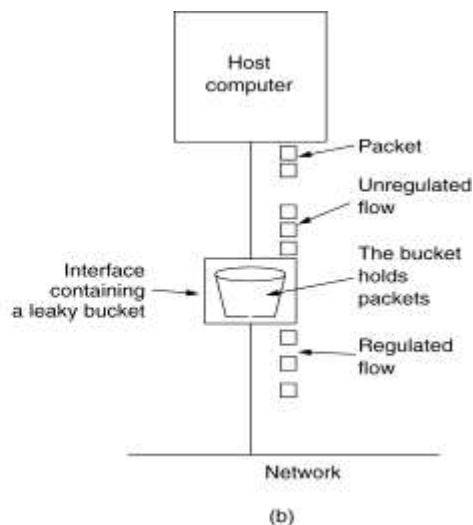
A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the congestion.

Traffic Shaping Algorithm

The Leaky Bucket Algorithm



(a) A leaky bucket with water

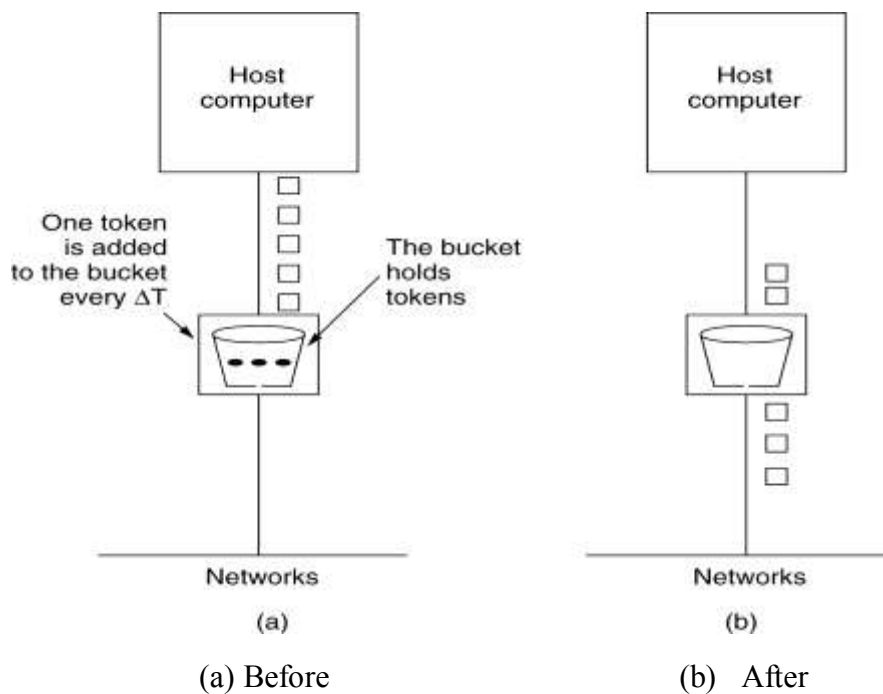


(b) a leaky bucket with packets.

Try to imagine a bucket with a small hole in the bottom, as illustrated in figure. No matter the rate at which water enters the bucket, the outflow is at a constant rate, R , when there is any water in the bucket and zero when the bucket is empty. Also, once the bucket is full to capacity, any additional water entering it spills over the sides and is lost. This bucket can be used to shape or police packets entering the network.

Conceptually, each host is connected to the network by an interface containing a leaky bucket. If a packet arrives when the bucket is full, the packet must either be queued until enough water leaks out to hold it or be discarded.

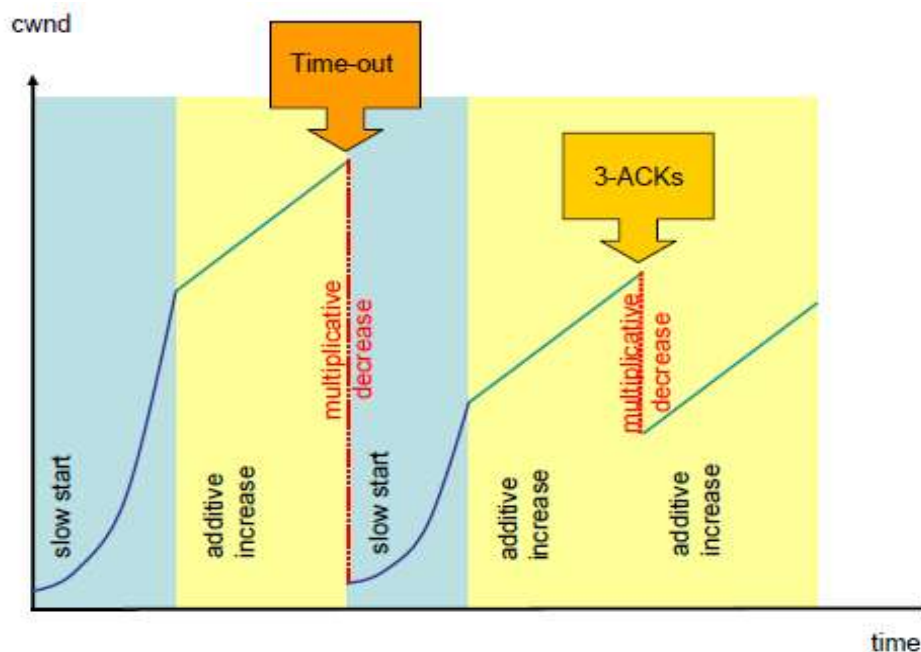
The Token Bucket Algorithm



A different but equivalent formulation is to imagine the network interface as a bucket that is being filled, as shown in figure. Now, to send a packet we must be able to take water, or tokens, as the contents are commonly called, out of the bucket (rather than putting water into the bucket). No more than a fixed number of tokens, can accumulate in the bucket. If the bucket is empty, we must wait until more tokens arrive before we can send another packet.

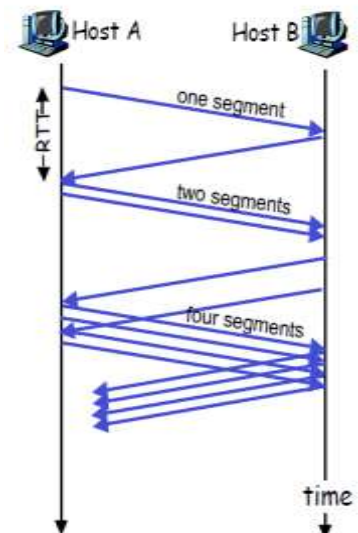
TCP congestion control: additive increase, multiplicative decrease (AIMD)

- Approach: increase transmission rate (window size), probing for usable bandwidth, until loss occurs.
 - additive increase: increase CongWin by 1 MSS every RTT until loss detected
 - multiplicative decrease: cut CongWin in half after loss
- It starts with slow start phase that exponentially increase CWND and continues to congestion avoidance threshold.
- When it reaches the congestion avoidance threshold then it additively increases CWND
- It follows multiplicative decreasing rate upon congestion detection.



TCP congestion control: TCP Slow Start

- A sender starts transmission with a slow rate
- Increases the rate as long as its rate is below a threshold.
- When the threshold is reached, the rate is decreased to avoid congestion.
- When connection begins, increase rate exponentially until first loss event:
 - double CongWin every RTT
 - done by incrementing CongWin **for** every ACK received



Chapter 8: Application layer Services and Protocols

Application layer provides end user services using various protocols.

Need of Application layer design

- Think of different people/teams, working on the client and server programs.
 - Different programming languages.
 - Diverse hardware, operating systems.
- Allow for future extensions
 - Leave room for additional data, meta-data

Functions of Application Layer

- File Transfer: It allows user to access, retrieve and manage files
- Mail Services: Basis for email forwarding and storage
- Directory Services: Distributed database for global information about various objects and services

DNS (Domain Name System)

DNS is usually used to translate a host name into an IP address. It automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. Domain names comprise a hierarchy so that names are unique, yet easy to remember. DNS implements a distributed database to store this name and address information for all public hosts on the Internet. Most network operating systems support configuration of primary, secondary, and tertiary DNS servers, each of which can service initial requests from clients.

