My notes

Recommendations

- **Please mainly focus on Red color . and *****
- **After reading all notes , Go to “Special Notes”.**

Chapter 1 (Intro)

- **Peer to Peer**
- **End devices**
- **Network Media (cables)**
- **Topology Diagrams**
- **Intranet (private LANS)**
- **Internet (WAN)**

Connection	Description
Cable	high bandwidth, always on, internet **offered by cable television** service providers.
DSL	high bandwidth, always on, internet connection that runs over a **telephone line.**
Cellular	uses a cell **phone network** to connect to the internet.
Satellite	major benefit to **rural areas** without Internet Service Providers.
Dial-up telephone	an inexpensive, **low bandwidth** option using a modem.

•Quality of Service (QoS) is the primary mechanism used to ensure reliable delivery of content for all users.

Network Security

•Confidentiality – only intended recipients can read the data

•Integrity – assurance that the data has not be altered with during transmission

•Availability – assurance of timely and reliable access to data for authorized users

- Dedicated firewall system
- Access control lists (ACL)
- Intrusion prevention systems (IPS)
- Virtual private networks (VPN)

Chapter 2 (Protocols and Models)

Message encoding: Converting data into a transmittable format.

Message formatting and encapsulation: Structuring and packaging data for transmission.

Message size: Defining the maximum data size.

Message timing: Synchronizing and managing transmission timing.

Message delivery options: Methods for delivering messages (e.g., unicast, multicast)

- **Unicast** – one to one communication
- **Multicast** – one to many, typically not all
- **Broadcast** – one to all

Network Protocols

Protocol Type	Description
Network Communications	**enable two or more devices** to communicate over one or more networks
Network Security	**secure data** to provide **authentication**, data **integrity**, and data **encryption**
Routing	enable routers to exchange route information, compare path information, and **select best path**
Service Discovery	used for the **automatic detection of devices or services**

Function	Description
Addressing	**Identifies** sender and receiver
Reliability	Provides **guaranteed delivery**
Flow Control	Ensures **data flows at an efficient rate**
Sequencing	Uniquely **labels** each transmitted segment of data
Error Detection	Determines if data became **corrupted** during transmission
Application Interface	**Process-to-process** communications between network applications

Protocol Suites

- •**A group of inter-related protocols necessary to perform a communication function**
- •**Sets of rules that work together to help solve a problem**

****

- **Internet Society (ISOC)** - Promotes the open development and evolution of internet
- **Internet Architecture Board (IAB)** - Responsible for management and development of internet standards
- **Internet Engineering Task Force (IETF)** - Develops, updates, and maintains internet and **TCP/IP** technologies
- **Internet Research Task Force (IRTF)** - Focused on **long-term research** related to internet and TCP/IP protocols

Standards organizations involved with the development and support of TCP/IP

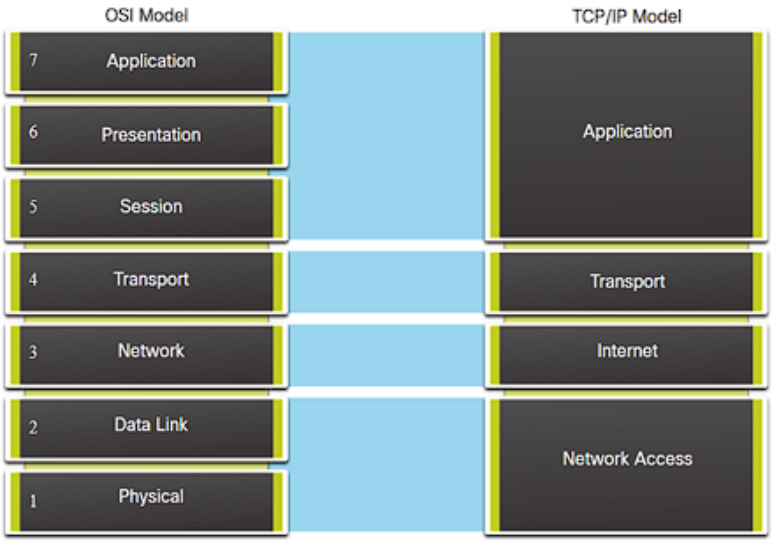
- **Internet Corporation for Assigned Names and Numbers (ICANN)** - Coordinates IP address allocation, the management of domain names, and assignment of other information
- **Internet Assigned Numbers Authority (IANA)** - Oversees and manages IP address allocation, domain name management, and protocol identifiers for ICANN

OSI 7 Layers

OSI Model Layer	Description
7 - Application	Contains protocols used for **process-to-process communications**.
6 - Presentation	Provides for common **representation of the data** transferred between application layer services.
5 - Session	Provides services to the presentation layer and to **manage data exchange**.
4 - Transport	Defines services to **segment, transfer, and reassemble** the data for individual communications.
3 - Network	Provides services to **exchange the individual pieces of data over the network**.
2 - Data Link	Describes methods for **exchanging data frames over a common media**.
1 - Physical	Describes the means to activate, maintain, and de-activate **physical connections**.

TCP/TP Model

TCP/IP Model Layer	Description
Application	**Represents data** to the user, plus encoding and dialog control.
Transport	Supports **communication between various devices** across diverse networks.
Internet	Determines the **best path through the network**.
Network Access	Controls the **hardware devices and media** that make up the network.



What is Multiplexing?

- **the processes of taking multiple streams of segmented data and interleaving them together.**

Sequencing messages is the process of numbering the segments so that the message may be reassembled at the destination.

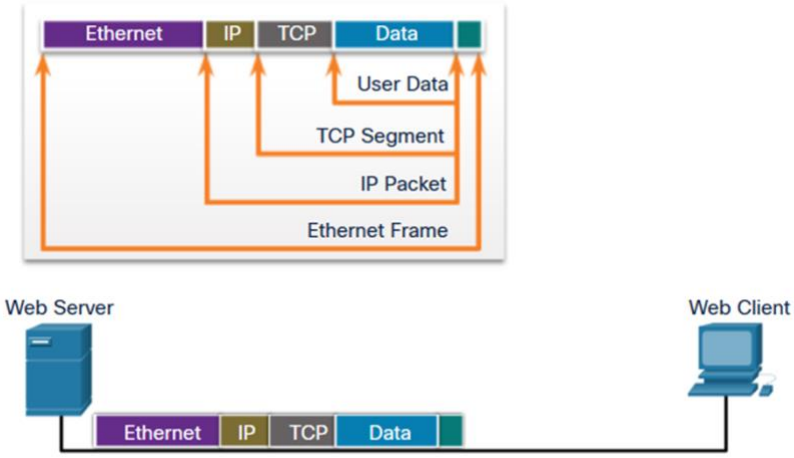
TCP is for sequencing

Encapsulation is the process where protocols add their information to the data.

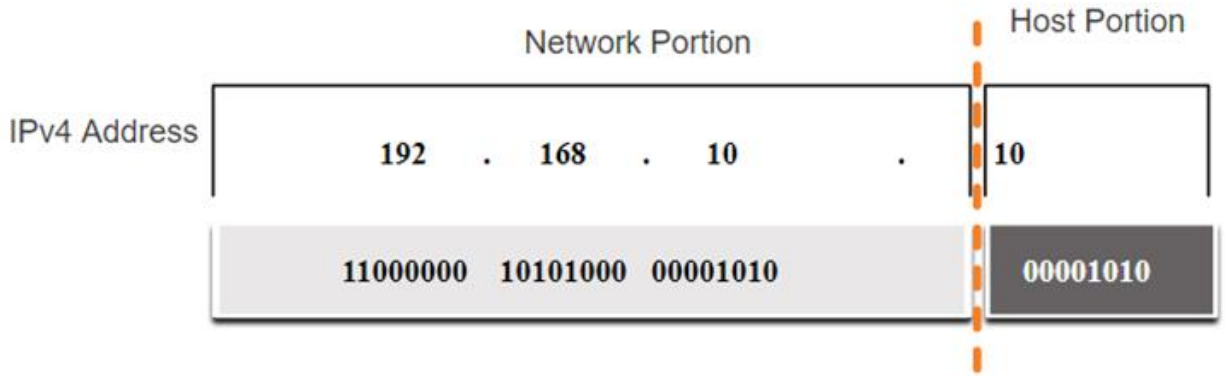
Protocol Data Units (PDU)

•**PDUs passing down the stack are as follows:**

1. **Data (Data Stream)**
2. **Segment**
3. **Packet**
4. **Frame**
5. **Bits (Bit Stream)**



