**TERM-2 CCNA Assignment**

**Module 7 Network fundamentals**

* **Advance Question**

1. Explain Network Topologies

* A network topology is the physical and logical arrangement of nodes and connections in a network. Nodes usually include devices such as switches, routers and software with switch and router features. Network topologies are often represented as a graph.

1. Explain TCP/IP Networking Model

* The TCP/IP model is a four-layer model that divides network communications into four distinct categories or layers. The model is often referred to as the TCP/IP stack. The four important layers are the application layer, the transport layer, the network layer, and the link layer.

1. Explain LAN and WAN Network

* LANs use local connections like ethernet cables and wireless access points. WANs use wide area connections like MPLS, VPNs, leased lines, and the cloud. LANs are faster, because they span less distance and have less congestion. WANs are slightly slower, but that may not be perceived by your users.

1. Explain Operation of Switch

* Switches may be operated by process variables such as pressure, temperature, flow, current, voltage, and force, acting as sensors in a process and used to automatically control a system. For example, a thermostat is a temperature-operated switch used to control a heating process.

1. Describe the purpose and functions of various network devices

* A network device is a node in the wireless mesh network. It can transmit and receive wireless HART data and perform the basic functions necessary to support network formation and maintenance. Network devices include field devices, router devices, gateway devices, and mesh hand-held devices. Field devices.

1. Make list of the appropriate media, cables, ports, and connectors to connect switches to other

* To connect switches to other network devices, you'll need a variety of media, cables, ports, and connectors, depending on the specific requirements of your network. Here's a list of some common components you might need:

1. Ethernet Cables:

Ethernet Patch Cable (Cat5e, Cat6, Cat6a, Cat7, Cat8): These cables are used to connect switches to various network devices, such as computers, servers, routers, and other switches. The choice of cable category depends on the required data rates and distance.

1. Fiber Optic Cables:

Single-mode or Multi-mode Fiber Cables: Fiber optic cables are used for high-speed and long-distance connections between switches. Choose single-mode for longer distances and multi-mode for shorter distances.

1. Ethernet Ports:

RJ-45 Ports: These are standard Ethernet ports commonly used for copper Ethernet connections. They are found on most switches and network devices.

1. Fiber Optic Ports:

SFP/SFP+ Ports: Small Form-Factor Pluggable (SFP) or Enhanced Small Form-Factor Pluggable (SFP+) ports are used for fiber optic connections. You can use SFP/SFP+ transceivers to adapt the ports to different types of fiber.

1. Console Port:

RS-232 or USB Console Port: These ports are used for initial configuration and management of switches. RS-232 is more traditional, while some modern switches offer USB console ports.

1. Power Connectors:

AC Power Cord: Most switches require an AC power cord to connect to a power source.

DC Power Connector: Some switches may use DC power connectors, especially in telecom and data center environments.

1. Media Converters:

Ethernet to Fiber Media Converters: These devices convert between Ethernet and fiber optic connections, allowing you to connect switches with different media types.

1. Patch Panels:

Ethernet Patch Panels: Used to organize and terminate Ethernet connections in a structured cabling system. They are useful in data centers and larger installations.

1. Ethernet Couplers and Adapters:

RJ-45 Couplers: Sometimes used to extend Ethernet cable lengths.

Ethernet Adapters: Convert between different Ethernet connector types (e.g., RJ-45 to RJ-45 or RJ-45 to USB).

1. Network Switch:

Make sure you have a switch with enough available ports to accommodate your network connections. Choose a switch with the appropriate number of Ethernet and/or fiber ports, depending on your network needs.

1. Rack or Enclosure:

If you're setting up a network in a data center or server room, you'll need a rack or enclosure to mount your switches and other network equipment.

1. Define Network devices and hosts

* A network node is any device participating in a network. A host is a node that participates in user applications, either as a server, client, or both. A server is a type of host that offers resources to the other hosts. Typically a server accepts connections from clients who request a service function.

