Ministry of Higher Education

And Scientific Research

Al-Furat Al-Awsat Technical University

Technical Institute of Karbala

Networks

Haider MohammedAli M.R. AlTomah

Technical Institute Of Karbala

Computers Systems Department

2022 - 2023

Introduction

- A set of data handling devices (DATA TERMINAL EQUPMENT) connected together through a communication channel.
- A set of computers, printers, or any other devices connected to each other wired or wireless, and each device is called a node (NODE).

Why do we need a network?

1 \ Easy and fast exchange of information and data.

2 \ Participate in Calculator Resources (H \ W & S \ W).

3 \ Solve complex and large problems.

Transaction Media

1- Wired:

I. TP – Twisted Pair

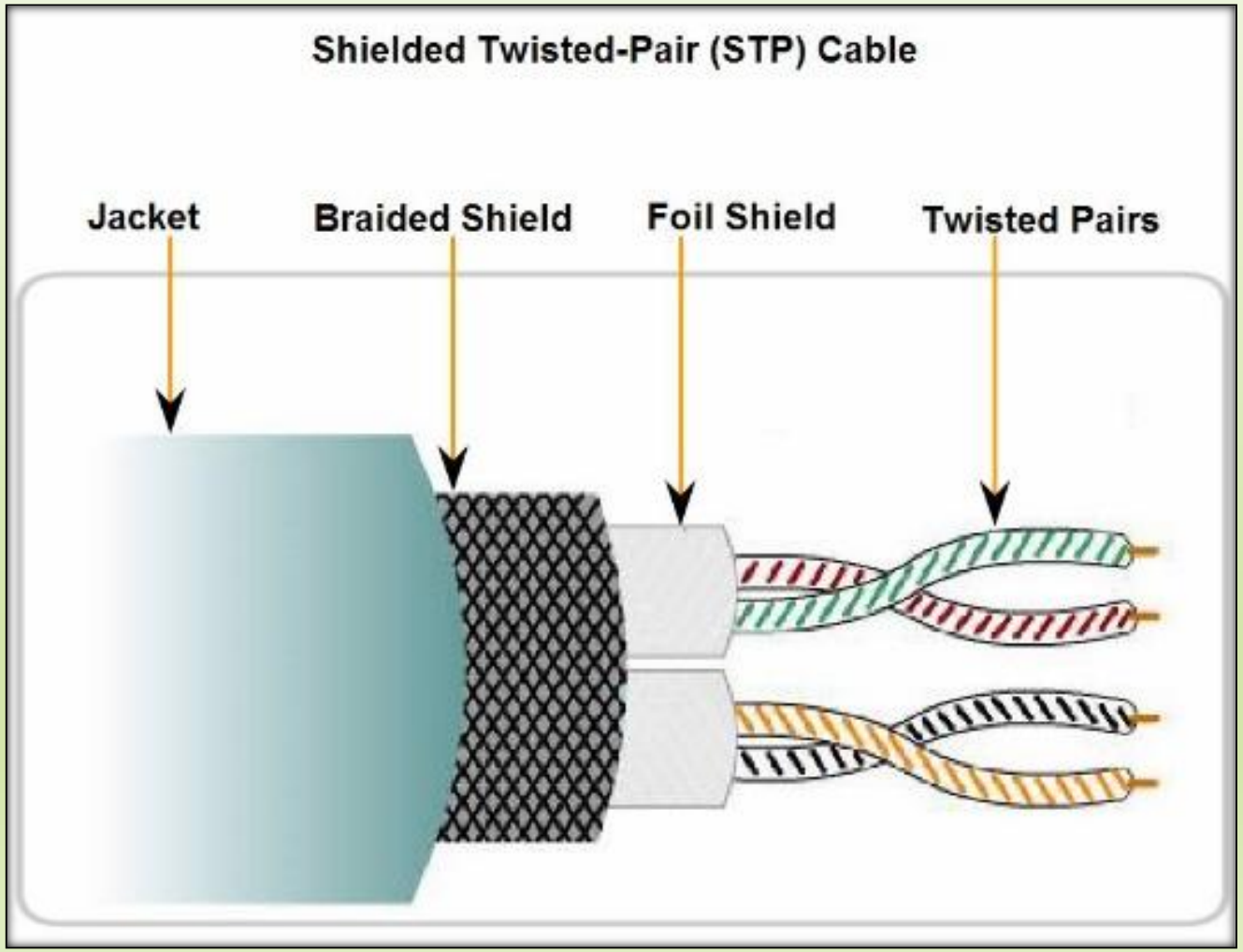
A. UTP – Unshielded Twisted Pair

Cat 5

Cat 6

Transaction Media (cont.)

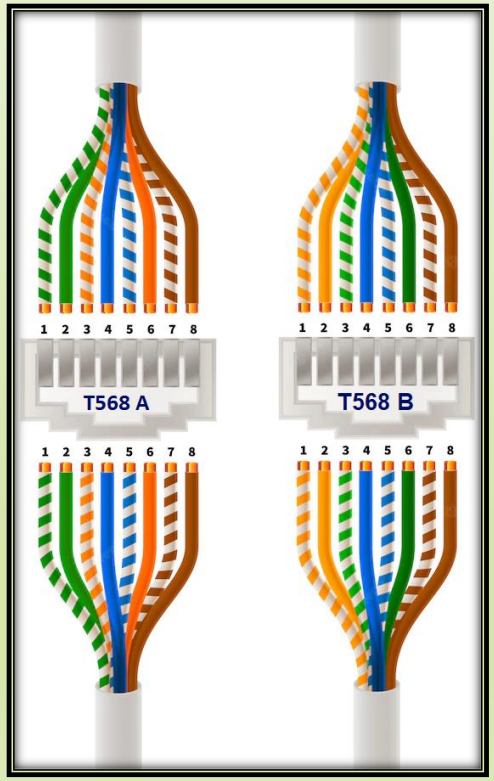
B. STP – Shielded Twisted Pair

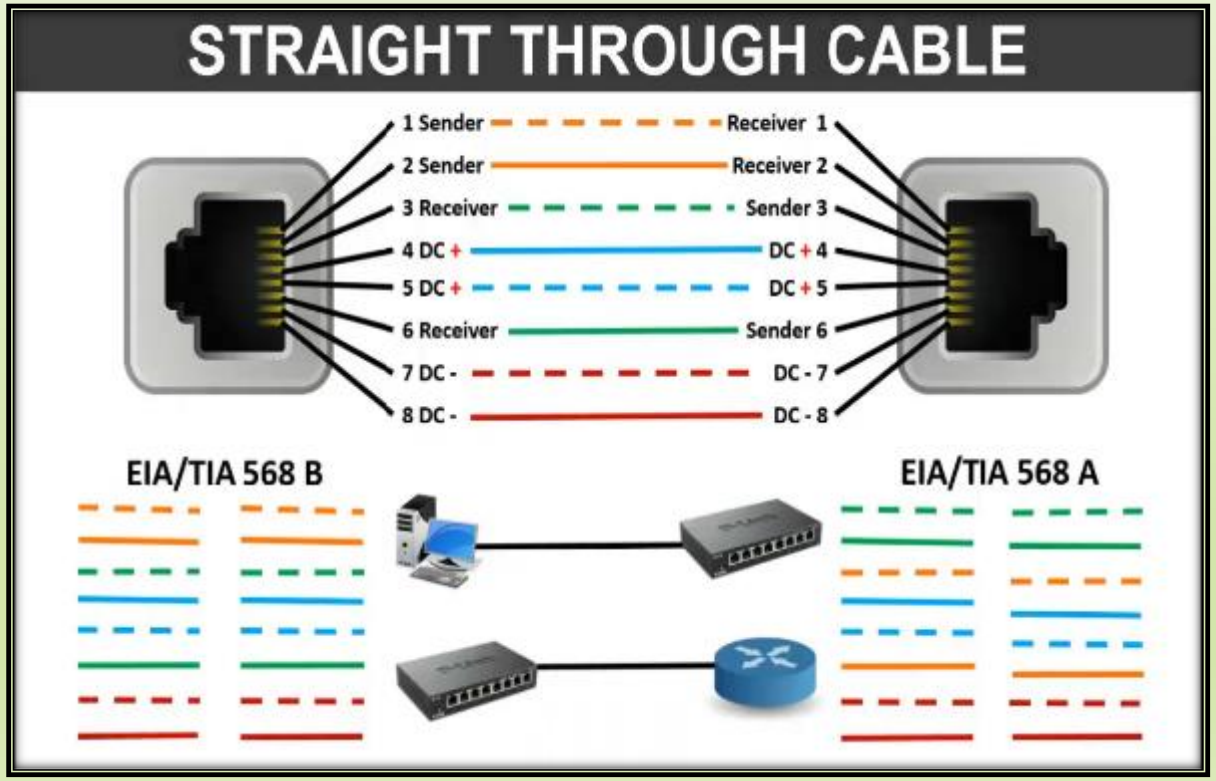


Transaction Media (cont.)

Types of connect for cables

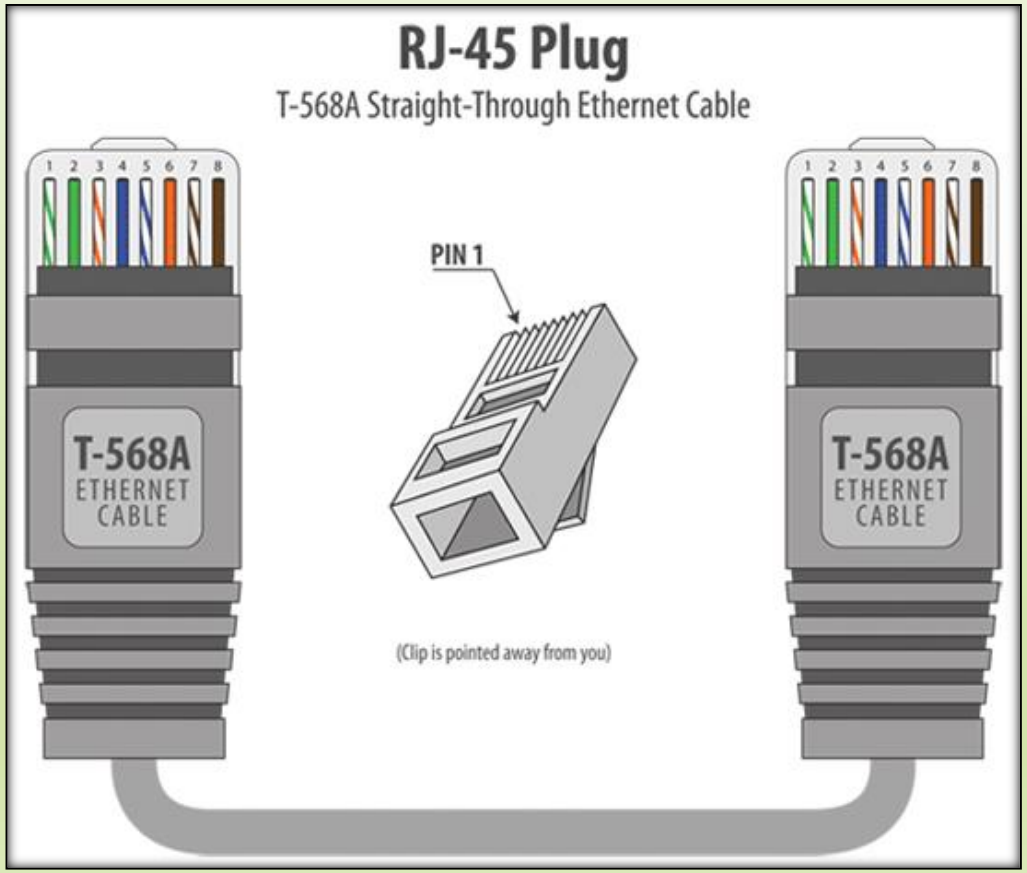
I. Straight Through

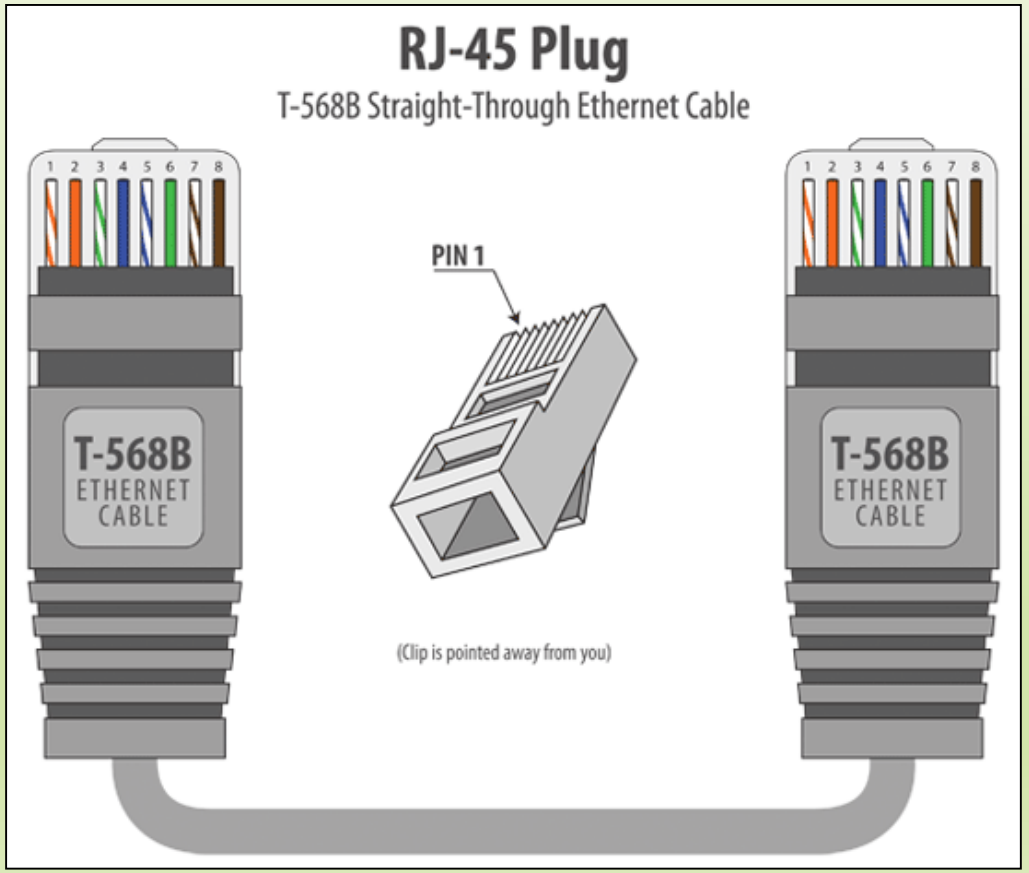




Transaction Media (cont.)

