The Basics of Networking

COMP 4670 - Network Security

Lesson 01

Outlines

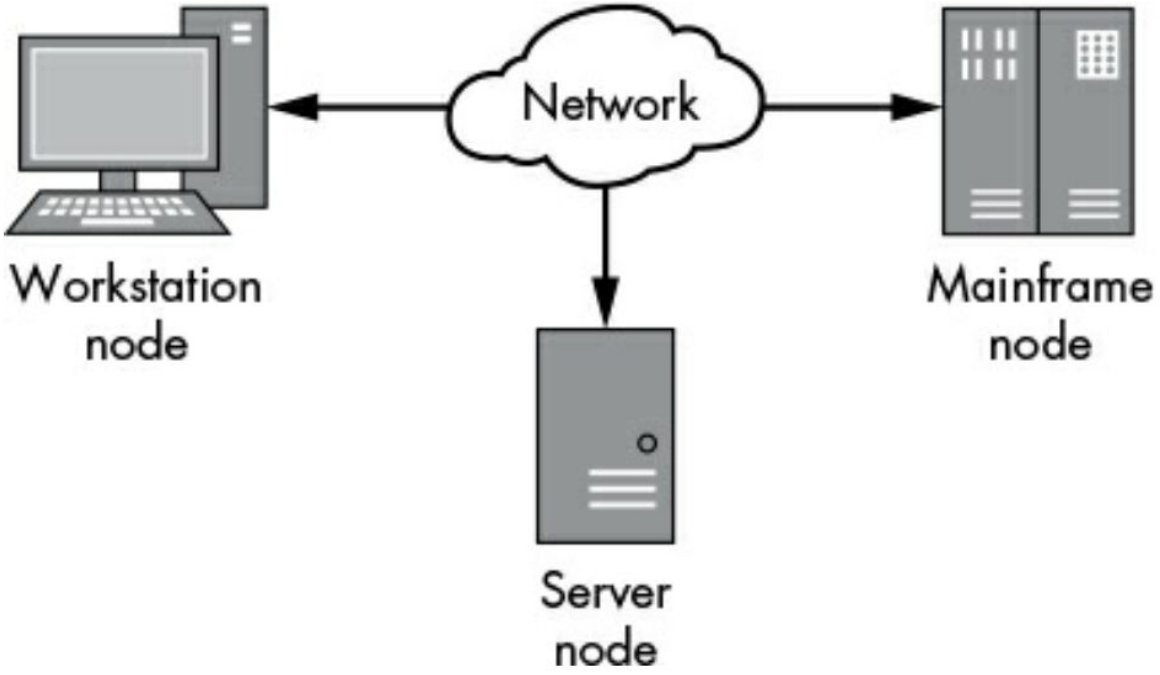
- Computer Networks & Communications
- OSI Model
- TCP/IP Model
- Data Transmission and Routing

What is Computer Network?

Computer Networks

- A computer network is a set of two or more computers connected together to share information.
- It’s common to refer to each connected device as a node on the network to make the description applicable to a wider range of devices.
- The term host usually used to refer to a computer node (PC, Server, Workstation) and not any network device (switch, router, network storage, network printer).

Computer Networks



Computer Network Communication

- In the early days of network development, communications between computers of different vendors were often difficult, if not impossible.
- This is because each node might have a different operating system, software application and/or hardware.
- As long as each node follows a set of rules, or network protocol, it can communicate with the other nodes on the network.
- Communications between computers over networks are made possible by network protocols.

Network Protocols

- Network Protocol is a set of restrictions and rules that define communication between two or more devices over a network.
- Network Protocol defines how the data transmitted over a network medium.
- All nodes on a network must understand the same network
- protocol.
- Examples: ARP, ICMP, HTTP, SMTP, TCP, UDP, and IP protocol

What are the common functions or features network protocols provide to enable two or more nodes to communicate?

Key Functions of Network Protocols

1. **Maintaining session state** Protocols typically implement mechanisms to create new connections and terminate existing connections.
2. **Identifying nodes through addressing** Data must be transmitted to the correct node on a network. Some protocols implement an addressing mechanism to identify specific nodes or groups of nodes.

Key Functions of Network Protocols

3. **Controlling data flow** The amount of data transferred across a network is limited. Protocols can implement ways of managing data flow to increase throughput and reduce latency.
4. **Guaranteeing the order of transmitted data** Many networks do not guarantee that the order in which the data is sent will match the order in which it's received. A protocol can reorder the data to ensure it's delivered in the correct order.

Key Functions of Network Protocols

5. **Detecting and correcting errors** Many networks are not 100 percent reliable; data can become corrupted. It's important to detect corruption and, ideally, correct it.
6. **Formatting and encoding data** Data isn't always in a format suitable for transmitting on the network. A protocol can specify ways of encoding data, such as encoding English text into binary values.

Protocol Stack

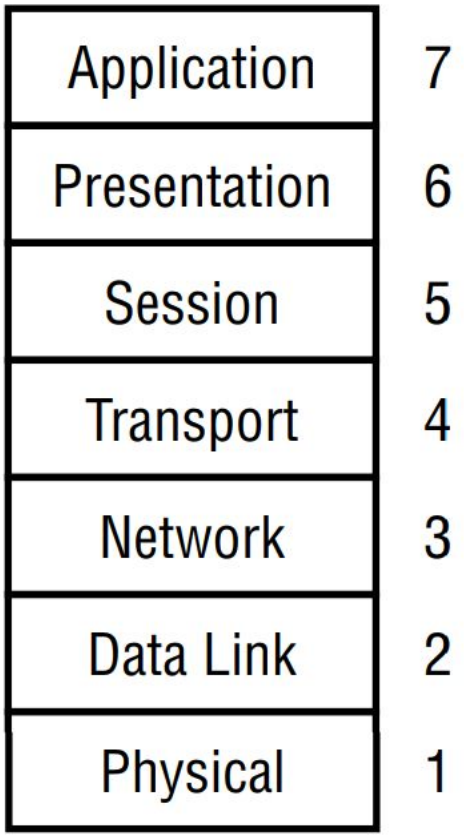
What is Network or Protocol Stack?

- A protocol stack refers to a group of protocols that are running concurrently and are employed for the implementation of network protocol suite.
- The protocol stack or network stack is an implementation of a computer networking protocol suite or protocol family.

