CCST Networking – Module 14 Quiz

Questions

1. You're troubleshooting an issue with a remote host. You begin troubleshooting by using the "ping" command to test network connectivity to that remote host. Which of the following troubleshooting approaches are you using?

    a. bottom-up
    b. divide and conquer
    c. inside-out
    d. top-down

2. A help desk technician received a report of a network outage and opened a trouble ticket. Which of the following is least likely to be included in the trouble ticket?

    a. a unique identifier
    b. system logs
    c. category of reported issue
    d. urgency of reported issue

3. You are working on a Microsoft Windows computer, and you want to trace the path a packet takes to a specific destination. What command would be most appropriate?

    a. tracert
    b. nslookup
    c. traceroute
    d. ping

4. You are located at your company's headquarters site, and you want to troubleshoot a Microsoft Windows computer at a branch office site. You need to see the remote computer's screen and interact with it using your keyboard and mouse, much like the way you would if you were physically in front of the computer. Which of the following protocols can best meet your needs?

    a. VPN
    b. NMS
    c. SNMP
    d. RDP

5. You install Wireshark on your laptop and connect into a Cisco Catalyst switch. You want to monitor traveling between a client and a printer, each connected to the switch into which you connected. However, Wireshark is not capturing packets traveling between the client and printer. Which of the following will most likely resolve your issue?

    a. Configure the SNMP feature on the Cisco Catalyst switch.
    b. Configure the STP feature on the Cisco Catalyst switch.
    c. Configure the SPAN feature on the Cisco Catalyst switch.
    d. Configure the SDM feature on the Cisco Catalyst switch.

6. You've opened a large .pcap file in Wireshark, and you wish to only see packets that are using the HTTP protocol and are going to or from an IP address of 172.16.100.110. Which of the following Wireshark filters should you use?

    a. tcp.port=80 and ip.addr=172.16.100.110
    b. tcp.port== 443 & ip.addr==172.16.100.110
    c. tcp.port==443 and ip.addr==172.16.100.110
    d. tcp.port==80 and ip.addr==172.16.100.110

Questions and Answers

1. You're troubleshooting an issue with a remote host. You begin troubleshooting by using the "ping" command to test network connectivity to that remote host. Which of the following troubleshooting approaches are you using?

    a. bottom-up
    b. divide and conquer
    c. inside-out
    d. top-down

    Answer: b

    Explanation: The OSI Model can be leveraged as a troubleshooting tool by giving you a clear starting point and next steps. For example, you could begin at the top of the OSI Model (i.e., the Application Layer) and work your way down. This is called a "top-down" approach.

    Alternately, you could start at the bottom of the OSI Model (i.e., the Physical Layer) and work your way up. This is called a "bottom-up" approach.

    However, it's often most efficient to start somewhat in the middle of the OSI Model. This is called a "divide and conquer" approach. For example, you could issue a "ping" command to check reachability to a remote host. The "ping" command uses a Layer 3 protocol (i.e., ICMP). Therefore, if the ping is successful, you know Layers 1 – 3 are operational, and you can focus your troubleshooting efforts on the upper layers of the IOS Model.

    Conversely, if the ping is not successful, you can focus your troubleshooting efforts on the lower layers of the OSI Model.

    Video Reference: Troubleshooting Methodology

2. A help desk technician received a report of a network outage and opened a trouble ticket. Which of the following is least likely to be included in the trouble ticket?

    a. a unique identifier
    b. system logs
    c. category of reported issue
    d. urgency of reported issue

    Answer: b

Explanation: A trouble ticket might contain tracking information (e.g., a unique identifier, date/time the ticket was issued, contact information, and the status of the ticket). A trouble ticket might also categorize the issue, so that it can better be assigned to an appropriate technician. Additionally, to better prioritize multiple trouble tickets, a trouble ticket might contain information about the urgency of the reported issue.

However, a trouble ticket would not be a place for system logs. Instead, log files are often stored on a server, such as a Syslog server.

