Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

Network Fundamentals

People matter, results count.

Networks - What is a network ?

- A *network* is simply two or more computers that are linked together.
- A network is a system that transmits any combination of voice, video and/or data between users.
- A network can be defined by its geographical dimension and by the method by which the user's PC accesses it.
- A network consists of
  - The network operating system (Windows NT/2000™) on the user's PC (client) and server;
  - The cables connecting all network devices (user's PC, server, peripherals, etc.);
  - All supporting network components (hubs, routers and switches, etc.).

Examples of Today's Popular Communication

How Networks Impact Daily Life

- Decide what to wear using online current weather conditions
- Find the least-congested route to your destination, displaying weather and traffic video from webcams
- Check your bank balance and pay bills electronically
- Receive and send e-mail at an Internet cafe over lunch
- Obtain health information and nutritional advice from experts all over the world, and post to a forum to share related health or treatment information
- Download new recipes and cooking techniques to create a spectacular dinner
- Post and share your photographs, home videos, and experiences with friends or with the world
- Use Internet phone services
- Shop and sell at online auctions
- Use instant messaging and chat for both business and personal use

How Networks Impact Daily Life Cntd..

- The characteristics and purpose of popular communication media such as, IM, Wikis , Blogs, Podcasting, and Collaboration Tools
  - Instant messaging
    - Real time communication
    - between 2 or more
    - people based on typed text
  - Web logs (Blogs)
    - Web pages created
    - by an individual
  - Podcasting
    - Website that contains
    - audio files available
    - for downloading

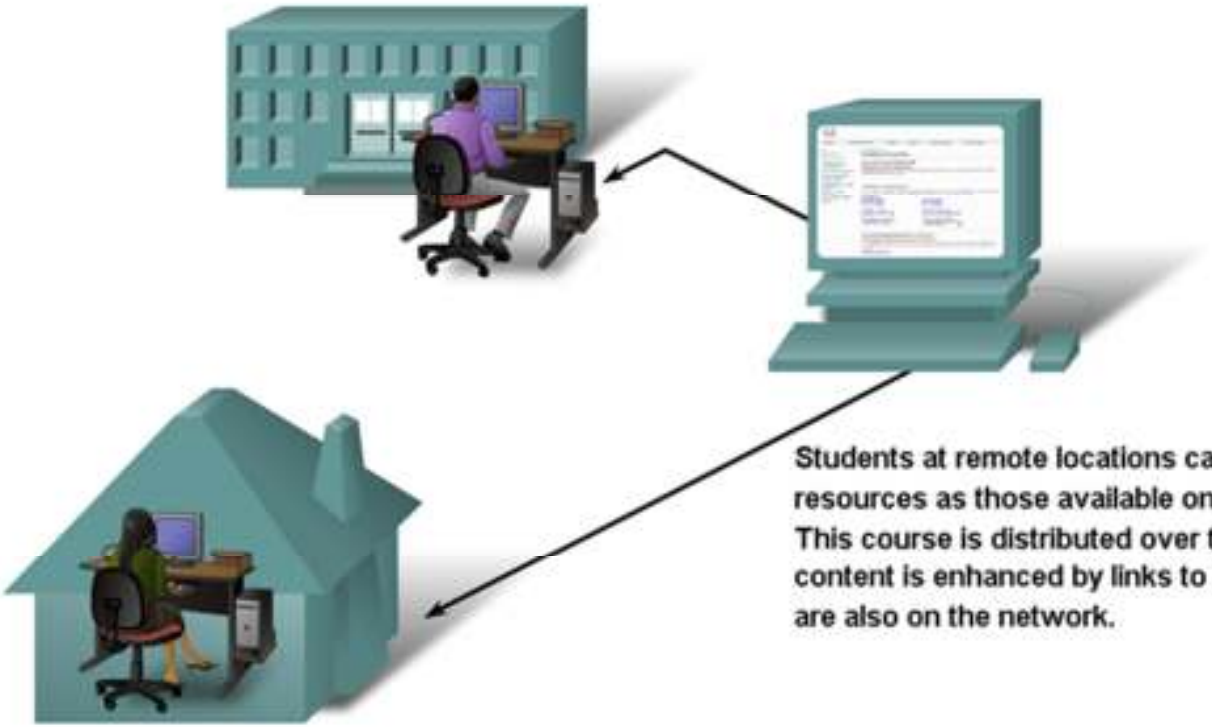
Instant Messaging

Weblog

Podcasting

How Networks Impact Daily Life Cntd..

Networks Supporting the Way We Learn



Students at remote locations can access the same resources as those available on campus.
This course is distributed over the network and the content is enhanced by links to other resources, which are also on the network.

How Networks Impact Daily Life Cntd..

- Networks Supporting the Way We Work

- Business Applications can be accessed remotely as if employees were on site
- Workers in any location can reach each other and access multiple resources on the network

How Networks Impact Daily Life Cntd..

- Networks Supporting the Way We Play

Online Interest Groups

Online Entertainment

The onboard data network provides a range of services to airline personal seatback video systems.

Instant Messaging

Communication

- Basic characteristics of communication
  - Rules or agreements are 1st established
  - Important information may need to be repeated
  - Various modes of communication may impact the effectiveness of getting the message across.

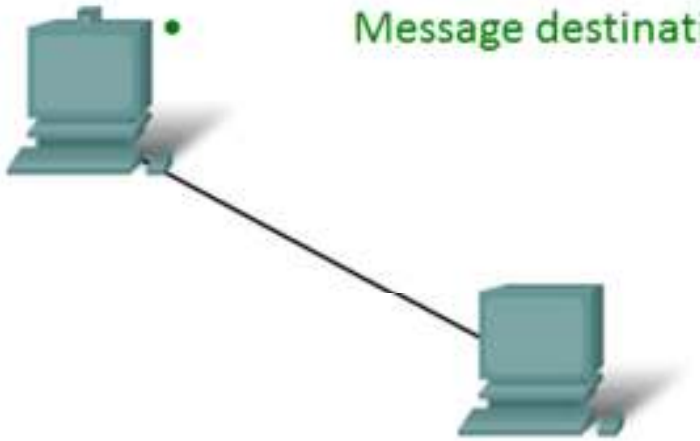
- An identifier sender and receiver
- Agreed Upon method of communicating (face-to-face, telephone, letter, photograph)
- Common language and grammar
- Speed and timing of delivery
- Confirmation or acknowledgement requirements

Elements of Communication

The Elements of communication

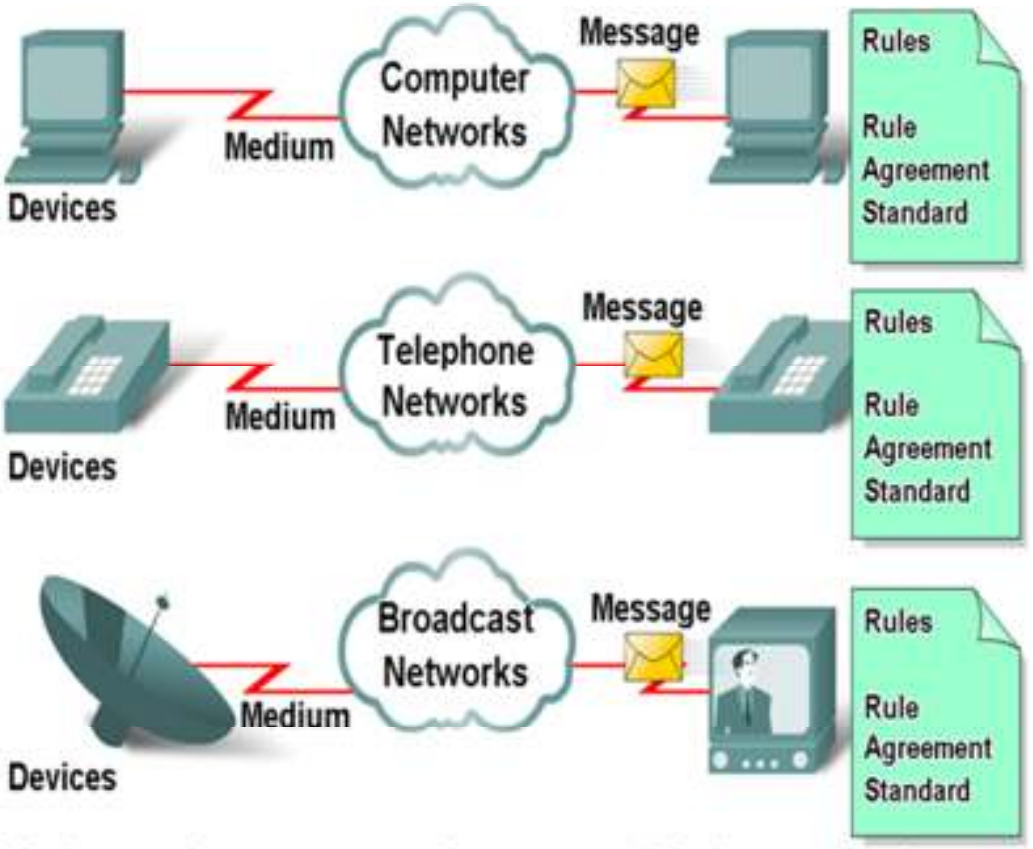
3 common elements of communication

- Message source
- The channel
- Message destination



Elements of Communication Cntd..

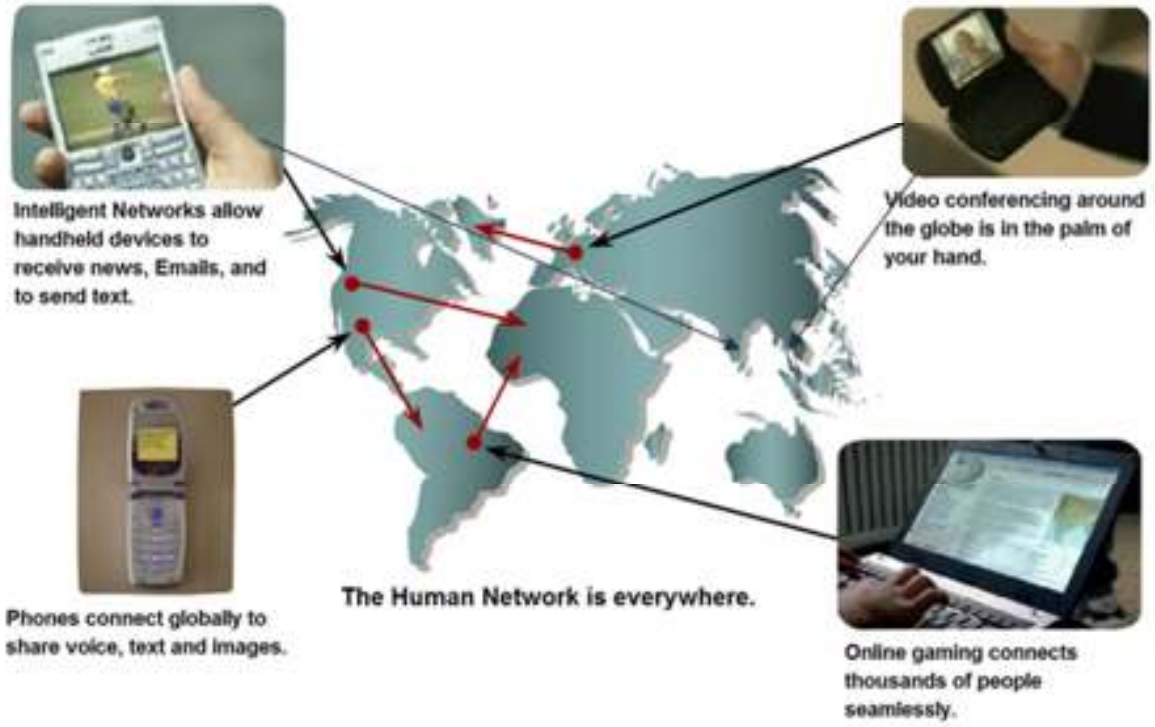
- The various elements that make up a network
  - Devices
    - These are used to communicate with one another
  - Medium
    - This is how the devices are connected together
  - Messages
    - Information that travels over the medium
  - Rules
    - Governs how messages flow across network



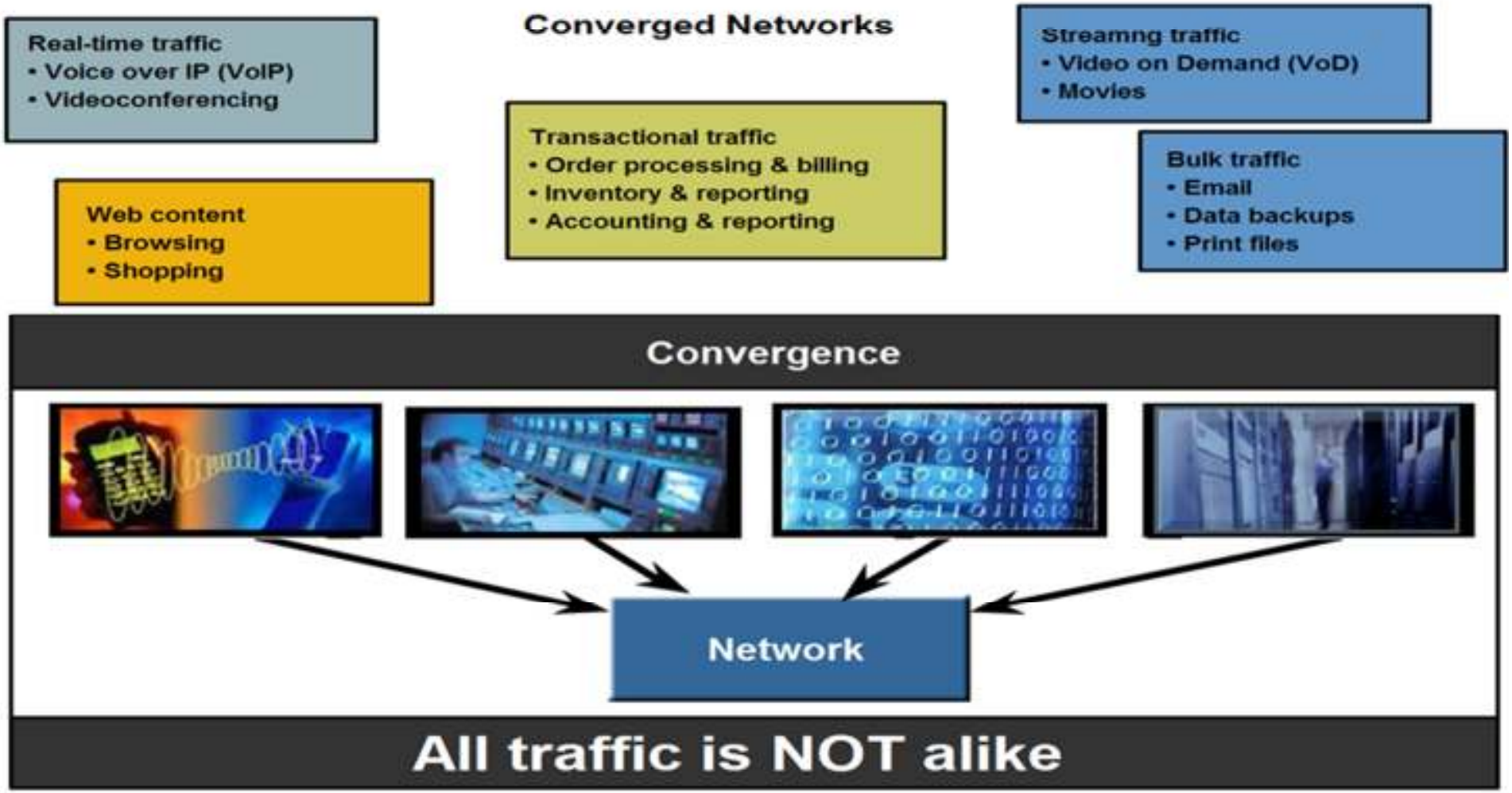
Multiple services are running on multiple networks

Converged Network

- The role of converged networks in communications
  - Converged network
    - A type of network that can carry voice, video & data over the same network



Converged Network Cntd..



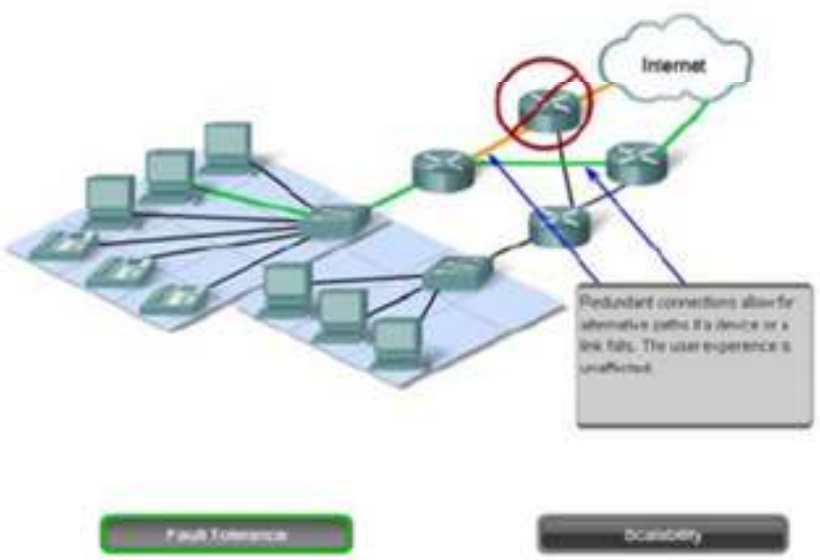
Network Architecture Characteristics

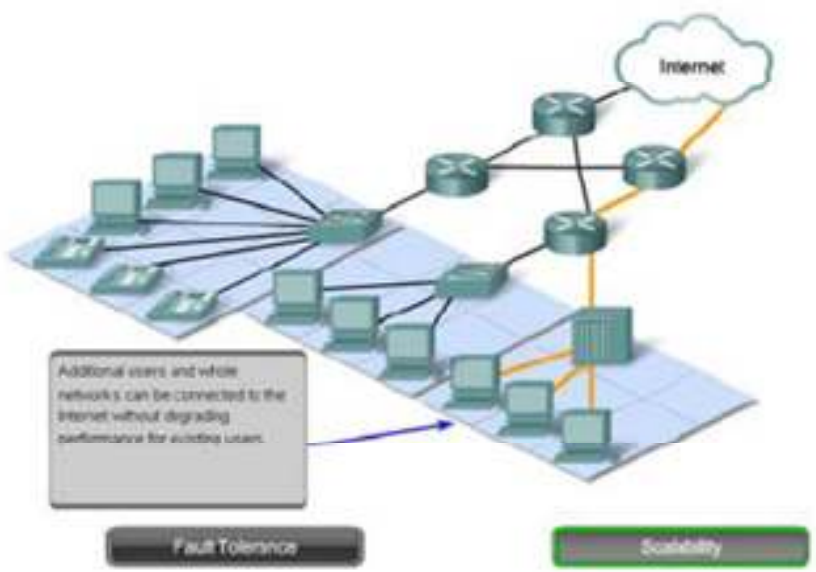
- The four characteristics that are addressed by network architecture design
  - Fault tolerance
  - Scalability
  - Quality of service
  - Security

Network Architecture Characteristics Cntd...

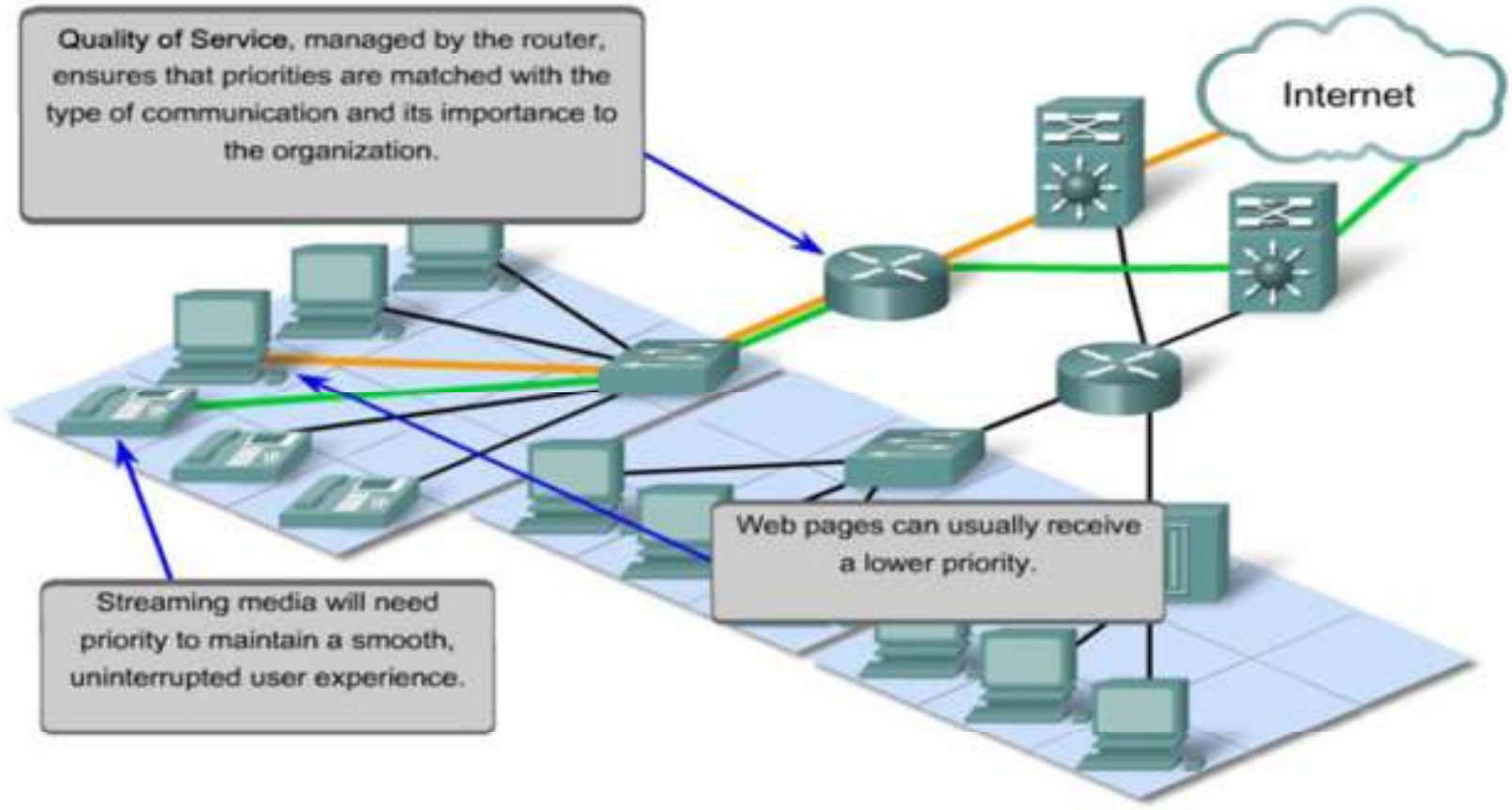
- Fault tolerance :A fault Tolerant network is one that limits the impact of a hardware or software and can recover quickly when such a failure occurs

- A scalable network can expand quickly to support new users and applications without impacting the performance of the service being delivered to existing users.





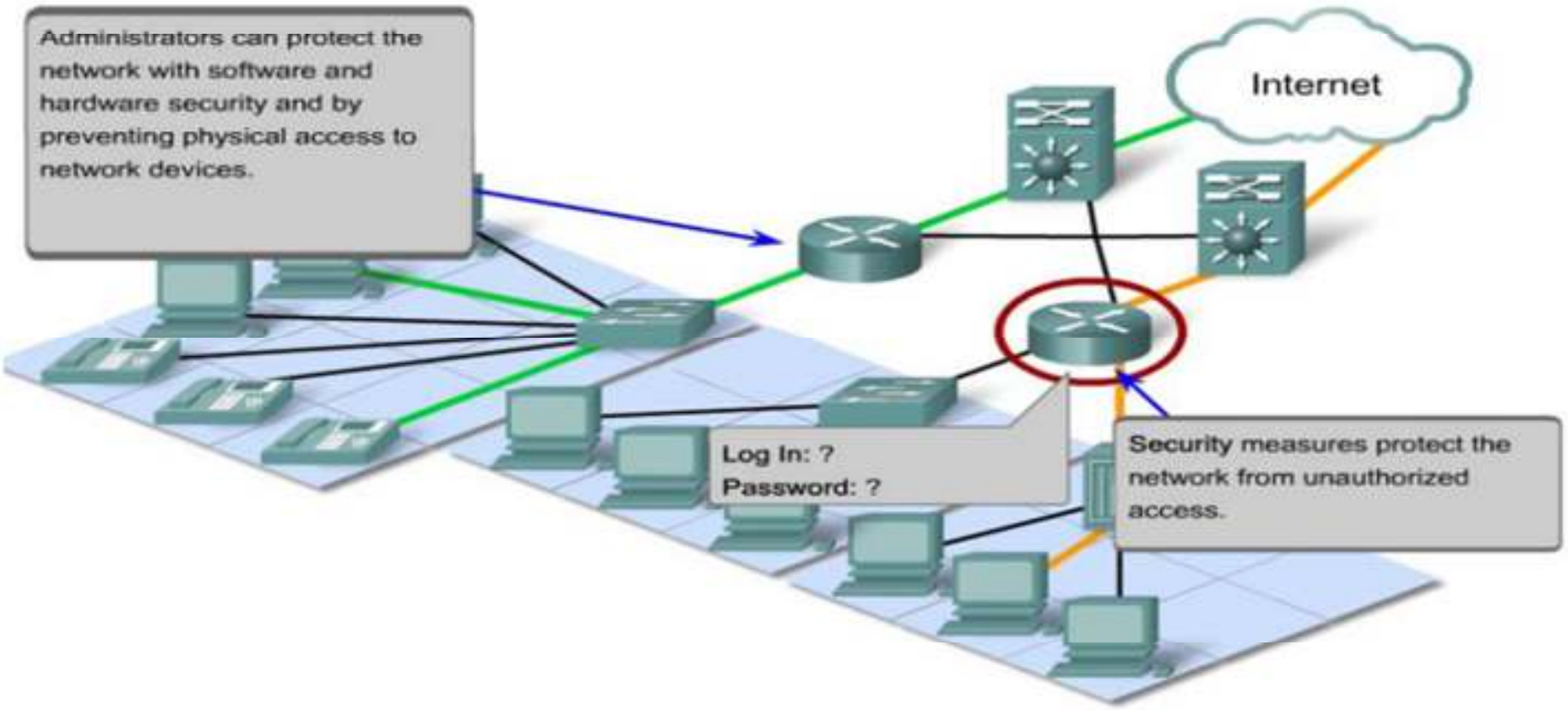
Network Architecture Characteristics Cntd...



Quality of Service

Security

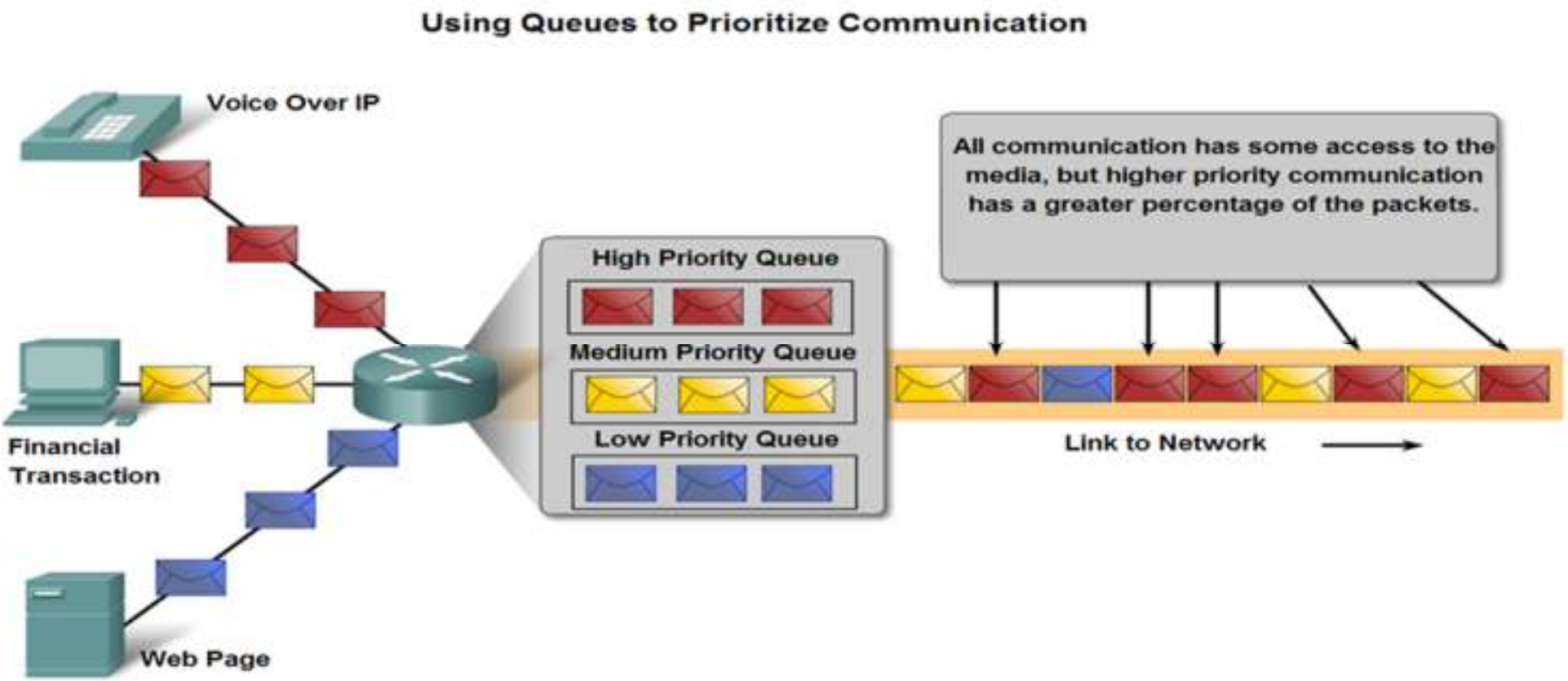
Network Architecture Characteristics Cntd...



Quality of Service

Security

Network Architecture Characteristics Cntd...



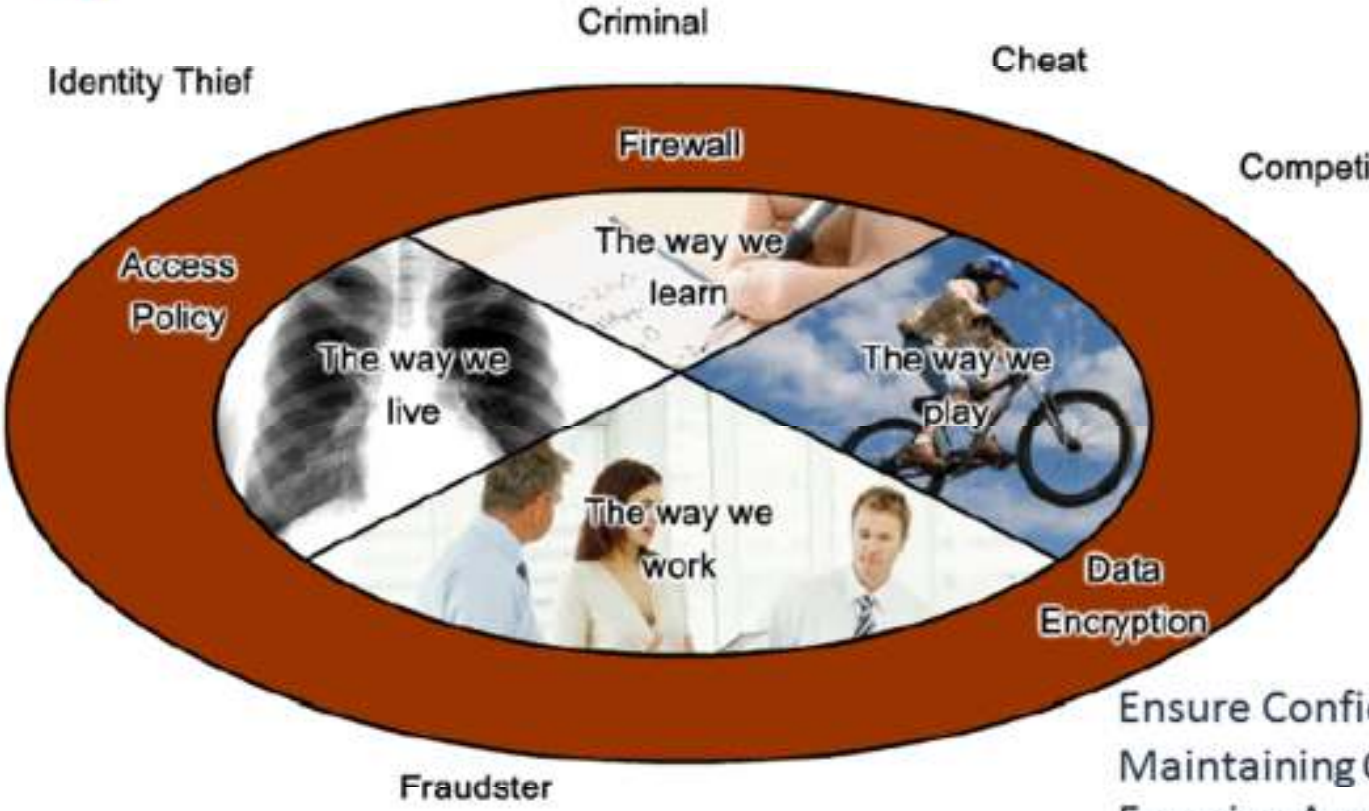
Different types of communications flowing across our data networks need to be prioritized so that the time-sensitive and important data have the first use of limited network resources

Network Architecture Characteristics Cntd...

Quality of Service Matters

Communication Type	Without QoS	With QoS
Streaming video or audio	 Choppy picture starts and stops.	 Clear, continuous service.
Vital Transactions	Time : Price 02:14:05 $1.54 Just one second earlier...	Time : Price 02:14:04 $1.52 The price may be better.
Downloading web pages (often lower priority)	 Web pages arrive a bit later...	 But the end result is identical.

Network Architecture Characteristics Cntd...



Ensure Confidentiality
Maintaining Communication Integrity
Ensuring Availability

Integrating security into data networks is essential if our private, personal, and business communications are not going to be intercepted , stolen or damaged.

Advantages of a Network

- **Information sharing:** Authorized users can use other computers on the network to access and share information and data. This could include special group projects, databases, etc.
- **Hardware sharing:** One device connected to a network, such as a printer or scanner, can be shared by many users.
- **Software sharing:** Instead of purchasing and installing a software program on each computer, it can be installed on the server. All of the users can then access the program from a single location.
- **Collaborative environment:** Users can work together on group projects by combining the power and capabilities of diverse equipment.

Disadvantages of a Network

- The security of a computer network is challenged everyday by:
  - Equipment malfunctions
  - System failures
    - Note: equipment malfunctions and system failures may be caused by natural disasters such as floods, storms, or fires, and electrical disturbances
  - Computer hackers
  - Virus attacks

Fundamental Network Characteristics

Protocol

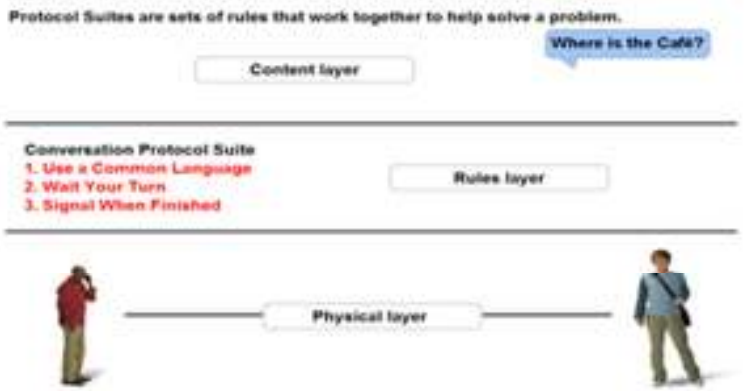
- A protocol is a standard used to define a method of exchanging data over a computer network such as local area network, Internet, Intranet, etc. Each protocol has its own method of how data is formatted when sent and what to do with it once received, how that data is compressed or how to check for errors in data.

- One of the most common and known protocols is HTTP(Hyper Text Transfer Protocol), which is a protocol used to transmit data over the world wide web (Internet).

Function of Protocol

The importance of protocols and how they are used to facilitate communication over data networks

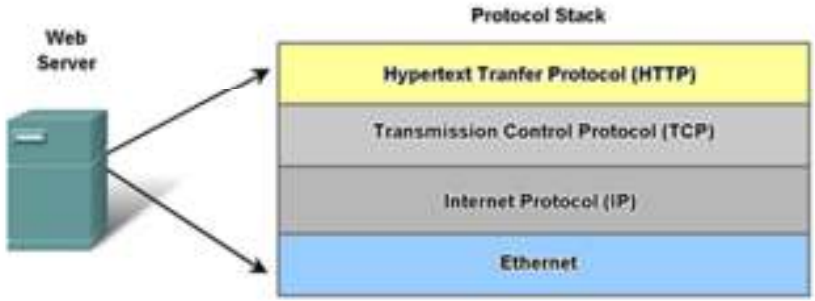
- A protocol is a set of predetermined rules



Network protocols are used to allow devices to communicate successfully

Technology independent Protocols

-Many diverse types of devices can communicate using the same sets of protocols. This is because protocols specify network functionality, not the underlying technology to support this functionality.



Protocols provide:

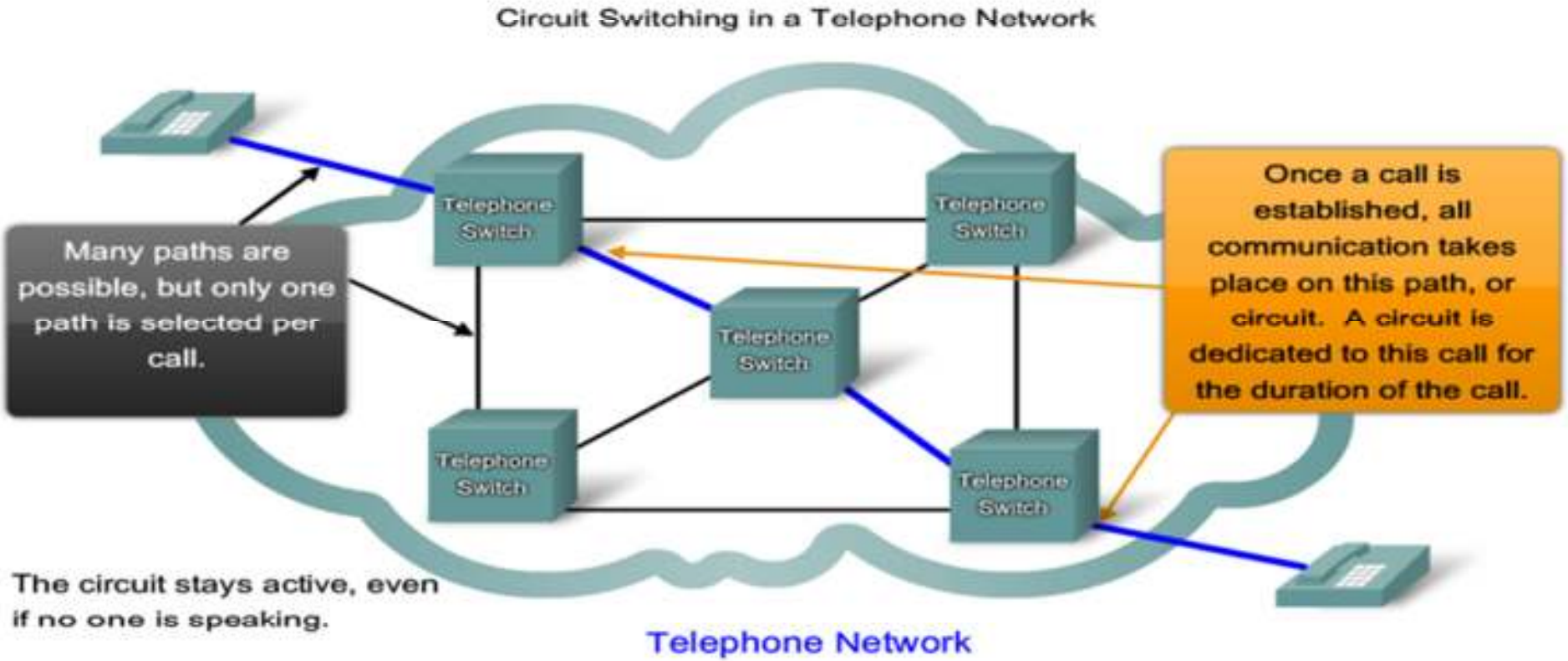
The format or structure of the message

The process by which networking devices share information about pathways to other networks

How and when error and system messages are passed between devices

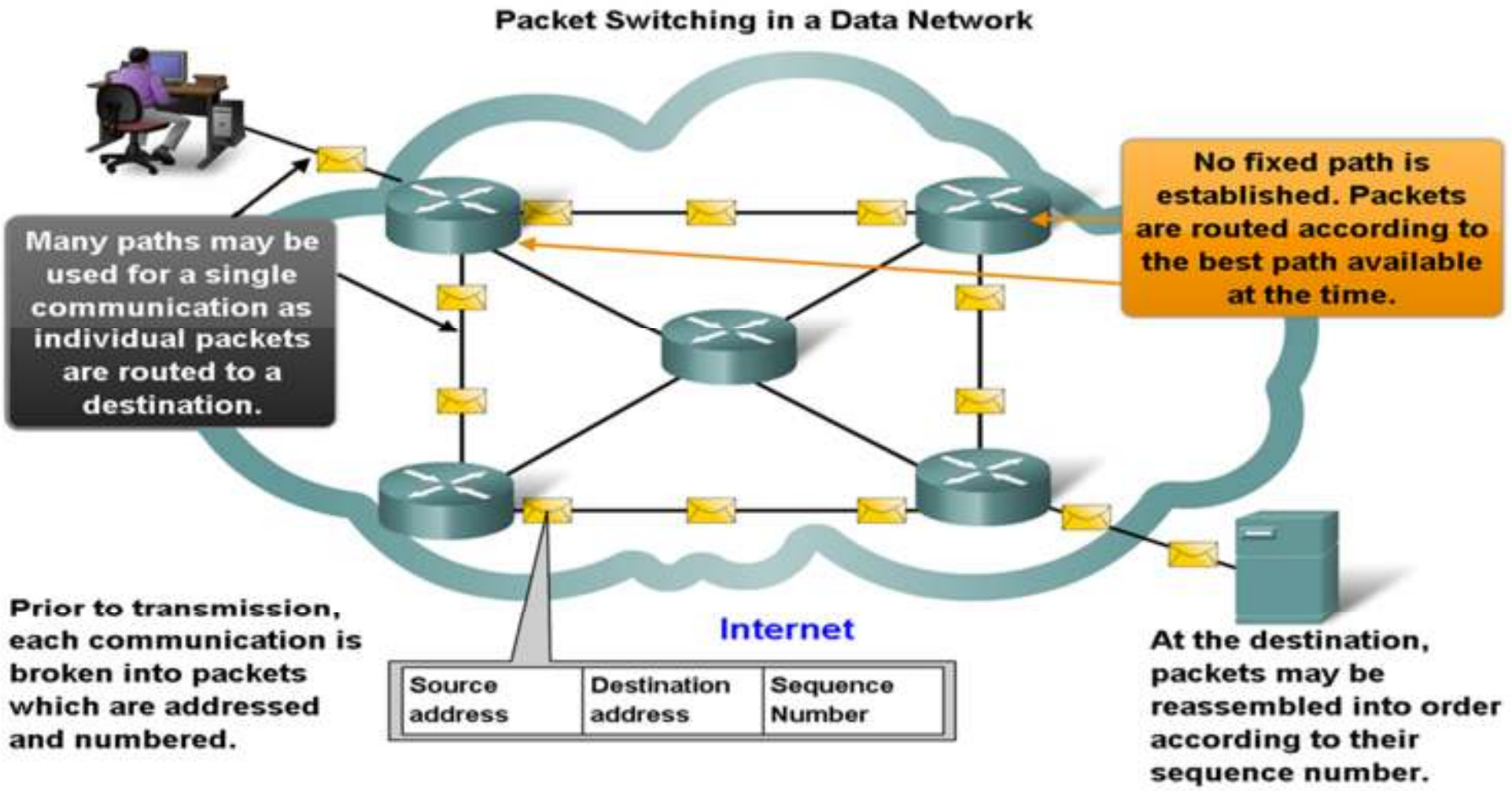
The setting up and termination of data transfer sessions

Circuit Switching



There are many, many circuits, but a finite number. During peak periods, some calls may be denied.

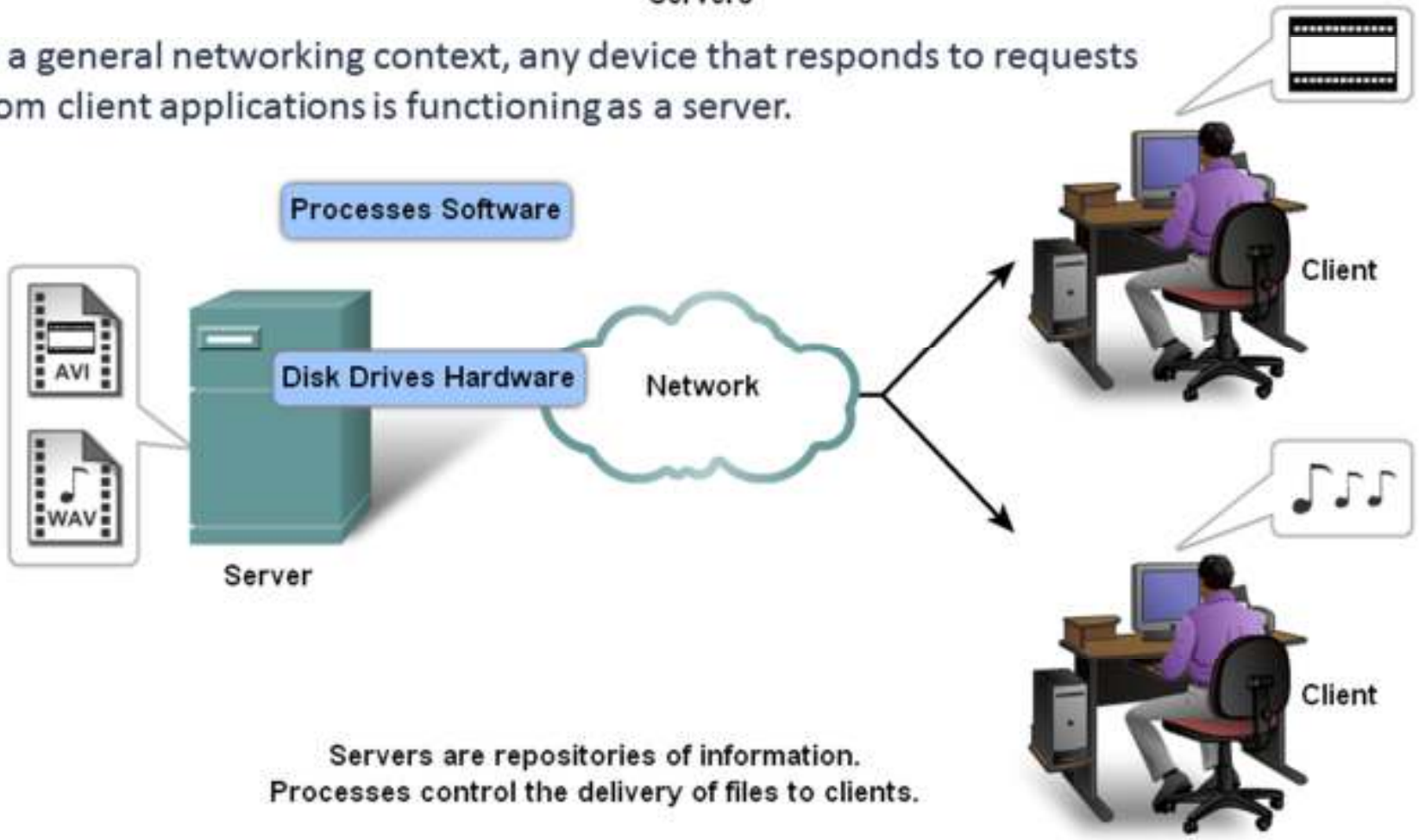
Packet Switching



Servers

Servers

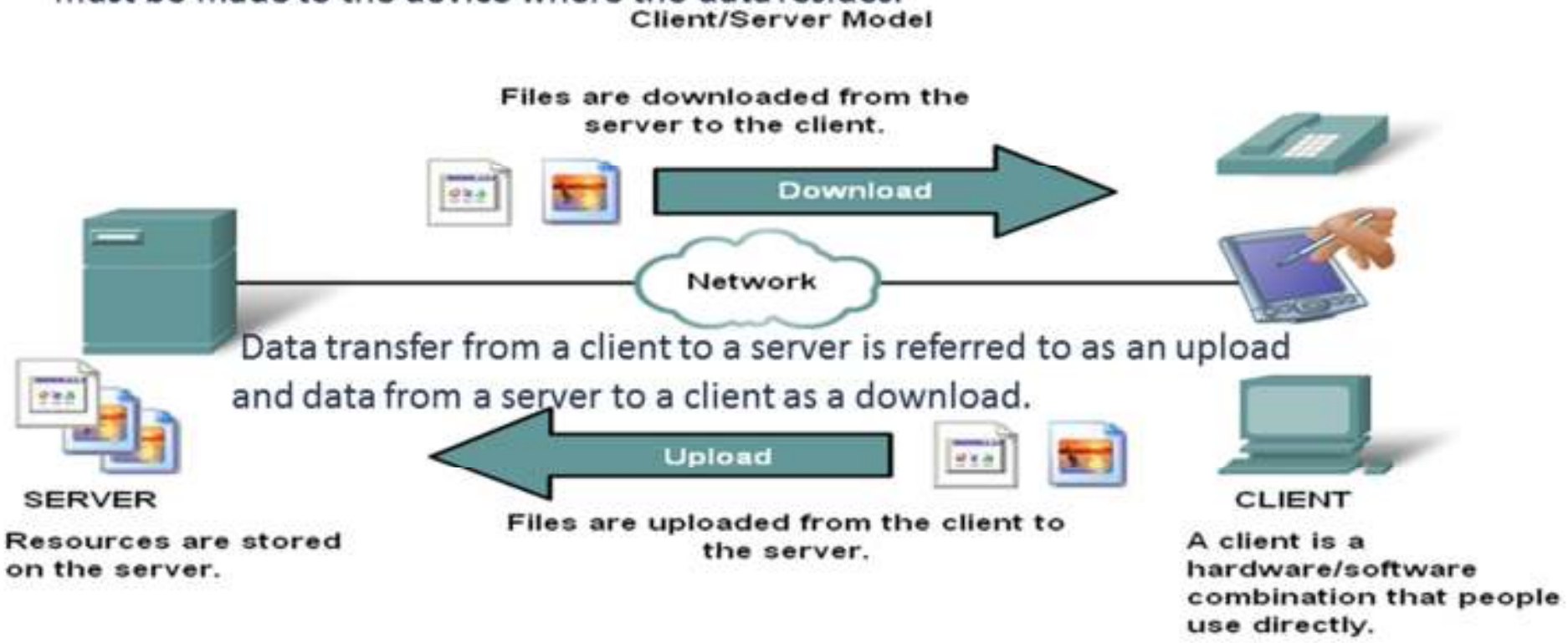
In a general networking context, any device that responds to requests from client applications is functioning as a server.



Servers are repositories of information.
Processes control the delivery of files to clients.

The Client-Server Model

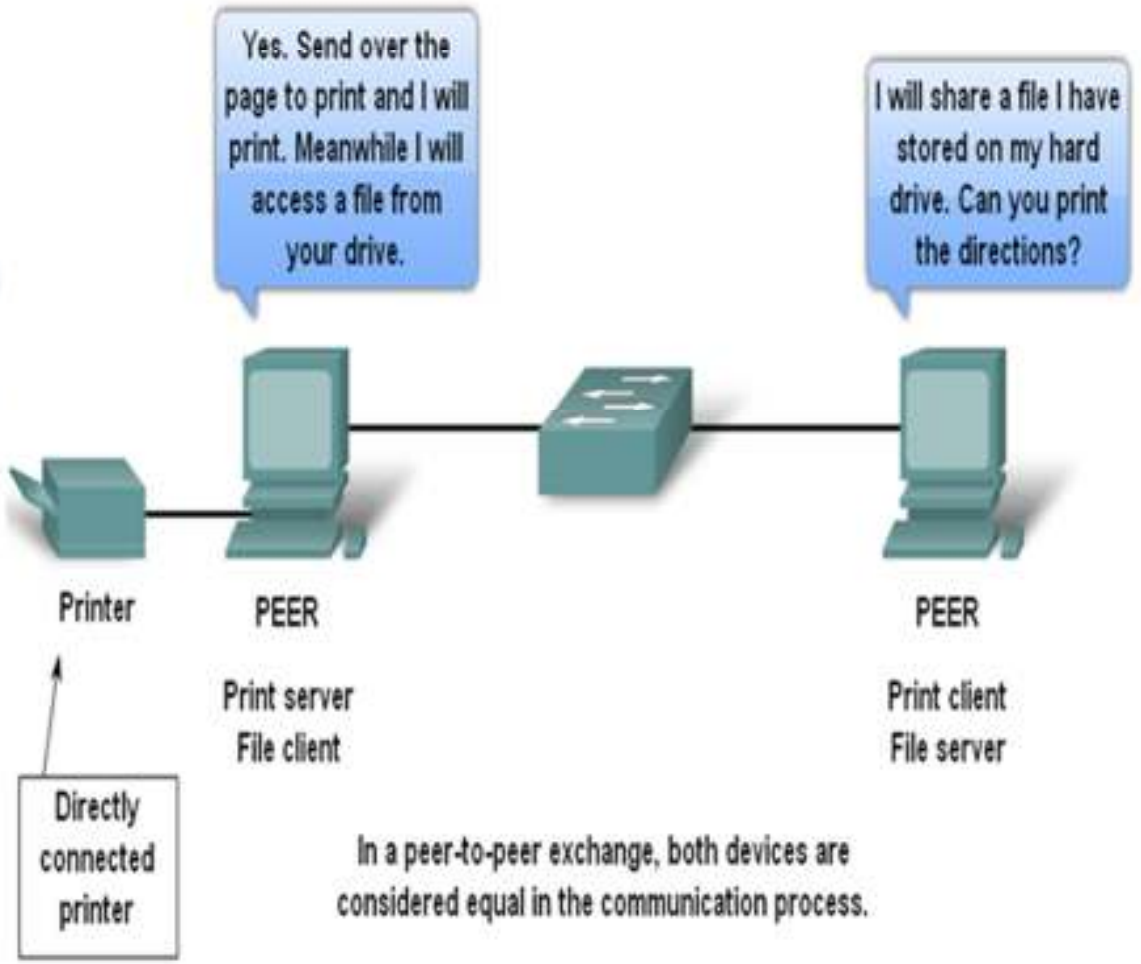
When people attempt to access information on their device, whether it is a PC, laptop, PDA, cell phone, or some other device connected to a network, the data may not be physically stored on their device. If that is the case, a request to access that information must be made to the device where the data resides.



Peer-to-Peer Networking and Applications (P2P)

Peer-to-Peer Networks

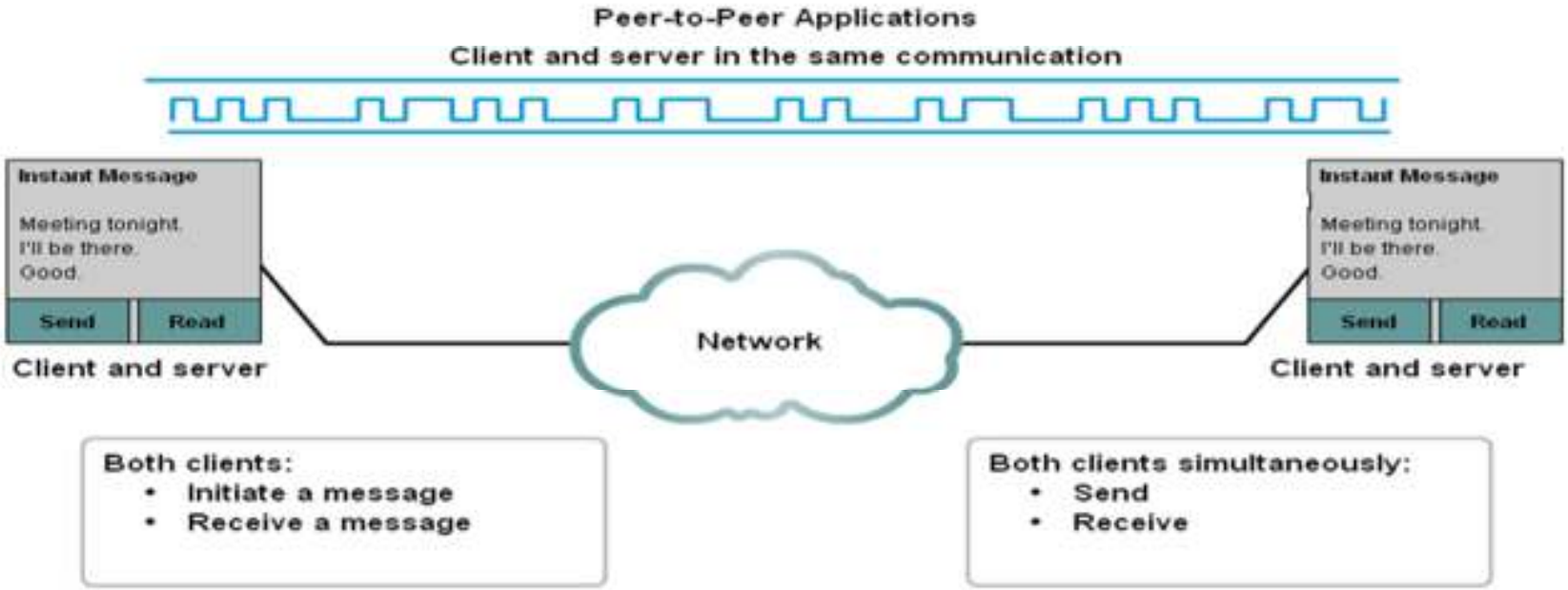
In a peer-to-peer network, two or more computers are connected via a network and can share resources (such as printers and files) without having a dedicated server. Every connected end device (known as a peer) can function as either a server or a client. One computer might assume the role of server for one transaction while simultaneously serving as a client for another. The roles of client and server are set on a per request basis.



Peer-to-Peer Networking and Applications (P2P)

A peer-to-peer application (P2P), unlike a peer-to-peer network, allows a device to act as both a client and a server within the same communication. In this model, every client is a server and every server a client. Both can initiate a communication and are considered equal in the communication process.

Peer-to-peer applications can be used on peer-to-peer networks, client/server networks, and across the Internet.



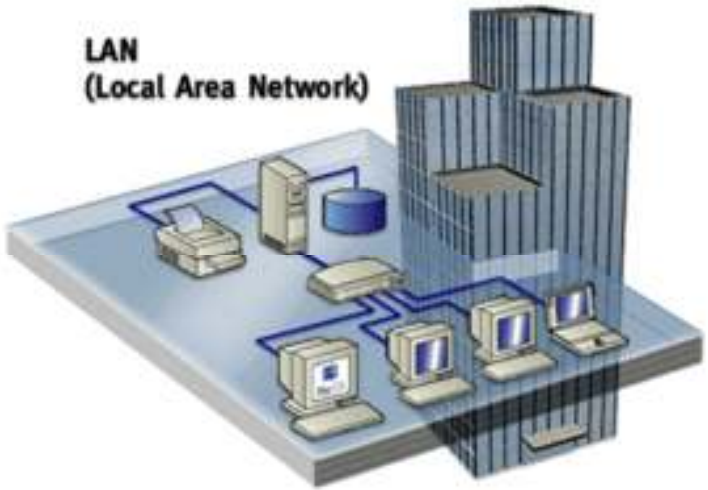
Communicating over the Network

Types of Network:

- One way to categorize the different types of computer network designs is by their scope or scale.
- Common examples of area network types are:
  - LAN - Local Area Network
  - WLAN - Wireless Local Area Network
  - WAN - Wide Area Network
  - MAN - Metropolitan Area Network

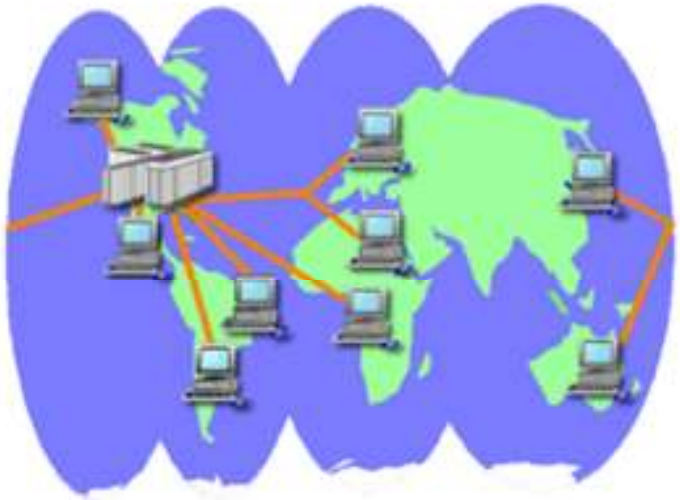
LAN - Local Area Network:

- A LAN connects network devices over a relatively short distance.
- A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings.
- In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.
- In addition to operating in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization.
- They also tend to use certain connectivity technologies, primarily Ethernet and Token Ring.



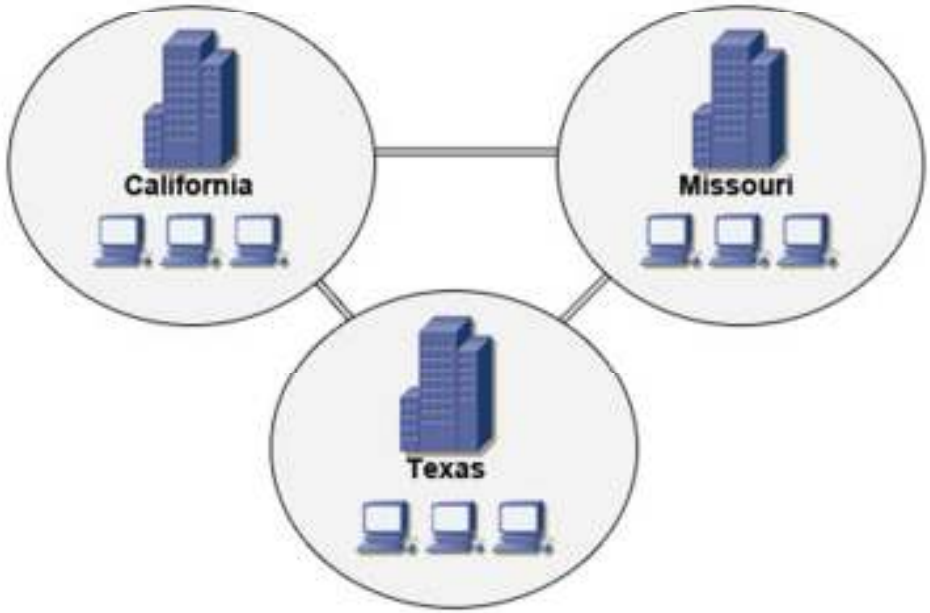
WAN - Wide Area Network:

- As the term implies, a WAN spans a large physical distance.
- The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs.
- A network device called a router connects LANs to a WAN.
- In IP networking, the router maintains both a LAN address and a WAN address.
- A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management.
- WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.



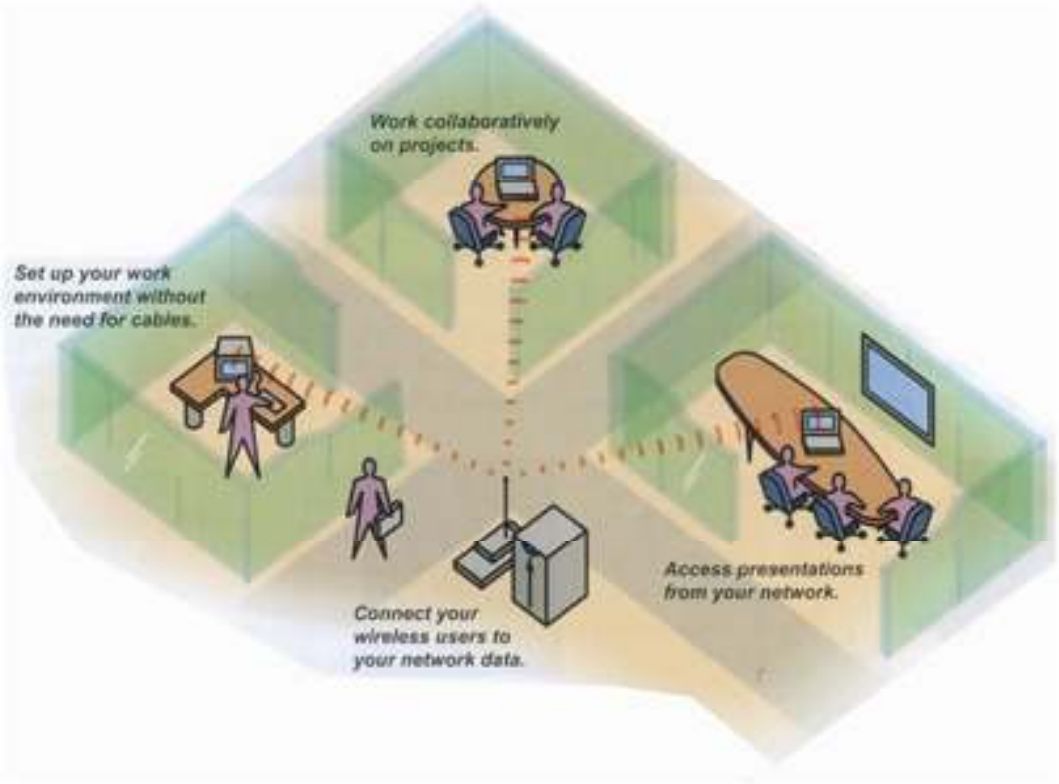
MAN - Metropolitan Area Network:

- A network spanning a physical area larger than a LAN but smaller than a WAN, such as a city. A MAN is typically owned and operated by a single entity such as a government body or large corporation.



WLAN - Wireless Local Area Network:

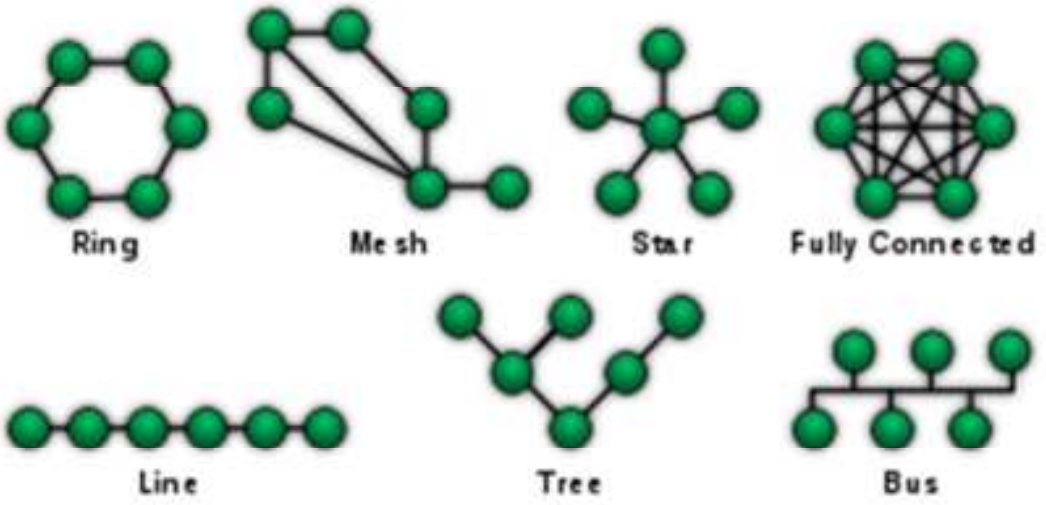
- A LAN based on Wi-Fi wireless network technology



Topology in Network

- Network topologies are categorized into the following basic types:

- Point-to-Point
- Bus
- Star
- Ring
- Mesh
- Tree
- Hybrid



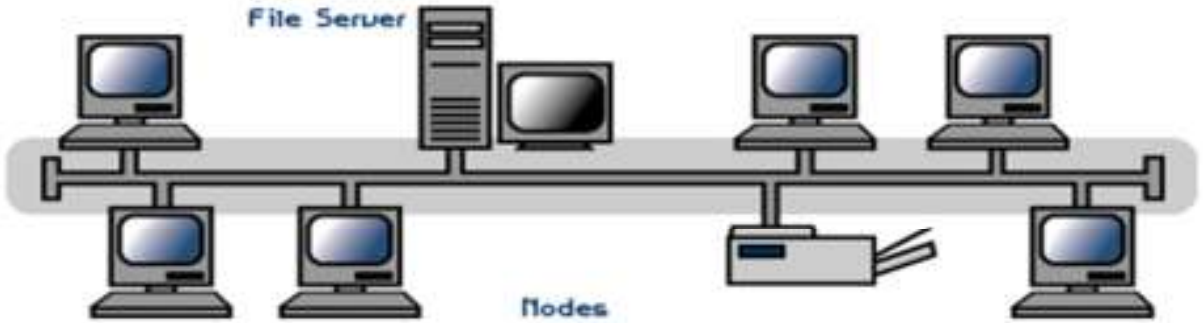
Point-to-Point Topology:

- The simplest topology is a permanent link between two endpoints
- Physical media Connected between same type device depends upon DCE & DTE.