OSI Model

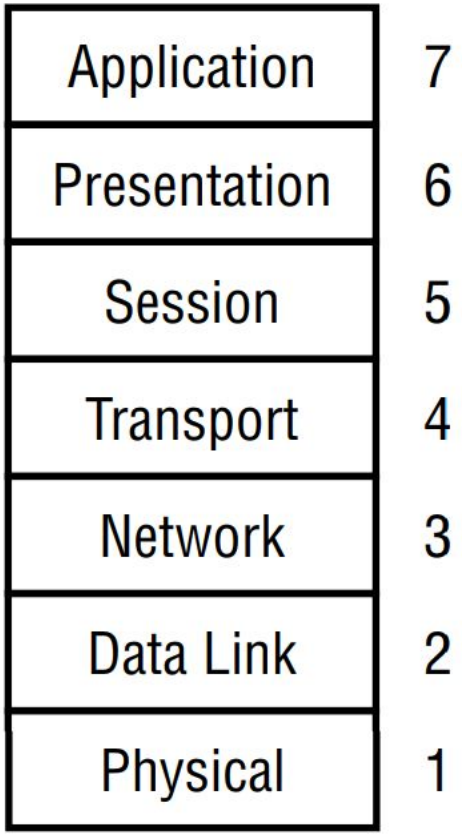
OSI Model

- The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) Reference Model for protocols in the early 1980s.
- The OSI model is a conceptual model that provides a common foundation for the development of new network protocols, networking services, and even hardware devices.

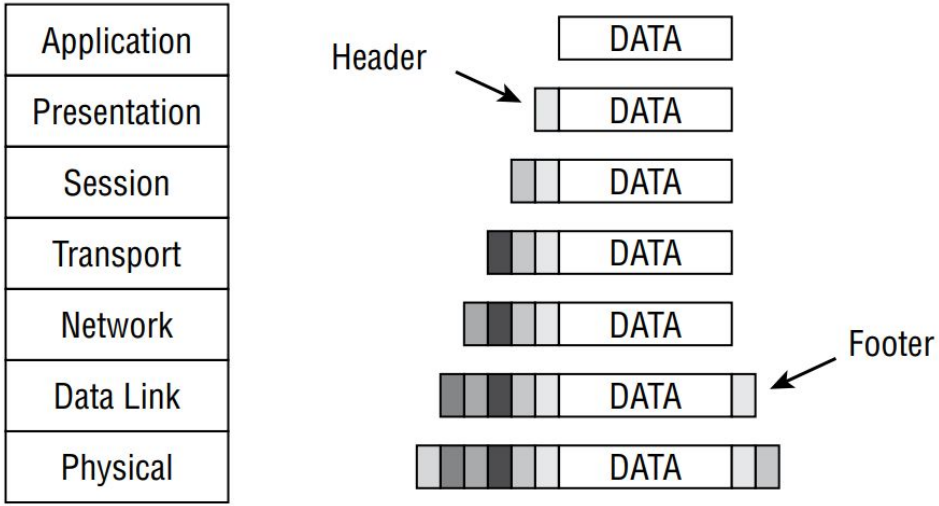


OSI Model

- Each layer provides specific function to support moving the data from one node to another over the network.
- Each layer communicates directly with the layer above it as well as the layer below it, plus the peer layer on a communication partner system
- **Note:** The layers are always numbered from bottom to top.



Encapsulation & Decapsulation

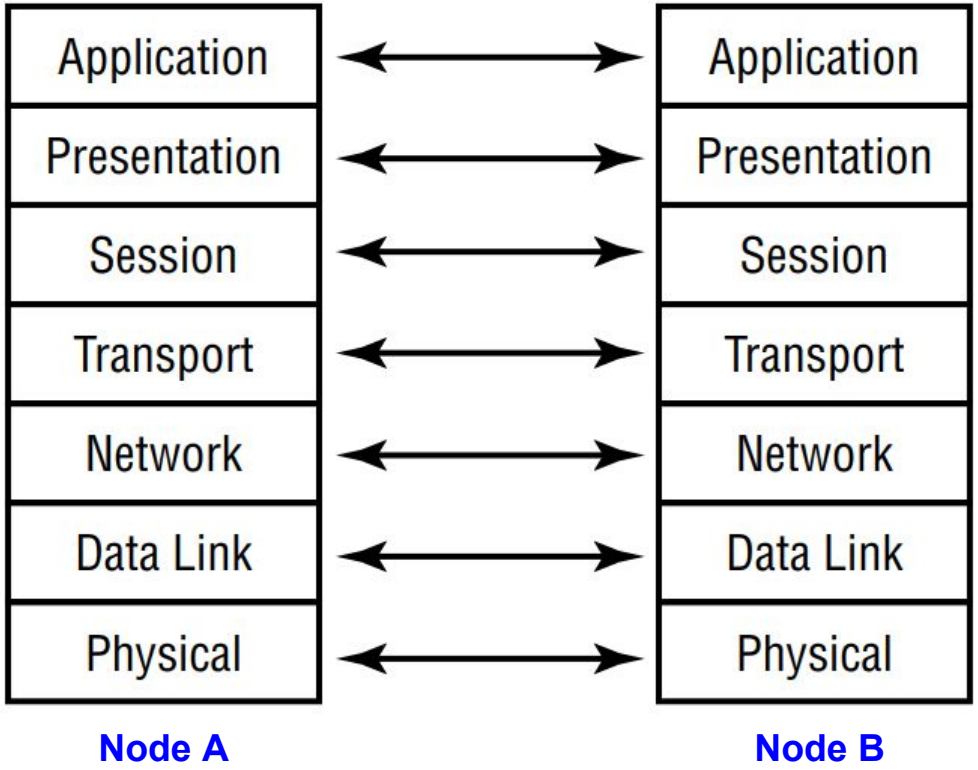


Network protocol based on the OSI model apply encapsulation and decapsulation.

