Datacom

Day 1

Naveen K Lakshman
Email: naveen.k.ipv6@gmail.com

Network Fundamentals

- Models and Protocols
- OSI and TCP/IP Model
- Understand the Seven Layers of the OSI Reference Model and their functions
- Understand the TCP/IP protocol suite and its layers
- Compare and contrast the OSI & TCP/IP models in terms of their layer structures and functionalities
- TCP/UDP Protocols
- Understand the characteristics and functionalities of TCP and UDP
- Compare and contrast TCP and UDP in terms of reliability,
- Connection-oriented vs. connectionless communication, and use cases

Hands-On:

- Visually understand how data is handled and transmitted over TCP and UDP.
- Capture packets during a TCP file transfer and a UDP stream.
- Analyze how packets are formed, managed, and transported.

- IPv4/IPv6 Addressing and Subnetting, Configure, verify, and troubleshoot IPv4 addressing and subnetting
- Understand IPv4 address classes, subnetting, and subnet masks
- Implement and troubleshoot IPv4 addressing schemes for LANs and WANs
- Identify the appropriate IPv6 addressing scheme to satisfy addressing requirements in a LAN/WAN environment
- Understand IPv6 addressing types, address allocation, and subnetting
- Configure and troubleshoot IPv6 addressing on network devices
- IPv4 Address Types, Understand different types of IPv4 addresses, unicast, broadcast, multicast addresses
- Discuss the purposes and use cases of each IPv4 address type, Private IPv4 Addressing
- Describe the need for private IPv4 addressing in enterprise networks
- Discuss the advantages and limitations of using private IPv4 addresses

Hands-On:

- Understand how to assign IPv4 addresses to network devices.
- Use a network simulator to set up a small network. Assign static IP addresses to each device, ensuring they are on the same subnet. Verify the connectivity using the ping command.
- Given an IPv4 address and a requirement for a number of subnets, calculate the appropriate subnet mask and determine the range of addresses for each subnet.
- Assign static IPv6 addresses to each device, verify connectivity using the ping6 command.
- Using a network simulator, configure network devices to support both IPv4 and IPv6 addressing.

(SDO) Standards Organization

IEEE (Institute of Electrical & Electronics Engineers)

– LAN, Wireless LAN, IoT Standards

www.ieee.org

IETF (Internet Engineering Task Force)

– Internet Protocols: TCP, UDP, QUIC, IP, IPv6, ICMP, ICMPv6

– IPv4 Routing Protocols: RIP, EIGRP, OSPF, ISIS, BGP

– IPv6 Routing: RIPng, EIGRPv6, OSPFv3, ISIS v6, MP-BGP

www.ietf.org

ITU (International Telecommunications Union)

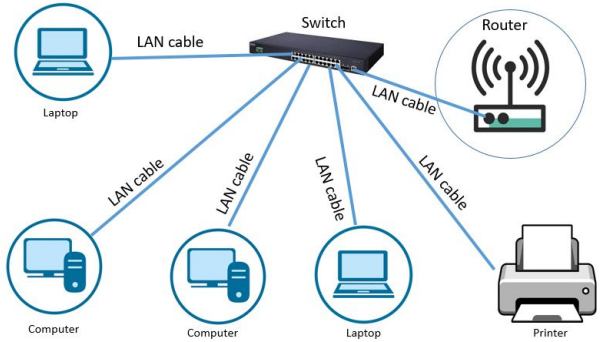
– Telecom standards, Signaling, Spectrum, SS7, MPLS.

www.itu.int

Networking and its types

Local Area Networks (LANs)

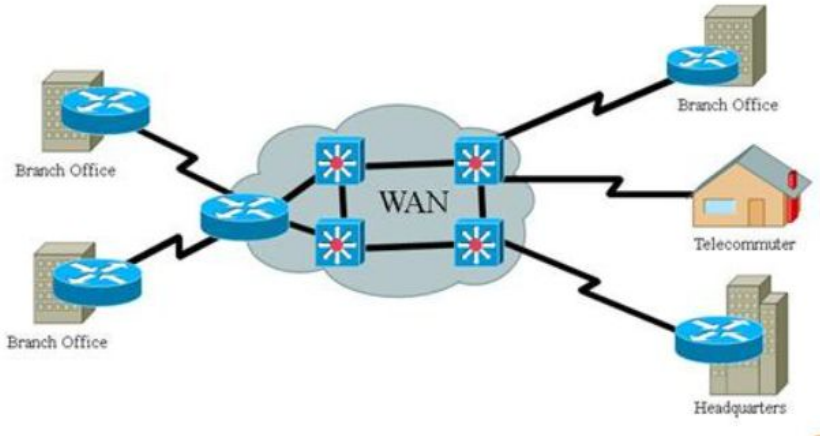
- LANs connect groups of computers devices together across short distances (within a building) to share information and resources.
- A LAN comprises cables, access points, switches, routers, and other components that enable devices to connect to internal servers, web servers, and other LANs via wide area networks.



Local Area Network

Wide Area Network (WAN)

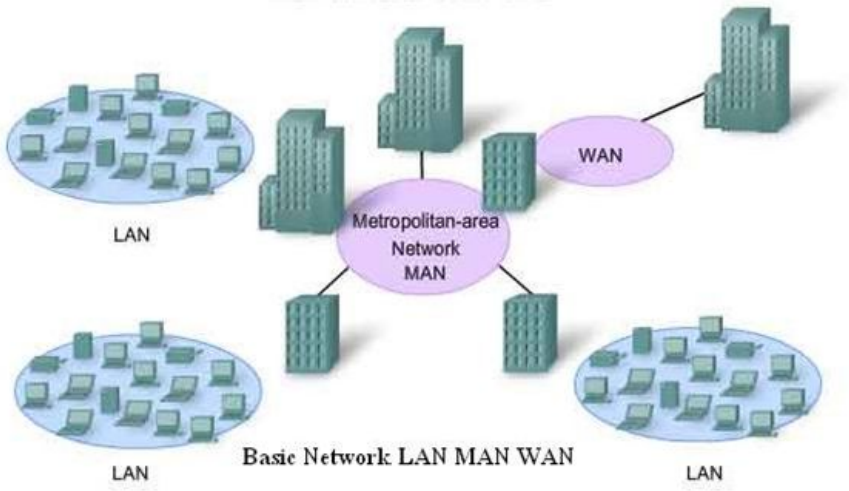
- WAN connects computers together across longer physical distances.
- This allows computers to be remotely connected to each other over one large network to communicate even when they’re miles apart.
- The Internet is the most basic example of a WAN, connecting all computers together around the world.



Metropolitan Area Network (MAN)

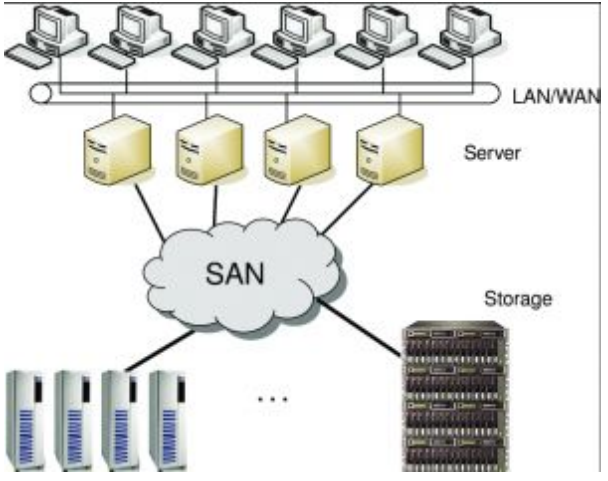
- These types of networks are larger than LANs but smaller than WANs – and incorporate elements from both types of networks.
- MANs span an entire geographic area (typically a town or city, but sometimes a campus).

  eg. Metro Ethernet



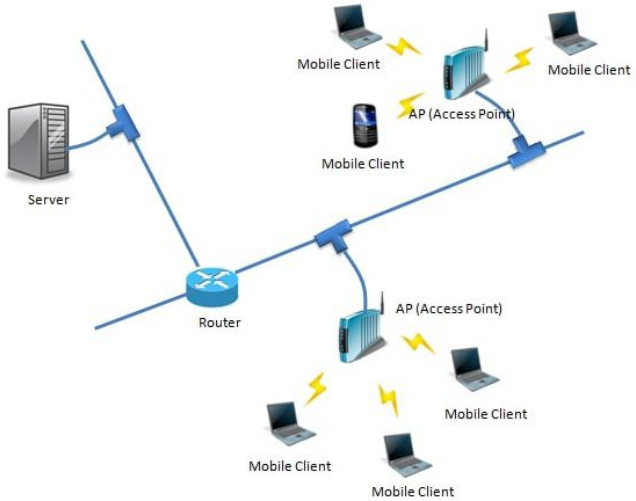
Storage Area Networks (SAN)

- As a dedicated high-speed network that connects shared pools of storage devices to several servers, these types of networks don’t rely on a LAN or WAN.
- Instead, they move storage resources away from the network and place them into their own high-performance network.
- SANs can be accessed in the same fashion as a drive attached to a server.



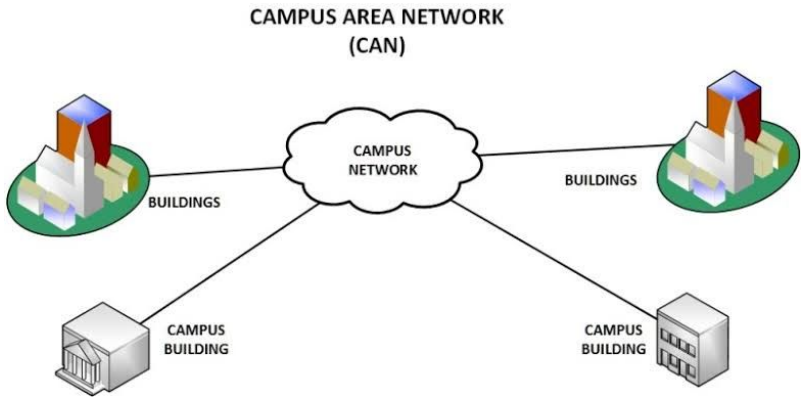
Wireless Local Area Network (WLAN)

- Functioning like a LAN, WLANs make use of wireless network technology, such as Wi-Fi.
- Typically seen in the same types of applications as LANs, these types of networks don’t require that devices rely on physical cables to connect to the network.



Campus Area Networks (CAN)

- Larger than LANs, but smaller than metropolitan area networks (MANs), these types of networks are typically seen in universities, colleges or schools.
- They can be spread across several buildings that are fairly close to each other so users can share resources.



Personal Area Network (PAN)

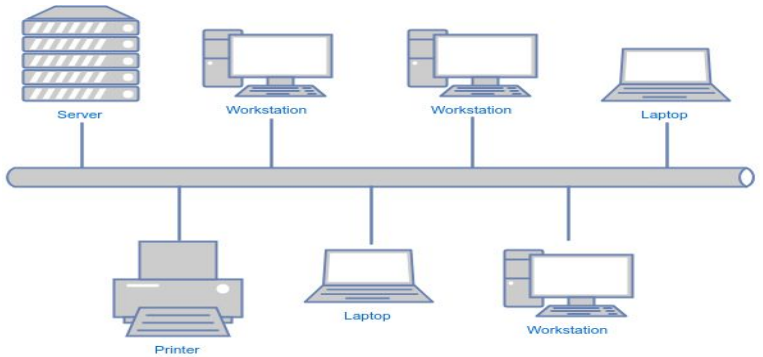
- The smallest and most basic type of network, a PAN is made up of a wireless modem, a computer or two, phones, printers, tablets, etc., and revolves around one person in one building.
- These types of networks are typically found in small offices or residences, and are managed by one person or organization from a single device.

Network Topology

- Network topology refers to the manner in which the links and nodes of a network are arranged to relate to each other.
- Topologies are categorized as either physical network topology, which is the physical signal transmission medium, or logical network topology, which refers to the manner in which data travels through the network between devices, independent of physical connection of the devices.

Bus Topology

- In bus network topology, every node is connected in series along a single cable.
- This arrangement is found today primarily in cable broadband distribution networks.

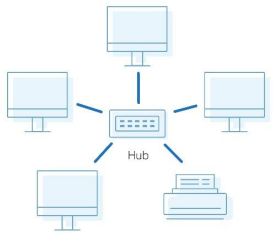


Bus Topology Network

Star Topology (Normal LAN)

- In star topology, is laid out so every node in the network is directly connected to one central hub via coaxial, twisted-pair, or fiber-optic cable.

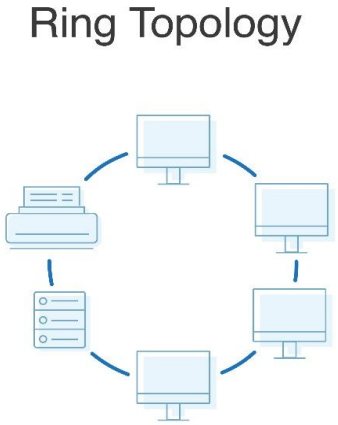
Star Topology



Ring Topology

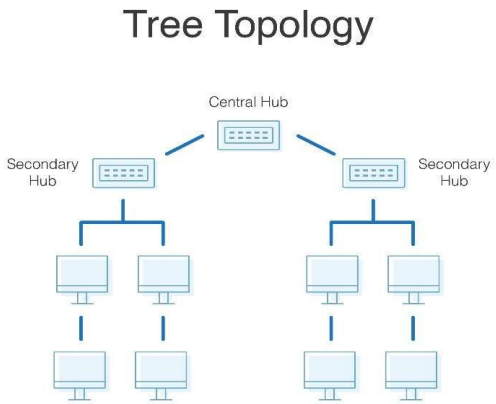
- Ring topology is where nodes are arranged in a circle (or ring).
- The data can travel through the ring network in either one direction or both directions, with each device having exactly two neighbors.

IBM Token Ring



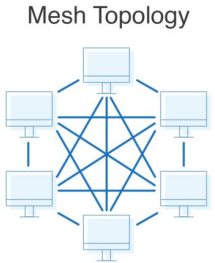
Tree Topology (modern LAN)

- The tree topology structure gets its name from how the central node functions as a sort of trunk for the network, with nodes extending outward in a branch-like fashion.
- A tree topology has a parent-child hierarchy to how the nodes are connected.



Mesh Topology

- A mesh topology is an intricate and elaborate structure of point-to-point connections where the nodes are interconnected.
- Mesh networks can be full or partial mesh.
- Partial mesh topologies are mostly interconnected, with a few nodes with only two or three connections, while full-mesh topologies are fully interconnected.

