Network Technologies

by,

Prof. Viral S Patel
viral_s_patel@yahoo.co.in
(8866676410)

What is data Communications ?

Data Communication are the exchange of data between two devices via some form of transmission medium such as a wire cable.

What is network ?

A network is a set of devices (often referred to as ***nodes***) connected by communication links. A node can be a computer, printer or any other device. Most networks use **distributed processing**, in which a task is divided among multiple computers.

Communication/data flow between two devices can be :

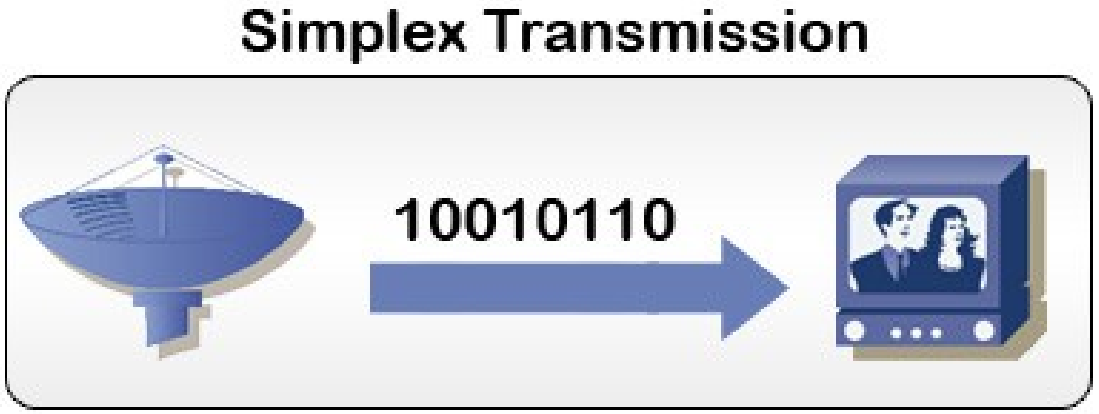
- Simplex Mode
- Half duplex Mode
- Full duplex Mode

Simplex Mode :

- Communication is Unidirectional.
- ➔ One device for transmit (send) and other for receive.
- ➔ **Example** : loudspeaker, television broadcasting, keyboard and monitor.

Simplex communication

Example : Television broadcasting

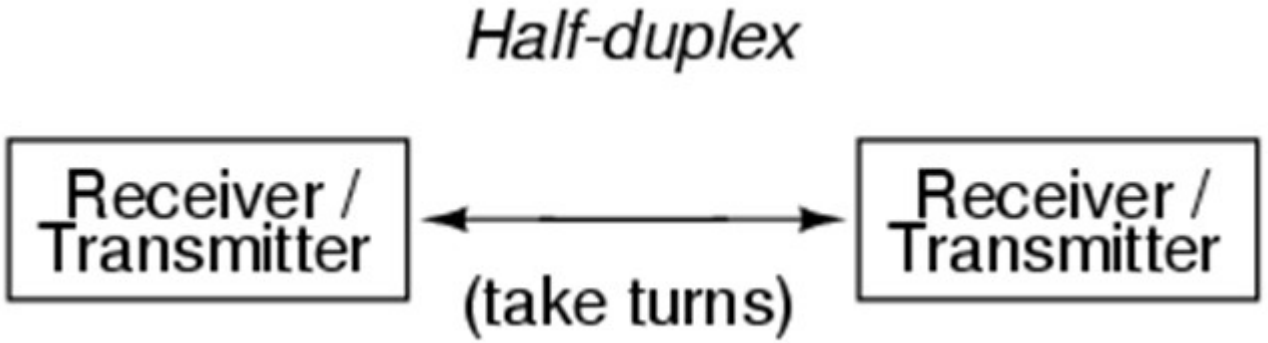


Half-Duplex Mode :

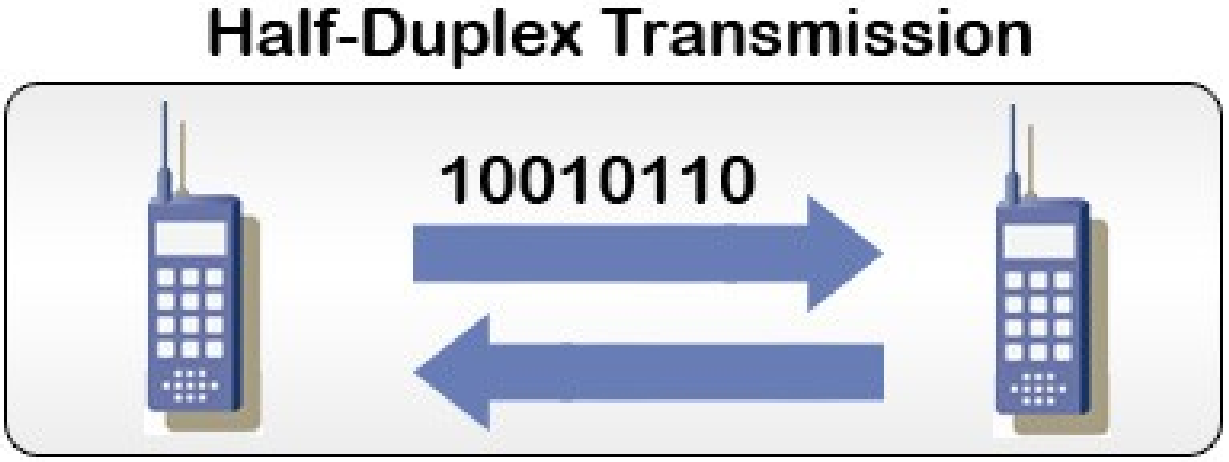
- Communication in both directions but **not at the same time.**

➔ When one device is sending and other can only receive,

an



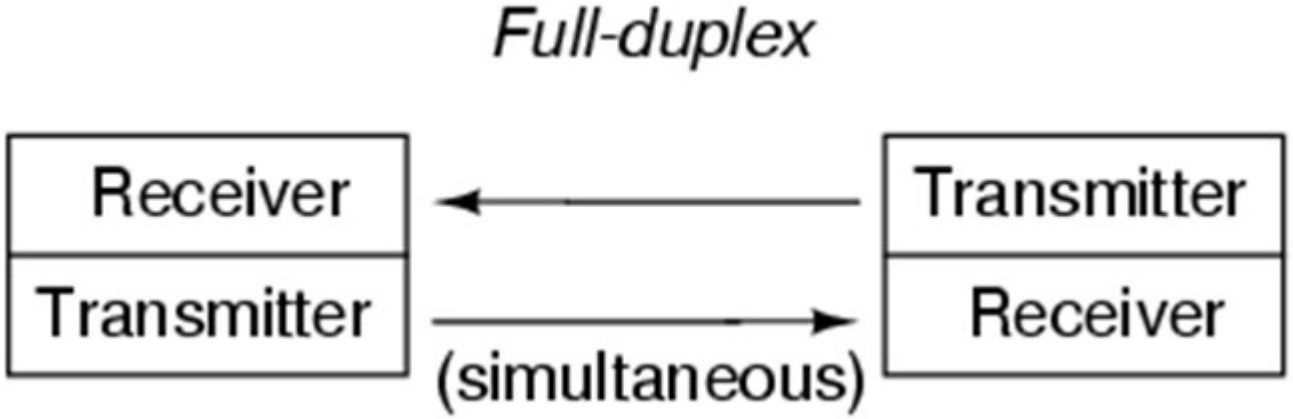
➔ **Exam**



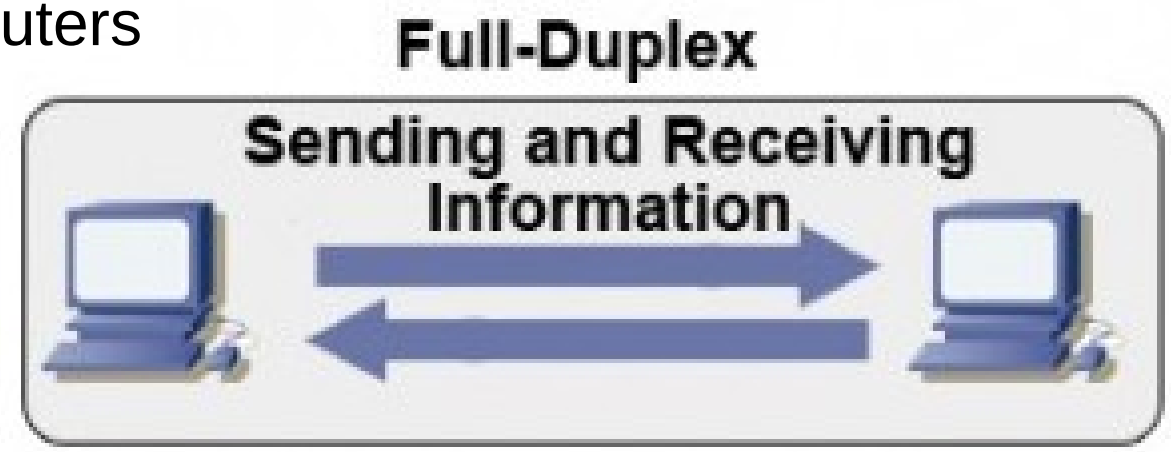
Full-Duplex Mode :

Communication in both directions **at the same time**.

➔ Two physically separate transmission paths, one for sending and the other for receiving ; Or the capacity of the channel is divided between signals travelling in both directions



➔ **Example** : Telephone network, data flow between computers



Servers

- They are a core component of the network, providing a link to the resources (services) to perform any task.
- It is the “leader of the pack”.
- Capability of centralizing the control of resources in network.
- Increase speed and performance by distribute processes.

- Categorize as dedicated and non dedicated :

Dedicated servers : Provide **specific** applications or services or tasks for the network. Requires fewer resources so give **high efficiency and performance**.

Non dedicated servers : Provide one or **more** services and local access. **More flexible** in day-to-day use. Direct network traffic and perform administrative actions. Act as workstation as well as server.

Server Types

Common **server types** include these :

1. File servers
2. Print servers
3. Application servers
4. Message servers
5. Database servers

1) File servers offers services that allow network users to share files. File services are the network applications that store, retrieve and move data.

Example : file servers, such as WindowsNT, NetWare and AppleShare.

The following sections consider these **types of file services**

- File transfer
- File storage and data migration
- File update synchronization
- File archiving

File Transfer

- To transfer a file from one computer to another, you would save the file in **floppy disk or pen drive** and take it over to other computer. Even in a small office this was an inconvenience. For longer distance it was impossible.
- Networks offer file transfer services by File servers. Users can now typically transfer files between **clients and servers** and between multiple servers.
- ➔ With all this file transferring taking place, the need for file **security** arises. **Password and Encryption** schemes used to prevent data from being obtained by unauthorized users.

File Storage and Data Migration

- Three main categories of file storage are these :
  - ❖ Online storage
  - ❖ Offline storage
  - ❖ Near-line storage

Prof. Viral S. Patel

Online storage : Best example is **hard drive storage.**

➔ Information stored on a hard drive can be **called very quickly,** so hard drives used to store files that are **accessed regularly**.

➔ **Disadvantage :**

Prof. Viral S. Patel

- Hard drive space is **expensive**.

- Internal hard drive is permanent part of a computer, they **cannot be conveniently removed**, placed in storage and replaced when needed.

Offline storage : Best examples are **data tapes and removable optical disks.**

➔ Used for **not urgent data (rarely used) and for backup**.

For **example** financial records from previous years may be stored on a company's network, waiting only for the day when an audit is necessary. This type of data can be stored just as well on l**ess accessible, less expensive devices.**

➔ **Disadvantage** : **Requires a person** to retrieve the disk or tape and mount it on the server.

Near-line storage : Best examples are **tape carousel or jukebox.**

➔ **Advantages :**
- **Automatically** retrieves and mounts the tap or disk.
- Low costs and high storage capacities
- No need of network administrator for storage process
- Offer faster, more efficient data access than offline systems, but they are still only fast enough **for infrequently used data and applications.**

➔ The process by which data is moved from online to offline or near-line storage is called **data migration.**

➔ Files are selected for migration based on **factors** such as the **last time the file was accessed, the file owner, or the file size.**

File Update Synchronization :

- File update synchronization has the **goal** of ensuring that each user of a file has the **latest version**.
- By **using time and date stamping and user tracking**, file synchronization works to ensure that files are **properly updated.**

File Archiving :

- File archiving is the process of **backing up files on offline storage device**s, such as tapes or optical disks.
- we can backup files that reside on **multiple client workstations** without leaving chair. This way, we may be able to store every file on a network on a single central storage device.

Prof. Viral S. Patel

2) Print servers

Network

- Allow users to **share printers**
- Allow to **place** printers where convenient, not just near individual computers
- Achieve better workstation **performance** by using high-speed network data transfer, print queues and spooling
- Allow users to share network **fax services**

➔ **Print services** manage and control printing on a network. Print jobs are stored on storage areas and sent to the printer in an organized fashion or may be prioritized in accordance with other criteria.

➔ **Advantage :** Network printing also cuts costs by allowing shared access to printing devices.

With network print services, we can **fax** straight from workstation to a receiving fax machine. So this way we can eliminate the step of printing a hard copy and scanning it into a fax machine.

With a **fax server,** we can receive faxes directly on workstation. **Optical character recognition (OCR)** software can even convert these faxes into editable text, thereby saving a lot of time and effort.

3) Application servers

- **Application services** allow client PCs to access and use extra computing power and expensive software applications that reside on a shared computer.

- Some time **specialized server** provide specific applications on a network. For example, one organization needs a powerful database, so we can add a server to provide this application.

- Application server can be **dedicated** for providing application services **or** they can **serve multiple functions** like provide file, print, communication and database services. It minimizing the drain on file serves' resources.

4) Message servers

➔ With file services, data can pass between users only in file form. With message services, data can take form of graphics, digitized video, or audio, as well as text and binary data.

➔ As **hypertext links** become more common in messages, which transmitting data across a network.

➔ Four main types of message services are
- **Electronic Mail**
- **Workgroup applications**
- **Object-oriented applications**
- **Directory services**

➔ **Electronic Mail :** With email we can easily send a message to another user on internet. Email can transfer video, audio, and graphics as well. Integrated voice is the one of the most popular of the recent developments. Email is much faster, cheaper and simple than courier and file transferring services in communication system.

➔ **Workgroup Applications :** Workgroup applications produce more efficient processing of tasks among multiple users on a network.

The two main workgroup applications are

- **Workflow management applications**
- **Linked-object documents**

Workflow management applications route documents, forms and notices among network users for require the input of multiple users. The application would send the form around from one person to the next.

Linked-object documents are documents containing multiple data objects. For example, a single linked object document could contain voice, video, text and graphics linked together. A network message service can then act as an agent for each of these objects, passing messages between the object and its originating application or file.

Object-Oriented Applications are programs that can accomplish complex tasks by combining smaller applications, called objects. By using a combination of objects, object-oriented applications gain the ability to handle large tasks. Message services facilitate communication between these objects by acting as a go-between.

Directory Services servers help users locate, store, and secure information on the network. Both Active Directory and Novell Directory services store information about users and computers.

5) Database servers

- Database services can provide a network with powerful database capabilities that are available for use on relatively weak PCs. Most database systems are client-server based. Client send data requests and server perform database operations managing the database, processing queries and replying to clients.

- Database server also providing security, database optimization and data distribution.

Topology

The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

OR

A Network Topology is the arrangement with which computer systems or network devices are connected to each other.

➔Topologies may define both physical and logical aspect of the network.

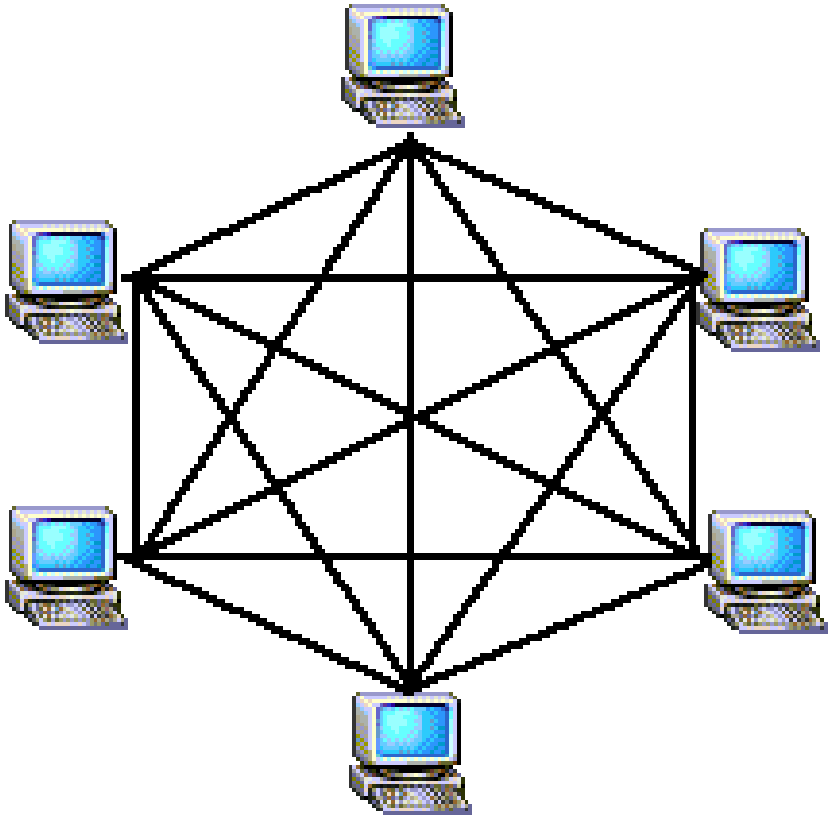
➔The term **Physical topology** refers to the way in which a network is laid out physically. Means how they are actually interconnected with wires and cables.

➔The term **Logical topology** means is the arrangement of devices on a computer network and logically how they communicate with one another.

Mesh Topology :

In mesh topology every device is connected by **point-to-point** link to every other device.

Total number of links in Mesh Topology is **n(n-1)** for simplex mode and **n(n-1)/2** for duplex mode.



Advantages :

Links guarantees : Each connection can carry its own data load means eliminating the traffic problem.
Robust : if one link becomes unusable, it does not stop entire system.
Privacy or Security : When every message travels along a dedicated line, only the intended recipient sees it.
Fault Identification and fault isolation easy : Because of point-to-point links.

Disadvantages :

More number of cabling and I/O ports required, So it becomes expensive and also required more space for wiring.

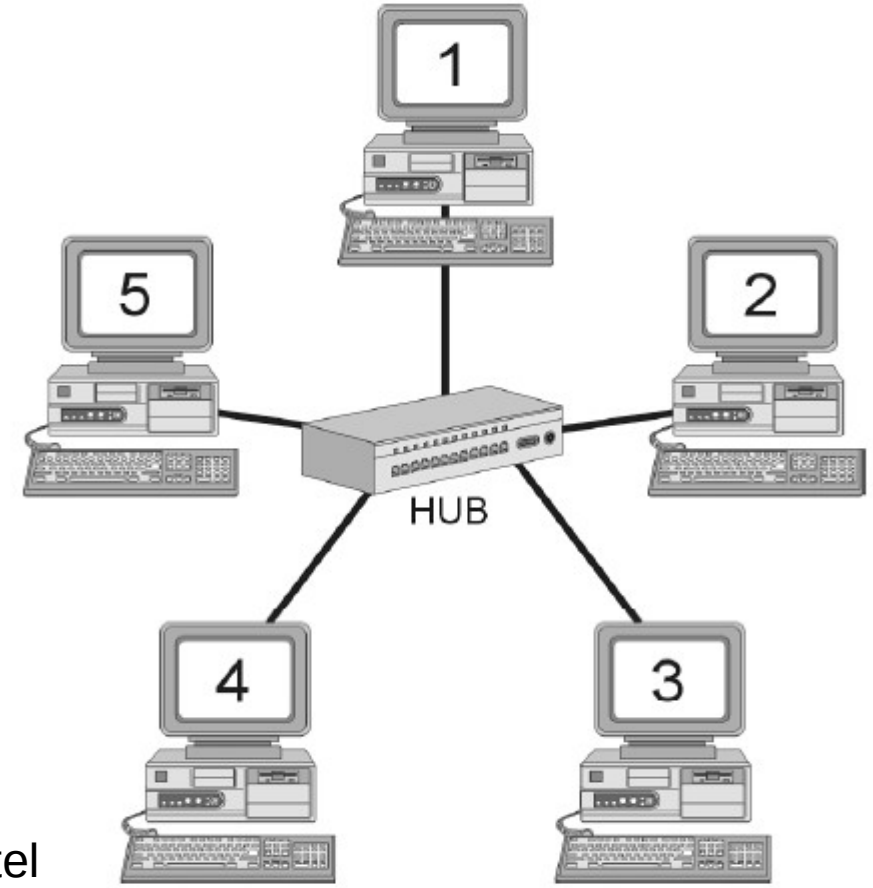
Example of Mesh Topology:
Connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Star Topology :

In star topology, each device has a dedicated **point-to-point** link only to a **central controller**, usually called a **HUB**. The devices are not directly linked to one another.

The controller (HUB) acts as an exchange :

If one device wants to send data to another, it sends the data to controller, which then relays the data to the other connected device



Prof. Viral S. Patel

Advantages :

- Less cabling and Less expensive then Mesh Topology.
- Each device needs only one link and one I/O port to connect.
- Easily add, move and delete nodes.
- Easy to install and reconfigure.
- Robustness : If one link fails, all other links remain active.
- Easy to fault identification and fault isolation.

Disadvantages :

- Whole topology depend on one single point, the HUB. If HUB goes down, the whole system is dead.
- more cabling required than ring and bus topology.

Example of Star Topology:

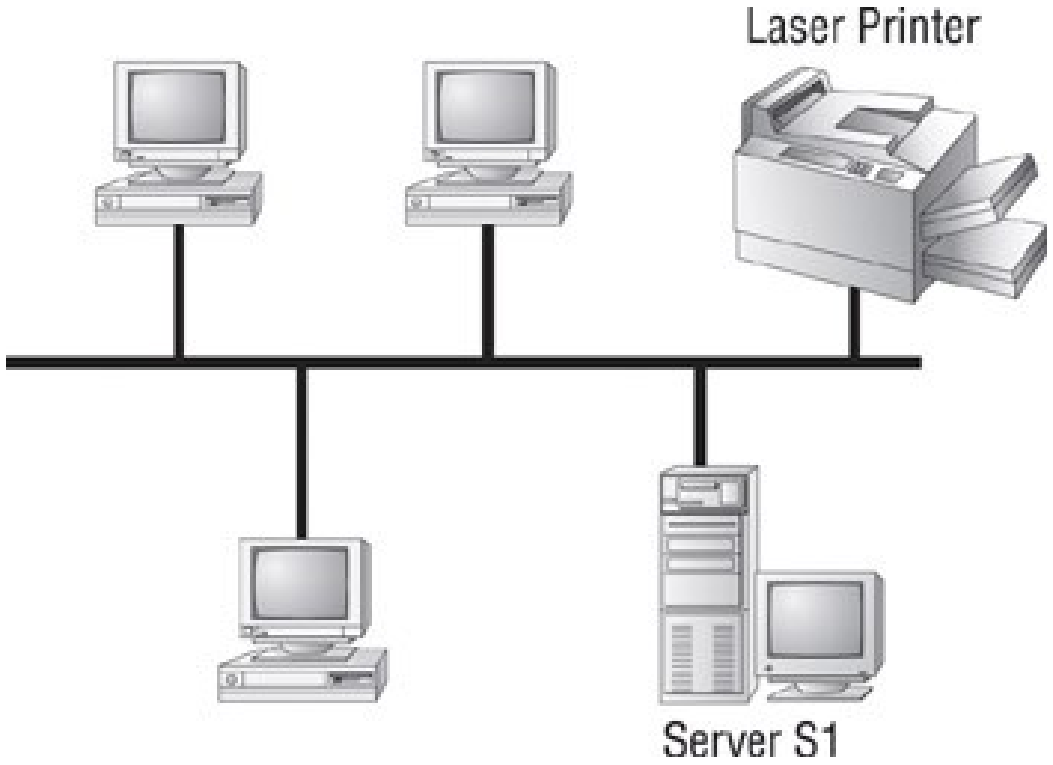
- Used in High-speed Local-area networks (LAN) with a central HUB.

Bus Topology :

Bus topology is **multipoint**. One long cable acts as a backbone to link all the devices in a network.

Nodes are connected to the bus cable by **drop lines and taps.**

Signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a **limit on the number of taps** a bus can support **and** on the **distance between those taps**.



Advantages :

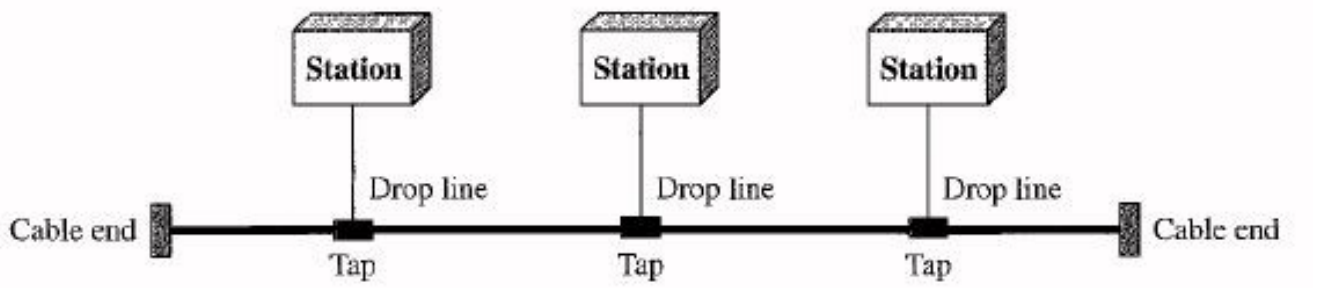
- Ease of installation : Backbone cable connected with nodes by drop lines of various lengths. So bus uses less cabling than mesh or star topologies.

Disadvantages :

- Difficult to reconnection and fault isolation.
- Difficult to add new devices. It require modification or replacement in backbone.
- Signal reflection at the taps can cause degradation in quality.
- fault or break in the bus cable stops all transmission.
- Damaged area reflects signals back in the direction of origin, creating noise in both direction.

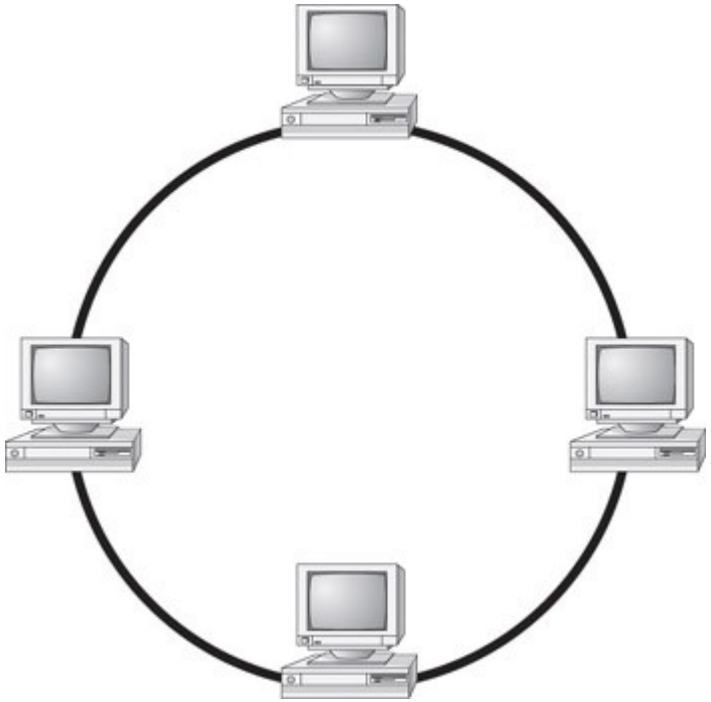
Example of Bus Topology:

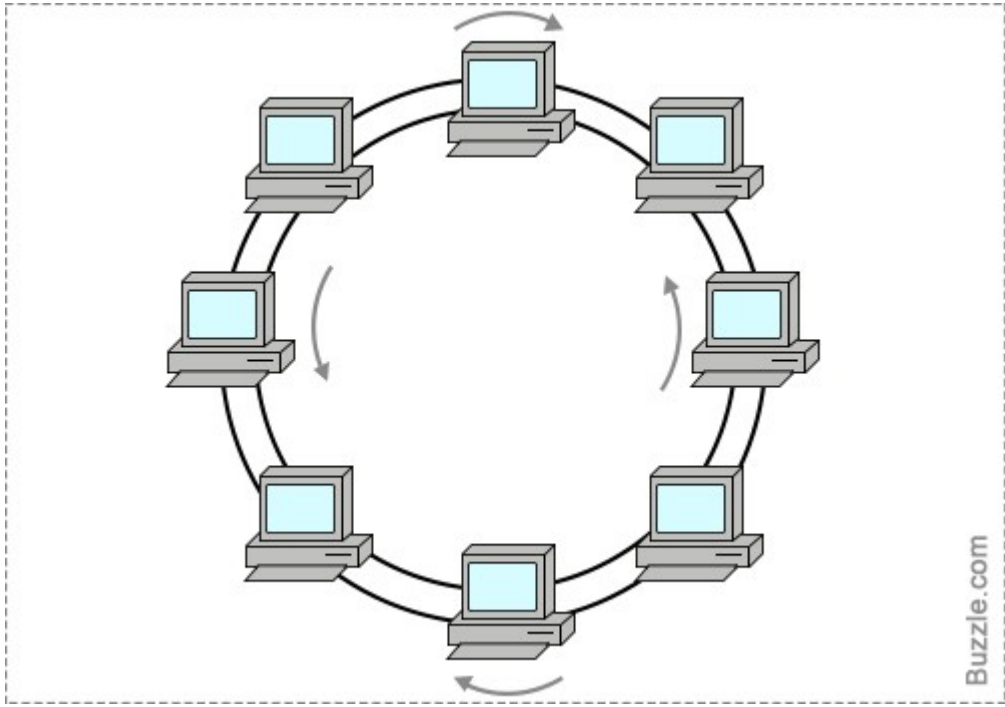
- Used in early local-area networks. Ethernet LANs can use a bus topology.



Ring Topology :

In ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.





Advantages :

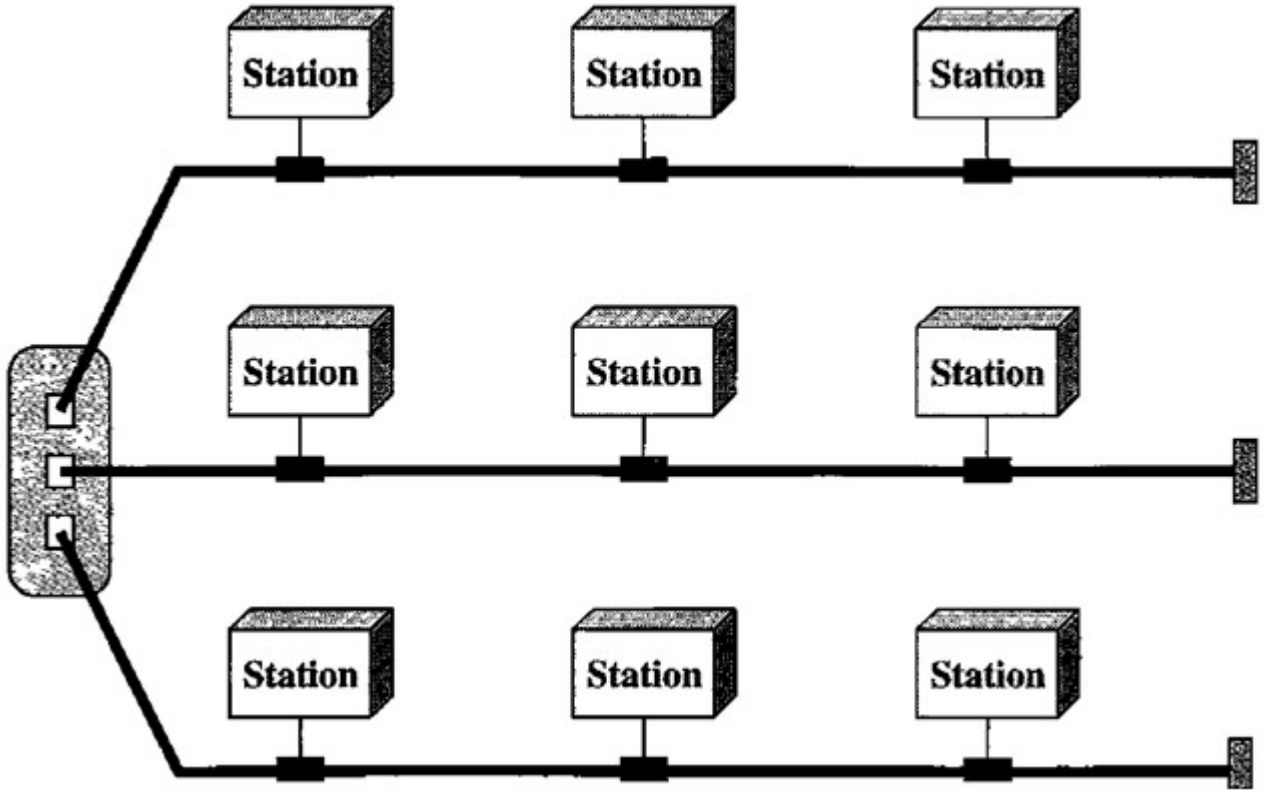
Easy to install and reconfigure.
Each device is linked to only its immediate neighbors. To add or delete a device requires changing only two connections.
Fault isolation is simplified.
Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

Disadvantages :

Unidirectional traffic.
In a simple ring, a break in the ring can disable the entire network. This weakness can be solved by using a **dual ring** or a switch capable of closing off the break.

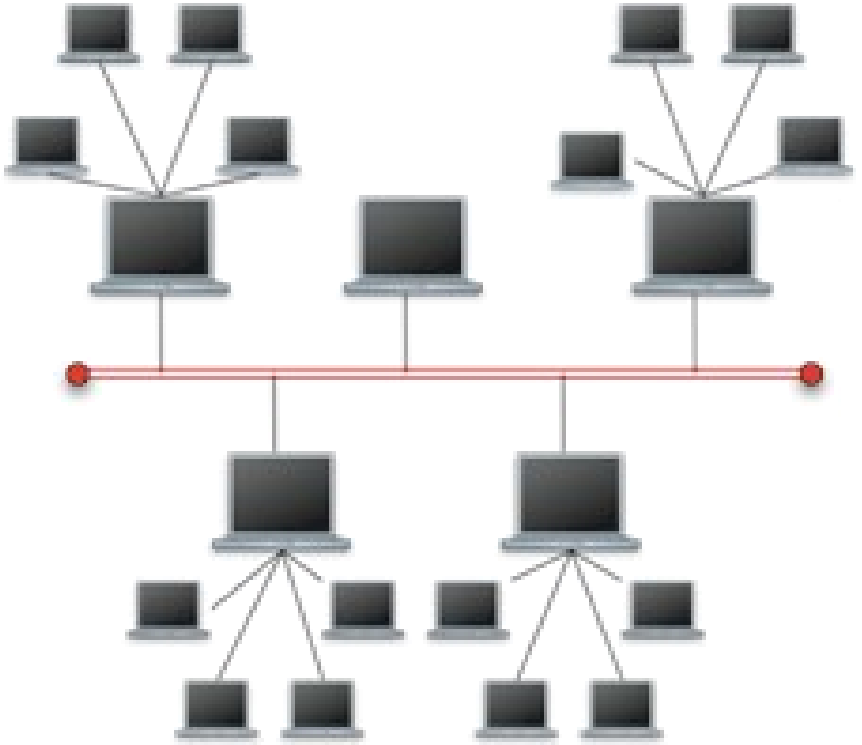
Hybrid Topology :

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in fig.



Star Bus (Tree) Topology :

➔A Star Bus network consists of two or more star topologies connected using a bus backbone. One of the most popular LAN technologies.



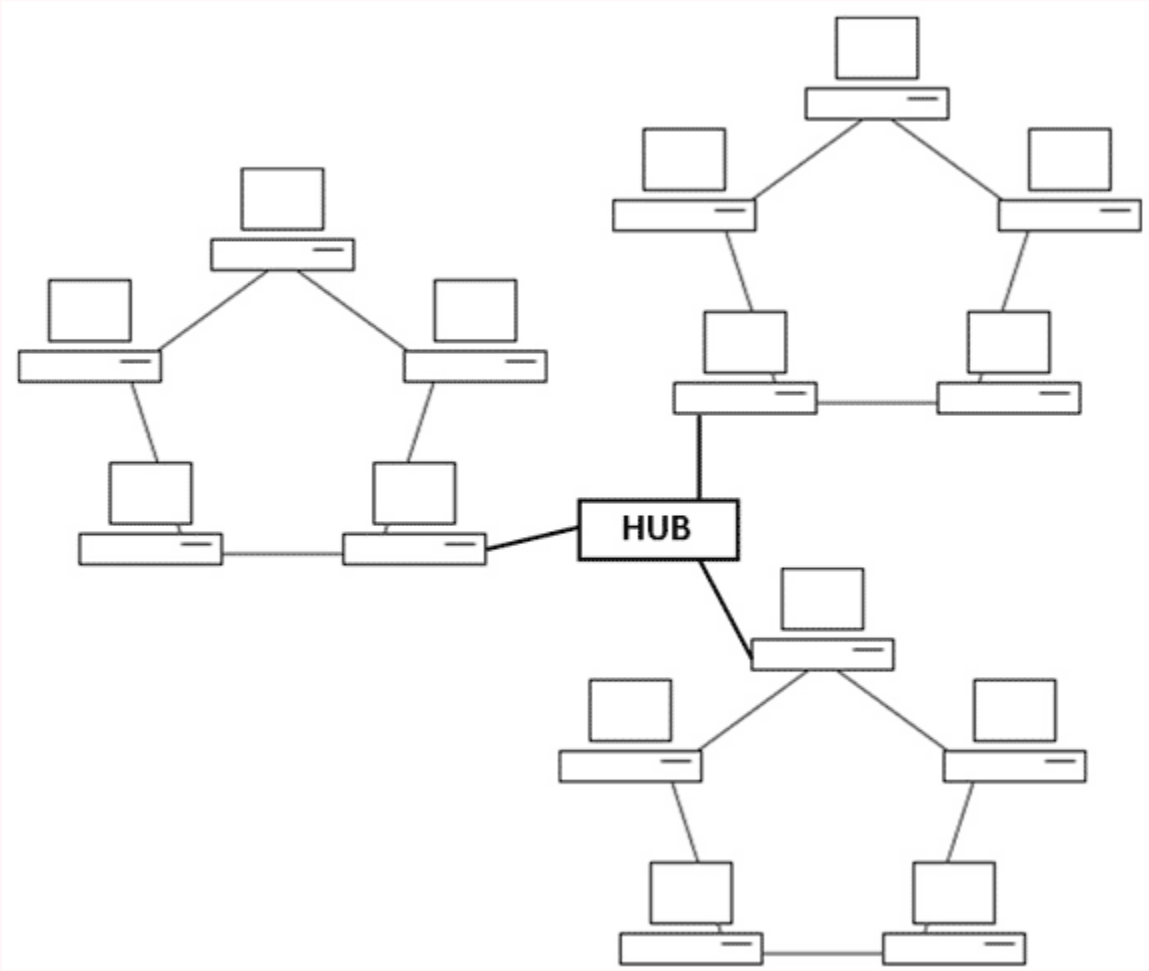
Advantages :

➔Fault tolerant
➔Flexible and easy to use
➔Easy to removing and adding nodes from the hub (scalability achieved)
Fast processing (up to 1Gbps)

Disadvantages :

Expensive because of additional cable and the purchase of a hub.
The network depends heavily on the bus. Its failure affects the entire network.
Complexity of design.

Star Ring Topology :



Bus Logical Topology :

Ethernet is probably the best-know example of a logical bus Topology; It is the most popular LAN type.

Each time a node on the network has data for another node, the sending node **broadcasts the data** to the entire network. The various nodes hear it and look to see if the data is for them. If so, they keep the data. If not, they ignore the data.

Every **Ethernet card has a 48 bit address** and each piece of data that travels the network is directed to the address of the card in the node that should receive the data.

Before a workstation broadcasts to the network, it listens to see if any one else is using the network. **If the coast is clear, then the workstation broadcasts.**

If the **distance between two computers** on the same network **is too great**, they may not hear each other on the line. If they can't "hear" each other, then Node A can't tell whether Node B is transmitting or not. So Node A may therefore begin to transmit data when Node B is already transmitting data.

If this happens and two nodes transmit at the same time, an event called a packet **collision occurs**, causing a frequency “ripple” on the cable.

The **first node** to detect this **increased frequency** ripple will send out a high-frequency signal that will cancel out other signals.

This signal tells all nodes that a collision has occurred and that **all nodes** on the network should **stop sending packets**.

Prof. Viral S. Patel

At this point, each node waits a random amount of time and then tries broadcasting again. They will do this up to 16 times before giving up.

Having **cable no longer than** it is supposed to decrease your chance of collision because the nodes can hear other nodes broadcasting. But the way the bus logical topology works increase the packet collisions.

If a node can’t broadcast until the network is clear and more than one node has information to send. Then **as soon as the line’s free both nodes will send** their information out first and result is a collision.

All of this processing takes place at the Ethernet NIC. Ethernet can run on top of a physical bus, physical star or physical ring.

Prof. Viral S. Patel

Ring Logical Topology

In this topology, only one node can be allowed to transfer the data in a network at a given time. This mechanism is achieved by **token** (the node having token only can transmit the data in a network) and hence the **collision can be avoided** in a network.

When a workstation is done with the token packet, it releases token to whatever station is next in line. If nobody grabs it, the workstation releases it a second time. **If nobody responds to the token** packet for a second time, then the **workstation sends** out a general query, known as a **solicit successor frame.**

This frame goes out over the network, asking, “Who’s supposed to get the token next ? “ If a workstation responds, the sending workstation addresses the token to that workstation and passes the token.

In the logical ring topology, one computer is dedicated to token management in network. This computer called **the token master** or **active monitor**, detects lost tokens, monitors frame transmissions and creates a new token when necessary. The active monitor also maintains a regular clock tick on the network that keeps all other nodes synchronized.

IEEE Standards :

- The Institute of Electrical and Electronics Engineers (IEEE) has standardized some network types.
- They are defined at the physical and data link layers of the Open System Interconnect (OSI) model.
- These standards describe both physical media and methods of packet transmittal.
- In other words, we can know how a network will behave and how that network is designed to work.

Prof. Viral S. Patel

IEEE 802.2	Standards for Data link layer. **Logical Link Control(LLC) and Media access control (MAC)** standards for connectivity.
IEEE 802.3	**Ethernet** Standards for Carrier Sense Multiple Access with Collision Detection **(CSMA/CD). (* logical bus topology)**
IEEE 802.4	Standards for **token bus access.**
IEEE	

IEEE standards (This page is only for knowledge):

Prof. Viral S. Patel

IEEE 802.6	Standards for information exchange between systems.
IEEE 802.7	Standards for broadband LAN cabling.
IEEE 802.8	**Fiber optic** connection.
IEEE 802.9	Standards for integrated services, like voice and data.
IEEE 802.10	Standards for **LAN/MAN security** implementations.
802.12	
IEEE 802.14	Standards for cable television broadband communications.
IEEE 802.15.2	**Bluetooth**
IEEE 802.15.4	Wireless Sensor/Control Networks – "**ZigBee**"
IEEE 802.15.6	Wireless Body Area Network(BAN) – (e.g. Bluetooth low energy)

IEEE standards :

IEEE	Name	Physical topology and media	bandwidth
802.3	10Base2	**Thin Coaxial Cable (RG-58)** in bus topology	10Mbps
802.3	10Base5	**Thick Coaxial Cable (RG-8 or RG-11)** for the backbone; Taps to the backbone from each PC	10Mbps
802.3u	100BaseT or Fast Ethernet	**Unshielded twisted pair** in a star topology	100Mbps (10Mbps version in 802.3)
802.3z	Gigabit	Ethernet **fiber-optic** for the backbone, coaxial cable for the taps to the hub, all in the star topology	1000Mbps
802.11 b	Wireless	CSMA/CA cellular	1 or 11Mbps

IEEE 802.2 Standard : (Data link layer rules)

- This standard defines the **rules for data link communication** for networking topologies 802.3 – 802.5.
- Working for both Token Ring and Ethernet, it **provides the interface** between networking protocols such as TCP/IP and the network types.
- The 802.2 standard can function either in **connectionless mode or in connection-oriented mode** for protocols that do require such as explicit connection to be made.

- The IEEE divides the data link layer into two sections :
  Logical link connection (LLC) and
  Media access control (MAC).

LLC: The LLC handles the **interface between** all networking **topologies and** their network-layer communication **protocols.**

MAC : The LLC relies on the MAC layer to provide it with certain **addressing information**. The method or addressing information it uses **defines the network type**.

IEEE 802.3x Standard :
(Ethernet Standard) (logical bus topology) (CSMA/CD)

- Ethernet was standardized as a **10 Mbps** network by 802 committee of IEEE.

- **10Base2,10Base5,10BaseT and 10BaseF** all are types of Ethernet networks.

- Ethernet is also called logical bus topology and a method of error detection and recovery called **carrier sense multiple access with collision detection (CSMA/CD).**

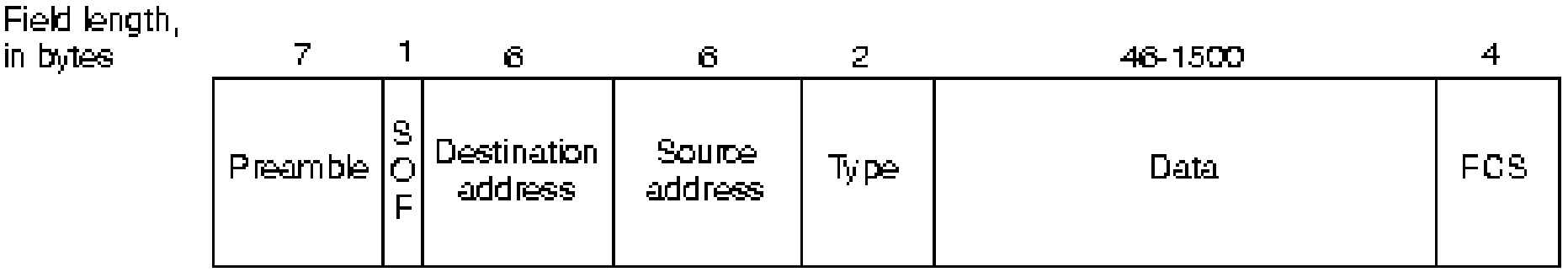
- The various forms of Ethernet use different **physical topologies** (for example **bus and star**) and cabling types (such as UTP, coaxial and fiber)

Information travels in Ethernet network in frame consists of six parts.

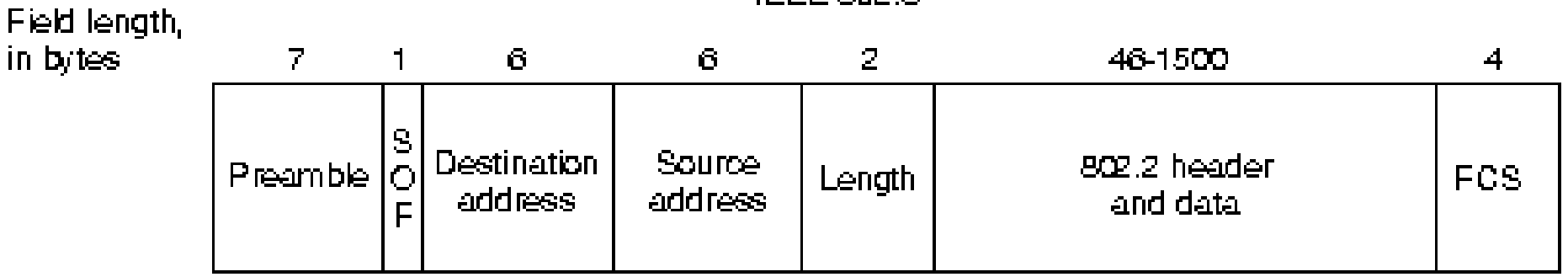
- **Preamble :** Consists of eight bytes of information used to coordinate the rest of the information in the frame.
- **Destination address :** Consists of the hardware address of the workstation that receive this information

- **Source's address :** Consists of the hardware address of the workstation that sent the information.
- **Type :** Designates the type of information that is held within the data part of this frame, whether it is graphic information, ASCII text information or whatever.
- **Actual data :** Can be anywhere from 46 to 1500 bytes long.
- **Frame checked sequence :** Resembles a packing slip; it is used to verify that the rest of the frame reached its destination intact.

Ethernet



IEEE 802.3



S1291a

SOF = Start-of-frame delimiter
FCS = Frame check sequence

Prof. Viral S. Patel

The 802.3n standard feature is the carrier sense multiple access with collision detection (CSMA/CD).

Prof. Viral S. Patel

- **“Carrier sense”** means that **all nodes on the network listen** to the network to see whether it is clear before attempting to transmit.

- **“Multiple access”** means that **all nodes on the network have access to the same cable** – that signals are broadcast across the entire LAN.

- **“Collision detection”** means that **each node can tell** if another node starts transmitting data at the same time the first node is already sending data.

- In short, CSMA/CD provides a means for reducing packet collision by having each PC broadcast a signal known as the **carrier sensing signal** before transmitting in order to see if any other workstations are broadcasting.

- If not, the signal gives the workstation the “**all-clear**” and the workstation **transmits** its packet. If the carrier-sensing signal **detects another** workstation’s transmittal, the workstation **waits** before

Problem :

- This process avoids collisions so long as network traffic isn't heavy and the LAN's cables are not any longer than their rating. If either of those conditions exit, then collisions are likely to happen regardless of CSMA/CD.

➔ CSMA/CD is **not in charge of** making sure that **only one workstation transmits at a time**, it is in charge of making sure all workstations are quiet before one transmits.

➔ If two workstations happen to begin **transmitting at the same time**, there's **nothing that CSMA/CD can do** to avoid the collision.

Solution :

- If two packets collide, CSMA/CD tries to avoid a repeat collision. First time a collision happens, each workstation chooses a **random number** between **one and two** before transmitting again.

  If the workstations choose the same number, causing another collision by beginning their broadcasts at the same time, they each choose a number between **one and four** and try again.

  This process goes on until either the workstations have both successfully completed their transmissions or they have **tried 16 times** without success.

  If they flunk out by the sixteenth try, both workstations have to pause and **give the other workstations a chance to transmit.**

In short, CSMA/CD is not designed to prevent every collision, but it tries to minimize the time that collisions tie up the network.

The Token Bus (802.4) standard (Logical Ring + Physical bus)

- The IEEE 802.4 subcommittee designed a combination bus/ring topology that transmitted information via a token but would use the **bus physical topology.**

- Only the workstation that has the **token** can send information, and once that workstation has received acknowledgement of the receipt of that information, it must then pass the token to the next workstation in line.

- In the 802.4 standard, the network **keeps track** of who gets the token next. It is possible for some workstations to have higher **priority** to get the token than others.

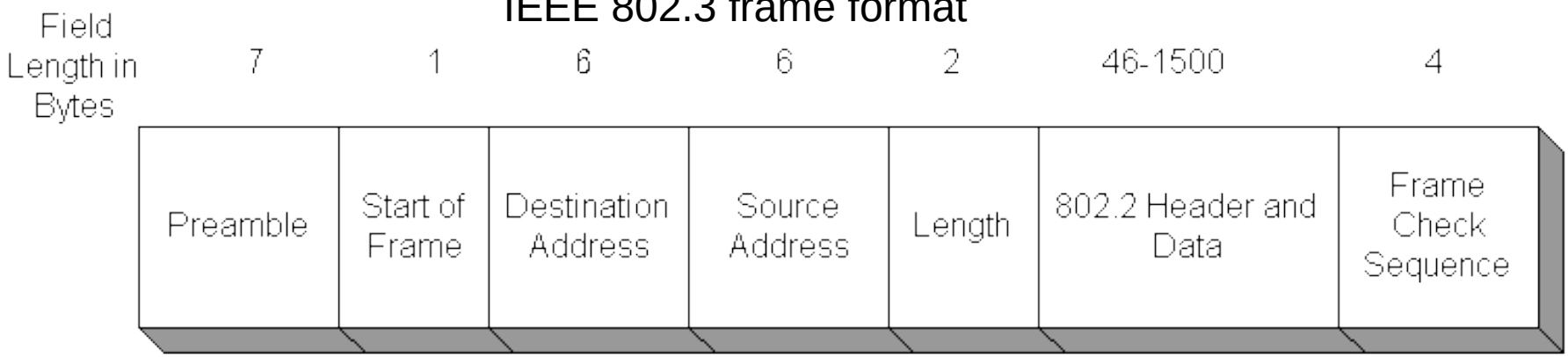
Difference between 802.3 and 802.4 :

- 802.4 , the medium is a token bus network runs on either 70 ohm coaxial cable or fiber (unlike the 50 ohm used by 10Base2)
- Frame looks different. (see fig.)
- 802.4 **avoids collisions** because token/bus combination (advantage)

1 byte	1 byte	1 byte	2-6 byte	2-6 byte	0-8182	4 byte	1 byte
Preamble	Start Delimiter	Frame Control	Destination Address	Source Address	Data	Checksum	End Delimiter

Frame format of IEEE 802.4

IEEE 802.3 frame format



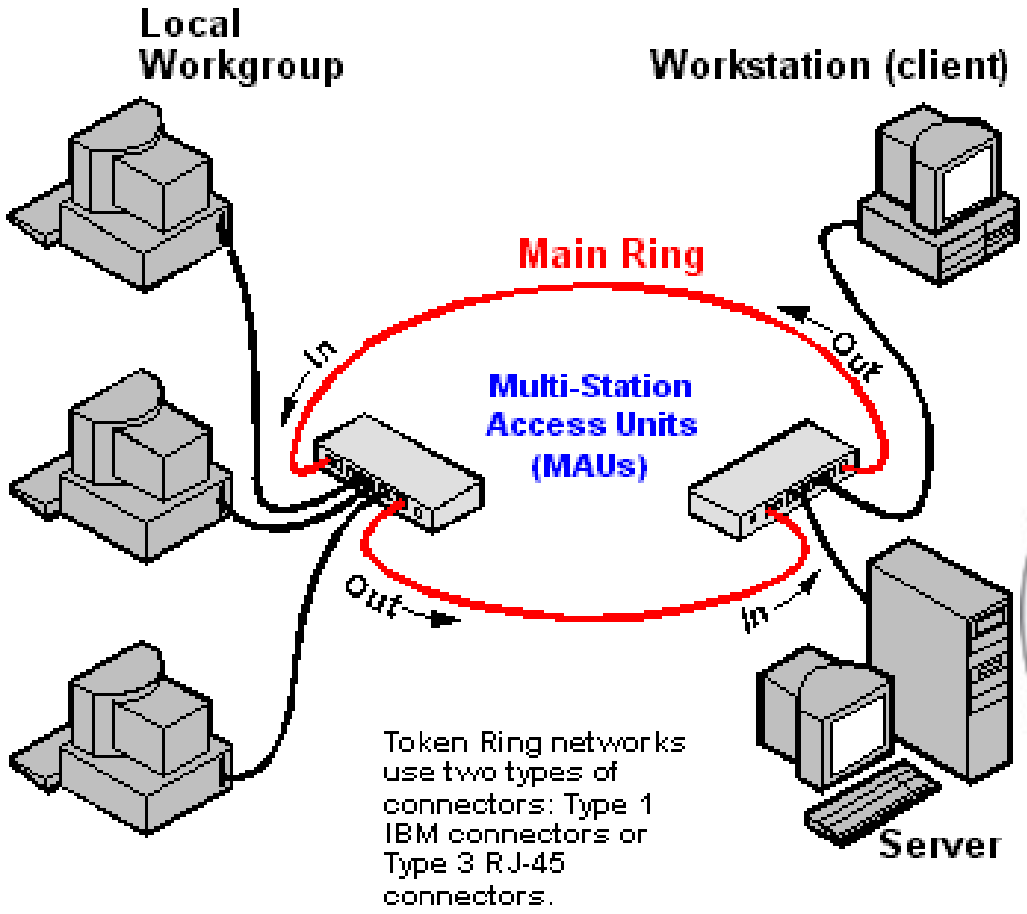
Disadvantage/Problem of token bus format :

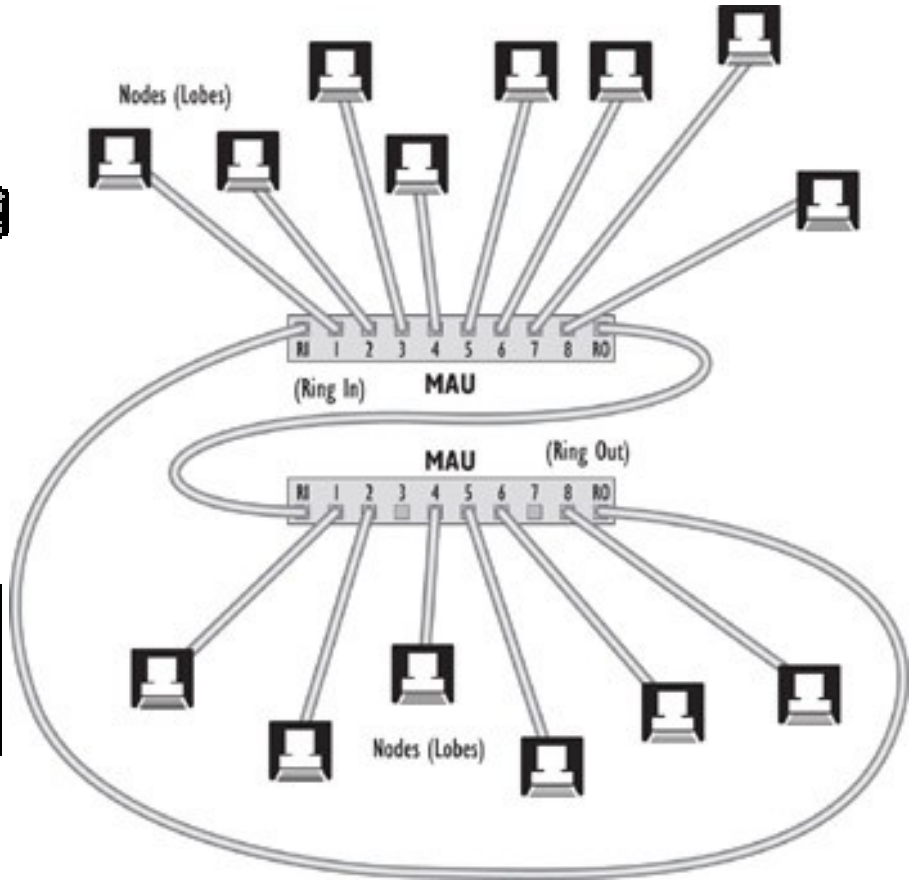
Due to **malfunctioning hardware**, which can result in the token being lost, or shadowed tokens that make it look as there are **multiple tokens** on the network.

The Token Ring (802.5) standard

(Logical Ring + Physical Ring topology (Star topology in the form of Ring using MAU as show in fig.) **)**

- A token ring network use the multistation access unit (MAU) with D shell and IBM type connector. Eight PCs can attach to one MAU which attach to other MAUs as shown in fig. There are no terminators.





- This standard use the token specification to pass information from one workstation to another.

Working :

The workstations on a Token Ring network **use a token** to determine which workstation gets to transmit data at any given time. If a workstation **doesn't need** to transmit anything, **it passes** the free token to the next workstation and so on until it gets to a workstation that needs to transmit something.

- Data travels from the originating workstation to every node on the network is succession. Each workstation **examines the address** on the data packet. If the data is for that station, it **keeps a copy** of the data and sends the original on. If the data isn't for that station, it only sends it to the next workstation on the network. **When** the sending workstation **gets back** the copy or its first data packet, it knows that it is **time to stop** transmitting and **passes** the free token **to the next workstation**.

Solve problem of 802.4 :

With a **smart hub**, the Token Ring standard can help the network recover from problems due to malfunctioning hardware – a nice feature that the Token bus standard doesn't have.

- If a workstation malfunctions, either not releasing the token when its turn is up or jabbering over the network, the smart hub can tell that there's trouble and **cut that workstation** form LAN allowing the rest of the network to function normally.

- **Advantage over 802.3 or 802.4 :**
  An 802.5 network can also extend for longer distances than either the 802.3 or the 802.4 because the packet travels from one workstation to another, **retransmitted at every step** and so it never has very far to go before being retransmitted.

LAN	MAN	WAN
LOCAL AREA NETWORK	**METROPOLITAN NETWORK**	**WIDE AREA NETWORK**
All the devices that are part of LAN are generally within a building. Generally up to **2 km** distance.	All the devices that are part of MAN are span across several buildings in same city or town. Generally up to **200 km** distance.	All the devices that are part of WAN have no geographical boundaries. Unlimited rage. Usually in **1000 km rage**.
LAN network has very **high speed** mainly due to proximity of computer and network devices.	MAN network has **lower speed** compared to LAN.	WAN **speed varies** based on geographical location of the servers. WAN connects several LANs.
speeds can be 10Mbps or 100Mbps or **1000Mpbs.**	speeds can be **10Mbps or 100Mbps.**	speeds can be **1.5Mbps** (vary based on technology)
LAN uses generally **Guided Media.**	MAN uses **Guided Media or Unguided media**	WAN mainly uses **Guided Media or Unguided media.**
Example : **University or Institute lab network.**	Example : **Cable Television**	Example : communication services like **satellite**

Prof. Viral S. Patel

Clients, Servers and Peers

There are three roles for computers in a local area network :

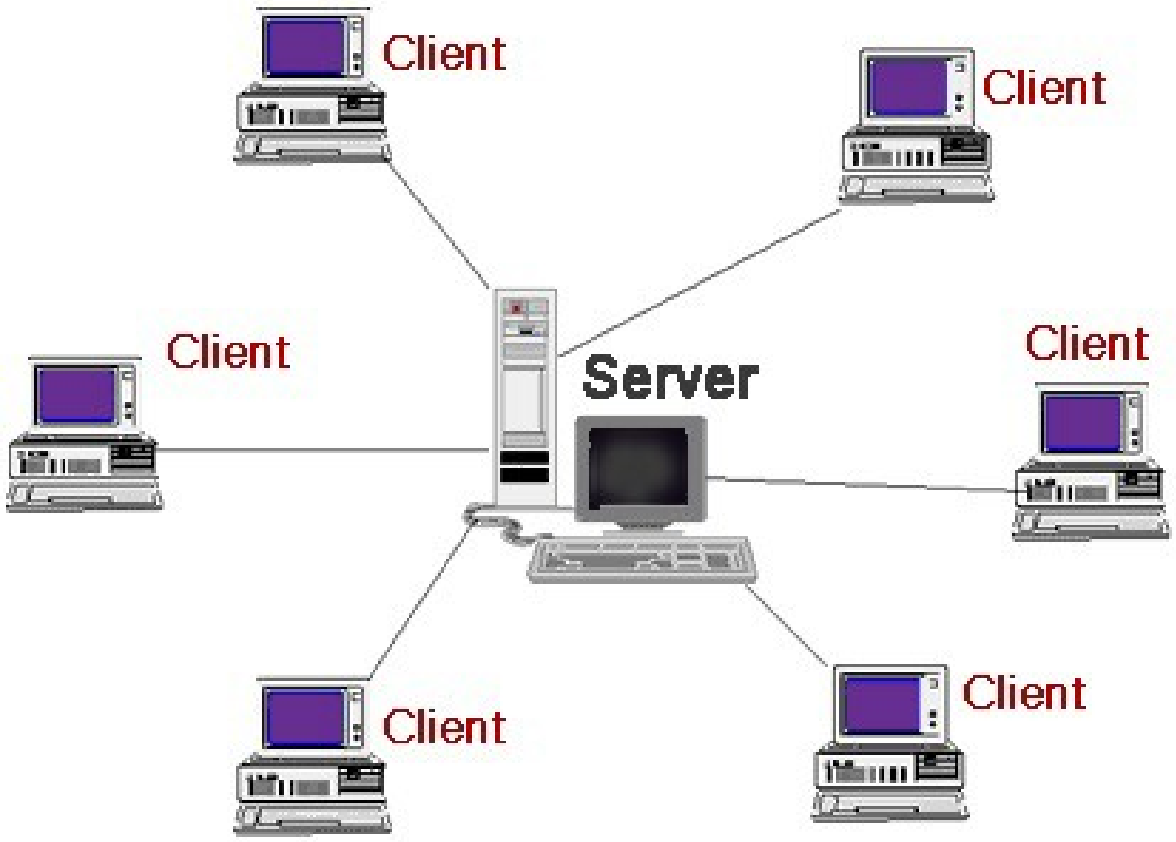
1. Clients : which use but do not provide network resources
2. Peers : which both use and provide network resources
3. Servers : which provide network resources

Networks are divided into three types based on roles of the computers attached to them.

4. Server-based (also called client-server) : Contains clients and the servers that support them.
5. Peer (also called peer-to-peer) : Has no servers and uses the network to share resources among independent peers.
6. Hybrid network : Is a client-server network that also has peers sharing resources. Most networks are actually hybrid networks.

Server-base Network (Client-server network) :

- This network divide processing tasks between clients and servers.
- client (front end) request services such a file storage and printing and servers (back end) deliver them.
- Server computers are more powerful than client computers.



Advantages of Server-Based Networks :

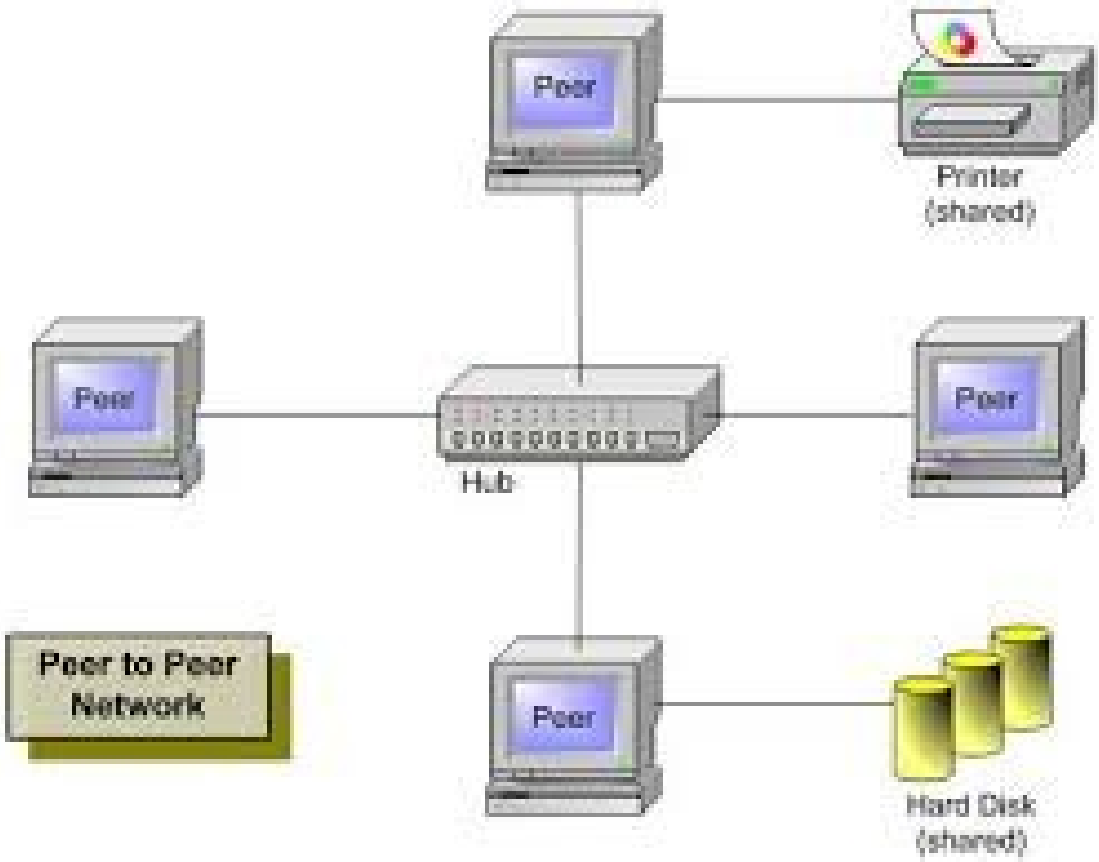
- Strong central security.
- Central file storage and shared resources.
- Ability of servers to pool available hardware and software, lowering overall costs.
- Ability to share expensive equipment
- faster than peers at sharing network resources.
- easy manageability of large number of users.
- central organization which keeps data from getting lost among computers.

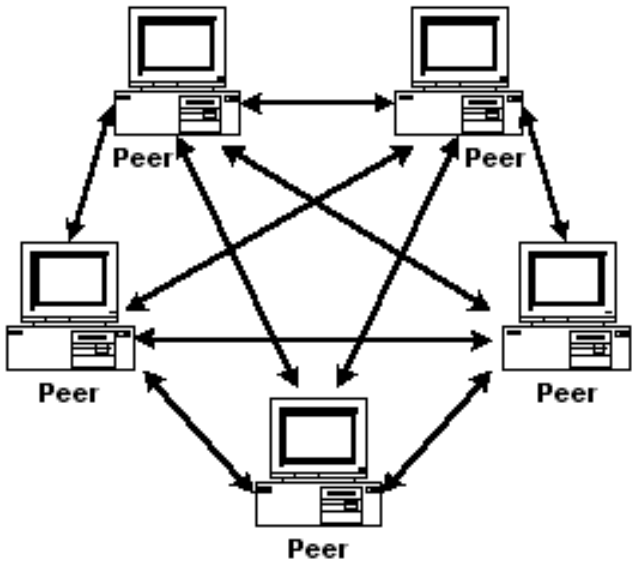
Disadvantages of Server-Based Networks :

- Expensive dedicated hardware.
- Expensive network operating system software and client licenses
- Required a dedicated network administrator.

Peer Networks :

Peer networks are defined by a **lack of central control** over the network. There are **no servers** in peer networks; users simply share disk space and resources, such as printers and faxes.





Peer networks are organized into workgroups. Workgroups have very **little security control**. There is no central login process. If you have logged in to one peer on the network, you will be able to use any resources on the network that are not controlled by a specific password.

Access to individual resources can be controlled if the user who shared resource required password to access it. Because there is no central security, you will have to know the **individual password for each secured shared resource** you wish to access. This can be quite inconvenient.

Peers are also not optimized to share resources. Generally, when a number of users are accessing resources on a peer, the user of that peer will notice significantly **degraded performance.** Peers also generally have licensing limitations that prevent more than a small number of users from simultaneously accessing resources.

Advantages of Peer Networks :

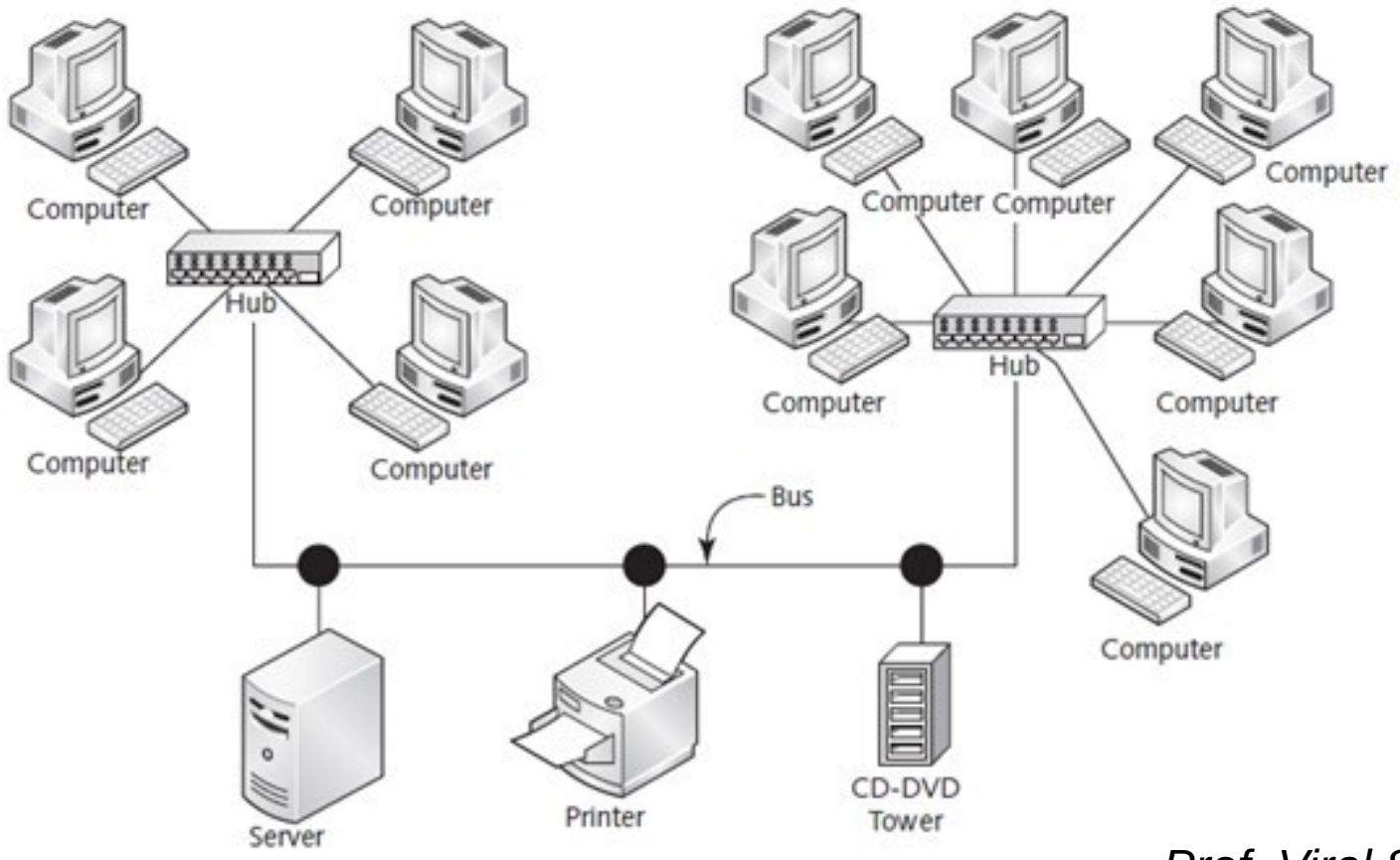
- No extra investment in server hardware or software required.
- Easy setup.
- Little network administration required.
- Ability of users to control resource sharing.
- No reliance on other computers for their operation
- Lower cost for small networks.

Disadvantages of Peer Networks :

- Additional load on computers because of resource sharing.
- Inability of peers to handle as many network connections as servers.
- Lack of central organization, which can make data hard to find.
- No central point of storage.
- requirement that users administer their own computers.
- Weak and intrusive security.
- Lack of central management, which makes large peer networks difficult to work with.

Hybrid Networks :

- They have active directory domains (servers) + workgroups.
- Shared resources are located on servers.
- Network users still have access to any resources being shared by peers in your workgroup.
- It also means network users do not have to log on to the domain controller to access workgroup resources being shared by peers.



Network Security :

Security of the network is considered as the important aspect for improving the network performance. The network security may be affected due to viruses and unauthorized access of other users. To provide network security :

- Avoid opening unknown e-mail attachments which may contain virus.
- use anti-virus software for securing the systems from virus.
- Firewalls can be implemented for detecting and preventing unauthorized access of other users in the network.
- Use backup tools to store the important data on removable media like CD or ZIP disks. This helps to secure your data.

What is Protocol ?

A protocol is a set of rules that govern data communications. OR
Protocols are the agreed-upon ways that computers exchange information.

- A computer needs to know exactly **how messages will arrive** from the network so it can make sure the message gets to the right place. It needs to know **how the network expects the message to be formatted** so the network can convey the data to its destination.
- A protocol defines what is communicated, how it is communicated and when it is communicated.

Hardware Protocols : Hardware protocols define how hardware devices operate and work together.

- The 10BaseT Ethernet protocol is a hardware protocol specifying exactly how two 10BaseT Ethernet devices will exchange information and what they will do if it is improperly transmitted or interrupted.
- It determines such things as voltage levels and which pairs of wires will be used for transmission and reception. There is no program involved; it is all done with circuitry.

Software Protocols :

Programs communicate with each other via software protocols.

- Network client computers and network servers both have protocol packages that must be loaded to allow them to talk to other computers.
- These packages contain the protocols the computer needs to access a certain network device or service.
- There are different protocol packages for different networks and even for different kinds of servers on the same network.

