CCNA Security Pretest Exam Answers – Implementing Network Security (Version 2.0)

itexamanswers.net/ccna-security-pretest-exam-answers-implementing-network-security-version-2-0.html

May 29, 2021

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

Implementing Network Security (Version 2.0) – CCNA Security 2.0 Pretest Exam Answers

1. Which statement describes the Cisco ASAv product?

- It is a Cisco ASA feature added on a Cisco router.
- It is a cloud-based Cisco ASA firewall product.
- It is a Cisco FirePOWER service that can be added on a Cisco router.
- **It is a virtual machine version of Cisco ASA product.**

Explanation: The Cisco Adaptive Security Virtual Appliance (ASAv) brings the power of ASA appliances to the virtual domain. The Cisco ASAv operates as a virtual machine (VM) using the interfaces on a host server to process traffic.

2. What two features must match between ASA devices to implement a failover configuration? (Choose two.)

- **device model**
- software configuration
- source IP address
- **amount of RAM**
- next-hop destination

Explanation: In order for two Cisco ASA 5505 devices to work in a failover configuration, both devices must be identical models with the same hardware configuration, number and types of interfaces, and the same amount of RAM.

3. What protocol is used to query the revocation status of an X.509 certificate?

- SSL
- EAP
- **OCSP**
- LDAP

Explanation: Online Certificate Status Protocol (OCSP) is an internet protocol used to query an OCSP server for the revocation status of an X.509 digital certificate.

4. Which Cisco platform supports Cisco Snort IPS?

- 800 series ISR
- 3900 series ISR
- **4000 series ISR**
- 2900 series ISR

Explanation: The newer ISR routers, Cisco 4000 series, no longer support IOS IPS. The 4000 series routers provide IPS services using Snort.

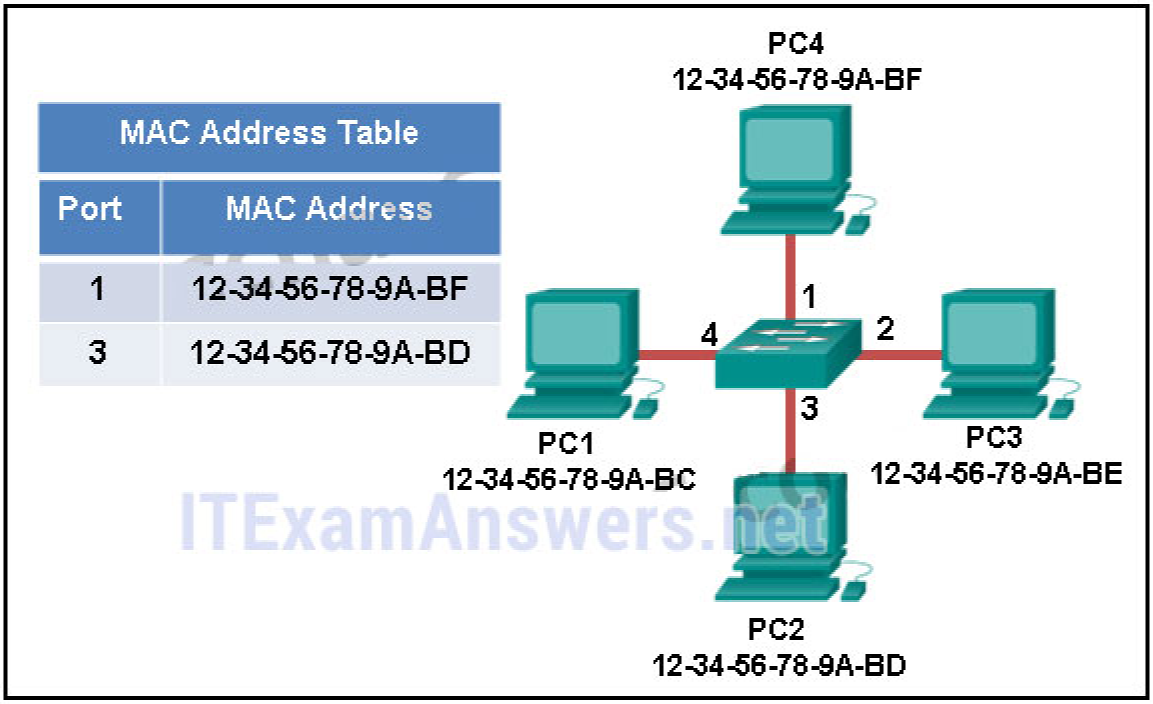
5. Which IDS/IPS signature alarm will look for packets that are destined to or from a particular port?

- signature-based
- policy-based
- anomaly-based
- honey pot-based

Explanation: Cisco IDS and IPS sensors can use four types of signature alarms or triggers:

- **Pattern-based detection** – also known as signature-based detection, searches for a specific and pre-defined pattern. In most cases, the pattern is matched to the signature only if the suspect packet is associated with a particular service or destined to or from particular ports.
- **Anomaly-based detection** – also known as profile-based detection, involves first defining a profile of what is considered normal for the network or host. After defining normal activity, the signature triggers an action if excessive activity occurs beyond a specified threshold that is not included in the normal profile.
- **Policy-based detection** – also known as behavior-based detection, is similar to pattern-based detection, but instead of trying to define specific patterns, the administrator defines behaviors that are suspicious based on historical analysis.
- **Honey pot-based detection** – uses a dummy server to attract attacks.

6. Refer to the exhibit. The exhibit shows a small switched network and the contents of the MAC address table of the switch. PC1 has sent a frame addressed to PC3. What will the switch do with the frame?



MAC Address Table	
Port	MAC Address
1	12-34-56-78-9A-BF
3	12-34-56-78-9A-BD

- The switch will discard the frame.
- The switch will forward the frame only to port 2.
- The switch will forward the frame to all ports except port 4.
- The switch will forward the frame to all ports.
- The switch will forward the frame only to ports 1 and 3.

Explanation: The MAC address of PC3 is not present in the MAC table of the switch. Because the switch does not know where to send the frame that is addressed to PC3, it will forward the frame to all the switch ports, except for port 4, which is the incoming port.