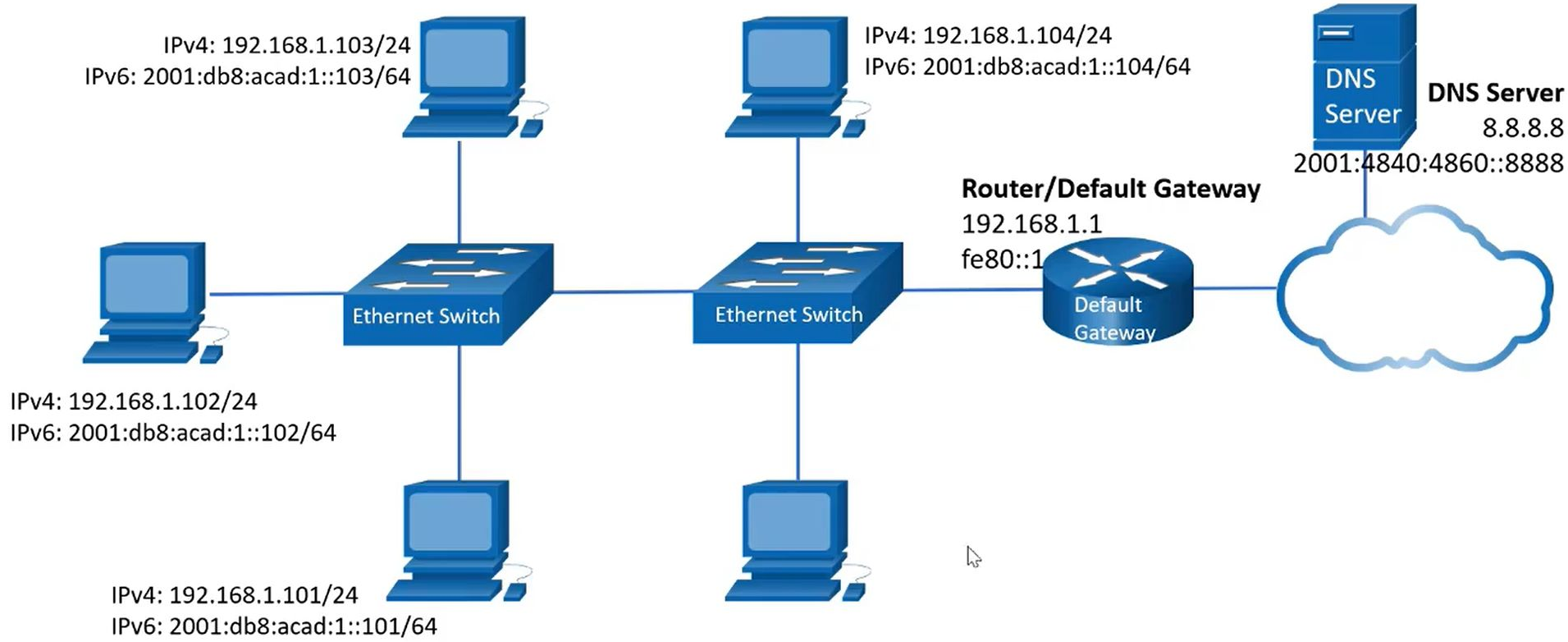


Network Reference Models

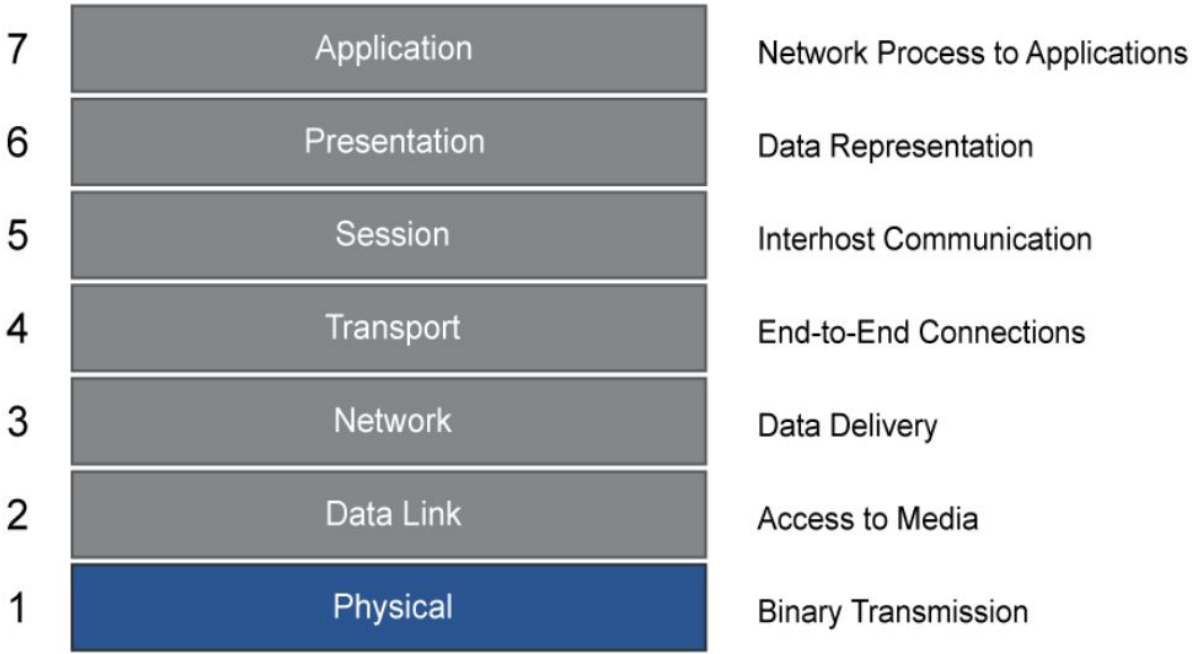
- A computer network connects two or more devices together to share information and services. Multiple networks connected together form an internetwork.
- Internetworking present challenges - **interoperating** between products from different manufacturers requires consistent standards.
- Network reference models were developed to address these challenges.
- It serves as a blueprint, detailing how communication between network devices should occur.
    - OSI (Open Systems Interconnection) Reference Model
    - TCP/IP Model

- Without the framework that network models provide, all network hardware and software would have been proprietary.
- Organizations would have been locked into a single vendor’s equipment, and global networks like the
- Internet would have been impractical, if not impossible.
- **Network models are organized into layers, with each layer representing a specific networking function.**
- **These functions are controlled by protocols, which are rules that govern end-to-end communication between devices**

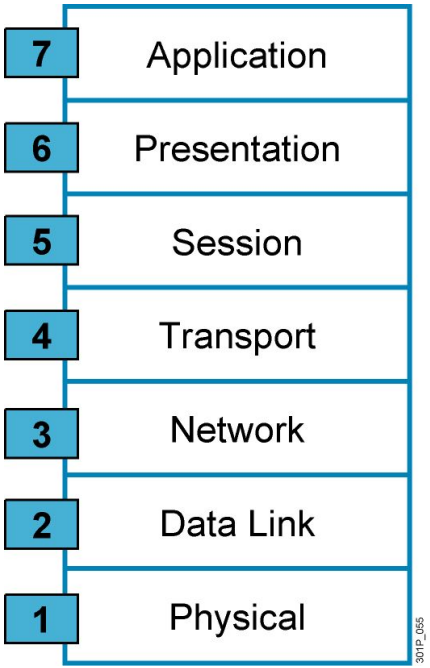
How we "see" the network



OSI Reference Model

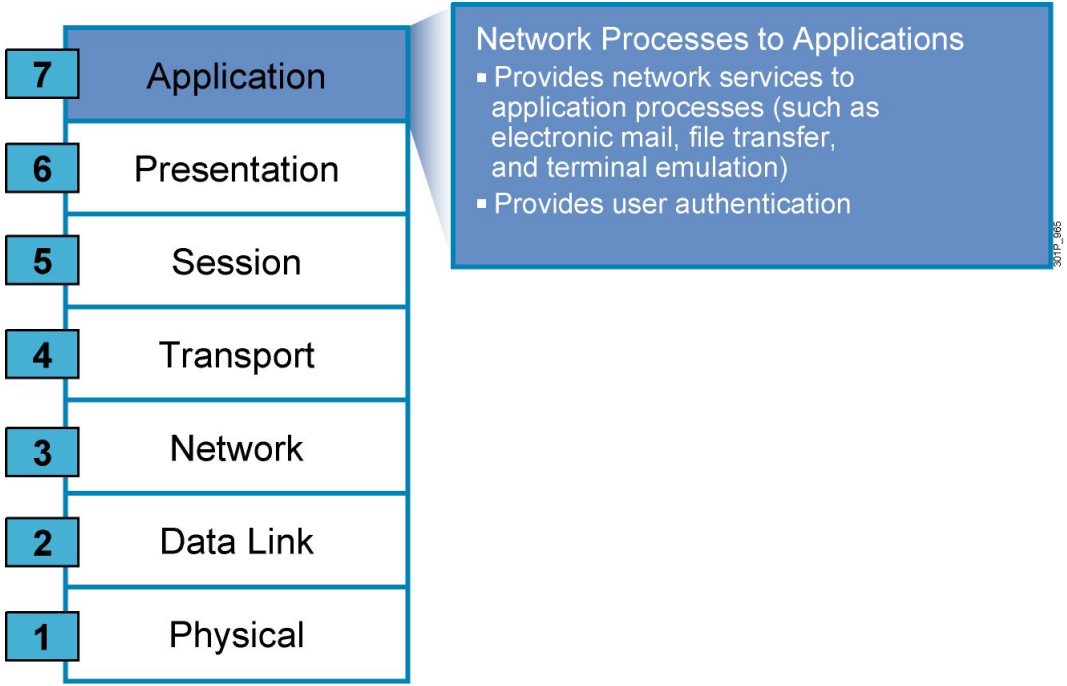


OSI | Why a Layered Network Model?



- Reduces complexity
- Standardized interfaces
- Facilitates modular engineering
- Ensures interoperability of technology
- Accelerates evolution
- Simplifies teaching & learning

OSI | Layer 7: Application Layer

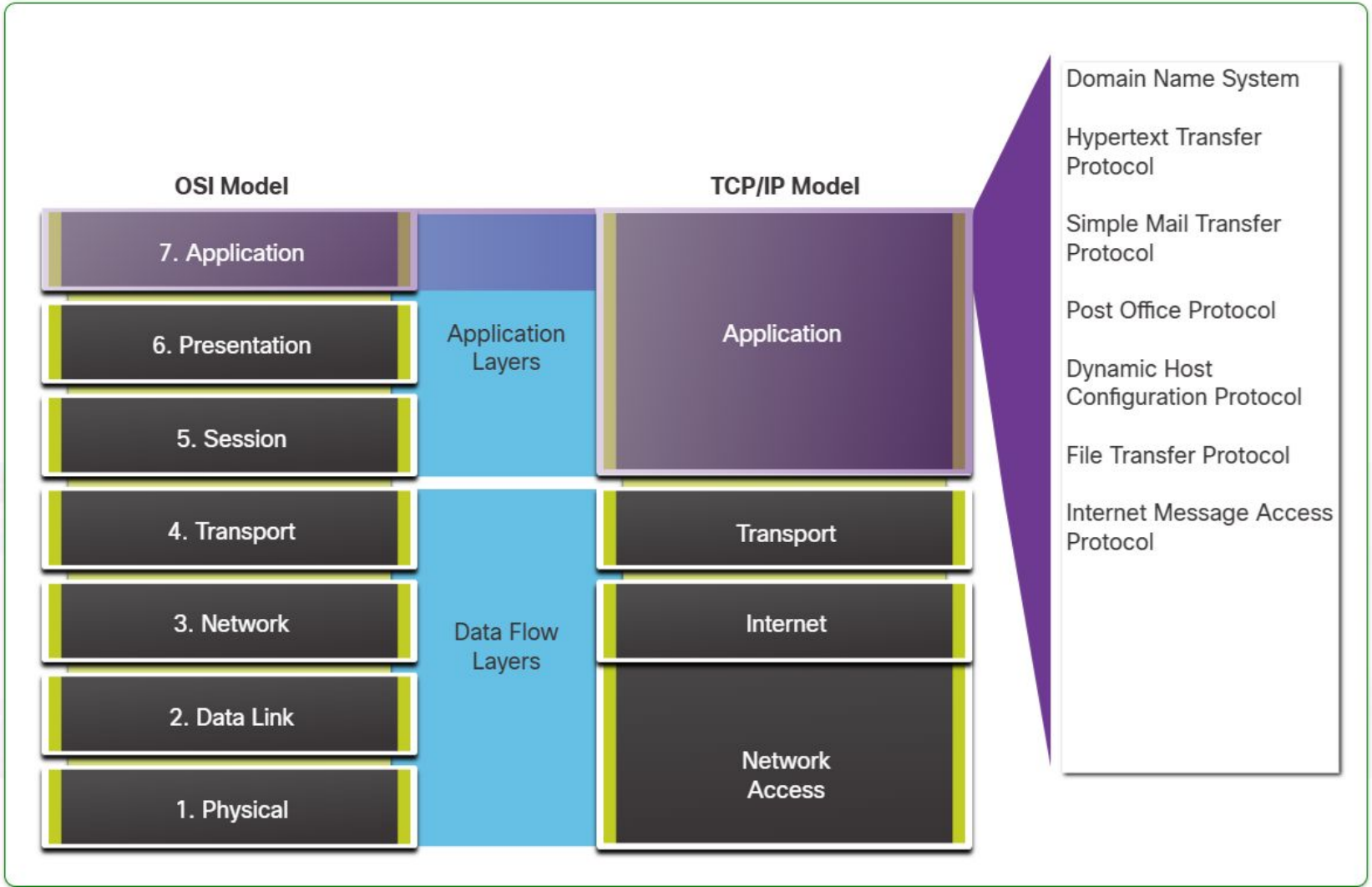


- The Application layer (Layer-7) provides the interface between the user application and the network.
- A web browser & email client are examples of user application.
- The user application itself does not reside at the Application layer - the protocol does.
- The user interacts with the application, which in turn interacts with the application protocol.