1. What are Ethernet Standard (802.3) and Frame Formats?

* Ethernet (IEEE 802.3) Frame Format: PREAMBLE – Ethernet frame starts with a 7-Bytes Preamble. This is a pattern of alternative 0's and 1's which indicates starting of the frame and allow sender and receiver to establish bit synchronization.
* **Intermediate Question**

1. Comparison between UTP, MM and SM Ethernet Cabling

* UTP (Unshielded Twisted Pair), MM (Multi-Mode) Fiber, and SM (Single-Mode) Fiber are three common types of Ethernet cabling used in networking. Let's compare them in terms of key characteristics:

1. Transmission Medium:

* UTP: UTP cables are copper-based and use twisted pairs of copper wires for signal transmission. They are the most common type of Ethernet cabling.
* MM Fiber: MM Fiber uses glass or plastic fibers to transmit data in the form of light signals.
* SM Fiber: SM Fiber also uses glass or plastic fibers but is designed for longer distances and uses a single path for data transmission.

1. Distance:

* UTP: UTP cables are typically limited to shorter distances, generally up to 100 meters (328 feet) for Gigabit Ethernet.
* MM Fiber: MM Fiber can support longer distances than UTP, typically up to 550 meters (1804 feet) for Gigabit Ethernet using OM4 fiber.
* SM Fiber: SM Fiber is designed for much longer distances, potentially reaching tens of kilometers for Gigabit Ethernet.

1. Data Rates:

* UTP: UTP cables can support various data rates, including 10/100/1000/10,000 Mbps (Gigabit).
* MM Fiber: MM Fiber can support higher data rates, including Gigabit and 10 Gigabit Ethernet.
* SM Fiber: SM Fiber is capable of even higher data rates, including 10 Gigabit, 40 Gigabit, and 100 Gigabit Ethernet.

1. Immunity to Interference:

* UTP: UTP cables are susceptible to electromagnetic interference (EMI) and radio-frequency interference (RFI) due to their unshielded nature.
* MM Fiber: Fiber optic cables are immune to EMI and RFI because they transmit data as light signals.
* SM Fiber: Like MM Fiber, SM Fiber is also immune to EMI and RFI.

1. Cost:

* UTP: UTP cables are typically the most cost-effective option for shorter-distance Ethernet connections.
* MM Fiber: MM Fiber is more expensive than UTP but can be cost-effective for longer-distance connections.
* SM Fiber: SM Fiber is generally the most expensive option due to its advanced technology and long-distance capabilities.

1. Connector Types:

* UTP: Common connectors for UTP cables include RJ-45 connectors.
* MM Fiber: Common connectors for MM Fiber include LC and SC connectors.
* SM Fiber: Common connectors for SM Fiber include LC and SC connectors.

1. Use Cases:

* UTP: UTP cables are often used for LAN connections within buildings, data centers, and short-distance connections where EMI/RFI is not a concern.
* MM Fiber: MM Fiber is suitable for medium-distance connections within data centers and campus networks.
* SM Fiber: SM Fiber is ideal for long-distance connections, such as connecting buildings across a campus or for telecommunications infrastructure.

1. Make Cross cable

* Done.

1. Make Straight-Through Cable

* Done.

1. Differentiate between LAN/WAN operation and features

* LANs use local connections like ethernet cables and wireless access points. WANs use wide area connections like MPLS, VPNs, leased lines, and the cloud. LANs are faster, because they span less distance and have less congestion. WANs are slightly slower, but that may not be perceived by your users.

1. Explain ARP, ICMP and Domain name

* ARP (Address Resolution Protocol) is a protocol used to map an IP address to a physical (MAC) address on a local network. ARP is used when a device wants to communicate with another device on the same network, but it only knows the IP address of the destination device.

1. Describe the components required for network and Internet communications

* Some important network components are NIC, switch, cable, hub, router, and modem. Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

1. Explain Encapsulation and DE capsulation in OSI Reference model

* Encapsulation adds information to a packet as it travels to its destination. Decapsulation reverses the process by removing the info, so a destination device can read the original data. Many people take networks for granted, despite the significant roles they play in our daily lives.

1. Explain network segmentation and basic traffic management concepts

* When we segment a network, we divide it into multiple smaller networks, each acting as its own small network called a subnet. We can control the flow of traffic between subnets, allowing or disallowing traffic based on a variety of factors, or even blocking the entire flow of traffic if necessary.