7. What is a difference between ASA IPv4 ACLs and IOS IPv4 ACLs?

- ASA ACLs do not have an implicit deny any at the end, whereas IOS ACLs do.
- ASA ACLs are always named, whereas IOS ACLs are always numbered.
- ASA ACLs use forward and drop ACEs, whereas IOS ACLs use permit and deny ACEs.
- ASA ACLs use the subnet mask in defining a network, whereas IOS ACLs use the wildcard mask.
- Multiple ASA ACLs can be applied on an interface in the ingress direction, whereas only one IOS ACL can be applied.

Explanation: There are many similarities between ASA ACLs and IOS ACLs, including:

- In both, there is an implicit **deny any**
- Only one ACL per interface, per protocol, per direction still applies.
- Both use **deny** and **permit** ACEs.
- ACLs can be either named or numbered.

ASA ACLs differ from IOS ACLs in that they use a network mask (e.g., 255.255.255.0) instead of a wildcard mask (e.g. 0.0.0.255). Although most ASA ACLs are named, they can also be numbered.

8. What type of algorithms require sender and receiver to exchange a secret key that is used to ensure the confidentiality of messages?

- hashing algorithms
- public key algorithms
- symmetric algorithms
- asymmetric algorithms

Explanation: Symmetric algorithms use the same key, a secret key, to encrypt and decrypt data. This key must be pre-shared before communication can occur. Asymmetric algorithms require more processing power and overhead on the communicating devices because these keys can be long in order to avoid being hacked.

9. What is the one major difference between local AAA authentication and using the login local command when configuring device access authentication?

- Local AAA authentication allows more than one user account to be configured, but login local does not.
- The login local command uses local usernames and passwords stored on the router, but local AAA authentication does not.
- Local AAA authentication provides a way to configure backup methods of authentication, but login local does not.
- The login local command requires the administrator to manually configure the usernames and passwords, but local AAA authentication does not.

Explanation: Local AAA authentication works very similar to the **login local** command, except that it allows you to specify backup authentication methods as well. Both methods require that local usernames and passwords be manually configured on the router.

10. What is a result of securing the Cisco IOS image using the Cisco IOS Resilient Configuration feature?

- The Cisco IOS image file is not visible in the output of the show flash command.
- The Cisco IOS image is encrypted and then automatically backed up to a TFTP server.
- The Cisco IOS image is encrypted and then automatically backed up to the NVRAM.
- When the router boots up, the Cisco IOS image is loaded from a secured FTP location.

Explanation: When using the Cisco IOS Resilient Configuration feature, a secure copy of the IOS image is stored in flash and is hidden from view and and not included in any directory listings.

11. Which two wildcard masks are required in an extended access list entry that blocks the traffic from network 192.168.20.0/26 to network 172.16.32.0/28? (Choose two.)

- 0.0.63.255
- 0.0.0.63
- 0.0.0.31
- 0.0.0.15
- 0.0.0.0

12. Which two statements describe static routes? (Choose two.)

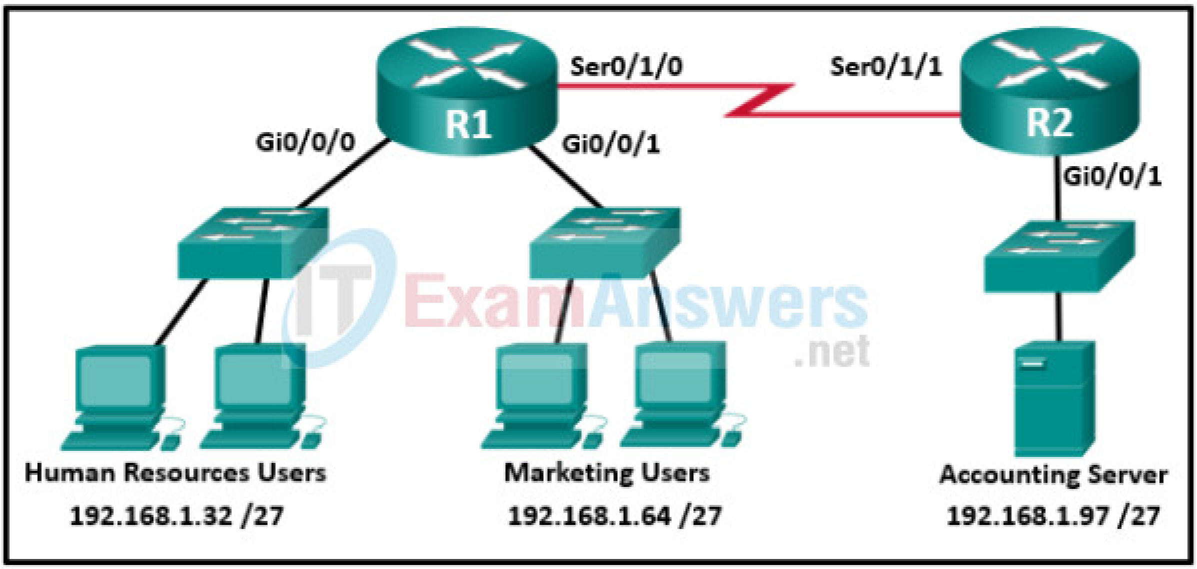
- They are created in interface configuration mode.
- They require manual reconfiguration to accommodate network changes.
- They automatically become the default gateway of the router.
- They are identified in the routing table with the prefix S.
- They are automatically updated whenever an interface is reconfigured or shutdown.

13. When is UDP preferred to TCP?

- when a client sends a segment to a server
- when all the data must be fully received before any part of it is considered useful
- when an application can tolerate some loss of data during transmission
- when segments must arrive in a very specific sequence to be processed successfully

Explanation: UDP can be used when an application can tolerate some data loss. UDP is the preferred protocol for applications that provide voice or video that cannot tolerate delay.