Encapsulation & Decapsulation

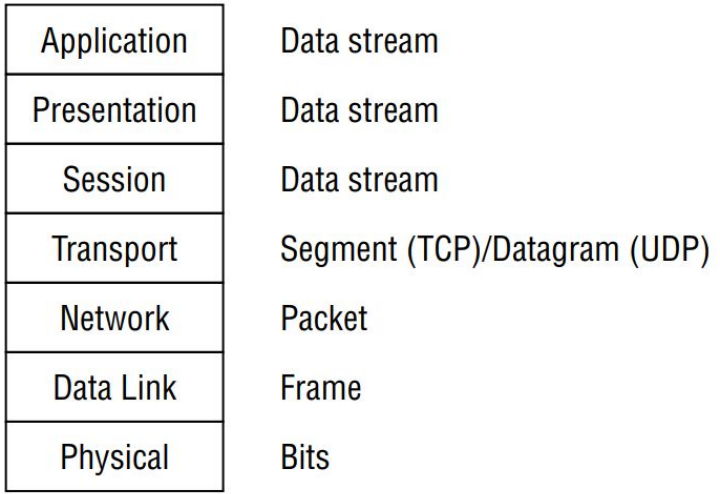
- Encapsulation is the addition of a header, and possibly a footer, to the data received by each layer from the layer above before it's handed off to the layer below.
- Encapsulation occurs as the data moves down through the OSI model layers from Application to Physical.
- Decapsulation occurring as data moves up through the OSI model layers from Physical to Application.
- In the header each layer add instructions, checksum, and other information that can be understood only by the peer layer that originally added or created the information.

OSI model Peer Layer Logical Channels



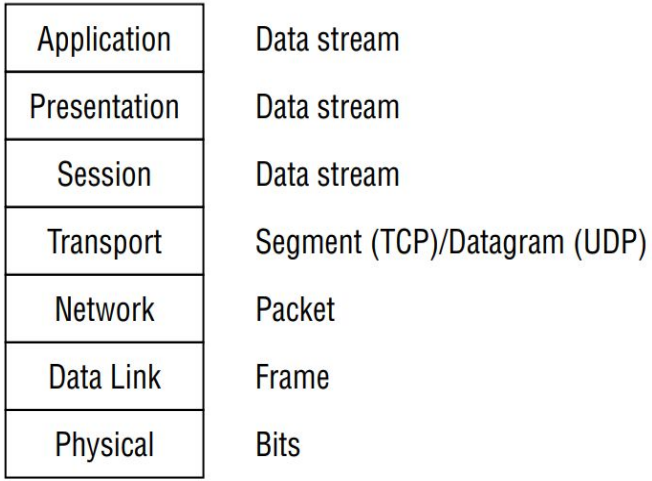
OSI Model: Physical Layer

- Accepts the frame from the Data Link layer and converts the frame into bits for transmission over the physical connection medium.
- Contains the device drivers that tell the protocol how to use the hardware for the transmission and reception of bits.



OSI Model: Data Link Layer

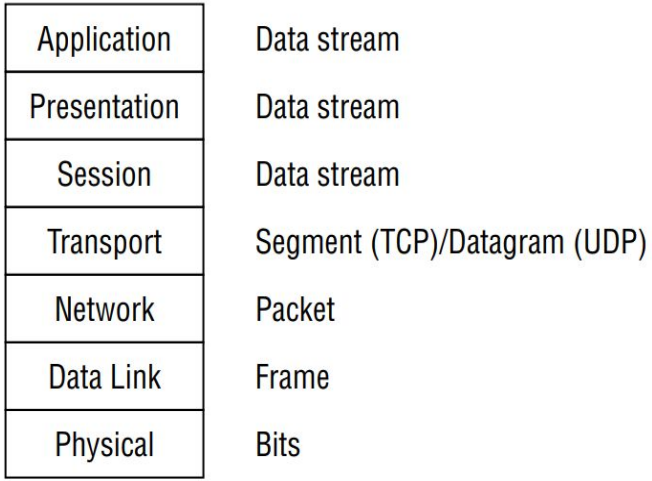
- Part of the processing performed on the data within the Data Link layer includes adding the hardware source and destination addresses to the frame. The hardware address is the Media Access Control (MAC) address.
- The MAC address is a 6-byte (48-bit) binary address written in hexadecimal notation (for example, 00-13-02-1F-58-F5).
- No two devices can have the same MAC address in the same local Ethernet broadcast domain; otherwise an address conflict occurs.



OSI Model: Data Link Layer

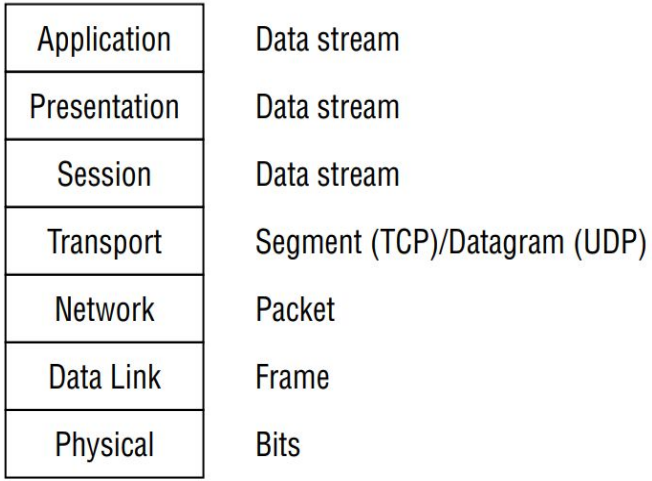
Several protocols exist within the Data Link layer such as:

1. Serial Line Internet Protocol (SLIP)
2. Point-to-Point Protocol (PPP)
3. Address Resolution Protocol (ARP)
4. Reverse Address Resolution Protocol (RARP)
5. Layer 2 Forwarding (L2F)
6. Layer 2 Tunneling Protocol (L2TP)
7. Point-to-Point Tunneling Protocol (PPTP)



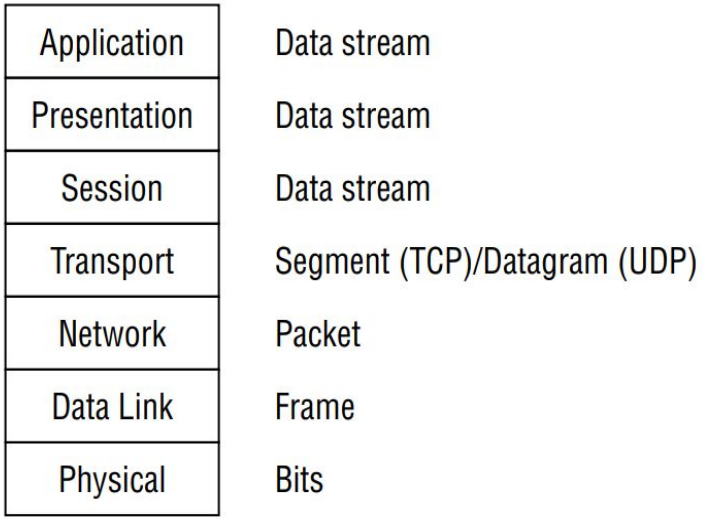
OSI Model: Data Link Layer

- Address Resolution Protocol (ARP):
  - is used to resolve IP addresses into MAC addresses.
- Reverse Address Resolution Protocol (RARP):
  - is used to resolve MAC addresses into IP addresses.