Bus Topology:

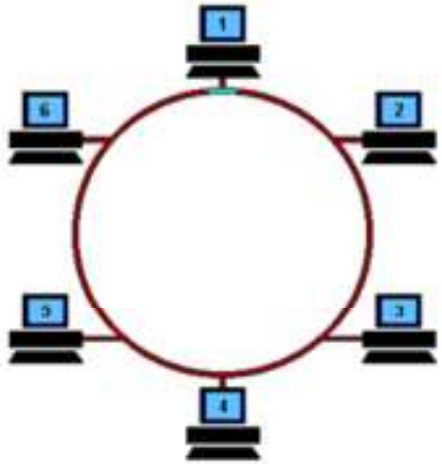
Bus networks (not to be confused with the system bus of a computer) use a common backbone to connect all devices.

A single cable, the backbone functions as a shared communication medium that devices attach or tap into with an interface connector.



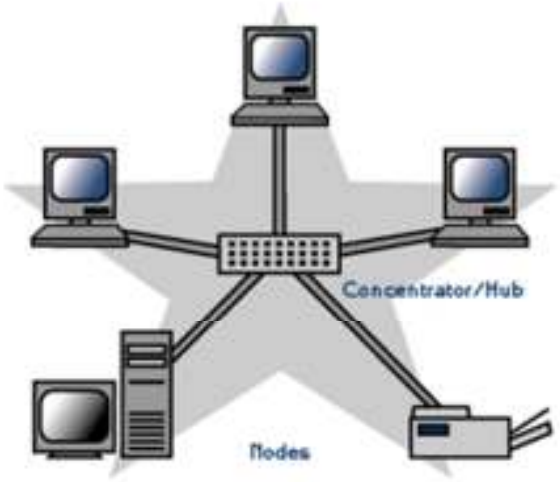
Ring Topology:

In a ring network, every device has exactly two neighbors for communication purposes.
All messages travel through a ring in the same direction (either "clockwise" or "counterclockwise").
A failure in any cable or device breaks the loop and can take down the entire network.



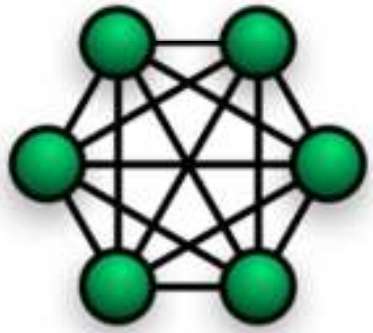
Star Topology:

Many home networks use the star topology.
A star network features a central connection point called a "hub" that may be a hub, switch or router.
Devices typically connect to the hub with Unshielded Twisted Pair (UTP) Ethernet.
Compared to the bus topology, a star network generally requires more cable, but a failure in any star network cable will only take down one computer's network access and not the entire LAN. (If the hub fails, however, the entire network also fails.)

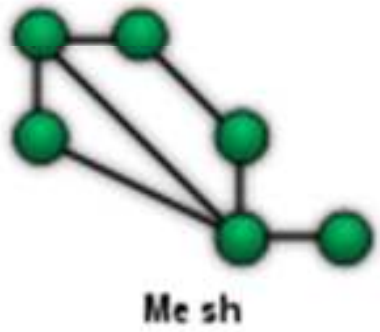


Mesh Topology:

A Mesh network in which every device connects to every other is called a full mesh. As shown in the illustration below, partial mesh networks also exist in which some devices connect only indirectly to others.



Full Mesh topology

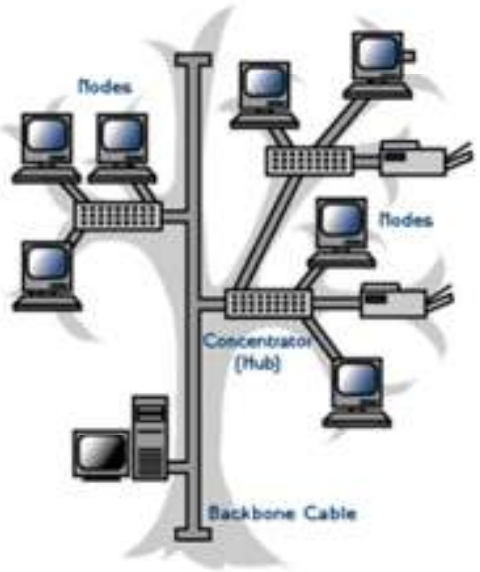


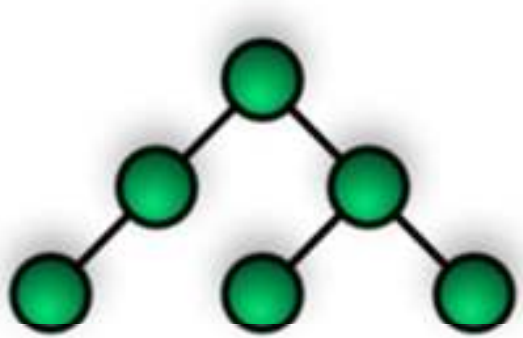
Partial Mesh topology

Tree Topology:

Tree topologies integrate multiple star topologies together onto a bus.

In its simplest form, only hub devices connect directly to the tree bus, and each hub functions as the "root" of a tree of devices.





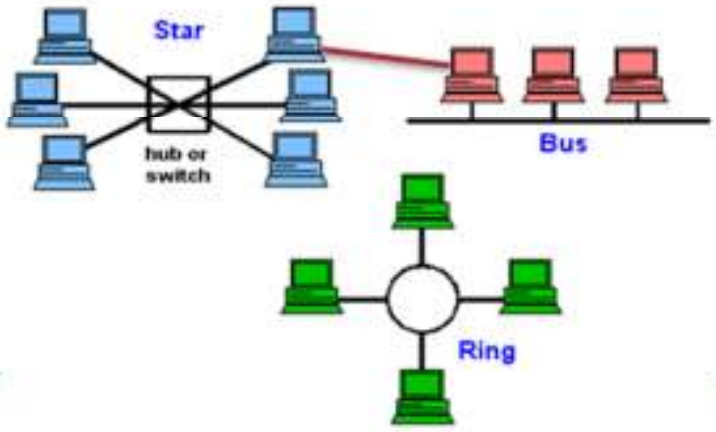
Hybrid Network Topology:

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.).

For example, a tree network connected to a tree network is still a tree network topology.

A hybrid topology is always produced when two different basic network topologies are connected.

Two common examples for Hybrid network are: star ring network and star bus network



Network Terminologies

Internet, Intranet, Extranet

- ***Internet*** - sometimes called simply "the Net," is a worldwide system of computer networks - a network of networks in which users at any one computer can, if they have permission, get information from any other computer

- ***Intranet*** – An intranet is a private LAN designed for use by everyone within an organization. An intranet might consist of an internal e-mail system, a message board and one or more Web site portals that contain company news, forms, and personnel information.

  Access to an intranet's web site/Resources is restricted by a ***firewall***.

- ***Extranet*** – a network that connects people within your company with people who are outside your company--all within a secure, password-protected network that can be accessed from anywhere.

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

People matter, results count.

Measuring Bandwidth

Unit of Bandwidth	Abbreviation	Equivalence
Bits per second	bps	1 bps = fundamental unit of bandwidth
Kilobits per second	kbps	1 kbps = ~1,000 bps = 10^3 bps
Megabits per second	Mbps	1 Mbps = ~1,000,000 bps = 10^6 bps
Gigabits per second	Gbps	1 Gbps = ~1,000,000,000 bps = 10^9 bps
Terabits per second	Tbps	1 Tbps = ~1,000,000,000,000 bps = 10^{12} bps

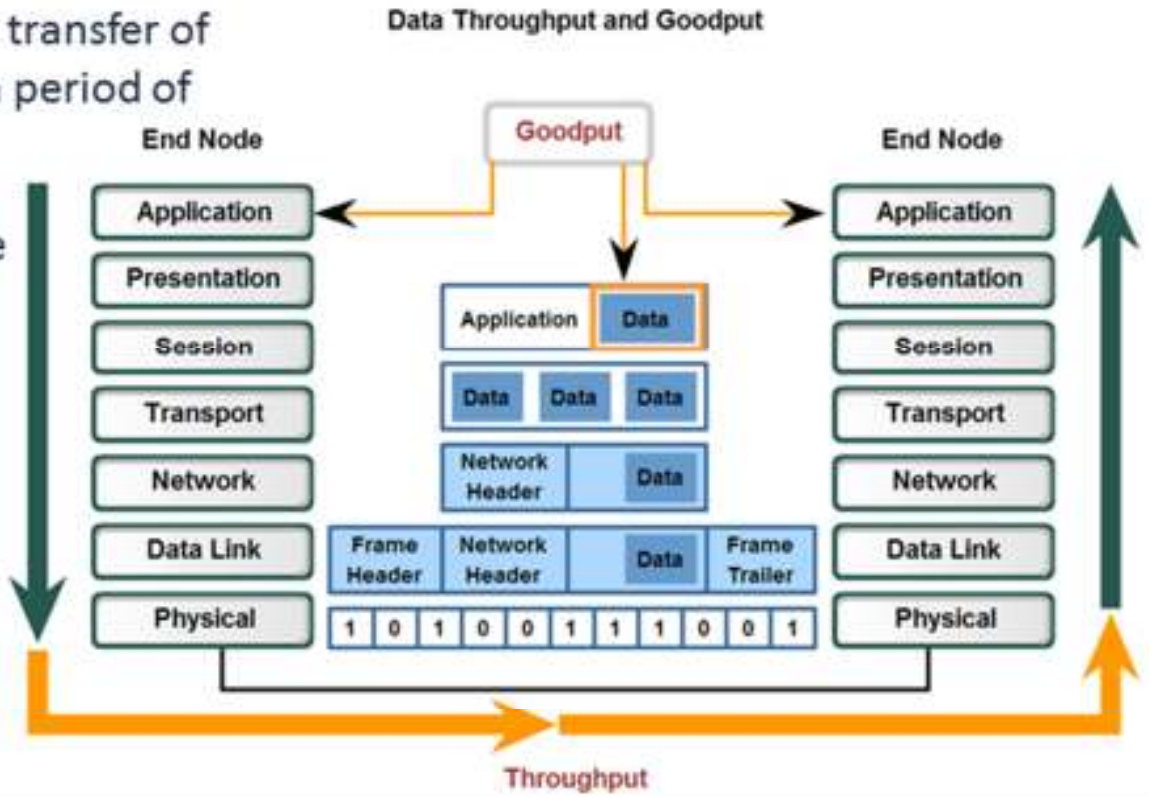
Keep in mind in data communication 1 kilobit = 1000 bits,(Kbps) while in data storage 1 Kilobyte = 1024 Bytes. (KBps)

Throughput & Goodput

Throughput

Throughput is the measure of the transfer of bits across the media over a given period of time.

Goodput is the measure of usable data transferred over a given period of time, and is therefore the measure that is of most interest to network users



Data throughput is actual network performance. Goodput is a measure of the transfer of usable data after protocol overhead traffic has been removed.

Latency

- The term *latency* refers to any of several kinds of delays typically incurred in processing of network data. A so-called *low latency* network connection is one that generally experiences small delay times, while a *high latency* connection generally suffers from long delays.

Types of Communications systems:

- The communication system can be classified into three categories
  - Simplex
  - Full Duplex
  - Half Duplex

Simplex:

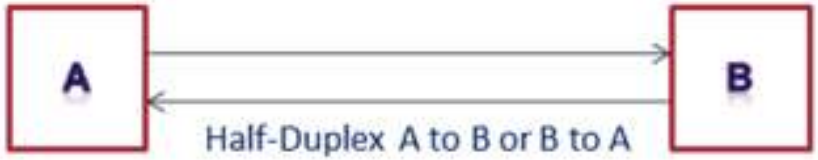
A simplex system is a communication system in which the message can be send in one direction only.
Radio and TV broadcasting are e.g.
User – Transmitter – Receiver – User

Types of Communications systems:

HALF-DUPLEX

- In a half duplex system, each end may transmit, but only one at a time. This requires both transmitting and receiving circuitry at each end, but the actual link between the two ends may be shared.

  Eg : A citizen's band radio where a frequency channel is shared and each party has to say "over" to switch the direction of the communication.



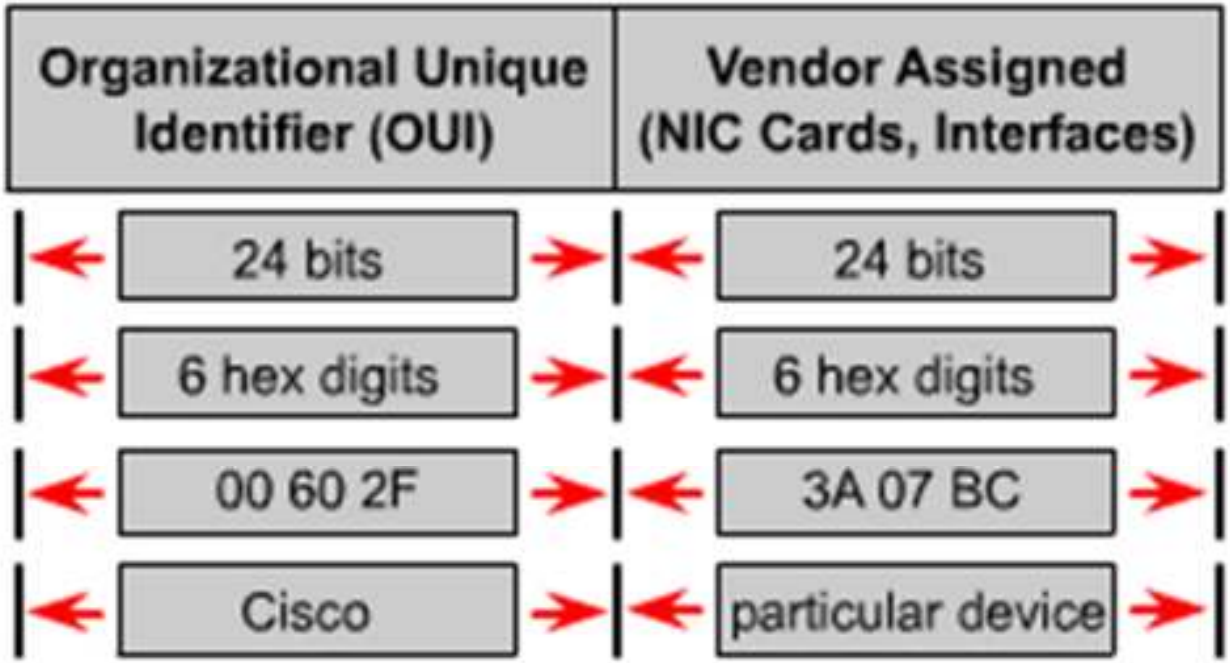
FULL-DUPLEX

- A full duplex system is one in which the link is capable of transmitting in both the direction, at the same.

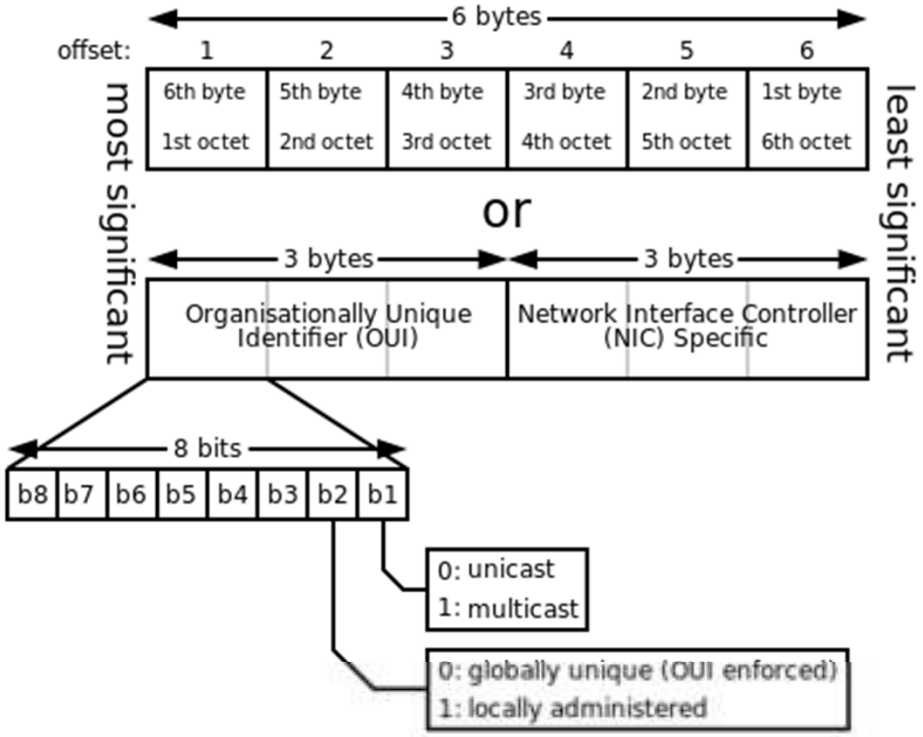
- Eg : telephone system.

MAC Address

MAC address is 48 bits in length and expressed as twelve hexadecimal digits.MAC addresses are sometimes referred to as burned-in addresses (BIA) because they are burned into read-only memory (ROM) and are copied into random-access memory (RAM) when the NIC initializes.



MAC Address

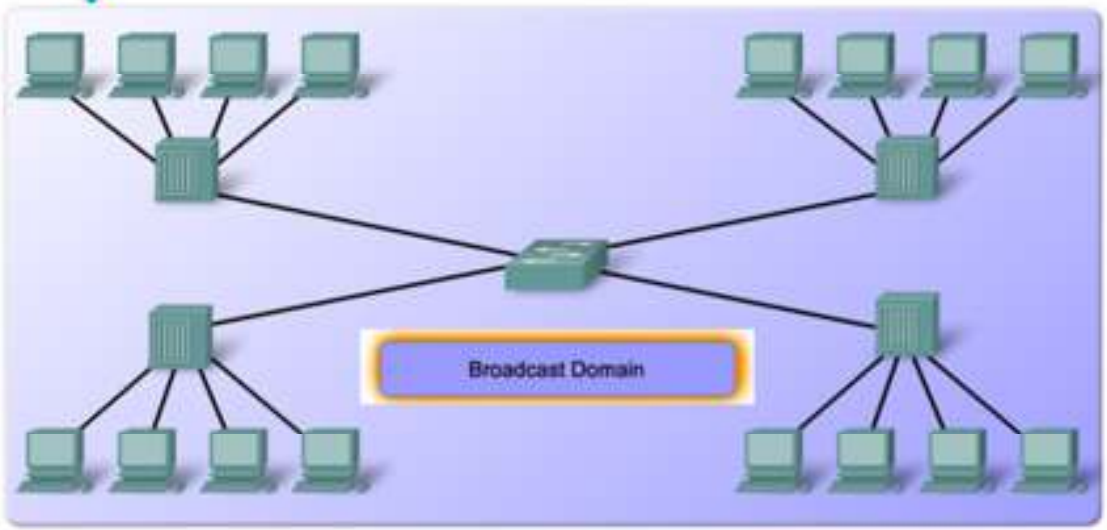


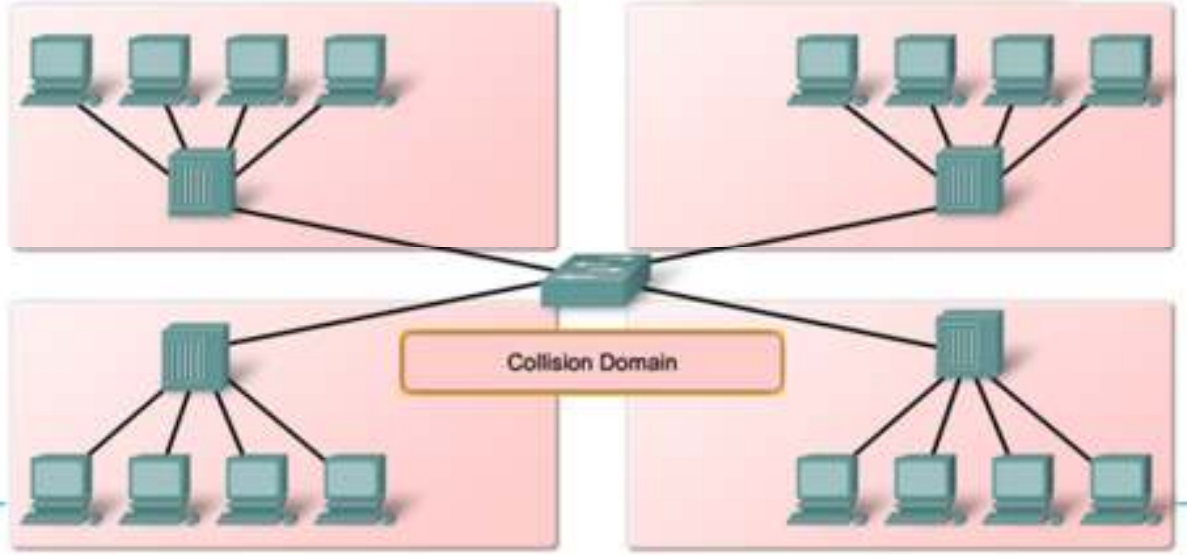
Network-Broadcast/Collision

- A **broadcast domain** is a logical division of a computer network, in which all nodes can reach each other by **broadcast** at the data link layer. A **broadcast domain** can be within the same LAN segment or it can be bridged to other LAN segments.

- A **collision domain** is a section of a network connected by a shared medium or through repeaters where data packets can **collide** with one another when being sent, particularly when using early versions of Ethernet.

Network-Broadcast/Collision





Components of Network:

i) Network cards

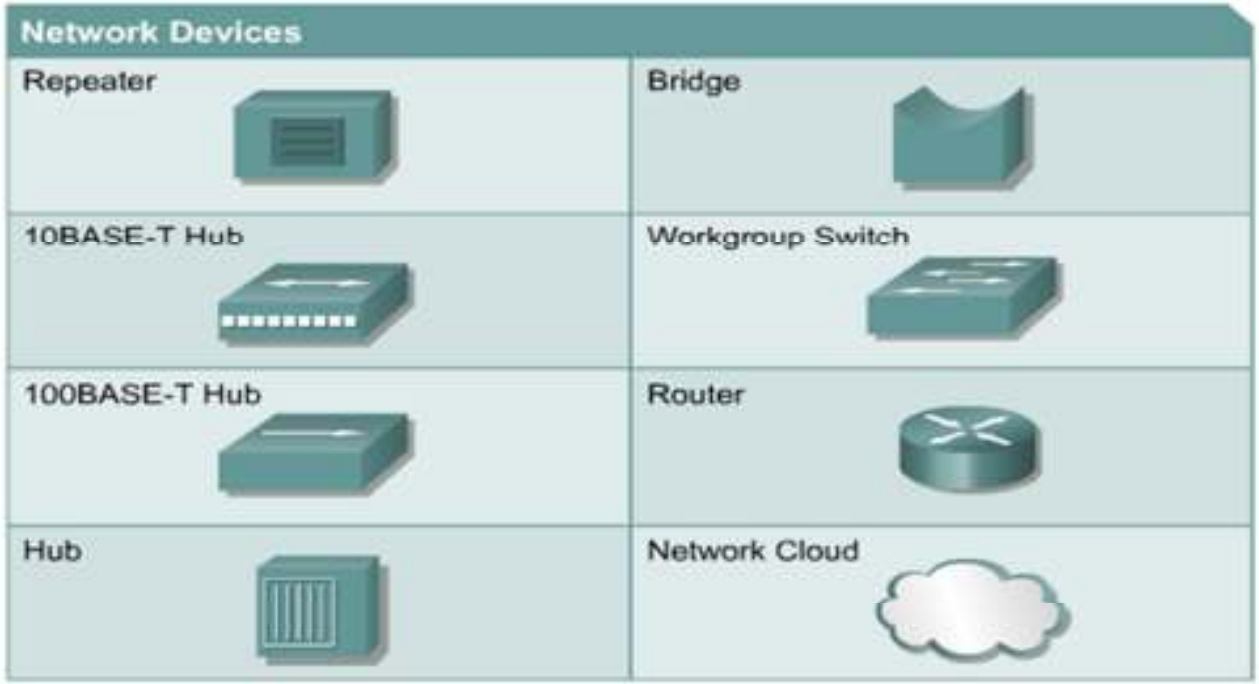
ii) Hub

iii) Switch

iv) Bridges

v) Repeater

vi) Router



Network Interface Card:

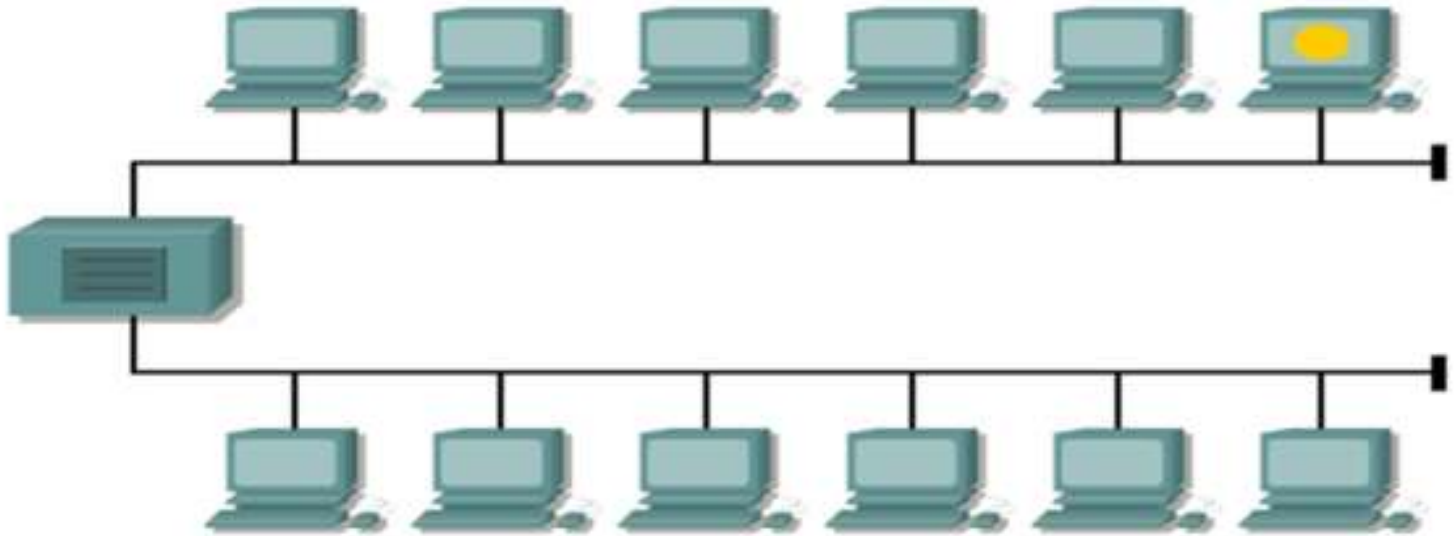
- A network interface card (NIC) is a printed circuit board that provides network communication capabilities to and from a personal computer. Also called a LAN adapter.

Internal network interface card

PCMCIA Network interface card

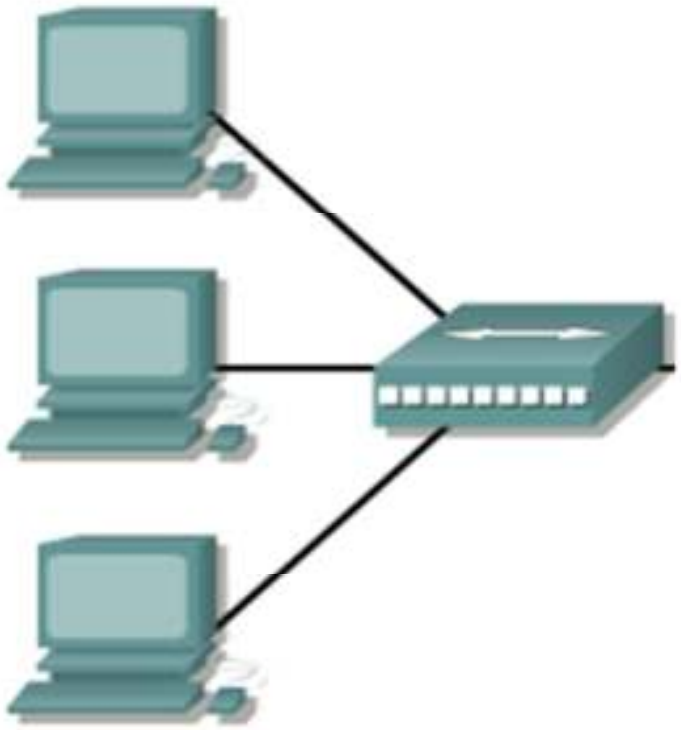
Repeater:

- A repeater is a network device used to regenerate a signal.
- Repeaters regenerate analog or digital signals distorted by transmission loss due to attenuation. A repeater does not perform intelligent routing.



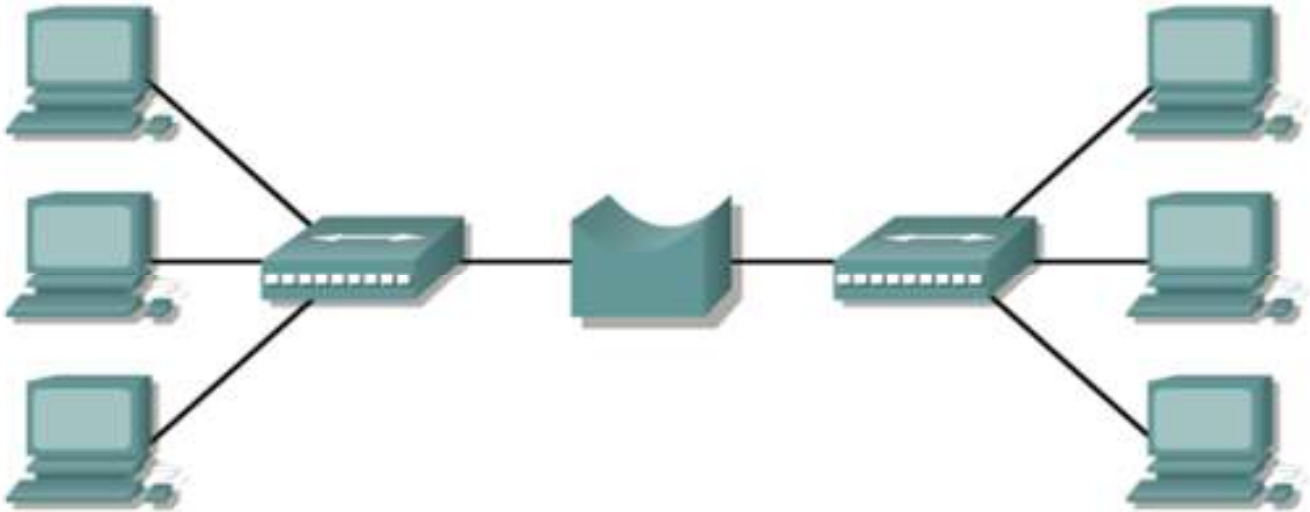
Hub:

- Hubs concentrate connections. In other words, they take a group of hosts and allow the network to see them as a single unit.
- This is done passively, without any other effect on the data transmission.
- Active hubs not only concentrate hosts, but they also regenerate signals.



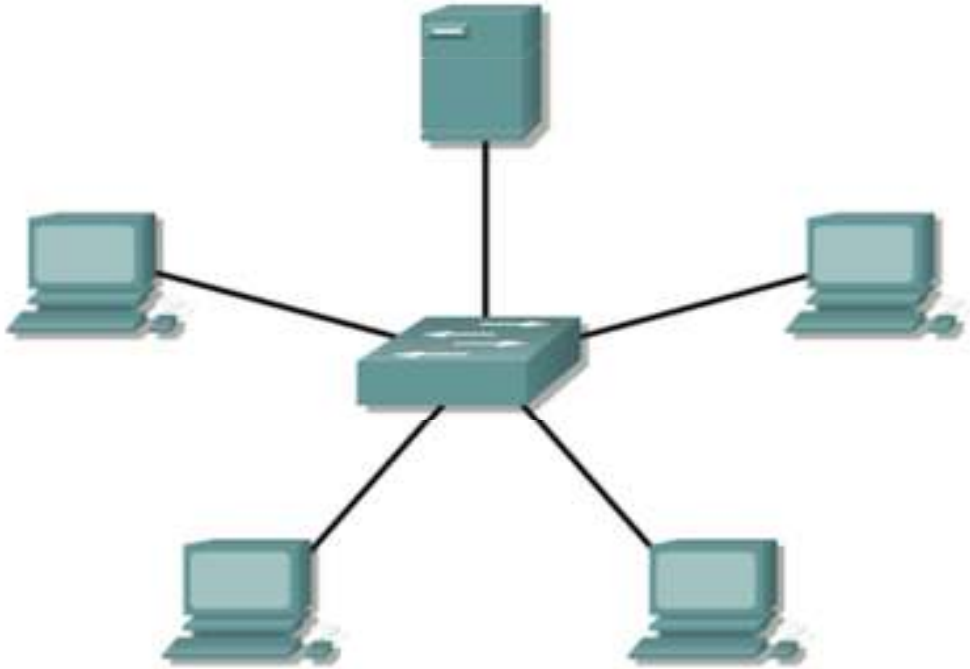
Bridge:

- Bridges convert network transmission data formats as well as perform basic data transmission management. Bridges, as the name implies, provide connections between LANs. Not only do bridges connect LANs, but they also perform a check on the data to determine whether it should cross the bridge or not. This makes each part of the network more efficient.

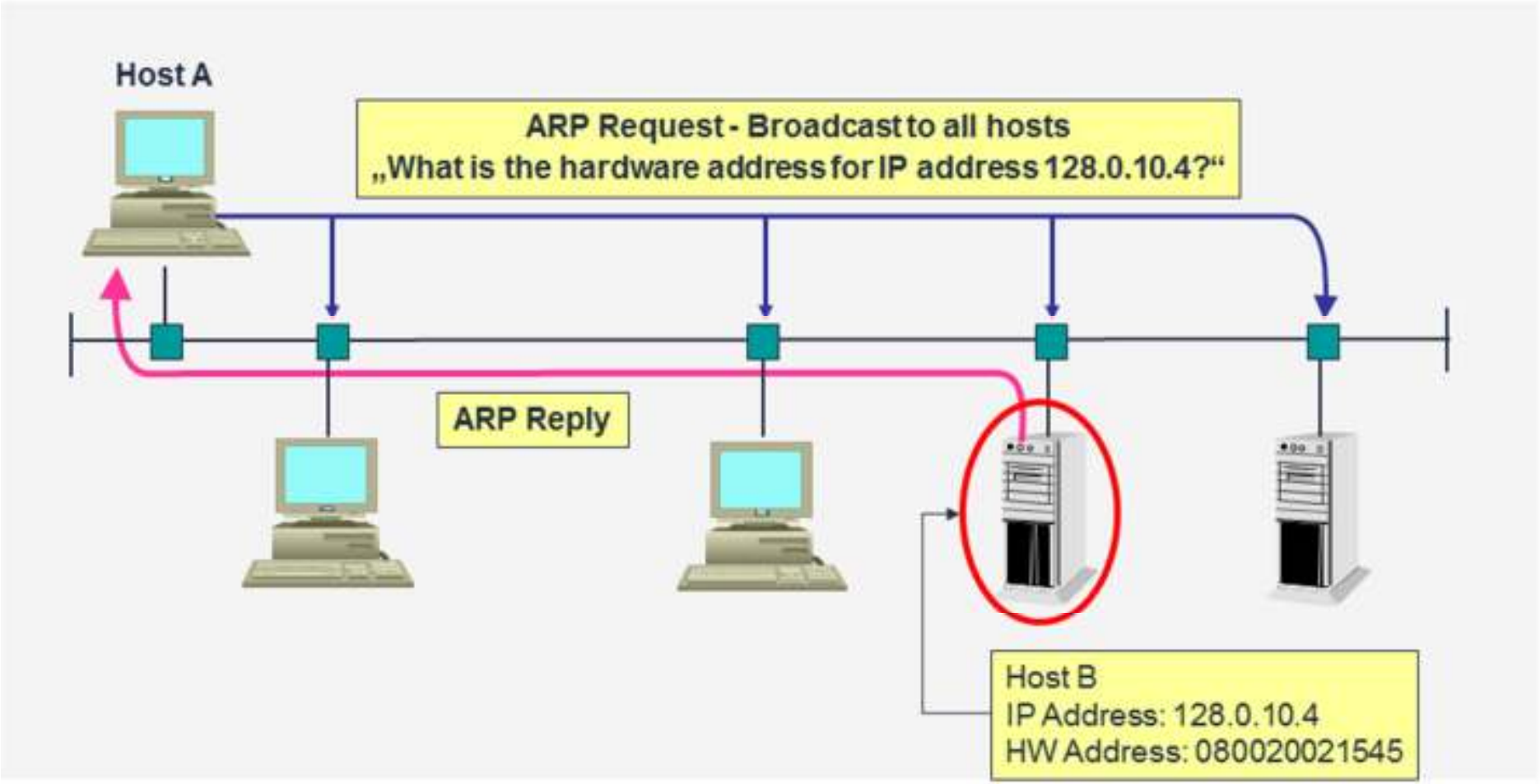


Switch:

- Switches are Data Link layer devices.
- Each Switch port has a unique MAC address.
- Connected host MAC addresses are learned and stored on a MAC address table.

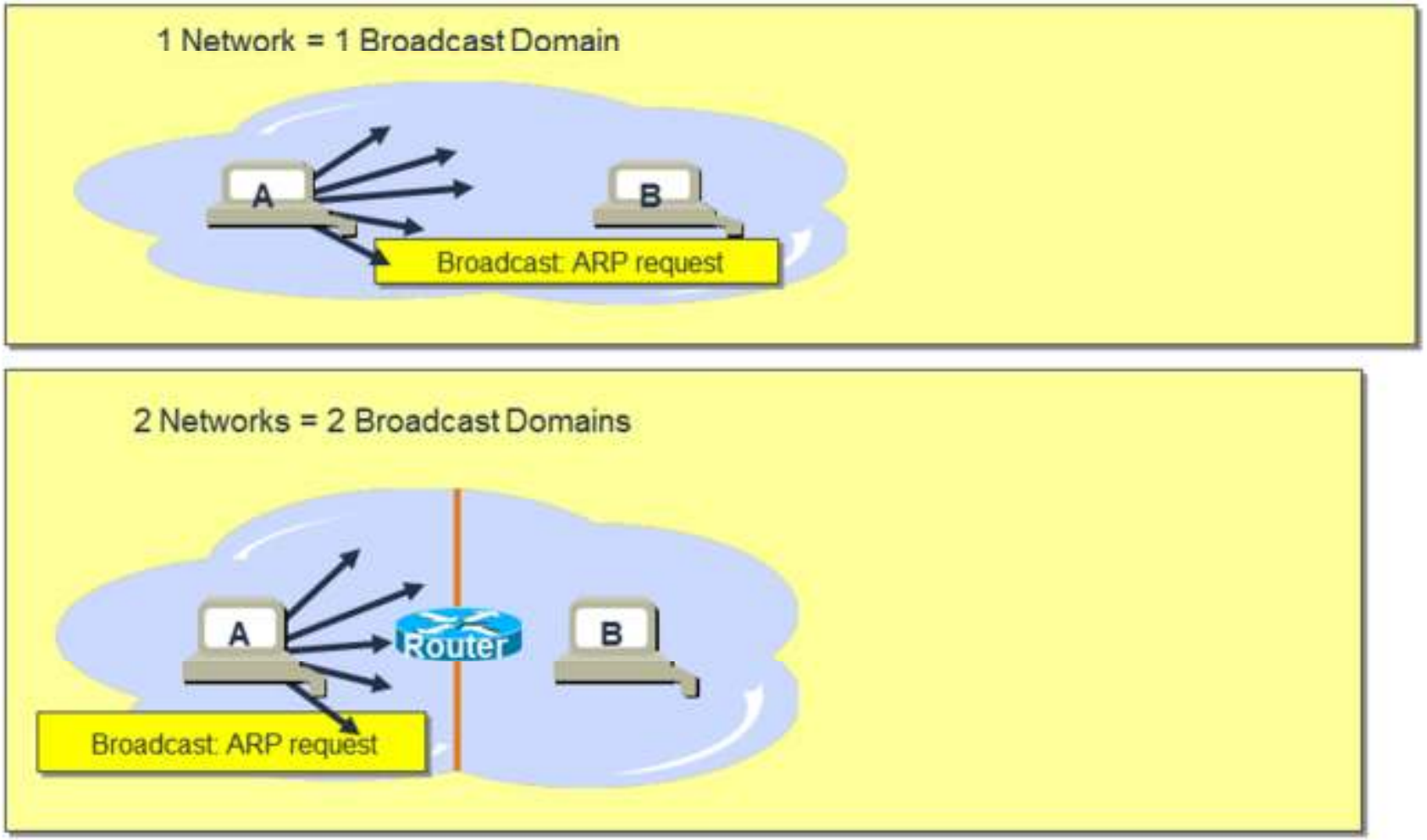


ARP-(Address Resolution Protocol)



ARP

Broadcast



RARP

Reverse Address Resolution Protocol (RARP) associates a known MAC addresses with an IP addresses.

A network device, such as a diskless workstation, might know its MAC address but not its IP address. RARP allows the device to make a request to learn its IP address.
Devices using RARP require that a RARP server be present on the network to answer RARP requests.

Computer FE:ED:F9:23:44:EF stores the IP address received in the RARP reply for later use.

Switching Modes:

Cut-through

- A switch starts to transfer the frame as soon as the destination MAC address is received. No error checking is available.
- Must use synchronous switching.

Store-and-forward

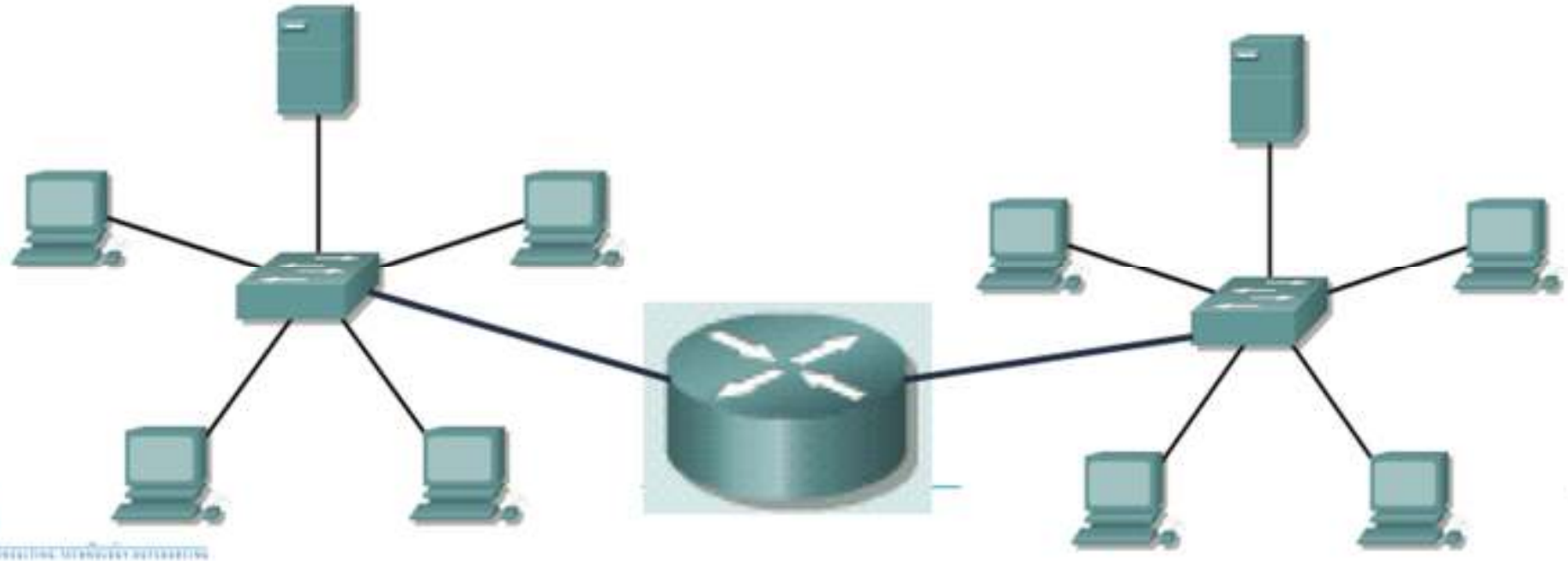
- At the other extreme, the switch can receive the entire frame before sending it out the destination port. This gives the switch software an opportunity to verify the Frame Check Sum (FCS) to ensure that the frame was reliably received before sending it to the destination.
- Must be used with asynchronous switching.

Fragment-free

- A compromise between the cut-through and store-and-forward modes.
- Fragment-free reads the first 64 bytes, which includes the frame header, and switching begins before the entire data field and checksum are read.

Router:

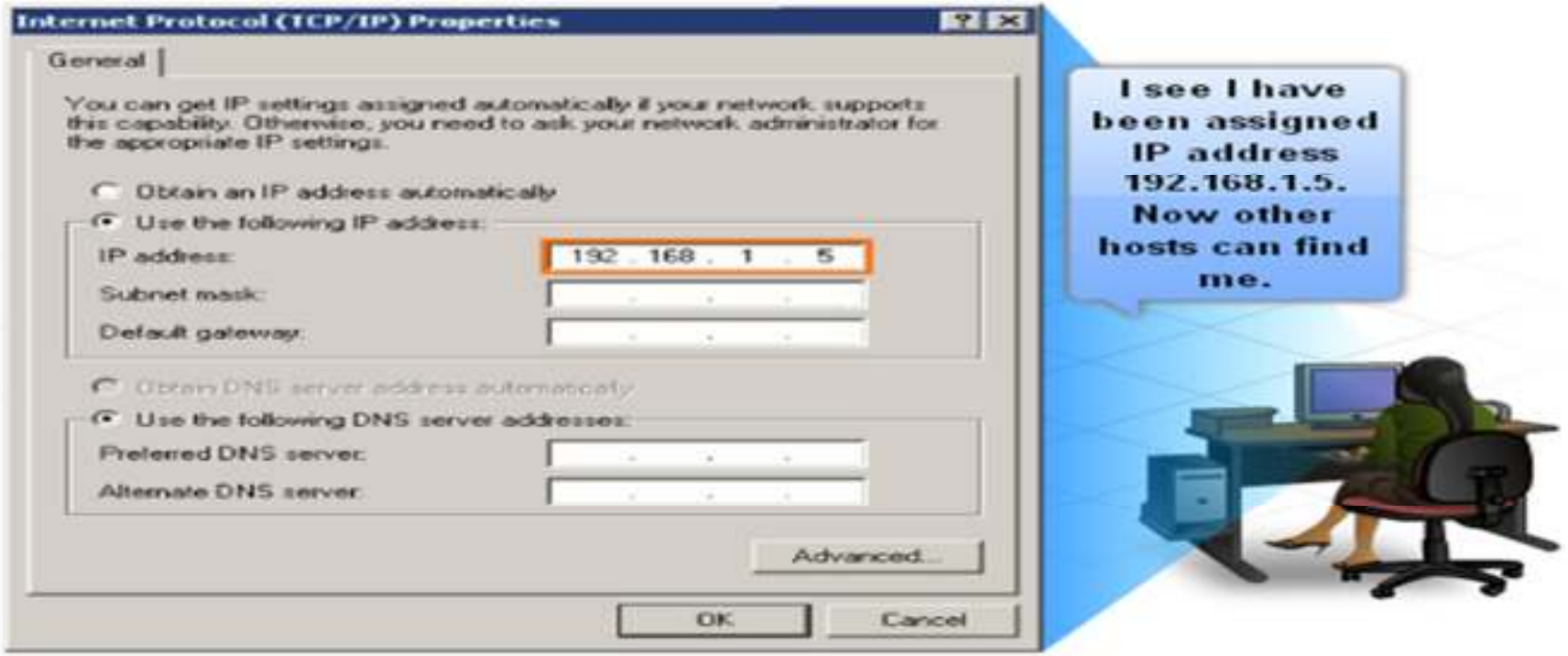
- Routers have all capabilities of the previous devices. Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers. They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.



TCP/IP MATH

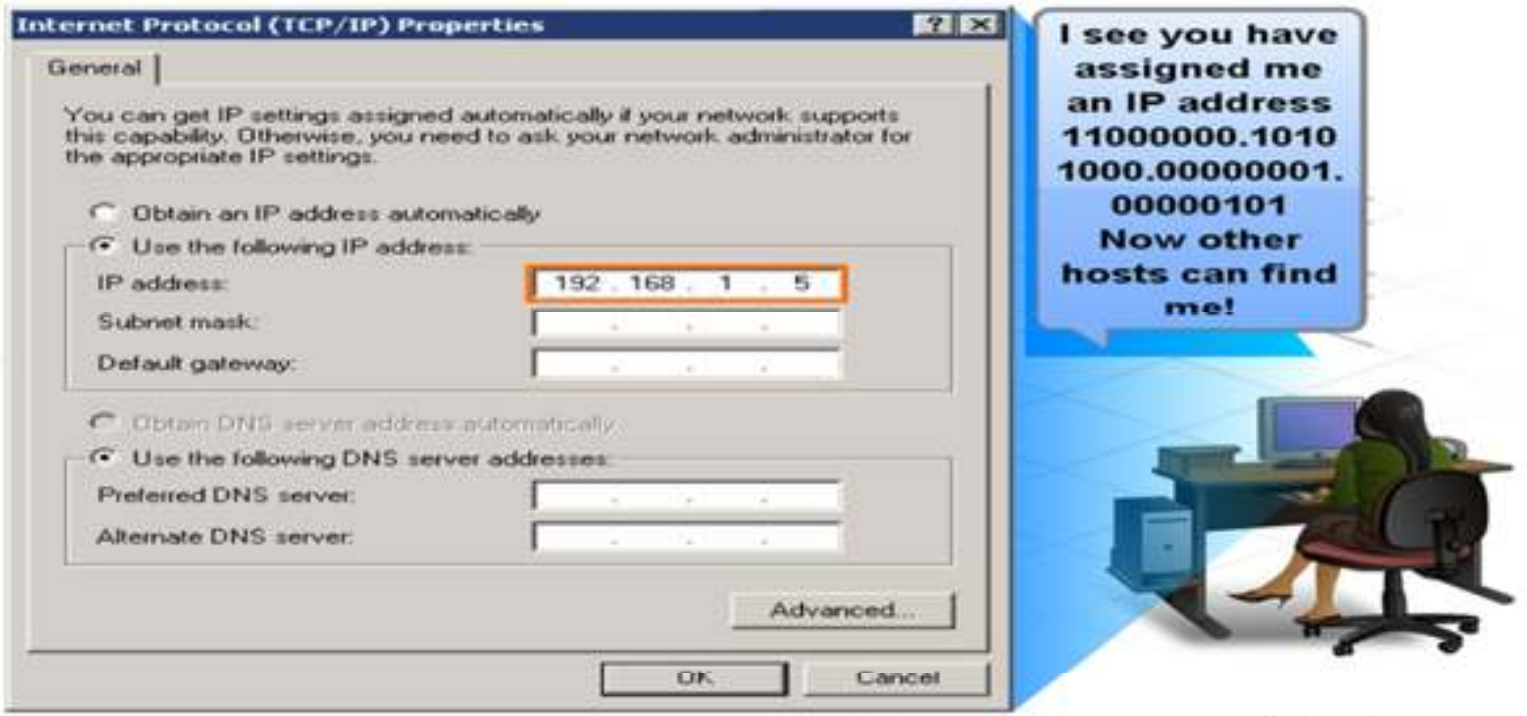
Addressing the Network – IPv4

Addressing is a key function of Network layer protocols that enables data communication between hosts on the same network or on different networks. Internet Protocol version 4 (IPv4) provides hierarchical addressing for packets that carry our data.



IP version 4 (IPv4) is the current form of addressing used on the Internet.

Addressing the Network – IPv4



IP version 4 (IPv4) is the current form of addressing used on the Internet.

Addressing the Network – IPv4

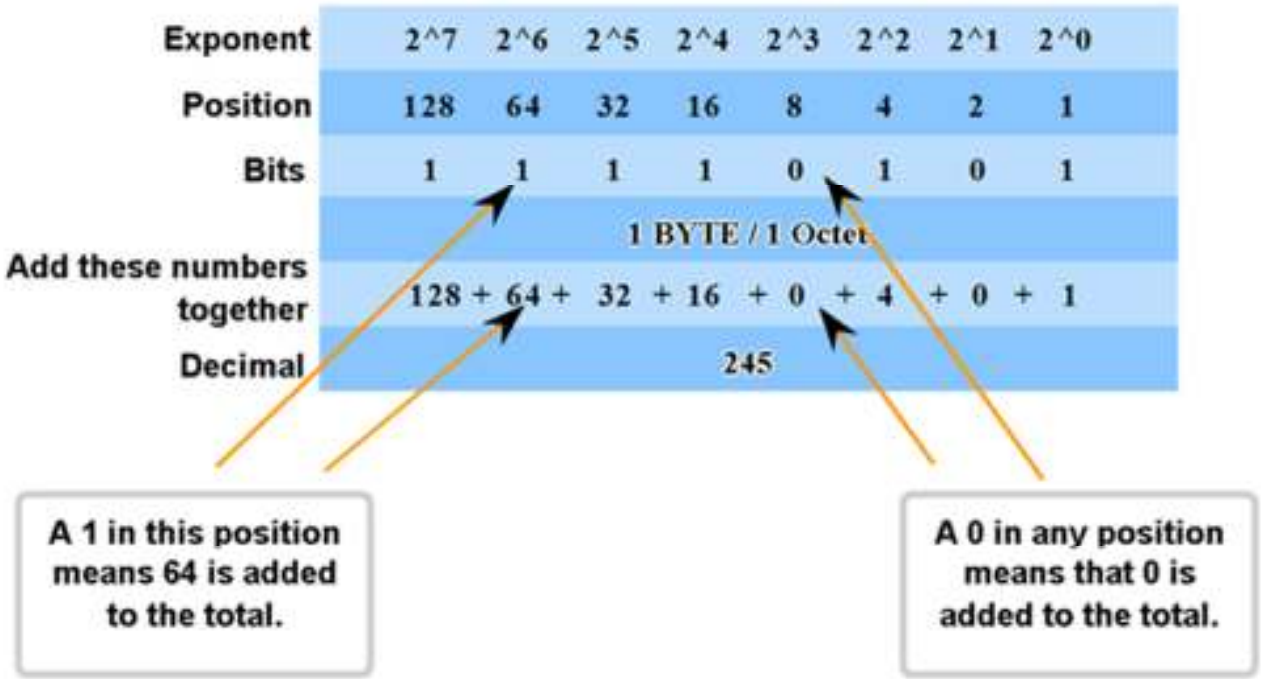
IPv4 Addresses

192	.	168	.	10	.	1
11000000		11000000		11000000		11000000

The computer using this IP address is on network 192.168.10.0.

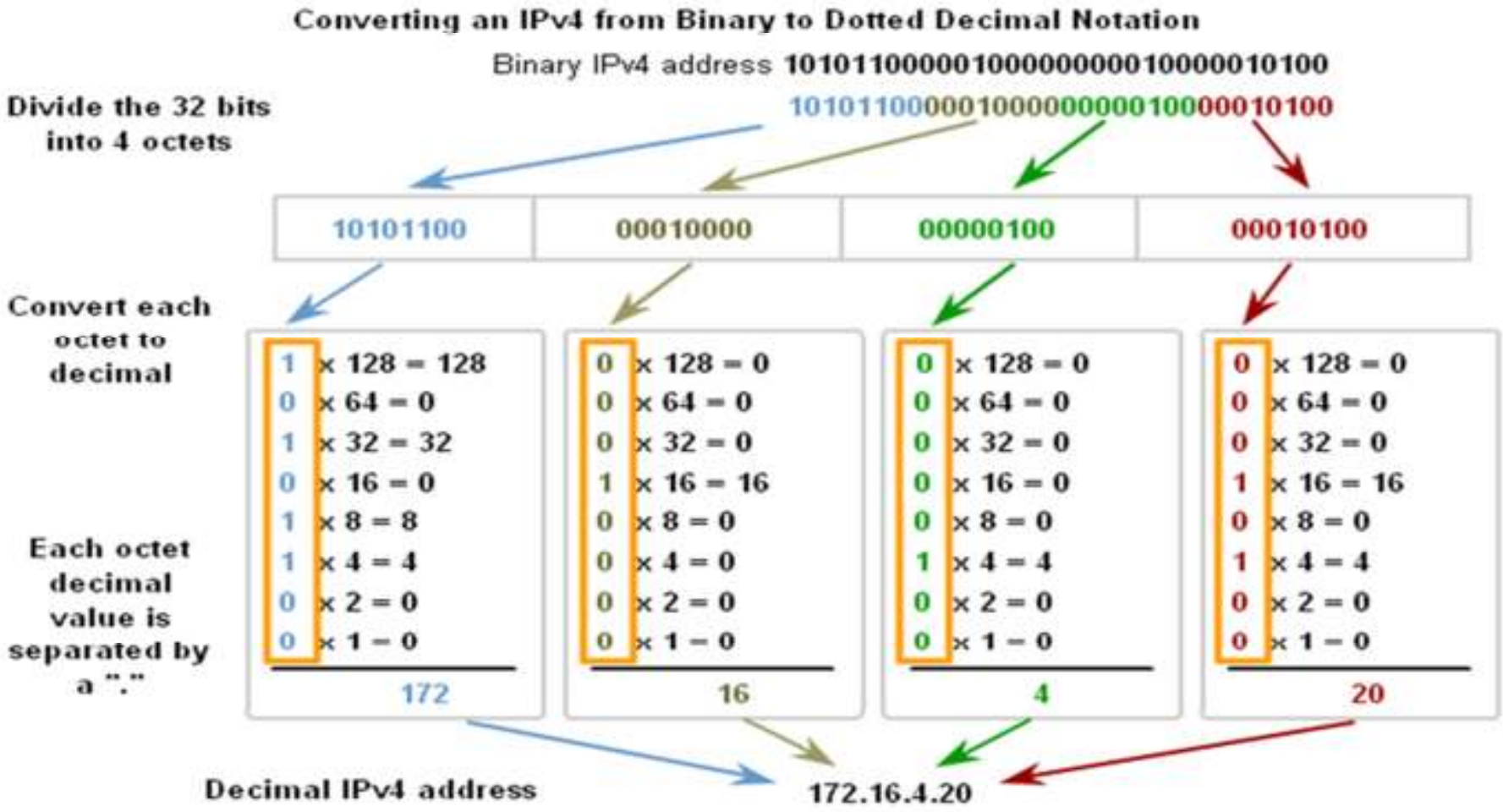
Addressing the Network – IPv4

Binary To Decimal Conversion

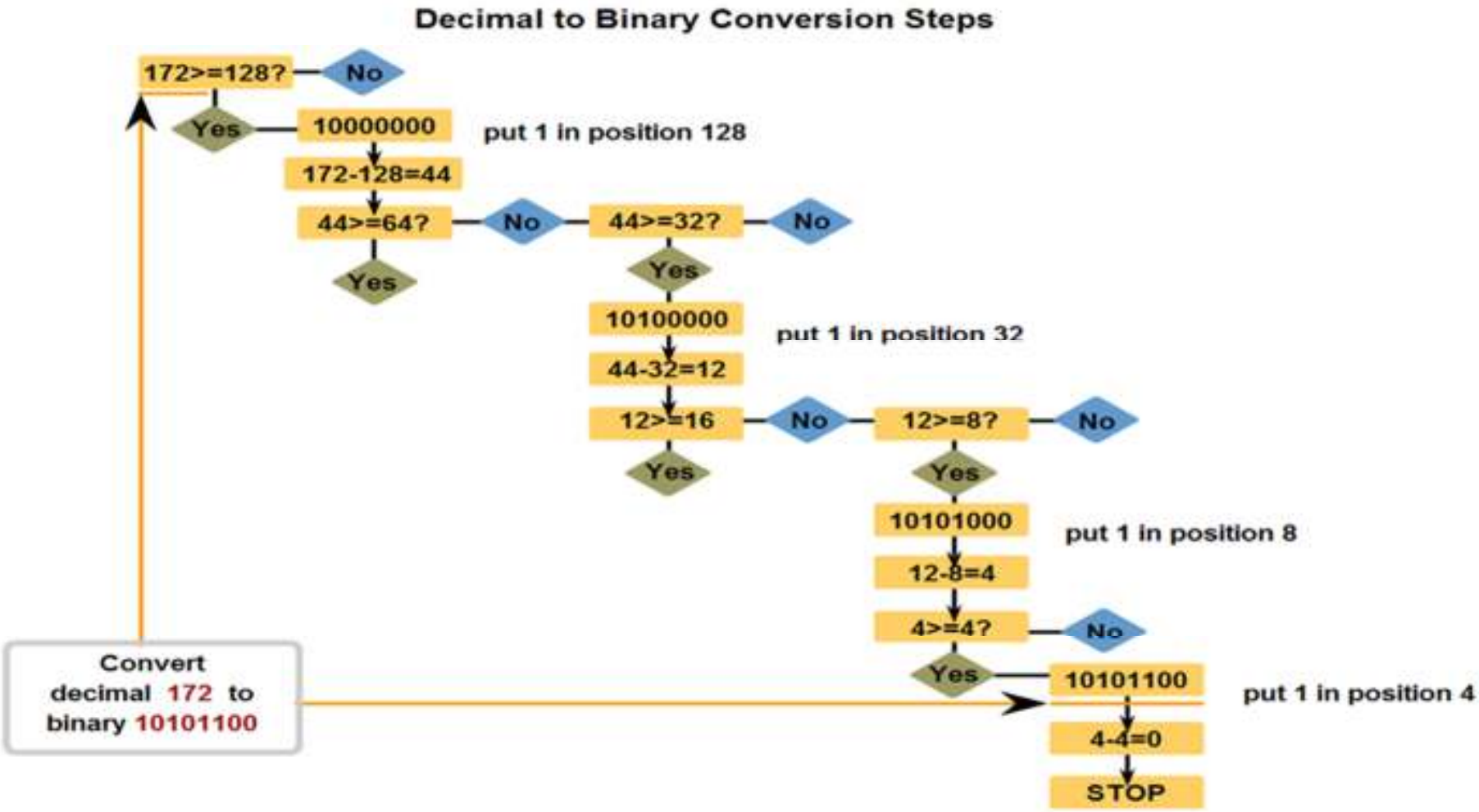


11110101 in Binary = Decimal Number 245

Addressing the Network – IPv4



Addressing the Network – IPv4



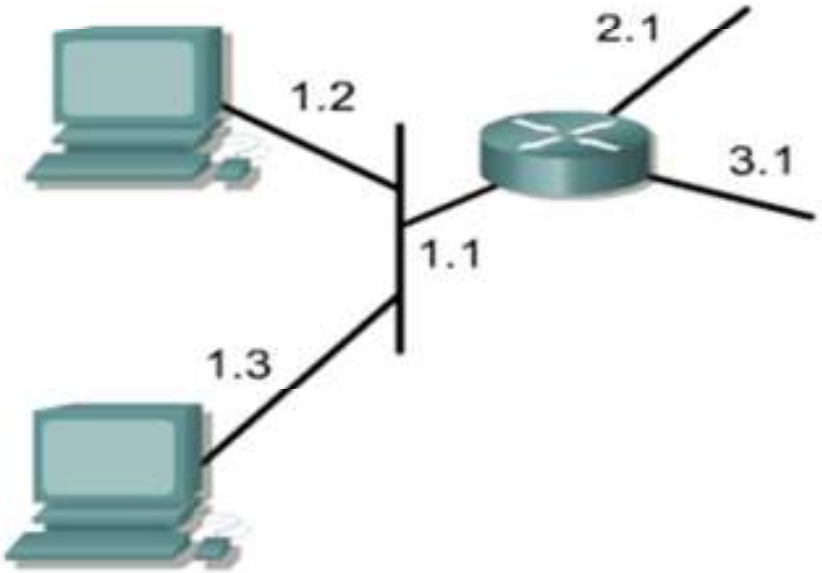
IP Addressing

Network and Host Addressing

Using the IP address of the destination network, a router can deliver a packet to the correct network.

When the packet arrives at a router connected to the destination network, the router uses the IP address to locate the particular computer connected to that network.

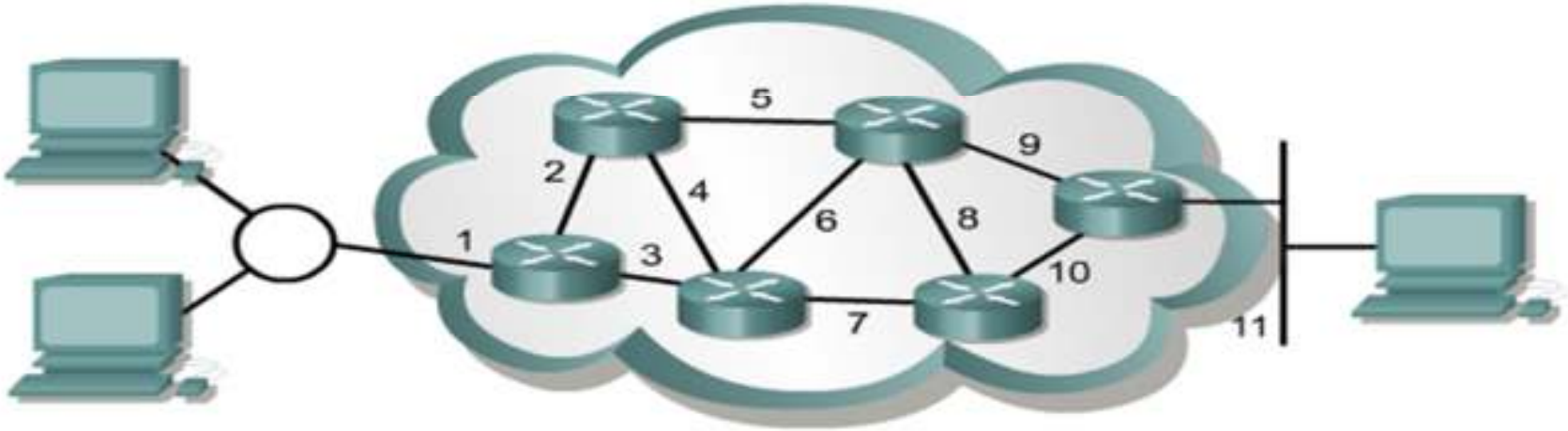
Accordingly, every IP address has two parts.



Network	Host
1	1 2 3
2	1
3	1

Network Layer Communication Path

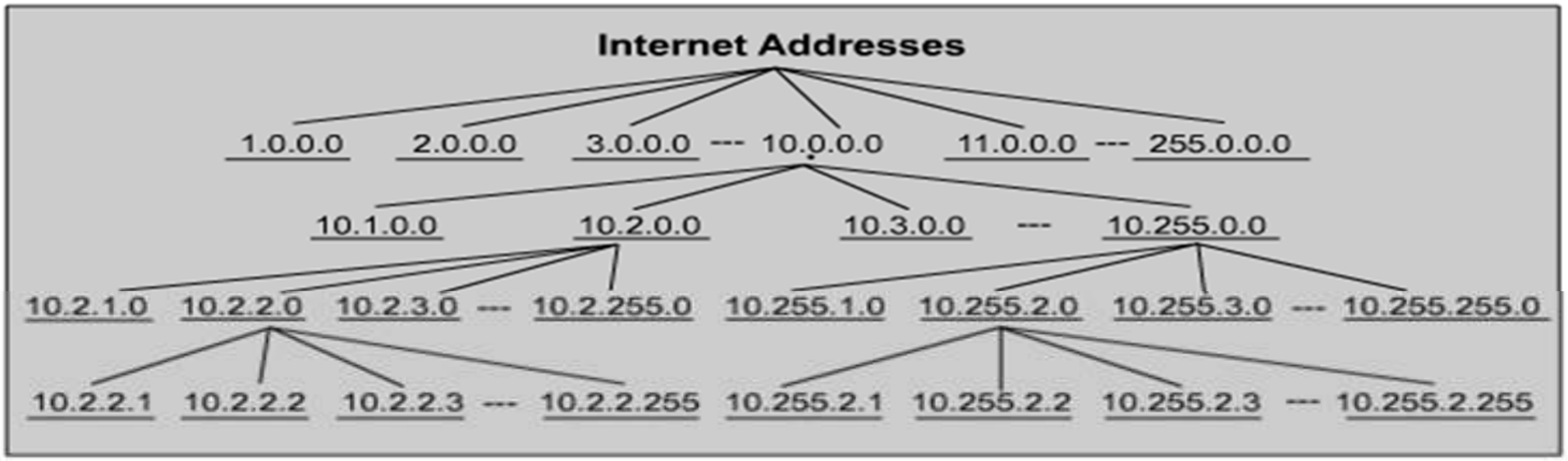
A router forwards packets from the originating network to the destination network using the IP protocol. The packets must include an identifier for both the source and destination networks.



Address represent the path of media connections

Internet Addresses

IP Addressing is a hierarchical structure. An IP address combines two identifiers into one number. This number must be a unique number, because duplicate addresses would make routing impossible. The first part identifies the system's network address. The second part, called the host part, identifies which particular machine it is on the network.



IP Address Classes

IP addresses are divided into classes to define the large, medium, and small networks.

Class A addresses are assigned to larger networks.
Class B addresses are used for medium-sized networks, &
Class C for small networks.

Address Class	Number of Networks	Number of Host per Network
A	126 *	16,777,216
B	16, 384	65,535
C	2,097,152	254
D (Multicast)	N/A	N/A

Identifying Address Classes

IP Address Class	High Order Bits	First Octet Address Range	Number of Bits in the Network Address
Class A	0	0 - 127 *	8
Class B	10	128 - 191	16
Class C	110	192 - 223	24
Class D	1110	224 - 239	28

* The 127.x.x.x address range is reserved as a loopback address, used for testing and diagnostic purposes.

Address Class Prefixes

To accommodate different size networks and aid in classifying these networks, IP addresses are divided into groups called classes. This is **classful addressing**.