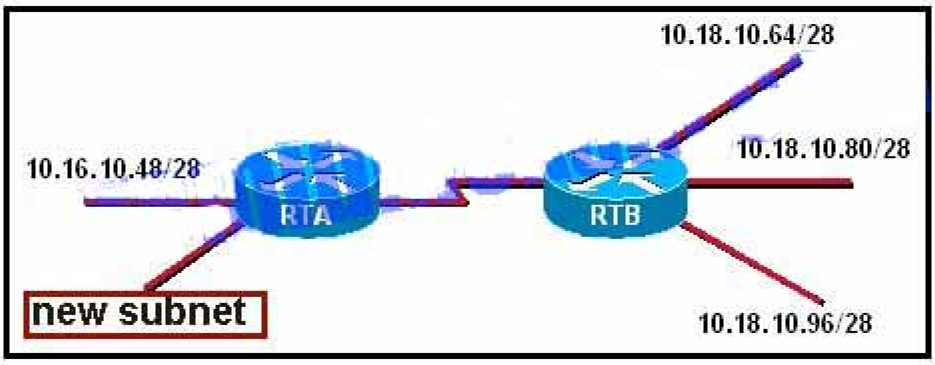
14. Refer to the exhibit. An extended access list has been created to prevent human resource users from gaining access to the accounting server. All other network traffic is to be permitted. When following the ACL configuration guidelines, on which router, interface, and direction should the access list be applied?



- router R1, interface S0/1/0, outbound
- router R1, interface Gi0/0/0, inbound
- router R1, interface Gi0/0/0, outbound
- router R2, interface S0/1/1, inbound
- router R2, interface Gi0/0/1, inbound
- router R2, interface Gi0/0/1, outbound

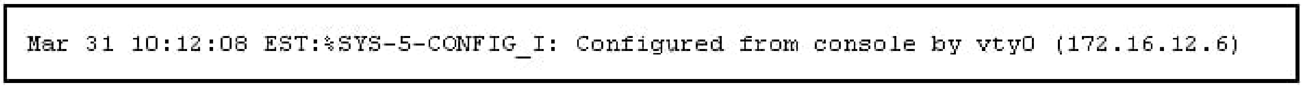
Explanation: The ACL configuration guidelines recommend placing extended access control lists as close to the source of network traffic as possible and placing standard access control lists as close to the destination of network traffic as possible.

15. Refer to the exhibit. What would be a valid network address for the new subnet on RTA?



- 10.16.10.16/28
- 10.16.10.24/28
- 10.16.10.30/28
- 10.16.10.56/28
- 10.16.10.72/28

16. Refer to the exhibit. What two pieces of information can be gathered from the generated message? (Choose two.) This message is a level five notification message.

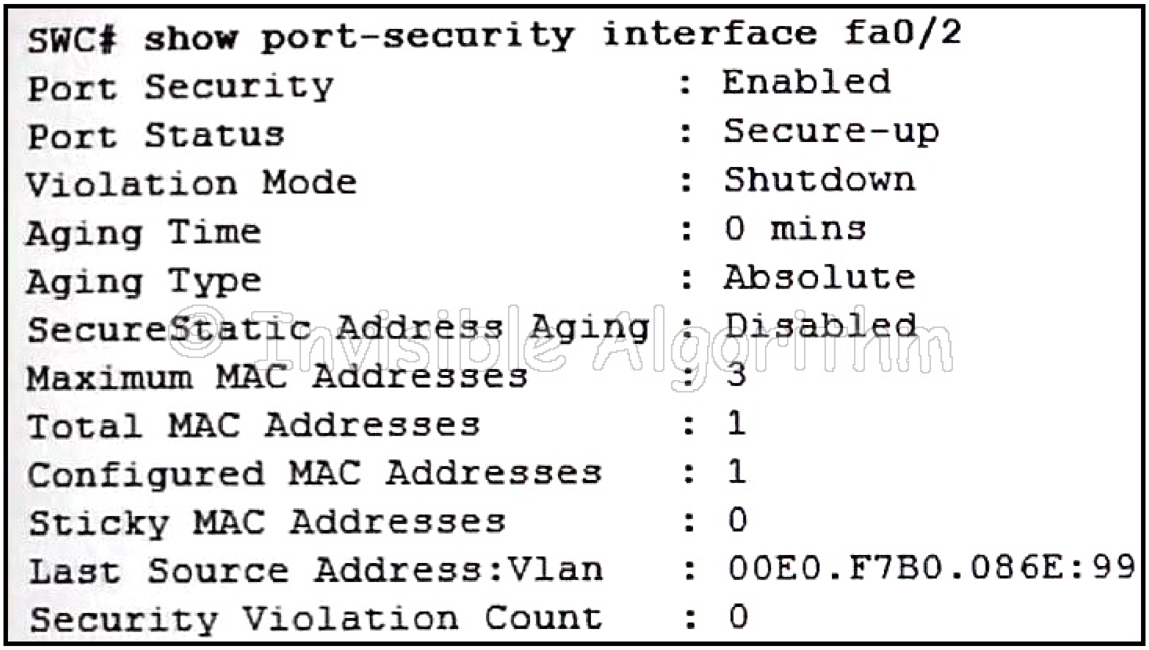


```
Mar 31 10:12:08 EST:%SYS-5-CONFIG_I: Configured from console by vty0 (172.16.12.6)
```

- **This message is a level five notification message.**
- **This message indicates that service timestamps have been globally enabled.**
- This message indicates that enhanced security was configured on the vty ports.
- This message appeared because a major error occurred that requires immediate action.
- This message appeared because a minor error occurred that requires further investigation.

Explanation: A Cisco router log message consists for three parts:
1) the timestamp
2) the log message and severity level
3) the message text

17. Refer to the exhibit. The network administrator is configuring the port security feature on switch SWC. The administrator issued the command show port-security interface fa 0/2 to verify the configuration. What can be concluded from the output that is shown? (Choose three.)



```
SWC# show port-security interface fa0/2
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode               : Shutdown
Aging Time                   : 0 mins
Aging Type                   : Absolute
SecureStatic Address Aging   : Disabled
Maximum MAC Addresses        : 3
Total MAC Addresses          : 1
Configured MAC Addresses     : 1
Sticky MAC Addresses         : 0
Last Source Address:Vlan     : 00E0.F7B0.086E:99
Security Violation Count     : 0
```

- This port is currently up.
- The port is configured as a trunk link.
- There is no device currently connected to this port.
- Three security violations have been detected on this interface.

- The switch port mode for this interface is access mode.
- Security violations will cause this port to shut down immediately.

