**TERM-2 CCNA Assignment**

**Module 7 Network fundamentals**

 Advance Question

1. Network topology is a connection of a various devices to communicate with each other network.
2. Application, Transport, Internet, Network
3. LAN – Two or more than two devices are connected with each other in same network its called LAN

WAN – Two or more than two MAN are connected

1. A switch is work on datalink layer of the osi model and send the data packet to the destination devices and the first packet will deliver as broadcast packet and its called BPDU packet.
2. NIC – It is a network adaptor to connect the computer network.

SWITCH – A switch is works at data link layer of the OSI model.

Router – It is use for connect two different network together.

1. Straight Cable – they are used to connect two different device.

Crossover Cable – they are used to connect same device.

Rollover Cable – they are used to configure Router.

1. Network Device – A network device is an individual component of the network that participates at one or more of protocol layers.

Hosts – A host is any hardware device that has the capability of permitting access to a network via user interface.

1. In case of classic ethernet it is an 8 byte filed and in case IEEE 802.3 it is 7 bytes. Start of frame delimiter. It is a 1 byte filed in a IEEE 802.3 Frane that contains an alternating pattern of ones and zeros ending with two ones.

 Intermediate Question

1. Comparison between UTP, MM and SM Ethernet Cabling.
2. Done in lab.
3. Done in lab.
4. LAN and WAN are two types of computer network while LAN network are used for localized area and WAN network are used for Wide area network.
5. ARP – it is used for converting IP address to mac address

ICMP – it is stand for internet control message protocol

Domain Name – a domain name is an easy to remember name that’s associated with a physical IP address on the internet.

1. Client, server, channels, Interface devices, OS
2. The data is encapsulated in every layer at the sender’s side and also de-encapsulated in the same layer at the receiver’s end of the OSI model.
3. Network segmentation divides a network into multiple zones and manages each zone or segment.
4. It is a set measures taken to regulate the amount of data that a sender sends so that a fast sender does not over 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. The department of defence model is basically a condensed version of the OSI model – it’s composed of four instead of seven layers – Application, Transport, Internet, Network Access.
2. Physical Layer – it is a lowest layer of OSI model and it is convert all data into bit format.

Data link layer – The data link layer is responsible for the node to node delivery of the message.

Network Layer – The network layer works for the transmission of data from one host to the other located in different network.

Application Layer – It is the top layer of OSI model and it is communicates between web client and web server.

1. CSMA/CD – Carries sense multiple access with collision detection. It is used to control the traffic in the switch in wire network.

CSMA/CA - Carries sense multiple access with collision Avoidance. It is use to control traffic in wireless network.

1. A frame is the protocol data unit at the data link layer. Frames are the result of the final layer of encapsulation before the data is transmitted over the physical layer.
2. Done in lab
3. Done in lab
4. Straight Cable – It is mainly used for connect different device.

Crossover Cable – It is used for connecting same devices.

|  |  |
| --- | --- |
| Layer 2 | Layer 3 |
| Unmanageable | Manageable |
| It has no storage space | It uses NVRAM |
| It stores temporary files | It stores permanent files. |

1. A broadcast domain is a type of domain where in traffic flows all over the network. The collision domain refers to a set of devices in which packet collision could occur.
2. STP stop the loop which occurs when you have multiple links between switch . STP is open standard.
3. Unicast – It has one sender and one receiver.

Multicast – It has one sender multi receiver but not all

Broadcast – It has one sender all receiver.

1. Explain CAM ( Content Addressable Memory)
2. Explain CAM (Ternary Content Addressable Memory)
3. Show mac-address

**Module 8 Network Access**

 Beginner Question

1. Switch are networking devices operating at layer 2 or a data link layer of the OSI model. A switch has many ports, to which computers are plugged in.
2. First the switch loads a power on self test program stored in ROM.

Next, the switch loads the boot loader software

The boot loader performs low-level CPU initialization.

The boot loader initializes the flash file system on the system board.

1. You can access the CLI through a console connection, through telnet, a SSH or by using browser.
2. Cisco IOS is a proprietary OS that runs on cisco systems routers and switches.
3. It is a smart network devices that function as a multiport network bridge.
4. Done in lab.
5. Done in lab.
6. Done in lab.
7. Done in lab.
8. Done in lab.
9. In a switch if we have created group then its called VLAN.
10. VTP is Cisco proprietary protocol used to maintain consistency throughout the network.
11. CDP is a network discovery tool, which assists network administrators and engineers in identifying neighbouring Cisco devices.
12. Each VLAN is identified by a single IP Subnetwork.
13. STP stops the loops which occurs when you have multiple links between switches.
14. IPv4 allows for a variation of the network and host segments of an IP address, known as subnetting.
15. A Subnet mask is defined as a 32 bit address that segregates an IP address into network bits that identify the network and host bits that identify the host device operating on the network.
16. Binary representation which is a base 2, and hexadecimal representation which is a base 16 representation.
17. Public IP can be seen by other devices on the Internet and Private IP can not.
18. Subnet mask prefixes identify the range of IP address that make up a subnet or group of IP address on the same network.
19. Router and Switch connect using a Ethernet Cable.
20. Enable – to enter enable mode, Configure terminal – to enter configure mode.
21. Done in lab.
22. Done in lab.
23. Done in lab.
24. EIGRP is a network protocol that enables routers to exchange information more efficiently than earlier network protocols.
25. OSPF broadcast interface is connected to a shared network.
26. A logical collections of OSPF networks, routers, links that have the same area identification.
27. OSPF use a DR and BDR on each multi access network.
28. OSPF is a link state routing protocol that sends information about directly connected links to all routers in the network.
29. IPv6 address is 128 bits in length.
30. Wireless technology refers to the seamless transmission of data without physical connections.
31. Mobile, Laptop, Radio, TV Remote.
32. Wireless Security is the protection of devices and network connected in a wireless environment.