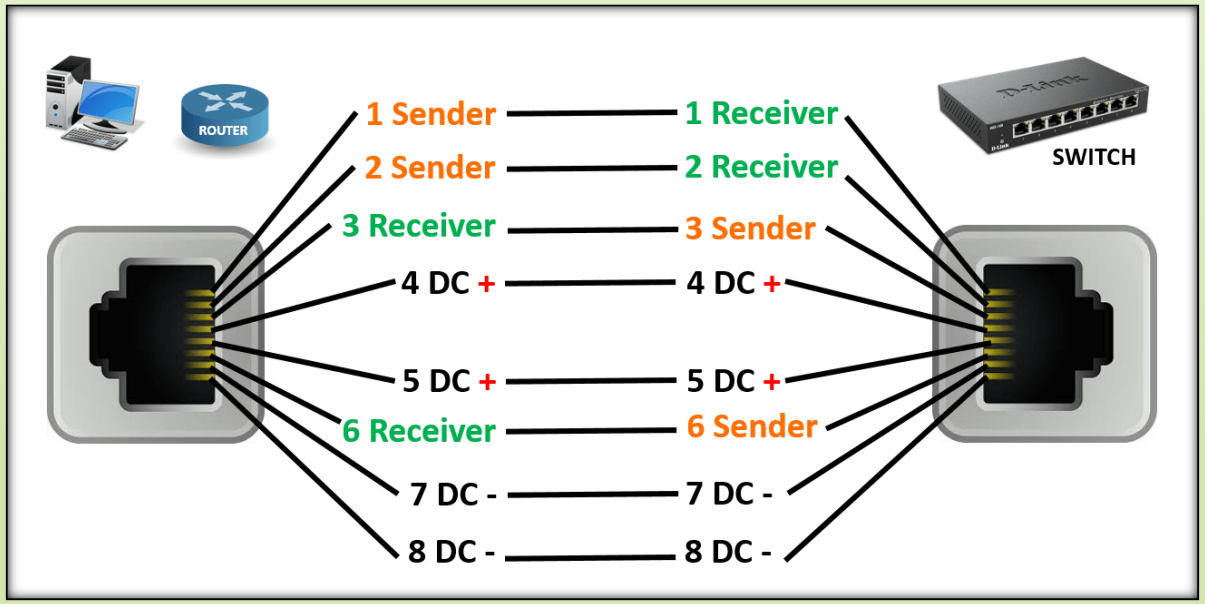
I. Straight Through

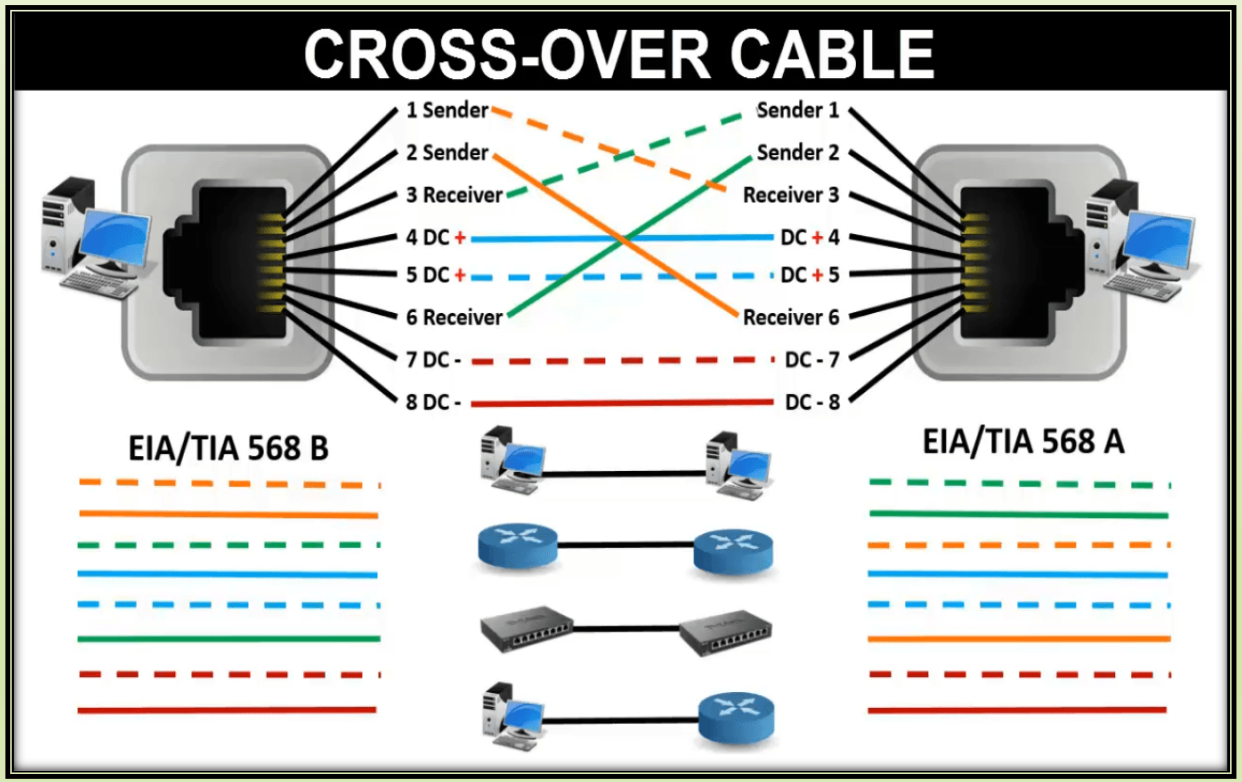




Transaction Media (cont.)

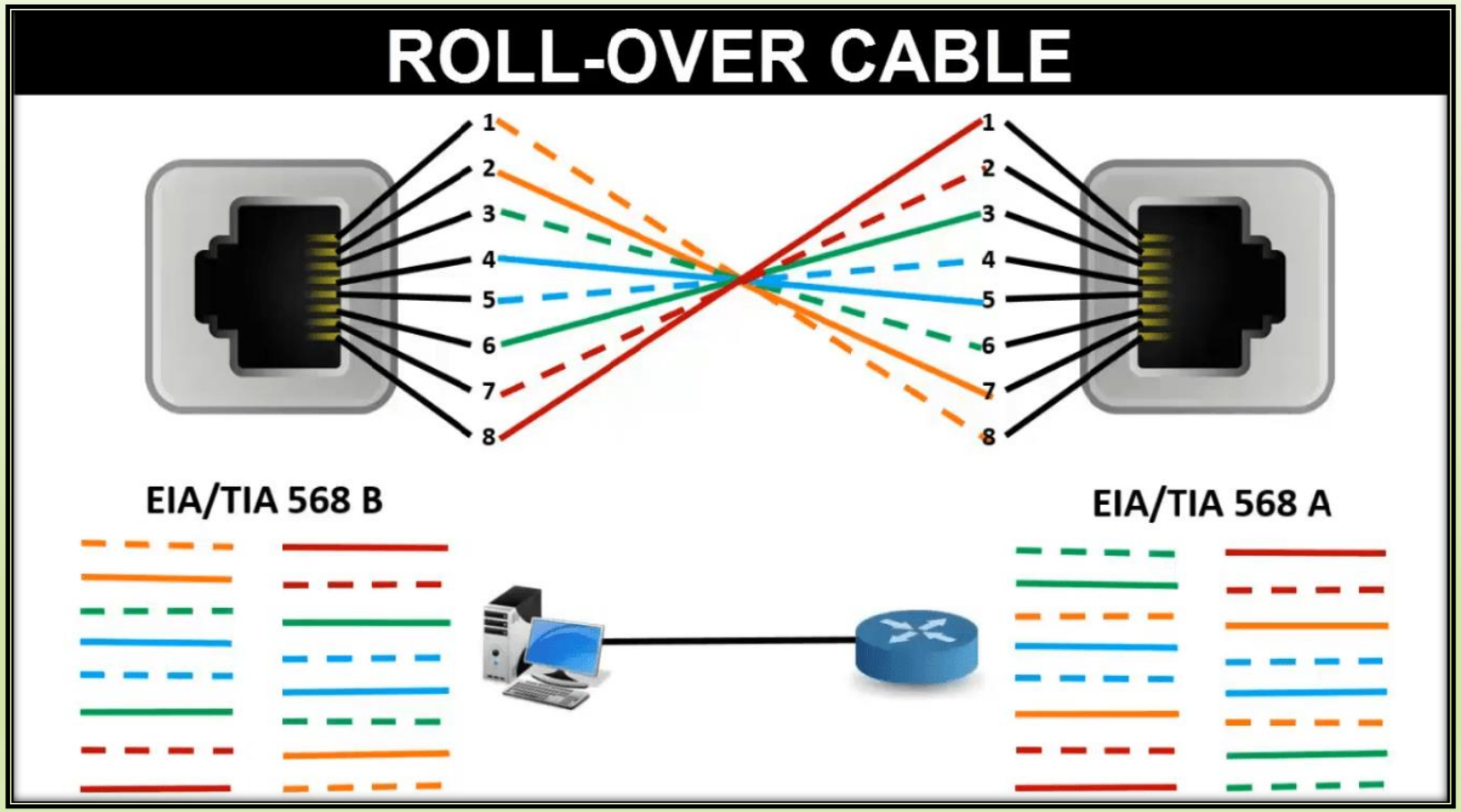
II. Cross Over





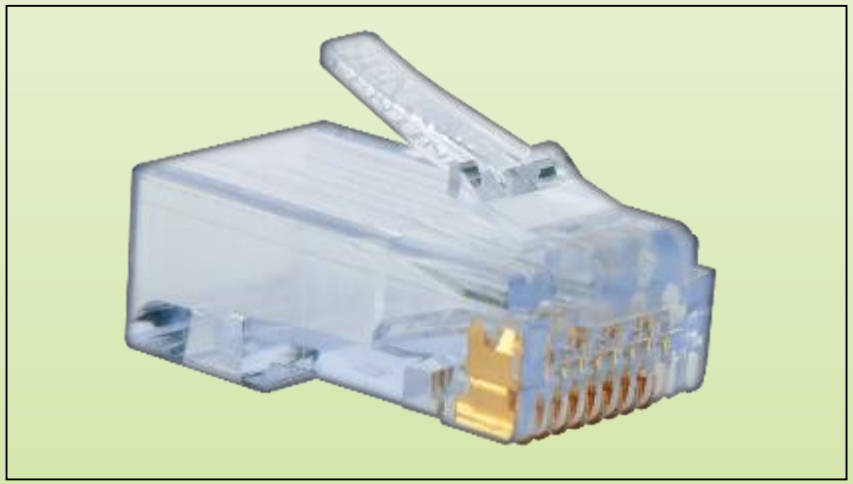
Transaction Media (cont.)

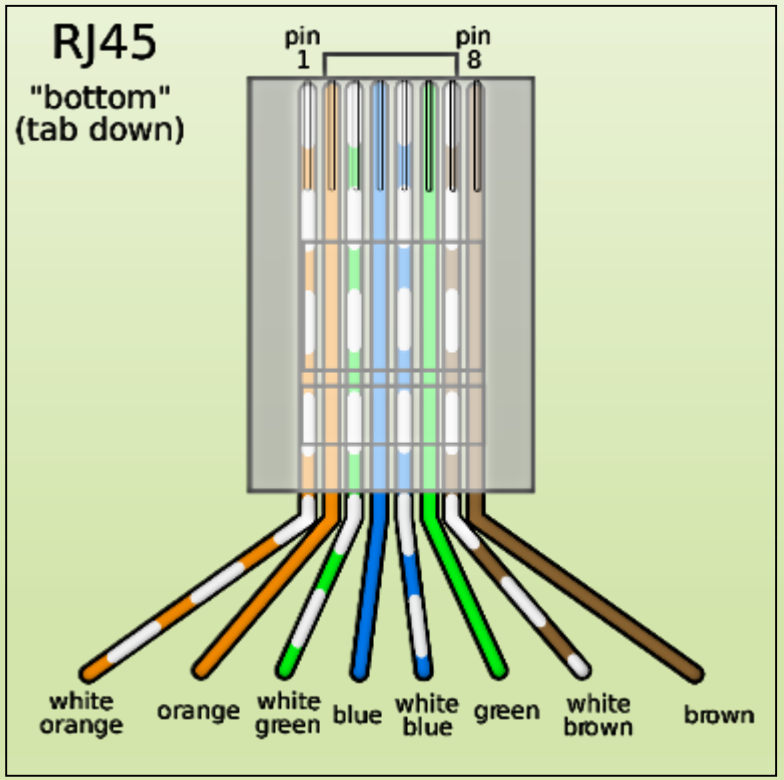
III. Roll Over



Transaction Media (cont.)

RJ45 Connector



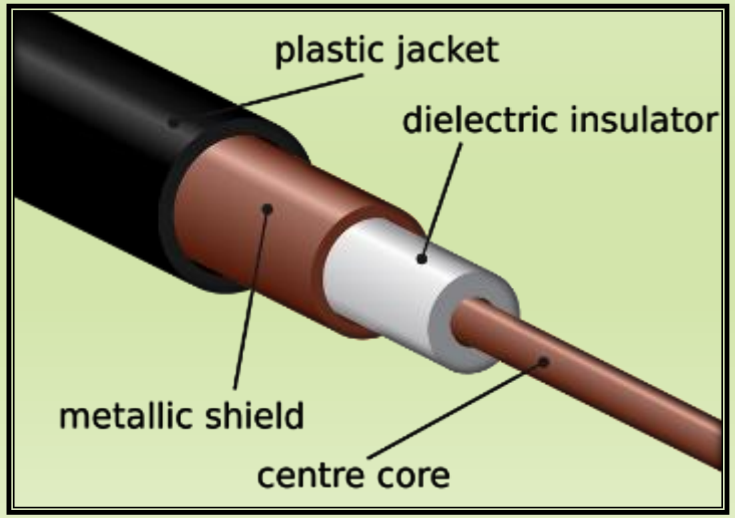


Transaction Media (cont.)

Connectors Tools

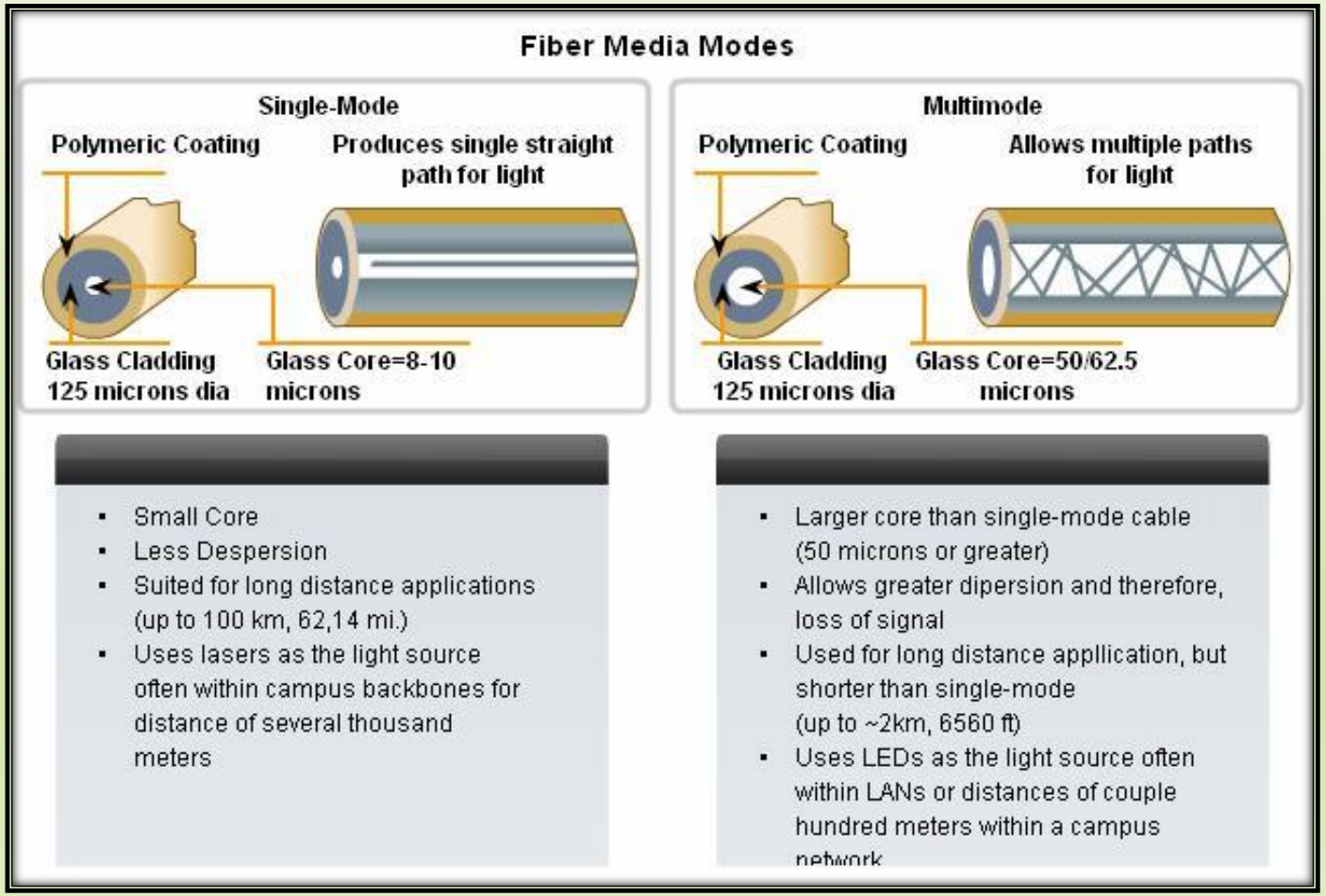
Transaction Media (cont.)

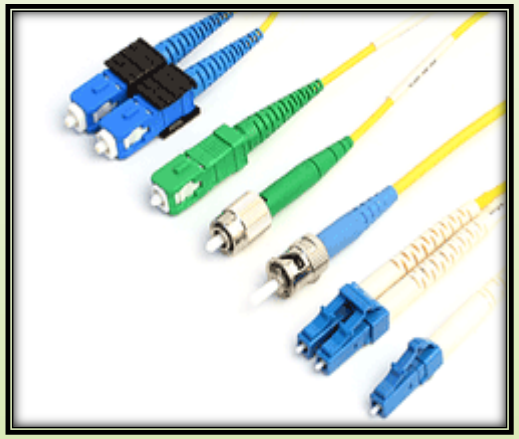
II. Coaxial cable " BNC "



Transaction Media (cont.)