Class A	Network	Host		
Octet	1	2	3	4

Class B	Network		Host	
Octet	1	2	3	4

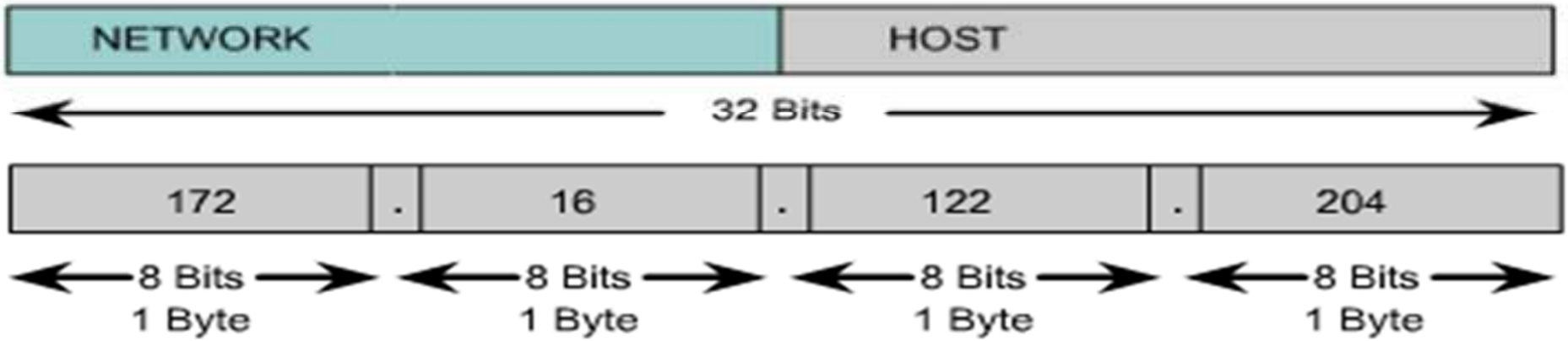
Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Class D addresses are used for multicast groups. There is no need to allocate octets or bits to separate network and host addresses. Class E addresses are reserved for research use only.

Network and Host Division

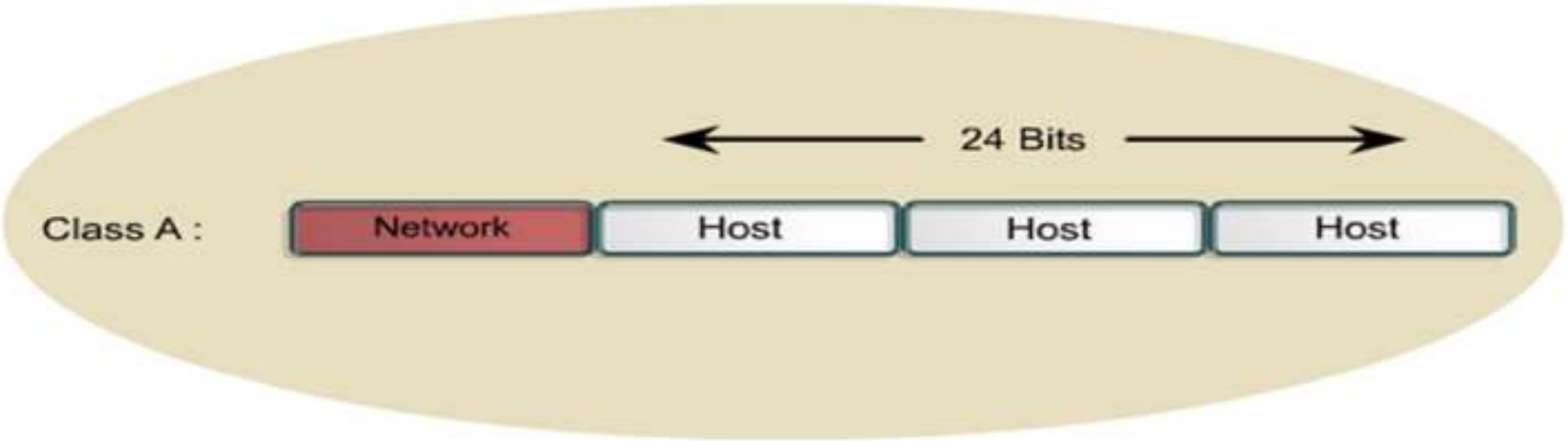
Each complete 32-bit IP address is broken down into a network part and a host part. A bit or bit sequence at the start of each address determines the class of the address. There are 5 IP address classes.



An IP address will always be divided into a network and host portion. In a classful addressing scheme, these divisions take place at the octet boundaries.

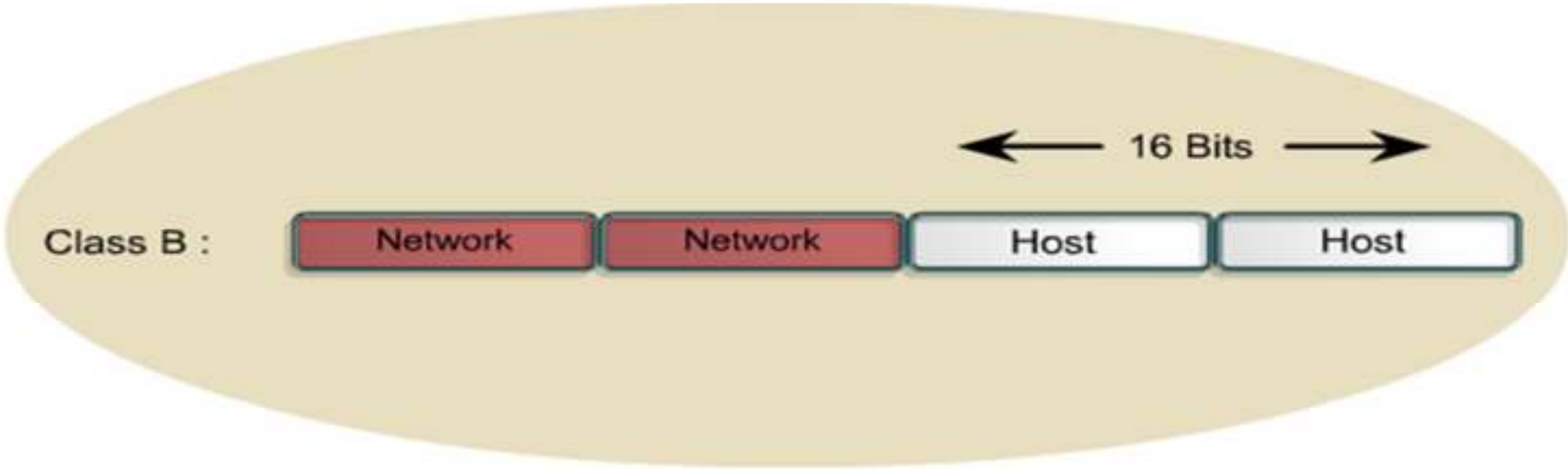
Class A Addresses

The Class A address was designed to support extremely large networks, with more than 16 million host addresses available. Class A IP addresses use only the first octet to indicate the network address. The remaining three octets provide for host addresses.



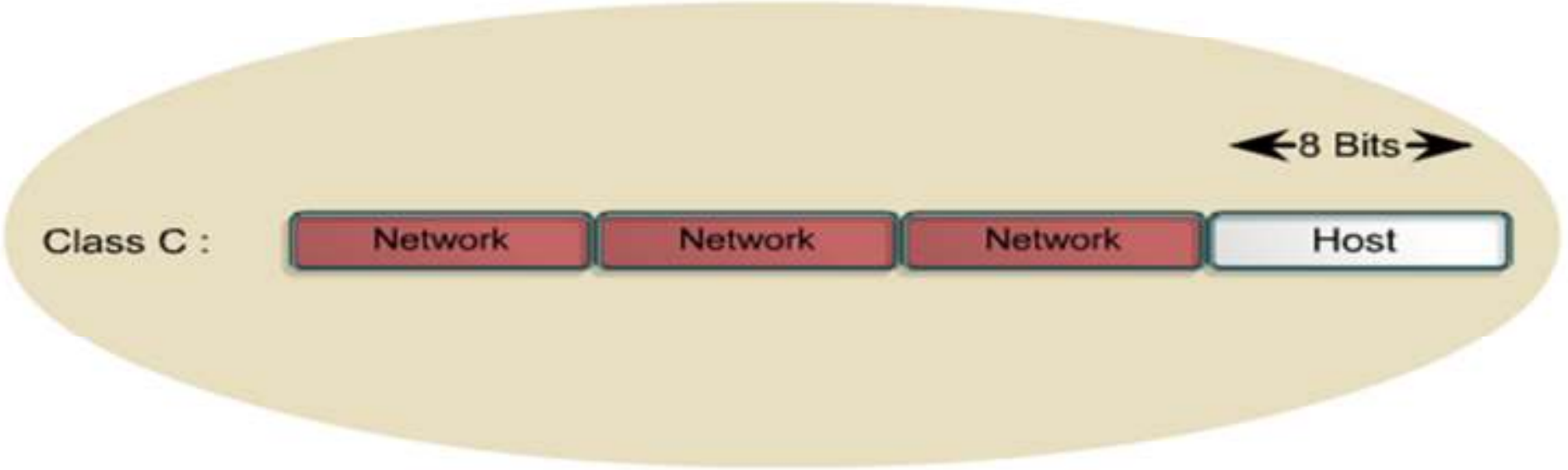
Class B Addresses

The Class B address was designed to support the needs of moderate to large-sized networks. A Class B IP address uses the first two of the four octets to indicate the network address. The other two octets specify host addresses.



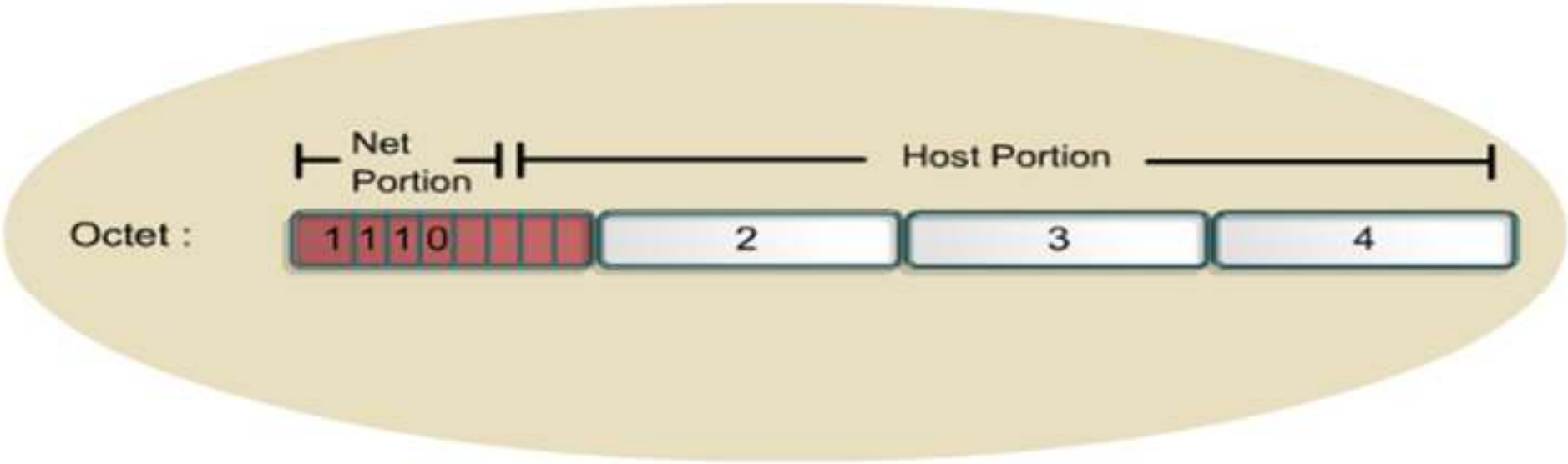
Class C Addresses

The Class C address space is the most commonly used of the original address classes. This address space was intended to support small networks with a maximum of 254 hosts.



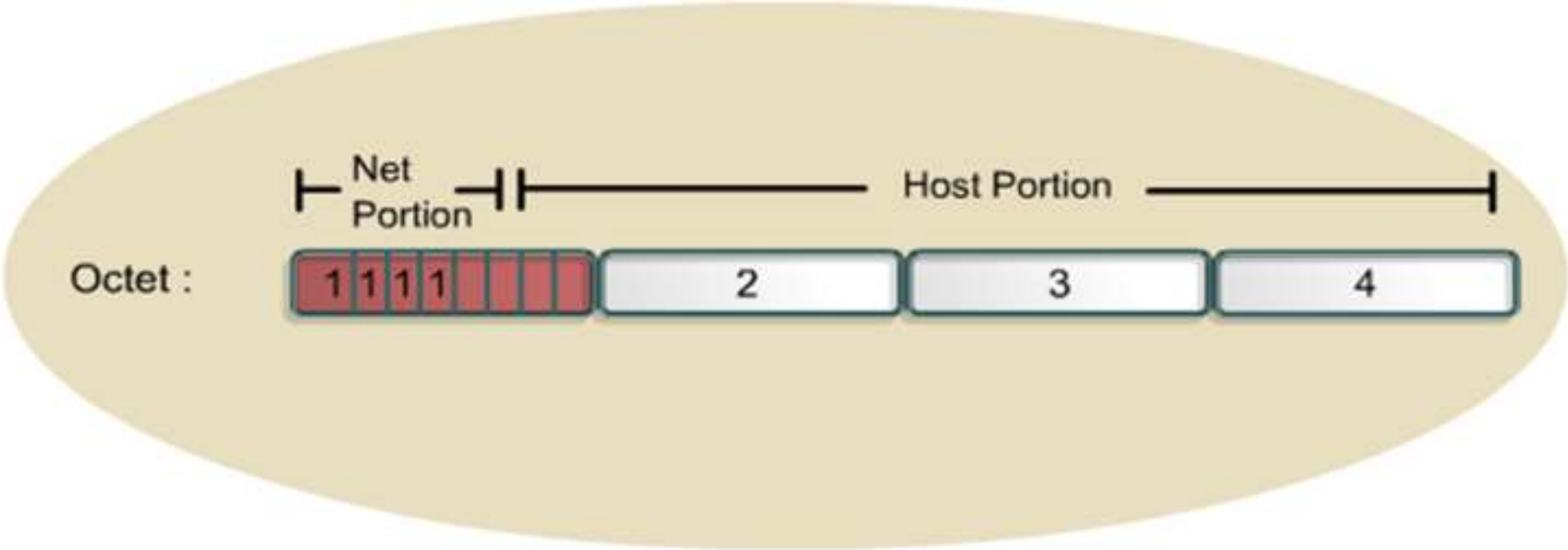
Class D Addresses

The Class D address class was created to enable multicasting in an IP address. A multicast address is a unique network address that directs packets with that destination address to predefined groups of IP addresses. Therefore, a single station can simultaneously transmit a single stream of data to multiple recipients.



Class E Addresses

A Class E address has been defined. However, the Internet Engineering Task Force (IETF) reserves these addresses for its own research. Therefore, no Class E addresses have been released for use in the Internet.



IP Address Ranges

The graphic below shows the IP address range of the first octet both in decimal and binary for each IP address class.

IP address class	IP address range (First Octet Decimal Value)
Class A	1-126 (00000001-01111110) *
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

Determine the class based on the decimal value of the first octet

* 127 (011111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

IPv4

As early as 1992, the Internet Engineering Task Force (IETF) identified two specific concerns: Exhaustion of the remaining, unassigned IPv4 network addresses and the increase in the size of Internet routing tables.

Over the past two decades, numerous extensions to IPv4 have been developed. Two of the more important of these are subnet masks and classless interdomain routing (CIDR).

With Class A and B addresses virtually exhausted, Class C addresses (12.5 percent of the total space) are left to assign to new networks.

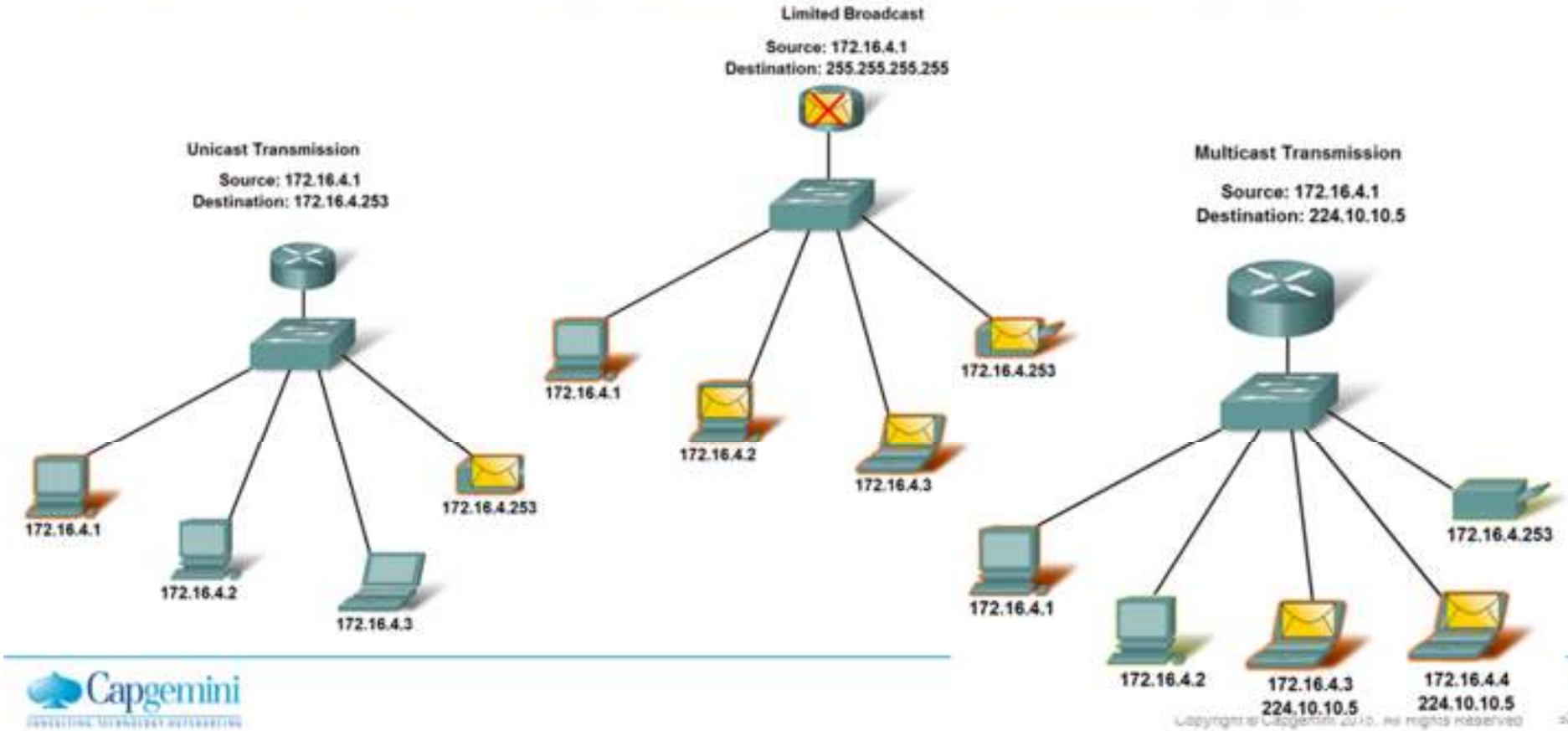
Types of Communication

In an IPv4 network, the hosts can communicate one of three different ways:

Unicast - the process of sending a packet from one host to an individual host

Broadcast - the process of sending a packet from one host to all hosts in the network

Multicast - the process of sending a packet from one host to a selected group of hosts

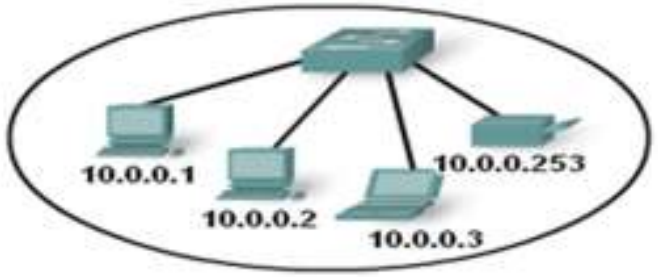


Types of Addresses

Network address - The address by which we refer to the network
Broadcast address - A special address used to send data to all hosts in the network
Host addresses - The addresses assigned to the end devices in the network

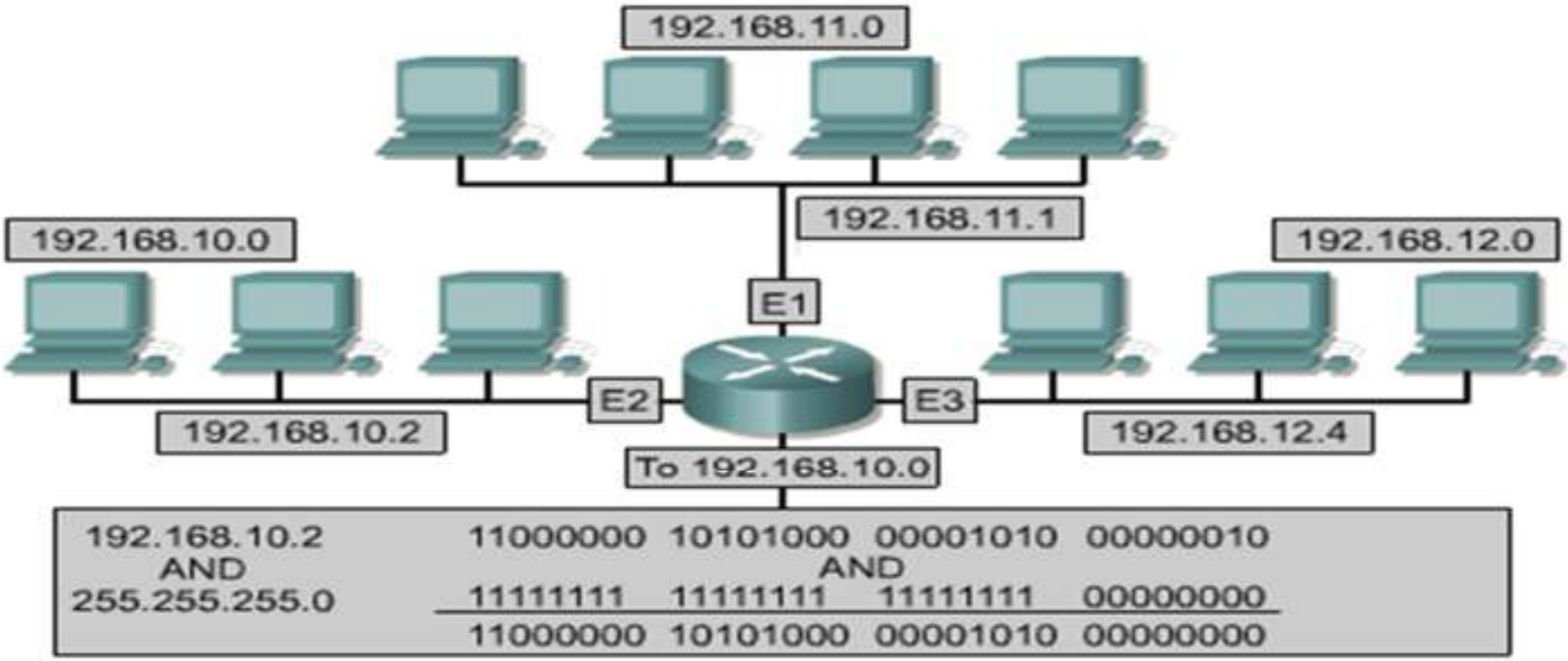
Address Types

	Network			Host
Network Address	10	0	0	0
	00001010	00000000	00000000	00000000
Broadcast Address	10	0	0	255
	00001010	00000000	00000000	11111111
Host Address	10	0	0	1
	00001010	00000000	00000000	00000001

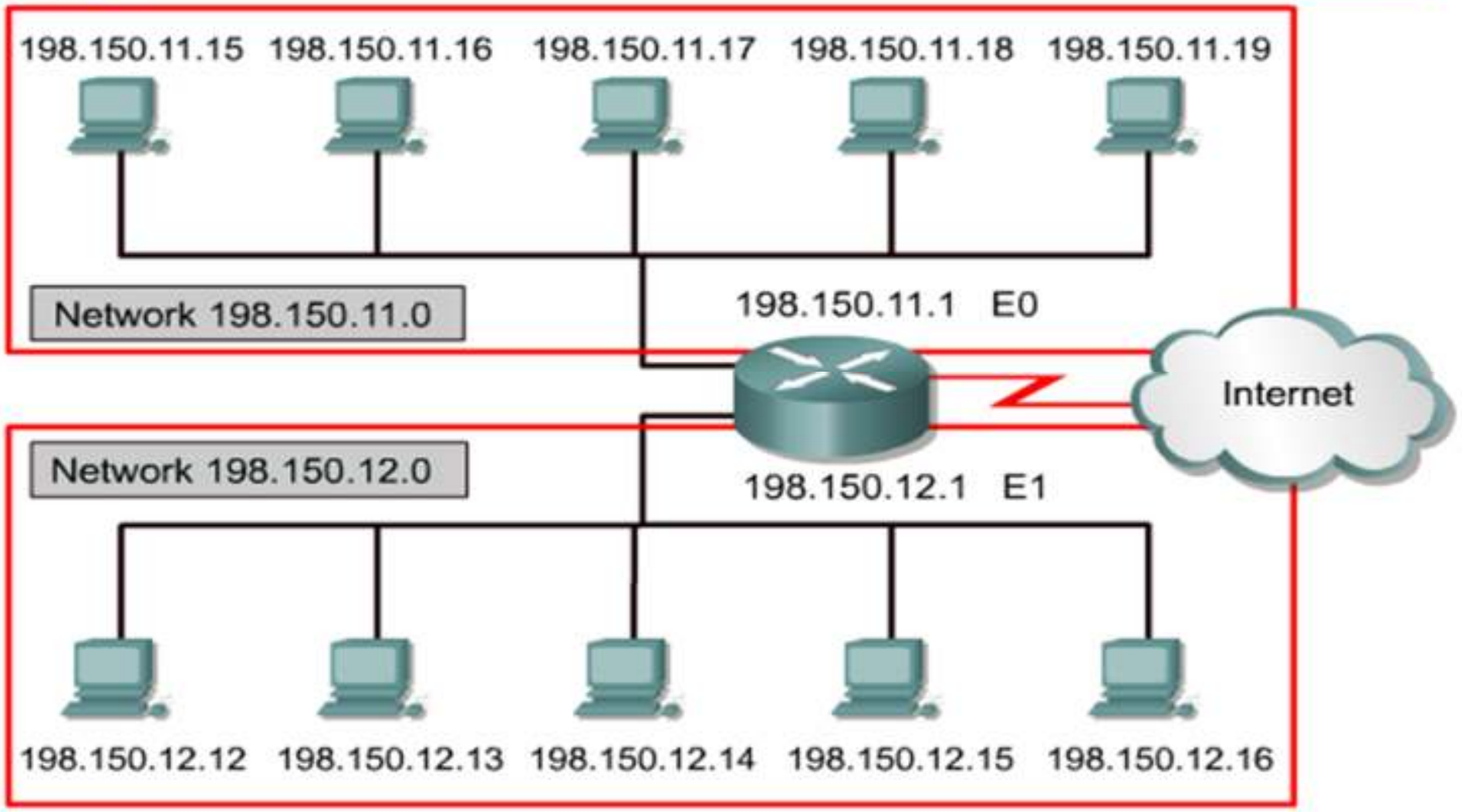


Finding the Network Address with ANDing

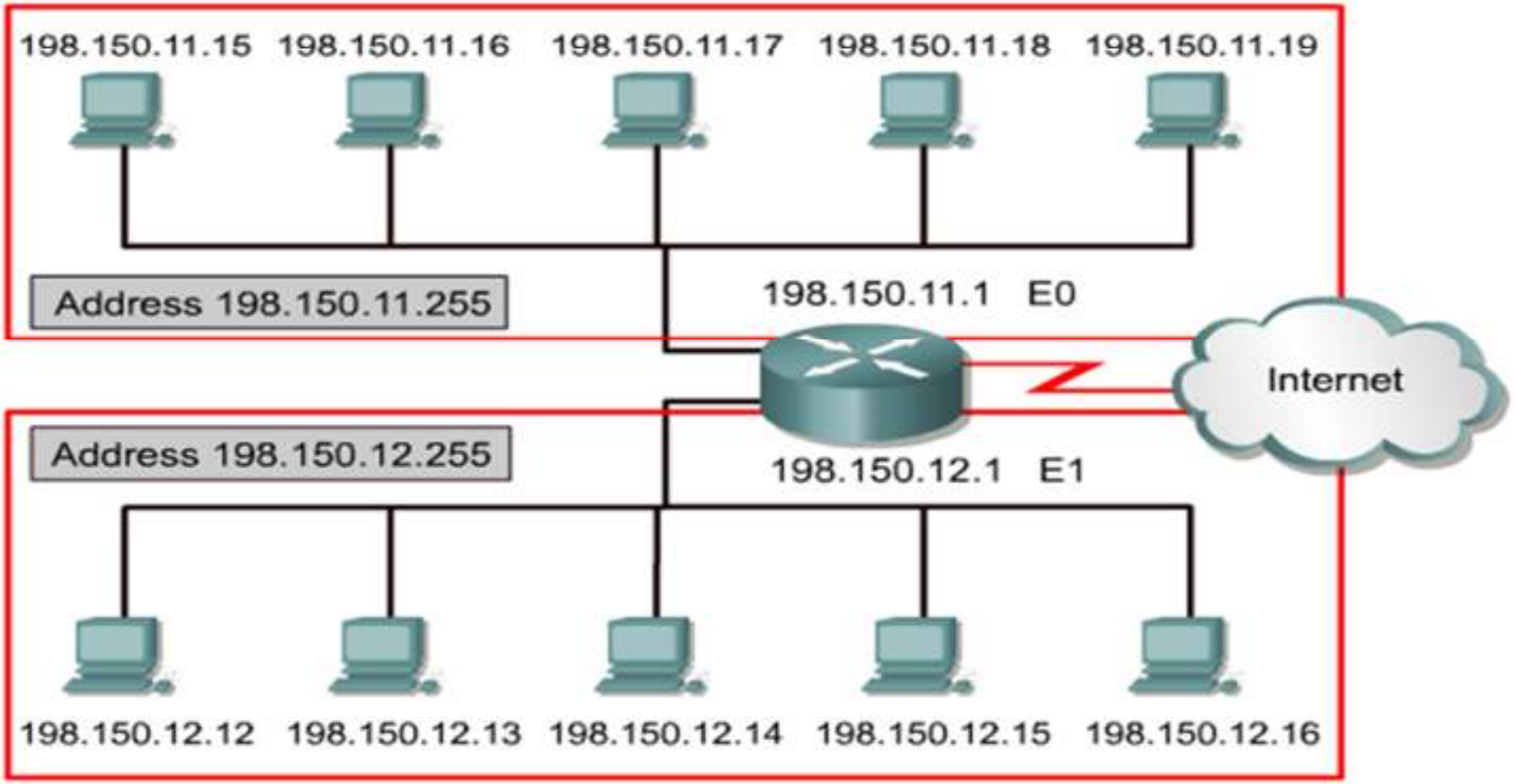
By ANDing the Host address of **192.168.10.2** with **255.255.255.0** (its network mask) we obtain the network address of **192.168.10.0**



Network Address



Broadcast Address



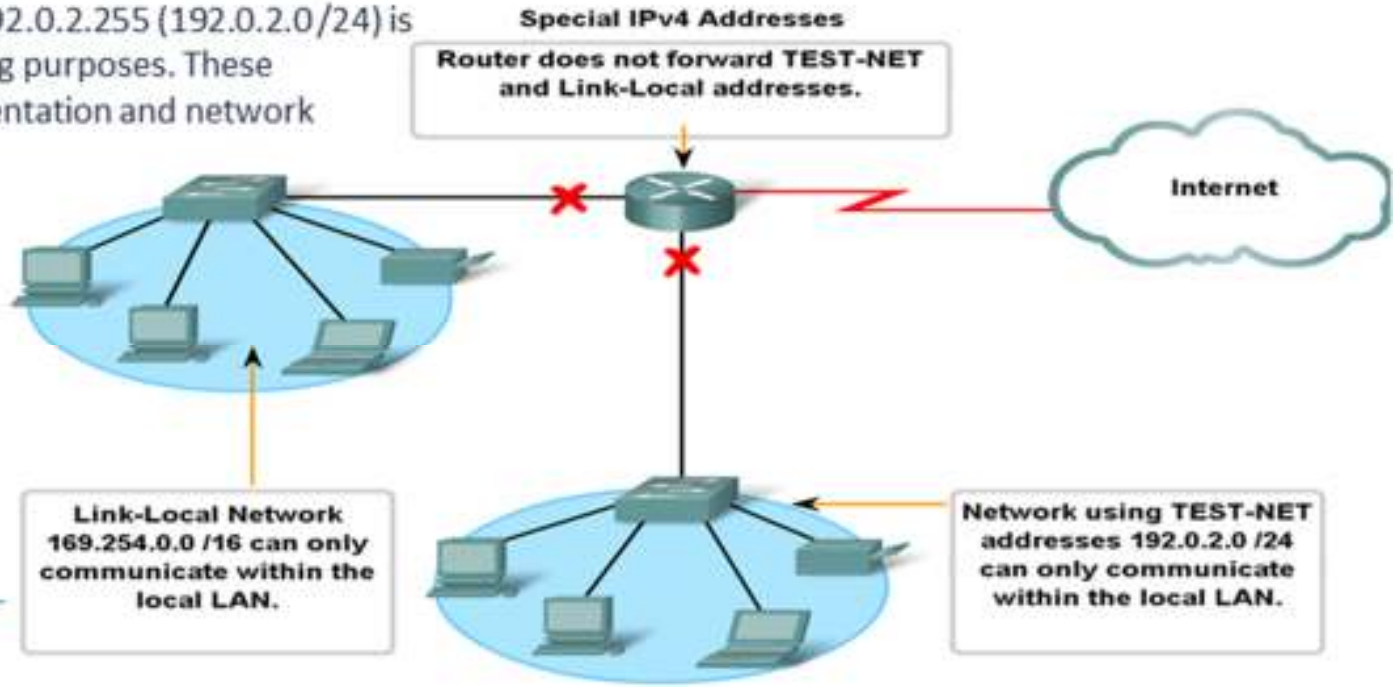
Special IPv4 Addresses

Link-Local Addresses

IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.

TEST-NET Addresses

The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples



Public IP Addresses

Unique addresses are required for each device on a network.

Originally, an organization known as the Internet Network Information Center (InterNIC) handled this procedure.

InterNIC no longer exists and has been succeeded by the Internet Assigned Numbers Authority (IANA).

No two machines that connect to a public network can have the same IP address because public IP addresses are global and standardized.

All machines connected to the Internet agree to conform to the system.

Public IP addresses must be obtained from an Internet service provider (ISP) or a registry at some expense.

Who Assigns the Different Address ?

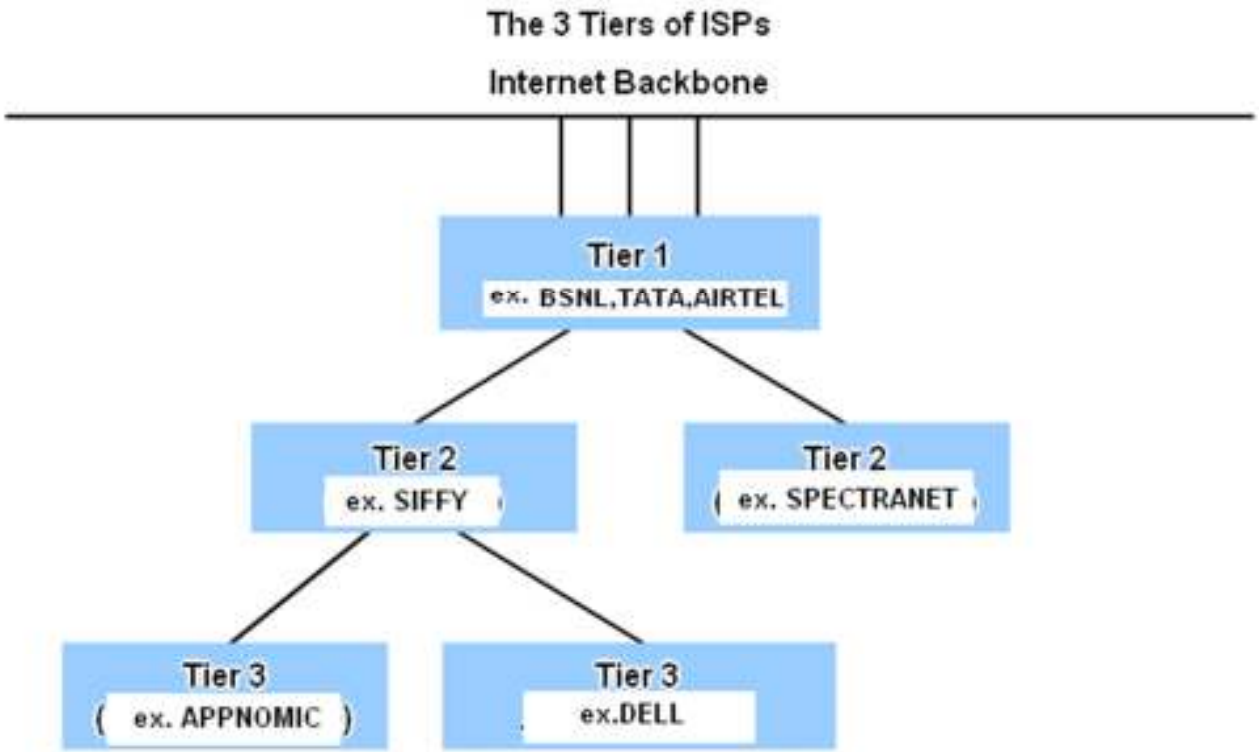
A company or organization that wishes to have network hosts accessible from the Internet must have a block of public addresses assigned. The use of these public addresses is regulated and the company or organization must have a block of addresses allocated to it. This is true for IPv4, IPv6, and multicast addresses.

Internet Assigned Numbers Authority (IANA) (http://www.iana.net) is the master holder of the IP addresses.

Entities that Oversee IP Address Allocation

Global	IANA				
Regional Internet Registries	AfriNIC Africa Region	APNIC Asia/ Pacific Region	LACNIC Latin America And Caribbean Region	ARIN North America Region	RIPE NCC Europe, Middle East, Central Asia Region

ISPs



Private IP Addresses

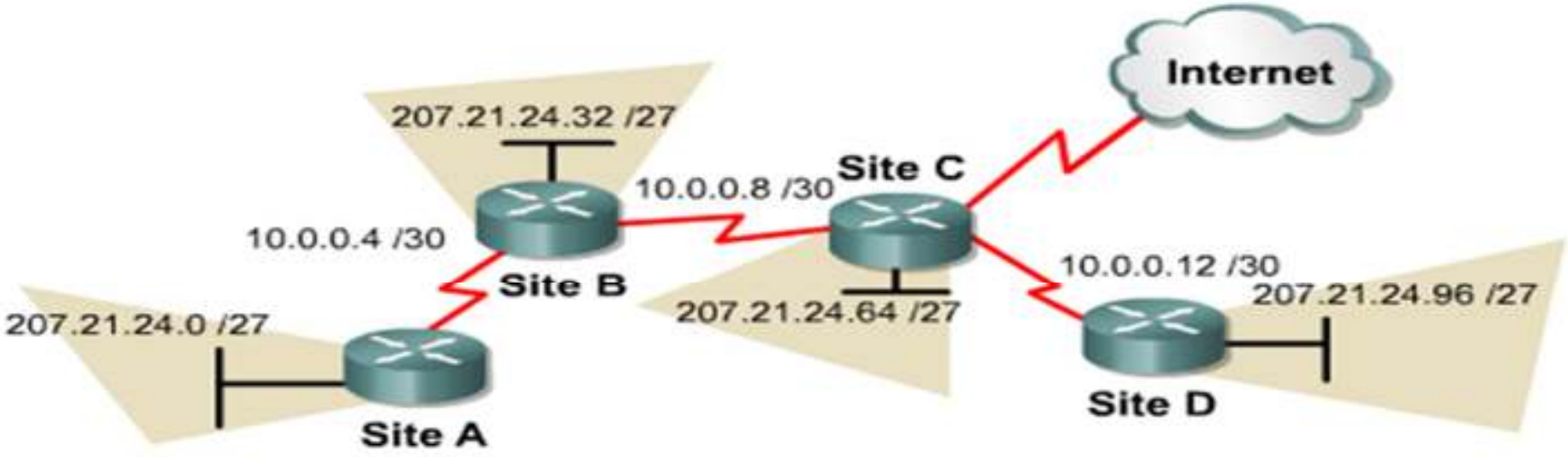
Private IP addresses are another solution to the problem of the impending exhaustion of public IP addresses. As mentioned, public networks require hosts to have unique IP addresses.

However, private networks that are not connected to the Internet may use any host addresses, as long as each host within the private network is unique.

Class	RFC 1918 internal address range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Mixing Public and Private IP Addresses

Private IP addresses can be intermixed, as shown in the graphic, with public IP addresses. This will conserve the number of addresses used for internal connections. Connecting a network using private addresses to the Internet requires translation of the private addresses to public addresses. This translation process is referred to as Network Address Translation (NAT).



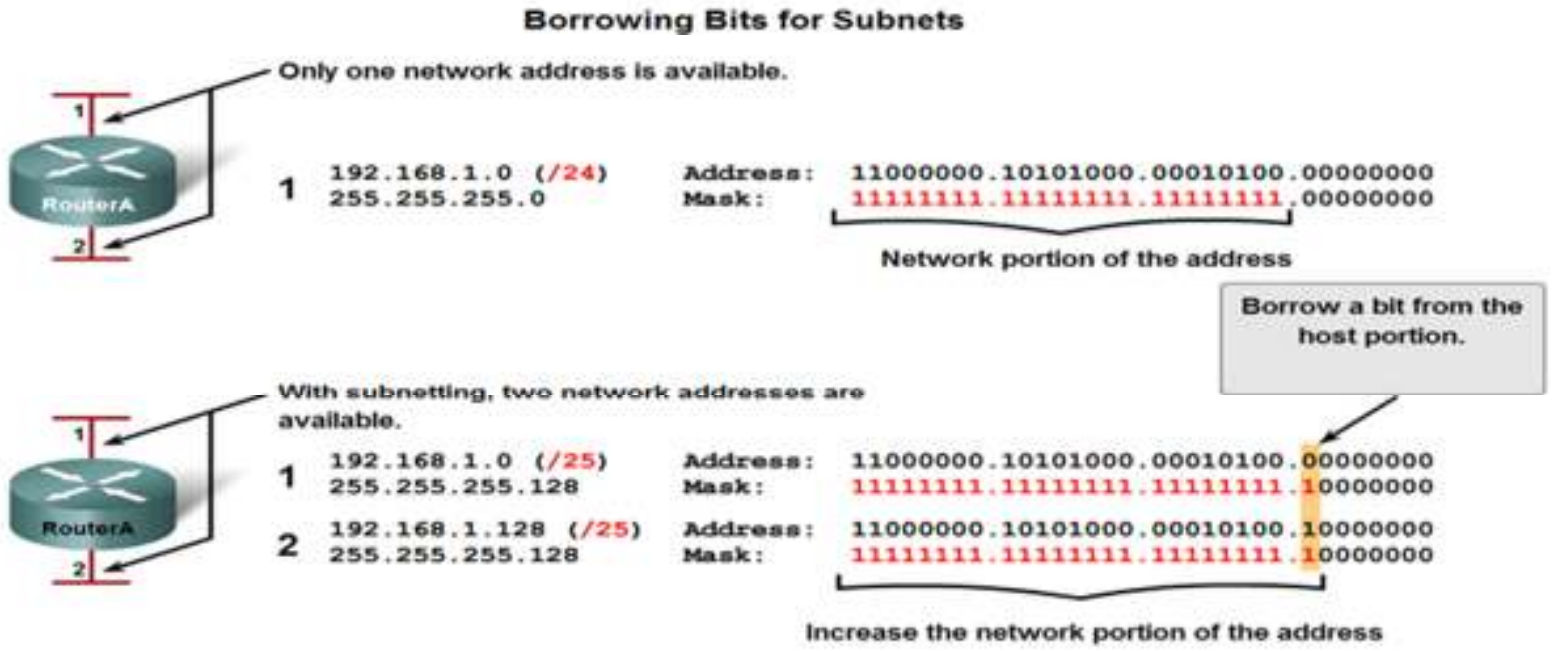
Introduction to Subnetting

Subnetting a network means to use the subnet mask to divide the network and break a large network up into smaller, more efficient and manageable segments, or subnets.

With subnetting, the network is not limited to the default Class A, B, or C network masks and there is more flexibility in the network design.

Subnet addresses include the network portion, plus a subnet field and a host field. The ability to decide how to divide the original host portion into the new subnet and host fields provides addressing flexibility for the network administrator.

Basic Subnetting



Addressing Scheme: Example of 2 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Basic Subnetting

Borrowing Bits for Subnets

-	192.168.1.0 (/24) 255.255.255.0	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.00000000
0	192.168.1.0 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.11000000
1	192.168.1.64 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.01000000 11111111.11111111.11111111.11000000
2	192.168.1.128 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.10000000 11111111.11111111.11111111.11000000
3	192.168.1.192 (/26) 255.255.255.192	Address: Mask:	11000000.10101000.00010100.11000000 11111111.11111111.11111111.11000000

Two bits are borrowed to provide four subnets.

Unused address in this example.

A 1 in these positions in the mask means that these values are part of the network address.

More subnets are available, but fewer addresses are available per subnet.

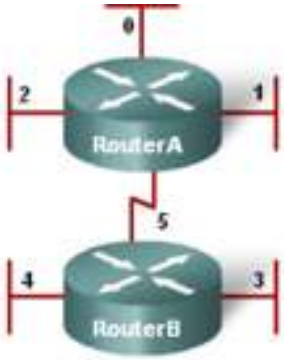
Addressing Scheme: Example of 4 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129 - 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

Basic Subnetting

Borrowing Bits for Subnets

Start with this address	-	192.168.1.0 (/24) 255.255.255.0	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.00000000
Make 8 subnets	0	192.168.1.0 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.00000000 11111111.11111111.11111111.11100000
	1	192.168.1.32 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.00100000 11111111.11111111.11111111.11100000
	2	192.168.1.64 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.01000000 11111111.11111111.11111111.11100000
	3	192.168.1.96 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.01100000 11111111.11111111.11111111.11100000
	4	192.168.1.128 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.10000000 11111111.11111111.11111111.11100000
	5	192.168.1.160 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.10100000 11111111.11111111.11111111.11100000
	6	192.168.1.192 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.11000000 11111111.11111111.11111111.11100000
	7	192.168.1.224 (/27) 255.255.255.224	Address: Mask:	11000000.10101000.00010100.11100000 11111111.11111111.11111111.11100000



Three bits are borrowed to provide eight subnets.

Basic Subnetting

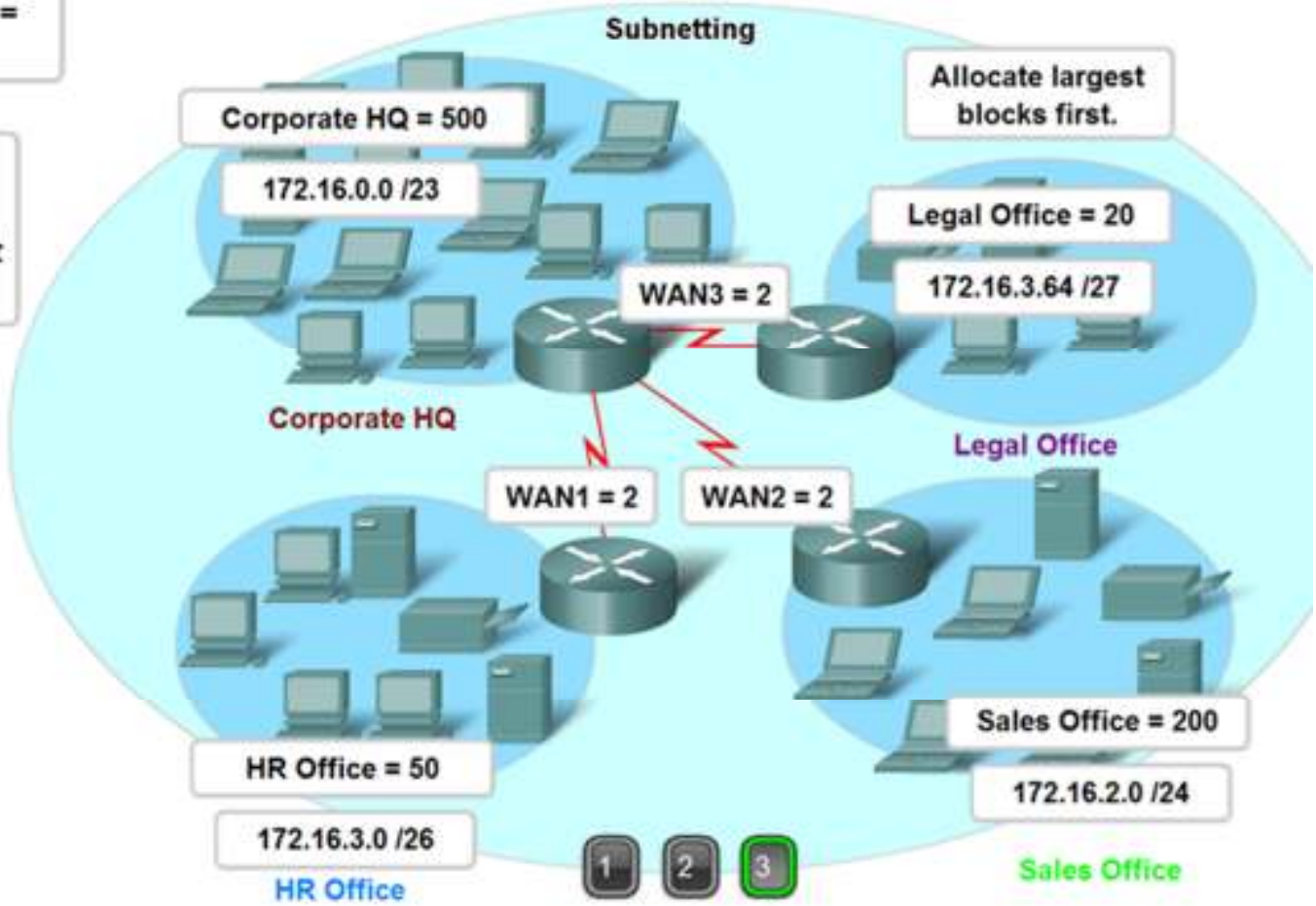
Addressing Scheme: Example of 6 networks

Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/27	192.168.1.1 - 192.168.1.30	192.168.1.31
1	192.168.1.32/27	192.168.1.33 - 192.168.1.62	192.168.1.63
2	192.168.1.64/27	192.168.1.65 - 192.168.1.94	192.168.1.95
3	192.168.1.96/27	192.168.1.97 - 192.168.1.126	192.168.1.127
4	192.168.1.128/27	192.168.1.129 - 192.168.1.158	192.168.1.159
5	192.168.1.160/27	192.168.1.161 - 192.168.1.190	192.168.1.191
6	192.168.1.192/27	192.168.1.193 - 192.168.1.222	192.168.1.223
7	192.168.1.224/27	192.168.1.225 - 192.168.1.254	192.168.1.255

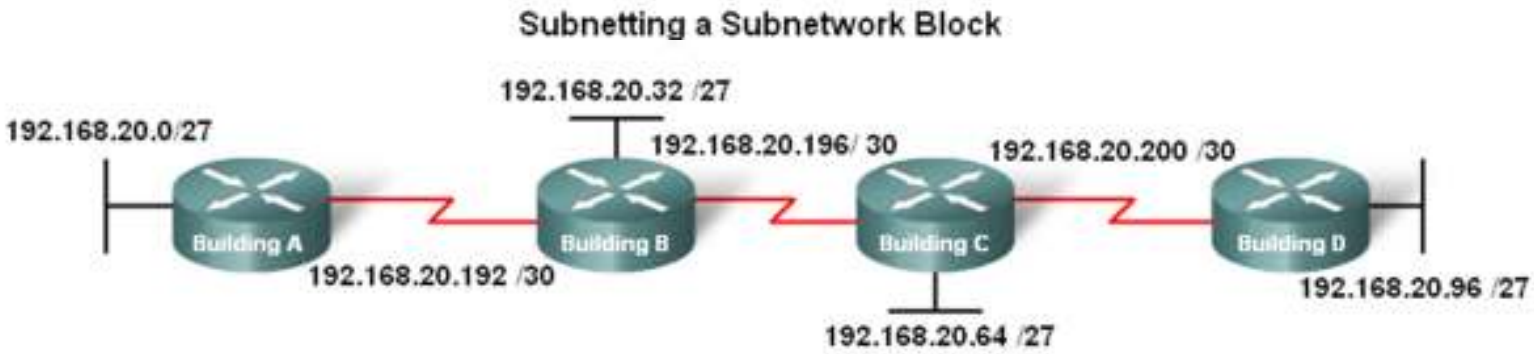
Basic Subnetting

In this example, the total number of hosts in the corporate network = 800 hosts.

Choose a block of addresses to accommodate the hosts.172.16.0.0 /22 = 1022 host addresses.



Subnet - Subnetting a Subnet

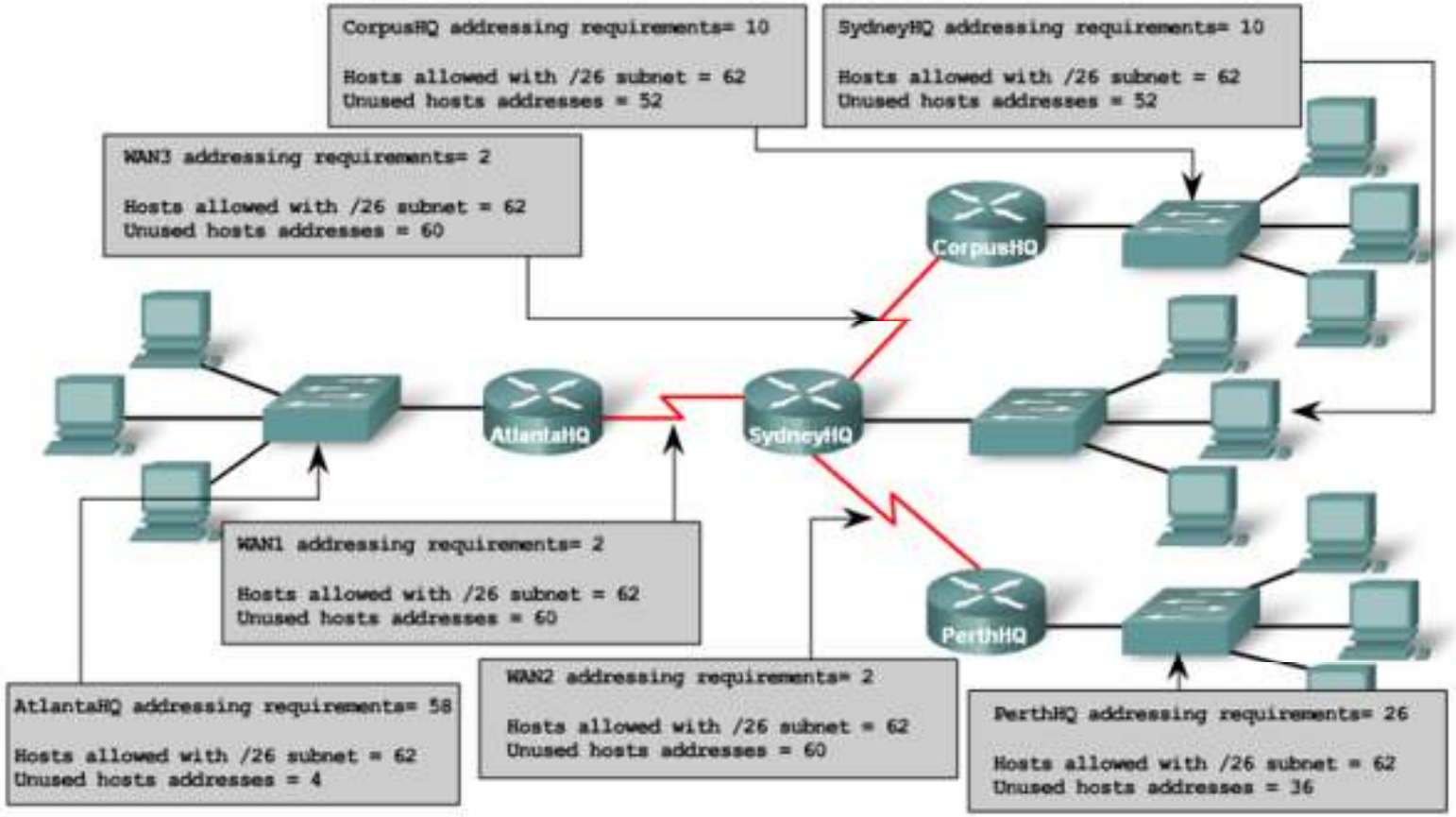


Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.20/30

Subnet - Subnetting a Subnet

Network Requirements: Using standard subnetting would be inefficient.



Subnet - Subnetting a Subnet

	Actual Requirements	Total Wasted Addresses
AtlantaHQ	58 host addresses	4 addresses
PerthHQ	26 host addresses	36 addresses
SydneyHQ	10 host addresses	52 addresses
CorpusHQ	10 host addresses	52 addresses
WAN links	2 host addresses (each)	60 addresses

Name -required addresses	Subnet address	Address range	Broadcast Address	Network /prefix
AtlantaHQ - 58	192.168.15.0	.1 - 62	.63	192.168.15.0 /26
PerthHQ - 28	192.168.15.64	.65 - .94	.95	192.168.15.64 /27
SydneyHQ - 10	192.168.15.96	.97- .110	.111	192.168.15.96 /28
CorpusHQ - 10	192.168.15.112	.113 - .126	.127	192.168.15.112 /28
WAN1 - 2	192.168.15.128	.129 - .130	.131	192.168.15.128 /30
WAN2 - 2	192.168.15.132	.133 - 134	.135	192.168.15.132 /30
WAN3 - 2	192.168.15.136	.137 - .138	.139	192.168.15.136 /30

The networking problem is solved

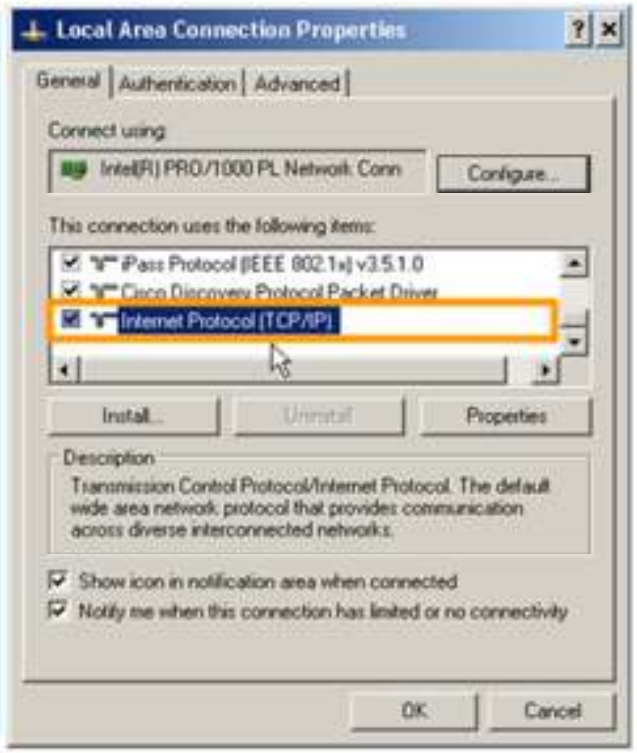
Testing Network Layer - Ping

Ping is a utility for testing IP connectivity between hosts. Ping sends out requests for responses from a specified host address. Ping uses a Layer 3 protocol that is a part on the TCP/IP suite called Internet Control Message Protocol (ICMP). Ping uses an ICMP Echo Request datagram.

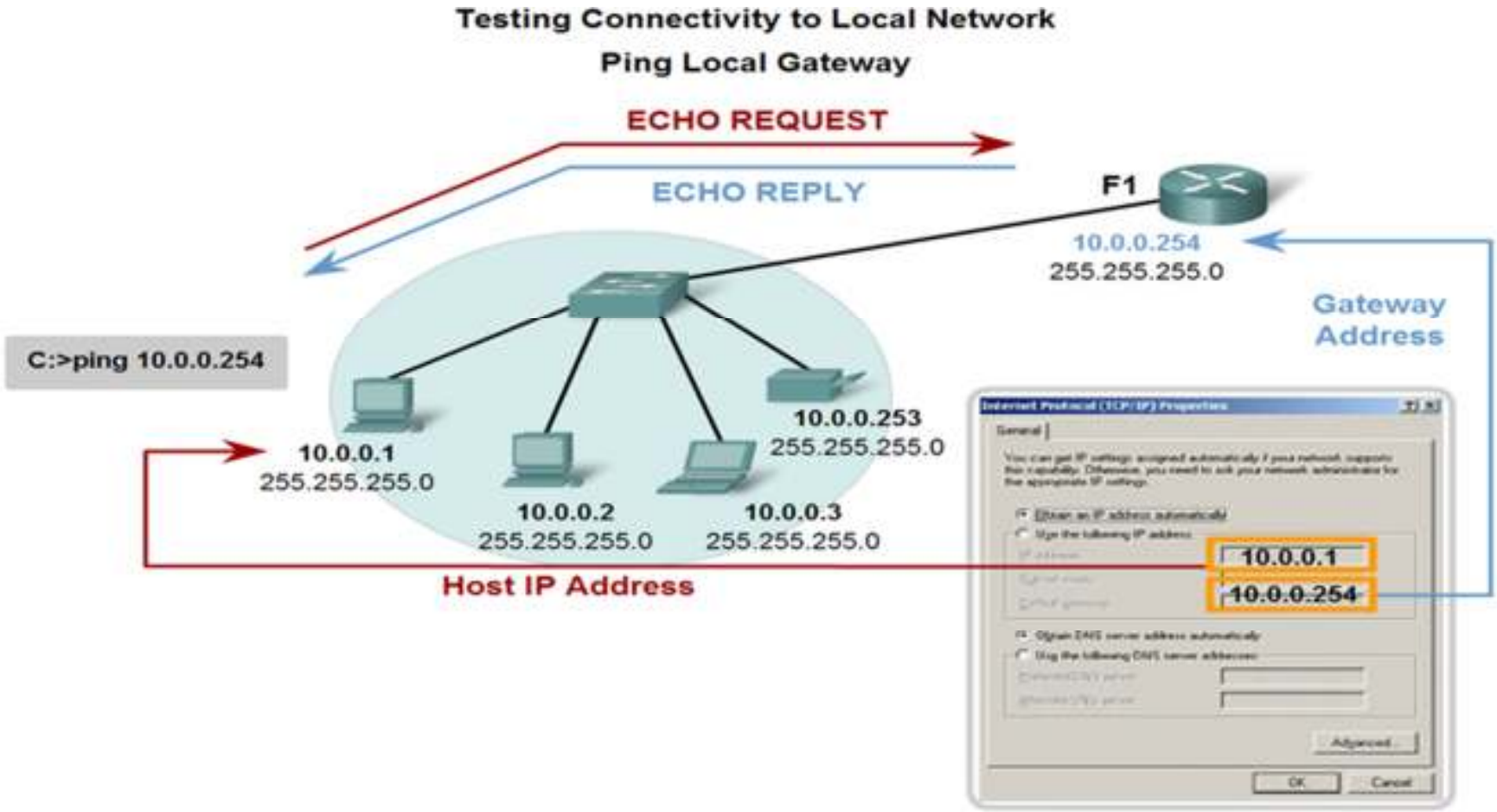
Testing Local TCP/IP Stack

Pinging the local host confirms that TCP/IP is installed and working on the local host.

Pinging 127.0.0.1 causes a device to ping itself.



Testing Network Layer – Ping Gateway

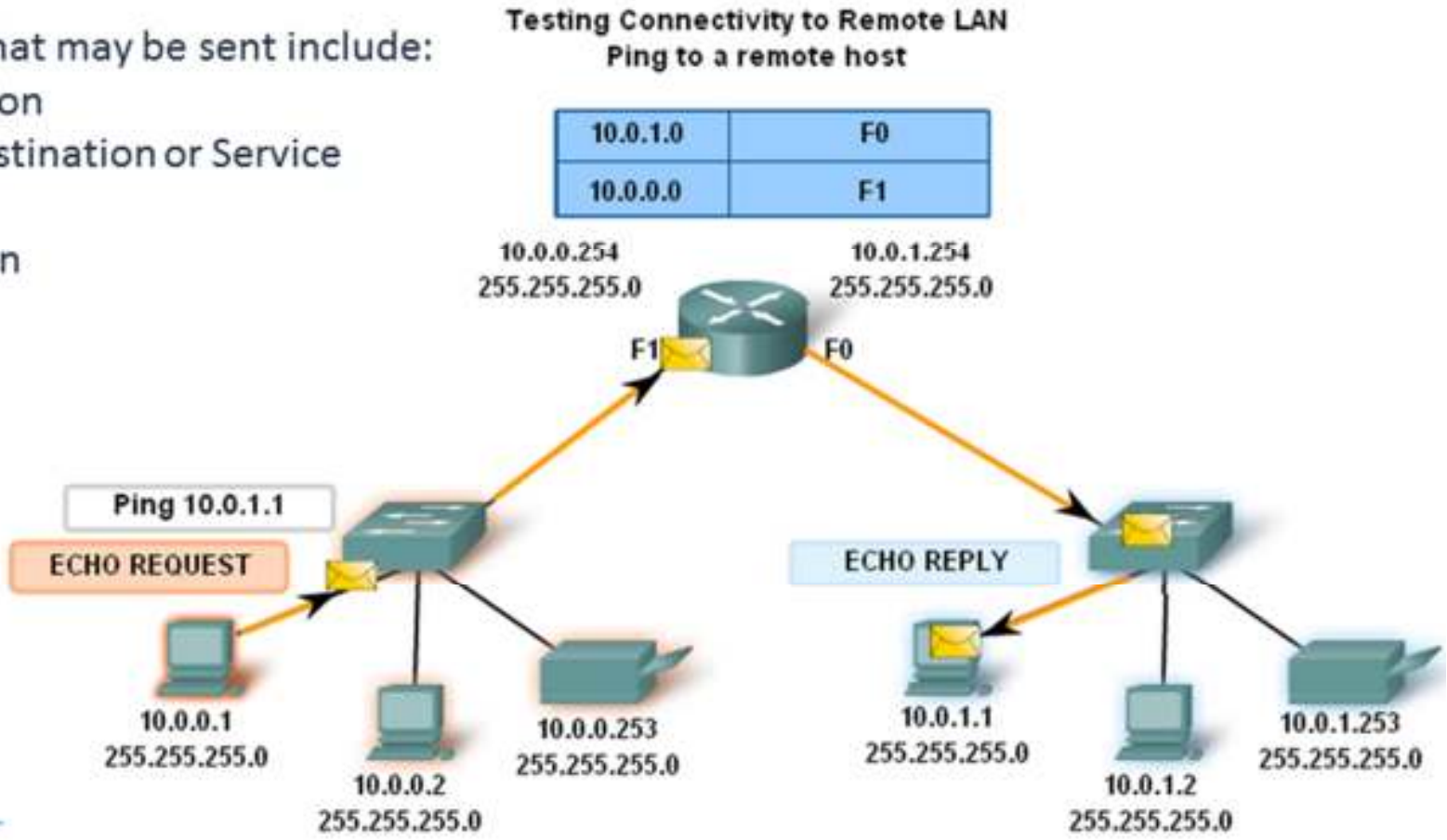


Ping Remote Host – Testing connectivity to Remote LAN

The types of ICMP messages - and the reasons why they are sent - are extensive. We will discuss some of the more common messages.

