1.2. OSI Model

The OSI model classifies and organizes the tasks that hosts perform to prepare data for transport across the network. You should be familiar with the OSI model because it is the most widely used method for understanding and talking about network communications.

However, remember that it is only a theoretical model that defines standards for programmers and network administrators, not a model of actual physical layers.

Using the OSI model to discuss networking concepts has the following advantages:

- Provides a common language or reference point between network professionals
- Divides networking tasks into logical layers for easier comprehension
- Allows specialization of features at different levels
- Aids in troubleshooting
- Promotes standards interoperability between networks and devices
- Provides modularity in networking features (developers can change features without changing the entire approach)

However, you must remember the following limitations of the OSI model:

- OSI layers are theoretical and do not actually perform real functions.
- Industry implementations rarely have a layer-to-layer correspondence with the OSI layers.
- Different protocols within the stack perform different functions that help send or receive the overall message.
- A particular protocol implementation may not represent every OSI layer (or may spread across multiple layers).

To help remember the layer names of the OSI model, try the following mnemonic devices:

Layer	Name	Mnemonic (Bottom to top)	Mnemonic (Top to bottom)
Layer 7	**Application**	Away	**All**
Layer 6	**Presentation**	Pizza	**People**
Layer 5	**Session**	Sausage	**Seem**
Layer 4	**Transport**	Throw	**To**
Layer 3	**Network**	Not	**Need**
Layer 2	**Data Link**	Do	**Data**
Layer 1	**Physical**	Please	**Processing**

Have some fun and come up with your own mnemonic for the OSI model, but stick to just one so you don't get confused.

1.2. Lower OSI Layer

The following table summarizes basic characteristics of the lower OSI model layers.

Layer		Description
Physical		The Physical layer of the OSI model sets standards for sending and receiving electrical signals between devices. It describes how digital data (bits) are converted to electric pulses, radio waves, or pulses of lights. Devices that operate at the physical layer send and receive a stream of bits.
Data Link	**Media Access Control (MAC)**	The Media Access Control (MAC) layer defines specifications for controlling access to the media. The MAC sublayer is responsible for: • Adding frame start and stop information to the packet • Adding Cyclical Redundancy Check (CRC) for error checking • Converting frames into bits to be sent across the network • Identifying network devices and network topologies in preparation for media transmission • Defining an address (such as the MAC address) for each physical device on the network • Controlling access to the transmission medium
	Logical Link Control (LLC)	The Logical Link Control (LLC) layer provides an interface between the MAC layer and upper-layer protocols. LLC protocols are defined by the IEEE 802.2 committee. The LLC sublayer is responsible for: • Maintaining orderly delivery of frames through sequencing

	• Controlling the flow or rate of transmissions using the following: o **Acknowledgements** o **Buffering** o **Windowing** • Ensuring error-free reception of messages by retransmitting • Converting data into an acceptable form for the upper layers • Removing framing information from the packet and forwarding the message to the Network layer • Provide a way for upper layers of the OSI model to use any MAC layer protocol • Defining Service Access Points (SAPs) by tracking and managing different protocols
Network	The Network layer describes how data is routed across networks and on to the destination. Network layer functions include: • Maintaining addresses of neighboring routers. • Maintaining a list of known networks. • Determining the next network point to which data should be sent. Routers use a routing protocol to take into account various factors such as the number of hops in the path, link speed, and link reliability to select the optimal path for data. Packets forwarded from the Transport to the Network layer become datagrams and network-specific (routing) information is added. Network layer protocols then ensure that the data arrives at the intended destinations.
Transport	The Transport layer provides a transition between the upper and lower layers of the OSI model, making the upper and lower layers transparent from each other.

- Upper layers format and process data without regard for delivery
- Lower layers prepare the data for delivery by fragmenting and attaching transport required information

Transport layer uses the following:

- Port (or socket) numbers are used to identify distinct applications running on the same system. This allows each host to provide multiple services.
- The Transport layer receives large packets of information from higher layers and breaks them into smaller packets called *segments*. Segmentation is necessary to enable the data to meet network size and format restrictions.
- The receiving Transport layer uses packet sequence numbers to reassemble segments into the original message.
- Connection-oriented protocols perform error detection and correction and identify lost packets for retransmission. A connection-oriented protocol is a good choice where:
  - Reliable, error-free communications are more important than speed
  - Larger chunks of data are being sent
- Connectionless services assume an existing link between devices and allow transmission without extensive session establishment. Connectionless communications use no error checking, session establishment, or acknowledgements. Connectionless protocols allow quick, efficient communication at the risk of data errors and packet loss. Connectionless protocols are a good choice where:
  - Speed is important
  - Smaller chunks of data are being sent

1.3. Upper OSI Model Layer

The following table summarizes basic characteristics of the upper OSI model layers.