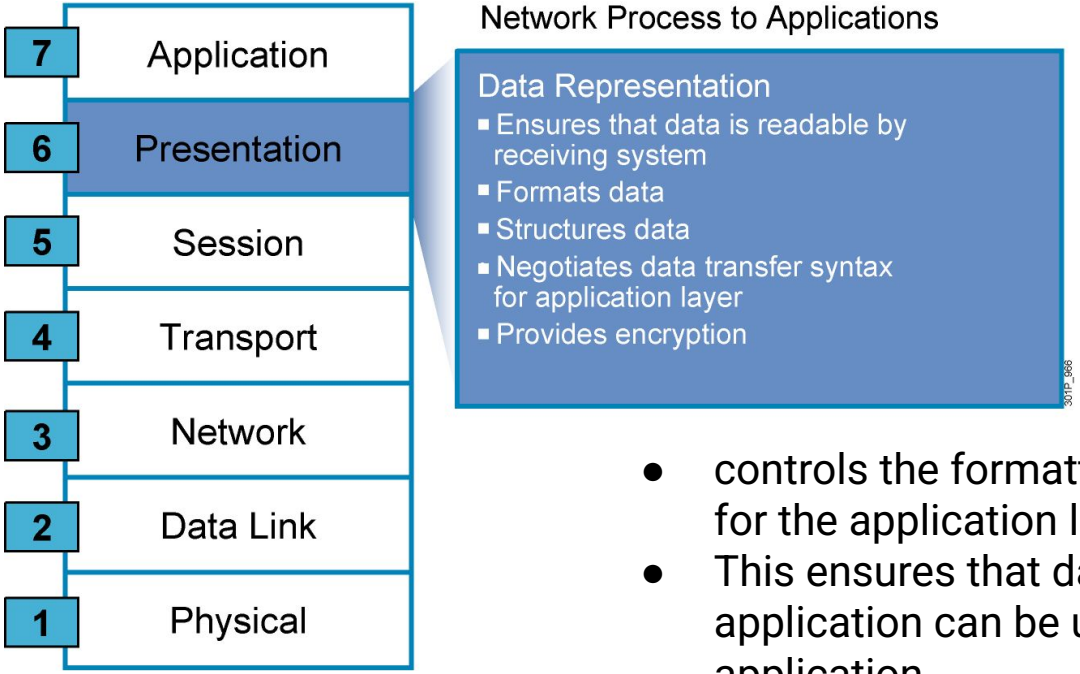
Examples of Application layer protocols include:

- FTP, via an FTP client
- HTTP, via a web browser
- POP3 and SMTP, via an email client
- Telnet

Application layer interacts with the Presentation layer below it

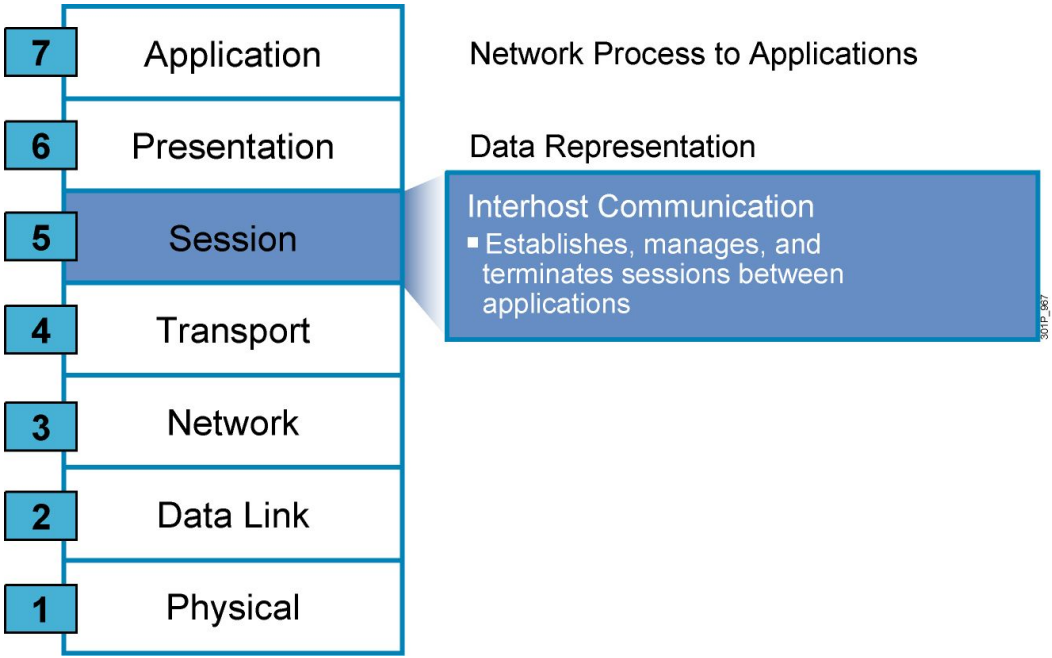

OSI Model
TCP/IP Model
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical
Application Layers
Data Flow Layers
Application
Transport
Internet
Network Access
Domain Name System
Hypertext Transfer Protocol
Simple Mail Transfer Protocol
Post Office Protocol
Dynamic Host Configuration Protocol
File Transfer Protocol
Internet Message Access Protocol

OSI | Layer 6: Presentation Layer



- controls the formatting and syntax of user data for the application layer.
- This ensures that data from the sending application can be understood by the receiving application.

OSI | Layer 5: Session Layer



- Session layer is responsible for establishing, maintaining, and ultimately terminating sessions between devices.
- If a session is broken, this layer can attempt to recover the session.

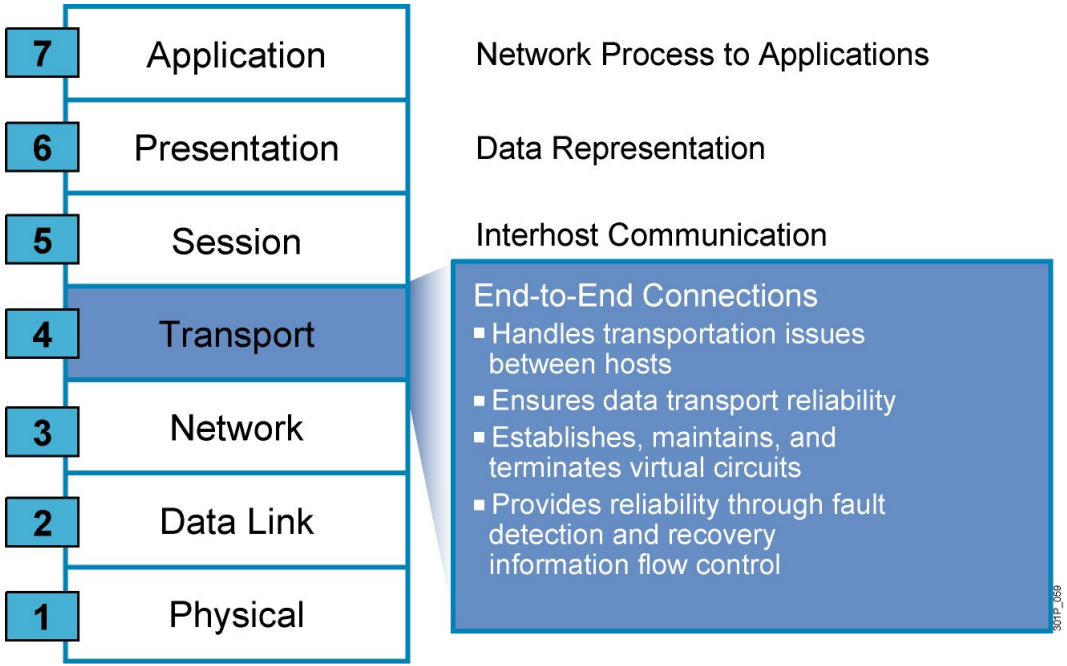
Sessions communication falls under one of three categories:

  - Full-Duplex – simultaneous two-way communication
  - Half-Duplex – two-way communication, but not simultaneous
  - Simplex – one-way communication

- Many modern protocol suites, such as TCP/IP, do not implement Session layer protocols.
- Connection management is often controlled by lower layers,

  such as the Transport layer

OSI | Layer 4: Transport Layer



- The Transport layer (Layer-4) does not actually send data, despite its name.
- Instead, this layer is responsible for the reliable transfer of data, by ensuring that data arrives at its destination error-free and in order.

Transport layer communication falls under two categories:

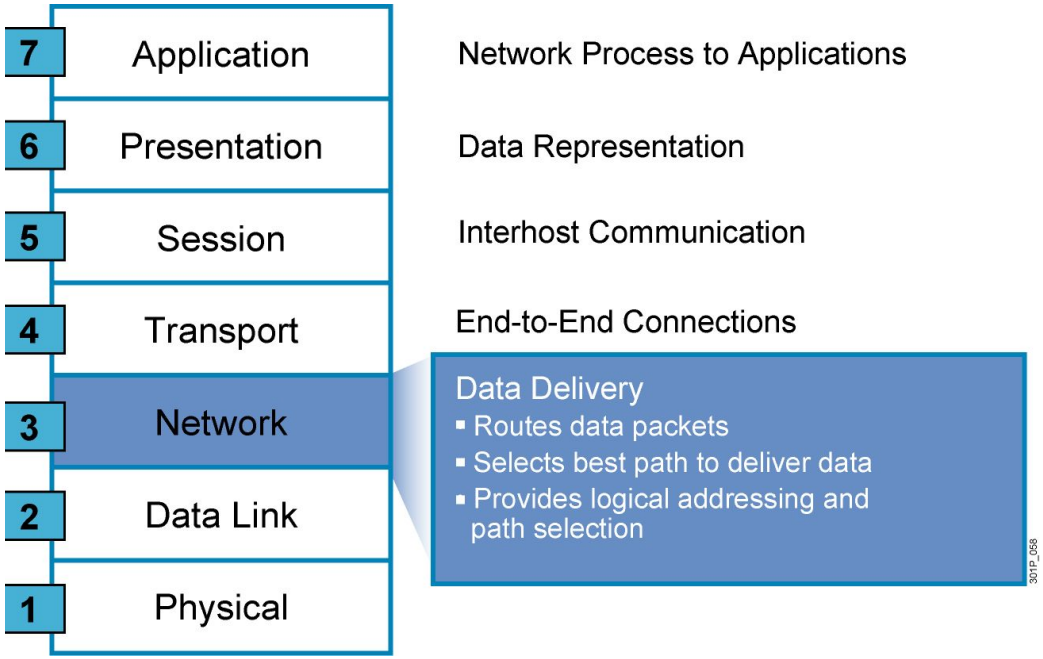
- **Connection-oriented** – requires that a connection with specific agreed-upon parameters be established before data is sent.
  - eg. TCP (Transmission Control Protocol)
- **Connectionless** – requires no connection before data is sent.
  - e.g UDP (User Datagram Protocol)

Transport Layer protocol features

Connection-oriented protocols provide several important services:

- **Connection establishment** – connections are established, maintained, and ultimately terminated between devices.
- **Segmentation and sequencing** – data is segmented into smaller pieces for transport. Each segment is assigned a sequence number, so that the receiving device can reassemble the data on arrival.
- **Acknowledgments** – receipt of data is confirmed through the use of acknowledgments. If a segment is lost, data can be retransmitted to guarantee delivery
- **Flow control (or windowing)** – data transfer rate is negotiated to prevent congestion.

OSI | Layer 3: Network Layer

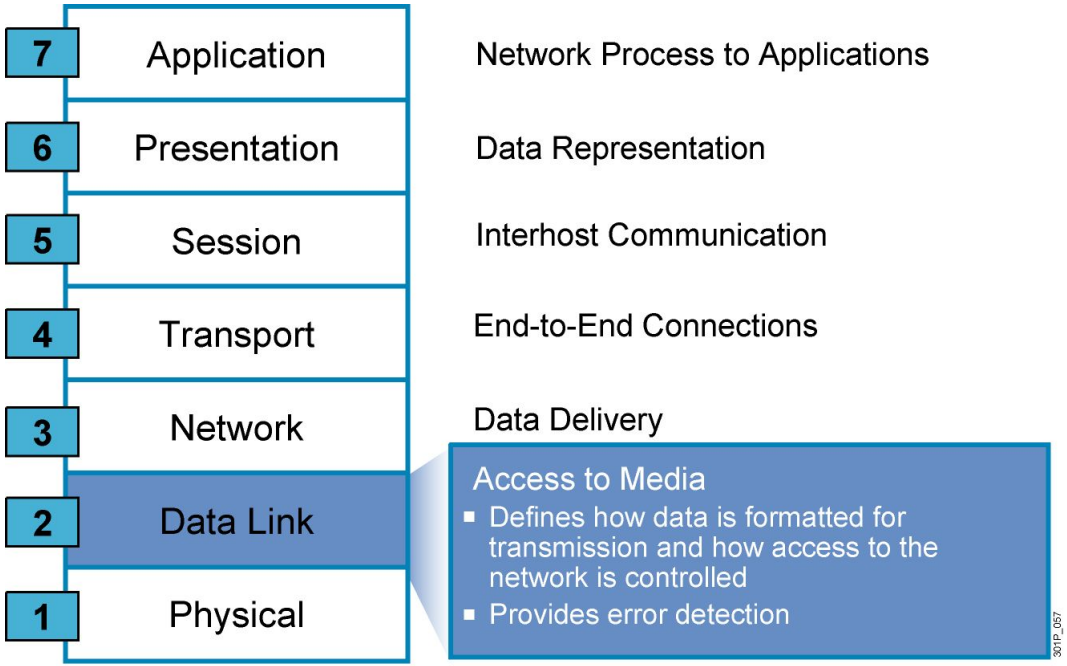


The Network layer (Layer-3) controls internetwork communication, and has two key responsibilities:

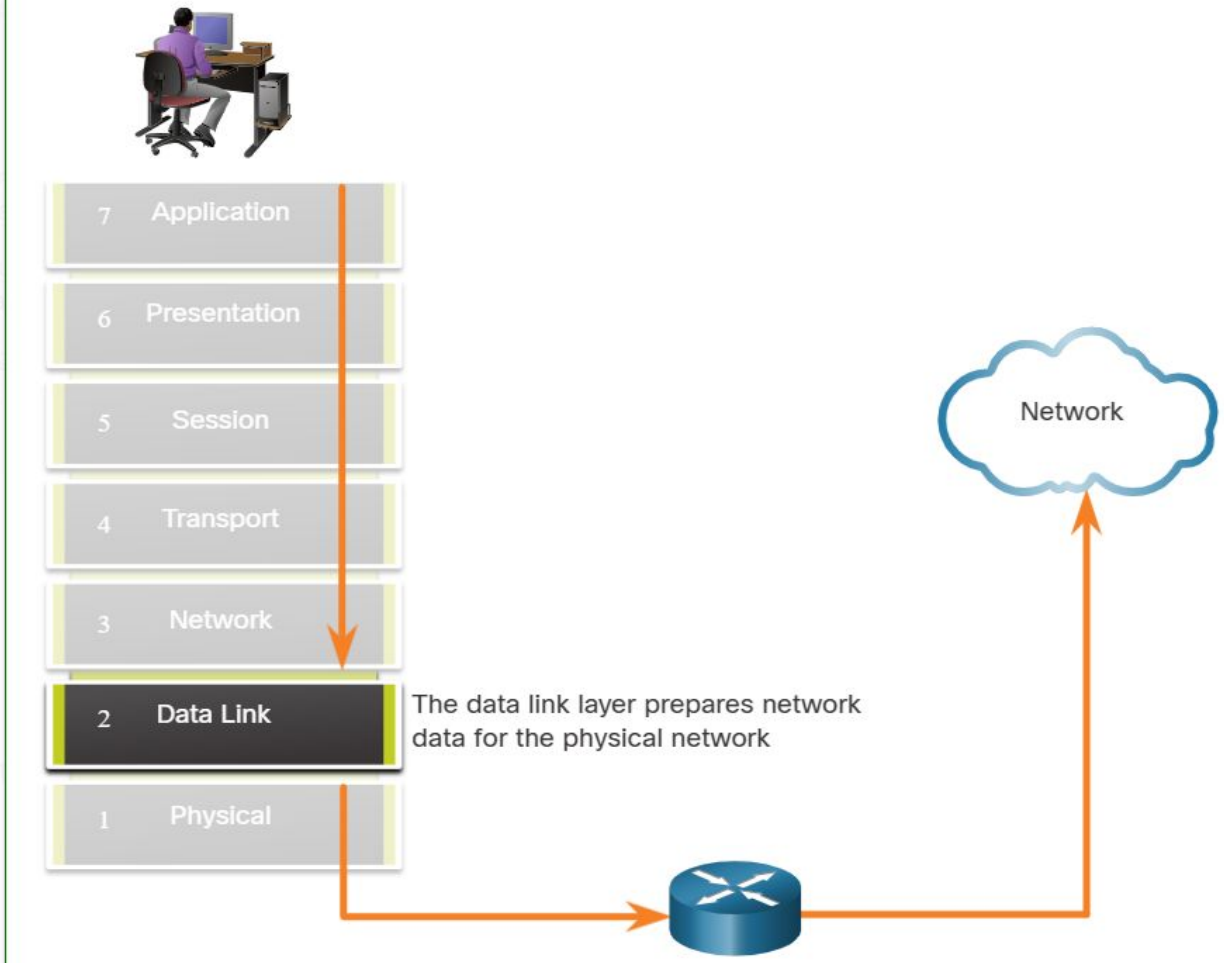
- Logical addressing – provides a unique address that identifies both the host, and the network that host exists on.
- Routing – determines the best path to a particular destination network, and then routes data accordingly

  - IPv4, IPv6
  - Novell’s Internetwork Packet Exchange (IPX).