1. What is flow control and acknowledgment?

* It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver. In data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver.
* **Advance question**

1. Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

* OSI Model:

1. The OSI model consists of seven layers, each responsible for a specific aspect of network communication. Here's how data flows through the OSI model:
2. Physical Layer (Layer 1):

* At this layer, data is converted into electrical signals, light pulses (for optical connections), or radio waves (for wireless connections).
* Protocols: Ethernet, USB, Bluetooth, Wi-Fi.

1. Data Link Layer (Layer 2):

* This layer is responsible for framing the data into packets, adding MAC (Media Access Control) addresses, and error detection/correction.
* Protocols: Ethernet, MAC addresses, IEEE 802.1Q (for VLANs).

1. Network Layer (Layer 3):

* The network layer is responsible for routing packets between different networks. It uses logical addressing (e.g., IP addresses) to identify devices and routes packets accordingly.
* Protocols: IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol).

1. Transport Layer (Layer 4):

* The transport layer ensures reliable data transfer between two devices. It breaks data into segments, adds sequencing and error checking, and manages flow control.
* Protocols: TCP (Transmission Control Protocol), UDP (User Datagram Protocol).

1. Session Layer (Layer 5):

* The session layer establishes, maintains, and terminates communication sessions between two devices. It handles session synchronization and checkpoints.
* Protocols: NetBIOS, RPC (Remote Procedure Call).

1. Presentation Layer (Layer 6):

* This layer is responsible for data translation, encryption, and compression to ensure data is in a format that the receiving device can understand.
* Protocols: SSL/TLS (Secure Sockets Layer/Transport Layer Security).

1. Application Layer (Layer 7):

* The application layer is where user applications and network services interact. It provides a platform-independent interface for application software.
* Protocols: HTTP, FTP, SMTP, POP3, DNS.

TCP/IP Model:

The TCP/IP model is a simplified model with four layers, which closely align with the OSI model. Here's how data flows through the TCP/IP model:

Link Layer (equivalent to OSI Layers 1 and 2):

* Similar to the data link layer, it handles physical addressing and framing.
* Protocols: Ethernet, ARP.

Internet Layer (equivalent to OSI Layer 3):

* Equivalent to the network layer in OSI, it routes packets across networks using logical IP addressing.
* Protocols: IP, ICMP.

ransport Layer (equivalent to OSI Layer 4):

* Similar to the transport layer in OSI, it ensures reliable data transfer.
* Protocols: TCP, UDP.

Application Layer (equivalent to OSI Layers 5, 6, and 7):

* Combines functionalities of the session, presentation, and application layers in OSI.
* Protocols: HTTP, FTP, SMTP, POP3, DNS.

1. Identify and explain at layers 1, 2, 3, and 7 using a layered model approach

* Layer 1- Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

Layer 2- Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.

The Data Link Layer is divided into two sublayers:

Logical Link Control (LLC)

Media Access Control (MAC)

Layer 3- Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

Layer 7- Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

1. Explain CSMA/CD and CSMA/CA

* The CSMA/CD type is utilized to identify a shared channel collision. It's a mechanism for detecting collisions and works with both wired and wireless networks. While CSMA/CA is used to keep a shared channel free of collision. And it's a mechanism for avoiding collisions and can connect to wireless networks.