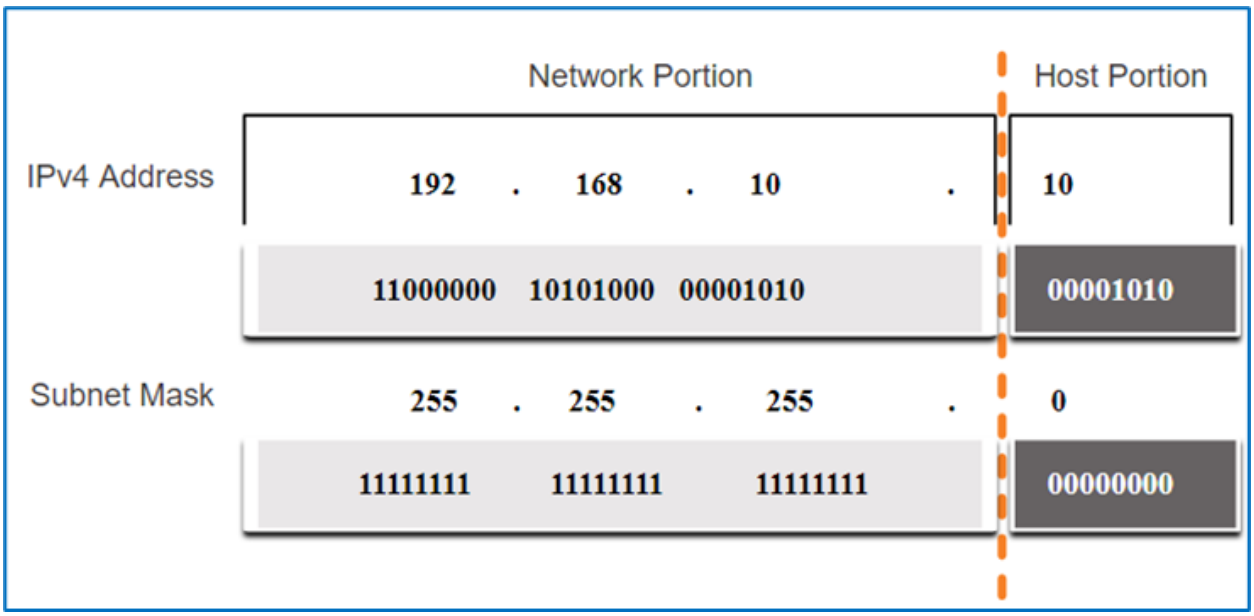
Chapter - 3 (IPV4)



•**An IPv4 address is a 32-bit hierarchical address that is made up of a network portion and a host portion.**

•**A subnet mask is used to determine the network and host portions.**

Subnet Mask



-

•A prefix length is a less cumbersome method used to identify a subnet mask address.

•The prefix length is the number of bits set to 1 in the subnet mask. For eg: 11111111.000000.000…. (will be /8)

Subnetting reduces overall network traffic and improves network performance

Class A: Default mask is 255.0.0.0

Class B: Default mask is 255.255.0.0

Class C: Default mask is 255.255.255.0

*Public and Private IPV4

•Private IPv4 addresses are not unique and can be used internally within any network.

Network Address and Prefix	RFC 1918 Private Address Range
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Remember the range!!!!

NAT (Network Address Translation)

-•It translates the internal private address to a public global IP address.

Special Use of IPv4

-Loopback addresses

•127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)

•Commonly identified as only 127.0.0.1

- Local Host is kind of loopback addresses

Link-Local addresses

•169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
•Commonly known as the Automatic Private IP Addressing (APIPA) addresses or self-assigned addresses.
•Used by Windows DHCP clients to self-configure when no DHCP servers are available.

*RFC 790 (1981) allocated IPv4 addresses in classes

•Class A (0.0.0.0/8 to 127.0.0.0/8)

•Class B (128.0.0.0 /16 – 191.255.0.0 /16)

•Class C (192.0.0.0 /24 – 223.255.255.0 /24)

•Class D (224.0.0.0 to 239.0.0.0)

•Class E (240.0.0.0 – 255.0.0.0)

What problem can a large broadcast domain cause?

- **It can generate excessive broadcasts, negatively affecting the network.**

How does subnetting solve the issue of excessive broadcasts?

- **Subnetting creates smaller broadcast domains, limiting the scope of broadcasts.**

*Subnet Calculation

1. **Determine the Number of Subnets Needed: Decide how many subnets you need and the number of hosts per subnet.**
2. **Find the Subnet Bits: Convert the total number of subnets into binary to find out how many bits you need. For example, for 4 subnets, you need 2 bits (since 2^2 = 4).**
3. **For example, if you start with a Class B network (255.255.0.0) and need 4 subnets, the new mask will be 255.255.255.192.**
4. **Convert the New Mask to Decimal: Combine the default mask bits with the subnet bits and convert the result into decimal format. For example, for a Class C network needing 4 subnets, the new mask in binary would be 11111111.11111111.11111111.11000000, which converts to 255.255.255.192.**
5. **Verify: Ensure the number of hosts and subnets match your requirements.**

Example:

If you need 8 subnets in a Class C network:

- **8 subnets need 3 bits (2^3 = 8).**

- **Starting with 255.255.255.0 (Class C default), add 3 subnet bits: 255.255.255.224 (11100000 in binary for the last octet).**

VLSM

Variable Subnet Sizes:

- **Subnets are created with varying sizes based on requirements.**
- **More efficient use of IP address space by tailoring subnet sizes to specific needs.**
- **Reduces waste of IP addresses.**

***VLSM provides more efficient and flexible network design, better suited for networks with varying sizes of subnet requirements. Traditional subnetting is simpler but less efficient, making it suitable for smaller networks with uniform requirements.**

Physical and Network Layer

Chapter - 4 (Physical Layer)

- **Physical Components**
- **Encoding**
- **Signaling**

Encoding

- **converts the stream of bits into a format recognizable by the next device**

Signaling

- **is how the bit values, “1” and “0” are represented on the physical medium.**

Bandwidth

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

Latency

Amount of time, including delays, for data to travel from one given point to another

Throughput

The measure of the transfer of bits across the media over a given period of time

Goodput

The measure of usable data transferred over a given period of time

Goodput = Throughput - traffic overhead

Copper Cabling

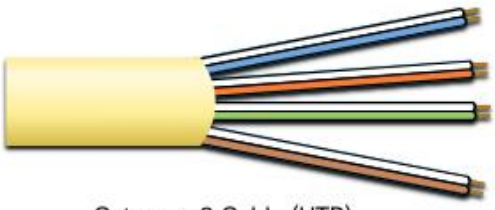
Unshielded Twisted-Pair (UTP) Cable

Shielded Twisted-Pair (STP) Cable

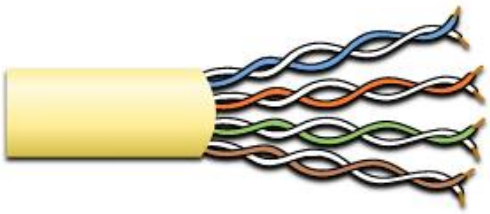
Coaxial Cable

UTP (twisted pair)

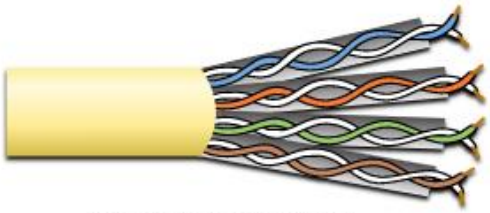
- most common networking media
- terminated with RJ-45
- interconnects hosts with intermediary network devices
- use opposite polarity (one is negative and one is positive)
- TIA/EIA. TIA/EIA-568



Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)



Category 6 Cable (UTP)

Cable Type	Standard	Application
Ethernet Straight-through	Both ends T568A or T568B	Host to Network Device
Ethernet Crossover *	One end T568A, other end T568B	Host-to-Host, Switch-to-Switch, Router-to-Router
* Considered Legacy due to most NICs using Auto-MDIX to sense cable type and complete connection		
Rollover	Cisco Proprietary	Host serial port to Router or Switch Console Port, using an adapter

STP

- Better noise protection than UDP
- More expensive
- Harder to install

Coaxial Cable

- Commonly used in the following situations:
- Wireless installations **-** attach antennas to wireless devices
- Cable internet installations **-** customer premises wiring

Fiber-Optic Cabling

- Not as common as UTP due to higher cost
- - Ideal for specific networking scenarios
- Transmits data over long distances at high bandwidth
- - Less susceptible to attenuation, immune to EMI/RFI
- Made of thin, pure glass strands
- Uses laser or LED to encode bits as light pulses
- Acts as a waveguide to transmit light with minimal signal loss

Single-Mode Fiber

- **Very small core**
- **Users expensive lasers**
- **Long-distance application**

Multimode Fiber

- **Larger core**
- **User less expensive LEDS**
- **LEDS transmit at different angels**
- **Up to 10 Gps over 550 meters.**

Fiber-Optic cabling usage

- **Enterprise Network**
- **Fiber to the home**
- **Long haul networks (countries and cities)**
- **Submarine cable network**

Straight-Tip (ST) Connectors

Lucent Connector (LC) Simplex Connectors

ubscriber Connector (SC) Connectors

Duplex Multimode LC Connectors

SC-SC MM Patch Cord

LC-LC SM Patch Cord

ST-LC MM Patch Cord

ST-SC SM Patch Cord

A yellow jacket is for single-mode fiber cables and orange (or aqua) for multimode fiber cables.

Fiber Vs Copper

Implementation Issues	UTP Cabling	Fiber-Optic Cabling
Bandwidth supported	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Distance	Relatively short (1 - 100 meters)	Relatively long (1 - 100,000 meters)
Immunity to EMI and RFI	Low	High (Completely immune)
Immunity to electrical hazards	Low	High (Completely immune)
Media and connector costs	Lowest	Highest
Installation skills required	Lowest	Highest
Safety precautions	Lowest	Highest

Immunity to EMI and RFI ensuring reliable performance of electronics in various environments where such interference is common, such as in industrial settings

Wireless Standards:

Wi-Fi (IEEE 802.11) - Wireless LAN (WLAN) technology

Bluetooth (IEEE 802.15) - Wireless Personal Area network (WPAN) standard

WiMAX (IEEE 802.16) - Uses a point-to-multipoint topology to provide broadband wireless access

Zigbee (IEEE 802.15.4) - Low data-rate, low power-consumption communications, primarily for Internet of Things (IoT) applications

Chapter - 5(Data Link Layer)

- responsible for communications between end-device network interface cards

How does the Data Link Layer handle error detection?