III.Fiber optics



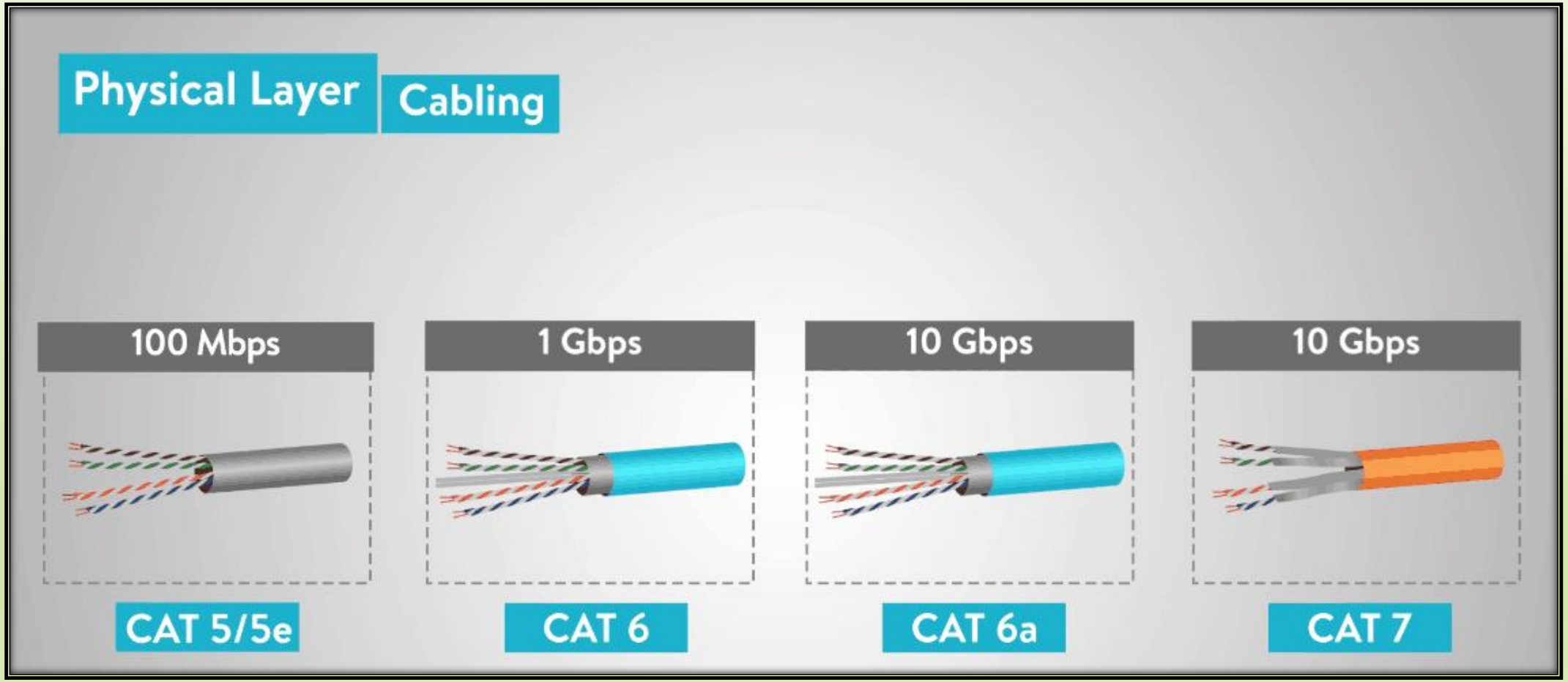


- Small Core
- Less Despersion
- Suited for long distance applications (up to 100 km, 62,14 mi.)
- Uses lasers as the light source often within campus backbones for distance of several thousand meters

- Larger core than single-mode cable (50 microns or greater)
- Allows greater dipersion and therefore, loss of signal
- Used for long distance appllication, but shorter 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

Transaction Media (cont.)

Unshielded Twisted Pair Types



Transaction Media (cont.)

Ethernet Cable Comparison Chart			
Category	Shielded	Max. Transmission	Max. Bandwidth
Cat 3	No	10 Mbps at 100m	16 MHz
Cat 5	No	10/100 Mbps at 100m	100 MHz
Cat 5e	No	1 Gbps at 100m	100 MHz
Cat 6	Yes & No	1 Gbps at 100m	250 MHz
Cat 6a	Yes	10 Gbps at 100m	500 MHz
Cat 7	Yes	10 Gbps at 100m	600 MHz
Cat 7a	Yes	10 Gbps at 100m	1000 MHz
Cat 8	Yes	25 Gbps/40 Gbps	2000 MHz at 30m

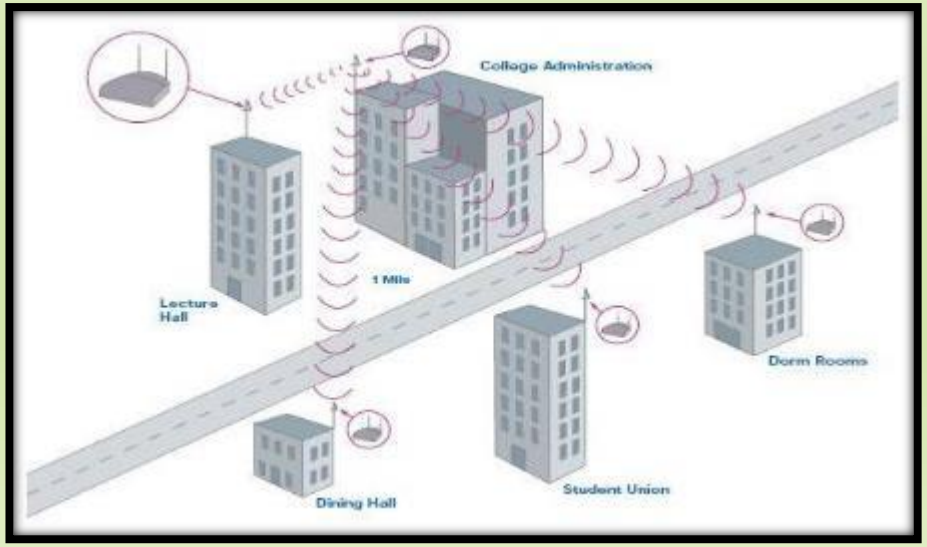
Transaction Media (cont.)

Ethernet Type	Bandwidth	Cable Type	Maximum Distance
10Base-T	10Mbps	Cat 3/Cat 5 UTP	100m
100Base-TX	100Mbps	Cat 5 UTP	100m
100Base-TX	200Mbps	Cat 5 UTP	100m
100Base-FX	100Mbps	Multi-mode fiber	400m
100Base-FX	200Mbps	Multi-mode fiber	2Km
1000Base-T	1Gbps	Cat 5e UTP	100m
1000Base-TX	1Gbps	Cat 6 UTP	100m
1000Base-SX	1Gbps	Multi-mode fiber	550m
1000Base-LX	1Gbps	Single-mode fiber	2Km
10GBase-T	10Gbps	Cat 6a/Cat 7 UTP	100m
10GBase-LX	10Gbps	Multi-mode fiber	100m
10GBase-LX	10Gbp	Single-mode fiber	10Km

Transaction Media (cont.)

2 - Wireless

- Direct connection
  - Microwave
  - Infrared
  - Satellite
- Indirect connection
  - Radio
  - Blue tooth



Types of Networks

- **Peer to peer (P2P)**

A peer-to-peer network is one in which two or more PCs share files and access to devices such as printers without requiring a separate server computer or server software.

Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers.

Types of Networks (cont.)

- **Client/server**

Is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called servers, and service requesters, called clients. Often clients and servers communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server host runs one or more server programs, which share their resources with clients. A client does not share any of its resources, but it requests content or service from a server. Clients therefore initiate communication sessions with servers, which await incoming requests. Examples of computer applications that use the client–server model are Email, network printing, and the World Wide Web.

Wireless Network Standardizations Types

- **IEEE Standardizations**

  - **The IEEE (Institute of Electrical and Electronics Engineers)and telecommunications industry standards for wireless data communications cover both the Data Link and Physical layers. Four common data communications standards that apply to wireless media are:**

I. **Standard IEEE 802.11 - Commonly referred to as Wi-Fi, is a Wireless LAN (WLAN) technology that uses a contention or non-deterministic system with a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) media access process.**

Wireless Network Standardizations Types (cont.)

II. Standard IEEE 802.15 - Wireless Personal Area Network (WPAN) standard, commonly known as "Bluetooth", uses a device pairing process to communicate over distances from 1 to 100 meters.

III. Standard IEEE 802.16 - Commonly known as WiMAX (Worldwide Interoperability for Microwave Access), uses a point-to-multipoint topology to provide wireless broadband access.

IV. Global System for Mobile Communications (GSM) - Includes Physical layer specifications that enable the implementation of the Layer 2 General Packet Radio Service (GPRS) protocol to provide data transfer over mobile cellular telephony networks.

Networks Classification

We can classify the networks in to two parts :

I. By distance

- **LAN** Local Area Network (0.5 M → 100 M).
- **CAN** Compound Area Network (100 M → 1 KM).
- **MAN** Metropolitan Area Network (1 KM → 50 KM).
- **WAN** Wide Area Network (50 KM → 1000 KM).
- **INTERNET** Planet.

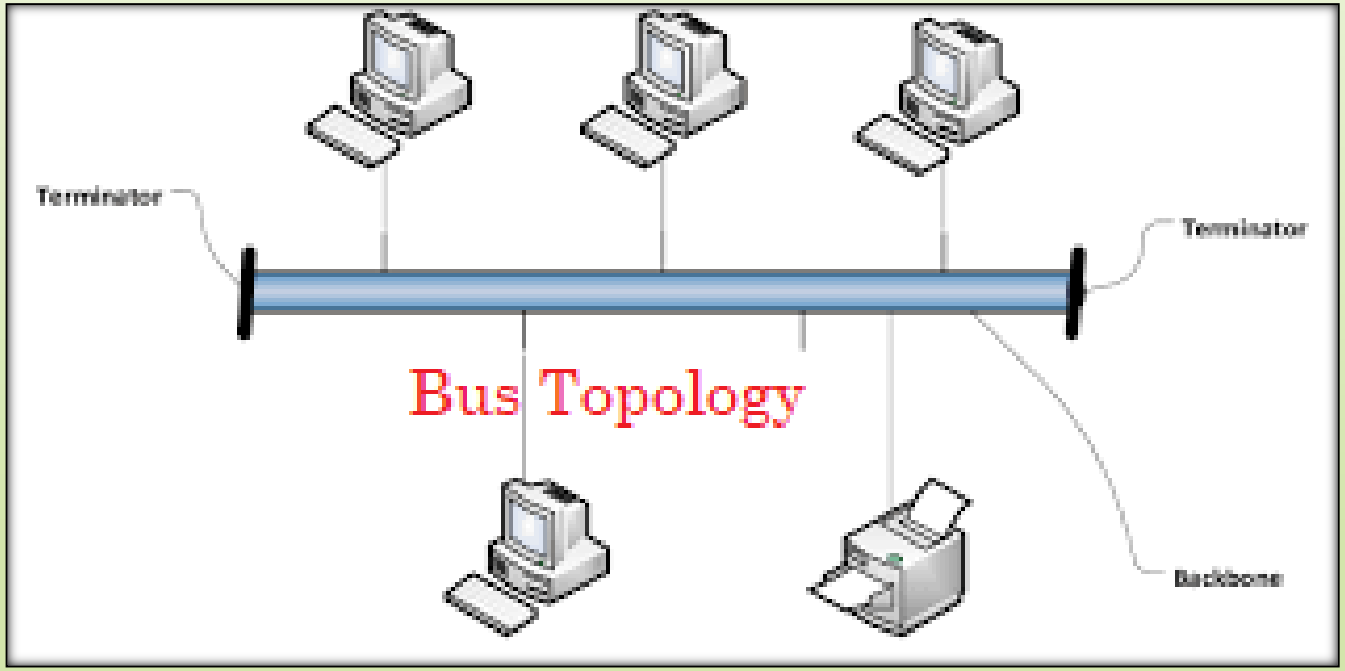
Networks Classification (cont.)

II. By topology

A. Bus

- **Advantage**
  - Low coast
- **Disadvantage**

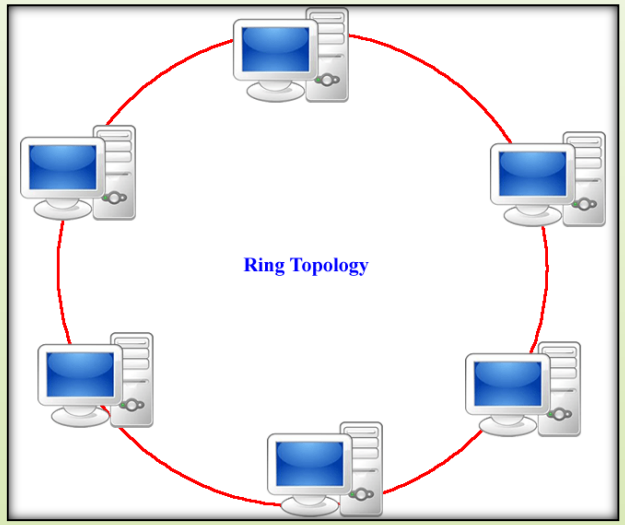
- 1 / When the disconnection occurs in the wire the connection stops.
- 2 / The distance should be accurate to avoid the error in The receipt.

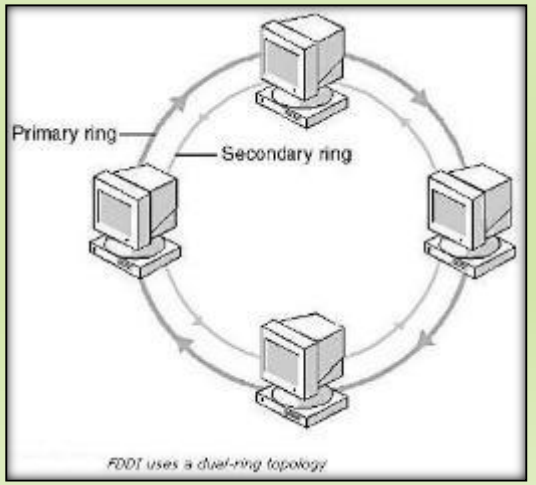


Networks Classification (cont.)

B. Ring

- **Advantage**
  - Not affected by the failure of a station.
- **Disadvantage**
  - Data transmitted between two stations passing on all stations, the flow of information is only one way.
  - difficulty connecting and adding new stations.

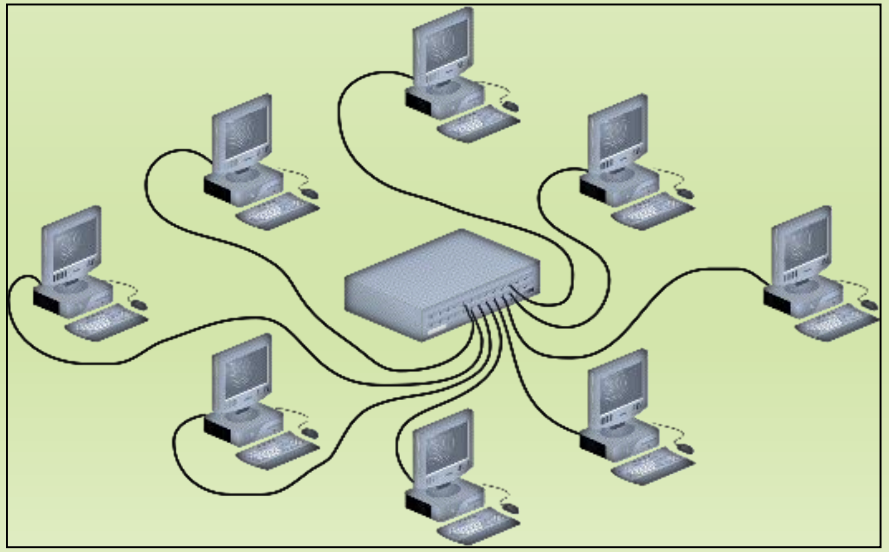




Networks Classification (cont.)