Layer	Description
Application	The Application layer integrates network functionality into the host operating system, and enables network services. The Application layer does not include specific applications that provide services, but rather provides the capability for services to operate on the network. These services include: • File services--transferring, storing, and updating shared data • Print services--enabling network printers to be shared by multiple users • Message services--transferring data in many formats (text, audio, video) from one location to another, or from one user to another • Application services--sharing application processing throughout the network and enabling specialized network servers to perform processing tasks • Database services--storing, retrieving, and coordinating database information throughout the network The Application layer specifies many important network services that are used on the Internet. These include: • HTTP • Telnet • FTP • TFTP • SNMP ***Note:*** *Most Application layer protocols operate at multiple layers down to the Session and even Transport layers. However, they are classified as Application layer protocols because they start at the*

	Application layer (the Application layer is the highest layer where they operate).
Presentation	The Presentation layer formats or "presents" data into a compatible form for receipt by the Application layer or the destination system. Specifically, the Presentation layer ensures: • Formatting and translation of data between systems • Negotiation of data transfer syntax between systems, through converting character sets to the correct format. • Compatibility with the host • Encapsulation of data into message envelopes by encryption and compression • Restoration of data by decryption and decompression The Presentation layer formats data for the Application layer. Therefore, it also sets standards for multimedia and other file formats. These include standard file formats such as: • JPEG, BMP, TIFF, PICT • MPEG, WMV, AVI • ASCII, EBCDIC • MIDI, WAV
Session	The Session layer's primary function is managing the sessions in which data is transferred. Functions at this layer may include: • Establishment and maintenance of communication sessions between the network hosts, ensuring that data is transported. • Management of multiple sessions (each client connection is called a *session*). A server can concurrently maintain thousands of sessions. • Assignment of the session ID number to each session, which is then used by the Transport layer to properly route the messages.

	• Dialog control--specifying how the network devices coordinate with each other (simplex, half-duplex, and full-duplex). • Termination of communication sessions between network hosts upon completion of the data transfer. The Session layer protocols and interfaces coordinate requests and responses between different hosts using the same application. These protocols and interfaces include: • Network File System (NFS) • Apple Session Protocol (ASP) • Structured Query Language (SQL) • Remote procedure call (RPC) • X Window

1.4. OSI Layer Review

The following table compares the functions performed at each OSI model layer.

Layer	Description and Keywords	Protocols	Devices	Encapsulation
Application	Provides an interface for a service to operate Communication partner identification	HTTP Telnet FTP TFTP SNMP		User information and data
Presentation	Data format (file formats) Encryption, translation, and compression Data format and exchange	JPEG, BMP, TIFF, PICT MPEG, WMV, AVI ASCII, EBCDIC MIDI, WAV		Data
Session	Keeps data streams separate (session identification) Set up, maintain, and tear down communication sessions	SQL NFS ASP RPC X window		Data
Transport	Reliable (connection-oriented) and unreliable	TCP (connection-oriented)		Segments

		(connectionless) communications End-to-end flow control Port and socket numbers Segmentation, sequencing, and combination	UDP (connectionless)		
Network		Logical addresses Path determination (identification and selection) Routing packets	IP IPX AppleTalk DECNET	Routers Layer 3 switches	Packets
Data Link	**Logical Link Control (LLC)**	Convert bits into bytes and bytes into frames MAC address, hardware address Logical network topology Media access Flow control: Acknowledgements Buffering Windowing Parity and CRC	LAN protocols: 802.2 (LLC), 802.3 (Ethernet), 802.5 (Token Ring), 802.11 (Wireless) WAN protocols: HDLC, PPP, Frame Relay, ISDN, ATM	Network Interface Card (NIC) transceivers Switch Bridge	Frames
	Media Access Control (MAC)				

Physical	Move bits across media Cables, connectors, pin positions Electrical signals (voltage, bit synchronization) Physical topology (network layout)	EIA/TIA 232 (serial signaling) V.35 (modem signaling) Cat5 RJ45	Transmission media (cable and wires) Media connectors Transceivers (including transceivers built into NICs) Modems Repeaters Hubs Multiplexers CSUs/DSUs Wireless Access Points	Bits