Example :

- Name used by human – www.example.com
- translated to the addresses 93.184.216.119 ([IPv4](#))

Host name structure

- Each host name is made up of a sequence of *labels* separated by periods.
 - Each label can be up to 63 characters
 - The total name can be at most 255 characters.

Examples:

- whitehouse.gov
- Wikipedia.org
- Iamtheproudownerofthelongestlongestlongestdomainnameinthisworld.com

DNS Query Types

Recursive Query

A DNS client provides a hostname and DNS resolver must provide either a relevant resource or an error message if it can't be found

Iterative Query

A DNS client provides a hostname and DNS resolver returns the best answer. If DNS resolver has the relevant resource in cache, it returns them. If not refers to the root server or another Authoritative Name Server

Non-Recursive Query

In this case DNS resolver already knows the answer. It either directly returns the DNS record from cache or queries a DNS Name server which is authoritative for the record.

How DNS Works

When a user tries to access a web address like "example.com", their web browser performs a DNS query. The DNS server takes the hostname and resolve it into numeric IP address. The DNS resolver is responsible for checking if the hostname is available in local cache. If not contacts a series of DNS Name Servers, until it receives the IP of the service

Root name servers

It is contacted by local name server that can not resolve name. Root name server contacts authoritative name server if name mapping not known, gets mapping and returns mapping to local name server

TLD and Authoritative Servers

Top-level domain (TLD) servers:

Generic top level domains: responsible for .com, .org, .net, .edu, .gov, etc

Countries have a 2 letter top level domain: Example., uk, fr, np, ca, jp

Authoritative DNS servers

It is organization's DNS servers, providing authoritative hostname to IP mappings for organization's servers (e.g., Web and mail). It can be maintained by organization or service provider

Local Name Server

It does not strictly belong to hierarchy. Each ISP (residential ISP, company, university) has one. It is also called "default name server". When a host makes a DNS query, query is sent to its local DNS server. It acts as a proxy, forwards query into hierarchy.

HTTP and HTTPS

HTTP stands for Hyper Text Transfer Protocol . HTTP is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web (ie. internet) since 1990 . It allows the transmitting and receiving of information across the Internet

The S stands for "Secure" in HTTPS i.e., Secure hypertext transfer protocol. HTTPS is http using a Secure Socket Layer (SSL). Secure HTTP (HTTPS) is one of the popular protocols to transfer sensitive data over the Internet. A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS. Most implementations of the HTTPS protocol involve online purchasing or the exchange of private information. HTTPS is only slightly slower than HTTP

HTTP Connection

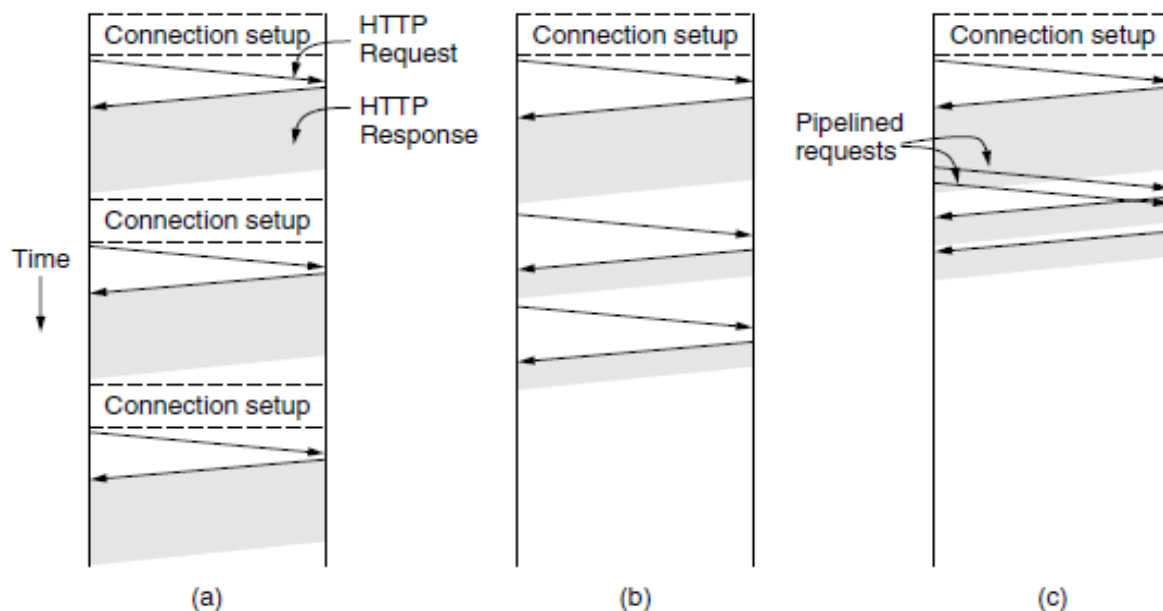


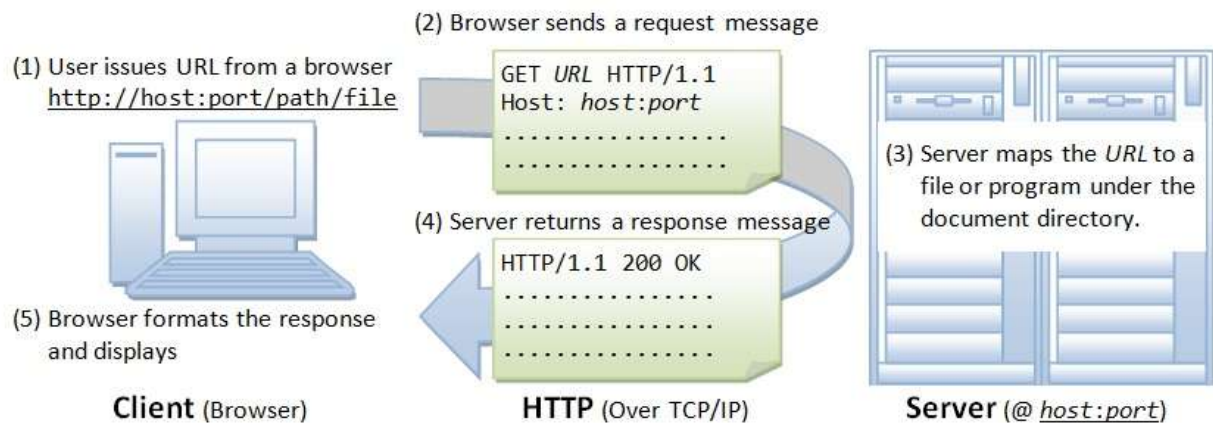
Figure: (a) multiple connections and sequential requests. (b) A persistent connection and sequential requests (c) A persistent connection and pipelined requests.

Figure (a) shows non-persistent connections. Browser makes connection and request for each object. Server parses request, responds and closes connection. It has performance problem.

Figure (b) shows persistent connections. On same TCP connection server parses request, responds, parses new request upon responds and so on . It improves performance.

