7.3.7 Lesson Review

Date: 11/30/2025, 4:41:14 PM

Time Spent: 11:25

Score: 90%

Passing Score: 80%

Question 1 ✓ Correct

After several new computers are connected to a network device, every computer connected to the device begins to experience slow transfer speeds.

Which of the following is the FIRST step to troubleshoot this problem?

- (●) Determine whether the network device is a hub or a switch. ✓ Correct
- ( ) Use a cable tester to determine whether all cables between each computer and the device are good.
- ( ) Use a loopback plug to determine whether the NIC in each computer is good.
- ( ) Use a loopback plug to determine whether each port on the network device is good.

Explanation

When troubleshooting slow speeds, you need first to determine which device is running slowly (such as a hub or switch). If a specific resource is experiencing slow speeds, you need to focus your efforts on that resource.

The problem is unlikely to be a bad port on the network device, which would only affect one computer.

If the problem is a bad NIC, already knowing whether the network device is a hub or switch would help isolate the problem.

A bad cable would only affect the computer it was connected to, but all computers are experiencing slow transfer speeds in this scenario.

Related Content

7.3.2 Troubleshoot Network Speed Issues
resources\questions\q_troubleshoot_network_speed_issues_01.question.xml

Question 2 ✓ Correct

A user reports intermittent connectivity and slow transfer speeds on the office Wi-Fi network. Upon investigation, you find that the user's device is connected to the 2.4 GHz band, while other devices connected to the 5 GHz band are not experiencing any issues.

Additionally, the Wi-Fi analyzer shows that the 2.4 GHz band is heavily congested with multiple overlapping networks.

What is the BEST course of action to resolve the issue?

- Replace the wireless access point with a newer model that supports higher speeds.
- Configure the user's device to connect to the 5 GHz band instead of the 2.4 GHz band. ✓ Correct
- Adjust the channel settings on the wireless access point to a less congested channel in the 2.4 GHz band.
- Move the user's device closer to the wireless access point to improve the signal strength.

Explanation

The 5 GHz band is less congested and offers better performance in terms of speed and reliability compared to the 2.4 GHz band, especially in environments with many overlapping networks. Configuring the user's device to connect to the 5 GHz band will resolve the issue of congestion and improve connectivity. This is the most effective solution based on the analysis of the problem.

While adjusting the channel settings can reduce interference in the 2.4 GHz band, it does not address the fundamental issue of congestion caused by multiple overlapping networks. Switching to the 5 GHz band is a more effective solution in this scenario.

Moving closer to the access point might improve signal strength, but it does not resolve the issue of congestion in the 2.4 GHz band. The problem is not related to signal strength but to interference and congestion.

Replacing the access point is unnecessary in this scenario because the issue is related to the user's device being connected to the congested 2.4 GHz band. The existing access point already supports the 5 GHz band, which is a viable solution. Replacing the hardware would be an excessive and costly approach.

Related Content

5.4.11 Long-Range Fixed Wireless

7.3.4 Troubleshoot Wireless Issues

7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wireless_issues_04.question.xml

Question 3 ✓ Correct

A user reports limited connectivity on their workstation. Upon investigation, you find that the workstation is connected to the network but cannot access certain external websites. Other users on the same network do not have this issue.

You run the **ipconfig** command and notice that the workstation has a valid IP address, subnet mask, and default gateway.

What is the MOST likely cause of the issue, and what should you do next?

- ○ The network cable is faulty. Replace the cable with a known good one.
- ○ The switch port is experiencing port flapping. Check the switch logs for port status changes.
- ◉ The DNS server settings are incorrect. Reconfigure the workstation to use the correct DNS server. ✓ Correct
- ○ The user's computer has a malware infection. Disconnect the workstation and run a malware scan.

Explanation

If the workstation has a valid IP address, subnet mask, and default gateway but cannot access certain external websites, the issue is likely related to DNS resolution. Incorrect DNS server settings can prevent the workstation from resolving domain names to IP addresses, leading to limited connectivity for external websites. Reconfiguring the DNS server settings to point to a valid DNS server will resolve the issue.

A faulty network cable would likely result in no connectivity or intermittent connectivity, not an issue limited to accessing certain external websites. Since the workstation has a valid IP configuration, the cable is functioning properly.

Port flapping causes intermittent connectivity as the port repeatedly transitions between up and down states. This would affect all network activity, not just access to certain external websites. The issue described is more specific to DNS resolution.