1.5. TCP/IP Protocol Suite

Groups of protocols (called ***protocol suites*** or ***protocol stacks***) are designed to interact and be used together. The TCP/IP protocol suite is used on the Internet and on most networks. Nearly all computers today use TCP/IP protocols for communication because it is highly scalable and routable. When learning about TCP/IP protocols, it is common to use a theoretical layered model called the TCP/IP model (also known as the Department of Defense (DoD) model). The layers of the DoD model are as follows:

- The Application layer (also called the Process layer) corresponds to the Session, Presentation, and Application layers of the OSI model.
- The Host-to-host layer is comparable to the Transport layer of the OSI model and is responsible for error checking and reliable packet delivery. Here, the data stream is broken into segments that must be assigned sequence numbers so that the segments can be reassembled correctly on the remote side after they are transported.
- The Internet layer is comparable to the Network layer of the OSI model. It is responsible for moving packets through a network. This involves addressing of hosts and making routing decisions to identify how the packet transverses the network.
- The Network Access layer corresponds to the functions of the Physical and Data Link layers of the OSI model. It is responsible for describing the physical layout of the network and how messages are formatted on the transmission medium. Sometimes this layer is divided into the Network Access and the Physical layer.

Note: *The TCP/IP model focuses specifically on the functions in the Internet layer and the Host-to-Host layer. All other functions of the traditional OSI model are encompassed in the first and fourth layers.*

The following table lists several protocols in the TCP/IP protocol suite.

Protocol	Description	OSI Model Layer(s)	DoD Model Layer
File Transfer Protocol (FTP)	File Transfer Protocol (FTP) provides a generic method of transferring files. It can include file security through usernames and passwords, and it allows file transfer between dissimilar computer systems.	**Application, Presentation, Session**	Application/Process
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol (TFTP) is similar to FTP. It lets you transfer files between a host and an FTP server. However, it provides no user authentication and uses UDP instead of TCP as the transport protocol.	**Application, Presentation, Session**	Application/Process
Hypertext Transfer Protocol (HTTP)	The Hypertext Transfer Protocol (HTTP) is used by Web browsers and Web servers to exchange files (such as Web pages) through the World Wide Web and intranets. HTTP can be described as an information requesting and responding protocol. It is typically used to request and send Web	**Application, Presentation, Session**	Application/Process

	documents, but is also used as the protocol for communication between agents using different TCP/IP protocols.		
Simple Mail Transfer Protocol (SMTP)	Simple Mail Transfer Protocol (SMTP) is used to route electronic mail through the internetwork. E-mail applications provide the interface to communicate with SMTP or mail servers.	**Application, Presentation, Session**	Application/Process
Simple Network Management Protocol (SNMP)	Simple Network Management Protocol (SNMP) is a protocol designed for managing complex networks. SNMP lets network hosts exchange configuration and status information. This information can be gathered by management software and used to monitor and manage the network.	**Application, Presentation, Session**	Application/Process
Telnet	Remote Terminal Emulation (Telnet) allows an attached computer to act as a dumb terminal, with data processing taking place on the TCP/IP host computer. It is still widely used to provide connectivity	**Application, Presentation, Session**	Application/Process

	between dissimilar systems.		
Network File System (NFS)	Network File System (NFS) was initially developed by Sun Microsystems. It consists of several protocols that enable users on various platforms to seamlessly access files from remote file systems.	**Application, Presentation, Session**	Application/Process
Voice Over Internet Protocol (VoIP)	Voice over Internet Protocol (VoIP) is a protocol optimized for the transmission of voice through the Internet or other packet switched networks. Voice over IP protocols carry telephony signals as digital audio encapsulated in a data packet stream over IP.	**Application, Presentation, Session**	Application/Process
Transmission Control Protocol (TCP)	Transmission Control Protocol (TCP) operates at the Transport layer. It provides connection-oriented services and performs segment sequencing and service addressing. It also performs important error-checking functions and is considered a host-to-host protocol.	**Transport**	Host-to-Host (Transport)