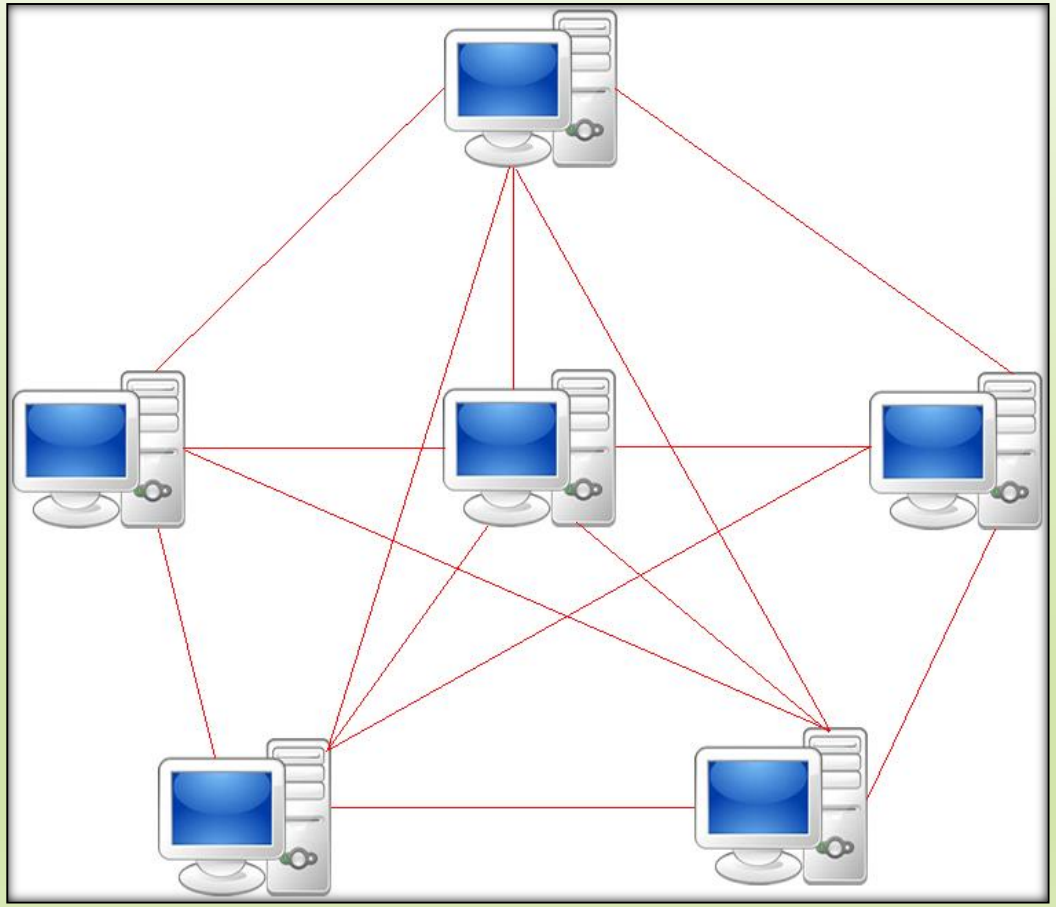
C. Star

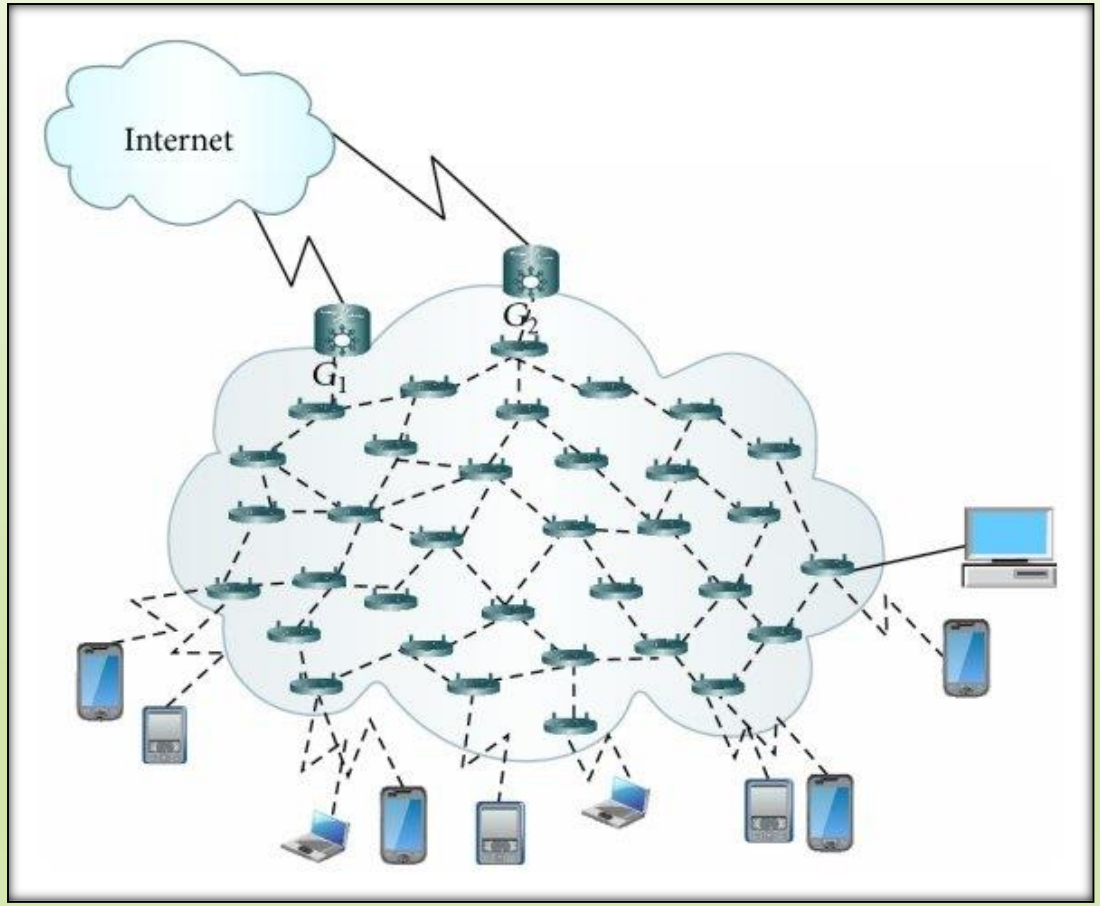
- **Advantage**
  - **Easy linking and addition.**
  - **Unlimited number of stations.**
- **Disadvantage**
  - **When the center point fails, the network will stop working.**



Networks Classification (cont.)

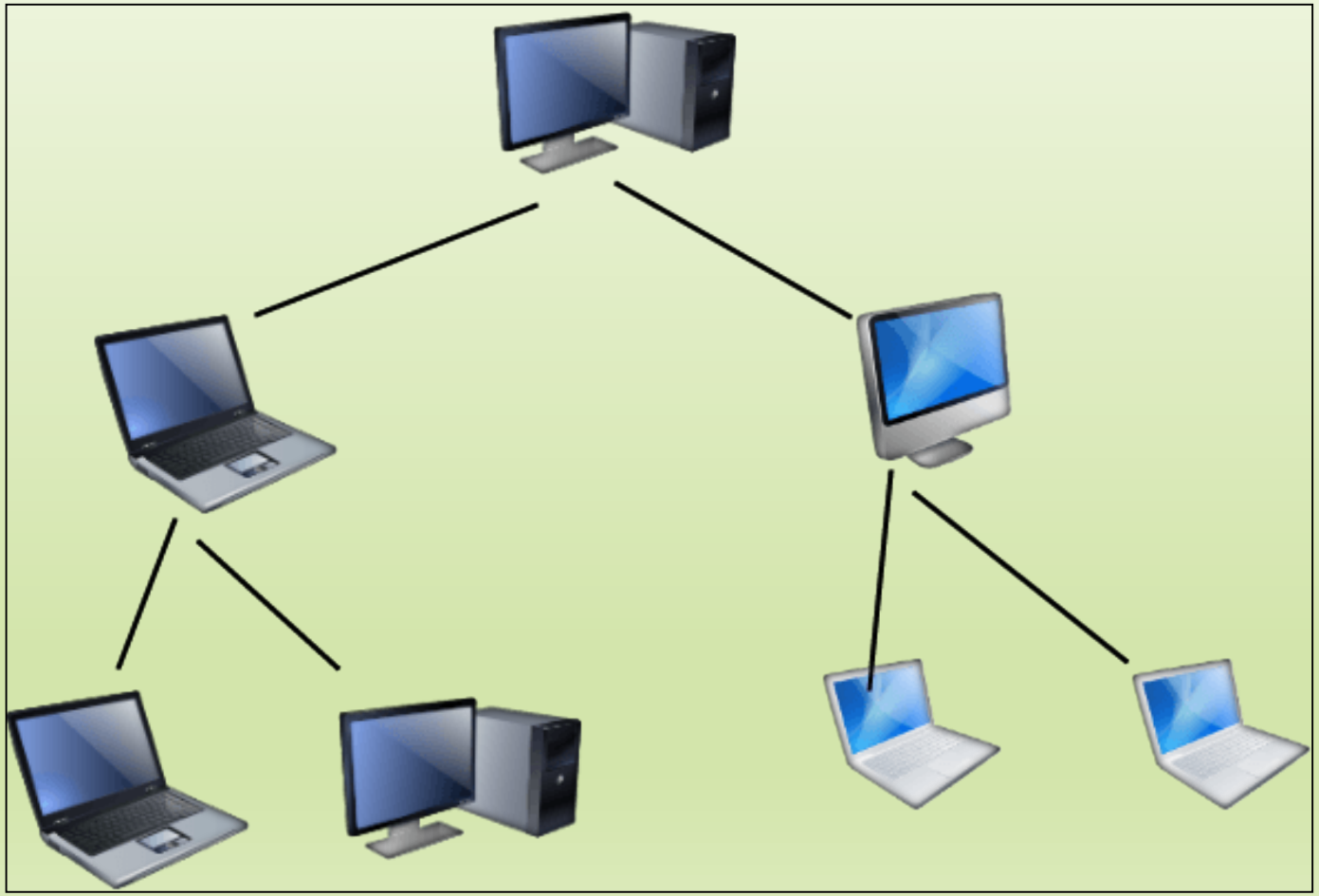
D. Mesh





Networks Classification (cont.)

D. Tree



Networks Classification (cont.)

- **Intranet**

An intranet is a computer network for sharing corporate information, collaboration tools, operational systems, and other computing services only within an organization, and to the exclusion of access by outsiders to the organization. The term is used in contrast to public networks, such as the Internet, but uses most of the same technology based on the Internet Protocol Suite.

- **Extranet**

An extranet is a controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet. An extranet is similar to a DMZ(demilitarized zone) in that it provides access to needed services for authorized parties, without granting access to an organization's entire network.

Bandwidth

- **Bandwidth (signal processing) or analog bandwidth, frequency bandwidth or radio bandwidth, a measure of the width of a range of frequencies, measured in hertz**
- **Bandwidth (computing), the rate of data transfer, bit rate or throughput, measured in bits per second (bit/s).**

Throughput

- Throughput is the rate of production or the rate at which something is processed.
- When used in the context of communication networks, such as Ethernet or packet radio, throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link, or it can pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.
- The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network.
- The throughput of a communication system may be affected by various factors, including the limitations of underlying analog physical medium, available processing power of the system components, and end-user behavior. useful rate of the transferred data can be significantly lower than the maximum achievable throughput; the useful part is usually referred to as goodput.

Networks Devices

• Network Interface Card (NIC)

- **Network Interface Card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so that it can connect to a network. Modern NICs provide functionality to computers such as support for I/O interrupt, Direct Memory Access (DMA) interfaces, data transmission, network traffic engineering and partitioning.**
- **A NIC provides a computer with a dedicated, full-time connection to a network by implementing the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network. The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer.**
- **The network card operates as a middleman between a computer and a data network.**

Networks Devices (cont.)

- **Modem**
  - **Is a hardware device that converts data into a format suitable for a transmission medium so that it can be transmitted from computer to computer (historically over telephone wires). A modem modulates one or more carrier wave signals to encode digital information for transmission and demodulates signals to decode the transmitted information. The goal is to produce a signal that can be transmitted easily and decoded reliably to reproduce the original digital data. Modems can be used with almost any means of transmitting analog signals from light-emitting diodes to radio. A common type of modem is one that turns the digital data of a computer into modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.**
  - **Modems are generally classified by the maximum amount of data they can send in a given unit of time, usually expressed in bits per second (symbol bit(s), sometimes abbreviated "bps") or rarely in bytes per second (symbol B(s)). Modems can also be classified by their symbol rate, measured in baud. The baud unit denotes symbols per second, or the number of times per second the modem sends a new signal.**

Networks Devices (cont.)

- **Repeater**

  - a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. Some types of repeaters broadcast an identical signal, but alter its method of transmission, for example, on another frequency or **baud rate.**
  - The **baud rate** is the rate at which information is transferred in a communication channel. ... In the serial port context, "9600 baud" means that the serial port is capable of transferring a maximum of 9600 bits per second.

Networks Devices (cont.)

- **Hub**

  - **A hub, also called a network hub, is a common connection point for devices in a network. Hubs are devices commonly used to connect segments of a LAN. The hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.**

Networks Devices (cont.)

- **Switch**

- A network switch (also called switching hub, bridging hub, officially MAC bridge)is networking hardware that connects devices on a computer network by using packet switching to receive, and forward data to the destination device.
- A network switch is a multiport network bridge that uses media access control addresses to forward data at the data link layer (layer 2) of the OSI model. Some switches can also forward data at the network layer (layer 3) by additionally incorporating routing functionality. Such switches are commonly known as layer-3 switches or multilayer switches.
- Switches for Ethernet are the most common form of network switch.
- a network switch forwards data only to the devices that need to receive it.

Networks Devices (cont.)

- **Bridge**

  - **A bridge is a type of computer network device that provides interconnection with other bridge networks that use the same protocol.**
  - **Bridge devices work at the data link layer of the Open System Interconnect (OSI) model, connecting two different networks together and providing communication between them. Bridges are similar to repeaters and hubs in that they broadcast data to every node. However, bridges maintain the media access control (MAC) address table as soon as they discover new segments, so subsequent transmissions are sent to only to the desired recipient.**
  - **Bridges are also known as Layer 2 switches**

Networks Devices (cont.)

• Router

- Router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. Data sent through the internet, such as a web page or email, is in the form of data packets. A packet is typically forwarded from one router to another router through the networks that constitute an internetwork (e.g. the Internet) until it reaches its destination node.
- A router is connected to two or more data lines from different IP networks. When a data packet comes in on one of the lines, the router reads the network address information in the packet header to determine the ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey.
- The most familiar type of IP routers are home and small office routers that simply forward IP packets between the home computers and the Internet.

Networks Devices (cont.)

- **Gateway**

  - **A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another. Gateways are distinct from routers or switches in that they communicate using more than one protocol, and can operate at any of the seven layers of the open systems interconnection model (OSI).**
  - **The term gateway can also refer to a computer or computer program configured to perform the tasks of a gateway, such as a default gateway or router.**

Networks Software

- **Protocols**
  - a set of rules and regulations that determine how data is transmitted in telecommunications and computer networking.
  - Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices -- from servers and routers to endpoints -- can communicate regardless of the differences in their underlying infrastructures, designs or standards.
  - To successfully send and receive information, devices on both sides of a communication exchange must accept and follow protocol conventions. Support for network protocols can be built into software, hardware or both.
  - Standardized network protocols provide a common language for network devices. Without them, computers wouldn't know how to engage with each other. As a result, except for specialty networks built around a specific architecture, Virtually all network end users rely on network protocols for connectivity.

Networks Software (cont.)