OSI Model: Network Layer

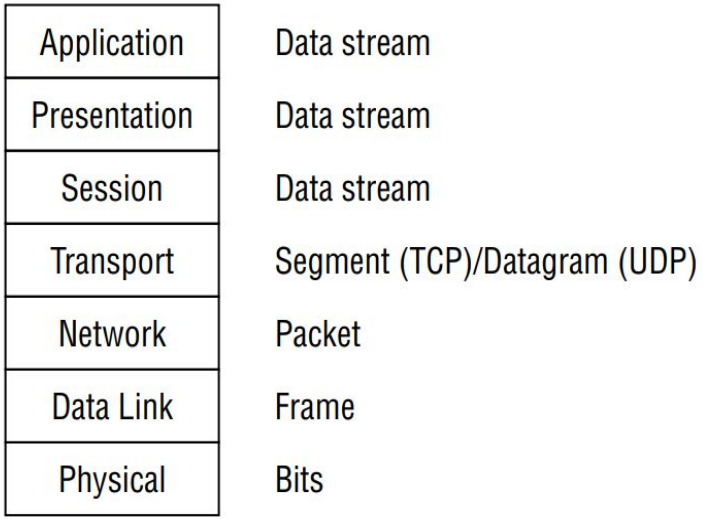
- Is responsible for adding routing and addressing information to the data.
- The Network layer accepts the segment from the Transport layer and adds information to it to create a packet. The packet includes the source and destination IP addresses.



OSI Model: Network Layer

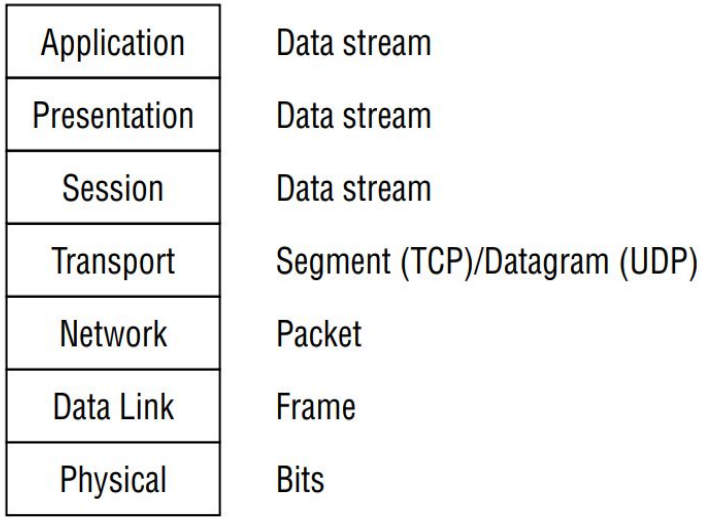
The routing protocols are located at this layer and include the following:

1. Internet Control Message Protocol (ICMP)
2. Routing Information Protocol (RIP)
3. Open Shortest Path First (OSPF)
4. Border Gateway Protocol (BGP)
5. Internet Group Management Protocol (IGMP)
6. Internet Protocol (IP)
7. Internet Protocol Security (IPSec)



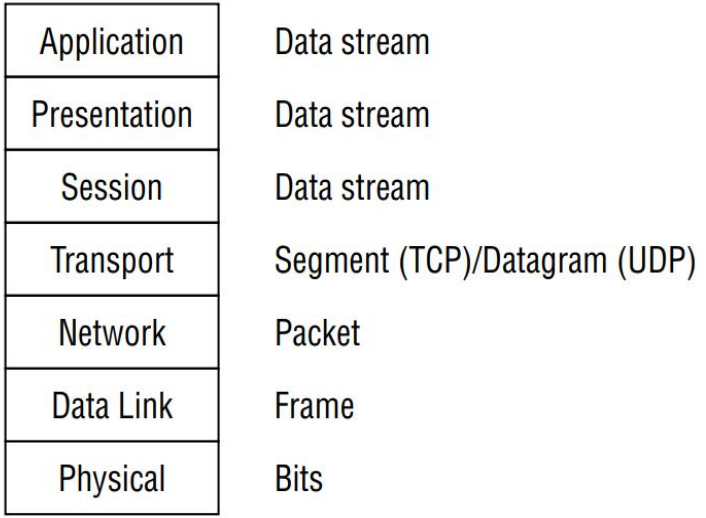
OSI Model: Transport Layer

- The Transport layer (layer 4) is responsible for managing the integrity of a connection and controlling the session.
- It accepts Payload Data Unit from the Session layer and converts it into a segment.



OSI Model: Transport Layer

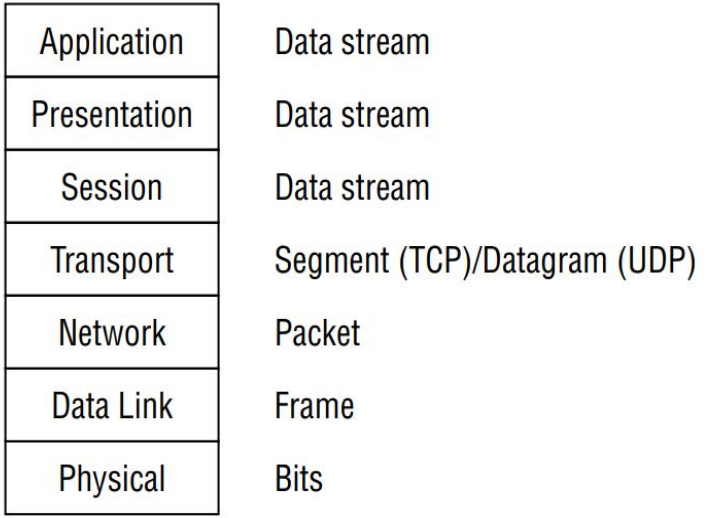
- The Transport layer establishes a logical connection between two devices and provides end-to-end transport services to ensure data delivery.
- Transport layer implements mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction, multiplexing, and network service optimization.