User Datagram Protocol (UDP)	User Datagram Protocol (UDP) is considered a host-to-host protocol like TCP. It also performs functions at the Transport layer. However, it is not connection-oriented like TCP. Because of less overhead, it transfers data faster, but is not as reliable.	**Transport**	Host-to-Host (Transport)
Domain Name System (DNS)	Domain Name System (DNS) is a system that is distributed throughout the internetwork to provide address/name resolution. For example, the name "www.testout.com" would be identified with a specific IP address.	**Transport**	Host-to-Host (Transport)
Internet Protocol (IP)	Internet Protocol (IP) is the main TCP/IP protocol. It is a connectionless protocol that makes routing path decisions, based on the information it receives from ARP. It also handles logical addressing issues through the use of IP addresses.	**Network**	Internet
Internet Control Message	Internet Control Message Protocol (ICMP) works closely with IP in	**Network**	Internet

Protocol (ICMP)	providing error and control information that helps move data packets through the internetwork.		
Internet Group Membership Protocol (IGMP)	Internet Group Membership Protocol (IGMP) is a protocol for defining host groups. All group members can receive broadcast messages intended for the group (called multicasts). Multicast groups can be composed of devices within the same network or across networks (connected with a router).	**Network**	Internet
Address Resolution Protocol (ARP)	Address Resolution Protocol (ARP) is used to get the MAC address of a host from a known IP address. ARP is used within a subnet to get the MAC address of a device on the same subnet as the requesting device.	**Network**	Internet
Reverse Address Resolution Protocol (RARP)	Both BOOTP (Bootstrap Protocol) and RARP (Reverse Address Resolution Protocol) are used to discover the IP	**Network**	Internet

Bootstrap Protocol (BOOTP)	address of a device with a known MAC address. BOOTP is an enhancement to RARP, and is more commonly implemented than RARP. As its name implies, BOOTP is used by computers as they boot to receive an IP address from a BOOTP server. The BOOTP address request packet sent by the host is answered by the server.	**Network**	Internet
Dynamic Host Configuration Protocol (DHCP)	The Dynamic Host Configuration Protocol (DHCP) simplifies address administration. DHCP servers maintain a list of available and assigned addresses, and communicate configuration information to requesting hosts. DHCP has the following two components. • A protocol for delivering IP configuration parameters from a DHCP server to a host • A protocol specifying how IP	**Network**	Internet

	addresses are assigned		
Open Shortest Path First (OSPF)	Open Shortest Path First (OSPF) is a route discovery protocol that uses the link-state method. It is more efficient than RIP in updating routing tables, especially on large networks.	**Network**	Internet
Routing Information Protocol (RIP)	Routing Information Protocol (RIP) is a route discovery protocol that uses the distance-vector method. If the network is large and complex, OSPF should be used instead of RIP.	**Network**	Internet

The TCP/IP protocol suite was developed to work independently of the Physical layer implementation. You can use a wide variety of architectures with the TCP/IP protocol suite.

1.6. IP Address and Class

IP addresses allow hosts to participate on IP based networks. An IP address:

- Is a 32-bit binary number represented as four octets (four 8-bit values). Each octet is separated by a period.
- IP addresses can be represented in one of two ways:
  - Decimal (for example 131.107.2.200).
    In decimal notation, each octet must be between 0 and 255.
  - Binary (for example 10000011.01101011.00000010.11001000).
    In binary notation, each octet is an 8-digit number.
- The IP address includes both the network and the host address.
- Each IP address has an implied address class that can be used to infer the network portion of the address.
- The subnet mask is a 32-bit number that is associated with each IP address that identifies the network portion of the address. In binary form, the subnet mask is always a series of 1's followed by a series of 0's
  (1's and 0's are never mixed in sequence in the mask).
  A simple mask might be 255.255.255.0.

IP addresses have a default *class*. The address class identifies the range of IP addresses and a default subnet mask used for the range. The following table shows the default address class for each IP address range.

Class	Address Range	First Octet Range	Default Subnet Mask
A	**1.0.0.0** **126.255.255.255**	**1-126** **00000001 01111110**	**255.0.0.0**
B	**128.0.0.0** **191.255.255.255**	**128-191** **10000000 10111111**	**255.255.0.0**
C	**192.0.0.0** **223.255.255.255**	**192-223** **11000000 11011111**	**255.255.255.0**

D	224.0.0.0 239.255.255.255	224-239 11100000 11101111	n/a
E	240.0.0.0 255.255.255.255	240-255 11110000 11111111	n/a

When using the default subnet mask for an IP address, you have the following number of subnet addresses and hosts per subnet:

- There are only **126** Class A network IDs (most of these addresses are already assigned). Each Class A address gives you **16,777,214** hosts per network.
- There are **16,384** Class B network IDs. Each class B address gives you **65,534** hosts per network.
- There are **2,097,152** Class C network IDs. Each class C address gives you **254** hosts per network.
- Class D addresses are used for multicast groups rather than network and host IDs.
- Class E addresses are reserved for experimental use.