Explanation: Because the security violation count is at 0, no violation has occurred. The system shows that 3 MAC addresses are allowed on port fa0/2, but only one has been configured and no sticky MAC addresses have been learned. The port is up because of the port status of secure-up. The violation mode is what happens when an unauthorized device is attached to the port. A port must be in access mode in order to activate and use port security.

18. Which three statements describe limitations in using privilege levels for assigning command authorization? (Choose three.)

- There is no access control to specific interfaces on a router.
- The root user must be assigned to each privilege level that is defined.
- Commands set on a higher privilege level are not available for lower privilege users.
- Views are required to define the CLI commands that each user can access.
- Creating a user account that needs access to most but not all commands can be a tedious process.
- It is required that all 16 privilege levels be defined, whether they are used or not.

Explanation: An administrator can create customized privilege levels and assign different commands to each level. However, this method of controlling he level of access to the router has limitations. Using privilege levels access to specific interfaces or ports cannot be controlled and availability of commands cannot be customized across levels.

19. What are two protocols that are used by AAA to authenticate users against a central database of usernames and password? (Choose two.)

- NTP
- TACACS+
- SSH
- HTTPS
- RADIUS
- CHAP

Explanation: By using TACACS+ or RADIUS, AAA can authenticate users from a database of usernames and passwords stored centrally on a server such as a Cisco ACS server.

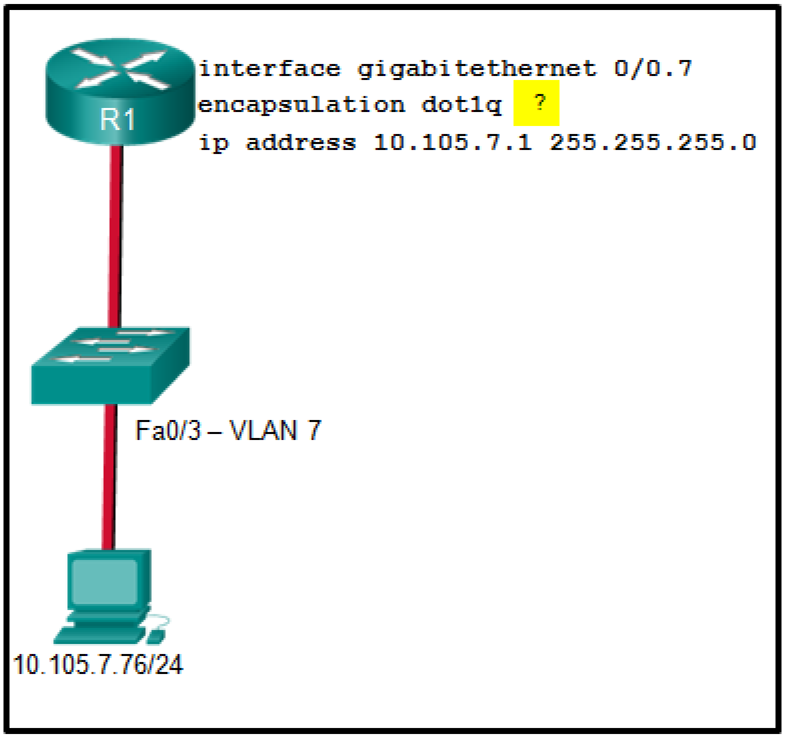
20. What is the main difference between the implementation of IDS and IPS devices?

- An IDS can negatively impact the packet flow, whereas an IPS can not.
- An IDS needs to be deployed together with a firewall device, whereas an IPS can replace a firewall.

- An IDS would allow malicious traffic to pass before it is addressed, whereas an IPS stops it immediately.
- An IDS uses signature-based technology to detect malicious packets, whereas an IPS uses profile-based technology.

Explanation: An IPS is deployed in inline mode and will not allow malicious traffic to enter the internal network without first analyzing it. An advantage of this is that it can stop an attack immediately. An IDS is deployed in promiscuous mode. It copies the traffic patterns and analyzes them offline, thus it cannot stop the attack immediately and it relies on another device to take further actions once it detects an attack. Being deployed in inline mode, an IPS can negatively impact the traffic flow. Both IDS and IPS can use signature-based technology to detect malicious packets. An IPS cannot replace other security devices, such as firewalls, because they perform different tasks.

21. Refer to the exhibit. A network administrator is configuring inter-VLAN routing on a network. For now, only one VLAN is being used, but more will be added soon. What is the missing parameter that is shown as the highlighted question mark in the graphic?



```
interface gigabitethernet 0/0.7
encapsulation dot1q  ?
ip address 10.105.7.1 255.255.255.0
```

- It identifies the subinterface.
- It identifies the VLAN number.
- It identifies the native VLAN number.
- It identifies the type of encapsulation that is used.
- It identifies the number of hosts that are allowed on the interface.

Explanation: The completed command would be **encapsulation dot1q** 7. The **encapsulation dot1q** part of the command enables trunking and identifies the type of trunking to use. The 7 identifies the VLAN number.

22. A network technician has been asked to design a virtual private network between two branch routers. Which type of cryptographic key should be used in this scenario?

- asymmetric key
- digital signature
- hash key
- symmetric key

Explanation: A symmetric key requires that both routers have access to the secret key that is used to encrypt and decrypt exchanged data.

23. Which three actions can the Cisco IOS Firewall IPS feature be configured to take when an intrusion activity is detected? (Choose three.)