- **OSI Model VS TCP/IP Model**

1/ Physical Layer_(H/W)

2/ Datalink Layer_()

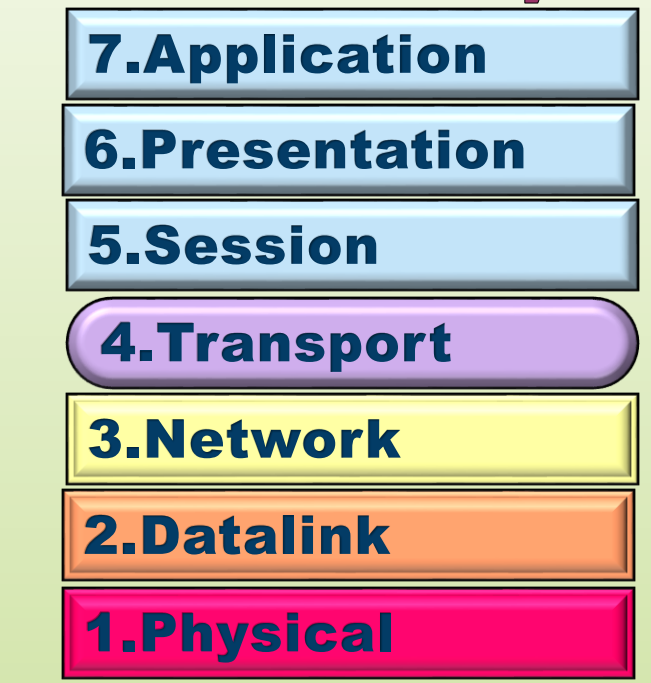
3/ Network Layer_(addressing & routing)

4/ Transport Layer_(intermediate)

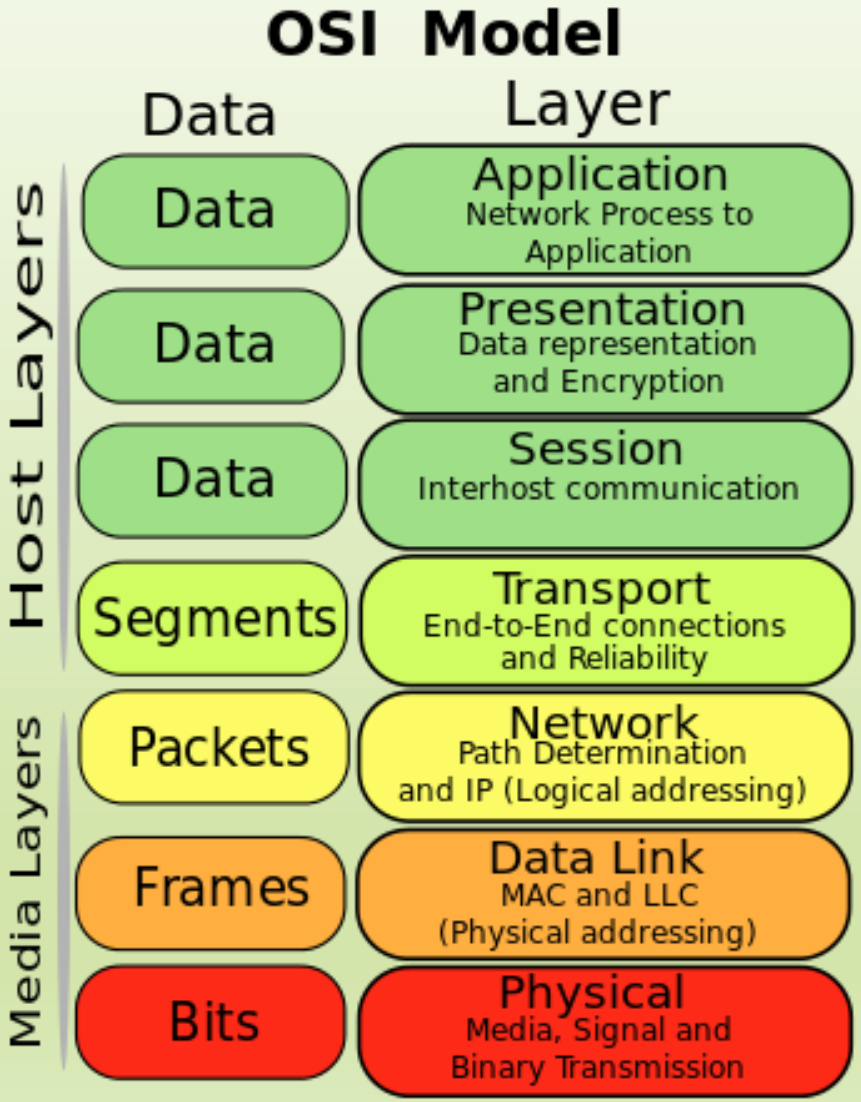
5/ Session Layer_()

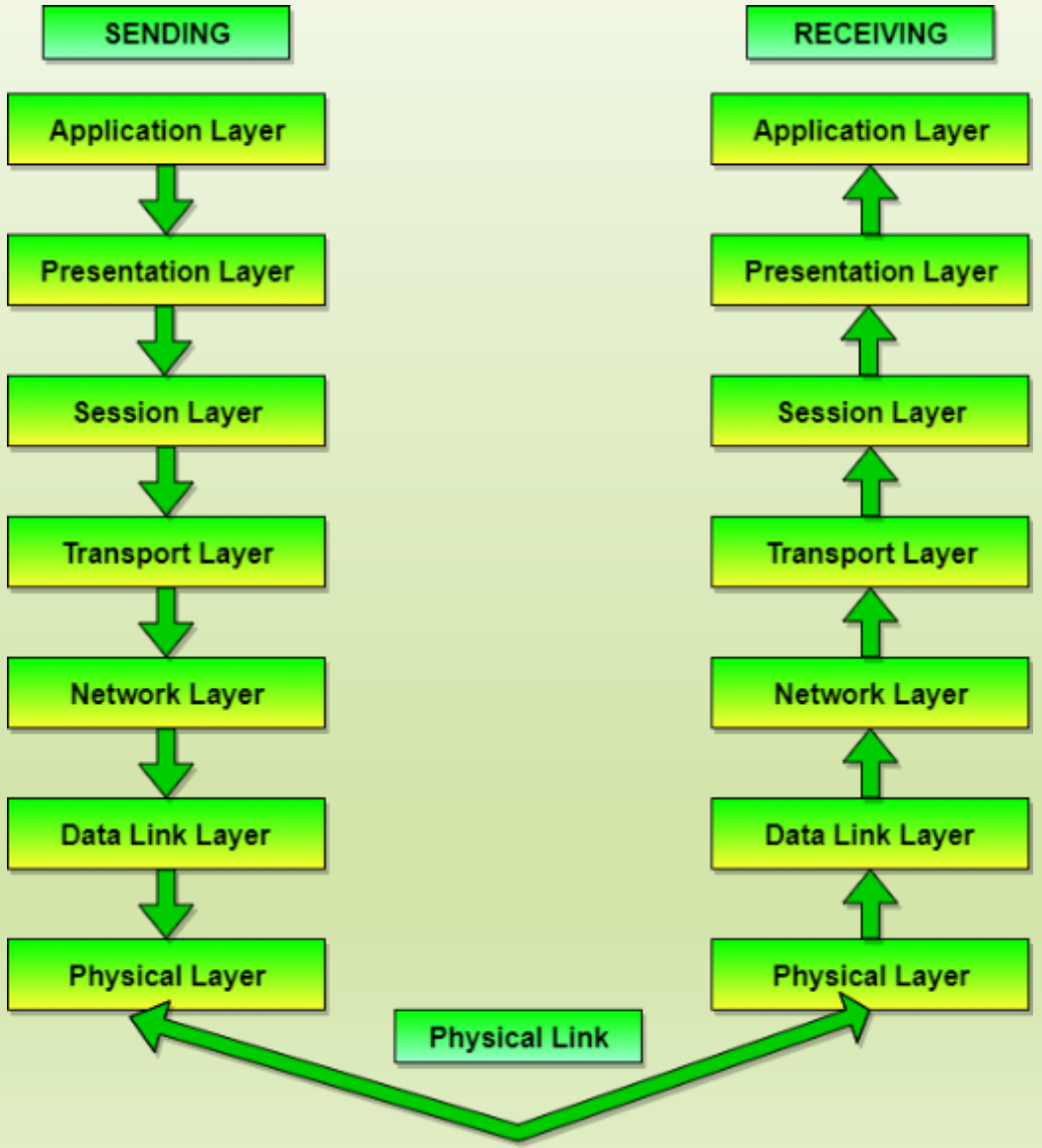
6/ Presentation Layer_(syntax)

7/Application Layer_(a-file transfer & management , b-E-mail)



Networks Software (cont.)





Networks Software (cont.)

- **OSI Model Layers**

7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

Networks Software (cont.)

- **OSI Model Layers**

5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into "segments" on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

Networks Software (cont.)

- **OSI Model Layers**

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

Networks Software (cont.)

- **TCP**
  - **It was known as the DoD model based on the Department of Defense which helped in its development**
  - **Transmission Control Protocol is a connection-oriented protocol, which means that it requires handshaking to set up end-to-end communications. Once a connection is set up, user data may be sent bi-directionally over the connection.**
  - **Reliable – Strictly only at transport layer, TCP manages message acknowledgment, retransmission and timeout. Multiple attempts to deliver the message are made. If it gets lost along the way, the server will re-request the lost part. In TCP, there's either no missing data, or, in case of multiple timeouts, the connection is dropped. (This reliability however does not cover application layer, at which a separate acknowledgement flow control is still necessary) .**

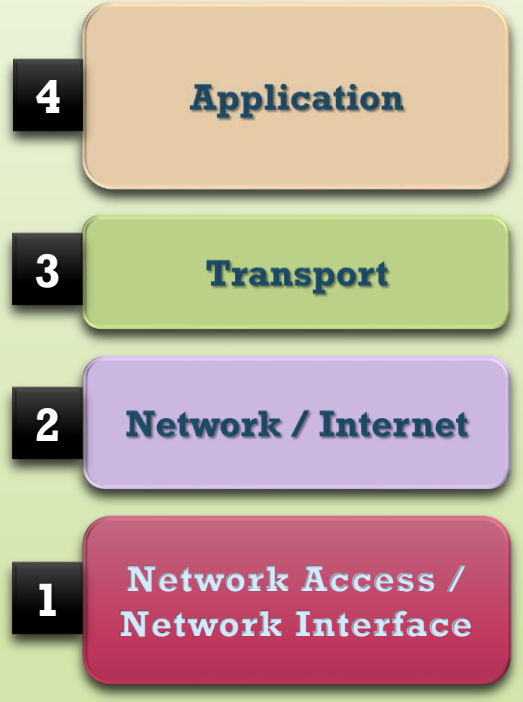
Networks Software (cont.)

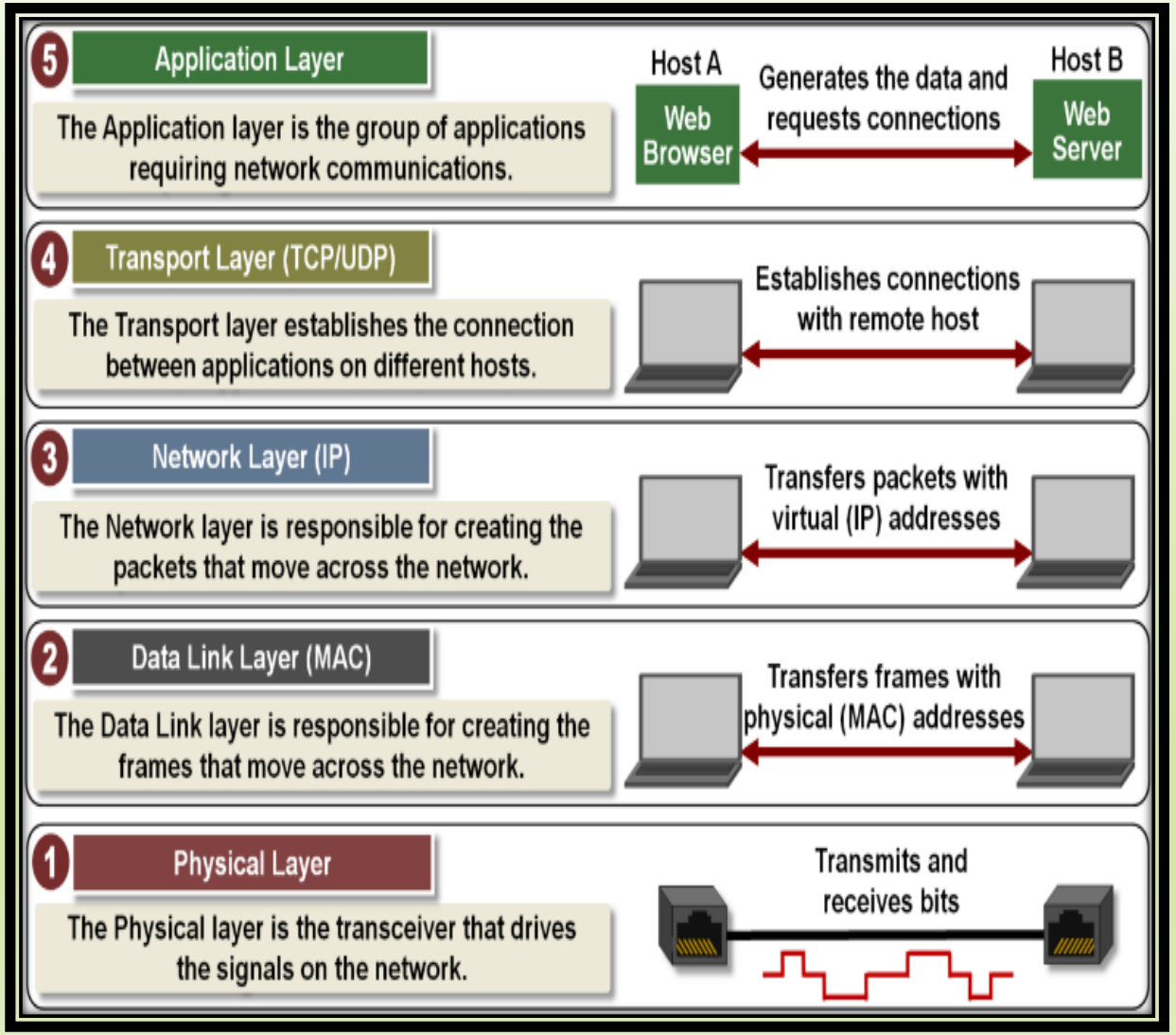
- **TCP**

  - **Ordered – If two messages are sent over a connection in sequence, the first message will reach the receiving application first. When data segments arrive in the wrong order, TCP buffers delay the out-of-order data until all data can be properly re-ordered and delivered to the application.**
  - **Heavyweight – TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.**
  - **Streaming – Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.**

Networks Software (cont.)

- **TCP**





Networks Software (cont.)

• TCP Layers

Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.
Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model. Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are:

•Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
•It allows users to log on to a remote host
•This layer provides various e-mail services
•This application offers distributed database sources and access for global information about various objects and services.

Networks Software (cont.)

Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Networks Software (cont.)

Internet Layer

An internet layer is a second layer of TCP/IP layers of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take. The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks. Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. Routing protocols
2. Multicast group management
3. Network-layer address assignment.

Networks Software (cont.)

The Network Interface Layer

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network.

It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables.

A network layer is a combination of the data line and defined in the article of OSI reference model. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Networks Software (cont.)

- **UDP**

- **User Datagram Protocol is a simpler message-based connectionless protocol. Connectionless protocols do not set up a dedicated end-to-end connection. Communication is achieved by transmitting information in one direction from source to destination without verifying the readiness or state of the receiver.**
- **Unreliable – When a UDP message is sent, it cannot be known if it will reach its destination; it could get lost along the way. There is no concept of acknowledgment, retransmission, or timeout.**
- **Not ordered – If two messages are sent to the same recipient, the order in which they arrive cannot be predicted.**

Networks Software (cont.)

- **UDP**

  - **Lightweight – There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.**
  - **Datagrams – Packets are sent individually and are checked for integrity only if they arrive. Packets have definite boundaries which are honored upon receipt, meaning a read operation at the receiver socket will yield an entire message as it was originally sent.**
  - **No congestion control – UDP itself does not avoid congestion. Congestion control measures must be implemented at the application level.**
  - **Broadcasts – being connectionless, UDP can broadcast - sent packets can be addressed to be receivable by all devices on the subnet.**
  - **Multicast – a multicast mode of operation is supported whereby a single datagram packet can be automatically routed without duplication to very large numbers of subscribers.**

OSI Model vs TCP/IP Model

OSI model				
Layer			Protocol data unit(PDU)	Function
Host layers	7	Application	Data	High-level APIs, including resource sharing, remote file access
	6	Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption
	5	Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes
	4	Transport	Segment, Datagram	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing
Media layers	3	Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control
	2	Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer
	1	Physical	Symbol	Transmission and reception of raw bit streams over a physical medium

IANA

- **The Internet Assigned Numbers Authority (IANA) a nonprofit private American corporation that oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol-related symbols and Internet numbers.**

iana

Internet Assigned Numbers Authority

Internet Protocol - IP

- An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.
- IPv4 was the first version deployed for production in the ARPANET in 1983
- Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number. However, because of the growth of the Internet and the depletion of available IPv4 addresses.
- An IPv4 address has a size of 32 bits, which limits the address space to 4.294.967.296 (2^{32}) addresses. Of this number, some addresses are reserved for special purposes such as private networks (~18 million addresses) and multicast addressing (~270 million addresses).
- IPv4 addresses are usually represented in dot-decimal notation.

Internet Protocol IP (cont.)

- a new version of IP (IPv6), using 128 bits for the IP address, was standardized in 1998.IPv6 deployment has been ongoing since the mid-2000s.
- In IPv6, the address size was increased from 32 bits in IPv4 to 128 bits, thus providing up to 2^{128} (approximately 3.4×10^{38}) addresses. This is deemed sufficient for the foreseeable future.
- IPv6 addresses are 128 bits in length and written as a string of hexadecimal digits. Every 4 bits can be represented by a single hexadecimal digit, for a total of 32 hexadecimal values (0_{16} [0000_2] through f_{16} [1111_2]).

Internet Protocol IP (cont.)