- by adding error detection codes in the frame trailer, which allow the receiving device to detect and reject corrupted frames.

What are the two sublayers of the Data Link Layer according to IEEE 802 standards?

- Logical Link Control (LLC) sublayer and the Media Access Control (MAC) sublayer.

What is the function of the Logical Link Control (LLC) sublayer?

- responsible for communicating between the networking software at the upper layers and the device hardware at the lower layers.

What is the function of the Media Access Control (MAC) sublayer?

- responsible for data encapsulation and media access control.

How does the Data Link Layer encapsulate Layer 3 packets?

- by adding a frame header and trailer around the packet, creating a frame that can be transmitted over the physical medium.

Standards

- **IEEE**
- **ITU**
- **ISO**

- **ANSI**

CSMA/CD

- **Used by legacy Ethernet LANs.**
- **Operates in half-duplex mode where only one device sends or receives at a time.**
- **Uses a collision detection process to govern when a device can send and what happens if multiple devices send at the same time.**
- **Pros: Simple and effective for wired networks.**
- **Cons: Inefficient under high traffic; collisions can still occur.**

CSMA/CD collision detection process:

- **Devices transmitting simultaneously will result in a signal collision on the shared media.**
- **Devices detect the collision.**
- **Devices wait a random period of time and retransmit data.**

CSMA/CA

- **Used by IEEE 802.11 WLANs.**
- **Operates in half-duplex mode where only one device sends or receives at a time.**
- **Uses a collision avoidance process to govern when a device can send and what happens if multiple devices send at the same time.**
- **• Pros: Reduces collisions in wireless environments.**
- **Cons: Overhead from RTS/CTS can reduce efficiency.**

  Request to Send (RTS): Clear to Send (CTS):

CSMA/CA collision avoidance process:

- When transmitting, devices also include the time duration needed for the transmission.

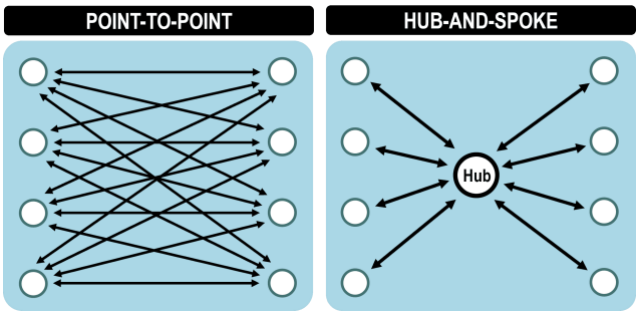
Other devices on the shared medium receive the time duration information and know how long the medium will be unavailable

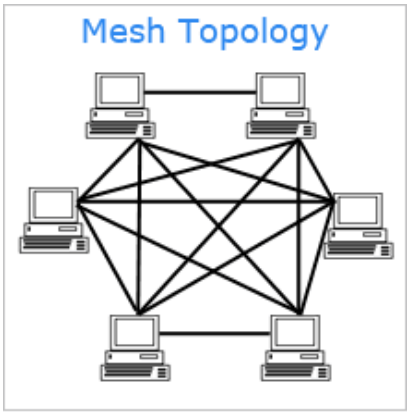
Physical and Logical Topologies

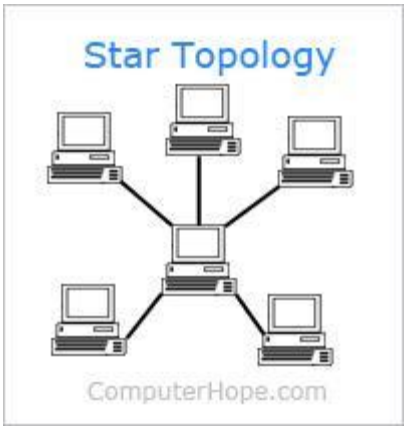
- Physical topology – shows physical connections and how devices are interconnected.
- Logical topology – identifies the virtual connections between devices using device interfaces and IP addressing schemes.

***WAN Topology**

- Point-to-point – the simplest and most common WAN topology. Consists of a permanent link between two endpoints.
- Hub and spoke – similar to a star topology where a central site interconnects branch sites through point-to-point links.
- Mesh – provides high availability but requires every end system to be connected to every other end system.





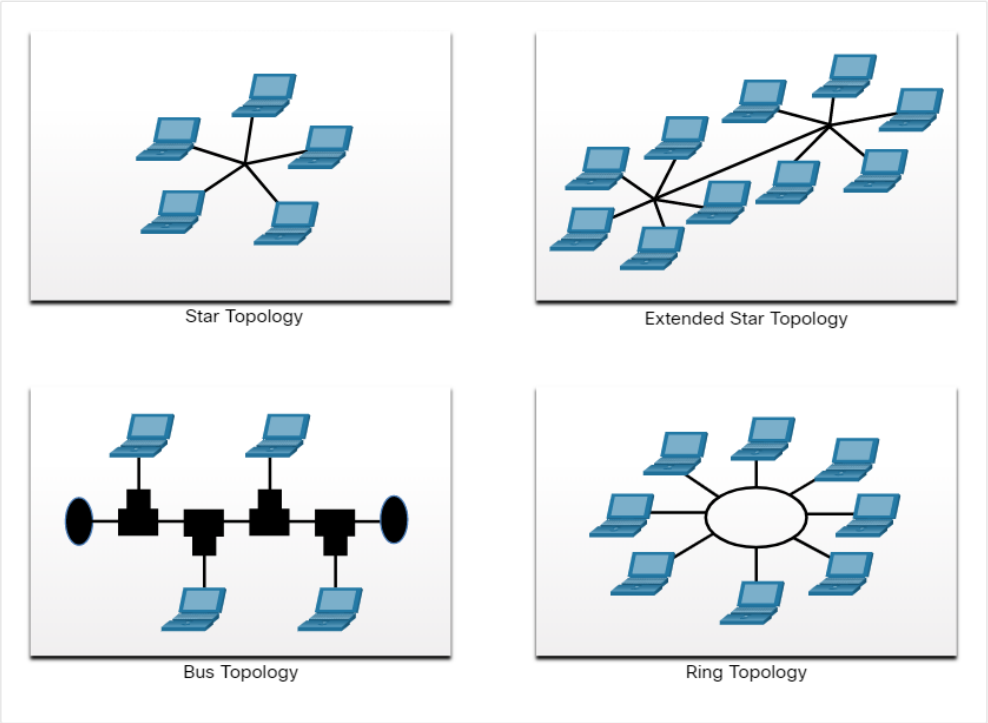


Difference between Star and Hub and Spoke

- Different context (LAN vs WAN)
- Star topology uses a hub or switch, while hub and spoke topology uses a central site as the hub.
- devices connect to the hub/switch directly. In hub and spoke, branch sites connect to a central hub.
- Star topology allows direct communication through the central device, whereas hub and spoke requires data to pass through the central hub for inter-spoke communication.

LAN TOPOLOGIES

Physical Topologies



Bus – All end systems chained together and terminated on each end.

- **Ring – Each end system is connected to its respective neighbors to form a ring.**

- **Star and extended star topologies are easy to install, very scalable and easy to troubleshoot.**

Half and Full Duplex Communication

Half duplex

- **Only allows one device to send or receive at a time on a shared medium.**

Full Duplex

- **Allows both devices to simultaneously transmit and receive on a shared medium.**

Contention-based access
CSMA/CD used on bus-topology
CSMA/CA used on Wireless LANS.

Controlled access
- Deterministic access where each node has its own time on the medium.
- Used on legacy networks such as Token Ring and ARCNET.

Data Link Frame
- **Header**
- **Data**
- **Trailer**

What fields are typically found in the header of a data link frame?

- Frame Start, Addressing, Type/Length, and Control.

The logical topology and physical media determine the data link protocol used:
- **Ethernet**
- **802.11 Wireless**
- **Point-to-Point (PPP)**
- **High-Level Data Link Control (HDLC)**
- **Frame-Relay**

What is the purpose of switch?
- **to forward data frames to the correct destination, which reduces collisions by creating separate collision domains.**

Chapter -6 (Ethernet)

- A family of networking technologies defined in the IEEE 802.2 and 802.3 standards, operating at the data link layer and physical layer
- IEEE 802.11 is used for WLAN
- IEEE 802.15 is used for WPANS.

MAC (Media Access Control) Sublayer:

- Responsible for data encapsulation and media access control. Provides data link layer addressing

Ethernet Frame

- The internal structure of data transmitted in Ethernet networks, including source and destination MAC addresses and error detection

MAC Address

- 48-bit address used for identifying devices on an Ethernet network, expressed in 12 hexadecimal digits

OUI is organizationally unique identifier the first (3 bytes) assigned by IEEE.

Vendored assigned by vendor.

Unicast MAC Address

- **One to One.**

Boardcast Address

- **One to many**
- **ARP (Address Resolution Protocol) requests.**

Multicast Address

- **One to specific group of devices**
- **Streaming a live video to a set of subscribed devices**

Switch Forwarding

Store-and-Forward Switching

- A method where the switch receives the entire frame and checks for errors before forwarding
- **determines if a frame has errors before propagating the frame**

Cut-Through Switching:

- A method where the switch starts forwarding the frame before it is completely received. Variants include fast-forward and fragment-free switching
- Very fast switching.