OSI Model: Transport Layer

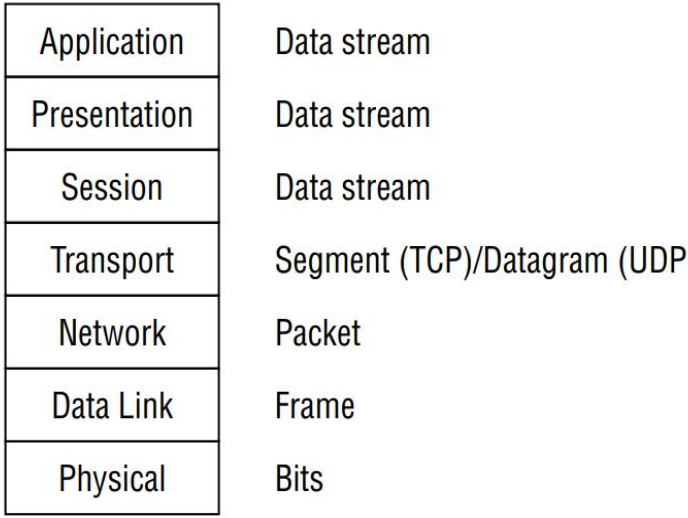
The following protocols operate within the Transport layer:

1. Transmission Control Protocol (TCP)
2. User Datagram Protocol (UDP)
3. Sequenced Packet Exchange (SPX)
4. Secure Sockets Layer (SSL)
5. Transport Layer Security (TLS)



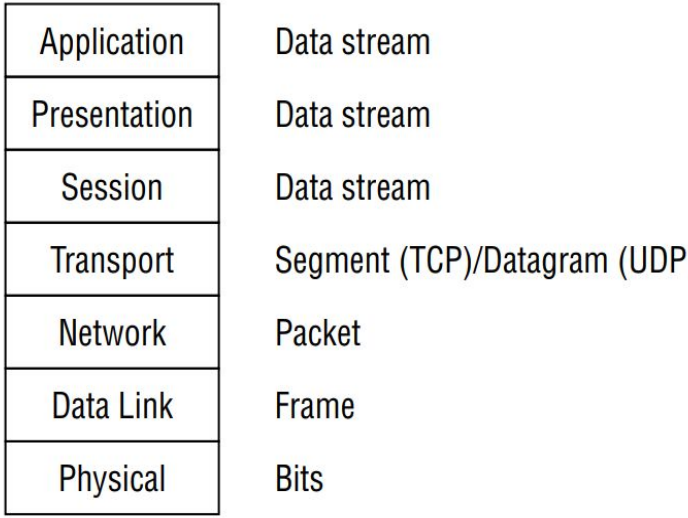
OSI Model: Session Layer

- Session layer (layer 5) is responsible for establishing, maintaining, and terminating communication sessions between two computers.
- Communication sessions can operate in one of three different discipline or control modes: Simplex, Half-Duplex, and Full-Duplex



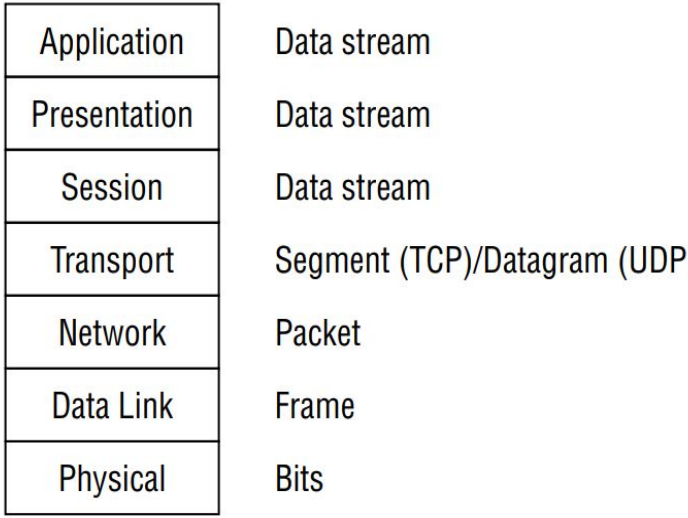
OSI Model: Presentation Layer

- The Presentation layer (layer 6) is responsible for transforming data received from the Application layer into a format that any system following the OSI model can understand.
- It allows various applications to interact over a network, and it does so by ensuring that the data formats are supported by both systems.



OSI Model: Application Layer

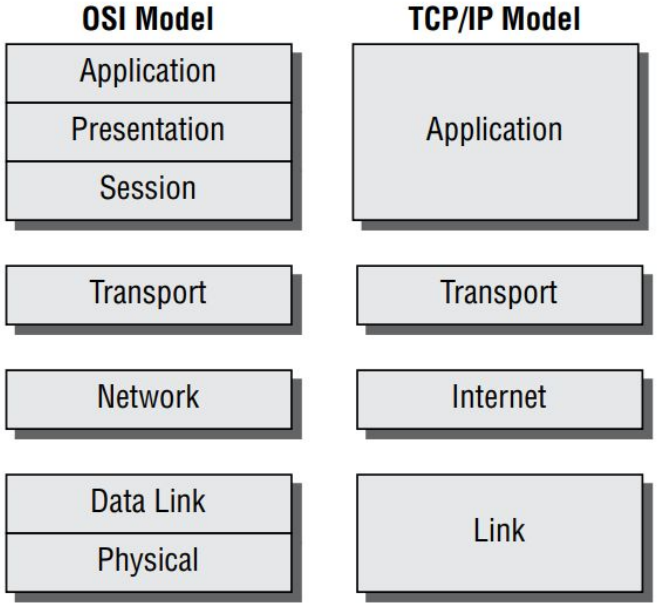
- The Application layer (layer 7) is responsible for interfacing user applications, network services, or the operating system with the protocol stack.
- The application layer allows applications to communicate with the protocol stack.
- Examples of application layer protocols are HTTP, SMTP, FTP, SSH, etc



TCP/IP Model

TCP/IP Model

- The TCP/IP model (also called the DARPA or the DOD model) consists of only four layers.



TCP/IP Model

- The most widely used protocol suite is TCP/IP, but it is not just a single protocol; rather, it is a protocol stack comprising dozens of individual protocols.
- TCP/IP is a platform-independent protocol based on open standards. However, this is both a benefit and a drawback.
- TCP/IP can be found in just about every available operating system, but it consumes a significant amount of resources and is relatively easy to hack into because it was designed for ease of use rather than for security.