- **IPv4**

Reserved IPv4 Address Ranges

Type of Address	Usage	Reserved IPv4 Address Range	RFC
Host Address	used for IPv4 hosts	0.0.0.0 to 223.255.255.255	790
Multicast Addresses	used for multicast groups on a local network	224.0.0.0 to 239.255.255.255	1700
Experimental Addresses	• used for research or experimentation • cannot currently be used for hosts in IPv4 networks	240.0.0.0 to 255.255.255.254	1700 3330

IP Classes

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

All Zeros (0) and all Ones (1) are Invalid Hosts addresses

Internet Protocol IP (cont.)

IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.In December 1998, IPv6 became a Draft Standard for the IETF, who subsequently ratified it as an Internet Standard on 14 July 2017.

Pv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit the expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for the delivery of services. Device mobility, security, and configuration aspects have been considered in the design of the protocol.

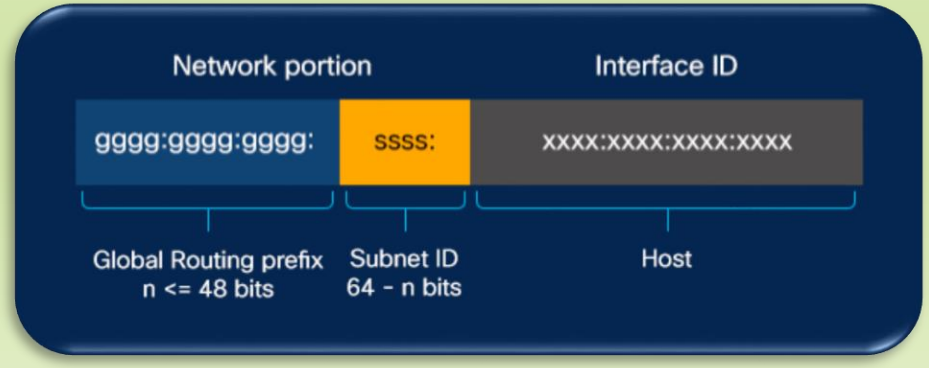
IPv6 addresses are represented as eight groups of four hexadecimal digits each, separated by colons.

Internet Protocol IP (cont.)

IPv6 addressing structure

IPv6 uses hexadecimal digits (hex digit) for addressing with each hex digit representing 4 bits.
IPv6 addressing can reduce routing table size by allowing ISPs to aggregate customers' prefixes into a single prefix and present only that one prefix out to the IPv6 internet.
Many networks will implement IPv6 concurrently with IPv4 in a dual-stack design, while newer networks will deploy IPv6 natively but still allow for compatibility with IPv4 if needed. This addresses current government mandates for IPv6 use.

- **An IPv6 address is eight groupings of numbers:**
- **Network address - the first three groupings of numbers (first 48 bits) in the subnet mask**
- **Subnet address - the fourth grouping of numbers (the 49th through 64th bits) in the subnet mask**
- **Device address - the last four groupings of numbers (the last 64 bits) in the subnet mask**



The full representation may be shortened; for example :

2001:0db8:0000:0000:0000:8a2e:0370:7334 becomes 2001:db8::8a2e:370:7334.

Internet Protocol IP (cont.)

Expanded notation of IPv6 address at start of the range	IPv6 address (condensed notation)	IPv6 address with prefix length	Device range in subnetwork
2001:0DB8:ABCD:0012:0000:0000:0000:0000	2001:DB8:ABCD:12::	2001:db8:abcd:0012::0/64	2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF
2001:0DB8:ABCD:0012:0000:0000:0000:0000	2001:DB8:ABCD:12::	2001:db8:abcd:0012::0/80	2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:0000:FFFF:FFFF:FFFF
2001:0DB8:ABCD:0012:0000:0000:0000:0000	2001:DB8:ABCD:12::	2001:db8:abcd:0012::0/96	2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:0000:0000:FFFF:FFFF
2001:0DB8:ABCD:0012:0000:0000:0000:0000	2001:DB8:ABCD:12::	2001:db8:abcd:0012::0/112	2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:0000:0000:0000:FFFF
2001:0DB8:ABCD:0012:0000:0000:0000:0000	2001:DB8:ABCD:12::	2001:db8:abcd:0012::0/128	2001:0DB8:ABCD:0012:0000:0000:0000:0000 - 2001:0DB8:ABCD:0012:0000:0000:0000:0000

Table 1. Network ranges for prefix lengths of IPv6 addresses

Private IP

- Home routers have their local address set to a default, private IP address number. It's usually the same address for the other models from that manufacturer, and it can be seen in the manufacturer's documentation. Here's a look at the default private (also called "local") IP addresses for popular brands of routers:
- Linksys routers use 192.168.1.1
- D-Link , EuGenius, NETGEAR and TP-Link routers are set to 192.168.0.1
- Cisco routers use either 192.168.10.2, 192.168.1.254 or 192.168.1.1
- Belkin and SMC routers often use 192.168.2.1
- In theory, your computer must have its own unique IP address so that it will only receive the information that is meant for you.
- However, that's not how it works out, because of one major exception—network computers that are linked to a router and share the same public IP address.

Private IP (cont.)

- The organizations that distribute IP addresses to the world reserves a range of IP addresses for private networks.

  10.0.0.0/8 IP addresses: 10.0.0.0 – 10.255.255.255

  172.16.0.0/12 IP addresses: 172.16.0.0 – 172.31.255.255

  192.168.0.0/16 IP addresses: 192.168.0.0 – 192.168.255.255

- Your simple home network, with its router at the center and computers connected to it—wired or wireless—classifies as one of those networks.
- Your router—once it makes its Internet connection through your Internet Service Provider—sends Internet activity to any computer connected to your router, and is the basis of a networking innovation called a **N**etwork **A**ddress **T**ranslation (**NAT**).
- **NAT** is a process in which your router changes your private IP Address into a public one so that it can send your traffic over the Internet, keeping track of the changes in the process.
- When the information comes back to your router, it reverses the change—from a real IP address into a private one—and forwards the traffic back to your computer.

Subnet mask

Subnetting allows for creating multiple logical networks from a single address block. Since we use a router to connect these networks together, each interface on a router must have a unique network ID. Every node on that link is on the same network.

We create the subnets by using one or more of the host bits as network bits. This is done by extending the mask to borrow some of the bits from the host portion of the address to create additional network bits. The more host bits used, the more subnets that can be defined. For each bit borrowed we double the number of subnetworks available. For example, if we borrow 1 bit, we can define 2 subnets. If we borrow 2 bits, we can have 4 subnets. However, with each bit we borrow, fewer host addresses are available per subnet.

To define the network and host portions of an address the devi6es use a separate 32-bit pattern called a subnet mask.

We express the subnet mask in the same dotted decimal format as the IPv4 address.

The subnet mask is created by placing a binary 1 in each bit position that represents the network portion and placing a binary 0 in each bit position that represents the host portion.

The prefix and the subnet mask are different ways of representing the same thing - the network portion of an address.

Subnet mask (cont.)

For Example a/24 prefix is expressed as a subnet mask as 255 . 255 . 255 . 0
(11111111.11111111.11111111.00000000)
The remaining bits (low order) of the subnet mask are zeroes) indicating the host address within the network.
The subnet mask is configured on a host in conjunction with the IPv4 address to define the network portion of that address.

For example let's look at the host 172.16.4.35/27:
address
172 . 16 . 20 . 35
10101100.00010000.00010100.00100011
subnet mask
255 . 255 . 255 . 224
11111111.11111111.11111111.11100000
network address
172 . 16 . 20 . 32
10101100.00010000.00010100.00100000

Subnet mask (cont.)

Prefix size	Network mask	Usable hosts per subnet
/1	128.0.0.0	2,147,483,646
/2	192.0.0.0	1,073,741,822
/3	224.0.0.0	536,870,910
/4	240.0.0.0	268,435,454
/5	248.0.0.0	134,217,726
/6	252.0.0.0	67,108,862
/7	254.0.0.0	33,554,430

Subnet mask (cont.)

Class A		
/8	255.0.0.0	16,777,214
/9	255.128.0.0	8,388,606
/10	255.192.0.0	4,194,302
/11	255.224.0.0	2,097,150
/12	255.240.0.0	1,048,574
/13	255.248.0.0	524,286
/14	255.252.0.0	262,142
/15	255.254.0.0	131,070

Subnet mask (cont.)

Class B		
/16	255.255.0.0	65,534
/17	255.255.128.0	32,766
/18	255.255.192.0	16,382
/19	255.255.224.0	8,190
/20	255.255.240.0	4,094
/21	255.255.248.0	2,046
/22	255.255.252.0	1,022
/23	255.255.254.0	510

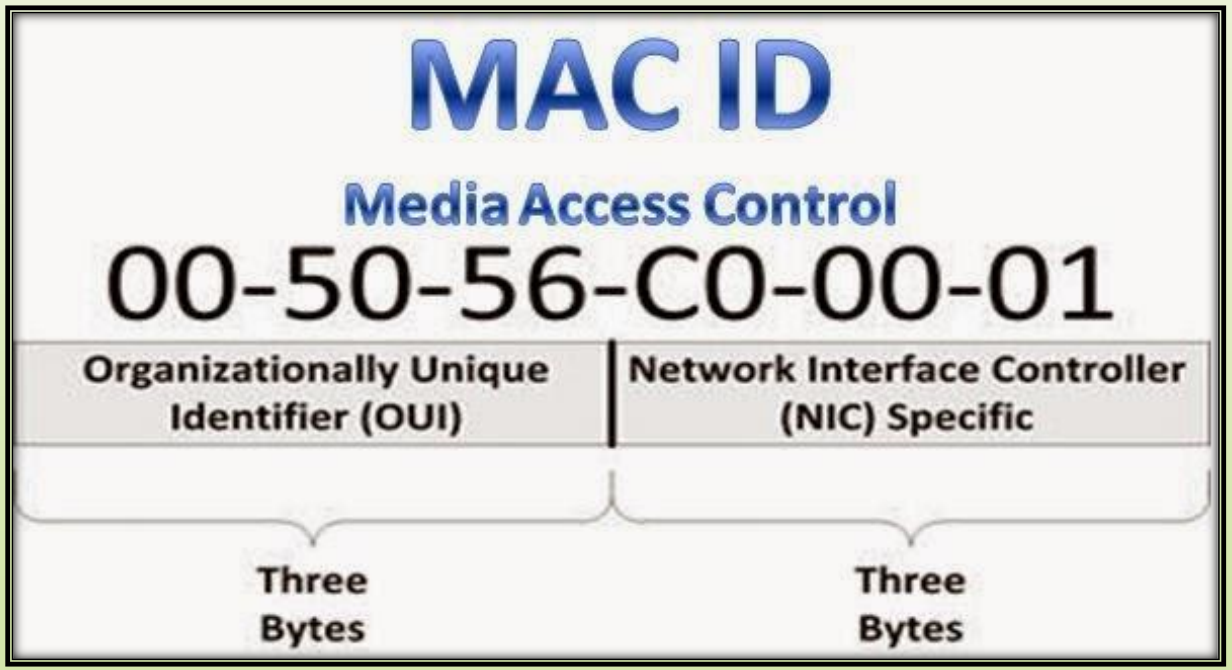
Subnet mask (cont.)

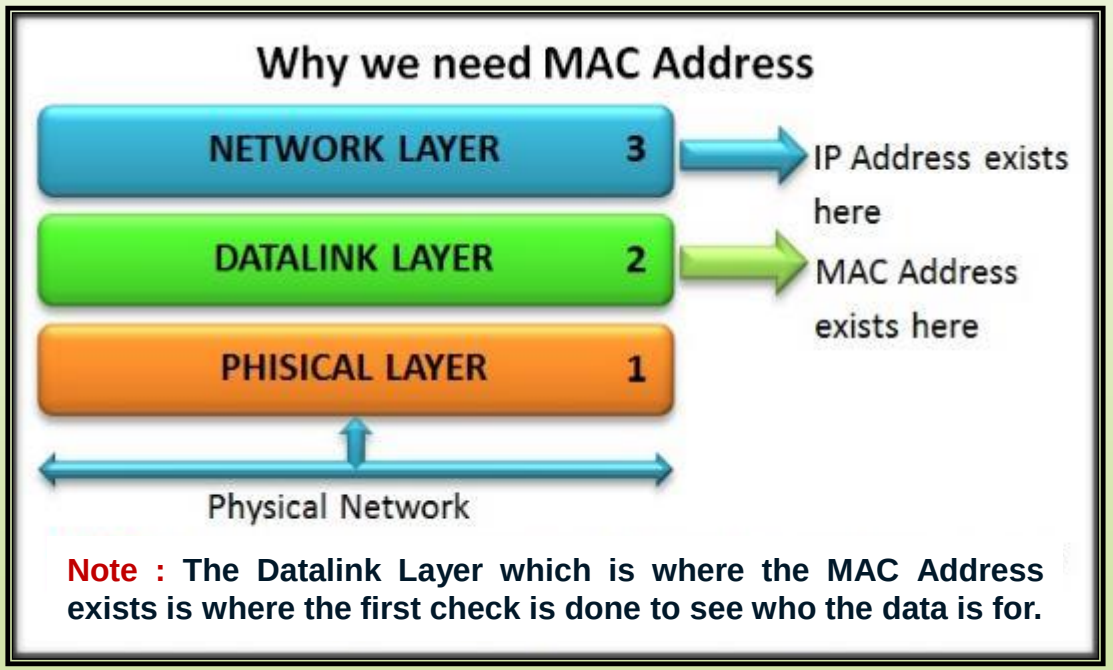
Class C		
/24	255.255.255.0	254
/25	255.255.255.128	126
/26	255.255.255.192	62
/27	255.255.255.224	30
/28	255.255.255.240	14
/29	255.255.255.248	6
/30	255.255.255.252	2
/31	255.255.255.254	0
/32	255.255.255.255	0

MAC Address

- A Media Access Control address (MAC address) of a device is a unique identifier assigned to a network interface controller (NIC). For communications within a network segment, it is used as a network address for most IEEE 802 network technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or no separator .

MAC Address (cont.)





Note : **The Datalink Layer which is where the MAC Address exists is where the first check is done to see who the data is for.**

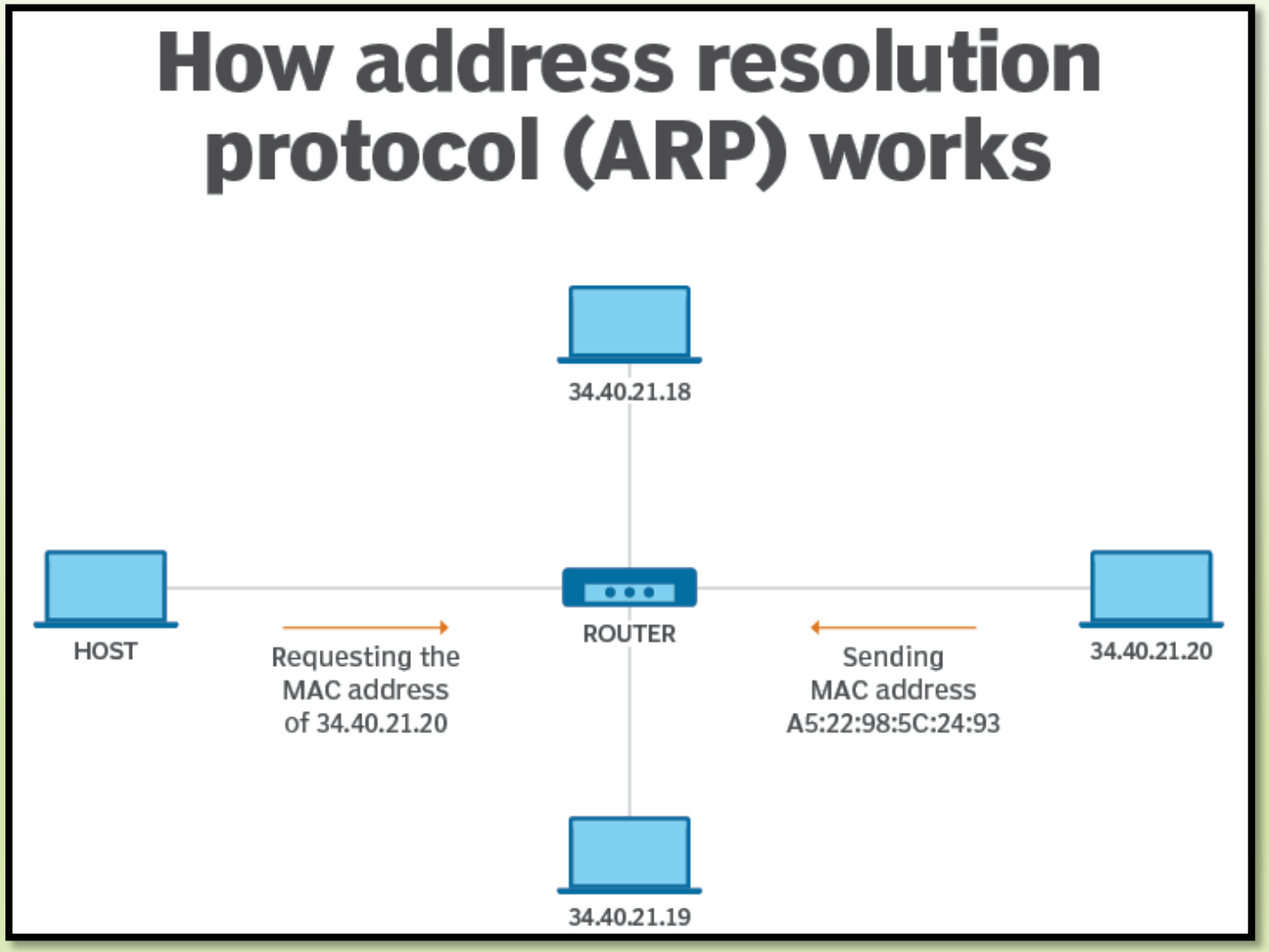
MAC Address (cont.)