OSI | Layer 2: DataLink Layer



- Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
- Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
- Controls how data is placed and received on the media.
- Exchanges frames between endpoints over the network media.
- Receives encapsulated data, usually Layer 3 packets, and directs them to the proper upper-layer protocol.
- Performs error detection and rejects any corrupt frame.


7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
The data link layer prepares network data for the physical network
Network

Data link layer

- It plays a crucial role in ensuring reliable communication between two directly connected devices over a physical medium.
- The primary function of the Data Link Layer is to organize data into frames and to handle error detection and correction that may occur at the physical layer.

Key Functions of the Data Link Layer:

Framing:

- It breaks down the data from the Network Layer into smaller, manageable chunks called frames.
- Frames include the data to be transmitted, as well as control information (such as addresses and error-checking codes).

Addressing:

- The Data provides physical addressing through MAC (Media Access Control) addresses, which uniquely identify devices on a network (e.g., Ethernet or Wi-Fi devices).

Error Detection and Correction:

- The Data Link Layer is responsible for detecting and, in some cases, correcting errors that occur during data transmission (e.g., through checksums or CRC (Cyclic Redundancy Check)).

Flow Control:

- It manages the rate of data transmission to ensure that the receiver isn't overwhelmed by a faster sender.

Media Access Control:

- It handles access to the shared physical medium. For instance, in Ethernet networks, it determines when a device can transmit data to avoid collisions (using methods like CSMA/CD).

Sub-layers of the Data Link Layer:

The Data Link Layer is typically divided into two sublayers:

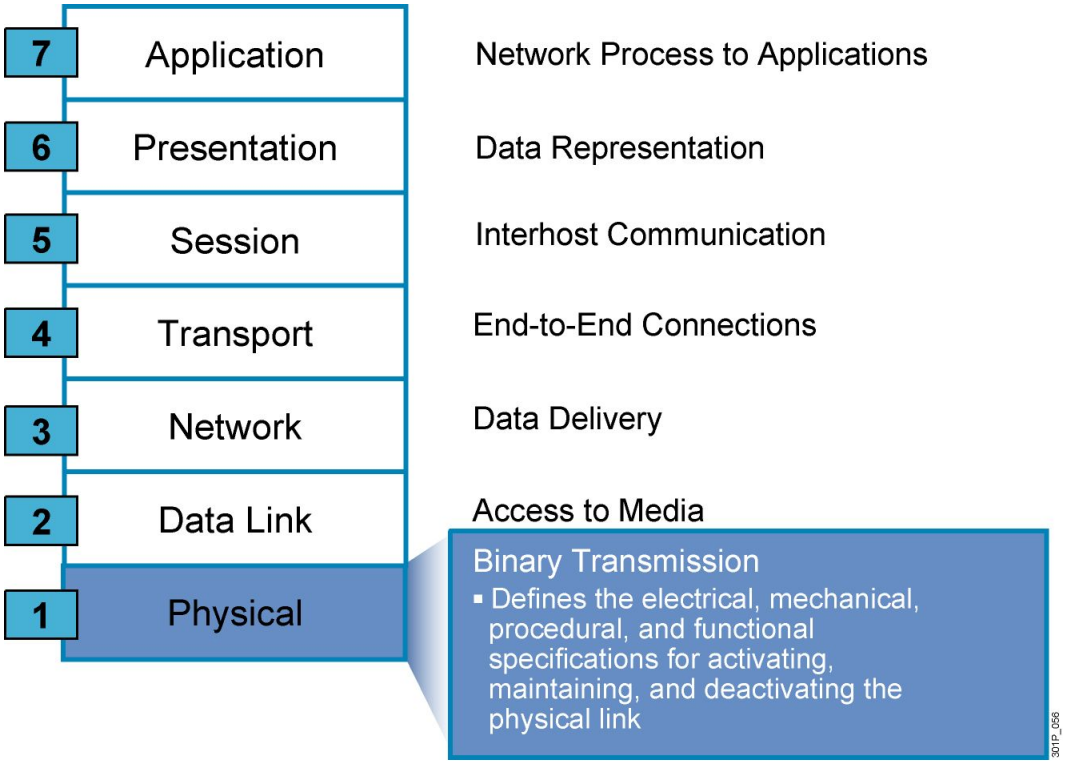
1. **MAC (Media Access Control)**:
    - Manages access to the physical medium and defines how devices on the network can share and take turns using the communication channel.
    - Handles MAC addressing, determining which device gets to transmit data and when.

2. LLC (Logical Link Control):

- Provides error and flow control and ensures data integrity by communicating with the Network Layer.
- It also handles communication between different types of networks (like Ethernet, Wi-Fi, etc.), abstracting them for upper layers.

Protocols that work in Data link Layer:
Ethernet, Frame Relay, X.25, PPP, HDLC, Wi-Fi (IEEE 802.11), ATM, FDDI, CDDI, BlueTooth

OSI | Layer 1: Physical Layer



- Physical Layer is responsible for the actual transmission of raw data over a physical medium, such as cables or wireless channels.
- This layer deals with the electrical, mechanical, and procedural aspects of data transmission.

Key Functions of the Physical Layer:

1. **Transmission of Raw Bits**:
    - The Physical Layer is responsible for converting the data into electrical, optical, or radio signals that can travel across the transmission medium (e.g., copper wires, fiber-optic cables, or air in the case of wireless communication).
    - It transmits **raw binary data (0s and 1s)** over a physical medium without any interpretation of the data's meaning.

2. Defines Physical Medium:

- Specifies the hardware devices and materials used to transfer data (e.g., cables, connectors, wireless signals).
- It ensures the appropriate type of medium is used for the desired transmission distance and speed.

3. Signal Encoding and Decoding:

- Defines how bits are represented in the form of signals, and ensures that the transmission medium properly carries the data signals.
- This includes defining how digital data is encoded into physical signals (e.g., voltage levels, light pulses, or radio waves).

4. **Bit Rate Control**:

- The Physical Layer establishes the bit rate (the number of bits transmitted per second) that can be supported by the medium, which directly impacts the speed of communication.

5. **Synchronization**:

- It provides synchronization between the sender and receiver by ensuring that both sides understand when a bit starts and ends. This is done by using clocking mechanisms.

6. **Physical Topology**:

- defines the physical layout of the network (topology), such as star, ring, or bus.

7. **Error Detection**:

- Although error detection is more typically associated with higher layers (e.g., the Data Link Layer), the Physical Layer can also play a role by detecting physical issues like signal degradation or interference.

Types of physical media

Copper Cables, Fiber Optic Cables, Radio Waves, IR

Client / Server Model (Point to Point) - Single point of failure.
P2P

Switch is used for connecting multiple devices, Switches forwards frames based on the destination MAC address.
Routers forwards IP packets based on Destination IP address.

Switch(config)#ip routing

Switch(config)#int fa0/2
Switch(config-if)#no switchport —-becomes routed port.

What are the 3 main addresses in your network.

IPv4 Address - 32 bits, decimal
IPv6 Address - 128 bits, hexadecimal
MAC Address - 48 bits, Hexadecimal

Encapsulation & Layered Communication

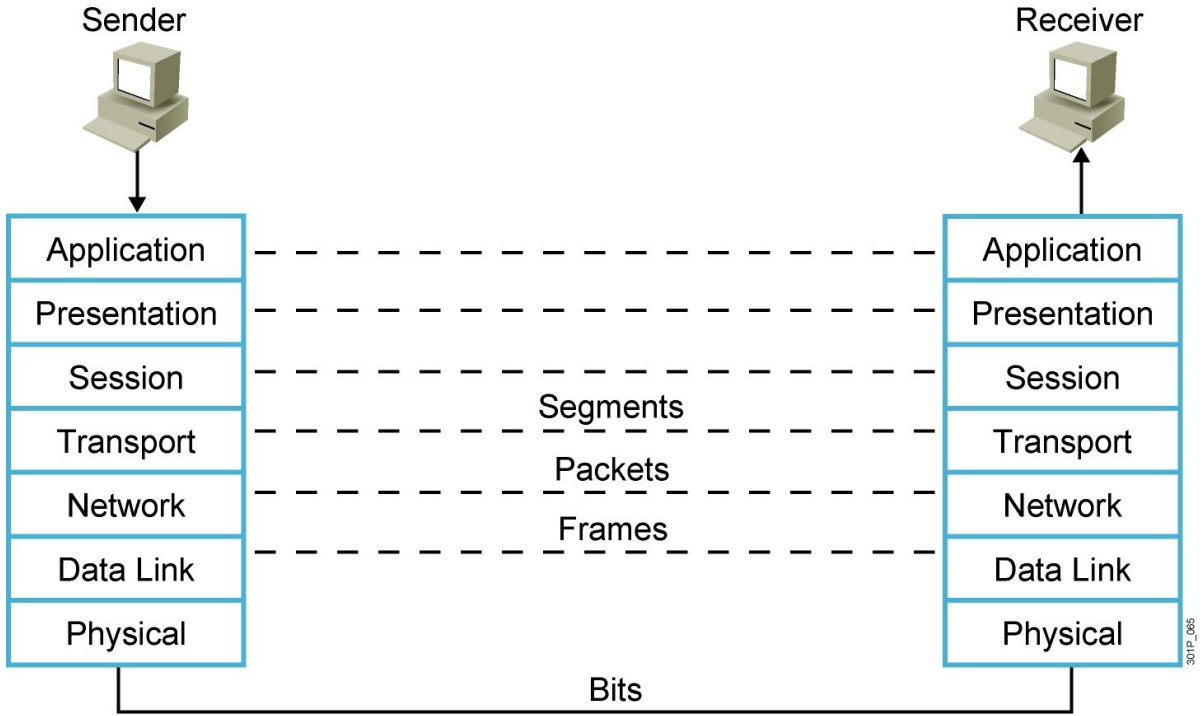
- As data is passed from the user application down the virtual layers of the OSI model, each layer adds a header (and sometimes a trailer) containing protocol information specific to that layer.
- These headers are called Protocol Data Units (PDUs), and the process of adding these headers is called encapsulation.
- In the TCP/IP protocol suite only the lower layers perform encapsulation, generally. (Transport - Network - Data Link - Physical)

- Transport layer protocol such as TCP will add a header containing flow control, port numbers, and sequencing.
- The Network layer header contains logical addressing information.
- The Data-link header contains physical addressing and other hardware specific information.

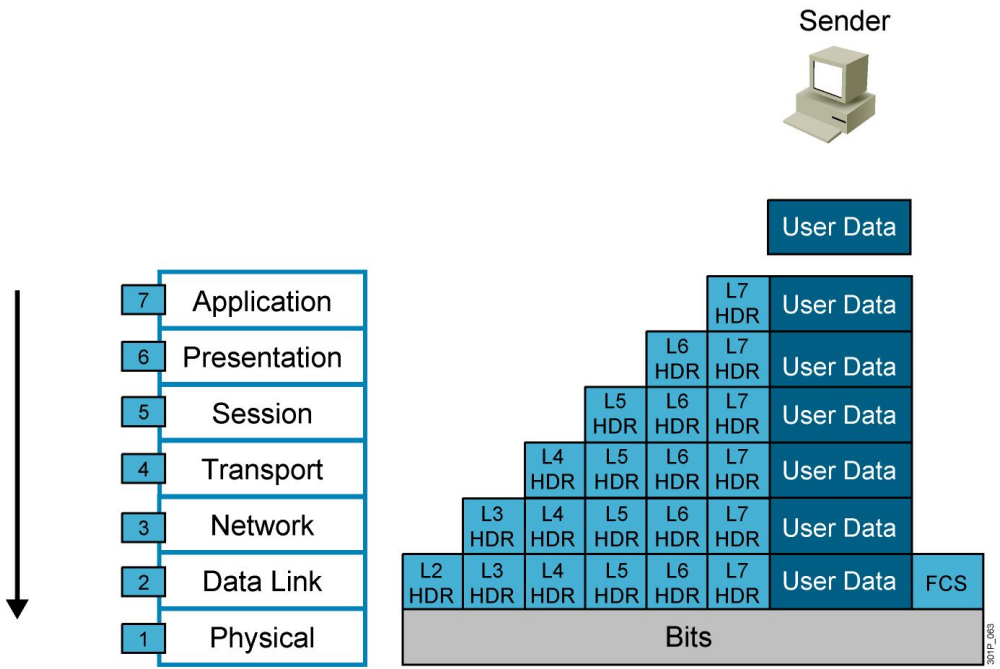
PDU (Protocol Data Unit) Names of the Layers of the OSI Model

OSI Model Layers	PDU Names
Application	PDU
Presentation	PDU
Session	PDU
Transport	Segment
Network	Packet
Data Link	Frame
Physical	Bits