 Intermediate Question

1. Done in lab.
2. Switch user mode – for switch user, enable mode – to enable the router, Configuration mode – to Configure router.
3. To connect multi devices in same network like PCs, printer.
4. SSH is a network communication protocol that enable two computers
5. Done in lab.
6. TELNET is a network protocol for enabling computers to connect to local computer.
7. Done in lab.
8. Done in lab.
9. Done in lab.
10. Done in lab.
11. VLAN use for create group in switch
12. Static VLAN is create manually like VLAN name, ID, port.
13. Dynamic VLAN is automatically assign VLAN
14. Done in lab.
15. Done in lab.
16. Done in lab.
17. Done in lab.
18. Port security is a network administrator can associate specific MAC addresses with the interface.
19. Class A – 255.0.0.0 Class B – 255.255.0.0 Class C – 255.255.255.0
20. CIDR address are represented using a slash notation, which specifies the number of bits in the network prefix.
21. Class A – 0-126, Class B – 128-191, Class C – 192-233.
22. Classful Addressing is uses fixed length subnet masks, Classless uses variable length subnet mask.
23. VLSM is IP network into subnet with different subnet masks.
24. Static routing does not have the ability to select the path on its own path.
25. Default routing is the method where the router is configured to send all packets towards a single router.
26. Done in lab.
27. Done in lab.
28. Done in lab.
29. Done in lab.
30. IPv6 is more secure.
31. IPv6 is use MNC Company for secure the network.
32. Done in lab.
33. Wireless Access Point is a networking device that allows wireless capable devices to connect to a wired network.

 Advance question

1. Done in lab.
2. Done in lab.
3. Done in lab.
4. Done in lab.
5. Done in lab.
6. Done in lab.
7. Done in lab.
8. Done in lab.
9. Layer 3 Switch after configured we can use, NV RAM
10. Done in lab.
11. 802.1q Protocol is the networking standards that supports virtual LANs on an Ethernet network.
12. Switch port mode command allows us to configure the trunking mode.
13. Removing command of VLAN use to remove all VLANs from the Switch ethernet port.
14. VLAN routing use for create group in Switch.
15. It requires routers to exchange information with other router to learn about paths.
16. Routing loop are formed when an error occurs in the operation of the routing algorithm.
17. Done in lab.
18. Done in lab.
19. Done in lab.
20. Done in lab.
21. Done in lab.
22. Done in lab.
23. Done in lab.
24. First IP Address is called the network address and last IP Address is called broadcast address.
25. Classful network is fixed length subnet mask.
26. Done in lab.
27. Done in lab.
28. Done in lab.
29. Two or more then devices connected in each other.
30. 192.168.55.1/30
31. A routed protocol can be used by all hosts on the internetwork.
32. IGP are the protocols used within a domain for the exchange of routing information.
33. Distance-vector routing protocols make routing decisions based on hop count, link-state routing protocols are able to consider multiple factors such as bandwidth and Hybrid routing protocols exhibits both types.
34. Done in lab.
35. A wildcard mask allows or denies all the traffic from a network IP address.
36. Physical Address and Logical address
37. Done in lab.
38. RIP is Open standard protocol, EIGRP is hybrid routing protocol, OSPF is Standard protocol.
39. Done in lab.
40. Wireless topology is simply the way network components are arranged.

**Module 9 CCNA -IP connectivity and IP services**

 Beginner Question

1. Standard, Extended, Dynamic ACLs
2. DHCP is automatically provides an IP host with its IP.
3. Discover Offer Request Acknowledgment.
4. NAT is a router function where IP address of IP datagrams are replaced at the boundary of a private network.

 Intermediate Question

1. Disabling unused services running on the router.
2. Switch port security provide the ability to limit what address will be allowed to send traffic on individual switchports.
3. Access-list access-list-number {permit|deny}{host|source source-wildcard|any}
4. DHCP relay agent is to forward the DHCP messages to other subnets so that the DHCP server does not have to be on the same subnet as the DHCP clients.
5. Static NAT, Dynamic NAT
6. Done in lab.

 Advance question

1. Access-list access-list-number {permit|deny}{host|source source-wildcard|any}
2. TELNET/SSH both are taking remote other device via CLI.
3. Done in lab.
4. Ip nat
5. Done in lab.
6. Done in lab.

**Module 10 CCNA - Security threat landscape**

 Beginner Question

1. Security threats are any type of malicious activity or attack that could potentially cause harm or damage to an orag.
2. Protecting an organization from the impact of risk events by using different techniques is called mitigating risks.

 Intermediate Question

1. DoS attack is a malicious attempt.
2. DDoS attack is designed to force a website, computer.
3. IP spoofing is the creation of IP packets which have a modified source address in order to either hide the identity of the sender

 Advance Question

1. Social engineering attack is a cybersecurity attack.