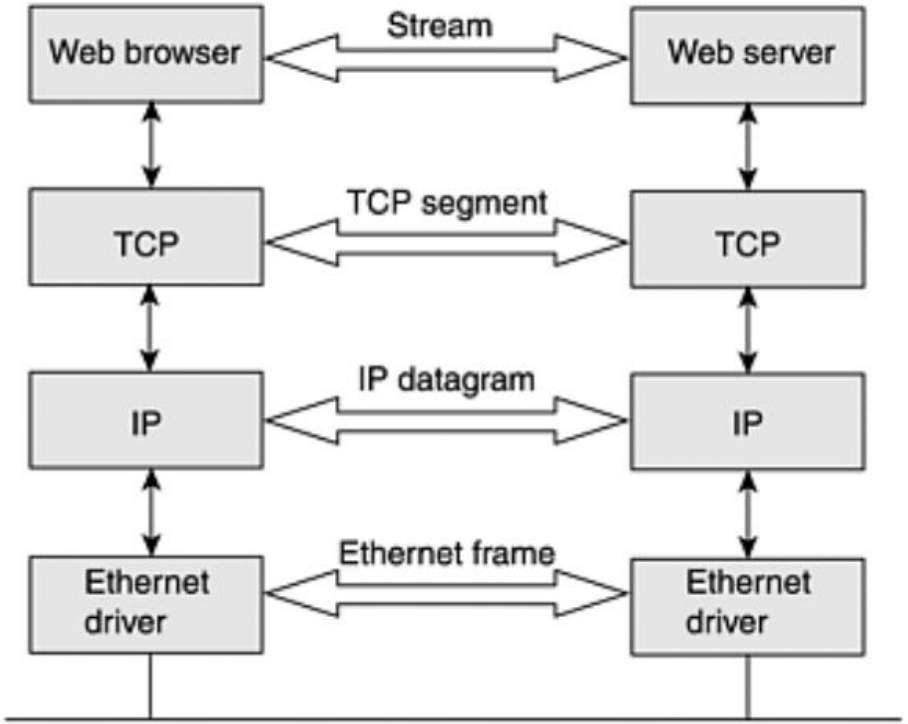
TCP/IP Model

APPLICATION LAYER:
Handles implementation of user applications

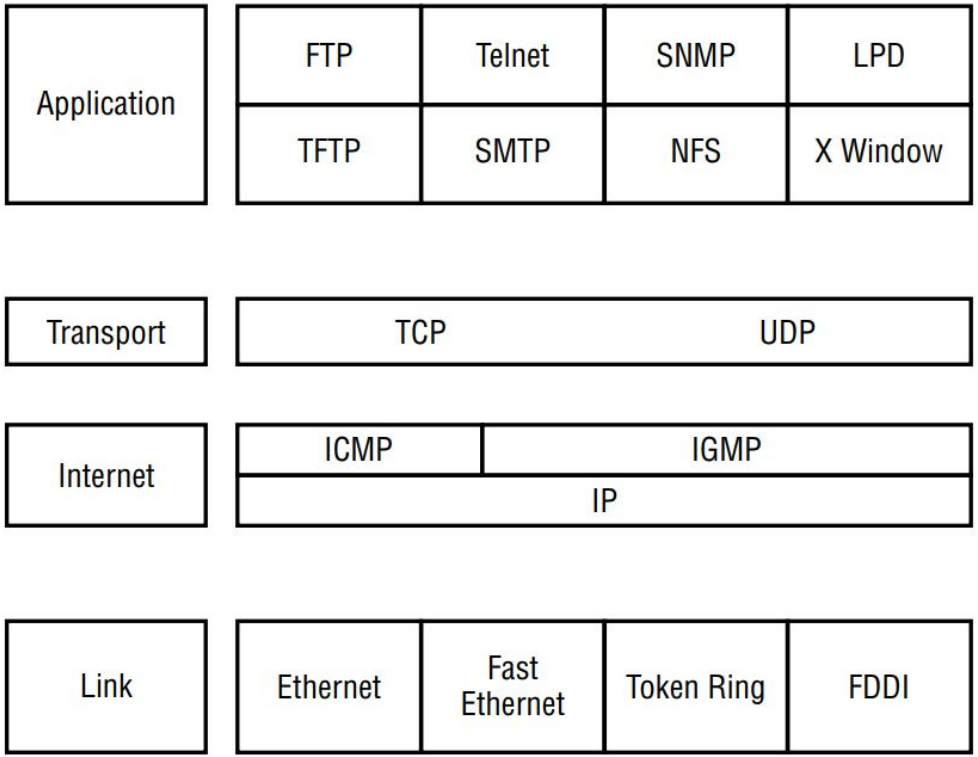
TRANSPORT LAYER:
Manages end-to-end communications between hosts

NETWORK LAYER:
Gets data from source to destination

LINK LAYER:
Manages data transfer to and from physical medium



TCP/IP Model


Application
FTP
Telnet
SNMP
LPD
TFTP
SMTP
NFS
X Window
Transport
TCP
UDP
Internet
ICMP
IGMP
IP
Link
Ethernet
Fast Ethernet
Token Ring
FDDI

TCP/IP: Transport Layer

- The two primary Transport layer protocols of TCP/IP are TCP and UDP.
- TCP connection-oriented protocol, whereas UDP is a connectionless protocol.
- When a communication connection is established between two systems, it is done using ports. TCP and UDP each have 65,536 ports.

Network Ports

- A port (also called a socket) is little more than an address number that both ends of the communication link agree to use when transferring data.
- Ports allow a single IP address to be able to support multiple simultaneous communications, each using a different port number.
- The first 1,024 of these ports (0–1,023) are called the well-known ports or the service ports. This is because they have standardized assignments as to the services they support.

TCP Header

TCP header has a minimum size of 20 bytes and maximum of 60 bytes

Size in Bits	Field
16	Source port
16	Destination port
32	Sequence number
4	Data offset
4	Reserved for future use
8	Flags (see Table 12.2)
16	Window size
16	Checksum
16	Urgent pointer
Variable	Various options; must be a multiple of 32 bits

The TCP header Flag Field Values

Flag Bit Designator	Name	Description
CWR	Congestion Window Reduced	Used to manage transmission over congested links; see RFC 3168
ECE	ECN-Echo (Explicit Congestion Notification)	Used to manage transmission over congested links; see RFC 3168
URG	Urgent	Indicates urgent data
ACK	Acknowledgement	Acknowledges synchronization or shutdown request
PSH	Push	Indicates need to push data immediately to application
RST	Reset	Causes immediate disconnect of TCP session
SYN	Synchronization	Requests synchronization with new sequencing numbers
FIN	Finish	Requests graceful shutdown of TCP session

TCP Handshake

- The three-way handshake process:
  1. The client sends a SYN (synchronize) flagged packet to the server.
  2. The server responds with a SYN/ACK (synchronize and acknowledge) flagged packet back to the client.
  3. The client responds with an ACK (acknowledge) flagged packet back to the server.

