**DV162\_65\_PAS\_Troubleshooting Networks**

**Possible Answers Sheets**

Q1. What is a challenging troubleshooting task on a network?

Ans: When someone is trying to communicate with a device but getting no response at all, indicating a lack of connectivity to the remote device.

Q2. What should be the first step taken to troubleshoot this network issue?

Ans: The first step should be to check for any network connectivity by observing the link light associated with the ethernet interface to determine if there is a connection to the network.

Q3. What do we do to start testing how far we can communicate through a network?

Ans: To start testing how far we can communicate through a network, we begin by pinging the loopback IP address (127.0.0.1) on our own device to confirm if we can communicate using the built-in network capabilities.

Q4. What is the loopback IP address?

Ans: The loopback IP address is the internal IP address of our own device, typically represented as 127.0.0.1.

Q5. What if our loopback address responds to the ping?

Ans. If our loopback address responds to the ping, it confirms that we are able to communicate using the built-in network capabilities of our own device.

Q6. Our next step would be to ping the IP address that’s been assigned to our \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Ans. Local Network Adapter

Q7. What does pinging the IP address do?

Ans: Pinging the IP address allows us to check the local configuration of our system and the physical network adapter to confirm that we are connected to the network.

Q8. What should we do if the devices on the network respond to our ping?

Ans: If the devices on the network respond to our ping, we should proceed further into the network and try pinging our default gateway.

Q9. Why is it important to check the default gateway?

Ans: It's important to check the default gateway because it serves as the critical link between us and the rest of the world, confirming if our device is able to send packets out to the local network and receive packets back.

Q10. What is a common way to check if a network is connected to the internet?

Ans: A common way to check if a network is connected to the internet is by pinging some device that may be on the internet, such as Google’s DNS server at 8.8.8.8 or the server Quad9 at 9.9.9.9.

Q11. What could be the reason for intermittent connectivity on a wireless network?

Ans: Intermittent connectivity on a wireless network could be caused by interference from other nearby devices using the same frequencies or signal strength issues due to distance from the access point.

Q12. How can we check if the signal strength is strong enough?

Ans: We can check if the signal strength is strong enough by evaluating the signal-to-noise ratio (SNR) of the wireless network and ensuring that there is a wide ratio between the good signal and the noise.

Q13. Can access points be configured to automatically find the best frequency?

Ans: Yes, many access points can be configured to automatically find the best frequency to use for the particular area, optimizing the wireless network performance.

Q14. How can I improve the overall performance of my wireless network?

Ans: We can improve the overall performance of our wireless network by manually configuring different channels, optimizing the location of the access point, and ensuring that there is minimal interference.

Q15. What can be done to optimize wireless signals?

Ans: To optimize wireless signals, we can adjust the location of the access point, configure it to automatically find the best frequency, and minimize interference from other devices.

Q16. What is the goal of resolving intermittent connectivity issues?

Ans: The goal of resolving intermittent connectivity issues is to ensure a stable and reliable connection to the network, minimizing disruptions and improving overall network performance.

Q17. What built-in utilities can give you information about the interference?

Ans: Built-in utilities such as those provided by the operating system or third-party utilities can give our information about the interference on a wireless network.

Q18. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_you can install that can give you more details about the difference between the good signal and the bad signal.

Ans. With third party utility

Q19. What could be causing interference on a wireless network?

Ans: Interference on a wireless network could be caused by other devices nearby using the same frequencies, such as fluorescent lights, microwave ovens, or neighboring wireless networks.

Q20. How can you evaluate wireless network interference?

Ans: Wireless network interference can be evaluated by examining the signal-to-noise ratio (SNR) and using utilities that can calculate SNR to visually identify interference.

Q21. What if this ratio was 1:1, where there was just as much noise as there was signal?

Ans. If the ratio was 1:1, where there was just as much noise as there was signal, it would indicate poor wireless network performance and likely result in connectivity issues.

Q22. \_\_\_\_\_\_\_\_\_\_\_\_\_\_is very good about giving you information in the system tray that can help you with troubleshooting.

Ans. Windows.

Q23. What if you’re looking at the system tray and Windows says there is limited or no connectivity, or in some cases, no internet access then what's th issue?

Ans. If Windows says there is limited or no connectivity, or no internet access, it indicates an issue with communicating out to the internet, possibly due to IP address configuration or network connectivity problems.