OSI model

The **Open Systems Interconnection model** (**OSI**) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into **7 layers**.

The model is a product of the Open Systems Interconnection project at the **International Organization for Standardization (ISO)**.

Why Layering ?

To provide well-defined interfaces between adjacent layers.

- A change in one layer does not affect the other layers.
- Interface must remain the same.

Allows a structured development of network software.

Physical Layer

Type of Transmission media - Physical characteristic of interfaces and medium

Transmission rate (Data rate) – bits per second

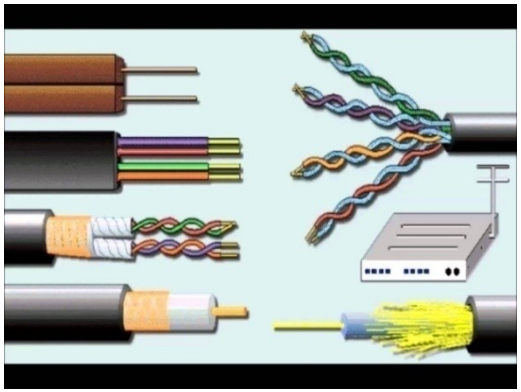
Synchronization of bits – sender and receiver use clocks.

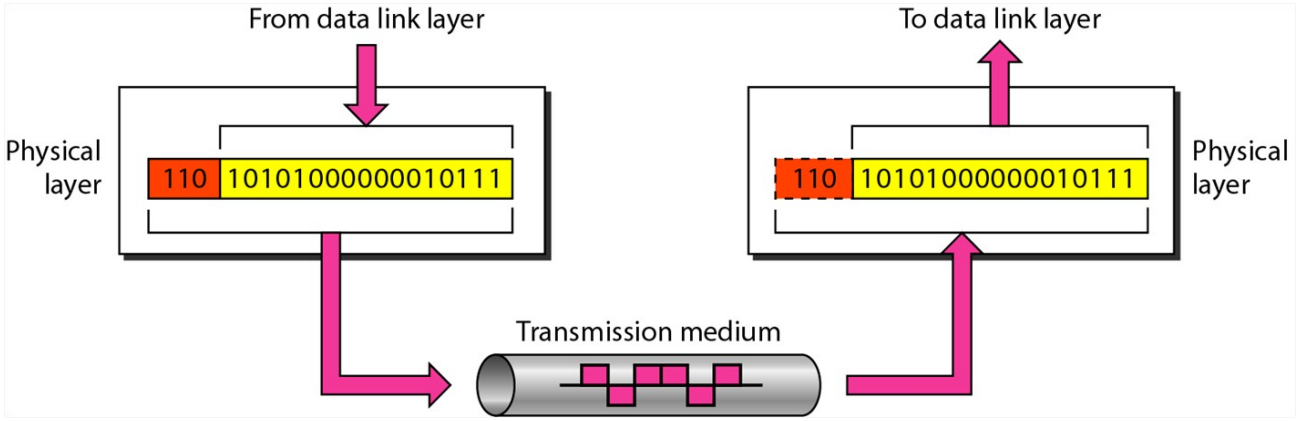
Line configuration – point to point , multipoint

Physical topology - mesh, star, ring, bus

Transmission mode – simplex, half-duplex, full-duplex

Prof. Viral S. Patel





Prof. Viral S. Patel

Data Link Layer

Framing : Divides the stream of bits received from network layer into frames.

Physical addressing : adds a header to the frame to define address of sender and/or receiver of the frame.

Flow control : data absorbed by the receiver is less than the rate at which data are produced in the sender managed by flow control mechanism

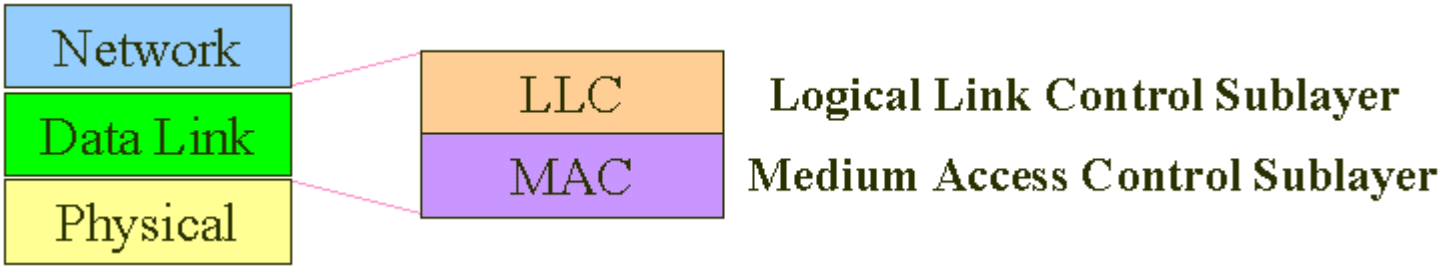
Error control : trailer added to the end of the frame. Prof. Viral S. Patel

Access control : when more devices are connected to the same link.

Hop-to-Hop (node-to-node) delivery of packet on the same network

LLC sublayer handles error control, flow control, framing and MAC sublayer addressing

MAC sublayer handles access to share media such as Token passing or Ethernet.

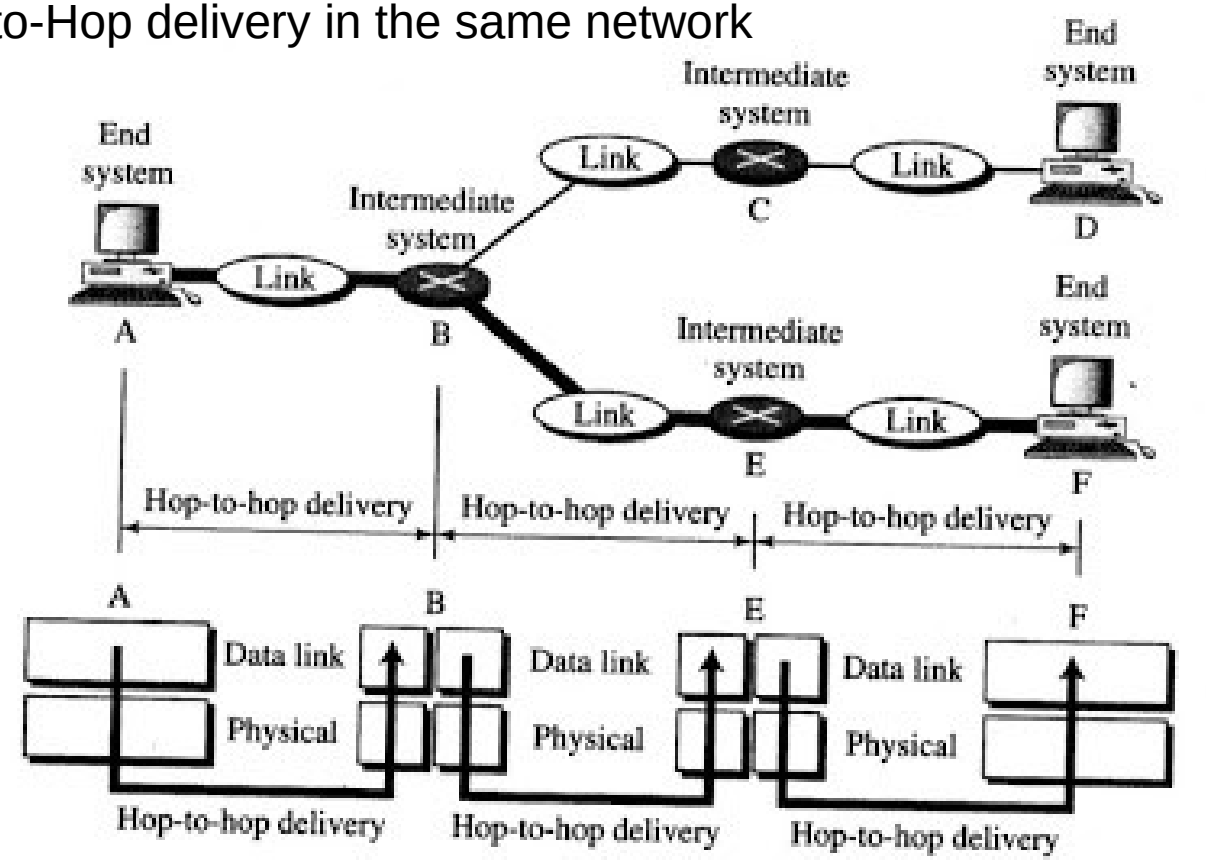


Data Link Layer

- Frame format

Start delimiter	Access control	Frame control	Destination Address	Source Address	Data	FCS	End delimiter	Frame status

- Hop-to-Hop delivery in the same network



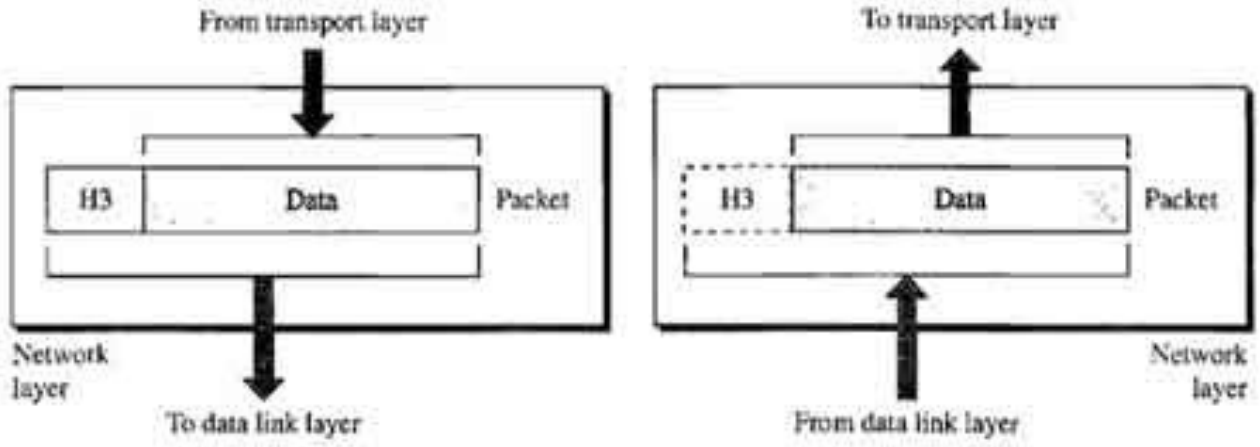
Network Layer

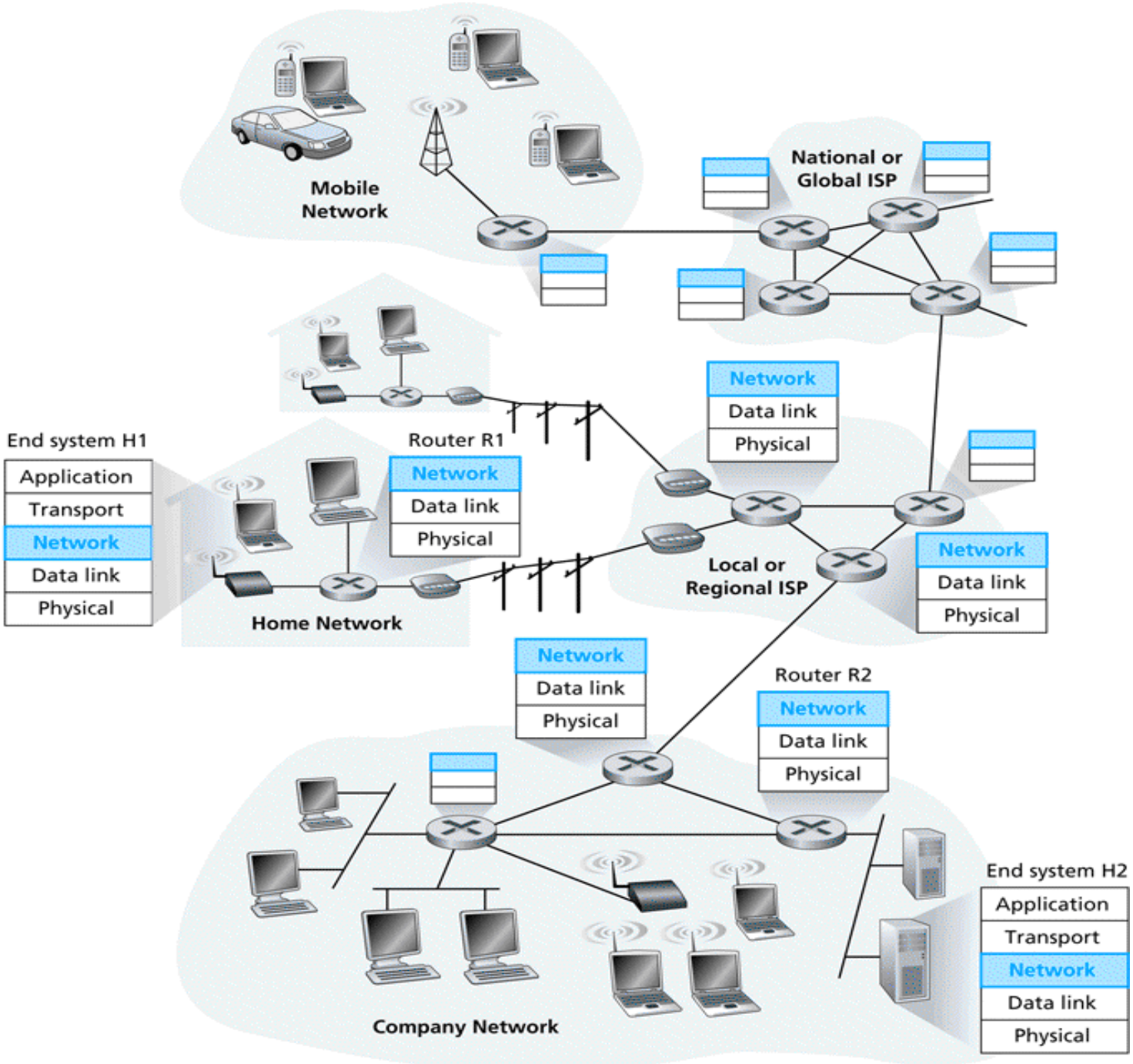
Logical addressing : Physical addressing implement by data link layer only handles addressing problem locally but a packet passes the network boundary we need logical addressing (IP address)

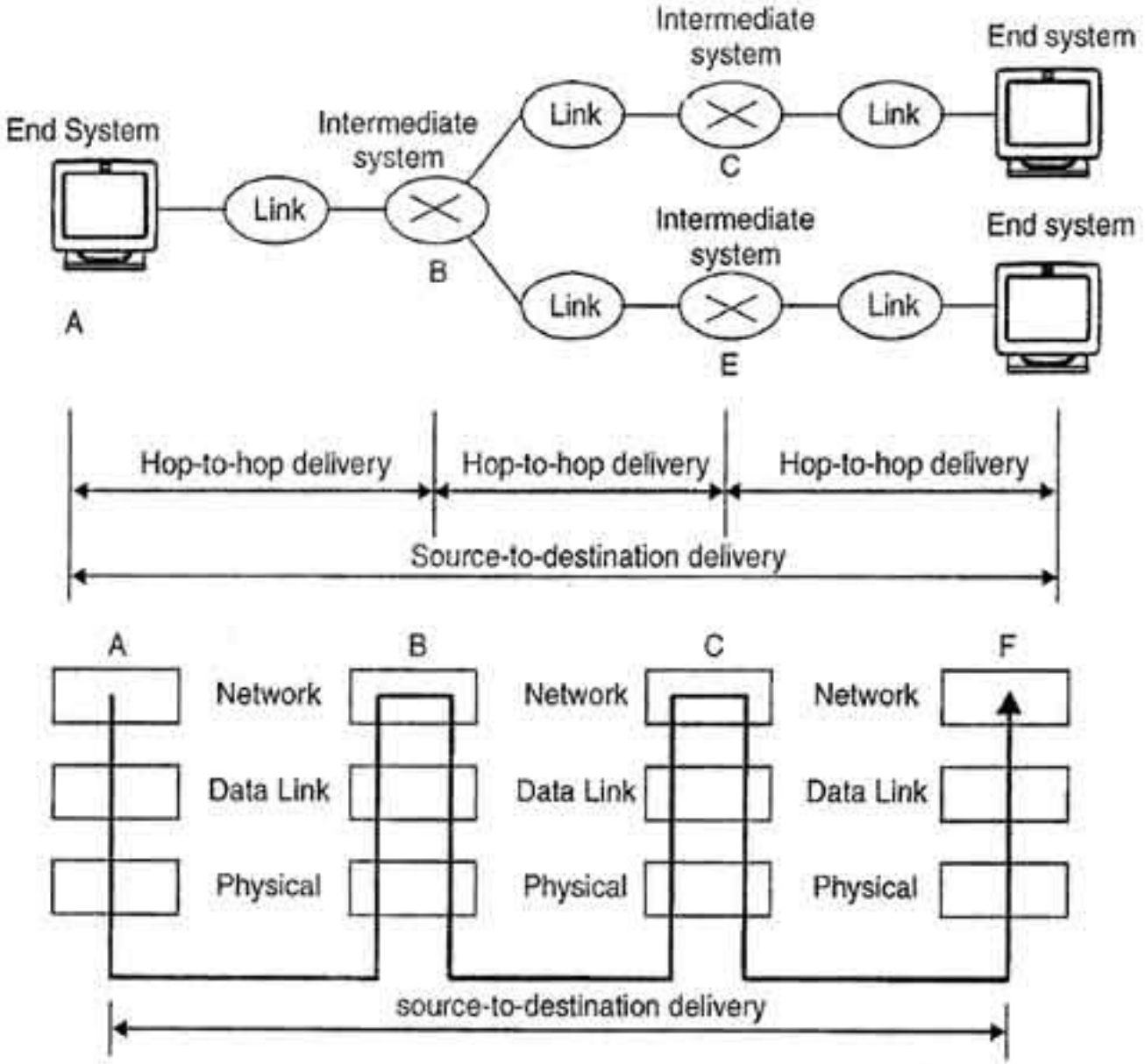
Routing : Independent networks are connected by devices (routers) route the packets to their destination.

Source-to-Destination Host delivery of packets across multiple networks.

Protocols : IP, ARP, RARP, ICMP, IGMP




Mobile Network
National or Global ISP
Network
Data link
Physical
End system H1
Application
Transport
Network
Data link
Physical
Router R1
Network
Data link
Physical
Home Network
Local or Regional ISP
Network
Data link
Physical
Network
Data link
Physical
Router R2
Network
Data link
Physical
Company Network
End system H2
Application
Transport
Network
Data link
Physical



Source to Destination Delivery by Network Layer

Transport Layer

Process-to-Process delivery of message

Service point addressing (port address) : network layer gets each packet to the correct computer and transport layer gets the entire message to the correct process on computer.

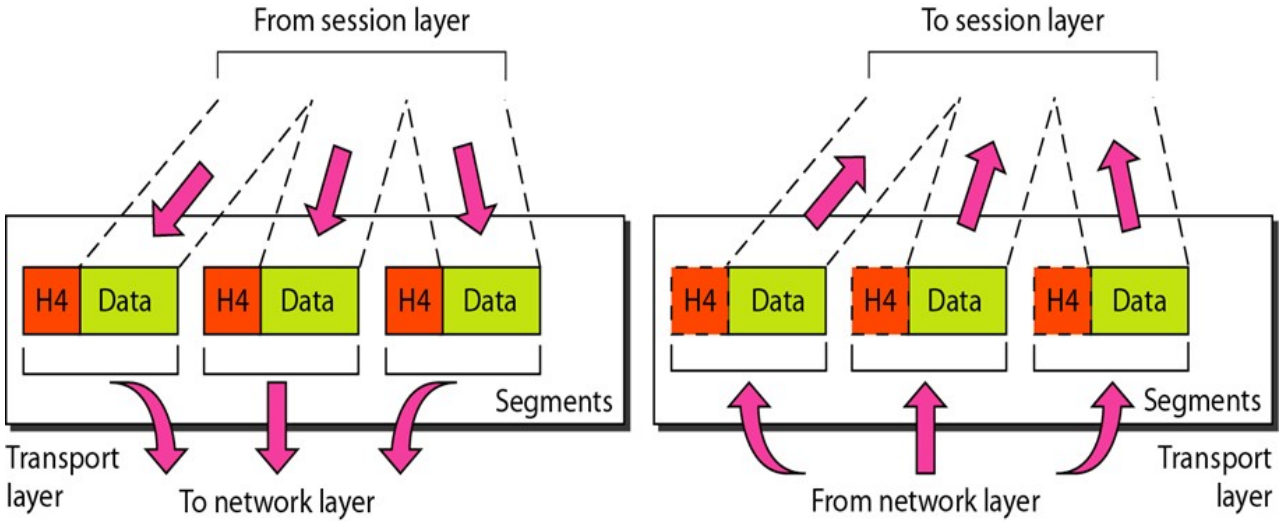
Segmentation (with **sequence number**) **and reassembly :** message coming from session layer divided into segments and sequence number is given which enable the reassemble the message at the destination.

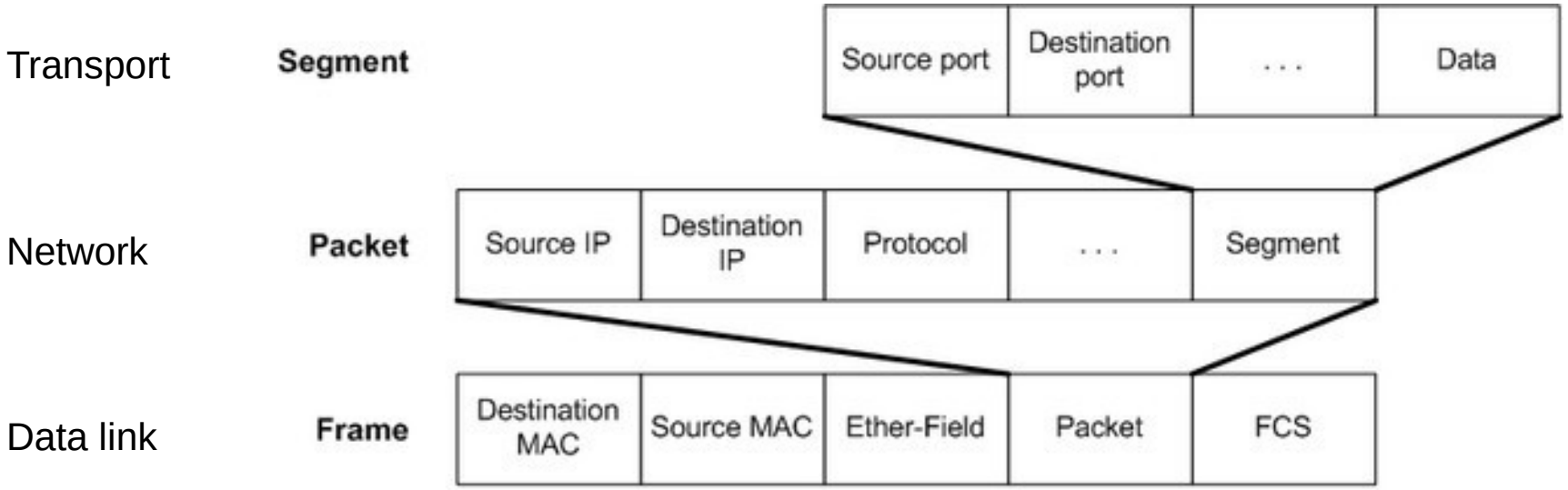
Connection control – Transport layer is either connection less or connection oriented.

Flow control and Error Control is performed process to process rather than across a single link as performed by data link layer. Error correction is usually achieved through retransmission.

Protocols : TCP , UDP, SCTP

Transport layer





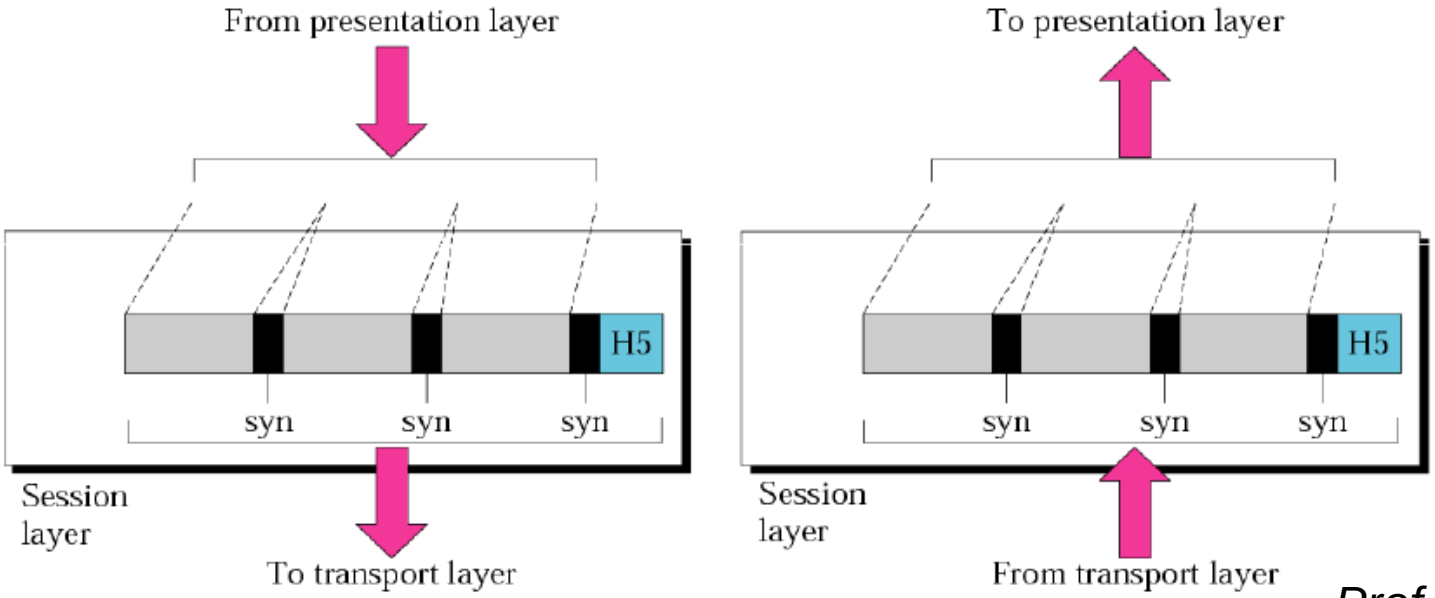
Session Layer

Dialog controller : It allows the communication between two processes either in half duplex or full duplex

Synchronization : The session layer add checkpoints (synchronization points) after some pages.

Example : file of 2000 pages and checkpoints add after every 100 pages. If page 523 crash then only 501 to 523 need to resent. Pages previous to 501 need not to be resent.

To establish, manage and terminate sessions



Presentation Layer

Translation : Different computers use different encoding system. Presentation layer is responsible for interoperability between these different encoding system.

Encryption and Decryption for privacy maintain by presentation layer.

Compression : Important in the transmission of multimedia such as text, audio and video.

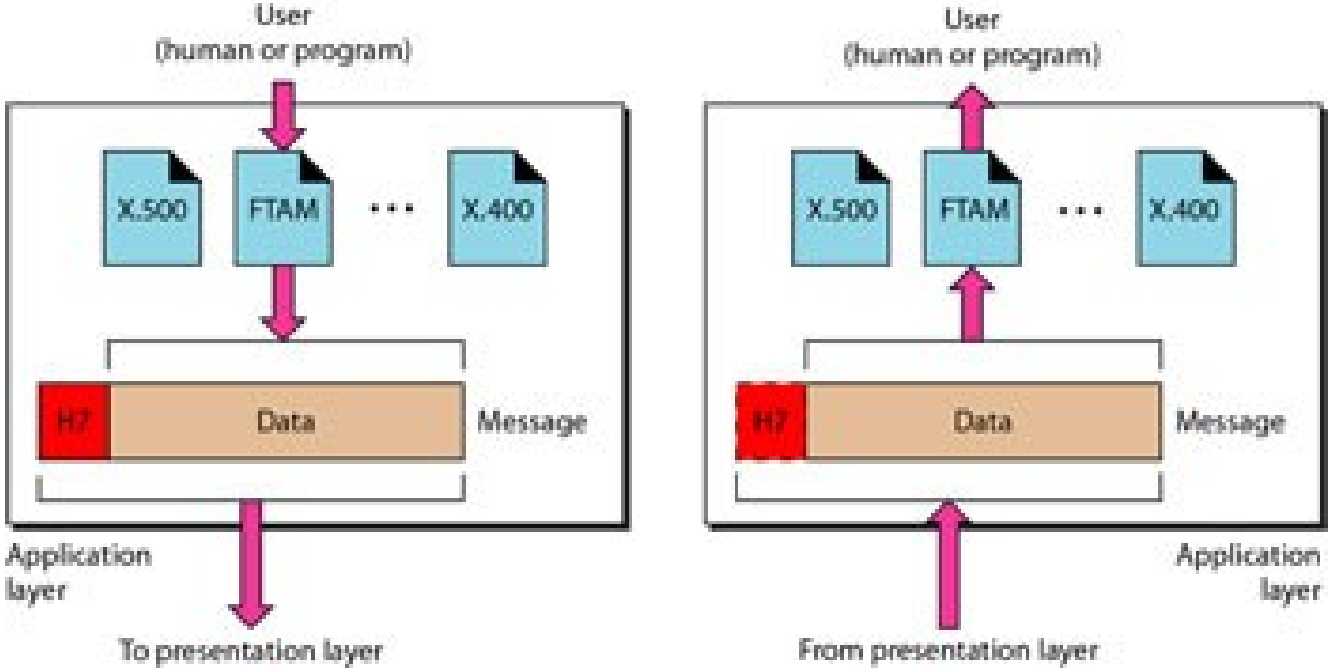
Application Layer

User interfaces to access the network.

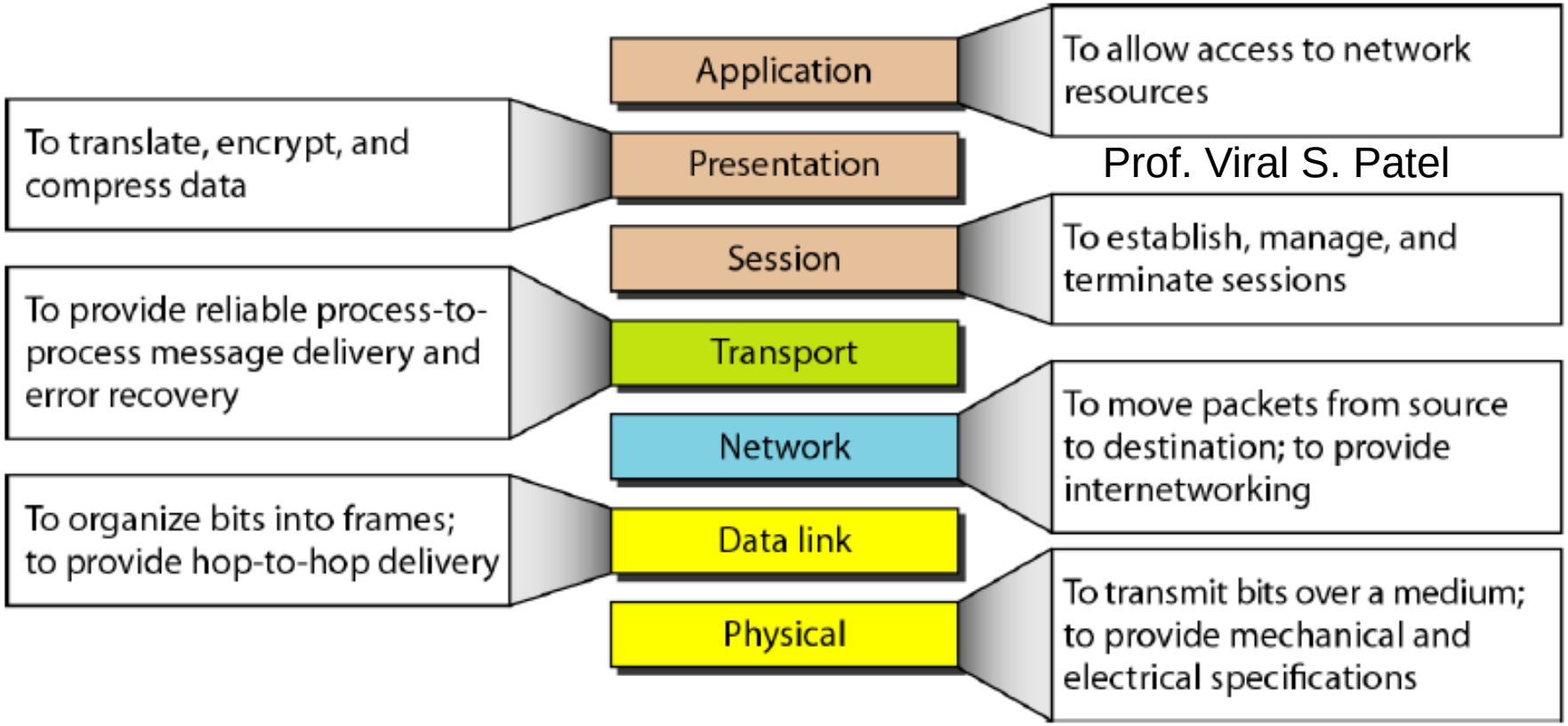
Network virtual terminal allows a user to log on to a remote host.

Message-handling services (X.400) , Directory services (X.500), File transfer, access and management (FTAM).

Directory services provide to access distributed database



Summary of OSI layers



Prof. Viral S. Patel

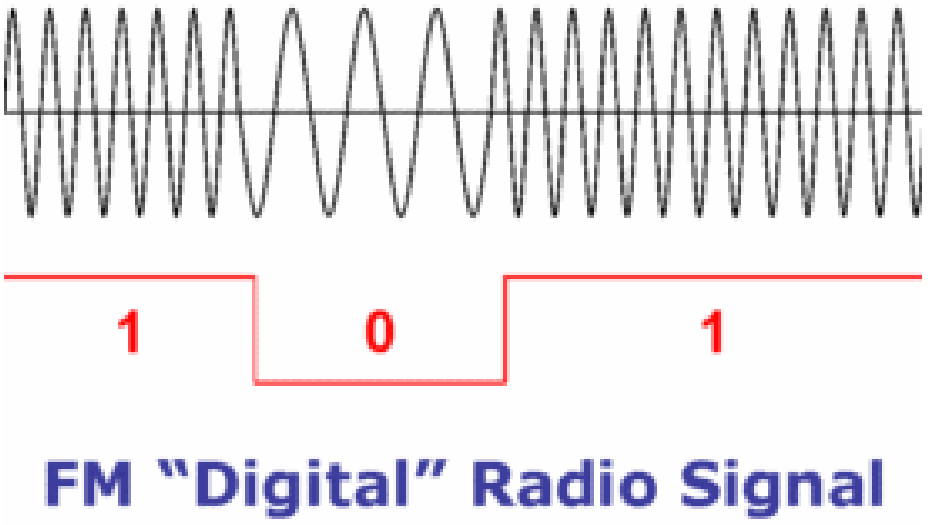
Digital and Analog Data

Analog Data refers to information that in the form of signal one which has a value that varies smoothly.

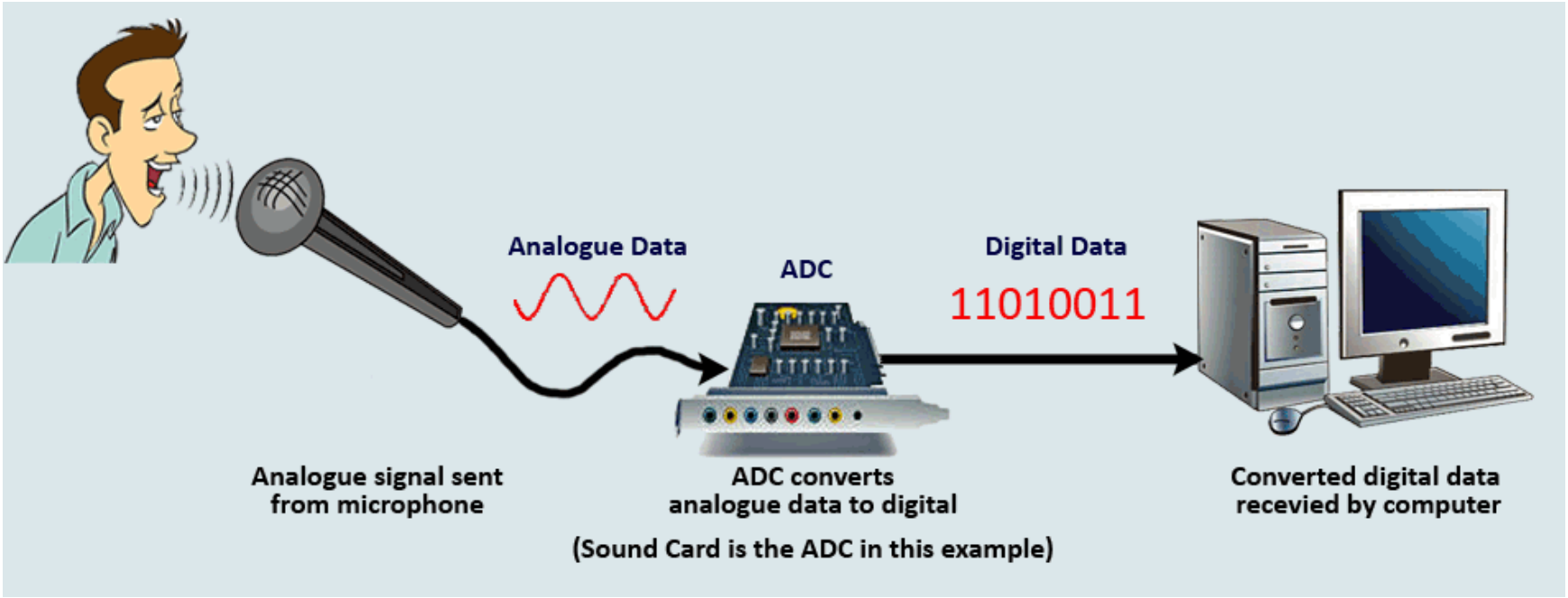
Example : Human Voice take on continuous values

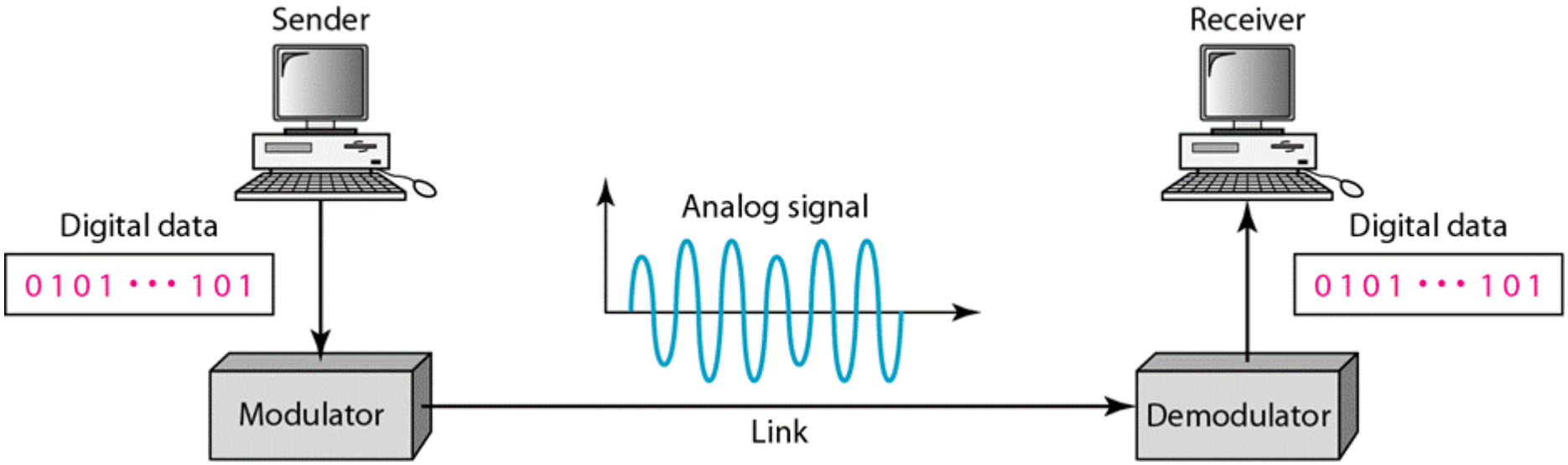
Digital Data are discrete, discontinuous representations of information.

Example : Data stored in Computer memory in the form of 0s and 1s

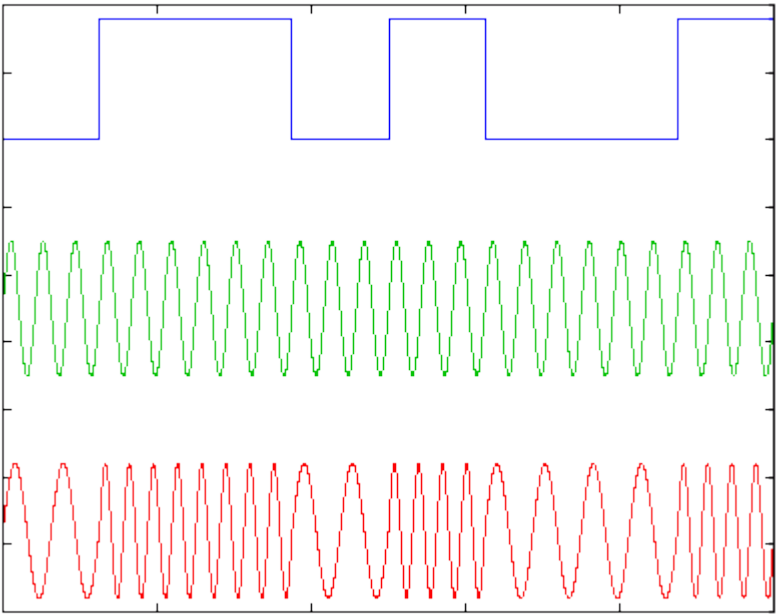


Digital and Analog Data

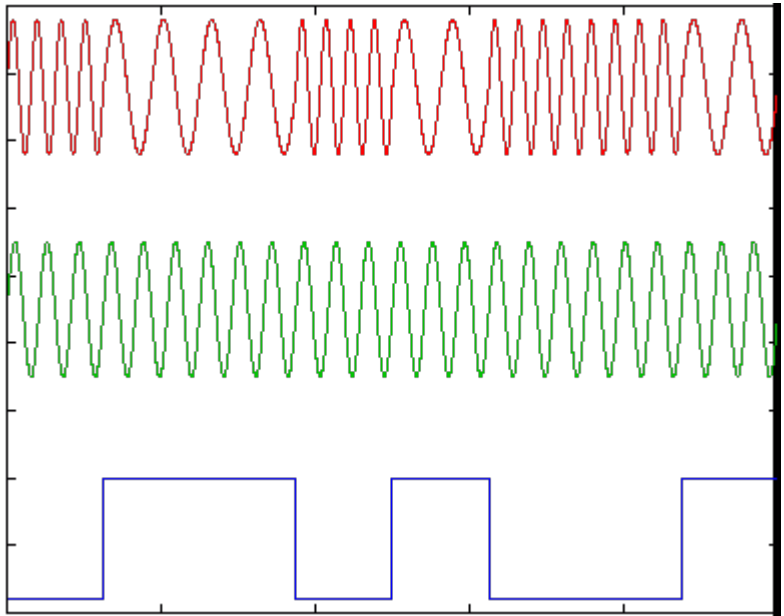




Prof. Viral S. Patel

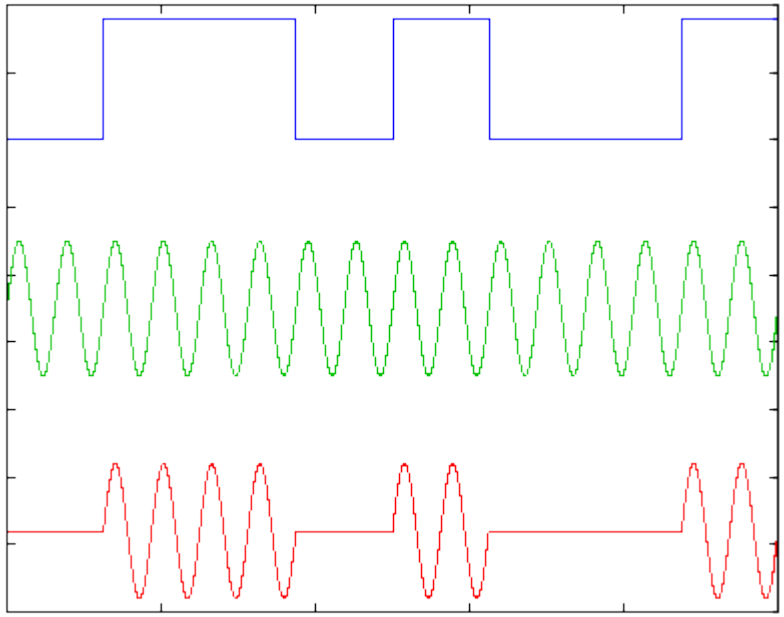


Frequency Modulation (FM)

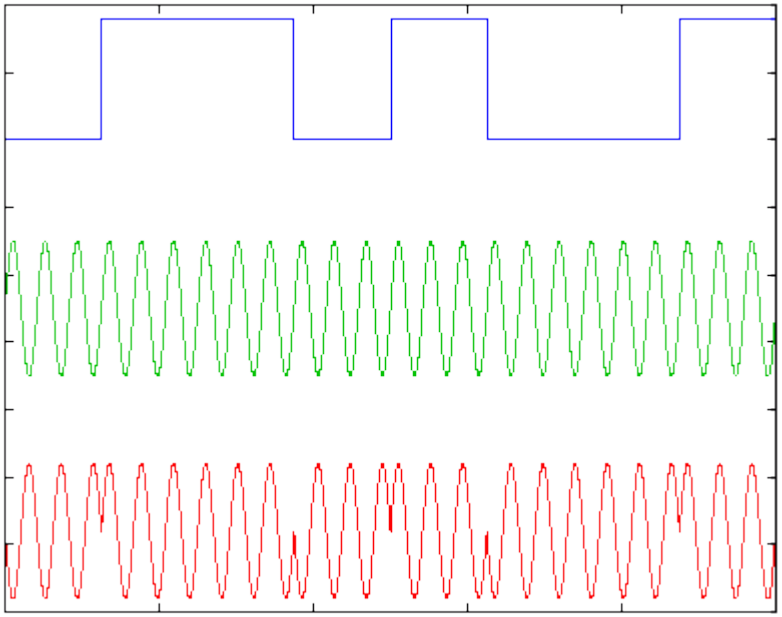


Digital and Analog Data

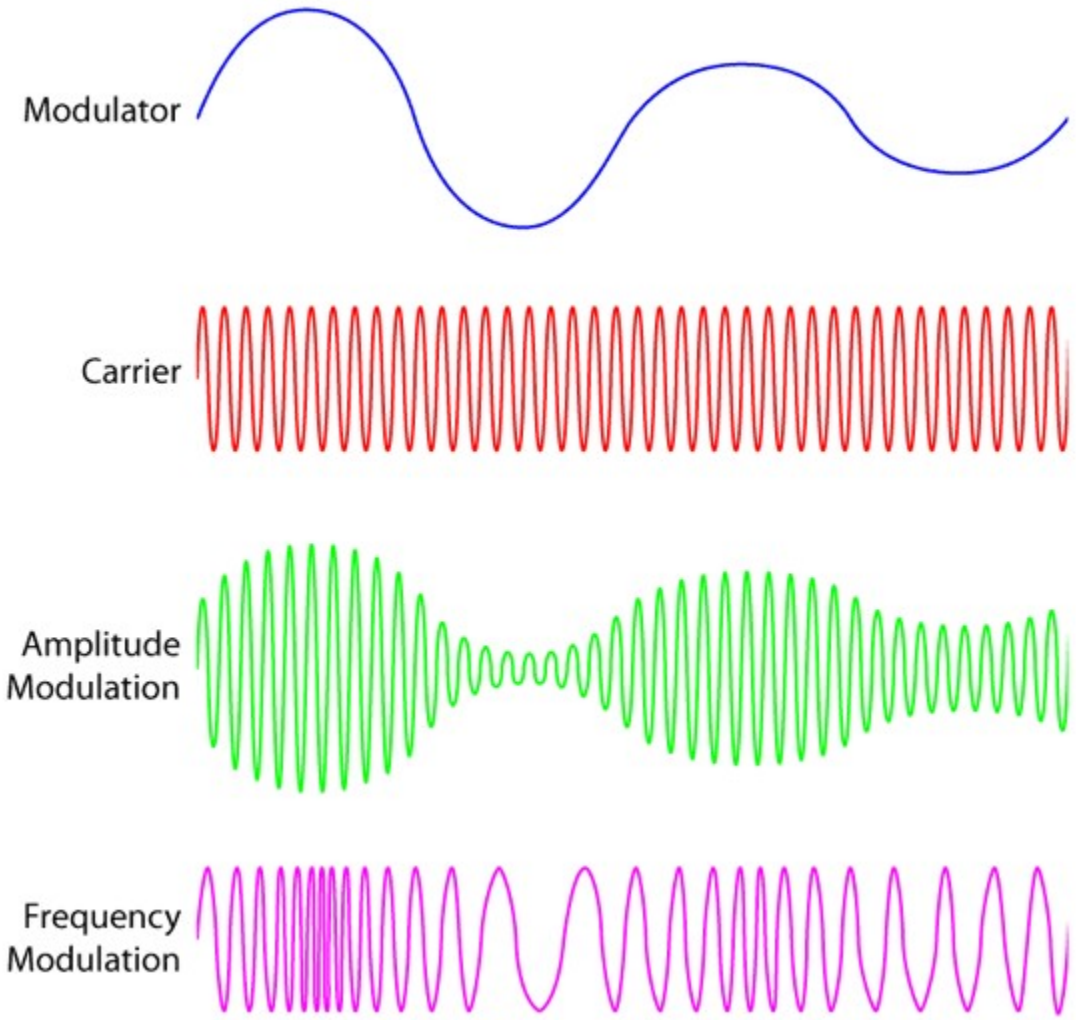
Amplitude Modulation



Phase Modulation



Modulation – AM & FM



Prof. Viral S. Patel

Prof. Viral S. Patel

Periodic signal : Complete a pattern within a measurable time frame called a period and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle.

Non-periodic signal : changes without exhibiting a pattern or cycle that repeats over time.

Period : It refers to the amount of time, in seconds, a signal need to complete 1 cycle.

Frequency : It refers to the number of periods in 1 s.

$$f = 1 / T \quad \text{or} \quad T = 1 / f$$

Frequency and period are inverse of each other.

Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (µs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

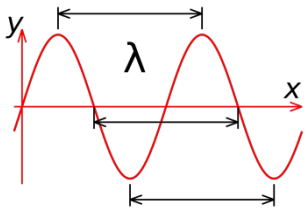
Wavelength : The wavelength is the distance a simple signal can travel in period. The wavelength is depend on both the frequency and the medium.

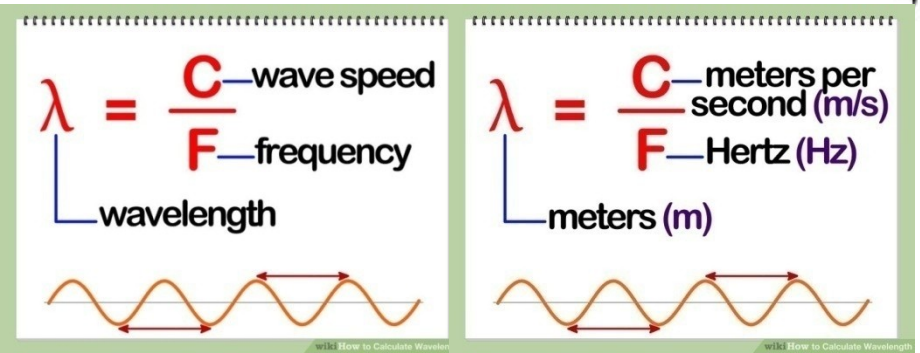
Wavelength

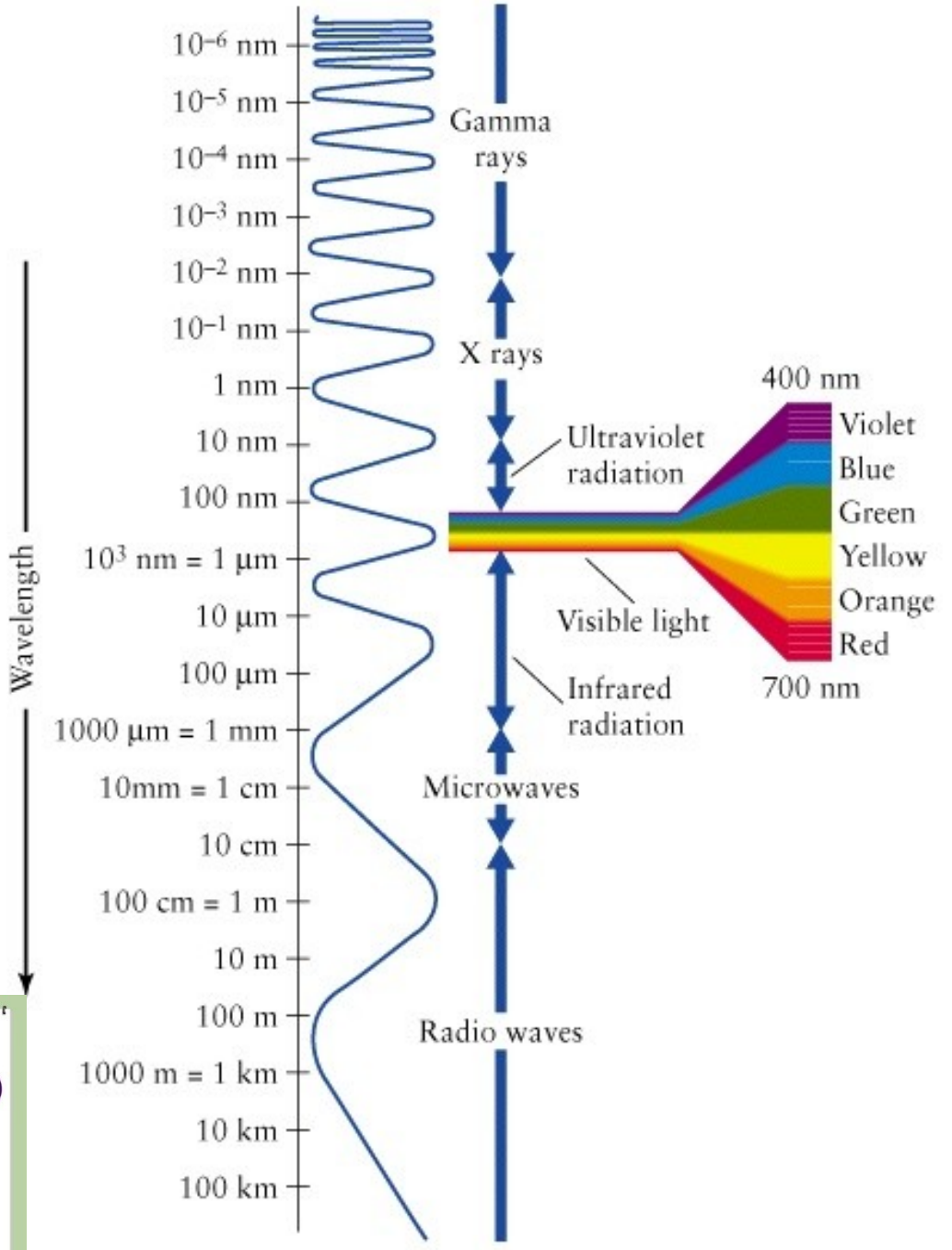
= Propagation speed * period

or

= Propagation speed / frequency







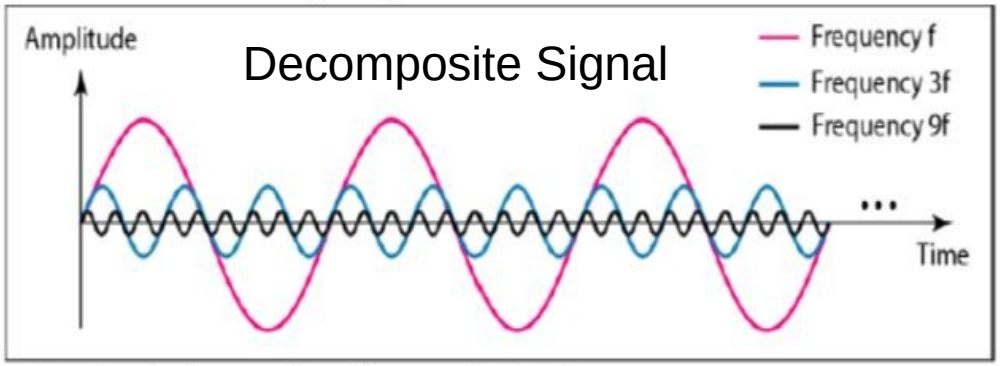
Prof. Viral S. Patel

Composite Signals :

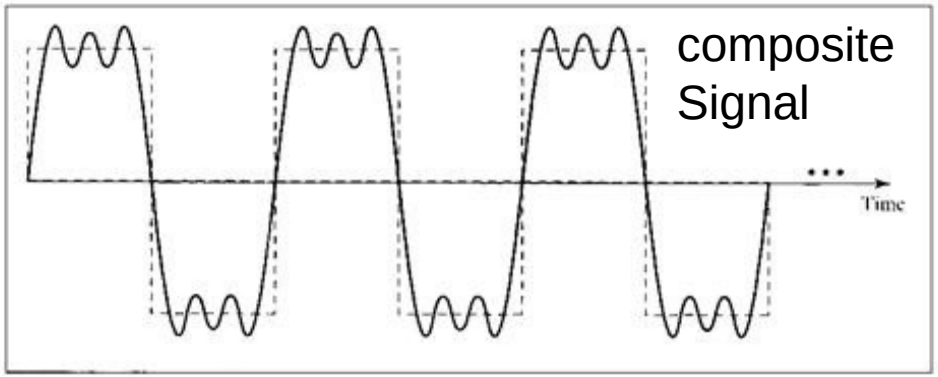
A single-frequency sine wave is not useful in data communication; we need to send a composite signal, a signal made of many simple sine waves.

According to Fourier analysis, any composite signal is a combination of **simple sine waves with different frequencies**, amplitudes and phases.

Prof. Viral S. Patel



a. Time-domain decomposition of a composite signal



If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composition signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.

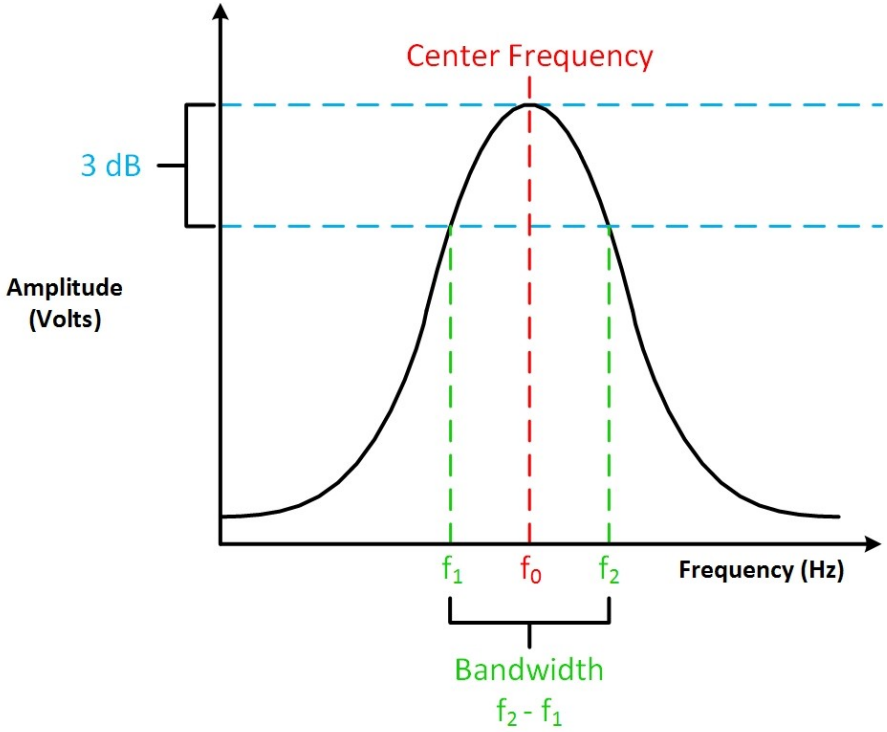
Prof. Viral S. Patel

Bandwidth : The **range of frequencies** contained in a composite signal is its bandwidth. The bandwidth is normally a difference between two numbers.

Example : if a composite signal contains frequencies between 1000 and 5000, its bandwidth is 5000 – 1000 = 4000

[***Note** : The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.]

Prof. Viral S. Patel



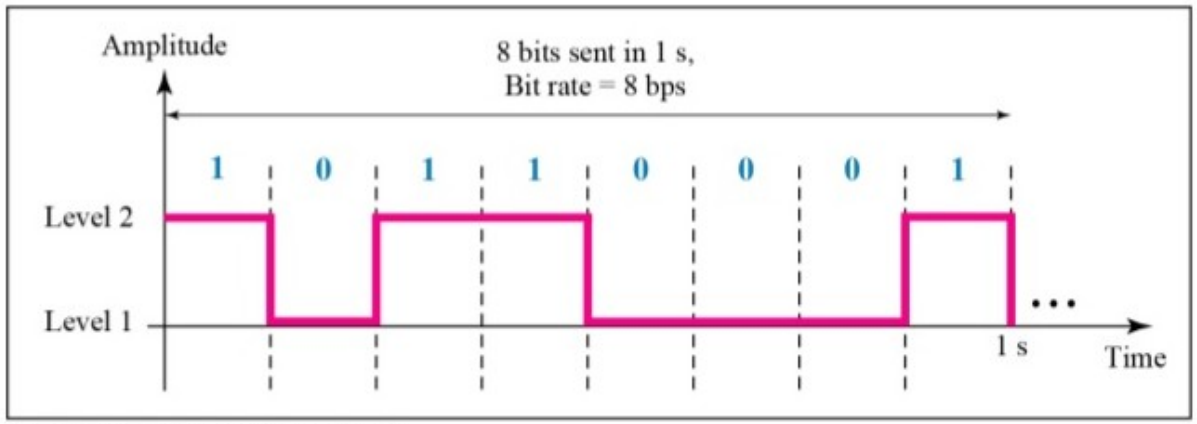
Bandwidth = f2 – f1. (Hz)

➔The bandwidth of a periodic signal contains all integer frequencies.

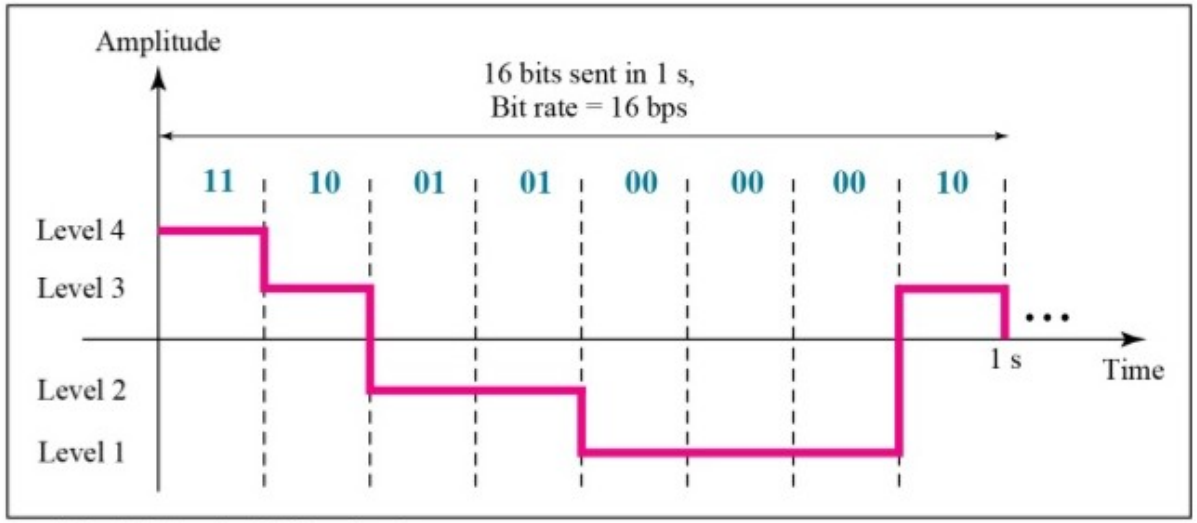
➔The bandwidth of a non-periodic signals contain the frequencies are continuous.

Prof. Viral S. Patel

Bit Rate : Most digital signals are non periodic and thus period and frequency are not appropriate characteristics. Another term – bit rate – is used to describe digital signals. The bit-rate is the **number of bits sent in 1s**, expressed in **bits per second (bps)**



a. A digital signal with two levels



b. A digital signal with four levels

Number of bits per level = $\log_2 L$

Example : Digital signal has eight level then number of bits per level is $\log_2 8 = 3$

Bit length : It is the distance one bit occupies on the transmission medium.

Bit length = propagation speed x bit duration

Data Rate Vs Signal Rate (or Data Element Vs Signal Element):

Data Rate (bit rate): The data rate defines the number of data elements (bits) send in 1s. The unit is **bits per second (bps)**. The data rate is sometimes called the **bit rate.**

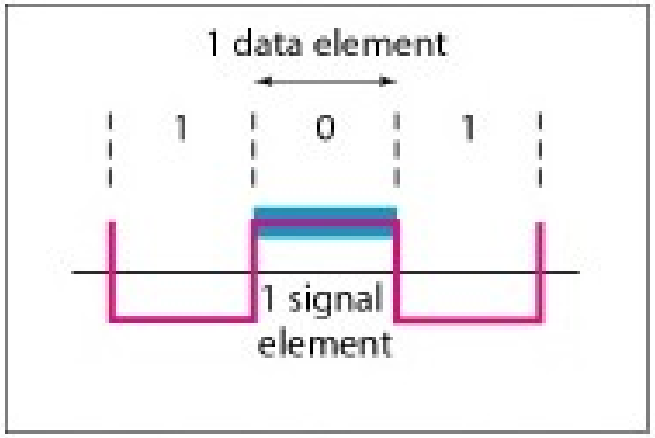
Signal Rate (baud rate): Baud rate refers to the number of signal or symbol changes per second. The signal rate is sometimes called the **pulse rate**, the **modulation rate** or the **baud rate**.

In digital data communications, a signal element carries data elements. In other words, data elements are what we need to send and signal elements are what we can send.

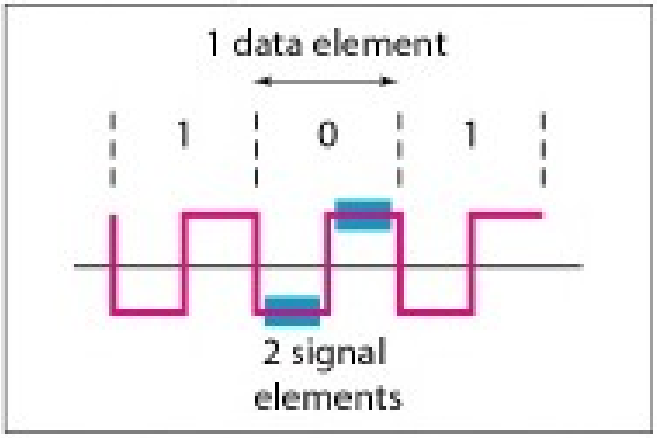
Data elements are being carried and signal elements are the carriers.

Our goal in Data communications is to increase the data rate while decreasing signal rate. Increasing the data rate increases the speed of transmission; decreasing the signal rate decreases the bandwidth requirement. Example : vehicle-people analogy.

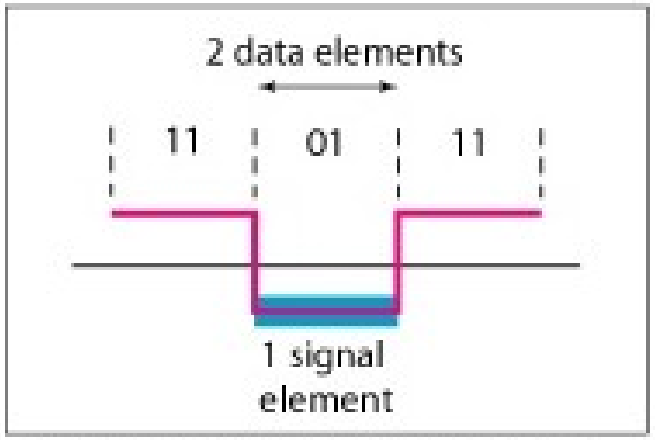
We define a ratio r which is the number of data elements carried by each signal element. Figure shows several situations with different values of r.



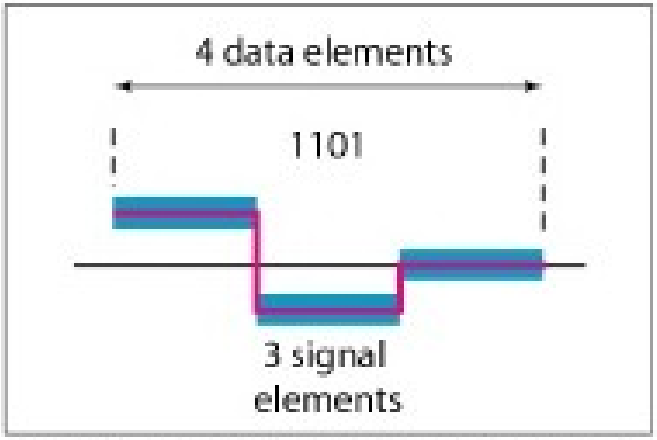
a. One data element per one signal element (r = 1)



b. One data element per two signal elements $\left(r = \frac{1}{2}\right)$



c. Two data elements per one signal element (r = 2)



d. Four data elements per three signal elements $\left(r = \frac{4}{3}\right)$

Relationship between data rate and signal rate as

S = c x N x (1 / r) baud

N is the data rate (bps)
c is the case factor (worst, best and average case)
S is the number of signal elements
r is the previously defined factor

Transmission Impairment (Attenuation, Distortion, Noise)

Attenuation : Attenuation means a loss of energy.

- When a signal simple or composite travels through a medium, it loses some of its energy in overcoming the resistance of the medium. Some of the electrical energy in the signal is converted to heat.

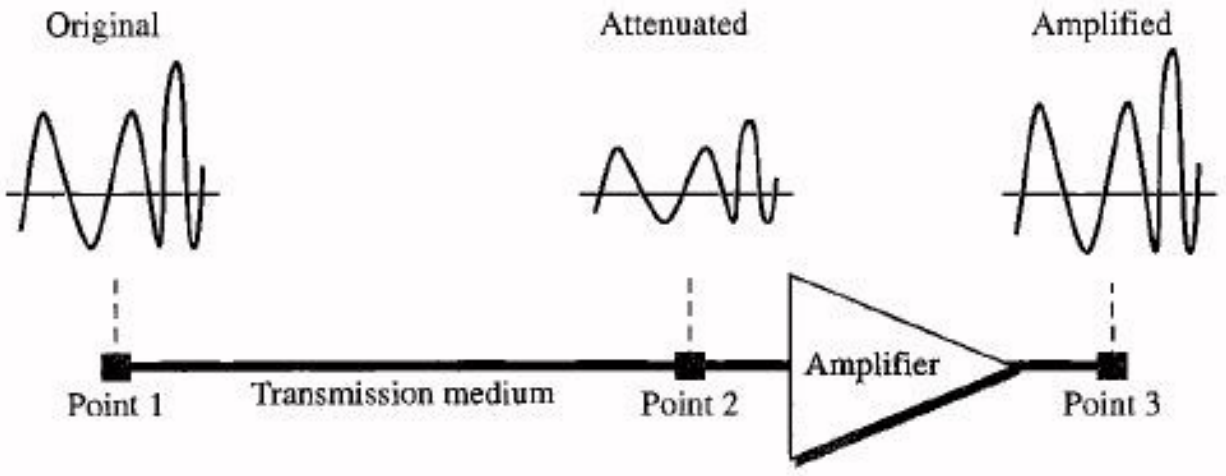
To compensate for this loss, amplifiers are used to amplify the signal.

dB = 10 $\log_{10}$(P2/P1)

P1 is power at point 1
P2 is power at point 2

dB = 20 $\log_{10}$(V2/V1)

V1 and V2 is voltage

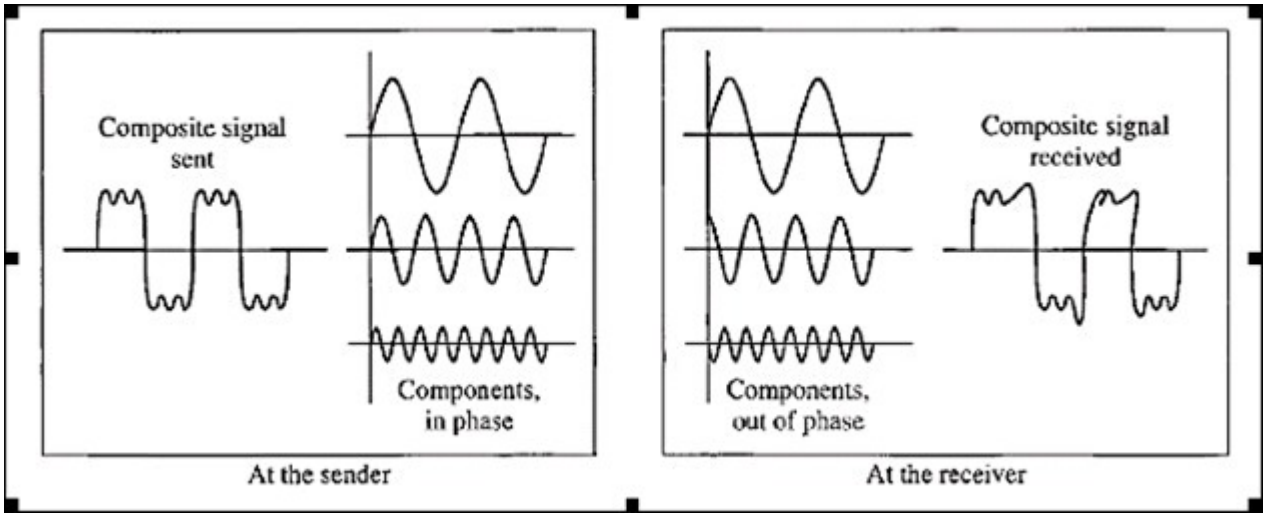


- The decibel (dB) measures the relative strengths of two signals or one signal at two different points.
- Note that the decibel is negative if a signal is attenuated and positive if a signal is amplified.

Distortion : Distortion means that the signal changes its form or shape. Distortion can occur in a composite signal made of **different frequencies.**

- Each signal component has its **own propagation speed** through a medium and therefore, its own delay in arriving at the final destination.

- **Difference in delay** may create a **difference in phase** if the delay is not exactly the same as the period duration.
- In other words, signal components the receiver have phase difference from what they had at the sender. The shape of the composite signal is therefore not the same.



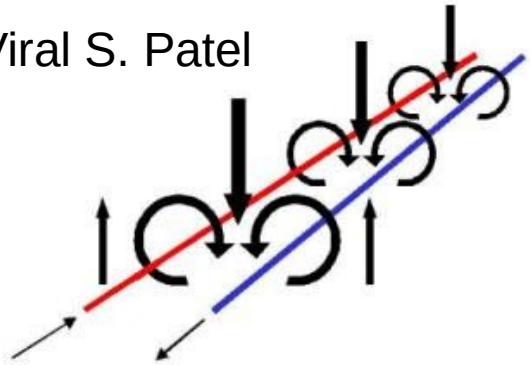
Noise :

Noise is another cause of impairment. Several types of noise, such as thermal noise, induced noise, crosstalk, and impulse noise, may corrupt the signal.

➔**Thermal noise** is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter.

➔**Induced noise** comes from sources such as motors and appliances. These devices act as a sending antenna, and the transmission medium acts as the receiving antenna.

➔**Crosstalk** is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna.



➔**Impulse noise** is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on.

SNR (signal-to-noise ratio) :

To find the theoretical bit rate limit, we need to know the ratio of the signal power to the noise power. The signal-to-noise ratio is defined as

SNR = average signal power / average noise power

- A high SNR means the signal is less corrupted by noise; a low SNR means the signal is more corrupted by noise.