UDP Header

- UDP header is relatively simple in comparison with the TCP header. A UDP header is 8 bytes (64 bits) long. This header is divided into four sections, or fields (each 16 bits long):
  - Source port
  - Destination port
  - Message length
  - Checksum

IP Address

- An IP address (version 4) is a 32-bit number that uniquely identifies a host
- IP addresses are normally expressed in dotted decimal format, with four numbers separated by periods, such as **192.168.123.132.**
- An IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address.

IP Classes and Subnets

- These IP addresses are divided into classes. The most common of these classes are classes A, B, and C.
- Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet.

Class	First Binary Digits	Decimal Range of First Octet
A	0	1–126
B	10	128–191
C	110	192–223
D	1110	224–239
E	1111	240–255

IP Classes and Subnet

- In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions.

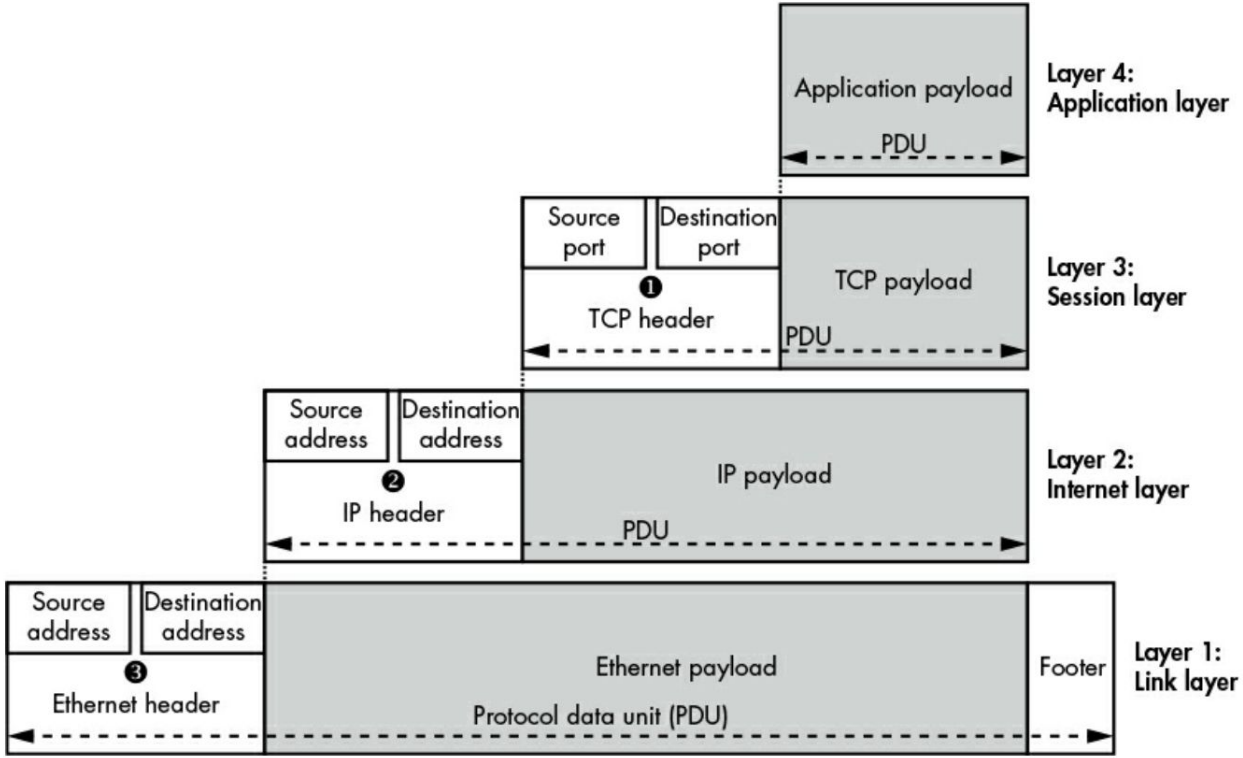
Class	Default Subnet Mask	CIDR Equivalent
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

IP Classes and Subnet

- In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions.

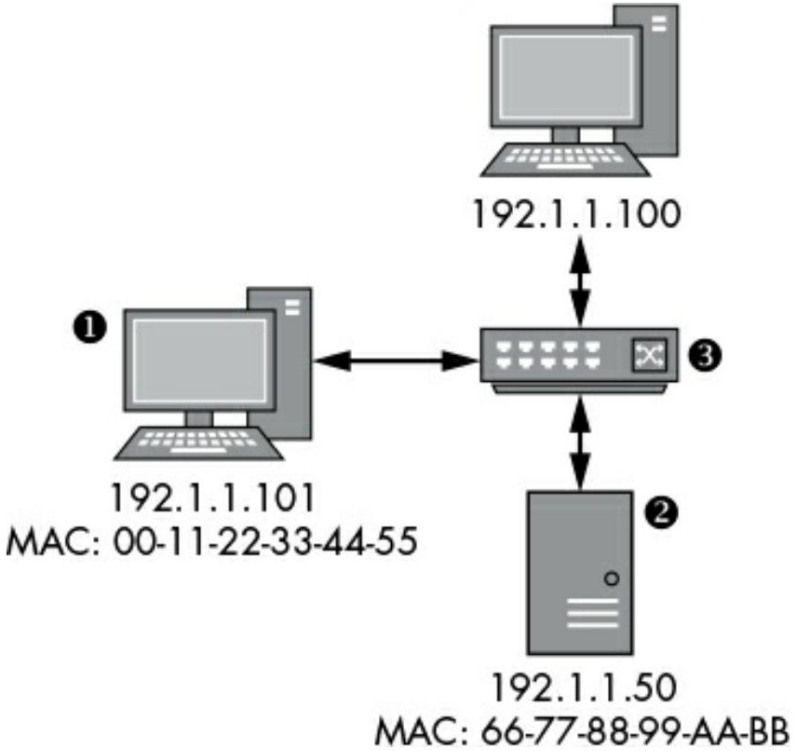
Class	Default Subnet Mask	CIDR Equivalent
A	255.0.0.0	/8
B	255.255.0.0	/16
C	255.255.255.0	/24

TCP/IP Data Encapsulation



Data Transmission & Network Routing

Data Transmission & Networking



Data Transmission

1. The operating system network stack node ❶ encapsulates the application and transport layer data and builds an IP packet with a source address of 192.1.1.101 and a destination address of 192.1.1.50.
2. The operating system can at this point encapsulate the IP data as an Ethernet frame, but it might not know the MAC address of the target node. It can request the MAC address for a particular IP address using the Address Resolution Protocol (ARP), which sends a request to all nodes on the network to find the MAC address for the destination IP address.