- alert
- drop
- inoculate
- isolate
- reset TCP connection
- reset UDP connection

Explanation: In IPS implementation, when a signature detects a matching activity, the signature triggers one or more of these actions:

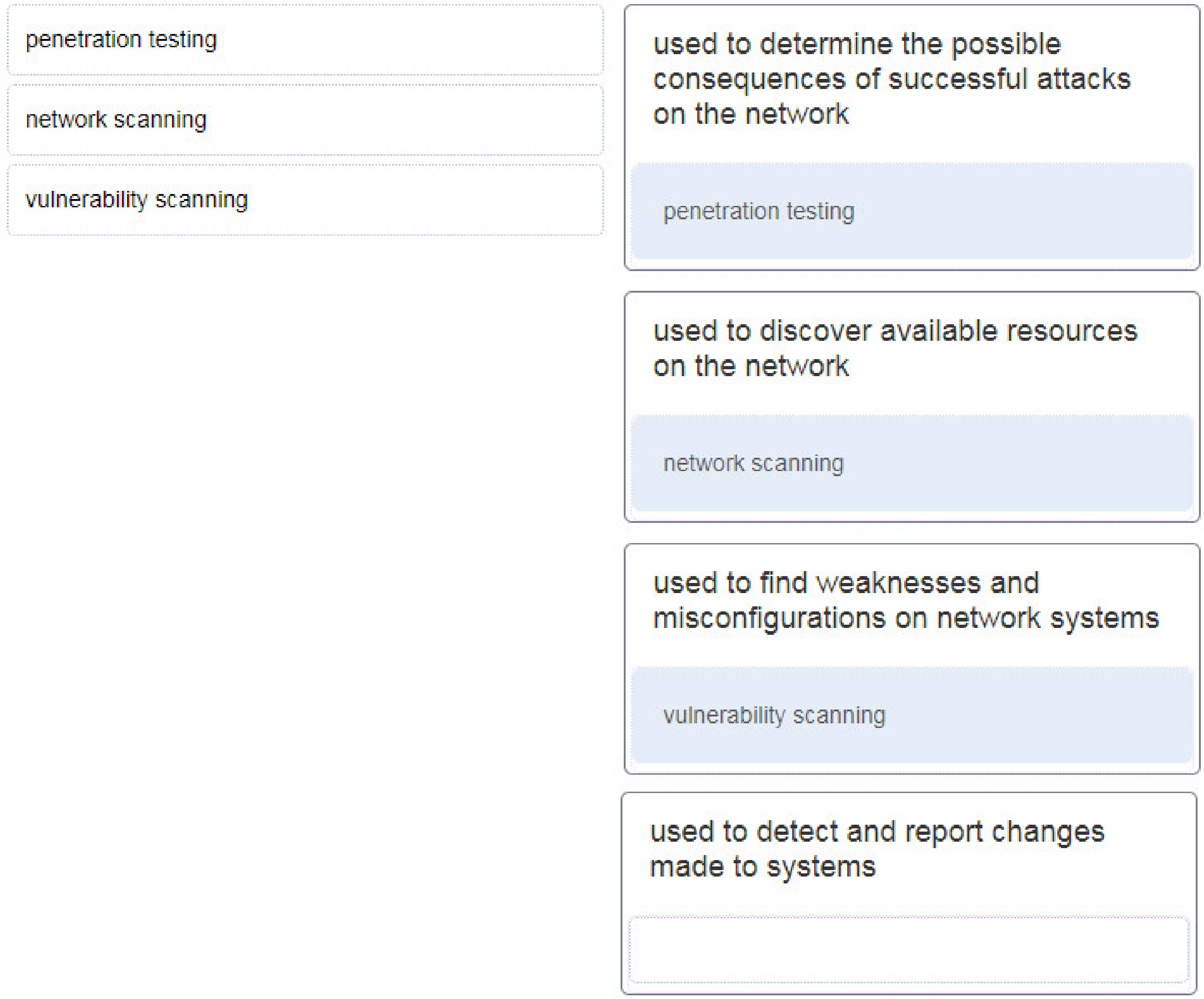
- Generates an alert
- Logs the activity
- Drops or prevent the activity
- Resets a TCP connection
- Blocks future activity
- Allows the activity

24. What Layer 2 attack is mitigated by disabling Dynamic Trunking Protocol?

- VLAN hopping
- DHCP spoofing
- ARP poisoning
- ARP spoofing

Explanation: Mitigating a VLAN hopping attack can be done by disabling Dynamic Trunking Protocol (DTP) and by setting the native VLAN of trunk links to VLANs not in use.

25. Match the network security testing technique with how it is used to test network security. (Not all options are used.)



penetration testing

network scanning

vulnerability scanning

used to determine the possible consequences of successful attacks on the network

penetration testing

used to discover available resources on the network

network scanning

used to find weaknesses and misconfigurations on network systems

vulnerability scanning

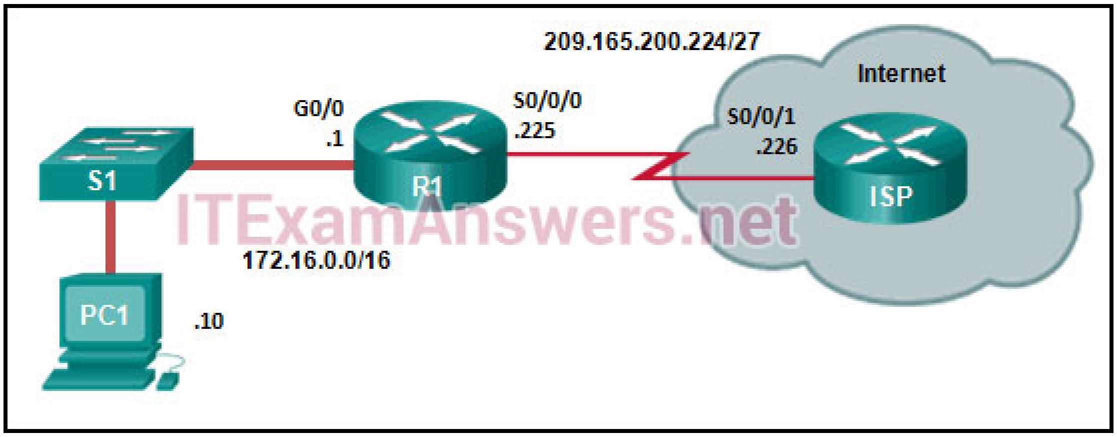
used to detect and report changes made to systems

- Penetration testing = **used to determine the possible consequences of successful attacks on the network**.
- Vulnerability scanning = **used to find weaknesses and misconfigurations on network systems**.
- Network scanning = **used to discover available resources on the network**.

Explanation: Network scanning tools are used to probe network devices, servers and hosts for open TCP or UDP ports. Vulnerability scanning tools are used to discover security weaknesses in a network or computer system. Penetration testing tools are used to determine the possible outcome of a successful attack on a network or computer system.