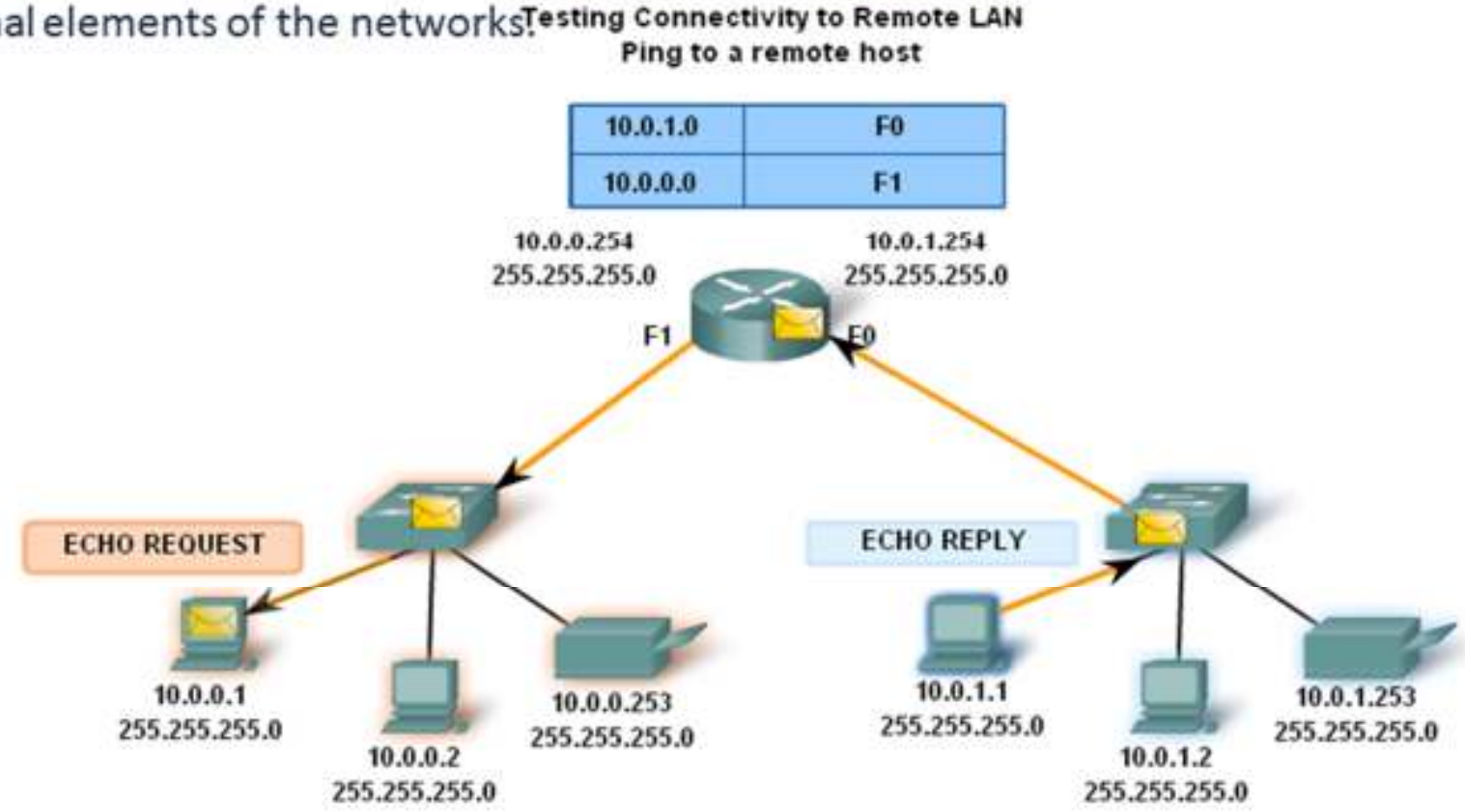
ICMP messages that may be sent include:

- Host conformation
- Unreachable Destination or Service
- Time exceeded
- Route redirection
- Source quench



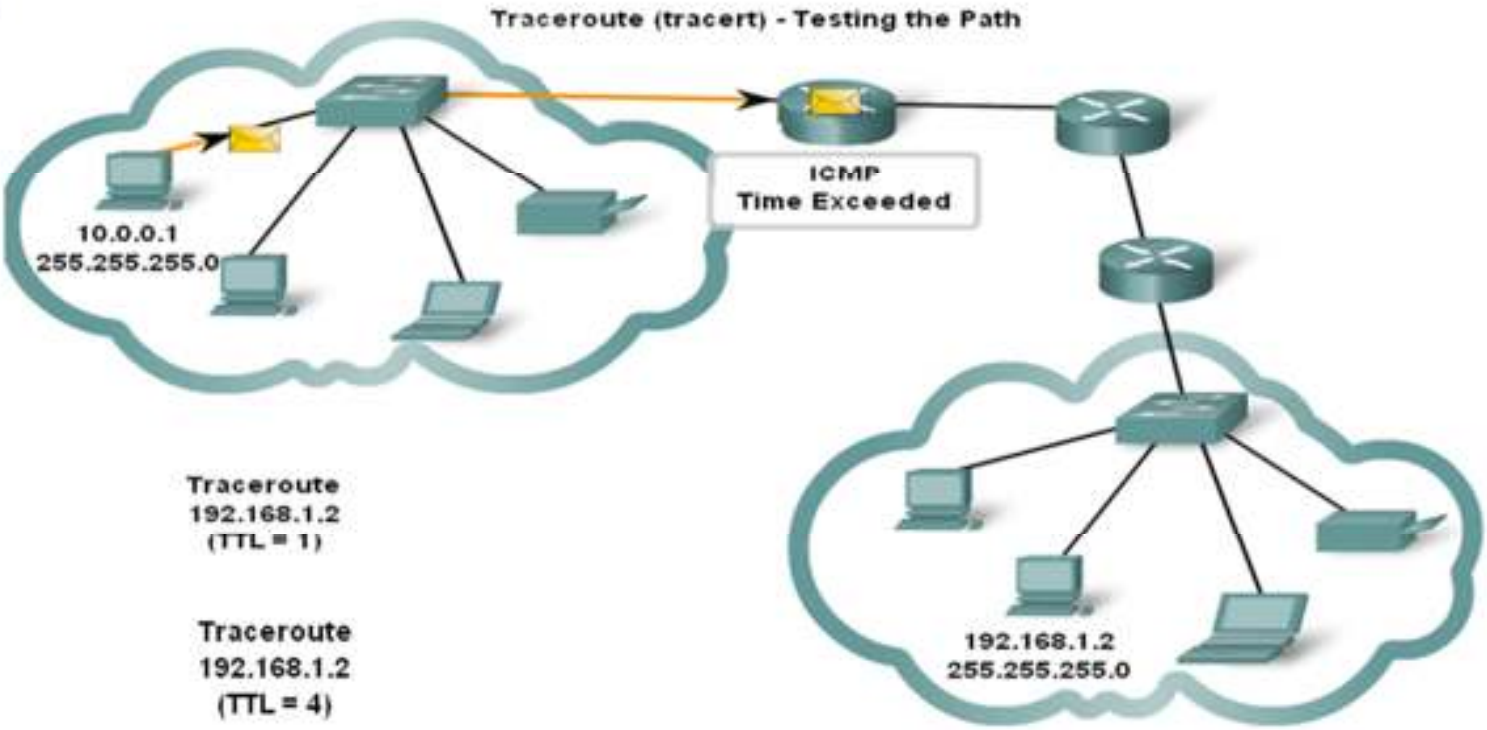
Ping Remote Host – Testing connectivity to Remote LAN

Remember, many network administrators limit or prohibit the entry of ICMP datagram's into the corporate network. Therefore, the lack of a ping response could be due to security restrictions and not because of non-operational elements of the networks.



Traceroute (tracert) –Testing the Path

Ping is used to indicate the connectivity between two hosts. Traceroute (tracert) is a utility that allows us to observe the path between these hosts. The trace generates a list of hops that were successfully reached along the path.



OSI Model

OSI Model & TCP/IP Model

OSI

Open System Interconnection. International standardization program created by ISO (International Organization for Standardization) and ITU-T (international Telecommunication Union) to develop standards for data networking that facilitate multi vendor equipment interoperability

TCP/IP

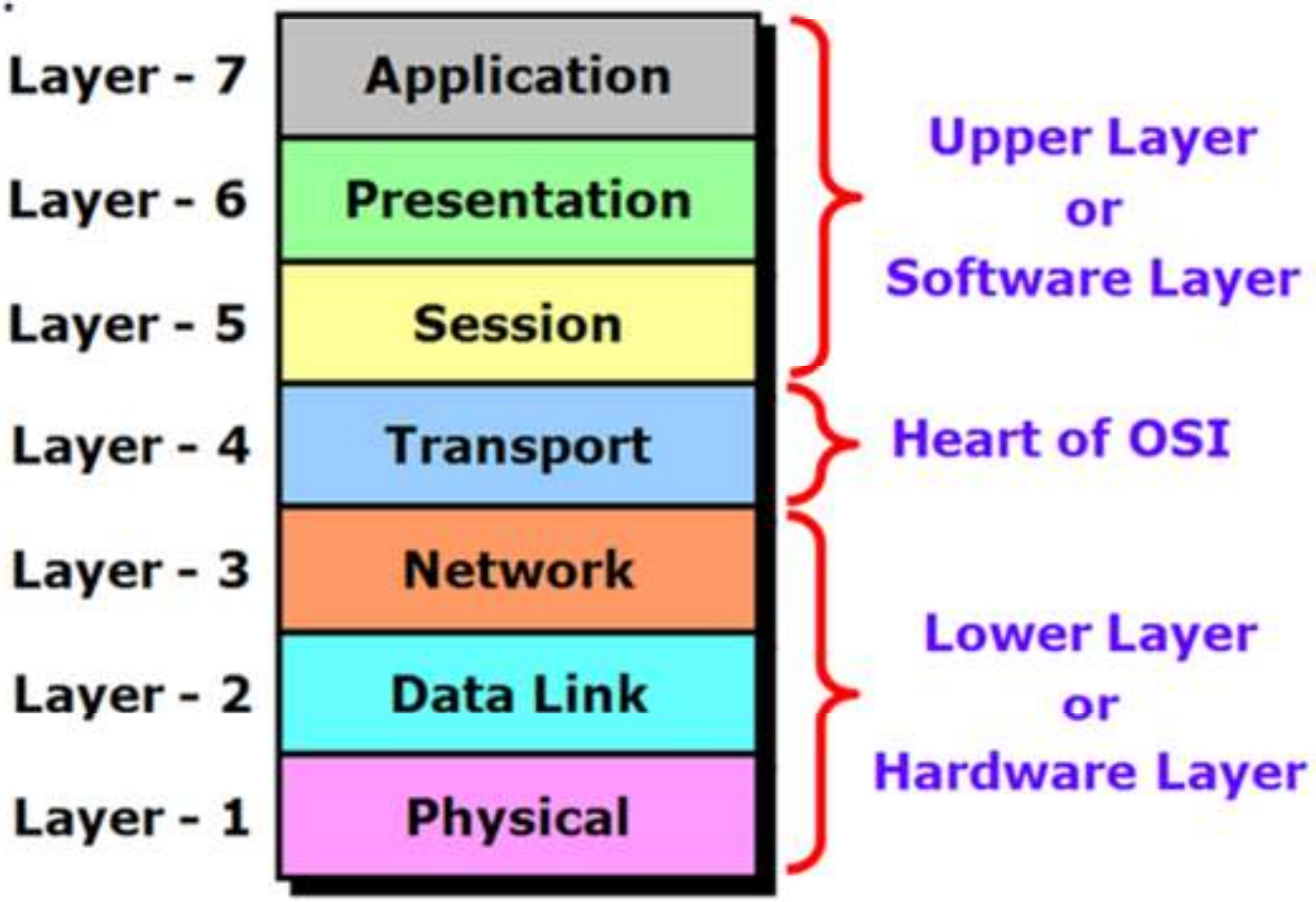
(Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

PROTOCOL

Set of rules governing communications.

Layers with OSI Model

OSI Layer:



Layers with OSI Model

Application Layer:

Application Layer is responsible for providing Networking Services to the user. It is also known as Desktop Layer. Identification of Services is done using Port Numbers.

Ports are Entry and Exit Points to the Layer

Total No. Ports	**0 – 65535**
Reserved Ports	**0 – 1023**
Open Client Ports	**1024 – 65535**

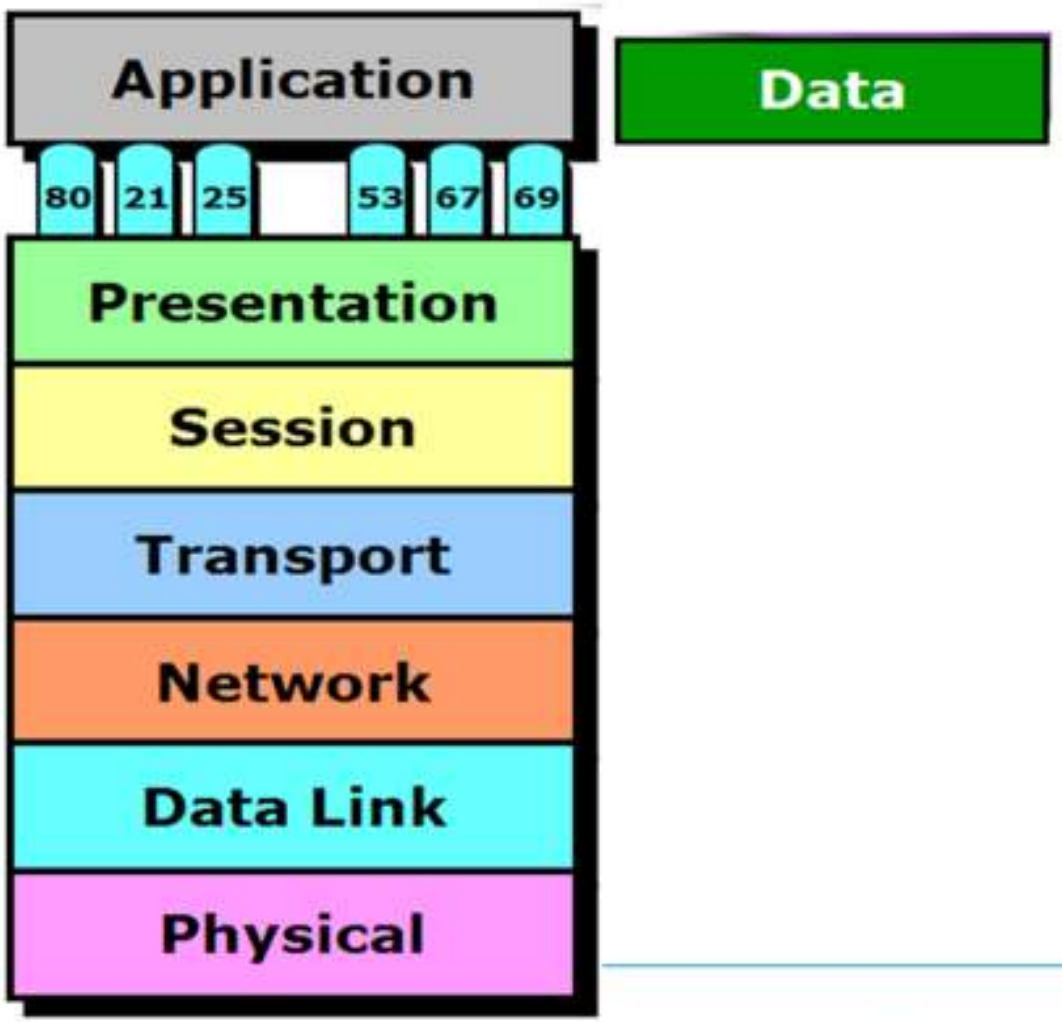
Layers with OSI Model

Examples of Network Services:

Service	Port No.
HTTP	80
FTP	21
SMTP	25
TELNET	23
TFTP	69

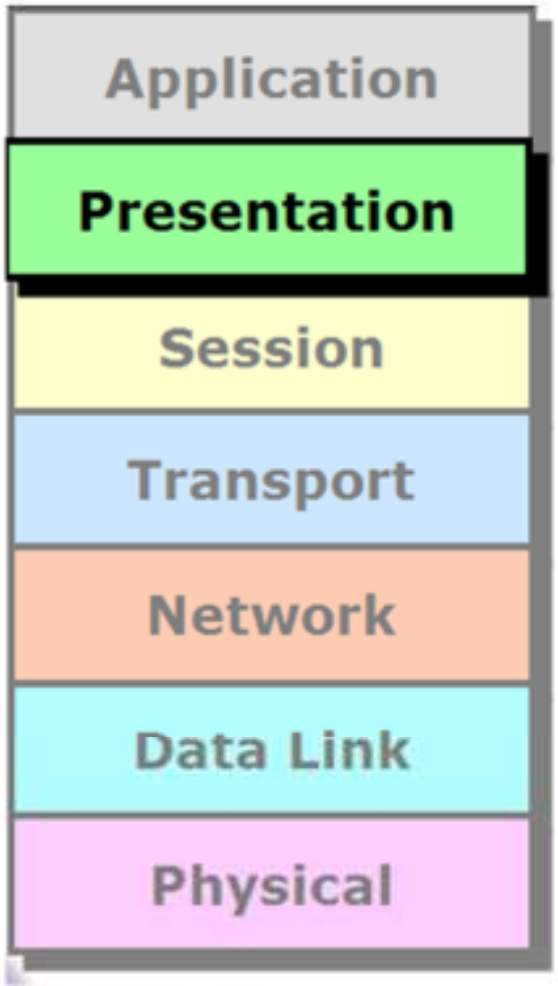
Layers with OSI Model

Data Flow from Application Layer:



Layers with OSI Model

Presentation Layer:



Presentation Layer is responsible for converting data into standard format.

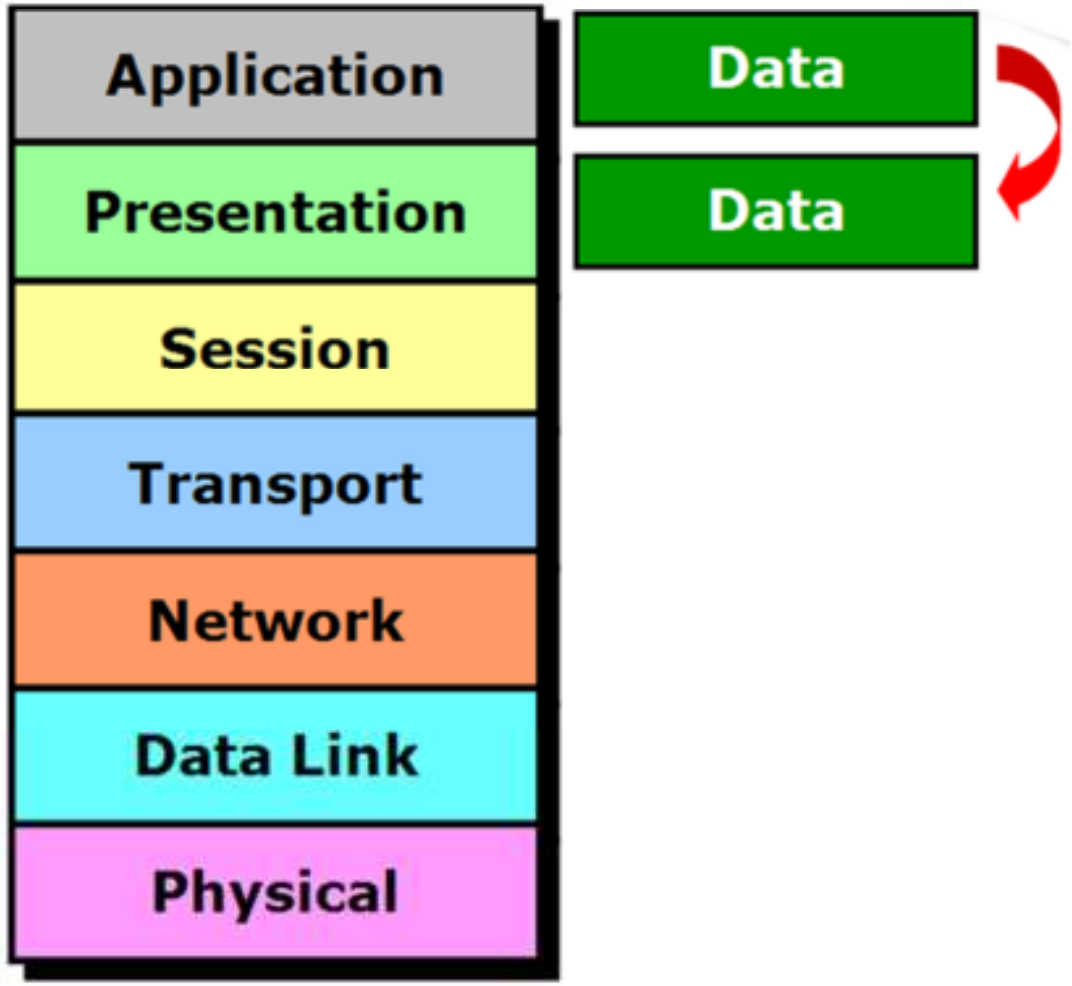
Examples : ASCII, EBCDIC, JPEG, MPEG, BMP, MIDI, WAV, MP3

Following tasks are perform at Presentation layer :

Encoding – Decoding
Encryption – Decryption
Compression – Decompression

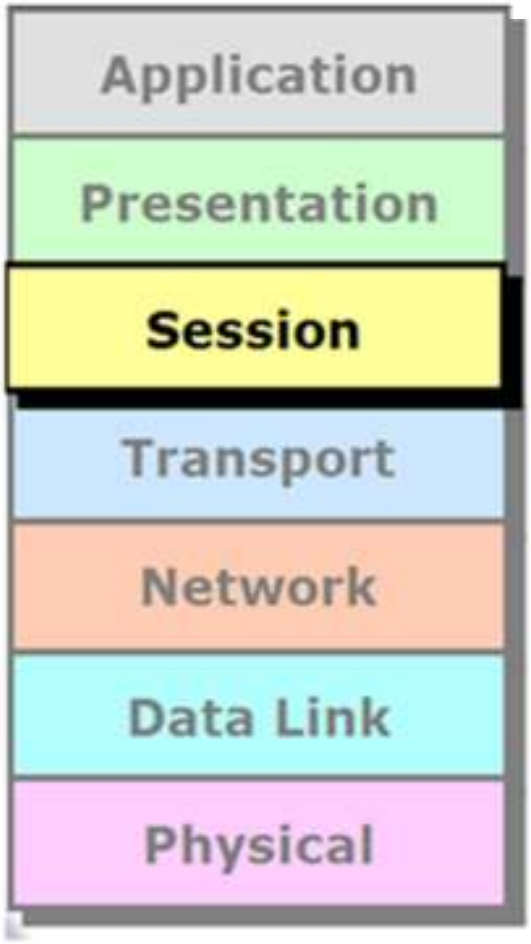
Layers with OSI Model

Data Flow from Presentation Layer:



Layers with OSI Model

Session Layer:



Session Layer is responsible for establishing, maintaining and terminating session.

Session ID works at Session Layer.

Examples :

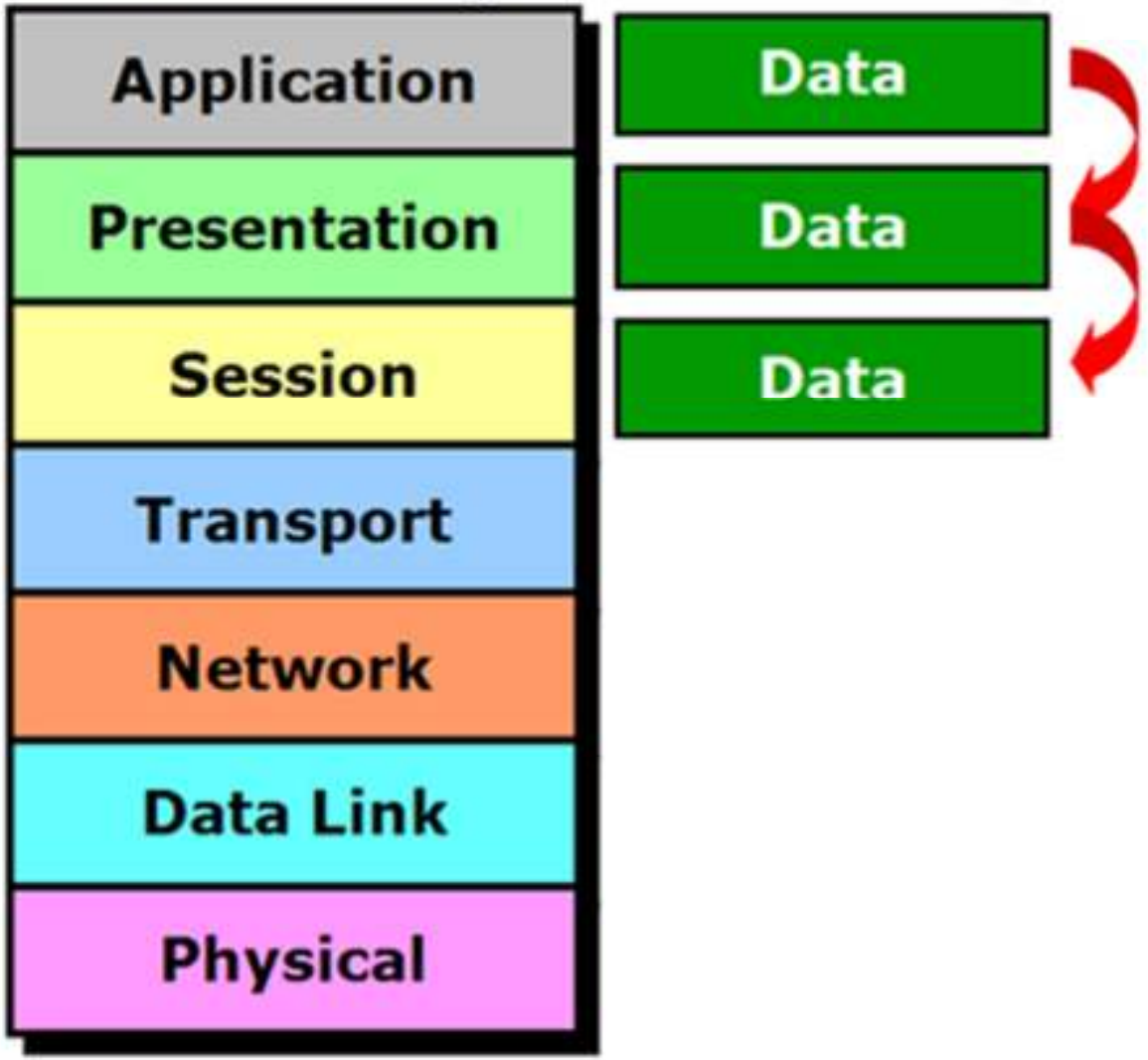
RPC → Remote Procedure Call

SQL → Structured Query Language

NFS → Network File System

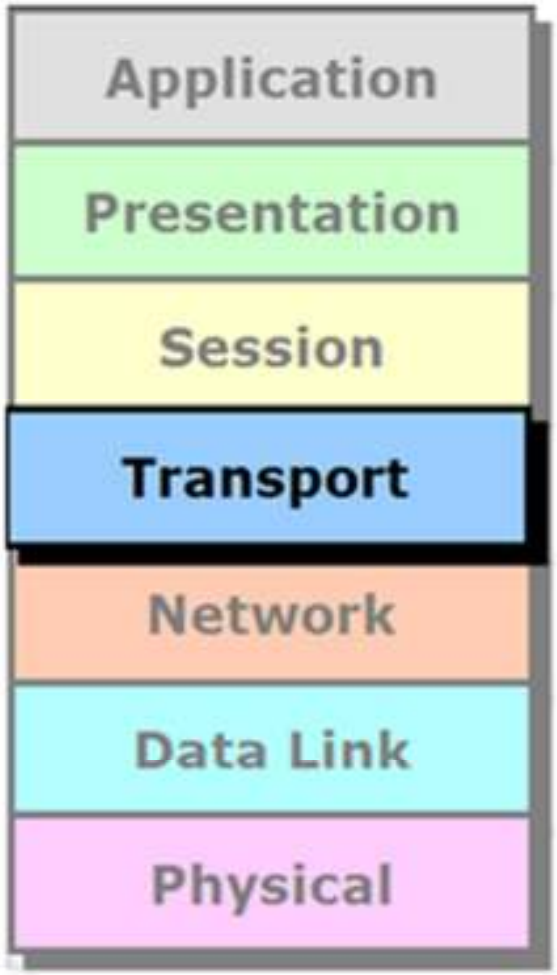
Layers with OSI Model

Data Flow from Session Layer:



Layers with OSI Model

Transport Layer:

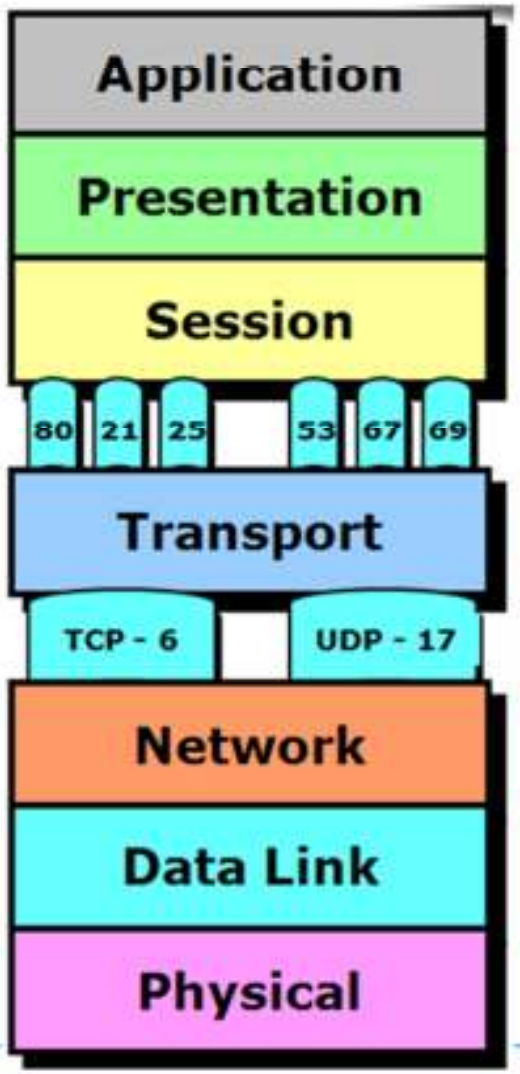


Transport Layer is responsible for end-to-end connectivity. It is also known as the heart of OSI Layers. Following tasks are performed at the Transport Layer : -

- **Identifying Service**
- **Multiplexing & De-multiplexing**
- **Segmentation**
- **Sequencing & Reassembling**
- **Error Correction**
- **Flow Control**

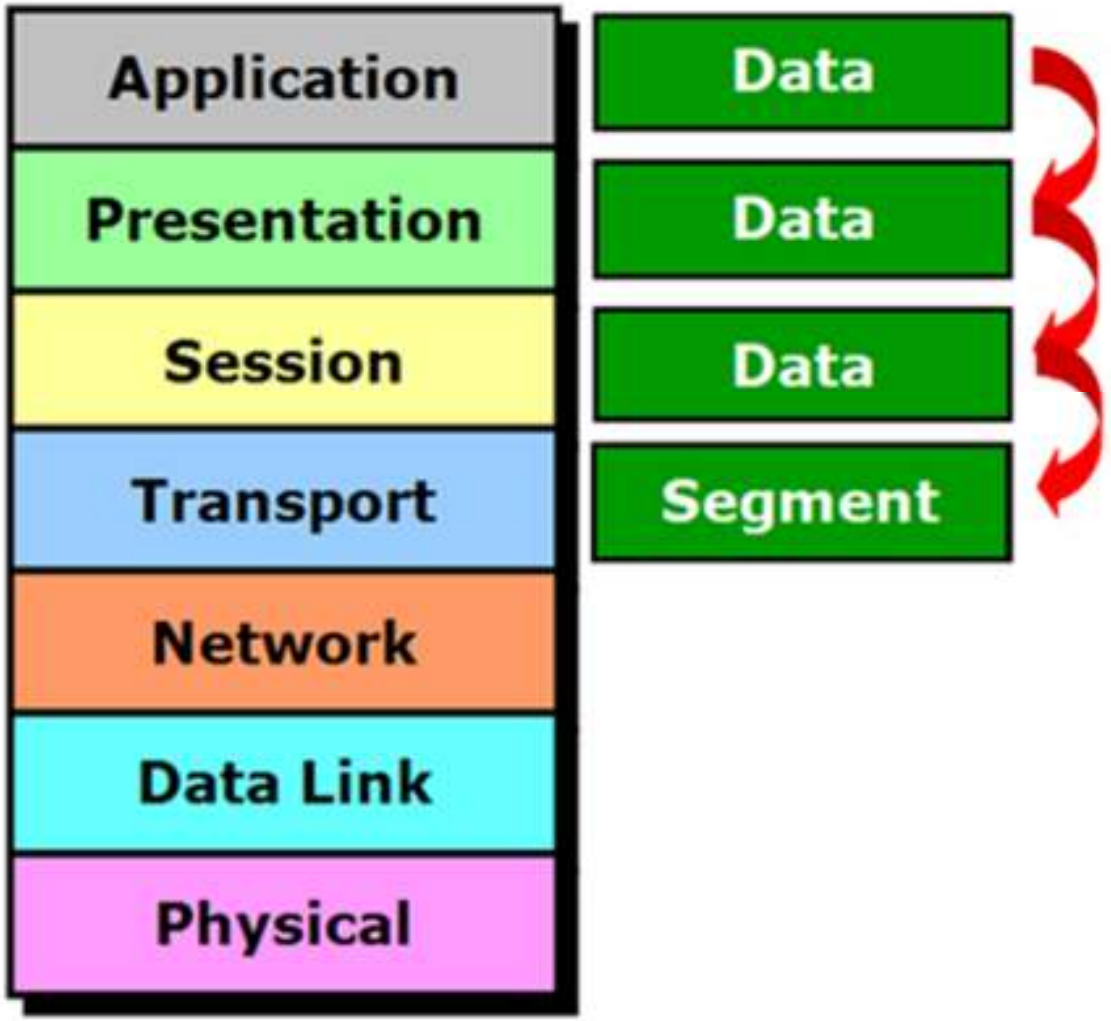
Layers with OSI Model

Multiplexing vs. Demultiplexing:



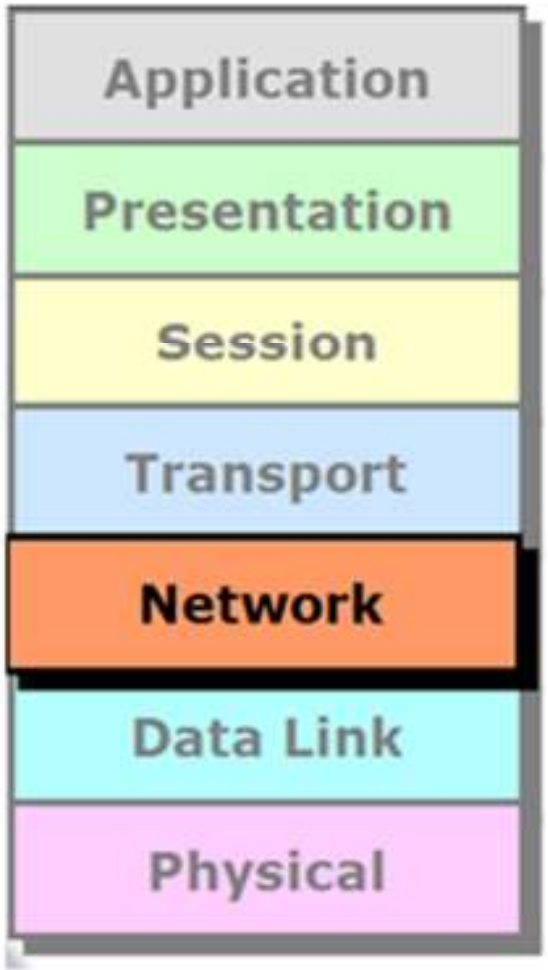
Layers with OSI Model

Data Flow from Transport Layer:



Layers with OSI Model

Network Layer:



Network Layer is responsible for providing best path for data to reach the destination. Logical Addressing works on this layer. Router is a Network Layer device.

It is divided into two parts

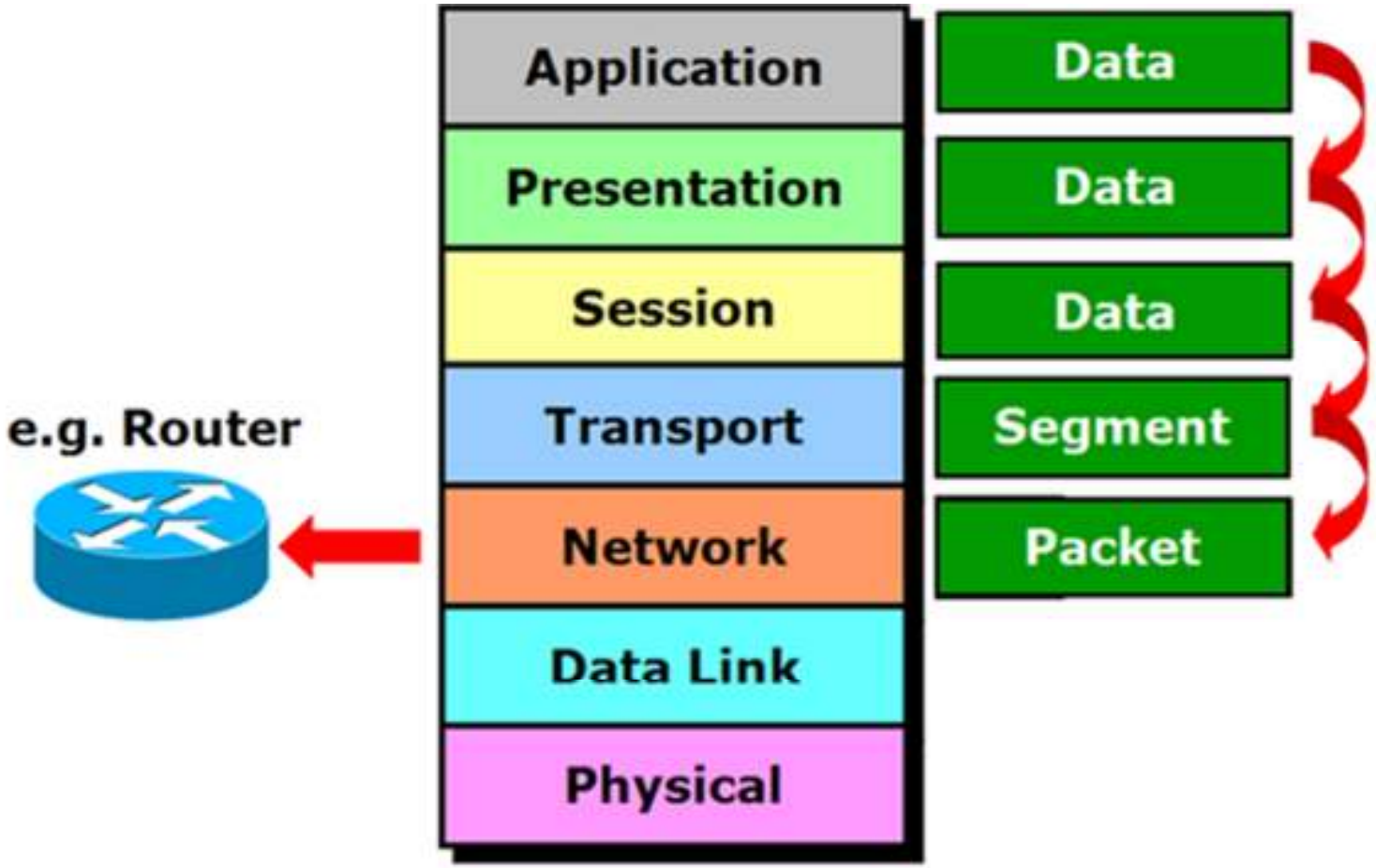
- **Routed Protocols**

  e.g. IP, IPX, Apple Talk.
- **Routing Protocols**

  e.g. RIP, IGRP, OSPF, EIGRP

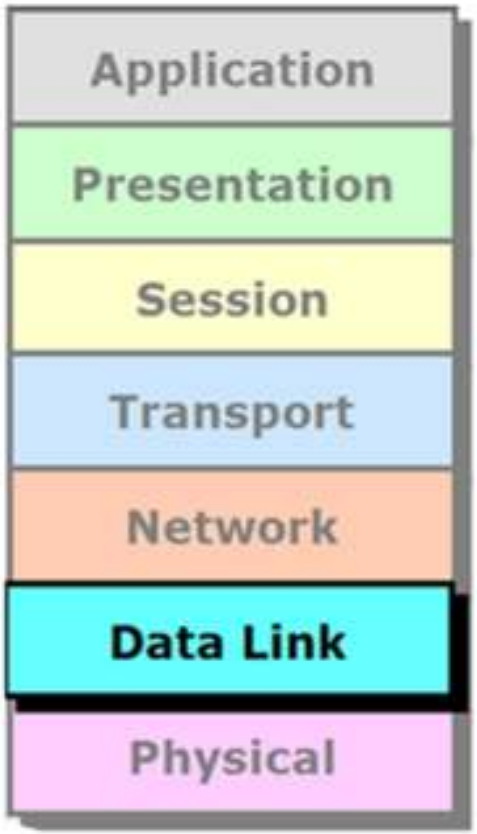
Layers with OSI Model

Data Flow from Network Layer:



Layers with OSI Model

Data Link Layer:



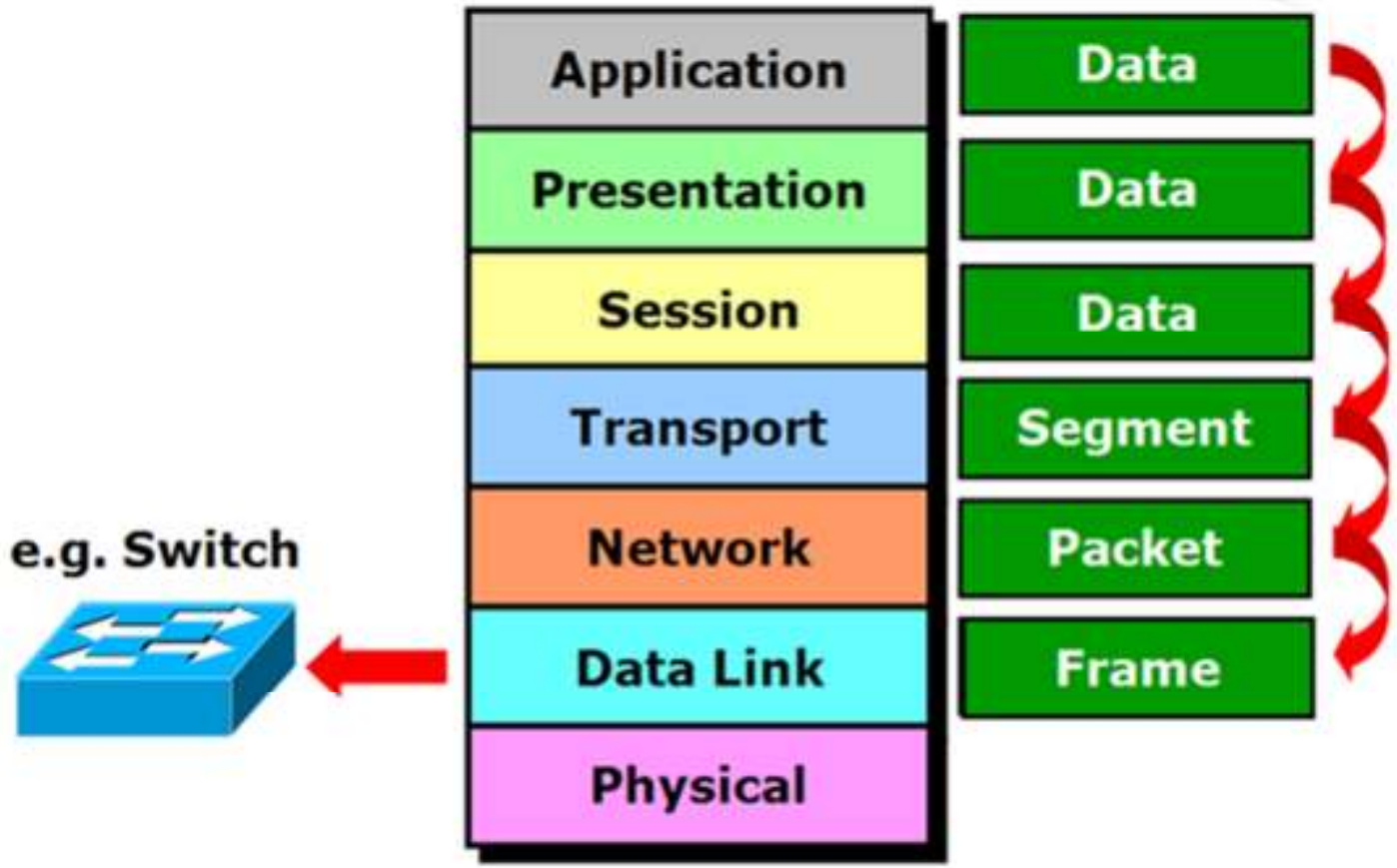
Datalink Layer is divided into two Sub Layers :

- **LLC – Logical Link Control**
  It talks about Wan protocols e.g. PPP, HDLC, Frame-relay

- **MAC – Media Access Control**
  It talks about Physical Address. It is a 48 bit address i.e. 12 digit Hexadecimal Number.
  It is also responsible for Error Detection
  Devices working on Data Link Layer are Switch, Bridge, NIC.

Layers with OSI Model

Data Flow from Data Link Layer:



Layers with OSI Model

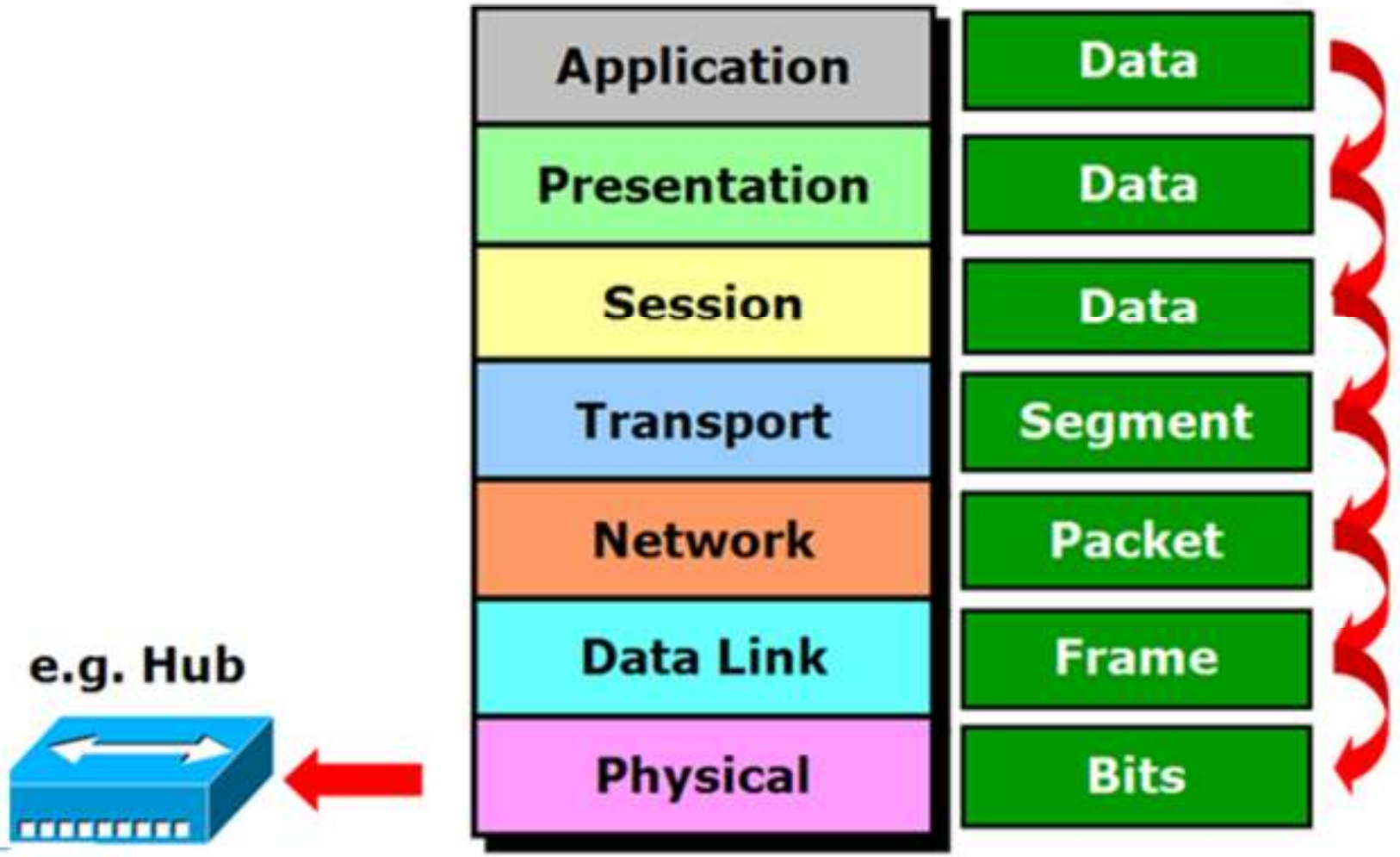
Physical Layer:

Physical Layer is responsible for electrical, mechanical and procedural checks. Data will be converted into Binary (i.e) 0's & 1's. Data will be in the form of electrical pulses if it is Coaxial or Twisted Pair cable and in the form of Light if it is Fiber Optic Cable.

Devices working at Physical Layer are Hubs, Repeaters, Cables, Modems etc.

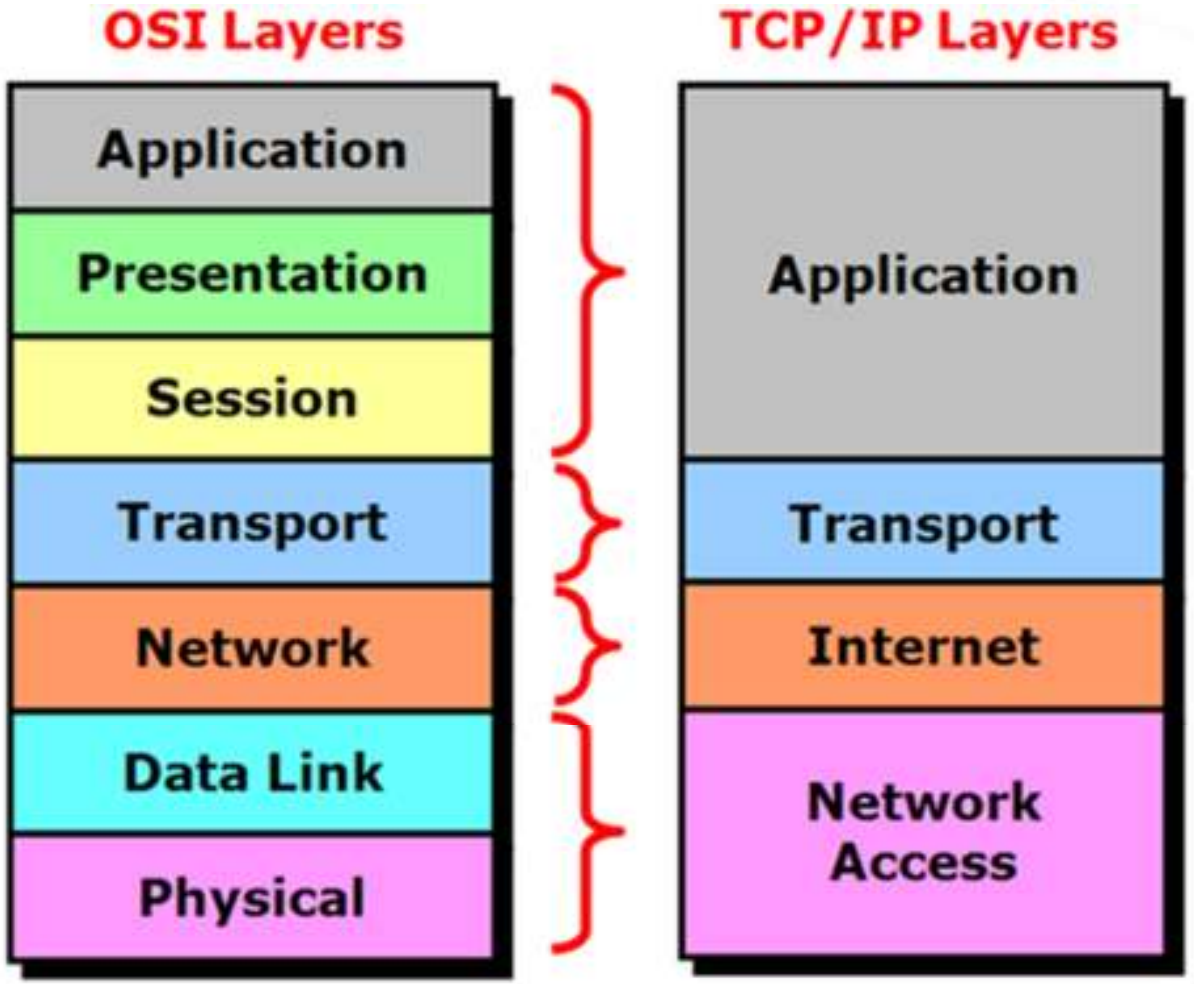
Layers with OSI Model

Data Flow from Physical Layer:

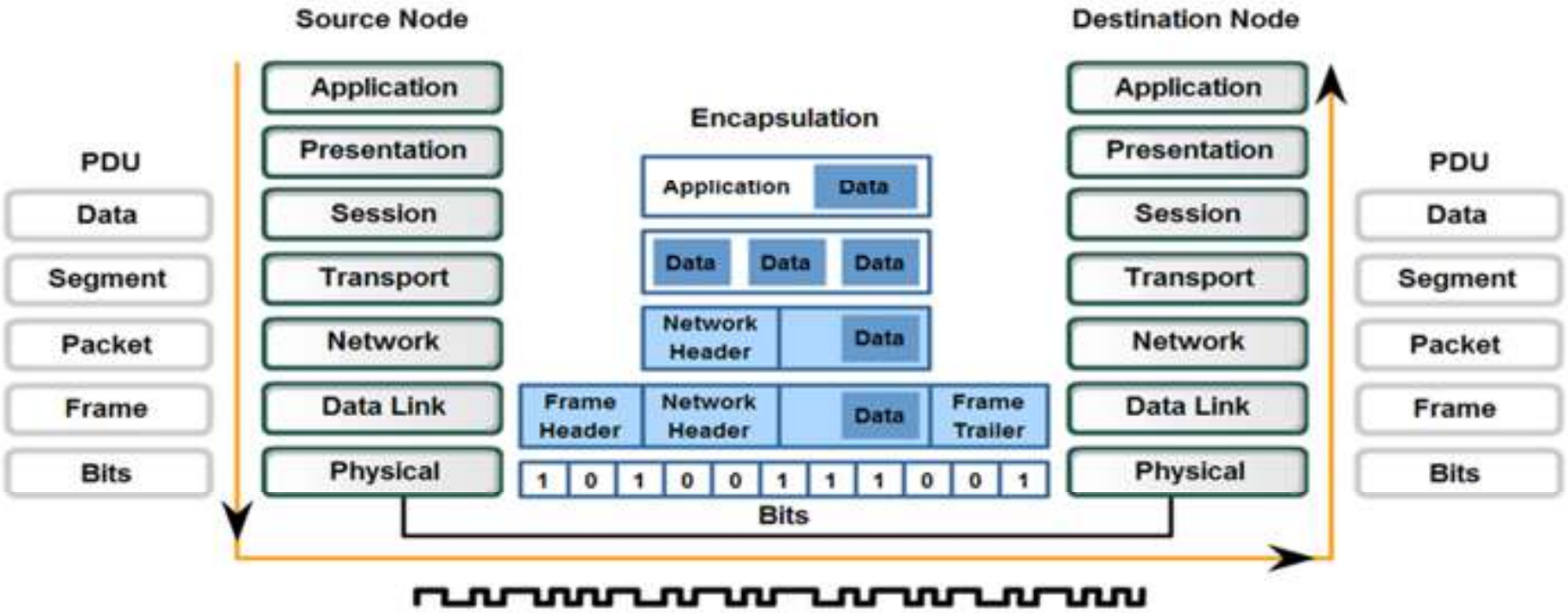


Layers with TCP/IP and OSI Model

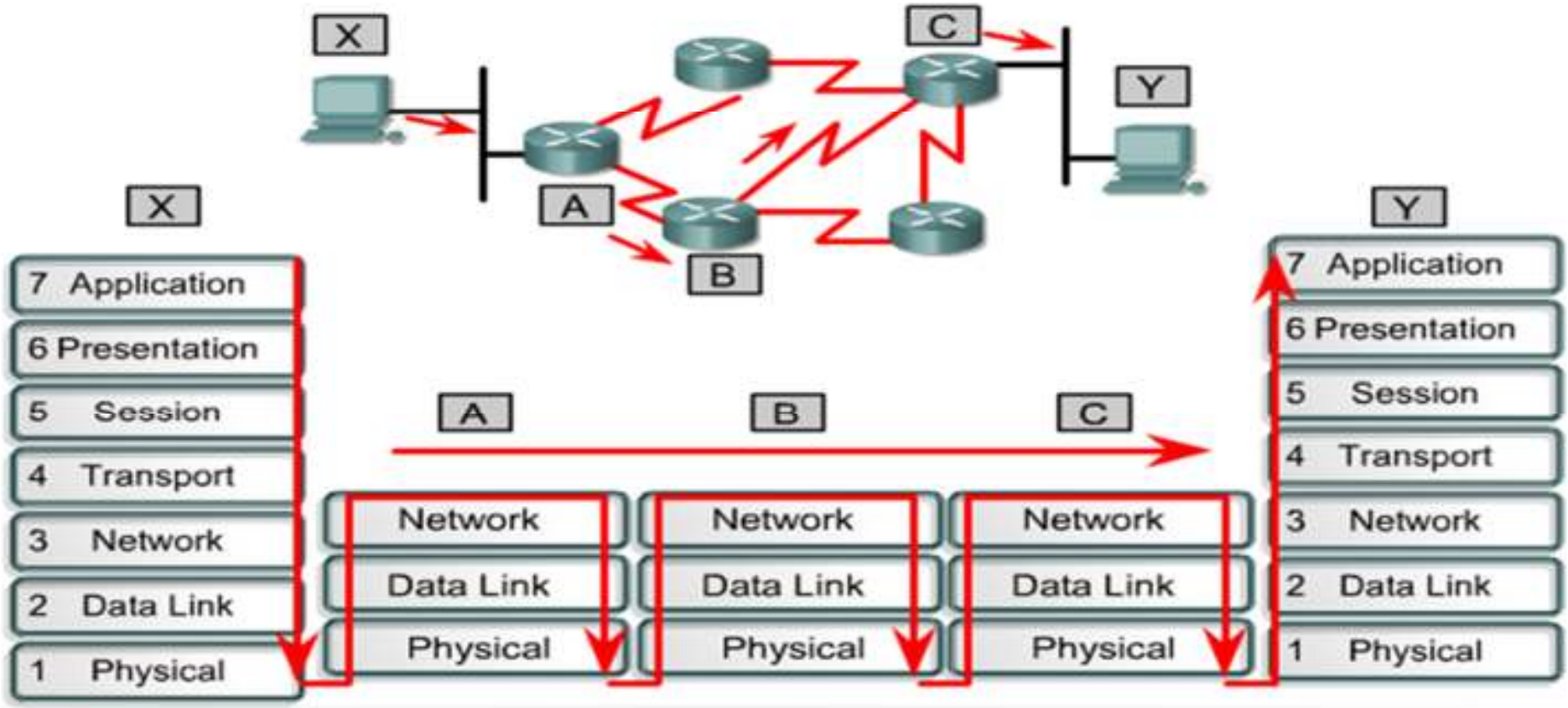
OSI vs. TCP:



Encapsulation Process



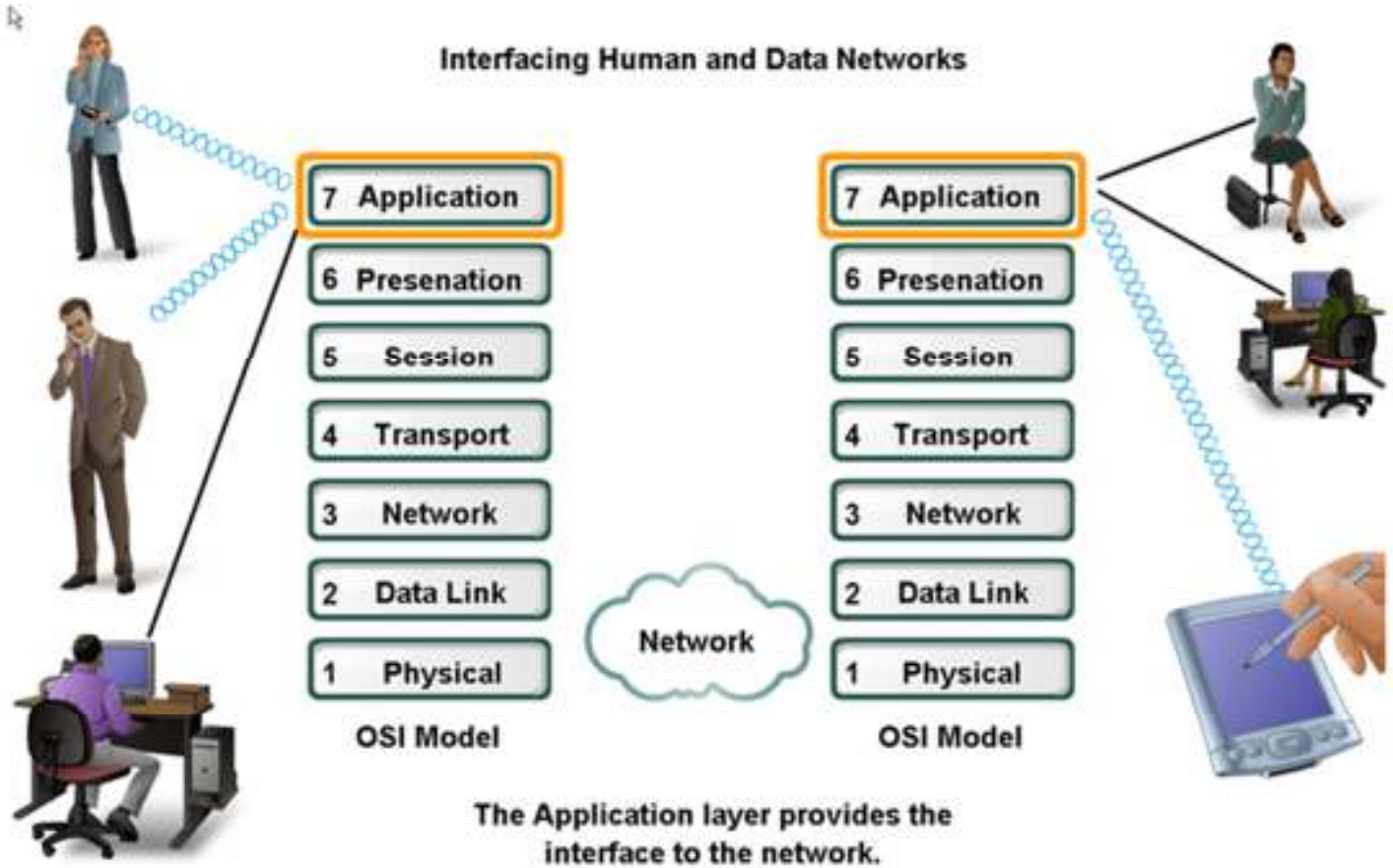
Data Flow Through a Network



Data flow in a network focuses on layers one, two and three of the OSI model. This is after being transmitted by the sending host and before arriving at the receiving host.

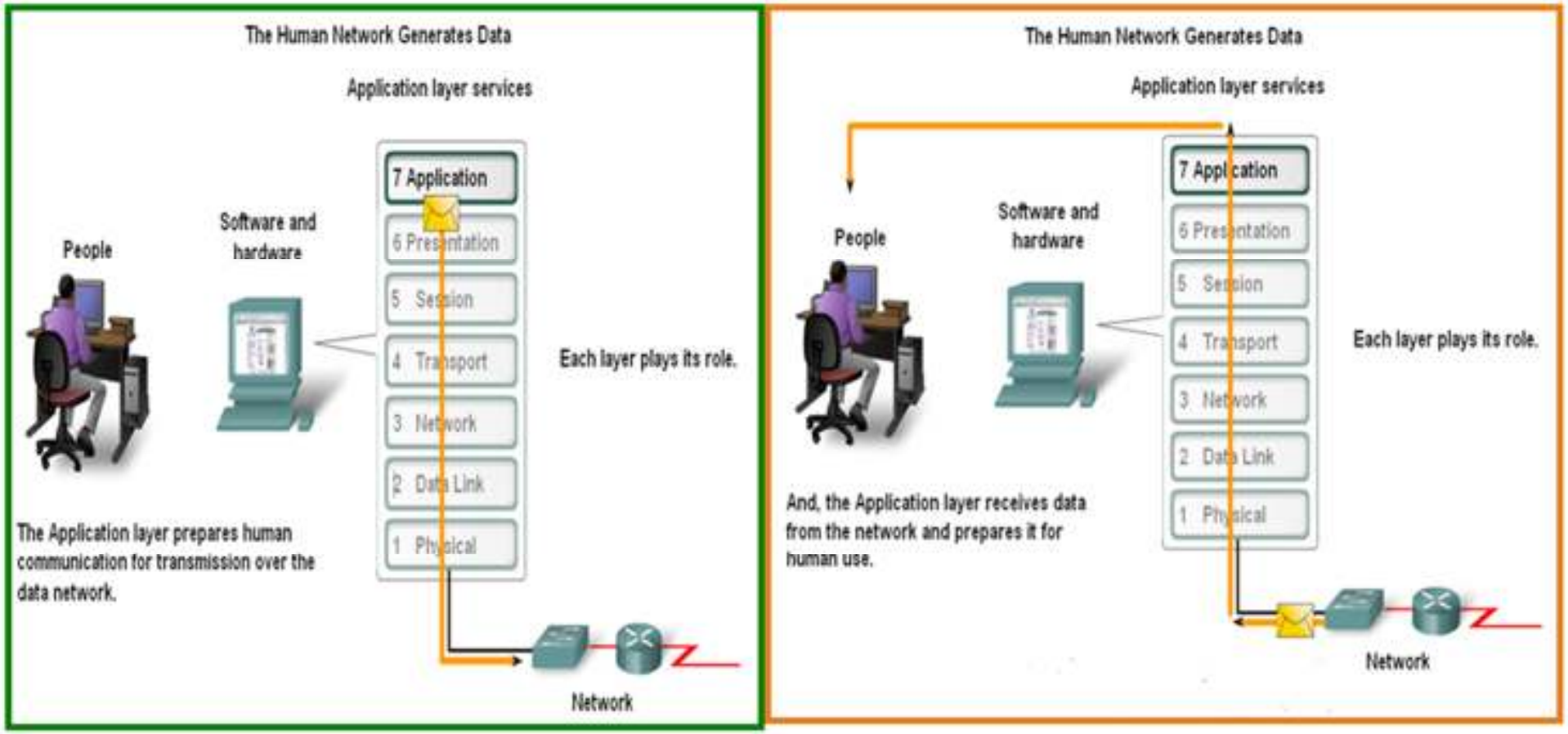
Application Layer

Application Layer Functionality and Protocols (OSI & TCP/IP Model)



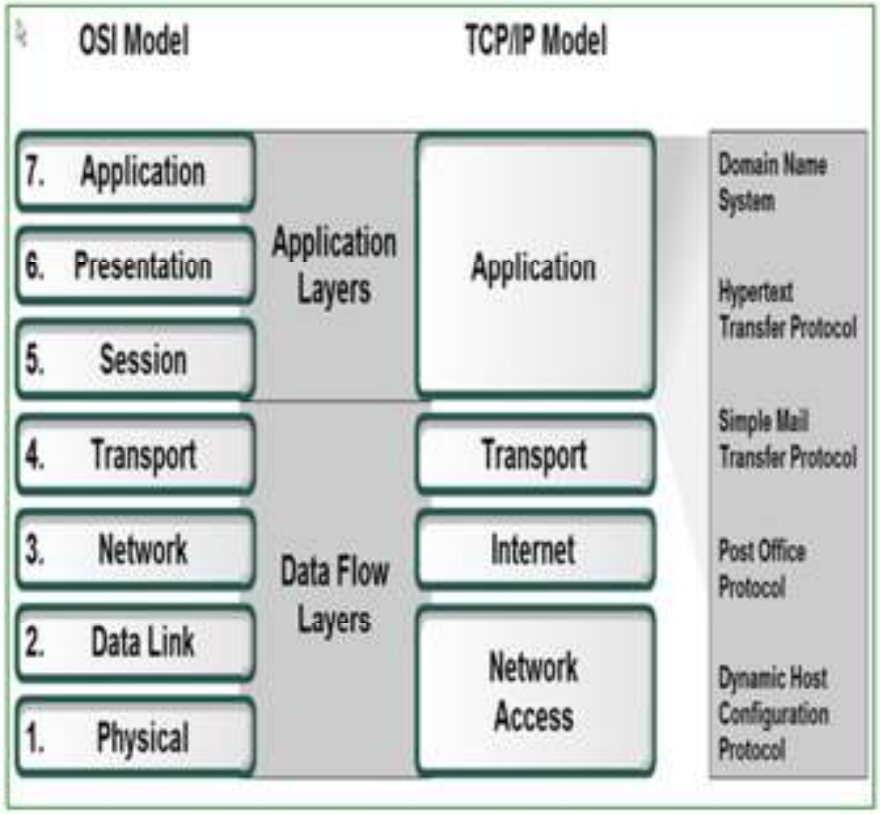
Application Layer Functionality and Protocols (OSI & TCP/IP Model)

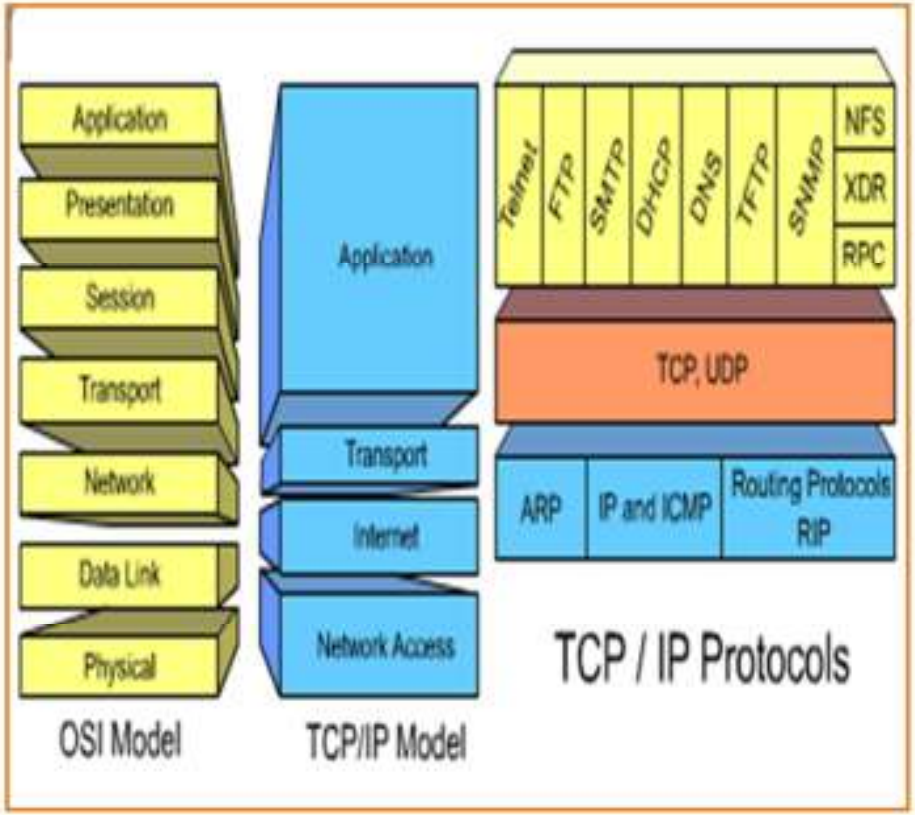
The Application layer, Layer seven, is the top layer of both the OSI and TCP/IP models.