Figure (c) shows pipelining with persistent connections. It send next request before previous response is received. Pipelining with persistent connection improves performance

HTTP Example



FTP (File Transfer Protocol)

It allows a user to copy files to/from remote hosts. FTP uses the services of TCP. It needs two TCP connections. The well-known port 21 is used for the control connection and the well-known port 20 for the data connection

Goal of FTP (Objective of FTP)

- promote sharing of files
- encourage indirect use of remote computers
- shield user from variations in file storage
- transfer data reliably and efficiently

Working of FTP

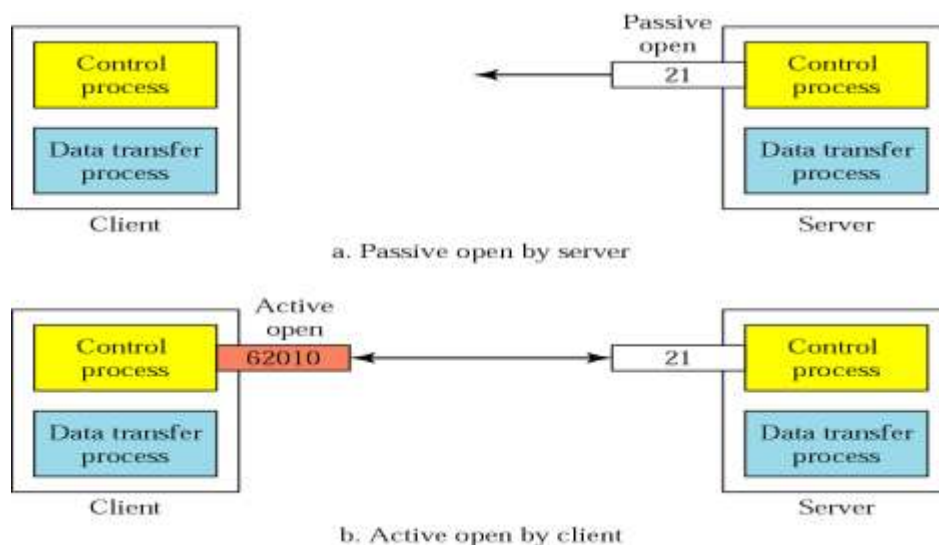


Figure: FTP Connections- control connection

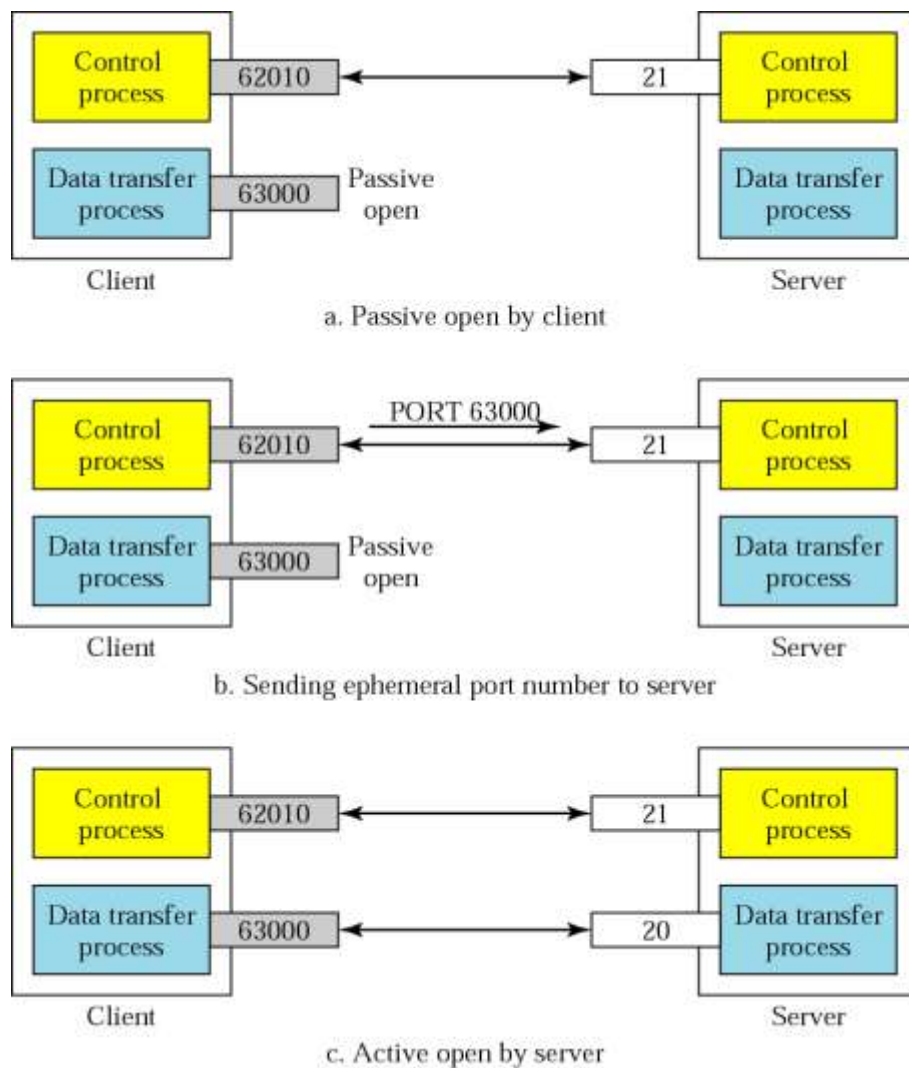
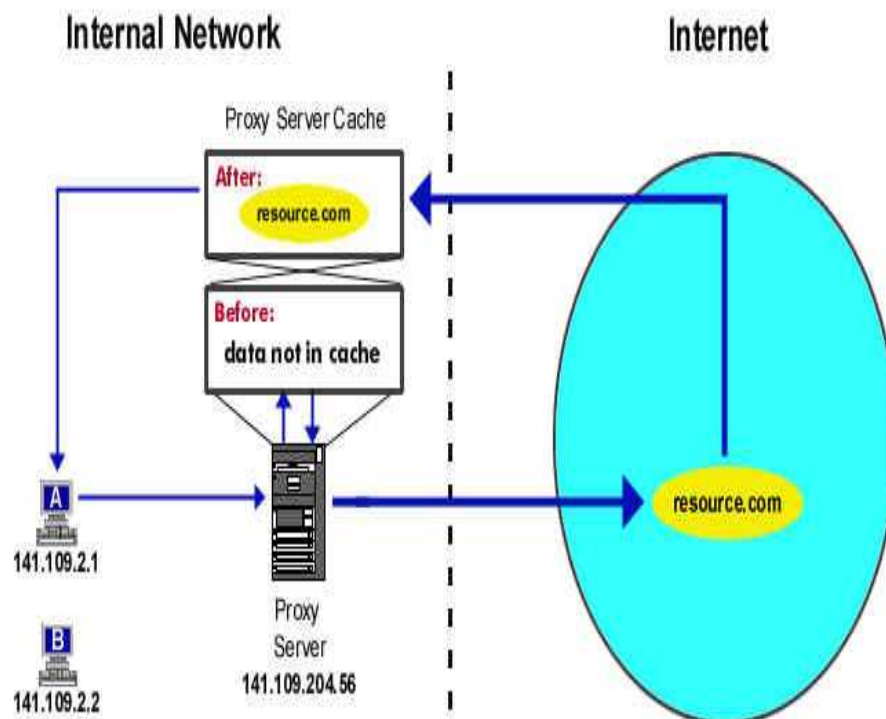


Figure: FTP connection- data connection

- Uses Server's well-known port 20
- Client issues a passive open on an ephemeral port, say x .
- Client uses PORT command to tell the server about the port number x .
- Server issues an active open from port 20 to port x .
- Server creates a child server/ephemeral port number to serve the client

Proxy Server

Proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. Proxy server stores all the data it receives as a result of placing requests for information on the internet in its *cache*. Cache simply means memory. The cache is typically hard disk space, but it could be RAM. Caching documents means keeping a copy of internet documents so the server doesn't need to request them over again. With proxy caching, clients make requests to servers, but the requests first go through a proxy cache.