Encapsulation & Layered Communication

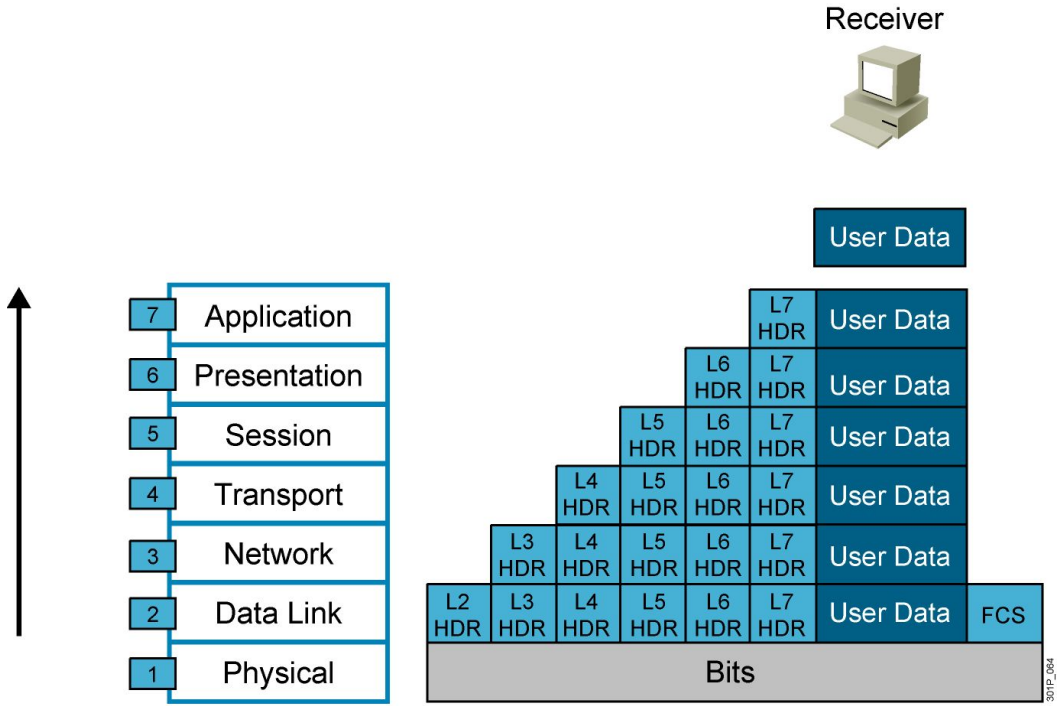


Data Encapsulation



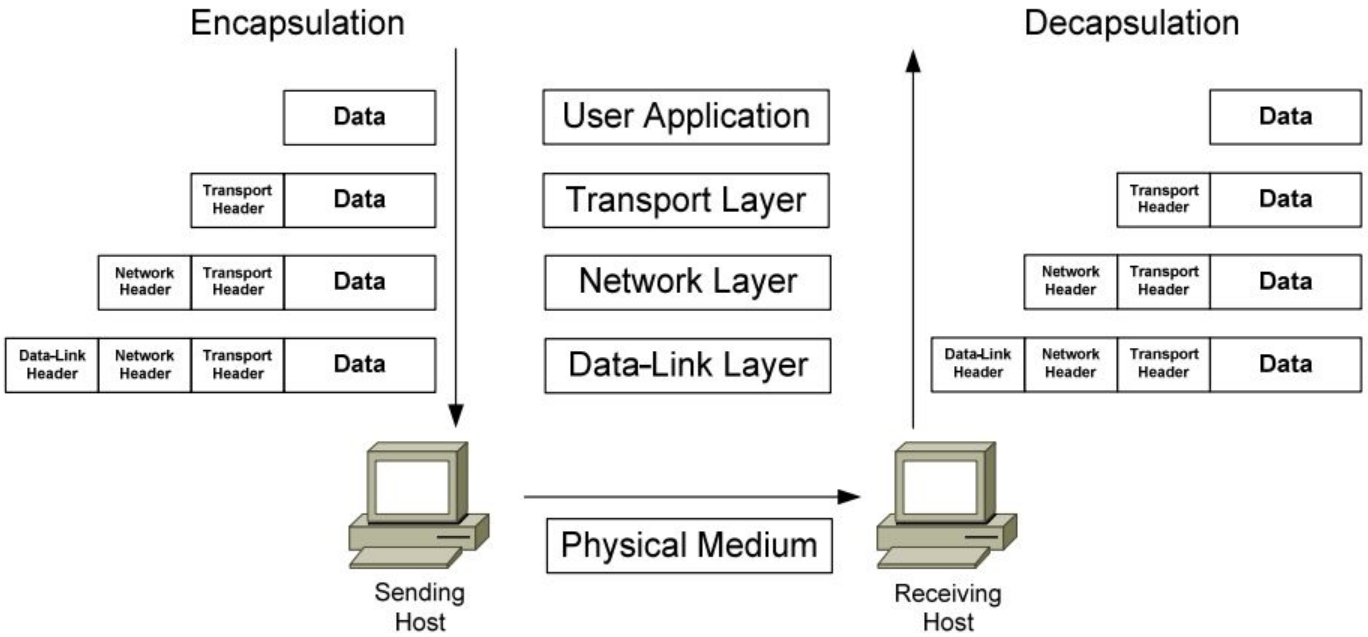
HDR = Header

Data De-Encapsulation



HDR = Header

Encapsulation Illustrated



During encapsulation on the sending host:

- Data from the user application is handed off to Transport layer.
- The Transport layer adds a header containing protocol specific information, then hands the segment to Network layer.
- The Network layer adds a header containing source and destination logical addressing, and then hands the packet to the Data-Link layer.
- The Data-Link layer adds a header containing source and destination physical addressing and other hardware-specific information.
- The Data-Link frame is then handed off to the Physical layer to be transmitted on the network medium as bits.

During decapsulation on the receiving host, the reverse occurs:

- The frame is received from the physical medium.
- The Data-Link layer processes its header, strips it off, and then hands it off to the Network layer.
- The Network layer processes its header, strips it off, and then hands it off to the Transport layer.
- The Transport layer processes its header, strips it off, and then hands the data to the user application

OSI in real world

- A web browser serves as a good practical illustration of the OSI model and the TCP/IP protocol suite: The web browser serves as the user interface for accessing a website. The browser itself does not function at the Application layer. Instead, the web browser invokes the Hyper Text Transfer Protocol (HTTP) to interface with the remote web server, which is why http:// precedes every web address.

- The Internet can provide data in a wide variety of formats, a function of the Presentation layer. Common formats on the Internet include HTML, XML, PHP, GIF, and JPEG. Any encryption or compression mechanisms used on a website are also considered a Presentation layer function.

- The Session layer is responsible for establishing, maintaining, and terminating the session between devices, and determining whether the communication is half-duplex or full-duplex. However, the TCP/IP stack generally does not include session layer protocols, and is reliant on lower-layer protocols to perform these functions.

- HTTP utilizes the TCP Transport layer protocol to ensure the reliable delivery of data. TCP establishes and maintains a connection from the client to the web server, and packages the higher-layer data into segments. A sequence number is assigned to each segment so that data can be reassembled upon arrival.

- The best path to route the data between the client and the web server is determined by IP, a Network layer protocol. IP is also responsible for the assigned logical addresses on the client and server, and for encapsulating segments into packets.

- Data cannot be sent directly to a logical address. As packets travel from network to network, IP addresses are translated to hardware addresses, which are a function of the Data Link layer. The packets are encapsulated into frames to be placed onto the physical medium

- The data is finally transferred onto the network medium at the Physical layer, in the form of raw bits. Signaling and encoding mechanisms are defined at this layer, as is the hardware that forms the physical connection between the client and the web server.

Overview of Protocols

- A protocol is a set of rules that governs the communications between computers on a network.
- In order for two computers to talk to each other, they must be speaking the same language.
- Many different types of network protocols and standards are required to ensure that your computer (no matter which operating system, network card, or application you are using) can communicate with another computer located on the next desk or half-way around the world.

OSI Layer	Name	Protocols
7	Application Layer	HTTP, HTTPs, FTP, Telnet, SMTP
6	Presentation Layer	
5	Session Layer	
4	**Transport Layer**	**TCP, UDP, QUIC**
3	**Network Layer**	**IPv4, IPv6, ICMP, ICMPv6**
2	**Datalink Layer**	**Ethernet, ATM, Token Ring, FDDI, ARP**
1	**Physical Layer**	

Internet Protocols

- **Hypertext Transfer Protocol (HTTP)** is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers, but it can also be used for other purposes.
- **Hypertext Transfer Protocol Secure (HTTPS)** is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provide

- **FTP (File Transfer Protocol)** is a network protocol for transmitting files between computers over TCP/IP connections.
- Within the TCP/IP suite, FTP is considered an application layer protocol. In an FTP transaction, the end user's computer is typically called the local host. The second computer involved in FTP is a remote host, which is usually a server. Both computers need to be connected via a network and configured properly to transfer files via FTP. Servers must be set up to run FTP services, and the client must have FTP software installed to access these services.

- **Simple Mail Transfer Protocol (SMTP)** is a communication protocol that allows the users on the same or different computers to send an email over the internet. It involves a particular set of guidelines according to which the communication via mail occurs.
- **Internet Control Message Protocol (ICMP)** is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. **(ping, Traceroute, Tracert, pathping)**

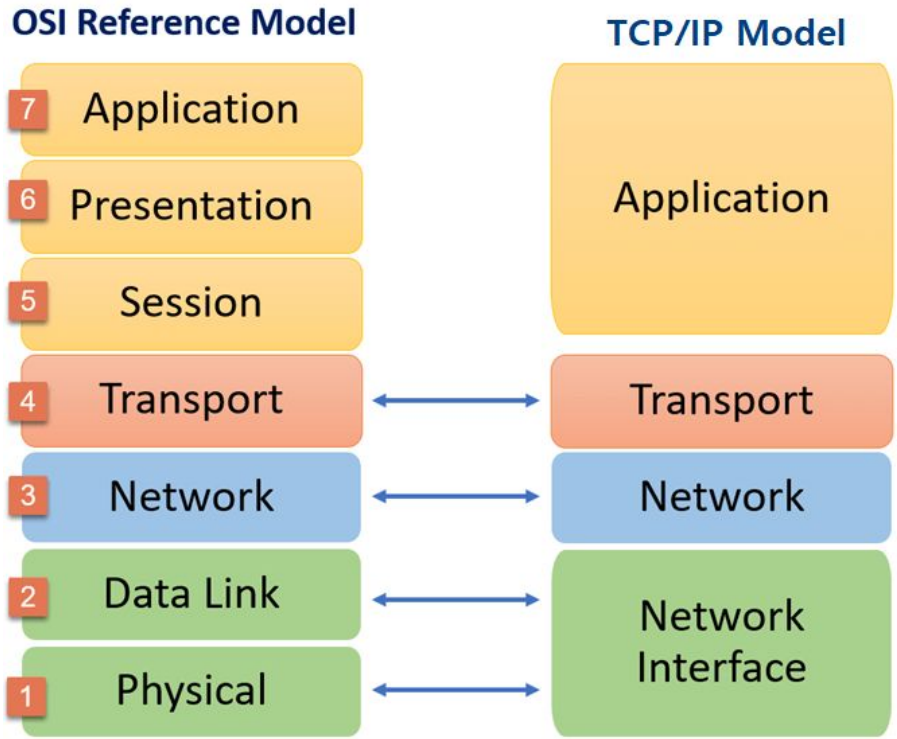
  Packet Internet Groper (PING)

:\>

C:\>tracert cisco.com

```
Tracing route to cisco.com [2001:420:1101:1::185]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  2401:4900:1cde:a3d1:32bd:13ff:fe07:e358
  2     *        *        *     Request timed out.
  3     5 ms     6 ms     6 ms  2404:a800:3a00:207::85
  4   223 ms   226 ms   224 ms  2404:a800::5
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7   220 ms   219 ms   220 ms  level3-as3356.port-channel2.switch2.lax1.he.net [2001:470:0:4ec::2]
  8   257 ms   257 ms   257 ms  2001:1900::3:135
  9   250 ms   252 ms   251 ms  CISCO-SYSTE.edge5.Dallas3.Level3.net [2001:1900:2100::2226]
 10   252 ms   252 ms   253 ms  2001:420:89:1::
 11   261 ms   261 ms   262 ms  2001:420:1100:1c::1
 12   252 ms   251 ms   252 ms  rcdn9-cd1-dmzdcc-gw1-por1.cisco.com [2001:420:1100::1]
 13   258 ms   258 ms   258 ms  2001:420:1100:118::1
 14   260 ms   259 ms   259 ms  2001:420:1103::1
 15     *        *        *     Request timed out.
 16   257 ms   258 ms   256 ms  hsrp-2001-420-1101-1-1.cisco.com [2001:420:1101:1::1]
 17   258 ms   258 ms   259 ms  2001:420:1101:1::185
```

TCP/IP Model


OSI Reference Model
TCP/IP Model
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface

- The **TCP/IP Model** (Transmission Control Protocol/Internet Protocol) is a more simplified, practical model compared to the OSI Reference Model and is the foundation of the internet and most modern network communications.
- The TCP/IP model is divided into four layers, each responsible for different aspects of communication over a network.

The 4 Layers of the TCP/IP Model:

1. Application Layer
2. Transport Layer
3. Internet Layer
4. Network Access Layer

TCP/IP Model (Application)

Application layer:

- application layer refers to programs that need TCP/IP to help them communicate with each other.
- This is the level that users typically interact with, such as email systems and messaging platforms.
- It combines the session, presentation, and application layers of the OSI model.

Protocols:

- **HTTP** (Hypertext Transfer Protocol) – used for web browsing.
- **FTP** (File Transfer Protocol) – for file transfers.
- **SMTP** (Simple Mail Transfer Protocol) – for email transmission.
- **DNS** (Domain Name System) – for resolving domain names to IP addresses.
- **POP3** (Post Office Protocol) – for retrieving email.
- **IMAP** (Internet Message Access Protocol) – for managing email on a server.
- **TELNET** – for remote terminal access.

TCP/IP Model (Transport)

Transport layer:

- **Purpose**: This layer is responsible for end-to-end communication between devices and ensures reliable data transfer. It provides error detection and correction, as well as flow control.

Key Functions:

- Establishes, maintains, and terminates communication sessions between devices.
- Segments data into smaller packets for transmission and reassembles them at the destination.
- Provides flow control to ensure that data is sent at a rate that can be handled by the receiver.
- Ensures reliable transmission through error detection and retransmission of lost packets (in the case of TCP).

Protocols:

- **TCP (Transmission Control Protocol)** – a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data.
- **UDP (User Datagram Protocol) –** a connectionless protocol that is faster but does not guarantee reliability or ordering.
- **SCTP (Stream Control Transmission Protocol)** – a transport layer protocol that combines the features of TCP and UDP, used for applications requiring high availability and redundancy.

TCP/IP Model (Internet)

Purpose: The Internet Layer is responsible for addressing, routing, and forwarding data packets across networks. It enables data to travel between devices on different networks.

Key Functions:

- Defines logical addressing (IP addressing) and packet forwarding.
- Routes packets from the source device to the destination across multiple networks, possibly through intermediate routers.
- Handles fragmentation and reassembly of data packets for transmission across networks with varying maximum transmission unit (MTU) sizes.

Protocols:

- **IP (Internet Protocol) –** defines IP addressing and packet routing. The most common versions are:
  - **IPv4** – the older and widely used version with a 32-bit address space.
  - **IPv6** – the newer version with a 128-bit address space, designed to handle the limitations of IPv4.
- **ICMP (Internet Control Message Protocol)** – used for diagnostic and error messages (e.g., Ping).
- **ARP (Address Resolution Protocol)** – used to map IP addresses to MAC addresses in local networks.
- **IGMP (Internet Group Management Protocol)** – used for managing multicast group memberships.

TCP/IP Model (Network Interface)

Network Access Layer (Layer 1 and 2 in the OSI model)

- **Purpose**: The Network Access Layer (sometimes referred to as the Link Layer or Data Link Layer) deals with the physical transmission of data over the network. It defines how data is transmitted over physical media such as Ethernet cables, wireless connections, or fiber-optic cables.
- **Key Functions**:
  - Specifies how data is physically transmitted on the network.
  - Defines the hardware and protocols needed to access the transmission medium.
  - Provides error detection and handles the framing of data.

Protocols:

- **Ethernet** – a protocol that defines how data is transmitted over local area networks (LANs) using a shared medium.
- **Wi-Fi** – a wireless networking protocol that defines how devices communicate over radio waves.
- **PPP** (Point-to-Point Protocol) – used for point-to-point communication, often in dial-up or VPN connections.
- **Frame Relay** – a WAN protocol used to transmit data over dedicated circuits.
- **DSL** (Digital Subscriber Line) – a protocol used for high-speed internet access over telephone lines.