Q24. What should be checked first when troubleshooting IP address issues?

Ans: When troubleshooting IP address issues, the first thing to check is whether the IP address has been assigned by a DHCP server or manually configured on the device.

Q25. What if we see an automatic private IP address in this configuration?

Ans. If we see an automatic private IP address (APIPA) in this configuration, it indicates that the device has not received an IP address from a DHCP server and has created its own private IP address, limiting communication to the local network.

Q26. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_addresses are link local addresses and can only communicate to other devices on our local network.

Ans: Automatic private IP (APIPA).

.

Q27. What type of error message would a Windows device display when attempting to access the internet with an APIPA address?

Ans: A Windows device would display an error message such as "Limited or no connectivity" and "No internet access" when attempting to access the internet with an APIPA address.

Q28. How can we check whether or not a device has a valid IP address?

Ans: We can check whether or not a device has a valid IP address by verifying if it has been assigned by a DHCP server or manually configured on the device.

Q29. What happens when a network experiences problems during a voice call?

Ans: When a network experiences problems during a voice call, it can result in choppy or difficult-to-understand audio, impacting the quality of the call.

Q30. If data doesn’t get through the network, there’s no way to rewind the conversation and rescind all of that data. (True/False)

Ans. True.

Q31. What is Jitter?

Ans: Jitter refers to the variation in the delay of packet arrival in a network, particularly in real-time communication applications such as voice over IP (VoIP) or video conferencing.

Q32. What is the purpose of evaluating jitter?

Ans: The purpose of evaluating jitter is to assess the consistency of packet delivery timing in a network. Consistent jitter levels are crucial for maintaining the quality of real-time communication services.

Q33. What happens when jitter is not consistent?

Ans: When jitter is not consistent, it can lead to irregularities in the timing of packet delivery, resulting in audio or video distortion, dropped frames, and overall degradation in the quality of communication services.

Q34. What could cause problems with the quality of our phone calls?

Ans: Problems with the quality of phone calls can be caused by various factors, including high jitter, packet loss, network congestion, insufficient bandwidth, and latency issues.

Q35. How to solve the issue of delay or latency on our network?

ANs. To solve the issue of delay or latency on a network, we can optimize network configurations, upgrade network hardware, prioritize traffic using quality of service (QoS) mechanisms, and minimize interference or congestion on the network.

Q36. What are some potential causes of network slowdowns?

Ans: Some potential causes of network slowdowns include bandwidth limitations, network congestion, hardware issues, software conflicts, security threats such as malware or denial-of-service (DoS) attacks, and improper network configurations.

Q37. What is the best way to diagnose a network issue?

Ans: The best way to diagnose a network issue is through systematic troubleshooting, which involves identifying symptoms, testing connectivity, analyzing network traffic, checking hardware configurations, and utilizing diagnostic tools to pinpoint the root cause of the problem.

Q38. What is latency?

Ans: Latency, also known as delay, is the amount of time it takes for data to travel from the source to the destination in a network. It is measured in milliseconds (ms) and can impact the responsiveness and performance of network applications.

Q37. What determines how much information can be transferred?

Ans: The available bandwidth and the speed of the network connection determine how much information can be transferred within a given timeframe. Higher bandwidth and faster network speeds allow for greater data transfer rates.

Q38. What can cause latency problems?

Ans: Latency problems can be caused by various factors, including network congestion, packet loss, routing inefficiencies, hardware limitations, long physical distances between devices, and inefficient network protocols.

Q39. What is one of the best ways to measure latency?

Ans: One of the best ways to measure latency is by conducting ping tests or traceroute tests to determine the round-trip time (RTT) between the source and destination devices. Additionally, network monitoring tools can provide real-time latency metrics and historical data for analysis.

Q40. What is port flapping?

Ans: Port flapping refers to the phenomenon where a network port on a device rapidly alternates between the up (active) and down (inactive) states. It typically indicates a physical or configuration issue with the network interface or connected cables.

Q41. What should you do when you encounter a port flapping problem?

Ans: When we encounter a port flapping problem, we should first inspect the physical connections, cables, and network interface for any signs of damage or misconfiguration. Additionally, updating firmware/drivers, replacing faulty hardware, or adjusting network settings may help resolve the issue.