1.7. Special Address

You should understand the following special addresses:

Address	Consideration
Network	The first octet(s) in an address range is used to identify the network itself. For the network address, the host portion of the address contains all 0's. For example: • Class A network address: 115.0.0.0 • Class B network address: 154.90.0.0 • Class C network address: 221.65.244.0 0.0.0.0 is the network address used by routers to specify the "default" route. Using a generic value reduces the number of routing table entries. Some older routers use this address as a broadcast address.
Host	The range of IP addresses available to be assigned to network hosts is identified by the subnet mask and/or the address class. For example: • For the class A network address 115.0.0.0, the host range is 115.0.0.1 - 115.255.255.254. • For the class B network address 154.90.0.0, the host range is 154.90.0.1 - 154.90.255.254. • For the class C network address 221.65.244.0, the host range is 221.65.244.1 - 221.65.244.254. ***Note:*** *A special way to identify a host on a network is by setting the network portion of the address to all 0's. For example, the address 0.0.64.128 means "host 64.128 on this network."*
Broadcast	The last address in the range is used as the broadcast address and is used to send messages to all hosts on the network. In binary form, the broadcast address has all 1's in the host portion of the address. For example, assuming the default subnet masks are used:

	• 115.255.255.255 is the broadcast address for network 115.0.0.0 • 154.90.255.255 is the broadcast address for network 154.90.0.0 • 221.65.244.255 is the broadcast address for network 221.65.244.0 Two other formats you might see for the broadcast address: • The broadcast address might also be designated by setting each of the network address bits to 0. For example, 0.0.255.255 is the broadcast address of a Class B address. This designation means "the broadcast address for this network." • 255.255.255.255 indicates a broadcast message intended for all hosts on this network.
Local host	Addresses in the 127.0.0.0 range are reserved for the local host (in other words "this" host or the host you're currently working at). The most commonly-used address is **127.0.0.1** which is the loopback address.
Private use	The following address ranges have been reserved for private use: • 10.0.0.0 - 10.255.255.255 • 172.16.0.0 - 172.31.255.255 • 192.168.0.0 - 192.168.255.255 Use addresses in these ranges for your private networks. Routers connected to the Internet typically filter messages within these ranges and prevent them from being propagated to the Internet.

1.8. Data Encapsulation

Encapsulation is the process of breaking a message into packets, adding control and other information, and transmitting the message through the transmission media. You need to know the following five-step data encapsulation process:

1. Upper (**Session**, **Presentation**, **Application**) layers prepare the ***data*** to be sent through the network.
2. The **Transport layer** breaks the data into pieces called ***segments***, adding sequencing and control information.
3. The **Network layer** converts the segments into ***packets***, adding logical network and device addresses.
4. The **Data Link layer** converts the packets into ***frames***, adding physical device addressing information.
5. The **Physical layer** converts the frames into ***bits*** for transmission across the transmission media.

The following short descriptions can help you remember the steps of the data encapsulation process:

1. Upper layers (L5, L6, L7) - ***data***
2. **Transport layer (L4)** - ***segments***
3. **Network layer (L3)** - ***packets*** containing ***logical addresses***
4. **Data Link layer (L2)** - ***framing*** *that* adds ***physical addresses***
5. Physical layer (L1) - ***bits***

1.9. Ethernet Architecture

The following table shows specifics of the Ethernet architecture.

Specification	Description
Topology	The *physical* topology is the mapping of the nodes of a network and the physical connections between them, such as the layout of wiring, cables, the locations of nodes, and the interconnections between the nodes and the cabling or wiring system. The *logical* topology is the way messages are sent through the network connections. Ethernet supports the following topologies: **Physical bus, logical bus** **Physical star, logical bus** **Physical star, logical star**
Media access	Ethernet uses Carrier Sense, Multiple Access/Collision Detection (CSMA/CD) to control access to the transmission medium. Devices use the following process to send data: 1. Because all devices have equal access to the transmission media (multiple access), a device with data to send first listens to the transmission medium to determine if it is free (carrier sense). 2. If it is not free, the device waits a random time and listens again to the transmission medium. When it is free, the device transmits its message. 3. If two devices transmit at the same time, a collision occurs. The sending devices detect the collision (collision detection) and send a jam signal. 4. Both devices wait a random length of time before attempting to resend the original message (called a *bakeoff*).