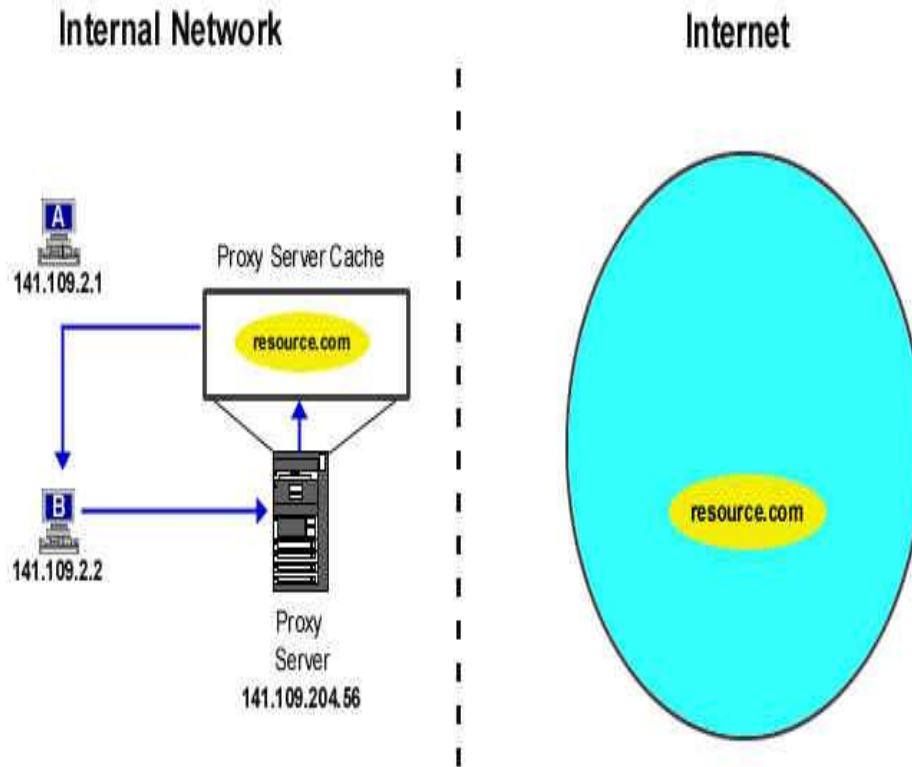


Scenario 1: Caching a Document on a Proxy Server

User **A** request a web page. The request goes to the proxy server, the proxy server checks to see if the document is stored in cache. If the document is not in cache so the request is sent to the Internet. The proxy server receives the request, stores (or caches) the page. The page is sent to user **A** where is viewed.

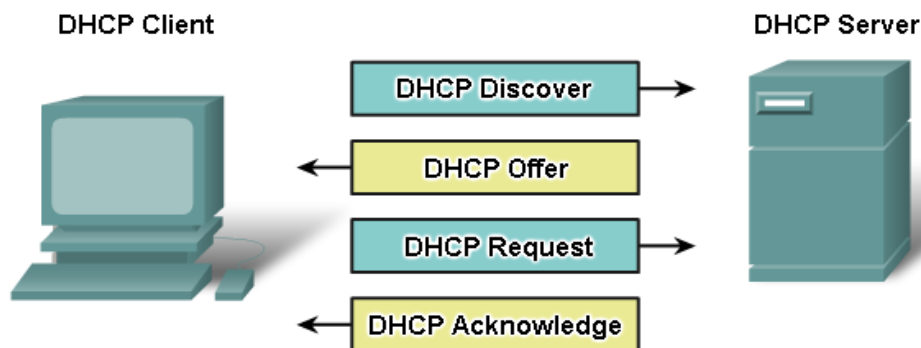
Scenario 2: Retrieving Cached Documents

User **B** request the same page as user **A** (ie. resource.com). The request goes to the proxy server. The proxy server checks its cache for the page. Since the page is stored in cache, the proxy server sends the page to user **B** where it is viewed. Connection to the Internet is required



DHCP (Dynamic Host Configuration Protocol)

When a DHCP-configured device boots up or connects to the network, the client broadcasts a DHCP DISCOVER packet to identify any available DHCP servers on the network. A DHCP server replies with a DHCP OFFER, which is a lease offer message with an assigned IP address, subnet mask, DNS server ... etc. The client might choose from multiple DHCP OFFERs it receives and broadcast a DHCP REQUEST. If the DHCP OFFER is still available the DHCP server will reply with DHCP ACKNOWLEDGE. If the DHCP OFFER is not available the server will reply with DHCP NAK the process will start all over again



Electronic Mail

It is one of the most widely used and popular internet applications. User can communicate with each other across the network. Every user owns his own mailbox which he uses to send, receive and store messages from other users. Every user can be uniquely identified by his unique email address. Mailbox principle-A sender does not require the receiver to be online nor the recipients to be present. A user's mailbox can be maintained anywhere in the internet on the server.

Three major components: user agents, mail servers and Simple Mail Transfer Protocol (SMTP)

User Agent: “mail reader”

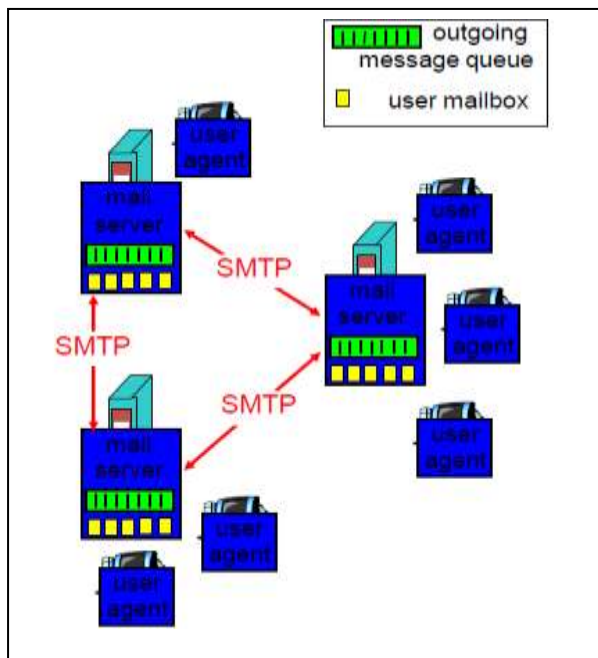
It consist of composing, editing, reading mail messages. e.g., Eudora, Outlook, elm, Netscape Messenger. All the outgoing, incoming messages are stored on server

Mail Servers

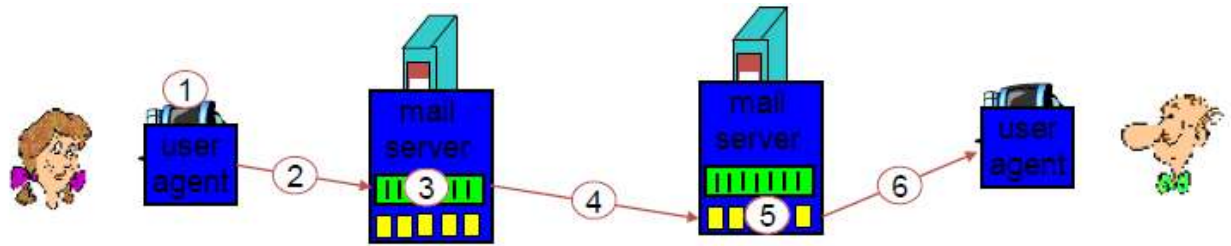
Mailbox contains incoming messages for user. The message queue of outgoing (to be sent) mail messages

SMTP

It is protocol between mail servers to send email messages; client: sending mail server and “server”: receiving mail server. It uses TCP to reliably transfer email message from client to server. It uses port 25. There are three phases of transfer: handshaking (greeting), transfer of messages and closure.



