Q1: Give the sequence of troubleshoots commands you will perform with proper justification if your network is not working.

A1: If a network is not working, the following sequence of troubleshooting commands should be performed: First, use `ping` to check basic connectivity to other devices on the local network and to external addresses. This verifies that the network interface is active and able to send and receive packets. Next, use `ipconfig` (on Windows) or `ifconfig` (on Linux/macOS) to examine the IP address, subnet mask, and default gateway configuration of the host. This ensures that the host is configured correctly for the network. Subsequently, use `traceroute` (or `tracert` on Windows) to identify the path that packets are taking and pinpoint any network hops where connectivity might be failing. Finally, use `nslookup` to verify that the DNS server is resolving domain names to IP addresses correctly, which is essential for accessing resources on the internet.

Q2: Give Advantages, disadvantages of each topology

A2: The document does not contain information regarding the advantages and disadvantages of different network topologies. Therefore, I cannot provide a response to your question.

Q3: Find out application case of each topology

A3: A star topology is commonly used in home and small office networks due to its ease of installation and management, where each device connects directly to a central switch or hub. A bus topology can be found in older networks or in specific applications like sensor networks where simplicity and low cost are important, though it's less common now due to its vulnerability to disruptions. A ring topology sees application in specific scenarios like token ring networks or in some MANs (Metropolitan Area Networks), offering a deterministic access method, but its reliance on each node can be a disadvantage. A mesh topology is employed in critical infrastructure networks or in the internet backbone to provide high redundancy and reliability through multiple paths between nodes.

Q4: Which topology you will implement in your campus and why? 220170107079

A4: I would implement a hybrid star topology in the campus network. A star topology provides centralized management and fault isolation, making it easier to troubleshoot and maintain. Combining this with elements of other topologies, such as a mesh for critical links, ensures redundancy and high availability. This hybrid approach balances cost-effectiveness with the need for a robust and scalable network infrastructure suitable for the diverse needs of a campus environment.

Q5: Give Advantages, disadvantages of VLAN

A5: Advantages of VLANs include enhanced security by isolating traffic, improved network performance through reduced broadcast domains, increased flexibility in network design, and simplified network management. Disadvantages include the need for VLAN-aware network devices, potential complexity in initial configuration, and the possibility of inter-VLAN routing overhead if not properly planned.

Q6: Find out application case of VLAN

A6: A common application case for VLANs is in departmental segmentation within an organization. For example, a company can create separate VLANs for its Sales, Marketing, and Engineering departments. This segmentation improves security by isolating network traffic between departments, controls broadcast traffic within each VLAN, and simplifies network management by grouping users with similar network requirements.

Q7: Give Advantages, disadvantages of Static routing

A7: Advantages of static routing include simplicity in configuration, especially for small networks, and enhanced security due to explicit route control. Disadvantages include the need for manual updates when network topology changes, lack of adaptability to network congestion or failures, and scalability issues in larger networks.

Q8: Find out application case of Static routing

A8: Static routing finds application in small networks with a simple topology where the routes do not change frequently. It is also useful in stub networks, which have only one exit point. Additionally, static routes can be used to create a backup route in case a primary route fails. Static routing offers simplicity and security benefits in these scenarios, as the administrator has direct control over the routing paths.

Q9: What is Ethernet?

A9: Ethernet is a networking technology primarily used for local area networks (LANs). It operates at the physical and data link layers of the OSI model, defining the cabling and signaling standards for transmitting data between devices on a network. Ethernet uses a shared media access method, originally employing Carrier Sense Multiple Access with Collision Detection (CSMA/CD), though modern implementations typically use switches for improved performance and collision avoidance.

Q10: Differentiate static and dynamic algorithm

A10: Static and dynamic routing algorithms differ primarily in how routing tables are created and maintained. Static routing requires manual configuration of routing tables by a network

administrator. These routes remain fixed unless the administrator intervenes to change them. Dynamic routing, on the other hand, automatically updates routing tables based on network conditions using routing protocols. These protocols enable routers to exchange information about network topology and adjust routes in response to changes such as link failures or congestion.