Real-World Example of Data Transmission:

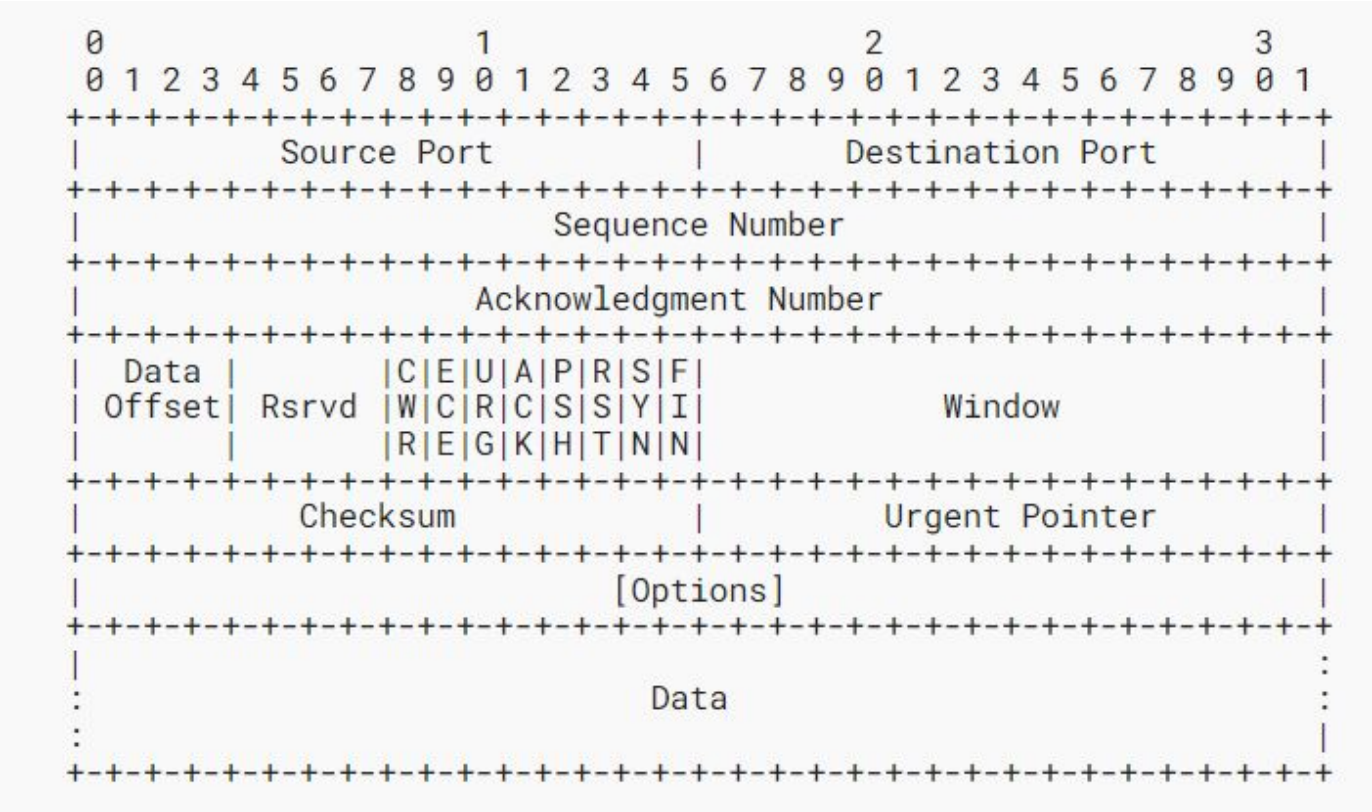
When you visit a website, the process might look like this:

1. **Application Layer**:
   - You enter the URL in a web browser, and the browser uses **HTTP** to request a page from the web server.
2. **Transport Layer**:
   - **TCP** ensures the connection is established between your computer and the web server, and data is transmitted reliably.
3. **Internet Layer**:
   - **IP** determines the best path for the data packets to travel across networks, possibly through multiple routers.
4. **Network Access Layer**:
   - The data is physically transmitted over the network medium (Ethernet, Wi-Fi, etc.) and is received by the web server, which processes the request and sends back the webpage.

illustrates where common protocols fit into the TCP/IP Protocol suite.

Layer	*Example Protocols*
Application	FTP, HTTP, SMTP
Host-to-Host	TCP, UDP
Internet	IP
Network Access	Ethernet

TCP Header


0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Source Port
Destination Port
Sequence Number
Acknowledgment Number
Data Offset
Rsrvd
C W R
E C G
U R K
A C H
P S T
R S N
S Y N
F I N
Window
Checksum
Urgent Pointer
[Options]
Data

The minimum length of the TCP header is **20 bytes**

- **Source Port** field identifies the application service on the sending host. (16 bits)
- **Destination Port** field identifies the application service on the remote host. (16 bits)
- **Sequence Number** field is used both during connection establishment, and during data transfer. During connection establishment (SYN message), an initial sequence number is randomly chosen. Sequence numbers are used to identify data bytes in a stream. (32 bits)
- **Acknowledgement Number** field, as its name suggests, is used to acknowledge a sequence number. During connection setup, this is set to the sending host's initial sequence number + 1. (32 bits)

- **Data Offset** field indicates where data begins in a TCP segment, by identifying the number of 32-bit multiples in the TCP header. A TCP header must end on a 32-bit boundary (4 bits)
- **Control Bits (8 bits)** field contains eight 1-bit flags, in the following order:
  - URG (Urgent) – prioritizes specified traffic.
  - ACK (Acknowledgment) – acknowledges a SYN or receipt of data.
  - PSH (Push) – forces an immediate send even if window is not full.
  - RST (Reset) – forcefully terminates an improper connection.
  - SYN (Synchronize) – initiates a connection.
  - FIN (Finish) – gracefully terminates a connection when there is further data to send.

WR: 1 bit Congestion Window Reduced

ECE: 1 bit ECN-Echo

- **Window field** identifies the number of data octets that the

receiver is able to accept. (16 bits)

- **Checksum field** is used for error-checking, and is computed

using both the TCP segment and select fields from IP header. The receiving host will discard the segment if it fails the checksum calculation. (16 bits)

- **Urgent Pointer** field is used to identify the last byte of

prioritized traffic in a segment, when the URG flag is set. (16 bits)

- **variable-length Options** field provides additional optional TCP parameters, outside the scope of this guide.
- **variable-length Padding** field ensures the TCP header ends on a 32-bit boundary, and is always set to zeros.

Example of TCP Header:

- **Source Port**: 5641
- **Destination Port**: 80 (HTTP)
- **Sequence Number**: 1000
- **Acknowledgment Number**: 1001
- **Flags**: SYN (indicating a connection initiation)
- **Window Size**: 8192 (receiver can accept 8192 bytes of data)
- **Checksum**: 0x1234 (checksum value)

UDP, TCP - Segment
IPv4, IPv6 - Packets
Ethernet - Frames

https://www.rfc-editor.org/rfc/rfc9293.html

- **TCP**
- **UDP**
- **DCCP - Datagram Congestion Control Protocol**
- **SCTP - Stream Control Transport Protocol**
- **QUIC - QUICK UDP INTERNET CONNECTION**

Client side Port Numbers

Select Command Prompt - netstat

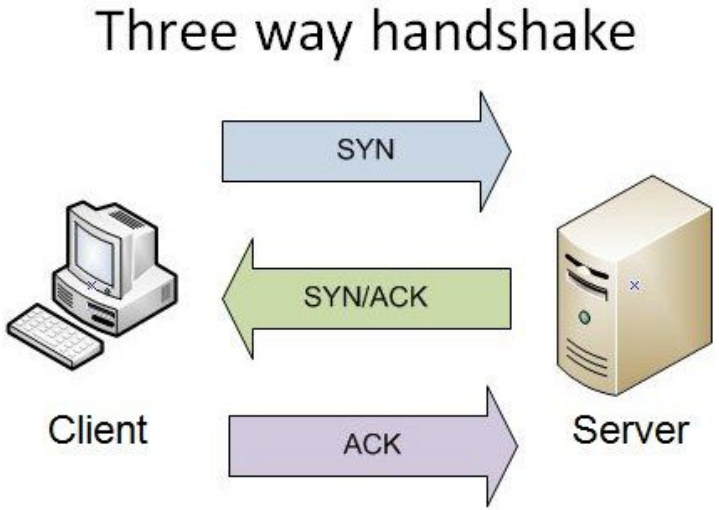
```
C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.3:49440      20.198.119.84:https    ESTABLISHED
  TCP    192.168.1.3:50037      ec2-54-243-132-124:https  ESTABLISHED
  TCP    192.168.1.3:52530      ec2-35-171-66-198:https  ESTABLISHED
  TCP    192.168.1.3:57115      ec2-18-213-148-154:https  ESTABLISHED
  TCP    192.168.1.3:59384      ec2-35-153-6-150:https  ESTABLISHED
  TCP    192.168.1.3:60115      ec2-54-227-144-19:https  ESTABLISHED
  TCP    192.168.1.3:60423      ec2-35-169-205-0:https  ESTABLISHED
  TCP    192.168.1.3:60663      ec2-34-237-108-91:https  ESTABLISHED
  TCP    192.168.1.3:60790      ec2-35-169-231-185:https  ESTABLISHED
  TCP    192.168.1.3:60954      ec2-35-169-205-0:7010  ESTABLISHED
  TCP    192.168.1.3:62284      ec2-34-230-120-115:https  ESTABLISHED
```

netstat -a

netstat -n

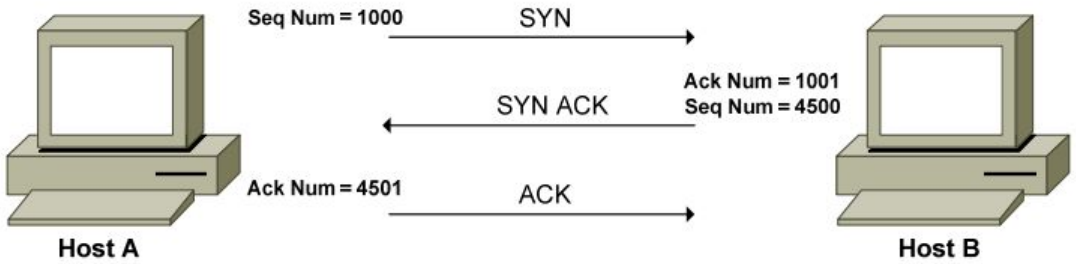
netstat -f

TCP 3 Way Handshake (always point to point)

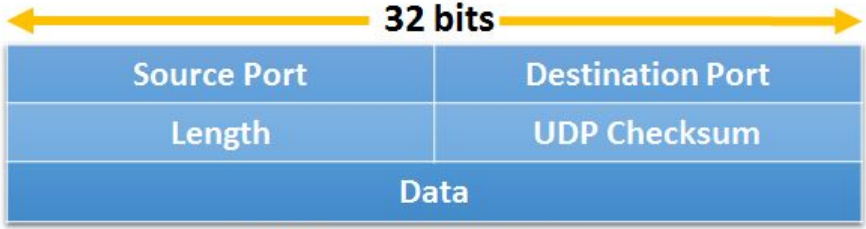


- **Step 1 (SYN):** In the first step, the client wants to establish a connection with a server, so it sends a segment with SYN(Synchronize Sequence Number) which informs the server that the client is likely to start communication and with what sequence number it starts segments with
- **Step 2 (SYN + ACK):** Server responds to the client request with SYN-ACK signal bits set. Acknowledgement(ACK) signifies the response of the segment it received and SYN signifies with what sequence number it is likely to start the segments with
- **Step 3 (ACK):** In the final part client acknowledges the response of the server and they both establish a reliable connection with which they will start the actual data transfer

TCP 3 Way handshake



User Datagram Protocol (UDP)



UDP Segment Structure

- Length of the header (16 bits)
- Checksum for error checking (16 bits)

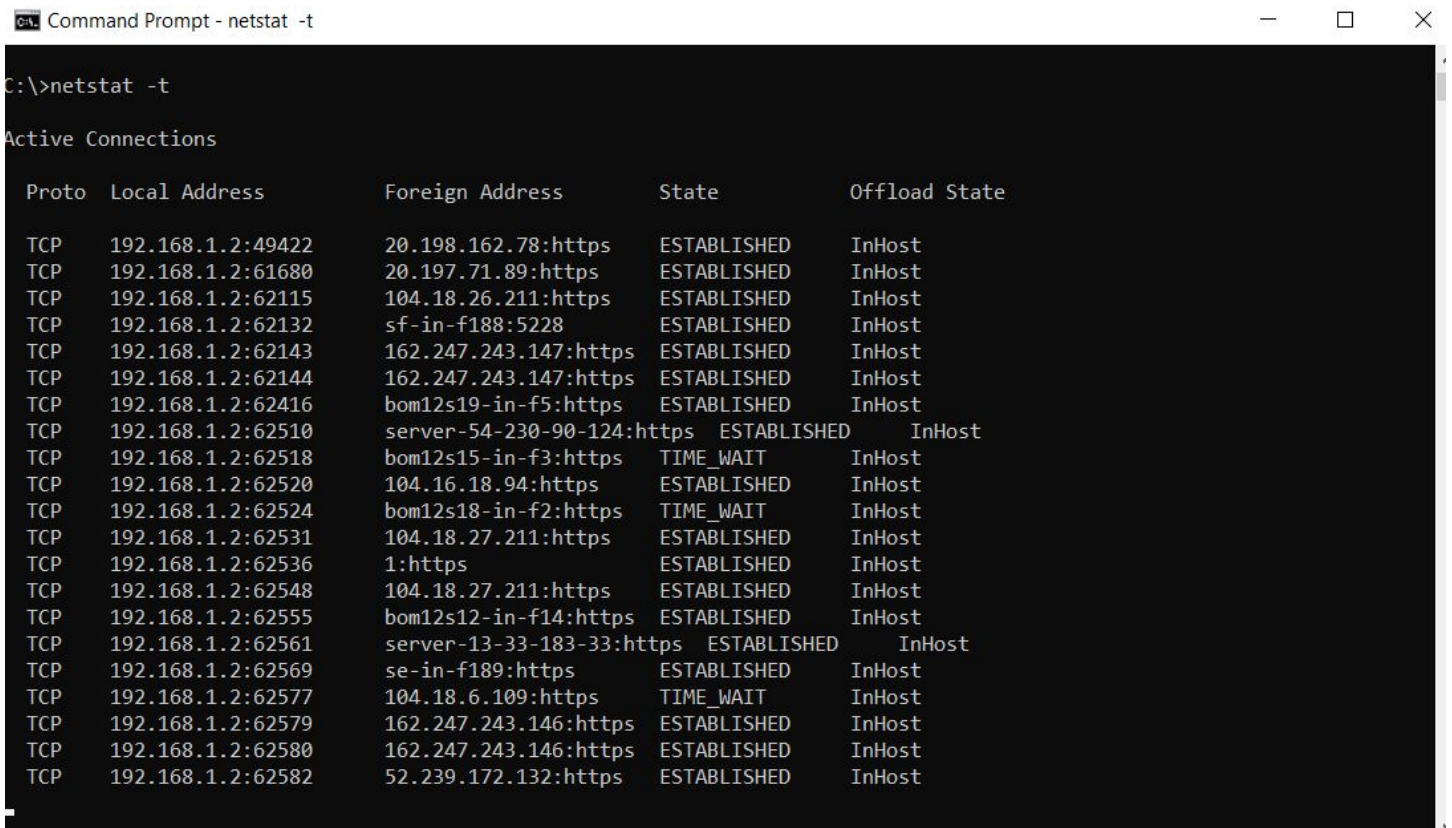
Transport Port Numbers and Sockets

- Both TCP and UDP provide a mechanism to differentiate applications (or services) running on the same host, through the use of port numbers.
- Range for port numbers is **0 – 65535,** for both TCP & UDP.
- Combination of the IP address and port number (identifying both the host and service) is referred to as a **socket**, and is written out as follows: **192.168.60.125:443**

- First **1024 ports (0 - 1023)** have been reserved for widely-used services, and are recognized as **well-known ports (Telnet, FTP, HTTP, HTTPs, SSH, SMTP, POP3….) —IANA**
- Ports ranging from **1024 – 49151** are referred to as **registered ports**, and are allocated by the IANA upon request.
- Ports ranging from **49152 – 65535** cannot be registered, and are considered dynamic. A client initiating a connection will randomly choose a port in this range as its source port (for some operating systems, the dynamic range starts at 1024 and higher).