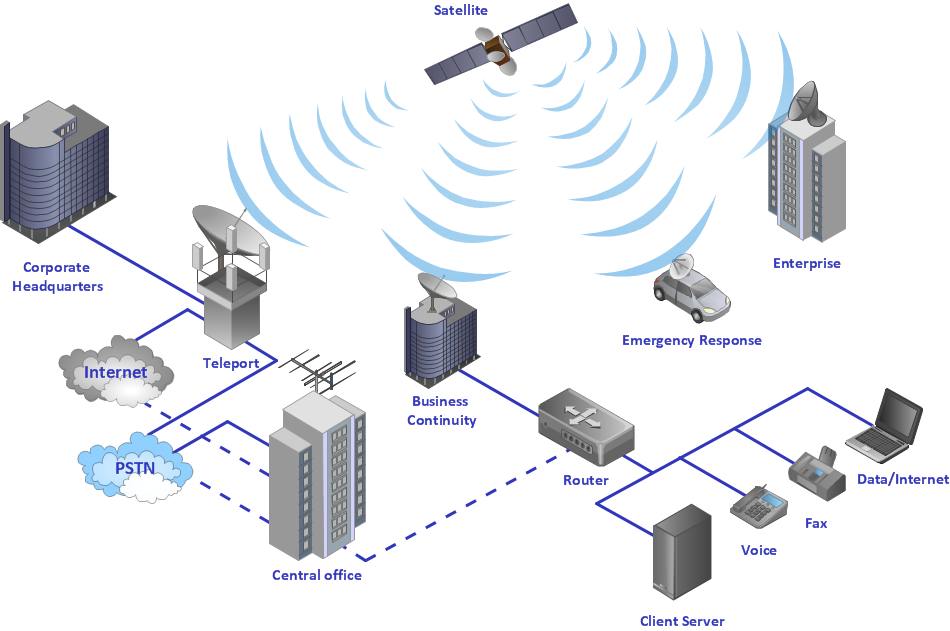
1. Explain this frame and find layer

* Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy. Frame is continuously used in Time Division Multiplexing process.

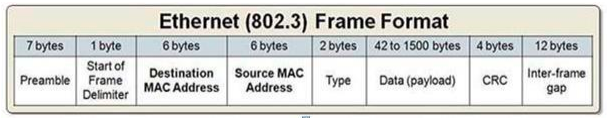
1. Draw and explain Cisco hierarchical model

* The Three-Layered Hierarchical Model in Cisco divides a network into the following three layers: The Access Layer: Provides access points for hosts to connect to the network. The Distribution Layer: Acts as an intermediary between the Core Layer and the Access Layer, and keeps local traffic confined to local networks.

1. Drawing of a typical wired and wireless enterprise LAN



7. Describe the uses of straight-through and crossover Ethernet cables

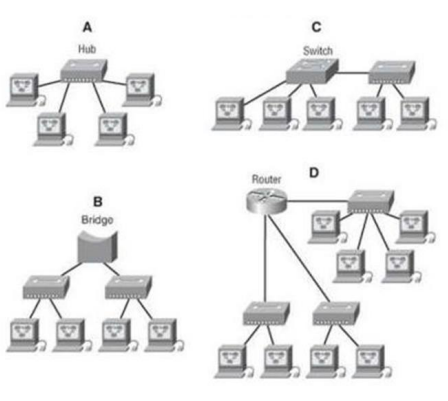


* Straight-through cables are mainly used for connecting non-similar devices, while crossover cables are mostly used for connecting similar devices. Straight-through cable connects a computer with a DSL modem, while Crossover cable connects Router to Router and Computer to Computer.

8. Explain Layer 2 and Layer 3 Switch

* The layer 2 and Layer 3 differs mainly in the routing function. A Layer 2 switch works with MAC addresses only and does not care about IP address or any items of higher layers. Layer 3 switch, or multilayer switch, can do all the job of a layer 2 switch and additional static routing and dynamic routing as well.

9. Identifying Collision and Broadcast Domains



* A collision domain is defined as the domain in which, the signals that are transmitted by the devices over the network collide with each other. A broadcast domain is a domain that consists of all the devices that can receive a broadcast message that is sent by any other device which is present in the domain.

1. Explain Spanning Tree Protocol

* Spanning Tree Protocol (STP) is a Layer 2 network protocol used to prevent looping within a network topology. STP was created to avoid the problems that arise when computers exchange data on a local area network (LAN) that contains redundant paths.

1. Explain Unicast, Multicast and Broadcast

* So let's begin to summarize the difference between these three: Unicast: from one source to one destination i.e. One-to-One. Broadcast: from one source to all possible destinations i.e. One-to-All. Multicast: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many.

1. Explain CAM (Content Addressable Memory)

* Content-addressable memory (CAM) is computer memory that operates like a hardware search engine for search-intensive applications. CAM is capable of searching its entire contents in a single clock cycle.

1. Explain CAM (Ternary Content Addressable Memory)

* TCAM (ternary content-addressable memory) is a specialized type of high-speed memory that searches its entire contents in a single clock cycle. The term “ternary” refers to the memory's ability to store and query data using three different inputs: 0, 1 and X.

1. Which command use of Show MAC TABLE?

* To display the MAC table, enter the show mac-address command.