Transmission media	Ethernet supports the following cable types: • Unshielded twisted-pair cables (UTP) with RJ-45 connectors. This is the most common transmission medium used for Ethernet. Each cable consists of eight wires, twisted into four pairs. UTP cables are classified by categories: o Cat3, rated up to 10 Mbps o Cat4, rated up to 16 Mbps o Cat5, rated up to 100 Mbps o Cat5e, rated up to 1,000 Mbps (gigabit) • Fiber optic, most commonly used in high-speed applications such as servers or streaming media. Fiber optic cables have ST, SC, LC, and MT-RJ connectors. • Coaxial for older Ethernet implementations (often called *thinnet* or *thicknet* networks). Coaxial cables have F-Type and BNC connectors.
Frame type	The Ethernet frame size is 64 to 1518 bytes (this is the same for all Ethernet standards). Four frame types are supported: • Ethernet 802.3 is the original Ethernet frame type. • Ethernet 802.2 is the frame type that accommodates standards set by the IEEE 802.2 committee related to the logical link control (LLC) sublayer. It is a more current frame type than 802.3. • Ethernet II is a frame type that provides the ability to use TCP/IP as a transport/network layer protocol. Other Ethernet frame types operate strictly with IPX/SPX as a transport/network layer protocol. • Ethernet SNAP (SubNetwork Address Protocol) is an enhanced version of Ethernet 802.2 that allows for greater compatibility with other network architectures such as Token Ring. This frame type also supports TCP/IP.

Physical address	The MAC address (also called the burned-in address) is the Data Link layer physical device address. • The MAC address is a 12-digit hexadecimal number (each number ranges from 0-9 or A-F). • The address is often written as 00-B0-D0-06-BC-AC or 00B0.D006.BCAC, although dashes, periods, and colons can be used to divide the MAC address parts. • The MAC address is guaranteed unique through design. The first half (first 6 digits) of the MAC address is assigned to each manufacturer. The manufacturer determines the rest of the address, assigning a unique value which identifies the host address. A manufacturer that uses all the addresses in the original assignment can apply for a new MAC address assignment. ***Note:*** *Some network cards allow you to change (logically assigned address) the MAC address through jumpers, switches, or software. However, there is little practical reason for doing so.*

1.10. Ethernet Standards

The following table compares the characteristics of various Ethernet implementations.

Category	Standard	Bandwidth	Cable Type	Maximum Segment Length
Ethernet	10Base5	10 Mbps	Coaxial (thicknet)	500 meters
	10Base2	10 Mbps	Coaxial (thinnet)	185 meters
	10BaseT	10 Mbps (half duplex) 20 Mbps (full duplex)	Twisted pair (Cat3, 4, or 5)	100 meters
Fast Ethernet	100BaseTX	100 Mbps (half duplex) 200 Mbps (full duplex)	Twisted pair (Cat5)	100 meters
	100BaseT4	100 Mbps (half duplex) 200 Mbps (full duplex)	Twisted pair (Cat5)	100 meters
	100BaseFX	100 Mbps (half duplex) 200 Mbps (full duplex)	Fiber optic	412 meters (half duplex multimode cable) 2,000 meters (full duplex singlemode cable)
Gigabit Ethernet	1000BaseSX (short)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Fiber optic	220 to 550 meters depending on cable quality

	1000BaseLX (long)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Fiber optic	550 to 5,000 meters depending on cable quality
	1000BaseCX (short copper)	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Special copper	25 meters, used within wiring closets
	1000BaseT	1,000 Mbps (half duplex) 2,000 Mbps (full duplex)	Twisted pair (Cat5e)	100 meters

Fast Ethernet was designed to be as compatible with 10BaseT Ethernet as possible. This provides an easy migration path from 10BaseT to 100BaseT/100BaseT4 (and even to Gigabit Ethernet).

- Most new networking devices that are Fast or Gigabit Ethernet capable also support 10BaseT standards. Devices autosense the specifics of the network configuration and set themselves to use the fastest communication method possible.
- If your network uses 10BaseT and has Cat5 cable, you can slowly migrate from 10BaseT to FastEthernet (remember that FastEthernet uses Cat5 cable). As you replace components such as NICs and hubs with FastEthernet devices, portions of the network will begin operating at FastEthernet speeds.
- You can begin your upgrade with:
    - Critical components, such as hubs, switches, and server NICs
    - Segments that service mission-critical applications
    - Workstations that have heavy bandwidth requirements

1.11. Half- and Full-Duplex

With the original Ethernet standards, all devices shared the same cable.
This caused two problems:

- Collisions occur when two devices transmit at the same time.
  Devices needed to be able to detect and recover from collisions.
- Each device could either transmit or receive data at any given time.
  This meant that the device was either receiving data or listening for incoming data. Devices were not able to both send and receive at the same time (much like using a one-lane road for traffic in two different directions).