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml?&page=2

Port Numbers and Sockets



TCP Utilities and Tools

>netstat –a (Listening and Connecting Ports)

```
C:\Users\naveen>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:445            LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:5040           LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49664          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49665          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49666          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49667          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49668          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    0.0.0.0:49670          LAPTOP-6VNOIOAD:0      LISTENING
  TCP    192.168.43.171:139     LAPTOP-6VNOIOAD:0      LISTENING
  TCP    192.168.43.171:49163   165.22.40.133:https    ESTABLISHED
  TCP    192.168.43.171:49226   20.198.119.84:https    ESTABLISHED
  TCP    192.168.43.171:49527   40.83.240.146:https    ESTABLISHED
  TCP    192.168.43.171:60978   ec2-34-237-55-225:https  ESTABLISHED
  TCP    192.168.43.171:60988   143.110.179.23:https   ESTABLISHED
  TCP    192.168.43.171:60989   141:https              ESTABLISHED
  TCP    192.168.43.171:60990   207:https              ESTABLISHED
  TCP    192.168.43.171:60997   server-18-67-161-27:https  TIME_WAIT
  TCP    192.168.43.171:61004   20.44.229.112:https    TIME_WAIT
```

TCPv6 Port and Connections

```
C:\Users\naveen>netstat -p tcpv6

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:49157  g2600-140f-0006-0384-0000-0000-0000-21cc:http  TIME_WAIT
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:49159  [2606:4700:4400::6812:2044]:http  TIME_WAIT
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:49215  [2620:1ec:c11::200]:https  ESTABLISHED
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:49673  maa05s18-in-x0e:http   CLOSE_WAIT
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:49674  maa05s18-in-x0e:http   CLOSE_WAIT
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:60980  [2620:1ec:c11::200]:https  ESTABLISHED
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:60986  https-2a02-3d0-623-a000--1:http  TIME_WAIT

C:\Users\naveen>
```

>netstat –f

(Displays Fully Qualified Domain Names (FQDN) for foreign addresses)

```
C:\Users\naveen>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.43.171:49163   165.22.40.133:https    ESTABLISHED
  TCP    192.168.43.171:49226   20.198.119.84:https    ESTABLISHED
  TCP    192.168.43.171:49527   40.83.240.146:https    ESTABLISHED
  TCP    192.168.43.171:60978   ec2-34-237-55-225.compute-1.amazonaws.com:https  ESTABLISHED
  TCP    192.168.43.171:60988   143.110.179.23:https   ESTABLISHED
  TCP    192.168.43.171:60989   141.164.46.99.vultrusercontent.com:https  ESTABLISHED
  TCP    192.168.43.171:60990   207.148.3.202.vultrusercontent.com:https  ESTABLISHED
  TCP    192.168.43.171:61006   20.44.229.112:https    TIME_WAIT
  TCP    192.168.43.171:61008   a104-85-66-81.deploy.static.akamaitechnologies.com:http  TIME_WAIT
  TCP    192.168.43.171:61009   20.44.229.112:https    TIME_WAIT
  TCP    192.168.43.171:61012   117.18.237.29:http     ESTABLISHED
  TCP    192.168.43.171:61014   20.205.248.73:https    ESTABLISHED
  TCP    192.168.43.171:61015   a23-64-122-99.deploy.static.akamaitechnologies.com:https  ESTABLISHED
  TCP    192.168.43.171:65506   ec2-54-227-144-19.compute-1.amazonaws.com:https  ESTABLISHED
  TCP    192.168.43.171:65507   ec2-34-237-189-140.compute-1.amazonaws.com:https  ESTABLISHED
^C
C:\Users\naveen>
```

>netstat –n (Displays addresses and port numbers in numerical form)

```
C:\Users\naveen>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.43.171:49163   165.22.40.133:443      ESTABLISHED
  TCP    192.168.43.171:49226   20.198.119.84:443      ESTABLISHED
  TCP    192.168.43.171:49527   40.83.240.146:443      ESTABLISHED
  TCP    192.168.43.171:60978   34.237.55.225:443      ESTABLISHED
  TCP    192.168.43.171:60988   143.110.179.23:443     ESTABLISHED
  TCP    192.168.43.171:60989   141.164.46.99:443      ESTABLISHED
  TCP    192.168.43.171:60990   207.148.3.202:443      ESTABLISHED
  TCP    192.168.43.171:61020   20.44.229.112:443      TIME_WAIT
  TCP    192.168.43.171:65506   54.227.144.19:443      ESTABLISHED
  TCP    192.168.43.171:65507   34.237.189.140:443     ESTABLISHED
  TCP    192.168.43.171:65508   104.18.26.251:443      ESTABLISHED
  TCP    [2401:4900:22d8:618f:e46e:4bfb:66c4:9950]:61016  [2404:6800:4007:809::2013]:443  CLOSE_WAIT

C:\Users\naveen>
```

IPv4 Routing Table

```
C:\Users\naveen>netstat -r
===========================================================================
Interface List
 19...68 54 5a 8a ab 61 ......Microsoft Wi-Fi Direct Virtual Adapter
  9...6a 54 5a 8a ab 60 ......Microsoft Wi-Fi Direct Virtual Adapter #2
 21...68 54 5a 8a ab 60 ......Intel(R) Wireless-AC 9462
  5...68 54 5a 8a ab 64 ......Bluetooth Device (Personal Area Network)
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.43.1   192.168.43.171     55
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
     192.168.43.0    255.255.255.0         On-link    192.168.43.171    311
   192.168.43.171  255.255.255.255         On-link    192.168.43.171    311
   192.168.43.255  255.255.255.255         On-link    192.168.43.171    311
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link    192.168.43.171    311
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link    192.168.43.171    311
===========================================================================
```

IPv6 Routing Table

```
IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
 21     71 ::/0                     fe80::a045:f7ff:fe9e:6e6c
  1    331 ::1/128                  On-link
 21     71 2401:4900:22d8:618f::/64 On-link
 21    311 2401:4900:22d8:618f:2504:87d4:aaa:c50c/128
                                    On-link
 21    311 2401:4900:22d8:618f:e46e:4bfb:66c4:9950/128
                                    On-link
 21    311 fe80::/64                On-link
 21    311 fe80::2504:87d4:aaa:c50c/128
                                    On-link
  1    331 ff00::/8                 On-link
 21    311 ff00::/8                 On-link
===========================================================================
```

Application and Port Numbers (IANA)

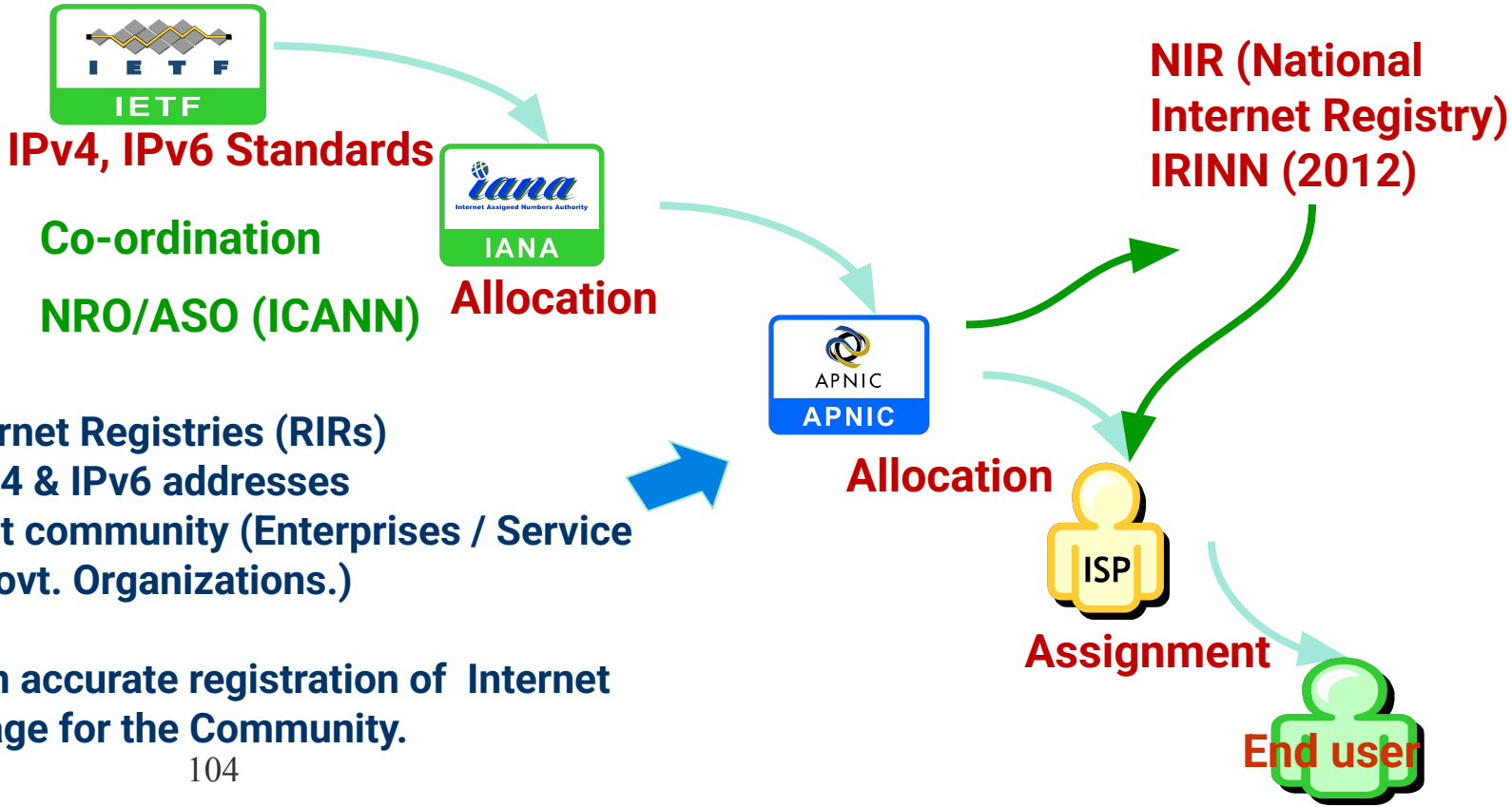
Port Number	Transport Protocol	Application
20, 21	TCP	FTP (File Transfer Protocol)
22	TCP	SSH (Secure Shell) - Remote Access
23	TCP	Telnet - Remote Access
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	**TCP or UDP**	**DNS (Domain Name System) - Zone Transfer for that purpose DNS will use TCP**
80	TCP	HTTP (HyperText Transfer Protocol)
110	TCP	POP3 (Post Office Protocol)
443	TCP	HTTPs/SSL/TLS Secure HTTP/Secure Socket Layer / Transport Layer Security

Hands-On Labs:

- **Visually understand how data is handled and transmitted over TCP and UDP.**
- **Capture packets during a TCP file transfer and a UDP stream. Analyze how packets are formed, managed, and transported.**

IPv4 Address

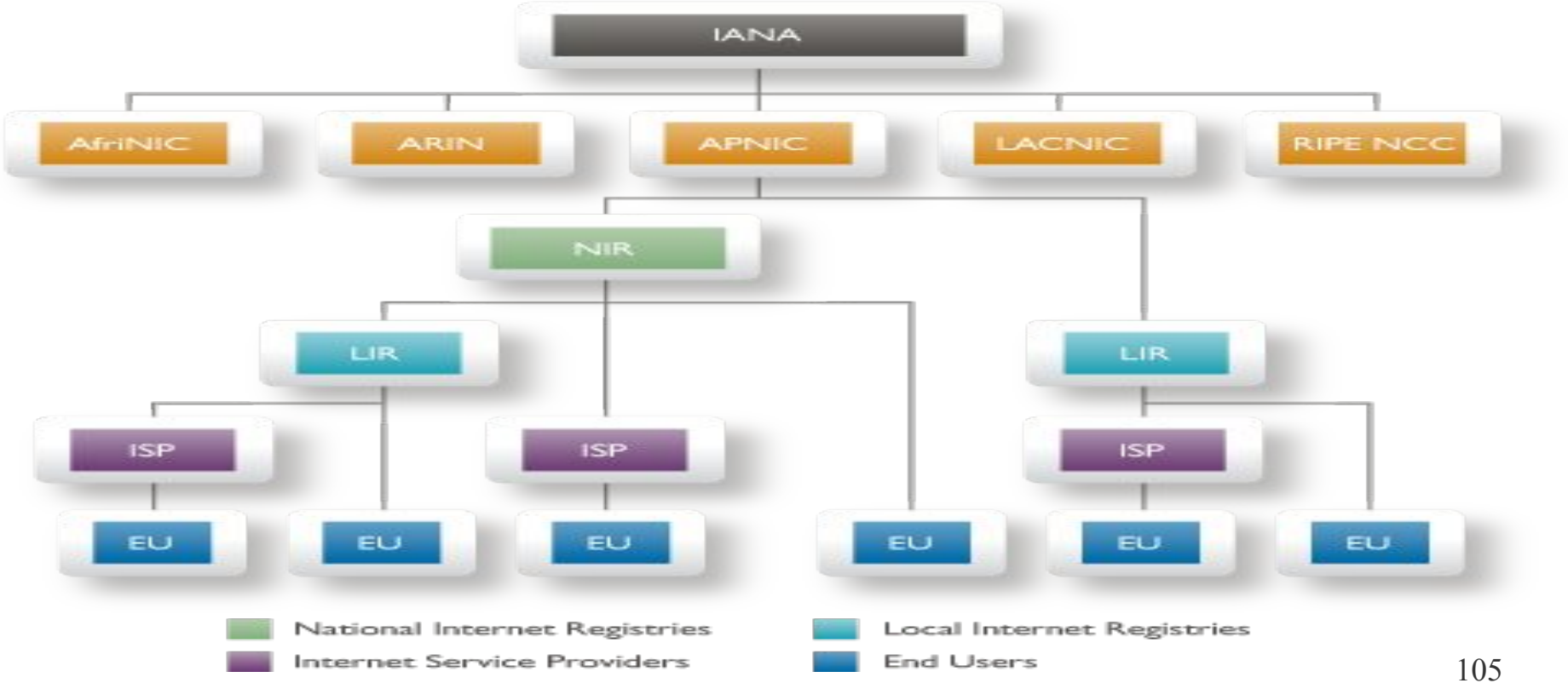
Where do we get an IP Address ?