Fast-Forward Switching

- Forwards packets immediately after reading the destination address, potentially relaying faulty packets

Fragment-Free Switching

- Checks the first 64 bytes of a frame for errors before forwarding, balancing latency and data integrity

Port-Based Memory

- Stores frames in queues linked to specific ports, which may delay transmission if the destination port is busy

Shared Memory Buffering

- Uses a common buffer for all ports, dynamically allocating memory based on port requirements, useful in asymmetric switching

FCS (Frame Check Sequence)

- Error-checking field in the Ethernet frame used to detect errors in transmitted data

Chapter -7 (IPV6)

128 bits

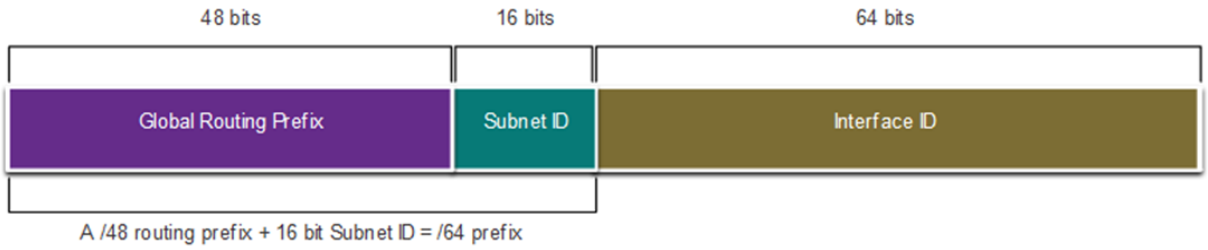
What is a Global Unicast Address (GUA)?

-These addresses are globally unique and routable on the IPv6 internet

- 2001:0db8 is commonly used prefix

What is a Link-Local Address (LLA)?

- **An LLA is required for every IPv6-enabled device and is used to communicate with other devices on the same local link.**
- **`fe80::` is the standard prefix for link-local addresses.**



Global routing prefix.

- **assigned by the provider , such as ISP, to customer**

Subnet ID

- **between GRP and Interface ID, used by organization**

Interface ID

- **host portion of an IPv4 address.**

****•Unicast – Unicast uniquely identifies an interface on an IPv6-enabled device.**

•Multicast – Multicast is used to send a single IPv6 packet to multiple destinations.

Anycast – This is any IPv6 unicast address that can be assigned to multiple devices.

Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

•**Router Solicitation (RS) messages are sent by host devices to discover IPv6 routers**

•**Router Advertisement (RA) messages are sent by routers to inform hosts on how to obtain an IPv6 GUA and provide useful network information such as:**

•**The RA can provide three methods for configuring an IPv6 GUA :**

•**SLAAC: IPv6 Stateless Address Auto-configuration**

•**SLAAC with stateless DHCPv6 server**

•**Stateful DHCPv6 (no SLAAC)**

SLACC (IPv6 Stateless Address Auto-configuration)

- **Function: Allows devices to automatically configure their own IPv6 addresses using information from Router Advertisements (RAs).**

- **Address Configuration: Devices generate their own addresses.**

- **Additional Information: No additional information (e.g., DNS) provided.**

SLACC (stateless DHCPv6)

- **Function:** Provides additional configuration information (e.g., DNS servers) to devices that have already configured their addresses using SLAAC.
- **Address Configuration:** Addresses are still self-configured using SLAAC.
- **Additional Information:** Provides configuration parameters not included in SLAAC.

Stateful DHCPv6

- **Function: Assigns IPv6 addresses and additional configuration information to devices.**
- **Address Configuration: DHCPv6 server assigns addresses to devices.**
- **Additional Information: Provides full configuration parameters, including IP addresses and other network settings.**

EUI-64 Process vs Randomly Generated

- When the Router Advertisement (RA) message indicates SLAAC (Stateless Address Autoconfiguration) or SLAAC with stateless DHCPv6, the client must create its own interface ID. This can be done using the EUI-64 process, which derives the ID from the device's MAC address, or by generating a random 64-bit number
- Adding 16 bit of fffe in the middle of mac address.

48-bit MAC	fc:99:47:75:ce:e0
EUI-64 Interface ID	fe:99:47:ff:fe:75:ce:e0

Randomly generated interface IDs

- Depending upon the operating system, a device may use a randomly generated interface ID instead of using the MAC address and the EUI-64 process

To ensure the uniqueness of any IPv6 unicast address, the client may use a process known as Duplicate Address Detection (DAD).

This is similar to an ARP request for its own address. If there is no reply, then the address is unique.

EUI-64 Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Random 64-bit Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

Well-known multicast addresses

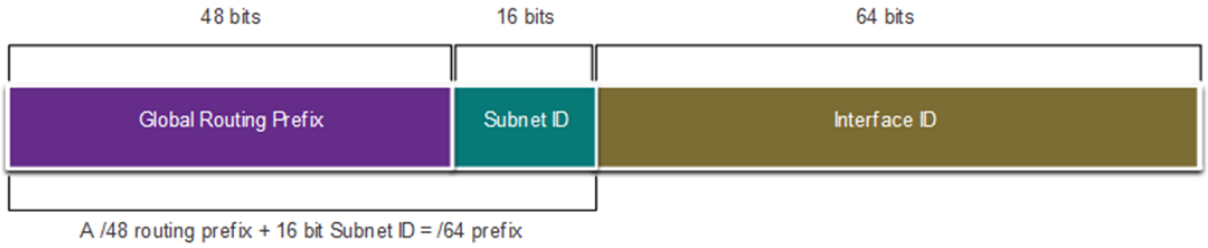
Solicited node multicast addresses

- **ff02::1 All-nodes multicast group** - This is a multicast group that all IPv6-enabled devices join. A packet sent to this group is received and processed by all IPv6 interfaces on the link or network.
- **ff02::2 All-routers multicast group** - This is a multicast group that all IPv6 routers join. A router becomes a member of this group when it is enabled as an IPv6 router with the **ipv6 unicast-routing** global configuration command.

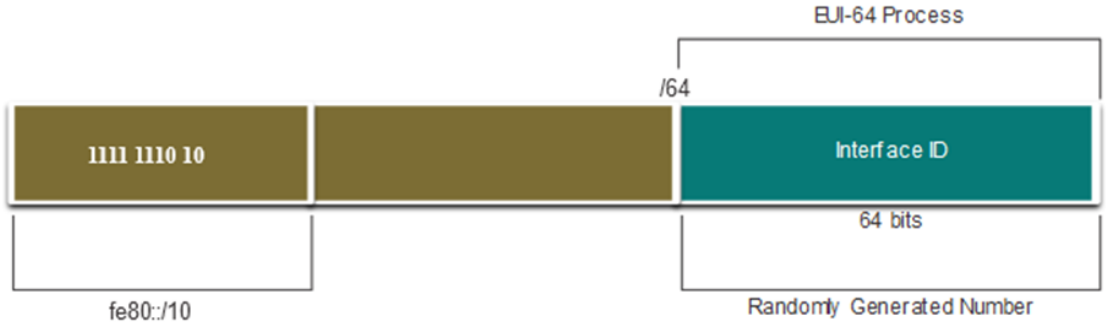
Subnet Using Subnet ID

- **A separate subnet ID field in the IPv6 GUA is used to create subnets.**
- **The subnet ID field is the area between the Global Routing Prefix and the interface ID.**

/64 prefix



Dynamic LLAs



- Like IPv6 GUAs, LLAs can be configured dynamically.

The figure shows the LLA is dynamically created using the fe80::/10 prefix

Chapter 8 (Transport Layer)

- Move that data between the application layer and internet layer(lower layers).
- Tracking the conversaion
- Segmenting and reassembling.
- Add headers information
- Identify , separate and manage multiple conversations
- IP does not know how to transfer the data, and so TCP and UDP in transport layer transfer the data from sender to receiver.

Segmentation

- Chopping the data into smaller parts.
- Adv – Efficiency , Error Control, Flow Control

Reassembling

- Reassemble the segmented data at the receiver's side to reconstruct the original message

What is the difference between a segment and a packet?

- Segment is a unit of data encapsulated at the transport layer.
- Packet is a unit of data encapsulated at the network layer.