26. Refer to the exhibit. R1 was configured with the static route command ip route 209.165.200.224 255.255.255.224 S0/0/0 and consequently users on network 172.16.0.0/16 are unable to reach resources on the Internet. How

should this static route be changed to allow user traffic from the LAN to reach the Internet?



- Add the next-hop neighbor address of 209.165.200.226.
- Change the exit interface to S0/0/1.
- Change the destination network and mask to 0.0.0.0 0.0.0.0.
- Add an administrative distance of 254.

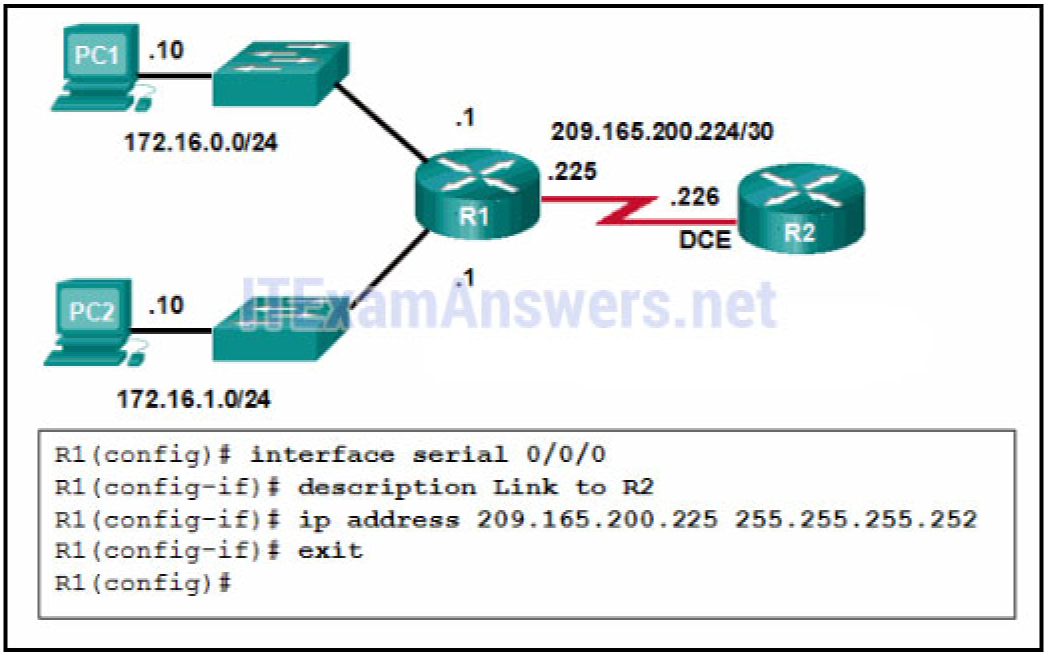
Explanation: The static route on R1 has been incorrectly configured with the wrong destination network and mask. The correct destination network and mask is 0.0.0.0 0.0.0.0.

27. A small company has a web server in the office that is accessible from the Internet. The IP address 192.168.10.15 is assigned to the web server. The network administrator is configuring the router so that external clients can access the web server over the Internet. Which item is required in the NAT configuration?

- an IPv4 address pool
- an ACL to identify the local IPv4 address of the web server
- the keyword overload for the ip nat inside source command
- the ip nat inside source command to link the inside local and inside global addresses

Explanation: A static NAT configuration is necessary for a web server that is accessible from the Internet. The configuration is achieved via an **ip nat inside source static** *<inside local> <inside global>* command under the global configuration mode. An IP address pool and an ACL are necessary when configuring dynamic NAT and PAT. The keyword **overload** is used to configure PAT.

28. Refer to the exhibit. A network administrator has configured R1 as shown. When the administrator checks the status of the serial interface, the interface is shown as being administratively down. What additional command must be entered on the serial interface of R1 to bring the interface up?

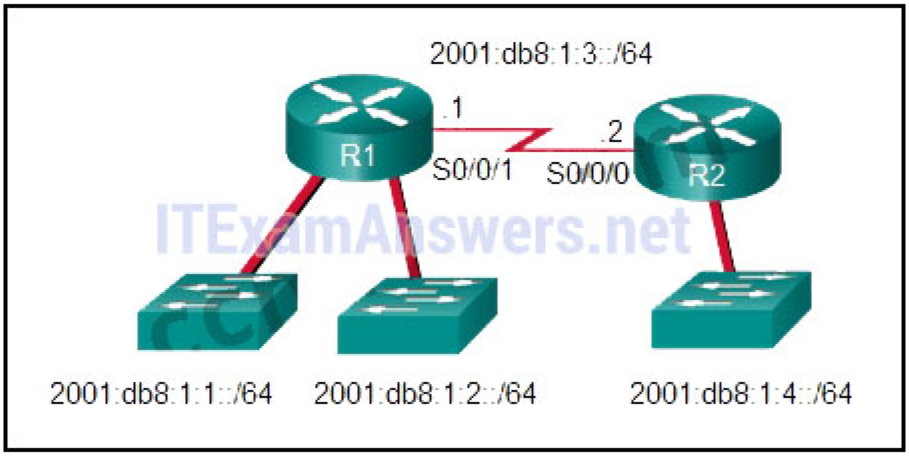


```
R1(config)# interface serial 0/0/0
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# exit
R1(config)#
```

- IPv6 enable
- clockrate 128000
- end
- no shutdown

Explanation: By default all router interfaces are shut down. To bring the interfaces up, an administrator must issue the **no shutdown** command in interface mode.

29. Refer to the exhibit. What command would be used to configure a static route on R1 so that traffic from both LANs can reach the 2001:db8:1:4::/64 remote network?



- ipv6 route ::/0 serial0/0/0
- ipv6 route 2001:db8:1:4::/64 2001:db8:1:3::1
- ipv6 route 2001:db8:1:4::/64 2001:db8:1:3::2
- ipv6 route 2001:db8:1::/65 2001:db8:1:3::1

Explanation: To configure an IPv6 static route, use the **ipv6 route** command followed by the destination network. Then add either the IP address of the adjacent router or the interface R1 will use to transmit a packet to the 2001:db8:1:4::/64 network.

30. A network administrator needs to configure a standard ACL so that only the workstation of the administrator with the IP address 192.168.15.23 can access the virtual terminal of the main router. Which two configuration commands can achieve the task? (Choose two.)