- Because SNR is the ratio of two powers, it is often described in decibel units,

$$\mathbf{SNR_{dB} = 10 \log_{10} SNR}$$

Data Rate limit :

A very important consideration in data communication is how fast we can send data, in bits per second, over a channel.

- Data rate depends on three factors :

1. The **bandwidth** available
2. The **level** of the signals we use
3. The **quality** of the channel (the level of noise)

- Two theoretical formulas were developed **to calculate the data rate :**

one by **Nyquist for a noiseless channel**,

another by **Shannon for a noisy channel**.

Noiseless Channel : Nyquist Bit Rate

Nyquist Bit Rate = 2 * bandwidth * $\log_2 L$

Bandwidth is the bandwidth of channel

L is the number of signal levels used to represent data

Bit rate in bits per second

Increasing the levels of a signal may reduce the reliability of the system as we **impose the burden on the receiver**.

Prof. Viral S. Patel

Noisy Channel : Shannon Capacity

Shannon Capacity = bandwidth * $\log_2(1+SNR)$

Bandwidth is the bandwidth of channel

SNR is the signal to noise ratio

This formula **defines a characteristics of the channel**, not the method of transmission.

Performance (Bandwidth, Throughput, Latency, Jitter)

Bandwidth : One characteristic that measures network performance is bandwidth.

However, the term can be used in two different contexts with two different measuring values :

bandwidth in **hertz** and bandwidth in **bits per second**

Bandwidth in Hertz :

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass.

For example, we can say the bandwidth of a subscriber telephone line is 4 kHz

Bandwidth in Bits per Seconds :

The term bandwidth can also refer to the number of bits per second that a channel, a link, or even a network can transmit.

For example, the bandwidth of a Fast Ethernet network is a maximum 100 Mbps. This means that this network can send 100 Mbps.

Throughput

The Throughput is a measure of how fast we can actually send data through a network.

Bandwidth in bits per second and throughput are different.

Example : **A** link may have a bandwidth of **B bps**, but we can only send **T bps** through this link with **T always less than B**.

In other words, the bandwidth is a potential measurement of a link and the throughput is an actual measurement of how fast we can send data.

For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

Latency (Delay)

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

➔We can say that latency is made of **four components** :

Latency = propagation time

+ transmission time

+ queuing time

+ processing delay.

Propagation time : Propagation time measures the time required for a bit to travel from the source to the destination.

propagation time = Distance / Propagation speed

It is depend on medium and frequency of signal. For example, in vacuum, light is propagated with a speed of 3×10^8 m/s. It is lower in air; it is much lower in cable.

Transmission time : Time between the first bit of message leaving the sender and the last bit arriving at the receiver. The time required for transmission of a message depends on the size of the message and the bandwidth of the channel.

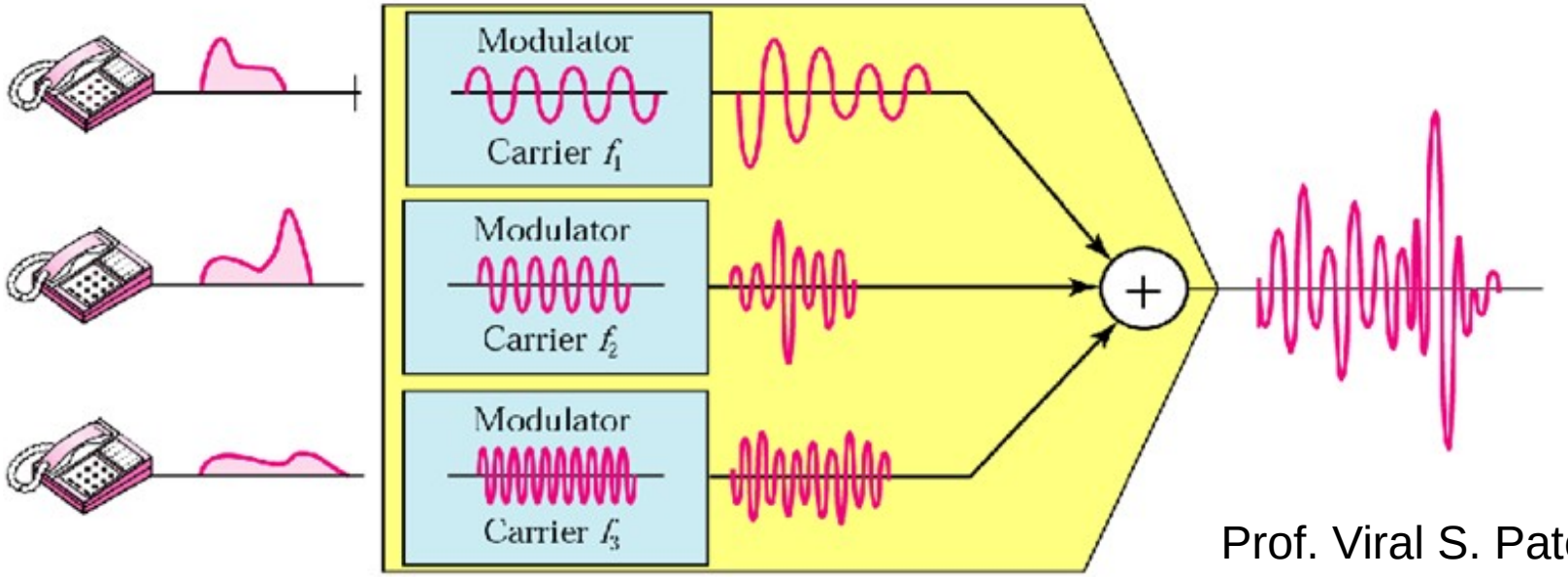
Transmission time = Message size / Bandwidth

Queuing Time : The time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor; it changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases.

Jitter : Jitter is a problem if different packets of data encounter **different delays** and the application using the data at the receiver site is time-sensitive (audio and video data, for example).

If the delay for the first packet is 20ms, for the second is 45 ms and for the third is 40 ms, then the **real-time application** that uses the packets endures jitter.

Frequency Division Multiplexing

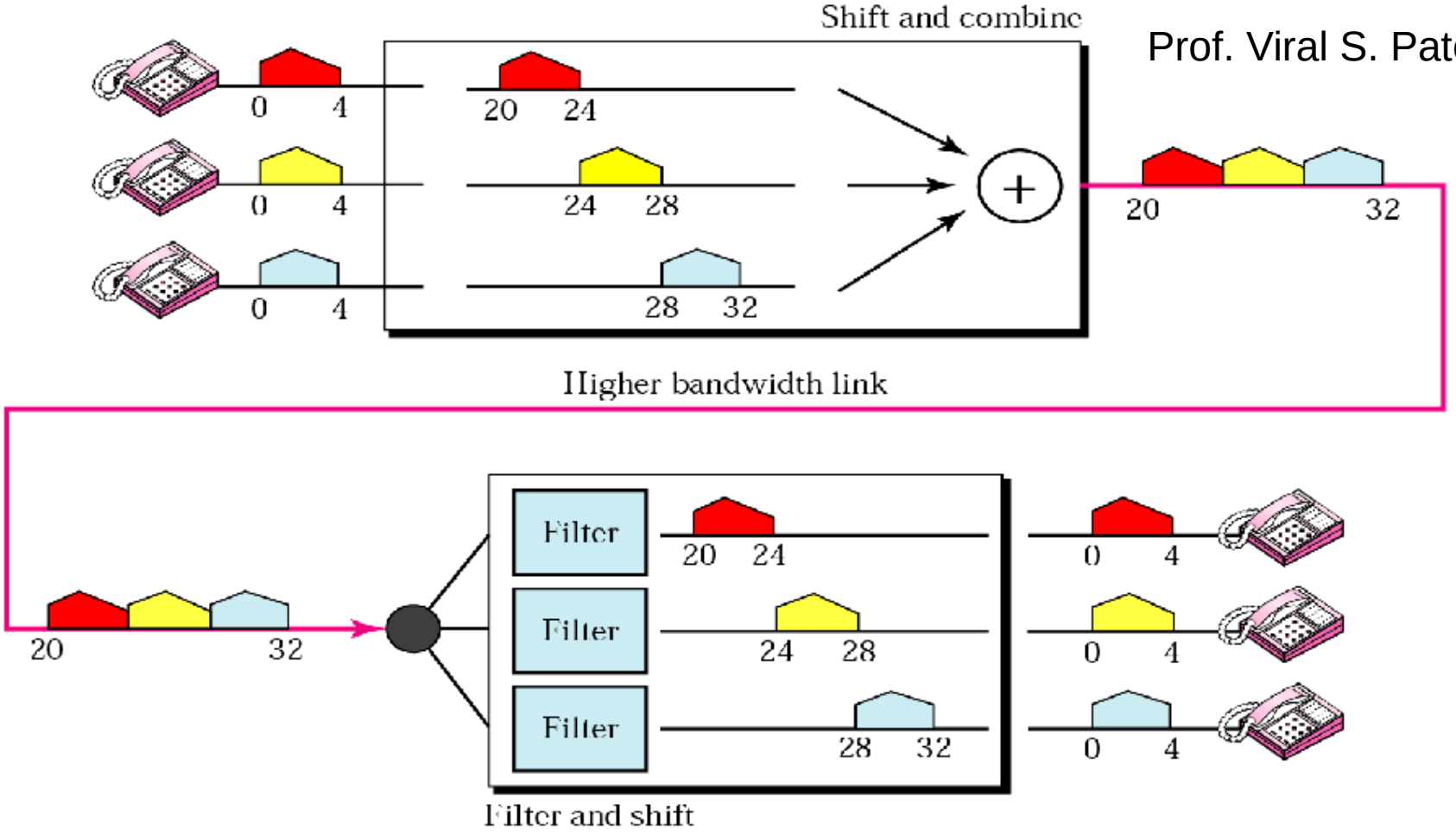


Prof. Viral S. Patel

Prof. Viral S. Patel

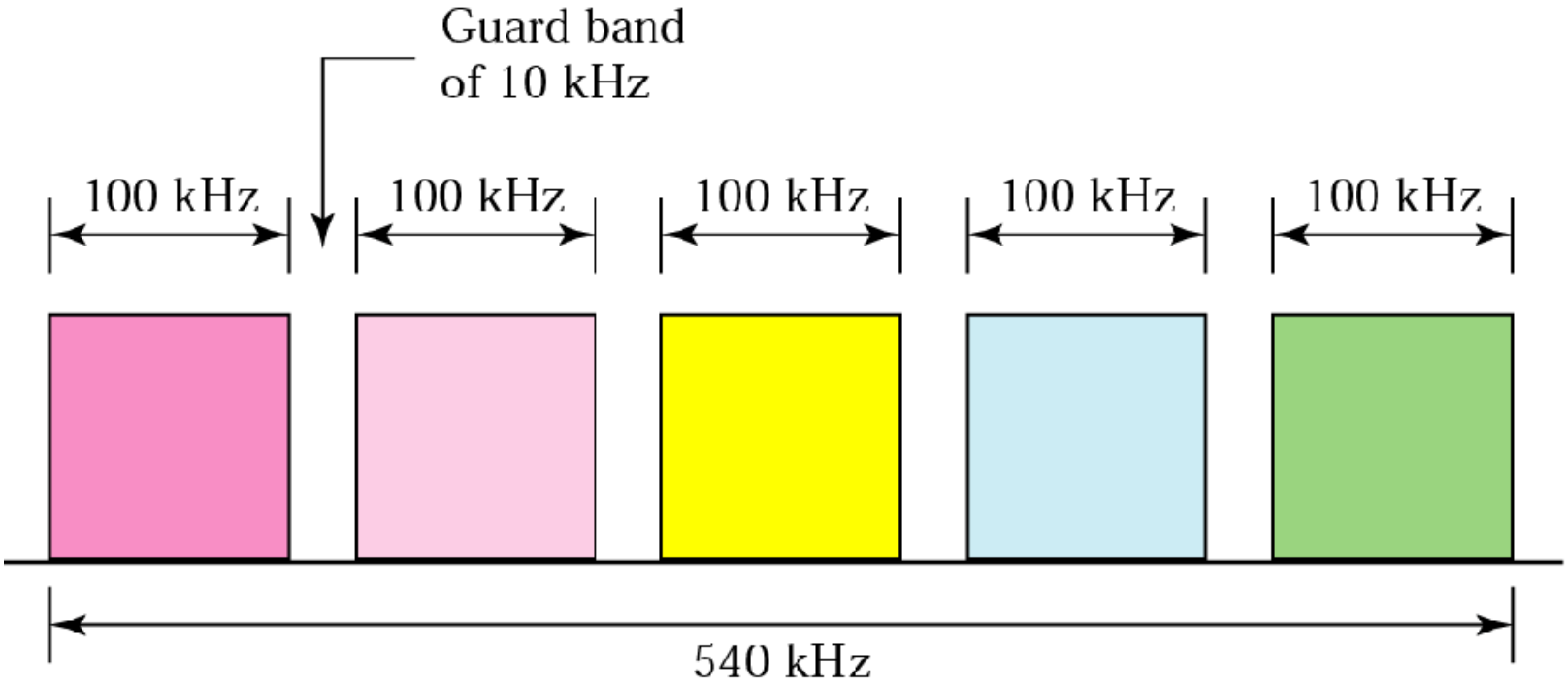
Question

—Assume that a voice channel occupies a bandwidth of 4 KHz. We need to combine three voice channels into a link with a bandwidth of 12 KHz, from 20 to 32 KHz. Show the configuration using the frequency domain without the use of guard bands.



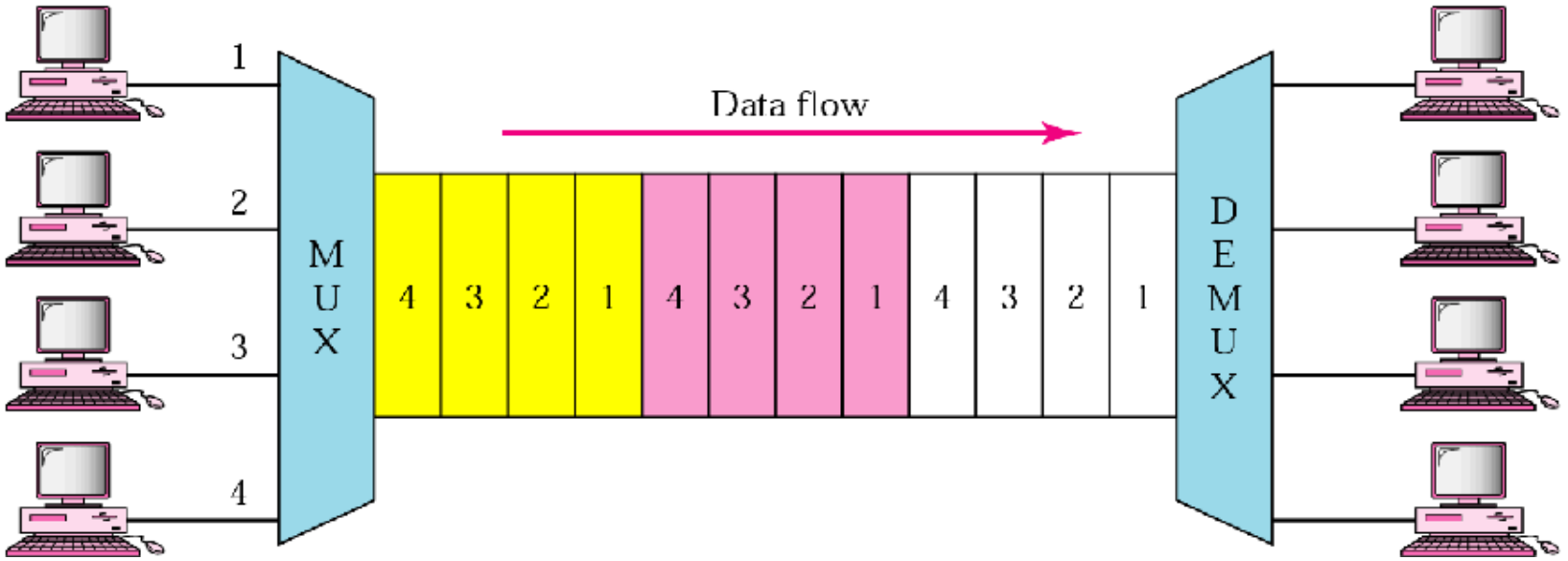
Prof. Viral S. Patel

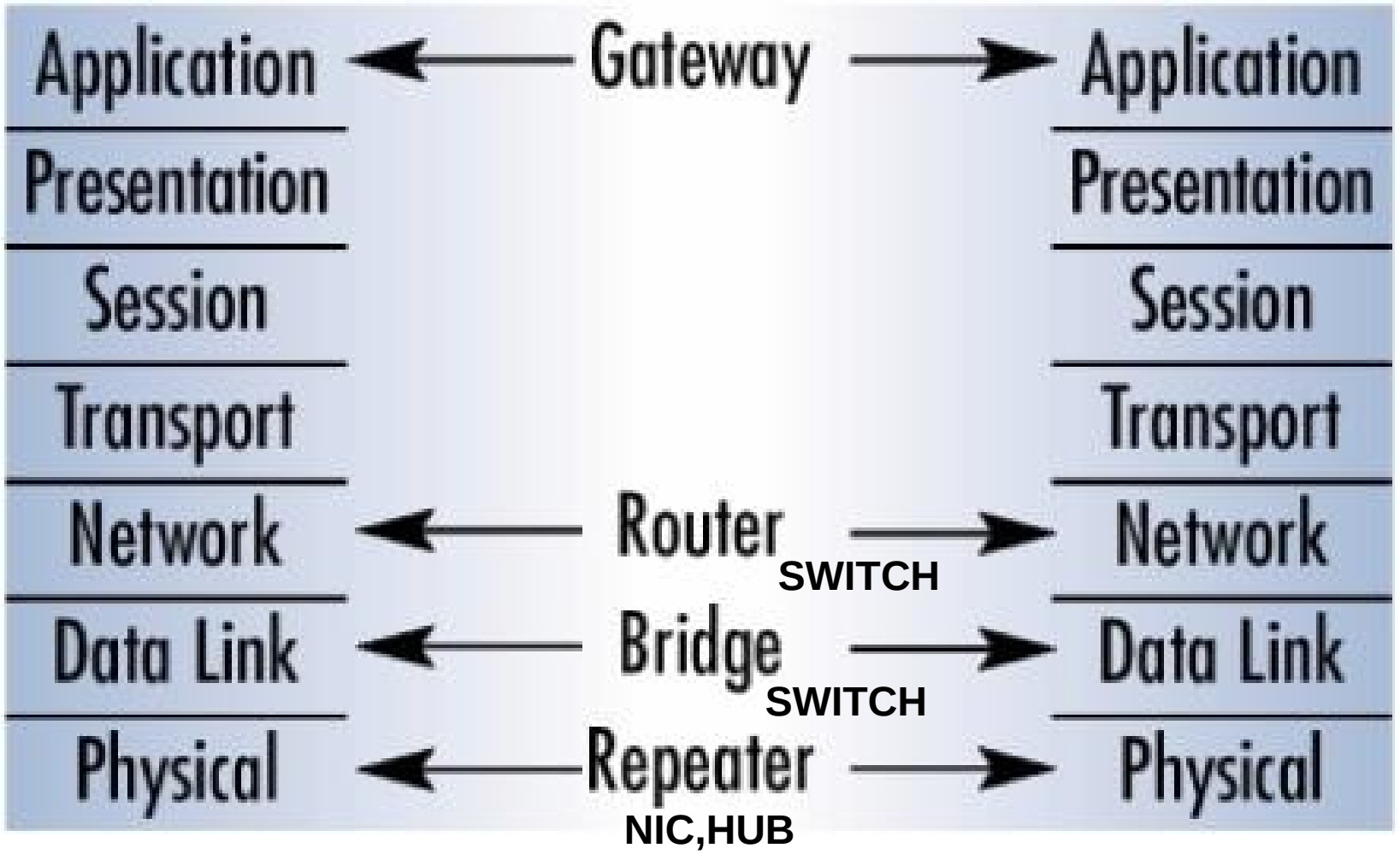
Frequency Division Multiplexing



Time Division Multiplexing

Prof. Viral S. Patel




Application
Gateway
Application
Presentation
Presentation
Session
Session
Transport
Transport
Network
Router
Network
SWITCH
Data Link
Bridge
Data Link
SWITCH
Physical
Repeater
Physical
NIC,HUB

NIC (Network Interface Card) :

It is a computer hardware component designed to allow computers to communicate over a computer network.

The NIC provides the physical **interface between computer and cabling**. It prepares data, sends data, and controls the flow of data. It can also receive and translate data into bytes for the CPU to understand.

➔It communicates at the **Physical layer** of the OSI model and comes in many shapes and sizes.

➔Most motherboards today come equipped with a network interface card in the form of a controller, with the hardware built into the board itself, eliminating the need for a standalone card.

Different NICs are distinguished by the PC bus type and the network for which they are used.

➔ Following **factors** should be taken into consideration when choosing a NIC :

- Preparing data
- Sending and controlling data
- Configuration
- Drivers
- Compatibility
- Performance

➔**Preparing Data :** In computer data moves along buses in parallel. But on a network cable, data travels in a single stream

This difference can cause problems transmitting and receiving data, because the paths traveled are not the same.

It is the NIC's job to translate the data from the computer into signals that can flow easily along the cable. It does this by **translating digital signals into electrical signals.**

➔**Sending and Controlling Data :** For two computers to send and receive data, the cards must agree on several things. These include the following :

- ➔The maximum **size** of the data **frames**
- ➔The **amount of data** sent before giving confirmation
- ➔The **time** needed **between transmission**
- ➔The **amount of** time needed to **wait** before sending confirmation
- ➔The amount of **data** a card can **hold**
- ➔The **speed** at which data **transmits**

If the cards can agree, then the sending of the data is successful.

If the cards can not agree, then the sending of data does not occur.

In order to send successfully send data on the network, you need to make sure the **network cards are of the same type** (All Ethernet or All Token Ring, etc) and they are connected to the same piece of cable. If you use cards of different types, neither of them will be able to communicate with the other.

➔Additionally, network cards can send data in either **full-duplex or half-duplex modes.**

Half-duplex communication means that between the sender and receiver, only one of them can transmit at any one time. In full-duplex communication, a computer can send and receive data simultaneously.

The main advantage to full-duplex over half-duplex communication is performance. Network cards can operate twice as fast (200 Mbps) in full-duplex mode than they do normally in half-duplex mode (100 Mbps).

Prof. Viral S. Patel

Configuration : The NIC's configuration includes things like manufacturer's **hardware address, IRQ (Interrupt Request) address, base I/O port address, and base memory address**. Some may also use **DMA channels** to offer better performance.

Each card must have a **unique hardware address**. If two cards have the same hardware addresses, neither one of them will be able

to communicate. For this reason, the IEEE committee has established

a standard for hardware addresses and assigns blocks of these addresses to NIC manufacturers, who then hard-wire the addresses into the cards.

➔**Token Ring cards** often have two memory addresses that must be excluded in reserved memory to work properly.

➔**<u>Drivers</u> :** For the computer to use the network interface card, it is very important to install the proper device drivers. These drivers communicate directly with the network redirector and adapter. They operate in the **Media Access Control** sublayer of the **Data Link Layer** of the OSI model.

➔**<u>PC Bus Type</u> :** When choosing a NIC, use one that fits the bus type of PC. If we have more than one type of bus in our PC (for example, a combination ISA/PCI), use a NIC that fits into the fastest

type (the PCI, in this case). This is especially important in servers, as the NIC can very quickly become a bottleneck if this guideline isn't followed.

Performance : The most important goal of the network adapter card is to optimize network performance and minimize the amount of time needed to transfer data packets across the network.

There are **several ways** of doing this, including assigning a DMA channel, using a shared memory adapter and deciding to allow bus mastering.

➔If the network card use **DMA channels**, then data can move directly from the card's buffer to the computer's memory, **bypassing the CPU.**

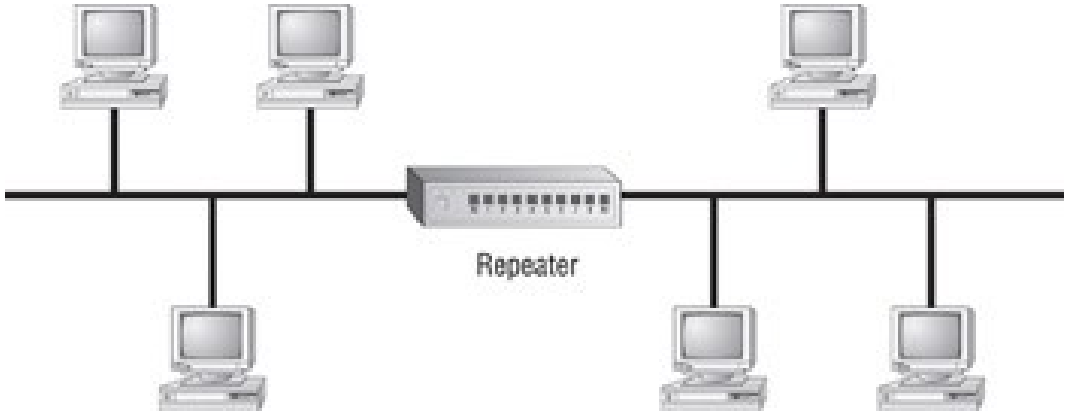
➔A **shared memory adapter** is a NIC that has its **own RAM**. This feature allows transfers to and from the computer to happen much more quickly, increasing the performance of the NIC. Shared system memory allows the NIC to **use a section of the computer's RAM** to process data.

➔**Bus mastering** lets the card **take temporary control** of the computer's bus to bypass the CPU and more directly to RAM. This is more expensive, but can improve performance by 20 to 70 percent.

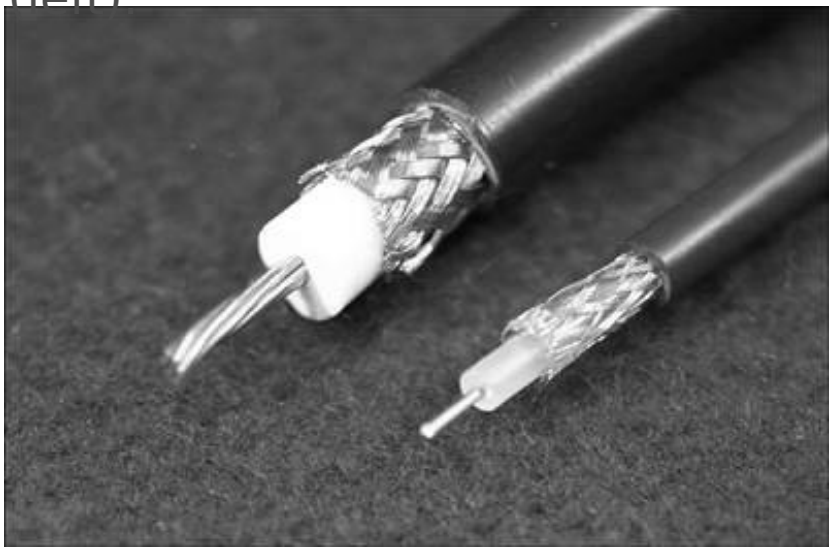
Each of these features can enhance the performance of a network interface card. Most cards today have at least one, or several, of these feature.

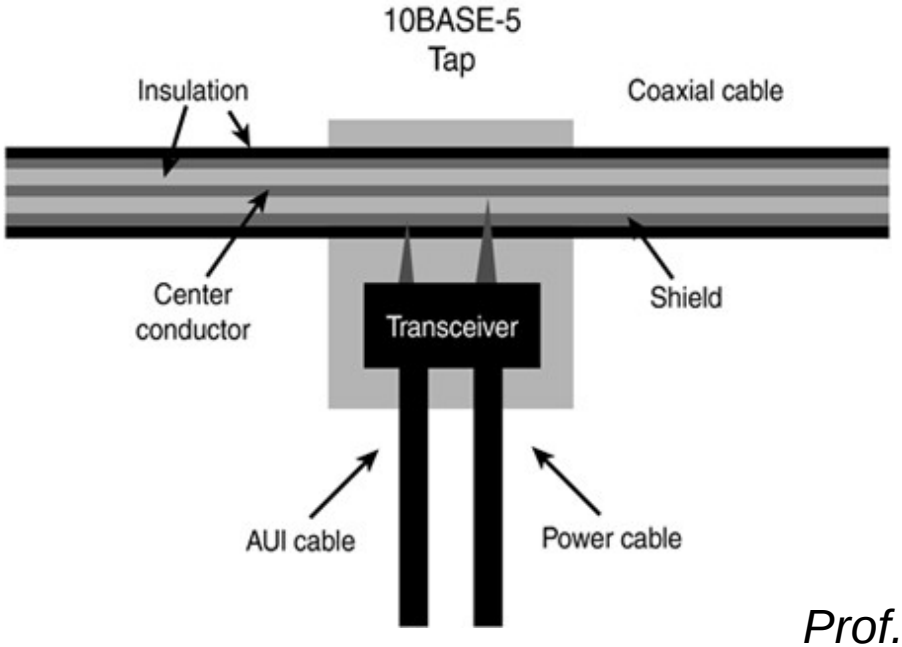
Repeaters :

- Repeaters work at the **physical layer** of the OSI reference model.
- Their job is to simply **amplifies an electrical signal's strength** so that it can travel farther across a wire.
- Being **passive** in nature, repeaters **do not look at or alter the contents** of the packets flowing across the wire.
- Repeaters are **used to extend the maximum length of a network segment.**
- Network backbones carried data across coaxial cable, Computers would connect into these either by **BNC connectors**, in the case of **thinnet**, or by **vampire taps**, in the case of **thicknet. Repeaters were used with coaxial cable** to amplify the signal.



Coaxial Cable : 10BASE-2 cable (right) over 10BASE-5 cable (left)

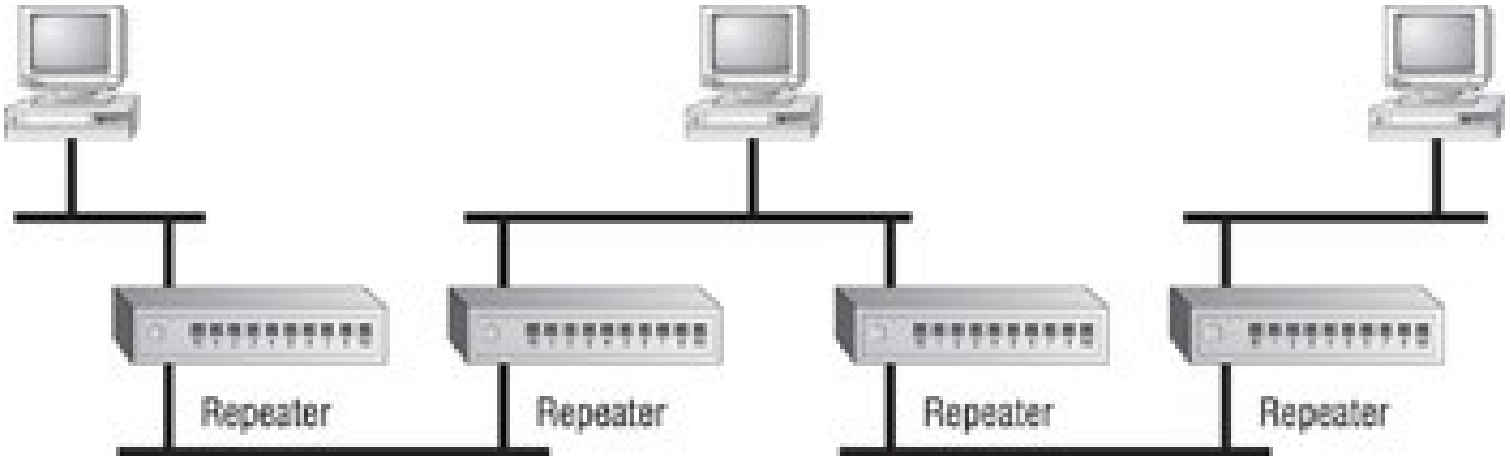




10Base-2 (thinnet) "T" connector used to attach the bus to the station. The leg of the "T" (facing forward) attaches to the interface card in the station, while the top of the "T" provides a straight through connection for the cable.

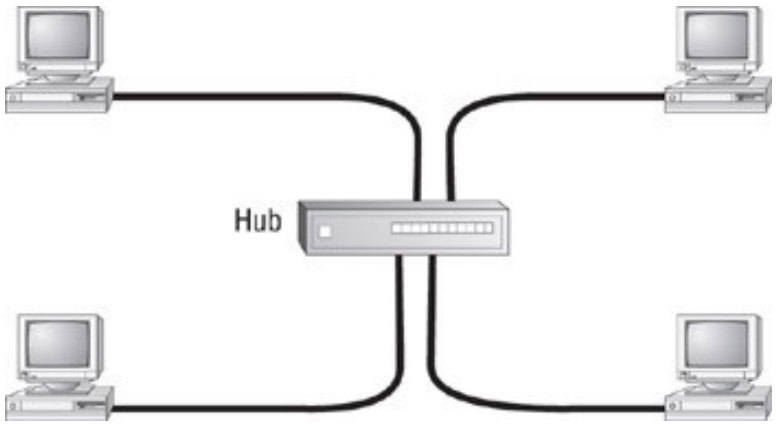
BNC connector

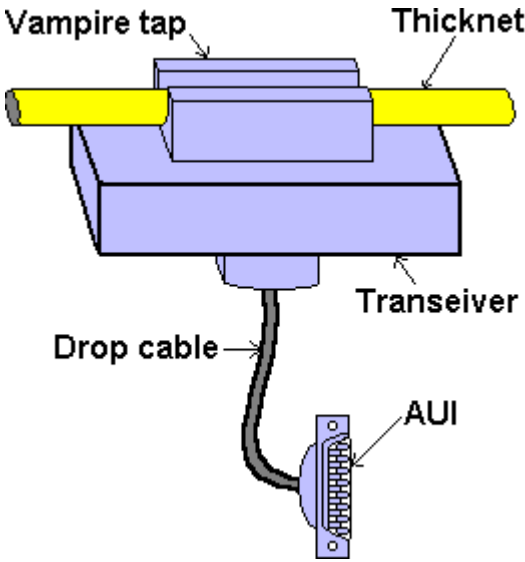
- The main **downfall of a repeater** is that it **repeats** everything it receives on one port, including **noise,** to its other ports.
- The **5-4-3 Rule** dictates how many repeaters can be used on a network and where they can be placed. According to this rule, a single network can have **five network segments** connected by **four repeaters**, with **three of the segments populated (3 segments may contain user connections).**
- Theoretically, repeaters could be used to **extend cables infinitely, but** due to the underlying limitations of communication architectures like Ethernet's collision domains, repeaters were used to tie together a **maximum of five coaxial-cable segments.**



HUBs : (also called a **concentrator or multiport repeater**)

- In twisted pair networking, Hubs amplified incoming signals (**same as repeaters**) before they are retransmitted across its ports.
- Repeater joins two backbone coaxial cables, whereas a hub joins two or more **twisted pair cables**.
- In twisted-pair networking, each network device is connected to an individual network cable. In coaxial networking, all network devices are connected to the same coaxial backbone. A hub **eliminates the need for BNC connectors and vampire taps**.

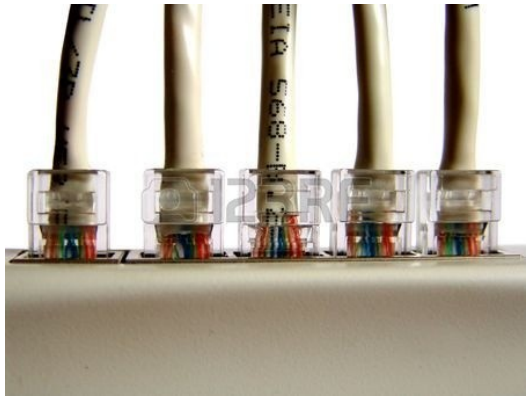




- Like repeaters, hubs operate at the OSI physical layer, which means they **do not alter or look at the contents** of a packet travelling across the wire.

Prof. Viral S. Patel

- Hubs typically provide from **8 to 24 twisted pair connections**, depending on the manufacturer and model of the hub.
- **Hubs can also be connected to each other by means of BNC (Bayonet Neill Concelman, AUI (attachment unit interface) ports** or crossover cables to provide flexibility as networks grow.
- Share bandwidth implication for Collision handling only for small scale, such as eight-port Hub.



In **shared-bandwidth configurations,** the amount of bandwidth available to a connected host is inversely proportional to the number of hosts sharing that bandwidth.

For **example** : cascading of four 24-port hubs, where 96 hosts share the same bandwidth (100Mbps). So each hub have only 1.042 Mbps. So throughput is decrease.

Classification of HUBs : Active and Passive

An **active hub** is usually **powered**, and it actually amplifies and clean up the signal it receives, thus doubling the effective segment distance limitation for the specific topology. (for example, extending an Ethernet segment another 100 meters)

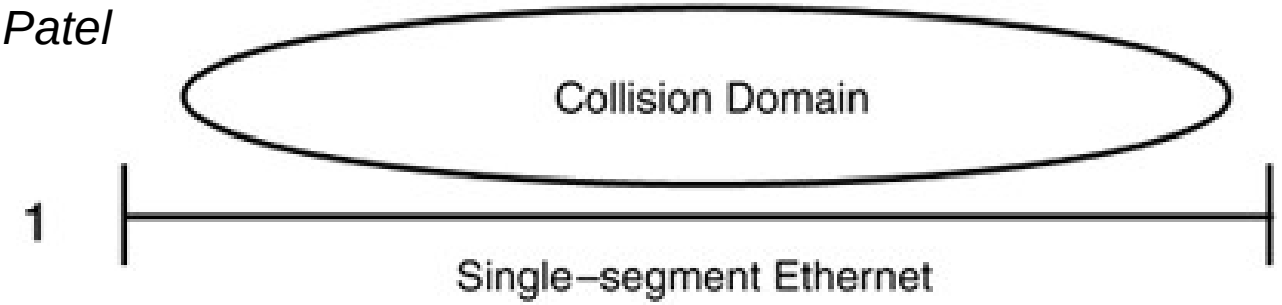
An **passive hub** is typically **unpowered** and makes only physical, electrical connections. Typically, the maximum segment distance of a particular topology is shortened because the hub **takes some power away from the signal strength** in order to do its job.

Bridges :

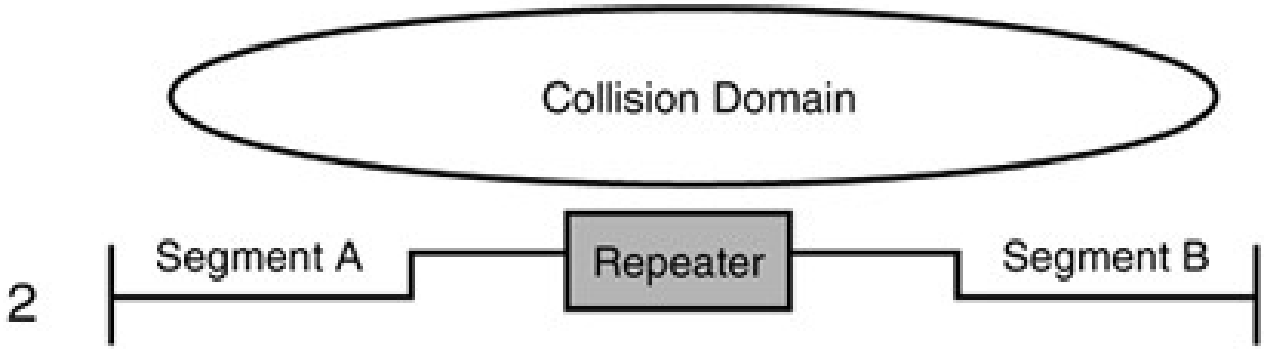
- Just like a repeater, a bridge is a network device used to connect two network segments.
- The main difference between them is that bridges operate at the **data link layer** of the OSI reference model and therefore provide translation services required to **connect dissimilar media access architectures such as Ethernet and Token Ring**.
- The primary use for a bridge is to **keep traffic** meant for stations **on one side** of the bridge and not let it pass to the other side.
- Four types of bridging:

1. **Transparent bridging :** Typically found in **Ethernet** environments, the transparent bridge analyzes the incoming frames and forwards them to the appropriate segments one hop at a time.

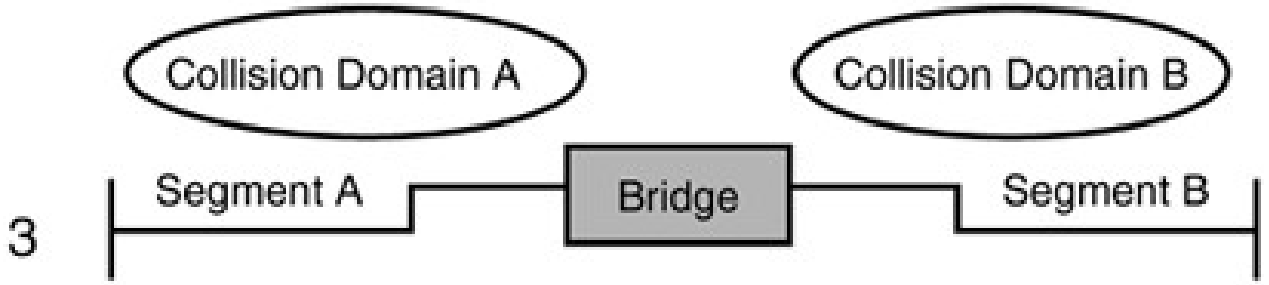
- They build a **table of addresses** (bridging table) as they receive packets. If the address is not in the bridging table, the packet is forwarded to all segments other than the one it came from.



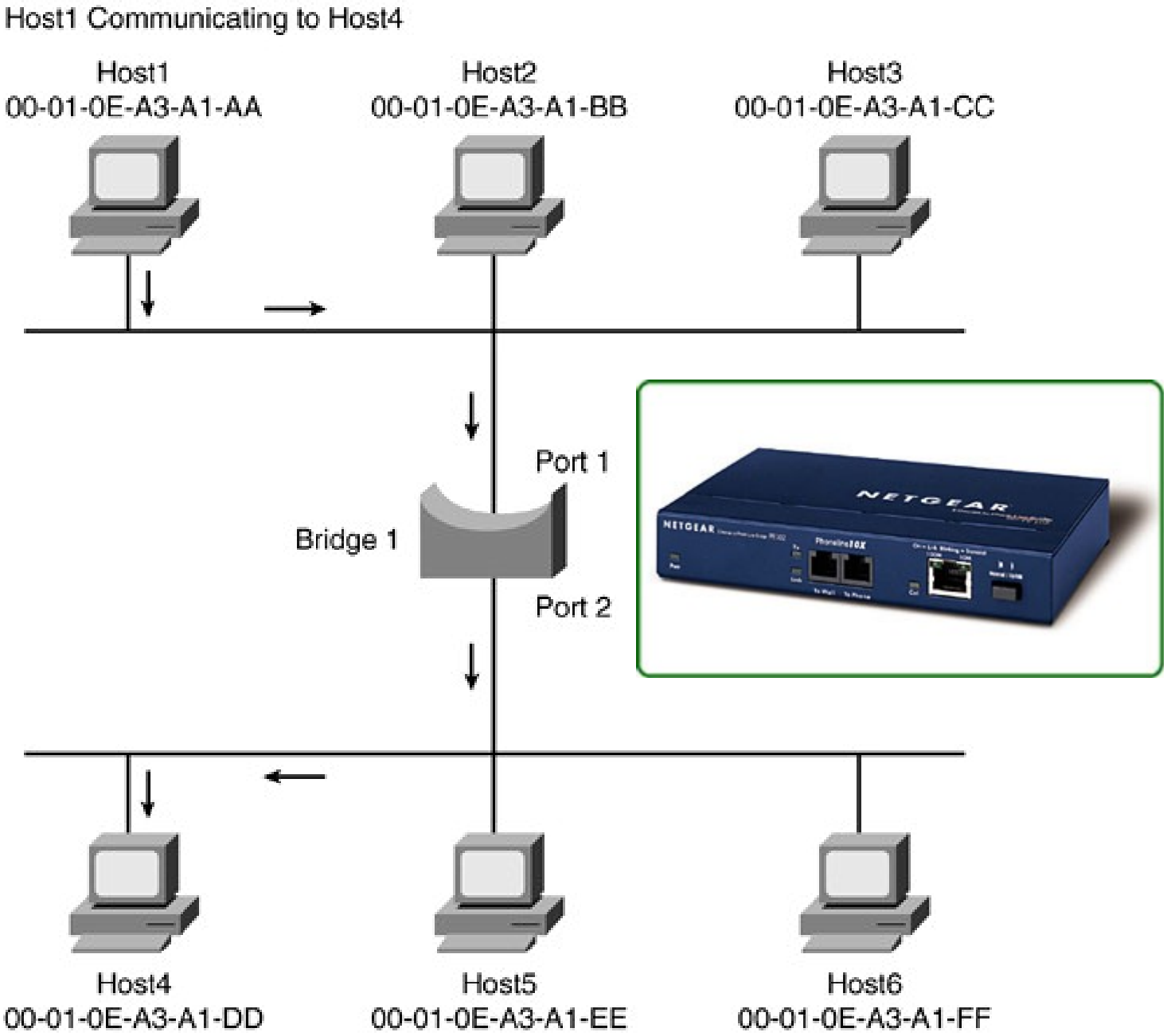
Single–segment Ethernet



Two–segment Ethernet with one collision domain



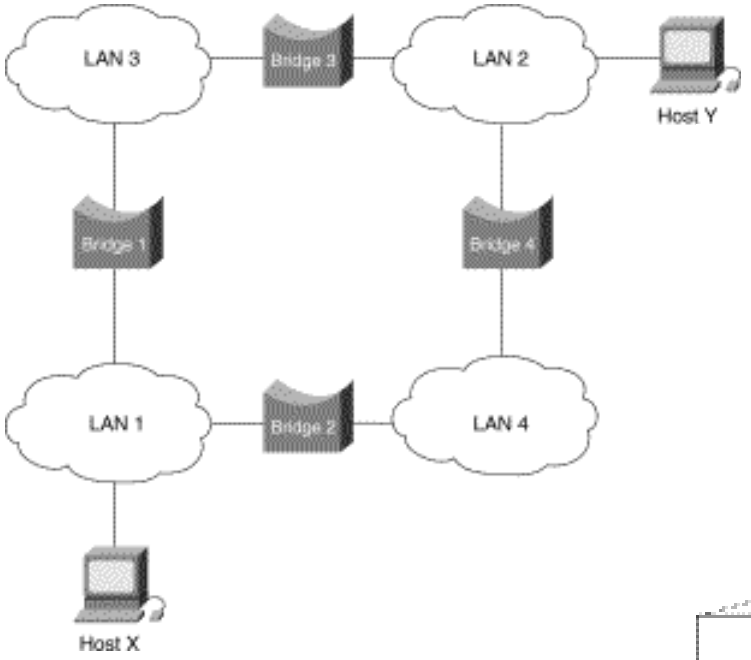
Two–segment Ethernet with two collision domains

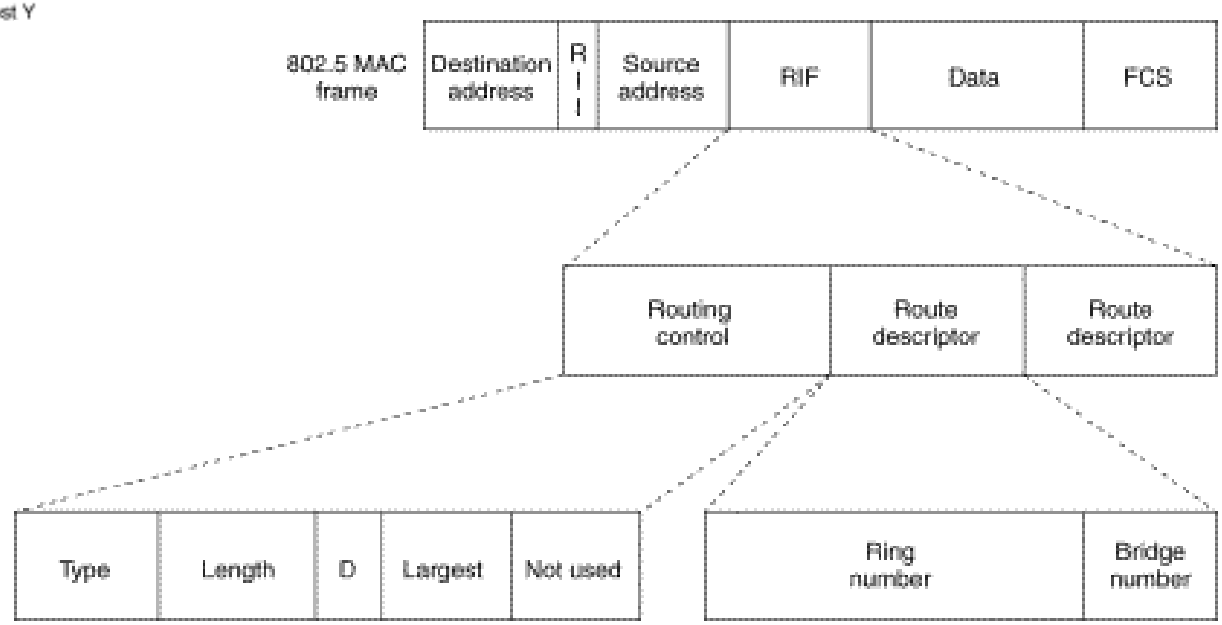


Prof. Viral S. Patel

2. **Source-route bridging :** Typically found in **Token Ring**, environments, source-route bridging provides alternative to transparent bridging for non-routable protocols such as NetBIOS and SNA (Systems Network Architecture).

➔ In source-route bridging, each ring is assigned a unique number on the source-route bridge port. The source computer provides **path information** inside the packet. Token Ring frames contain address information, **including a ring number**, which the bridge analyzes to forward the frame to the appropriate ring.





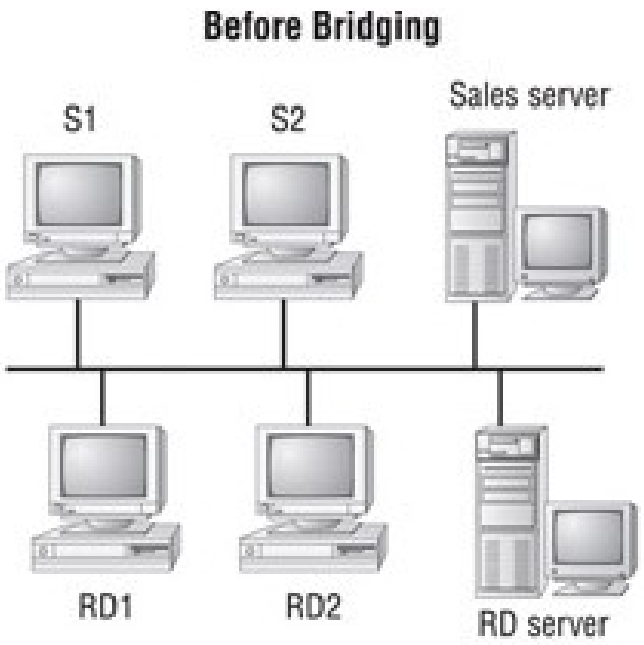
3. **Source-route transparent bridging :** Source-route transparent bridging is an extension of source-route bridging whereby non-routable protocols such as NetBIOS and SNA receive the **routing benefits** of source-route bridging **and** a **performance increase** associated with transparent bridging.

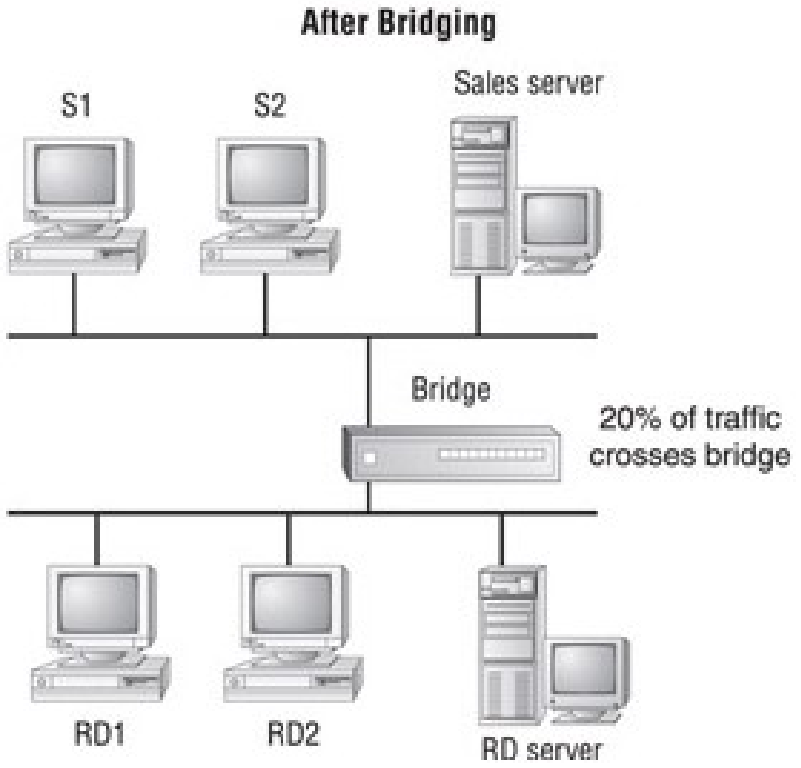
   [When an SRT bridge receives a frame, it immediately checks the frame's routing information indicator (RII) bit to see if the frame is a transparent bridging frame or an SRB frame. Once it determines the frame's type, it processes it accordingly.]

4. **Translation bridging :** Translation bridging is used to connect network segments with different underlying media-access technologies such as **Ethernet to Token Ring** or **Ethernet to FDDI** (Fiber Distributed data interface) etc.

- Bridging is one technique that can **solve the shared-bandwidth problem** that exists with hubs. In the hub example where we cascaded four 24 port hubs through the use of bridges, we can physically isolate each segment so that only 24 hosts compete for bandwidth; **throughput is** therefore **increased**.

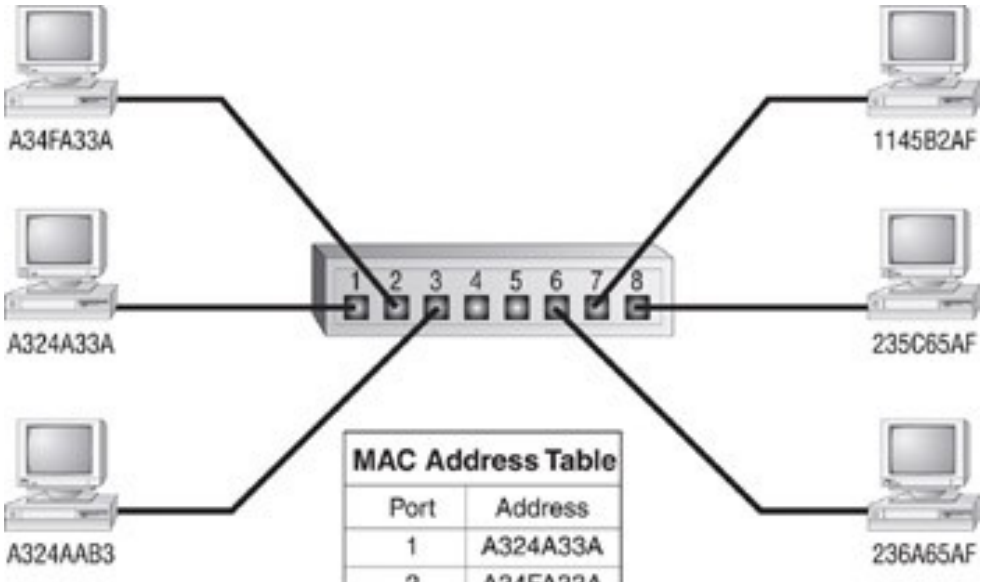
➔ Bridges can accommodate a **maximum of seven physical segments.**





Switches (Layer 2 Switches):

- Bridging is not only benefit of switch implement but also provide the benefit of **micro-LAN segmentation**, which means that every node connected to a switched port receives its own dedicated bandwidth. And with **layer 3 switching**, we can further segment the network into **virtual LANs**.
- **Layer 2 switches** operate up to the **data link layer** of the OSI reference model and in the case of **Layer 3 switches**, sometimes extend into the **network layer** can also perform routing functions.
- Switches build dynamic tables that **associate MAC address with switched ports.**



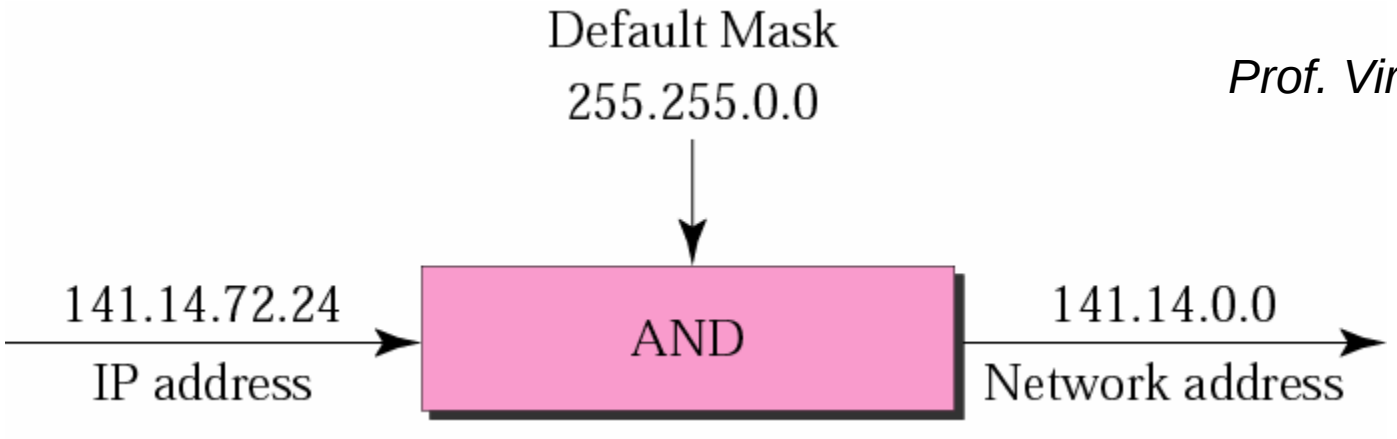
MAC Address Table	
Port	Address
1	A324A33A
2	A34FA33A
3	A324AAB3
4	—
5	—
6	236A65AF
7	1145B2AF
8	235C65AF

- Whereas bridges implement store-and-forward **bridging via software**, switches implement either store-and-forward or cut-through **switching via hardware**, with a marked **improvement of speed.**
- When two stations attached to the switch want to communicate, the sending station sends its data to the switch. When the switch receives the data, **rather than broadcasting** it over all its other ports as a hub would, the switch examines the Data Link header for the MAC address of the receiving station and **forwards it to the correct port**. This opens a **virtual pipe** between ports that can **use the full bandwidth** of the topology.
- If a server and several workstations were connected to the same 100 Mbps Ethernet switch, each workstation would need a dedicated 100 Mbps channel to the server and there would **never be any collisions.**

Routers:

- The router is the device that **connects multiple networks or segments** to form a large internetwork. Such as internet.
- Routers are **packet-forwarding devices**. Routers operate at the **network layer** of the OSI reference model, forwarding packets based on network ID.
- It is also the device that **facilitate communication** within this internetwork. It makes the choices about **how best to send packets** within the network so that they arrive at their destination.
- Router have **many functions** other than simply routing packets:
  - Router can **connect many small segments** into a network.
  - Routers can also **connect dissimilar lower-layer topologies**. For example, we can connect an Ethernet and a Token Ring network using a router.
  - Additionally, with added software, routers can perform **firewall functions and packet filtering.**

➔ In the case of IP protocol an **IP address** is 32 bits long. Those 32 bits contain both the **network ID and the host ID** of a network device. IP distinguishes between network and host bits by using a **default mask / subnet mask.**



Prof. Viral S. Patel

Example :**IP address 200.45.34.56 & default mask 255.255.255.0**

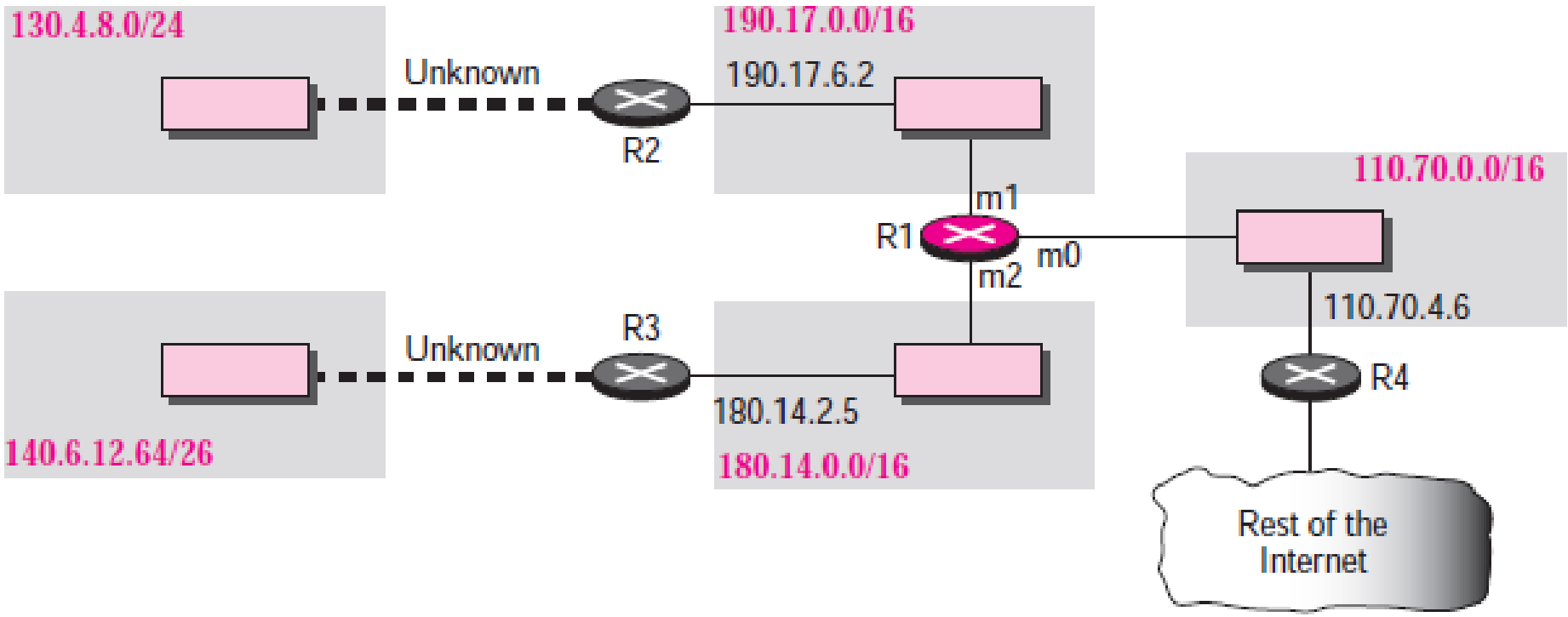
11001000 00101101 00100010 00111000	200.45.34.56
11111111 11111111 11111111 00000000	255.255.255.0
11001000 00101101 00100010 00000000	200.45.34.0

The **network address is 200.45.34.0.**

- When a router receives a packet arrived at its network interface, it examines the destination address to determine the best way to get it there. **It makes the decision based on** information contained within its own routing table.

Prof. Viral S. Patel

- **Routing table** are associations of **network IDs and interfaces** that know how to get to that network.
- By using this table, router **forwards the packet to** either the **intended recipient or** to the **next router** in the chain. Otherwise, the router informs the sender that it doesn't know how to reach the destination network.
- Routers enabled with the **TCP/IP protocol** and all networking devices configured to use TCP/IP make some sort of routing protocols. **IP is responsible** for forwarding or delivering packets.
- IP performs an **AND calculation** on destination IP address and subnet mask. And compare the result with connected networks' address using a routing table. If they are same then send data packets directly to the network. If not then check routing table for next hope address or default address to forwards it.



Mask	*Network Address*	*Next-Hop Address*	*Interface Number*
/26	140.6.12.64	180.14.2.5	m2
/24	130.4.8.0	190.17.6.2	m1
/16	110.70.0.0	----------	m0
/16	180.14.0.0	----------	m2
/16	190.17.0.0	----------	m1
Default	Default	110.70.4.6	m0

Brouter:

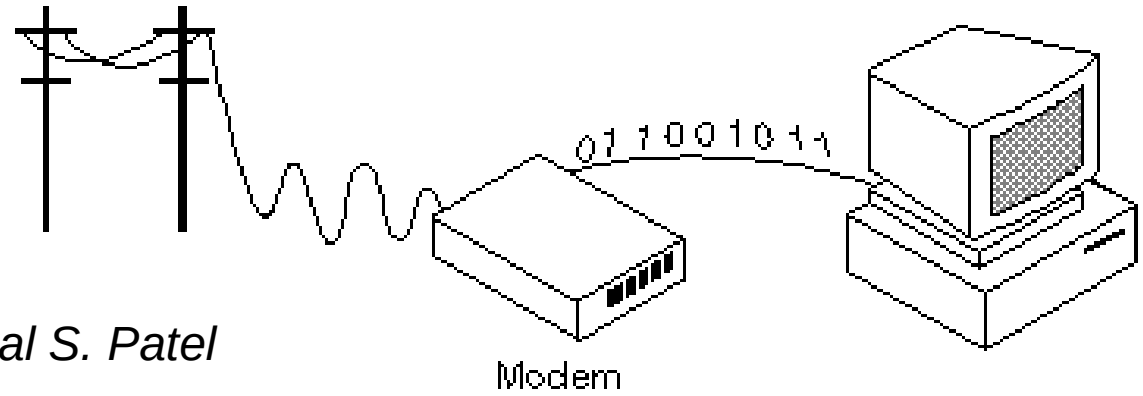
- The brouter is a unique device that **combines the functionality of a bridge and a router.**
- It **routes** most packets, but if it can't route a particular packet, it will try and **bridge** it.
- In short, we **can use a brouter as either a bridge or a router**.
- The brouter is mainly used to **connect different network topologies** and to bridge them, but it is not used much anymore.

Gateway:

- Gateway is normally a computer that operates in all five layers of Internet or seven layers of OSI model.
- It can be used as a connecting device between two networks that use different models.
- For example, One network using OSI model and another using the Internet model. We can connect these two different networks by gateway.

- Gateway is also called protocol translator.
- A gateway takes an application message, reads it and interprets it.
- In the network for an enterprise, a computer server acting as a gateway node is often also acting as a proxy server and a firewall server. So Gateways can also provide security.
- The gateway (or default gateway) is implemented at the boundary of a network to manage all the data communication that is routed internally or externally from that network.
- Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. Generally, a router is configured to work as a gateway device in computer networks.

Modem:



Prof. Viral S. Patel

- Modem short for **modulator-demodulator.** A modem is a device or program that enables a computer to transmit data over telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms.
- There is one standard interface for connecting external modems to computers called **RS-232**. Any **external modem** can be attached to any computer that has an RS-232 port, which almost all personal computers have.
- There are also modems that come as expansion board called onboard or **internal modems.**

- While the modem interfaces are standardized, a number of **different protocols for formatting** data to be transmitted over telephone lines exits.

  Some like CCITT V.34 are official standards, while others have been developed by private companies.
- Standards/Common protocols at slow data transmission speeds however the protocols are less standardized at high transmission speeds.
- Characteristics of Modem :
- **bps** : How fast the modem can transmit and receive data.

  At slow rates, modems are measured in terms of baud rates. The slowest rate is 300 baud.

  At higher speeds, modems are measured in terms of bits per second (bps). The fastest modems run at 57,600 bps.

  We can not receive data faster than it is being sent.

- **Data compression** : Some modems perform data compression, which enables them to send data at faster rates. However, the modem at the receiving end must be able to decompress the data using the same compression technique.
- **Voice/data** : Many modems support a **switch** to change between voice and data modes.

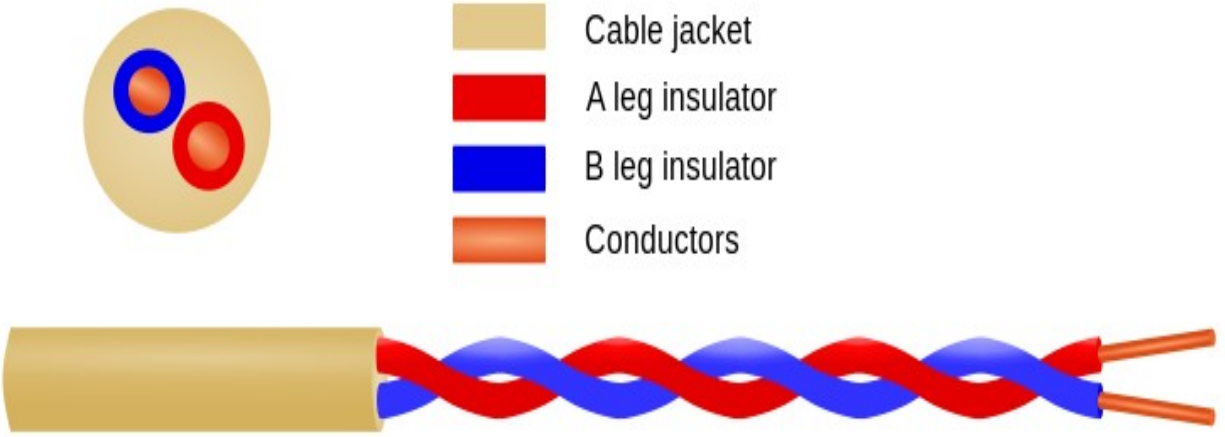
  In data mode, the modem acts like a regular modem.

  In voice mode, the modem acts like a regular telephone.

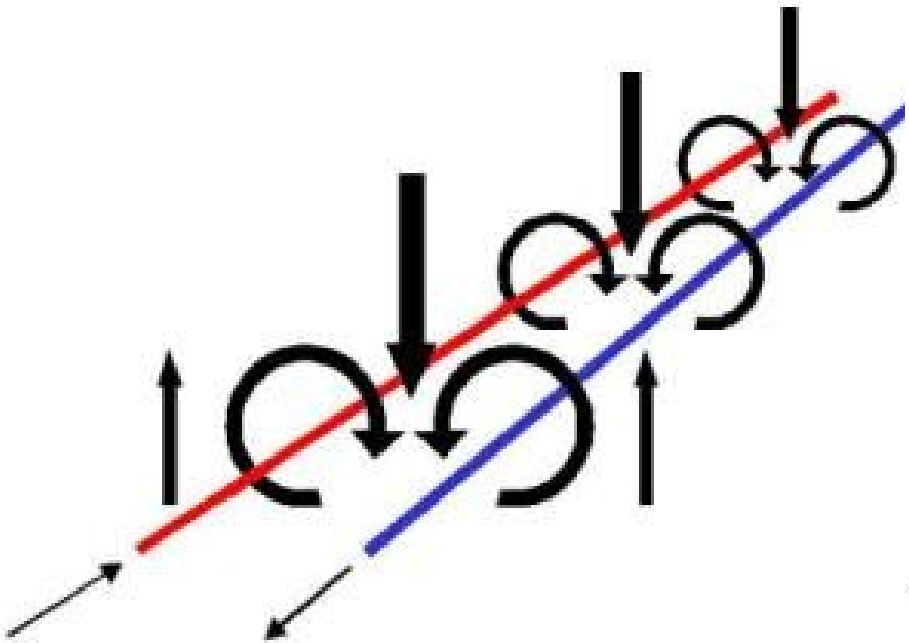
  Modems that support a voice/data switch have a built-in loudspeaker and microphone for voice communication.
- **auto-answer** : An auto-answer modem enables our computer to receive calls in our absence. This is only necessary if you are offering some type of computer service that people can call in to use.

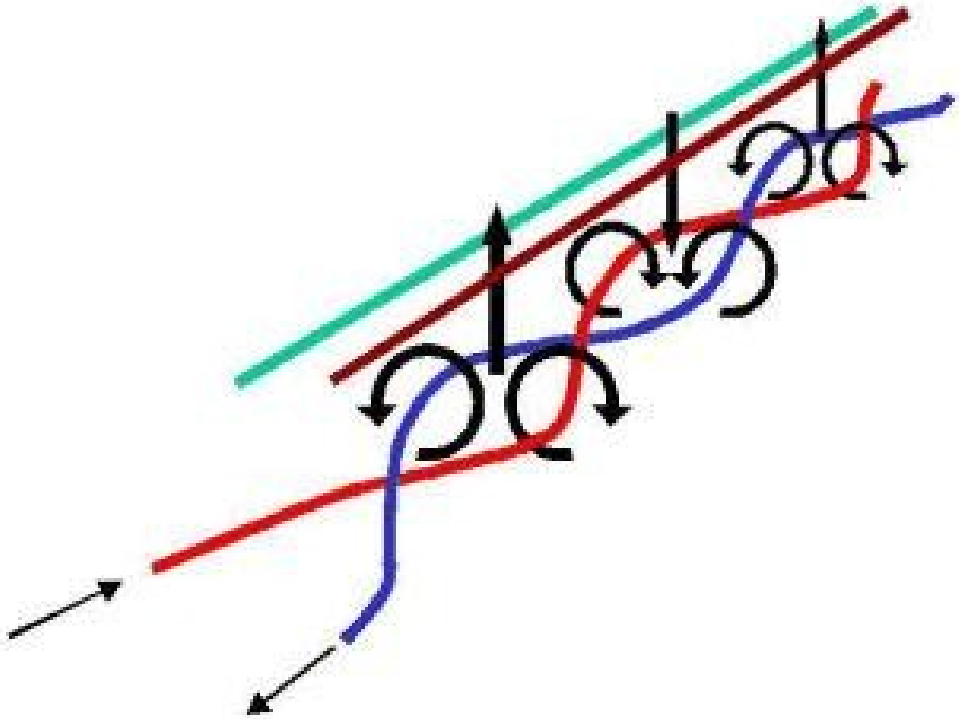
Twisted-Pair Cable :

- It consists of two conductors (normally copper), each with its own plastic insulation, twisted together as shown in figure.
- One of the wires is used to carry **signals** to the receiver and the other is used only as **ground reference**. The receiver uses the difference between the two.
- (when both wires are **near to each other**) In addition to the signal send by the sender on one of the wires, **interference (noise) and crosstalk** may affect both wires and **create unwanted signals**.



➔ (when both wires **away form each other**) If **two wires are parallel**, the effect of these unwanted signals is not the same in both wires because they are **at different locations** relative to the noise or crosstalk sources. (e.g. one is closer and the other is farther). This **results in a difference at the receiver.**





- By **twisting the pairs**, a balance is maintained. For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true.
- Twisting makes it probable that both wires are equally affected by external influence (noise or crosstalk). This means that the receiver, which calculates the difference between the two, receives **no unwanted signals.** The unwanted signal are mostly canceled out. So effect on quality of the cable.

- Twisted pair Connector Type : **RJ45**

- Local-area Networks, such as **10Base-T and 100Base-T**, also use twisted-pair cables.