Application Layer Functionality and Protocols (OSI & TCP/IP Model)

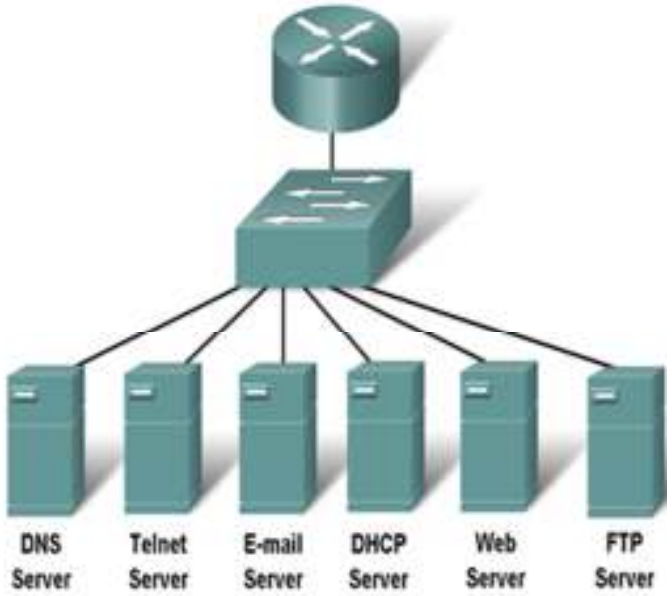
Most applications, like web browsers or e-mail clients, incorporate functionality of the OSI layers 5, 6 and 7.





Application Layer Functionality and Protocols (OSI & TCP/IP Model)

- DNS Server- service that provides the IP address of a web site or domain name so a host can connect to it
- Telnet Server- Service that allows administrators to login to a host from a remote location and control the host as though they were logged in locally
- Email Server - Uses Simple Mail Transfer Protocol (SMTP) Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP) Used to send e-mail messages from client to servers over the Internet Recipients are specified using the user@appnomic.com format
- Dynamic Host Configuration Protocol (DHCP) Server - Service that assigns the Ip address subnet mask default gateway and other information to clients
- WEB Server - Hypertext Transfer Protocol, Used to transfer information between web clients and web servers, Most web pages are accessed using HTTP
- File Transfer Protocol (FTP) Server - Service that allows for the download and upload of files between a client and server

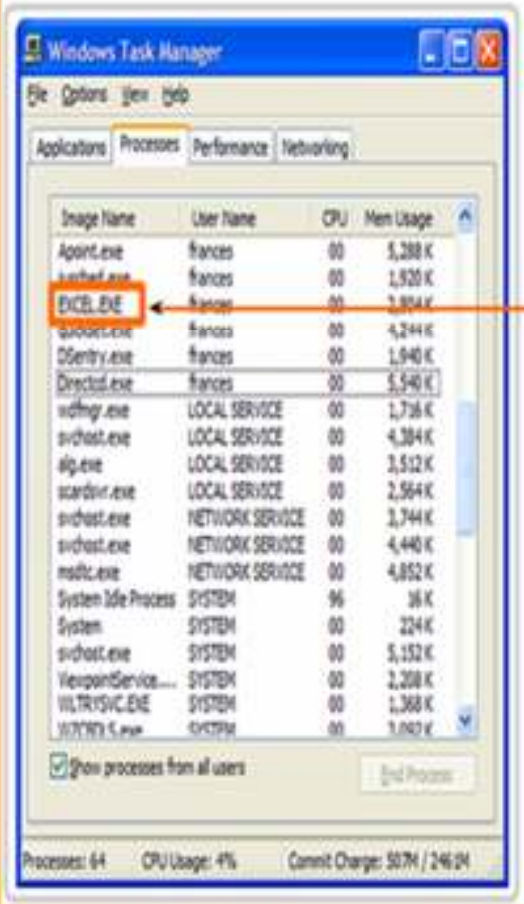


Well Known Port Number

- FTP – 20, 21
- TFTP – 69
- DHCP – 68 client, 67 server
- DNS – 53
- HTTP – 80
- HTTPS – 443
- TELNET – 23
- SSH – 22
- SNMP – 161, 162

Application Layer Services

Software Processes

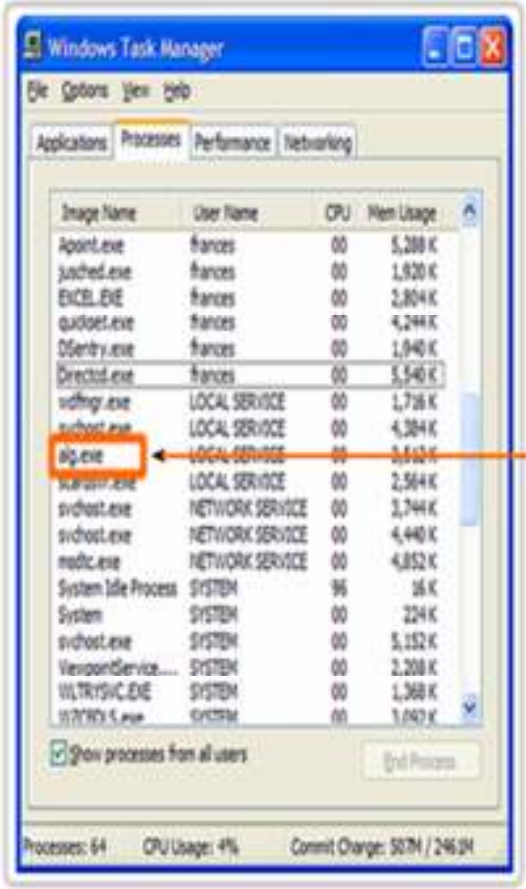


Processes are individual software programs running concurrently.

Processes can be

1. Applications
2. Services
3. System operations
4. One program may be running several times, each in its own process.

Software Processes

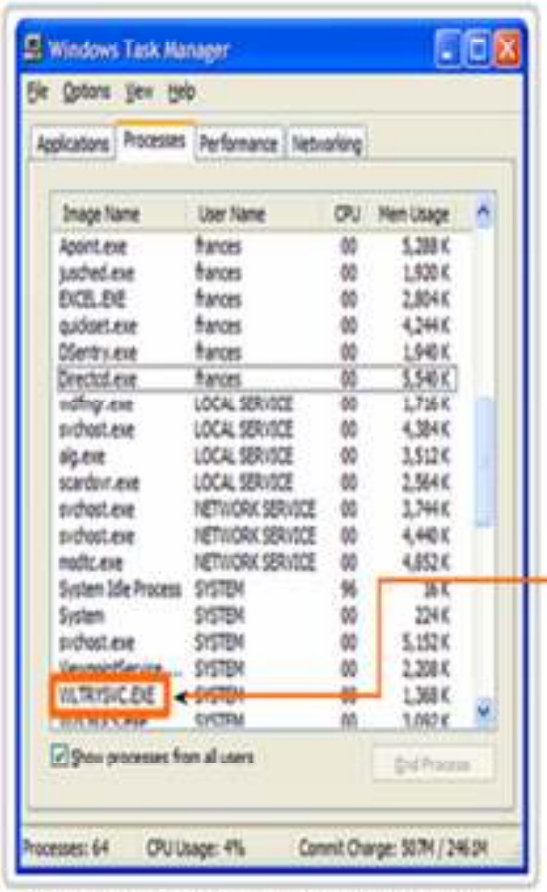


Processes are individual software programs running concurrently.

Processes can be

1. Applications
2. Services
3. System operations
4. One program may be running several times, each in its own process.

Application Layer Services

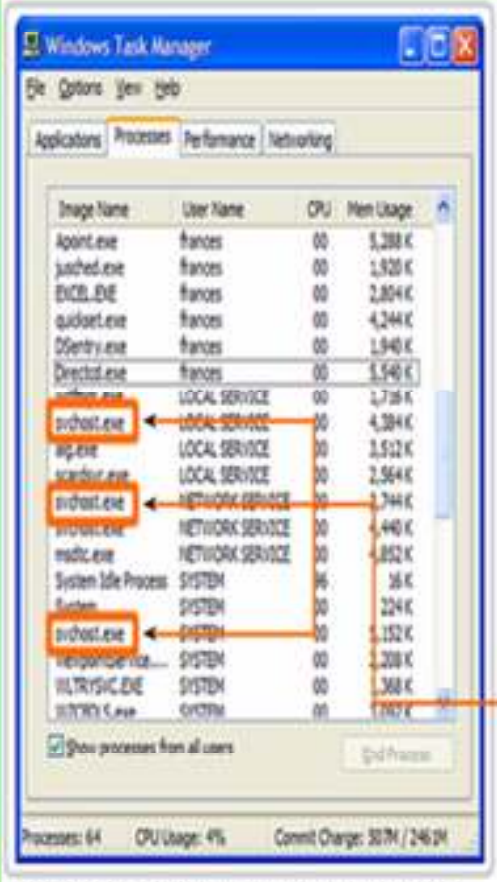


Processes are individual software programs running concurrently.

Processes can be

1. Applications
2. Services
3. System operations
4. One program may be running several times, each in its own process.

Examples of processes running in the Windows operating system



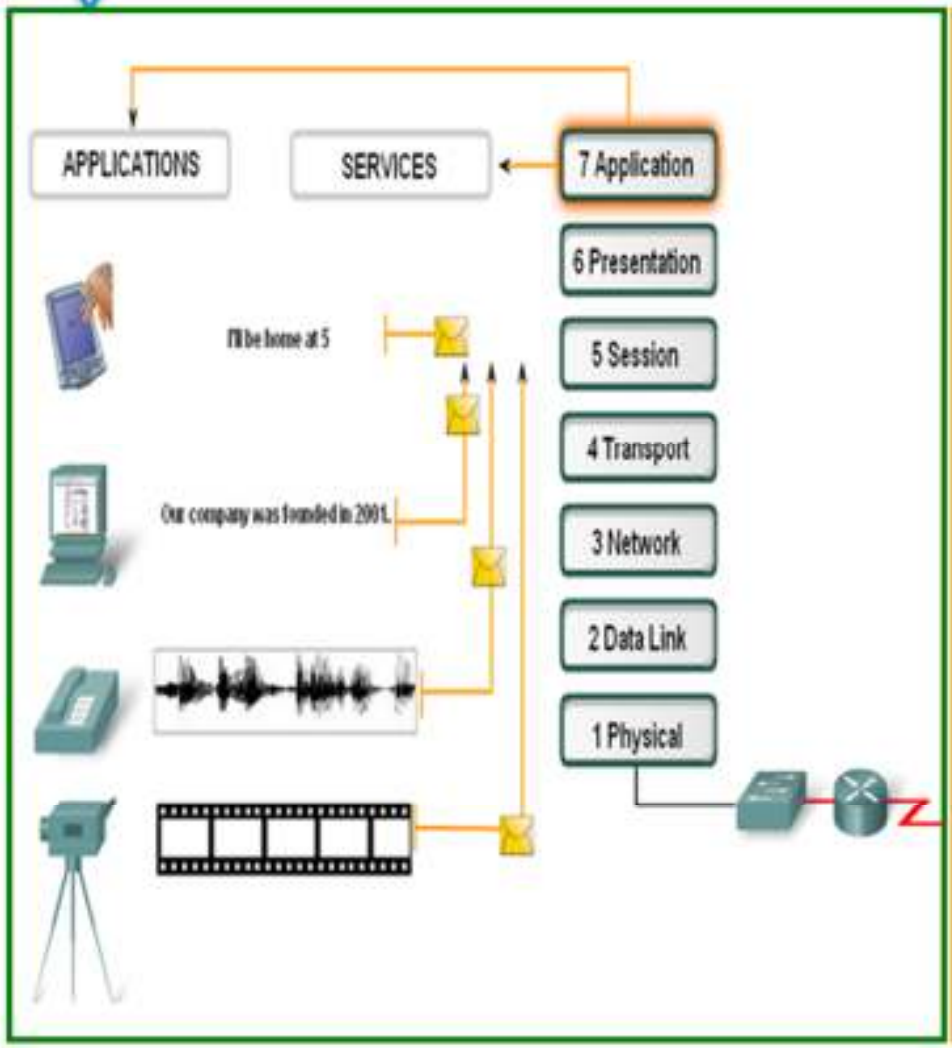
Processes are individual software programs running concurrently.

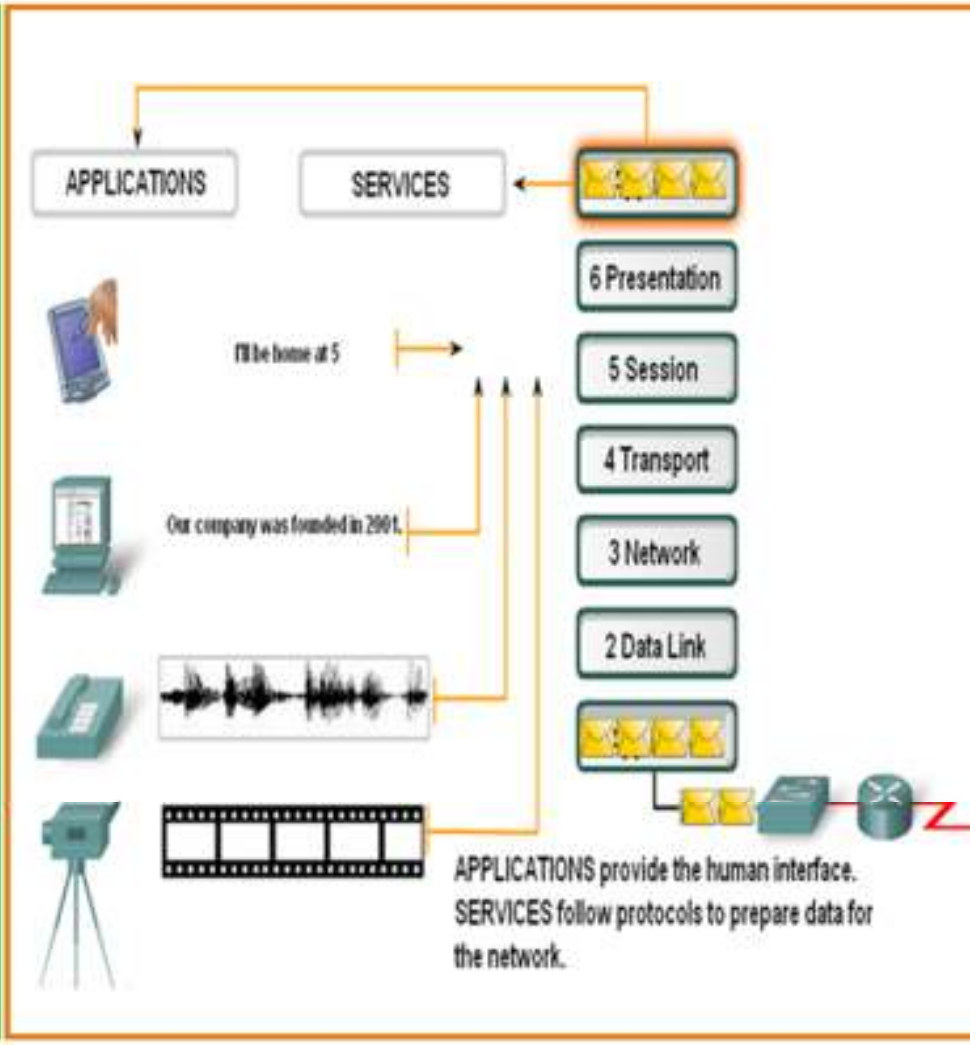
Processes can be

1. Applications
2. Services
3. System operations
4. One program may be running several times, each in its own process.

Examples of processes running in the Windows operating system

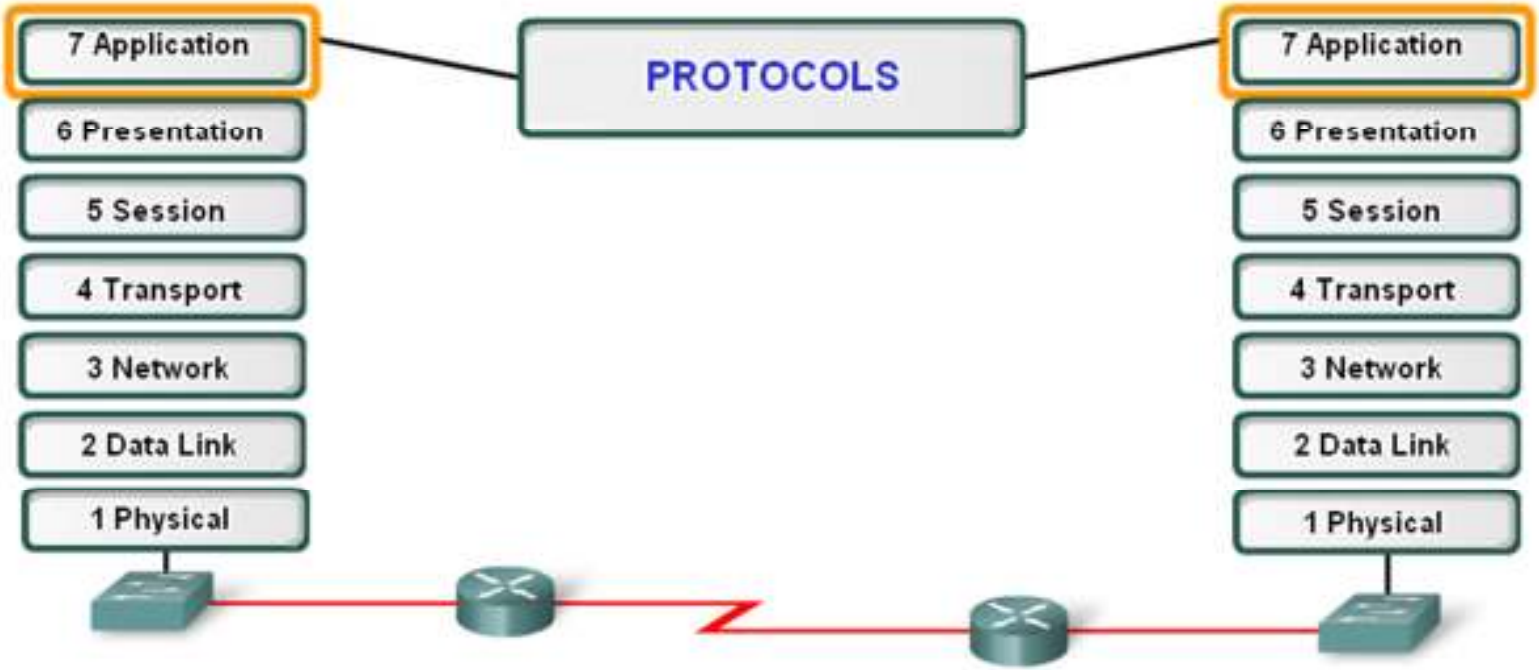
User Applications, Services, and Application Layer Protocols





Application Layer Protocol Functions

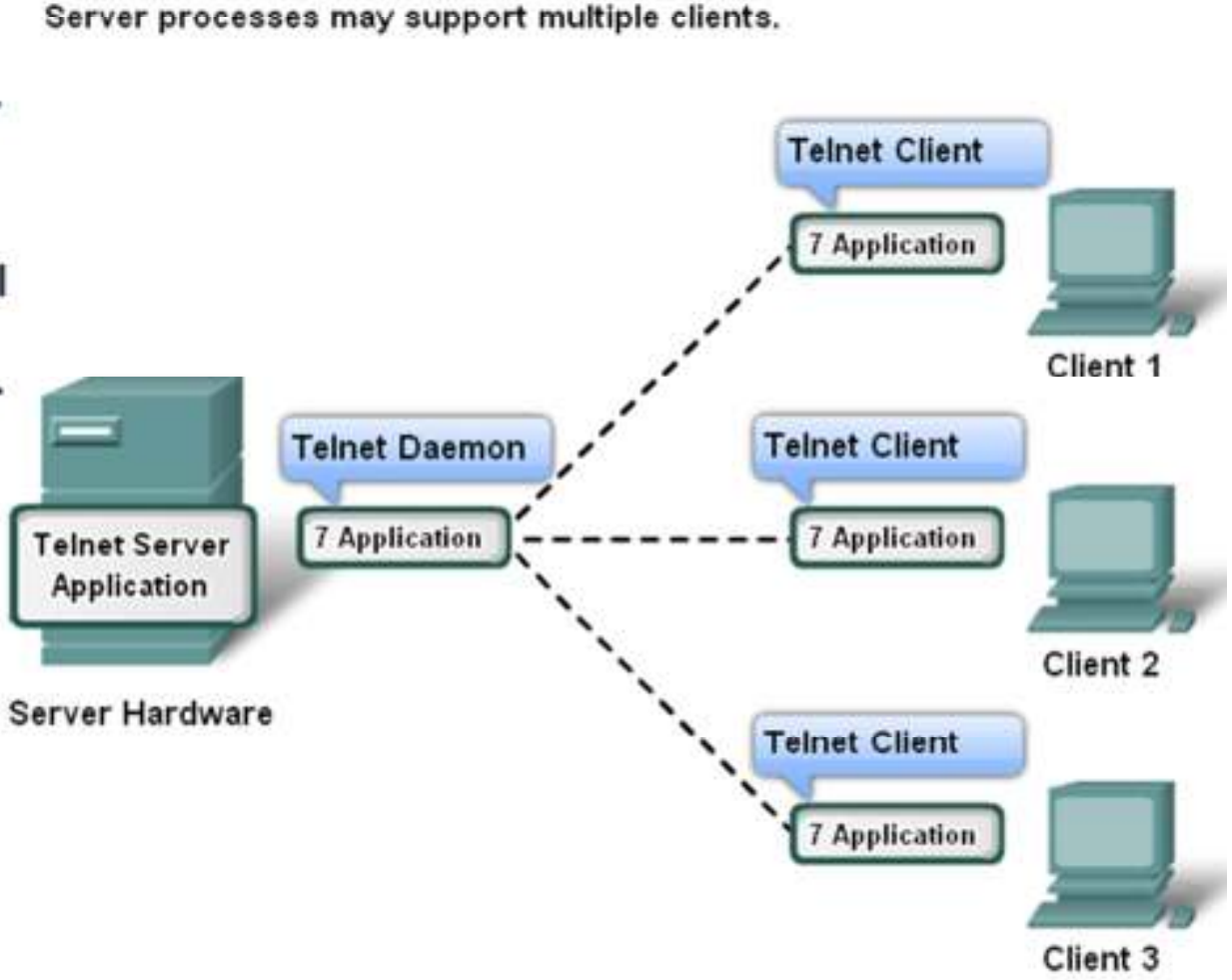
Application layer protocols are used by both the source and destination devices during a communication session. In order for the communications to be successful, the application layer protocols implemented on the source and destination host must match.



Application layer protocols provide the rules for communication between applications.

Application Layer Services and Protocols

Additionally, servers typically have multiple clients requesting information at the same time. For example, a Telnet server may have many clients requesting connections to it. These individual client requests must be handled simultaneously and separately for the network to succeed. The Application layer processes and services rely on support from lower layer functions to successfully manage the multiple conversations.



Presentation & Session Layer

Presentation & Session Layer Functionality and Protocols (OSI & TCP/IP Model)

The Presentation Layer

- The Presentation layer has three primary functions:

- Translation: Networks can connect very different types of computers together: PCs, Macintoshes, UNIX systems, AS/400 servers and mainframes can all exist on the same network. These systems have many distinct characteristics and represent data in different ways; they may use different character sets for example. The presentation layer handles the job of hiding these differences between machines.

- Compression: Compression (and decompression) may be done at the presentation layer to improve the throughput of data. (There are some who believe this is not, strictly speaking, a function of the presentation layer.)

- Encryption: Some types of encryption (and decryption) are performed at the presentation layer. This ensures the security of the data as it travels down the protocol stack. For example, one of the most popular encryption schemes that is usually associated with the presentation layer is the Secure Sockets Layer (SSL) protocol. Not all encryption is done at layer 6, however; some encryption is often done at lower layers in the protocol stack, in technologies such as Ipsec.

Presentation & Session Layer Functionality and Protocols (OSI & TCP/IP Model)

- Presentation layer implementations are not typically associated with a particular protocol stack. The standards for video and graphics are examples. Some well-known standards for video include QuickTime and Motion Picture Experts Group (MPEG). QuickTime is an Apple Computer specification for video and audio, and MPEG is a standard for video compression and coding.

- Among the well-known graphic image formats are Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and Tagged Image File Format (TIFF). GIF and JPEG are compression and coding standards for graphic images, and TIFF is a standard coding format for graphic images.

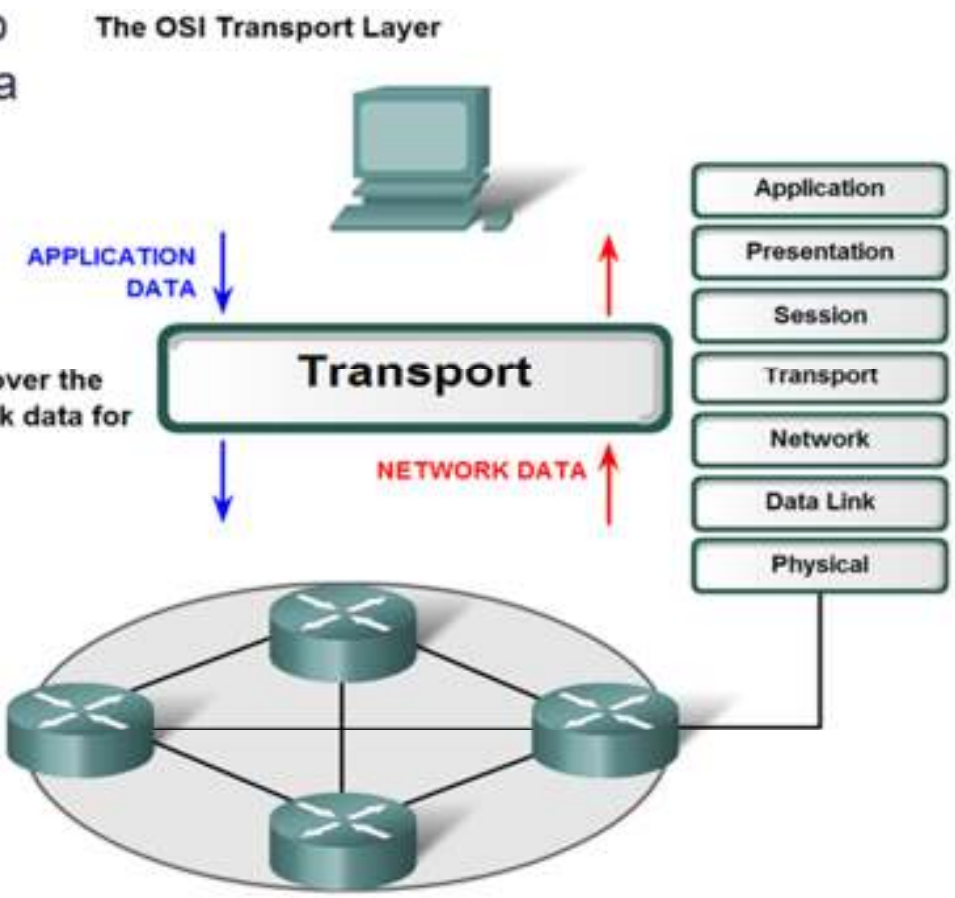
The Session Layer

- The name of this layer tells you much about what it is designed to do: to allow devices to establish and manage *sessions*. In general terms, a session is a persistent logical linking of two software application processes, to allow them to exchange data over a prolonged period of time. In some discussions, these sessions are called *dialogs*; they are roughly analogous to a telephone call made between two people

Transport Layer

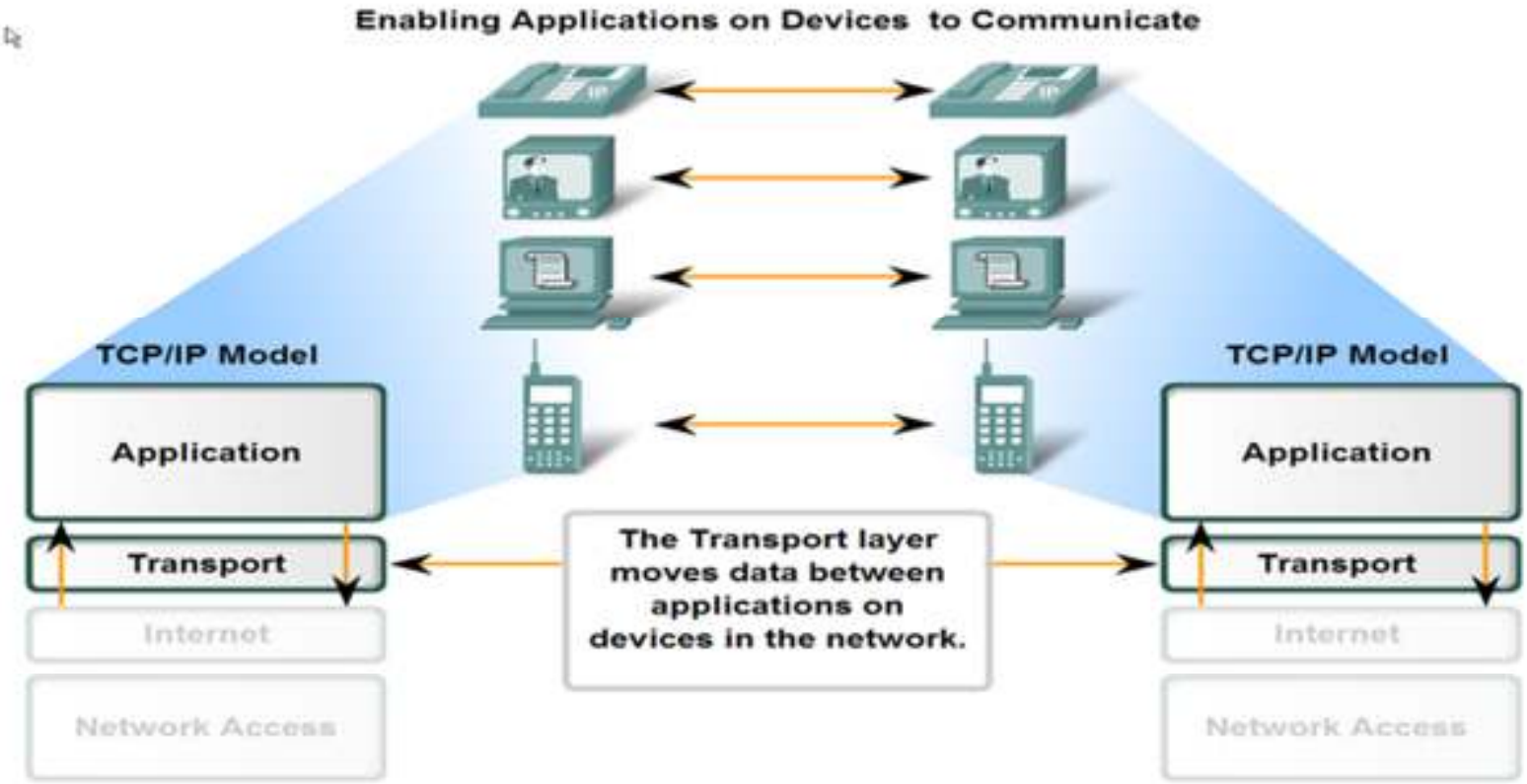
Transport Layer - Role and Services

The functionality of the transport layer is to provide "transparent transfer of data from a source end open system to a destination end open system"



The Transport layer prepares application data for transport over the network and processes network data for use by applications.

Transport Layer - Role and Services



Transport Layer - Role and Services

- Transport is responsible for creating and maintaining the basic end-to-end connection between communicating open systems, ensuring that the bits delivered to the receiver are the same as the bits transmitted by the sender; in the same order and without modification, loss or duplication
- It takes the information to be sent and breaks it into individual packets that are sent and reassembled into a complete message by the Transport Layer at the receiving node
- Also provide a signaling service for the remote node so that the sending node is notified when its data is received successfully by the receiving node
- Transport Layer protocols include the capability to acknowledge the receipt of a packet; if no acknowledgement is received, the Transport Layer protocol can retransmit the packet or time-out the connection and signal an error
- Transport protocols can also mark packets with sequencing information so that the destination system can properly order the packets if they're received out-of-sequence

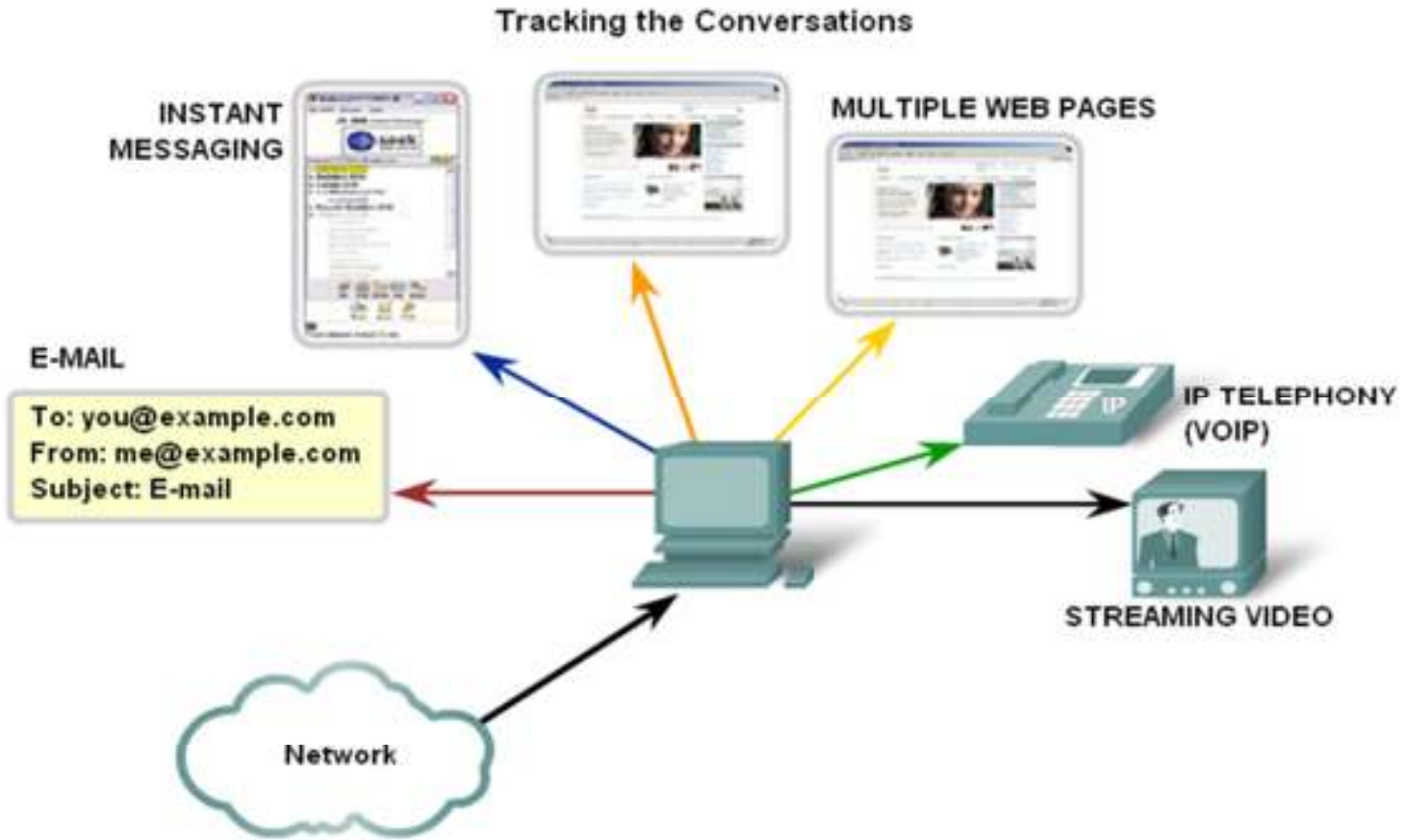
Transport Layer - Role and Services

- In addition, Transport protocols provide facilities for insuring the integrity of packets and requesting retransmission should the packet become garbled when routed.
- Transport protocols provide the capability for multiple application processes to access the network by using individual local addresses to determine the destination process for each data stream

Two standard transport protocols: TCP and UDP

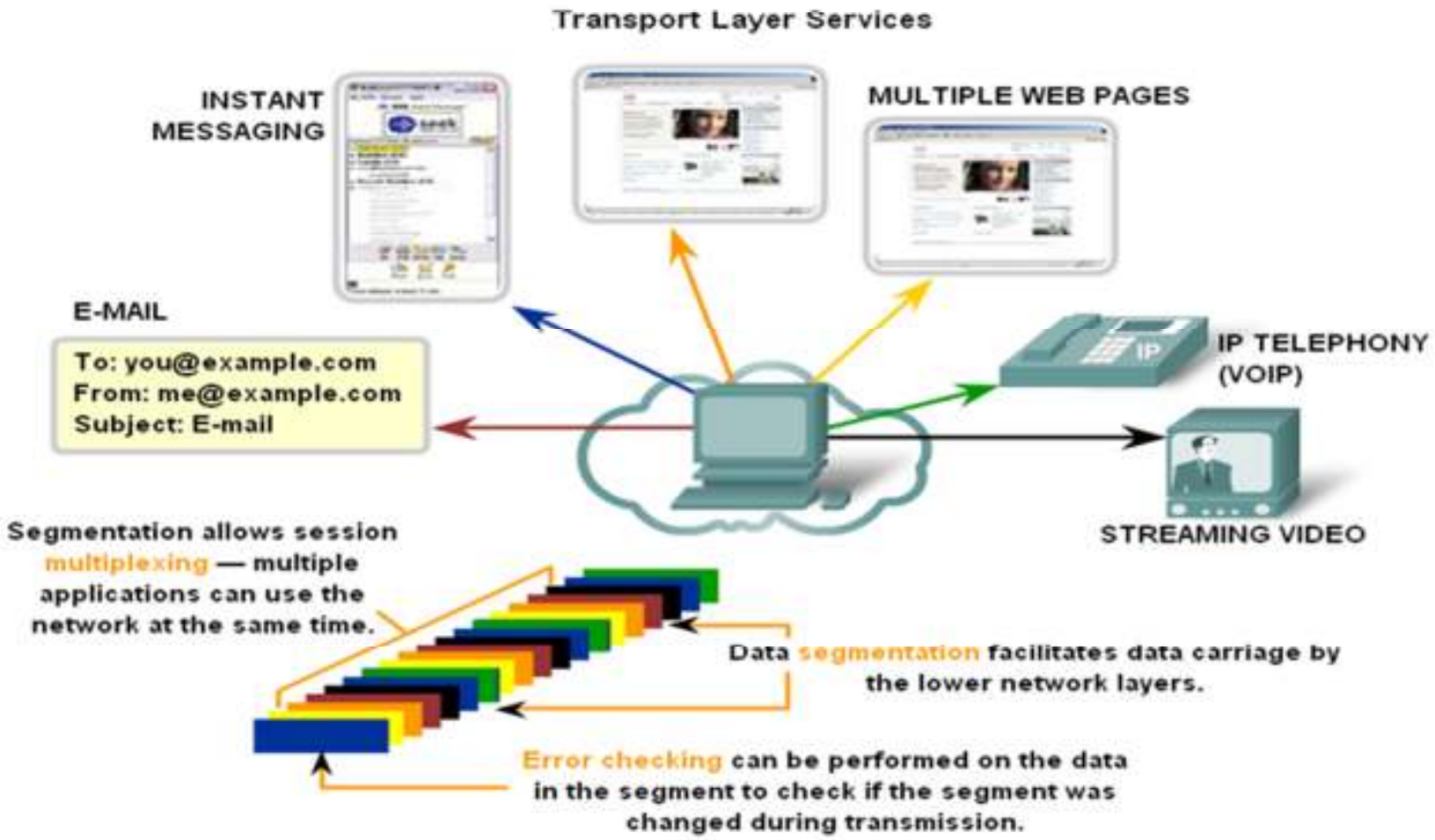
- TCP implements a reliable data-stream protocol
  - connection oriented
- UDP implements an unreliable data-stream
  - connectionless

Transport Layer - Role and Services

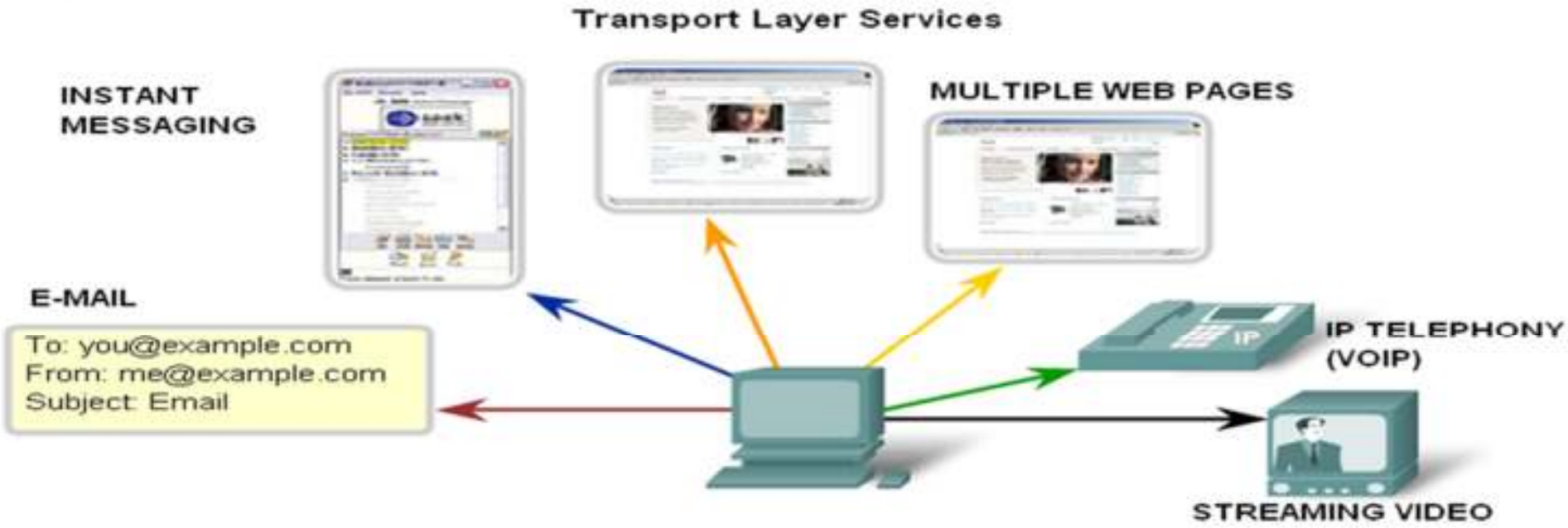


The Transport layer segments the data and manages the separation of data for different applications. Multiple applications running on a device receive the correct data.

Transport Layer - Role and Services



Transport Layer - Role and Services



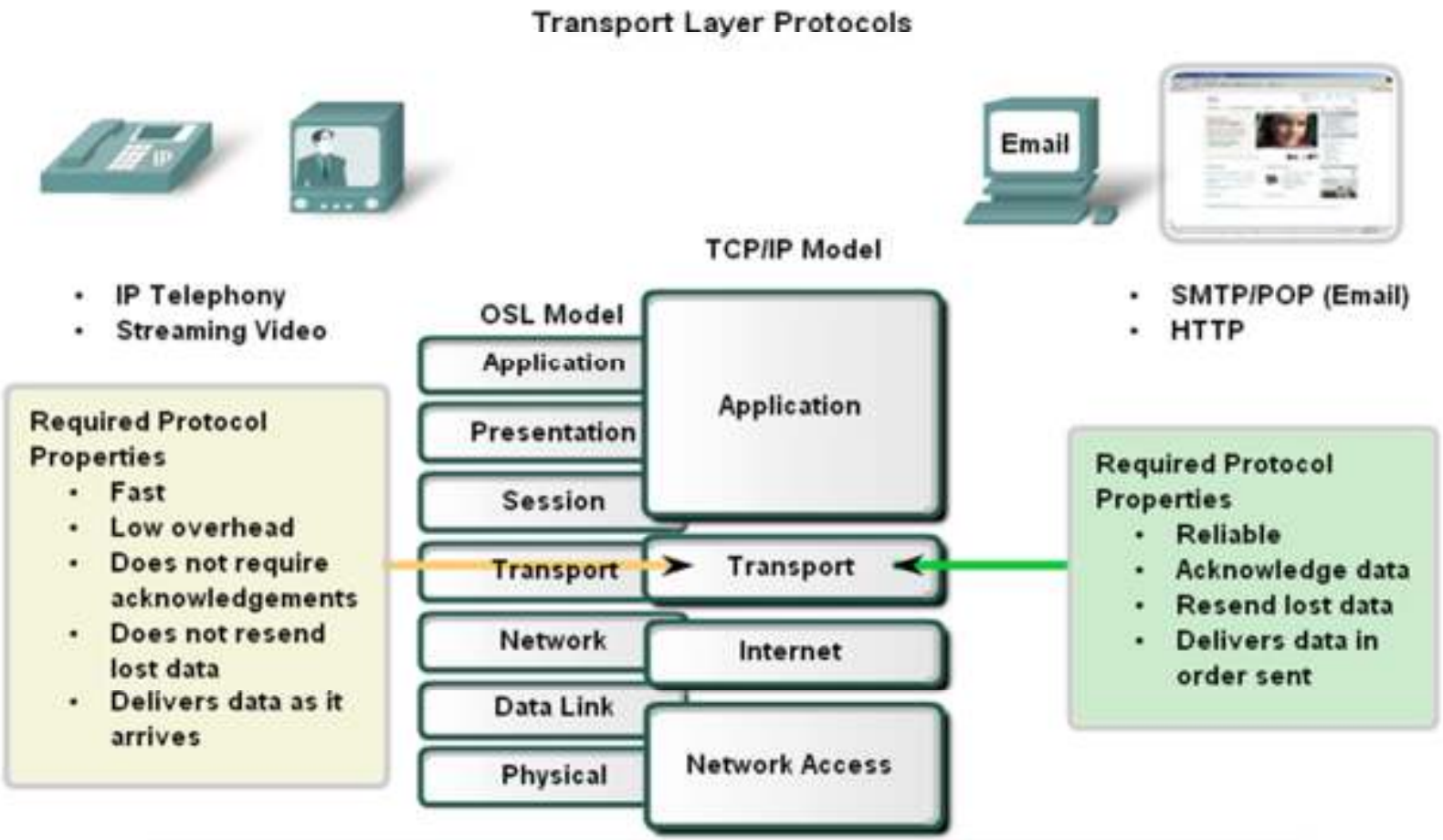
Establishing a Session ensures the application is ready to receive the data.

Reliable delivery means lost segments are resent so the data is received complete.

Same order delivery ensures data is delivered sequentially as it was sent.

Flow Control manages data delivery if there is congestion on the host.

Transport Layer - Role and Services



Transport Layer - TCP and UDP

The two most common Transport layer protocols of TCP/IP protocol suite are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). Both protocols manage the communication of multiple applications. The differences between the two are the specific functions that each protocol implements.

User Datagram Protocol (UDP)

- UDP is a simple, connectionless protocol, described in RFC 768. It has the advantage of providing for low overhead data delivery. The pieces of communication in UDP are called datagrams. These datagrams are sent as "best effort" by this Transport layer protocol.
- Applications that use UDP include:
- Domain Name System (DNS)
- Video Streaming
- Voice over IP (VoIP)

Transmission Control Protocol (TCP)

- TCP is a connection-oriented protocol, described in RFC 793. TCP incurs additional overhead to gain functions. Additional functions specified by TCP are the same order delivery, reliable delivery, and flow control. Each TCP segment has 20 bytes of overhead in the header encapsulating the Application layer data, whereas each UDP segment only has 8 bytes of overhead. See the figure for a comparison.
- Applications that use TCP are:
- Web Browsers
- E-mail
- File Transfers

Transport Layer - TCP and UDP

TCP and UDP Headers

TCP Segment

Bit (0)	Bit (15) Bit (16)	Bit (31)
Source Port (16)	Destination Port (16)	
Sequence Number (32)		
Acknowledgement Number (32)		
Header Length (4) Reserved (6) Code Bits (6)	Window (16)	
Checksum (16)	Urgent (16)	
Options (0 or 32 if any)		
APPLICATION LAYER DATA (Size varies)		

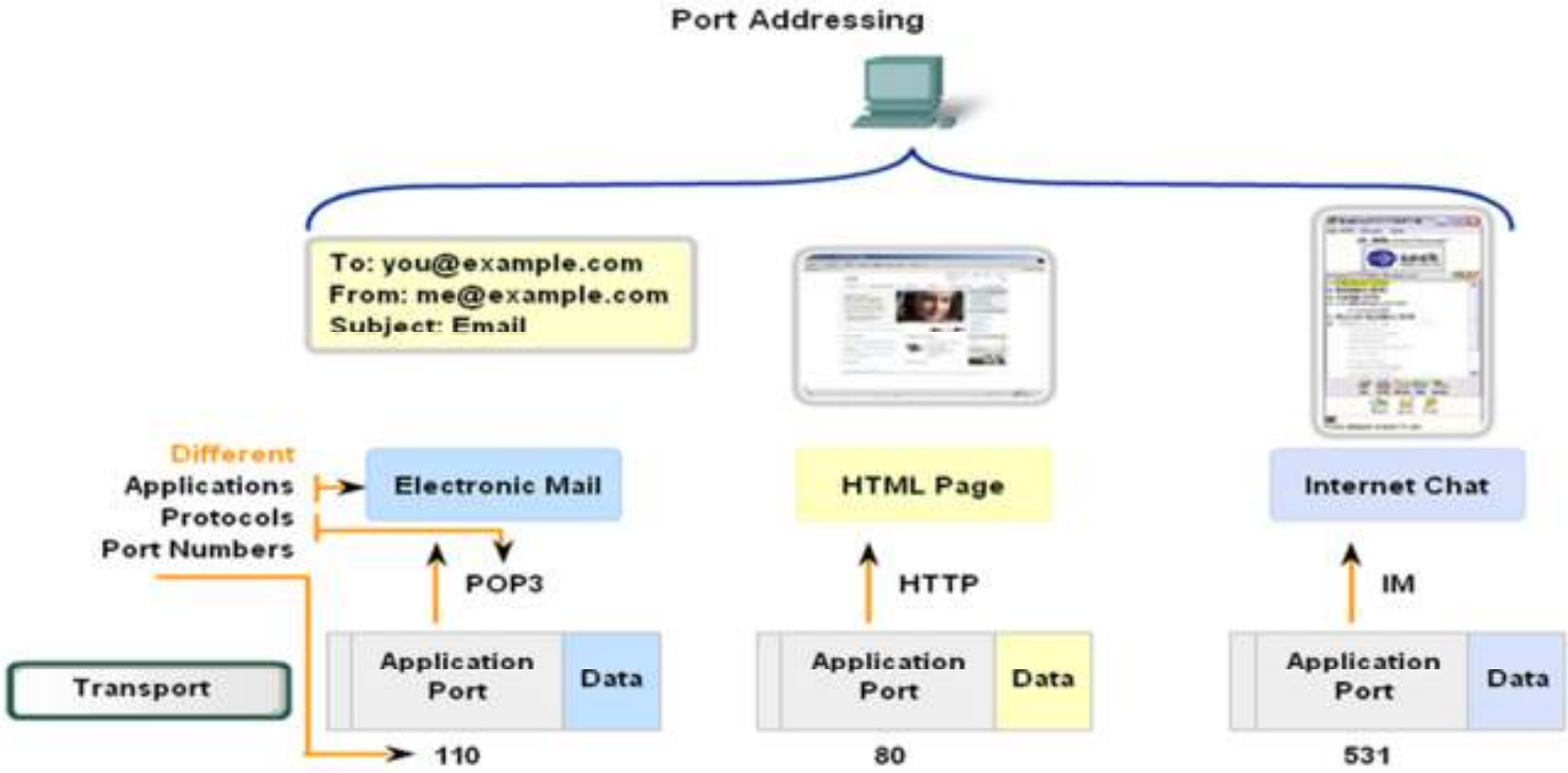
20 Bytes

UDP Datagram

Bit (0)	Bit (15) Bit (16)	Bit (31)
Source Port (16)	Destination Port (16)	
Length (16)	Checksum (16)	
APPLICATION LAYER DATA (Size varies)		

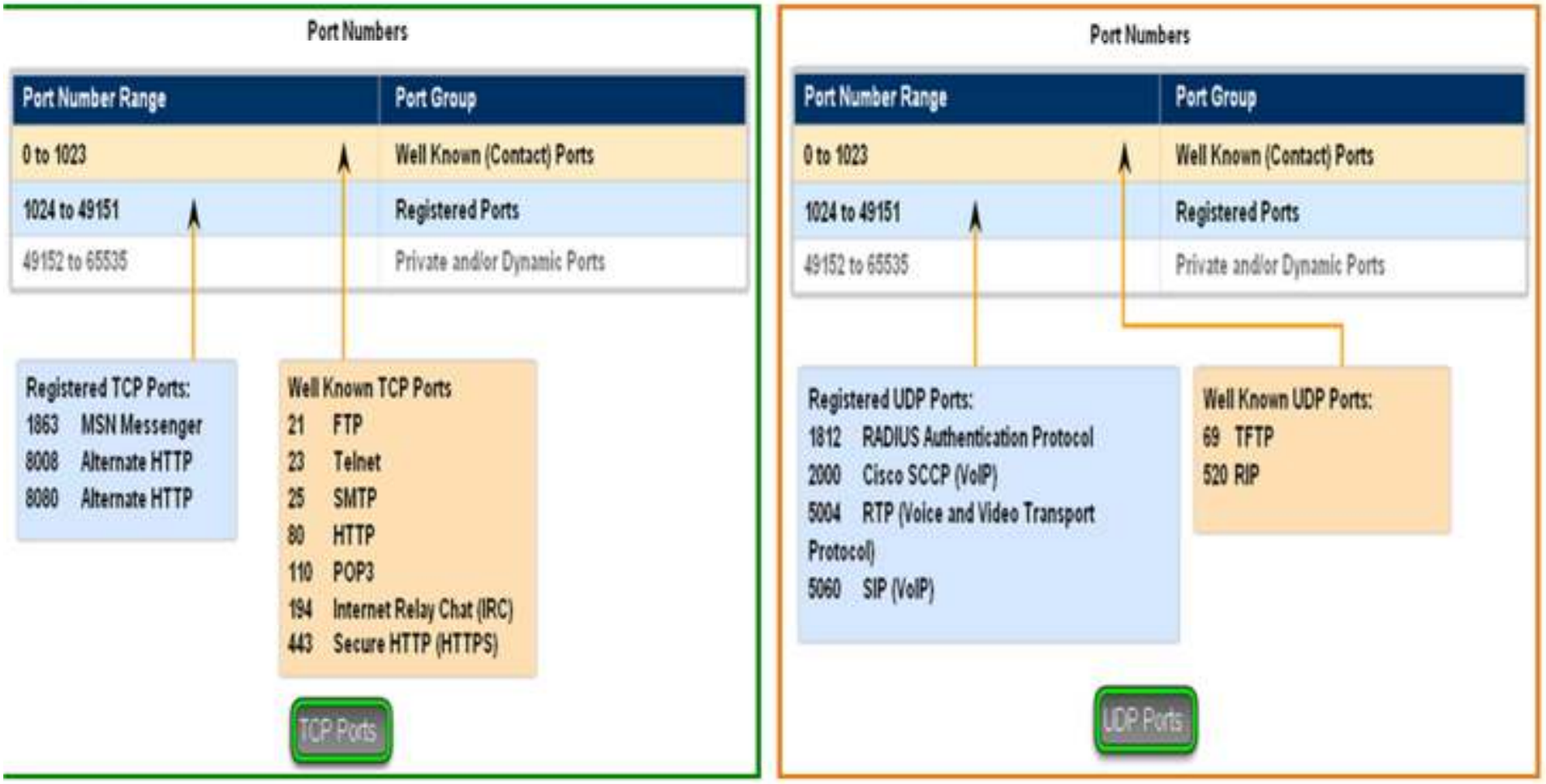
8 Bytes

Transport Layer - TCP and UDP



Data for different applications is directed to the correct application because each application has a unique port number.

Transport Layer - TCP and UDP



Transport Layer - TCP and UDP

Port Numbers

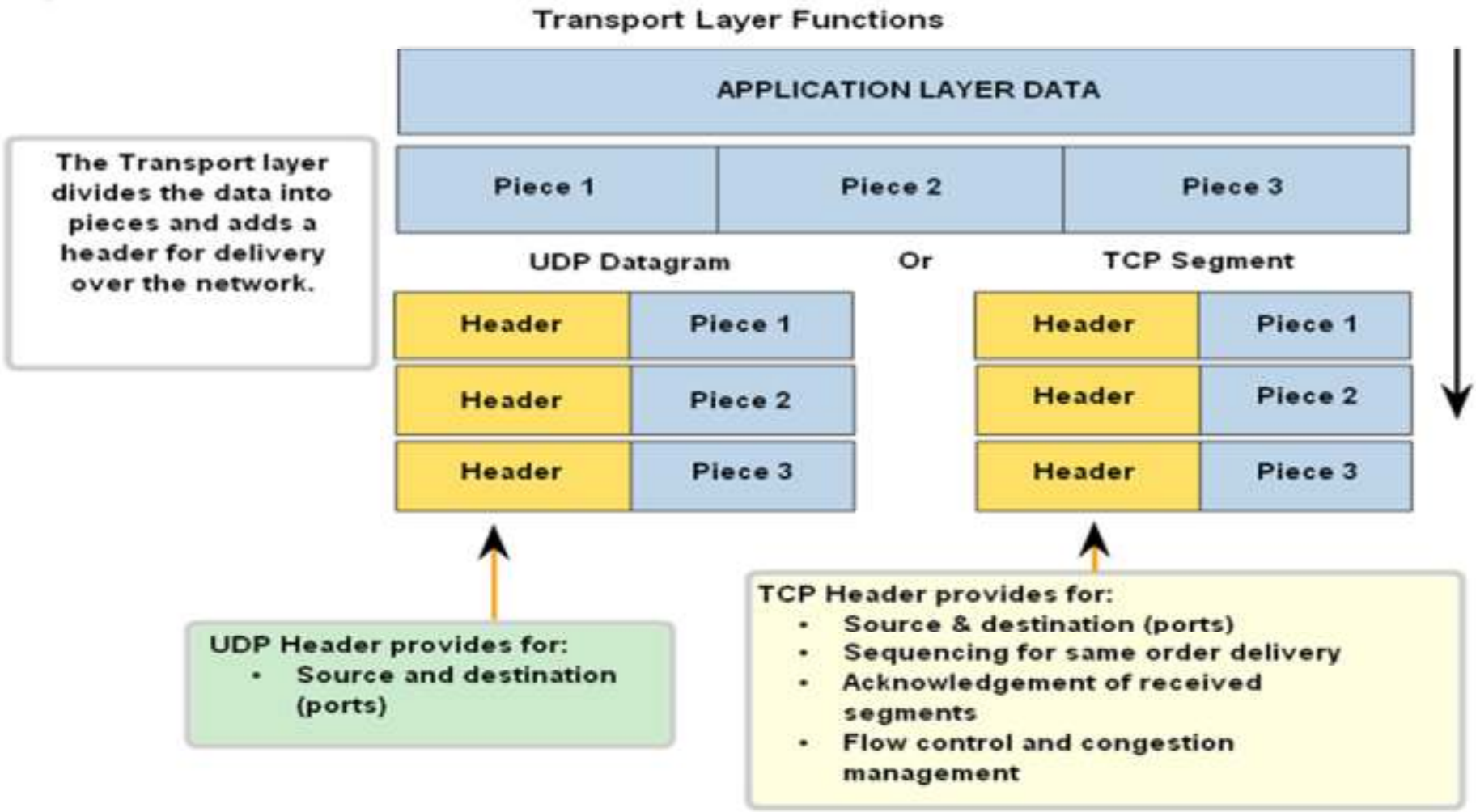
Port Number Range	Port Group
0 to 1023	Well Known (Contact) Ports
1024 to 49151	Registered Ports
49152 to 65535	Private and/or Dynamic Ports

Registered TCP/UDP Common Ports:
1433 MS SQL
2948 WAP (MMS)

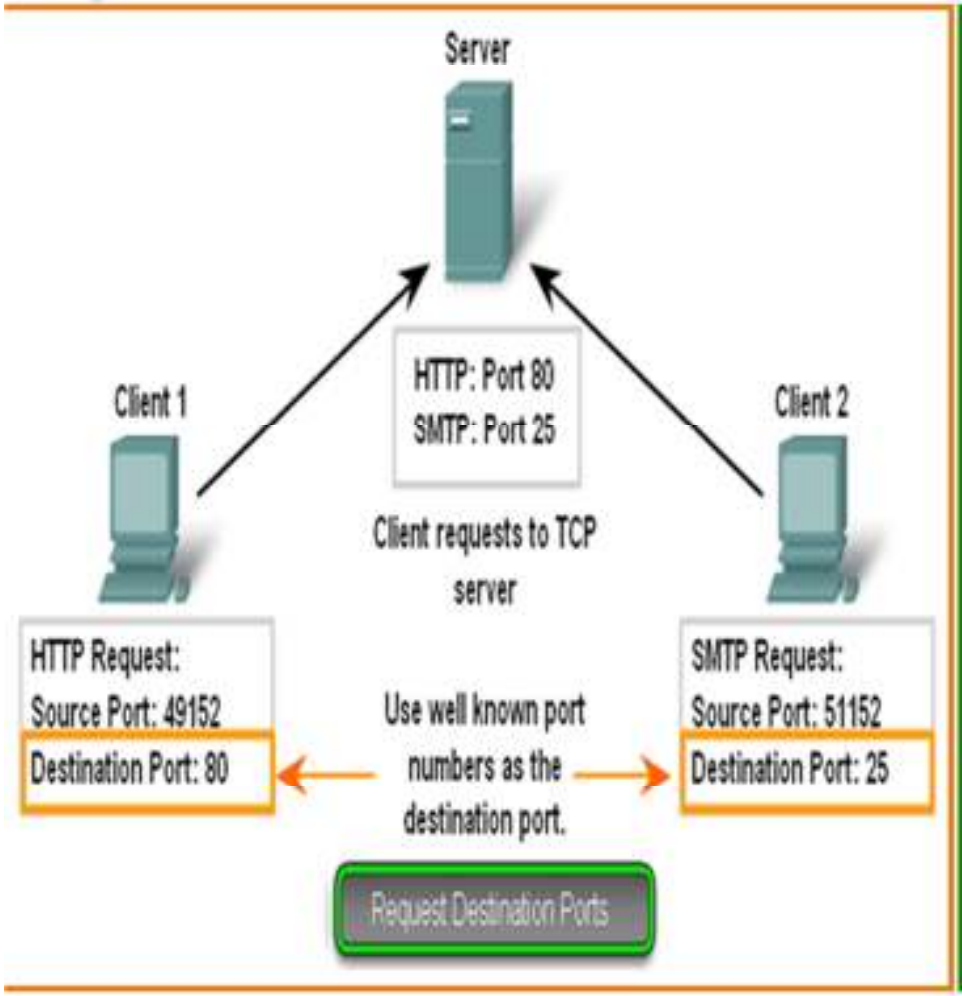
Well Known TCP/UDP Common Ports:
53 DNS
161 SNMP
531 AOL Instant Messenger, IRC