- Router1(config)# access-list 10 permit host 192.168.15.23
- Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.0
- Router1(config)# access-list 10 permit 192.168.15.23 0.0.0.255
- Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.0
- Router1(config)# access-list 10 permit 192.168.15.23 255.255.255.255

Explanation: To permit or deny one specific IP address, either the wildcard mask 0.0.0.0 (used after the IP address) or the wildcard mask keyword host (used before the IP address) can be used.

31. How many classful networks are summarized by the static summary route ip route 192.168.32.0 255.255.248.0 S0/0/0?

- 2
- 4
- 8
- 16

Explanation: A summary route of 192.168.32.0 with a network prefix of /21 will summarize 8 routes. The network prefix has moved from the classful boundary of 24 to the left by 3 bits. These 3 bits identify that 8 networks are summarized. The networks that are summarized would be 192.168.32.0/24 through 192.168.39.0/24.

32. Which two Layer 2 security best practices would help prevent VLAN hopping attacks? (Choose two.)

- Change the native VLAN number to one that is distinct from all user VLANs and is not VLAN 1.
- Change the management VLAN to a distinct VLAN that is not accessible by regular users.
- Statically configure all ports that connect to end-user host devices to be in trunk mode.
- Disable DTP autonegotiation on end-user ports.
- Use SSH for all remote management access.

Explanation: Allowing end-user devices to negotiate trunk settings via DTP can lead to a VLAN hopping attack, so DTP autonegotiation should be disabled on access ports. Configuring a trunk link with a native VLAN that is also used for end-users can lead to VLAN hopping attacks as well. The native VLAN should be set to a VLAN that is not used anywhere else.

33. A destination route in the routing table is indicated with a code D. Which kind of route entry is this?

- a static route
- a route used as the default gateway
- a network directly connected to a router interface
- a route dynamically learned through the EIGRP routing protocol

Explanation: Routes in a routing table are manually created or dynamically learned. Letter D indicates that the route was learned dynamically through the EIGRP routing protocol.

34. Refer to the exhibit. The administrator can ping the S0/0/1 interface of RouterB but is unable to gain Telnet access to the router by using the password cisco123. What is a possible cause of the problem?
More Questions: CCNA Security Pretest Exam Answers

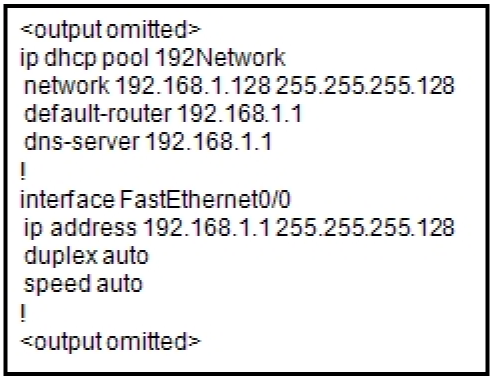
- The wrong vty lines are configured.
- The administrator has used the wrong password.
- AAA authorization is not configured.
- The administrator does not have enough rights on the PC that is being used.

Explanation: To authenticate and log in using a Telnet vty line, the network administrator is required to use the local username and password that has been configured on the local router. This is evidenced by the application of the **aaa authentication login telnet local-case** command. The administrator must use a capital C in Cisco123 to match the applied configuration.

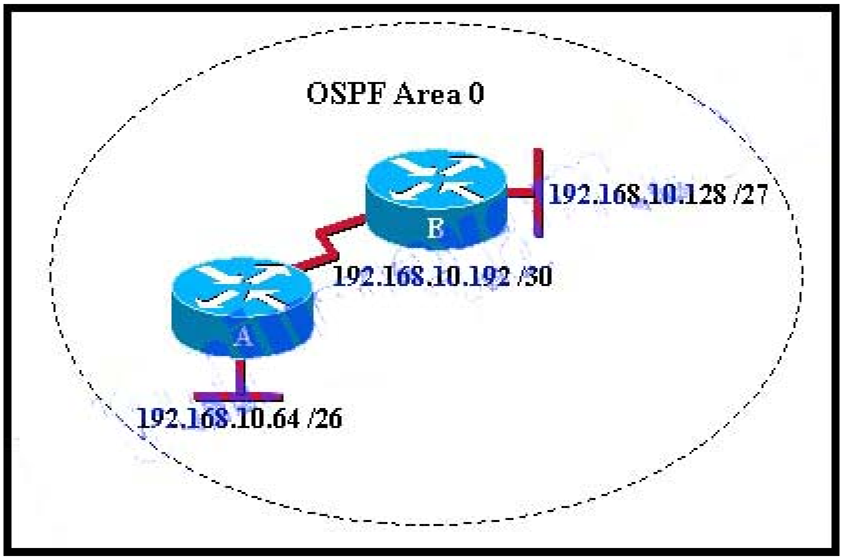
35. Refer to the exhibit. A host connected to Fa0/0 is unable to acquire an IP address from this DHCP server. The output of the debug ip dhcp server command shows “DHCPD: there is no address pool for 192.168.1.1”. What is the problem?

- The 192.168.1.1 address has not been excluded from the DHCP pool.
- The pool of addresses for the 192Network pool is incorrect.
- The default router for the 192Network pool is incorrect.
- The 192.168.1.1 address is already configured on Fa0/0.

36. Refer to the exhibit. Which sequence of commands will configure router A for OSPF?



```
<output omitted>
ip dhcp pool 192Network
 network 192.168.1.128 255.255.255.128
 default-router 192.168.1.1
 dns-server 192.168.1.1
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.128
 duplex auto
 speed auto
!
<output omitted>
```



- router ospf 0
  network 192.168.10.0
  network 192.168.10.192
- router ospf 0
  network 192.168.10.0
- router ospf 1
  network 192.168.10.64 0.0.0.63 area 0
  network 192.168.10.192 0.0.0.3 area 0
- router ospf 1
  network 192.168.10.64 255.255.255.192
  network 192.168.10.192 255.255.255.252
- router ospf 1
  network 192.168.10.0 area 0

37. Switch port Fa0/24 was previously configured as a trunk, but now it is to be used to connect a host to the network. How should the network administrator reconfigure switch port Fa0/24?