- A MAC address may be referred to as the burned-in address, and is also known as an Ethernet hardware address, hardware address, and physical address .
- A network node with multiple NICs must have a unique MAC address for each. Sophisticated network equipment such as a multilayer switch or router may require one or more permanently assigned MAC addresses.
- MAC addresses are most often assigned by the manufacturer of network interface cards. Each is stored in hardware, such as the card's read-only memory or by a firmware mechanism. A MAC address typically includes the manufacturer's organizationally unique identifier (OUI). MAC addresses are formed according to the principles of two numbering spaces based on Extended Unique Identifiers (EUI) managed by the Institute of Electrical and Electronics Engineers (IEEE): EUI-48, which replaces the obsolete term MAC-48, and EUI-64.

Networks Protocols

- **Address Resolution Protocol (ARP)**
  - **The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address. This mapping is a critical function in the Internet protocol suite. ARP was defined in 1982 which is Internet Standard STD 37.**
  - **ARP has been implemented with many combinations of network and data link layer technologies, such as IPv4, Chaos net, DEC net and Xerox PARC Universal Packet (PUP) using IEEE 802 standards, FDDI, X.25, Frame Relay and Asynchronous Transfer Mode (ATM). IPv4 over IEEE 802.3 and IEEE 802.11 is the most common usage.**
  - **In Internet Protocol Version 6 (IPv6) networks, the functionality of ARP is provided by the Neighbor Discovery Protocol (NDP).**

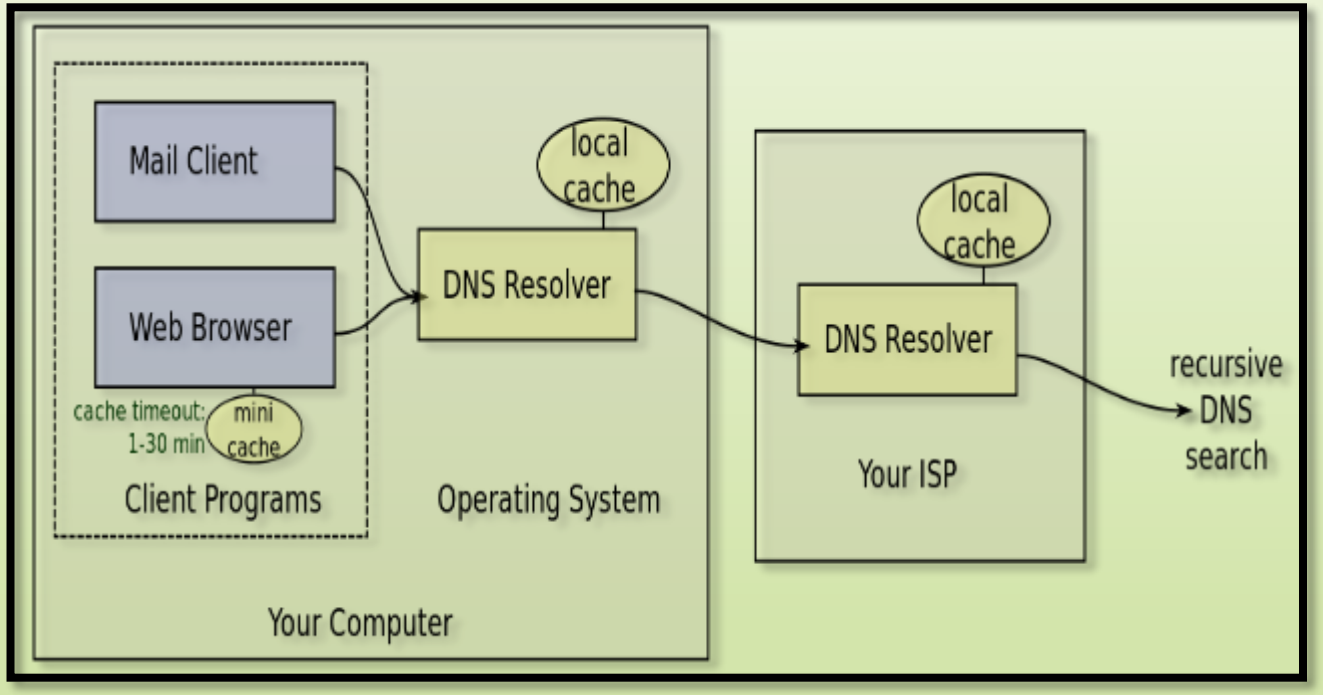
Networks Protocols (cont.)

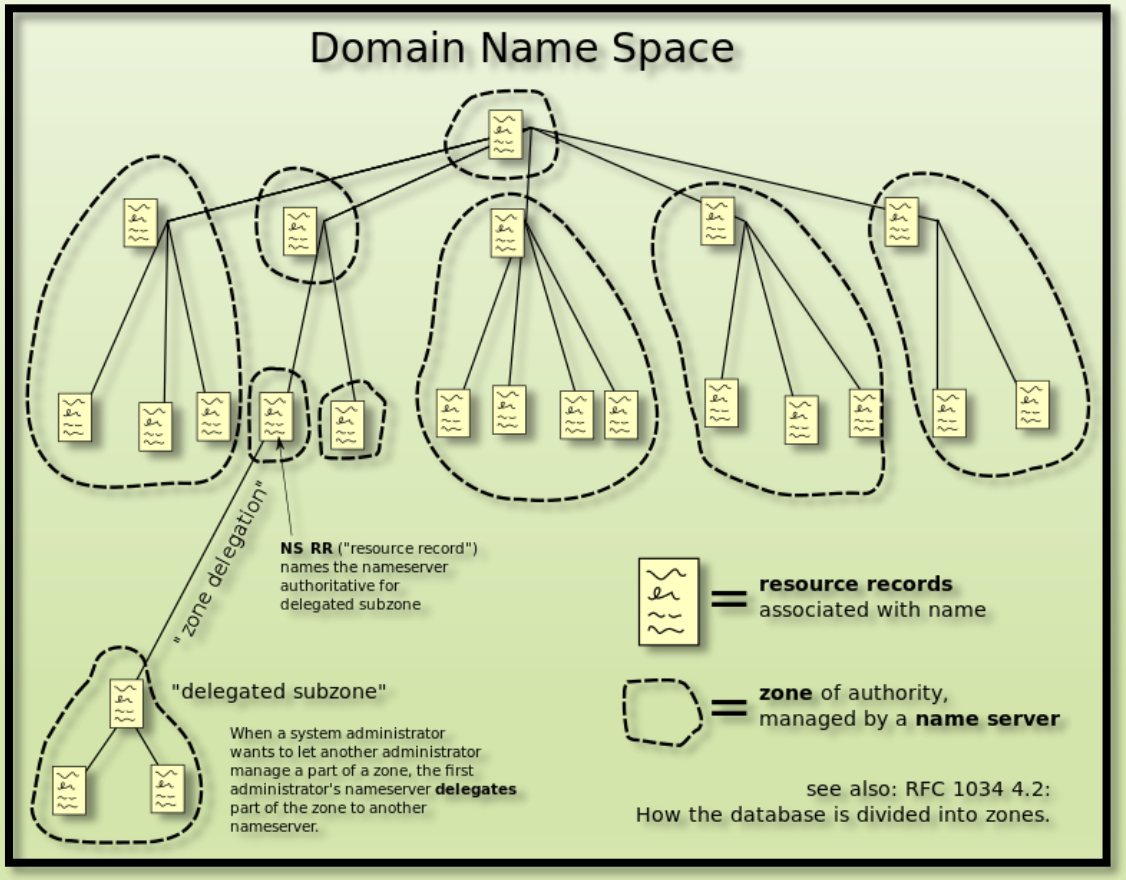


Networks Protocols (cont.)

- **DNS Server**
  - **The Domain Name System (DNS) is the phonebook of the Internet. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources. Humans access information online through domain names, like nytimes.com or espn.com.**
  - **Each device connected to the Internet has a unique IP address which other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as 192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2400:cb00:2048:1::c629:d7a2 (in IPv6).**

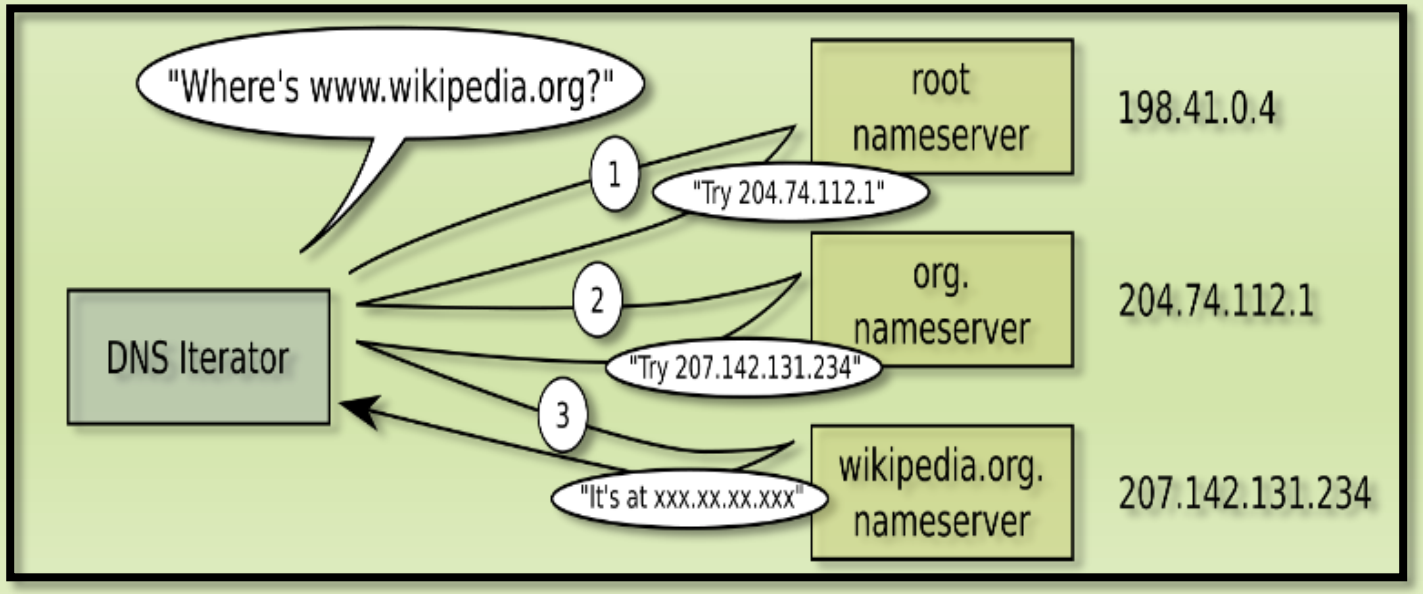
Networks Protocols (cont.)





Networks Protocols (cont.)

- The process of DNS resolution involves converting a hostname (such as www.example.com) into a computer-friendly IP address (such as 192.168.1.1). An IP address is given to each device on the Internet, and that address is necessary to find the appropriate Internet device - like a street address is used to find a particular home. When a user wants to load a webpage, a translation must occur between what a user types into their web browser (example.com) and the machine-friendly address necessary to locate the example.com webpage.



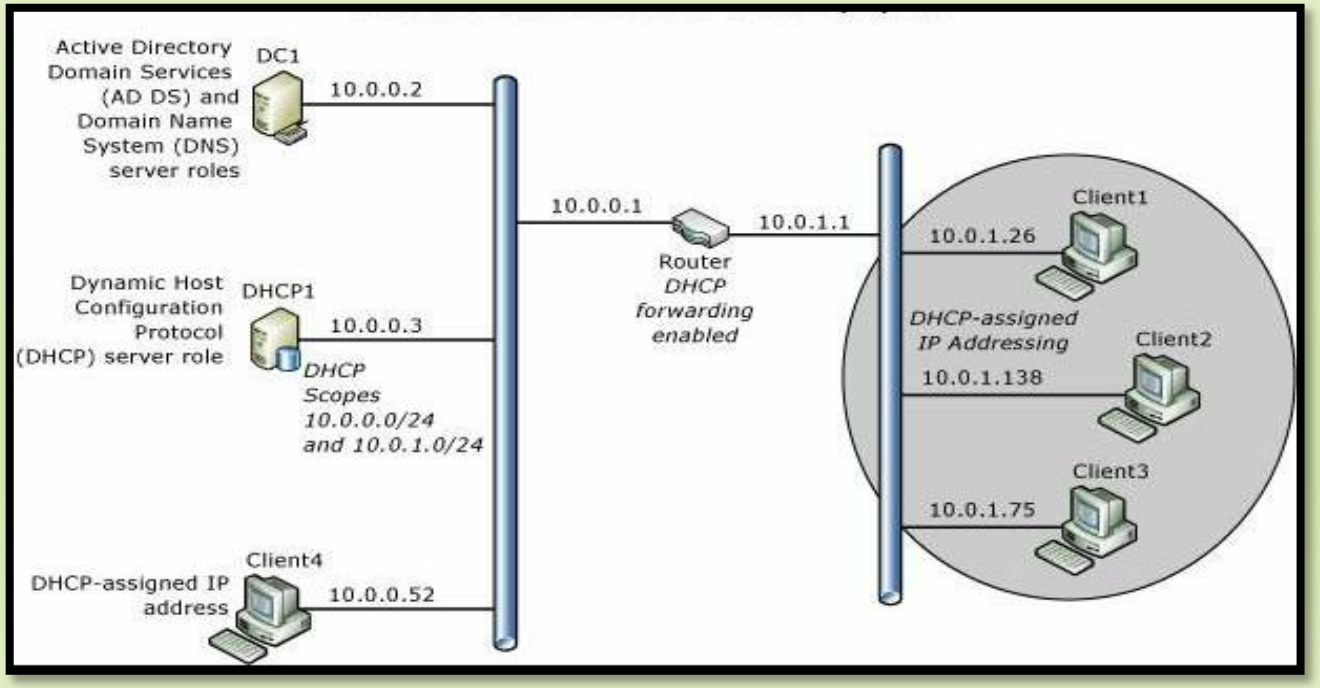
Networks Protocols (cont.)