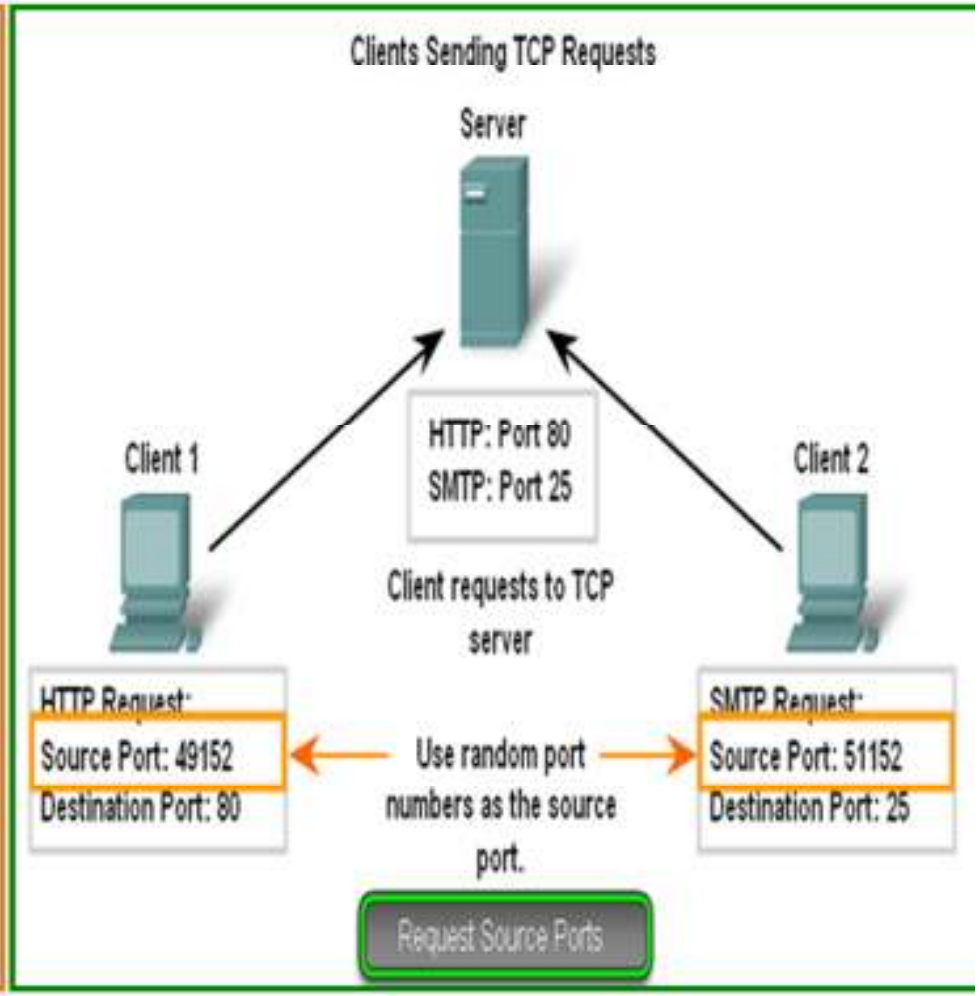
TCP/UDP Common Ports

Transport Layer - TCP and UDP

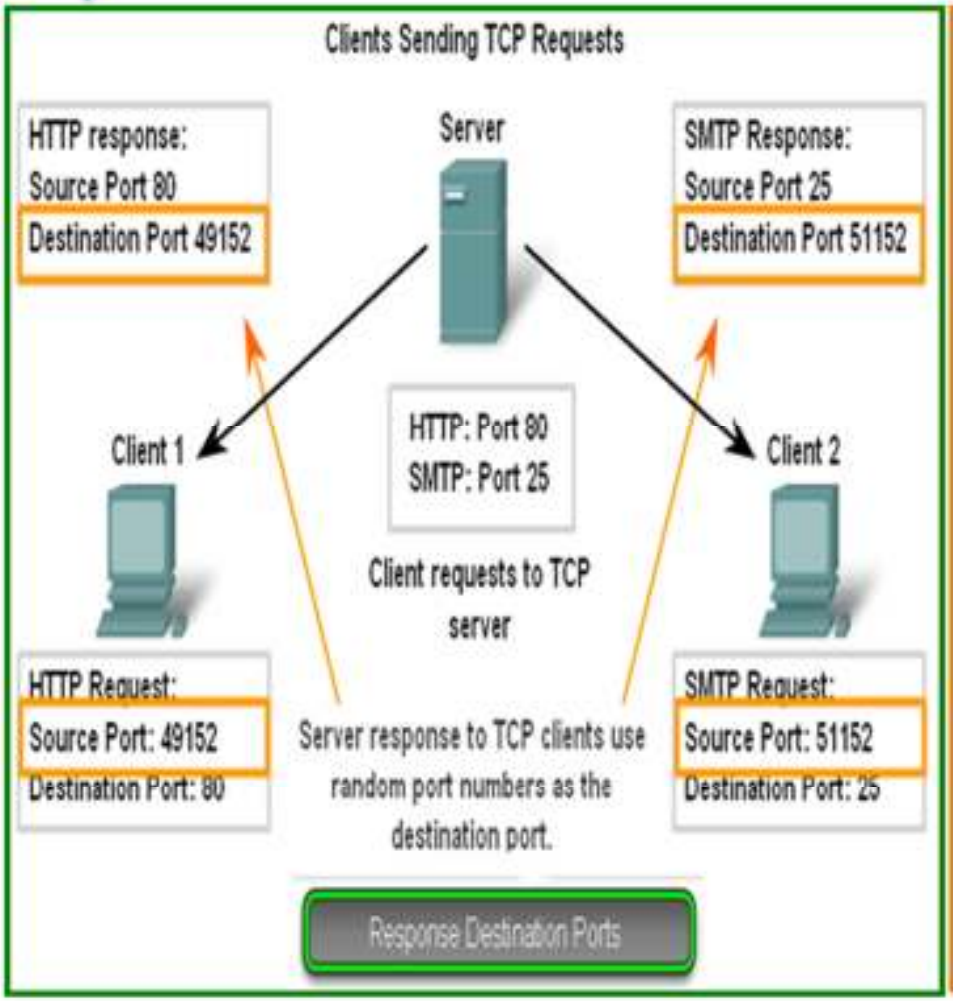


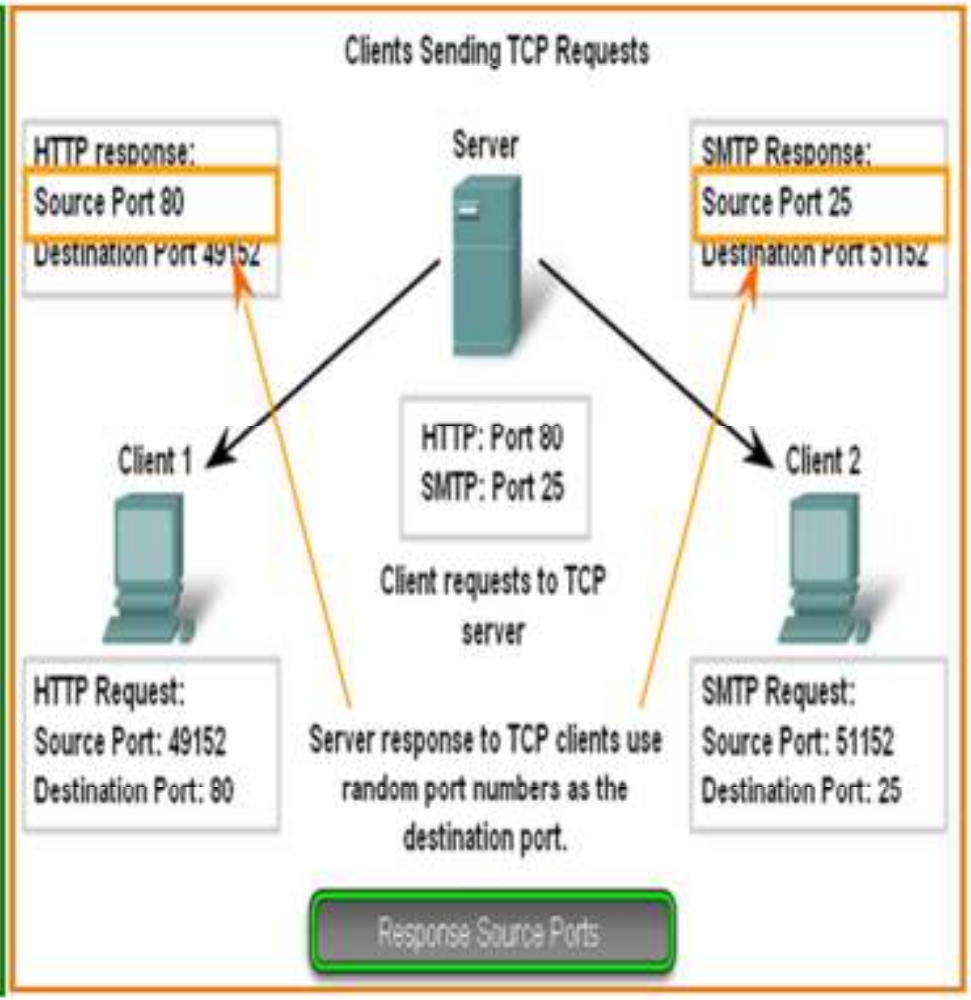
Transport Layer - TCP and UDP



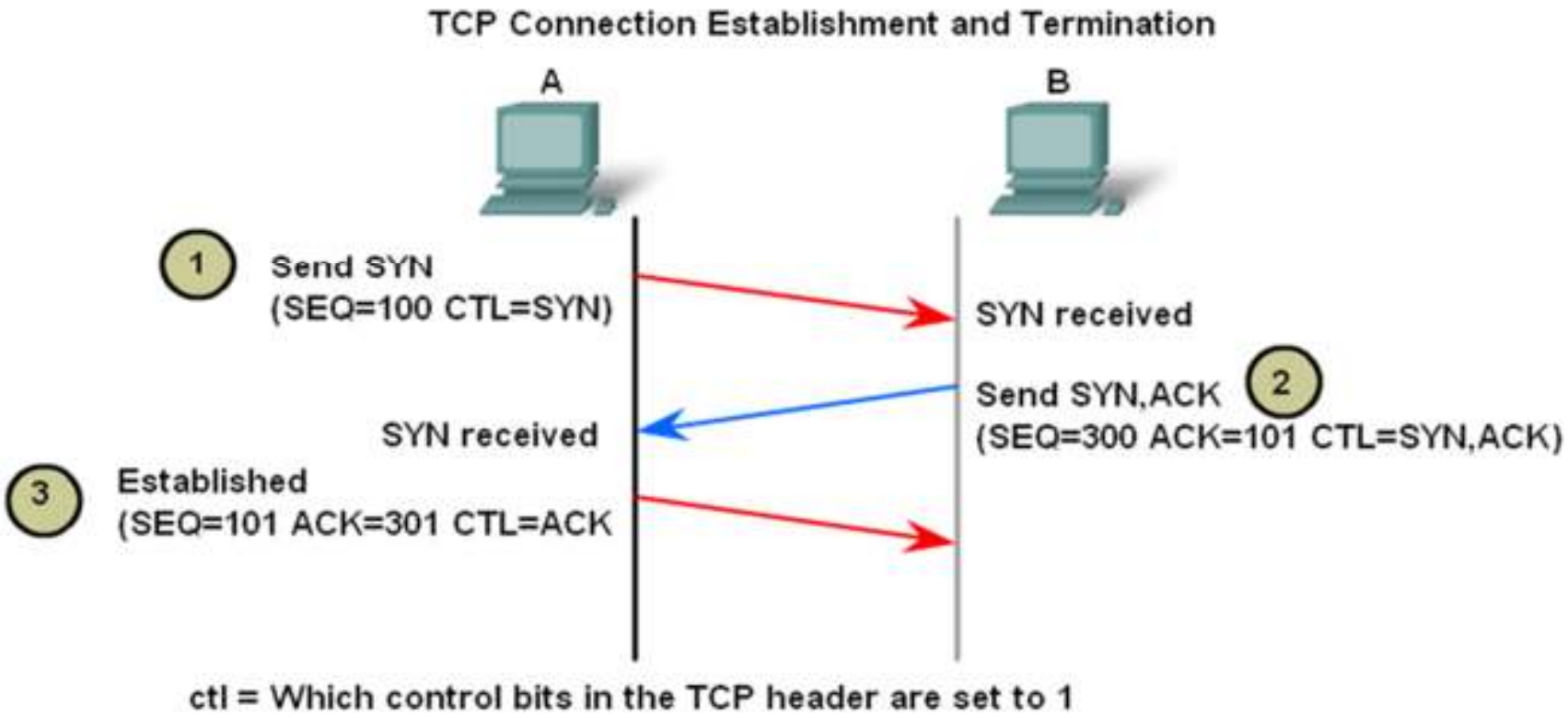


Transport Layer - TCP and UDP

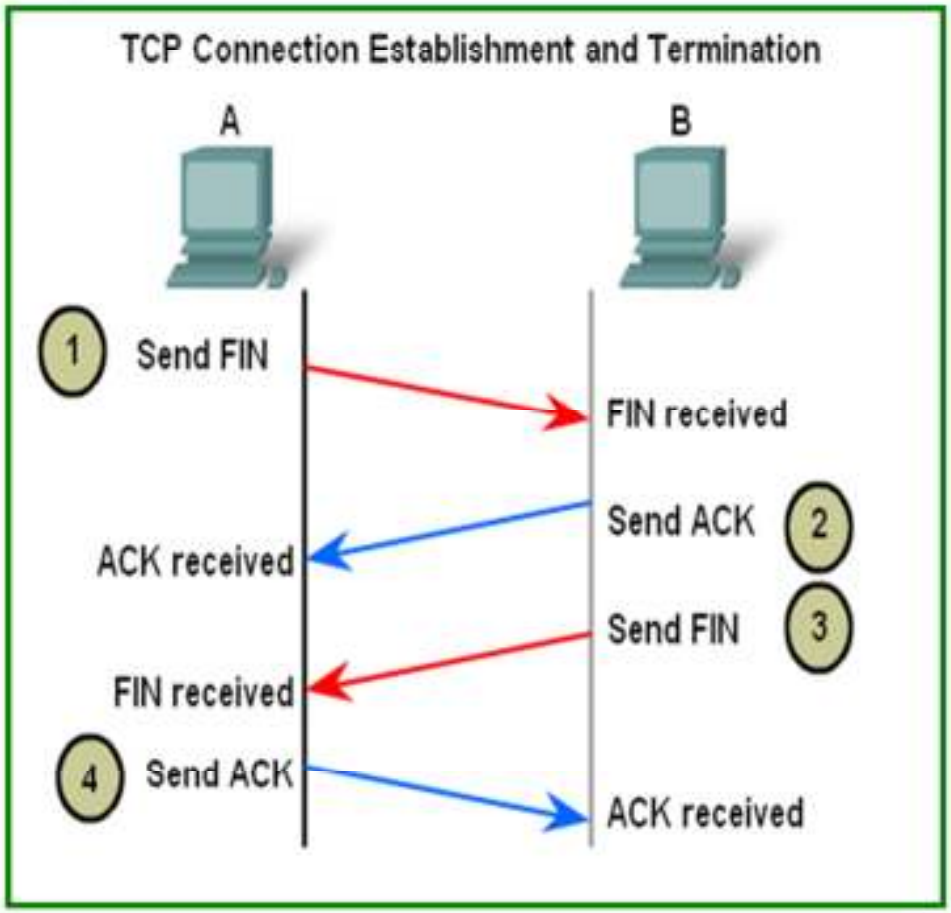


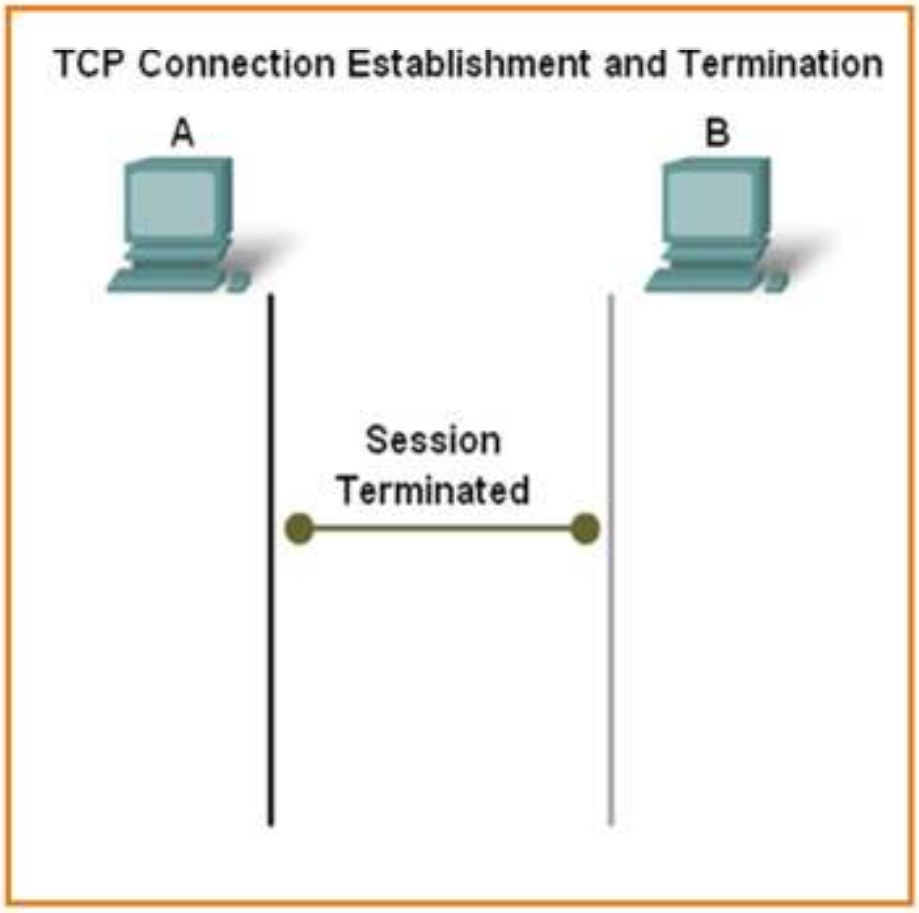


Transport Layer - TCP and UDP

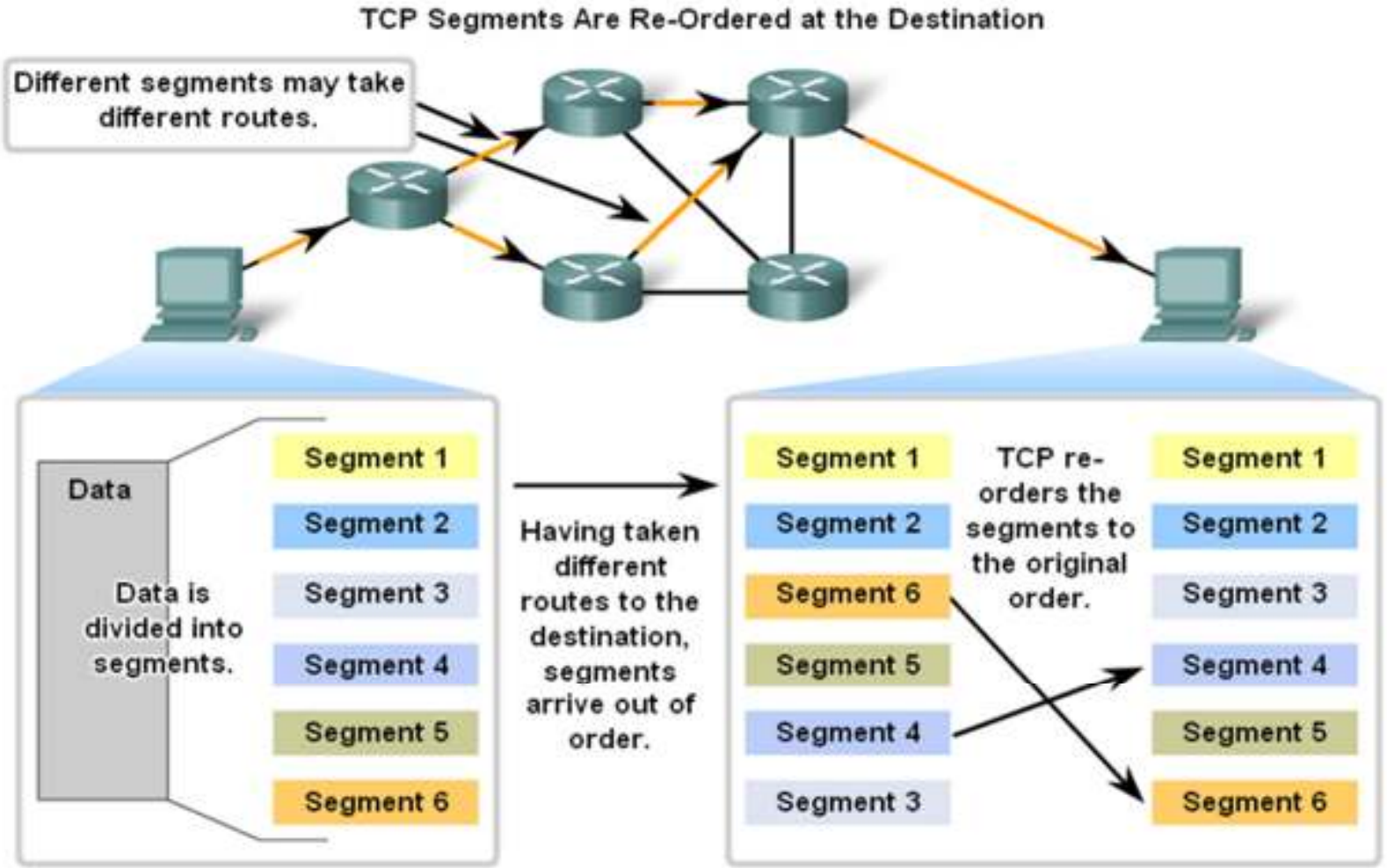


Transport Layer - TCP and UDP

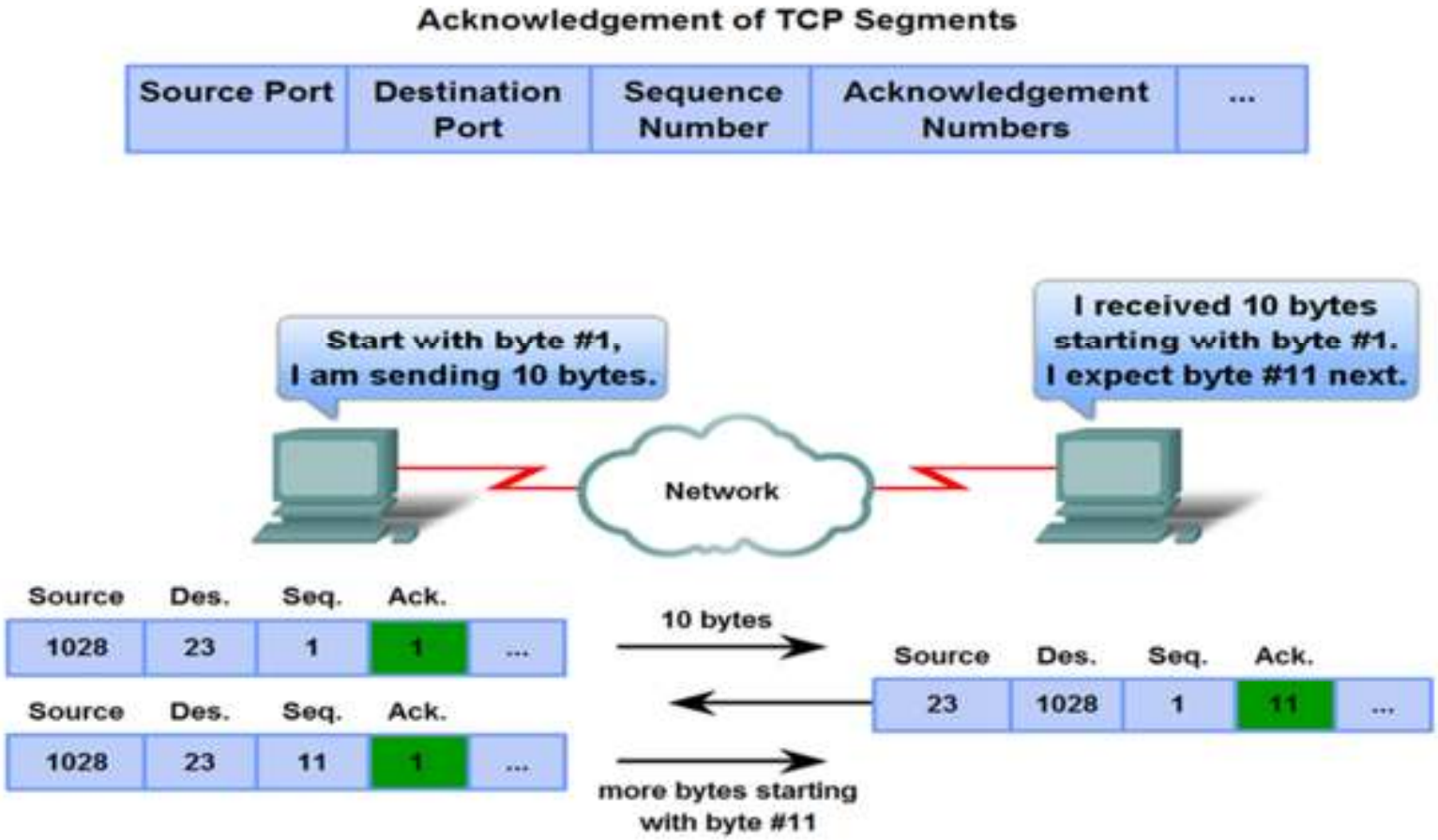




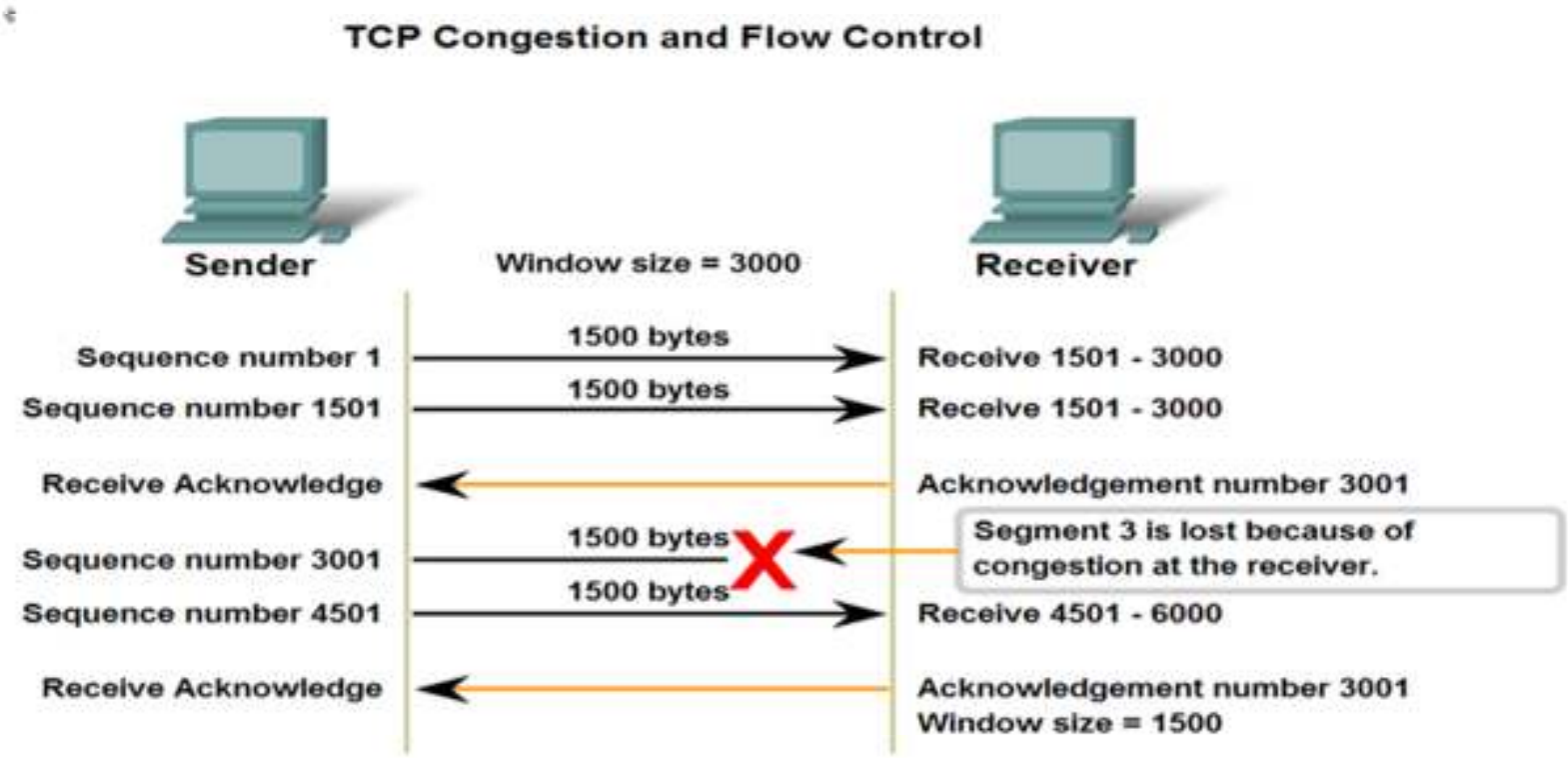
Transport Layer - TCP and UDP



Transport Layer - TCP and UDP



Transport Layer - TCP and UDP



If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

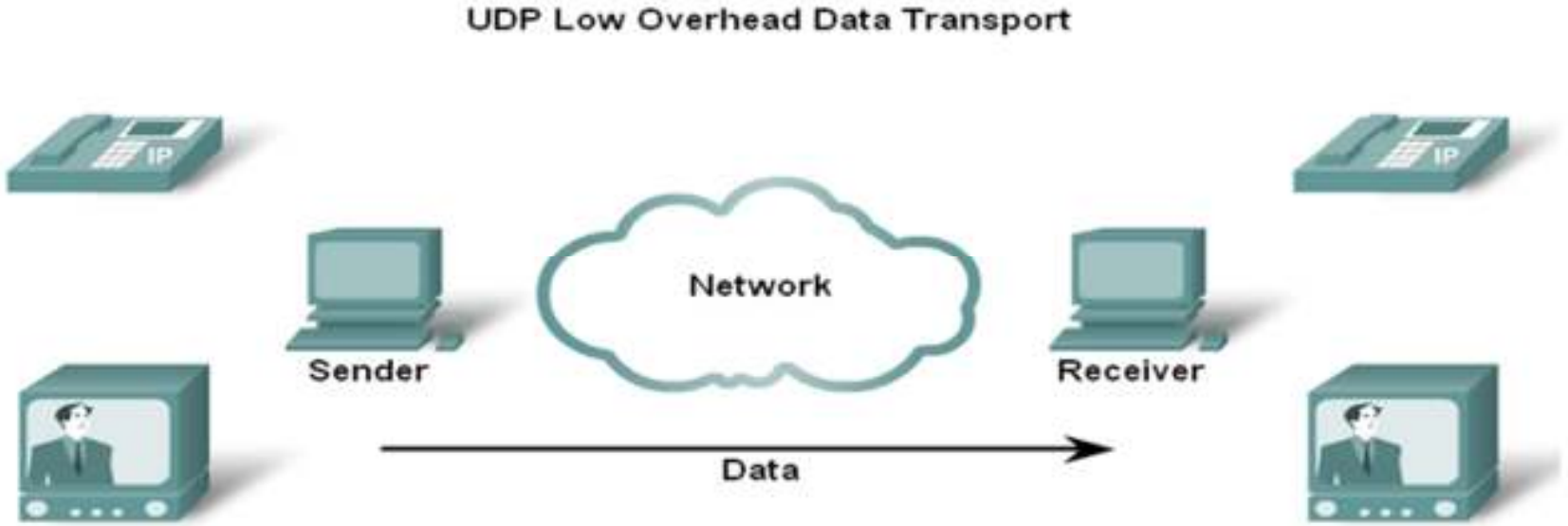
Transport Layer - TCP and UDP

UDP is a simple protocol that provides the basic Transport layer functions. It much lower overhead than TCP, since it is not connection-oriented and does not provide the sophisticated retransmission, sequencing, and flow control mechanisms.

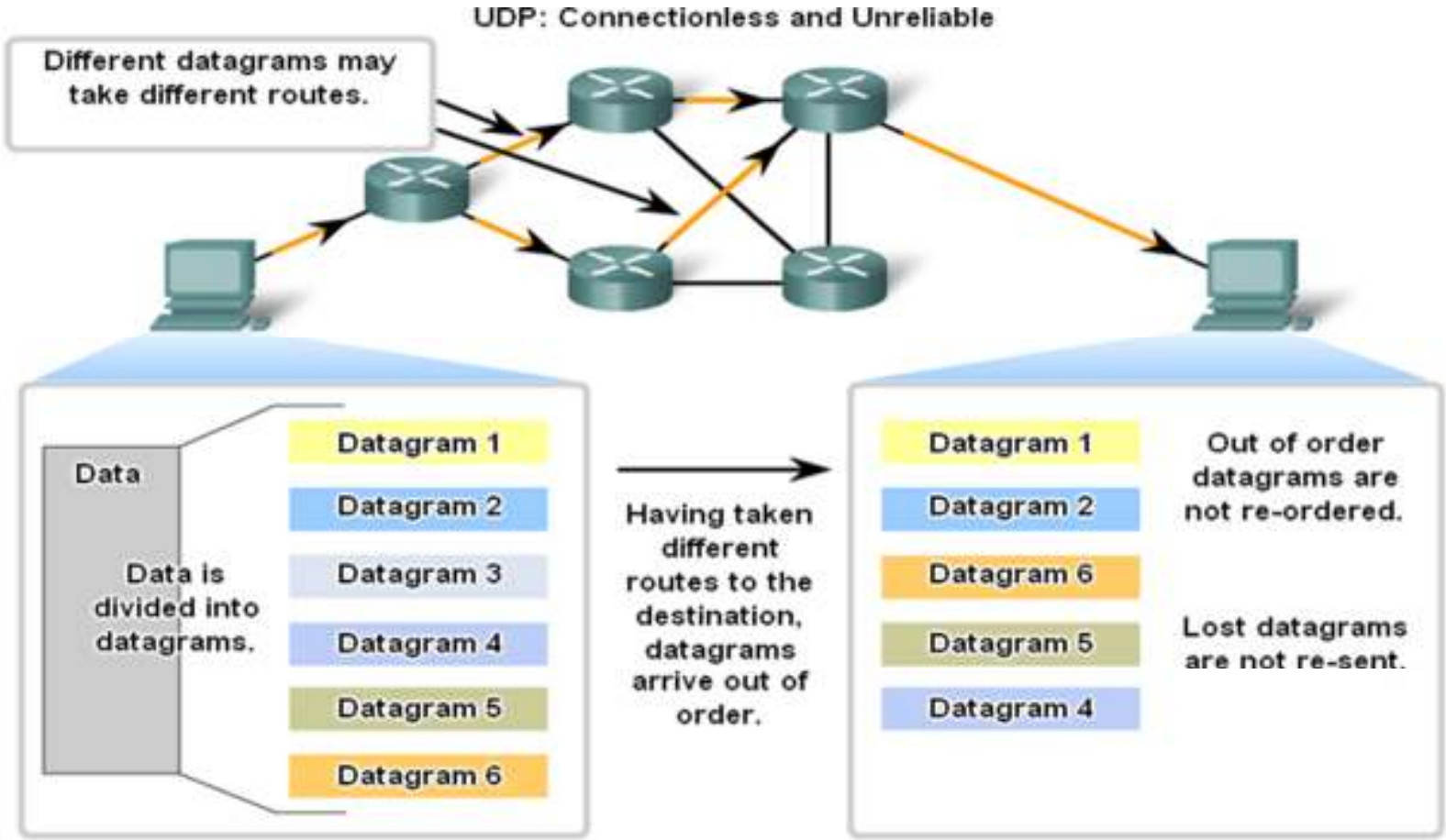
The total amount of UDP traffic found on a typical network is often relatively low, key Application layer protocols that use UDP include:

Domain Name System (DNS)
Simple Network Management Protocol (SNMP)
Dynamic Host Configuration Protocol (DHCP)
Routing Information Protocol (RIP)
Trivial File Transfer Protocol (TFTP)
Online games

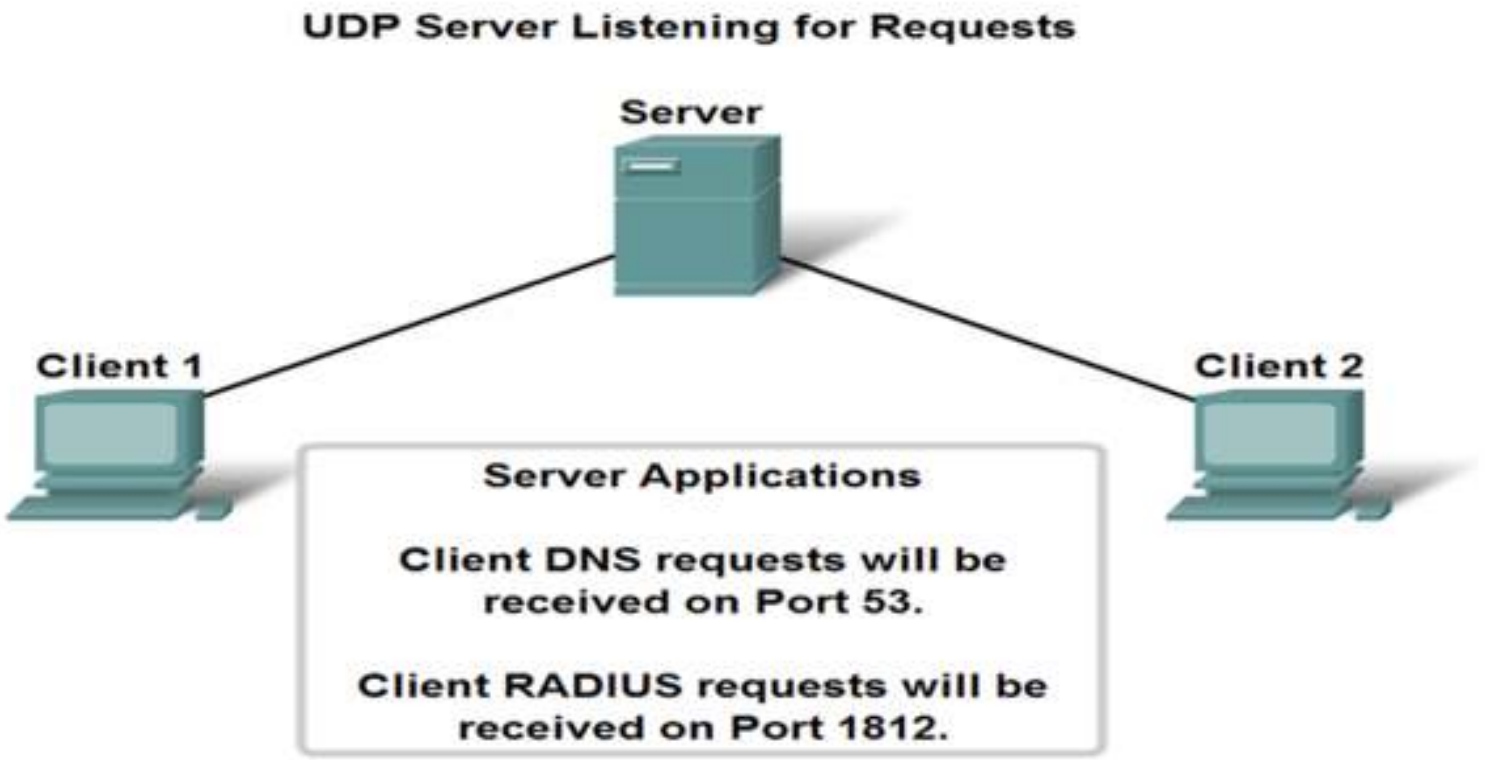
Transport Layer - TCP and UDP



Transport Layer - TCP and UDP

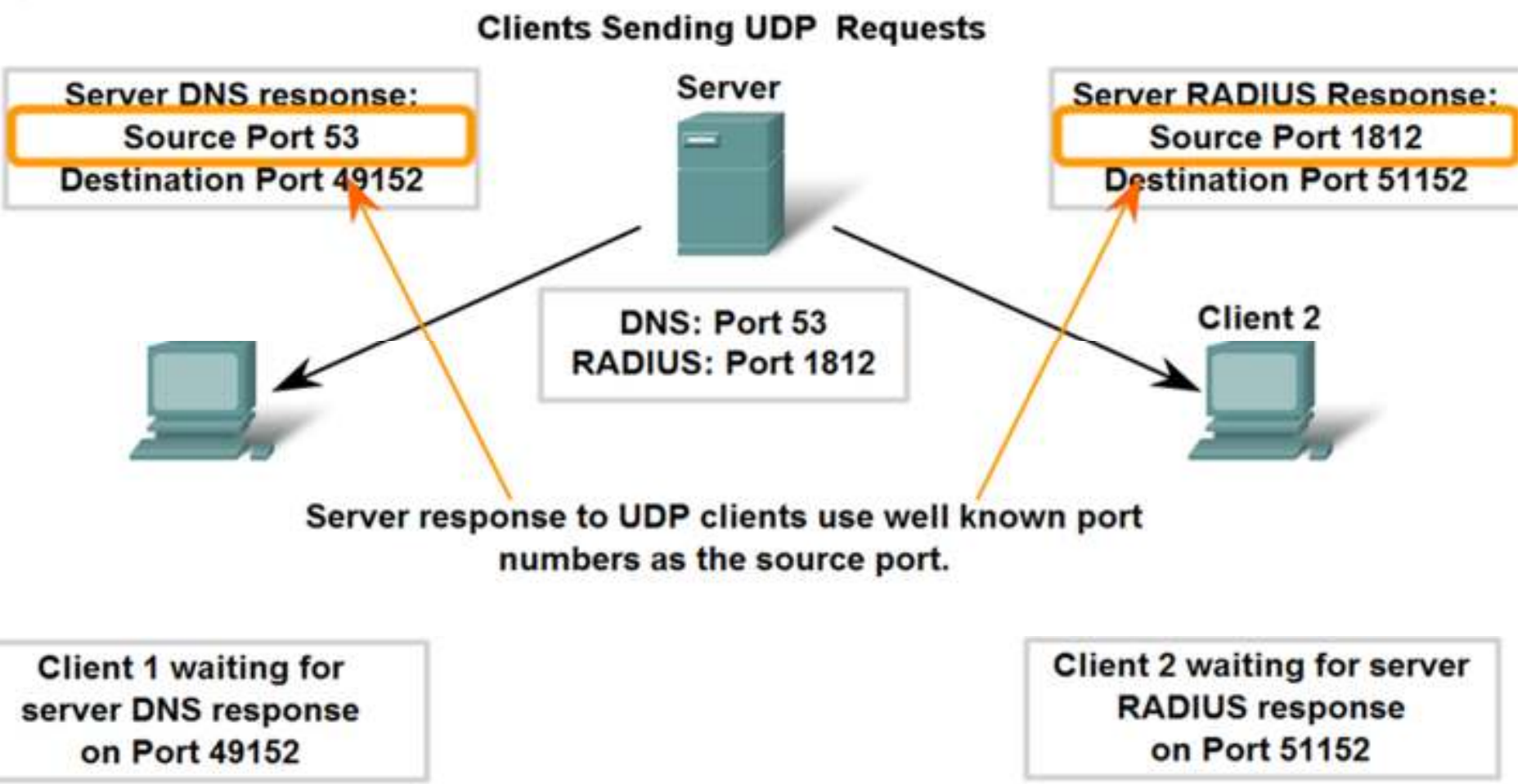


Transport Layer - TCP and UDP



Client requests to servers have well known ports numbers as the destination port.

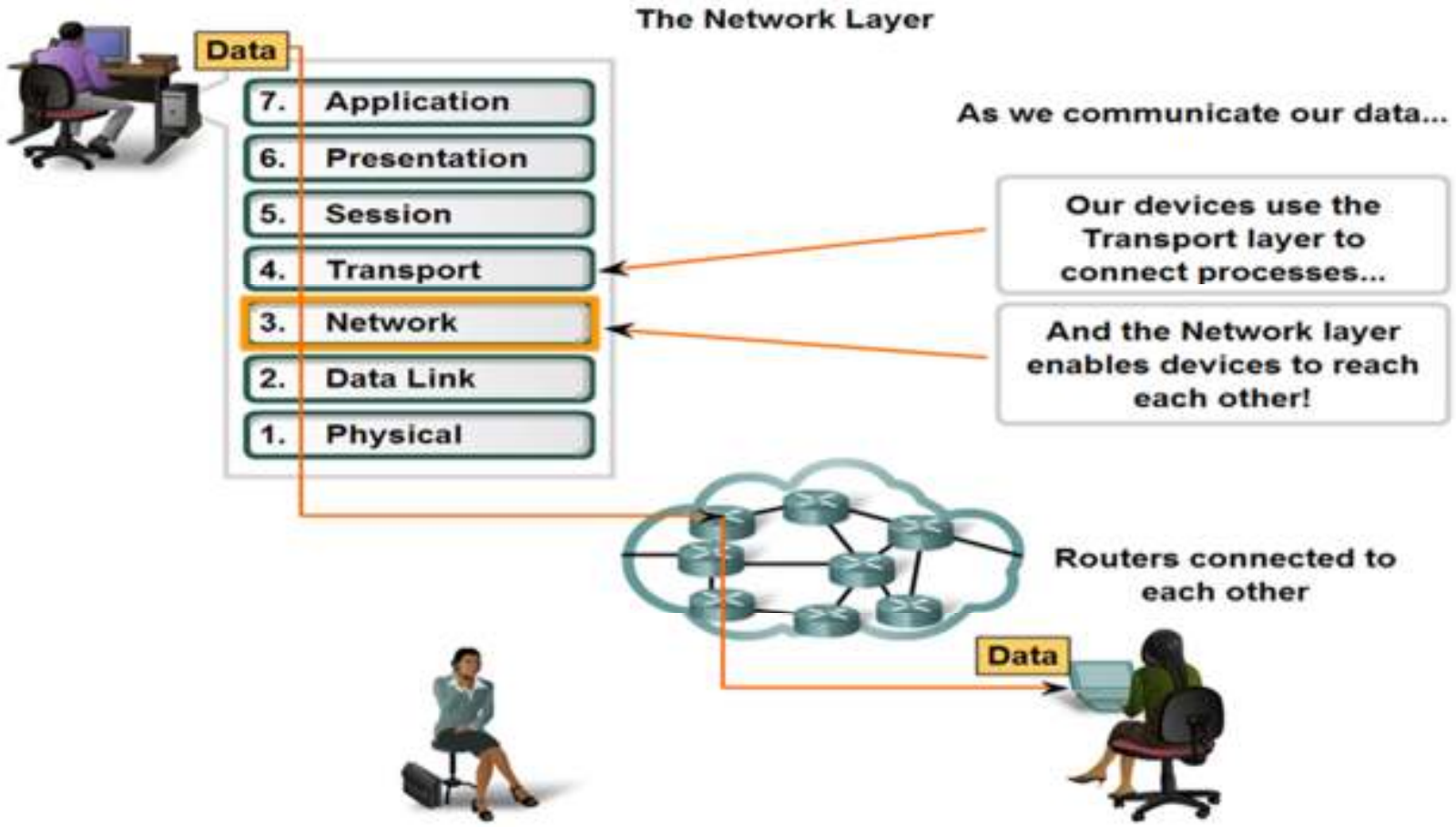
Transport Layer - TCP and UDP



Network Layer

Network Layer

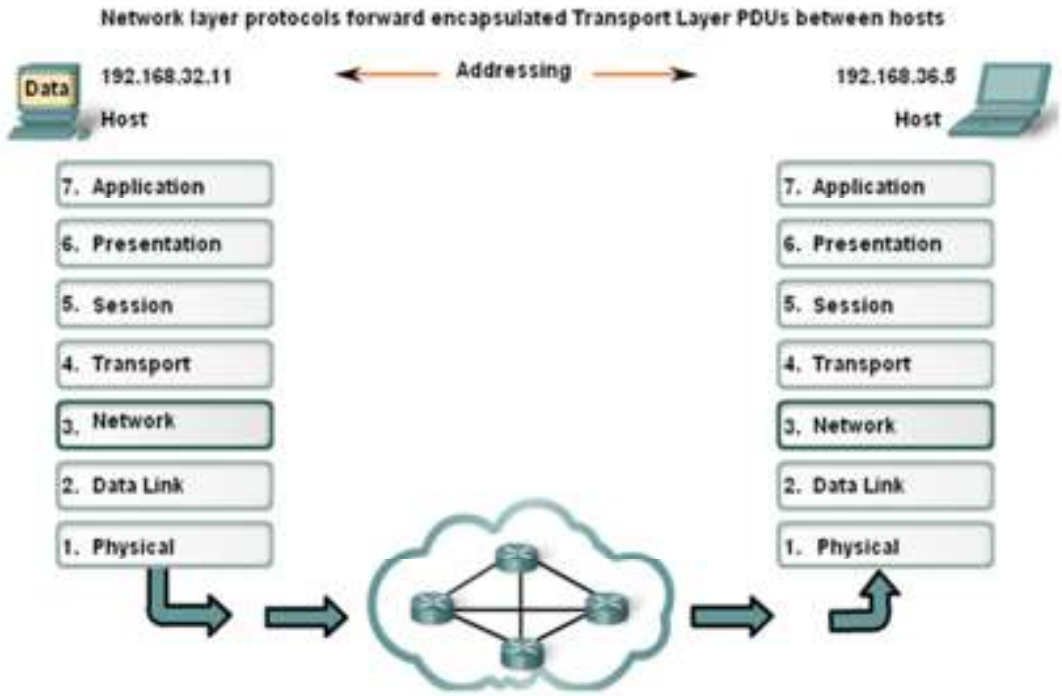
The most significant Network layer (OSI Layer 3) protocol is the Internet Protocol (IP).



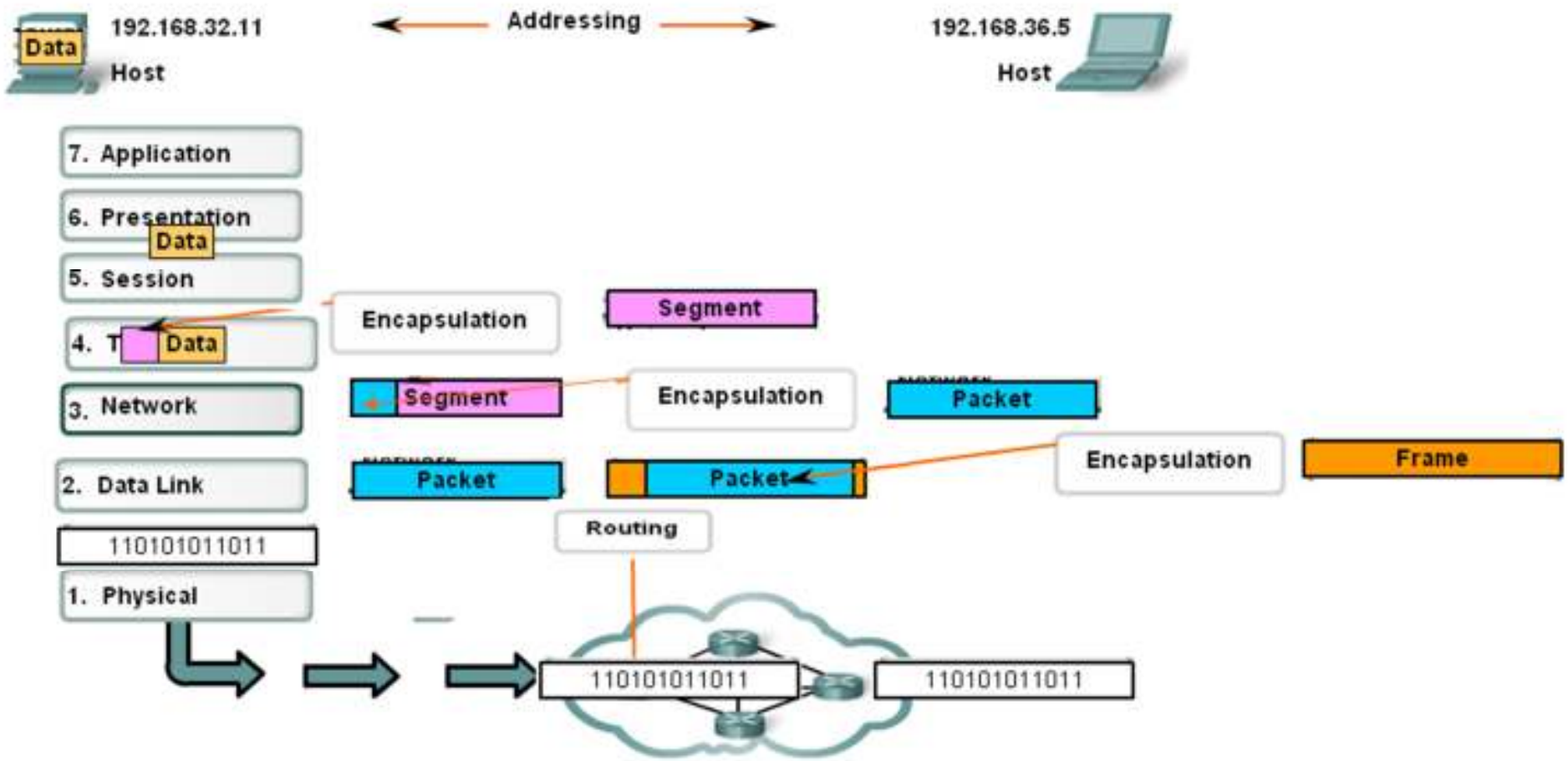
Network Layer

The Network layer, or OSI Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices. To accomplish this end-to-end transport, Layer 3 uses four basic processes:

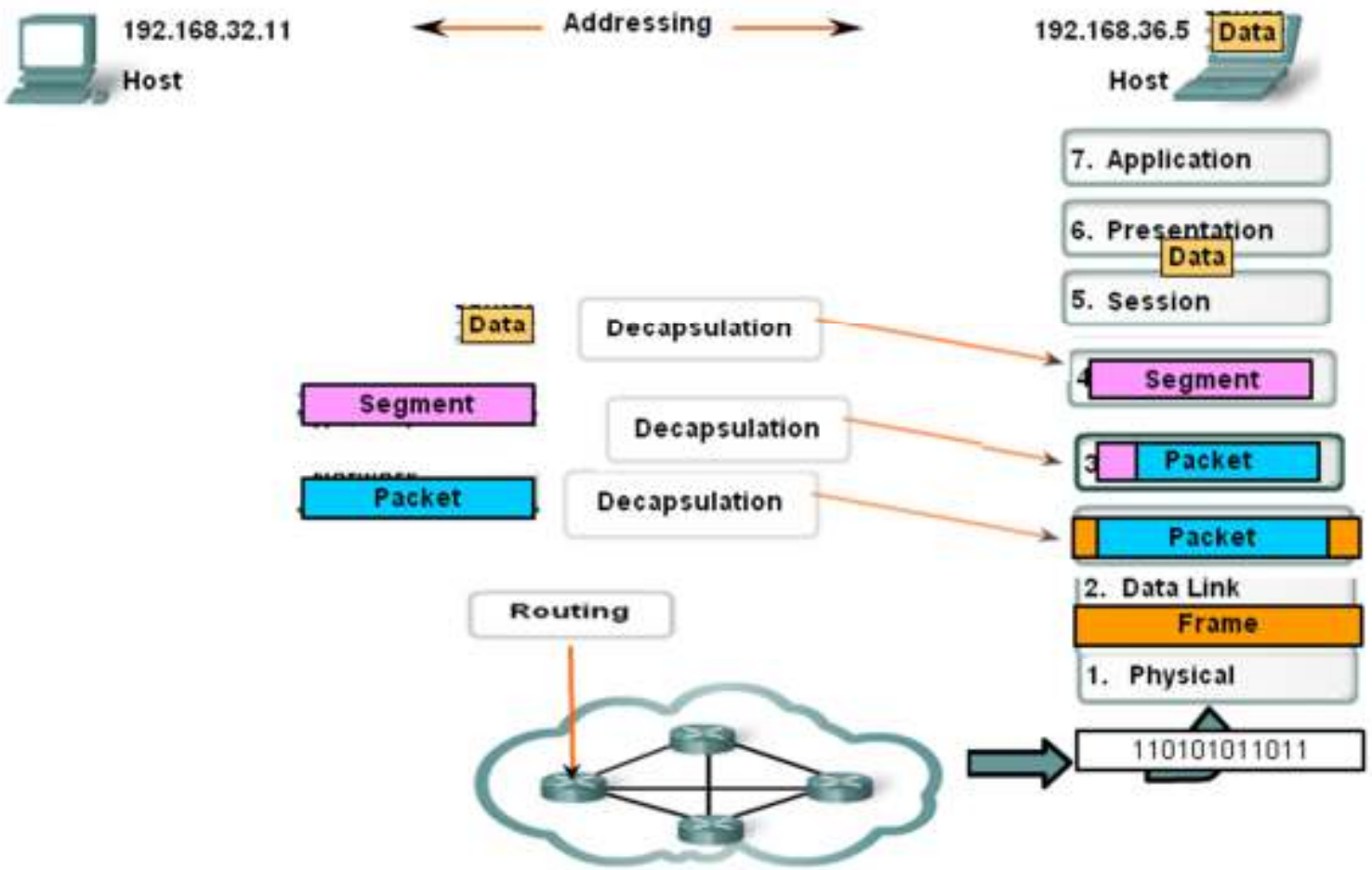
Addressing
Encapsulation
Routing
Decapsulation



Network Layer



Network Layer



Network Layer

Network Layer Protocols

Protocols implemented at the Network layer that carry user data include:

Internet Protocol version 4 (IPv4)

Internet Protocol version 6 (IPv6)

Novell Internetwork Packet Exchange (IPX)

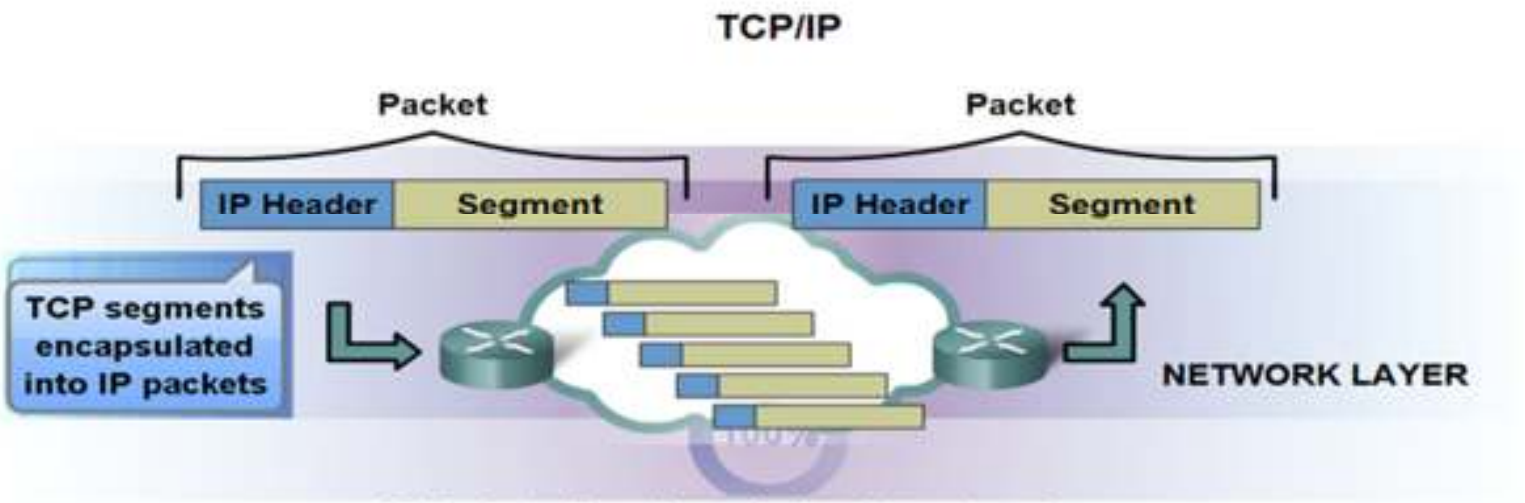
AppleTalk

Connectionless Network Service (CLNS/DECNet)

The Internet Protocol (IPv4 and IPv6) is the most widely-used Layer 3 data carrying protocol.

Network Layer

The Internet Protocol was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets. These functions are performed by other protocols in other layers.

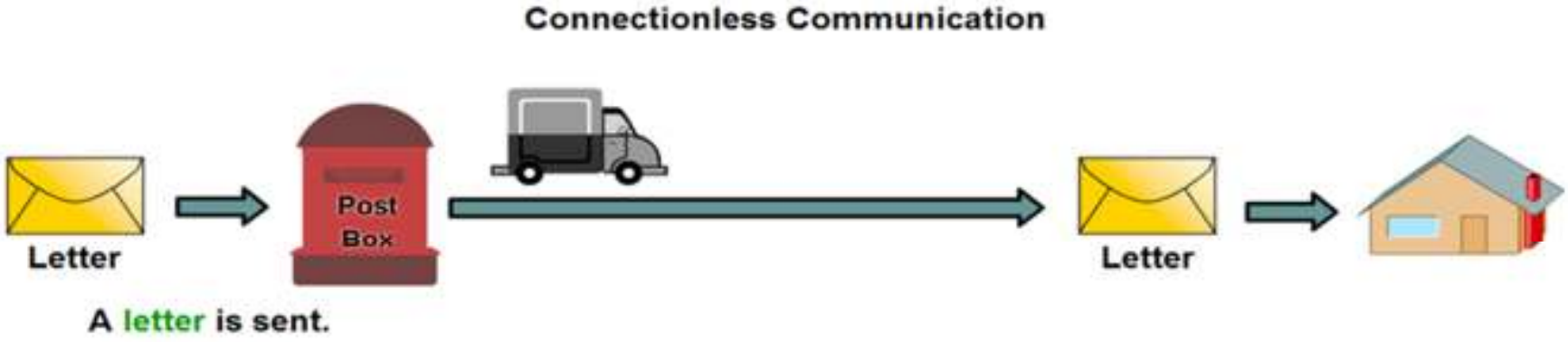


IP Packets flow through the internetwork.

- **Connectionless - No connection is established before sending data packets.**
- **Best Effort (unreliable) - No overhead is used to guarantee packet delivery.**
- **Media Independent - Operates independently of the medium carrying the data.**

Network Layer

Connectionless Service Postal Networks



The sender doesn't know:

- if the receiver is present
- if the letter arrived
- if the receiver can read the letter

The receiver doesn't know:

- when it is coming

Network Layer

Connectionless Service Data Networks

The sender doesn't know:

- if the receiver is present
- if the packet arrived
- if the receiver can read the packet

The receiver doesn't know:

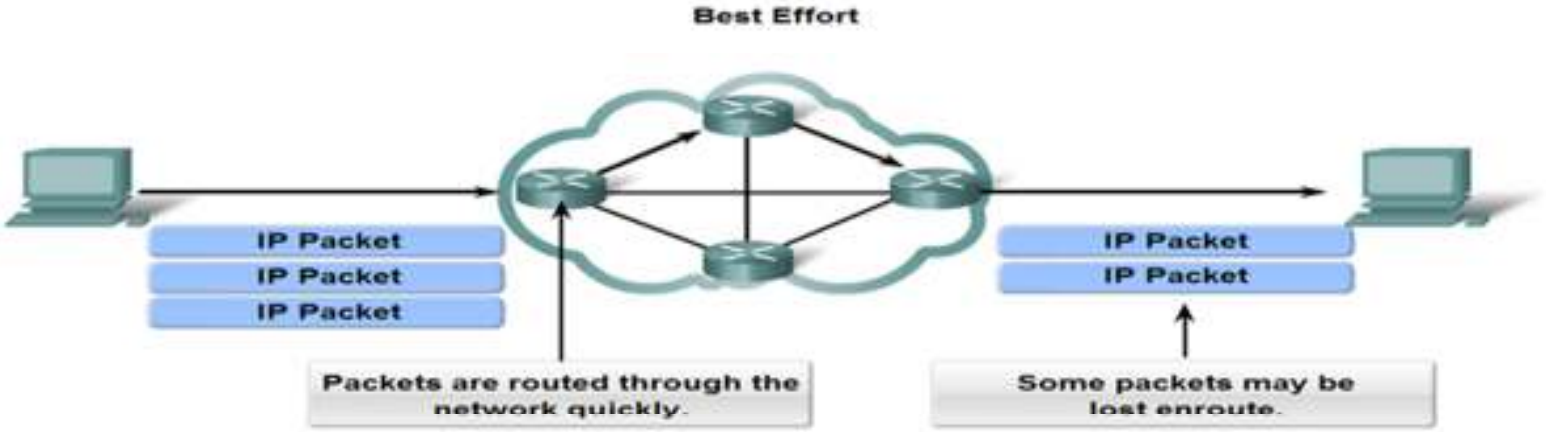
- when it is coming

Network Layer

Best Effort Service (unreliable)

Unreliable means simply that IP does not have the capability to manage, and recover from, undelivered or corrupt packets.

Since protocols at other layers can manage reliability, IP is allowed to function very efficiently at the Network layer.



As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

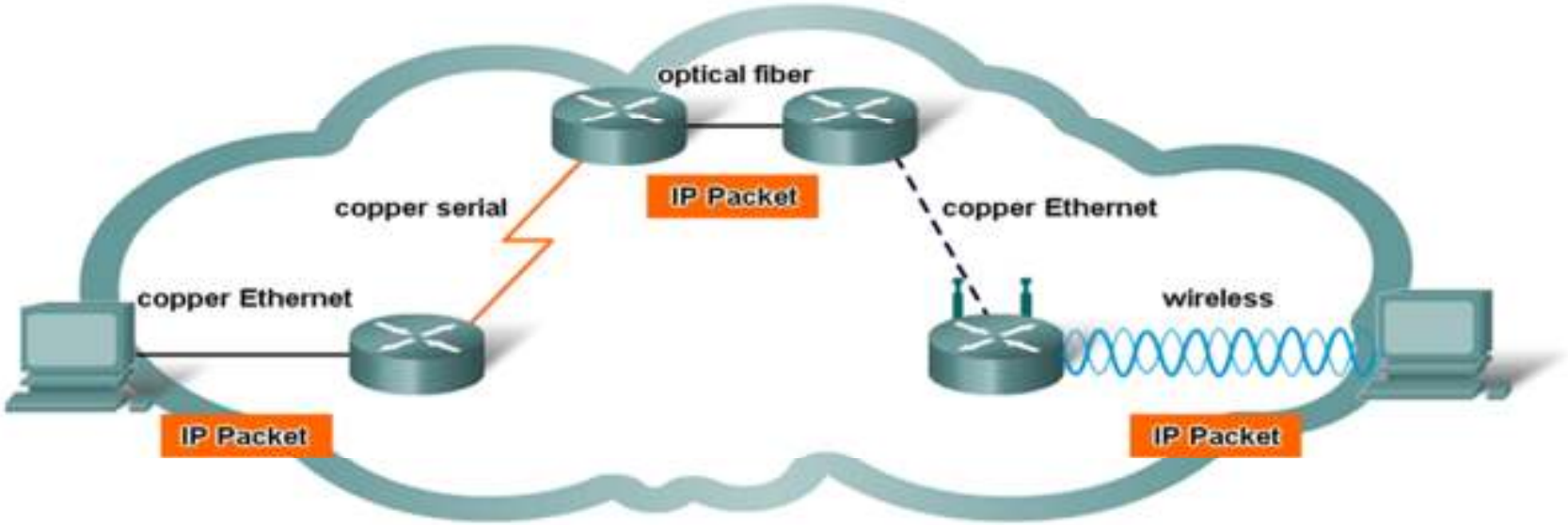
Other protocols manage the process of tracking packets and ensuring their delivery.

Network Layer

Media Independent

Any individual IP packet can be communicated electrically over cable, as optical signals over fiber, or wirelessly as radio signals.

Media Independence



IP packets can travel over different media.

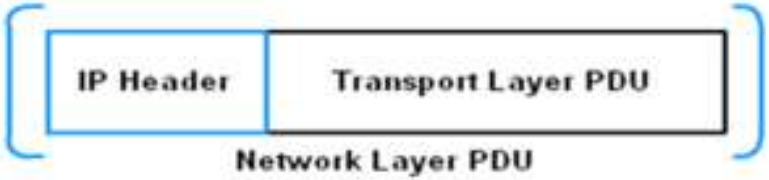
Network Layer

The Transport layer adds a header so segments can be accounted for and reordered at the destination.

Transport Layer Encapsulation

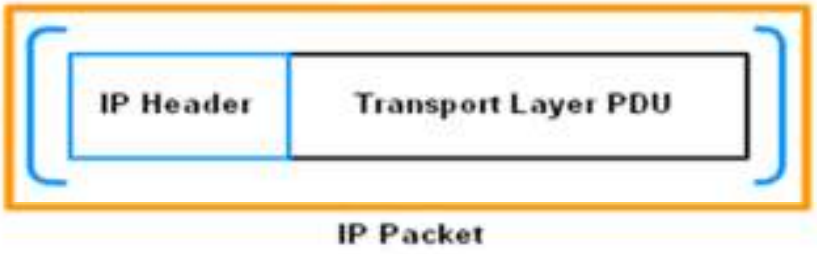
The Network layer adds a header so packets can be routed through complex networks and reach their destination.

Network Layer Encapsulation



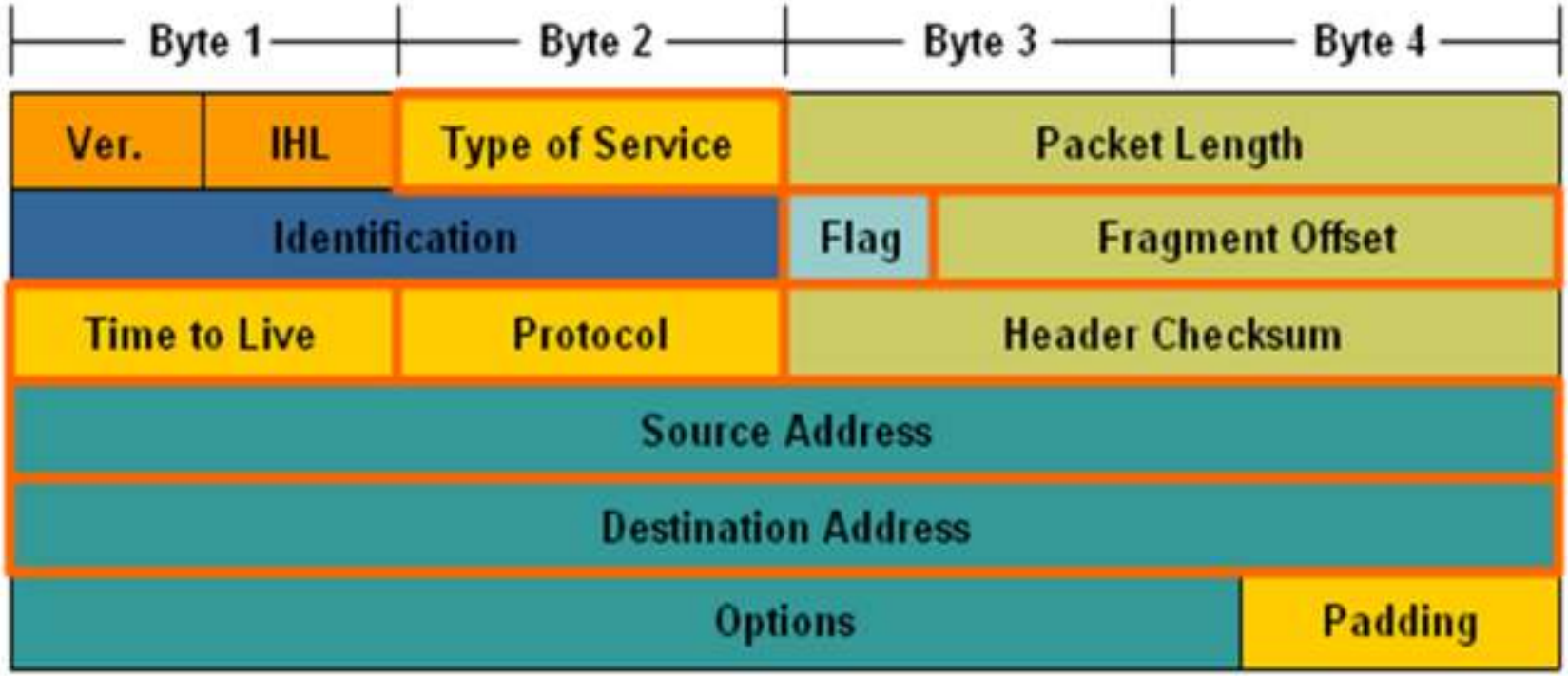
In TCP/IP based networks, the Network layer PDU is the IP packet.

Network Layer Encapsulation



In all cases, the data portion of the packet - that is, the encapsulated Transport layer PDU - remains unchanged during the Network layer processes.