Transmission Control Protocol (TCP)

- TCP is the most reliable protocol
- Remain the data until you terminate
- If the segment is lost in somewhere, TCP will find the place and regenerate those segments and send again.
- Connection-Oriented protocol

Advantages of TCP

- Reliability
- Ordered Data Delivery

- Error Detection
- Flow control (aware the limited resources and reduce the rate of data flow)
- Congestion Control (to manage network congestion and avoid packet loss)

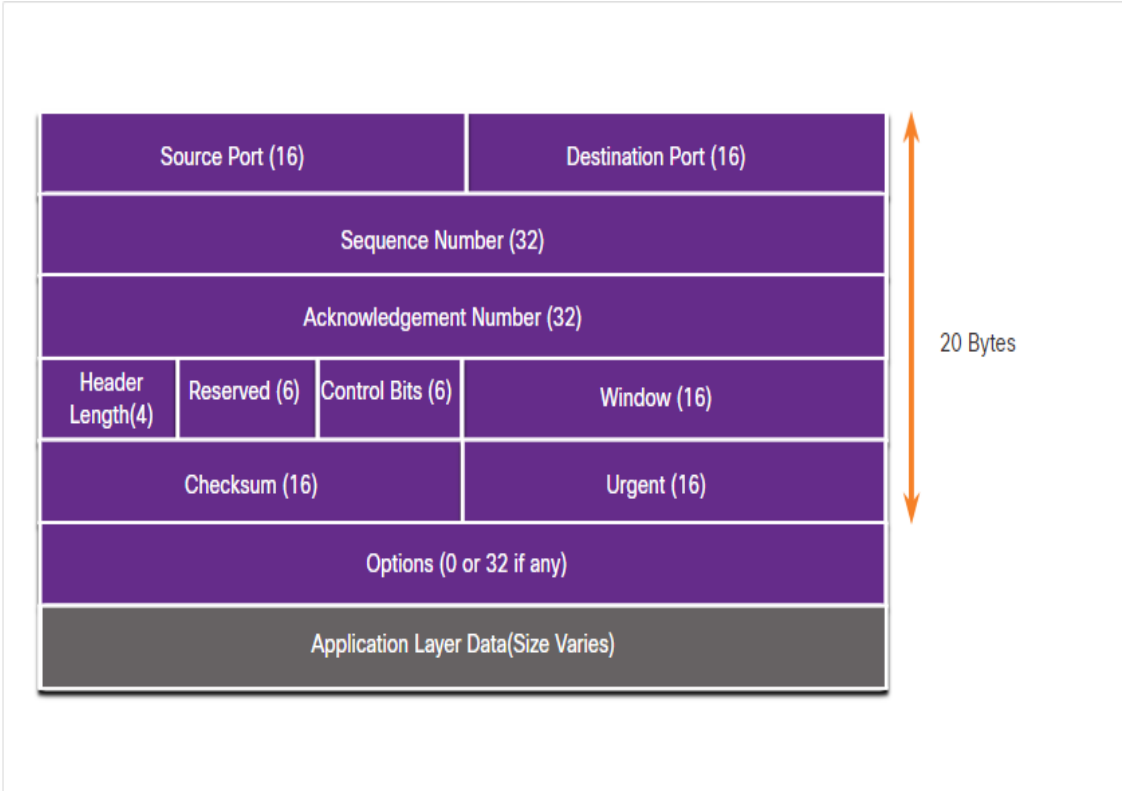
TCP features

- **Establish a session (a permanent connection)**
- **Ensures Reliable Delivery**
- **Provide Same-Order Delivery**
- **Support Flow Control**

TCP has **20 bytes**

UDP has **8 bytes**

- **Remember how many bits are there in each header.**



What is a sequence number in TCP?

- a value assigned to each byte in a TCP stream to keep track of data transmission and ensure reliability

What is an acknowledgment number in TCP?

- is used by the receiver to indicate the next expected byte from the sender

What is the purpose of the checksum in TCP/UDP headers?

- to detect errors in the transmitted data

TCP Header Field	Description
Source Port	A 16-bit field used to identify the source application by port number.
Destination Port	A 16-bit field used to identify the destination application by port number.
Sequence Number	A 32-bit field used for data reassembly purposes.
Acknowledgment Number	A 32-bit field used to indicate that data has been received and the next byte expecte
Header Length	A 4-bit field known as "data offset" that indicates the length of the TCP segment hea
Reserved	A 6-bit field that is reserved for future use.
Control bits	A 6-bit field used that includes bit codes, or flags, which indicate the purpose and f segment.
Window size	A 16-bit field used to indicate the number of bytes that can be accepted at one time
Checksum	A 16-bit field used for error checking of the segment header and data.
Urgent	A 16-bit field used to indicate if the contained data is urgent.

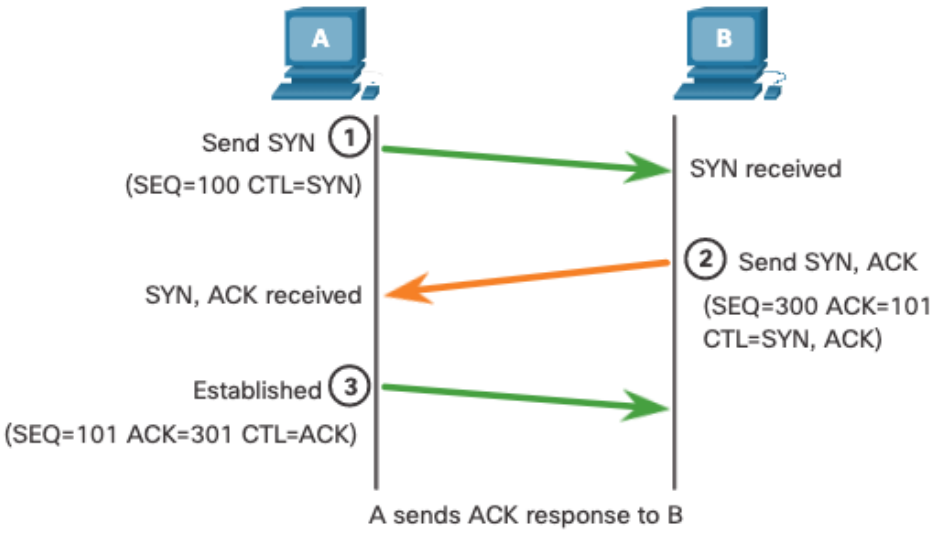
Applications that use TCP

- **FTP (file transfer protocol)**
- **SMTP (Simple Mail Transfer Protocol)**
- **HTTP (Hypertext Transfer Protocol)**
- **SSH (Secure Shell)**

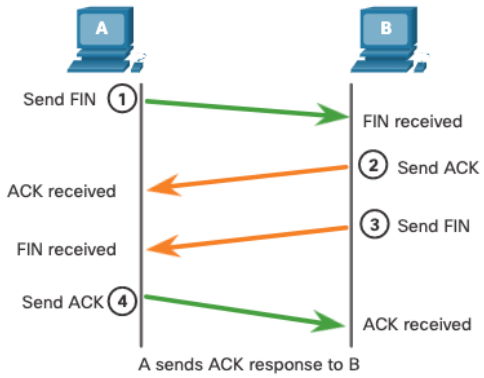
TCP Server Process

- Each server application uses a unique port number.
- Active ports accept and process segments.
- Correct socket requests are accepted and processed.

TCP 3 – Way Handshake



- The client sends a **SYN** packet to the server to initiate a connection.
- The server responds to the client's **SYN** packet with a **SYN-ACK** packet.
- The client sends an **ACK** packet back to the server to acknowledge the receipt of the server's **SYN-ACK** packet.
- The ACK packet contains the acknowledgment number
- After these three steps, the connection is established, and data transfer can begin.



Session Temination

- • Client FIN:
- Client sends FIN to indicate no more data.
- • Server ACK:
- Server acknowledges client's FIN with ACK.
- • Server FIN:
- Server sends FIN to terminate its session.
- • Client ACK:
- Client acknowledges server's FIN with ACK.

-

What is the purpose of the RST flag in TCP?

- used to reset a connection.

TCP Three-Way Handshake Analysis

- **URG** - Urgent pointer field significant
- **ACK** - Acknowledgment flag used in connection establishment and session termination
- **PSH** - Push function
- **RST** - Reset the connection when an error or timeout occurs
- **SYN** - Synchronize sequence numbers used in connection establishment
- **FIN** - No more data from sender and used in session termination

Selective Acknowledgment (SACK) in TCP

- The receiver can explicitly acknowledge received segments, including discontinuous ones.
- If both hosts support SACK, it is enabled.

TCP Flow Control

- Flow control helps maintain the reliability of TCP transmission by adjusting the rate of data flow between source and destination for a given session.
- MSS (Maximum Segment Size)
- **MSS is** the maximum amount of data a destination device can receive.
- A typical MSS value is 1,460 bytes when using IPv4.

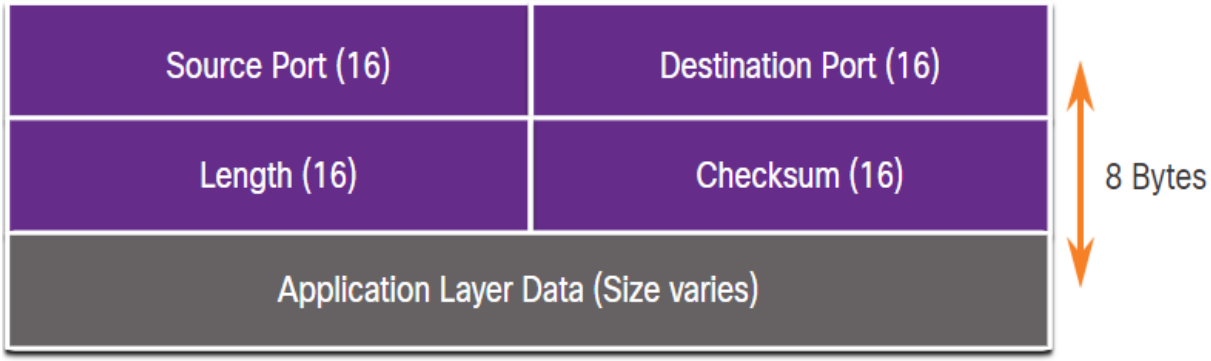
- calculated by subtracting the IP and TCP headers (total 40 bytes) from the default Ethernet MTU of 1500 bytes, resulting in 1460 bytes.
- 20 bytes for TCP and 20 bytes for IP.