Unshielded Twisted-Pair Cable :

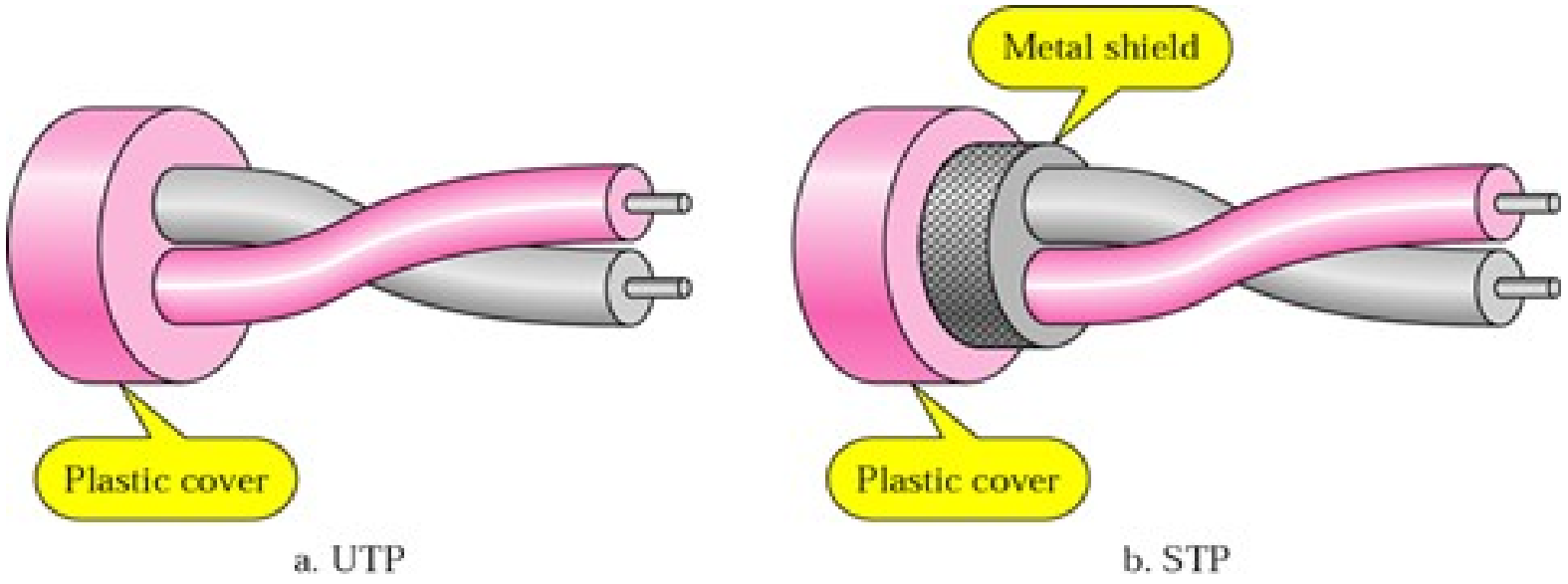
➔ UTP is a pair of **copper wires** wound by **plastic insulators**.

Advantages :

- It is the cheapest form of cables available for networking purposes.
- Easy to handle and install

Disadvantages :

- Highly prone to external interference and crosstalk.



a. UTP b. STP

Shielded Twisted-Pair Cable :

➔ STP is a pair of **copper wires** wound by **plastic insulators.** Each pair is also **cover by braided mesh or metal foil.**

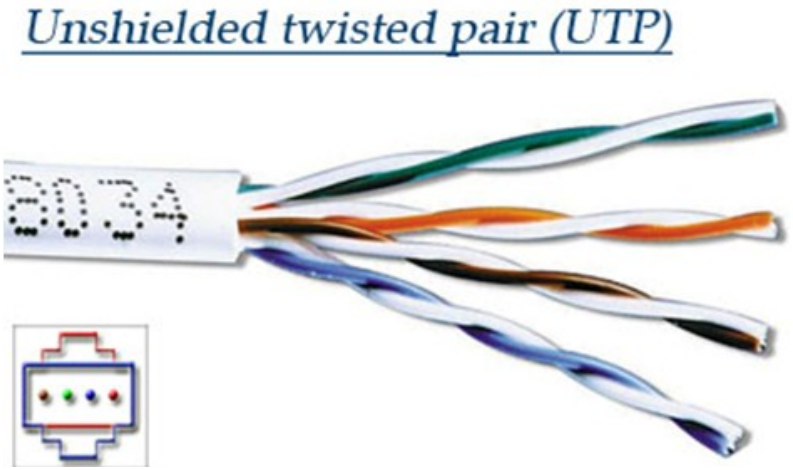
Advantages :

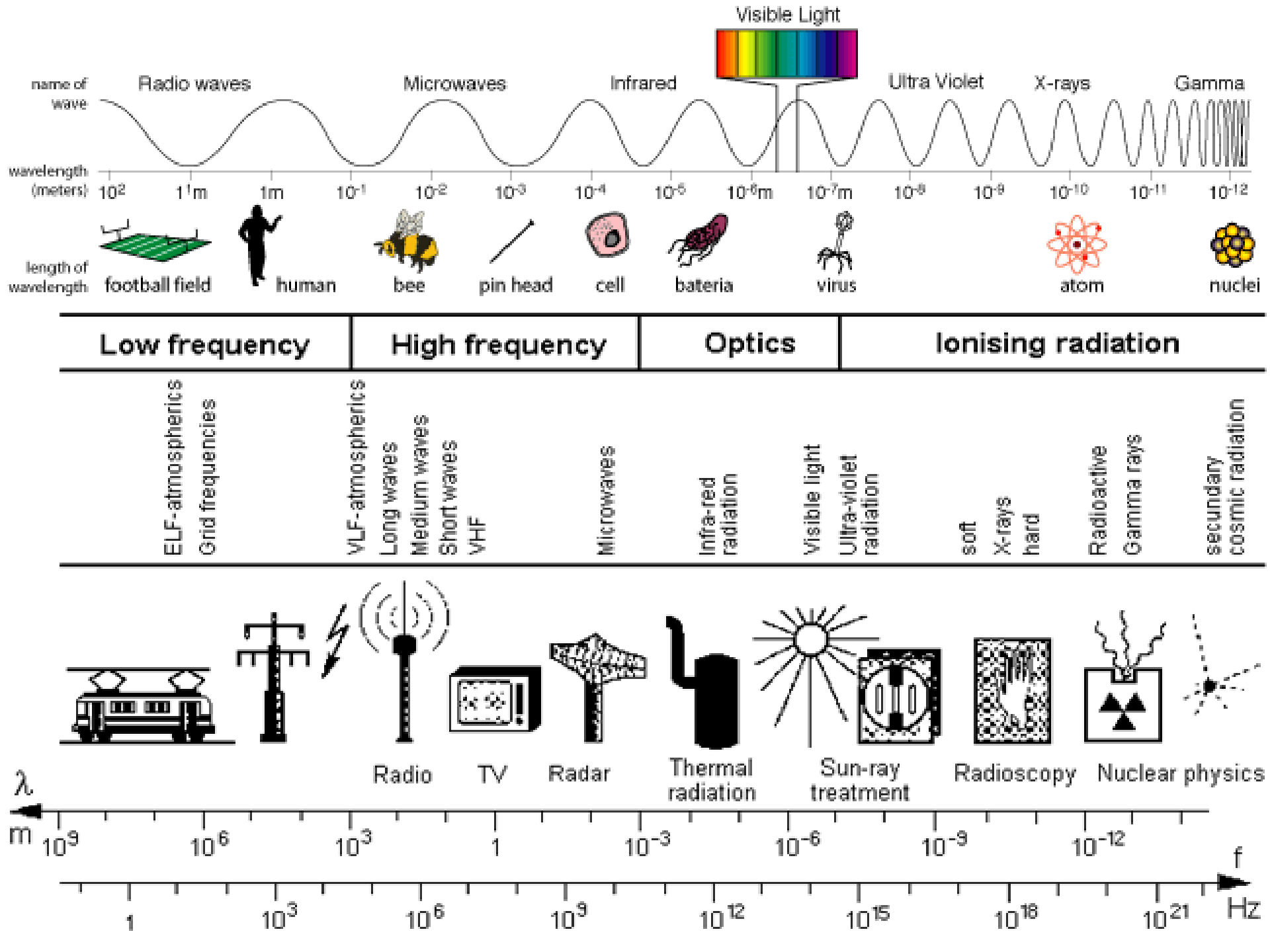
- Better protection from external interference and crosstalk.

Disadvantages :

- Costlier than UTP.
- difficult to install as compared to UTP

Prof. Viral S. Patel




Visible Light
name of wave
Radio waves
Microwaves
Infrared
Ultra Violet
X-rays
Gamma
wavelength (meters)
10^{2}
1^{1}m
1m
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}m
10^{-7}m
10^{-8}
10^{-9}
10^{-10}
10^{-11}
10^{-12}
length of wavelength
football field
human
bee
pin head
cell
bateria
virus
atom
nuclei
Low frequency
High frequency
Optics
Ionising radiation
ELF-atmospherics
Grid frequencies
VLF-atmospherics
Long waves
Medium waves
Short waves
VHF
Microwaves
Infra-red radiation
Visible light
Ultra-violet radiation
soft
X-rays
hard
Radioactive
Gamma rays
secundary cosmic radiation
Radio
TV
Radar
Thermal radiation
Sun-ray treatment
Radioscopy
Nuclear physics
λ
m
10^{9}
10^{6}
10^{3}
1
10^{-3}
10^{-6}
10^{-9}
10^{-12}
f
Hz
1
10^{3}
10^{6}
10^{9}
10^{12}
10^{15}
10^{18}
10^{21}

Radio waves	Microwave
Microwaves are actually a sub-class of radio waves. But generally divide in two part.	
frequency of radio waves 3 kHz to 1 GHz	Frequency of microwave 1 GHz to 300 GHz
Omni-directional property	Unidirectional (ling-of-sight) property
Radio waves in general have long distance communication capabilities	Repeaters are often needed for long distance communication.
Can penetrate walls	Cannot penetrate walls
Radio band is relatively narrow. Just under 1 GHz, compared to microwave. So subbands are also narrow leading to a low data rate.	Microwave band is relatively wide, almost 299 GHz. So subbands can be assigned and give high data rate.
Radio waves are mostly used in AM and FM radio, television, cordless phones, navigation.	microwaves are used in RADAR, astronomy, cellular phones, satellite communication.
Using any part of the band	Certain portions of the band

Infrared
Frequency of Infrared : 300 GHz to 400 THz
Unidirectional (ling-of-sight) property
Used in sort range communication system. Useless for long-range communication.
Cannot use outside a building because the sun’s rays contain infrared waves that can interfere.
Cannot penetrate walls. So cannot be affected by another system in the next room.
Very high data rate. The standard defined data rate of 75 kbps for a distance of 8 m. The recent standard defines a data rate of 4 Mbps.
Infrared used in communication between devices such as keyboards, mice, PCs and printers.
IrDA (Infrared Data Association) port that allows a wireless keyboard to communicate with a PC.

Baseband	Broadband
Digital Signals are used.	Analog Signals are used.
Baseband uses Time-Division Multiplexing (TDM). Frequency division multiplexing is not possible	Frequency division multiplexing is possible
Baseband is bi-directional transmission	Broadband is unidirectional data transmission.
Signal travelling distance is short	Signal travelling distance is long
Entire bandwidth of the cable is consumed by a single signal in a baseband transmission.	The signals are sent on multiple frequencies and allow all the multiple signals are sent simultaneously in broadband transmission.
Example : Ethernet LAN. The word "base"—for example, 10BaseT or 10BaseFL.	Example : Cable TV

Application layer protocols of TCP/IP :

HTTP, Telnet, POP3, FTP, TFTP, SNMP, SMTP, MIME, DHCP etc.

FTP (File Transfer Protocol) :

- The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server.

SMTP (Simple Mail Transfer Protocol) :

- SMTP is a communication protocol for mail servers to transmit **email** over the Internet. It is a ASCII (American Standard Code for Information Interchange) based.

MIME (Multipurpose Internet Mail Extensions) :

- SMTP had some limitation when it came to dealing with binary files e.g. Images because it is ASCII based. MIME allows non-ASCII data such as images, video, audio etc to be sent through e-mail.

Telnet (Termina**l Net**work **– for remote logging) :**

➔ Telnet is an underlying TCP/IP protocol for **accessing remote computers.** Through Telnet, an administrator or another user can access someone else's computer remotely on the Internet or local area networks. It provides a bidirectional interactive text-oriented communication facility using a virtual terminal connection.

POP3 (Post Office Protocol, version 3)

➔ Transfer email messages from a permanent remote mailbox on the server to a local computer or portable device.

(**IMAP4 –** Internet Mail Access Protocol, version 4 **–** is similar to POP3, but it has more features, more powerful and more complex)

DHCP (Dynamic Host Configuration Protocol) : Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway.

HTTP (Hypertext Transfer Protocol) :

- HTTP is the set of **rules for transferring files** (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.
- As soon as a Web user opens their **Web browser,** the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols.
- This protocol defines **how messages are formatted and transmitted,** and what actions Web servers and browsers should take in response to various commands.

➔For **example,** when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is **HTML**, which covers **how Web pages are formatted and displayed**

- HTTP is called a **stateless protocol** because each command is executed independently, without any knowledge of the commands that came before it.

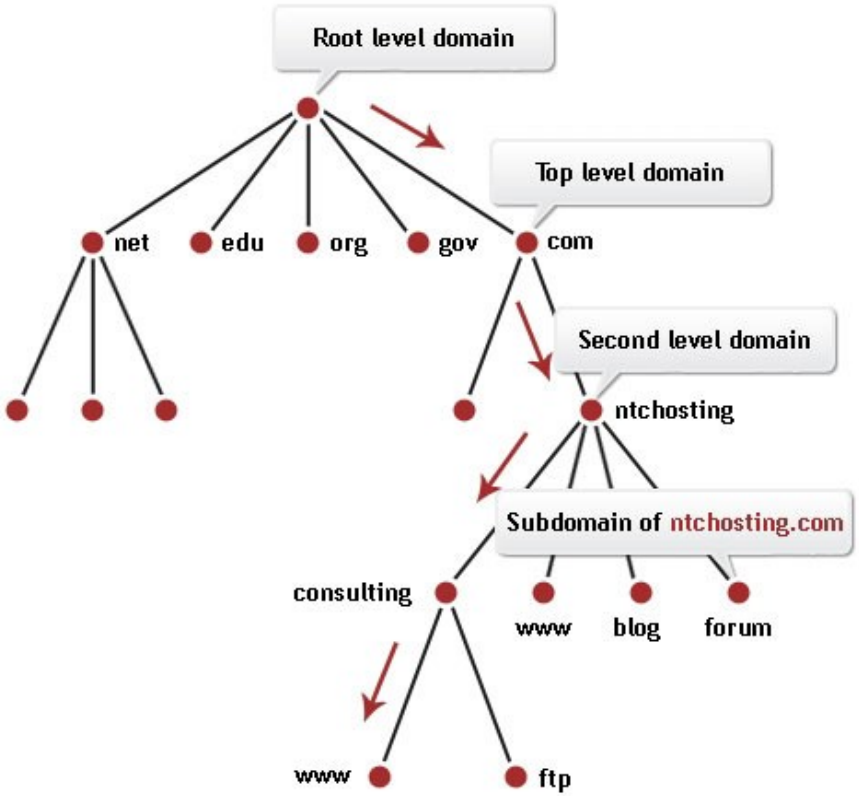
DNS (Domain Name System):

The Domain Name System is used to resolve human-readable hostnames like **www.svpatelcsbm.org** into machine-readable IP addresses like **103.1.173.190**

DNS also provides other information about domain names, such as mail services

DNS program can support an e-mail program to find the IP address of an e-mail recipient.

➔A user of an e-mail program may know the e-mail address of the recipient; however the IP protocol needs the IP address. The DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address.



DNS (Domain Name System):

Prof. Viral S. Patel

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

.cn	(China)
.de	(Germany)
.uk	(United Kingdom)
.nl	(Netherlands)
.eu	(European Union)
.ru	(Russian Federation)
.ar	(Argentina)
.it	(Italy)
.br	(Brazil)
.us	(United States)

SNMP (Simple Network Management Protocol) :

- It is a popular protocol for network management.
- It is a framework for managing devices in an internet using the TCP/IP protocol suit.
- It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network.

PGP (Pretty Good Privacy) :

This protocol provide security at the application layer. PGP is designed to create authentication and confidential e-mails.

SSL/TLS (Secure Socket Layer / Transport Layer Security)

This protocols works at the transport layer to provide security and compression services to data generated from the application layer.

Transport / Host-to-Host layer protocols of TCP/IP :

TCP, UDP, SCTP etc.

Prof. Viral S. Patel

TCP (Transmission Control Protocol) :

- TCP is a network communication protocol designed to send data packets over the Internet.
- TCP provides **reliable**, full-duplex, **connection-oriented** transport service to upper-layer protocols.
- Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same **order** in which they were sent.

UDP (User Datagram Protocol) :

- UDP is an alternative communications protocol to TCP to send data packets over the Internet. But **does not acknowledge of their receipt.**
- UDP is **unreliable**, best-effort, **connection-less** protocol.
- There is **no ordering** of messages.

Prof. Viral S. Patel

SCTP (Stream Control Transmission Protocol)

- ➔ It is a reliable, message-oriented and byte-oriented protocol.
- ➔ It combines the best features of UDP and TCP.
- ➔ It provides support for newer applications such as voice over the internet.

Internet / network layer protocols of TCP/IP :

IP, ARP, RARP, ICMP, IGMP etc.

Internetworking Protocol (IP) :

- IP is a transmission mechanism used by the TCP/IP protocol.
- IP support at the network layer.
- IP is a **connectionless** and **unreliable** datagram protocol and provides **no error checking**.
- IP transfers data in the form of packets called **datagrams.**
- Datagram can travel through various routes to reach the destination and may **not arrive in the order** in which they were sent.
- IP does not reorder the data once they reach the destination. Also, IP **does not keep a track** of the routes of the datagram.

Address Resolution Protocol (ARP) :

- ARP is used to **determine the physical address** (MAC address) of the device only when its IP address is known.
- Each device has a physical address imprinted on the Network Interface Card (NIC).

Reverse Address Resolution Protocol (RARP) :

- RARP is used to **determine the IP address** of the host only when the physical address (MAC address) is known.
- It is useful when the computer is connected to the network for the first time.

Internet Control Message Protocol (ICMP) :

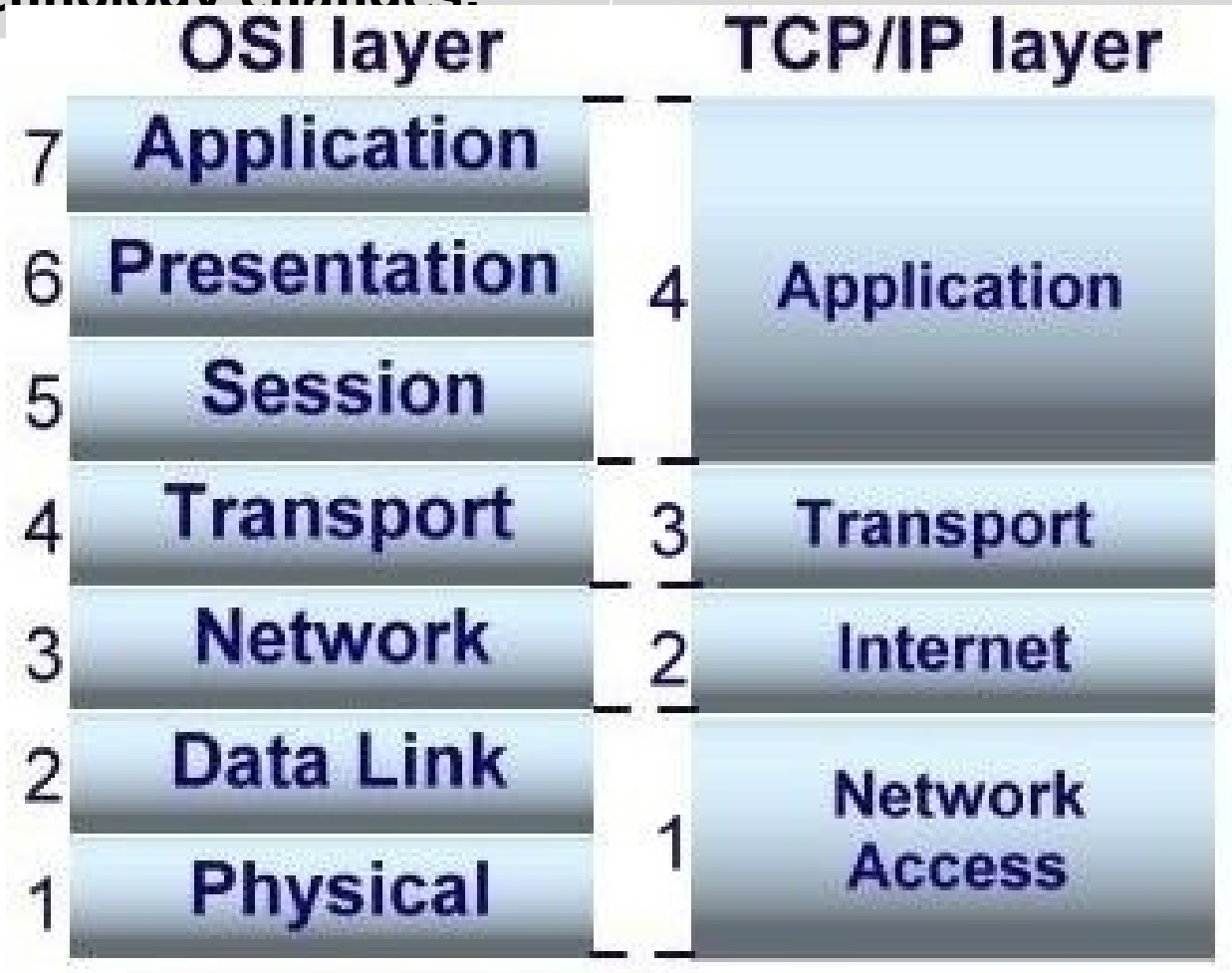
- This protocol is used by computer and gateways to send notification of datagram problems such as query and **error reporting** messages back to the sending device.
- Its only function is to **report problems to the original sender** not to correct them.
- **Ping** command is an example of ICMP protocol

Internet Group Message Protocol (IGMP) :

- This protocol is used for **multicasting** means to transmit message to multiple recipients at the same time.
- Class D IP address is used for this protocol.

OSI	TCP/IP
Open System Interconnection	**Transmission Control Protocol / Internet Protocol**
The Open Systems Interconnection (OSI) model is a "generic, protocol-independent standard" created by the International Organization for Standardization (ISO) to describe how the different software and hardware components involved in a network communication and interact with one another.	**TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.** Prof. Viral S. Patel
It has 7 layers	**It has 4 layers**
OSI model is a reference model	**TCP/IP is an implementation of OSI model.**
OSI model has a separate Presentation layer and Session layer.	**TCP/IP combines the presentation and session layer issues into its application layer**

OSI	TCP/IP
It is protocol independent. Protocols are hidden in OSI model and are easily replaced as the technology changes.	**It is protocol dependent. In TCP/IP replacing protocol is not easy.**



Satellite Networks :

What is satellite network ?

- A satellite network is a combination of nodes, some of which are satellites, that provides communication from one point on the earth to another. A node in the network can be a satellite, an Earth station, or an end-user terminal or telephone.

Why we use artificial satellite, not natural satellite ?

➔ Although Natural satellite, such as moon, can be used as a relaying node in the network, the use of artificial satellites is preferred because we can install electronic equipment on the satellite to regenerate the signal that has lost its energy during travel. Another restriction on using natural satellite is their distances form the earth, which create a long delay in communication.

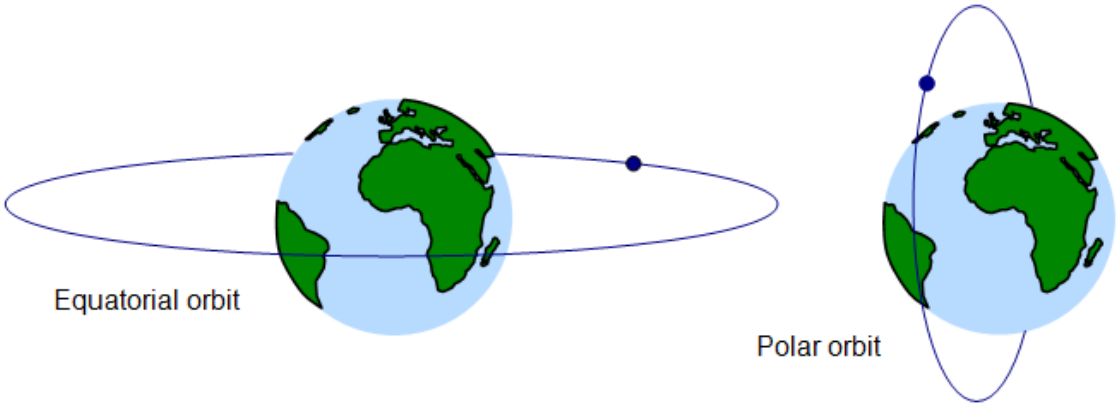
What is the advantage of Satellite networks ?

- Satellite networks are like cellular networks in that they divide the planet into cells. Satellites can provide transmission capability to and from any location on earth, no matter how remote. This advantage makes high-quality communication available to undeveloped parts of the world without requiring a huge investment in ground-based infrastructure.

What is Orbits ?

Prof. Viral S. Patel

An Artificial satellite needs to have an orbit, the path in which it travels around the earth. The orbit can be **equatorial, inclined, or polar,** as shown in figure.

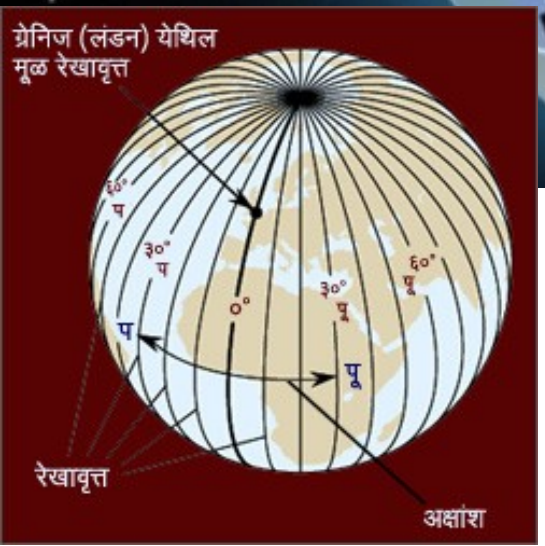


GPS?

Latitude

Longitude

Altitude



What is Kepler's law ?

The period of satellite, the time required for a satellite to make a complete trip around the earth, is determined by Kepler's law, which defines the period as a function of the distance of the satellite from the center of the earth.

$$\textbf{Period} = C \times \text{distance}^{1.5}$$

Example : the Moon is located approximately 3,84,000 km above the earth. The radius of the earth 6378 km. C is a constant approximately equal to 1/100. So the period of the moon, according to Kepler's law

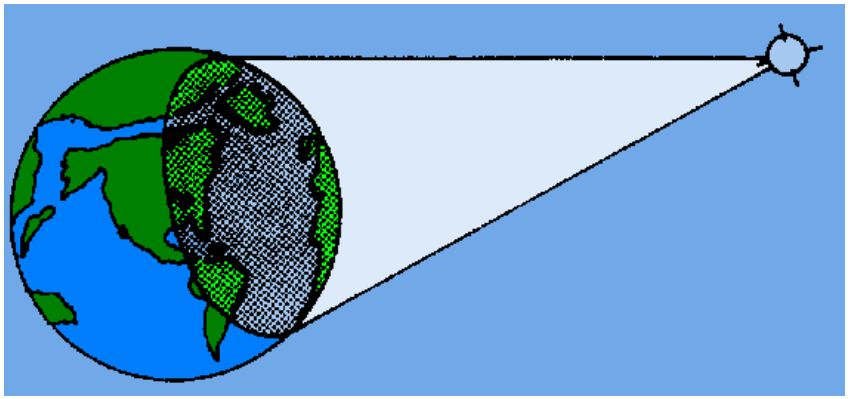
$$\text{period} = (1/100) \times (3{,}84{,}000+6378)^{1.5}$$

$$= 2{,}439{,}090 \text{ seconds}$$

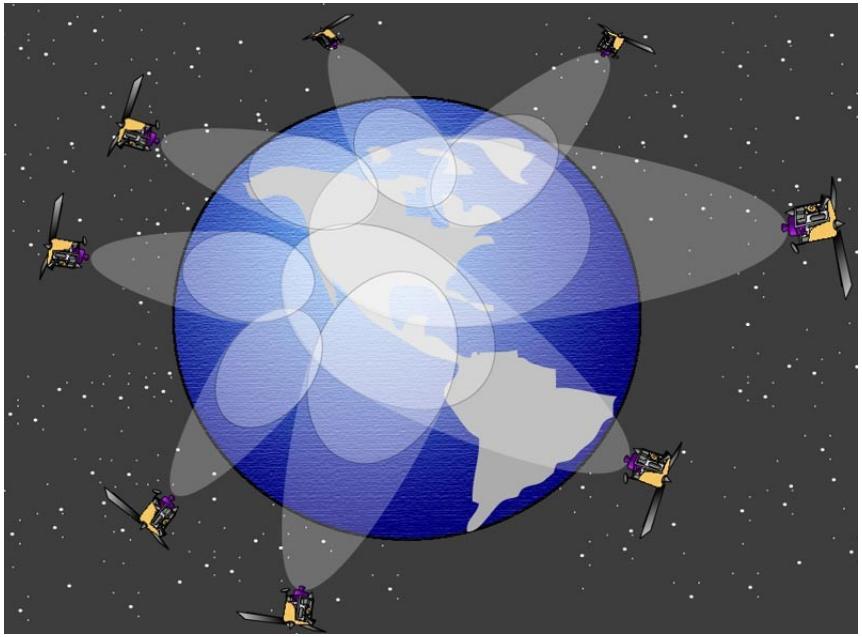
$$= 1 \text{ month}$$

What is Footprint?

Satellites process microwaves with (line-of-sight). Therefore, the signal from a satellites is normally aimed at a specific area called the footprint.



- The signal power at the center of the footprint is maximum. The power decreases as we move out form the footprint center.



- The boundary of the footprint is the location where the power level is at a predefined threshold.

Three Categories of Satellites :

Based on the location of the orbit, satellite can be divided into three categories :

GEO : geostationary-Earth-orbit,

LEO : low-Earth-orbit,

MEO : middle-Earth-orbit.

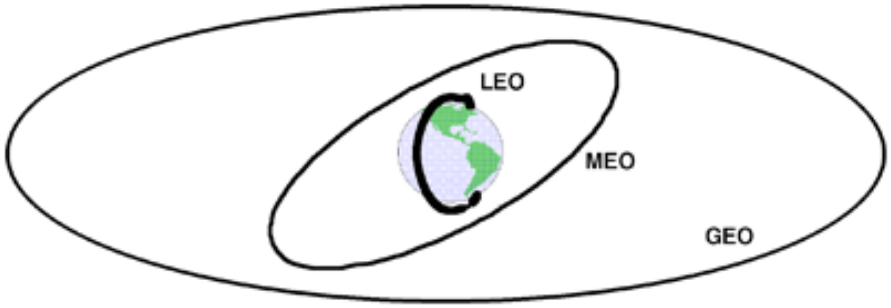
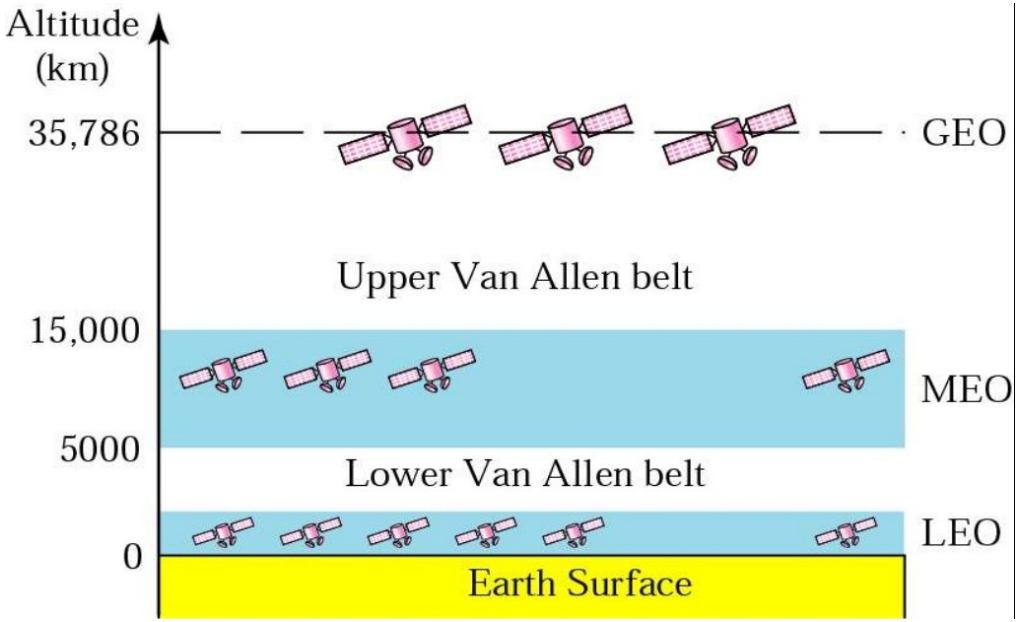


Figure shows the satellite Altitude with respect to the surface of the Earth.



- There is only one orbit, at an altitude of 35,786 km for the GEO satellite.
- MEO satellites are located at altitudes between 5000 and 15000 km.
- LEO satellites are normally below an altitude of 2000 km.

Why different orbits ?

➔ One reason for having different orbits is due to the existence of two Van Allen belts. **A Van Allen belt is a layer that contains charged particles.** A satellite orbiting in one of these two belts would be totally destroyed by the energetic charged particles. The MEO orbits are located between these two belts.

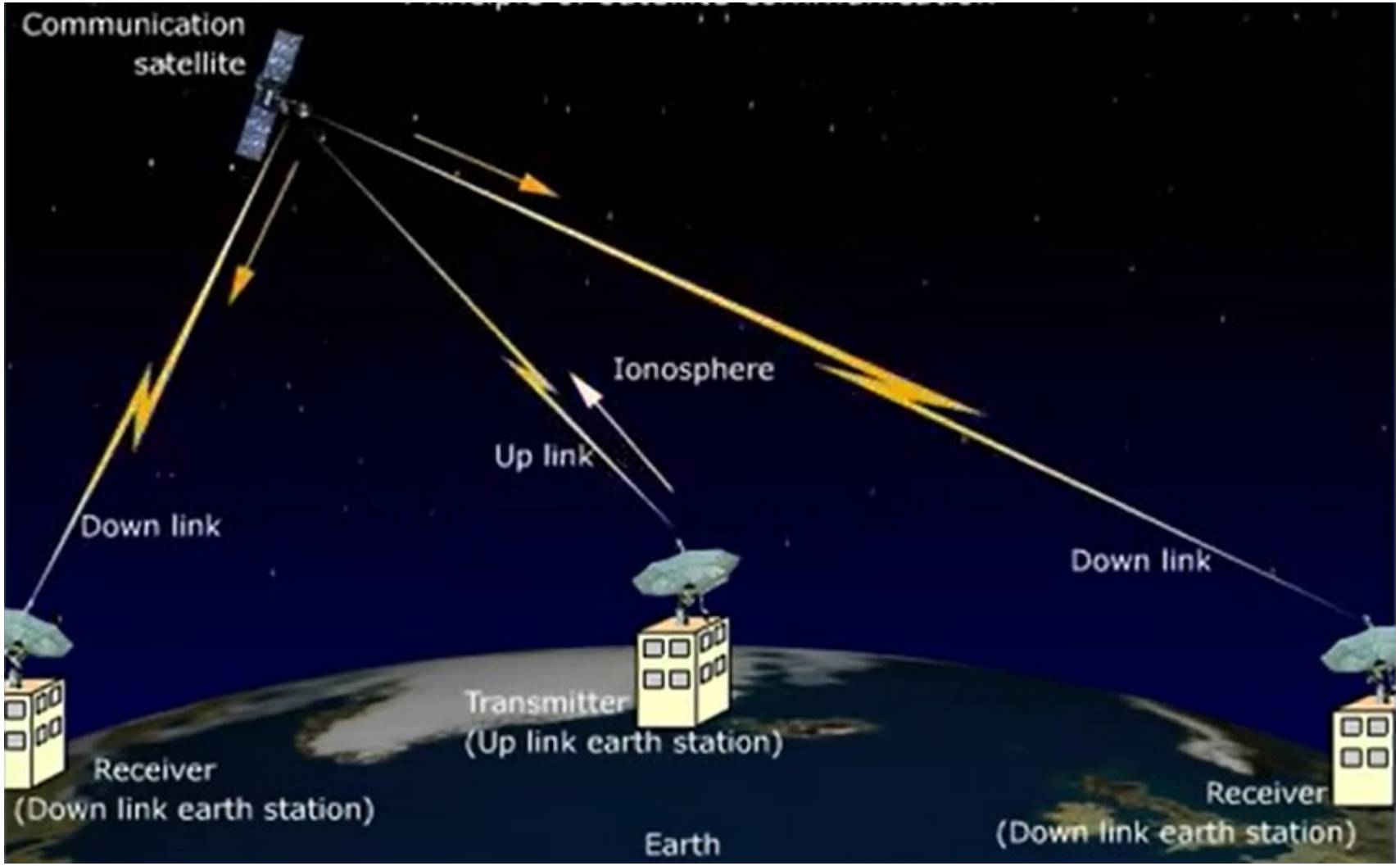
Frequency bands for satellite communication ?

➔ The frequencies reserved for satellite microwave communication are in the gigahertz (GHz) range. Each satellite sends and receives over two different bands. One for uplink and one for downlink.

What is uplink and downlink ?

➔ Transmission from the **Earth to the satellite** is called the uplink.

➔ Transmission from the **satellite to the earth** is called the downlink.


Communication satellite
Ionosphere
Up link
Down link
Down link
Transmitter
(Up link earth station)
Receiver
(Down link earth station)
Receiver
(Down link earth station)
Earth

GEO Satellites (Geostationary-Earth-Orbit)

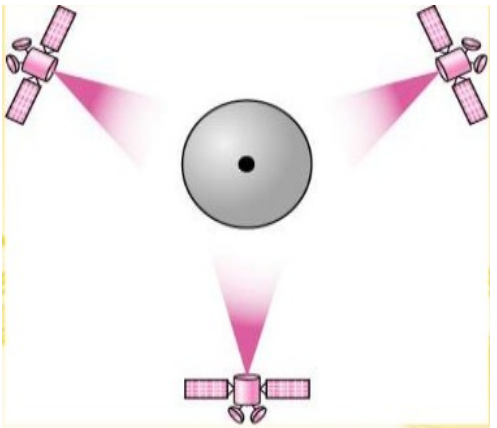
- Because of Light-of-sight propagation, a satellite that moves faster or slower than the earth's rotation is useful only for short periods.

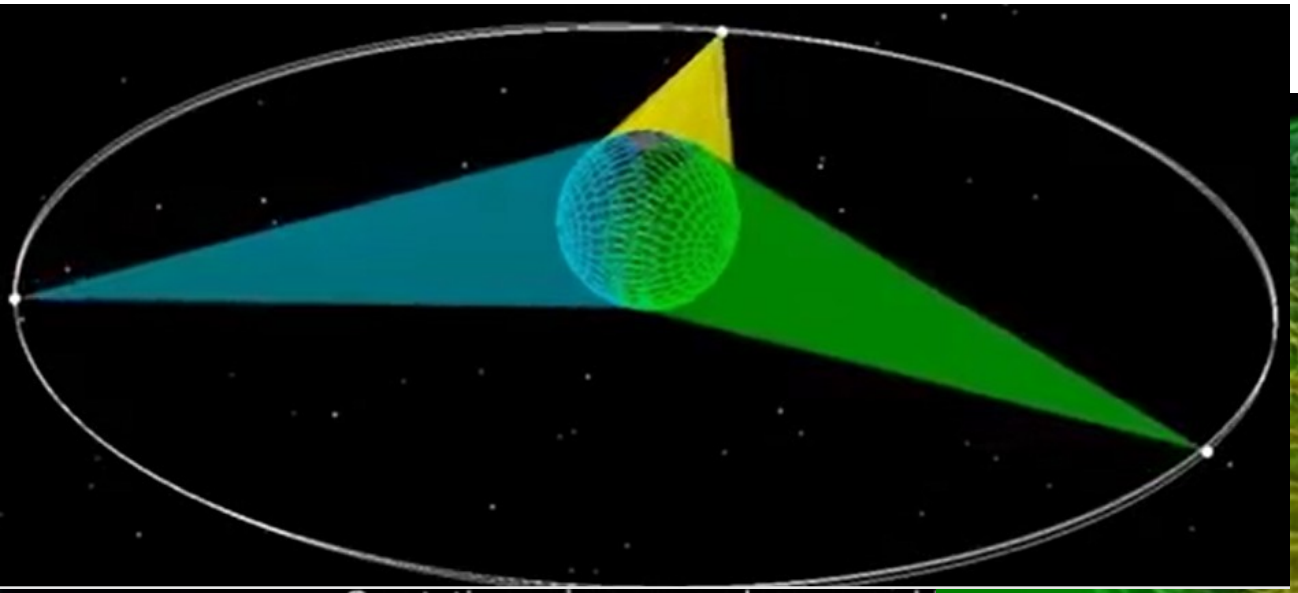
  To ensure constant communication, the satellite must move at the **same speed as the earth** so that it seems to remain fixed above a certain spot. Such satellites are called **geostationary**.

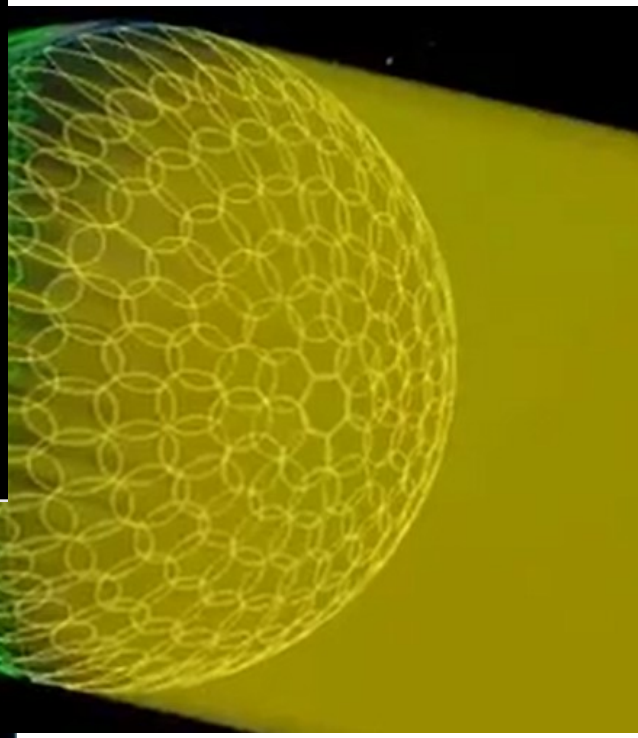
- Because orbital speed is based on the distance from the planet, only one orbit can be geostationary. This orbit occurs at the equatorial plane and is approximately **22000 mi** from the surface of the earth.

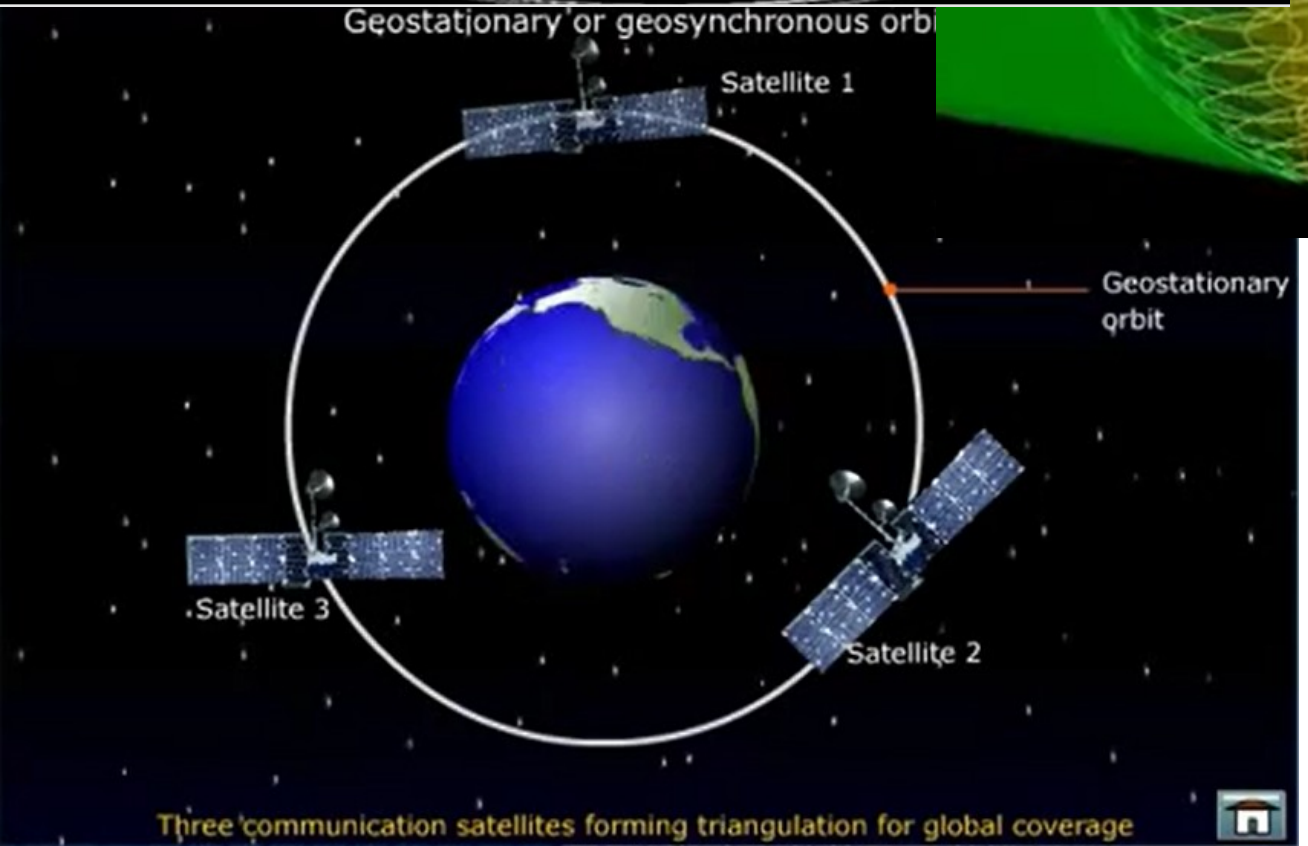
- But one geostationary satellite cannot cover the whole earth. It takes a minimum of **three satellites equi-distant** from each other in geostationary earth orbit (GEO) to provide full global transmission.

- Figure shows three satellites, each **120°** from another in geosynchronous orbit around the equator. The view is from the North Pole.








Geostationary or geosynchronous orbi
Satellite 1
Geostationary orbit
Satellite 3
Satellite 2
Three communication satellites forming triangulation for global coverage

MEO Satellites (Middle-Earth-orbit)

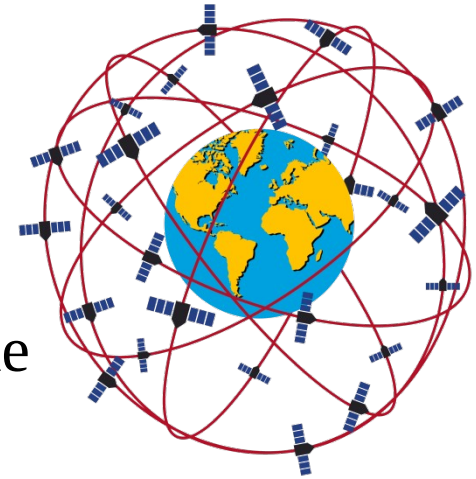
- MEO satellites are positioned between the two Van Allen belts. A satellite at this orbit takes approximately 6-8 hours to circle the Earth.

***Global Positioning System (GPS)**:*

- One example of a MEO satellite system is the Global Positioning System, constructed and operated by the US Department of Defense, orbiting at an altitude about **18000 (11000 mi)** above the earth.

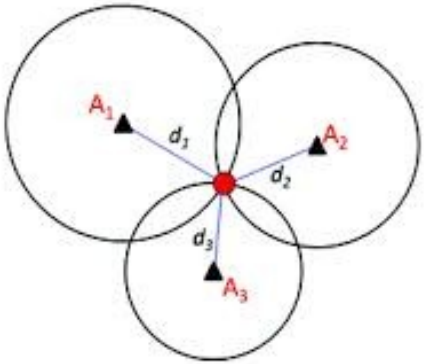
Prof. Viral S. Patel

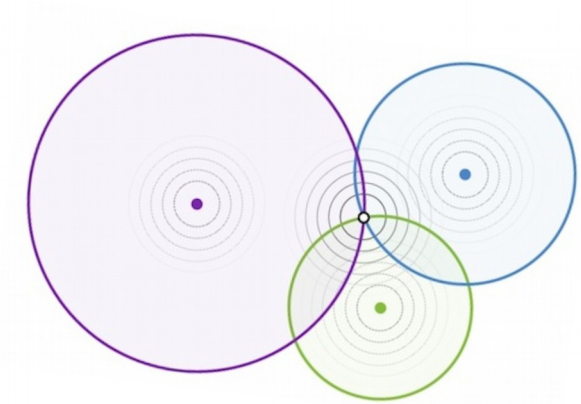
- The system consists of **24 satellites** and is used for land, sea and air navigation to provide time and locations for vehicles and ships.
- GPS uses 24 satellites in **six orbits.**
- The orbits and the locations of the satellites in each orbit are designed in such a way that, at any time **four satellites** are visible from any point on Earth. A GPS receiver has an almanac that tells the Current position of each satellite.

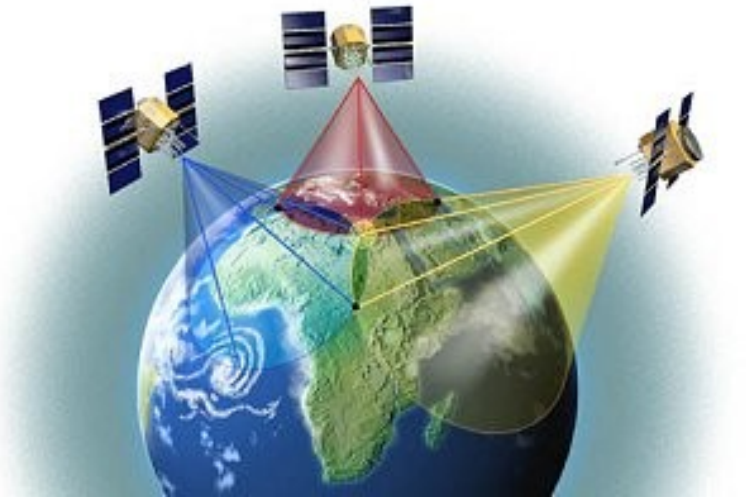


Trilateration : GPS is based on a principle called trilateration. On a plane, **if we know our distance from three points, we know exactly where we are.**

➔ Let us say that we are 10 miles away from point A, 12 miles away from point B, and 15 miles away from point C. If we draw three circles with the centers at A,B, and C, we find our position meet **three circles at one single point**.





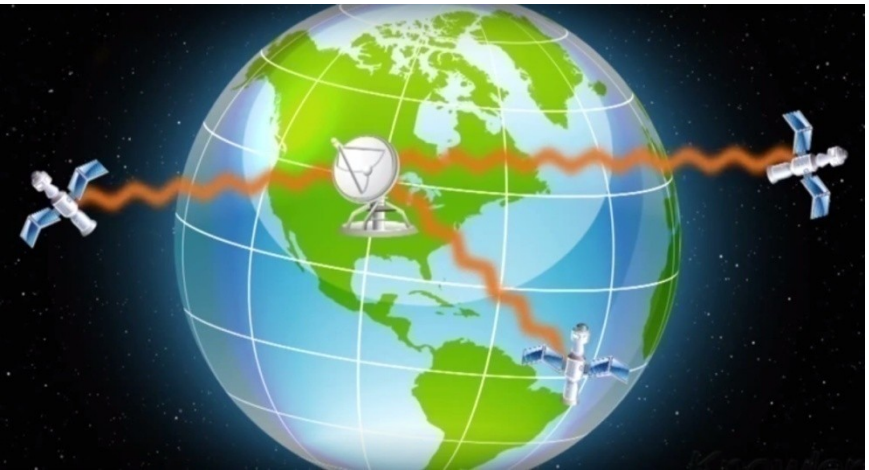


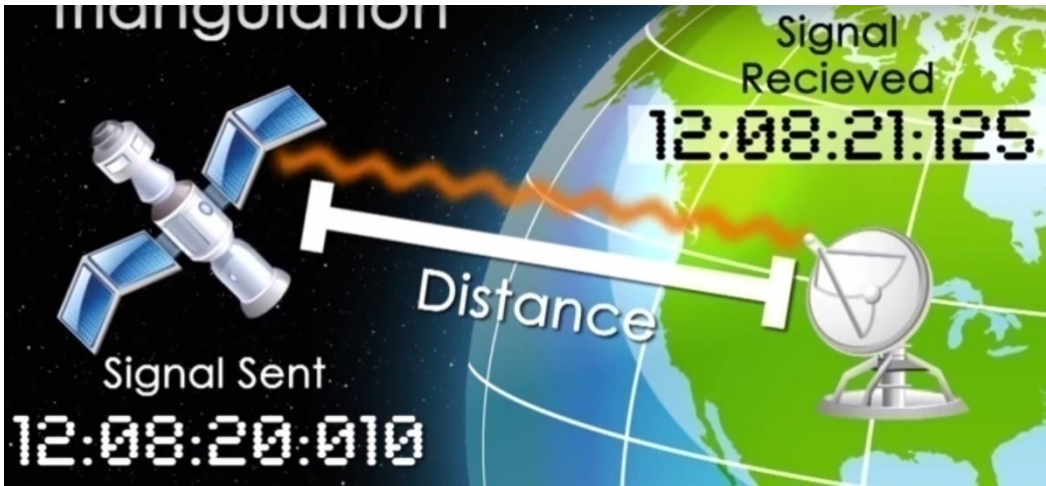
In three-dimensional space, the situation is different. We need at least four spheres to find our exact position in space. But three spheres are enough, because one of the two points, where the spheres meet is easily can be selected without a doubt.

Measuring the Distance : Measuring the distance is done using a principle called **one-way ranging.** For the moment, let us assume that all GPS satellites and the receiver on the Earth are synchronized.

➔ Each of **24 satellites** synchronously transmits a complex **signal** each having a **unique pattern**.

➔ The computer on the receiver **measures the delay between the signals** from the satellites and its copy of signals to **determine the distances** to the satellites.

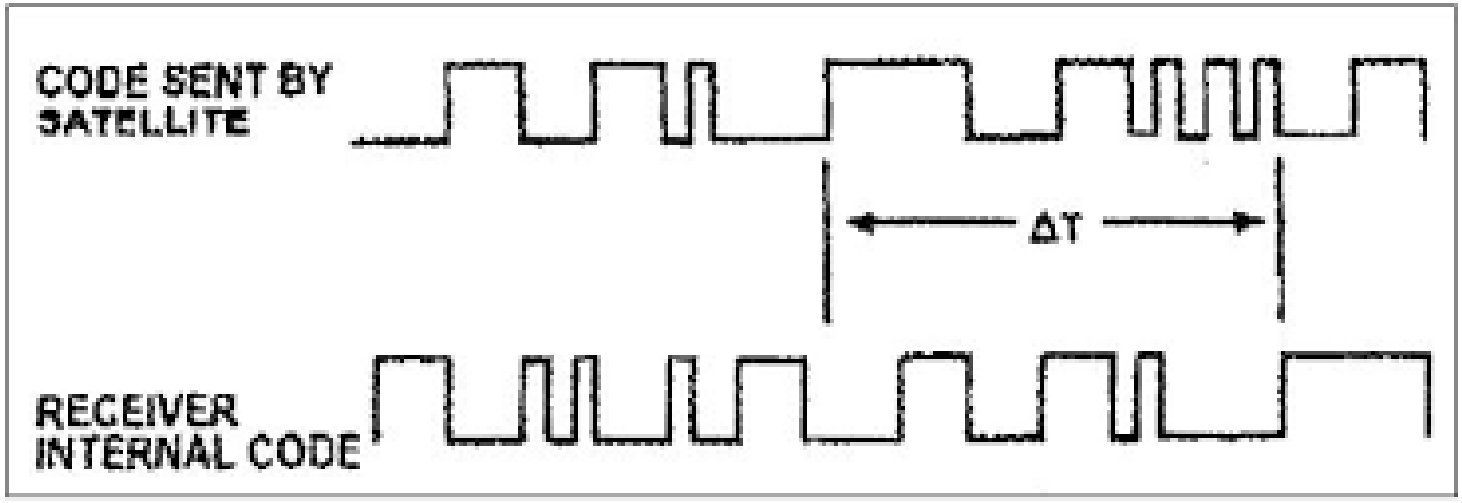




Synchronization : Satellites' clock are synchronized with each other and with the receiver's clock. Satellites use **atomic clock** that are precise and can function **synchronously with each other**.

➔ The receiver's clock however, is a normal **quartz clock** and there is no way to synchronize it with the satellite clocks.

➔ There is an **unknown offset** between the satellite clocks and the receiver clock that introduces a corresponding offset in the **distance calculation**. Because of this offset, the measured distance is called **pseudorange.**



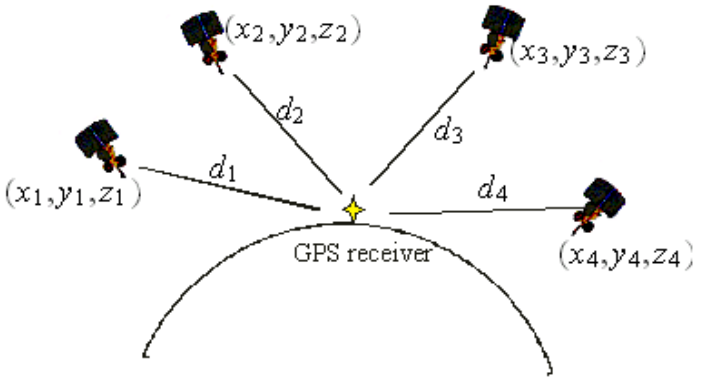
- GPS uses an elegant **solution** to the clock offset problem, by recognizing that the offset's value is the same for all satellite being used. The calculation of position becomes finding **four** unknowns : the $\mathbf{x_r}$, $\mathbf{y_r}$, $\mathbf{z_r}$ coordinates of the receiver, **and common clock offset dt**.
- For finding these four unknown values, we need at least four equations. This means that we need to measure pesudoranges from **four satellite** instead of three. If we call the four measured pseudoranges PR1, PR2, PR3 and PR4 and the coordinates of each satellite x_i, y_i and z_i (for i=1 to 4), we can find the four previously mentioned unknown values using the following four equations.

$$PR1 = \sqrt{(x_1 - x_r)^2 + (y_1 - y_r)^2 + (z_1 - z_r)^2} + c * dt$$

$$PR2 = \sqrt{(x_2 - x_r)^2 + (y_2 - y_r)^2 + (z_2 - z_r)^2} + c * dt$$

$$PR3 = \sqrt{(x_3 - x_r)^2 + (y_3 - y_r)^2 + (z_3 - z_r)^2} + c * dt$$

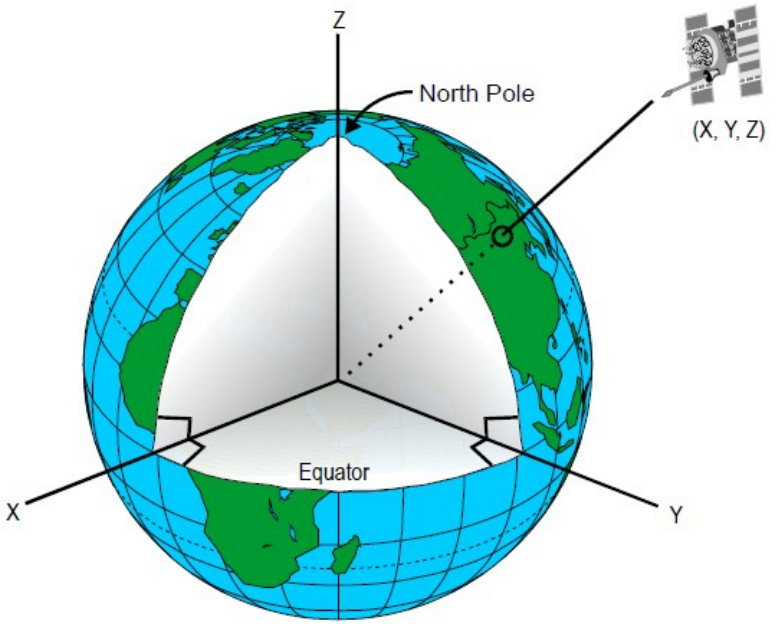
$$PR4 = \sqrt{(x_4 - x_r)^2 + (y_4 - y_r)^2 + (z_4 - z_r)^2} + c * dt$$



➔ The coordinates used in the above formulas are in an **Earth-Centered Earth-Fixed (ECEF)** reference frame, which means that the origin of the coordinate space is at the center of the Earth and the **coordinate space rotate with the Earth**. This implies that the ECEF coordinates of a fixed point on the surface of the earth do not change.

Application :

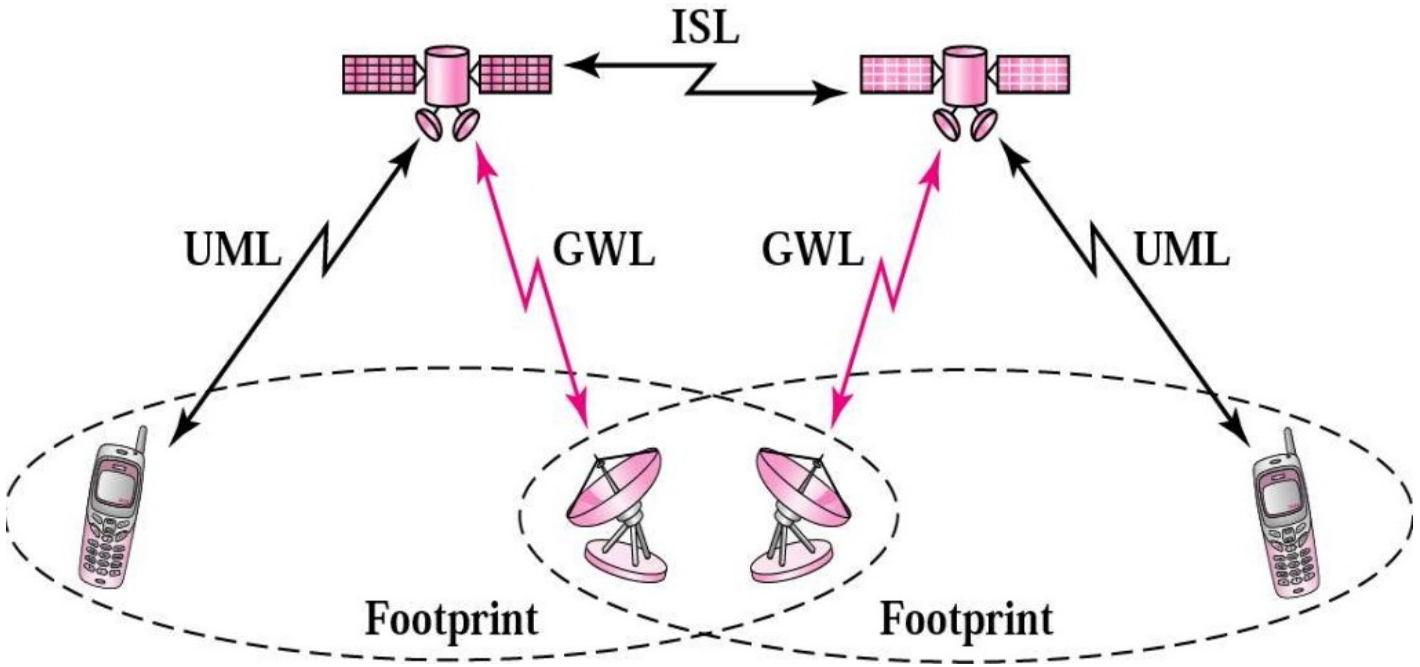
- GPS is used by **military forces**.
  For example, thousands of portable GPS Receivers were used during the war by Foot soldiers, vehicles and helicopters.
- Another use of GPS is in **navigation**.
  The driver of a car can find the location of the car and find a path to the destination.
- Another application is **clock synchronization**.
  The IS-95 cellular telephone system uses GPS to create time synchronization between the base stations.



LEO Satellite (Low-Earth-Orbit)

- Low-Earth-Orbit (LEO) satellite have **polar orbits**. The altitude is between **500 and 2000 km**, with a rotation period of **90 to 120 min**.
- ➔ The satellite has a speed of **20000 to 25000 km/h**.
- ➔ An LEO system usually has a cellular type of access, similar to the cellular telephone system.
- ➔ The footprint normally has a diameter of **8000 km.**
- ➔ Because LEO satellites are close to Earth, the round-trip time propagation delay is normally less than **20 ms**, which is acceptable for audio communication.
- ➔ The LEO system is made of a constellation of **satellites that work together as a network**; each satellite acts as a switch. Satellites that are close to each other are connected through **inter satellite links (ISLs)**.
- ➔ A mobile system communicates with the satellite through a **user mobile link (UML).**

➔ A satellite can also communicate with an Earth station (gateway) through a **gateway link (GWL).**



➔ LEO satellites can be divided into **three** categories :

little LEOs, big LEOs and broadband LEOs.

The little LEOs operate under 1 GHz. They are mostly used for low-data-rate **messaging.**

- The big LEOs operate between 1 and 3 GHz.

  Globalstar and Iridium systems are examples of big LEOs.

➔ The broadband LEOs provide communication similar to fiber optic networks. The first broadband LEO system was **Teledesic**.

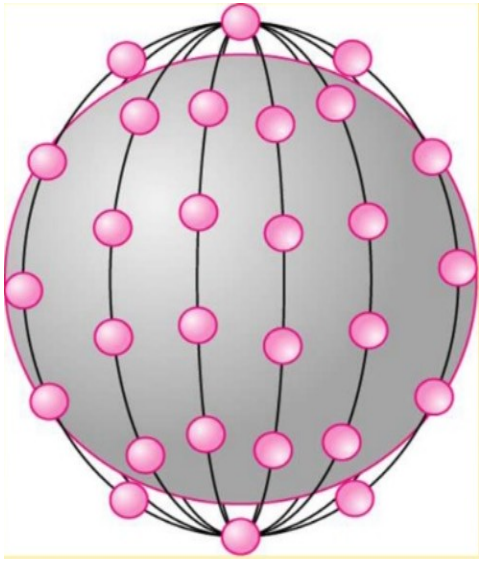
Iridium System :

➔ The concept of the Iridium system, a **77-satellite network**, was started by Motorola in 1990. The project took eight years to materialize. During this period, the number of satellites was reduced. Finally in 1998, the service was started with **66 satellites**. The original name, Iridium, came from the name of the 77th chemical element; a more appropriate name is **Dysprosium.**

➔ Iridium has gone through times. The system was halted in 1999 due to financial problems; it was sold and restarted in 2001 under new ownership.

➔ The system has 66 satellites divided into **six orbits, with 11 satellites** in each orbit. The orbits are at an **altitude of 750 km.**

- The satellites in each orbit are separated from one another by approximately **32° of latitude**. Figure shows a schematic diagram of the **constellation.**



- Since each satellite has **48 spot beams**, the system can have up to **3168 beams**. However some of the beams at any moment is approximately **2000.** Each spot beam covers a cell on Earth, which means that Earth is divided into approximately 2000 (**overlapping) cells**.
- In the Iridium system, communication between two users takes place through satellites. When a user calls another user, the call can go through several satellites before reaching the destination. This means that relaying is done in space and each satellite needs to be sophisticated enough to do relaying. This strategy **eliminates the need for many terrestrial stations.**

- The whole purpose of Iridium is to provide direct worldwide communication using handheld terminals. The system can be used for voice, data, paging, fax and even navigation.
- The system can provide connectivity between users at locations where other types of communication are not possible.
- The system provides **2.4 to 4.8 kbps** voice and data transmission between portable telephones.
- Transmission occurs in the **1.616 to 1.6126 GHz** frequency band. Inter satellite communication occurs in the **23.18 to 23.38 GHz** frequency band.

Globalstar :

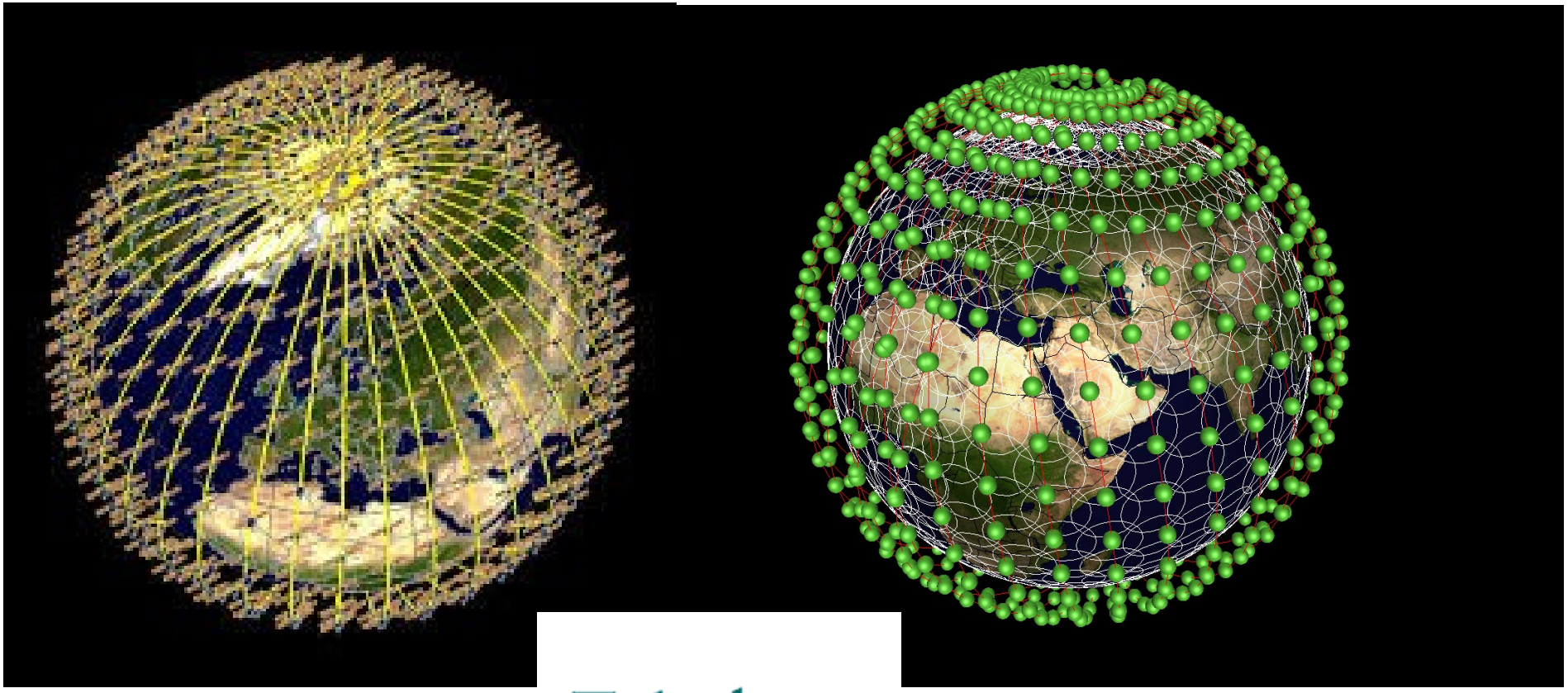
- Globalstar is another LEO satellite system. The system uses **48 satellites in six polar orbits** with each orbit hosting **eight satellites**. The orbits are located at an altitude of almost **1400 km.**

Difference between Iridium system and Globalstar system

- The Globalstar system is similar to the Iridium system; the main difference is the relaying mechanism.
- Communication between two distant users in the Iridium system requires relaying between several satellites; Globalstar communication requires both satellites and Earth stations, which means that ground stations can create more powerful signals.

Teledesic :

- Teledesic is a system of satellites that provides fiber-optic-like (broadband channels, low error rate and low delay) communication. Its main purpose is to provide broadband Internet access for users all over the world. It is sometimes called "**Internet in the sky**".
- The project was started in 1990 by Craig McCaw and Bill Gates; later, other investors joined the consortium. The project is scheduled to be fully functional in the near future.



Teledesic

Constellation

➔ Teledesic provides 288 satellites in 12 polar orbits with each orbit hosting 24 satellites. The orbits are at an altitude of 1350 km.

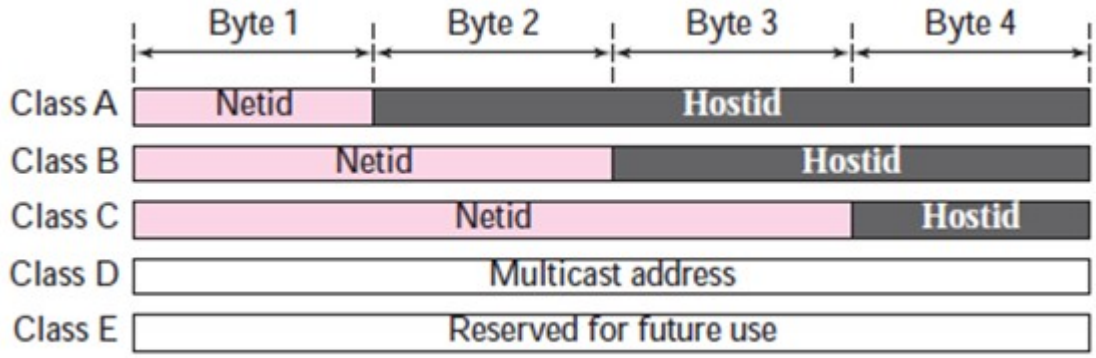
Communication

- The system provides three types of communication. Intersatellite communication allows **eight neighboring satellites** to communicate with one another. Communication is also possible between a satellite and an Earth gateway station. Users can communicate directly with the network using terminals. Earth is divided into **tens of thousands of cells**. Each cell is assigned a time slot, and the satellite focuses its beam to the cell at the corresponding **time slot**. The terminal can send data during its time slot. A terminal receives all packets intended for the cell, but selects only those intended for its address.

Bands Transmission occurs in the **Ka** bands.