Network Layer – IPv4 Packet Header fields

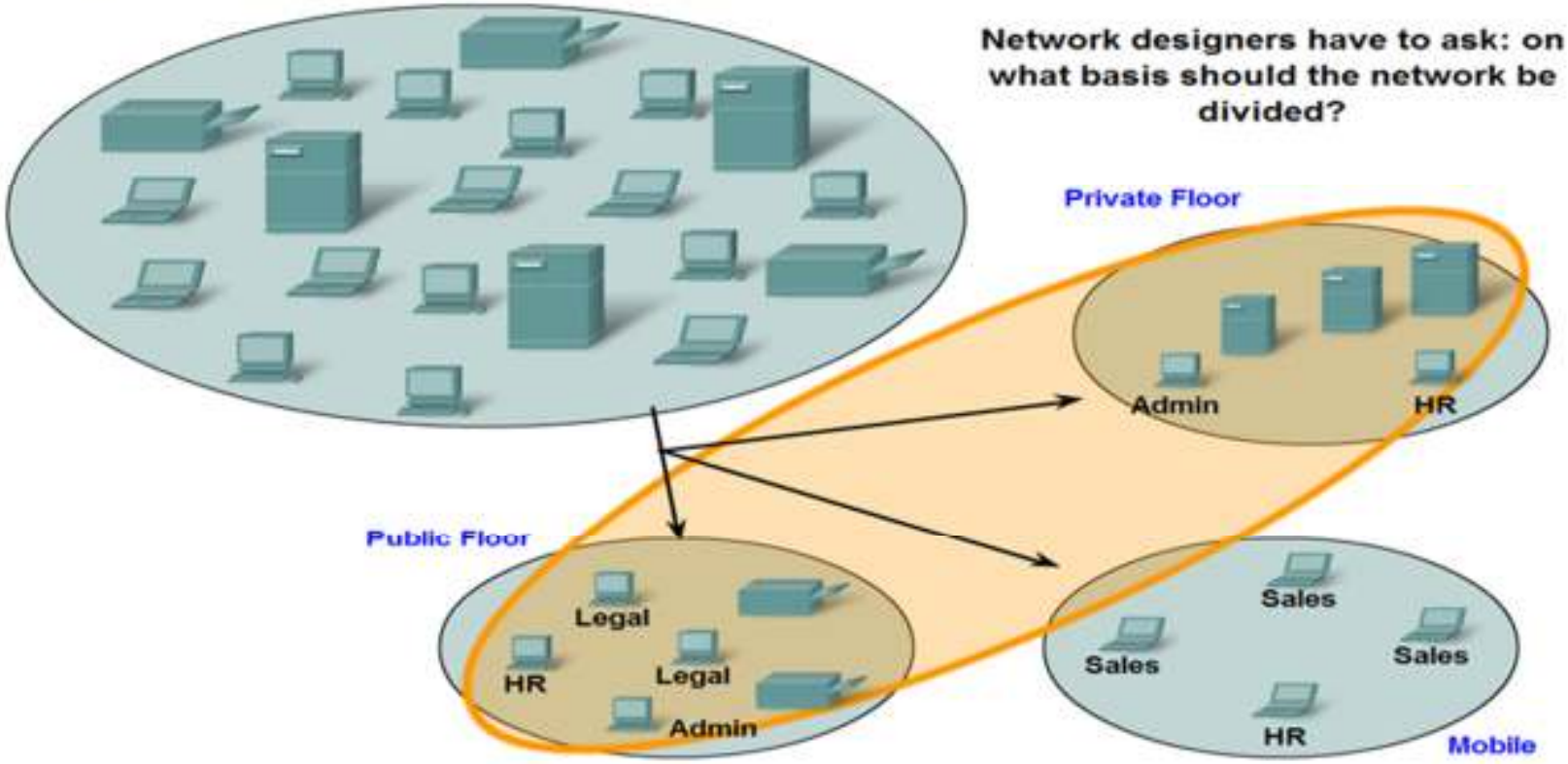


Network Layer

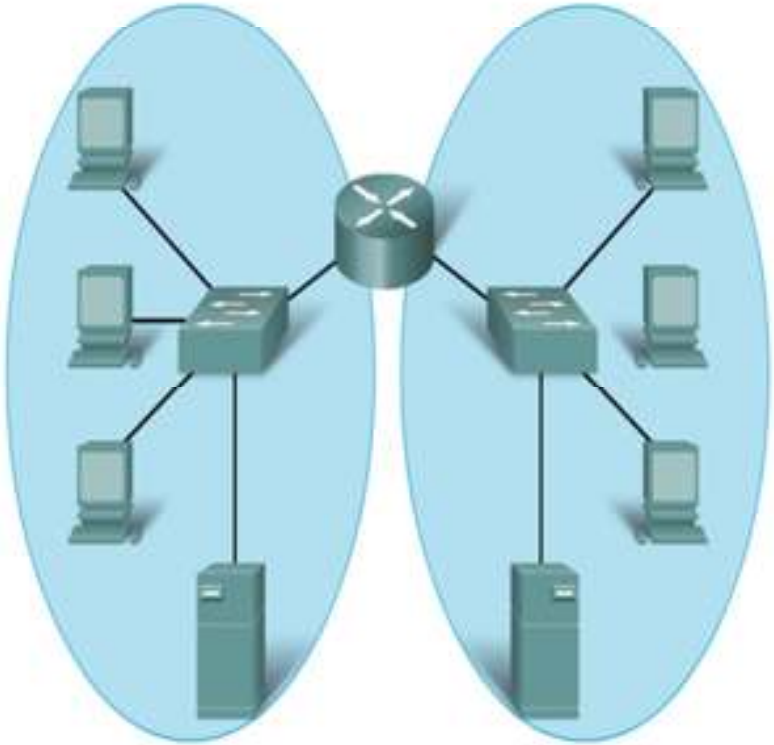
Version - Contains the IP version number (4)
Header Length (IHL) - Specifies the size of the packet header
Type-of-Service The Type-of-Service field contains an 8-bit binary value that is used to determine the priority of each Packet.
Packet Length - This field gives the entire packet size, including header and data, in bytes.
Identification - This field is primarily used for uniquely identifying fragments of an original IP packet
Fragment Offset - MTU Related issues addressing
Flag -- More Fragments Flag and Don't Fragment flag
Time-to-Live - The Time-to-Live (TTL) is an 8-bit binary value that indicates the remaining "life" of the packet. (routing loop)
Protocol - This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol.Example values are: 01 ICMP ,06 TCP and 17 UDP
Header Checksum - The checksum field is used for error checking the packet header.
IP Source Address - The IP Source Address field contains a 32-bit binary value that represents the packet source Network layer host address.
Destination Address -The IP Destination Address field contains a 32-bit binary value that represents the packet destination Network layer host address.
Options - There is provision for additional fields in the IPv4 header to provide other services but these are rarely used.
Padding - Used as a filler to guarantee that the data starts on a 32 bit boundary.

Network Layer

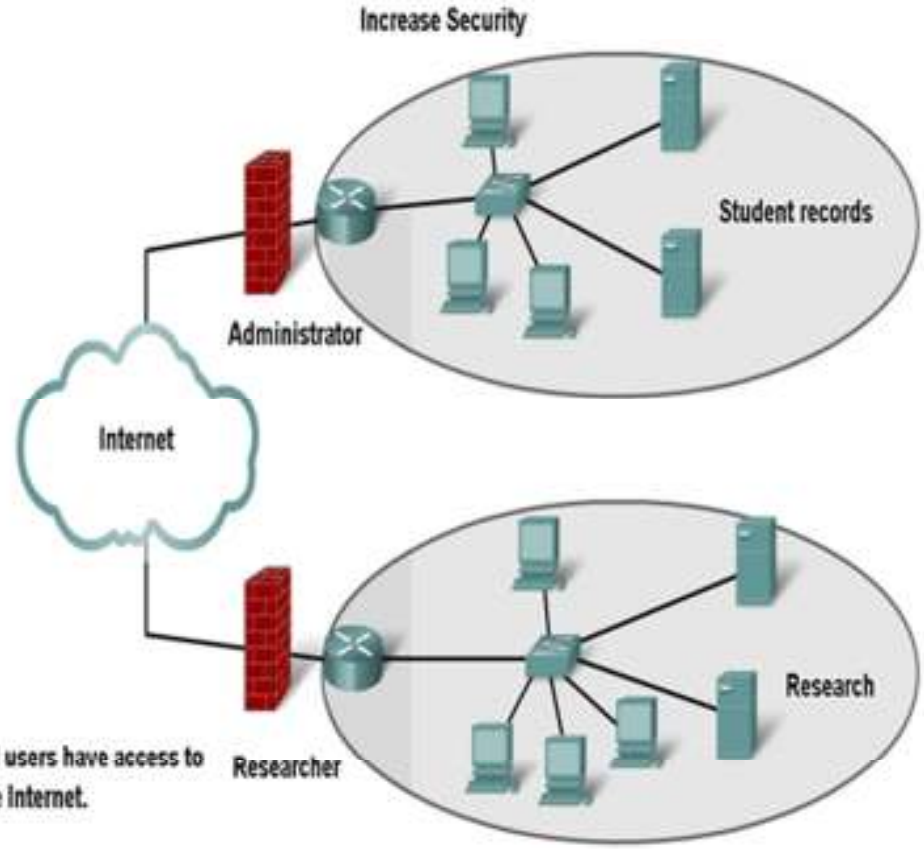
One of the major roles of the Network layer is to provide a mechanism for addressing hosts. As the number of hosts on the network grows, more planning is required to manage and address the network.



Network Layer



Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

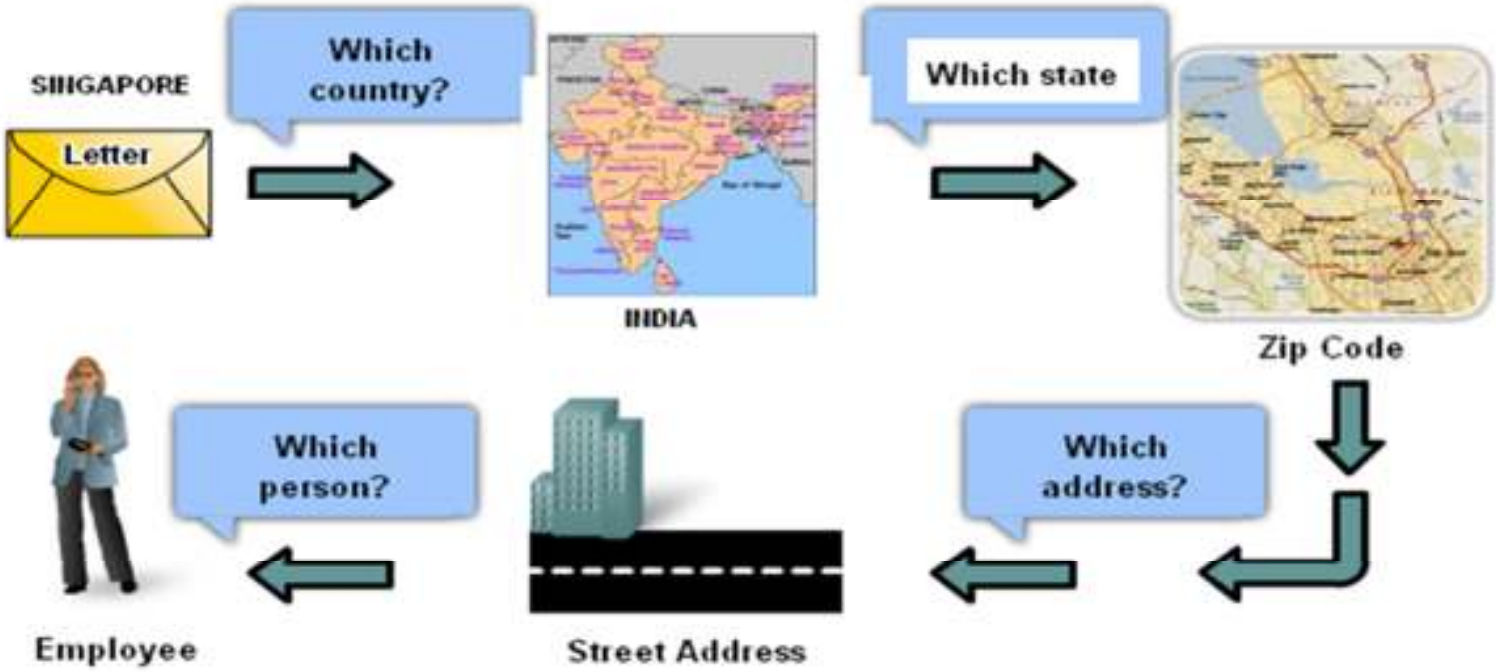


All users have access to the Internet.

Network Layer

Hierarchical Addressing

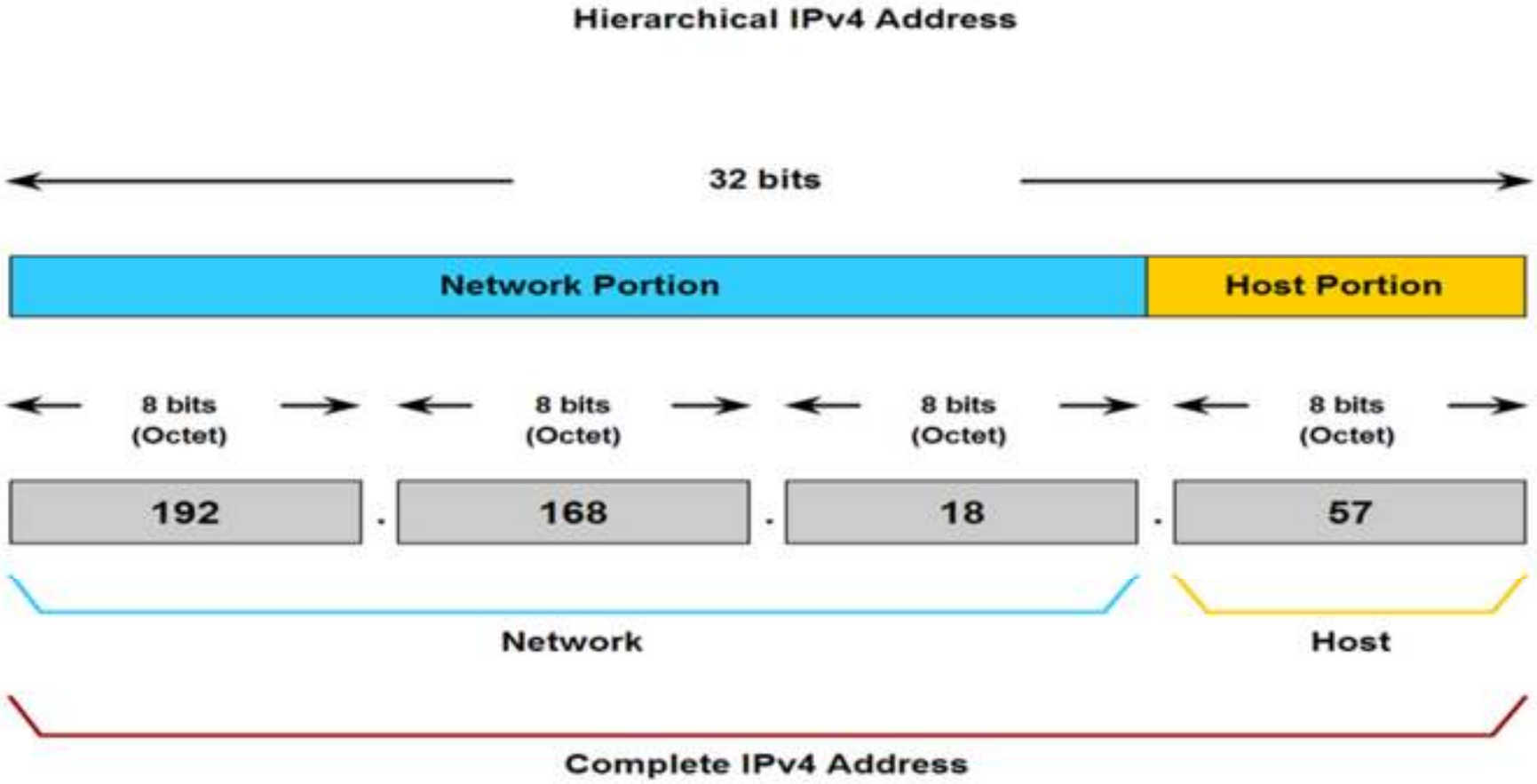
Appnomic System 201, 2nd Floor, 'Touchdown', No. 1 & 2 HAL Industrial Area, Bangalore – 560 037.



At each step of delivery, the post office need only examine the next hierarchical level.

Network Layer

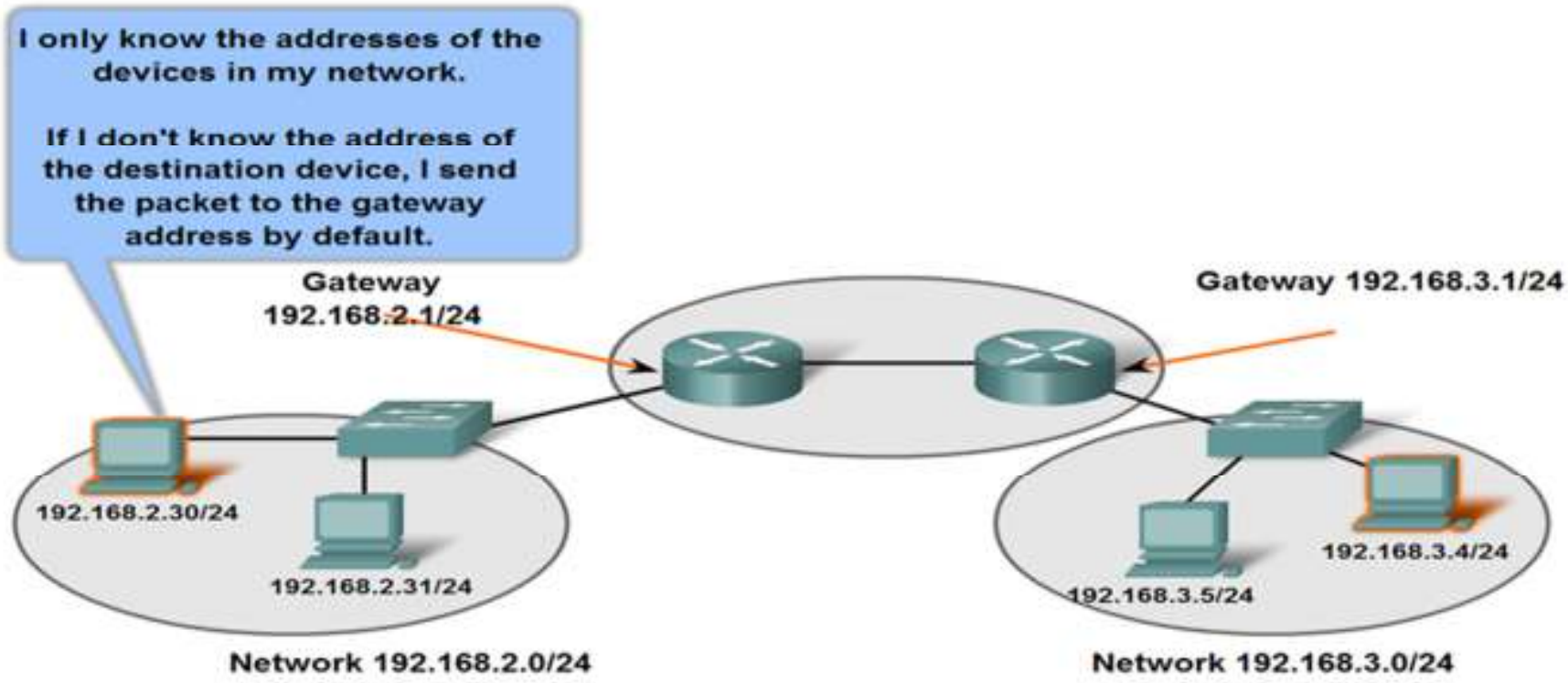
The logical 32-bit IPv4 address is hierarchical and is made up of two parts. The first part identifies the network and the second part identifies a host on that network. Both parts are required for a complete IP address.



Network Layer

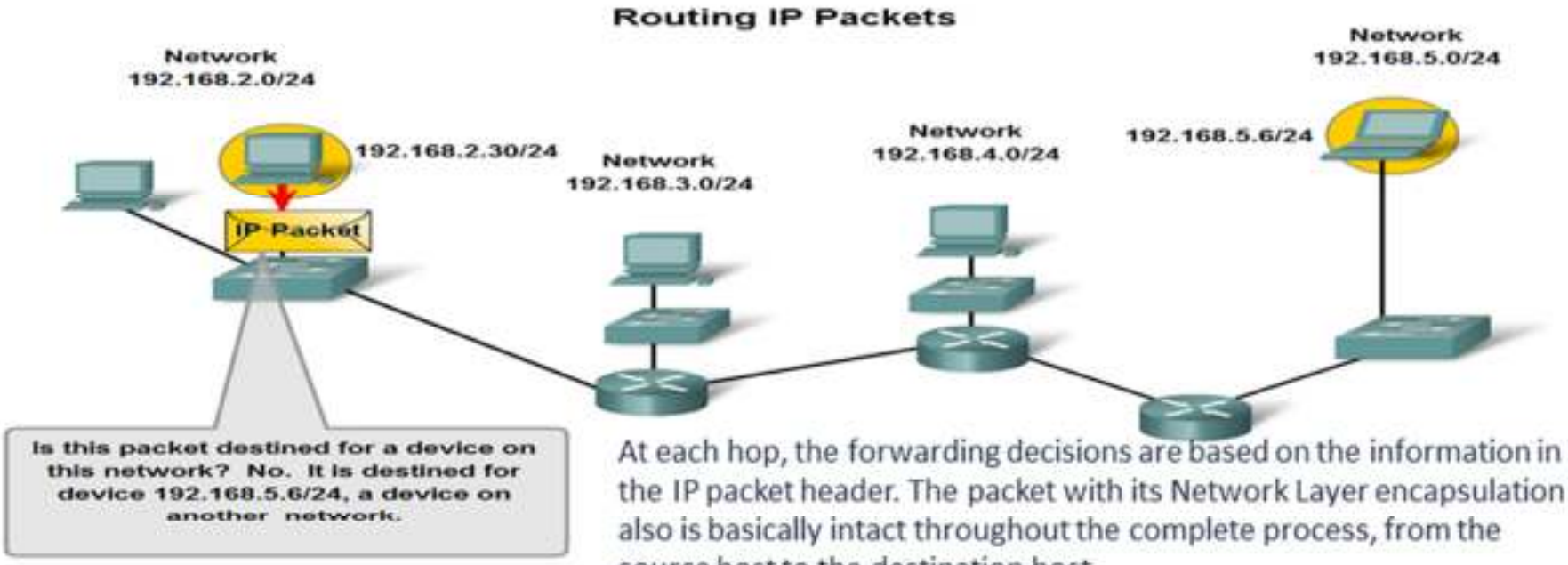
Within a network or a subnetwork, hosts communicate with each other without the need for any Network layer intermediary device. When a host needs to communicate with another network, an intermediary device, or router, acts as a gateway to the other network.

Gateways Enable Communications between Networks



Network Layer

As you know, the role of the Network layer is to transfer data from the host that originates the data to the host that uses it. During encapsulation at the source host, an IP packet is constructed Layer 3 to transport the Layer 4 PDU. If the destination host is in the same network as the source host, the packet is delivered between the two hosts on the local media without the need for a router.

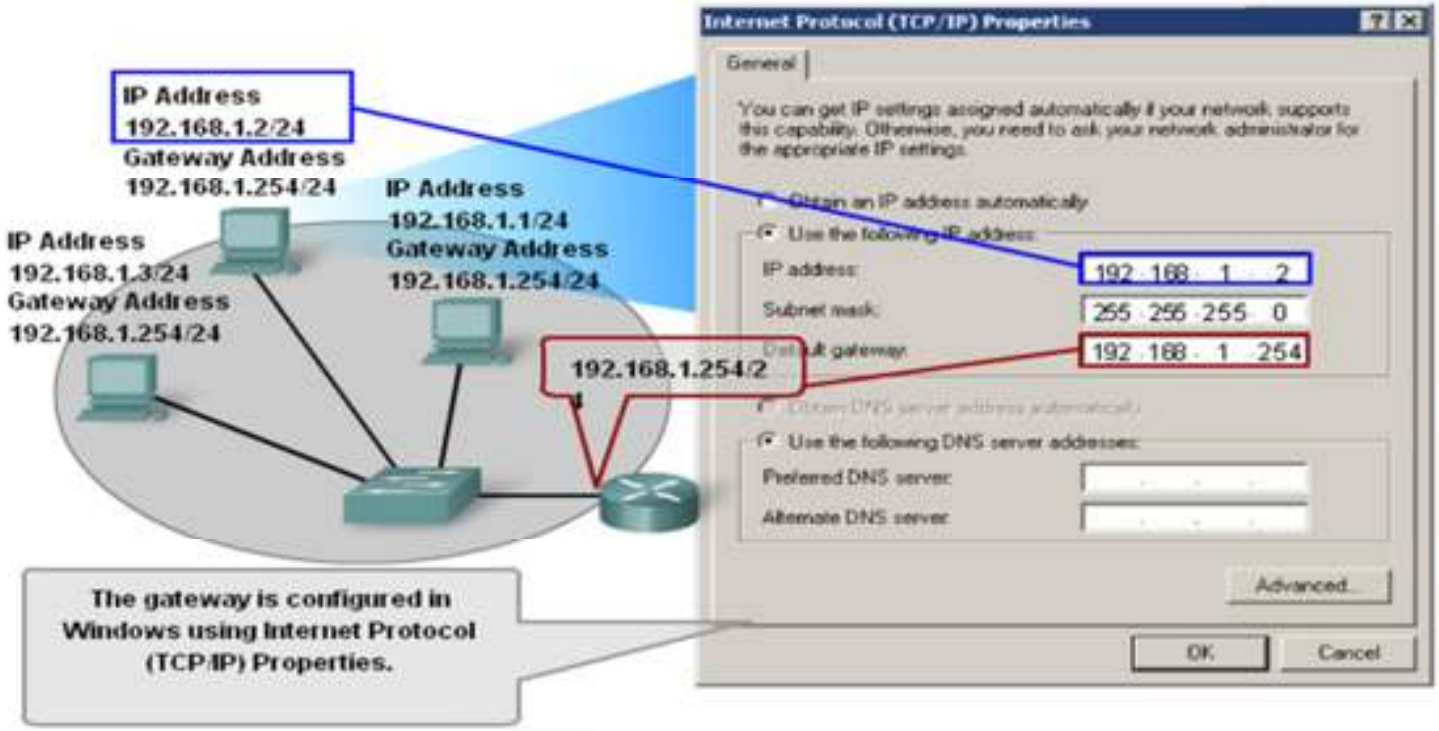


At each hop, the forwarding decisions are based on the information in the IP packet header. The packet with its Network Layer encapsulation also is basically intact throughout the complete process, from the source host to the destination host.

However, if the destination host and source host are not in the same network, the packet may be carrying a Transport layer PDU across many networks and through many routers. As it does, the information contained within is not altered by any routers when forwarding decisions are made.

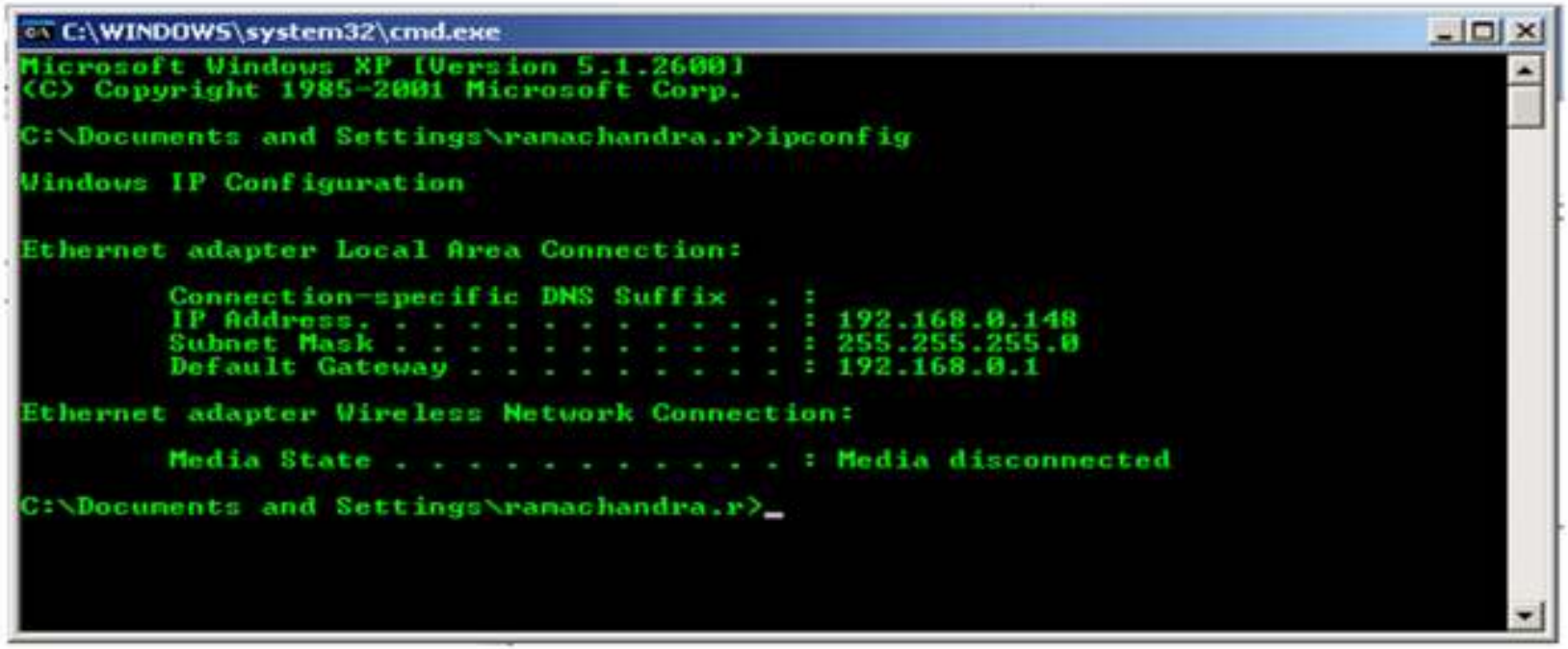
Network Layer – A Gateway – The Way Out of Our Network

The gateway, also known as the default gateway, is needed to send a packet out of the local network. If the network portion of the destination address of the packet is different from the network of the originating host, the packet has to be routed outside the original network. To do this, the packet is sent to the gateway. This gateway is a router interface connected to the local network. The gateway interface has a Network layer address that matches the network address of the hosts. The hosts are configured to recognize that address as the gateway.



A Gateway – The Way Out of Our Network

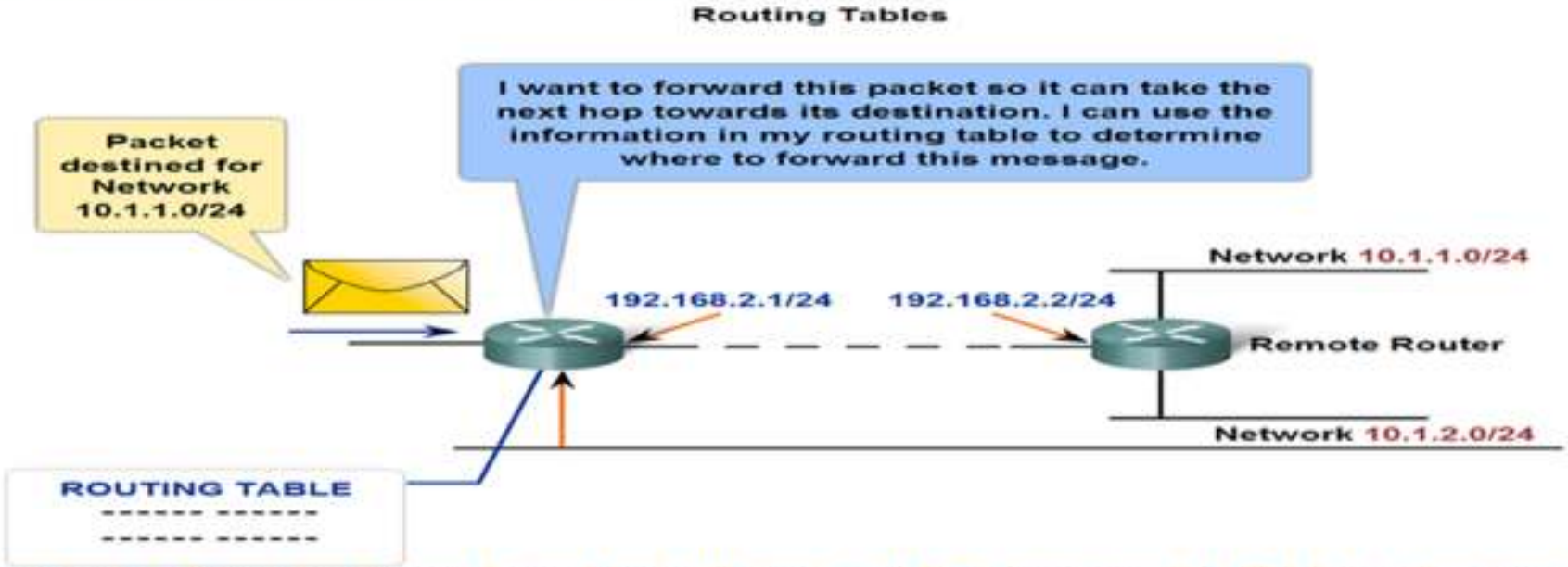
Confirming the Gateway and Route in PC



A Gateway – The Way Out of Our Network

No packet can be forwarded without a route. Whether the packet is originating in a host or being forwarded by an intermediary device, the device must have a route to identify where to forward the packet.

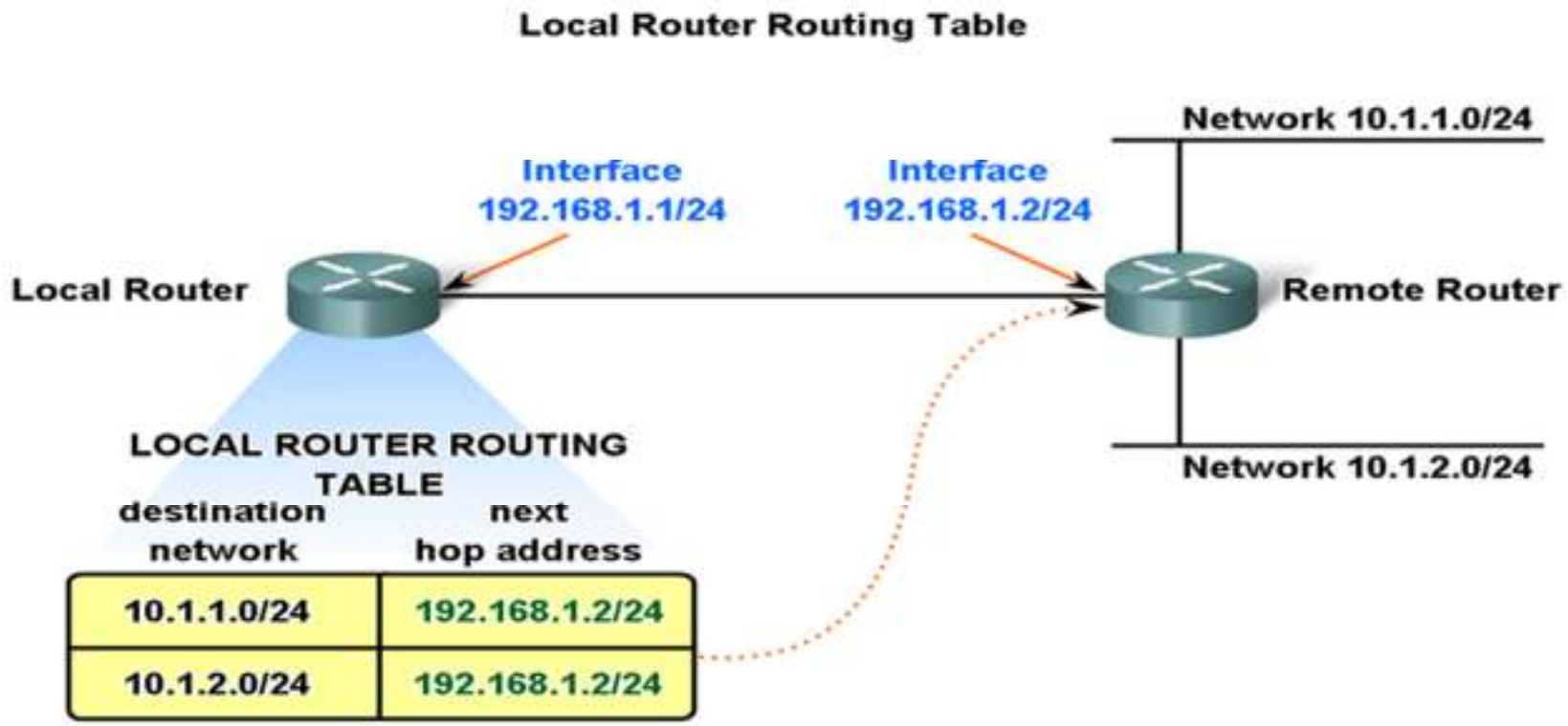
A host must either forward a packet to the host on the local network or to the gateway, as appropriate. To forward the packets, the host must have routes that represent these destinations.



A router makes a forwarding decision for each packet that arrives at the gateway interface. This forwarding process is referred to as routing. To forward a packet to a destination network, the router requires a route to that network. If a route to a destination network does not exist, the packet cannot be forwarded.

A Gateway – The Way Out of Our Network

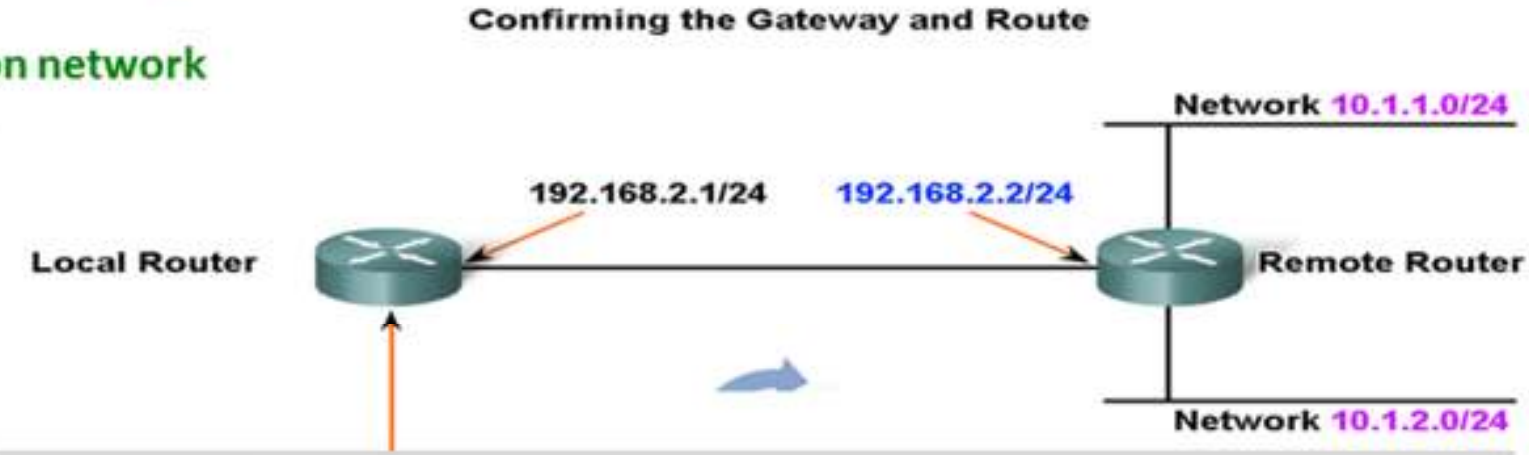
The destination network may be a number of routers or hops away from the gateway. The route to that network would only indicate the next-hop router to which the packet is to be forwarded, not the final router. The routing process uses a route to map the destination network address to the next hop and then forwards the packet to this next-hop address.



A Route – Path to a Network

Routes in a routing table have three main features:

Destination network
Next-hop
Metric



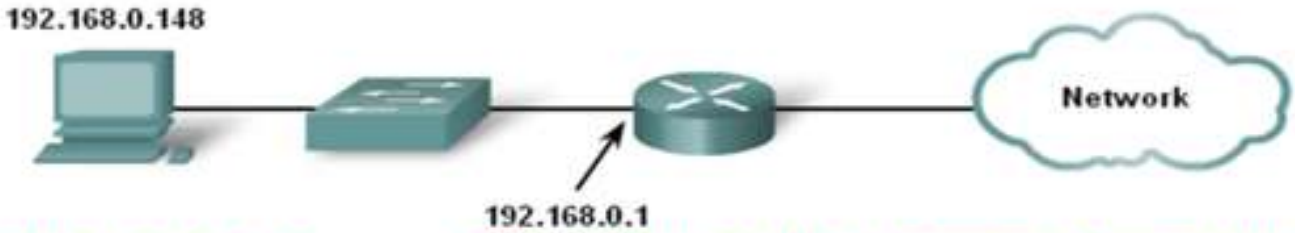

```
    10.0.0.0/24 is subnetted, 2 subnets
R       10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R       10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C   192.168.1.0/24 is directly connected, FastEthernet0/0
```

This is the routing table output of Local Router when the "show ip route" is issued.

The next hop for networks 10.1.1.0/24 and 10.1.2.0/24 from Local Router is 192.168.2.2.

A Route – Path to a Network

Host Routing Table




```
0x2 ...00 18 8b a4 85 08 ...... Broadcon 440x 10/100 Integrated Controller - Pac
ket Scheduler Miniport
0x3 ...00 18 de d3 95 e2 ...... Intel(R) PRO/Wireless 3945ABG Network Connection
 - Packet Scheduler Miniport
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.0.1    192.168.0.148      20
        127.0.0.0        255.0.0.0      127.0.0.1        127.0.0.1       1
      192.168.0.0    255.255.255.0  192.168.0.148    192.168.0.148      20
Default Gateway:       192.168.0.1
===========================================================================
```

This is an example of a routing table on an end device after the netstat -r command is issued. Note that it has a route to its network 192.168.0.0 and a default route (0.0.0.0) to the router gateway for all other networks.

The Destination Network

Routing Table Entries

```
S     101.0.0.0/8 [1/0] via 172.19.100.250
      71.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        71.11.26.80/29 is directly connected, Vlan1
C        172.19.100.248/29 is directly connected, GigabitEthernet0/0.3
S        172.19.8.0/24 [1/0] via 172.20.1.34
S        172.19.7.0/24 [1/0] via 172.20.1.22
S        172.19.6.0/24 [1/0] via 172.20.1.10
C        172.19.100.96/28 is directly connected, GigabitEthernet0/0.533
S        172.19.4.0/24 [1/0] via 172.20.1.18
S        172.19.3.0/24 [1/0] via 172.20.1.14
S        172.19.1.0/24 [1/0] via 172.20.1.6
```

Default Route

```
C        9.0.0.16 is directly connected, Tunnel4
S     192.168.5.0/24 is directly connected, Tunnel2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.12.12.0/30 is directly connected, Tunnel2
S        10.0.0.0/8 is directly connected, Tunnel2
S     192.168.3.0/24 is directly connected, Tunnel5
S*    0.0.0.0/0 [1/0] via 172.24.64.194
```

A router can be configured to have a default route. A default route is a route that will match all destination networks. In IPv4 networks, the address 0.0.0.0 is used for this purpose. The default route is used to forward packets for which there is no entry in the routing table for the destination network. Packets with a destination network address that does not match a more specific route in the routing table are forwarded to the next-hop router associated with the default route.

The Next Hop – Where the Packets Goes Next

A next-hop is the address of the device that will process the packet next. For a host on a network, the address of the default gateway (router interface) is the next-hop for all packets destined for another network.

In the routing table of a router, each route lists a next hop for each destination address that is encompassed by the route. As each packet arrives at a router, the destination network address is examined and compared to the routes in the routing table. When a matching route is determined, the next hop address for that route is used to forward of the packet toward its destination. The router then forwards the packet out the interface to which the next-hop router is connected. The next-hop router is the gateway to networks beyond that intermediate

```
S       172.19.100.0/24 [1/0] via 172.20.1.14
S       172.19.100.56/29 [1/0] via 172.20.1.38
S       172.19.100.48/29 [1/0] via 172.20.1.6
S       172.19.100.52/30 [1/0] via 172.20.1.38
```

```
  10.0.0.0/24 is subnetted, 2 subnets
R    10.1.1.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
R    10.1.2.0 [120/1] via 192.168.2.2, 00:00:08, FastEthernet0/0
C 192.168.1.0/24 is directly connected, FastEthernet0/0
```

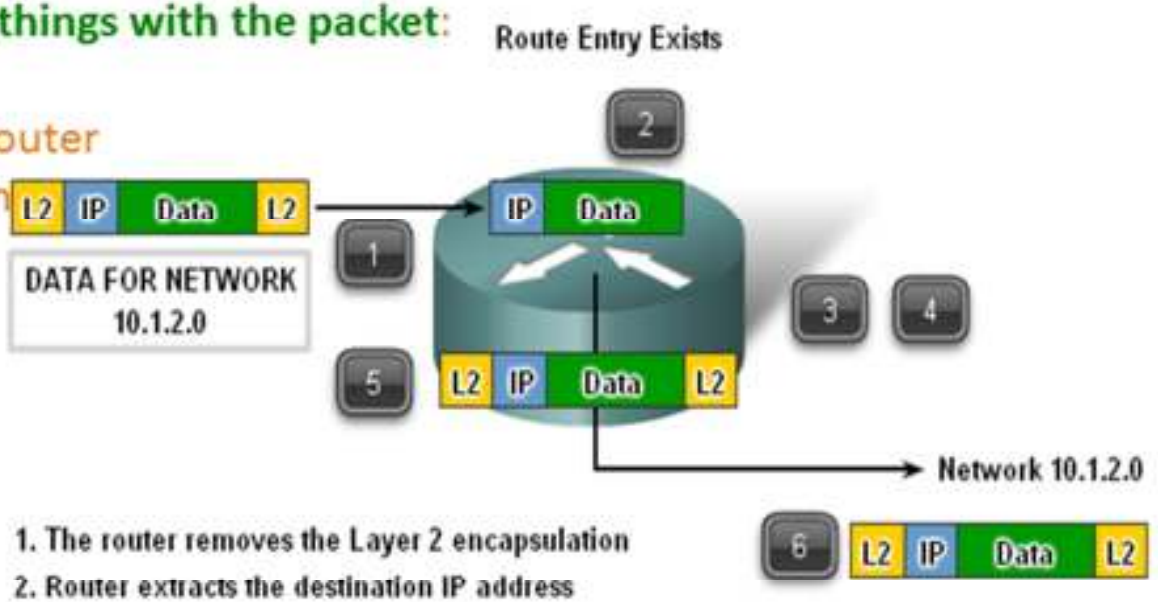
Networks directly connected to a router have no next-hop address because there is no intermediate Layer 3 device between the router and that network. The router can forward packets directly out the interface onto that network to the destination host. Some routes can have multiple next-hops. This indicates that there are multiple paths to the same destination network. These are parallel routes that the router can use to forward packets.

Packet Forwarding – Moving the Packet Toward its Destination

Routing is done **packet-by-packet and hop-by-hop**. Each packet is treated independently in each router along the path. At each hop, the router examines the destination IP address for each packet and then checks the routing table for forwarding information.

The router will do one of three things with the packet:

1. Forward it to the next-hop router
2. Forward it to the destination host
3. Drop it

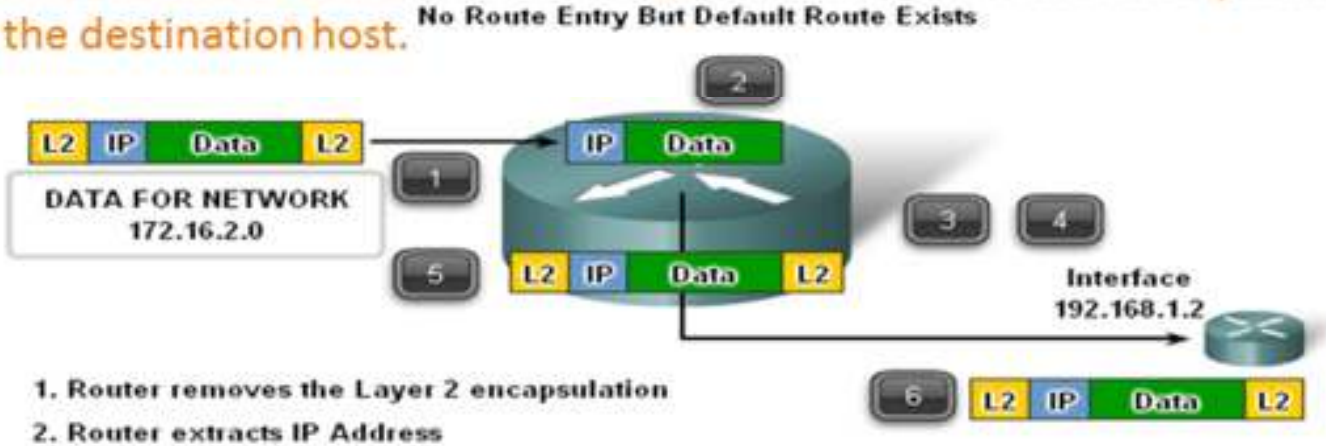


1. The router removes the Layer 2 encapsulation
2. Router extracts the destination IP address
3. Router checks the routing table for a match
4. Network 10.1.2.0 is found in the routing table
5. Router re-encapsulates the packet
6. Packet is sent to Network 10.1.2.0

Packet Forwarding – Moving the Packet Toward its Destination

Using the Default Route

Default routes are important because the gateway router is not likely to have a route to every possible network on the Internet. If the packet is forwarded using a default route, it should eventually arrive at a router that has a specific route to the destination network. This router may be the router to which this network is attached. In this case, this router will forward the packet over the local network to the destination host.

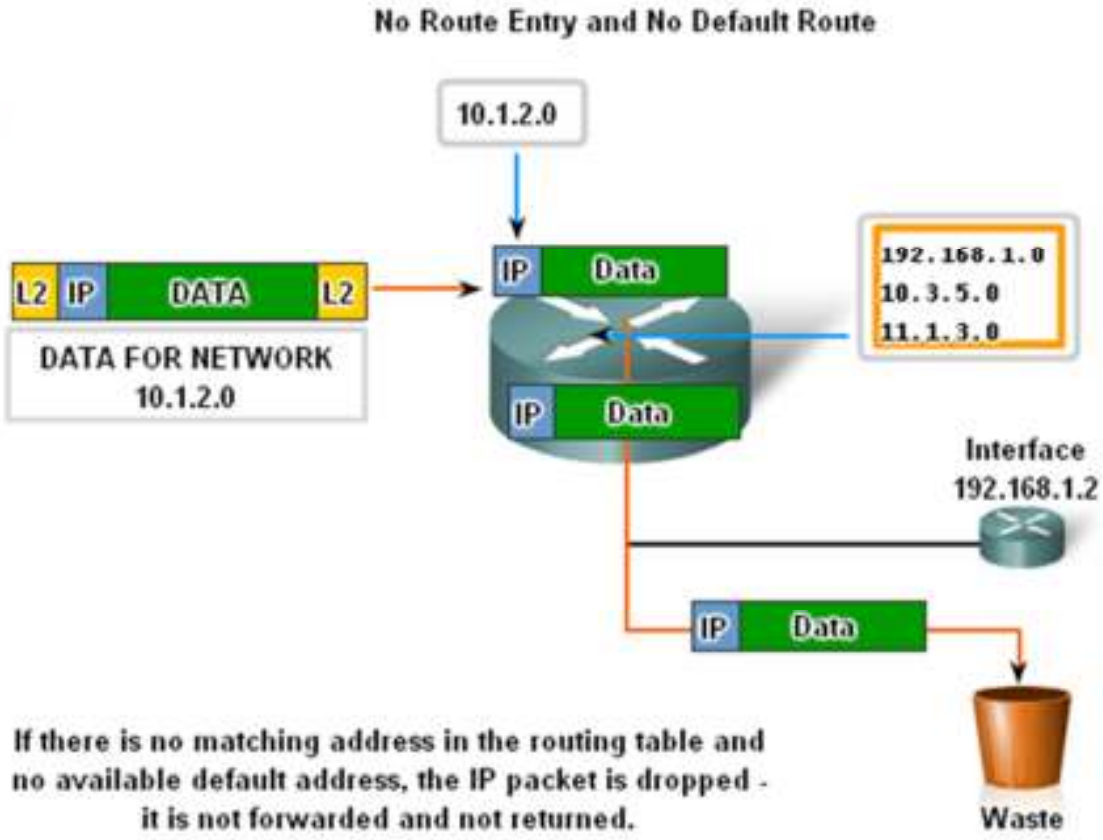


1. Router removes the Layer 2 encapsulation
2. Router extracts IP Address
3. Router checks the routing table for a match
4. Network 172.16.2.0 not in the routing table but default route to 192.168.1.2 exists
5. Router re-encapsulates the packet
6. Packet is sent to Interface 192.168.1.2

Packet Forwarding – Moving the Packet Toward its Destination

As a packet passes through the hops in the internetwork, all routers require a route to forward a packet. If, at any router, no route for the destination network is found in the routing table and there is no default route, that packet is dropped.

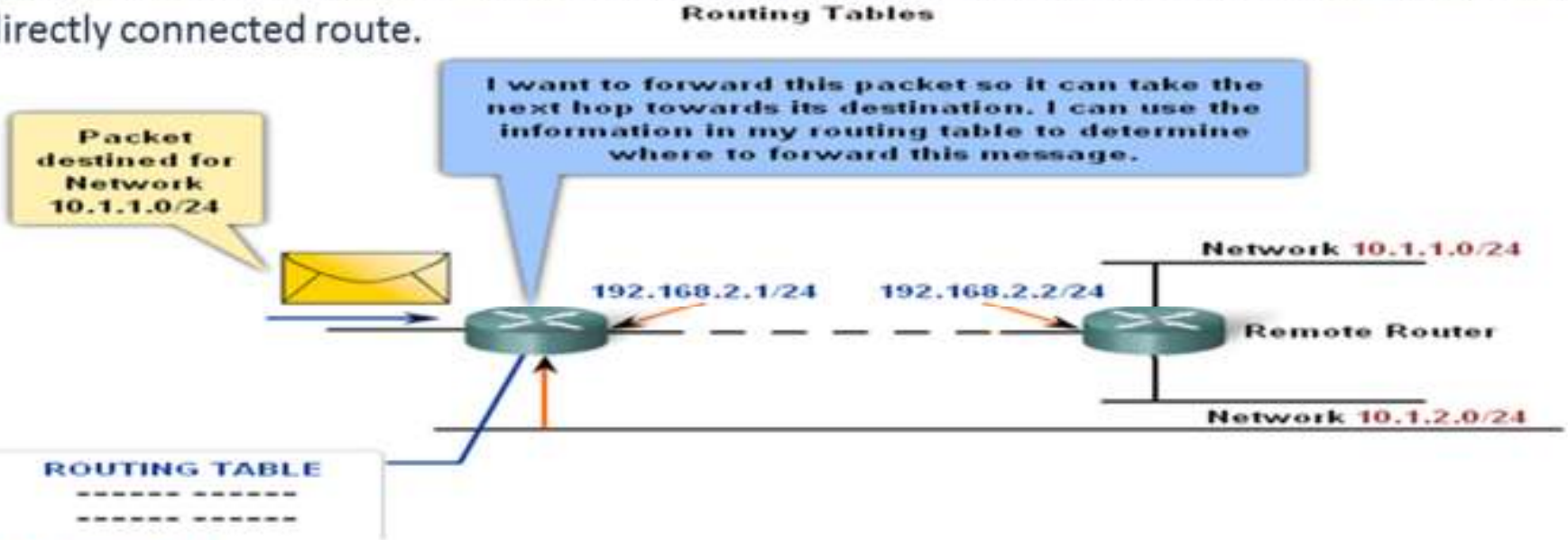
IP has no provision to return a packet to the previous router if a particular router has nowhere to send the packet.
Such a function would detract from the protocol's efficiency and low overhead.
Other protocols are used to report such errors.



Routing Protocols – Sharing the Routes

The routing table contains the information that a router uses in its packet forwarding decisions. For the routing decisions, the routing table needs to represent the most accurate state of network pathways that the router can access. Out-of-date routing information means that packets may not be forwarded to the most appropriate next-hop, causing delays or packet loss.

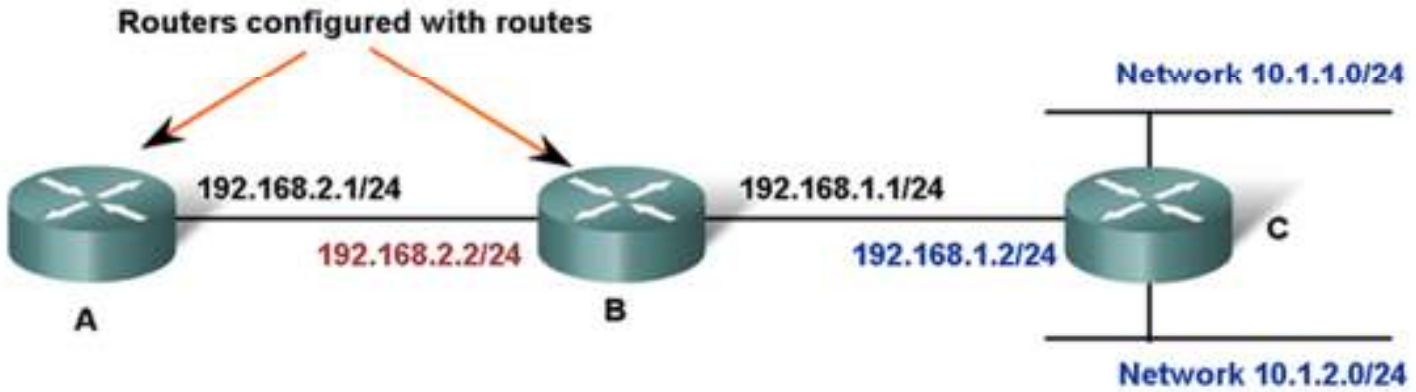
This route information can be manually configured on the router or learned dynamically from other routers in the same internetwork. After the interfaces of a router are configured and operational, the network associated with each interface is installed in the routing table as a directly connected route.



Routing Protocols – Sharing the Routes

Routes to remote networks with the associated next hops can be manually configured on the router. This is known as static routing. A default route can also be statically configured.

Static Routing



Router A:
192.168.2.2/24
configured manually as next hop for networks 10.1.1.0/24 and 10.1.2.0/24

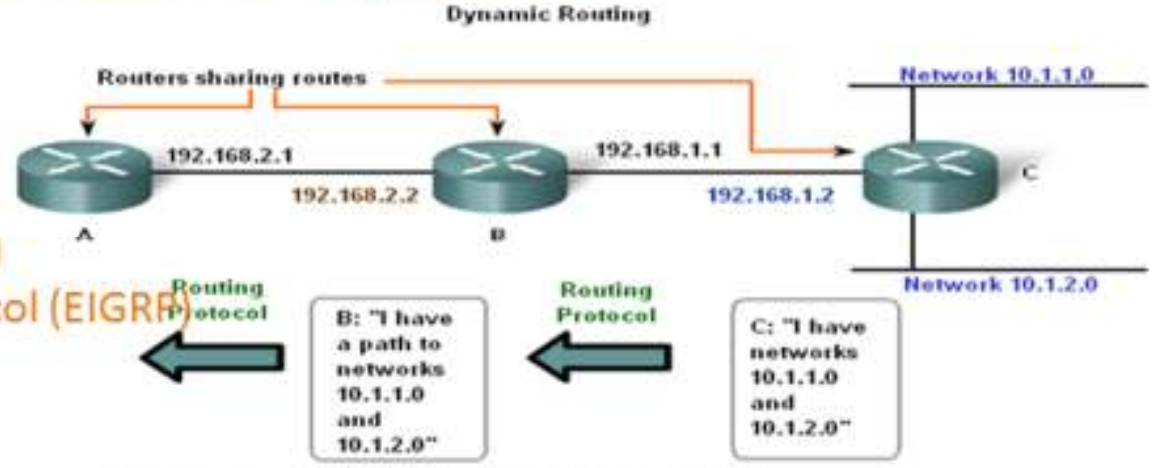
Router B:
192.168.1.2/24
configured manually as next hop for networks 10.1.1.0/24 and 10.1.2.0/24

Routing Protocols – Sharing the Routes

Although it is essential for all routers in an internetwork to have up-to-date extensive route knowledge, maintaining the routing table by manual static configuration is not always feasible. Therefore, dynamic routing protocols are used. Routing protocols are the set of rules by which routers dynamically share their routing information. As routers become aware of changes to the networks for which they act as the gateway, or changes to links between routers, this information is passed on to other routers. When a router receives information about new or changed routes, it updates its own routing table and, in turn, passes the information to other routers. In this way, all routers have accurate routing tables that are updated dynamically and can learn about routes to remote networks that are many hops way.

Common routing protocols are:

1. Routing Information Protocol (RIP)
2. Enhanced Interior Gateway Protocol (EIGRP)
3. Open Shortest Path First (OSPF)



Data Link Layer

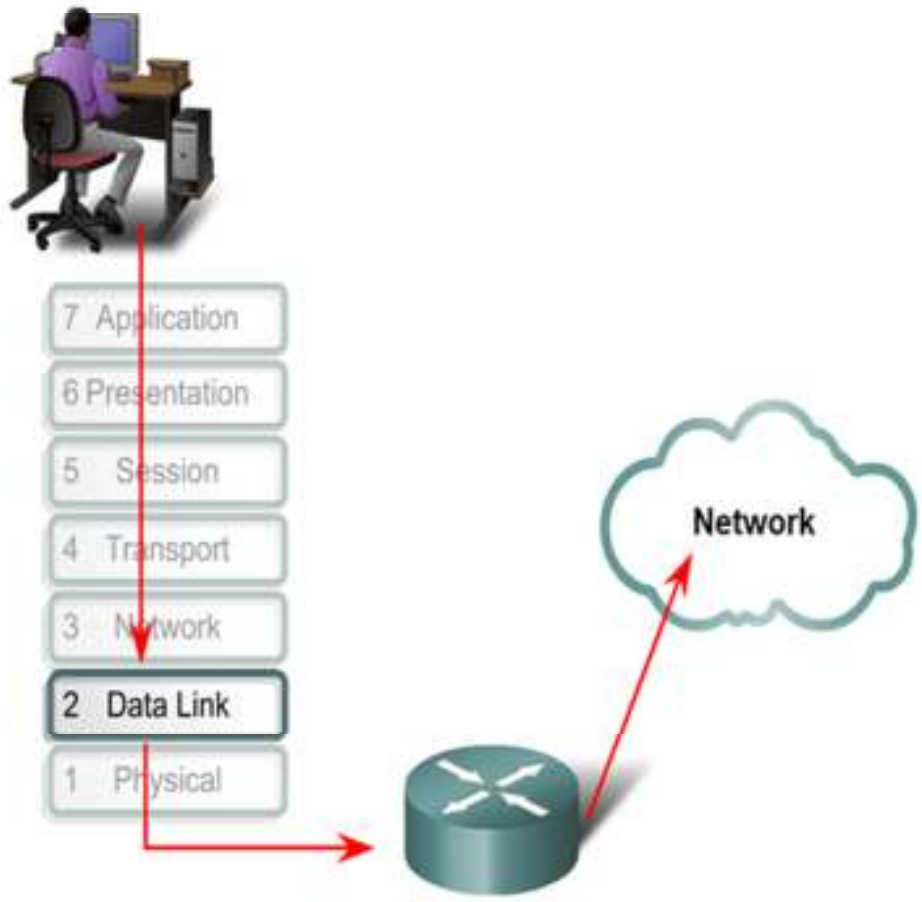
OSI Data Link Layer

The Data Link layer provides a means for exchanging data over a common local media.

The Data Link layer performs two basic services:
Allows the upper layers to access the media using techniques such as framing
Controls how data is placed onto the media and is received from the media using techniques such as media access control and error detection

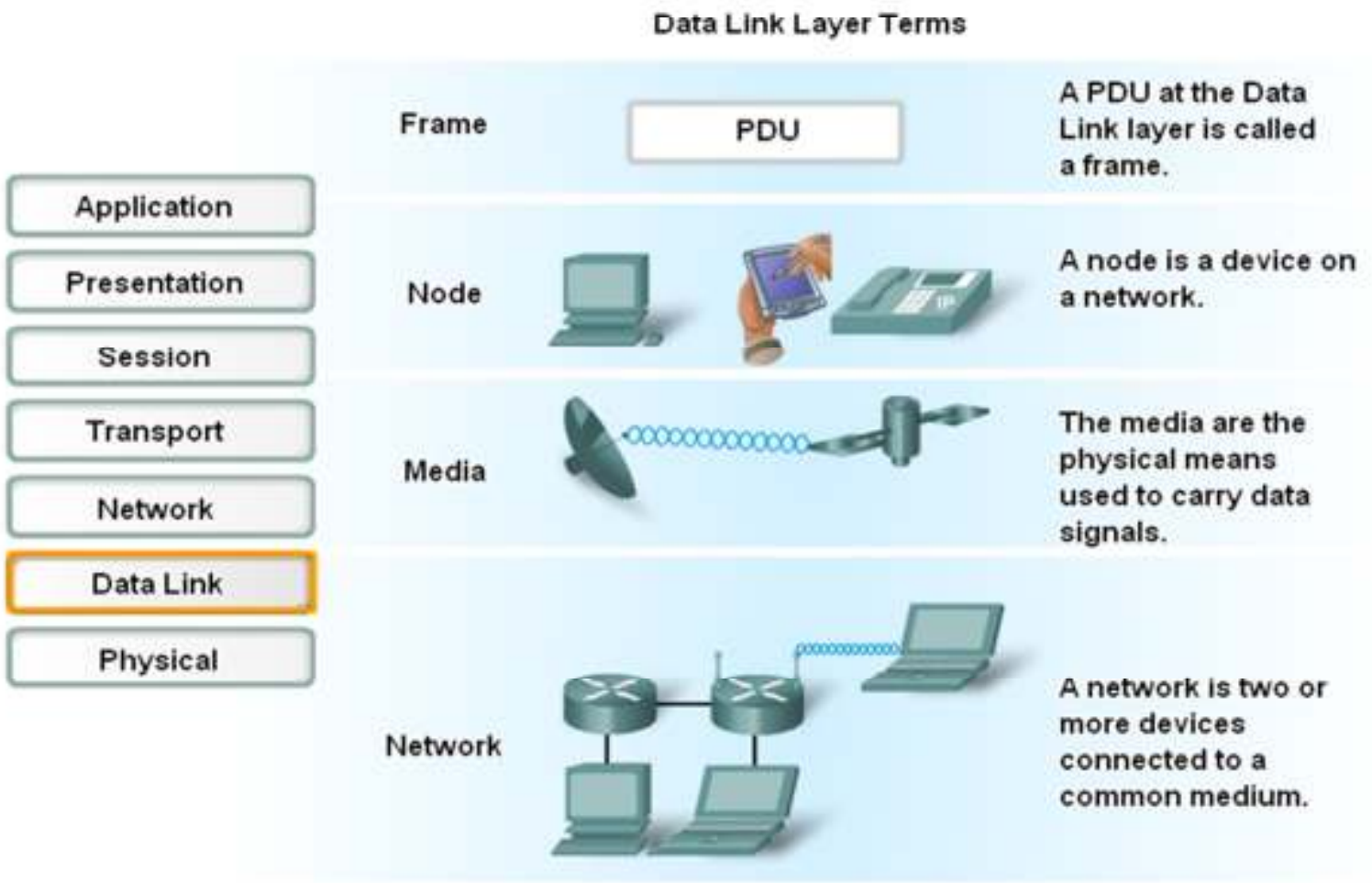
As with each of the OSI layers, there are terms specific to this layer:

Frame - The Data Link layer PDU



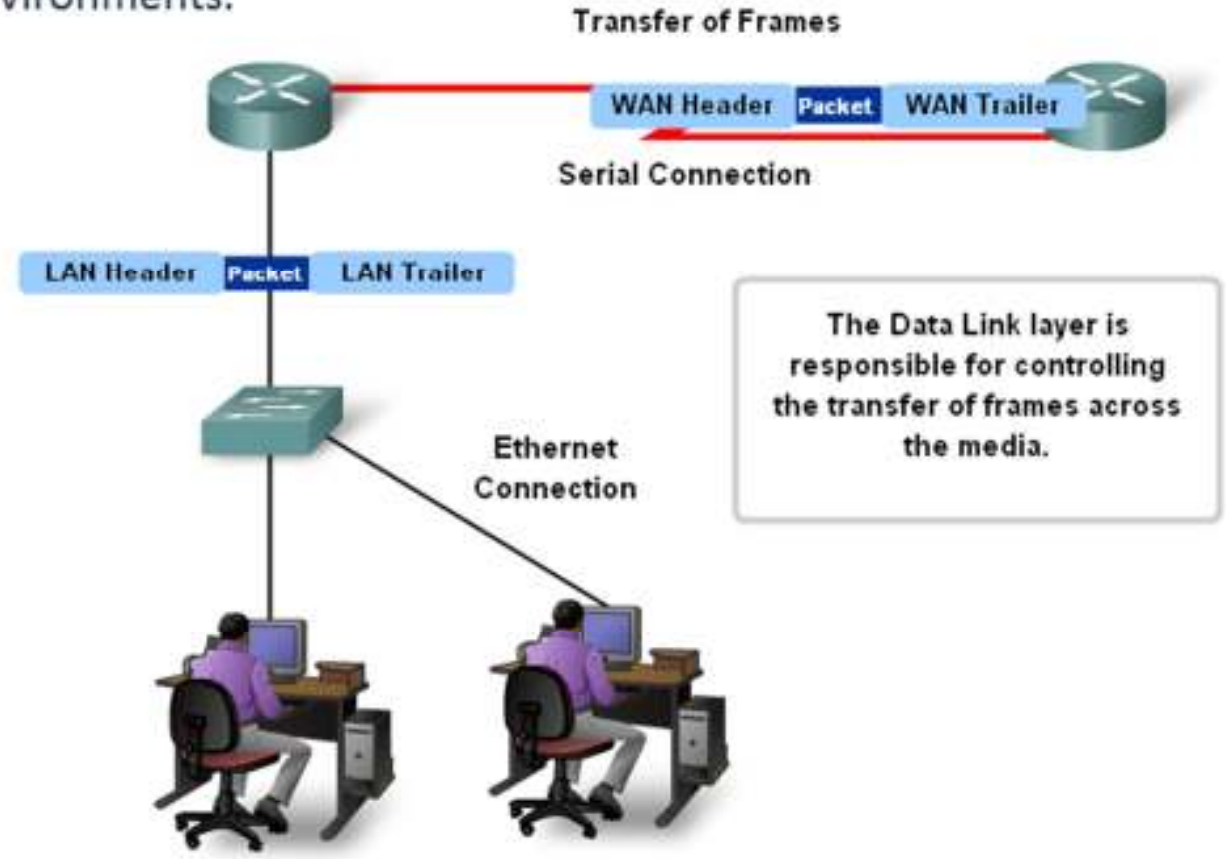
The Data Link layer prepares network data for the physical network.

Data Link Layer



Data Link Layer – Controlling Transfer across Local Media

The media access control methods described by the Data Link layer protocols define the processes by which network devices can access the network media and transmit frames in diverse network environments.