- Use the switchport mode access command from interface configuration mode.

- Enter the switchport nonegotiate command from interface configuration mode.
- Administratively shut down and re-enable the interface to return it to the default.
- Use the switchport access vlan vlan number command from interface configuration mode to remove the port from the trunk and add it to a specific VLAN.

38. Which device performs the function of determining the path that messages should take through internetworks?

- a router
- a firewall
- a web server
- a DSL modem

Explanation: A router is used to determine the path that the messages should take through the network. A firewall is used to filter incoming and outgoing traffic. A DSL modem is used to provide Internet connection for a home or an organization.

39. The ARP table in a switch maps which two types of address together?

- Layer 3 address to a Layer 2 address
- Layer 3 address to a Layer 4 address
- Layer 4 address to a Layer 2 address
- Layer 2 address to a Layer 4 address

Explanation: The switch ARP table keeps a mapping of Layer 2 MAC addresses to Layer 3 IP addresses. These mappings can be learned by the switch dynamically through ARP or statically through manual configuration.

40. When applied to a router, which command would help mitigate brute-force password attacks against the router?

- exec-timeout 30
- service password-encryption
- banner motd $Max failed logins = 5$
- login block-for 60 attempts 5 within 60

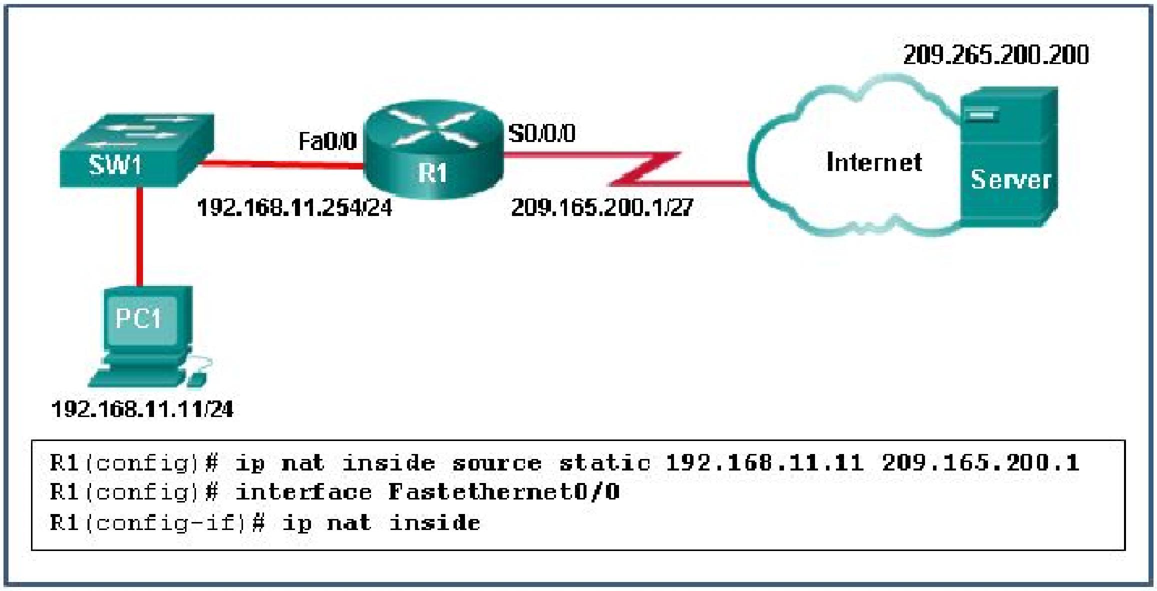
Explanation: The **login block-for** command sets a limit on the maximum number of failed login attempts allowed within a defined period of time. If this limit is exceeded, no further logins are allowed for the specified period of time. This helps to mitigate brute-force password cracking since it will significantly increase the amount of time required to crack a password. The **exec-timeout** command specifies how long the session can be idle before the user is disconnected. The **service password-encryption** command encrypts the passwords in the running configuration. The **banner motd** command displays a message to users who are logging in to the device.

41. Which statement describes a characteristic of the traceroute utility?

- It sends four Echo Request messages.
- It utilizes the ICMP Source Quench messages.
- It is primarily used to test connectivity between two hosts.
- It identifies the routers in the path from a source host to a destination host.

Explanation: Traceroute is a utility that generates a list of hops (or routers) along the path from a source host to the destination host.

42. Refer to the exhibit. What has to be done in order to complete the static NAT configuration on R1?



```
R1(config)# ip nat inside source static 192.168.11.11 209.165.200.1
R1(config)# interface Fastethernet0/0
R1(config-if)# ip nat inside
```

- R1 should be configured with the command ip nat inside source static 209.165.200.1 192.168.11.11.
- R1 should be configured with the command ip nat inside source static 209.165.200.200 192.168.11.11.
- Interface S0/0/0 should be configured with the command ip nat outside.
- Interface Fa0/0 should be configured with the command no ip nat inside.

Explanation: In order for NAT translations to work properly, both an inside and outside interface must be configured for NAT translation on the router.

43. Which statement accurately describes dynamic NAT?

- It always maps a private IP address to a public IP address.
- It provides an automated mapping of inside local to inside global IP addresses.
- It provides a mapping of internal host names to IP addresses.
- It dynamically provides IP addressing to internal hosts.

Explanation: Dynamic NAT provides a dynamic mapping of inside local to inside global IP addresses. NAT is merely the one-to-one mapping of one address to another address without taking into account whether the address is public or private. DHCP is automatic assignment of IP addresses to hosts. DNS is mapping host names to IP addresses.

44. Which command would be best to use on an unused switch port if a company adheres to the best practices as recommended by Cisco?

- shutdown
- ip dhcp snooping
- switchport port-security mac-address sticky
- switchport port-security violation shutdown
- switchport port-security mac-address sticky mac-address

Explanation: Unlike router Ethernet ports, switch ports are enabled by default. Cisco recommends disabling any port that is not used. The **ip dhcp snooping** command globally enables DHCP snooping on a switch. Further configuration allows defining ports that can respond to DHCP requests. The **switchport port-security** command is used to protect the network from unidentified or unauthorized attachment of network devices.