Exam Report: 7.3.8 Practice Questions

Date: 4/2/25 6:47:32 pm
Time Spent: 14:56

Candidate: Garsteck, Matthew
Login: mGarsteck

Overall Performance

Your Score: 77%

Passing Score: 80%

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Correct

You have been asked to help a small office with a limited budget set up and configure a Windows network. There are only five computers in this office. In addition to the ability to share network resources, security is a top priority.

Which of the following is the BEST course of action in this situation?

- Install a WorkGroup to allow each device to control what is shared and with whom.
- Install a HomeGroup to provide a single login and simplify security and sharing.
- Install a HomeGroup to allow each computer to control which items are shared and who can access them.
- Install a WorkGroup to provide a single login and simplify security and sharing.

Explanation

With only five PCs in this company, a Windows WorkGroup will let you organize your computers in a peer-to-peer network. This WorkGroup network lets you share files, internet access, and printers between the five employees. Unlike Windows HomeGroup, a WorkGroup has no centralized authority. Therefore, each workstation controls the database of users and privileges. Each device that is part of the WorkGroup can allow access on a user-by-user or group-by-group basis.

The HomeGroup is the least secure approach to networking and sharing. A HomeGroup allows anyone with access to the Homegroup access to everything shared on any computer in the group. A single password is used for access to the group, providing equal access to all joined devices.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_HOMEGROUP_VS]

Question 2: Correct

A technician is installing a new SOHO wireless router.
Which of the following is the FIRST thing the technician should do to secure the router?

- Adjust the radio power levels
- Press the WPS button
- Change the router's default password
- Disable SSID broadcast

Explanation

The first security configuration on the router should be to change the router's default password.

Disabling the SSID broadcast may be desirable for added security, but it is not the first action you should take.

Adjusting the radio power levels will limit the broadcast area and may be desirable for added security, but it is not the first action you should take.

Pressing the WPS button temporarily broadcasts the SSID and passphrase, which would degrade security.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_NETWORKS_02]

Question 3: Correct

A technician is installing a SOHO router at an after-school community center. The customer would like to keep children from accessing inappropriate while browsing the web.

Which of the following actions would help accomplish this goal?

- Disable SSID broadcast
- Disable DHCP
- Update firmware
- Enable content filtering

Explanation

Parental controls or content filters restrict or block specific web traffic based on keywords, URLs, or the time of day.

Disabling the SSID broadcast would increase security, but does nothing to restrict web browsing results.

Disabling DHCP would require static IP addresses, but does nothing to restrict web browsing results.

Updating firmware may improve security by fixing vulnerabilities, but does nothing to restrict web browsing results.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_NETWORKS_04]

Question 4: Correct

A technician receives notification from a SOHO router manufacturer of a specific vulnerability that allows attackers to exploit SNMP traps to take over the router. The technician verifies the settings outlined in the notification.

Which of the following actions should the technician take NEXT?

- Disable DHCP.
- Check for and apply firmware updates.
- Enable MAC filtering.
- Enable content filtering.

Explanation

Manufactures often accompany a vulnerability notification with firmware updates to address the vulnerability. These updates should be applied immediately.

Parental controls or content filters restrict or block specific web traffic based on keywords, URLs, or the time of day, but do not address network hacker vulnerabilities.

Disabling DHCP will require static IP addresses, but does nothing to address network hacker

vulnerabilities.
MAC filtering can be used to limit connectivity to a list of MAC addresses, but does nothing to address network hacker vulnerabilities.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_NETWORKS_05]

Question 5: Incorrect

A technician is installing a network-enabled smart home control system in a SOHO.
To access the system from the internet, which of the following configurations is MOST likely required on the SOHO router?

- QoS
- NAT
- Port forwarding
- ~~DHCP~~

Explanation

Access to the smart home control system from the internet through the SOHO router is most likely gained using port forwarding.

QoS gives priority to certain types of network traffic, such as VoIP phone traffic.
DHCP dynamically assigns IP addresses to clients in the local network.
NAT translates private IP addresses on the local network to public IP addresses on the internet.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_ROUTER_01]

Question 6: Correct

A SOHO customer finds that their VoIP conversations frequently break up and become unintelligible. This happens most often when one person in the office streams video from the internet.

Which of the following configuration changes on the SOHO router is MOST likely to improve VoIP performance?

- Forward UDP ports 5060 to 5065 to the VoIP phone.
- Create a DMZ and add the VoIP phone to it.
- Change QoS settings to give VoIP traffic more priority.
- Change DHCP to give the VoIP phone a static IP address.

Explanation

Poor VoIP performance is likely due to insufficient bandwidth to support both video streaming and VoIP calls. Changing the router's QoS settings to give a higher priority to VoIP traffic will most likely improve VoIP performance.

Since VoIP functions correctly but gives poor performance, any port forwarding needed for VoIP must already be in place.