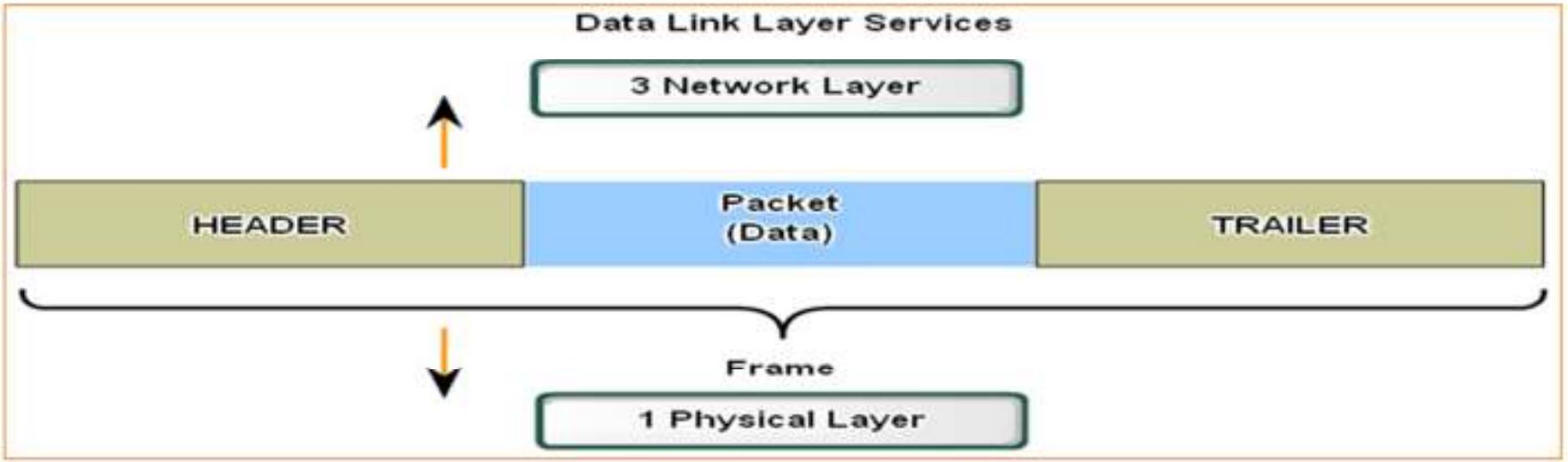


Data Link Layer – Creating a Frame

Data - The packet from the Network layer

Header - Contains control information, such addressing, and is located at the beginning of the PDU

Trailer - Contains control information added to the end of the PDU



Data Link Layer – Creating a Frame

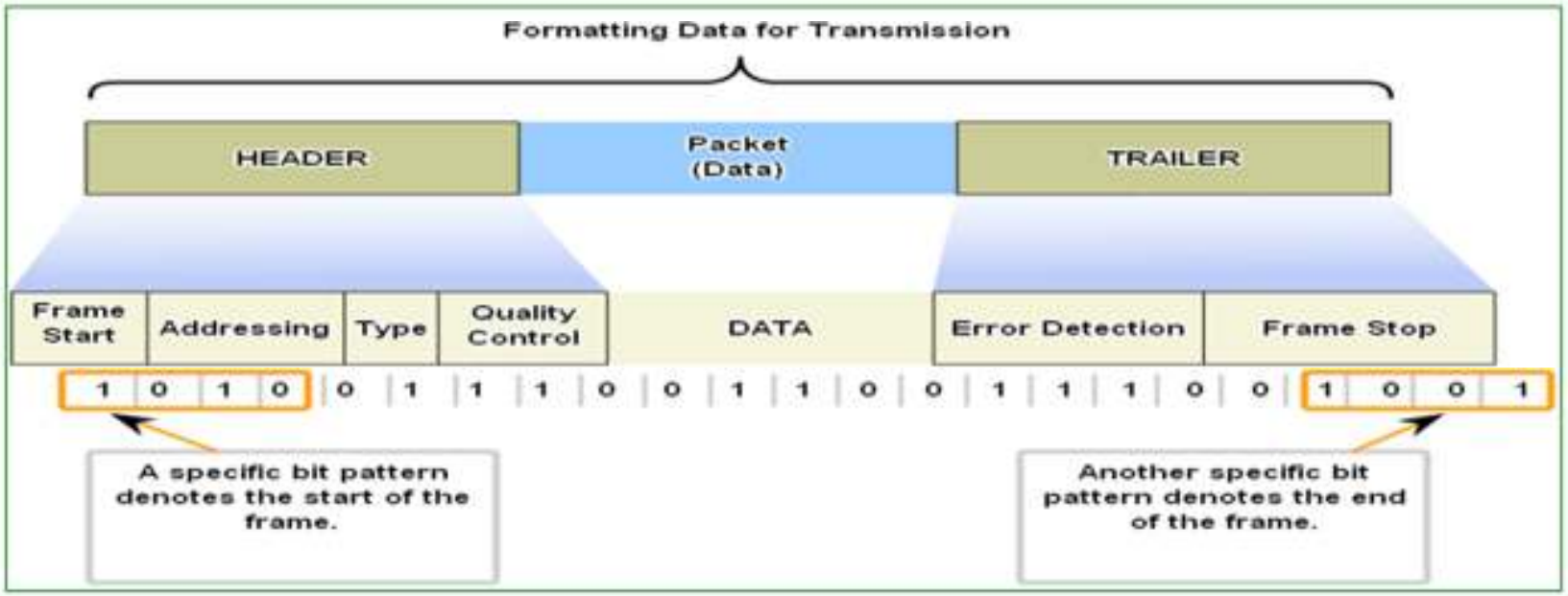
Start and stop indicator fields - The beginning and end limits of the frame

Naming or addressing fields

Type field - The type of PDU contained in the frame

Quality - control fields

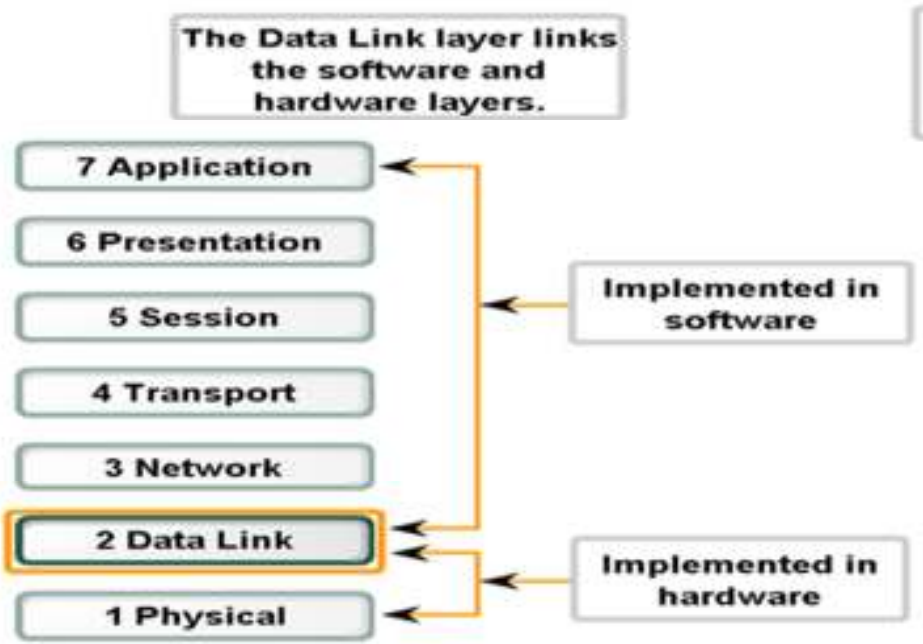
A data field -The frame payload (Network layer packet)



Data Link Layer – Supporting & Connecting to Upper Layer Services

The Data Link layer exists as a connecting layer between the software processes of the layers above it and the Physical layer below it. As such, it prepares the Network layer packets for transmission across some form of media, be it copper, fiber, or the atmosphere.

Connecting Upper Layer Services to the Media

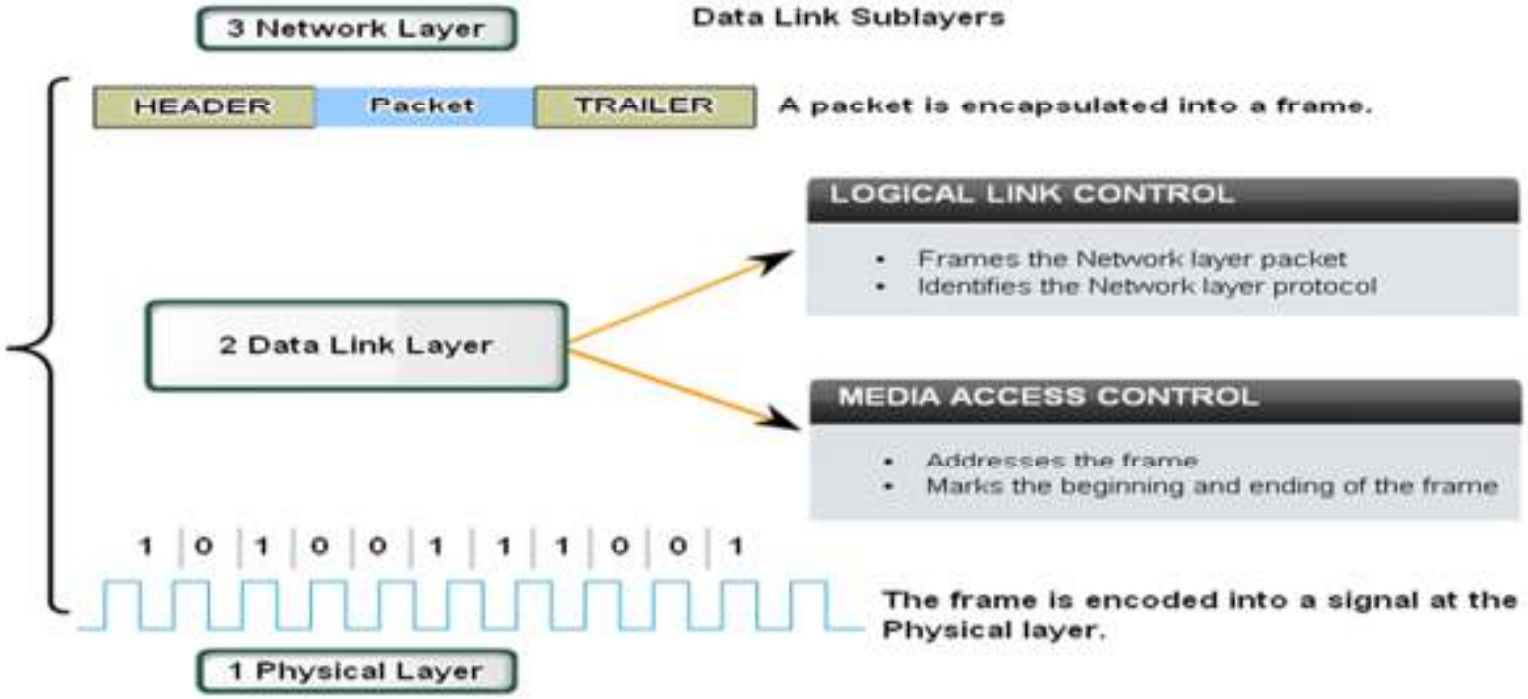


PC NIC

Data Link Layer – Supporting & Connecting to Upper Layer Services

To support a wide variety of network functions, the Data Link layer is often divided into two sublayers: an upper sublayer and an lower sublayer.

The upper sublayer defines the software processes that provide services to the Network layer protocols.
The lower sublayer defines the media access processes performed by the hardware.



Data Link Layer – Standards

Engineering organizations that define open standards and protocols that apply to the Data Link layer include:

International Organization for Standardization (ISO)

Institute of Electrical and Electronics Engineers (IEEE)

American National Standards Institute (ANSI)

International Telecommunication Union (ITU)

Standards for the Data Link Layer

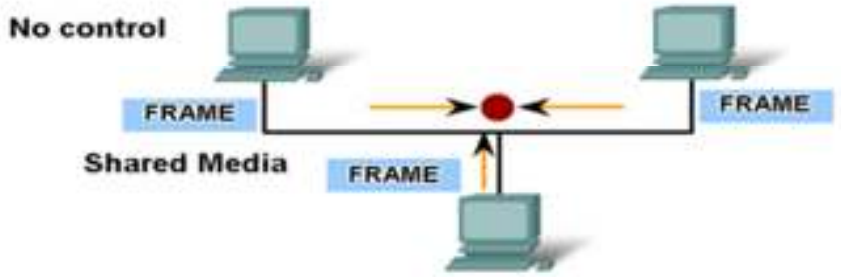
ISO:	HDLC (High Level Data Link Control)
IEEE:	802.2 (LLC), 802.3 (Ethernet) 802.5 (Token Ring) 802.11(Wireless LAN)
ITU:	Q.922 (Frame Relay Standard) Q.921 (ISDN Data Link Standard) HDLC (High Level Data Link Control)
ANSI:	3T9.5 ADCCP (Advanced Data Communications Control Protocol)

Data Link Layer – Placing Data on the Media

The protocols at the Data Link layer define the rules for access to different media. Some media access control methods use highly-controlled processes to ensure that frames are safely placed on the media. These methods are defined by sophisticated protocols, which require mechanisms that introduce overhead onto the network.

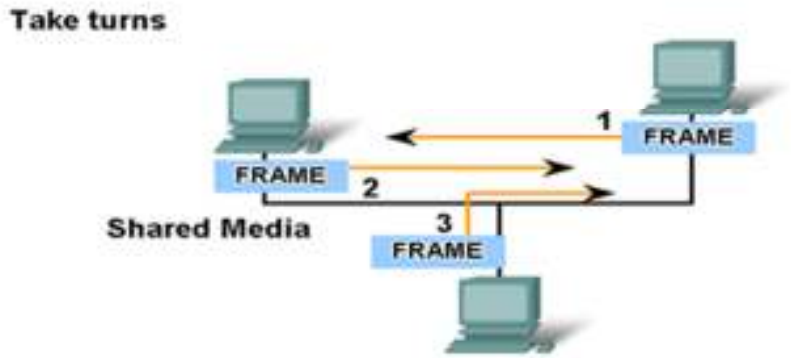
Media Access Control Methods

No control at all would result in many collisions. Collisions cause corrupted frames that must be resent.

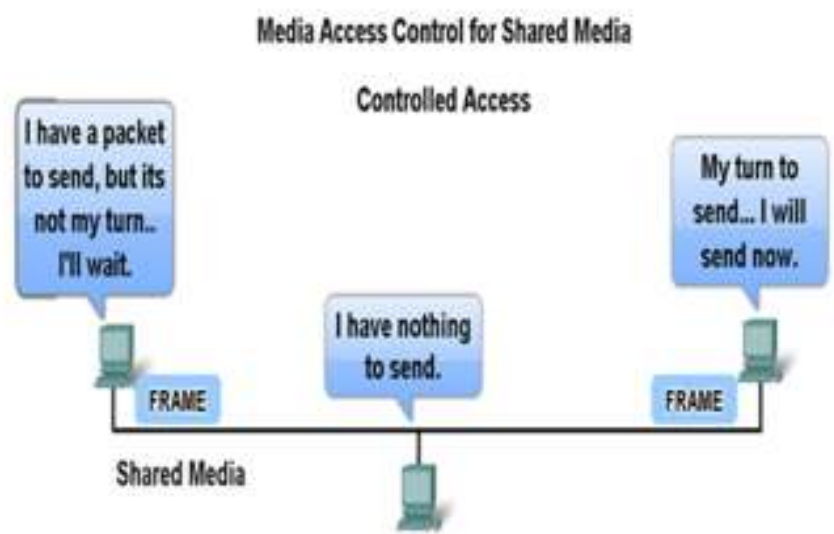


Methods that enforce a high degree of control prevent collisions, but the process has high overhead.

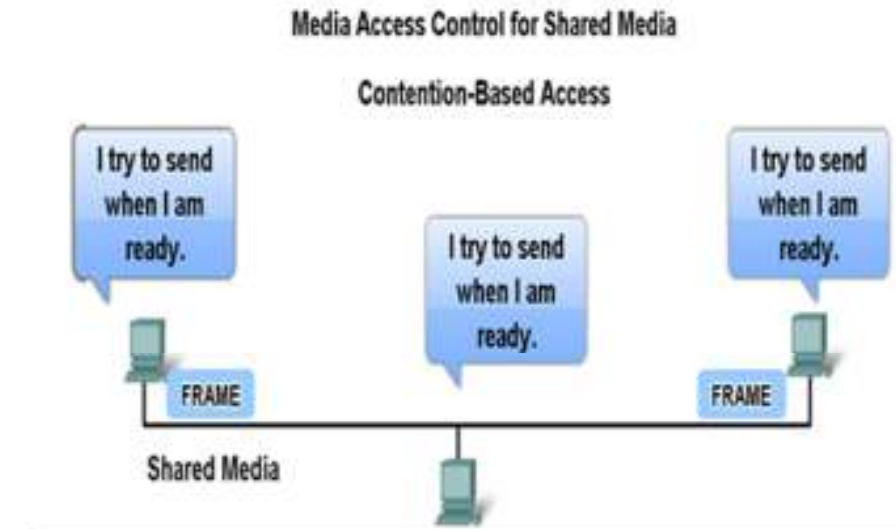
Methods that enforce a low degree of control have low overhead, but there are more frequent collisions.



Data Link Layer – Media Access Control for Shared Media



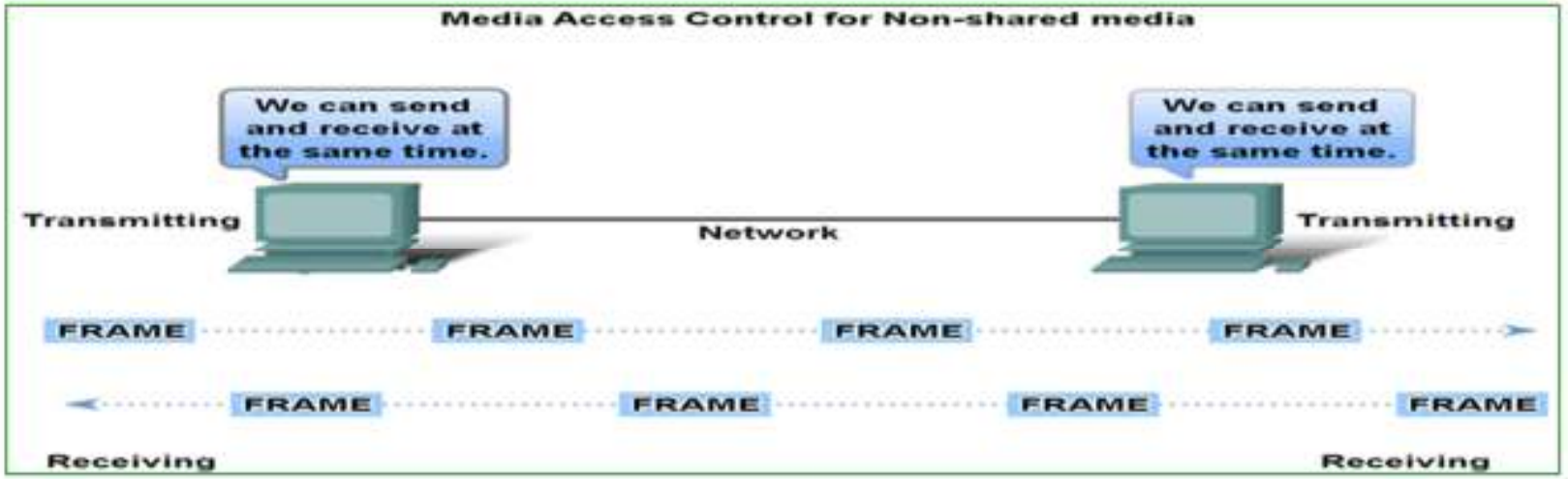
Method	Characteristics	Example
Controlled Access	• Only one station transmits at a time • Devices wishing to transmit must wait their turn • No collisions • Some deterministic networks use token passing	• Token Ring • FDDI



Method	Characteristics	Example

Contention Based Access	• Stations can transmit at any time
	• Collisions exist
	• Mechanisms exist to resolve contention:
	  • CSMA/CD for Ethernet networks
	  • CSMA/CA for 802.11 wireless networks
		• Ethernet
		• Wireless

Data Link Layer – Media Access Control for Non - Shared Media



Data Link Layer – Logical Topology vs Physical Topology

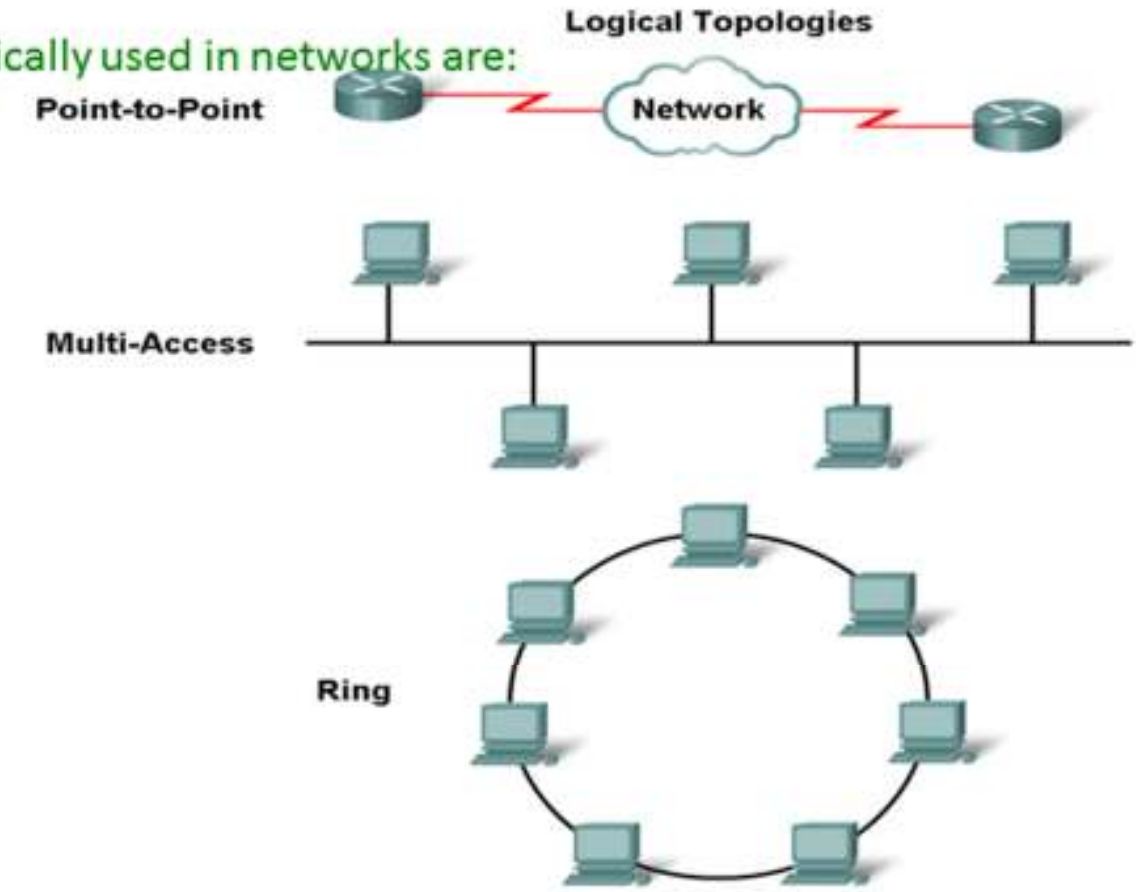
The physical or cabled topology of a network will most likely not be the same as the logical topology.

Logical and physical topologies typically used in networks are:

Point-to-Point

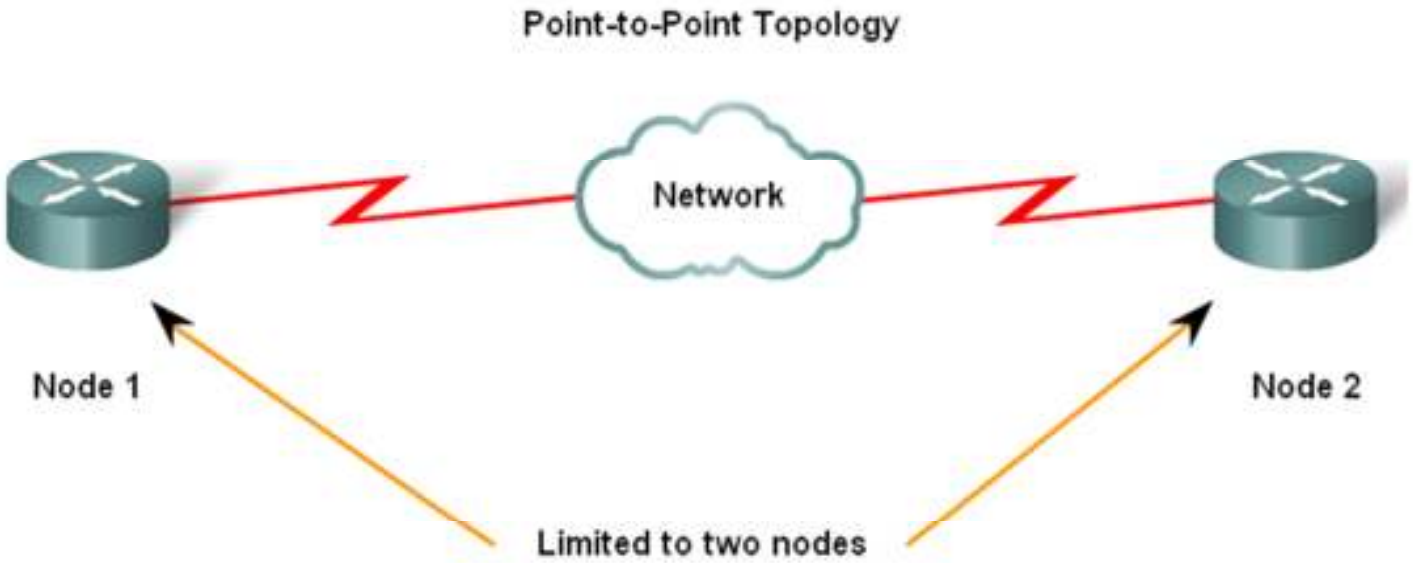
Multi-Access

Ring

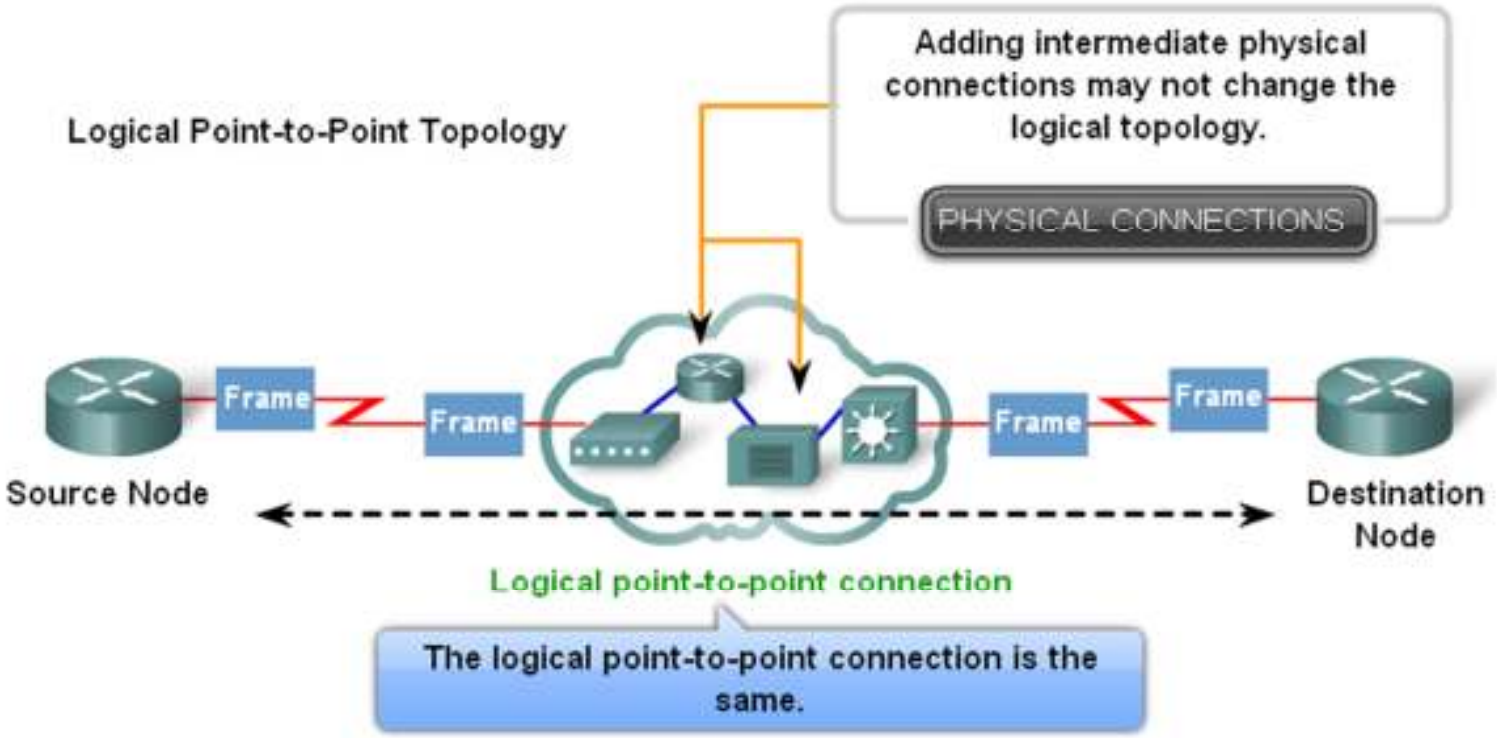


Data Link Layer – Point-to-Point Topology

In point-to-point networks, if data can only flow in one direction at a time, it is operating as a half-duplex link. If data can successfully flow across the link from each node simultaneously, it is a full-duplex link.



Data Link Layer – Point-to-Point Topology

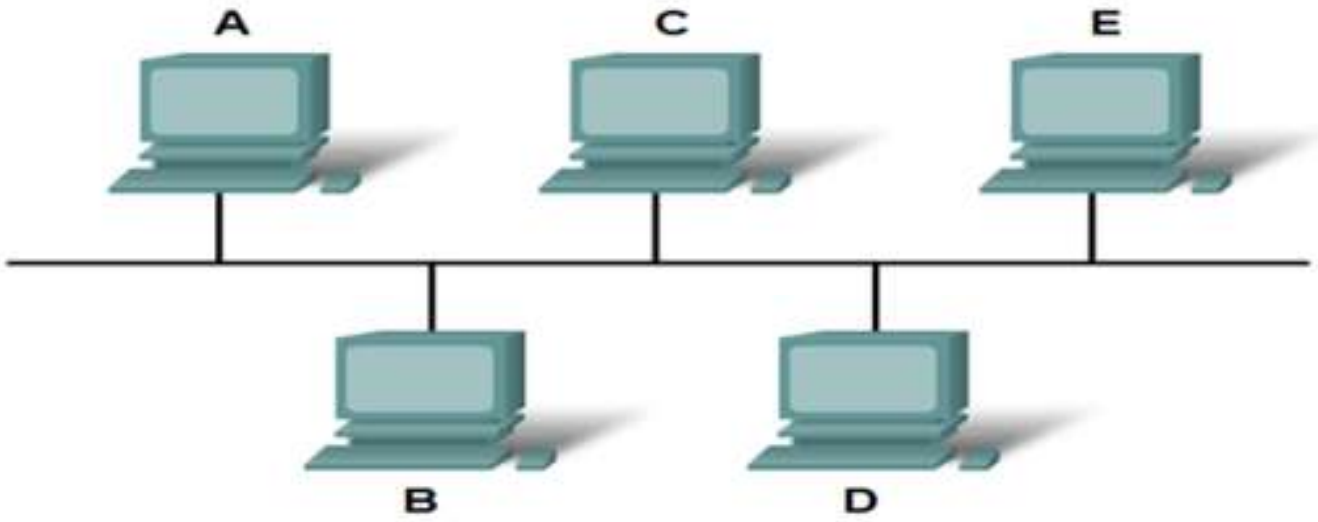


Data Link Layer – Multi- Access Topology

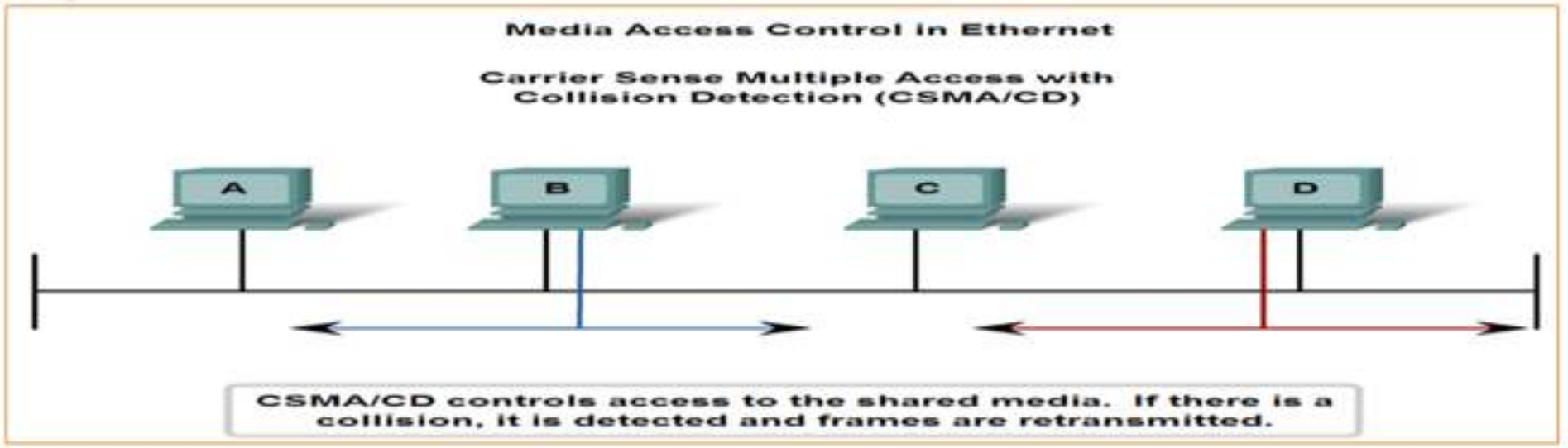
Having many nodes share access to the medium requires a Data Link media access control method to regulate the transmission of data and thereby reduce collisions between different signals.

The media access control methods used by logical multi-access topologies are typically CSMA/CD or CSMA/CA. However, token passing methods can also be used.

Logical Multi-Access Topology

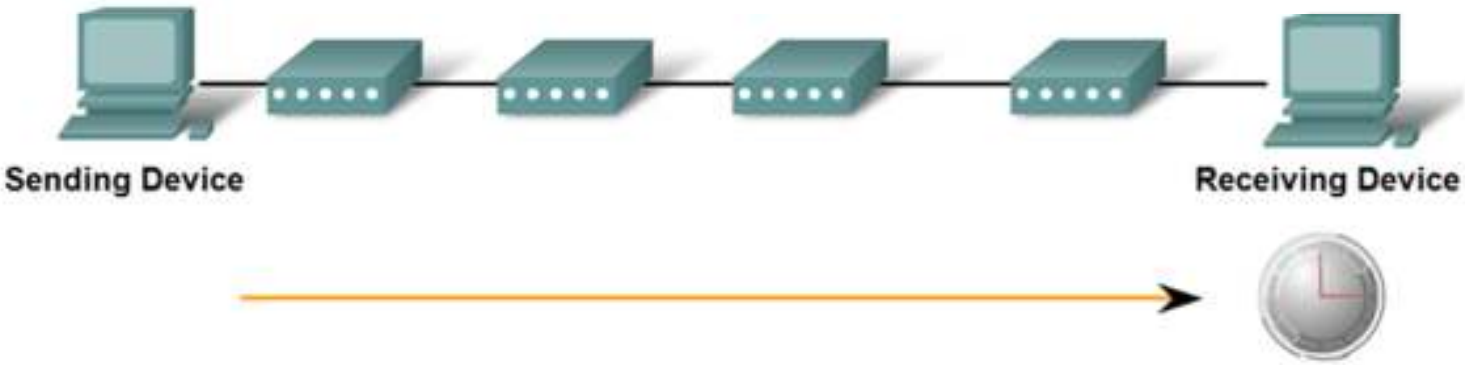


Data Link Layer - CSMA/CD



Data Link Layer - Timing

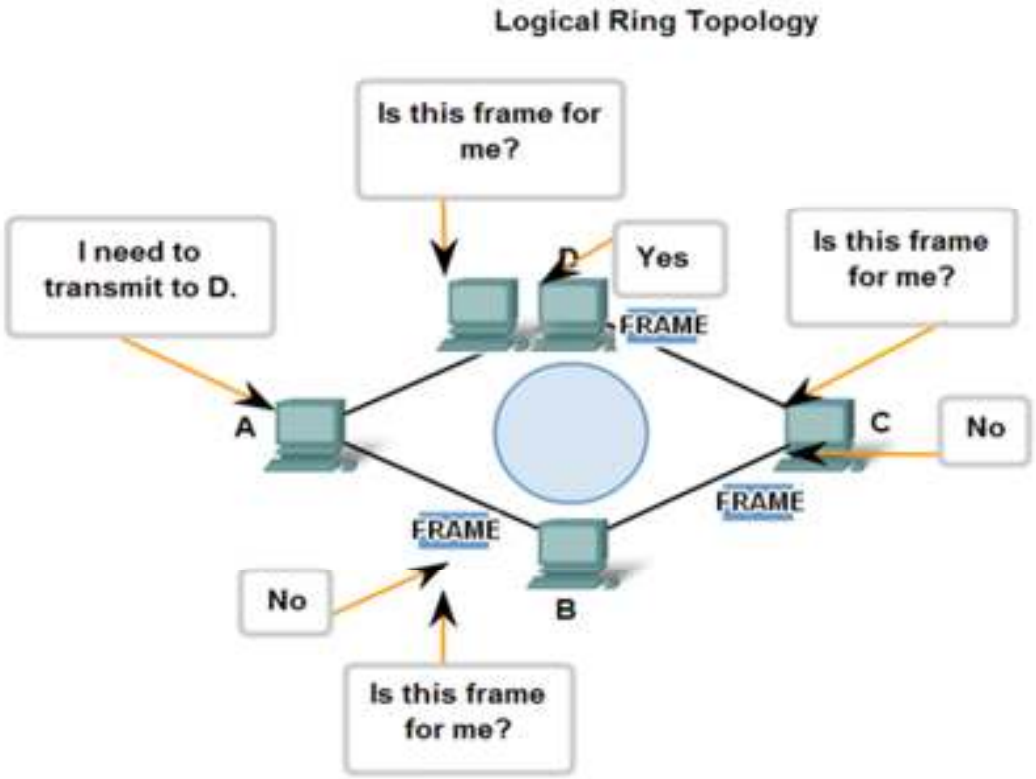
Ethernet Delay (Latency)



An Ethernet frame takes a measurable time to travel from the sending device to the receiver. Each intermediary device contributes to the overall latency.

Data Link Layer – Ring Topology

In a logical ring topology, each node in turn receives a frame. If the frame is not addressed to the node, the node passes the frame to the next node. This allows a ring to use a controlled media access control technique called token passing.



Data Link Layer – The Frame

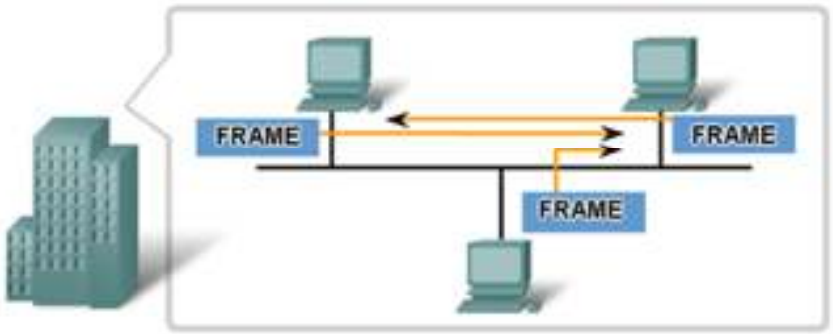
Data Link Layer Protocols - The Frame

In a fragile environment, more controls are needed to ensure delivery. The header and trailer fields are larger as more control information is needed.

Greater effort needed to ensure delivery = higher overhead = slower transmission rates

In a protected environment, we can count on the frame arriving at its destination. Fewer controls are needed, resulting in smaller fields and smaller frames.

Less effort needed to ensure delivery = lower overhead = faster transmission rates



Data Link Layer – Framing

Typical frame header fields include:

Start Frame field - Indicates the beginning of the frame

Source and Destination address fields - Indicates the source and destination nodes on the media

Priority/Quality of Service field - Indicates a particular type of communication service for processing

Type field - Indicates the upper layer service contained in the frame

Logical connection control field - Used to establish a logical connection between nodes

Physical link control field - Used to establish the media link

Flow control field - Used to start and stop traffic over the media

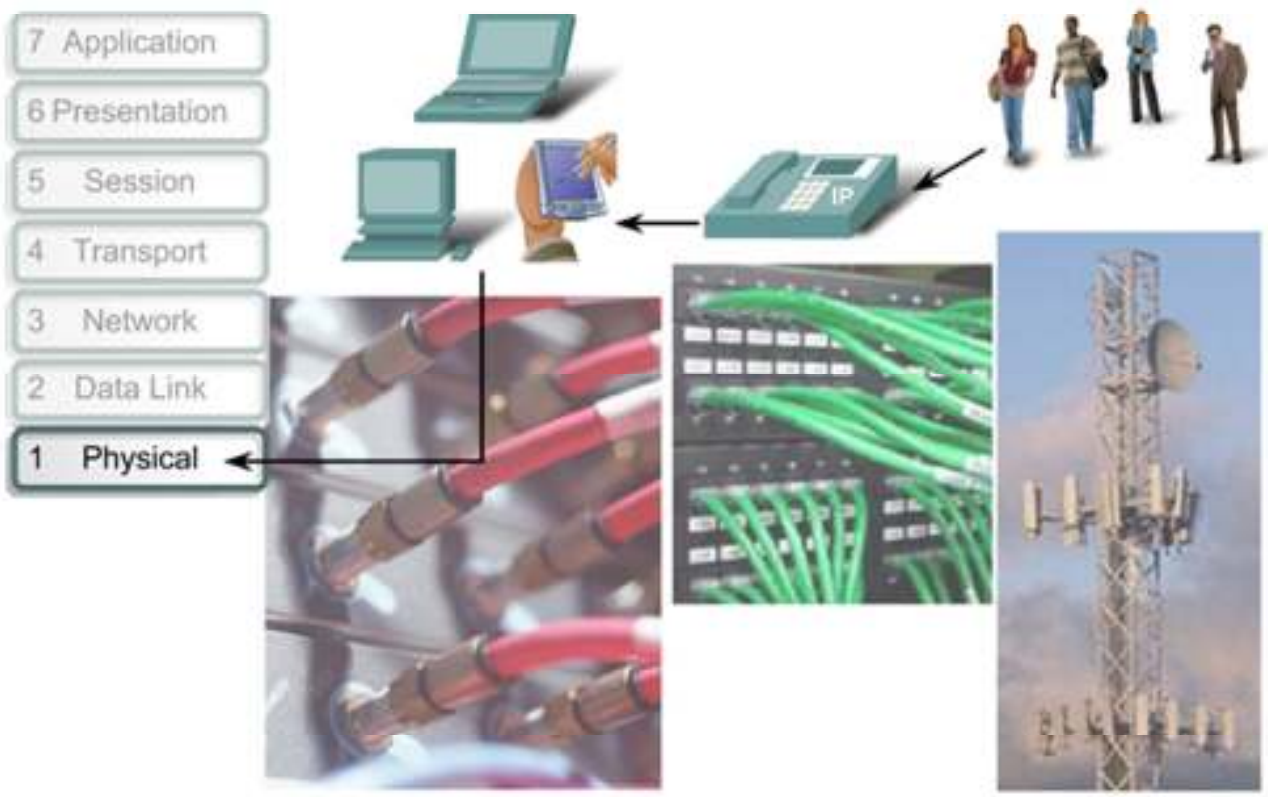
Congestion control field - Indicates congestion in the media

Data Link Layer – Role of The Trailer

The Frame Check Sequence (FCS) field is used to determine if errors occurred in the transmission and reception of the frame. Error detection is added at the Data Link layer because this is where data is transferred across the media.

Physical Layer

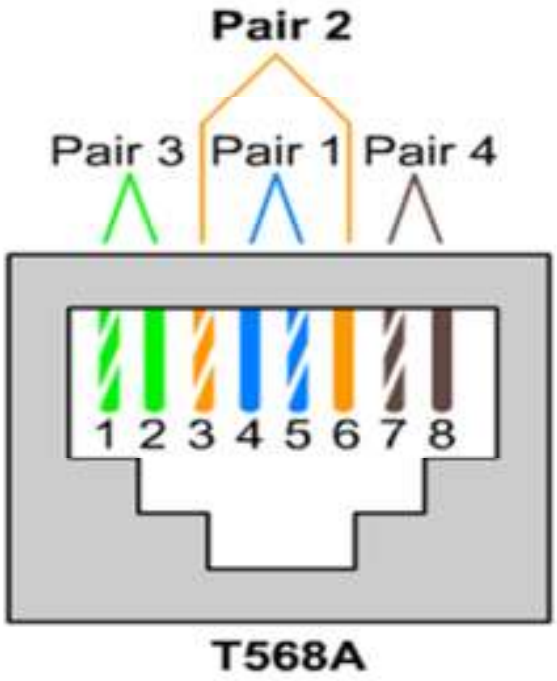
OSI Physical Layer

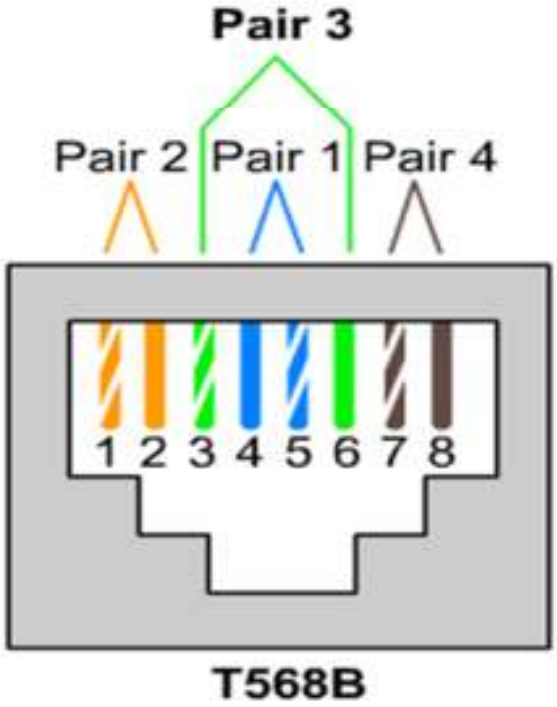


The Physical layer interconnects our data networks.

OSI PHYSICAL LAYER- Connecting to Ethernet Layer

- A straight-thru cable has T568B on both ends. A crossover (or cross-connect) cable has T568B on one end and T568A on the other. A console cable had T568B on one end and reverse T568B on the other, which is why it is also called a rollover cable.





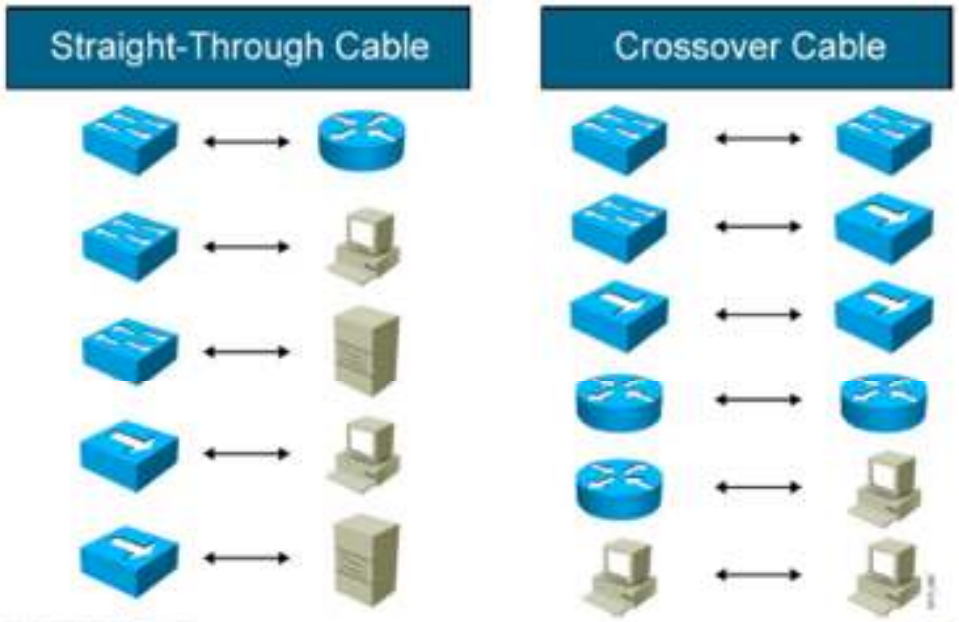
OSI PHYSICAL LAYER- Connecting to Ethernet Layer

Use straight-through cables for the following cabling:

- Switch to router
- Switch to PC or server
- Hub to PC or server

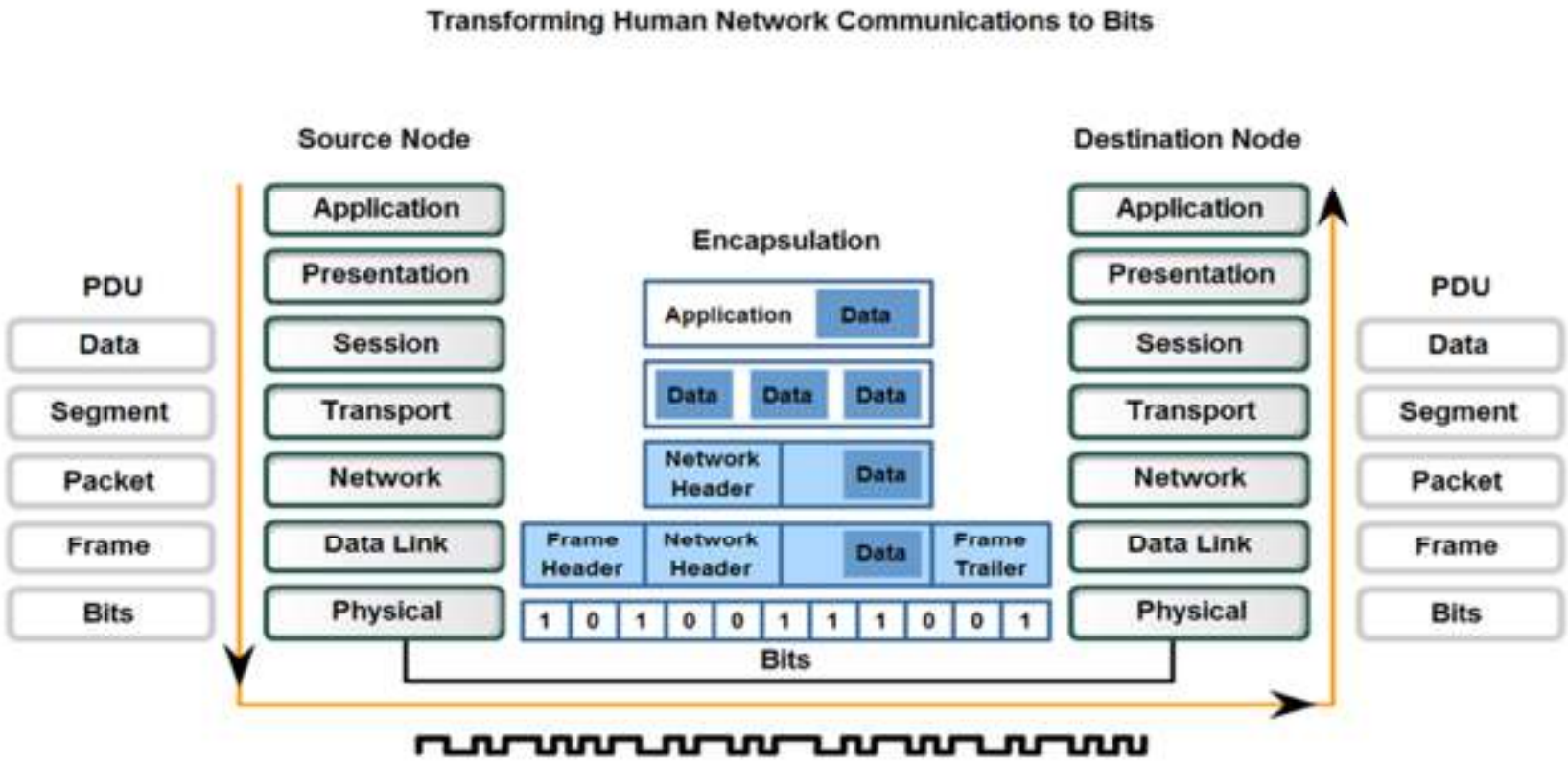
Use crossover cables for the following cabling:

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- PC to PC
- Router to PC



OSI PHYSICAL LAYER

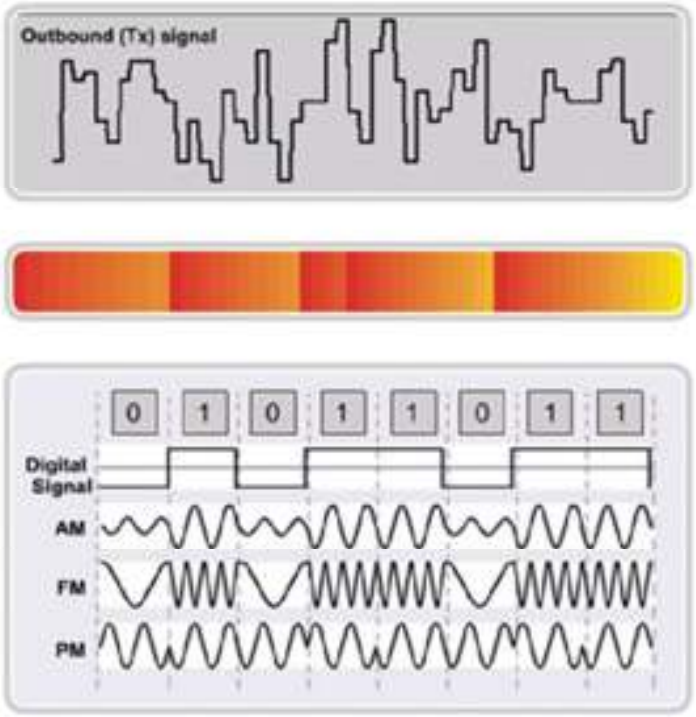
- Describe the role of bits in representing a frame as it is transported across the local media



OSI PHYSICAL LAYER

- Describe the role of signaling in the physical media

Representations of Signals on the Physical Media



Sample electrical signals transmitted on copper cable

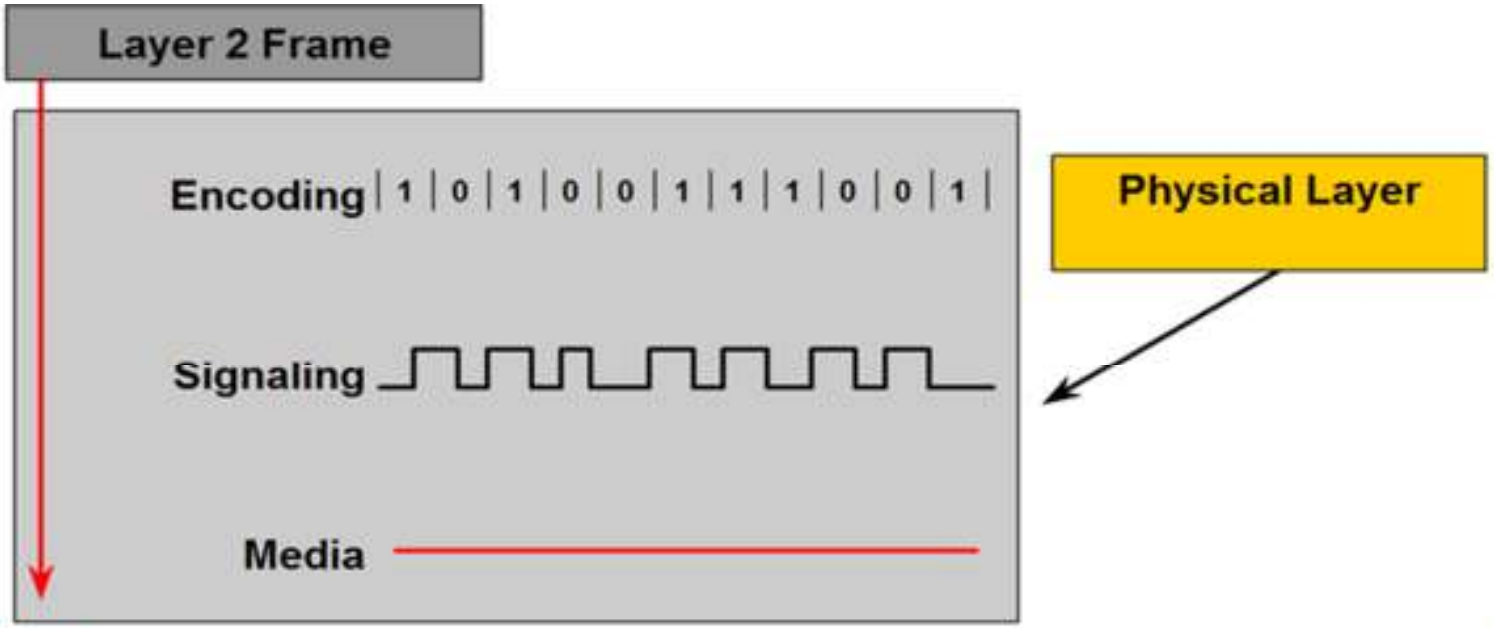
Representative light pulse fiber signals

Microwave (wireless) signals

OSI PHYSICAL LAYER

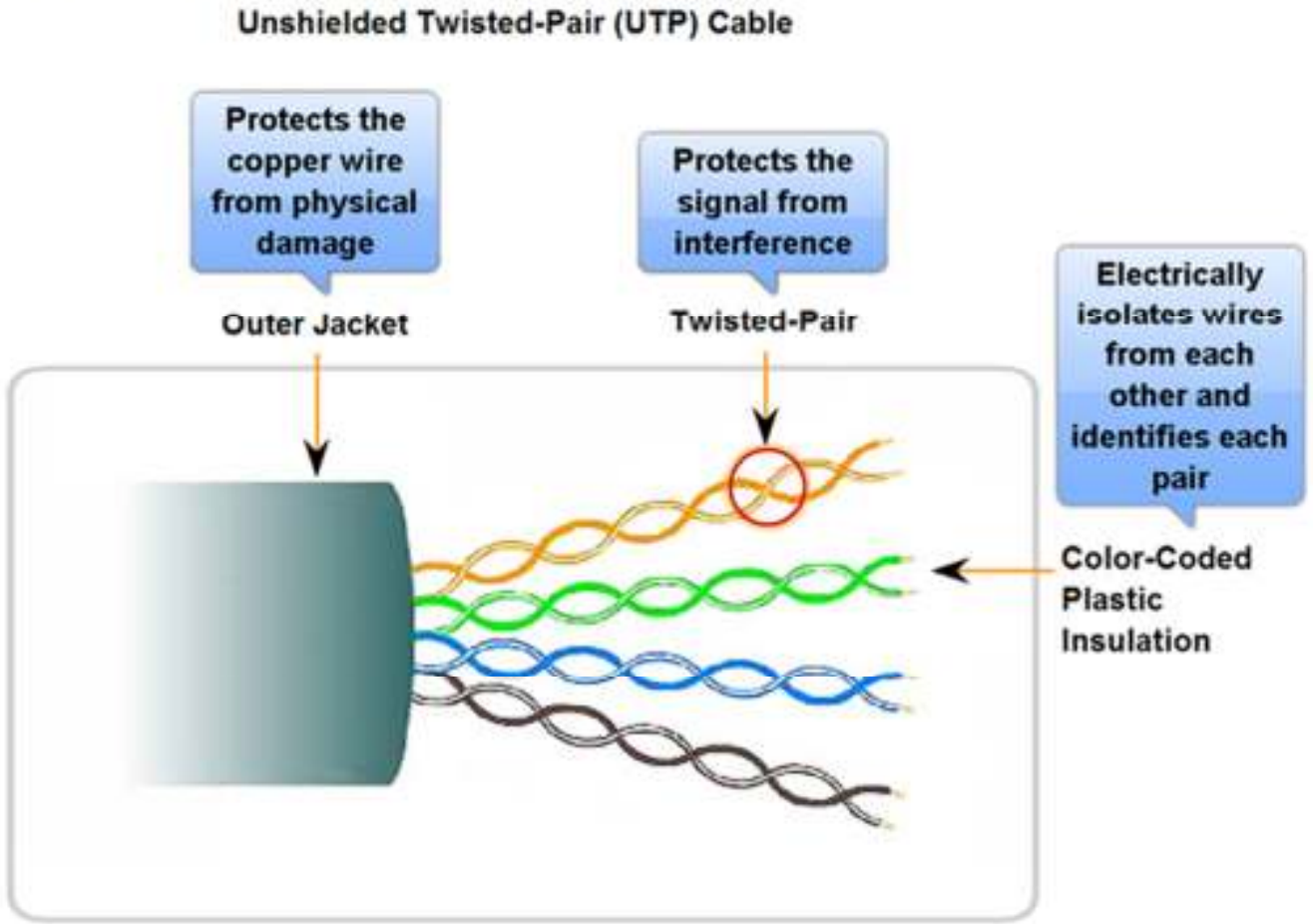
- Identify hardware components associated with the Physical layer that are governed by standards

Physical Layer Fundamental Principles



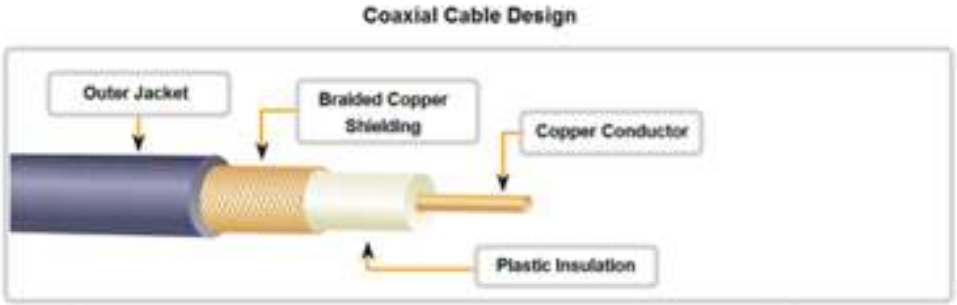
OSI PHYSICAL LAYER

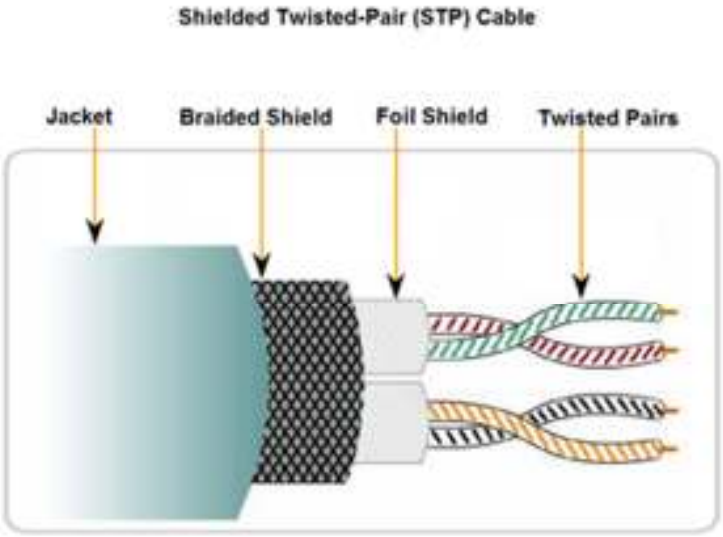
- Identify the basic characteristics of UTP cable



OSI PHYSICAL LAYER

- Identify the basic characteristics of STP and Coaxial cable





OSI PHYSICAL LAYER

- Identify types of safety issues when working with copper cabling

Copper Media Safety

The separation of data and electrical power cabling must comply with safety codes.

Cables must be connected correctly.

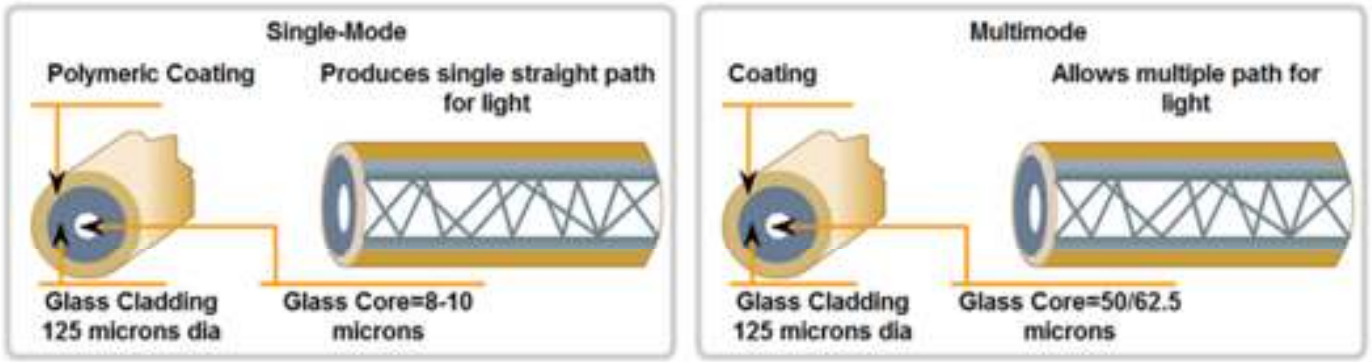
Installations must be inspected for damage.

Equipment must be grounded correctly.

OSI PHYSICAL LAYER

- Identify several primary characteristics of fiber cabling and its main advantages over other media

Fiber Media Modes

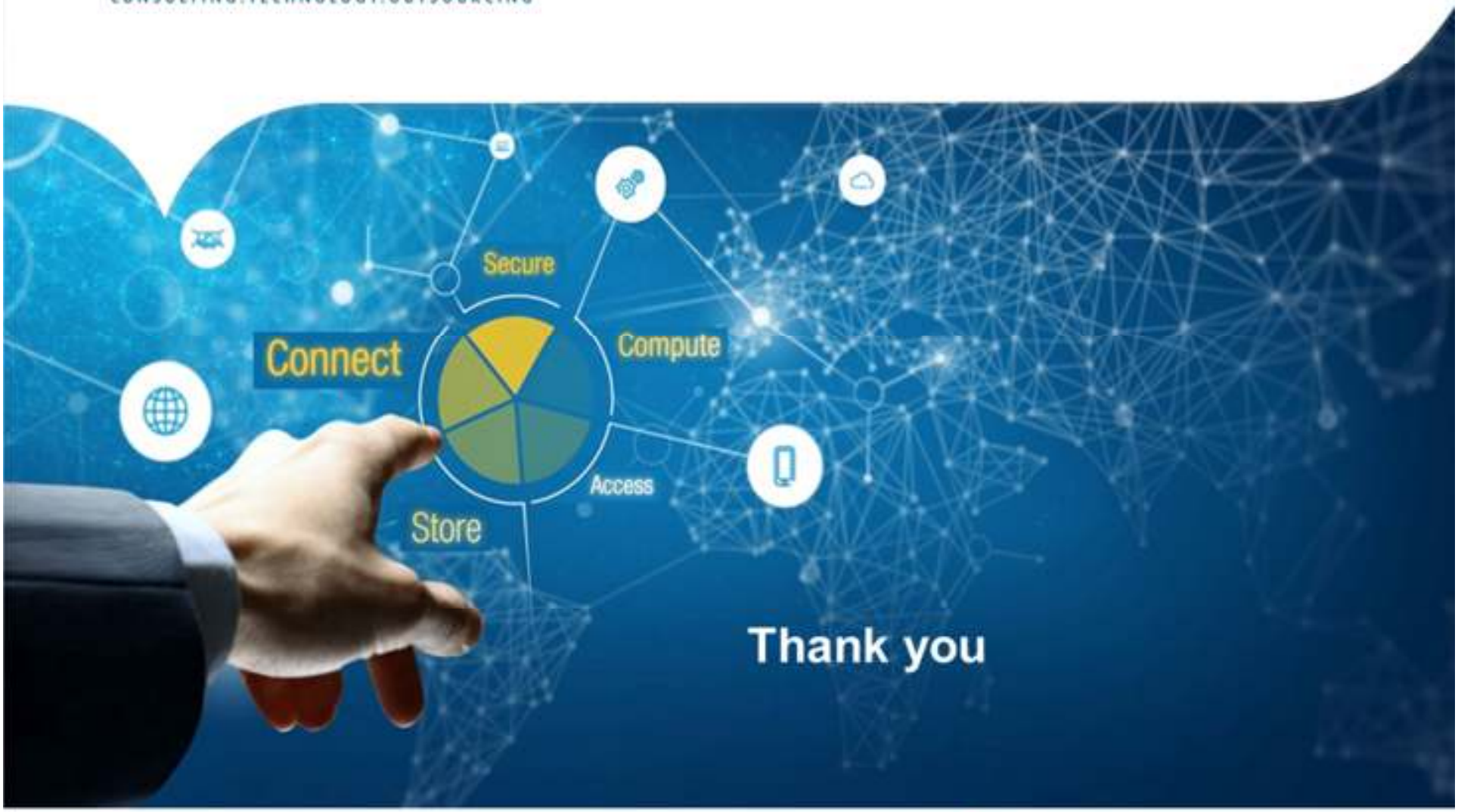


- Small Core
- Less Despersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance application, but shoter than single-mode (up to ~2km, 6560 ft)
- Uses LEDs as the light source often within LANs or distances of couple hundred meters within a campus network

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING



People matter, results count.