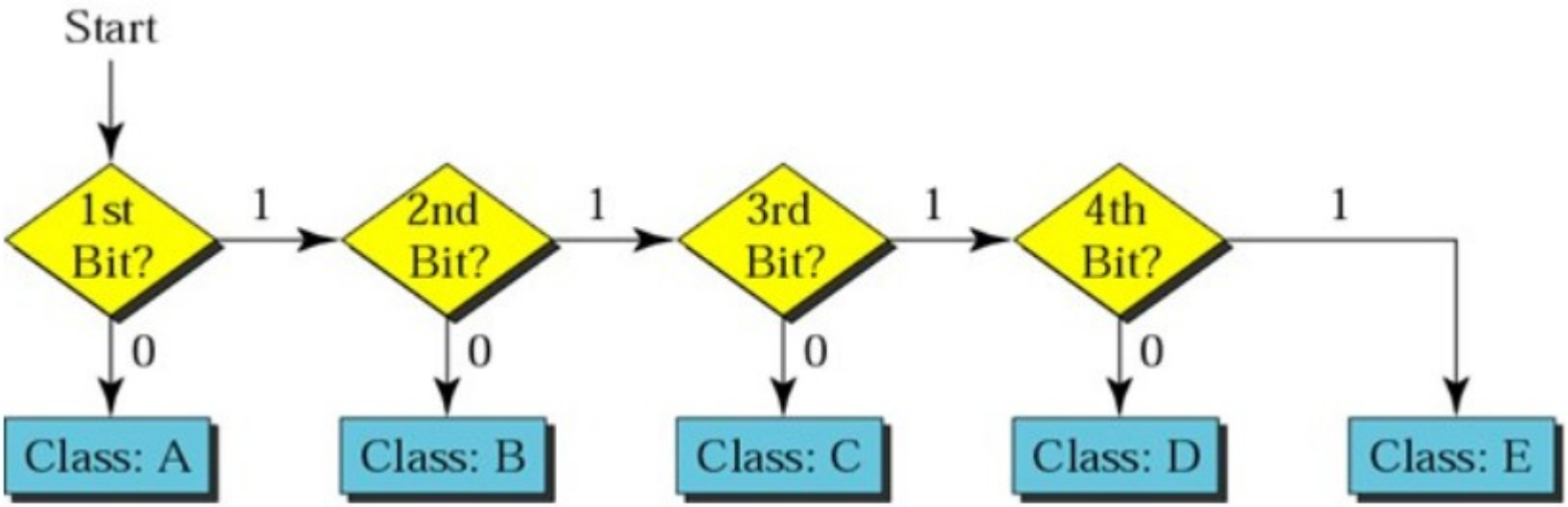
Data Rate The data rate is up to **155 Mbps** for the **uplink** and up to **1.2 Gbps** for the **downlink.**

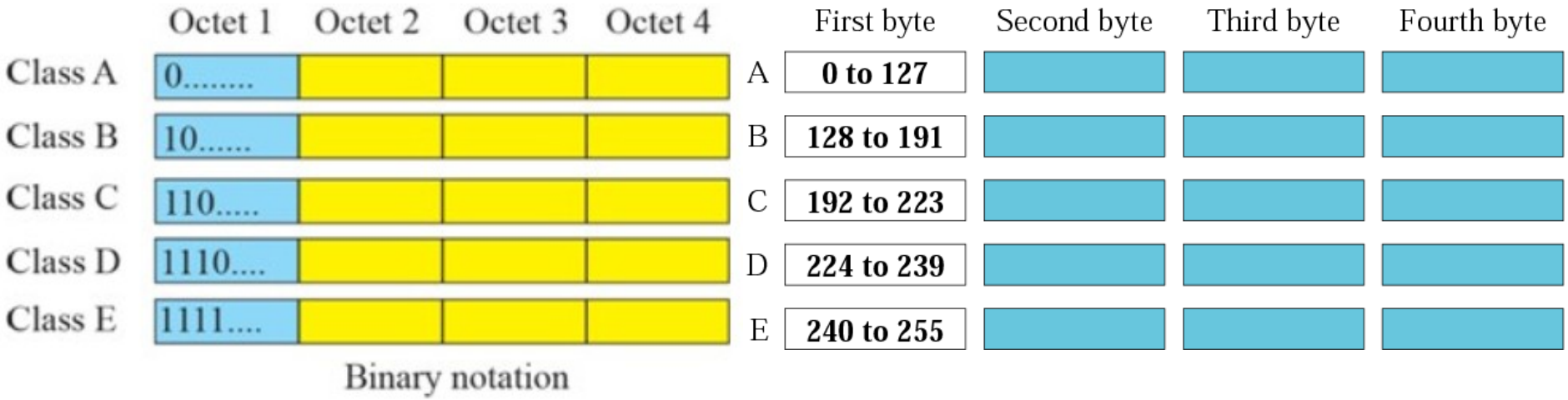
Classful IP Addressing

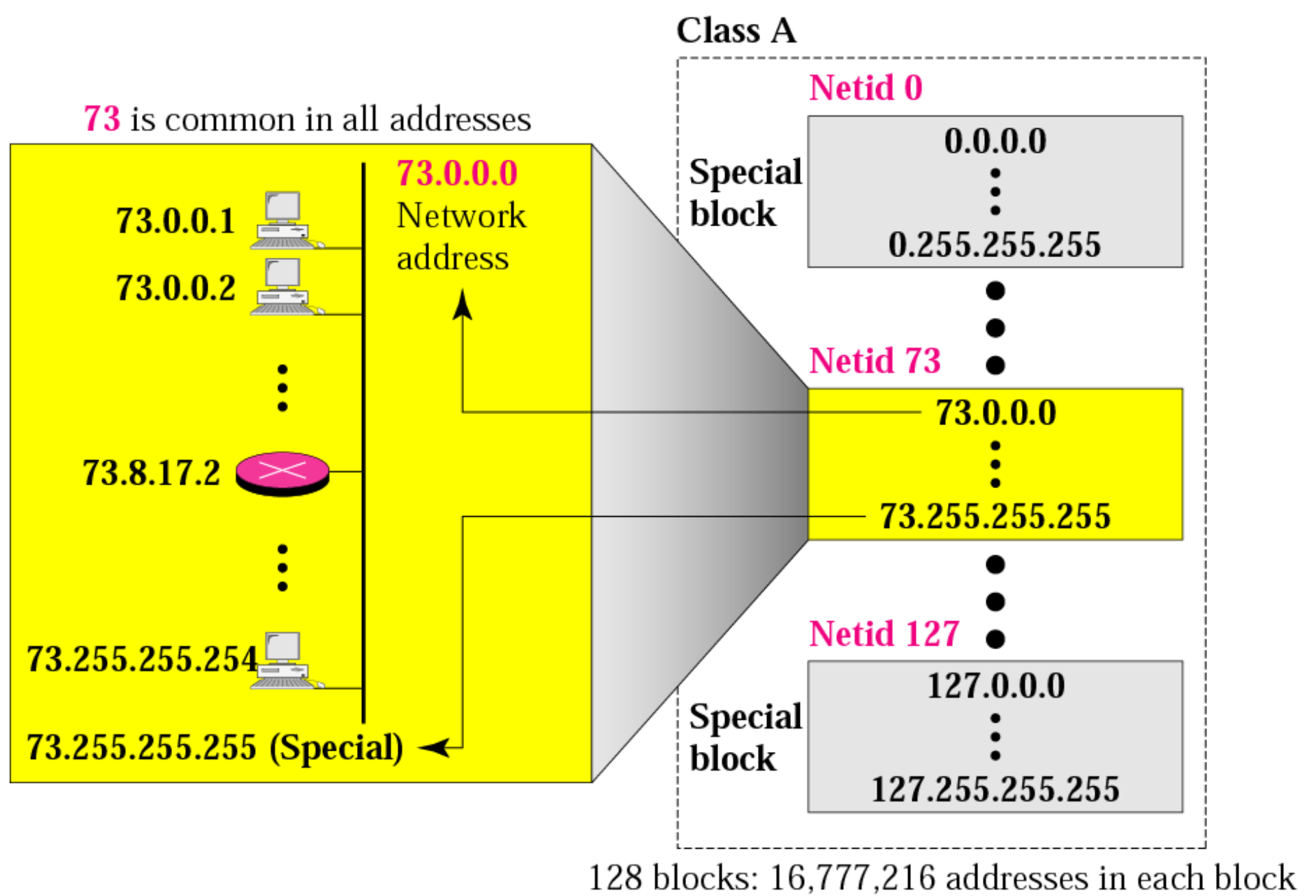


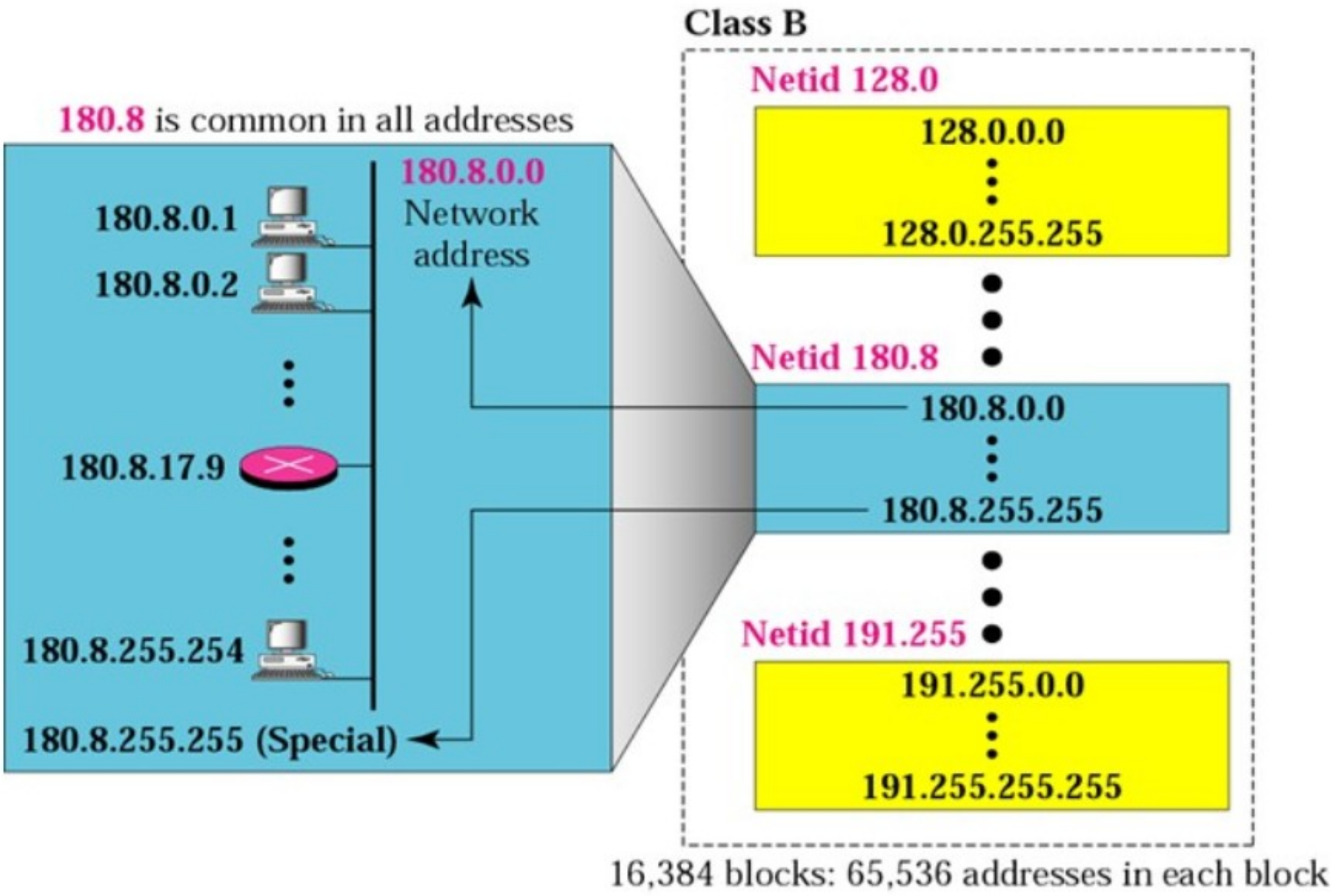
Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

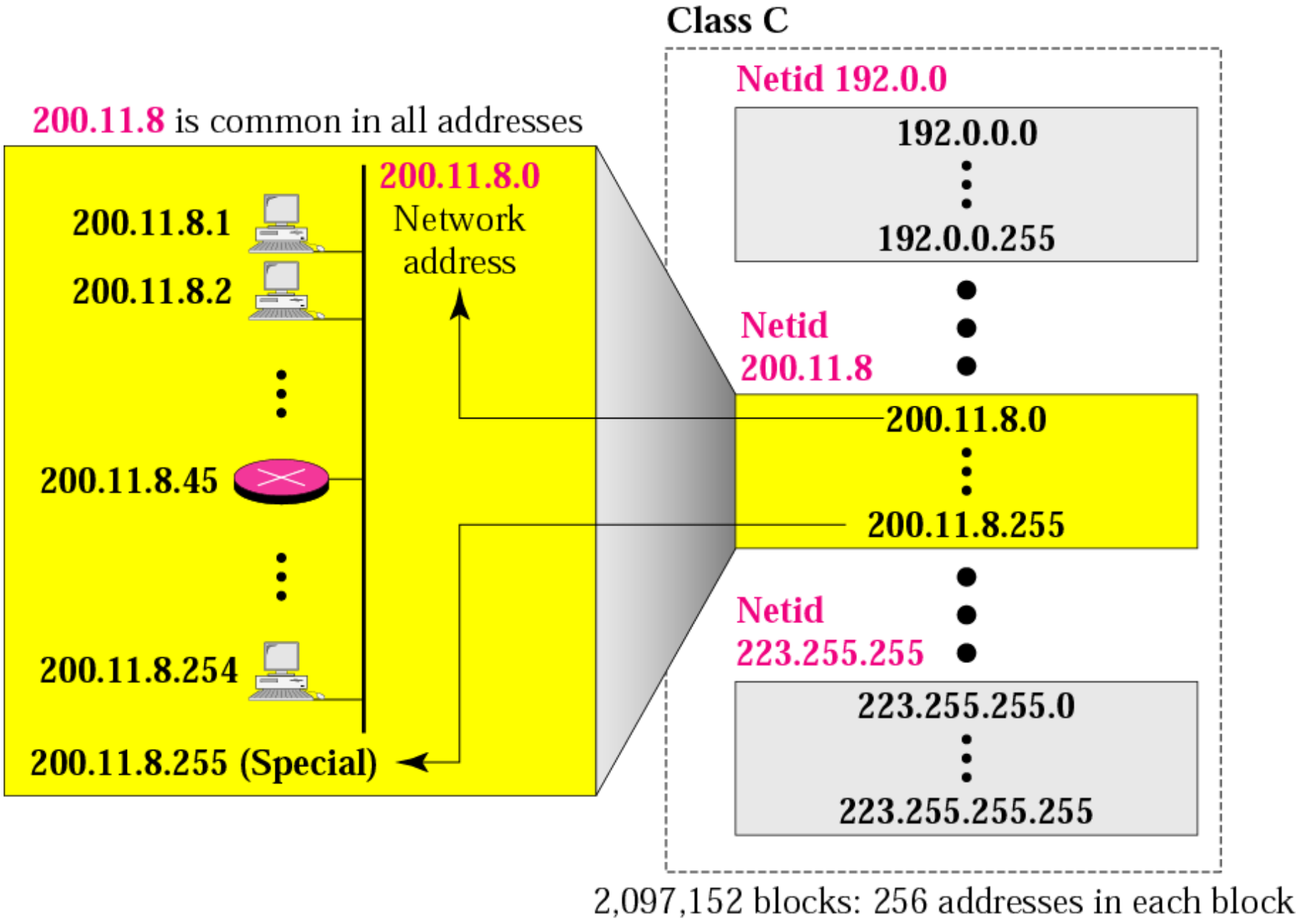
Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		


Start
1st Bit?
2nd Bit?
3rd Bit?
4th Bit?
1
1
1
1
0
0
0
0
Class: A
Class: B
Class: C
Class: D
Class: E


Octet 1
Octet 2
Octet 3
Octet 4
First byte
Second byte
Third byte
Fourth byte
Class A
0.....
A
0 to 127
Class B
10.....
B
128 to 191
Class C
110....
C
192 to 223
Class D
1110....
D
224 to 239
Class E
1111....
E
240 to 255
Binary notation


Class A
Netid 0
0.0.0.0
Special block
0.255.255.255
Netid 73
73.0.0.0
73.255.255.255
Netid 127
127.0.0.0
Special block
127.255.255.255
73 is common in all addresses
73.0.0.0
Network address
73.0.0.1
73.0.0.2
73.8.17.2
73.255.255.254
73.255.255.255 (Special)
128 blocks: 16,777,216 addresses in each block

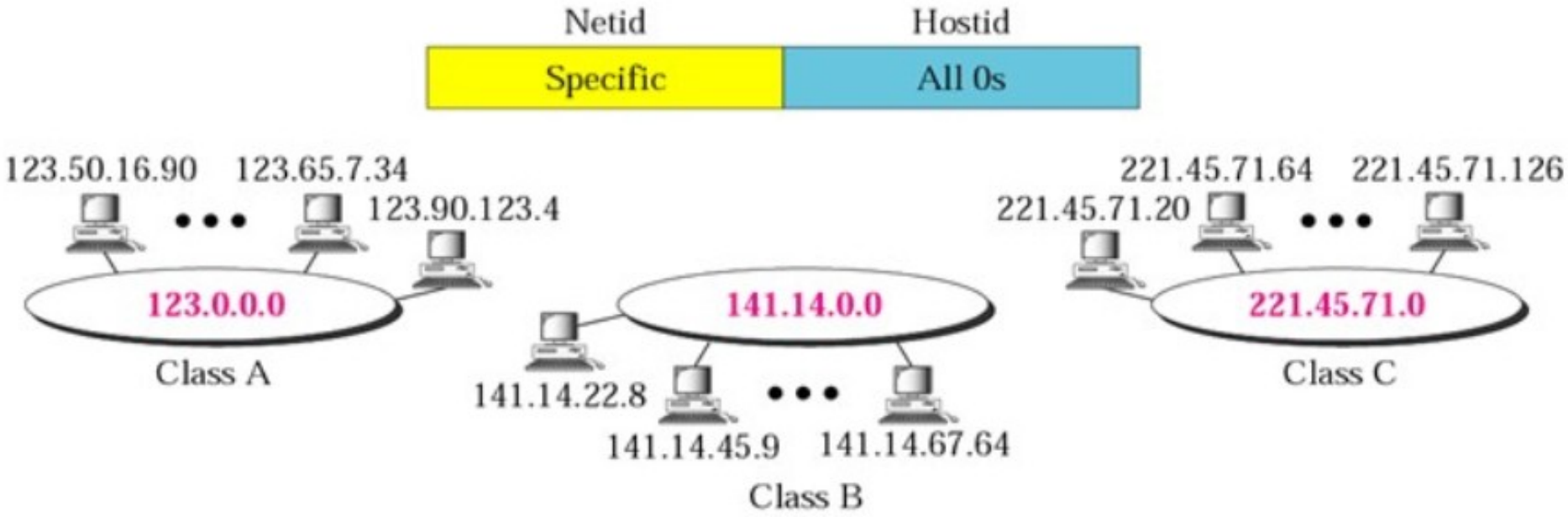

Class B
Netid 128.0
128.0.0.0
128.0.255.255
Netid 180.8
180.8.0.0
180.8.255.255
Netid 191.255
191.255.0.0
191.255.255.255
180.8 is common in all addresses
180.8.0.0
Network address
180.8.0.1
180.8.0.2
180.8.17.9
180.8.255.254
180.8.255.255 (Special)
16,384 blocks: 65,536 addresses in each block


Class C
Netid 192.0.0
192.0.0.0
192.0.0.255
200.11.8 is common in all addresses
200.11.8.0
Network
address
200.11.8.1
200.11.8.2
200.11.8.45
200.11.8.254
200.11.8.255 (Special)
Netid
200.11.8
200.11.8.0
200.11.8.255
Netid
223.255.255
223.255.255.0
223.255.255.255
2,097,152 blocks: 256 addresses in each block

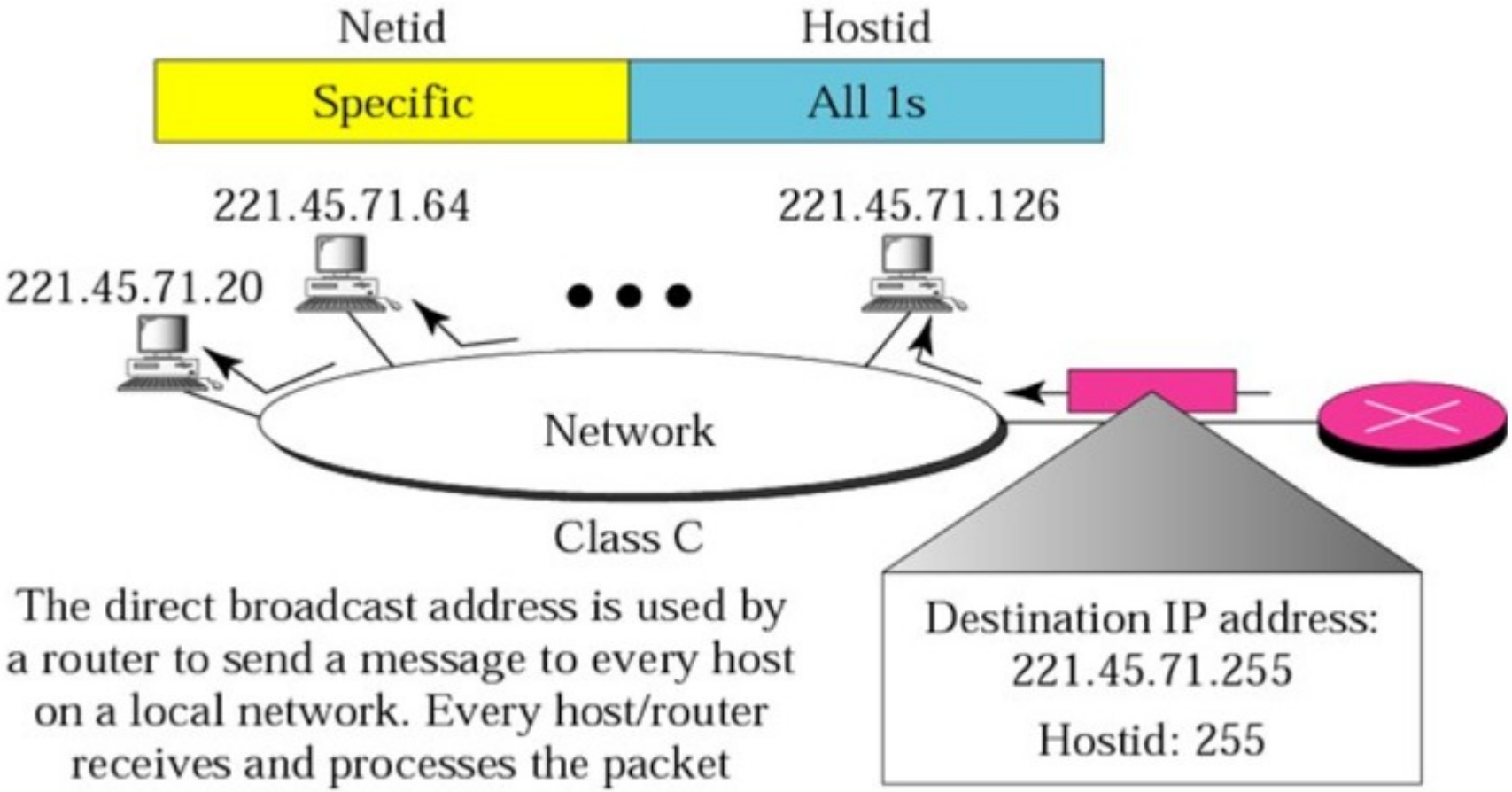
Special Addressing

Special Address	*Netid*	*Hostid*	*Source or Destination*
Network address	Specific	All 0s	None
Direct broadcast address	Specific	All 1s	Destination
Limited broadcast address	All 1s	All 1s	Destination
This host on this network	All 0s	All 0s	Source
Specific host on this network	All 0s	Specific	Destination
Loopback address	127	Any	Destination

Network Address

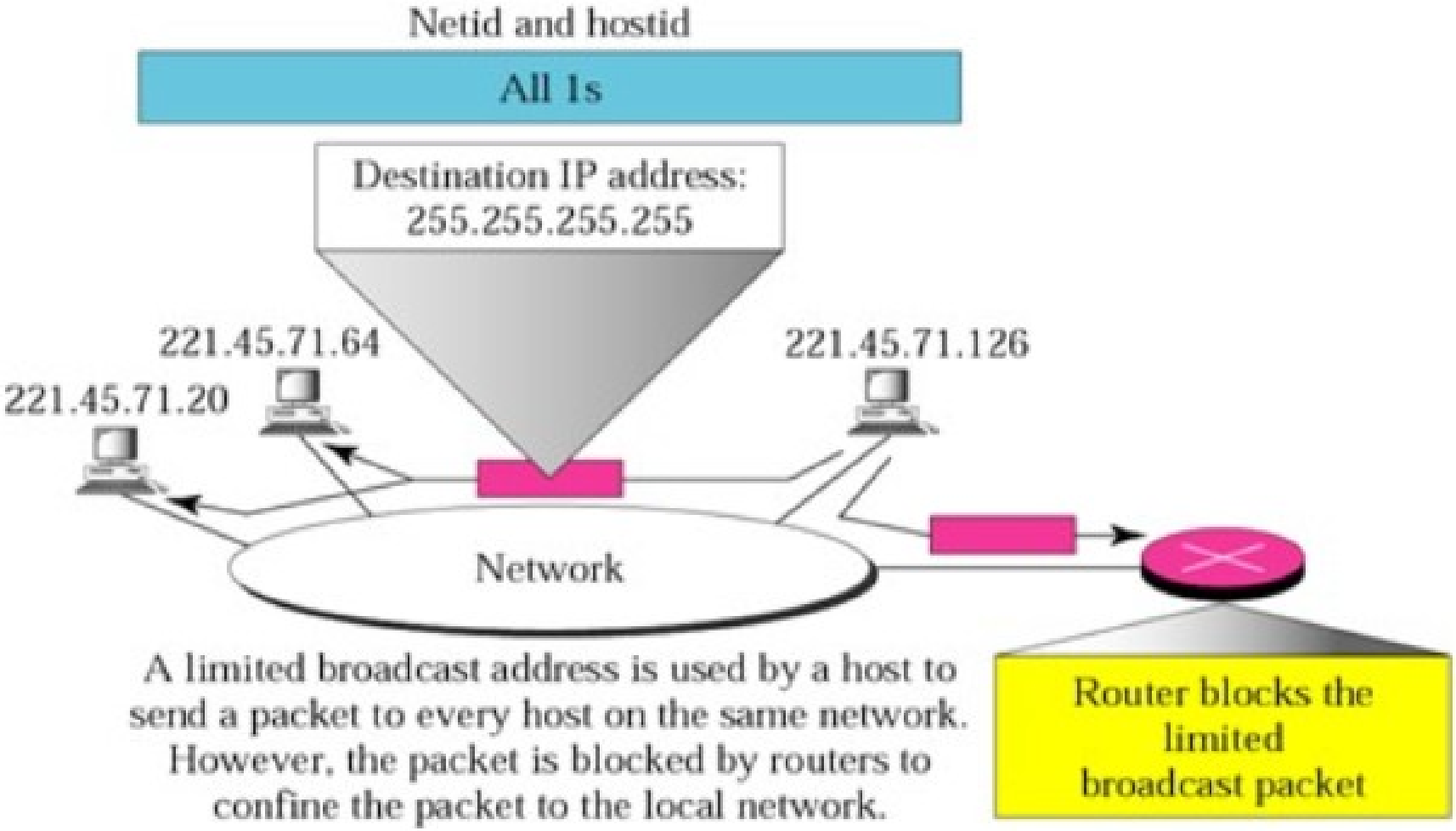


Direct Broadcast Address

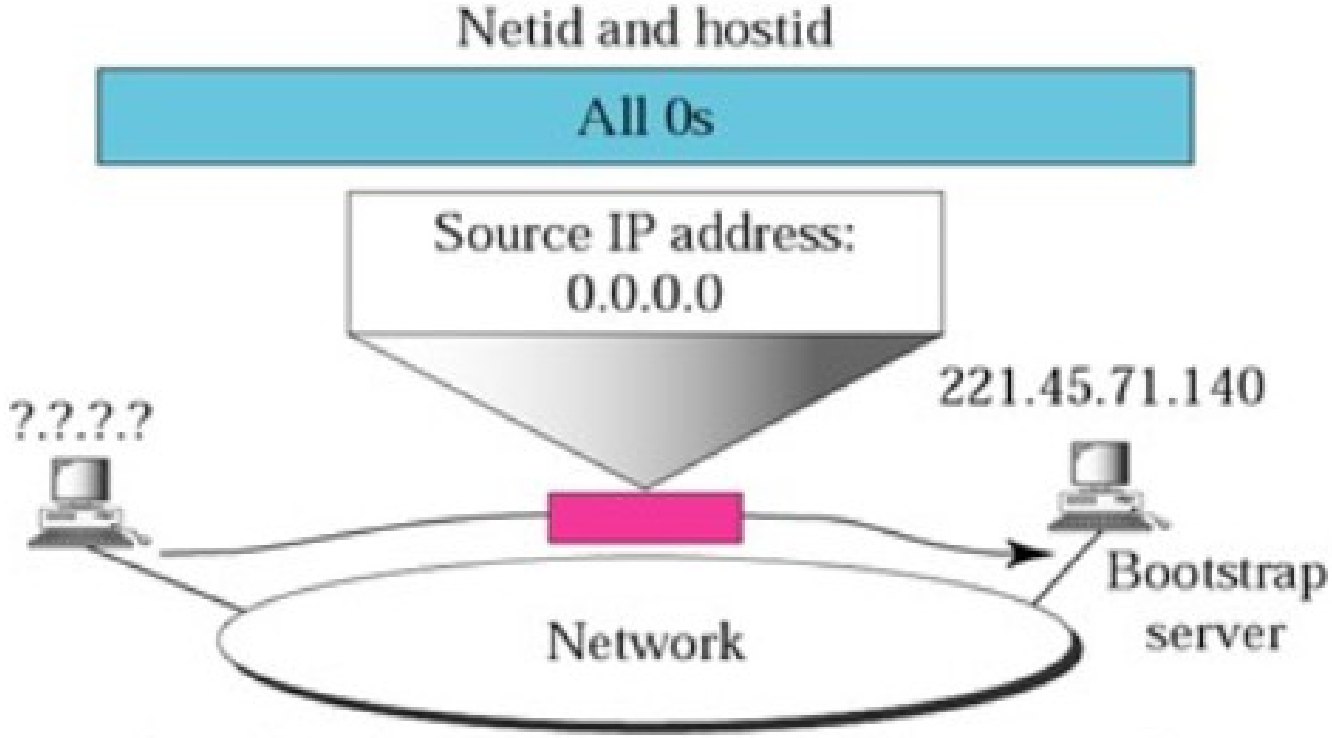


The direct broadcast address is used by a router to send a message to every host on a local network. Every host/router receives and processes the packet with a direct broadcast address.

Limited Broadcast Address

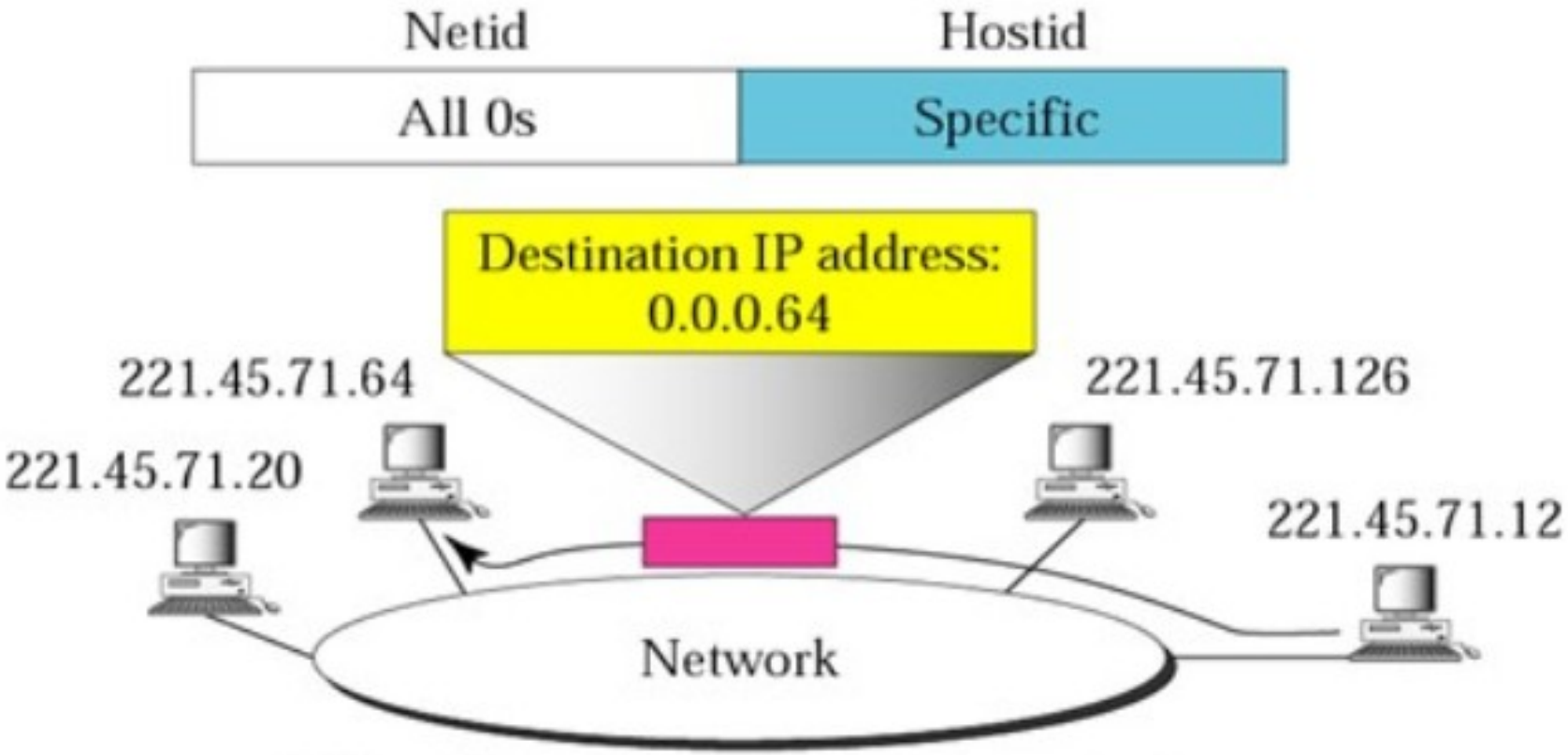


This host on this network



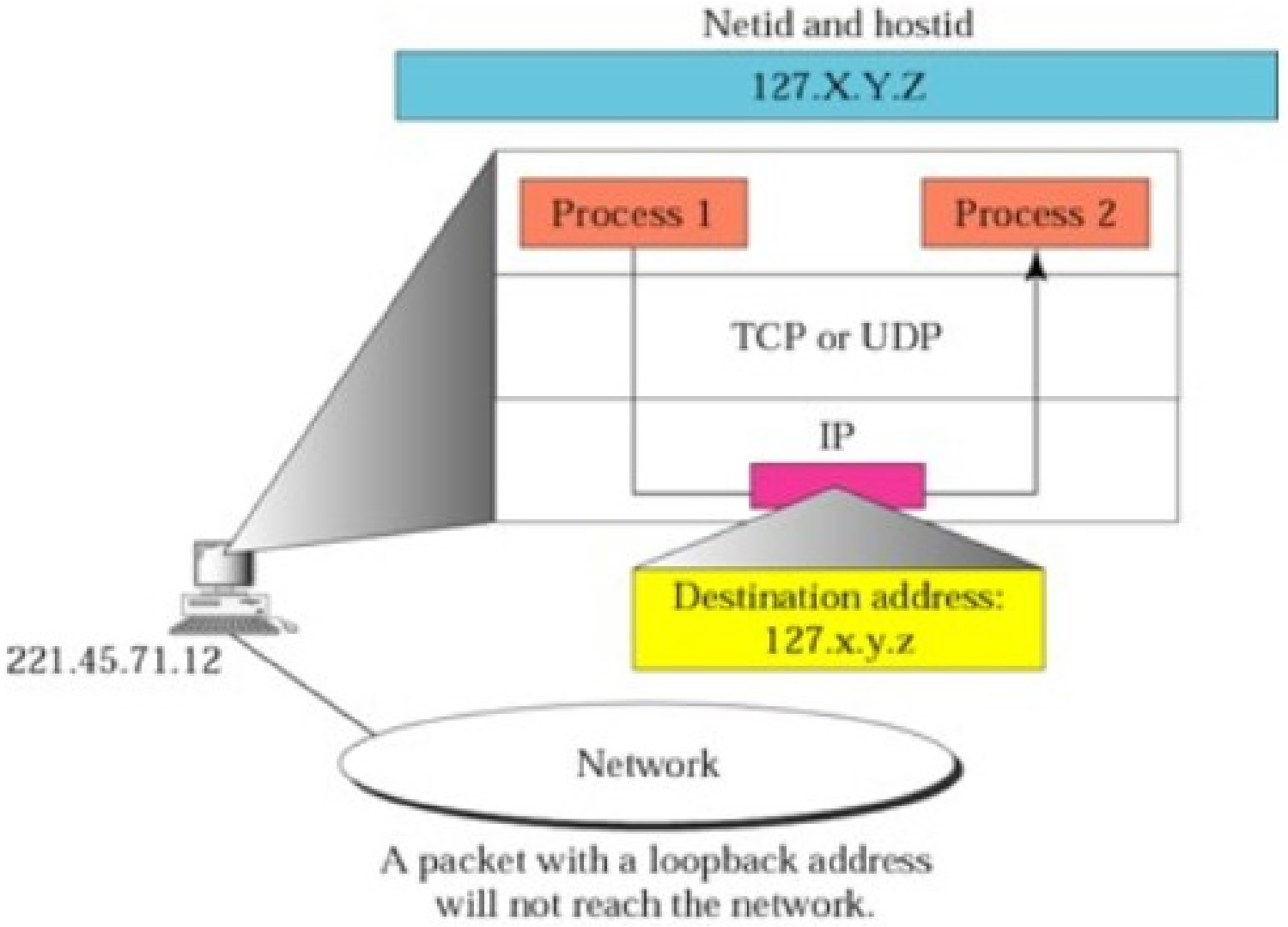
A host that does not know its IP address uses the IP address 0.0.0.0 as the source address and 255.255.255.255 as the destination address to send a message to a bootstrap server.

Specific host on this network



This address is used by a router or host
to send a message to a specific host on the same network.

Loopback Address



Private Address

Class	Netids	Blocks
A	10.0.0	1
B	172.16 to 172.31	16
C	192.168.0 to 192.168.255	256

Private addresses block

Table 5.2 *Addresses for private networks*

Block	Number of addresses	Block	Number of addresses
10.0.0.0/8	16,777,216	192.168.0.0/16	65,536
172.16.0.0/12	1,047,584	169.254.0.0/16	65,536

Unicast, Multicast, and Broadcast Addrsses

- **Unicast addresses**. Unicast communication is one-to-one. When a packet is sent from an individual source to an individual destination, a unicast communication takes place
- **Multicast addresses**. Multicast communication is one-to-many. When a packet is sent from an individual source to a group of destination, a multicast communication takes place
- **Broadcast Addresses**. Broadcast communication is one-to-all. The Internet allows broadcasting only at the local level

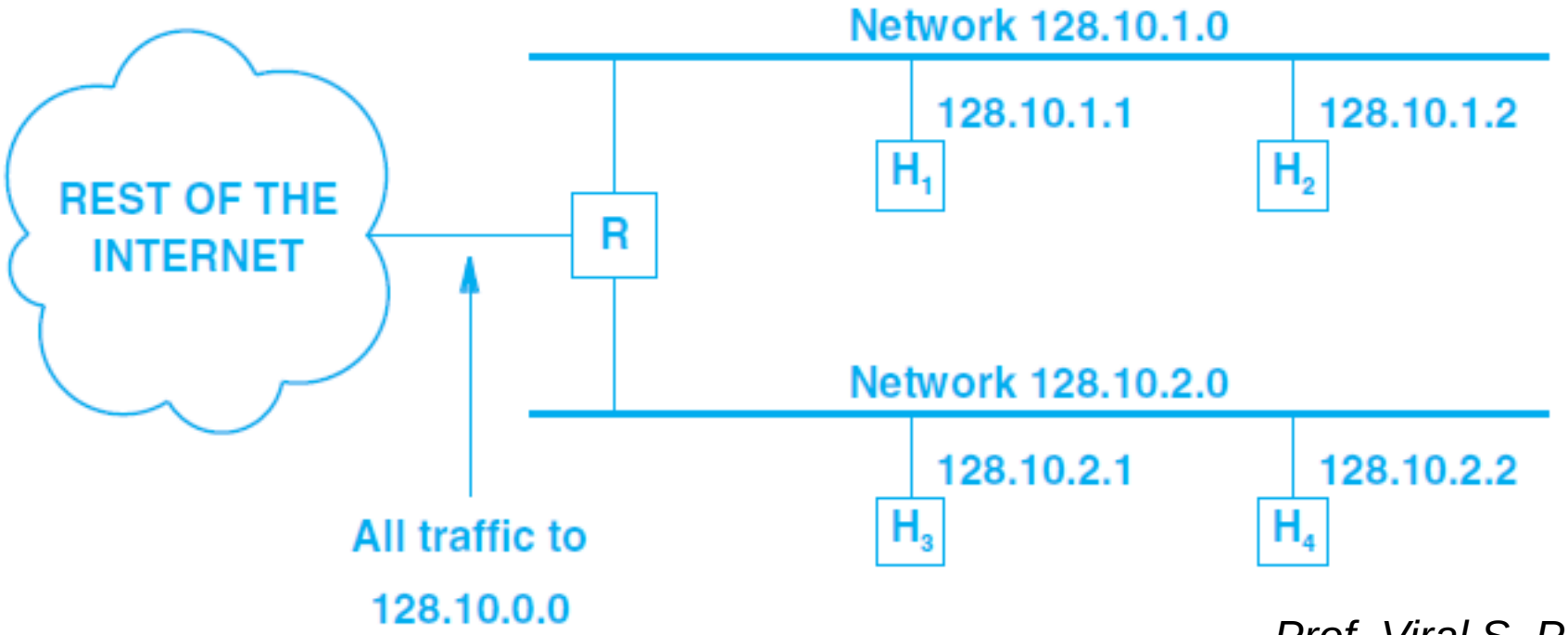
Subnetting

Problem :

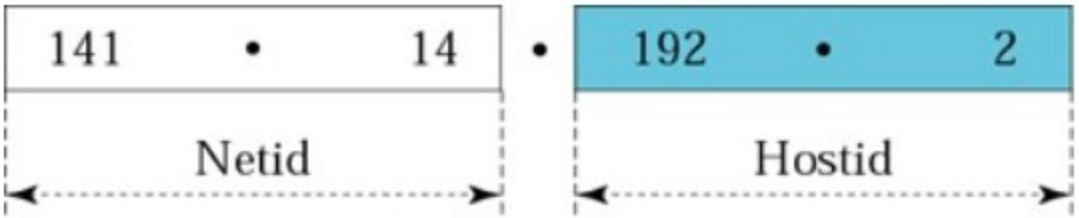
In the early 1980s, as Local Area Networks became widely available, it became apparent that the classful addressing scheme would have insufficient network addresses.

Solution :

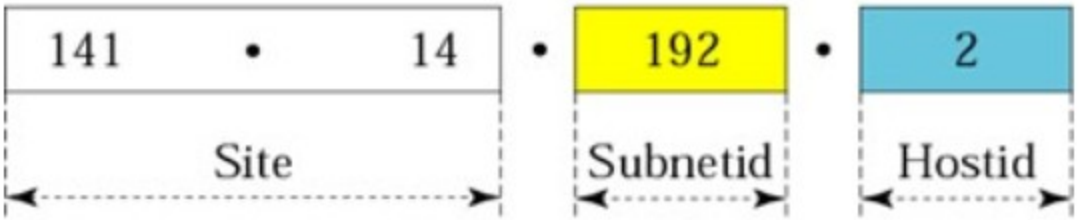
➔ ***subnet addressing*** *or* ***subnetting :*** Subnetting allows a single network prefix to be used for multiple physical networks



Subnetting



a. Without subnetting



b. With subnetting

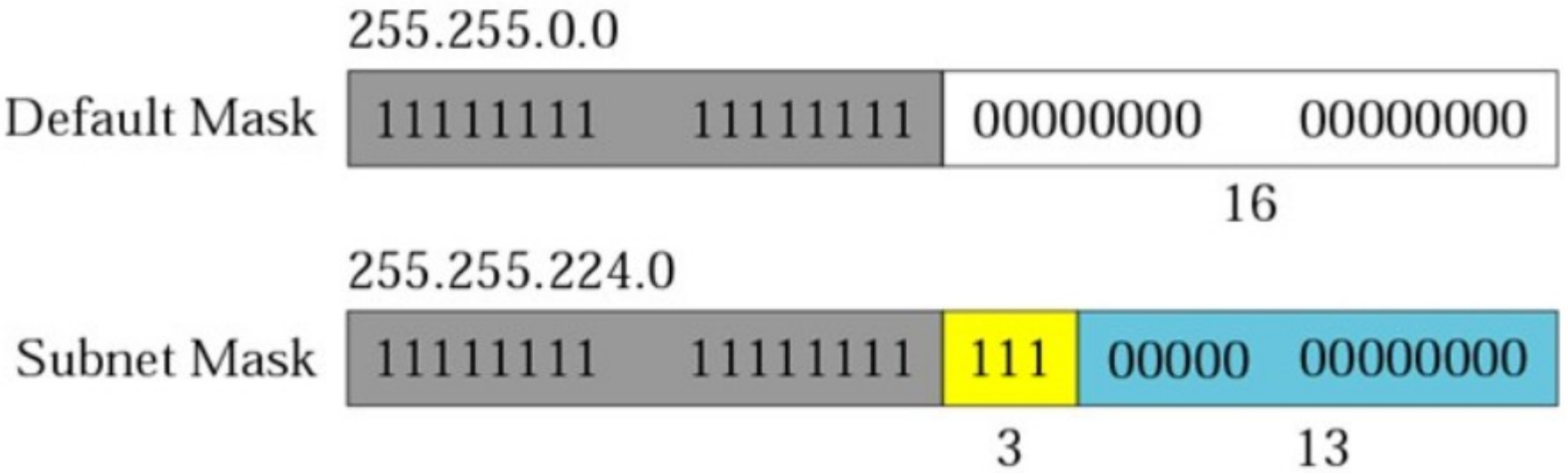
Default Mask

Class	*Mask in binary*	*Mask in dotted-decimal*
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

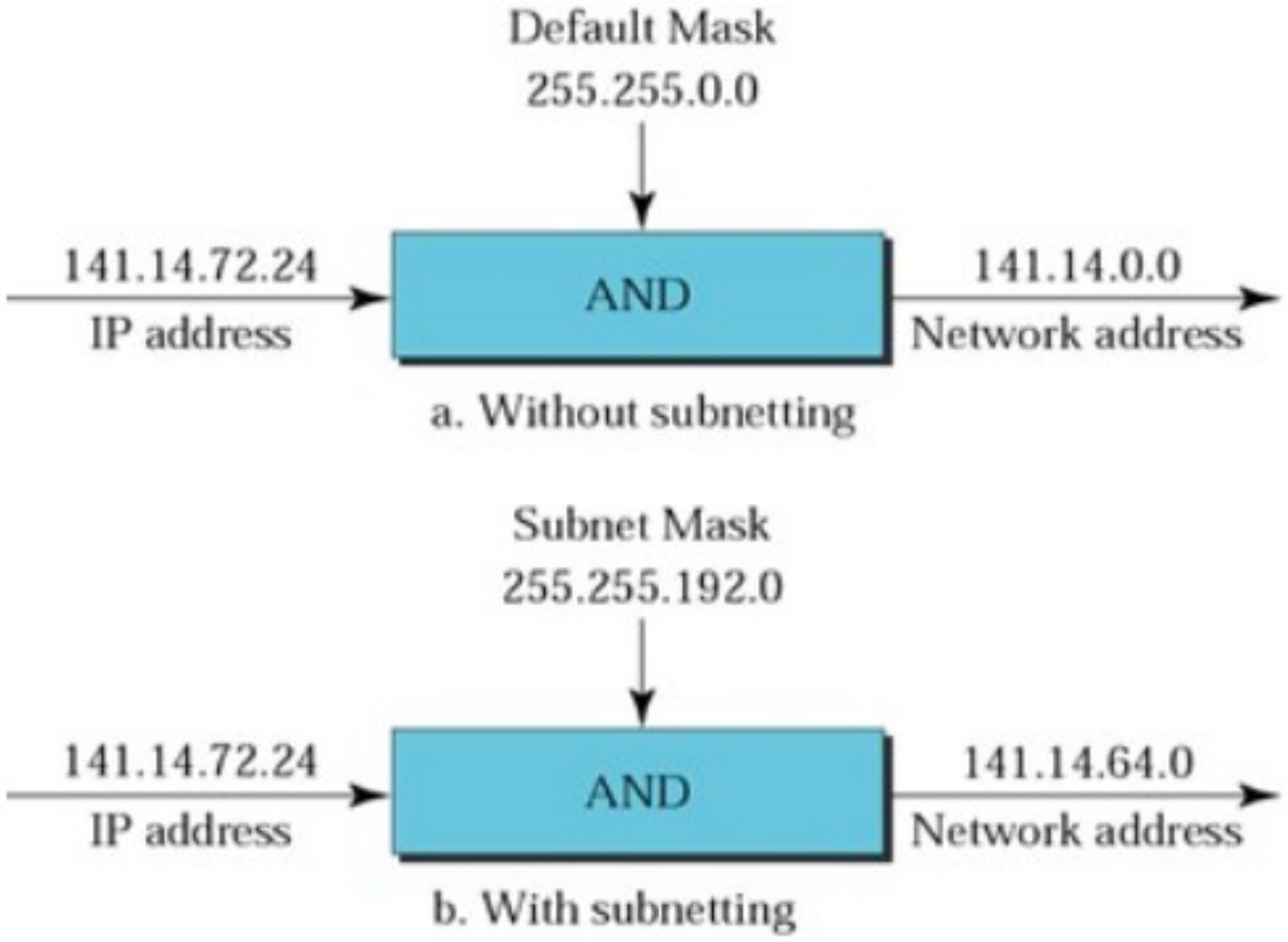
Subnet Mask

Number of Subnetworks/ Number of Addresses per Subnet

- The number of subnetworks can be found by counting the extra 1s that are added to the default mask to make the subnetmask
- The number of addresses per subnetwork can be found by counting the number of 0s in the subnet mask



Subnet Mask


Default Mask
255.255.0.0
141.14.72.24
IP address
AND
141.14.0.0
Network address
a. Without subnetting
Subnet Mask
255.255.192.0
141.14.72.24
IP address
AND
141.14.64.0
Network address
b. With subnetting

CIDR notation

The CIDR – **Classless InterDomain Routing**, notation used to explicitly indicate default mask or subnet mask.

In this notation, the number of 1s in the mask is specified after a slash at the end of the address.

For **example** :

18.48.74.10**/8** show that eight 1s in the mask means default mask is 255.0.0.0

141.14.192.3/**18** show that eighteen 1s in the mask means subnet mask is 255.255.192.0

Variable Length Subnet Addressing

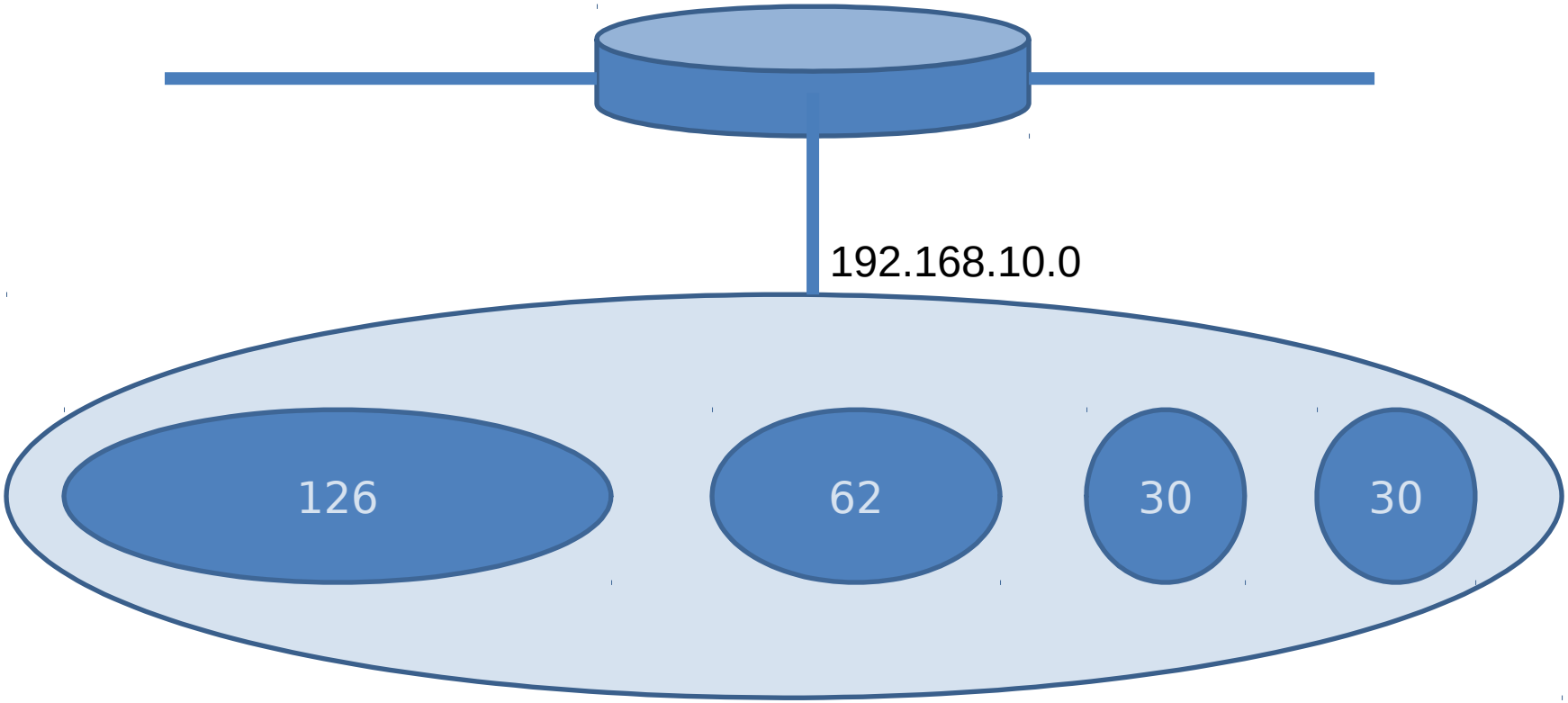
Example: We want to divide **192.168.10.0**, which is a Class C network, into four networks, each with unequal number of IPv4 addresses requirements as shown below.

Subnet A: 126 IPv4 Addresses.
Subnet B : 62 IPv4 Addresses.
Subnet C : 30 IPv4 Addresses.
Subnet D : 30 IPv4 Addresses.

Prof. Viral S. Patel

Prof. Viral S. Patel

Variable Length Subnet Addressing



Variable Length Subnet Addressing

➔Original Network (Network to be subnetted) – **192.168.10.0/24 Class C**

Step 1 : **For 126 IPv4 addresses : subnet A**

11000000.10101000.00001010.00000000 192.168.10.0
net id host id

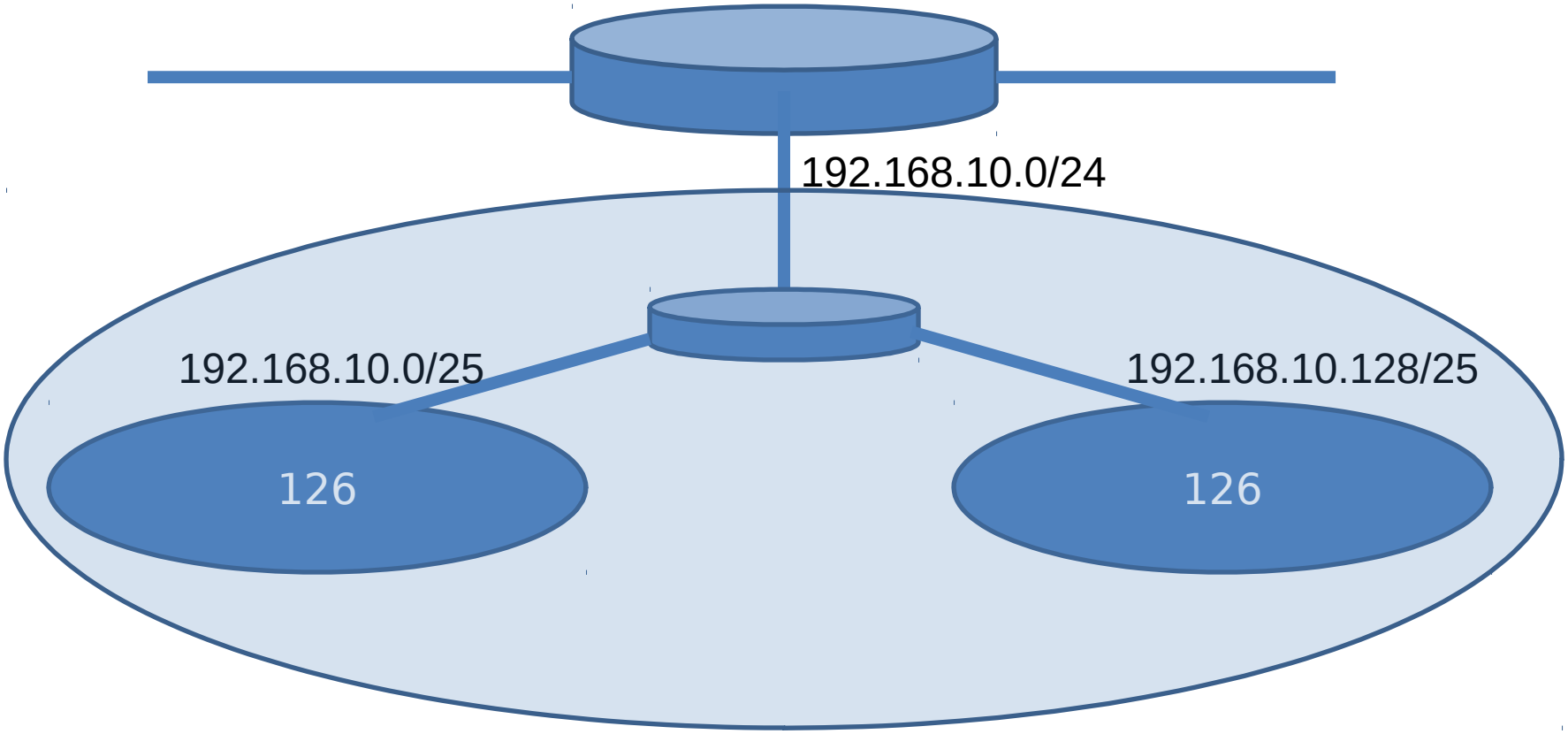
2^7 = 128 so 7 bits for host id and 1 bit for subnet id

11111111.11111111.11111111.10000000 subnet mask

11000000.10101000.00001010.00000000 192.168.10.0/25
11000000.10101000.00001010.10000000 192.168.10.128/25

So divide the two networks equally with 128 IPv4 addresses (126 usable IPv4 addresses) in each network using 255.255.255.128 subnet mask (192.168.10.0/25).

Variable Length Subnet Addressing



Variable Length Subnet Addressing

➔ we take 192.168.10.0/25 block for 126 IPv4 addresses so remaining 192.168.10.128/25 block is free.

Step 2 : **For 62 IPv4 addresses : subnet B**

11000000.10101000.00001010.10000000 192.168.10.128/25
net id host id

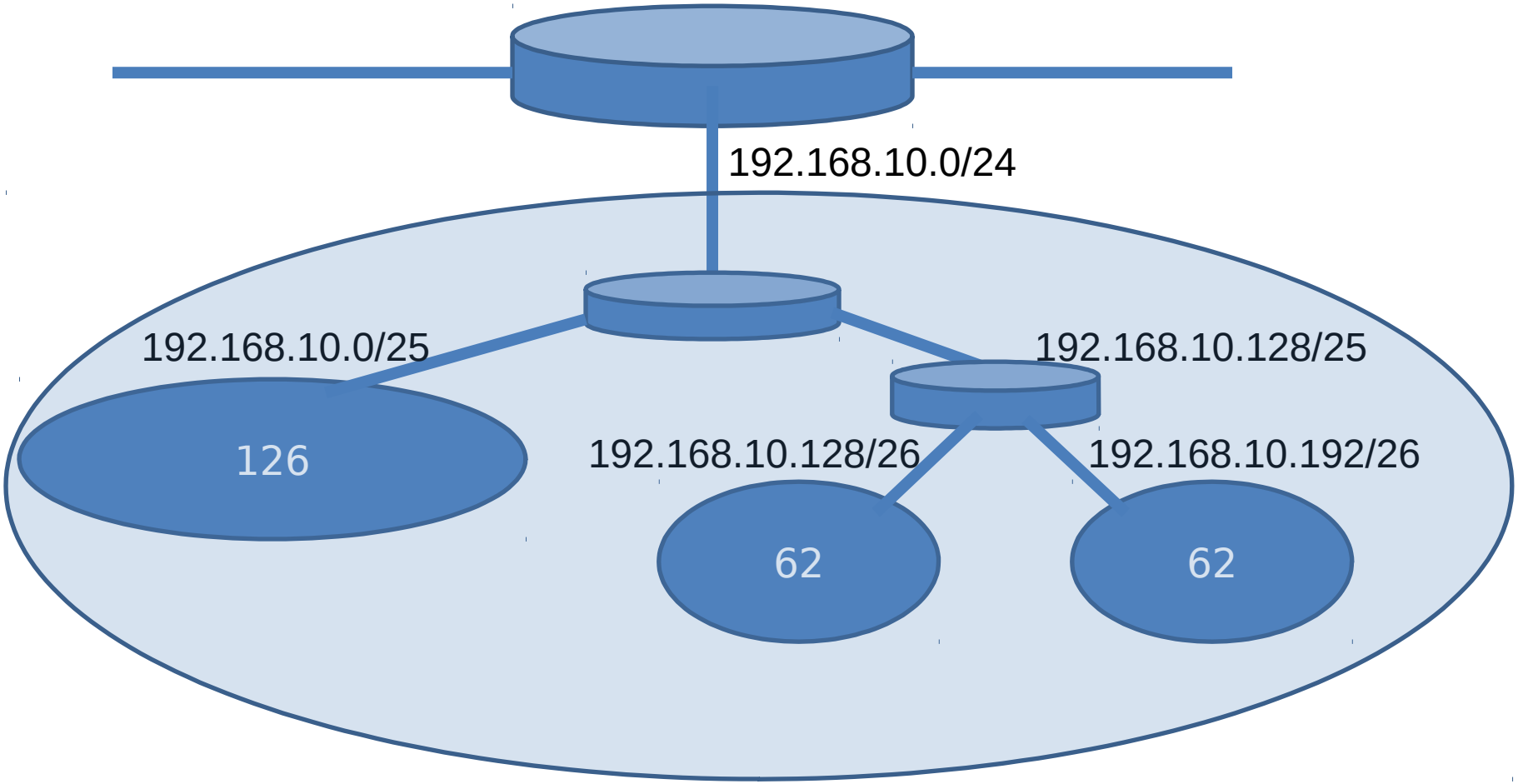
2^6 = 64 so 6 bits for host id

11111111.11111111.11111111.11000000 subnet mask

11000000.10101000.00001010.10000000 192.168.10.128/26
11000000.10101000.00001010.11000000 192.168.10.192/26

So divide second subnet (192.168.10.128/25) we got from the first division again into two Networks, each with 64 IP Addresses (62 usable IPv4 addresses) using 255.255.255.192 subnet mask

Variable Length Subnet Addressing



Variable Length Subnet Addressing

➔ we take 192.168.10.128/26 block for 62 IPv4 addresses so remaining 192.168.10.192/26 block is free.

Step 2 : **For 30 IPv4 addresses : subnet C and subnet D**

11000000.10101000.00001010.11000000 192.168.10.192/26
net id host id

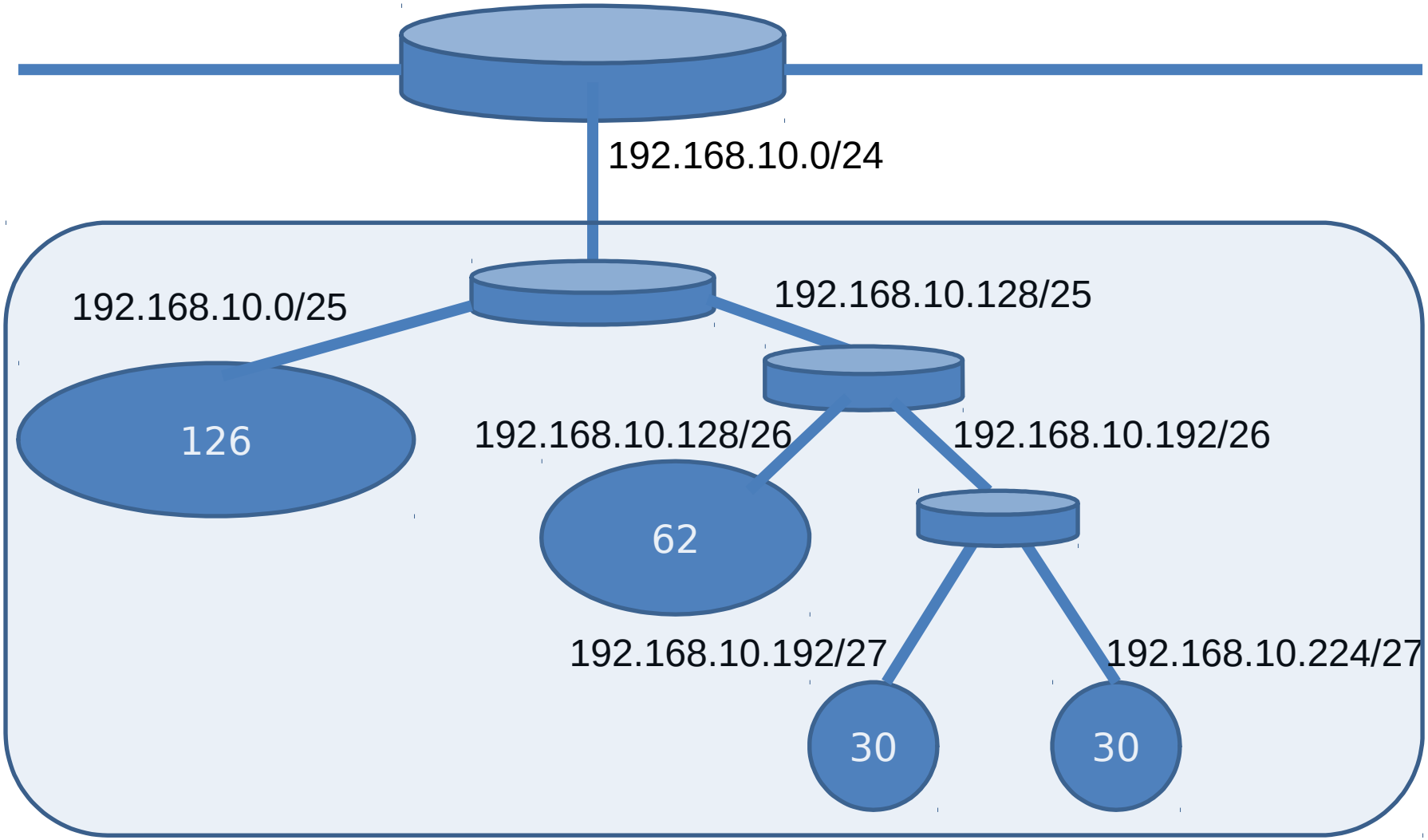
2^5 = 64 so 5 bits for host id

11111111.11111111.11111111.11100000 subnet mask

11000000.10101000.00001010.11000000 192.168.10.192/27
11000000.10101000.00001010.11100000 192.168.10.224/27

So divide 192.168.10.192/26 Network again into two Networks, each with 32 IPv4 addresses (30 usable IPv4 addresses) using 255.255.255.224 subnet mask.

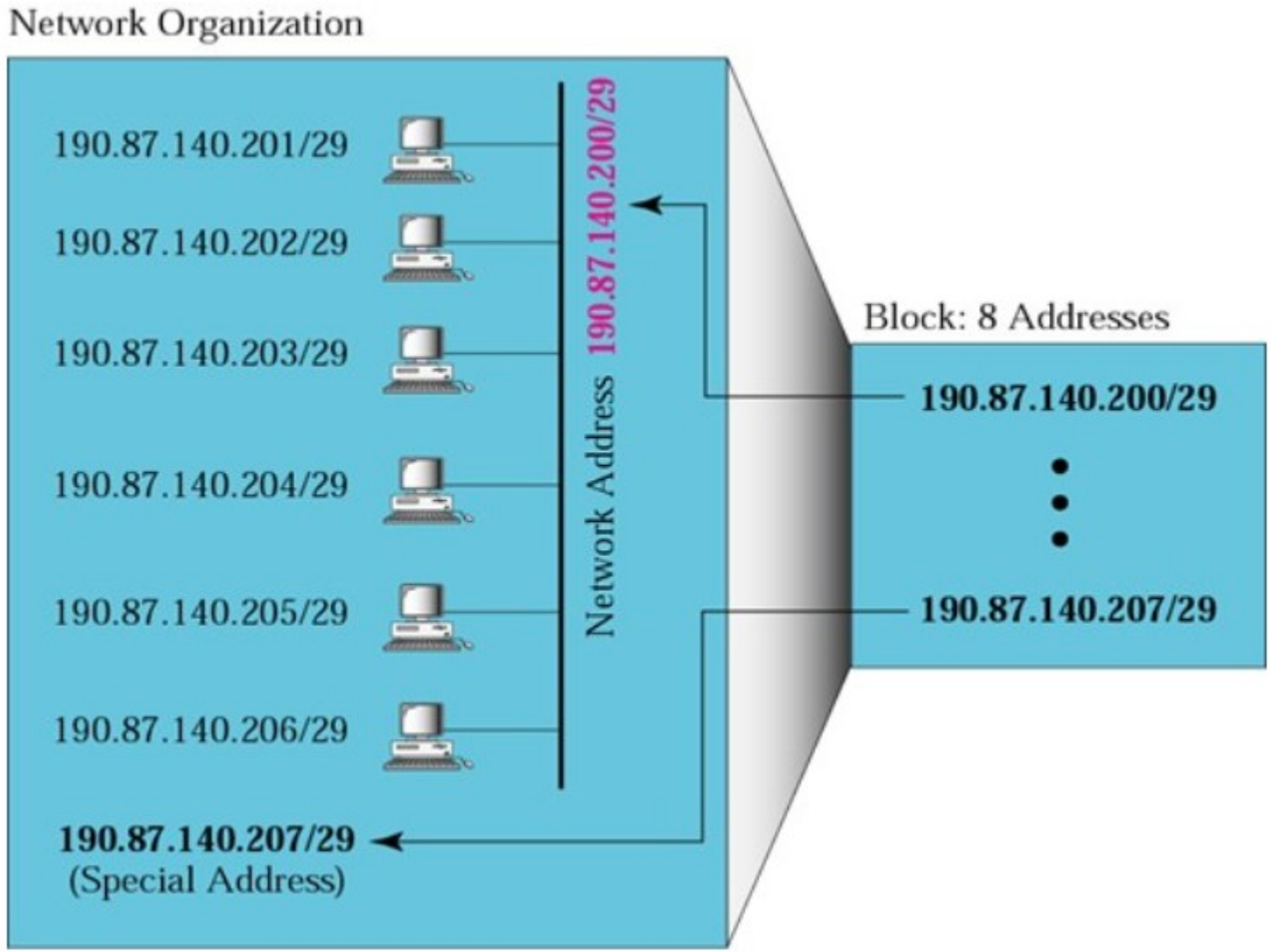
Variable Length Subnet Addressing



Variable Length Subnet Addressing

1) 192.168.10.0 - 192.168.10.127 (126 (128-2) usable IPv4 addresses)
2) 192.168.10.128 - 192.168.10.191 (62 (64-2) usable IPv4 addresses)
3) 192.168.10.192 - 192.168.10.223 (30 (32-2) usable IPv4 addresses)
4) 192.168.10.224 - 192.168.10.255 (30 (32-2) usable IPv4 addresses)

Prof. Viral S. Patel


Network Organization
190.87.140.201/29
190.87.140.202/29
190.87.140.203/29
190.87.140.204/29
190.87.140.205/29
190.87.140.206/29
190.87.140.207/29
(Special Address)
Network Address 190.87.140.200/29
Block: 8 Addresses
190.87.140.200/29
190.87.140.207/29

Variable Length Subnet Addressing

A small organization is given a block with the beginning address and the prefix length **205.16.37.24/29** (in slash notation). What is the range of the block? What is beginning address and ending address of it ?

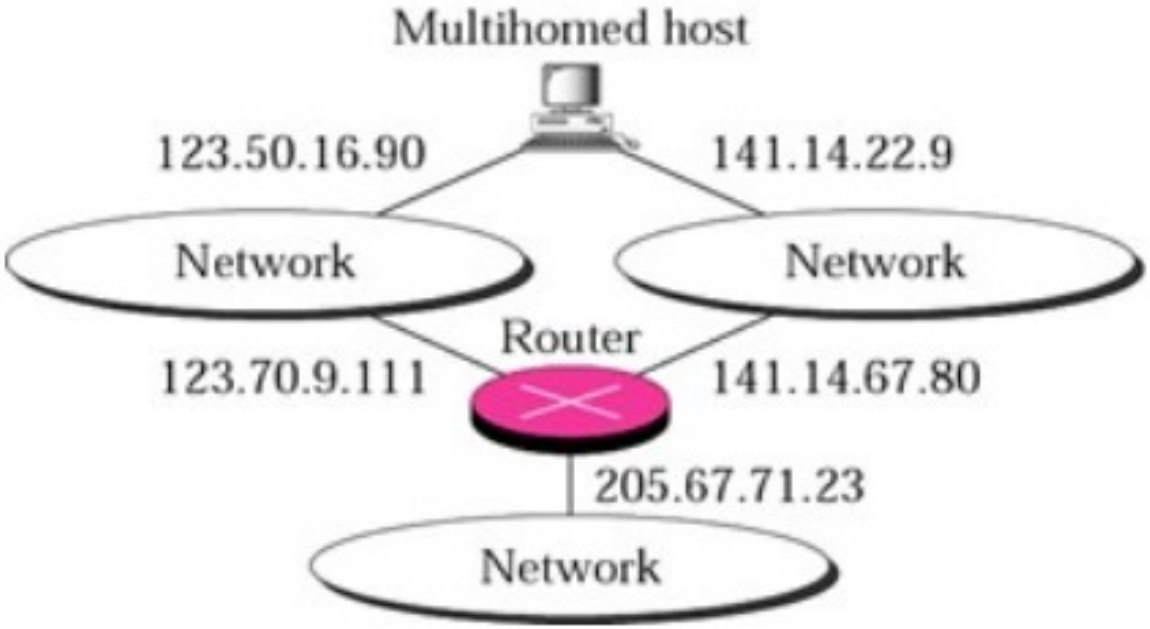
Solution :

Prof. Viral S. Patel

Beginning: **11001111 00010000 00100101 00011**000
Ending : **11001111 00010000 00100101 00011**111
There are only 8 addresses in this block.

We can argue that the length of the suffix is 32 - 29 or 3. So there are $2^3 = 8$ addresses in this block. If the first address is 205.16.37.24, the last address is 205.16.37.31 (24 + 7 = 31).

Prof. Viral S. Patel


Multihomed host
123.50.16.90
141.14.22.9
Network
Network
Router
123.70.9.111
141.14.67.80
205.67.71.23
Network

Ad hoc network / MANNET :

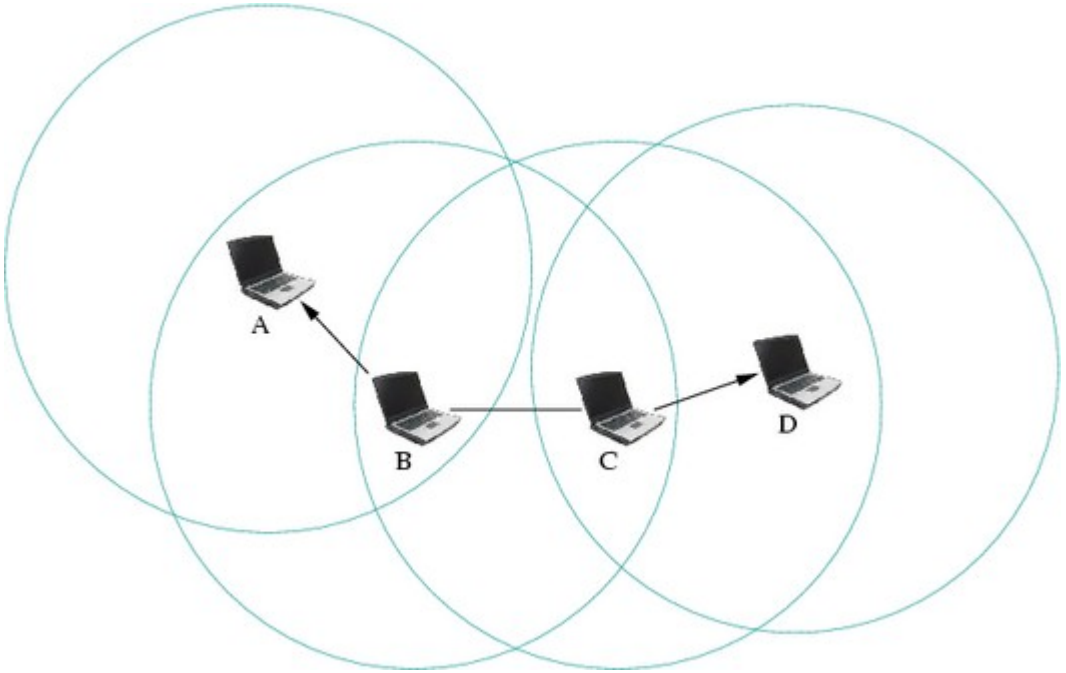
A **mobile ad hoc network (MANET) is an autonomous system of nodes connected by wireless links to form a network. Messages are exchanged and relayed between nodes.**

In fact, an ad hoc network has the capability of making communications possible even between two nodes that are not in direct range with each other, data packets are transmitted from a source to a destination via intermediate nodes.

Intermediate nodes serve as routers using a routing algorithm in this case.

Hence, a MANNET may spread over a large distance, provided that its ends are interconnected by a chain of links between nodes (also called routers).

In the ad hoc network shown in figure Node A can communicate with node D via nodes B and C, and vice versa.



Wireless sensor networks:

Wireless sensor networks are a special class of ad hoc networks, composed of devices equipped with sensors to monitor temperature, sound or any other environmental condition.