Video Reference: Help Desk Best Practices

3. You are working on a Microsoft Windows computer, and you want to trace the path a packet takes to a specific destination. What command would be most appropriate?

    a. tracert {*host* | *ip_address*}
    b. nslookup {*host*}
    c. traceroute {*host* | *ip_address*}
    d. ping {*host* | *ip_address*}

Answer: a

Explanation: The "tracert {*host* | *ip_address*}" command is a Microsoft Windows command used to determine the routers that are transited as a packet travels to its destination, along with the round-trip delay to each of those routers.

The "nslookup {*host*}" command returns DNS records for a specific host on a network.

The "traceroute {*host* | *ip_address*}" command is found on Linux (and other UNIX-like) operating systems and is used to determine the routers that are transited as a packet travels to its destination, along with the round-trip delay to each of those routers.

The "ping {*host* | *ip_address*}" command checks reachability to a device on a network.

Video Reference: Diagnostic Commands

4. You are located at your company's headquarters site, and you want to troubleshoot a Microsoft Windows computer at a branch office site. You need to see the remote computer's screen and interact with it using your keyboard and mouse, much like the way you would if you were physically in front of the computer. Which of the following protocols can best meet your needs?

    a. VPN
    b. NMS
    c. SNMP
    d. RDP

    Answer: d

    Explanation: A VPN (Virtual Private Network) establishes a tunnel between two locations and secures data traveling through the tunnel.

    An NMS (Network Management System), such as SNMP (Simple Network Management Protocol), allows you to monitor and manage multiple network devices from a single location. However, an NMS does not typically allow you to remotely access the desktop graphical interface of a Microsoft Windows computer.

    RDP (Remote Desktop Protocol) allows you to remotely accesses the desktop graphical interface of a remote computer and interact with that computer in much the same way you would if you were physically seated in front of that computer.

    Video Reference: Options for Accessing Network Devices

5. You install Wireshark on your laptop and connect into a Cisco Catalyst switch. You want to monitor traveling between a client and a printer, each connected to the switch into which you connected. However, Wireshark is not capturing packets traveling between the client and printer. Which of the following will most likely resolve your issue?

    a. Configure the SNMP feature on the Cisco Catalyst switch.
    b. Configure the STP feature on the Cisco Catalyst switch.
    c. Configure the SPAN feature on the Cisco Catalyst switch.
    d. Configure the SDM feature on the Cisco Catalyst switch.

    Answer: c

    Explanation: While all the listed features are valid Cisco Catalyst switch features, the SPAN (Switched Port Analyzer) feature will most likely resolve the issue described in this scenario.

Specifically, you can configure the SPAN feature to mirror traffic seen on the client's switch port (and/or on the printer's switch port). You can then configure the SPAN feature to send those mirrored frames out the port to which your laptop is connected.

Video Reference: Packet Analyzers

6. You've opened a large .pcap file in Wireshark, and you wish to only see packets that are using the HTTP protocol and are going to or from an IP address of 172.16.100.110. Which of the following Wireshark filters should you use?

    a. tcp.port=80 and ip.addr=172.16.100.110
    b. tcp.port== 443 & ip.addr==172.16.100.110
    c. tcp.port==443 and ip.addr==172.16.100.110
    d. tcp.port==80 and ip.addr==172.16.100.110

    Answer: d

    Explanation: The "tcp.port=80 and ip.addr=172.16.100.110" filter statement is not valid, because a single equals sign is used rather than a double equals sign, which is a Boolean operator.

    The "tcp.port== 443 & ip.addr==172.16.100.110" filter statement is not valid, because the compound instruction uses the invalid "&" symbol instead of the word "and" to sperate the individual instructions.

    While "tcp.port==443 and ip.addr==172.16.100.110" is a valid filter statement, it doesn't meet the criterial for this scenario. Specifically, the goal is to capture HTTP traffic (i.e., TCP port 80 traffic), not HTTPS traffic (i.e., TCP port 443 traffic).

    The "tcp.port==443 and ip.addr==172.16.100.110" is a valid filter statement, and it does meet this scenario's criterial.

    Video Reference: Working with Wireshark