Example



Alice uses UA to compose message and send “to” bob@some school.edu . Alice’s UA sends message to her mail server. The message is placed in message queue. Client side of SMTP opens TCP connection with Bob’s mail server. SMTP client sends Alice’s message over the TCP connection. Bob’s mail server places the message in Bob’s mailbox. Bob invokes his user agent to read message.

POP (Post Office Protocol)

It is a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an *e-mail client*) use the POP protocol. Examples of native mail system are MS outlook, Lotus Notes, MS Exchange, Eudora. There are two versions of POP: The first, called *POP2*, became a standard in the mid-80's and requires SMTP to send messages. The newer version, *POP3*, can be used with or without SMTP. POP3 uses TCP/IP port 110.

IMAP (Internet Message Access Protocol)

It is a method of accessing electronic mail messages that are kept on a possibly shared mail server. In other words, it permits a "client" email program to access remote message stores as if they were local. For example, email stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office and a notebook computer while travelling. IMAP uses TCP/IP port 143.

POP vs IMAP

Feature	POP3	IMAP
Where is protocol defined?	RFC 1939	RFC 2060
Which TCP port is used?	110	143
Where is e-mail stored?	User's PC	Server
Where is e-mail read?	Off-line	On-line
Connect time required?	Little	Much
Use of server resources?	Minimal	Extensive
Multiple mailboxes?	No	Yes
Who backs up mailboxes?	User	ISP
Good for mobile users?	No	Yes
User control over downloading?	Little	Great
Partial message downloads?	No	Yes
Are disk quotas a problem?	No	Could be in time
Simple to implement?	Yes	No
Widespread support?	Yes	Growing

Chapter 9: Network Management and Security

What is Network Management?

"Network management includes the deployment, integration and coordination of the hardware, software, and human elements to monitor, test, poll, configure, analyze, evaluate, and control the network and element resources to meet the real-time, operational performance, and Quality of Service requirements at a reasonable cost."

ISO Network Management Areas

The International Standards Organization (ISO) has defined a network management model and framework referred to as FCAPS (fault, configuration, accounting, performance, security).

- **Fault Management** : monitoring and management of faults that occur in a network
- **Configuration Management** : management of network device configurations and changes
- **Accounting Management** : billing management
- **Performance Management** : monitoring and management of the efficiency or utilization of the network
- **Security Management** : controlling access to the network and network devices

SNMP (Simple Network Management Protocol)

It is an application layer protocol used to monitor network-attached devices. It is part of the TCP/IP protocol suite. It allows Administrators to manage network performance, find and solve network problems, and plan for network growth. SNMP works as the manager/agent model: Manager (the monitoring "client") and Agent (running on the equipment server). The manager and agent use a Management Information Base (MIB) and a relatively small set of commands to exchange information. MIBs are files defining the objects that can be queried, including: Object name, Object description and Data type (integer, text, list). The MIB is organized in a tree structure with individual variables, represented as leaves on the branches. A long numeric tag or object identifier (OID) is used to distinguish each variable uniquely in the MIB and in SNMP messages.

How does it work?

Basic commands

GET (manager -> agent) - Query for a value

GET-NEXT (manager -> agent) - Get next value (list of values for a table)

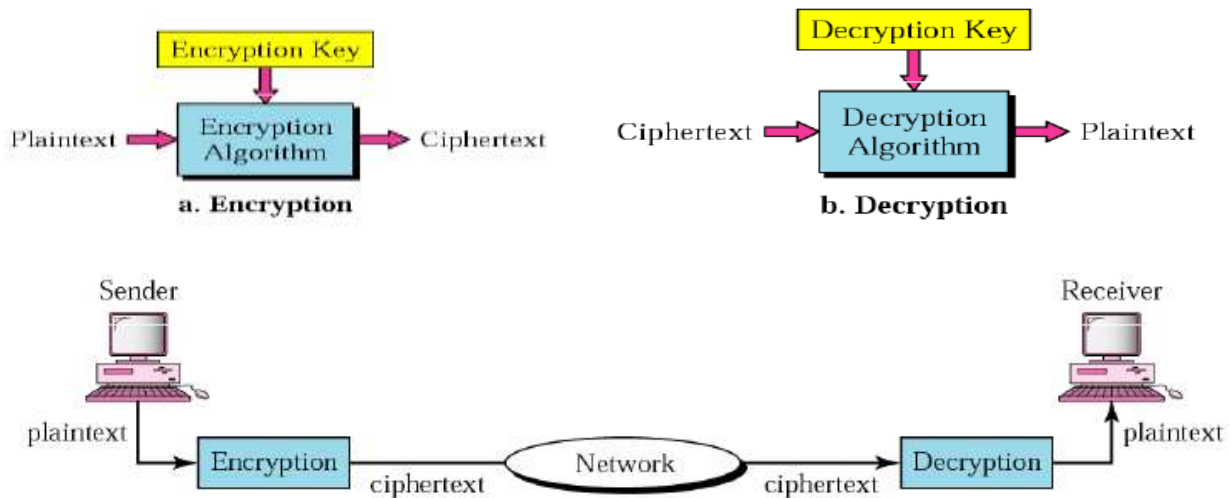
GET-RESPONSE (agent -> manager) - Response to GET/SET, or error

SET (manager -> agent) - Set a value, or perform action

TRAP (agent -> manager) - Spontaneous notification from equipment (line down, temperature above threshold, ...)

Cryptography

Cryptography in Greek means “Secret Writing”. It is science and art of transforming message to make them secure and immune to attack. Original message before transformation is Plaintext. An Encryption algorithm transforms Plaintext to Cipher-text. Decryption algorithm transforms Cipher-text to Plaintext. Cipher refers to different categories of algorithm in Cryptography.