Sensor networks are very useful in unpredictable, unreliable environments.

Sensor networks are primarily **data collection points**. They are widely used in defense, environment, meteorology and study of nature.

A wireless sensor network is a collection of **low-cost, low-power disposable devices.**

Prof. Viral S. Patel

Each of these devices holds **sensing, memory and communication modules.**

Sensors may not have any **power source** other than **small batteries.** Therefore power control is a major challenge in sensor networks to ensure long life of the network.

Study of the movement of glaciers(snow fall) is done through wireless ad hoc networks. Sensor networks are generally unmanned(remote controlled)

Prof. Viral S. Patel

Advantages and Disadvantages of a wireless network over wired network.

Advantages :

- The main advantages is that a wireless **network allows the machines to be fully mobile**, as long as they remain in radio range.

- Even when the machines do not necessarily need to be mobile, a wireless network avoids the burden of having cables between the machines. From this point of view, **setting a wireless network is simpler and faster**.

- While the immediate cost of a small wireless network may be higher than the cost of a wired one, extending the network is **cheaper**. As there are no wires, there is **no cost for material, installation and maintenance**. To add, remove or displace a machine – is easy.

Advantages and Disadvantages of a wireless network over wired network.

Disadvantages :

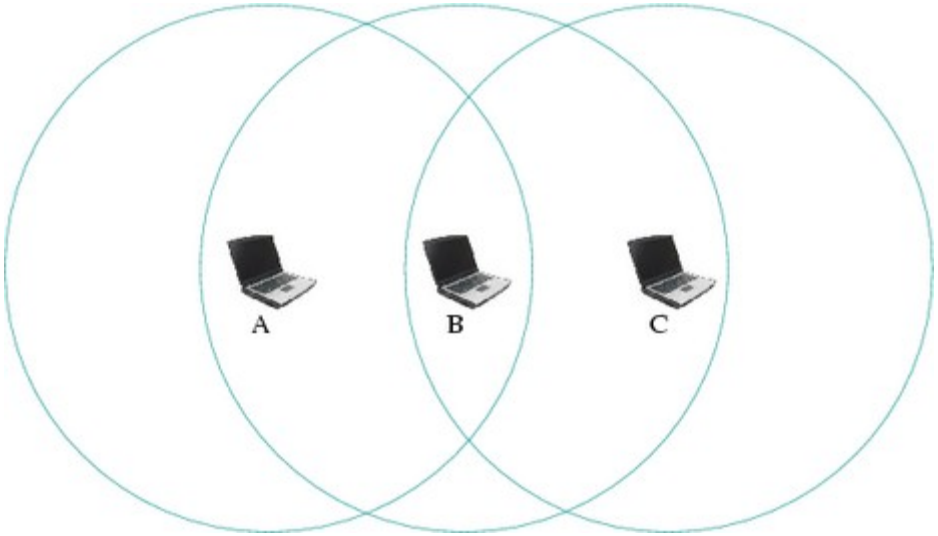
The strength of the radio signal weakens (with the square of the distance), hence the machines have **a limited radio and a restricted scope** of the network.

This causes the well-known **hidden station problem** consider three machines A,B and C, where both A and C are in radio range of B but they are not in radio range of each other.

This may happen because the A-C distance is greater than the A-B and B-C distances, as in figure, or because of an obstacle between A and C.

Prof. Viral S. Patel

The hidden station problem occurs whenever C is transmitting: when A wants to send to B, A cannot hear that B is busy and that a message collision would occur, hence A transmits when it should not; and when B wants to send to A, it mistakenly thinks that the transmission will fail, hence B abstains from transmitting when it would not need to.



The site variably influences the functioning of the network : radio waves are **absorbed** by some objects (brick walls, trees, earth, human bodies) and **reflected** by others (fences, pipes, other metallic objects, water). Wireless networks are also subject to **interferences** by other equipment that shares the same band, such as microwave ovens and other wireless networks.

Considering the limited range and possible interferences, the **data rate is often lower than that of a wired network**. However, nowadays some standards offer data rates comparable to those of Ethernet.

Due to limitations of the medium, it is **not possible to transmit and to listen at the same time**, therefore there are higher chances of message collisions. Collisions and interferences make message losses more likely.

Being mobile computers, the machines have limited battery and computation power. This may generate **high communication latency(delay/wait)** : machines may be off most of the time (i.e. power saving mode) and turning on their receivers periodically, therefore it is necessary to wait until they wake up and are ready to communicate.

As data is transmitted over wireless networks are inherently **less secure**. In fact, transmission between two computers can be eavesdropped by any similar equipment that happens to be in radio range.

Network Security Threats

Virus : A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user.

Warm : A virus replicates and executes itself, using system resources to extreme levels by generates **multiple copies** of process where each copy uses system resource. It can shut down entire network.

Trojan Horse : Such a program traps user **login information** like password, store them and do anything later to access system resources like webcam.

Trap Door : (**bypass security facilities**) Also refer to as Back door. This type of program is designed to work as required, have a security hole in its code (bits of code embedded in program) and perform illegal action without knowledge of user.

Prof. Viral S. Patel

Logic Bomb : (**triggers of automatic actions**) It is a situation when a program misbehaves only when certain conditions met otherwise it works as a normal program.

Spyware : A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your permission for profit or to capture personal information. Steal passwords and usernames, often for online banking.

Prof. Viral S. Patel

Network Security attacks

1. **Passive Attacks :** In passive attacks the goal of the opponent is to obtain information that is being transmitted. Passive attack is very difficult to detect because they do not involve any alteration of the data. But easy to prevent as measures are available.

   Two types of passive attacks :

   1. release of message contents : opponent read message of sender during transmissions.

   2. traffic analysis : Observe pattern of messages from frequency and length of messages.

2. **Active Attacks :** Active attacks involve some modification of the data stream or the creation of a false stream. It is easy to detect. Quite difficult to prevent active attacks absolutely.

Prof. Viral S. Patel

   Four categories :

   1. masquerade : sender's authentication sequence is captured and replayed by opponent after a valid authentication sequence take place.

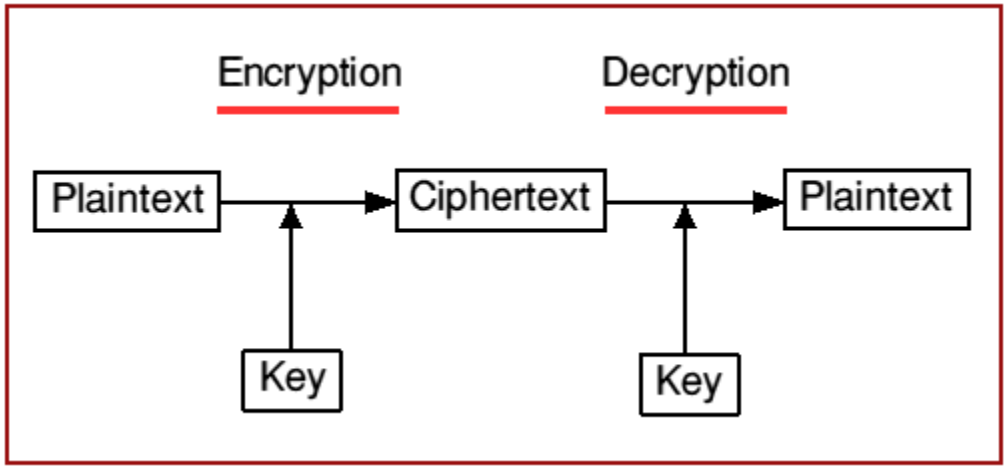
   2. Reply : Capture message from sender and Opponent give replay subsequent retransmission later.

   3. Modification of messages : Capture message from sender and later replay with altered message.

   4. Denial of service : It is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the network.

Network Security

Cryptography : A word with Greek origins, means **"secret writing".** However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks, Figure shows the components involved in cryptography.



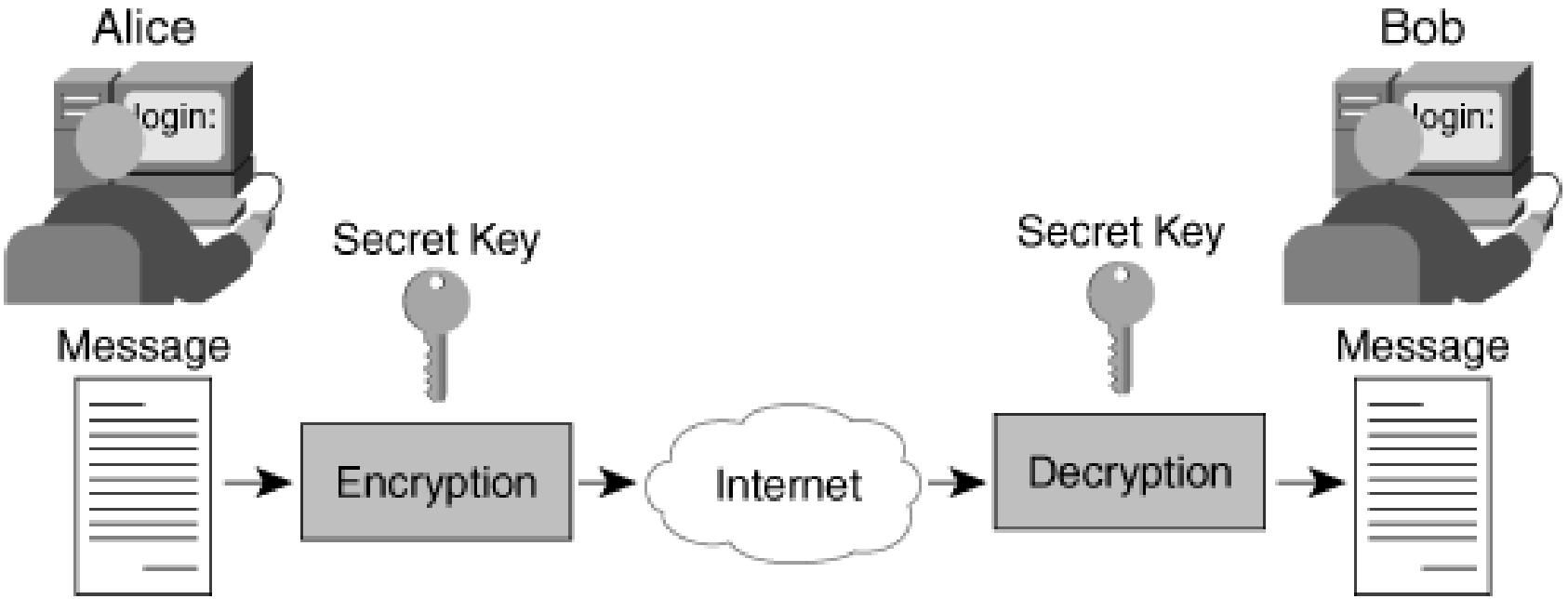
Prof. Viral S. Patel

Plaintext : The Original message before being transformed is called plaintext.
Ciphertext : After the messages is transformed, it is called Ciphertext.
An **encryption algorithm** transforms the plaintext into ciphertext.
A **decryption algorithm** transforms the ciphertext back into plaintext.
The sender uses the encryption algorithm, and the receiver uses a decryption algorithm.
Ciphers : The term ciphers refer to different categories of encryption and decryption **algorithms** in cryptography.

Prof. Viral S. Patel

Network Security

Key : A key is a number (or a set of numbers) that the algorithm operates on. To encrypt a message, we need an encryption algorithm, an encryption key and the plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key and the ciphertext. These reveal the original plaintext.

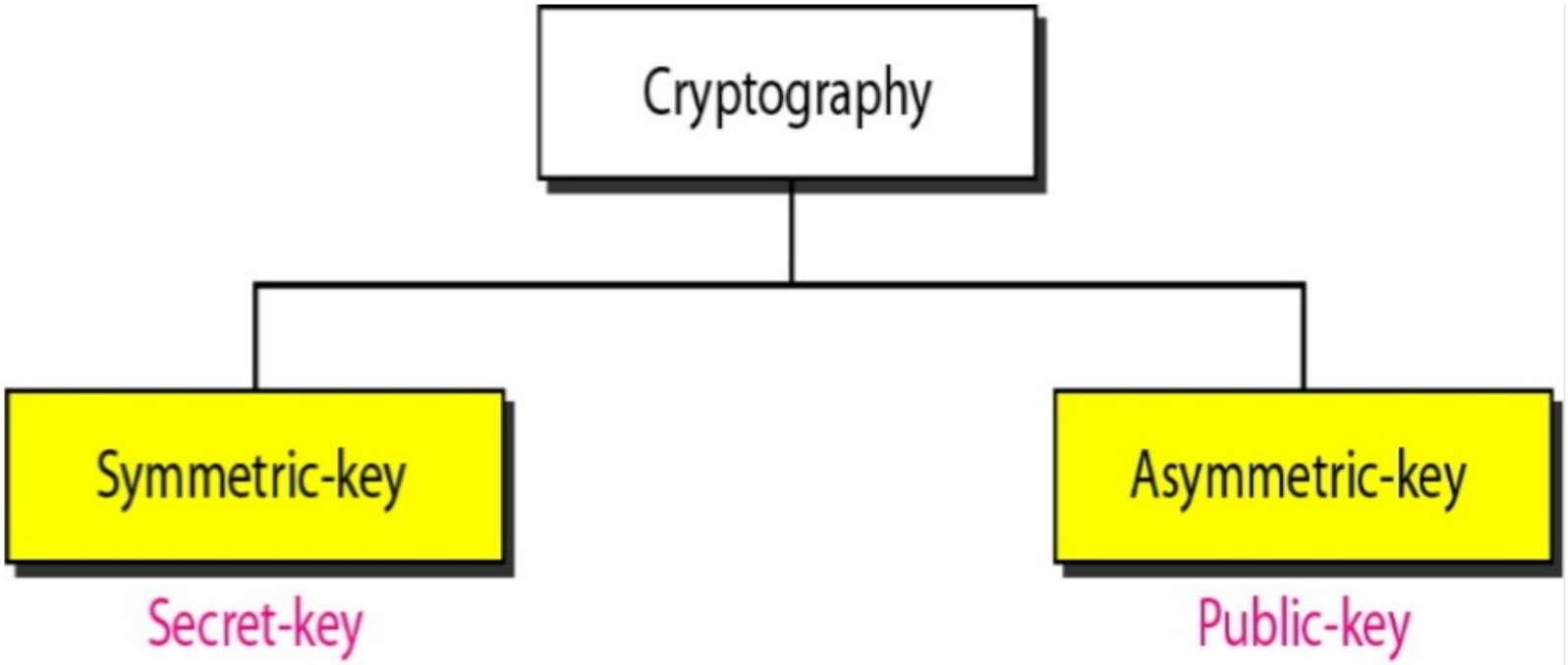


Network Security

Two Categories :

We can divide all the cryptography algorithms (ciphers) into two groups :

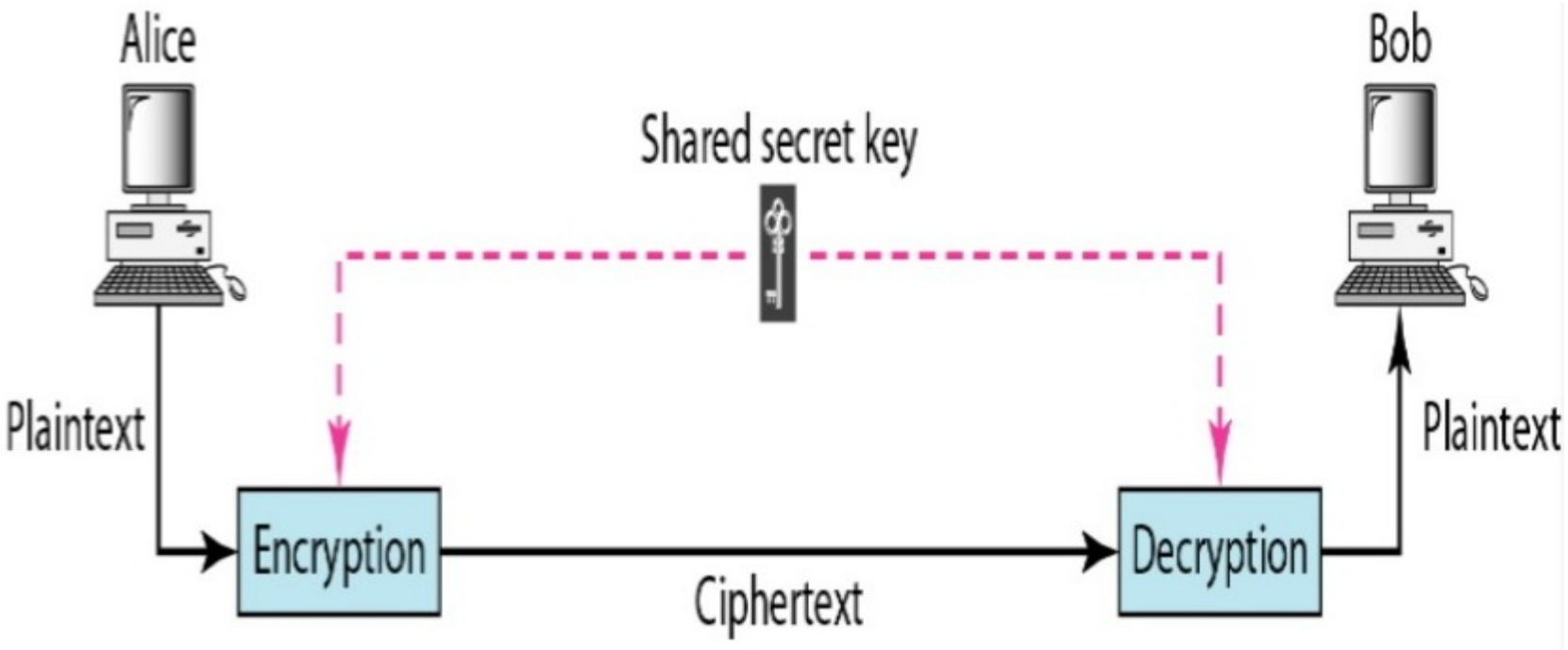
- **Symmetric key** (also called **secret-key**) cryptography algorithms and
- **Asymmetric key** (also called **public-key**) cryptography algorithms.



Network Security

Symmetric-Key Cryptography:

In Symmetric key cryptography, the **same key** is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. **(The key is shared.)**

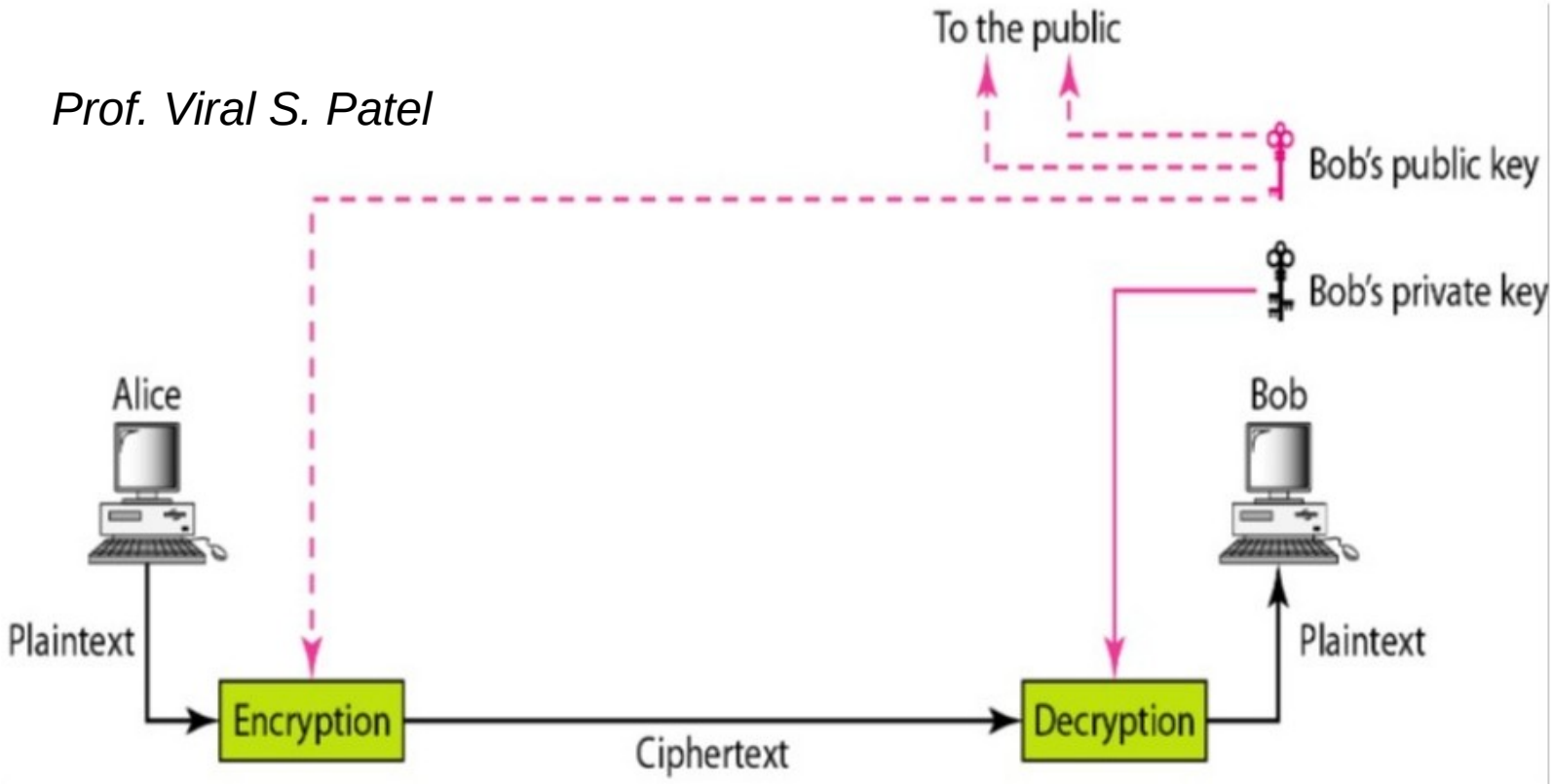


Network Security

Asymmetric-Key Cryptography:

- In Asymmetric or **public-key** cryptography, there are two keys : private key and a public key.
- Public key that is used by sender to encryption and private key that is different from the public key used by receiver to decryption.
- The public key is announced to the public. In figure, the imagine Alice wants to send a message to Bob. Alice uses the **public key to encrypt the message**. When the message is received by Bob, the **private key is used to decrypt the message**.

Prof. Viral S. Patel

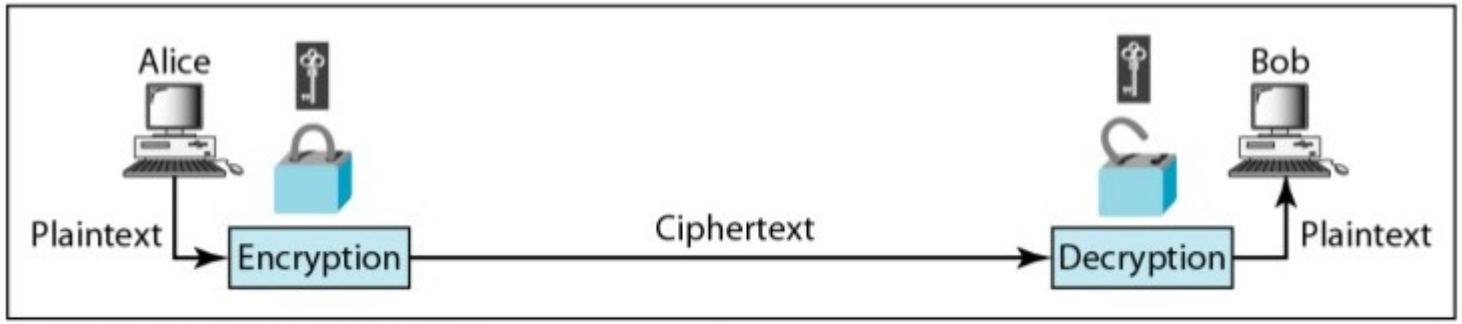


Types of Keys:

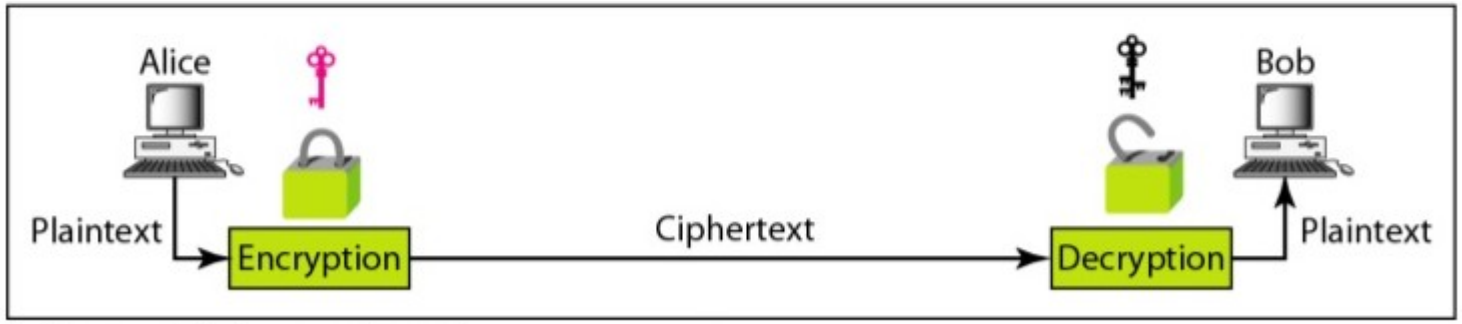
- The **secret key**, is the shared key used in **symmetric-key cryptography**.
  same key is used for encryption and decryption.
- The **public and private keys** used in **asymmetric-key cryptography.**
  different keys are used for encryption and decryption.

Symmetric-key cryptography

Asymmetric-key cryptography



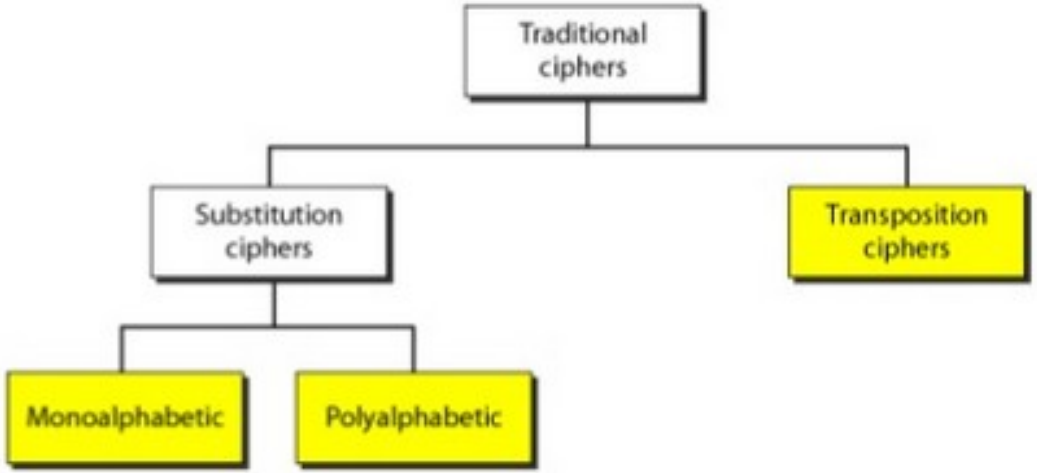
a. Symmetric-key cryptography



b. Asymmetric-key cryptography

Symmetric-key Cryptography

- **Traditional Ciphers**
  - Substitution Ciphers
    - Monoalphabetic Ciphers
      - Shift cipher
    - Polyalphabetic Ciphers
  - Transposition Ciphers



Prof. Viral S. Patel

- **Modern Ciphers**
  - Simple Modern Ciphers
    - ➔XOR Cipher
    - ➔Rotation Cipher
    - ➔Substitution Cipher : S-box
    - ➔Transposition Cipher : P-box
  - ➔Modern Round Ciphers
    - ➔Data Encryption Standard (DES)
    - ➔Triple DES
    - ➔Advanced Encryption Standard (AES)
    - ➔Other Ciphers : IDEA, Blowfish, Cast-128, RC5

Prof. Viral S. Patel

Symmetric-key Cryptography

- Traditional Ciphers
  - **Substitution Ciphers :**

    A substitution cipher substitutes one symbol with another.

<u>Monoalphabetic Ciphers</u>

A character (or a symbol) in the plaintext is always changed to the same character(or symbol) in the ciphertext regardless of its position in the text.

Example: Plaintext : HELLO
Ciphertext : KHOOR

Prof. Viral S. Patel

<u>Polyalphabetic Ciphers</u>

Each occurrence of a character can have a different substitute.
The relationship between a character in the plaintext to a character in the ciphertext is a one-to-many relationship.

Example: Plaintext : HELLO
Ciphertext : ABNZF

Symmetric-key Cryptography

- Traditional Ciphers
  - Substitution Ciphers :
    - Monoalphabetic Ciphers

Shift Cipher : The simplest monoalphabetic cipher is probably the shift cipher. We assume that the plaintext and ciphertext consist of uppercase letters (A to Z) only.

- In this cipher, the encryption algorithm is “shift key characters down” with key equal to some number. The decryption algorithm is “shift key characters up”

Example :

Use the shift cipher with key=15 to encrypt the message “HELLO” The ciphertext is “WTAD”.

- The shift cipher is sometimes referred to as the **Caesar cipher.**

Symmetric-key Cryptography

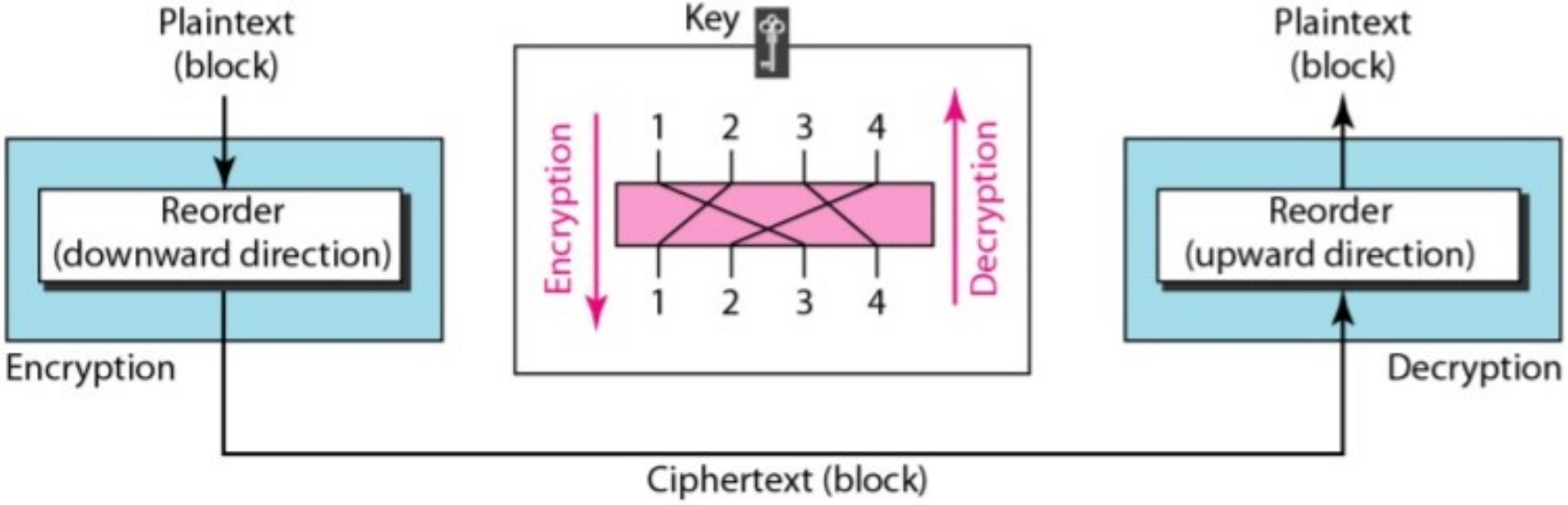
- Traditional Ciphers

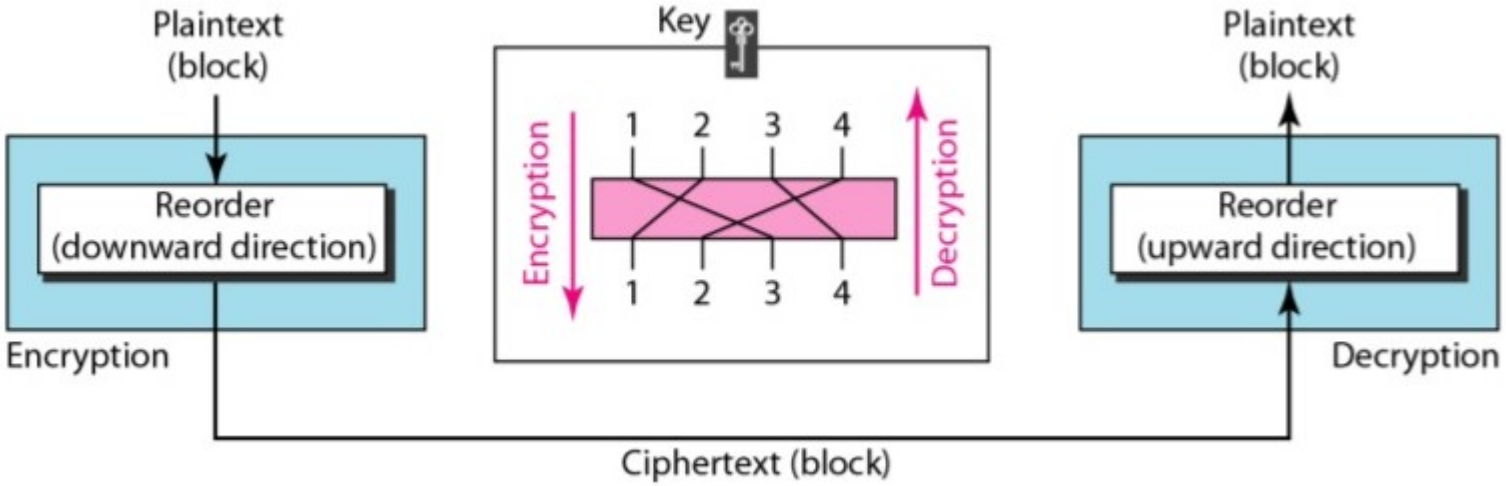
Transposition Ciphers :

In a transposition ciphers, there is no substitution of characters; instead their locations change.

A character in the first position of the plaintext may appear in the tenth position of the ciphertext.

A character in the eighth position may appear in the first position. In other words, a transposition cipher reorders the symbols in a block of symbols.





Example :

Position of characters in plaintext : 2 4 1 3

Position of characters in cypertext : 1 2 3 4

Message : “HELLO MY DEAR”

Prof. Viral S. Patel

Plain Text			
1	2	3	4
H	E	L	L
O	M	Y	D
E	A	R	**Z**

Cipher Text			
2	4	1	3
E	L	H	L
M	D	O	Y
A	Z	E	R

After encryption message : ELHLMDOYAZER

Prof. Viral S. Patel

Symmetric-key Cryptography

- Traditional Ciphers

Transposition Ciphers :

Transposition Cypher (Example)

PLAIN: F O U R S C O R E A N D S E
V E N Y E A R S A G O

1	2	3	4	5
F	C	N	E	R
O	O	D	N	S
U	R	S	Y	A
R	E	E	E	G
S	A	V	A	O

→

3	2	4	5	1
N	C	E	R	F
D	O	N	S	O
S	R	Y	A	U
E	E	E	G	R
V	A	A	O	S

CYPHER: N C E R F D O N S O S R Y A
U E E E G R V A A O S

Symmetric-key Cryptography

- Modern Ciphers
  - **Simple Modern Ciphers**

Traditional Ciphers are character-oriented. With the advent of the computer, ciphers need to be **bit-oriented.** This is so because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio and video data. So it is convenient to convert these types of data into a stream of bits, encrypt the stream, and then send the encrypted stream.

Modern ciphers provide more security than traditional ciphers.

Prof. Viral S. Patel

A modern symmetric cipher is a combination of simple ciphers.

XOR Cipher

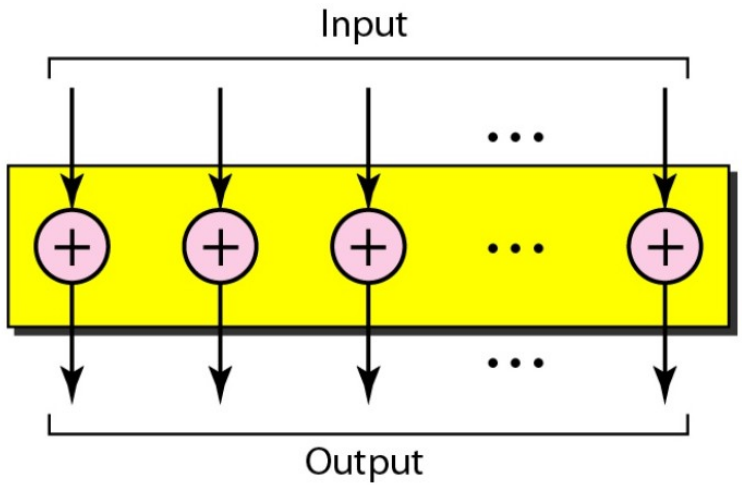
Simple Example (8 bit key and blocks):

- Encryption:

```
Plaintext:  10010101 00100110 01110101
Key:        10100110 10100110 10100110
Ciphertext: 00110011 10000000 01010011
```

- Decryption:

```
Ciphertext: 00110011 10000000 01010011
Key:        10100110 10100110 10100110
Plaintext:  10010101 00100110 01110101
```



Prof. Viral S. Patel

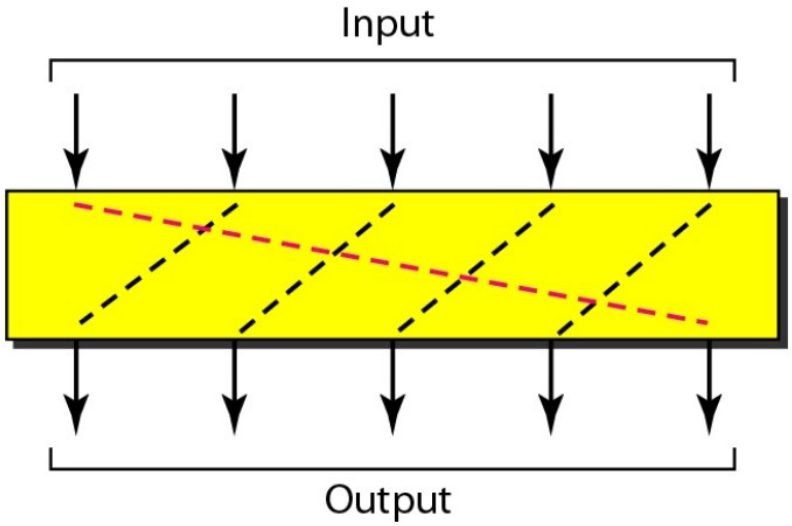
Symmetric-key Cryptography

- Modern Ciphers
  - Simple Modern Ciphers
    - **Rotation Cipher**

Special case of the transpositional cipher using bits instead of characters

If the length of the original stream is N, after N rotation we get the original input stream, So number of rotation must be between 1 and N-1

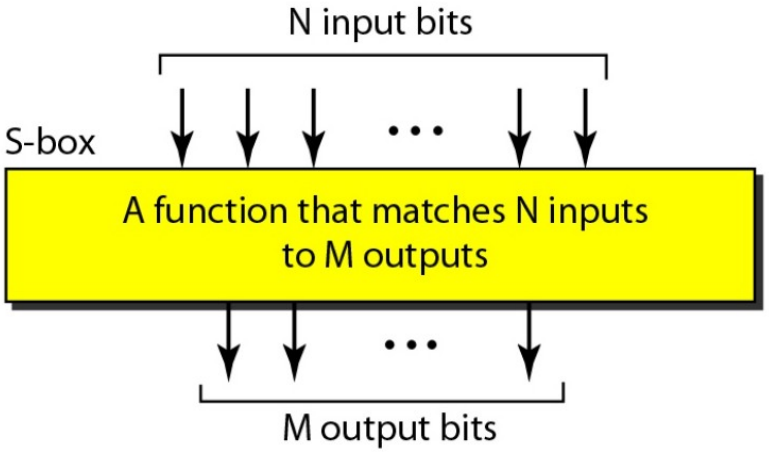
The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction. If we use a right rotation in the encryption, we use a left rotation in decryption and vice versa.

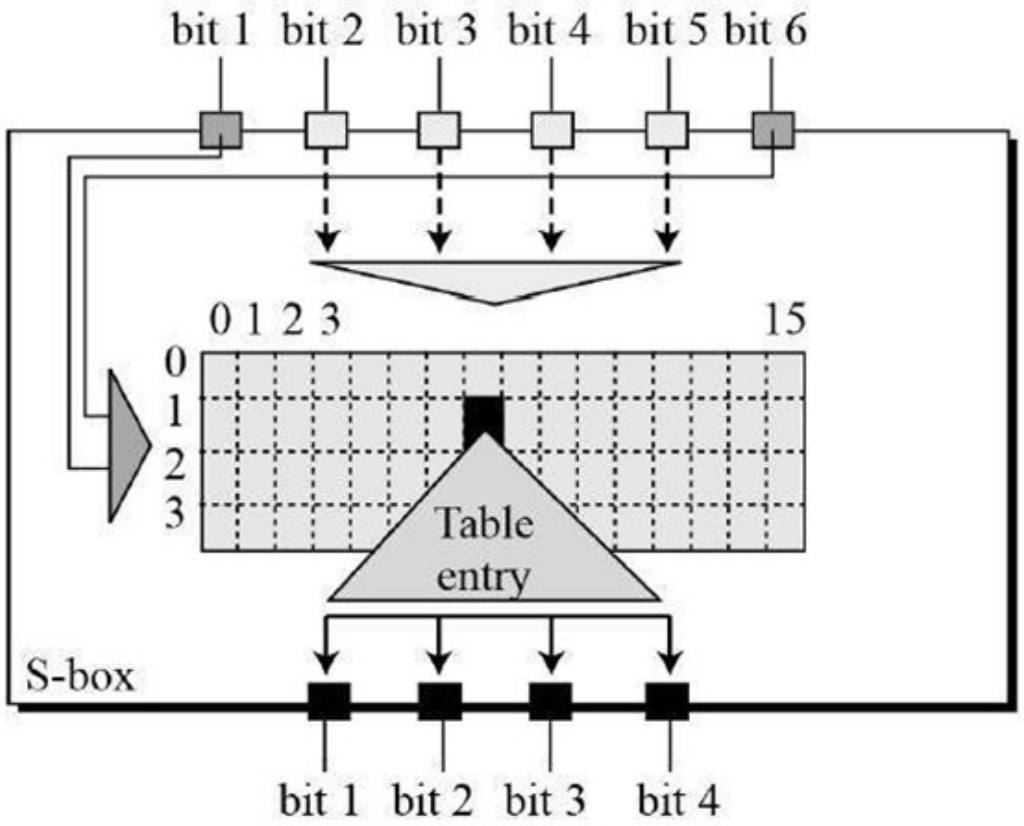


Symmetric-key Cryptography

- Modern Ciphers
  - Simple Modern Ciphers

Substitution Cipher : S-box
(Substitution box)





- Work at bit level.
- Keyless
- The function that matches the input to the output may be defined mathematically or by a table.

(we will see that s-box is used in DES)

Substitution Cipher : S-box
(Substitution box)

Prof. Viral S. Patel

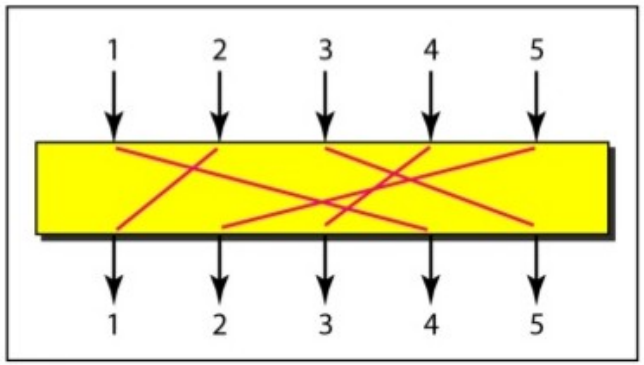
S_5		Middle 4 bits of input														
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
CL & CR	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Prof. Viral S. Patel

Symmetric-key Cryptography

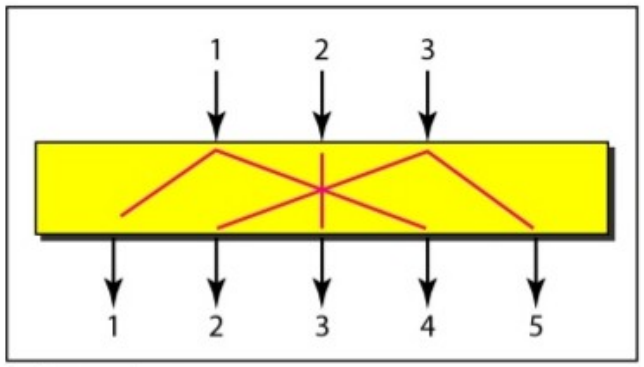
- Modern Ciphers
  - Simple Modern Ciphers

Transposition Cipher : P-box
(Permutation box)

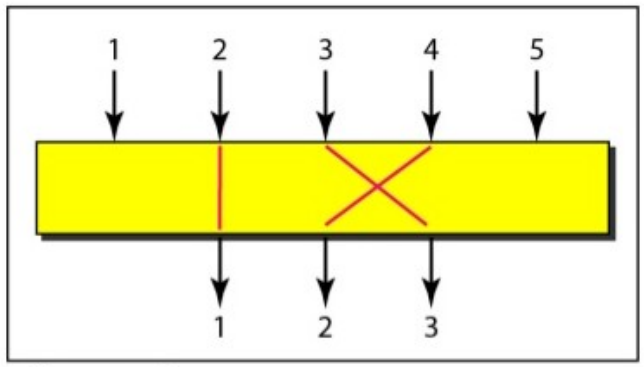


a. Straight

- Work at bit level.
- Keyless
- It can be implemented in software or hardware, but hardware is faster.



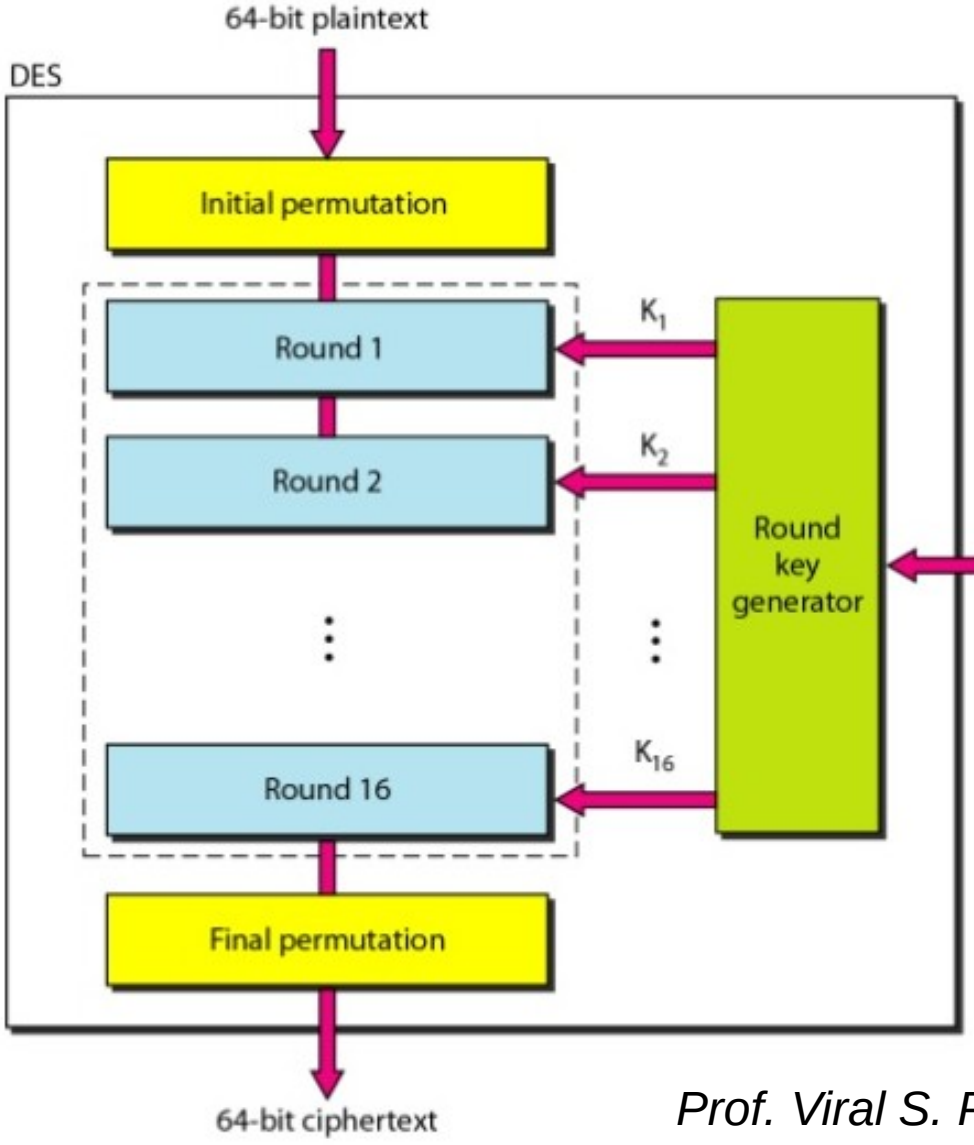
b. Expansion



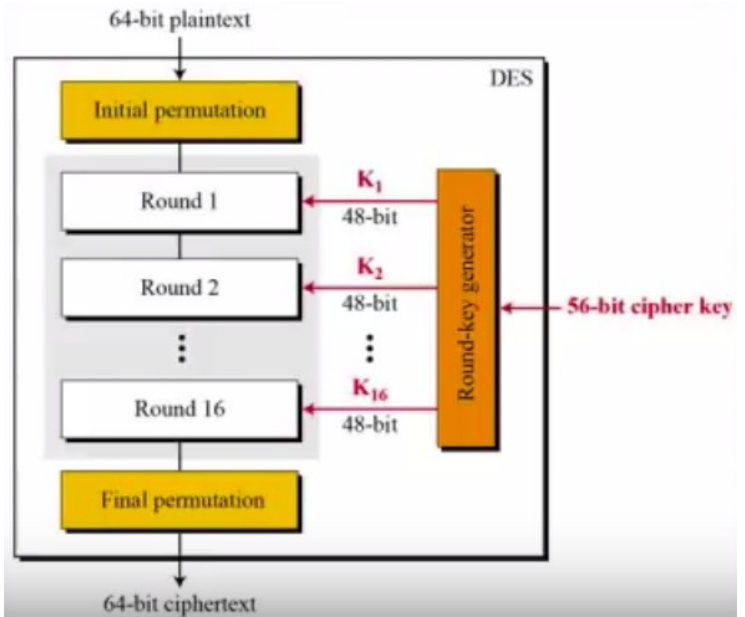
c. Compression

Symmetric-key Cryptography

- Modern Ciphers
  - **Modern Round Ciphers**
  - **Data Encryption Standard (DES)**



- 64 bit plaintext block
- 64/56 bit key. (The initial key consists of 64 bits. However, before the DES process even start, every eight bit of the key is discarded to produce a 56-bit key.)
- Two transposition blocks (p-boxes)
- 16 complex round ciphers
- Each round uses a different 48 bits key
- Initial and final permutations are keyless straight permutations and inverse of each other.

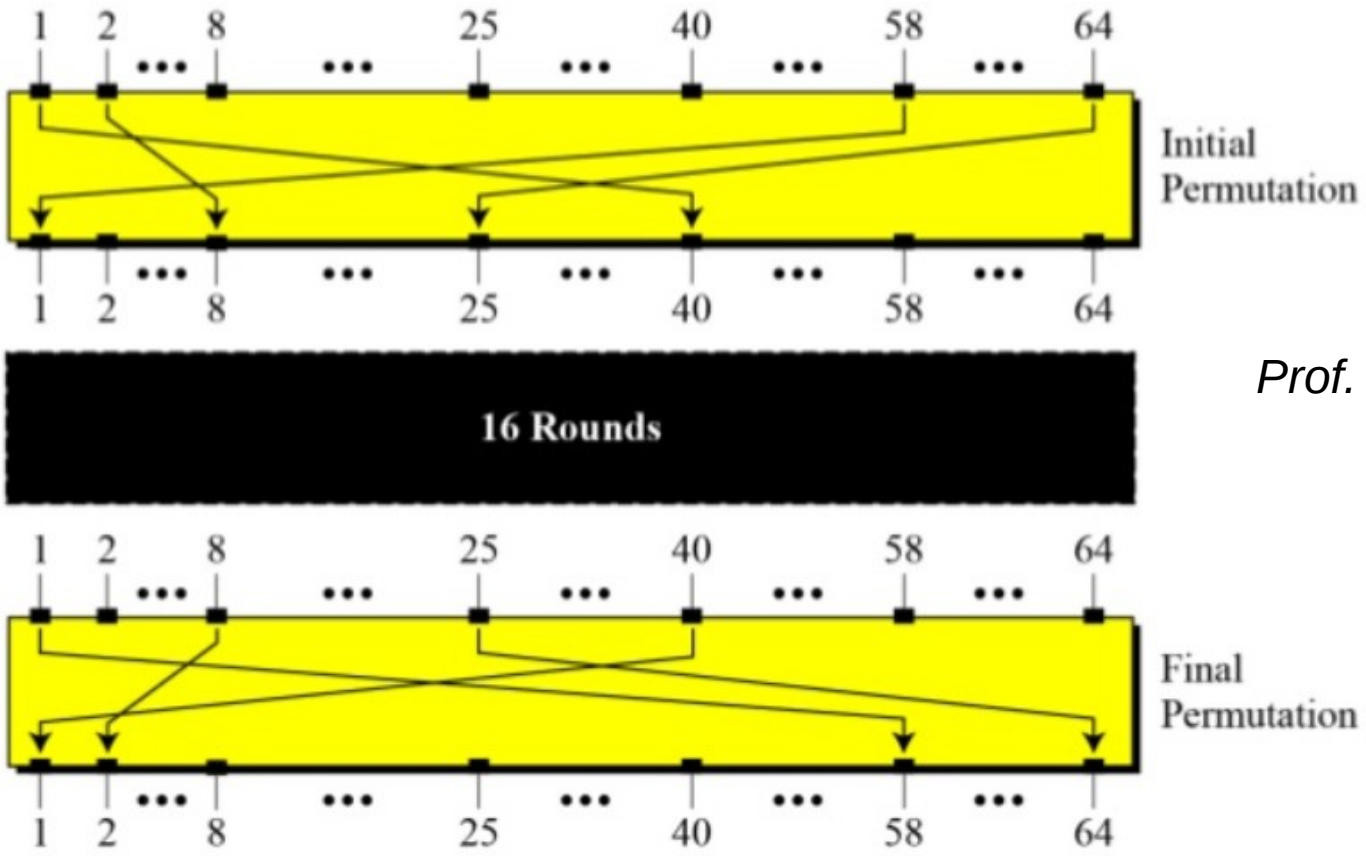


Symmetric-key Cryptography

Modern Ciphers

Modern Round Ciphers

Data Encryption Standard (DES)



Prof. Viral S. Patel

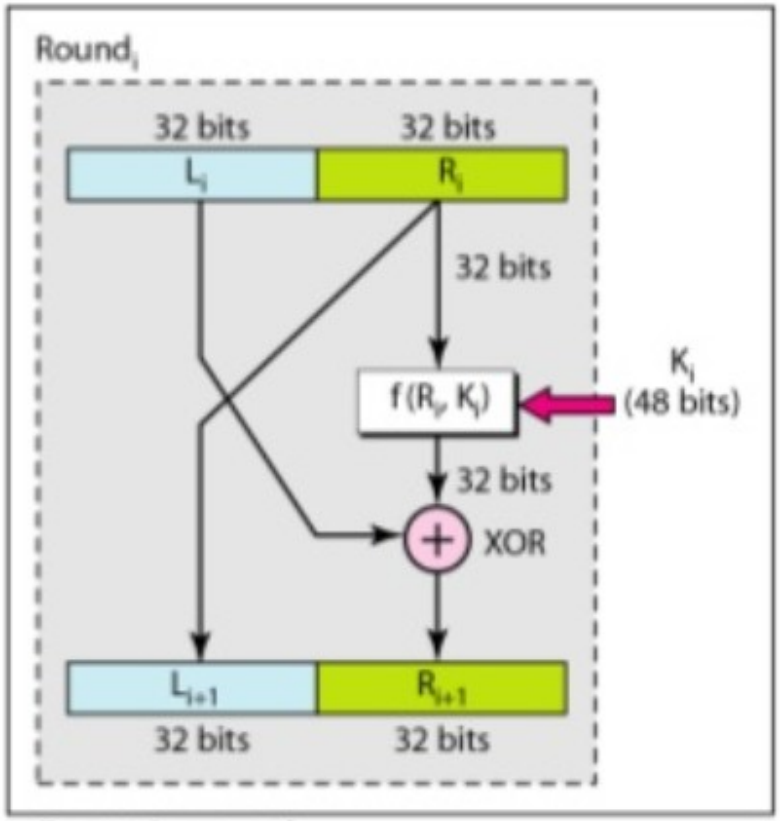
Prof. Viral S. Patel

Symmetric-key Cryptography

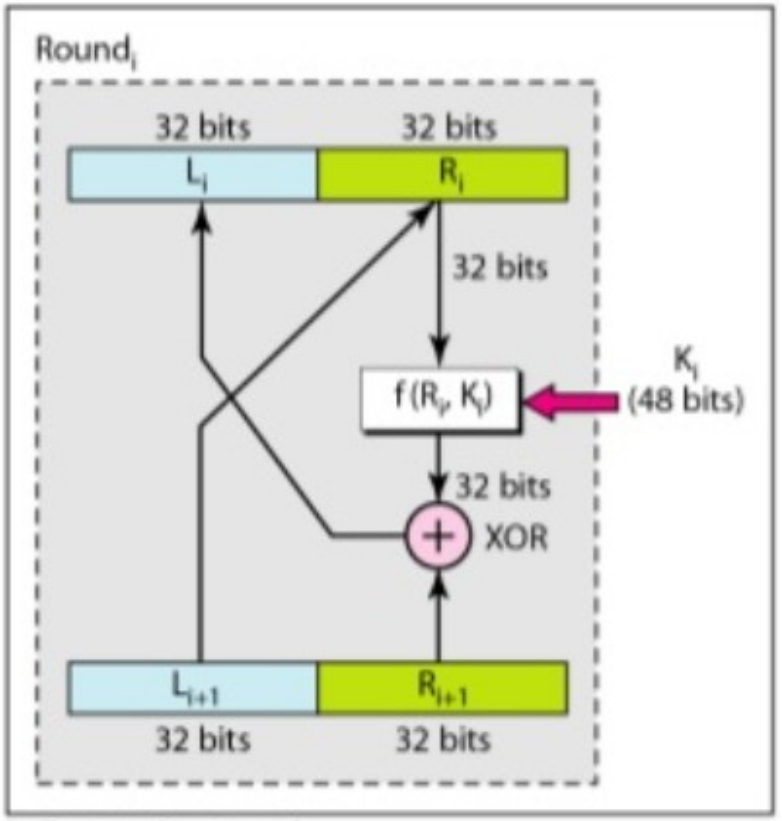
Modern Ciphers

Modern Round Ciphers

Data Encryption Standard (DES)



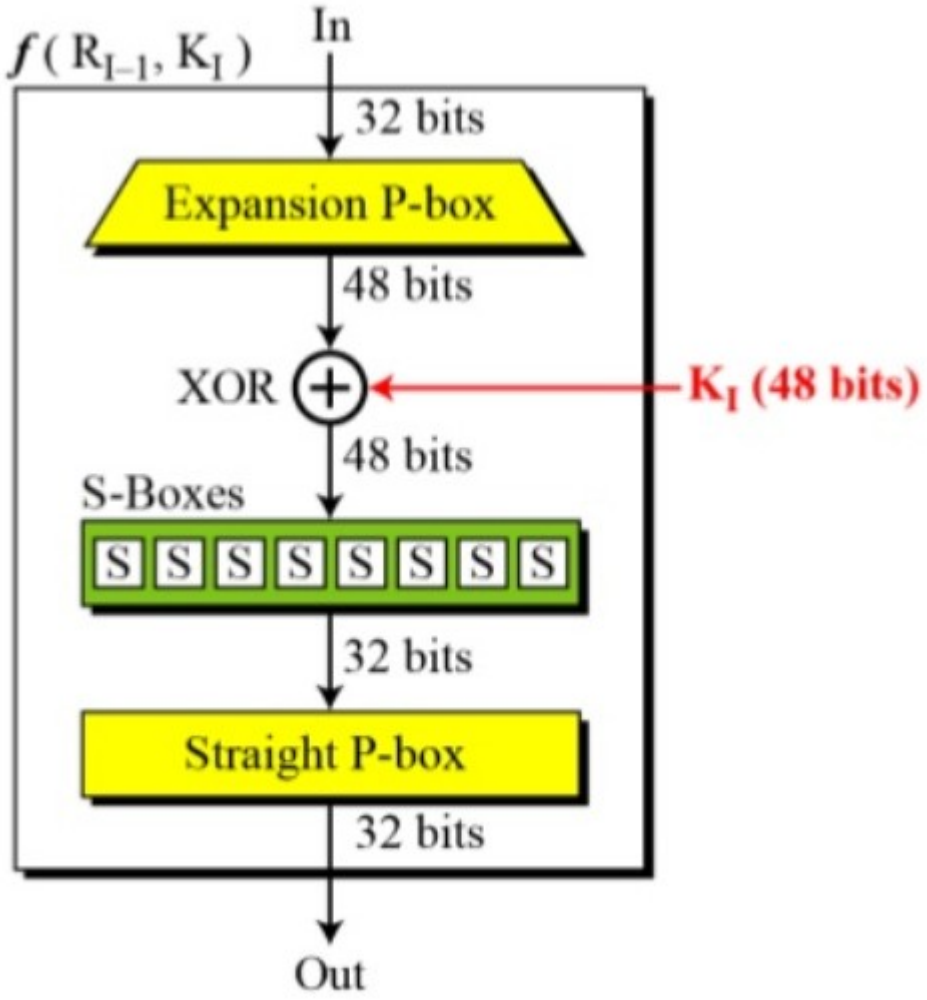
a. Encryption round



b. Decryption round

Symmetric-key Cryptography

- Modern Ciphers
  - Modern Round Ciphers
    - **Data Encryption Standard (DES)**



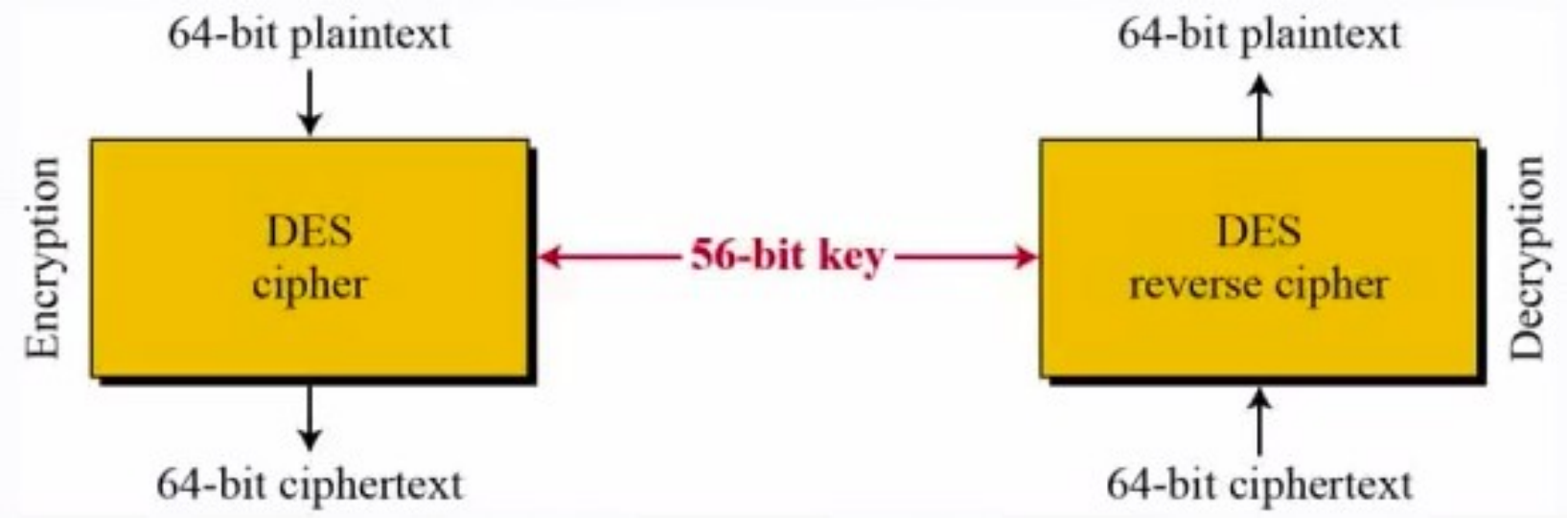
Symmetric-key Cryptography

Modern Ciphers

Modern Round Ciphers

Data Encryption Standard (DES)

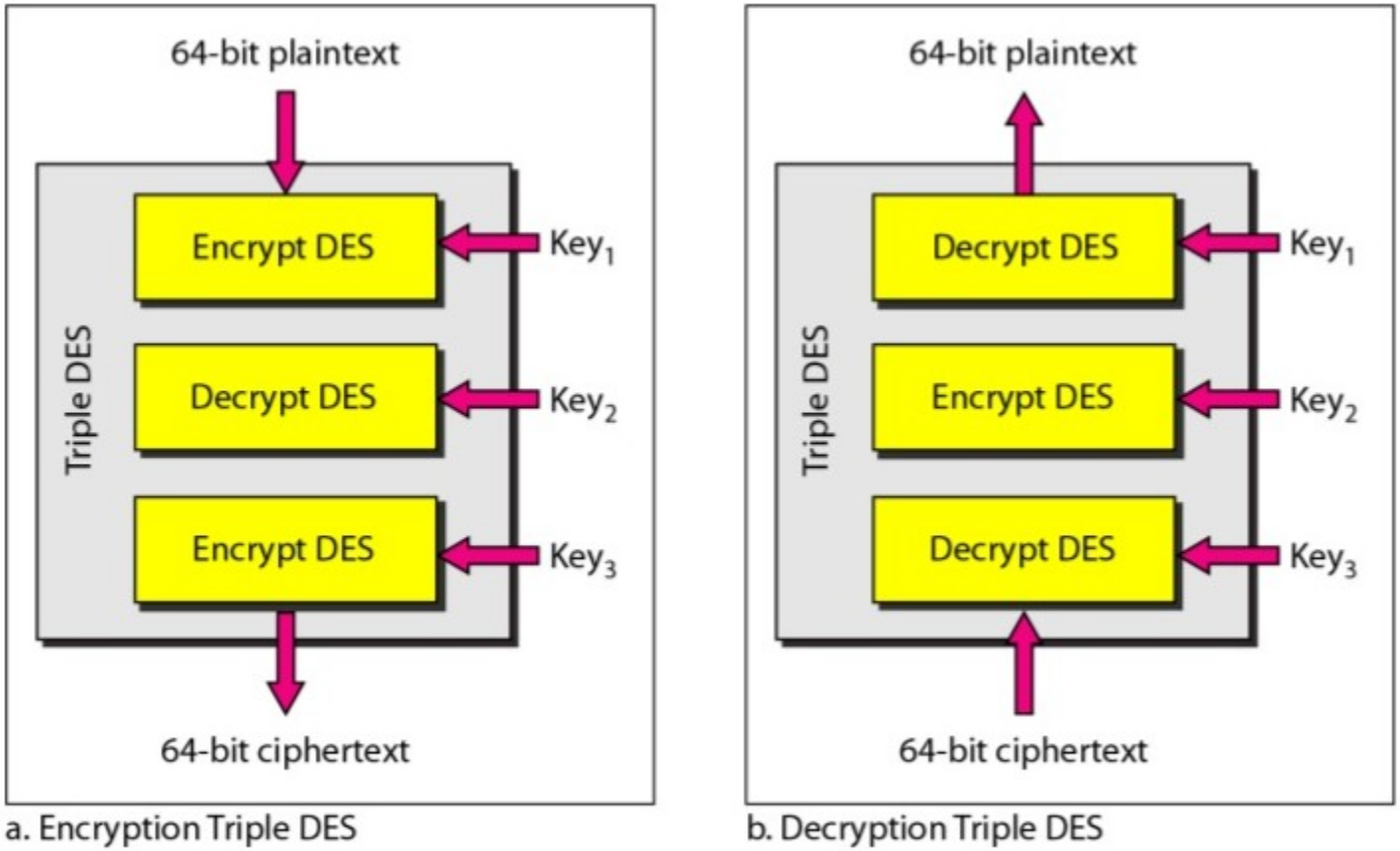
Using same key for encryption and decryption because it is symmetric-key cryptography



Problem : Key is short. A brute force attack that involves trying every possible combination of characters or data in order to find the key in order to decrypt ciphertext.

Symmetric-key Cryptography

- Modern Ciphers
  - Modern Round Ciphers
  - **3DES**



Problem in DES is that key is too short (brute-force-attack). So to lengthen the key 3DES has been implemented.

Two different versions of 3DES are in use :

3DES with two keys and 3DES with three keys.

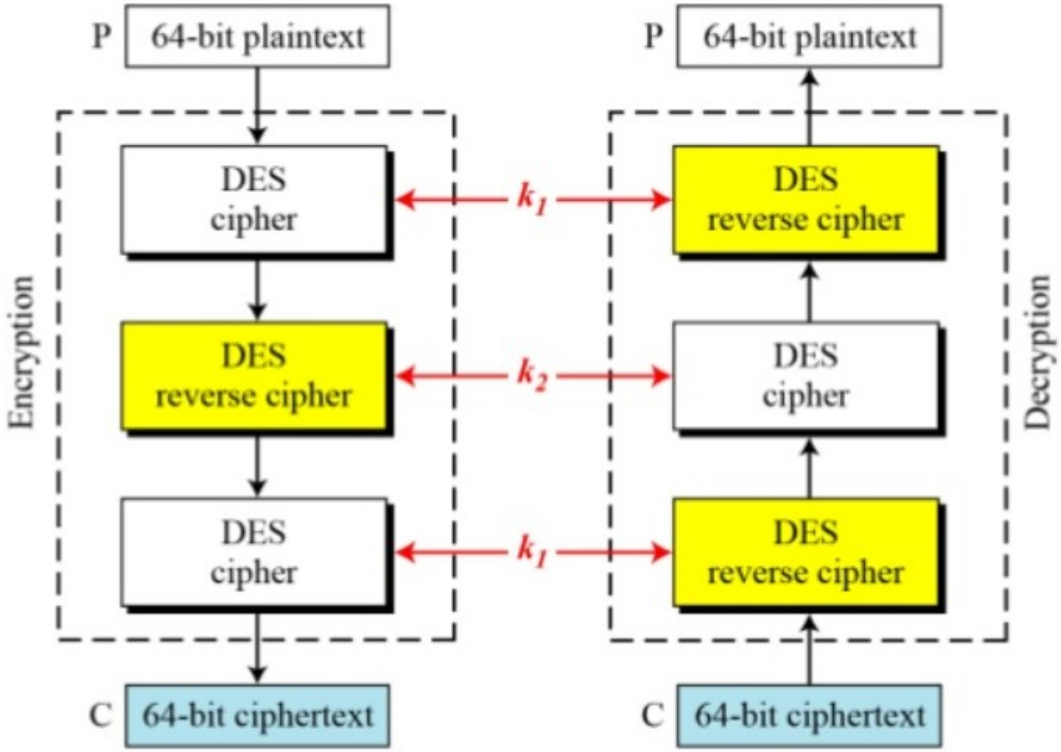
Symmetric-key Cryptography

Modern Ciphers

Modern Round Ciphers

3DES

To make the key size 112 bits and at the same time protect DES from attacks such as the man-in-middle attack, 3DES with two keys was designed. In this version, the first and the third keys are the same (key1=key3). This has the advantage in that a text encrypted by a single DES block can be decrypted by the new 3DES.
We just set all keys equal to key1.