Configuring the VoIP phone with a static IP address will not improve performance.
Creating a DMZ and adding the VoIP phone to it will not resolve any traffic contention between video and VoIP traffic.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_ROUTER_02]

Question 7: Correct

A technician is replacing a SOHO router and has configured DHCP to assign private IP addresses to hosts on the local network. These hosts can communicate with each other, but users can't browse the internet.

Which of the following changes to the SOHO router is MOST likely to restore internet connectivity?

- Remove any QoS settings that give low priority to HTTP traffic.
- Configure the SOHO router for NAT.
- Update the firmware on the SOHO router.
- Disable DHCP and configure the hosts with static IP addresses.

Explanation

Configuring NAT to translate the private IP addresses on the local network to public IP addresses on the internet will most likely restore internet connectivity.

QoS settings may cause HTTP traffic to be slower, but would not completely interrupt it.

Static IP addresses will not restore internet connectivity.

Updating the firmware is not likely to restore internet connectivity.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_SOHO_CFG_ROUTER_03]

Question 8: Correct

You are an IT technician for your company. Your boss has asked you to set up and configure a wireless network to service all of the conference rooms.

Which of the following features lets you allow or reject client connections by hardware address?

- MAC address filtering
- SSID
- WEP
- DHCP

Explanation

MAC address filtering allows or rejects client connections by hardware address. Wi-Fi Protected Access II (WPA2) provides encryption and user authentication for wireless networks. Wired Equivalent Privacy (WEP) also provides security, but WPA2 is considered more secure than WEP. The SSID is the network name or identifier.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_MAC_ADDRESS_FILTER]

Question 9: Correct

A technician is tasked with preparing a conference room so that at least 20 guests will be able to wirelessly connect laptop computers to the company network.

Which of the following network devices would be the BEST choice for this connectivity?

- Switch
- Firewall

- Router
- Access point

Explanation

An access point gives Wi-Fi access to a network.

A firewall filters network traffic based on a set of rules.

A switch maintains a table of MAC addresses by port and forwards network frames only to the port that matches the MAC address.

A router manages IP traffic between networks.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_NETWORK_DEVICES_02]

Question 10: Incorrect

A technician is installing a new SOHO wireless router in a home office. The customer wants to secure the wireless network so only a smartphone, tablet, and laptop can connect.

Which of the following router settings should the technician change?

- Disable SSID broadcast
- ~~Enable port forwarding~~
- Disable DHCP
- Enable MAC filtering

Explanation

MAC filtering can be used to limit connectivity to a list of MAC addresses.

Disabling the SSID broadcast will increase security, but SSID can be easily captured using wireless analyzers and then used to connect to the wireless network.

Disabling DHCP will require static IP addresses, but will not limit network connectivity.
Enabling port forwarding allows the router to redirected on the internal network. It will not limit network connectivity.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_SOHO_NETWORKS_03]

Question 11: Correct

Which of the following is used on a wireless network to identify the network name?

- WEP key
- WPA2 passphrase
- SSID
- MAC address

Explanation

Wireless devices use the SSID (Service Set Identification) to identify the network name. All devices on a wireless network use the same SSID. The MAC address is a unique physical device address. The WPA2 Personal passphrase and the WEP key are both mechanisms used to secure wireless communications.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_SSID]

Question 12: Incorrect

Which of the following locations will contribute the greatest amount of interference for a wireless access point? (Select TWO.)

- [x] Near backup generators
- [x] ~~In the top floor of a two-story building~~
- [ ] Near exterior walls
- [ ] Near cordless phones
- [ ] Near DCHP servers

Explanation

Other wireless transmitting devices (such as cordless phones or microwaves) and generators cause interference for wireless access points. In general, place access points high up to avoid the interference problems caused by going through building foundations. DHCP servers provide IP information for clients and do not cause interference.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_WIRELESS_07]

Question 13: Correct

Which of the following is true when the DHCP setting is disabled in a wireless network?

- (•) Wireless clients must use a static IP address within the correct IP address range to connect to the network.
- ( ) Wireless clients with specific MAC addresses are denied access to the network.
- ( ) Wireless clients must use the correct wireless access point identifier (SSID) to connect to the network.
- ( ) Wireless clients must use the correct encryption key with its packets.

Explanation

Disabling DHCP prevents addresses from being automatically assigned to wireless systems. If DHCP is disabled, clients must use a static IP address and only those who know the IP address range and other parameters will be able to connect. Enabling MAC address filtering denies access to clients with unauthorized MAC addresses. Encryption keys are only needed when wireless networks implement some type of encryption (WEP, WPA, or WPA2). The SSID is the identifier for the wireless access point and is used to associate wireless clients with the access point.

References

TestOut PC Pro - 7.3 SOHO Configuration
[e_soho_pp6.exam.xml Q_AP_CFG_WIRELESS_STATIC_ADDRESS]