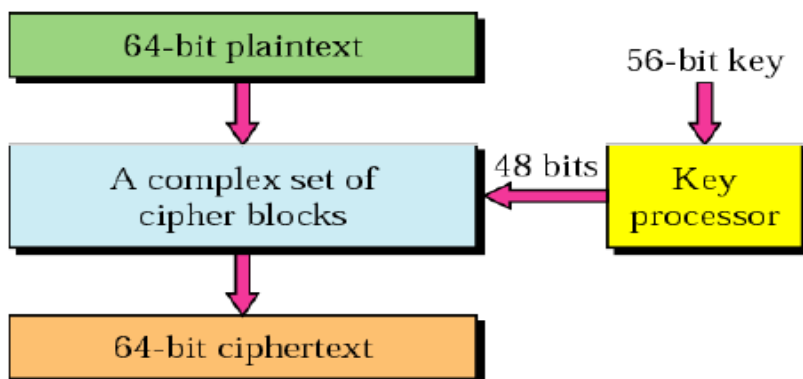


Symmetric key cryptography: sender, receiver keys *identical*

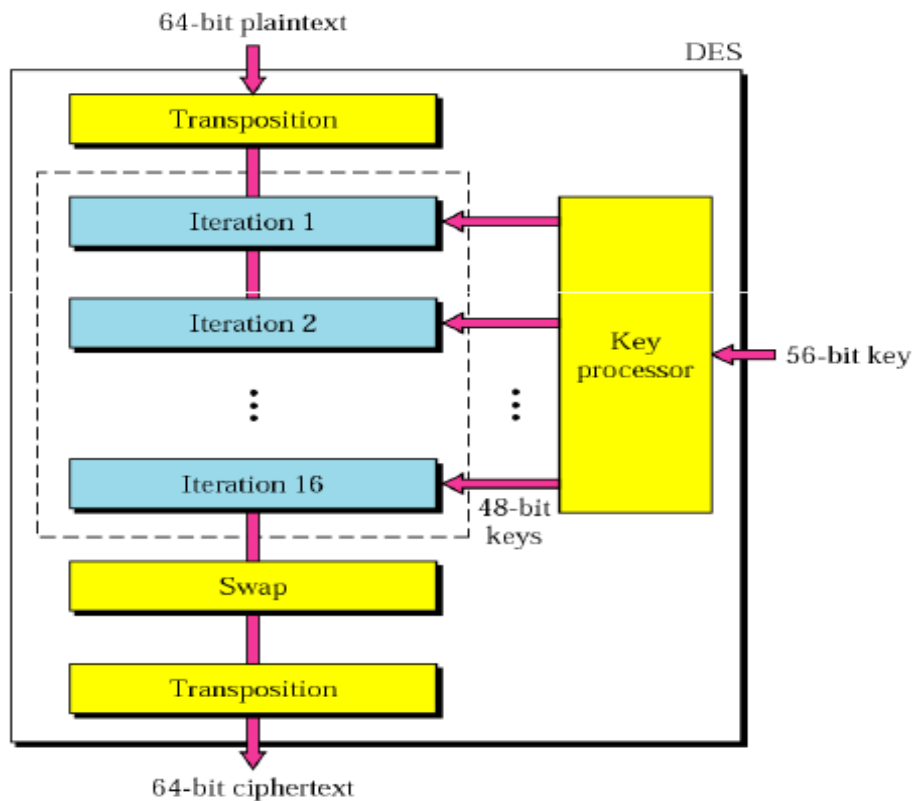
Public-key cryptography: encryption key *public*, decryption key *secret* (private)

Symmetric key cryptography: DES (Data Encryption Standard)

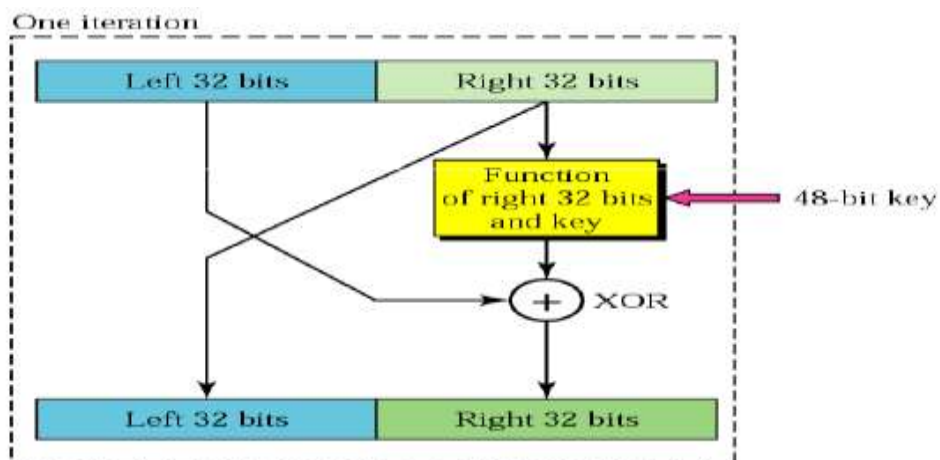
The cryptographic algorithm specified in this standard transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used



DES General Scheme



DES iteration block



During Encryption

$$L_n = R_{n-1}$$

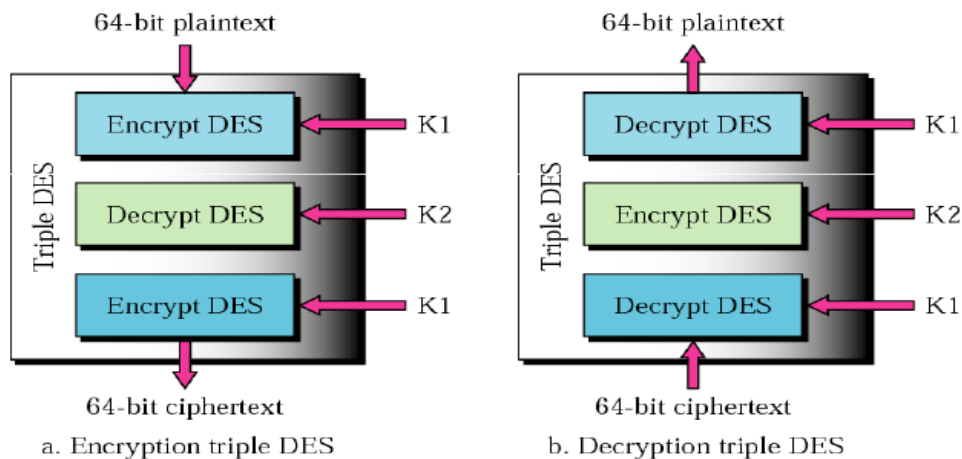
$$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

During Decryption

$$R_{n-1} = L_n$$

$$L_{n-1} = R_n \oplus f(L_n, K_n)$$

Triple DES



Public Key Cryptography: RSA

It was invented by Ron Rivest, Adi Shamir and Leonard Adleman . It supports Encryption and Digital Signatures. It is most widely used Public Key Algorithm. It gets its security from integer factorization problem. It is relatively easy to understand and implement. RSA is used in Security Protocols such as- IPSEC/IKE => IP Data Security, SSH => Terminal Connection Security, TLS/SSL => Transport Data Security

RSA Algorithm : Key Generation

1. Generate Two Large Prime Numbers, p and q
2. Let $n = pq$
3. Let $m = (p-1)(q-1)$
4. Choose a small number e ($1 < e < m$), co prime to m such that $GCD(e, m) = 1$.
5. Find d , such that $de \% m = 1$. Where $d = (1 + m * i)/e$
6. Publish e and n as the Public Key
7. Keep d and n as the Private Key

RSA example

Key Generation: Steps

1. Generate Two Large Prime Numbers, p and q
 $Let\ p = 7\ and\ q = 19$
2. Let $n = pq$
 $n = 7 * 19$
 $n = 133$

3. Let $m = (p-1)(q-1)$
 $m = (7-1)(19-1)$
 $m = 6 * 18$
 $m = 108$
4. Choose a small number e ($1 < e < m$), co prime to m such that $GCD(e, m) = 1$
 $e = 2 \Rightarrow GCD(e, 108) = 2$ (no)
 $e = 3 \Rightarrow GCD(e, 108) = 3$ (no)
 $e = 4 \Rightarrow GCD(e, 108) = 4$ (no)
 $e = 5 \Rightarrow GCD(e, 108) = 1$ (yes!) $\Rightarrow GCD(e, m) = 1$
5. Find d , such that $de \% m = 1$. Where $d = (1 + m * i)/e$
 [Go through Values of i until Integer Solution is Found]
 $i = 0 \Rightarrow d = 1 / 5$ (No Integer)
 $i = 1 \Rightarrow d = 109 / 5$ (No Integer)
 $i = 2 \Rightarrow d = 217 / 5$ (No Integer)
 $i = 3 \Rightarrow d = 325 / 5 = 65$ (Yes !! Satisfies the Condition)
6. $(n, e) = (133, 5)$ AND $(n, d) = (133, 65)$

RSA: Encryption, decryption

Given (n, e) and (n, d) as computed above

To encrypt bit pattern m , compute

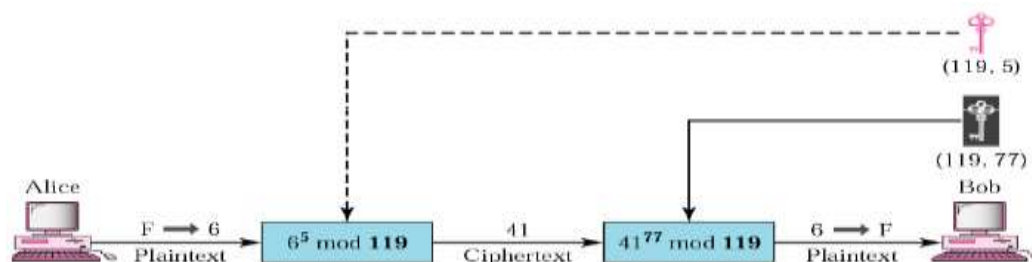
$$c = m^e \bmod n \quad (\text{i.e., remainder when } m^e \text{ is divided by } n)$$