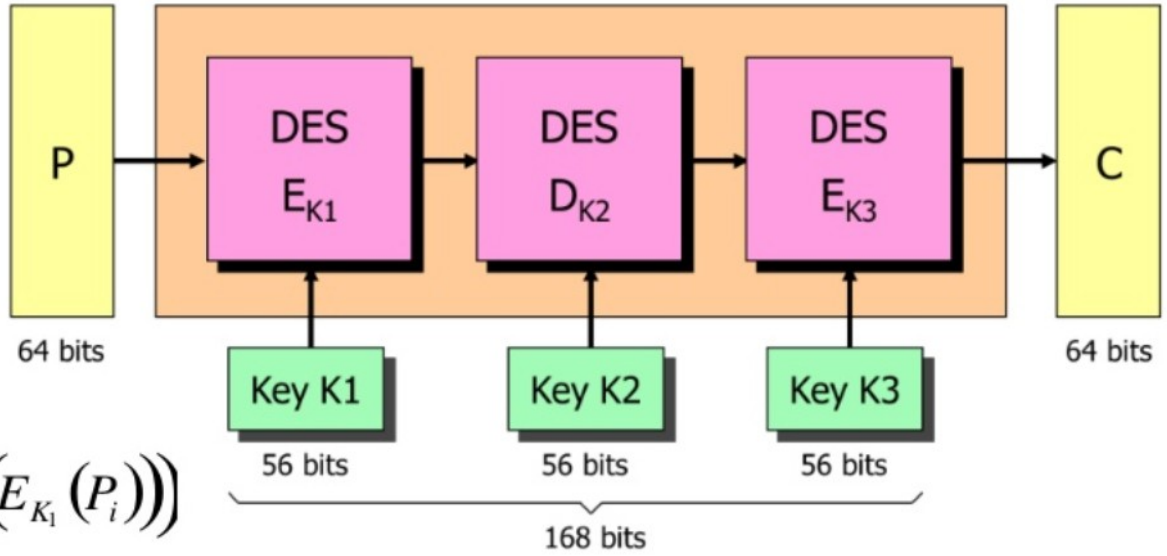


Triple DES with two keys

Symmetric-key Cryptography

- Modern Ciphers
  - Modern Round Ciphers
  - **3DES**

Many algorithms use a 3DES cipher with three keys. This increases the size of the key to **168 bits**.



$$C_i = E_{K_3}\left(D_{K_2}\left(E_{K_1}\left(P_i\right)\right)\right)$$

True cryptographic strength of 3DES key is 2x56 bits = 112 bits

Name of Algorithm	Block Size	Key Size
DES (Data Encryption Standard, IBM)[1]	64	56
3DES (Triple DES)	64	168

Symmetric-key Cryptography

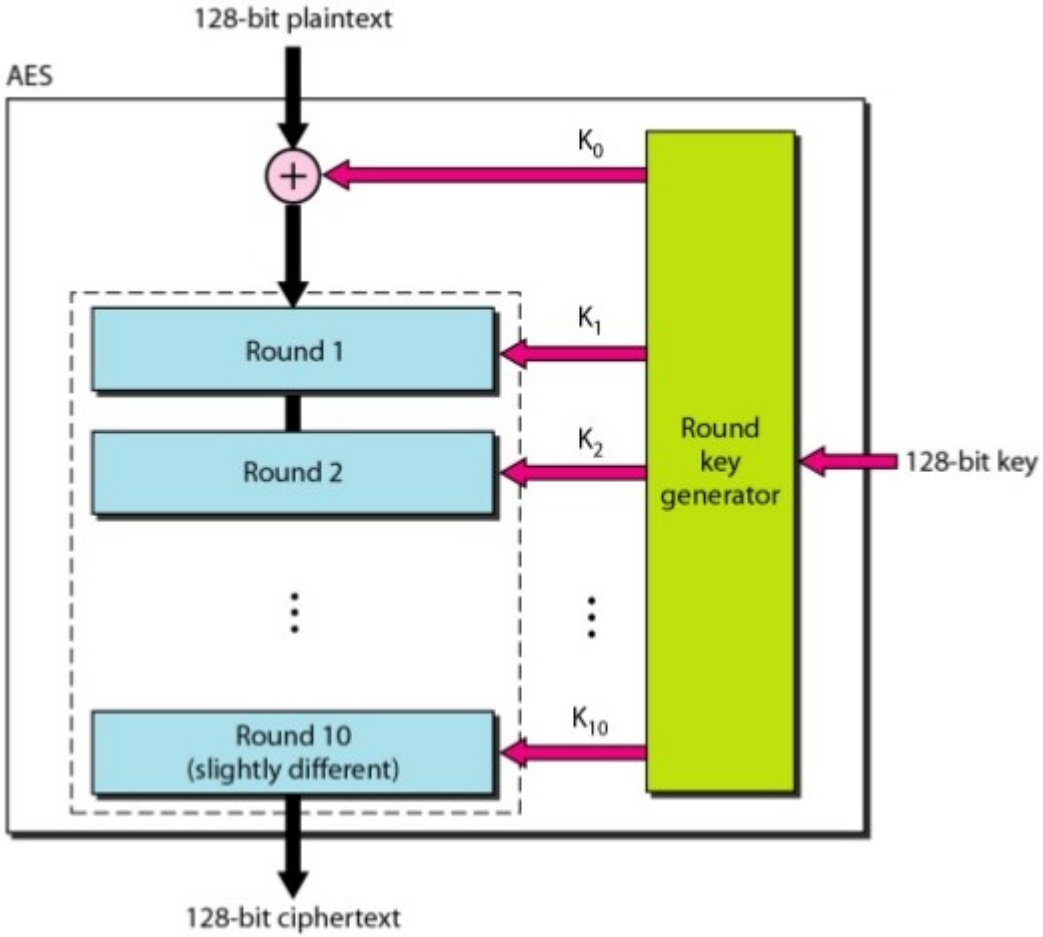
- Modern Ciphers
  - Modern Round Ciphers
    - **Advanced Encryption Standard (AES) or Rijndael algorithm**

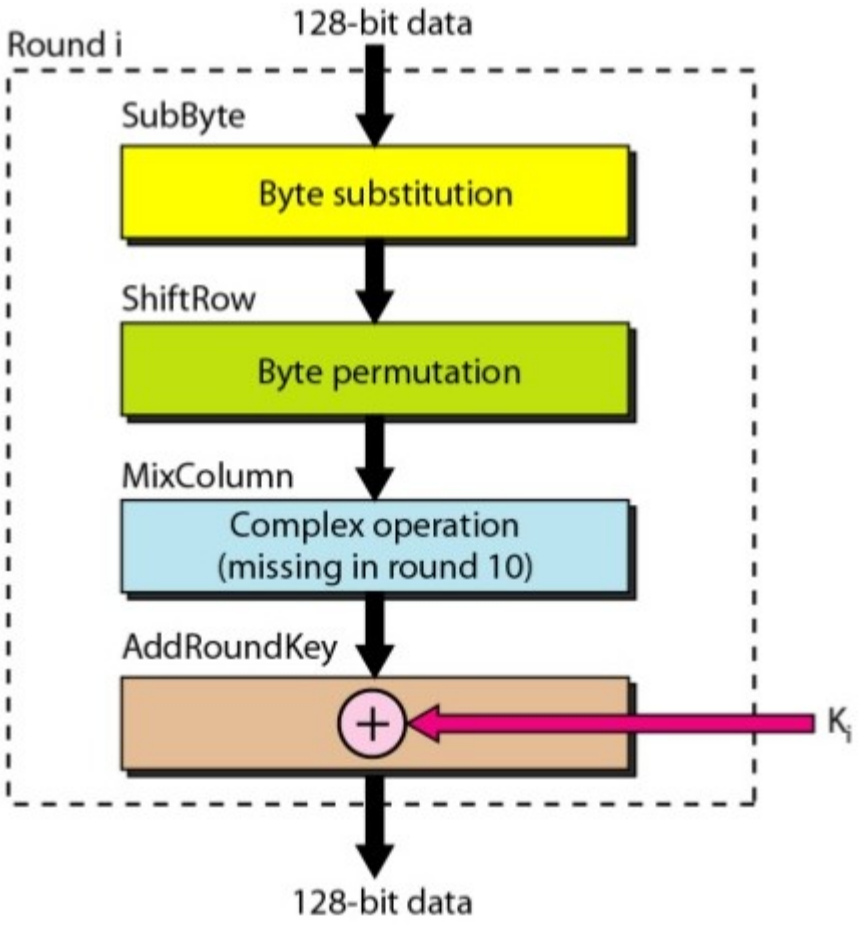
AES was designed because DES's key was too small. Although 3DES increased the key size, the process was too slow. AES is very complex round cipher. AES is designed with three key sizes : 128, 192 or 256 bits.

Size of Data Block	*Number of Rounds*	*Key Size*
128 bits	10	128 bits
	12	192 bits
	14	256 bits

Symmetric-key Cryptography

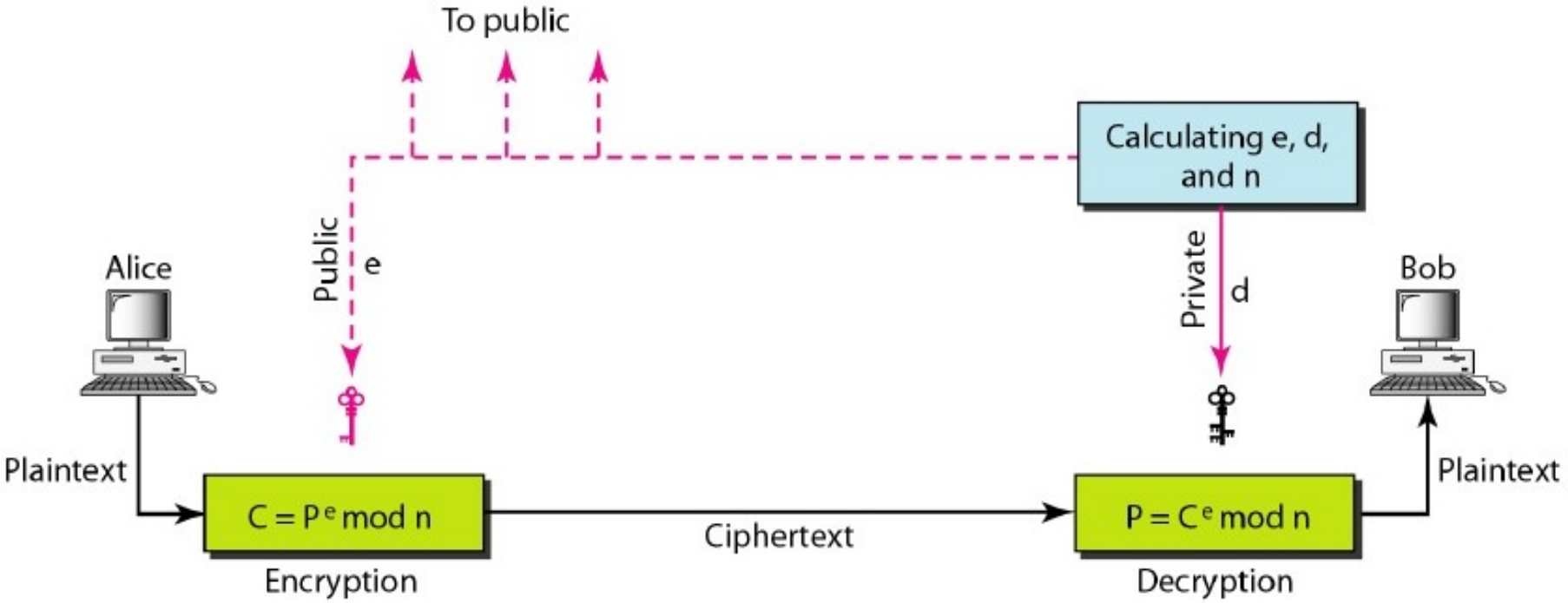
- Modern Ciphers
  - Modern Round Ciphers
    - **Advanced Encryption Standard (AES)**





Asymmetric-Key Cryptography

RSA (Rivest, Shamir, Adleman)



1. Select two large prime numbers p and q
2. $n = p \cdot q$
3. $\emptyset = (p-1) \cdot (q-1)$
4. Select e such that $e < \emptyset$ and $\gcd(e, \emptyset)=1$
5. Find d such that $d \cdot e \bmod \emptyset = 1$ **or** $d \cdot e = 1 \bmod \emptyset$ **or** $d = e^{-1} \bmod \emptyset$
6. e and n are announced to public. (**e is public key**)
7. d and Ø are kept secret. (**d is private key**)

Asymmetric-Key Cryptography

RSA (Rivest, Shamir, Adleman)

Encryption : $C = P^e \pmod n$
Decryption : $P = C^d \pmod n$

Example :

- p = 7 & q = 11
- ➔ n = p · q = 7 · 11 = 77
- ➔ Ø = (p-1) · (q-1) = (7-1) · (11-1) = 60
- ➔ We can select e = 13
  because e < Ø and gcd(e, Ø)=1
- ➔ d · e mod Ø = 1
  d · 13 mod 60 = 1

d may be 5,7,11,13,17,19,23,29,31,37...

5 ·13 = 65 65 mod 60=5
7 ·13 = 91 91 mod 60=31
...
37·13 = 481 481 mod 60=1

d = 37

Encryption : Plain text = 5

$C = P^e \pmod n$
$= 5^{13} \pmod{77}$
$= 26$

Decryption : Cipher text = 26

$P = C^d \pmod n$
$= 26^{37} \pmod{77}$
$= 5$

RSA (Rivest, Shamir, Adleman)

Applications :

RSA can be used to encrypt and decrypt actual messages, it is very slow if the message is long. RSA, therefore, is **useful for short messages** such as a small message digest or a symmetric key to be used for a symmetric-key cryptosystem.

RSA is **used in digital signatures** and other cryptosystems that often need to encrypt a small message without having access to symmetric key.

RSA is also **used for authentication**.

Prof. Viral S. Patel

RSA is also **used to encrypt and decrypt symmetric keys.**

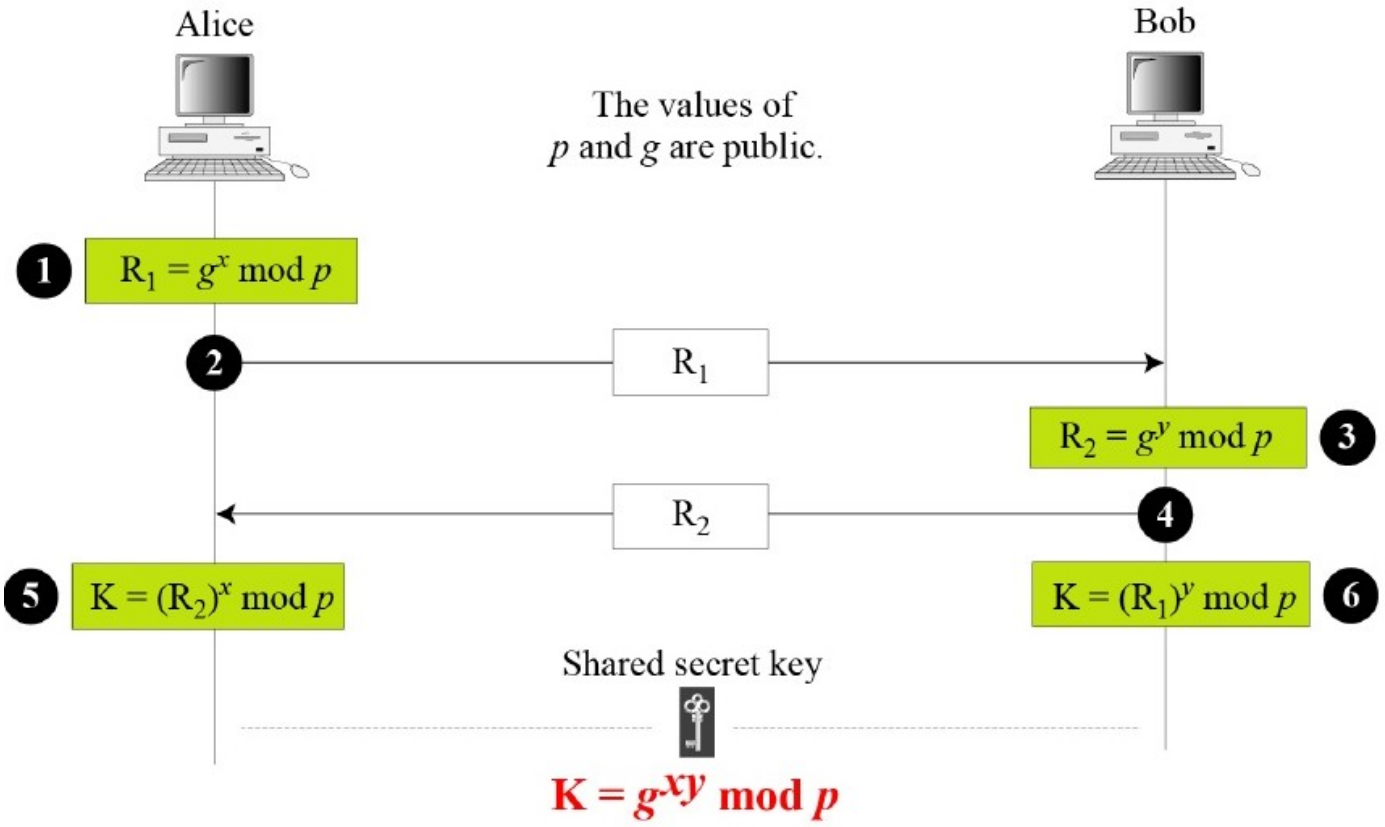
Compare DES and RSA.

Method	DES	RSA
Approach	Symmetric	Asymmetric
Encryption	Faster	Slow
Decryption	Faster	Slow
Key distribution	Difficult	Easy
Complexity	O(Log N)	O (N3)
Security	Moderate	Highest
Nature	Closed	Open
Inherent Vulnerabilities	Brute Forced, Linear and differential cryptanalysis attack	Brute Forced and Oracle attack
Vulnerabilities cause	Weak key usage	Weak implementation
Secure Services	Confidentially	Confidentially, integrity, non repudiation

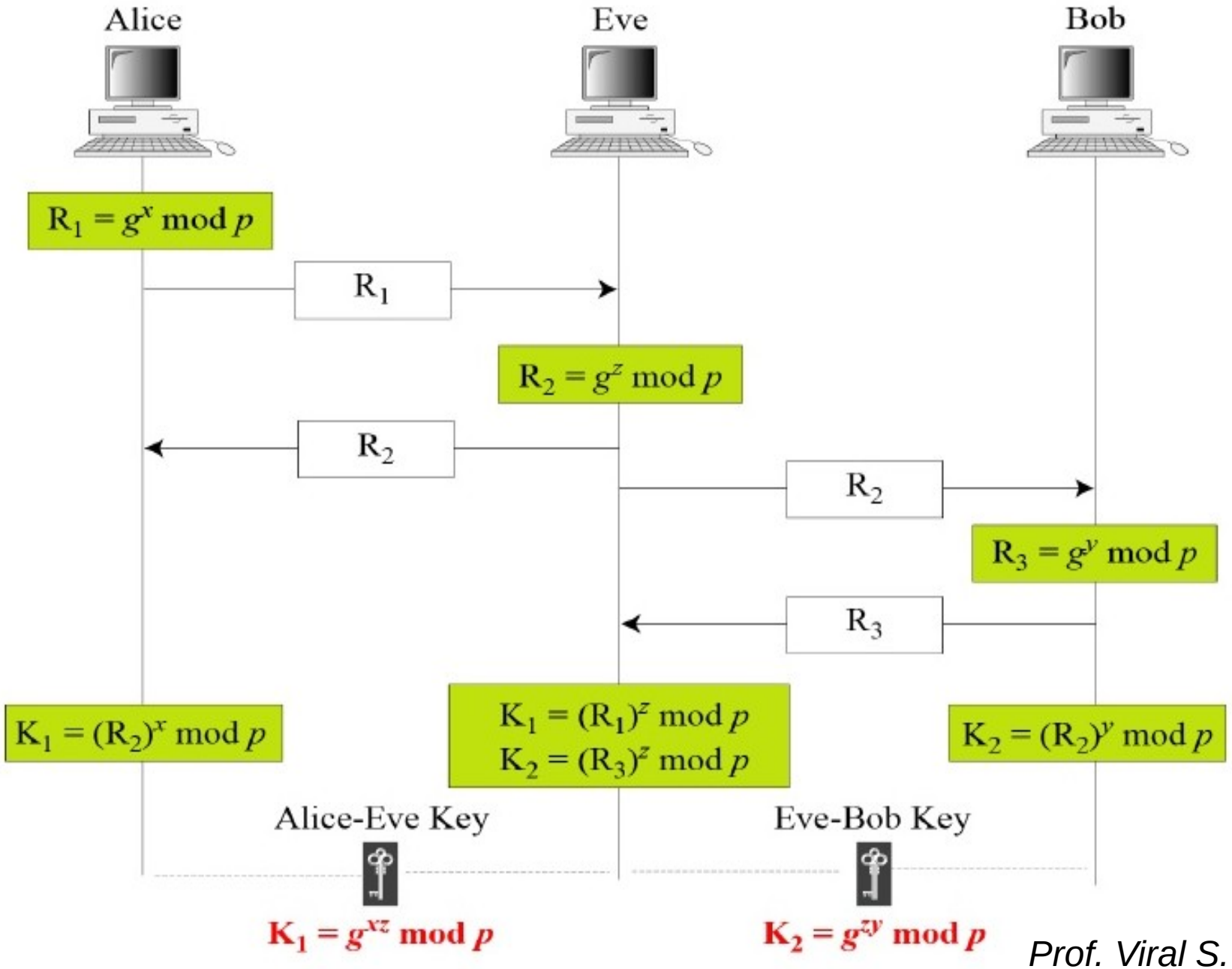
Asymmetric-Key Cryptography (public key cryptography)

Diffie-Hellman

- Create a symmetric session key (secret key) to exchange data.
- Problem is man-in-middle attack. But can be avoided by authentication scheme.
- DH is viewed as a public key (Asymmetric-key) algorithm because "two public numbers (computed from each party's secret number)" are used to derive a symmetric key."



Asymmetric-Key Cryptography : **Man-in-middle attack**
(Bucket brigade attack)



Prof. Viral S. Patel

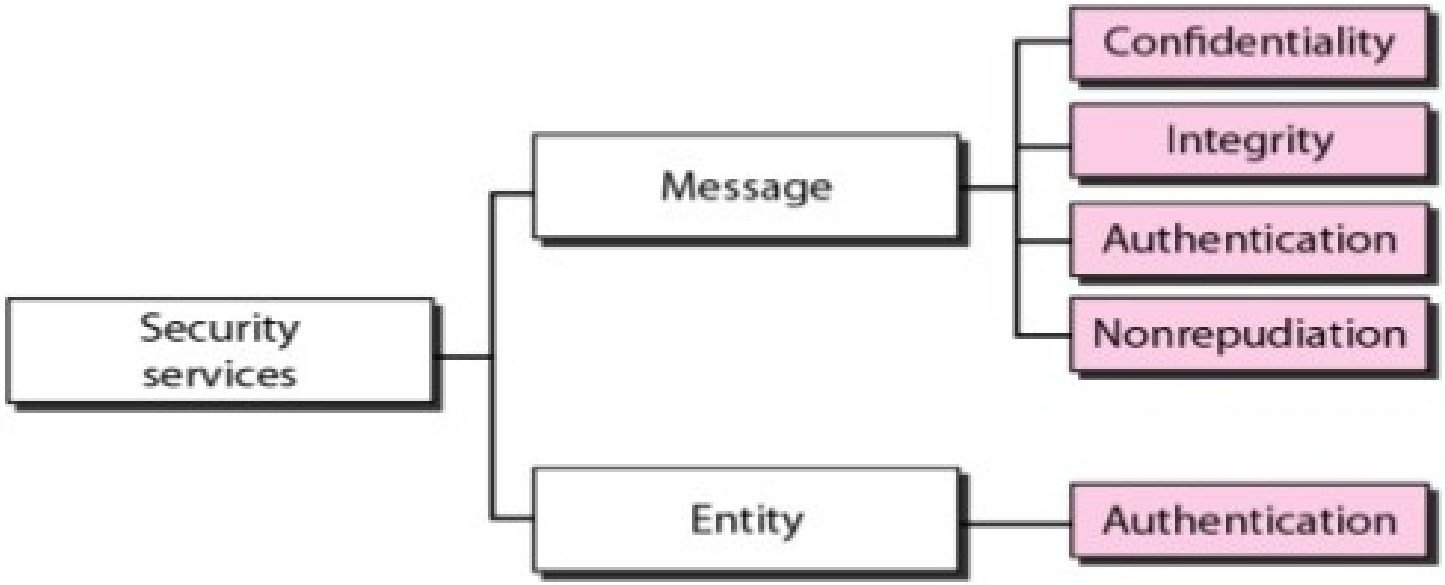
Example of Diffie-Hellman (Just for extra knowledge) :

Alice and Bob decide, publicly on a number (15). Alice then chooses a secret number(2) that no one knows and takes the public number and puts it to the power of her secret number (15^2=225) and sends the result (225) to Bob.

Bob then does the same exact thing that Alice does, but with his secret number(3). So he takes the public number(15) and puts it to the power of his secret number (15^3=3375) and then sends the result (3375) to Alice.

At this point in the game Alice has Bob's result 3375 and Bob has Alice's result of 225. Now the fun part. Alice takes' Bob's result (3375) and puts it to the power of her secret number(3375^2=11390625). Then Bob takes Alice's result and puts it to the power of his secret number (225^3=11390625). Magically they come up with the same number!

Security Services :

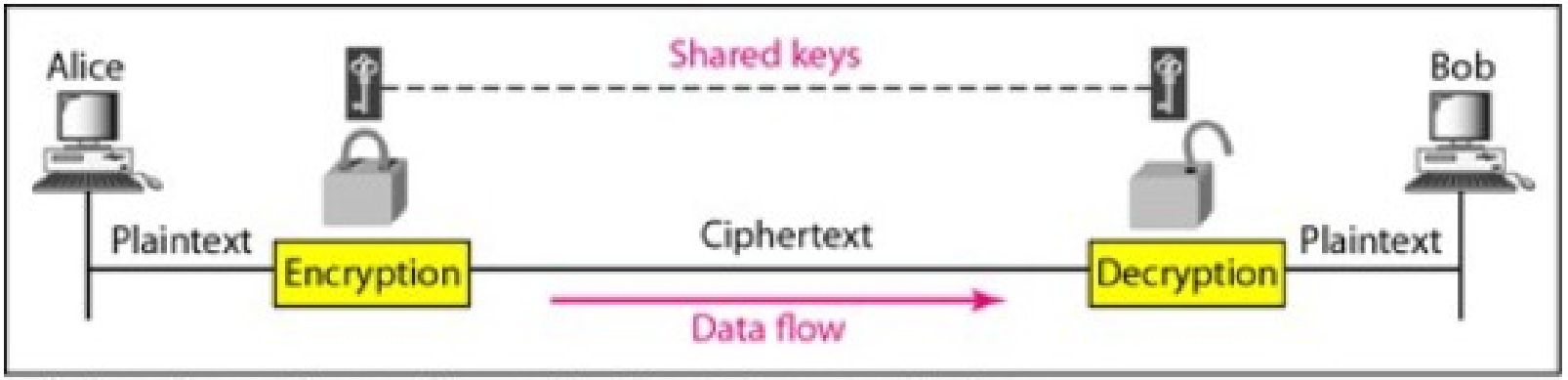


Prof. Viral S. Patel

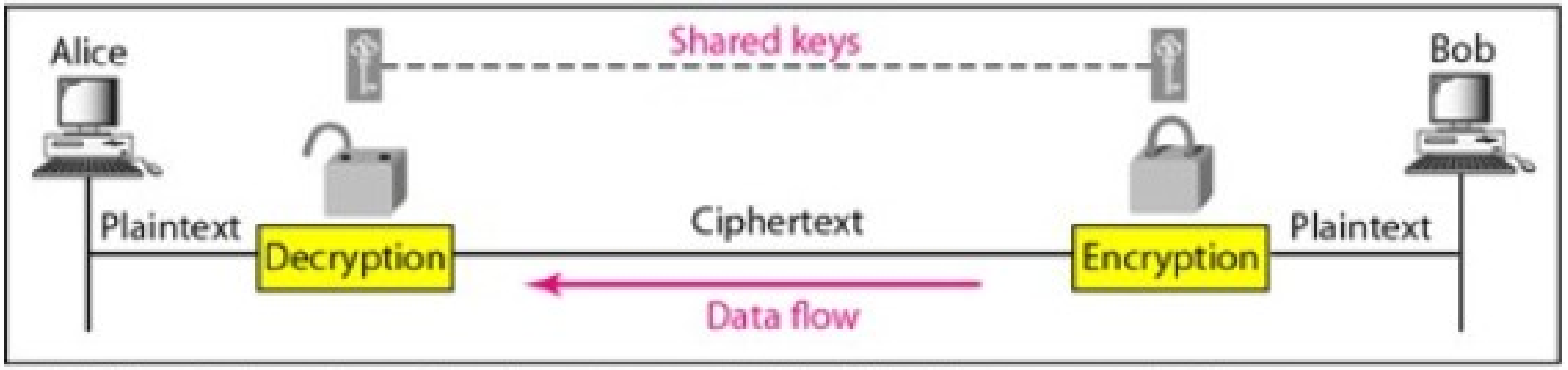
Message Confidentiality : message only send to and read by intended receiver.
Message Integrity : Message must no be changed and received as it sent.
Message Authentication : Sure of the sender's Identity.
Message Nonrepudiation : sender can send message only for its actual purpose not for other purpose.
Entity Authentication : entity or user identification and verified to access system resources.

Prof. Viral S. Patel

Message Confidentiality using symmetric keys in both directions :
Session key is used to key sharing. Session key exchange using asymmetric key cryptography.



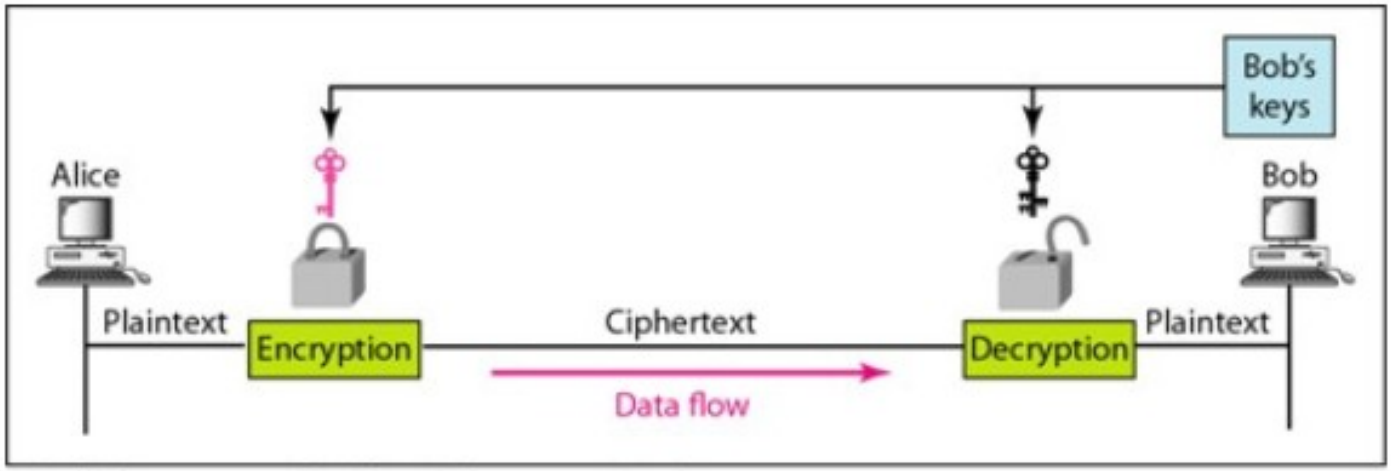
a. A shared secret key can be used in Alice-Bob communication



b. A different shared secret key is recommended in Bob-Alice communication

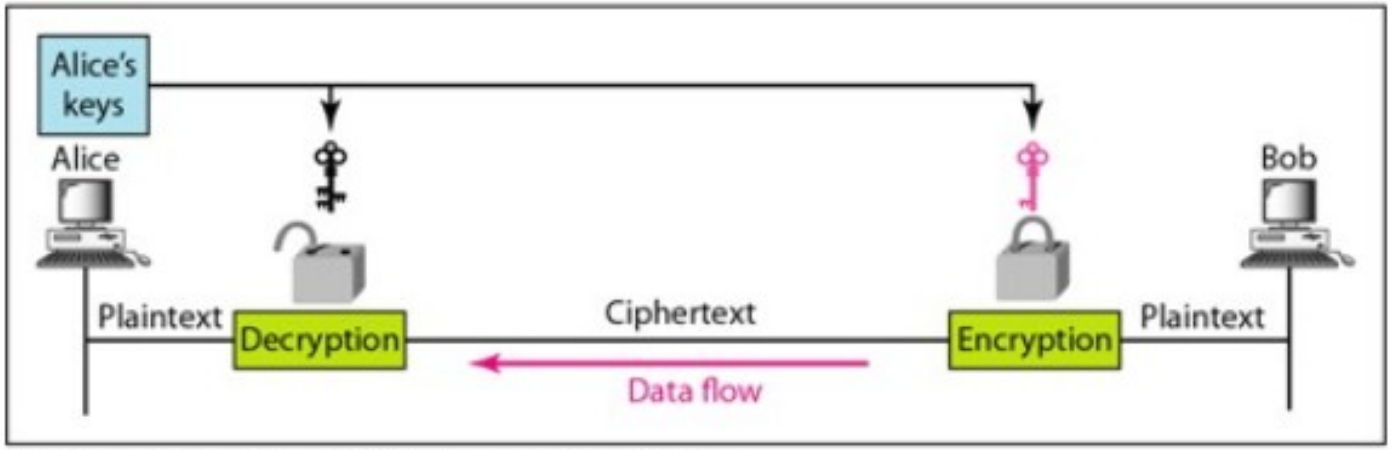
For long message, Symmetric-key cryptography is much more efficient than asymmetric-key cryptography.

Message confidentiality using asymmetric keys :



a. Bob's keys are used in Alice-Bob communication

Prof. Viral S. Patel



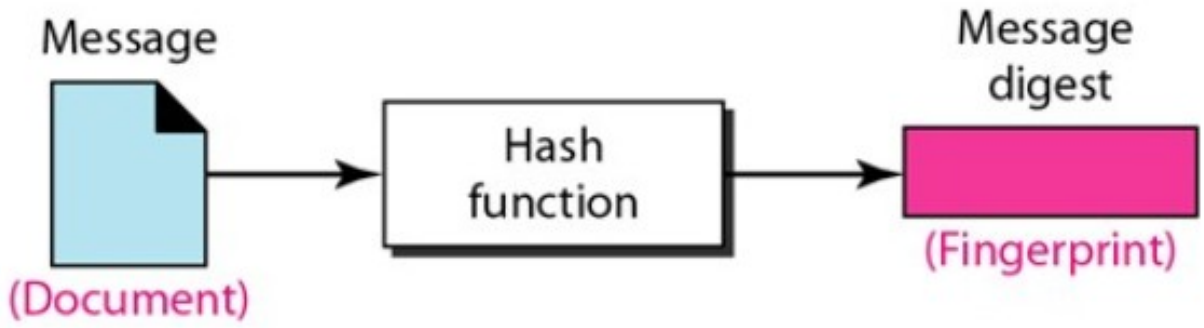
b. Alice's keys are used in Bob-Alice communication

Inefficient for long messages as method take long mathematical calculations using long keys. I should be applied **only to short messages.**

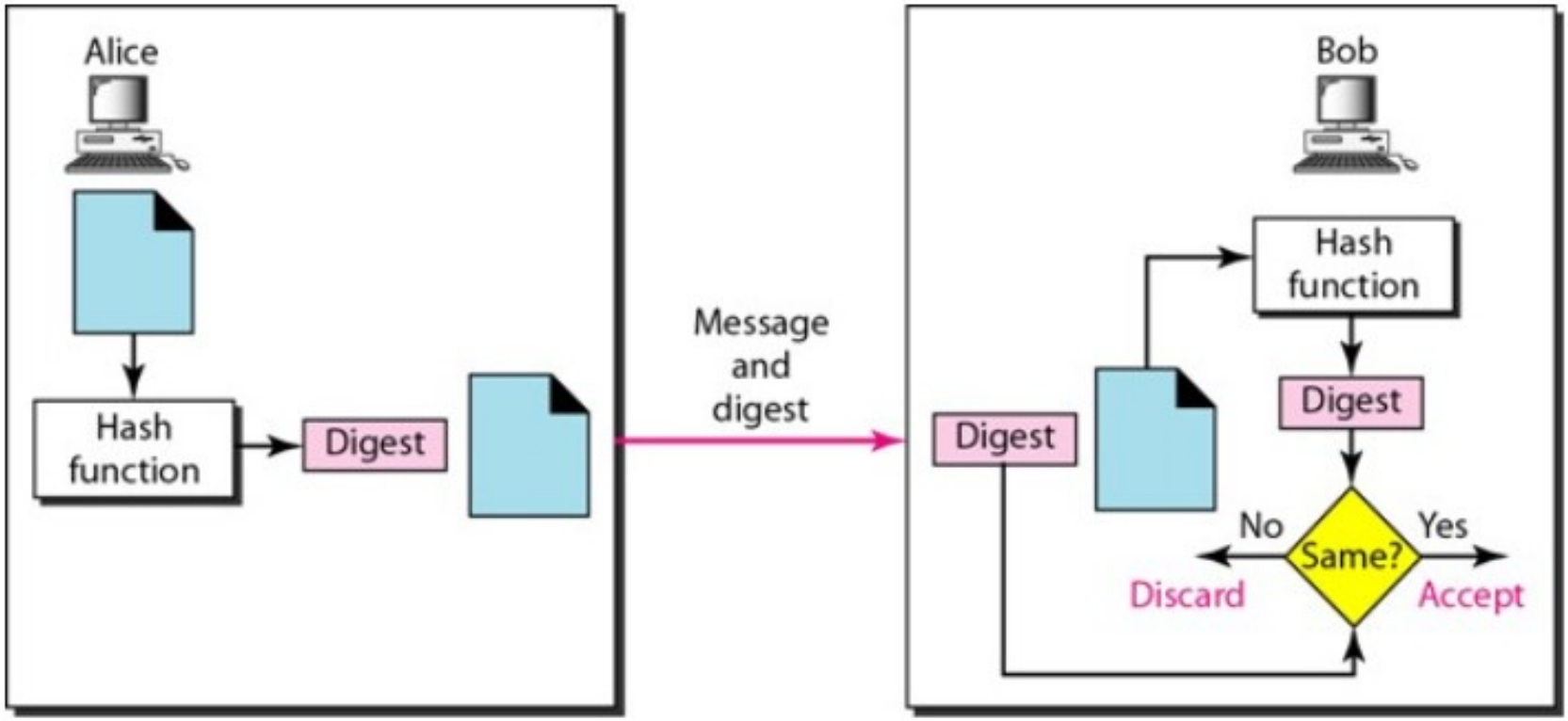
Message Integrity *Prof. Viral S. Patel*

Contents of Document will not be illegally changed

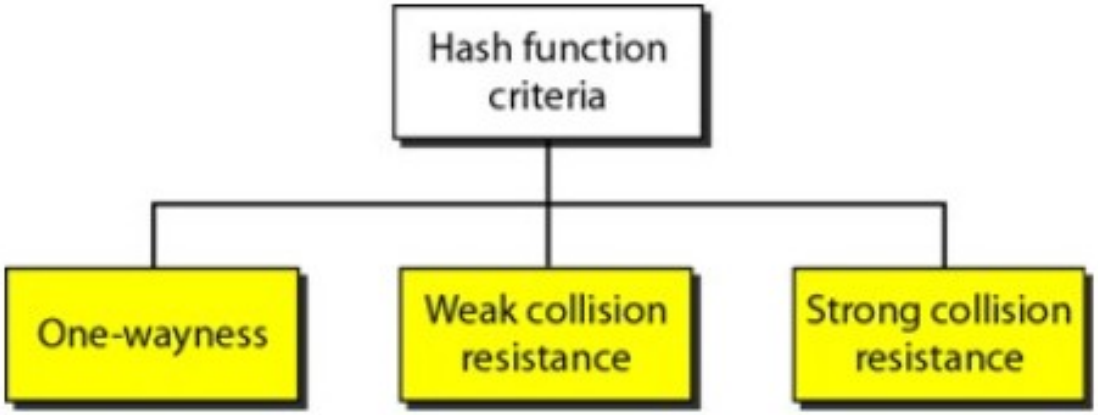
Message and Message Digest : provide message integrity



Creating and Checking the Digest :



Hash Function Criteria :



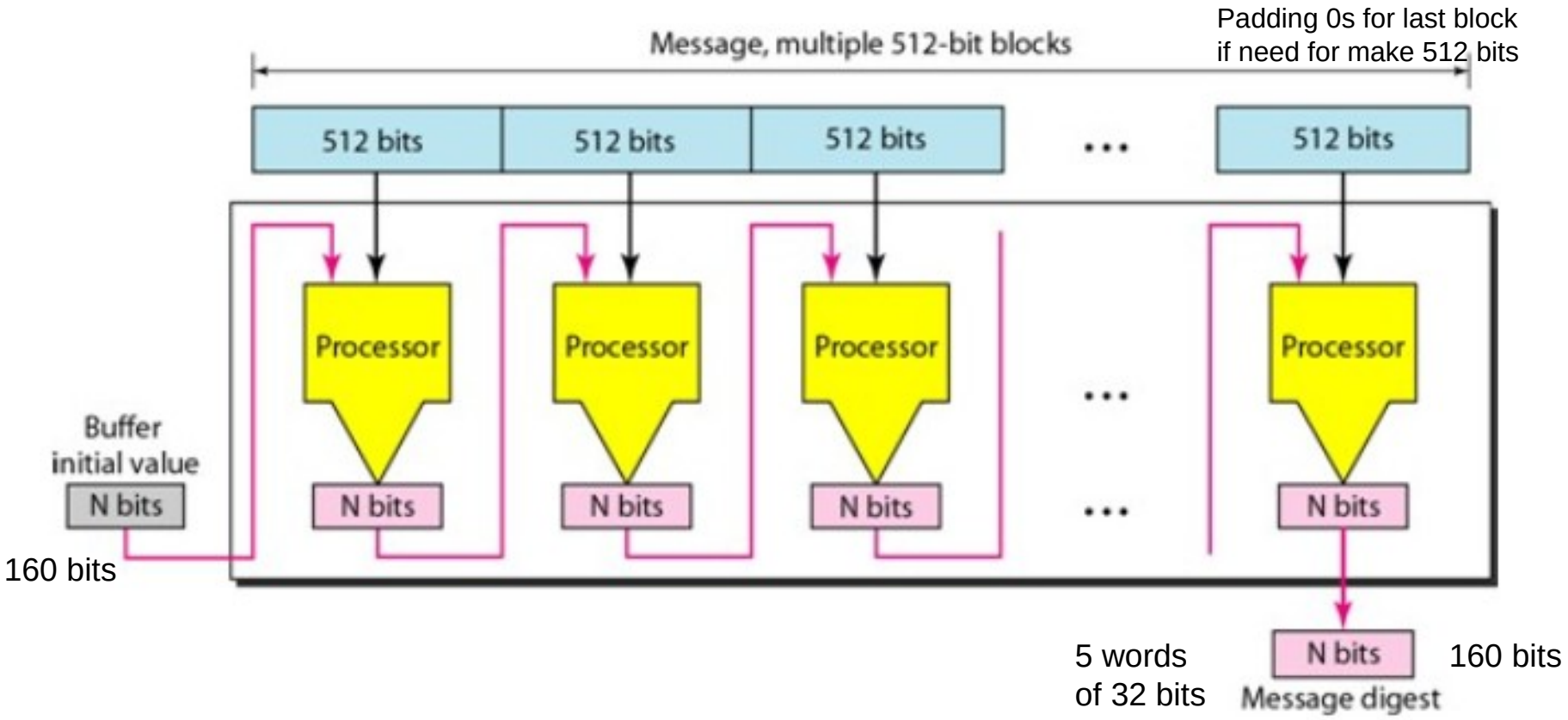
One-wayness : Once the message digest is created, we must not be able to recreate the message from the digest.

Prof. Viral S. Patel

Weak Collision Resistance : Once specific message and its digest create no other can create another message with same digest. For example, If Alice creates a message and a digest and sends both to Bob, this criterion ensures that Eve (hacker) cannot easily create another message that hashes exactly to the same digest.

Strong Collision Resistance : We cannot find two messages that has to the same digest from sender. For example, If Alice can create two messages that hash to the same digest, she can sending the first to Bob and claim that she sent only the second.

Hash Algorithm : SHA-1 (Secure Hash Algorithm -1)



SHA-1 hash algorithm create an N-bit message digest out of a message of 512-bit blocks.
SHA-1 has a message digest of 160 bits (5 words of 32 bits).

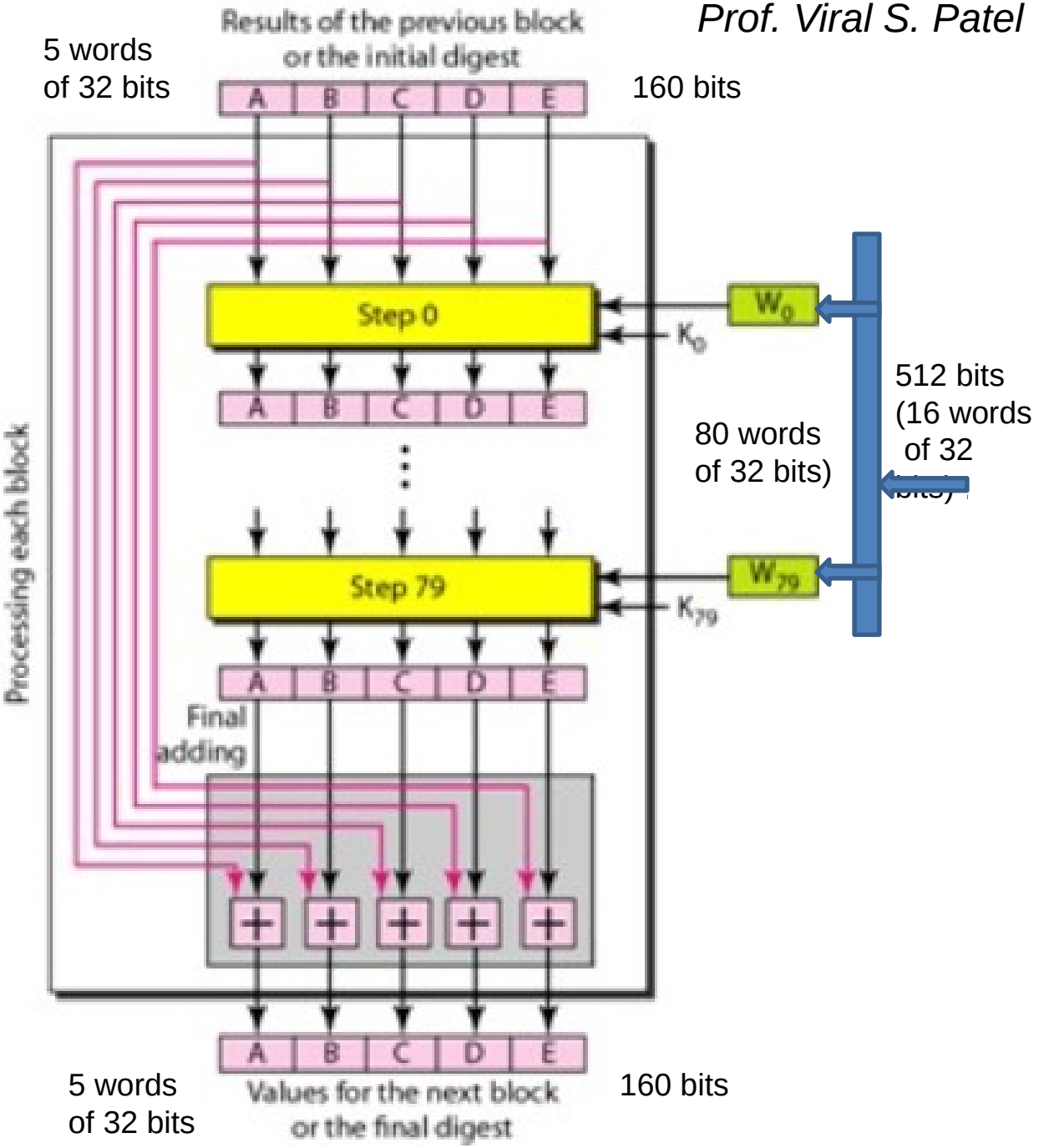
Message Integrity

Hash Algorithm : SHA-1

Processing of One block in SHA-1

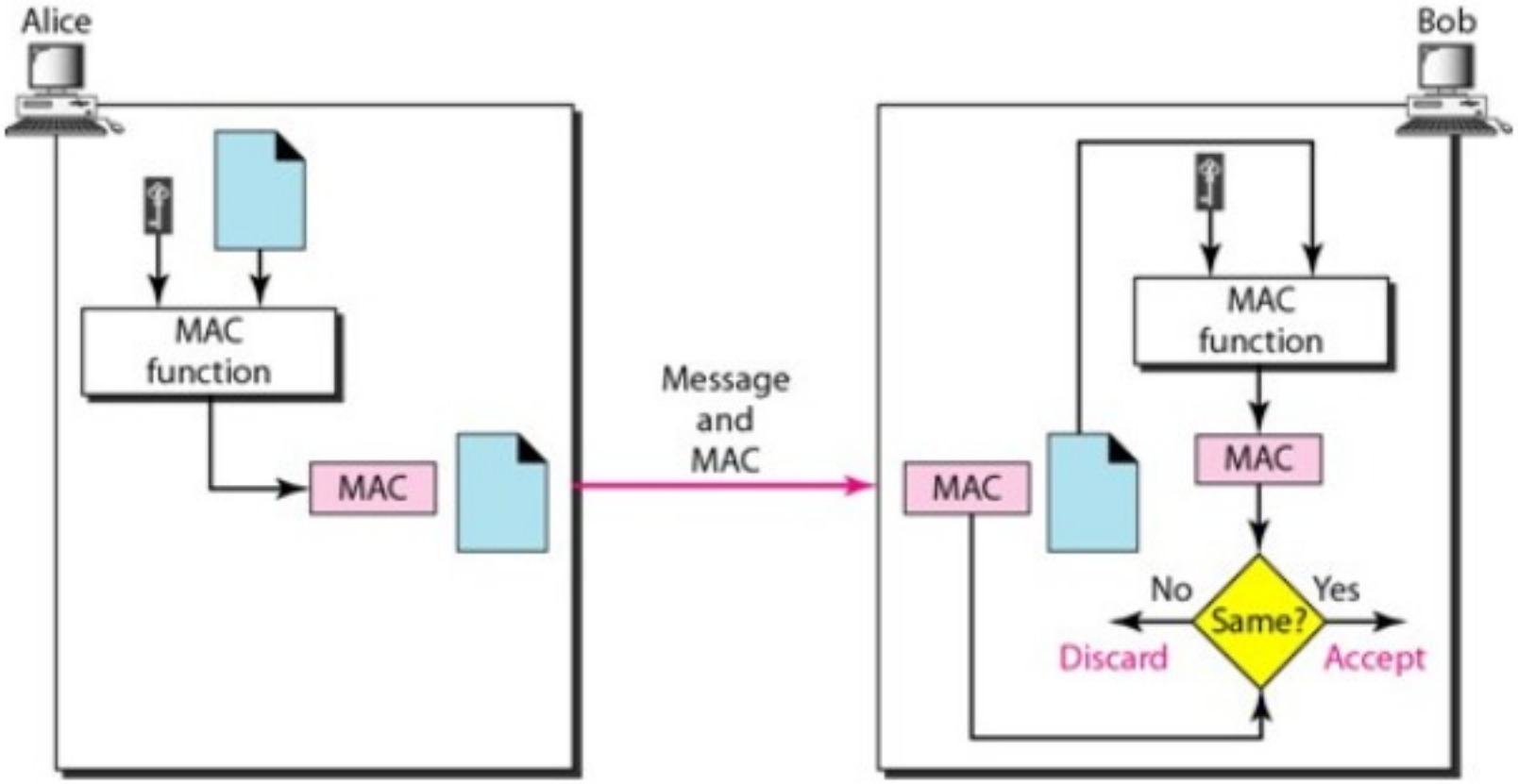
A block is made of 512 bits or 16 words of 32-bit, but we need 80 words in processing phase.

So the 16-word block Needs to be expanded to 80 words, word 0 to Word 79

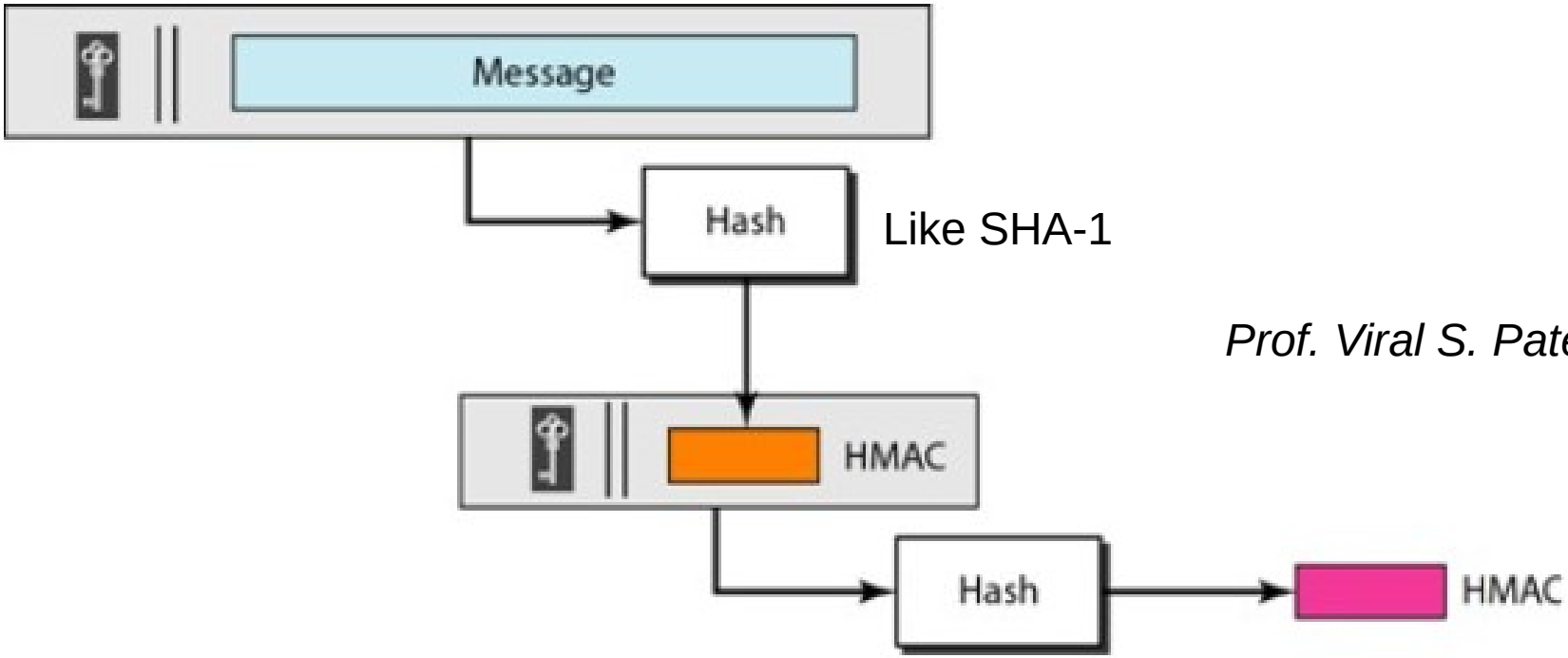


MDC (Modification Detection Code) : Hash function only give message integrity It is keyless Hash function.

MAC (Message Authentication Code) : Provide message integrity and message authentication. **symmetric key** established between sender and receiver. Use **keyed hash function**.



HMAC (Hashed Message Authentication Code) :
Use **keyless hash functions such as SHA-1**. Provide message integrity and message authentication.



A symmetric key is joined with message. This combination is hashed using a keyless hash function, such as SHA-1. The result of this process is an intermediate HMAC which is again joined with the same key and the result is again hashed using the same algorithm. The final result is an HMAC. This HMAC and original message received by receiver. The receiver creates its own HMAC from received message and symmetric key. Finally authenticate the data origin.

Digital Signature :
MAC provide message integrity and message authentication **using symmetric key.**
Digital signature use asymmetric keys (public and private key) for message integrity and message authentication. It is not used for confidentiality.

Comparison : conventional and digital signatures.
Inclusion : In conventional signature is included in the document. In digital signature sender send two separate documents : the message and signature. Receiver verifies signature and confirm the sender.

Verification Method : In conventional document signature compares with signature on file. In digital signature the recipient needs to apply a verification technique to the combination of the message and the signature to verity the authenticity.

Prof. Viral S. Patel

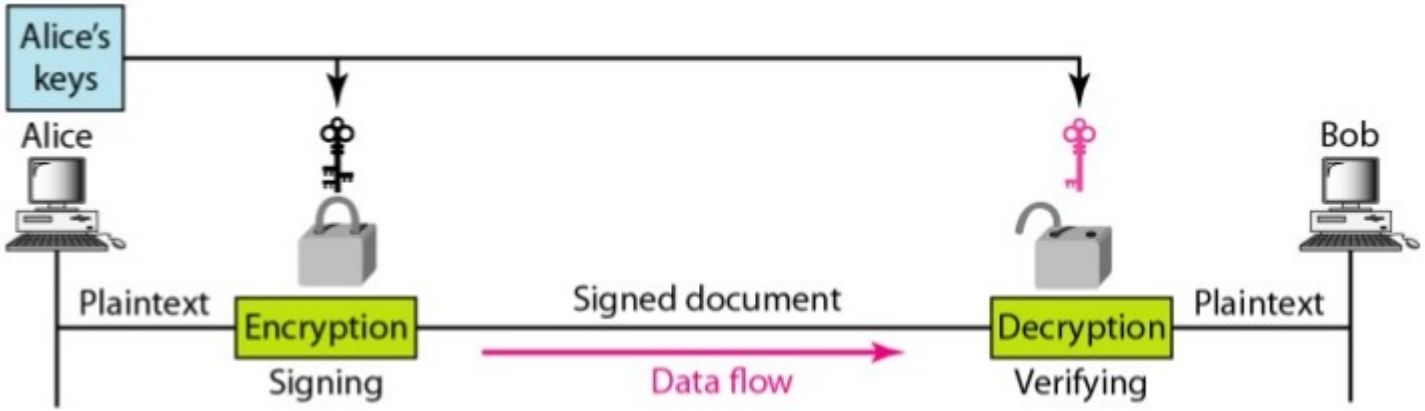
Relationship : A person use one signature for many documents. In digital signature, one-to-one relationship between a signature and a message. The signature of one message cannot be used for another message.

Duplicity : A copy of the signed document can be distinguished from original one on file. In digital signature, factor of time is used on document.

Digital Signature :

Needs for Keys

Private key is used with signing algorithm to sign the document means encrypt the document and public key is used with verify algorithm means decrypt it to verify the document.



We cannot use secret (symmetric) key to both sign and verify a signature.

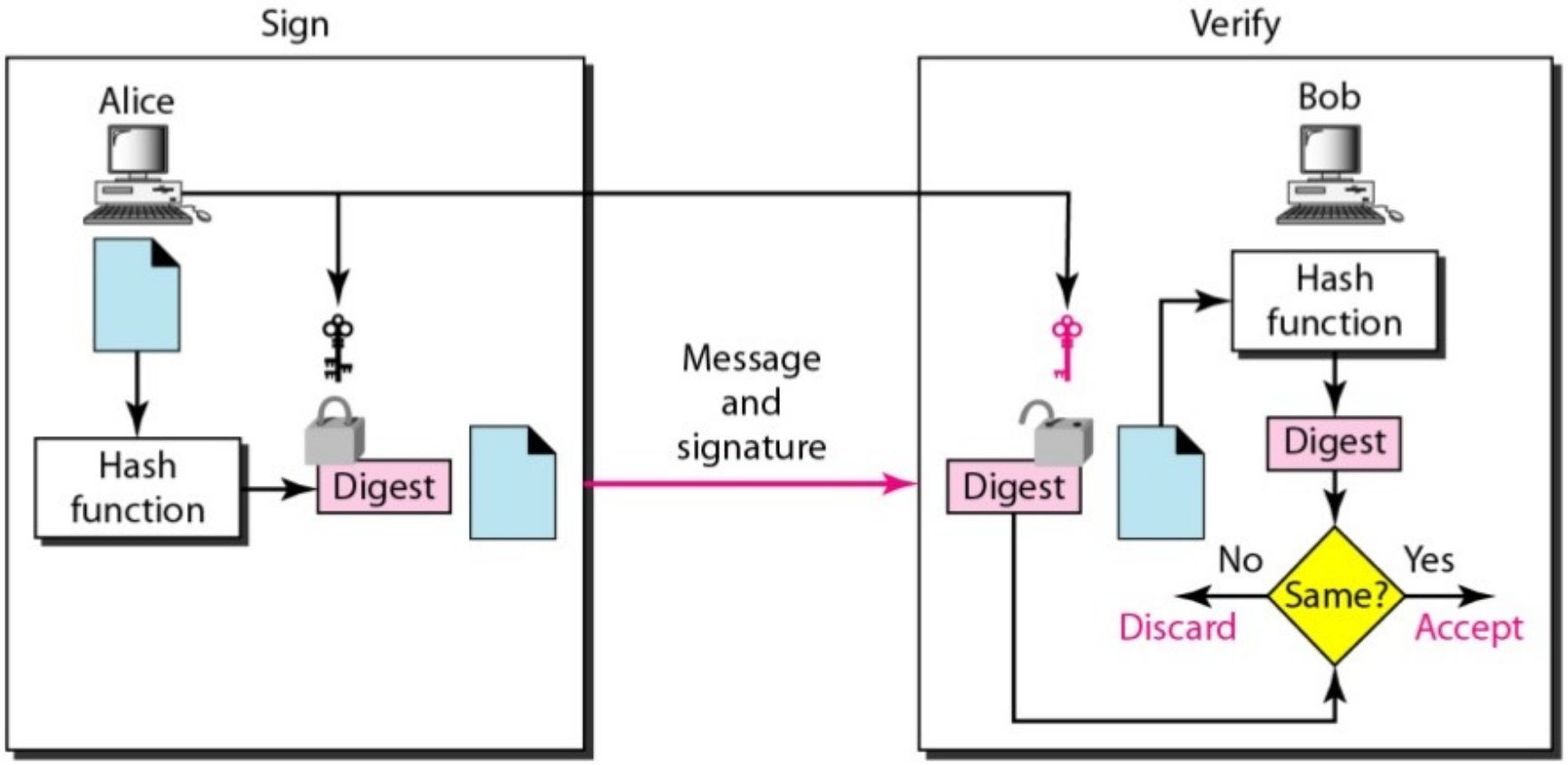
Prof. Viral S. Patel

Signing the Document Private and public keys are used for digital signature and for confidentiality are different ways.

- In **confidentiality** (cryptosystem) private and public keys of receiver are used. Sender use public key to encrypt and private key for decrypt.
- In **digital signature** private and public keys of sender are used. Sender used private key to encrypt and public key for decrypt.

Digital Signature :

Signing the Digest Asymmetric key is inefficient for long messages so we selected message digest and then process it using private key for signing. This way we create digital signature. Sender send message and digital signature Message digest may be used other secret keys. At receiver side same Hash function apply on received message to generate digest. Public key is used to decrypt received digest from sender. So calculations are done and verifying the result. If authentic, the message is accepted otherwise rejected.



Digital Signature :

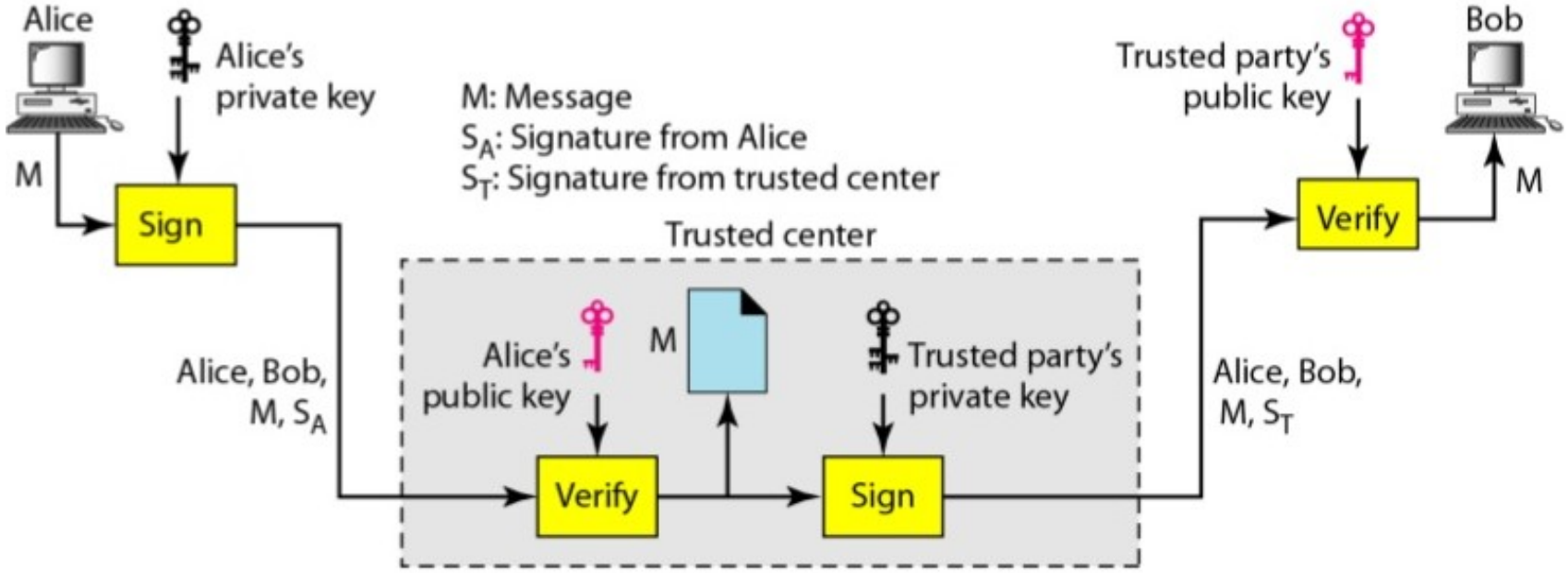
Services :

A digital signature can provide three out of the five services.

- **Message integrity :** Digital Signature provide message integrity as we cannot generate same signature if message is changed.
- **Message authentication :** receiver use public key of sender to verify the message of sender. Receiver cannot create same signature for other sender's private key.

Prof. Viral S. Patel

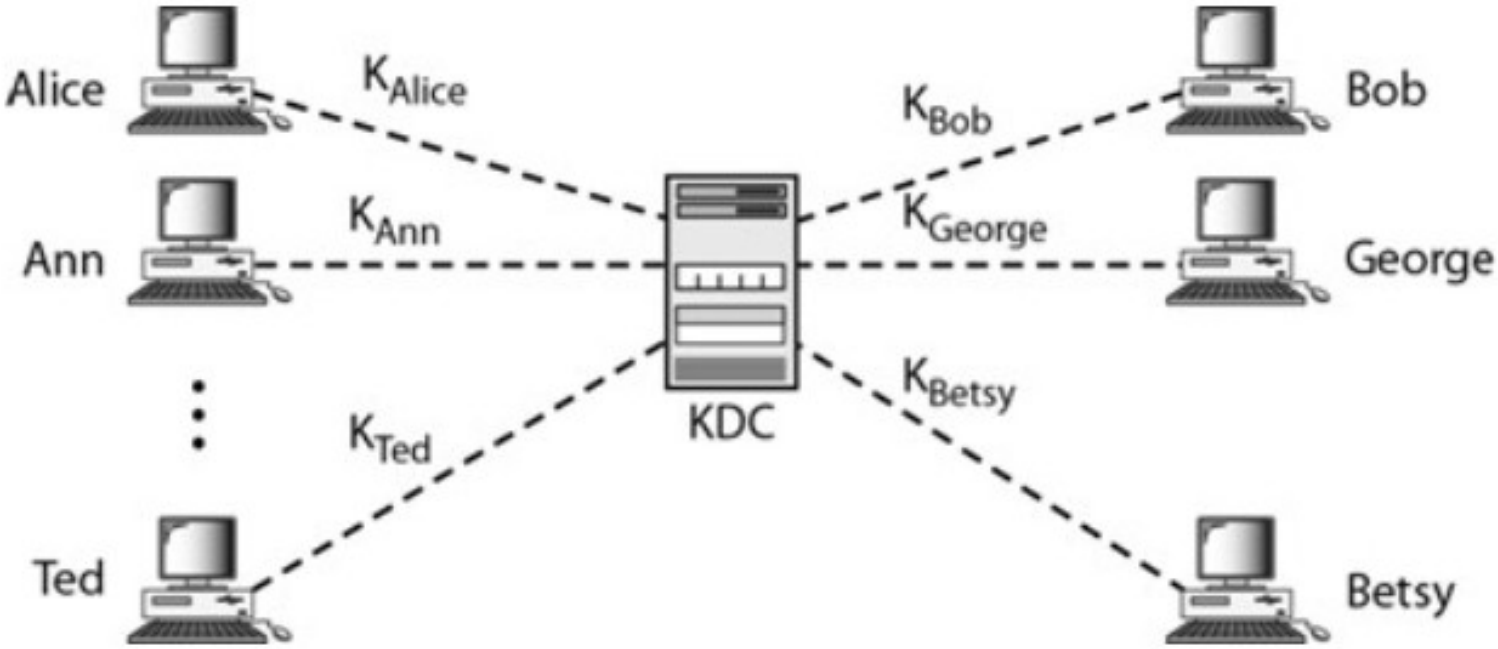
- **Nonrepudiation :** sender may deny later that he/she not sent message. Receiver might have a problem to prove because sender changed his/her private/ public key during this time. So one solution of this problem is trusted third party.



Symmetric-key Distribution :

KDC (key distribution center) :

We need an efficient way of maintaining and distributing **secret keys**. The solution is the use of trusted party, referred to as a **key distribution center (KDC)**



Each person establishes a shared secret key with the KDC.

Symmetric-key Distribution :

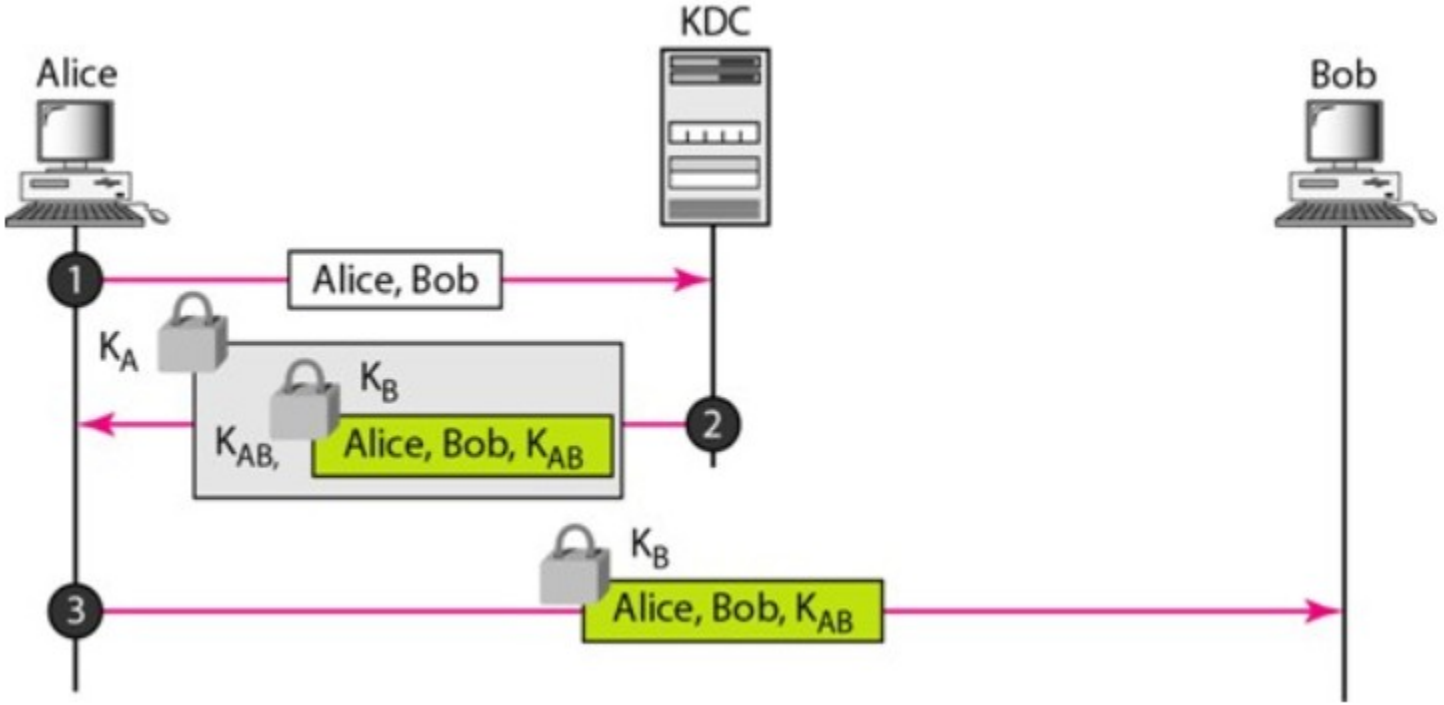
Creating/Sharing Session key between sender and receiver :

Step 1 : Alice send request to KDC to obtain symmetric session key between herself and Bob

Step 2 : KDC generate ticket which contain identity of Alice and Bob and the session key K_{AB}. Ticket is encrypted using Bob's key K_B and then again encrypted with the copy of session key K_{AB} using the Alice's secret key K_A and then send to Alice. Alice decrypt it and get session key but cannot decrypt ticket which is actually for Bob.

Prof. Viral S. Patel

Step 3 : Alice send the ticket to Bob. Bob open the ticket and know that Alice needs to send messages to him using K_{AB} as the session key.



Public-key Distribution :

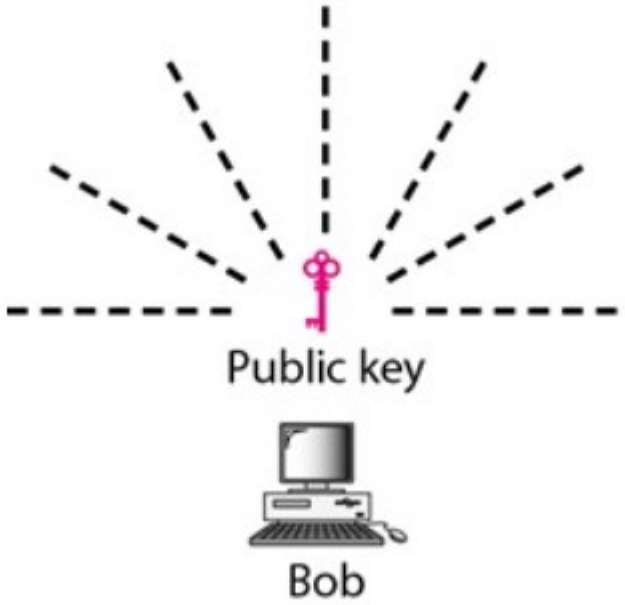
In public-key cryptography (Asymmetric-key cryptography) sender needs to know the public key of receiver to send message.

Public announcement :

In public announcement public key is announce publicly. But problem is subject to forgery.

Prof. Viral S. Patel

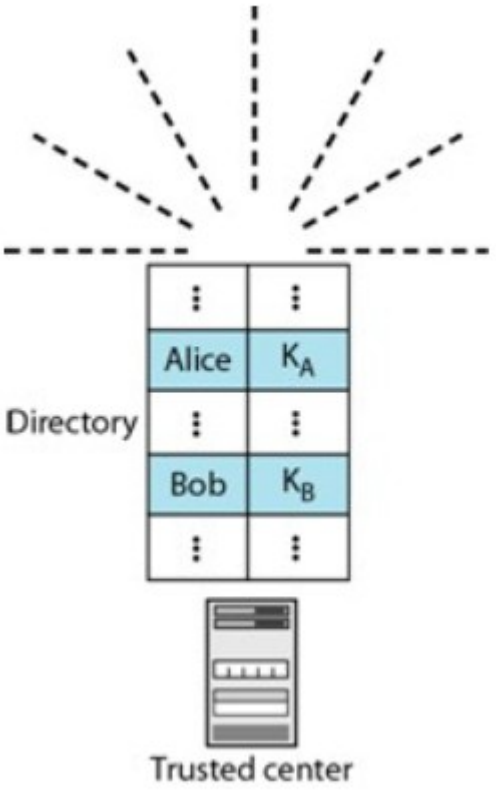
For example Alice need to send message to Bob. So Bob announce public key by newspaper or from his site or by send message. Eve could also make such a public announcement. Before Bob can react, damage could be done. Eve could also sign a document with a corresponding forged private key and make everyone believe it was signed by Bob.



Public-key Distribution :

Trusted Center :

A more secure approach is to have a trusted center retain a directory of public keys. The directory is dynamically updated. Each user can select a private/public key, keep the private key and deliver the public key for insertion into the directory. The center give respond to any inquiry about a public key.



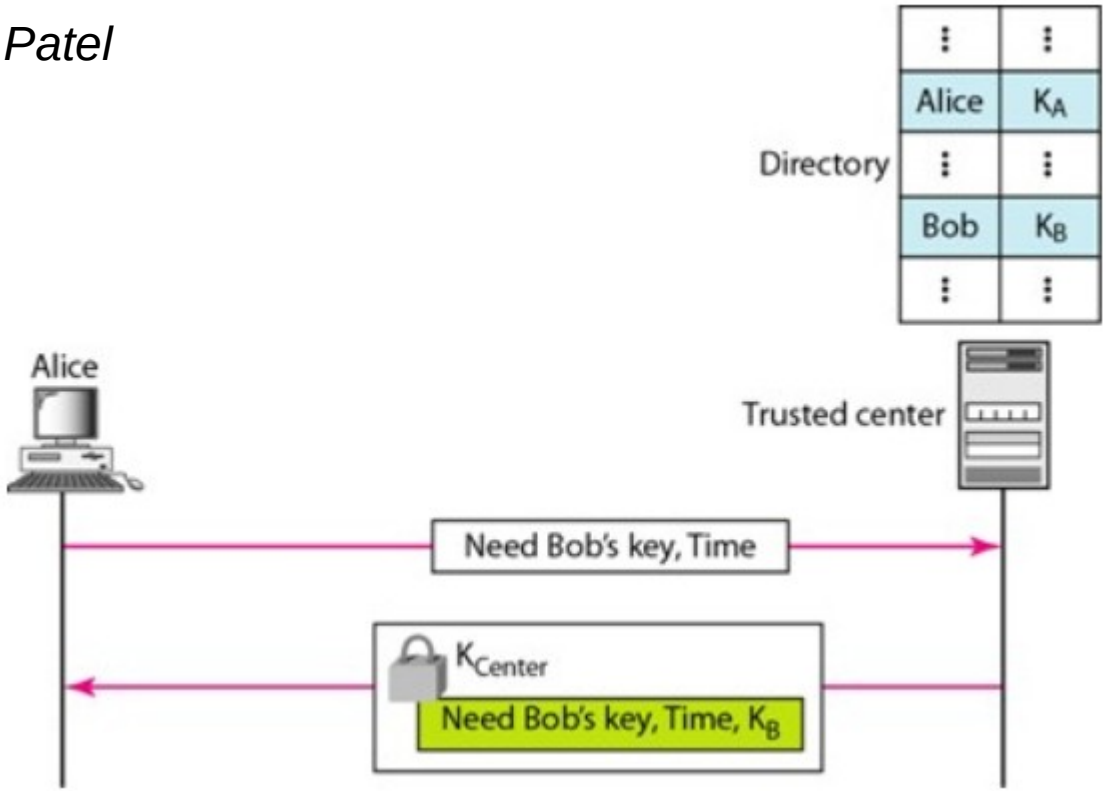
Public-key Distribution :

Controlled Trusted Center :

A timestamp and signed by an authority can be used to prevent interception and modification of the response.