To avoid and control congestion, TCP employs several congestion handling mechanisms, timers, and algorithms.

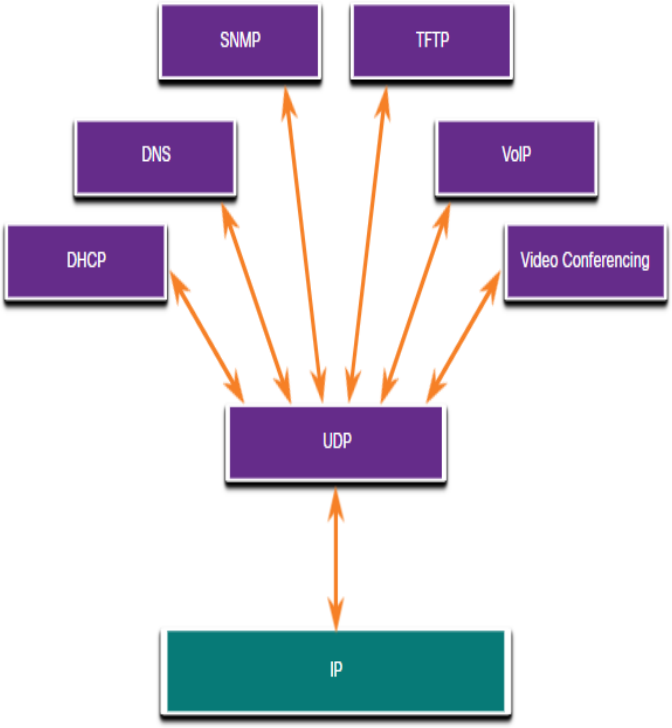
UDP (User Datagram Protocol)

- Data is reconstructed in the order that it is received.
- Any segments that are lost are not resent.
- There is no session establishment.
- The sending is not informed about resource availability.

UDP – 8 bytes



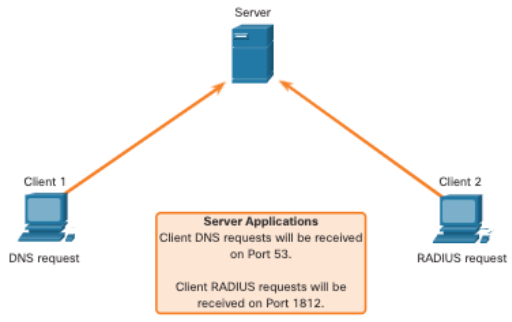
- **Source Port is the port used to identify source application.**
- **Destination Port is used to identify destination application.**
- **Length of UDP datagram header**
- **Checksum used for error checking**



- **SNMP (**Used for network management and monitoring)
- **TFTP (**file transfer protocol with minimal overhead)
- **DHCP (**Automatically assigns IP addresses)
- **DNS (**Translates domain names into IP addresses.)
- **VOIP (**Allows voice communication over IP networks.)
- **Video Conferencing (**Facilitates real-time video communication)

UDP Reassembly

- **Does not track the sequence of numbers like TCP does**
- **Does not reorder the datagrams**
- **So, When we use phone call, data is lost and cannot be retrackable.**
-



UDP SERVER PROCESS

- UDP-based server applications are assigned well-known or registered port numbers.
- UDP receives a datagram destined for one of these ports, it forwards the data to the

appropriate application based on its port number.

UDP CLIENT PROCESS

- **dynamically selects a port number from the range of port numbers and use as source port.**
- **destination port is usually the well-known**
- **client has selected the source and destination ports, the same pair of ports are used in the header of all datagrams in the transaction.**

PORT Numbers

-

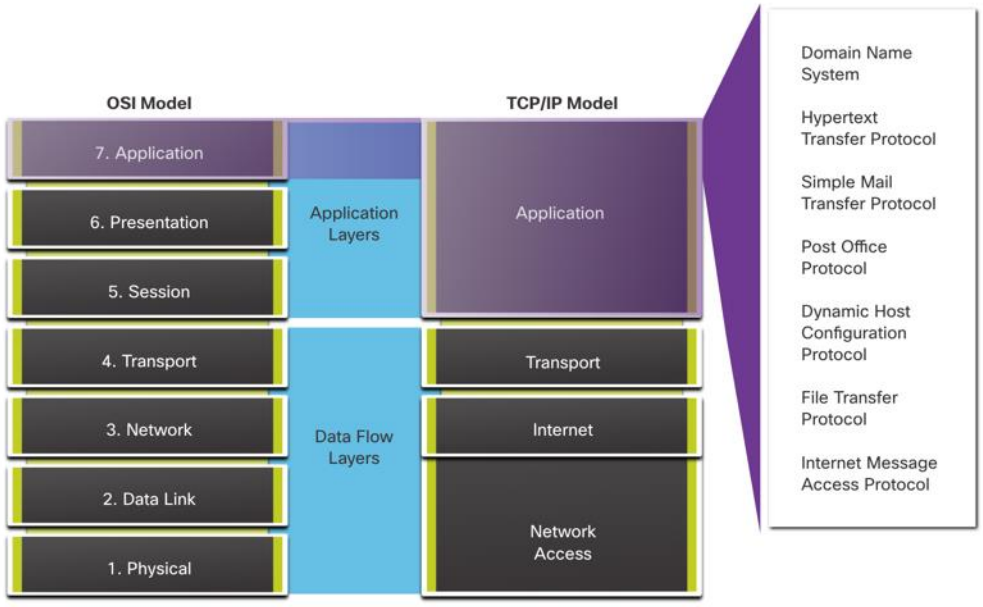
Port Group	Number Range
Well-known Ports	0 to 1,023
Registered Ports	1,024 to 49,151
Private and/or Dynamic Ports	49,152 to 65,535

Port Number	Protocol	Application
20	TCP	File Transfer Protocol (FTP) - Data
21	TCP	File Transfer Protocol (FTP) - Control
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	UDP, TCP	Domain Name Service (DNS)
67	UDP	Dynamic Host Configuration Protocol (DHCP) - Server
68	UDP	Dynamic Host Configuration Protocol - Client
69	UDP	Trivial File Transfer Protocol (TFTP)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol version 3 (POP3)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)

- **Remember this Services and PORT NUMBERS.**

Netstat is used for verification of connections.

Chapter -9 (APPLICATION LAYER)



- **The upper three layer include Application, Presentation and Session in TCP/TP model.**
- **provides the interface between the applications used to communicate.**
- **HTTP, FTP, TFTP, IMAP and DNS.**

How do the application, presentation, and session layers interact in the OSI model?

- provide network services to end user applications,
- where the application layer provides network services,
- the presentation layer ensures data is in a usable format, and
- the session layer manages sessions between applications.

Client Server Model

- the device requesting the information is called a client and the device responding to the request is called a server.
- **Application layer protocols describe the format of the requests and responses between clients and servers.**

Peer to Peer Networks

- two or more computers without the server.
- allows a device to act as **both a client and a server** within the same communication.
- **BitTorrent**
- Direct Connect
- eDonkey
- Freenet

Uniform Resource Locator (URL)

- http (the protocol or scheme)
- www.cisco.com (the server name)
- index.html (the specific filename requested)

Web and Email Protocols

What is the role of the SMTP protocol?

- SMTP is used to send email by connecting a client SMTP process with a server SMTP process on port 25.

How does POP protocol work?

- retrieves mail from a mail server and downloads it to the client, after which the messages are deleted from the server.

What is the difference between POP and IMAP protocols?

- Unlike POP, which deletes messages from the server after downloading, IMAP keeps the original messages on the server until manually deleted.

What is the primary function of HTTP?

- a protocol used to transfer web pages on the World Wide Web, utilizing ports 80 and 8080.

What is HTTPS and how does it differ from HTTP?

- the secure version of HTTP, using port 443 for encrypted communications.

What is the function of DNS?

- translates domain names like cisco.com into IP addresses.

DNS Message Format

- **A - An end device IPv4 address**
- **NS - An authoritative name server**
- **AAAA - An end device IPv6 address (pronounced quad-A)**
- **MX - A mail exchange record**

DNS message section	Description
Question	The question for the name server
Answer	Resource Records answering the question
Authority	Resource Records pointing toward an authority
Additional	Resource Records holding additional information

How does the HTTP request/response model work?

- an HTTP request (GET, POST, PUT) to a server, and the server responds with the requested resource or a status message.
- Get (request the message)
- POST (uploads data files to the web server, such as form data.
-)
- PUT (**uploads** resources or **content to the web** server, such as an image.)

File Sharing Services

What is the purpose of the FTP protocol?

- FTP allows for data transfers between a client and a server (21) for control traffic, and (20) for data transfers.

Describe the Server Message Block (SMB) protocol

- **Start, authenticate, and terminate sessions**
- **Control file and printer access**
- **Allow an application to send or receive messages to or from another device**
- **Unlike the file sharing supported by FTP, clients establish a long-term connection to servers.**

Chapter 10 (building Network)

redundancy **is required in the network design. Redundancy helps to eliminate single points of failure.**

Common Protocols

- **Types of Messages**
- **Syntax**
- **Meaning of informational fields**
- **How messages are sent and the expected response.**
- **Interaction with the next Lower Layer.**

****

Traceroute

•Traceroute can help locate Layer 3 problem areas in a network. A trace returns a list of hops as a packet is routed through a network.