While malware can cause network issues, the symptoms described (valid IP configuration but limited access to external websites) are more indicative of a DNS configuration problem. Malware is not the most likely cause in this scenario.

Related Content

7.3.1 Troubleshoot Wired Connectivity

7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_limited_connectivity_03.question.xml

Question 4 Correct

What is the first step in troubleshooting a limited connectivity issue for a single host in a wired network?

- Use a cable tester to verify the structured cabling.
- Verify that the patch cords are properly terminated and connected to the network ports. ✓ Correct
- Update the NIC's device driver software.
- Check the switch configuration for port security settings.

Explanation

The first step in troubleshooting limited connectivity for a single host is to check the physical connections, such as ensuring that the patch cords are properly terminated and securely connected to the network ports. This is a basic but essential step to rule out simple physical issues before moving on to more complex troubleshooting.

While port security settings on the switch can cause connectivity issues, this is not the first step in troubleshooting. Physical connections should be checked before investigating switch configurations.

Using a cable tester to verify structured cabling is a more advanced step in troubleshooting. It is performed after confirming that the patch cords and physical connections are not the source of the problem.

Updating the NIC's device driver software is a potential solution for connectivity issues caused by driver problems. However, this is not the first step in troubleshooting. Physical connections should be checked before addressing software-related issues.

Related Content

7.3.1 Troubleshoot Wired Connectivity

7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_limited_connectivity_01.question.xml

Question 5 ✓ Correct

A user reports that their file transfers over the network are significantly slower than usual. Upon investigation, you find that the issue is isolated to this user's workstation.

You check the cabling and find no visible damage or interference.

What should you do next to troubleshoot the issue?

- ○ Reposition the user's workstation closer to the router.
- ◉ Check the duplex settings on the user's network adapter and the switch port. ✓ Correct
- ○ Replace the user's Ethernet cable with a shielded cable.
- ○ Update the firmware on the router.

Explanation

Mismatched duplex settings on the network adapter and switch port can reduce network speed. Ensuring that both are set to auto-negotiate is a critical step in troubleshooting slow speeds. Since the issue is isolated to one workstation, this is the most logical next step.

You should use shielded cables only when interference is suspected. Since no interference or damage was found during the cabling check, replacing the cable is unnecessary at this stage.

Repositioning is a troubleshooting step for wireless networks, not for cabled connections. The user's workstation is connected via Ethernet, so physical proximity to the router is irrelevant.

The issue is isolated to a single workstation. Updating the router firmware would be a step to address network-wide issues, not a problem specific to one user.

Related Content

7.3.2 Troubleshoot Network Speed Issues

resources\questions\q_troubleshoot_network_speed_issues_03.question.xml

Question 6 ✕ Incorrect

You have just installed a wireless network, but the network is experiencing slow speeds, especially when accessing the internet from your workstation.

Which action should you try FIRST to resolve the issue?

- ◯ Move the wireless access point. ✓ Correct
- ◯ Reset your wireless router to the factory defaults.
- ◯ Add a network extender.
- ◉ Move your workstation closer to the wireless access point. ✕ Incorrect

Explanation

Slow wireless speeds can be caused by weak signal strength. If weak spots are found, the easiest and least expensive first step would be to move the wireless access point.

You could also try adding a network extender, but this solution would mean an additional cost.

Moving your workstation closer to the wireless access point could involve a lot of work (if it is even an option).

Resetting your wireless router to the factory defaults could cause other issues and probably won't resolve the issue with slow speeds.

Related Content

5.4.11 Long-Range Fixed Wireless

7.3.4 Troubleshoot Wireless Issues

7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wireless_issues_02.question.xml

Question 7 Correct

A company is experiencing poor VoIP call quality, including jitter and delays. You analyze the network and find that the issue occurs during peak usage times when multiple devices are streaming videos and downloading large files.

The company uses a SOHO router without advanced traffic management features.

What is the MOST likely cause of the VoIP issues?

- The Internet Service Provider (ISP) is throttling VoIP traffic during peak hours.
- The VoIP phones are outdated and cannot handle modern network traffic.
- The SOHO router lacks Quality of Service (QoS) configuration to prioritize VoIP traffic. ✓ Correct
- The VoIP application is not compatible with the SOHO router.