- **DHCP Server**

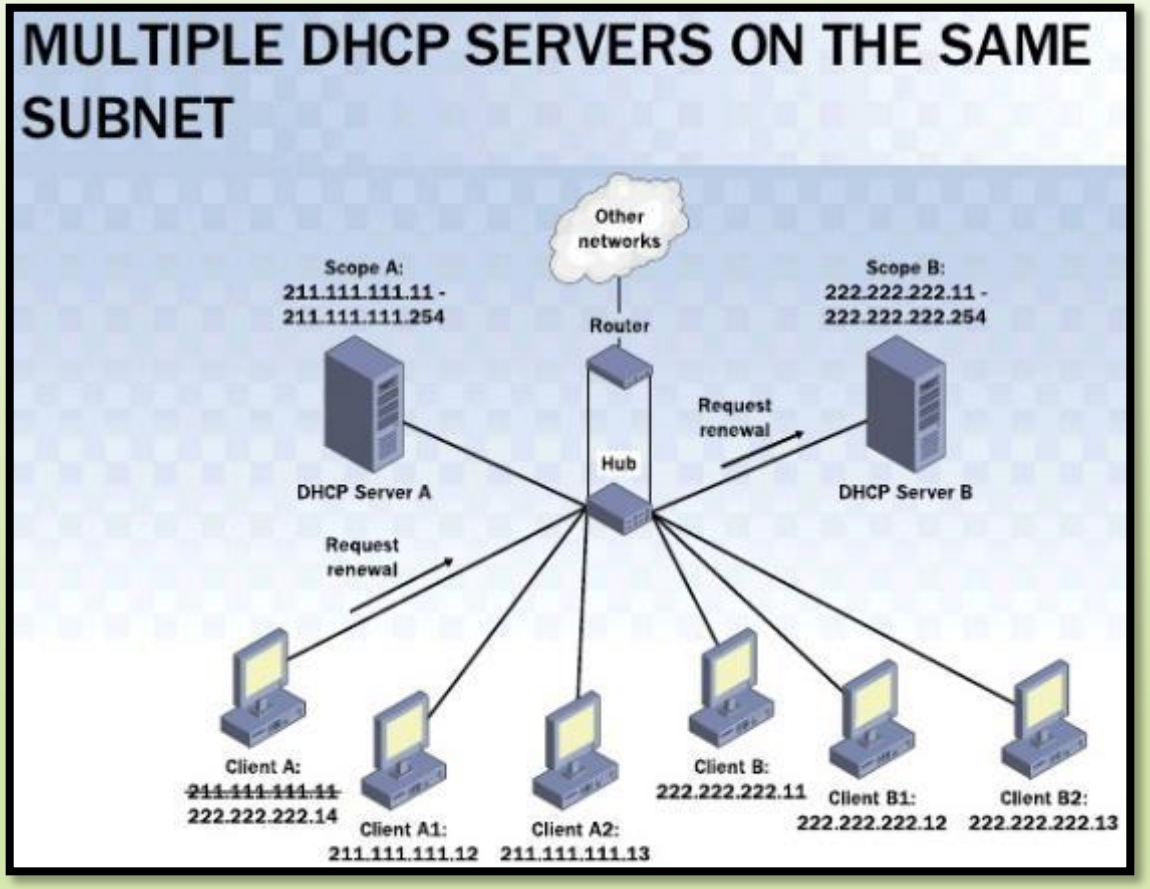
- **The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically from the Internet service provider (ISP), reducing the need for a network administrator or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address, or to assign itself an APIPA address, which will not enable it to communicate outside its local subnet.**

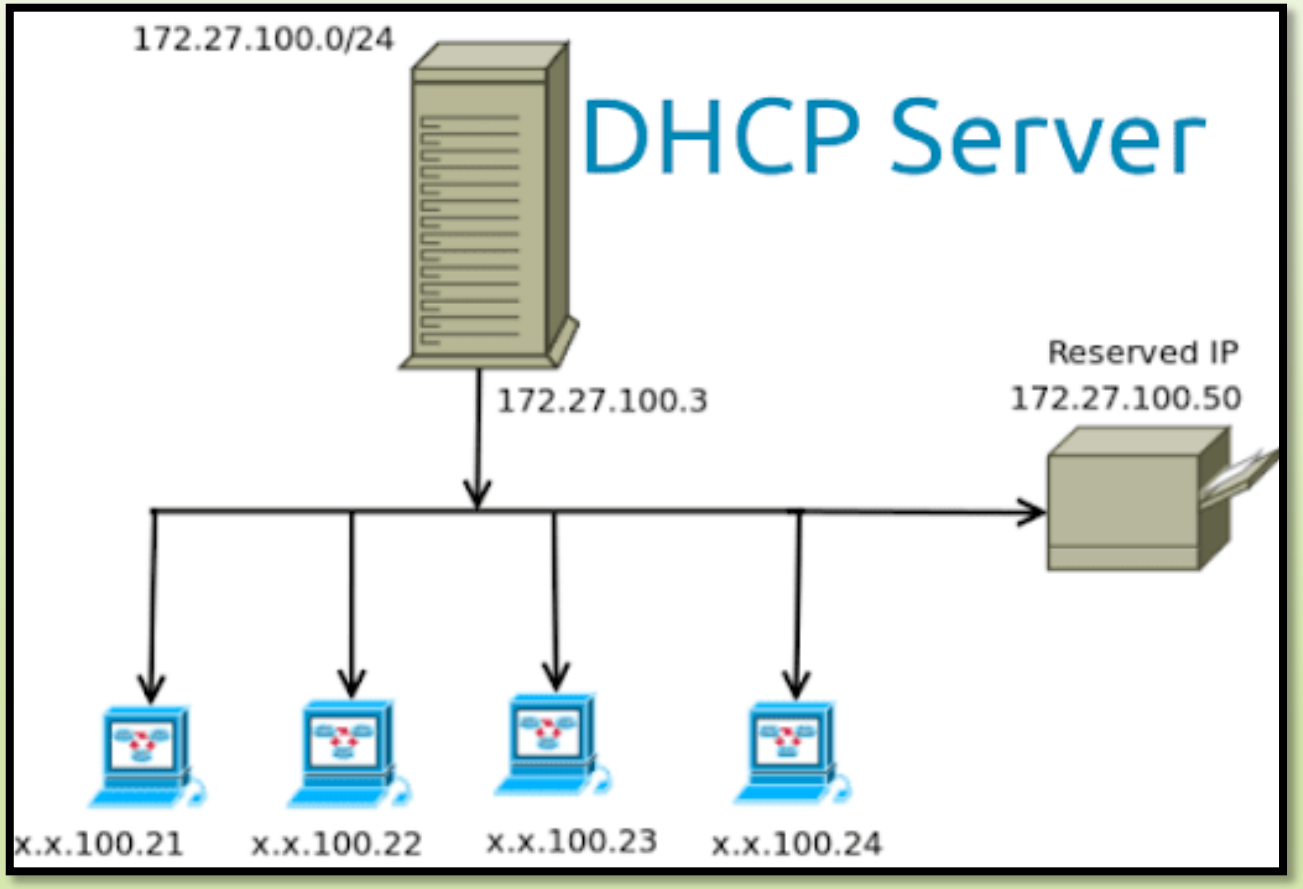
Networks Protocols (cont.)

- **DHCP can be implemented on networks ranging in size from home networks to large campus networks and regional Internet service provider networks. A router or a residential gateway can be enabled to act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.**



Networks Protocols (cont.)

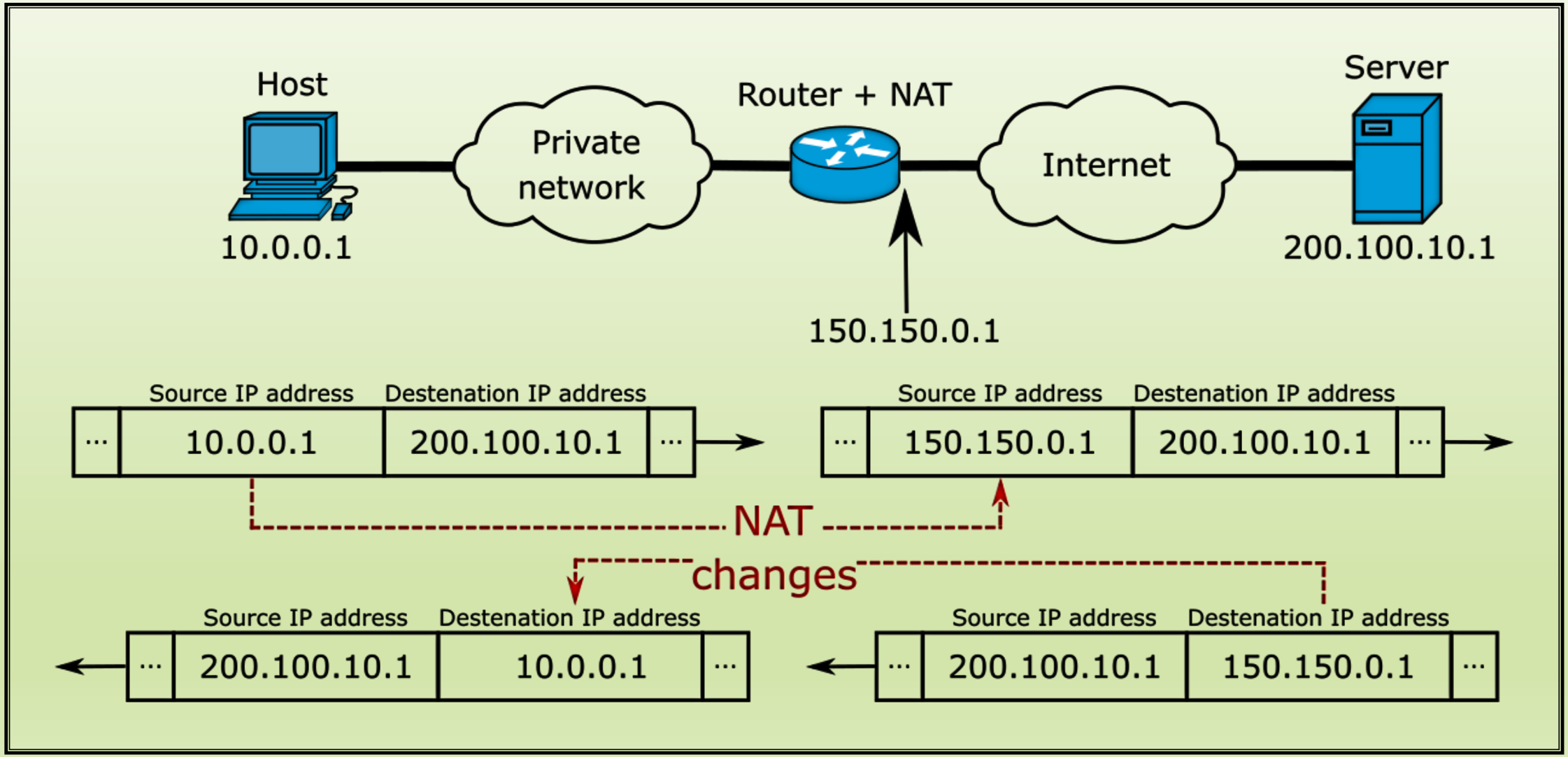




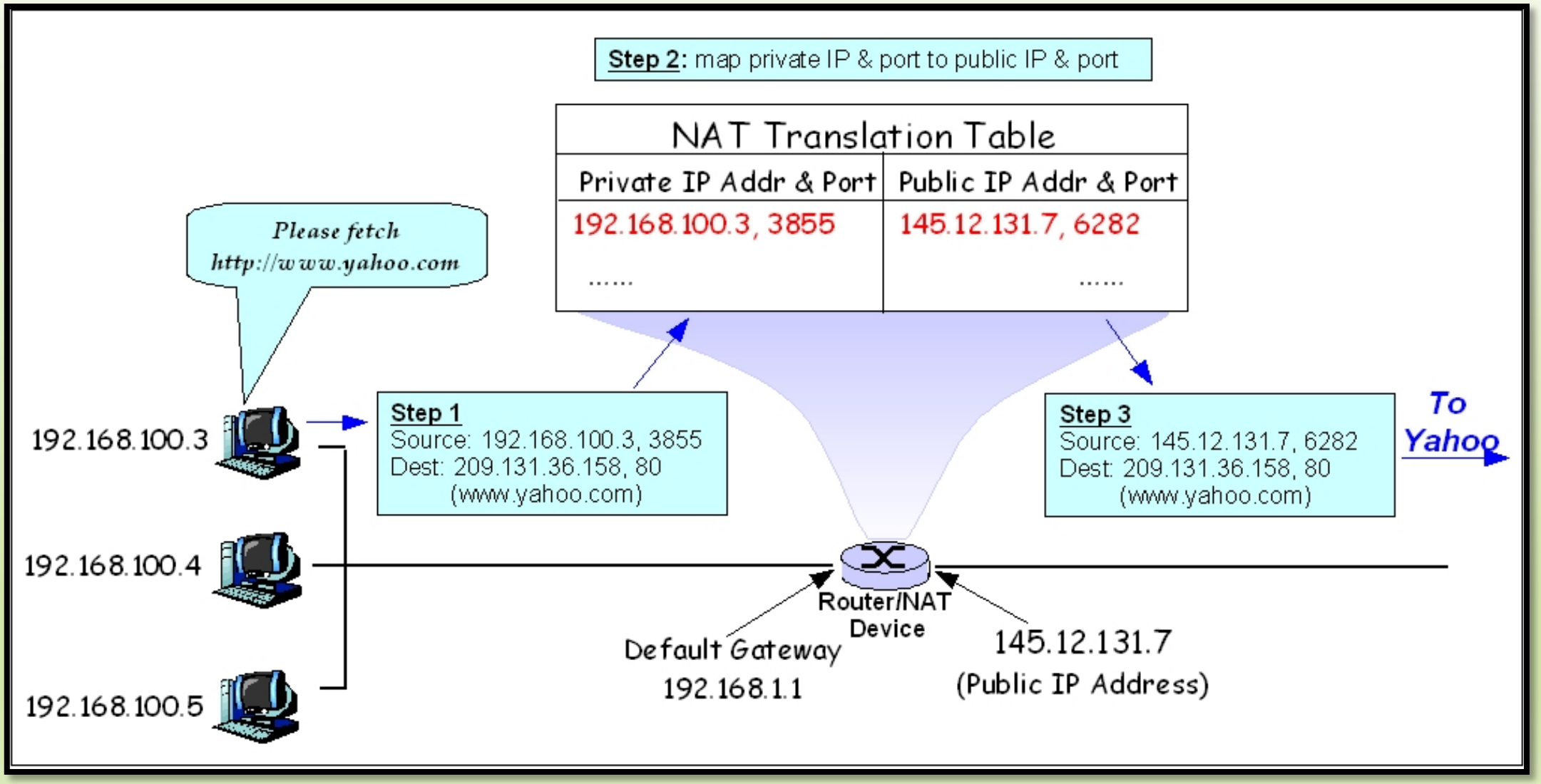
Networks Protocols (cont.)

- **NAT**
  - **Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.**
  - **The most common form of network translation involves a large private network using addresses in a private range (10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, or 192.168.0 0 to 192.168.255.255). The private addressing scheme works well for computers that only have to access resources inside the network. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, like the Internet, these computers have to have a public address in order for responses to their requests to return to them.**

Networks Protocols (cont.)



Networks Protocols (cont.)



Virtual Private Network (VPN)

- **A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common though not an inherent part of a VPN connection.**
- **VPN technology was developed to allow remote users and branch offices to access corporate applications and resources.**
- **A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols over existing networks.**

VPN Protocols

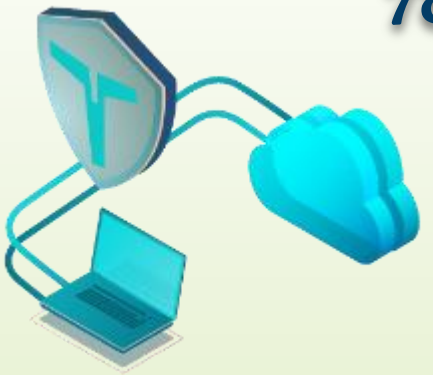
1. OpenVPN

OpenVPN is an open source VPN protocol. This means users can scrutinize its source code for vulnerabilities, or use it in other projects. OpenVPN has become one of the most important VPN protocols.

2. L2TP/IPSec

Layer 2 Tunnel Protocol is a very popular VPN protocol. L2TP is the successor to the depreciated PPTP (for more details, see the PPTP section below), developed by Microsoft, and L2F, developed by Cisco. However, L2TP doesn't actually provide any encryption or privacy itself.

VPN Protocols (cont.)



3. SSTP

Secure Socket Tunneling Protocol is another popular VPN protocol. SSTP comes with one notable benefit: it has been fully integrated with every Microsoft operating system since Windows Vista Service Pack 1

4. IKEv2

internet Key Exchange version 2 is another VPN protocol developed by Microsoft and Cisco. IKEv2 on its own is just a tunneling protocol, providing a secure key exchange session, therefore (and like its predecessor), IKEv2 is frequently paired with IPSec for encryption and authentication.

VPN Protocols (cont.)

5. PPTP

Point-to-Point Tunneling Protocol is one of the oldest VPN protocols. It is still in use in some places, but the majority of services have long upgraded to faster and more secure protocols.

6. SoftEther

Compared to most VPN encryption protocols (except Wireguard), SoftEther is relatively new. The protocol started out as a simple project at the University of Tsukuba, but ended up growing into a large open-source multi-protocol VPN software project.

VPN Protocols (cont.)

7. SSTP

SSTP stands for Secure Socket Tunneling Protocol, and it was introduced by Microsoft with Windows Vista. Despite that, it still works on other operating systems too (like Linux and Android).SSTP is significantly superior than PPTP when it comes to security since it can be configured with AES encryption.

8. Wireguard

Wireguard is a new VPN protocol. It's allegedly meant to replace IPsec, and it's claimed to be faster and lighter than it. Also, Wireguard is open-source, and since it only uses a single cryptographic suite, it's less likely to have security holes.