Command	Description
show running-config	Verifies the current configuration and settings
show interfaces	Verifies the interface status and displays any error messages
show ip interface	Verifies the Layer 3 information of an interface
show arp	Verifies the list of known hosts on the local Ethernet LANs
show ip route	Verifies the Layer 3 routing information
show protocols	Verifies which protocols are operational
show version	Verifies the memory, interfaces, and licenses of the device

CDP provides the following information about each CDP neighbor device:

```
R3# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S3               Gig 0/0/1         122              S I   WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

Chapter 11 (Security)

- **Physical Security**
- **Network Security**

Malware

- **Virus**
- **Worms**
- **Trojans**
- **Ransomware**
- **Rootkits**
- **Backdoor**
- **keyloggers**
- **spyware**
- **adware**

Reconnaissance Attackes

•Reconnaissance attacks - The discovery and mapping of systems, services, or vulnerabilities.

•Access attacks - The unauthorized manipulation of data, system access, or user privileges.

Denial of service - The disabling or corruption of networks, systems, or services

Access Attacks

- **PAssword Attacks (brute force, trojan, sniffers)**
- **Truset exploitation (use unauthorized privileges to gain access)**
- **port redirection (use compromised system as a base for attacks)**
- **Man in the middle (positioned between two entities)**

DDOS Attackes

- **using a lot of devices to attack with infected hosts, zombies.**

Defense in Depth

- **VPN**
- **ASA firewal**
- **IPS**
- **ESA/WSA**
- **AAA Server**

Upgrade, Update and Patch

Authentication, Authorization, and Accounting

Authentication: Verifying identity.

Authorization: Granting access.

Accounting: Tracking usage.

Firewall

- DMZ enables Network Administrator to apply specific policies.

- •Packet filtering - Prevents or allows access based on IP or MAC addresses

- •Application filtering - Prevents or allows access by specific application types based on port numbers

- •URL filtering - Prevents or allows access to websites based on specific URLs or keywords

- Stateful packet inspection (SPI) - Incoming packets must be legitimate responses to requests from internal hosts.

Endpoint Security

- Policies often include the use of antivirus software and host intrusion prevention. More comprehensive endpoint security solutions rely on network access control

Devices Security

- **Encrypt all plain text password**
- **set strong password**
- **Deter Brute-forece password guessing attacks.**
- **Disable Exec mode**
- **Disable Unused services**

Chapter 12 (Network Layer)

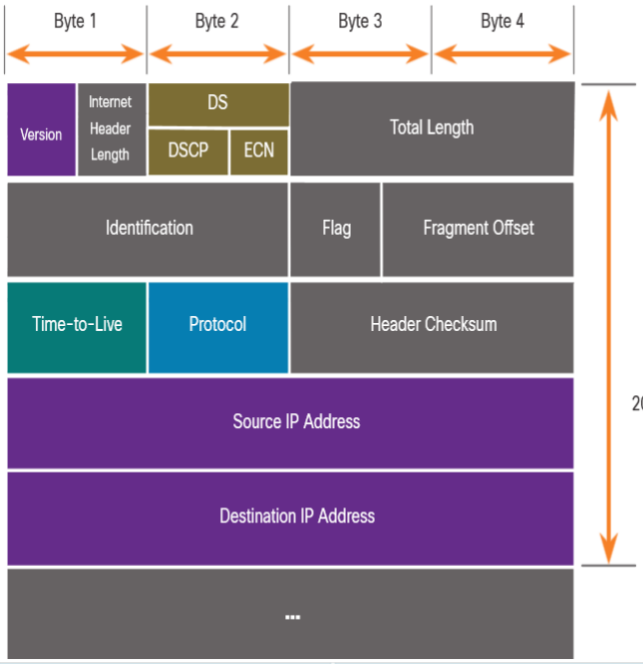
- **Connectionless**
- **Best Effort**
- **Media Independent**

Which layer will establish MTU?

- The network layer will establish the Maximum Transmission Unit (MTU).

Fragmentation is when Layer 3 splits the IPv4 packet into smaller units.

- Fragmenting causes latency.
- IPv6 does not fragment packets.
- Example: Router goes from Ethernet to a slow WAN with a smaller MTU



IP has 20 bytes

Function	Description
Version	This will be for v4, as opposed to v6, a 4 bit field= 0100
Differentiated Services	Used for QoS: DiffServ – DS field or the older IntServ – ToS or Type of Service
Header Checksum	Detect corruption in the IPv4 header
Time to Live (TTL)	Layer 3 hop count. When it becomes zero the router will discard the packet.
Protocol	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Source IPv4 Address	32 bit source address
Destination IPV4 Address	32 bit destination address

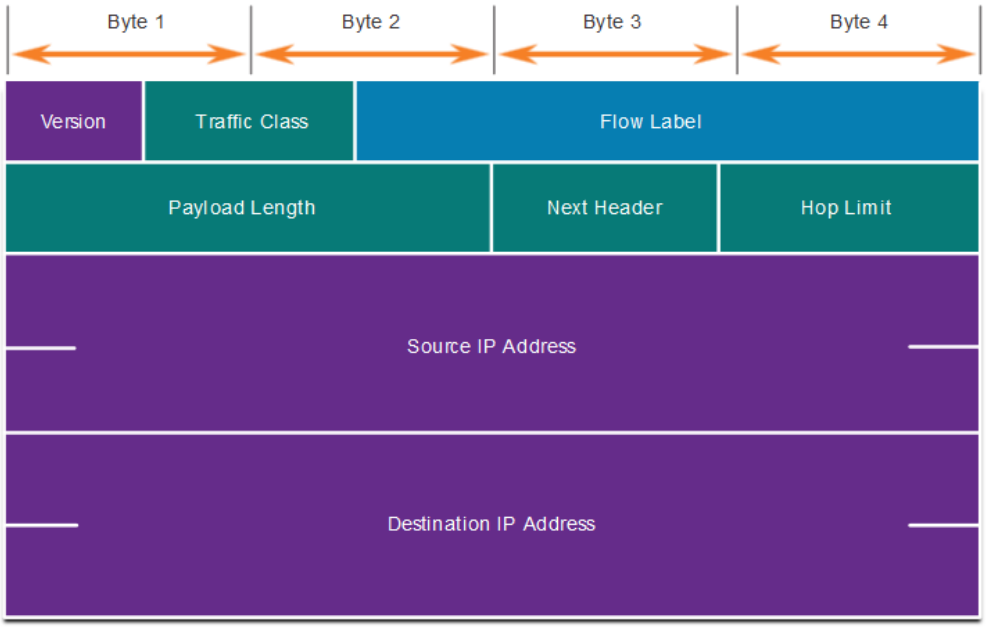
IPV6

- **IPv6 was developed by Internet Engineering Task Force (IETF).**

- Increased address space – based on 128 bit address, not 32 bits
- Improved packet handling – simplified header with fewer fields
- Eliminates the need for NAT – since there is a huge amount of addressing, there is no need to use private addressing internally and be mapped to a shared public address
- Several IPv4 fields were removed to improve performance.
- Some IPv4 fields were removed to improve performance:

- Flag
- Fragment Offset

- Header Checksum



Function	Description
Version	This will be for v6, as opposed to v4, a 4 bit field= 0110
Traffic Class	Used for QoS: Equivalent to DiffServ – DS field
Flow Label	Informs device to handle identical flow labels the same way, 20 bit field
Payload Length	This 16-bit field indicates the length of the data portion or payload of the IPv6 packet
Next Header	I.D.s next level protocol: ICMP, TCP, UDP, etc.
Hop Limit	Replaces TTL field Layer 3 hop count
Source IPv4 Address	128 bit source address
Destination IPV4 Address	128 bit destination address

HOST FORWARDING

- Packets are always created at the source.
- Each host devices creates their own routing table.
- A host can send packets to the following:
    - Itself – 127.0.0.1 (IPv4), ::1 (IPv6)
    - Local Hosts – destination is on the same LAN
    - Remote Hosts – devices are not on the same LAN

There three types of routes in a router's routing table:

- **Directly Connected** – These routes are automatically added by the router, provided the interface is active and has addressing.
- **Remote** – These are the routes the router does not have a direct connection and may be learned:
    - Manually – with a static route
    - Dynamically – by using a routing protocol to have the routers share their information with each other
- **Default Route** – this forwards all traffic to a specific direction when there is not a match in the routing table

- IP is connectionless, best effort, and media independent.
- IP does not guarantee packet delivery.
- IPv4 packet header consists of fields containing information about the packet.
- IPv6 overcomes IPv4 lack of end-to-end connectivity and increased network complexity.
- A device will determine if a destination is itself, another local host, and a remote host.
- A default gateway is router that is part of the LAN and will be used as a door to other networks.
- The routing table contains a list of all known network addresses (prefixes) and where to forward the packet.
- The router uses longest subnet mask or prefix match.
- The routing table has three types of route entries: directly connected networks, remote networks, and a default route.

Special Notes:

1.Which of the following is the name for all computers connected to a network that participate directly in network communication?

Host

2.When data is encoded as pulses of light, which media is being used to transmit the data?

Fiber optic

3. Which two devices are intermediary devices? (Choose two)

Router

Switches

4. Which network infrastructure provides access to users and end devices in a small geographical area, which is typically a network in a department in an enterprise, a home, or small business?]

Lan

5. Which network infrastructure might an organization use to provide secure and safe access to individuals who work for a different organization but require access to the organization's data?

Extranet

6. Which network infrastructure provides access to other networks over a large geographical area, which is often owned and managed by a telecommunications service provider?

Wan

7. Which connection physically connects the end device to the network?

Nic

8. Which connections are specialized ports on a networking device that connect to individual networks?

Interface

9. Which type of network topology lets you see which end devices are connected to which intermediary devices and what media is being used?

Logical topology

10. Which type of network topology lets you see the actual location of intermediary devices and cable installation?

Physical topology

11.When designers follow accepted standards and protocols, which of the four basic characteristics of network architecture is achieved?

Scalability

12. Confidentiality, integrity, and availability are requirements of which of the four basic characteristics of network architecture?

Security

13. With which type of policy, a router can manage the flow of data and voice traffic, giving priority to voice communications if the network experiences congestion?

QOS

14. Having multiple paths to a destination is known as redundancy. This is an example of which characteristic of network architecture?

Fault tolerance

15. Which feature is a good conferencing tool to use with others who are located elsewhere in your city, or even in another country.

Video communications

16. Which feature describes using personal tools to access information and communicate across a business or campus network?

BYOD

17. Which feature contains options such as Public, Private, Custom and Hybrid?

Cloud computing

18. Which feature is being used when connecting a device to the network using an electrical outlet?

Powerline

19. Which feature uses the same cellular technology as a smartphone?

Wireless broadband

20. Which attack slows down or crashes equipment and programs?

Denial of service dos

21. Which option creates a secure connection for remote workers?

Virtual private network (vpn)

22. Which option blocks unauthorized access to your network?

Firewall

23. Which option describes a network attack that occurs on the first day that a vulnerability becomes known?

Zero day or zero hour

24. Which option describes malicious code running on user devices?

Virus worm or trojan horse

25. During a routine inspection, a technician discovered that software that was installed on a computer was secretly collecting data about websites that were visited by users of the computer. Which type of threat is affecting this computer?

Spyware

26. Which term refers to a network that provides secure access to the corporate offices by suppliers, customers and collaborators?

Extranet