Example : if Alice needs to know Bob's public key, she can send a request to the center including Bob's name and a timestamp. The center responds with Bob's public key, the original request, and timestamp signed with the private key of the center. Alice uses the public key of the center to decrypt the message and extract Bob's public kev.

Prof. Viral S. Patel



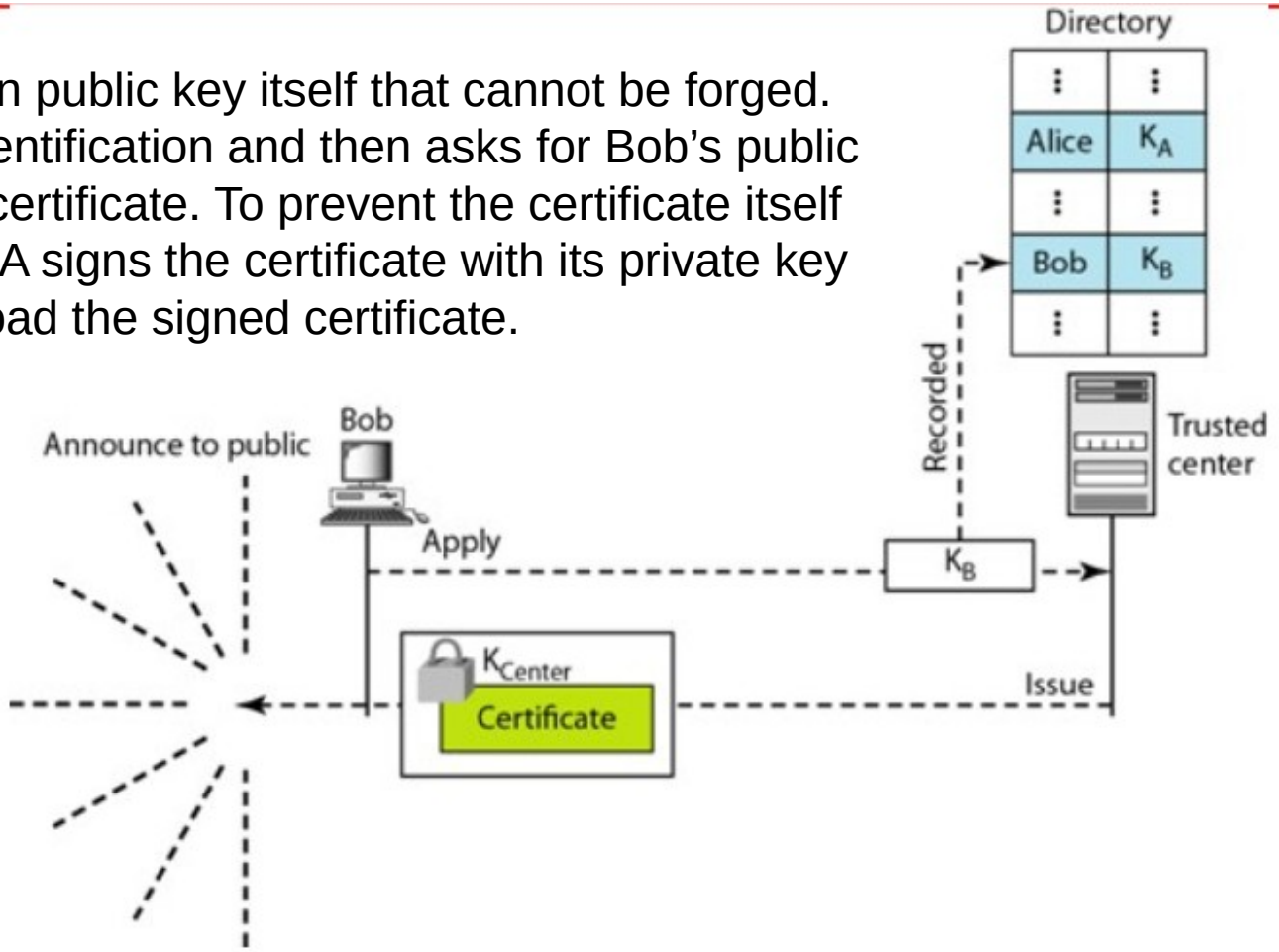
Public-key Distribution :

Certificate Authority (CA):

The previous approach can create a heavy load on the center if the number of requests is large. The alternative is to create public-key certificates. As shown in figure Bob can go to a Certification Authority (CA) – a federal or state organization that binds a public key to an entity and issues a certificates.

The CA has a well-known public key itself that cannot be forged. The CA checks Bob's identification and then asks for Bob's public key and writes it on the certificate. To prevent the certificate itself from being forged, the CA signs the certificate with its private key K_{center}. Now Bob can upload the signed certificate.

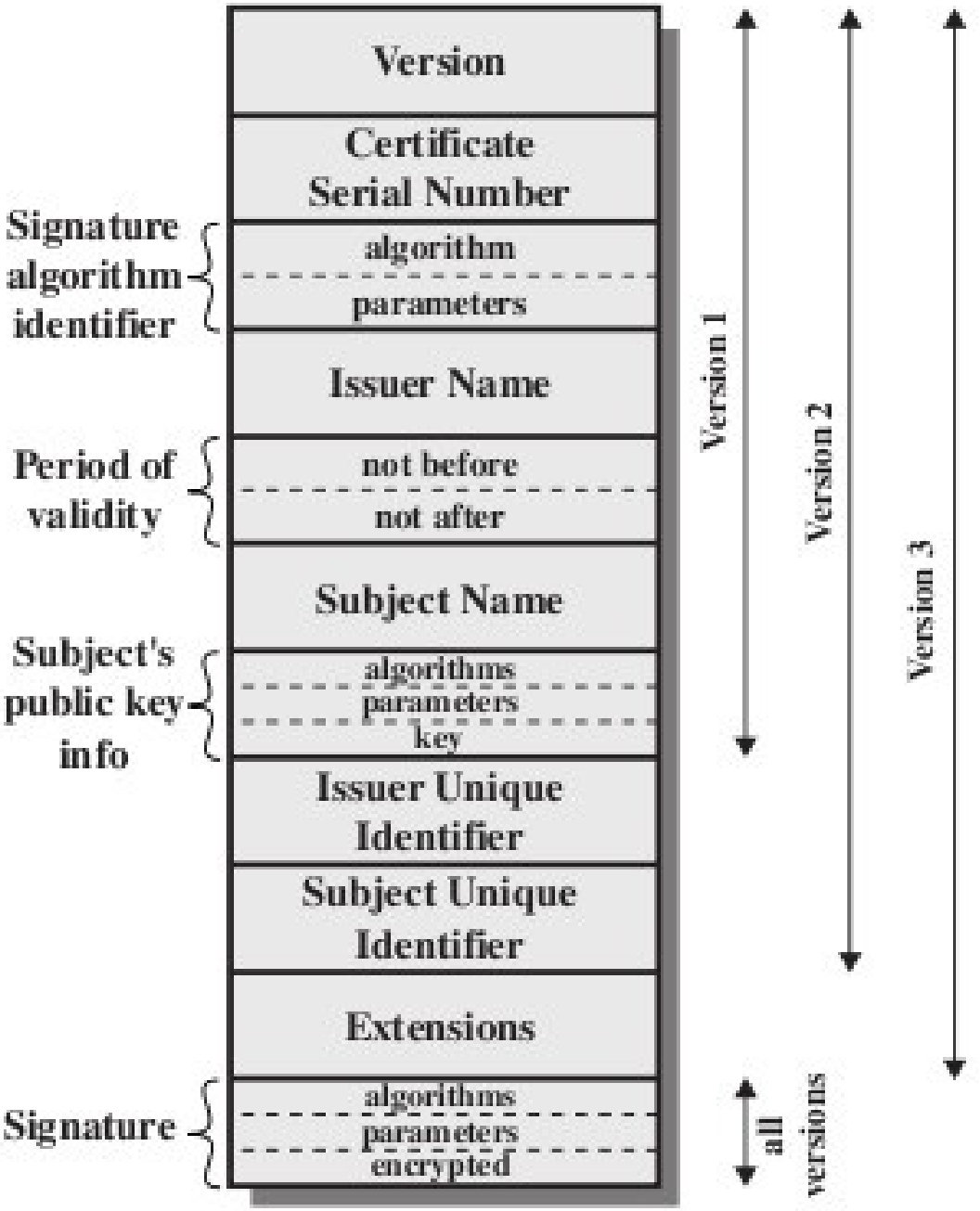
Anyone who wants Bob's public key downloads the signed certificate and uses the public key of the center to extract Bob's public key.



X.509 certificate

Each certificate have a different format. So for universal format ITU has designed a protocol called X.509. It uses a well know protocol called ASN.1 (Abstract Syntax Notation 1) that defines fields familiar to C programmers.

Version : started at 0.Current is 2 (3rd version).
Serial number : unique number given to certificate
Signature : specify algorithm used to sign and its parameters.
Issuer name :name of Certificate Authority
Period of validity : time of certificate valid.
Subject : name of owner / beholder of the public key.
Subject's public key : public key, corresponding algorithm and its parameters.
Issuer Unique identifier : allows two issuers unique identifiers.
Subject unique identifier : allows two different subject unique identifiers
Extension : allows issuer to add more private information
Signature : algorithm identifier, secure hash of other fields and digital signature of that hash.



(a) X.509 Certificate

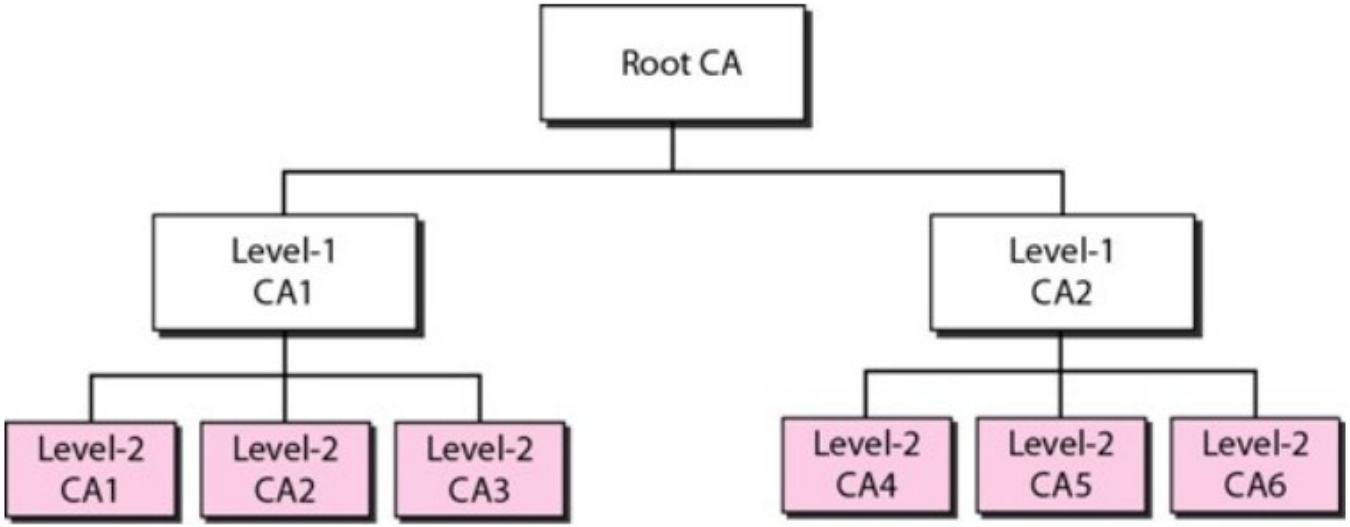
Public-Key Infrastructures (PKI)

Use public keys universally have problem in distribution (similar to secret-key) as number of request and users are very large so we cannot have only one KDC to answer the queries. We need many servers. The best solution is to put the servers in a hierarchical relationship called public-key infrastructure (PKI) as shown in fig.

Upper level CAs clarify their next level CAs. Upper level CAs operate in a large geographic or logical area. And Below level CAs may operate in smaller geographic areas.

Prof. Viral S. Patel

Everybody trusts the root. But people may or may not trust intermediate CAs. If Alice needs to get Bob's certificate, she may find a CA somewhere to issue the certificate. But Alice may not trust that CA. In a hierarchy Alice can ask the next-higher CA to certify the original CA. The inquiry may go all the way to the root.

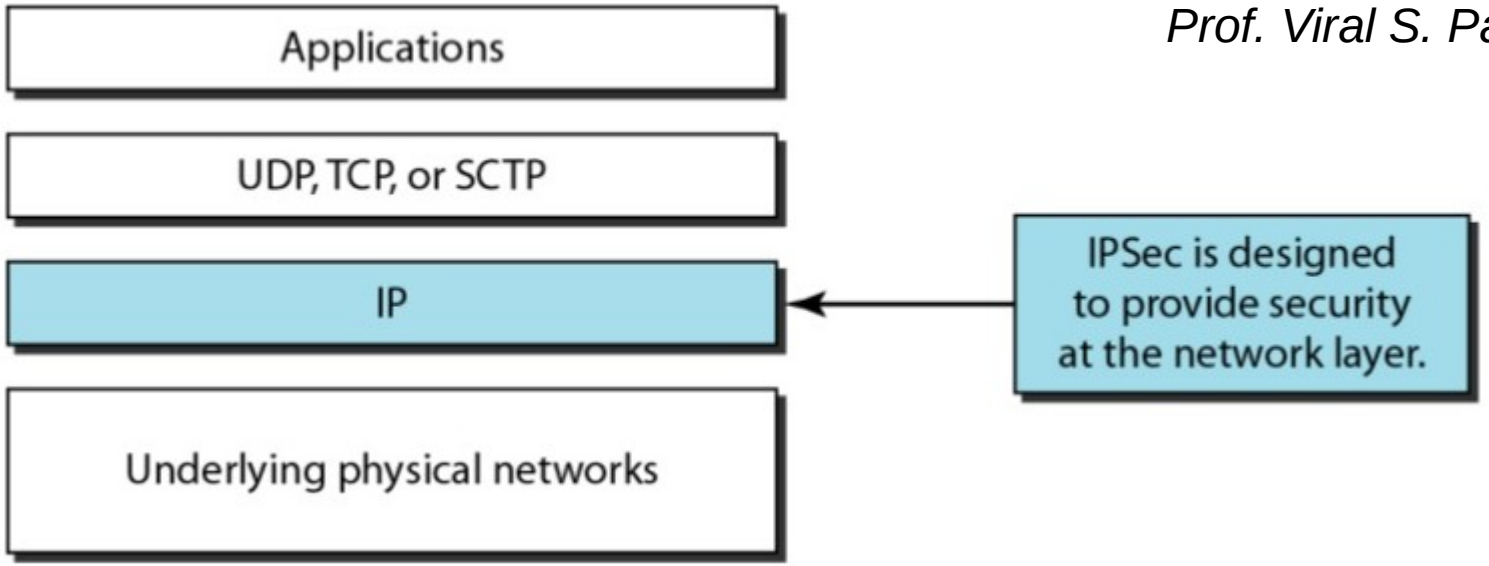


IPSecurity (IPSec)

IPSecurity (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to **provide security for a packet at the network level**.

IPSec helps to create authenticated and confidential packets for the IP layer as shown in fig.

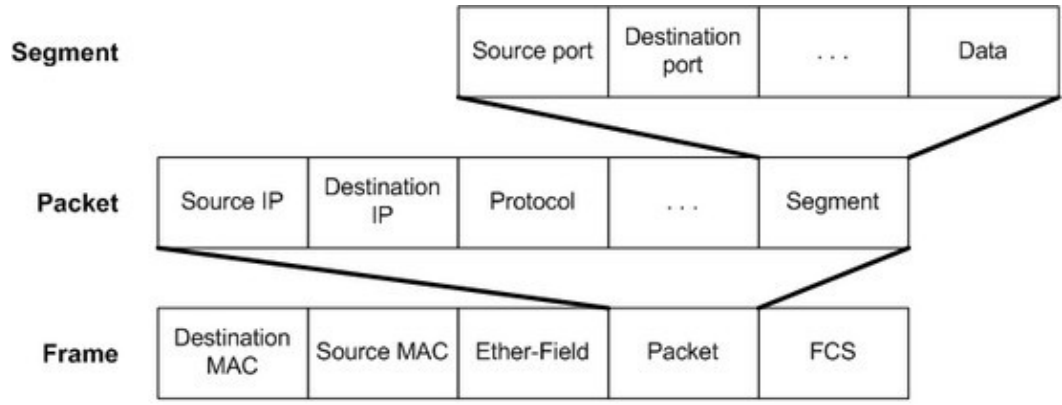
Prof. Viral S. Patel



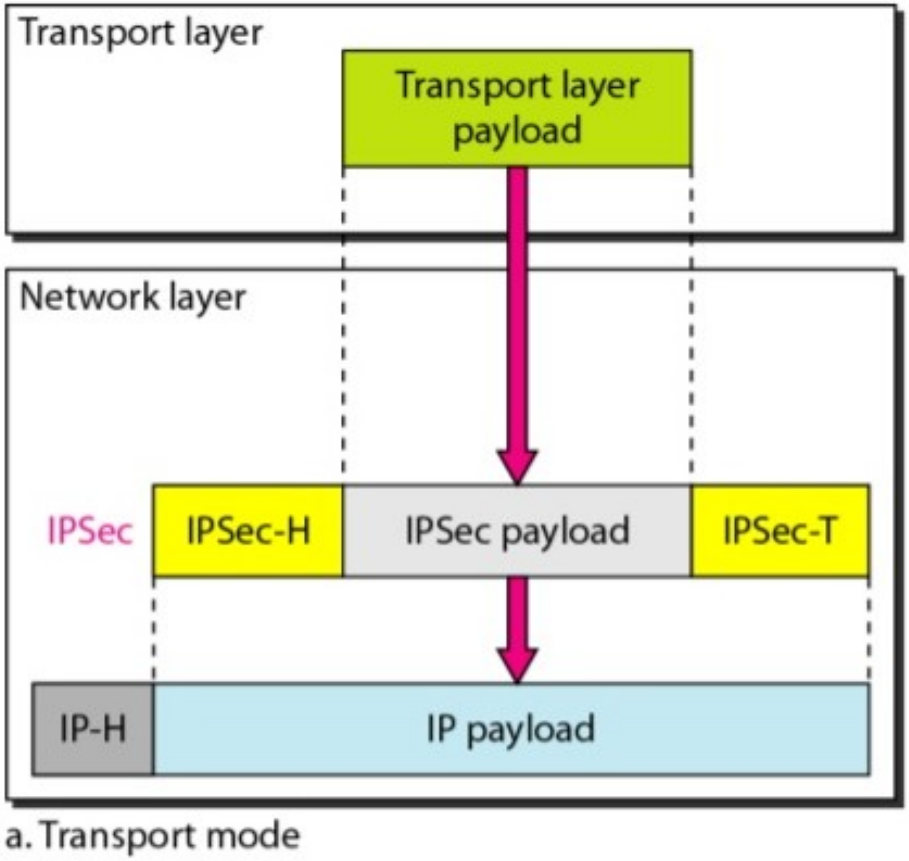
IPSecurity (IPSec)

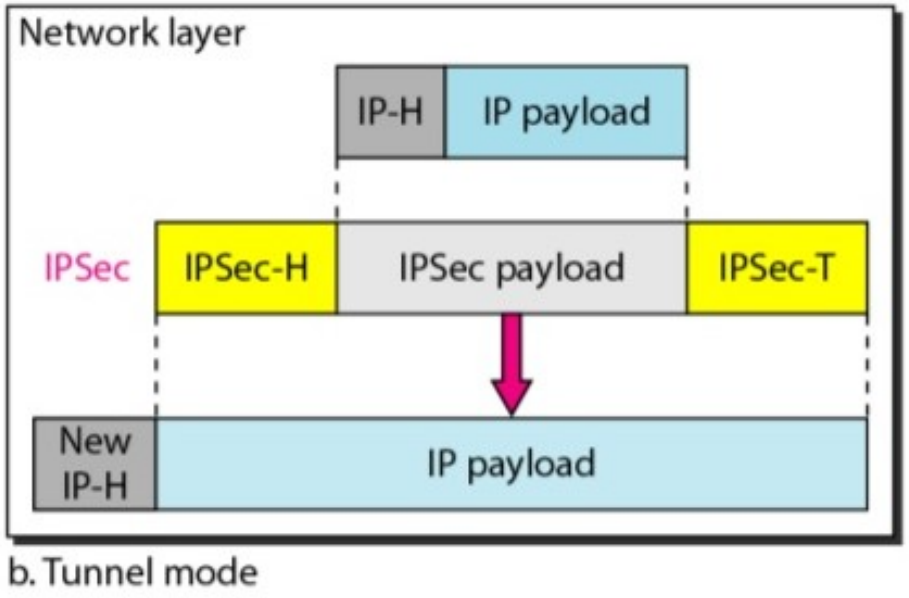
Two Modes :
IPSec operates in one of two different modes :

- **The transport mode**
- **The tunnel mode**



Prof. Viral S. Patel





IPSecurity (IPSec)

Transport mode

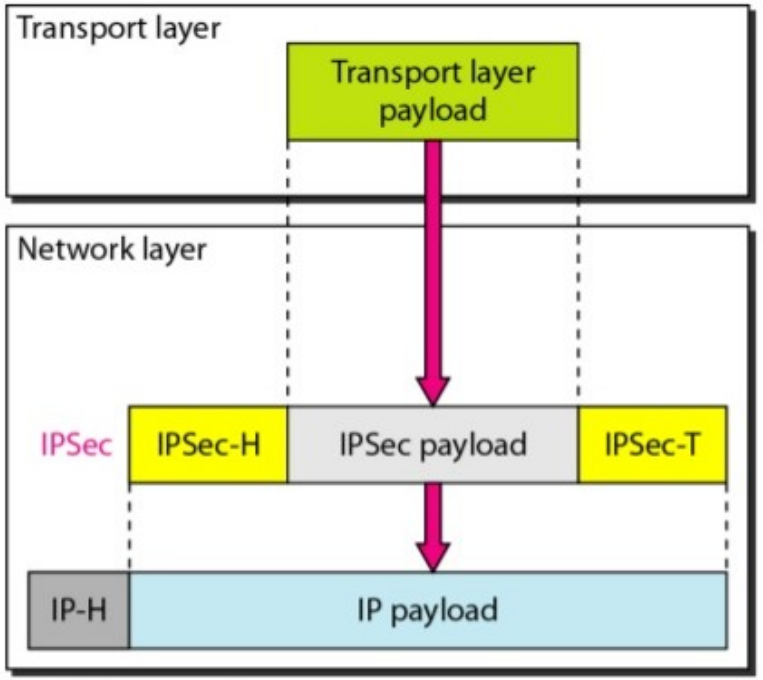
➔ It protects (authenticate and/or encrypt) what is delivered from the transport layer to the network layer, called IPSec payload.

IPSec header and trailer are then added.

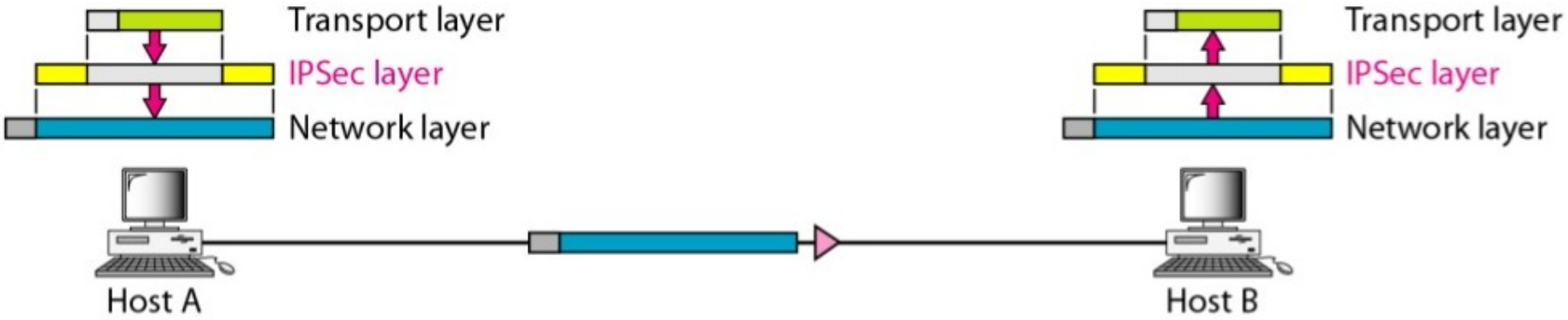
➔ It does not protect the IP header. Only protect information coming from transport layer.

➔This transport mode is normally used when we need host-to-host protection of data.

➔ The sending host uses IPSec to authenticate and/or encrypt the payload delivered from the transport layer. The receiving host uses IPSec to check the authentication and/or decrypt the IP packet and deliver it to the transport layer.



a. Transport mode



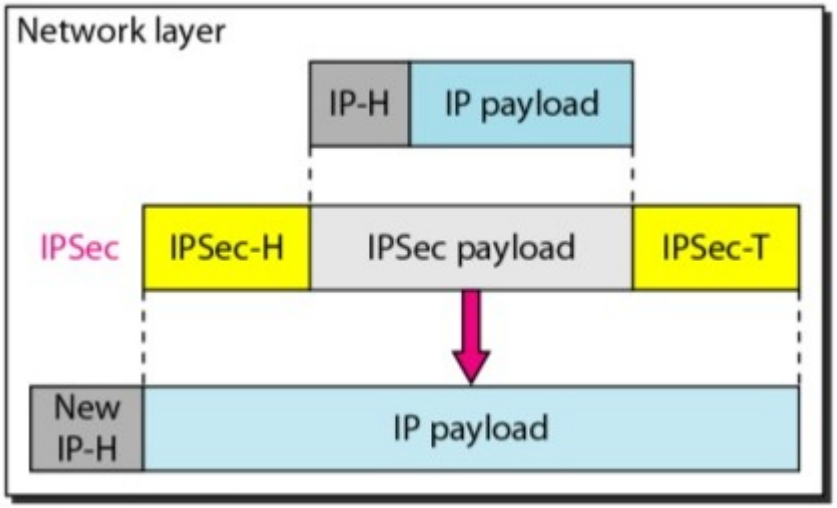
IPSecurity (IPSec)

Tunnel mode

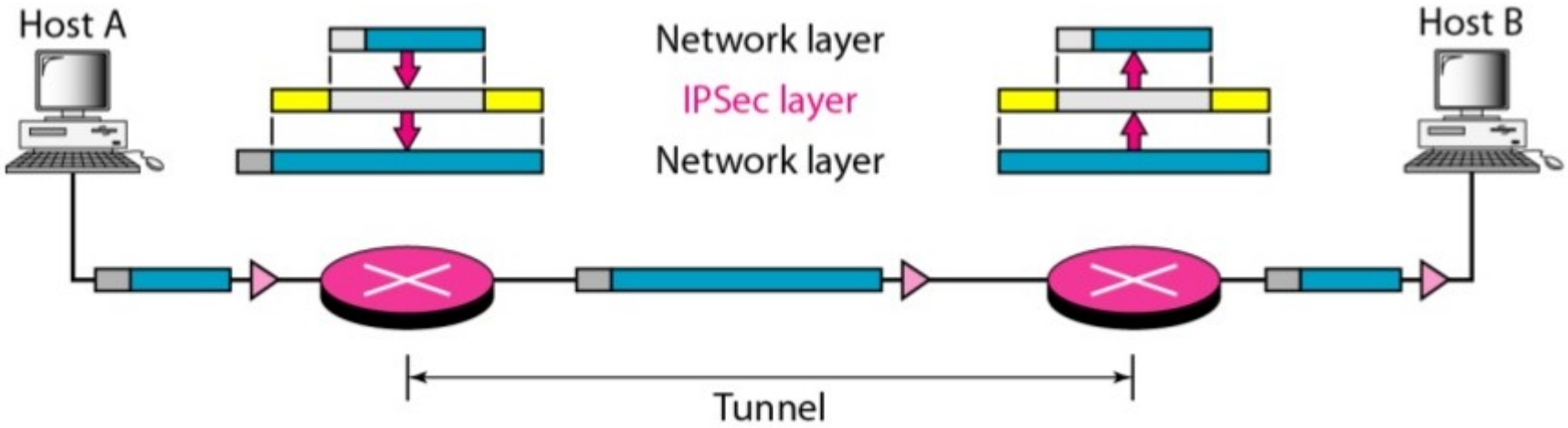
➔ In the tunnel mode, IPSec protects the entire IP packet. It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header as shown in fig.

The new IP header has different information than the original IP header. The tunnel mode is normally used between two routers, between a host and a router, or between a router and a host as shown in fig. *Prof. Viral S. Patel*

The entire original packet is protected from intrusion between the sender and receiver.



b. Tunnel mode



VPN – Virtual Private Network

It is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and inter-organization communication, but require privacy in their internal communications. It uses the IPSec Protocol to apply security to the IP datagrams.

Related Terms :

Internet : It is a public network, used to access global information and for instant communication by anyone, anywhere and anytime.

Prof. Viral S. Patel

Intranet : It is a private network of some organization which is accessible by authorised users of that organization. It is inaccessible from the outside. the Intranet is mainly used to share data, information, resources, company programs, software applications, as well as facilitate communication between people or work groups within the company. Intranet usually have a application program, firewall and router, which permits access to the public internet while protecting the internal intranet from malicious users.

Extranet : It is same as an intranet with one major difference : some resources may be accessed by specific groups of users outside the organization under control of the network administrator. For example, an organization may allow authorized customers access to product specification, availability and online ordering.

Private Networks

A private network is designed for use inside an organization. It allows access to shared resources and at the same time, provide privacy.

Private network that uses the Internet model must use IP addresses.

Addressing

Prefix	*Range*	*Total*
10/8	10.0.0.0 to 10.255.255.255	2^{24}
172.16/12	172.16.0.0 to 172.31.255.255	2^{20}
192.168/16	192.168.0.0 to 192.168.255.255	2^{16}

Prof. Viral S. Patel

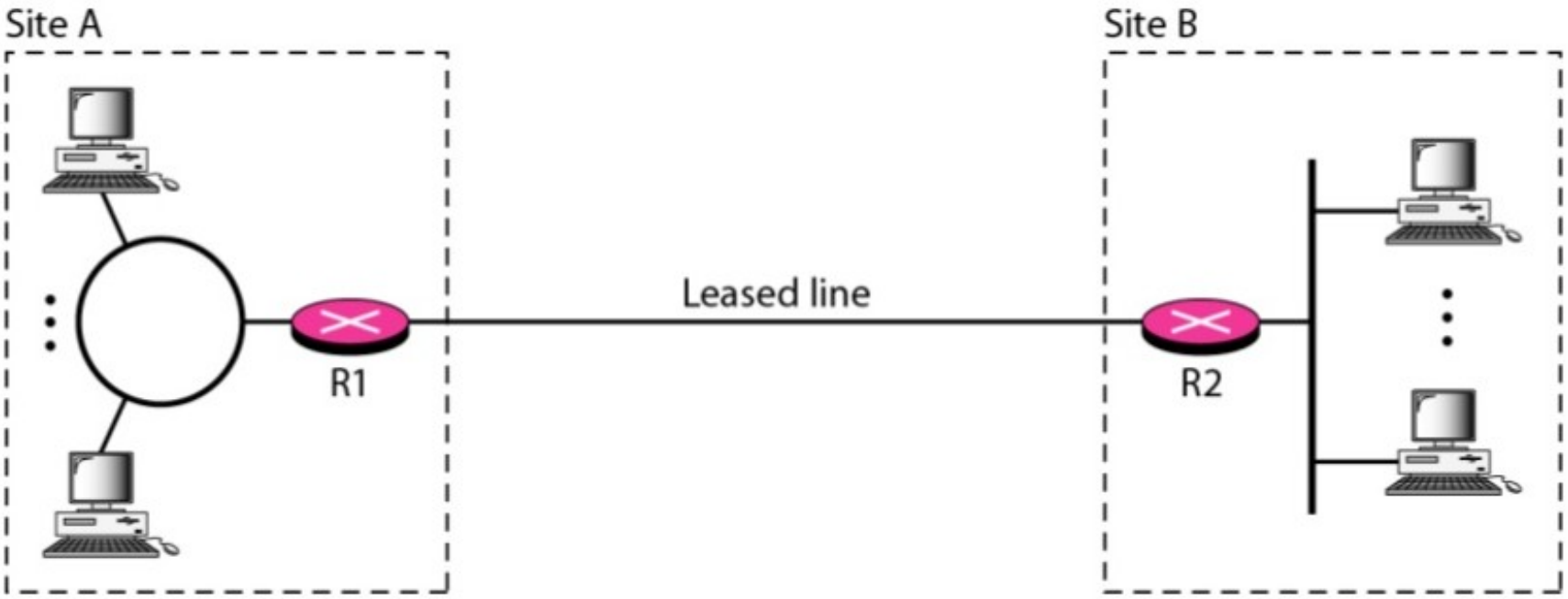
Any organization can use an address out of this set without permission from the Internet authorities, These reserved addresses are for private networks. No router will forward a packet that has one of these address as the destination address.

To achieve privacy, organizations can use one of three strategies :

- Private networks
- Hybrid networks
- Virtual private networks.

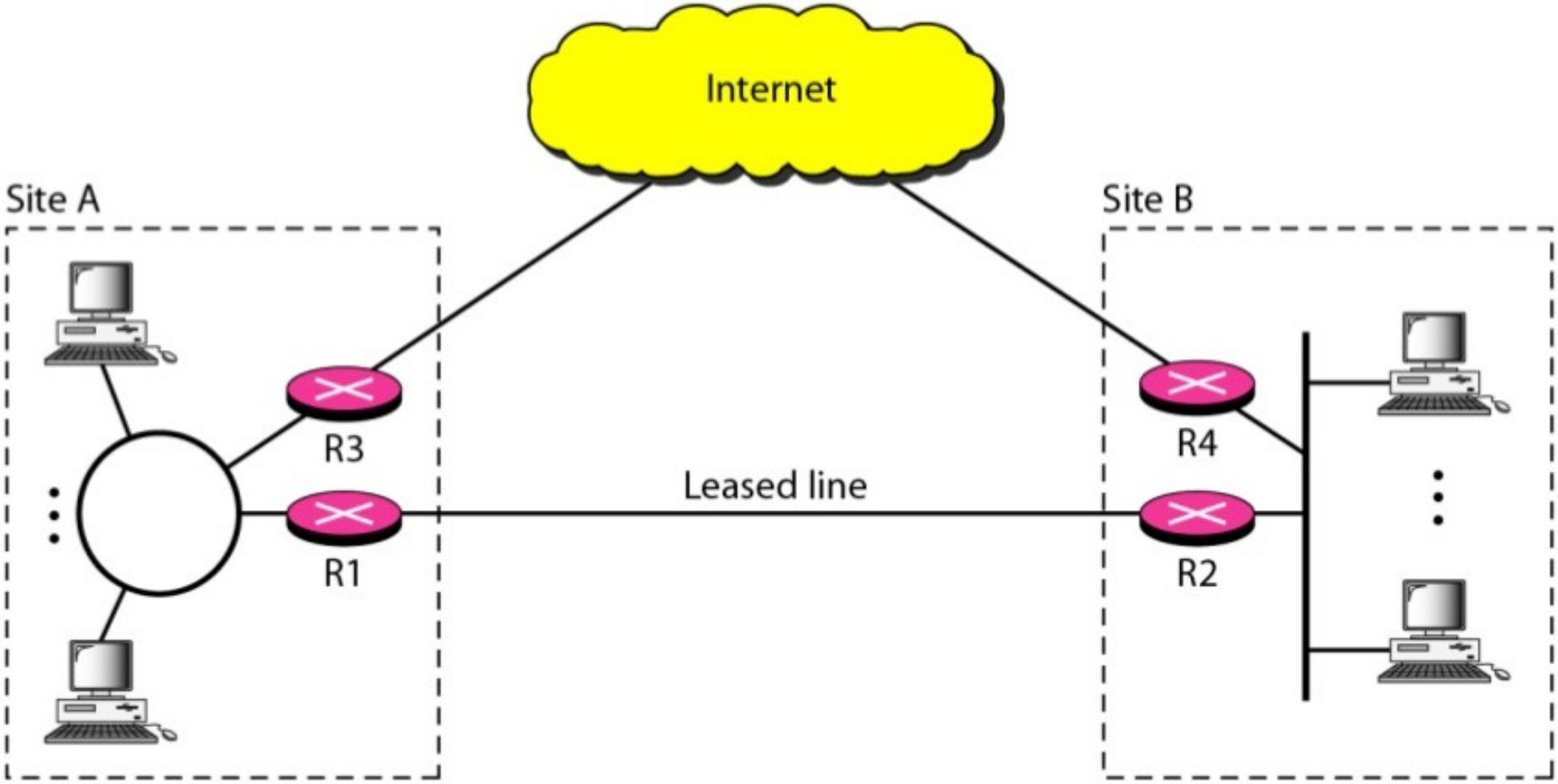
IPSecurity (IPSec)

Private Networks



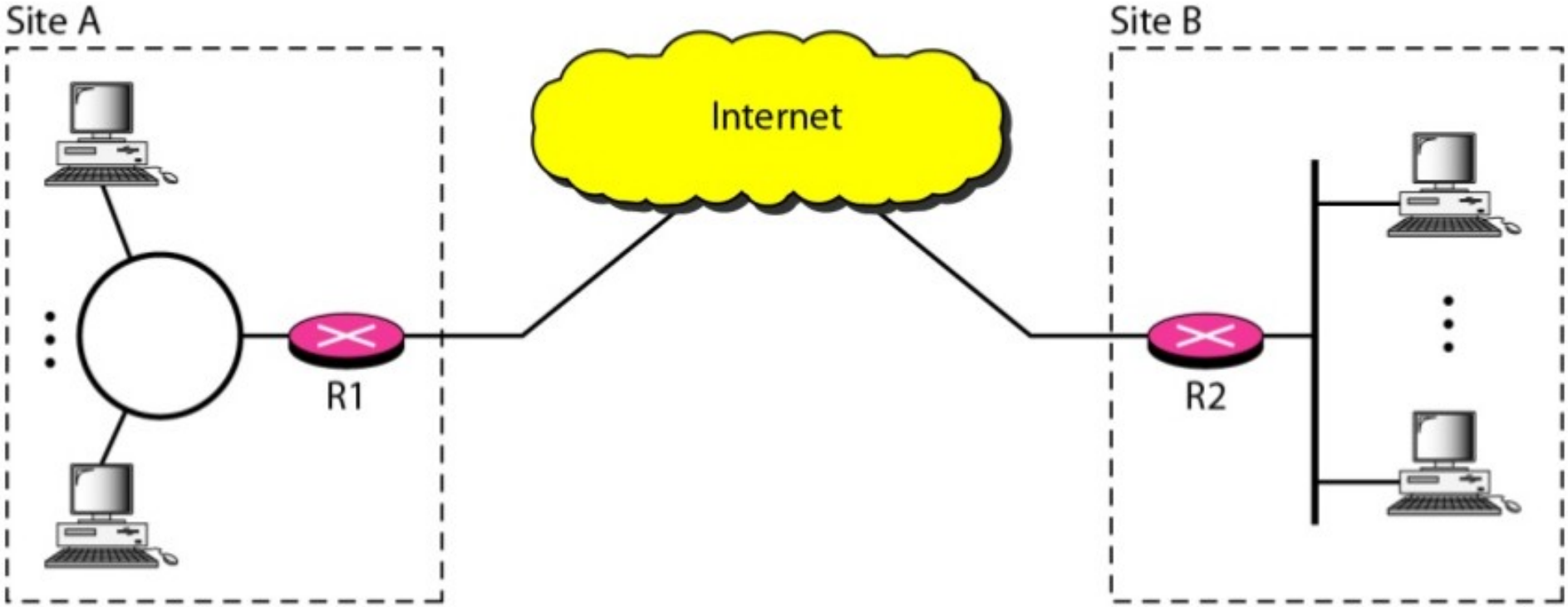
IPSecurity (IPSec)

Hybrid Networks



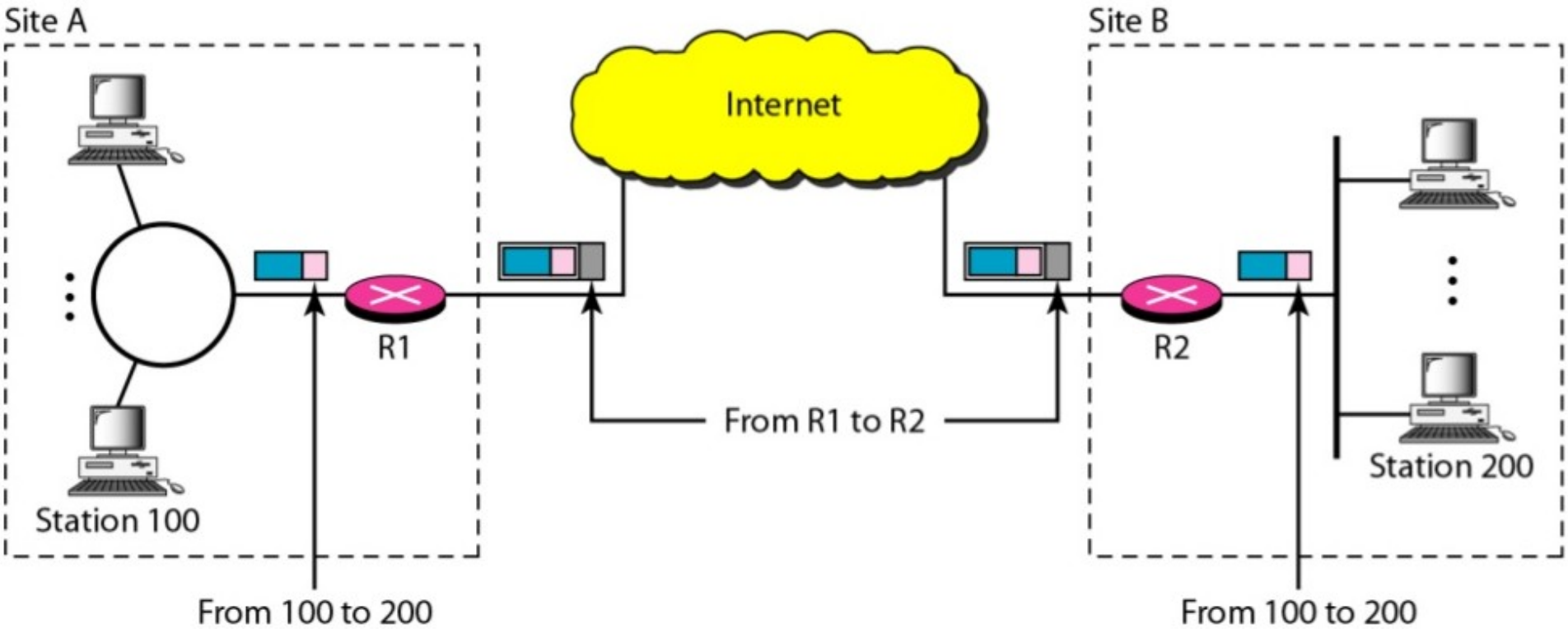
IPSecurity (IPSec)

Virtual Private Networks

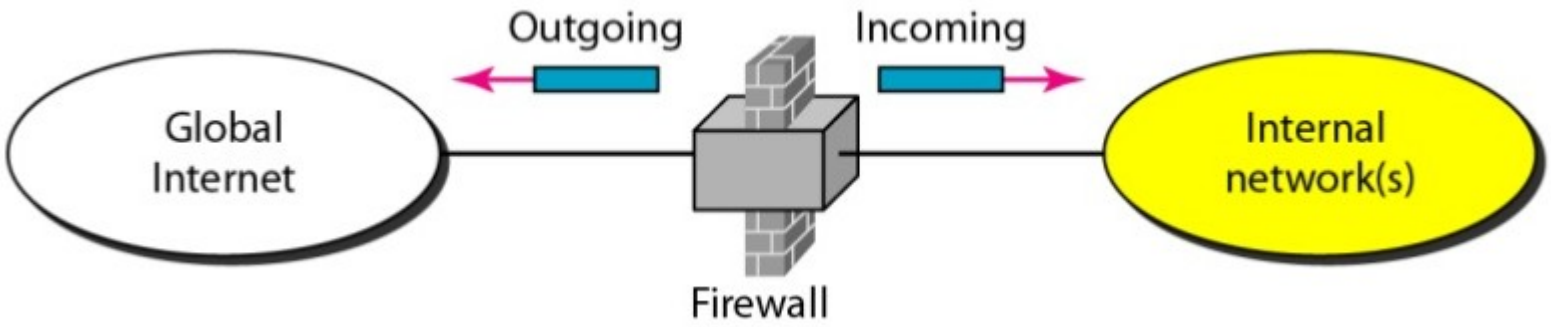


IPSecurity (IPSec)

Addressing in VPN

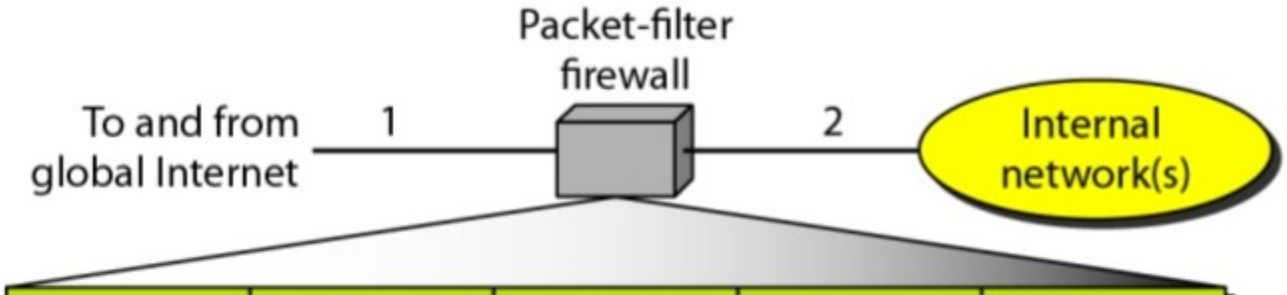


FIREWALL


Outgoing
Incoming
Global
Internet
Internal
network(s)
Firewall

FIREWALL

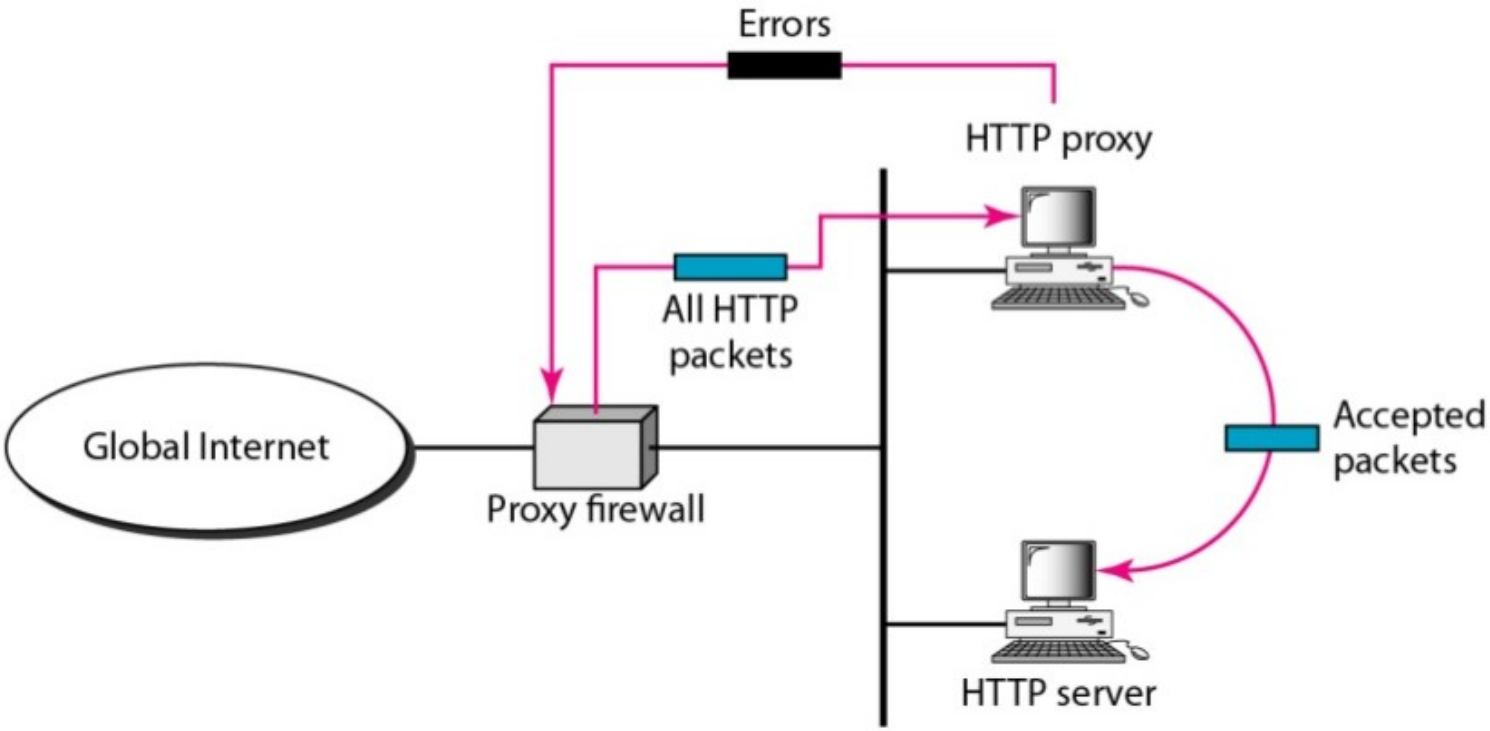
Packet-Filter Firewall

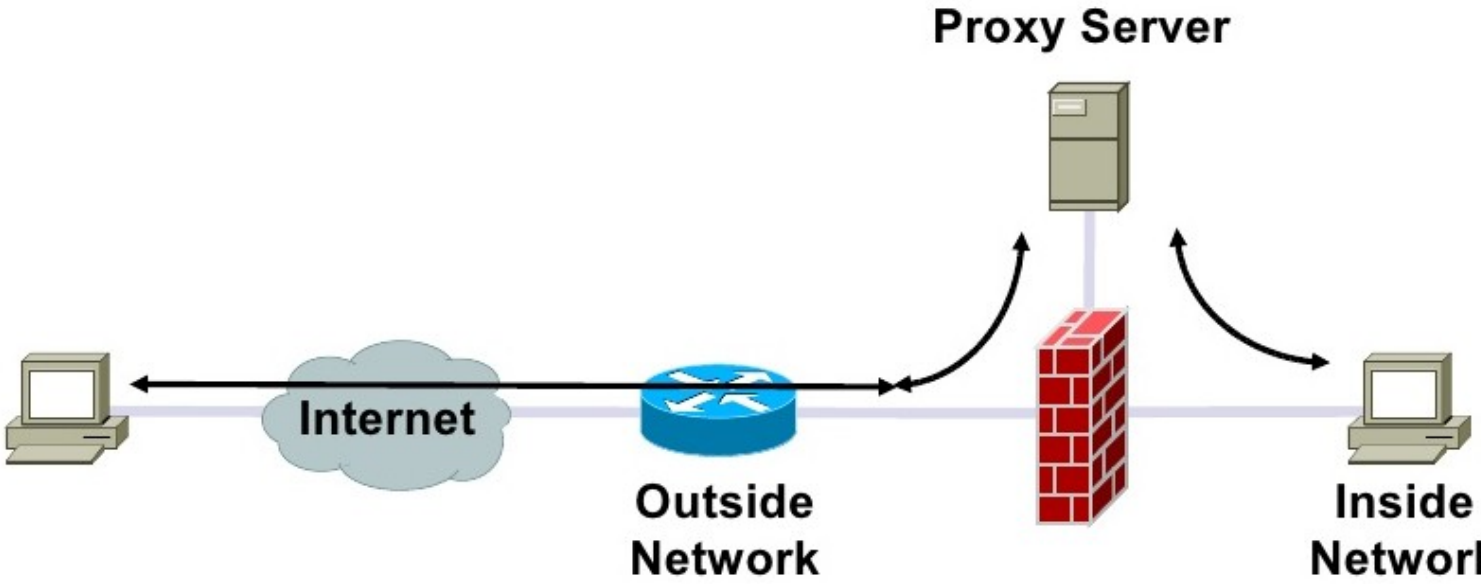


Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

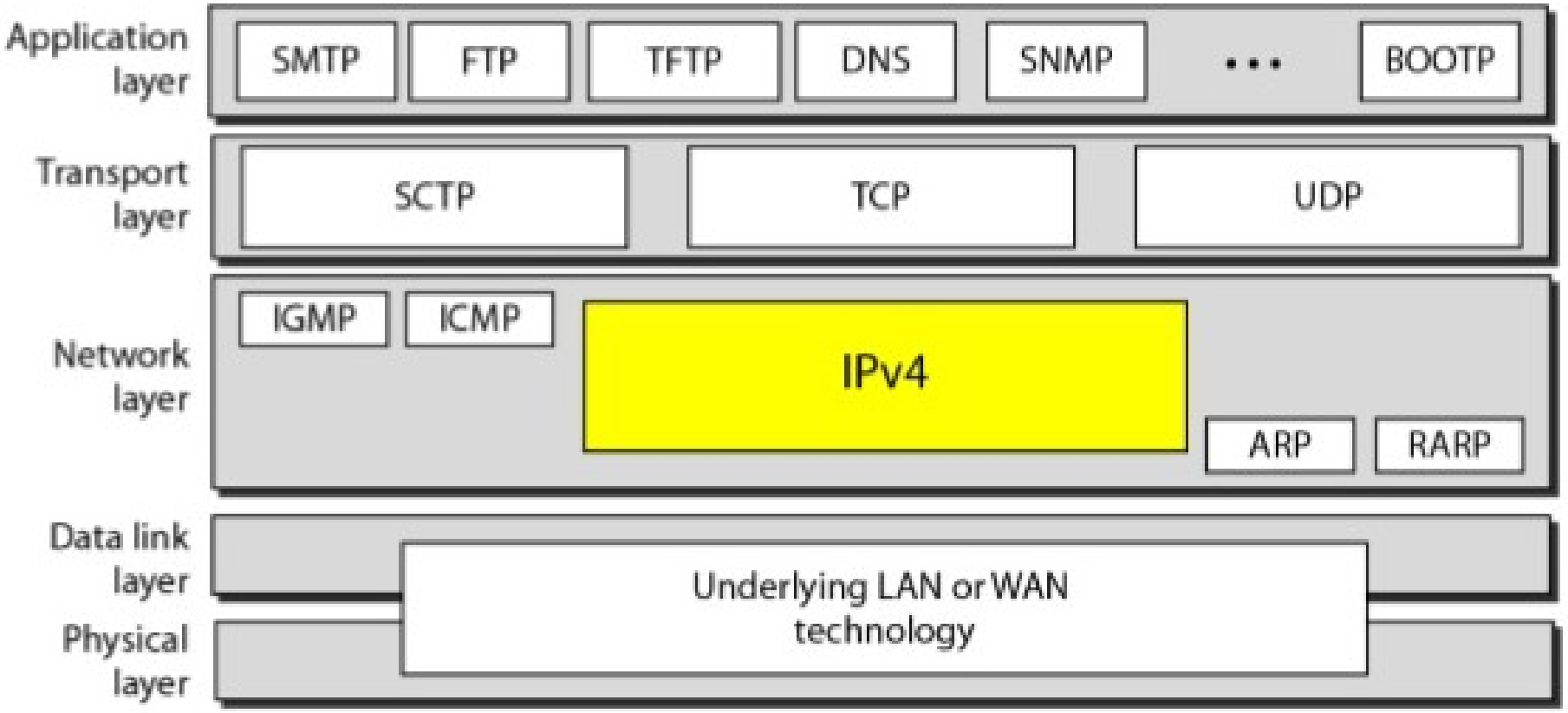
FIREWALL

Proxy Firewall





Protocols at different layers of TCP / IP protocol suite



What is port number ? Define ICANN Ranges.

➔The port number defines one of the processes on particular host.

➔ **ICANN (Internet Corporation for Assigned Names and Numbers)** has divided the port numbers into three ranges: well-known, registered and dynamic (or private).

➔**Well-know ports :** 0 to 1023 are assigned and controlled by ICANN.

➔**Registered ports :** 1024 to 49151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.

➔**Dynamic ports :** 49152 to 65535 are neither controlled nor registered. They can be used as temporary or private port numbers.

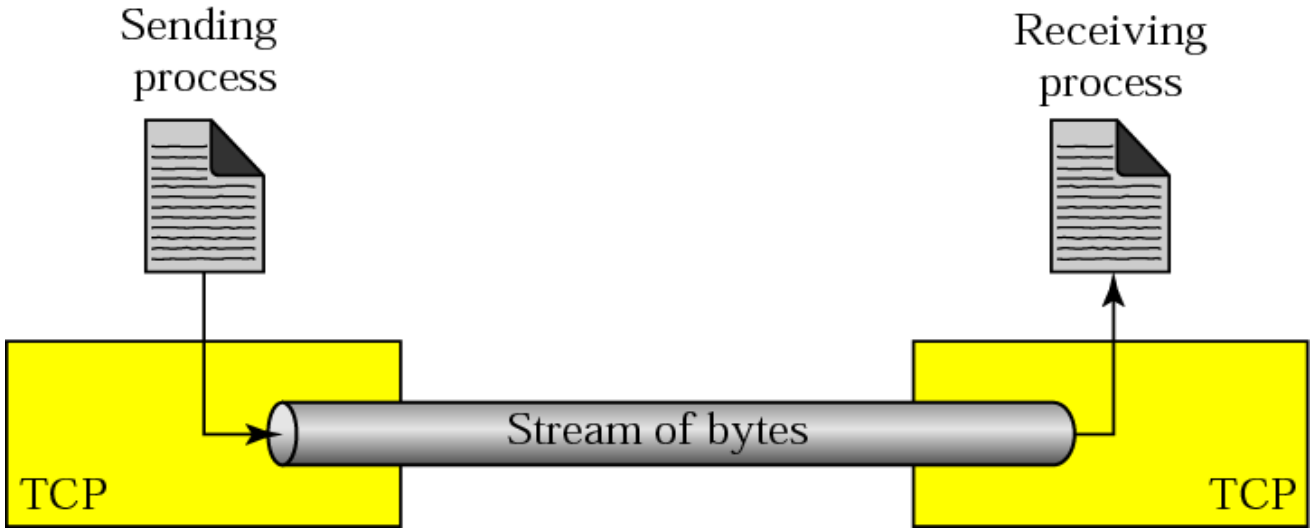
TCP

- It is called **Transmission Control Protocol** (TCP).
- It is a **process-to-process protocol** means provide port numbers.
- It is a **transport layer** protocol.
- TCP creates a virtual connection between two TCPs to send data. So TCP is called a ***connection-oriented*** protocol.
- TCP uses flow and error control mechanisms so it is called ***reliable*** protocol.

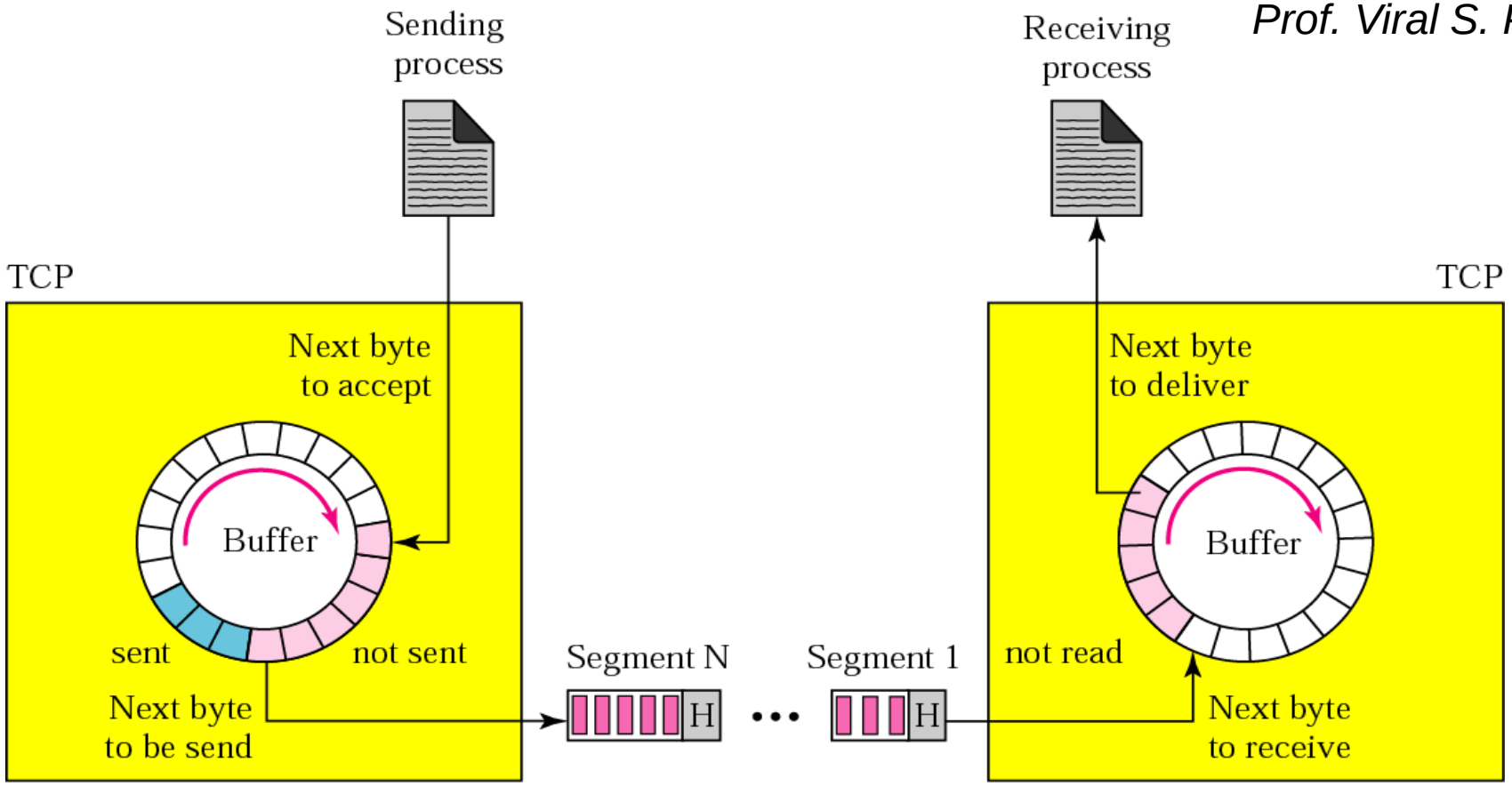
Unlike UDP, it is a **stream-oriented protocol**.

- TCP offers **full duplex service.**

Prof. Viral S. Patel



- Because the sending and the receiving processes may not write or read data at the same speed, TCP needs **buffers for storage**.

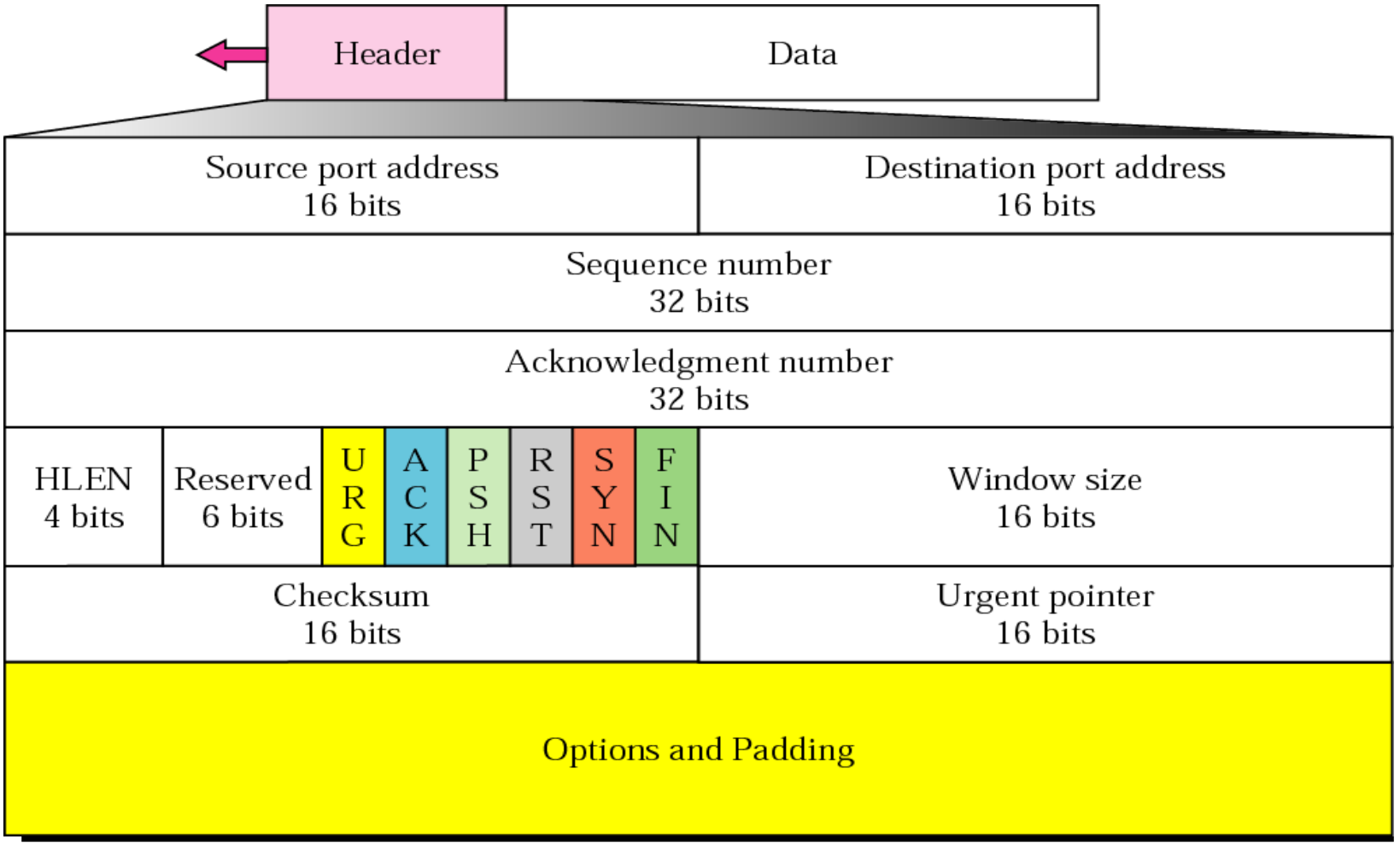


➔At the IP layer TCP needs to send data in packets, not as a stream of bytes. So TCP groups a number of bytes together into a packet called **segment.** The segments are encapsulated in IP datagrams and transmitted.

➔ TCP **numbers to all data bytes** that are transmitted in a connection. The numbering starts with a randomly generated number. For **example**, random number 1057 and total data are 6000 bytes, the bytes numbered from 1057 to 7056.

➔TCP rearranges **data packets in the order** specified by using **sequence number.**

TCP segment (segment = Header + data) format
Or
TCP Header format



➔ **Source port address :** This is a 16-bit field that defines the port number of the application program in the host that is sending the segment.

➔ **Destination port address :** This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.

➔ **Sequence number :** TCP assigns a sequence number in 32 bit field for each segment is the number of the first byte carried in that segment. For example,
Segment 1 ➡ Sequence Number: 10,001 (range of bytes: 10,001 to 11,000)
Segment 2 ➡ Sequence Number: 11,001 (range of bytes: 11,001 to 12,000)
Segment 3 ➡ Sequence Number: 12,001 (range of bytes: 12,001 to 13,000)…
Each party uses a random number generator to create an **initial sequence number (ISN)**.

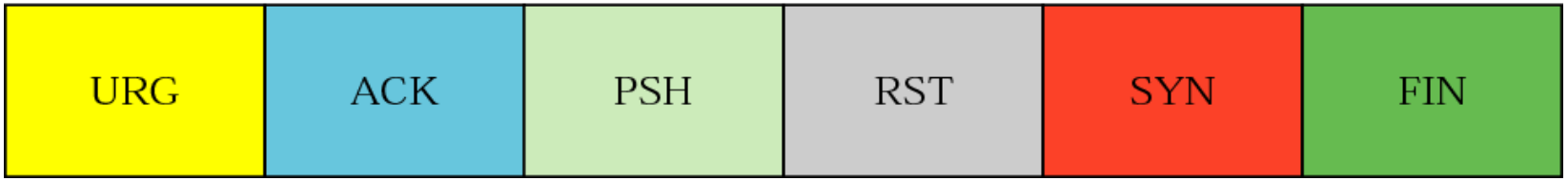
➔**Acknowledgment Number :** The value of the 32 bit acknowledgement field in a segment defines the number of the next byte a party expects to receive.

➔ **Header length :** This 4-bit field indicates the number of 4-byte words in the TCP header. The value of this field can be between 5 and 15. The length of the header can be between (5 x 4 =) 20 and (15 x 4 =) 60 bytes.

➔ **Reserved :** This is a 6-bit field reserved for future use.

➔ **Control :** This field defines 6 different control bits or flags as shown in fig.

URG: Urgent pointer is valid	RST: Reset the connection
ACK: Acknowledgment is valid	SYN: Synchronize sequence numbers
PSH: Request for push	FIN: Terminate the connection



➔ **Window size:** This field defines the size of the window, in bytes. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes.

Prof. Viral S. Patel

➔**Checksum :** This 16-bit field contains the checksum. In UDP it is optional but in TCP , it is mandatory. Pseudoheader is used in checksum calculation.

➔ **Urgent pointer :** This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

Prof. Viral S. Patel

➔ **Options :** There can be up to 40 bytes of optional information in the TCP header.

UDP

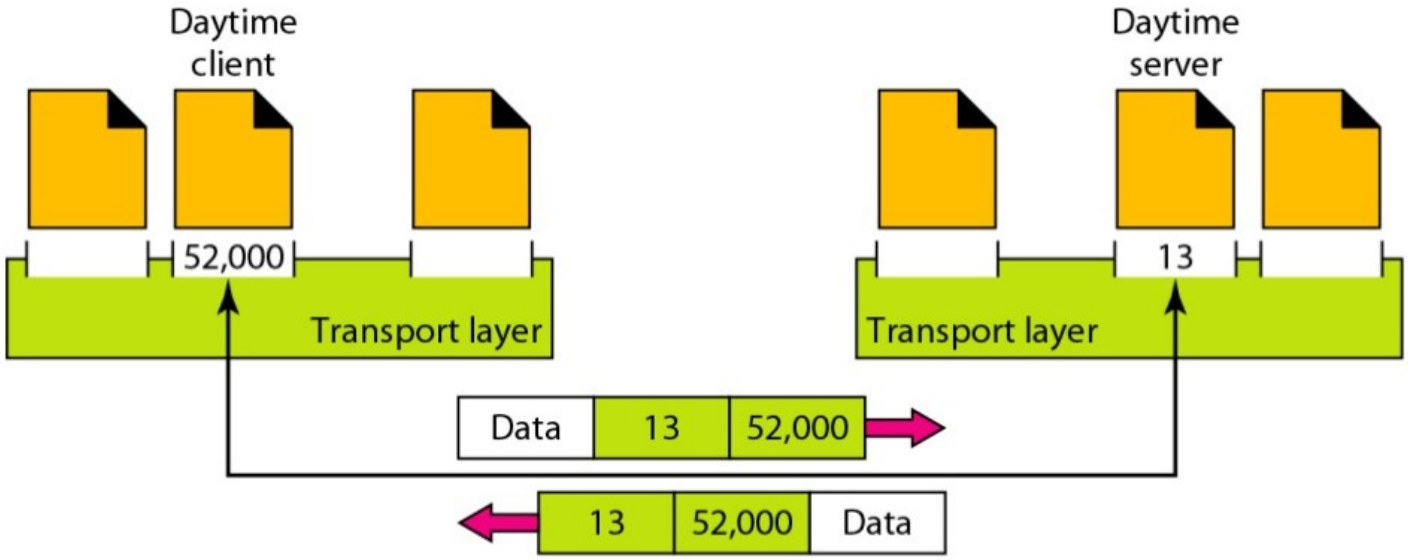
- It is called **User Datagram Protocol** (UDP).
- It is a **process-to-process protocol** means provide port numbers.
- It is a **transport layer** protocol.
- UDP is called a ***connectionless*** protocol.

➔UDP does not use flow and error control mechanisms so it is called ***unreliable*** protocol.

➔UDP does not support full duplex service.

Prof. Viral S. Patel

➔Example :

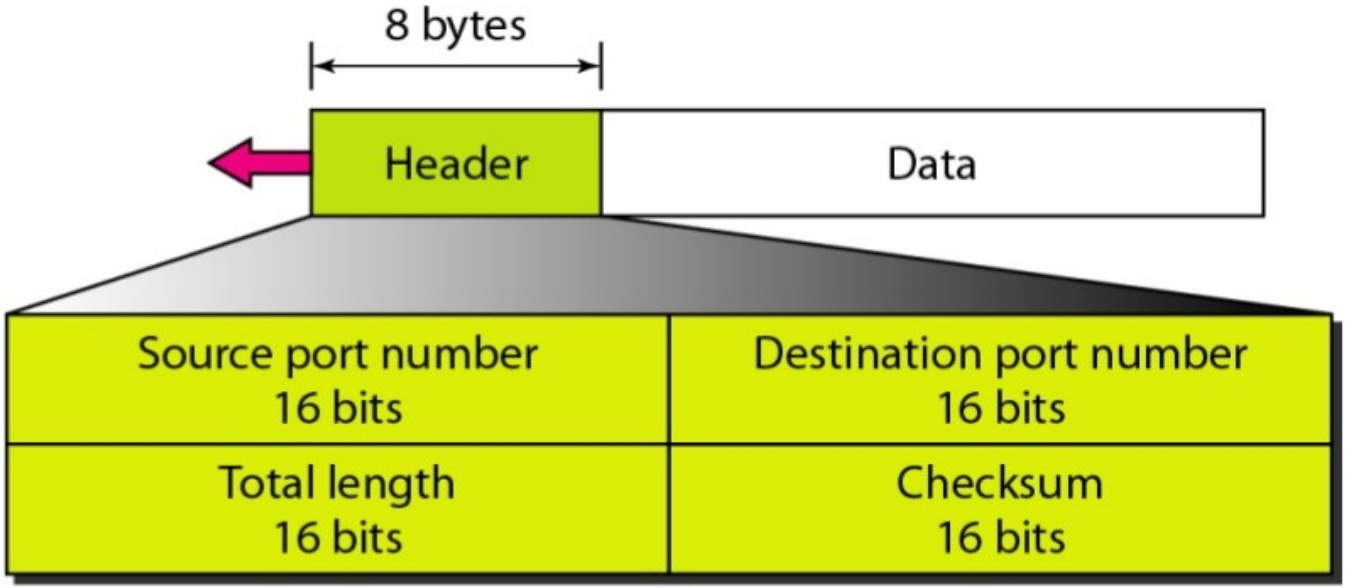


- TCP/IP has decided to use universal port numbers for servers called well-known port numbers and clients that are assigned temporary port numbers. Here fig. show that client process use ephemeral (temporary) port number 52000 to identify itself and Daytime server process must use the well-known (permanent) port number 13.

- ➔UDP is suitable for a process that requires simple request-response communication where flow and error control is not important. It is not usually used for a process such as FTP that needs to send bulk data.
- ➔UDP is suitable for a process which have internal flow and error-control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control.
- ➔UDP is a suitable transport protocol for multicasting.
- ➔UDP is used for management processes such as SNMP.
- ➔UDP is used for some route updating protocols such as Routing Information Protocol (RIP).

Prof. Viral S. Patel

UDP datagram (Header + data) format



➔**Source port number :** This is the port number used by the process running on the source host. It is 16 bits long. If source host is client, the port number is ephemeral (temporary) port number chosen by UDP software running on the source host. If the source host is server, the port number is well-known port number.

➔**Destination port number :** This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server the port number is a well-know port number. If the destination host is the client the port number is a ephemeral (temporary) port number. In this case, server copies the ephemeral port number it has received in the request packet.

Prof. Viral S. Patel

➔**Length :** This is a 16 bits field that defines the total length of the user datagram, header plus data. This 16 bits define a total length of 0 to 65535 bytes. This field is actually not necessary. Because this datagram is encapsulated in IP datagram. IP datagram have two fields IP length and IP header's length. So we can calculate

UDP length = IP length – IP header's length

🖧**Checksum :** This field is used to detect errors over the entire user datagram. For this checksum value the **pseudoheader** (IP header) is used to calculation.

Thank You…

by Prof. Viral S. Patel