These two problems were solved in the following ways:

- Using twisted pair cable, multiple strands of wires are combined into a single cable. Devices can use different wires to send and receive data (allowing them to do both simultaneously).
- Using switches, devices are given a dedicated communication path.
  With a single device connected to a switch port, collisions are eliminated.

With these problems solved, you can turn off collision detection.
Devices can transmit and receive data simultaneously,
and can begin transmitting data as soon as they have data to send.

Devices with **collision detection turned on** operate in ***half-duplex*** mode;
devices with **collision detection turned off** operate in ***full-duplex*** mode.

Mode	**Description**	**Bandwidth**
Half-duplex	• Collision detection is turned **on** • The device can only send or receive at any given time • Devices connected to a hub must use half-duplex communication	Up to the rated bandwidth (10 Mbps for 10BaseT, 100 Mbps for 100BaseT, etc.)

Full-duplex	• Collision detection is turned **off** • The device can send and receive at the same time • Requires full-duplex capable NICs • Requires switches with dedicated switch ports (a single device per port)	Double the rated bandwidth (20 Mbps for 10BaseT, 200 Mbps for 100BaseT, etc.)

1.12. Bridge

A ***bridge*** is a data forwarding device that provides data transfer.
You should understand the following concepts relating to the operation of bridges.

- Bridges connect two media segments that use the same protocol.
- Bridges examine the source address to determine the media segment of network devices.
- Bridges operate at the Data Link layer of the OSI model.
- Bridges maintain a table of device addresses and their corresponding segments.
- Each segment connected by a bridge can have the same network address.
- Messages within a media segment are prevented from crossing over to another segment.

Bridges offer the following advantages:

- Bridges prevent wasted bandwidth by eliminating unnecessary traffic between segments.
- Bridges increase the maximum network length.
- Bridges forward packets for multiple upper-layer protocols.
- Bridges can link segments with dissimilar transmission media and media access methods.

Bridges have the following limitations:

- Bridges cannot link multiple architectures because different frame types are used.
- Bridges cannot translate upper-layer protocols.
- Bridges cannot forward packets to different networks based on the network address.
- Bridges do not filter broadcast packets.

Use bridges to isolate traffic to a segment, or to prevent unwanted traffic from crossing over to other segments, or to slow WAN links. When designing the placement of bridges on the network, follow the 80/20 rule.

- At least 80% of network traffic should stay within a segment.
- No more than 20% of network traffic should pass through the bridge to another segment.

1.13. Switch

A ***switch*** is a multiport bridge.
It provides the same functionality, but with a higher port density.
In addition, switches provide features that cannot be found in bridges.

- Switches are associated with the Data Link layer of the OSI Model.
- Switches build a forwarding database in a manner similar to bridges. Switches examine the source and destination Data Link address in each packet to build the database and make forwarding decisions.
- Switches connect multiple segments or devices and forward packets to only one specific port.
- You can connect a single device to a switch port or multiple devices to a switch port by using a hub.

Switches offer the following advantages over a non-switched network.

- Switches create separate collision domains.
- Switches provide guaranteed bandwidth between devices, if dedicated ports are used.
- Switches can be used to provide collision-free networking, if only one device is connected to each switch port.
- Switches enable full-duplex communication.
- Switches induce less latency than other segmentation solutions.
- Switches can simultaneously switch multiple messages.
- Switches can mix 10 Mbps- and 100 Mbps-capable devices, if the switch is a 100 Mbps switch.
- Ethernet switches can be implemented without re-cabling.

Switches have replaced bridges in most network applications.

1.14. Bridge and Switch Forwarding

Both bridges and switches build a forwarding database.
The database is a list of Data Link (MAC) addresses and the port used to reach the device. Bridges and switches can automatically learn about devices to build the forwarding database. A network administrator can also program the device database manually.