To decrypt received bit pattern, c , compute

$$m = c^d \bmod n \quad (\text{i.e., remainder when } c^d \text{ is divided by } n)$$

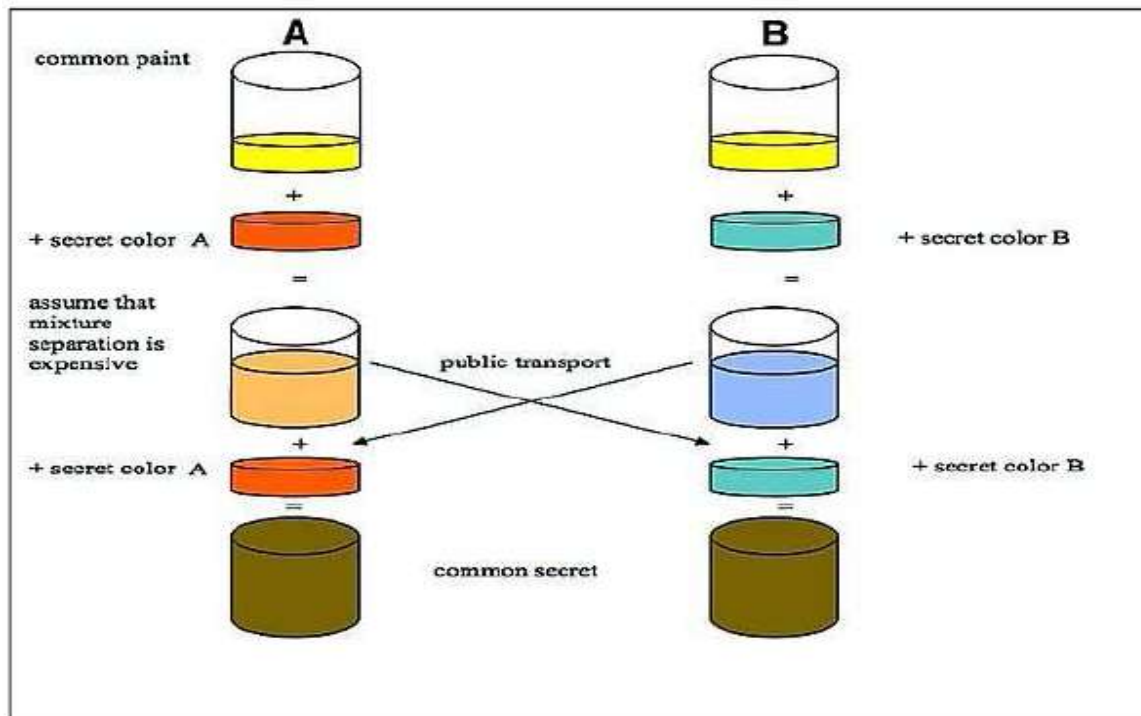
RSA : Encryption, Decryption Example

- Public Key Pair $\Rightarrow (n, e) \Rightarrow (119, 5)$
- Private Key Pair $\Rightarrow (n, d) \Rightarrow (119, 77)$



Key Exchange Protocol: Diffie Hellman Algorithm

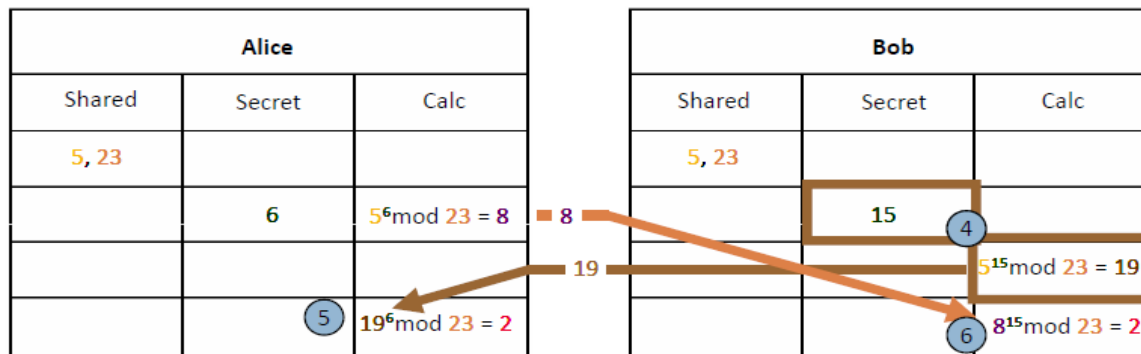
Analogy



Diffie Hellman Algorithm : Step by Step Illustration

Alice			Bob		
Shared	Secret	Calc	Shared	Secret	Calc
1 5, 23			1 5, 23		
	2 6	3 $5^6 \text{ mod } 23 = 8$			

1. Alice and Bob agree to use the same two numbers.
For example, the Base Number $g=5$ and Prime Number $P=23$
2. Alice now chooses a Secret Number $x=6$.
3. Alice performs the DH algorithm: $g^x \text{ MOD } P = (5^6 \text{ modulo } 23) = 8$ (Y)
and sends the New number 8 (Y) to Bob



4. Meanwhile Bob has also chosen a Secret Number $x=15$, performed the DH algorithm: $g^x \text{ modulo } P = (5^{15} \text{ MOD } 23) = 19$ (Y) and sent the new number 19(Y) to Alice.

5. Alice now computes $Y^x \text{ modulo } P = (19^6 \text{ MOD } 23) = 2$.

6. Bob now computes $Y^x \text{ modulo } P = (8^{15} \text{ MOD } 23) = 2$.

The Result (2) is the same for both Alice and Bob. This number can now be used as a shared secret key by the encryption algorithm.

Kerberos

In Greek Mythology, *Kerberos* (or *Cerberus*) is the Horrible three-headed guard dog of Hades.

Hades was the Ancient Greek god of the Underworld. The Underworld is a region that is thought to be under the surface of the Earth.

Kerberos is an authentication service developed as part of Project Athena. It is one of the best known and most widely implemented **Trusted Third Party** key Distribution Systems.

Designed to Provide Strong Authentication for Client/Server Applications by using Secret-Key Cryptography. It uses **Strong Cryptography** so that a Client can Prove its Identity to a Server (and vice versa) across an Insecure Network Connection. Two Versions of Kerberos are in Common Use: v4 & v5.

IPSec

IPSec is a framework of open standard for ensuring private communication over public network. It has become the most common network layer security control, typically used to create a VPN. A VPN is a virtual network built on top of existing physical networks that can provide a secure communications for data transfer. VPNs are used most often to protect communications carried over public networks such as the Internet. A VPN can provide several types of data protection: confidentiality, integrity, data origin authentication, replay protection and access control.

IPSec Components :

Two security protocols -Authentication Header (AH) and Encapsulating Security Payload (ESP). AH can provide integrity protection for packet headers and data, but it cannot encrypt them. ESP can provide encryption and integrity protection for packets, but it cannot protect the outermost IP header, as AH can. However, this protection is not needed in most cases. Accordingly, ESP is used much more frequently than AH because of its encryption capabilities.

Internet Key Exchange (IKE) protocol:

IPsec uses IKE to negotiate IPsec connection settings. It authenticates endpoints to each other. It defines the security parameters of IPsec-protected connections. It negotiates secret keys and manages, updates, and deletes IPsec-protected communication channels.

IP Payload Compression Protocol (IPComp):

Optionally, IPsec can use IPComp to compress packet payloads before encrypting them.