27. A large corporation has modified its network to allow users to access network resources from their personal laptops and smart phones. Which networking trend does this describe?

Bring your own device

28. What is an ISP?

It is an organization that enables individuals and businesses to connect to the internet

29. In which scenario would the use of a WISP be recommended?

A form in a rural are without wired broadband access

30. What characteristic of a network enables it to quickly grow to support new users and applications without impacting the performance of the service being delivered to existing users?

Scalability

31. A college is building a new dormitory on its campus. Workers are digging in the ground to install a new water pipe for the dormitory. A worker accidentally damages a fiber optic cable that connects two of the existing dormitories to the campus data center. Although the cable has been cut, students in the dormitories only experience a very short interruption of network services. What characteristic of the network is shown here?

Fault tolerance

32. What are two characteristics of a scalable network? (Choose two.)

..grown is size without impacting existing users

..suitable for modular devices that allow for expansion

33. Which device performs the function of determining the path that messages should take through internetworks?

A router

34. Which two Internet connection options do not require that physical cables be run to the building? (Choose two.)

…Cellular

…satellite

35. What type of network must a home user access in order to do online shopping?

the internet

36. How does BYOD change the way in which businesses implement networks?

BYOD provides flexibility in where and how users can access network resourced

37. An employee wants to access the network of the organization remotely, in the safest possible way. What network feature would allow an employee to gain secure remote access to a company network?

VPN

38. What is the Internet?

It provide connection through interconnected global networks

39. What are two functions of end devices on a network? (Choose two.)

…They originate the date that flows through the network

…They are the interface between humans and the communication

40. Which access method would be most appropriate if you were in the equipment room with a new switch that needs to be configured?

Console

41. Which access method would be most appropriate if your manager gave you a special cable and told you to use it to configure the switch?

Console

42. Which access method would be the most appropriate in-band access to the IOS over a network connection?

telnet/ssh

43. Which access method would be the most appropriate if you call your manager to tell him you cannot access your router in another city over the internet and he provides you with the information to access the router through a telephone connection?

Aux

44. Which IOS mode allows access to all commands and features?

Privileged EXEC mode

45. Which IOS mode are you in if the Switch(config)# prompt is displayed?

Global configuration mode

46. Which IOS mode are you in if the Switch> prompt is displayed?

User EXEC mode

47. Which two commands would return you to the privileged EXEC prompt regardless of the configuration mode you are in? (Choose two.)

Ctrl +Z

End

45. What is the command to assign the name “Sw-Floor-2” to a switch?

Hostname Sw-Floor-2

46. How is the privileged EXEC mode access secured on a switch?

Enable secret class

47. Which command enables password authentication for user EXEC mode access on a switch?

Login

48. Which command encrypts all plaintext passwords access on a switch?

Service password-encryption

48. Which is the command to configure a banner to be displayed when connecting to a switch?

banner motd

49. What is the structure of an IPv4 address called

Dotted-decimal format

50. how is an IPv4 address represented?

Four decimal numbers between 0 and 255 separated by periods

51. What type of interface has no physical port associated with it?

Switch virtual interface (SVI)

52. Which statement is true about the running configuration file in a Cisco IOS device?

it affect the operation of the device immediately when modified

53. Which two statements are true regarding the user EXEC mode? (Choose two.)

The device prompt for this mode ends with the “>”symbol

Only some aspects of the router configuration can be viewed

54. Which type of access is secured on a Cisco router or switch with the enable secret command?

Privileged EXEC

55.what is the default SVI on a cisco switch

VLAN1

56. When a hostname is configured through the Cisco CLI, which three naming conventions are part of the guidelines? (Choose three.)

No space

Begin with a letter

Fewer than 64

57. What is the function of the shell in an OS?

It interfaces between the users and the kernel

58. A router with a valid operating system contains a configuration file stored in NVRAM. The configuration file has an enable secret password but no console password. When the router boots up, which mode will display?

User EXEC mode

59. An administrator has just changed the IP address of an interface on an IOS device. What else must be done in order to apply those changes to the device?

Nothing must be done

60. Which memory location on a Cisco router or switch will lose all content when the device is restarted?

RAM

61. Why would a technician enter the command copy startup-config running-config?

To copy an existing configuration into ram

62. Which functionality is provided by DHCP?

Automatic assignment of an ip address to each host

63. Which two functions are provided to users by the context-sensitive help feature of the Cisco IOS CLI? (Choose two.)

Displaying a list of all available command within the current mode

Determining which option. Keyword or argument is available for the entered command

64. Which memory location on a Cisco router or switch stores the startup configuration file?

NVRAM

65. To what subnet does the IP address 10.1.100.50 belong if a subnet mask of 255.255.0.0 is used?

10.1.0.0

66. What is the process of converting information into the proper form for transmission?

Encoding

67. Which step of the communication process is concerned with properly identifying the address of the sender and receiver?

Formatting'

68. Which three are components of message timing? (Choose three.)

Flow control

Access method

Response timeout

69. Which delivery method is used to transmit information to one or more end devices, but not all devices on the network?

Multicast

70. BGP and OSPF are examples of which type of protocol?

Routing

71. Which two protocols are service discovery protocols? (Choose two.

DNS

DHCP

72. What is the purpose of the sequencing function in network communication?

To uniquely label transmitted segments of data for proper reassemble by receiver

73. This protocol is responsible for guaranteeing the reliable delivery of information.

TCP

74. Which of the following statements are true regarding network layer and data link layer addresses? (Choose three.

Network layer addresses are logical and date link addresses are expressed as 12 hexadecimal digits

Date link layer addresses are physical and network layer address are logical

Network layer addresses are either 32 or 128 bits in length

75.Which three acronyms/initialisms represent standards organizations? (Choose three.)

IANA ‘

IETF

IEEE

76. What type of communication will send a message to all devices on a local area network?
Broadcast
77. In computer communication, what is the purpose of message encoding?
To interpret information
78. Which message delivery option is used when all devices need to receive the same message simultaneously?
Broadcast

79. What are two benefits of using a layered network model? (Choose two.)
It prevent technology in one layer from affection other layers
It assist in protocol design
80.What is the purpose of protocols in data communications?
providing the rules required for a specific type of communication to occur
81.Which logical address is used for delivery of data to a remote network?
destination IP address
82.What is the general term that is used to describe a piece of data at any layer of a networking model?
protocol data unit
83.Which two protocols function at the internet layer? (Choose two.)

ICMP

IP

84.Which layer of the OSI model defines services to segment and reassemble data for individual communications between end devices?

transport

85.Which type of communication will send a message to a group of host destinations simultaneously?

multicast

86.What process is used to receive transmitted data and convert it into a readable message?

decoding

87.What is done to an IP packet before it is transmitted over the physical medium?

It is encapsulated in a Layer 2 frame.

88.What process is used to place one message inside another message for transfer from the source to the destination?

encapsulation

89.A web client is sending a request for a webpage to a web server. From the perspective of the client, what is the correct order of the protocol stack that is used to prepare the request for transmission?

HTTP, TCP, IP, Ethernet

90. When a connectionless protocol is in use at a lower layer of the OSI model, how is missing data detected and retransmitted if necessary?

Upper layer connection-oriented protocols keep trach of the data received and can request retransmission from the upper level protocols on the sending host

91. Which information is used by routers to forward a data packet toward its destination?

Destination ip address

92. Which field in an IPv4 packet header will typically stay the same during its transmission?

Destination address

93. Which field in an IPv6 packet is used by the router to determine if a packet has expired and should be dropped?

Hop limit