Q11: What is the approximate cost of establishing the network of 10 devices? (Take devices as per your requirements and choice) give details

A11: To approximate the cost of establishing a network of 10 devices, let's consider a basic setup suitable for a small office or home network. This will include the cost of the devices themselves, networking cables, and a central networking device. For the 10 devices, we'll assume desktop computers, each requiring a Network Interface Card (NIC). A basic desktop computer with a built-in NIC might cost around $300 each, totaling $3000. Alternatively, if we consider that users may also connect wirelessly, we'll need a Wireless Router costing about $50-$200, depending on features and range. To connect the wired devices, we need a network switch with at least 10 ports; a basic 16-port switch costs approximately $50-$100. We also need Ethernet cables to connect the devices to the switch; assuming each cable is about 10 feet long and costs $5, the total cost for 10 cables would be $50. Therefore, the approximate cost would be: 10 Desktops: $3000 16-Port Switch: $100 Ethernet Cables: $50 Wireless Router: $100 Total approximate cost: $3250. This is a rough estimate; actual costs may vary based on specific requirements and brand choices. Additional costs may also include software, setup and configuration, and internet service.

Q12: Explain the significance of a web server in the context of internet communication.

A12: In the context of internet communication, a web server is a crucial component responsible for storing, processing, and delivering web content to clients, such as web browsers. When a user requests a web page by entering a URL, the request is sent to the web server associated with that domain. The web server then retrieves the requested resources, which may include HTML files, images, and other media, and sends them back to the client's browser for rendering. Without web servers, the internet as we know it would not exist, as they are fundamental to hosting websites and delivering online content.

Q13: Outline the general steps involved in simulating web server configuration using Cisco Packet Tracer.

A13: To simulate web server configuration using Cisco Packet Tracer, first, place a server device in the workspace and configure its IP address, subnet mask, and default gateway. Next, access the server's configuration tab and navigate to the HTTP service, ensuring it is turned on. Customize the default HTML page if desired using the available text editor. Finally, place client devices, configure their IP settings, and use a web browser application on the

clients to access the server's IP address, verifying the web server setup.

Q14: Explain two benefits of using Cisco Packet Tracer to simulate e-mail server configuration.

A14: Two benefits of using Cisco Packet Tracer to simulate e-mail server configuration are cost savings and risk mitigation. Packet Tracer eliminates the need for physical hardware, reducing expenses associated with purchasing, maintaining, and powering equipment. Additionally, it provides a safe, virtual environment to experiment with configurations, minimizing the risk of disrupting a live network during testing and implementation.

Q15: Briefly describe the purpose of SMTP and IMAP/POP3 in the context of email communication

A15: SMTP (Simple Mail Transfer Protocol) is responsible for sending email messages from a client to a mail server, and between mail servers. IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol version 3) are both used for retrieving email messages from a mail server to a client. IMAP allows users to access and manage their email on the server, while POP3 downloads the email to the client device and typically deletes it from the server.

Q16: Explain various planes or windows shown in user interface of Wireshark tool

A16: Wireshark's user interface is typically divided into three primary panes or windows. The packet list pane displays a summary of each captured packet, including its number, timestamp, source, destination, protocol, and a brief info description. Selecting a packet from the packet list pane populates the packet details pane. The packet details pane shows the selected packet's structure, organized by protocol layers, allowing users to drill down into specific fields and values. Lastly, the packet bytes pane displays the raw data of the selected packet in hexadecimal and ASCII formats, providing a byte-level view of the captured information.

Q17: What is the use of Wireshark tool?

A17: Error generating answer.

Q18: Explore various important options available in Wireshark tool

A18: Wireshark offers several important options for network analysis. Capture filters allow you to specify the types of packets to capture, reducing the size of the capture file and focusing on relevant traffic. Display filters enable you to selectively view packets based on specific criteria, such as protocol, IP address, or port number. Following TCP streams allows

you to reconstruct and analyze the complete communication between two hosts. Wireshark also provides statistical summaries, offering insights into network traffic patterns and protocol usage. Additionally, Wireshark supports exporting captured data in various formats for further analysis or reporting.