Bridges and switches use the following process to dynamically build the forwarding database:

- The process begins by examining the source address of an incoming packet. If the source address is not in the forwarding database, an entry for the address is made in the database. The port it came in on is also recorded.
- The destination address is then examined.
    - If the destination address is in the database, the packet is forwarded to the appropriate port if the port is different than the one on which it was received.
    - If the destination address is not in the database, the packet is sent out all ports except for the one on which it was received. This is known as ***flooding***.
    - A broadcast packet is ***forwarded (flooded)*** to all ports except the one on which it was received.

Transparent bridges forward packets only if the following conditions are met.

- The frame contains data from the layers above the Data Link layer.
- The frame's integrity has been verified through a valid Cyclic Redundancy Check (CRC).
- The frame is not addressed to the bridge.

How switches forward packets depends on the switch type. The following table compares the different methods the switch uses to forward packets (some Cisco switches support all three methods).

Method	Characteristics
Store-and-forward	Store-and-forward switches: • Receive the entire frame. • Verify the frame's integrity (check the CRC). Frames with errors are not forwarded. • Forward the frame to the destination device. • Introduce more latency (delay) than cut-through switches.
Cut-through	Cut-through switches: • Read the destination device address. • Forward the packet without verifying frame integrity. • Are faster than store-and-forward switches (less latency).
Fragment-free	Fragment-free switches: • Read the first 64 bytes of a frame. • Verify that the packet is not a fragment. • Forward non-fragmented frames. • Introduce some latency, but not as great as store-and-forward switching.

Note: *Newer switches can monitor each port and determine which switching method to use. They can automatically change to store-and-forward if the number of errors on a port exceeds a configurable threshold.*

1.15. Routing

A ***router*** is a device that sends packets from one network to another network. Routers receive packets, read their headers to find addressing information, and send them on to their correct destination on the network or Internet. Routers can forward packets through an internetwork by maintaining routing information in a database called a ***routing table***.

The routing table typically contains the address of all known networks and routing information about that network such as:

- Interface
- Routing Path
- Next Hop
- Route Metric (Cost)
- Route Timeout

Routers build and maintain their routing database by periodically sharing information with other routers. The exact format of these exchanges is based on the routing protocol.

The routing protocol determines:

- The information contained in the routing table
- How messages are routed from one network to another
- How topology changes (i.e. updates to the routing table) are communicated between routers

Regardless of the method used, changes in routing information take some time to be propagated to all routers on the network. The term ***convergence*** is used to describe the condition when all routers have the same (or correct) routing information.

1.16. Message Routing

To send a message from one host to another on a different network, the following process is used:

1. The sending host prepares a packet to be sent. It uses its own IP address for the source Network layer address, and the IP address of the final receiving device as the destination Network layer address.
2. The sending host creates a frame by adding its own MAC address as the source Physical layer address. For the destination Physical layer address, it uses the MAC address of the default gateway router.
3. The sending host transmits the frame.
4. The next hop router reads the destination MAC address in the frame. Because the frame is addressed to that router, it processes the frame.
5. The router strips off the frame header and examines the packet destination address. It uses a routing protocol to identify the next hop router in the path.
6. The router repackages the packet into a new frame. It uses its own MAC address as the source Physical layer address. It uses the MAC address of the next hop router for the destination Physical layer address.
7. The router transmits the frame.
8. The next hop router repeats step 4 through 7 as necessary, until the frame arrives at the last router in the path.
9. The last router in the path receives the frame and checks the destination IP address contained in the packet.
10. Because the destination device is on a directly connected network, the router creates a frame using its own MAC address as the source address, and the MAC address of the destination device as the destination physical address.
11. The router transmits the frame.
12. The destination device receives the frame. Inside the packet it finds the destination address matching its own IP address, with the source IP address being that of the original sending device.

Be aware of the following:

- On an Ethernet network, the Data Link layer address is the MAC address. On an IP network, the Network layer address is the IP address.
- Both Data Link physical addresses and Network logical addresses are used to send packets between hosts.
- The Data Link address identifies the physical interface. The Network address contains both a logical network address and a logical device address.
- IP (Network layer) addresses are contained in the IP header; MAC (Data Link) addresses are contained in the Ethernet frame header.
- Both the source and destination Network and Data Link addresses are typically contained in the packet.
- Data Link addresses in the packet change as the packet is delivered from hop to hop. At any point in the process, the Data Link destination address indicates the physical address of the next hop on the route. The Data Link source address is the physical address of the device sending the frame.
- Network addresses remain constant as the packet is delivered from hop to hop. The Network addresses indicate the logical address of the original sending device and the address of the final destination device.
- A router uses the logical network address specified at the Network layer to forward messages to the appropriate network segment.