Regional Internet Registries (RIRs) distribute IPv4 & IPv6 addresses to the Internet community (Enterprises / Service Providers / Govt. Organizations.)

RIRs maintain accurate registration of Internet Resource usage for the Community.

Allocated Chart (Optional)



Regional Internet Registry (RIR)

- APNIC – Asia Pacific Network Information Center

  India belongs to the APNIC region.
- ARIN – American Registry for Internet Numbers
- LACNIC – Latin America & Caribbean Network Information Center
- AfriNIC – African Network Information Center
- RIPE – NCC RIPE Network Coordination Center

  [Europe & Middle East]

https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

Public IP Address Types (PA v/s PI)

Provider Independent (PI) (Portable)

- Customer holds addresses independent from ISP
    - bought directly from RIR or NIR
- Customer keeps addresses when changing ISP
- Bad for size of routing tables
- Bad for QoS: routes may be filtered by upstream provider

Provider Aggregatable (PA) (Non-portable)

- Customer uses ISP's address space
- Customer must renumber if changing ISP
- Only way to effectively scale the Internet

Network Address Translation (NAT)

- The rapid growth of Internet resulted in a Shortage of available IPv4 Addresses. In response, a specific range of IPv4 address space was designated or reserved as Private Address, which can be used inside a Organization's Network.
- NAT is the process of translating Private Address to Public Address. NAT allows a host configured with a Private Address to be stamped with a public address, thus allowing that host to communicate across the Internet.

Hand-On:

1. **Understand how to assign IPv4 addresses to network devices.**
2. **Use a network simulator to set up a small network. Assign static IP addresses to each device, ensuring they are on the same subnet. Verify the connectivity using the ping command.**
3. **Given an IPv4 address and a requirement for a number of subnets, calculate the appropriate subnet mask and determine the range of addresses for each subnet.**
4. **Set up a small network in a simulator. Assign static IPv6 addresses to each device and verify connectivity using the ping6 command.**
5. **Using a network simulator, configure network devices to support both IPv4 and IPv6 addressing (Dual Stack IPv4/IPv6)**

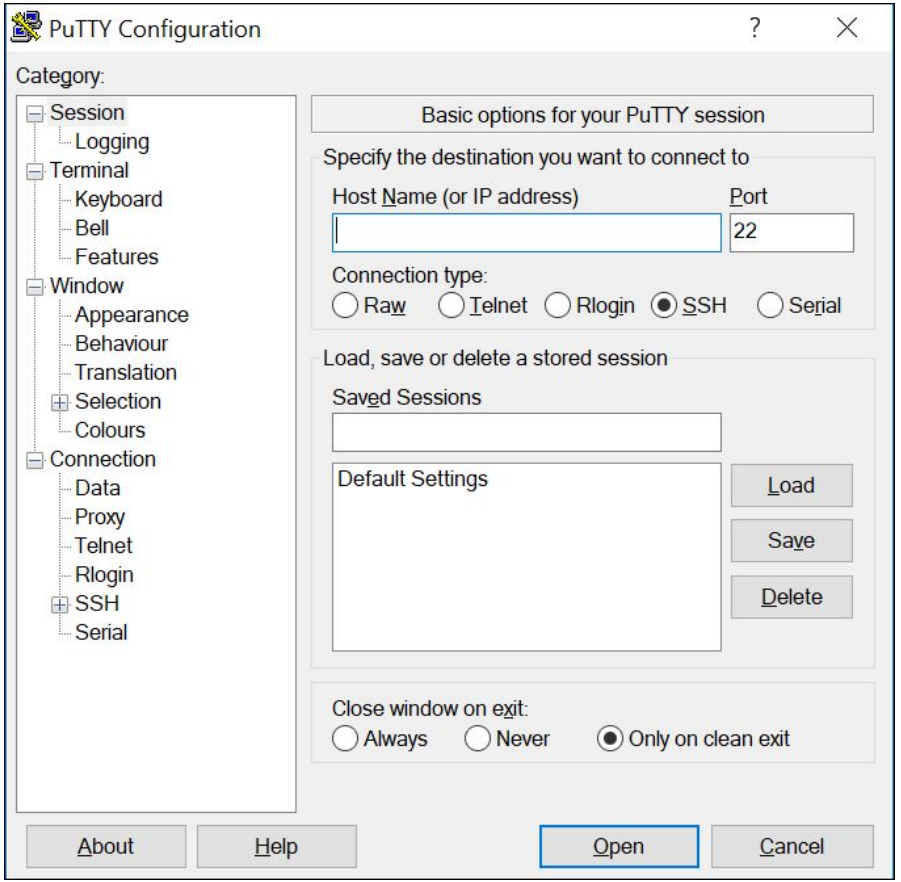
Cisco IOS (Internetwork Operating Systems)

Access Methods

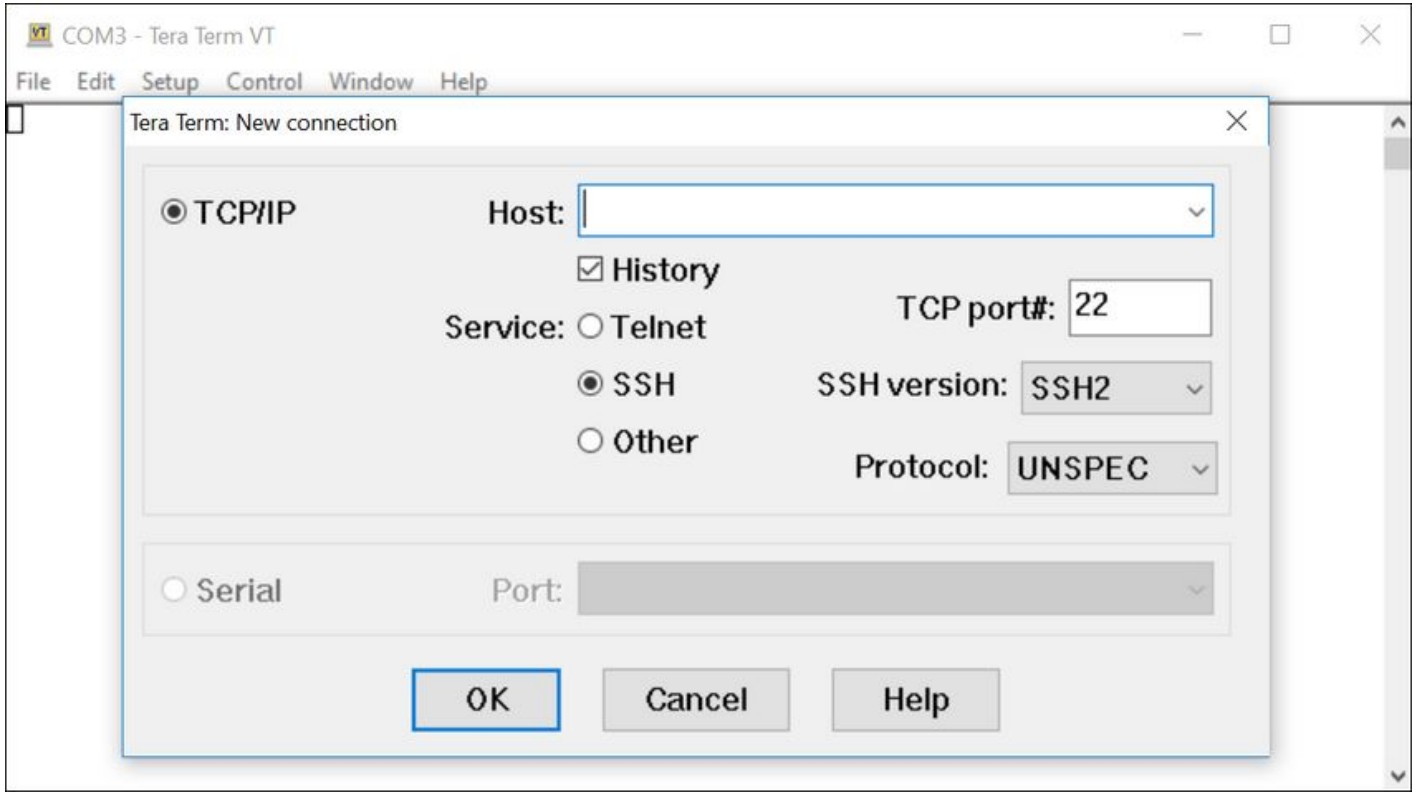
Method	Description
Console	This is a physical management port that provides out-of-band access to a Cisco device. Out-of-band access refers to access via a dedicated management channel that is used for device maintenance purposes only. The advantage of using a console port is that the device is accessible even if no networking services are configured, such as performing the initial configuration. A computer running terminal emulation software and a special console cable to connect to the device are required for a console connection.
Secure Shell (SSH)	SSH is an in-band and recommended method for remotely establishing a secure CLI connection, through a virtual interface, over a network. Unlike a console connection, SSH connections require active networking services on the device, including an active interface configured with an address. Most versions of Cisco IOS include an SSH server and an SSH client that can be used to establish SSH sessions with other devices.
Telnet	Telnet is an insecure, in-band method of remotely establishing a CLI session, through a virtual interface, over a network. Unlike SSH, Telnet does not provide a secure, encrypted connection and should only be used in a lab environment. User authentication, passwords, and commands are sent over the network in plaintext. The best practice is to use SSH instead of Telnet. Cisco IOS includes both a Telnet server and Telnet client.

Terminal Emulation Programs

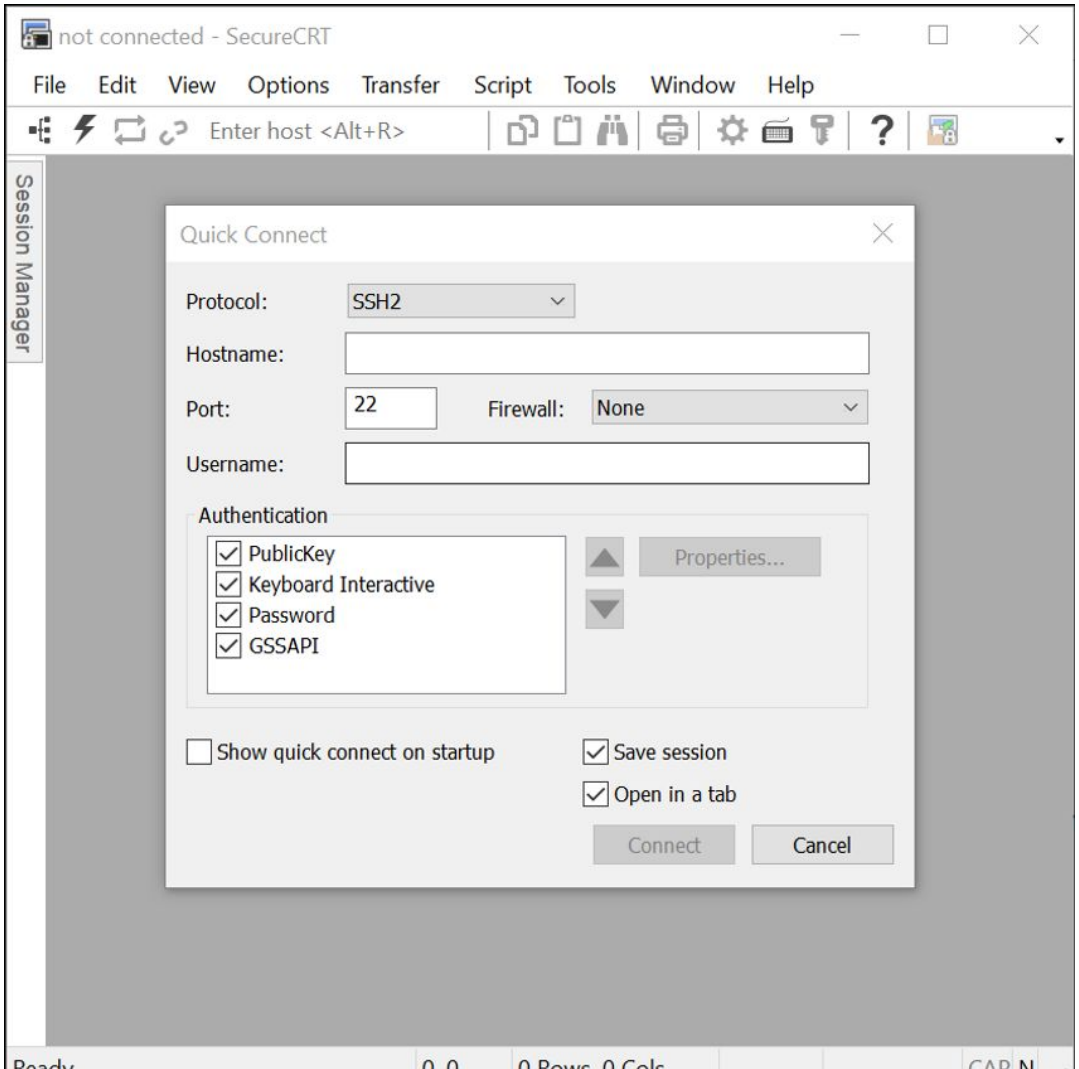
There are several terminal emulation programs you can use to connect to a networking device either by a serial connection over a console port, or by an SSH/Telnet connection. These programs allow you to enhance your productivity by adjusting window sizes, changing font sizes, and changing color schemes.



Tera Term


COM3 - Tera Term VT
File Edit Setup Control Window Help
Tera Term: New connection
TCP/IP
Host:
History
Service: Telnet
TCP port#: 22
SSH
SSH version: SSH2
Other
Protocol: UNSPEC
Serial
Port:
OK
Cancel
Help

Secure CRT


not connected - SecureCRT
File
Edit
View
Options
Transfer
Script
Tools
Window
Help
Enter host <Alt+R>
Session Manager
Quick Connect
Protocol:
SSH2
Hostname:
Port:
22
Firewall:
None
Username:
Authentication
PublicKey
Keyboard Interactive
Password
GSSAPI
Properties...
Show quick connect on startup
Save session
Open in a tab
Connect
Cancel
Ready

Primary Command Modes

the Cisco IOS software separates management access into the following two command modes:

- **User EXEC Mode -** This mode has limited capabilities but is useful for basic operations. It allows only a limited number of basic monitoring commands but does not allow the execution of any commands that might change the configuration of the device. The user EXEC mode is identified by the CLI prompt that ends with the **> symbol.**
- **Privileged EXEC Mode -** To execute configuration commands, a network administrator must access privileged EXEC mode. Higher configuration modes, like global configuration mode, can only be reached from privileged EXEC mode. The privileged EXEC mode can be identified by the prompt ending with the **# symbol.**

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as “view-only" mode.	`Switch>` `Router>`
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`

#show run
#show start
#show ip interface brief
#show ip route
#show run | section
#copy run start
#write memory
#configure terminal
#enable password
#enable secret
#service password encryption
#hostname
#line console 0
#line vty 0 4
#interface