Explanation

The lack of QoS on the SOHO router is the most likely cause of the VoIP issues. Without QoS, the router cannot prioritize VoIP traffic over other types of data, such as video streaming or file downloads. This results in jitter and delays during peak usage times, as VoIP packets are delayed or dropped due to network congestion.

VoIP applications are generally compatible with most routers, including SOHO models. The issue here is not compatibility but the router's inability to prioritize VoIP traffic during periods of high network usage.

The age of the VoIP phones is not the issue in this scenario. The problem lies in the network's inability to prioritize VoIP traffic, which is unrelated to the phones themselves.

While ISP throttling could theoretically cause issues, there is no evidence in this scenario to suggest that the ISP is specifically targeting VoIP traffic. The described problem is more likely due to the lack of QoS on the SOHO router.

Related Content

7.3.5 Troubleshoot VoIP Issues
resources\questions\q_troubleshoot_voip_issues_05.question.xml

Question 8 Correct

What is the maximum one-way latency that VoIP can support without significantly impacting call quality?

- 500 milliseconds (ms)
- 150 milliseconds (ms) ✓ Correct
- 50 milliseconds (ms)
- 300 milliseconds (ms)

Explanation

VoIP can support a maximum one-way latency of about 150 milliseconds. Latency beyond this threshold can lead to noticeable delays in voice communication, which can significantly degrade call quality.

While lower latency is always better for VoIP, 50 milliseconds is not the maximum one-way latency VoIP can support. VoIP systems are designed to tolerate latency of up to 150 milliseconds without significant impact on call quality.

A one-way latency of 300 milliseconds is too high for VoIP and would result in noticeable delays and poor call quality. This exceeds the acceptable threshold for effective real-time communication.

A one-way latency of 500 milliseconds is far beyond the acceptable limit for VoIP. Such high latency would make real-time communication nearly impossible, leading to severe disruptions in call quality.

Related Content

7.3.5 Troubleshoot VoIP Issues
resources\questions\q_troubleshoot_voip_issues_03.question.xml

Question 9 Correct

A network technician troubleshoots an issue where the video conferencing system keeps freezing up and dropping out. The technician determines that the network is not congested and the signal is not being processed fast enough to meet the streaming requirement.

What is this type of issue known as?

- Jitter
- QoS
- Latency ✓ Correct
- VoIP

Explanation

This issue is known as latency, which is the time it takes for a signal to reach the recipient. Processing delays at intermediate systems, such as routers, can cause latency to be worse.

Voice over Internet Protocol (VoIP) is a generic name for protocols that carry voice traffic over data networks.

Quality of service (QoS) means that switches, access points, and routers are all configured to identify VoIP data and prioritize it over bursty data.

Jitter is the amount of variation in delay over time, and network technicians can measure it by sampling the elapsed time between packets arriving. Jitter is typically caused by network congestion.

Related Content

7.3.5 Troubleshoot VoIP Issues
resources\questions\q_troubleshoot_voip_issues_01.question.xml

Question 10 ✓ Correct

You are an IT technician tasked with resolving a wired connectivity issue for a workstation in an office. The user reports intermittent connectivity problems.

Upon inspection, you notice that the link LEDs on the network adapter and switch port are flickering inconsistently.

What is the BEST next step to troubleshoot and resolve the issue?

- ○ Update the NIC's device driver software.
- ○ Use a loopback tool to test the switch port.
- ○ Replace the network adapter (NIC) on the workstation.
- ◉ Substitute the current patch cord with a known good cable. ✓ Correct

Explanation

The first step in troubleshooting intermittent connectivity issues is to check the physical connections, starting with the patch cord. A faulty or improperly terminated patch cord is a common cause of intermittent connectivity. Substituting it with a known good cable is a quick and effective way to rule out this potential issue.

Replacing the NIC is a more invasive and time-consuming step that should only be considered after ruling out simpler issues, such as faulty patch cords or bad switch ports. The problem may not be with the NIC at all.

Updating the NIC's driver is typically a solution for software-related issues, such as speed mismatches or configuration problems. In this scenario, the flickering LEDs suggest a physical connectivity issue, which should be addressed first.

Using a loopback tool is a more advanced diagnostic step that is typically performed after simpler troubleshooting steps, such as checking cables and connections, have been completed. It is not the best next step in this scenario.

Related Content

- 7.3.1 Troubleshoot Wired Connectivity
- 7.3.6 Troubleshoot Limited Connectivity

resources\questions\q_troubleshoot_wired_connectivity_03.question.xml