Data Transmission

1. Once the node at ❶ receives an ARP response, it can build the frame, setting the source address to the local MAC address of 00-11-22-33-44-55 and the destination address to 66-77-88-99-AA-BB. The new frame is transmitted on the network and is received by the switch ❸.
2. The switch forwards the frame to the destination node, which unpacks the IP packet and verifies that the destination IP address matches. Then the IP payload data is extracted and passes up the stack to be received by the waiting application.

Network Layer and IP Networking

- IP provides route addressing for data packets.
- It is this route addressing that is the foundation of global Internet communications
- IP is connectionless and is an unreliable datagram service.
- IP does not offer guarantees that packets will be delivered or that packets will be delivered in the correct order, and it does not guarantee that packets will be delivered only once.

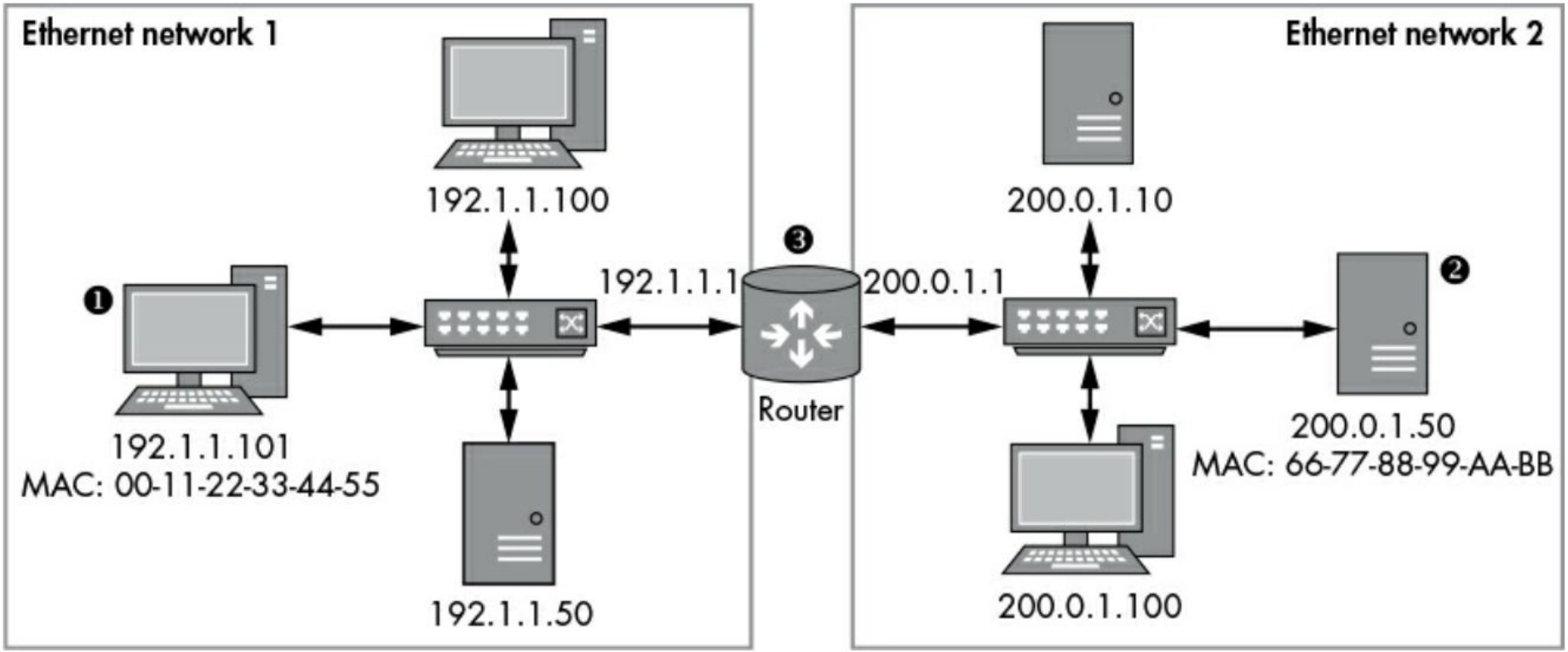
Network Layer and IP Networking

- IP provides route addressing for data packets.
- It is this route addressing that is the foundation of global Internet communications
- IP is connectionless and is an unreliable datagram service.
- IP does not offer guarantees that packets will be delivered or that packets will be delivered in the correct order, and it does not guarantee that packets will be delivered only once.

Routing

- The routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined.
- Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network.
- After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

Network Routing



Network Routing

1. The operating system network stack node ❶ encapsulates the application and transport layer data, and it builds an IP packet with a source address of 192.1.1.101 and a destination address of 200.0.1.50.
2. The network stack needs to send an Ethernet frame, but because the destination IP address does not exist on any Ethernet network that the node is connected to, the network stack consults its operating system routing table. In this example, the routing table contains an entry for the IP address 200.0.1.50. The entry indicates that a router ❸ on IP address 192.1.1.1 knows how to get to that destination address.

Network Routing

1. The operating system uses ARP to look up the router's MAC address at 192.1.1.1, and the original IP packet is encapsulated within the Ethernet frame with that MAC address.
2. The router receives the Ethernet frame and unpacks the IP packet. When the router checks the destination IP address, it determines that the IP packet is not destined for the router but for a different node on another connected network. The router looks up the MAC address of 200.0.1.50, encapsulates the original IP packet into the new Ethernet frame, and sends it on to network 2.
3. The destination node receives the Ethernet frame, unpacks the IP packet, and processes its contents.

Summary

In this class we covered:

- Computer Networks
- Network Protocols Models (OSI and TCP/IP)
- Basic Data Transmission and Routing

What is Next?

In our next Class we will focus on:

- Network Security Concepts.
- TCP/IP network attacks, mainly, scanning attacks, spoofing attacks, and denial of services.