IPSec Mode

Transport mode

IPSec header is inserted just after the IP header. The Protocol field in the IP header is changed to indicate that an IPSec header follows the normal IP header (before the TCP header). The IPSec header contains security information

Tunnel mode

AH or ESP fields are added to the IP packets, the entire packet. Tunnel mode is used when both ends or one end uses a firewall or router that implements IPSec. The unprotected packets can pass through external networks. Tunnel mode is also useful when the tunnel ends at a location other than the final destination. The disadvantage of tunnel mode is that it adds an extra IP header, thus increasing packet size substantially. In contrast, transport mode does not affect packet size.

Benefits of IPSec

- It provides strong security
- IPSec in a firewall is resistant to bypass if all traffic from outside sees IP
- IPSec is below transport layer and is transparent to applications
- IPSec can be transparent to end users
- IPSec can provide security to individual users if needed

Applications of IPSec

- Secure branch office connectivity over the internet
- Secure remote access over the internet
- Establishing extranet and intranet connectivity with partners

VPN (Virtual Private Network)

A VPN is a virtual network built on top of existing physical networks. It provides a secure communications mechanism for data and IP information transmitted between networks. VPN can be used over existing networks, such as the Internet. Thus, it can facilitate the secure transfer of sensitive data across public networks. This is often less expensive than alternatives such as dedicated private telecommunications lines between organizations or branch offices. Firewalls, VPNs, and IPsec with ESP in tunnel mode are a natural combination and widely used in practice. VPNs can use both symmetric and asymmetric forms of cryptography.

Three primary models for VPN architectures :

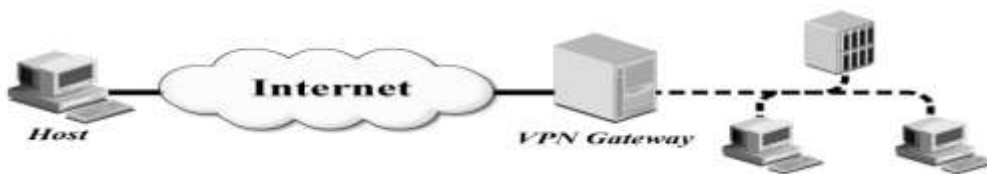
Gateway-to-gateway:

- Protects communications between two specific networks
- Eg., an organization's main office network and a branch office network, or two business partners networks.



Host-to-gateway:

- Protects communications between one or more individual hosts and a specific network belonging to an organization.
- Eg., traveling employees to gain access to internal organizational services, such as the organization's e-mail and Web servers.



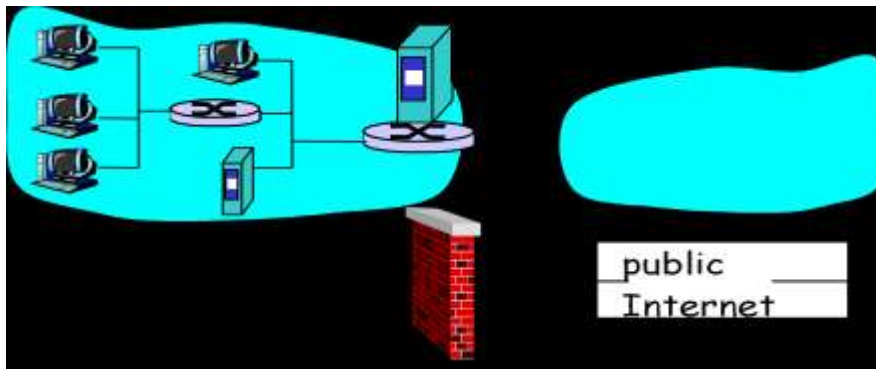
Host-to-Host :

- Protects communication between two specific computers.
- Eg., small number of users need to use or administer a remote system



Firewall

It Isolates organization's internal network from larger Internet, allowing some packets to pass, blocking others. It acts as a security gateway between two networks. A Firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks. The use of single choke point simplifies security management because security capabilities are consolidate on a single system. Windows Firewall helps protecting your computer by preventing unauthorized users from gaining access to your computer through a network or internet.



Firewalls: Why

- It prevents denial of service attacks: SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections.
- It prevents illegal modification/access of internal data. e.g., attacker replaces CIA's homepage with something else
- It allow only authorized access to inside network (set of authenticated users/hosts)
- It preserves customer and partner confidence: prevent viruses and worms on your network and prevent malicious attackers from getting into your network

Firewall : Types of Firewall

1. Packet Filtering Router

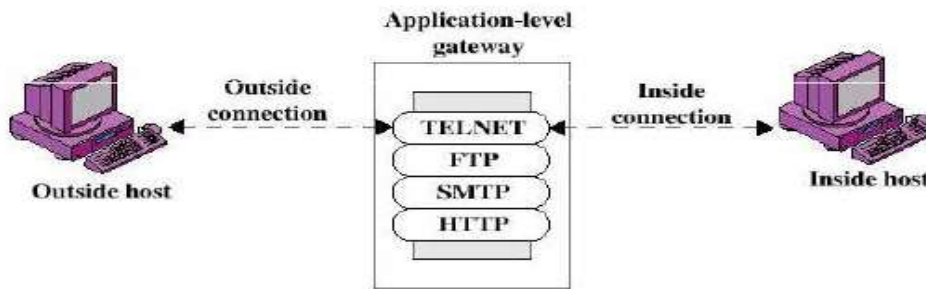
It applies a set of rules to each incoming IP Packet. The router is configured to filter packets going in both directions. Router filters packet-by-packet, decision to forward/drop packet based on: source IP address, destination IP address, TCP/UDP source and destination port numbers, ICMP message type, TCP SYN and ACK bits

Example : block incoming and outgoing datagram with IP protocol field = 17 and with either source or dest port = 23.

All incoming and outgoing UDP flows and telnet connections are blocked.

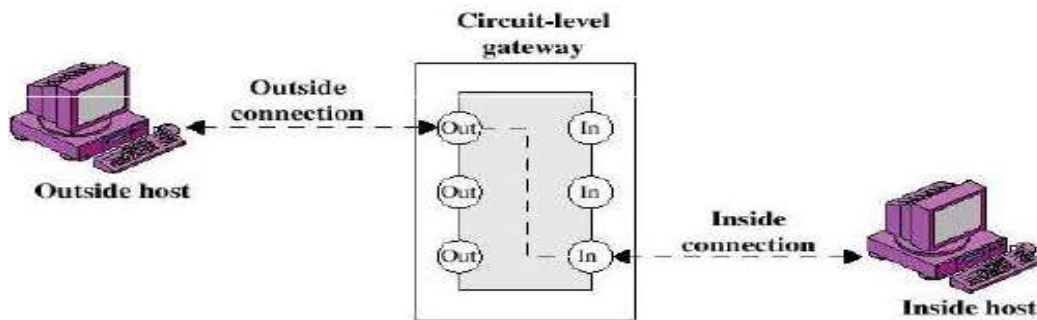
2. Application Level Gateway

They are called Proxy Servers and acts as a relay of application level traffic. Example: allow selected internal users to telnet outside. Require all telnet users to telnet through gateway. For authorized users, gateway sets up telnet connection to destination host. Gateway relays data between 2 connections. Router filter blocks all telnet connections not originating from gateway.



3. Circuit Level Gateway

It does not permit an end to end TCP Connection directly. The gateway setups two TCP Connections (IN and OUT). It monitor TCP handshaking between packets to determine whether a requested session is legitimate. Once two connections are established => Gateway Relays



Limitations of firewalls and gateways

- IP spoofing: router can't know if data "really" comes from claimed source
- The firewall cannot protect against attacks that bypass the firewall.
 - Internal systems may have dial-out capability to connect to an ISP.
- The firewall does not protect against internal threats, such as a dishonest employee or an employee who unwittingly cooperates with an external attacker.
- The firewall cannot protect against the transfer of virus-infected programs or files.