Chapters 21 – 23: Infrastructure Security and Management Exam Answers (CCNPv8 ENARSI)

itexamanswers.net/chapters-21-23-infrastructure-security-and-management-exam-answers-ccnpv8-enarsi.html

April 8, 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.

CCNP Enterprise: Advanced Routing (Version 8.0) – Infrastructure Security and Management Exam

1. Which two characteristics are shared by both standard and extended ACLs? (Choose two.)

- Both kinds of ACLs can filter based on protocol type.
- **Both can be created by using either a descriptive name or number.**
- Both filter packets for a specific destination host IP address.
- **Both include an implicit deny as a final statement.**
- Both can permit or deny specific services by port number.

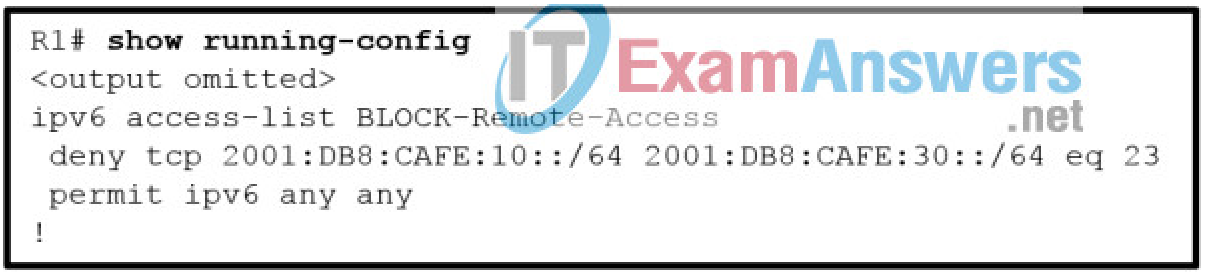
Explanation: Standard ACLs filter traffic based solely on a specified source IP address. Extended ACLs can filter by source or destination, protocol, or port. Both standard and extended ACLs contain an implicit deny as a final statement. Standard and extended ACLs can be identified by either names or numbers.

2. What method is used to apply an IPv6 ACL to a router interface?

- **the use of the ipv6 traffic-filter command**
- the use of the ipv6 access-list command
- the use of the access-class command
- the use of the ip access-group command

Explanation: A network administrator will use the ipv6 traffic-filter command within interface configuration mode to apply an IPv6 ACL.

3. Refer to the exhibit. A network administrator created an IPv6 ACL to block the Telnet traffic from the 2001:DB8:CAFE:10::/64 network to the 2001:DB8:CAFE:30::/64 network. What is a command the administrator could use to allow only a single host 2001:DB8:CAFE:10::A/64 to telnet to the 2001:DB8:CAFE:30::/64 network?



```
R1# show running-config
<output omitted>
ipv6 access-list BLOCK-Remote-Access
 deny tcp 2001:DB8:CAFE:10::/64 2001:DB8:CAFE:30::/64 eq 23
 permit ipv6 any any
!
```

- permit tcp 2001:DB8:CAFE:10::A/64 2001:DB8:CAFE:30::/64 eq 23
- **permit tcp host 2001:DB8:CAFE:10::A 2001:DB8:CAFE:30::/64 eq 23 sequence 5**
- permit tcp 2001:DB8:CAFE:10::A/64 eq 23 2001:DB8:CAFE:30::/64
- permit tcp host 2001:DB8:CAFE:10::A eq 23 2001:DB8:CAFE:30::/64

Explanation: When an IPv6 ACE is created and is to be processed before an existing ACE is processed, the next command entered must use the sequence argument with a number lower than the existing ACE. This allows an entry to be placed before an existing entry, as the default sequence numbers are commonly numbered by increments of 10. Thus, using a sequence number of 5 on an ACE will place it in front of a prior existing entry with a sequence number of 10.

4. Which two statements describe the effect of the access control list wildcard mask 0.0.0.15? (Choose two.)

- The last five bits of a supplied IP address will be ignored.
- The first 32 bits of a supplied IP address will be matched.
- **The last four bits of a supplied IP address will be ignored.**
- The first 28 bits of a supplied IP address will be ignored.
- The last four bits of a supplied IP address will be matched.
- **The first 28 bits of a supplied IP address will be matched.**

Explanation: A wildcard mask uses 0s to indicate that bits must match. 0s in the first three octets represent 24 bits and four more zeros in the last octet, represent a total of 28 bits that must match. The four 1s represented by the decimal value of 15 represents the four bits to ignore.

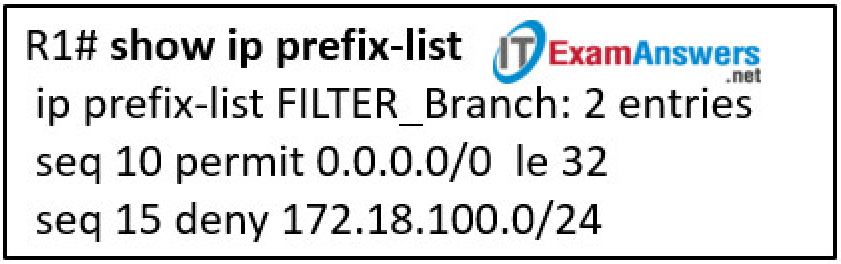
5. A network administrator is configuring an IPv6 ACL to deny Telnet access from all staff in the branch office to a file server in home office. All branch office staff use addressing from the IPv6 subnet 2001:DB8:100:20::/64. The file server

in home office uses the address 2001:DB8:100:50::15/64. Implementing the No-Telnet ACL on the LAN interface of the branch office router requires which three commands? (Choose three.)

- permit tcp any host 2001:DB8:100:20::15 eq 23
- deny tcp host 2001:DB8:100:50::15 any eq 23
- **deny tcp any host 2001:DB8:100:50::15 eq 23**
- **permit ipv6 any any**
- deny ipv6 any any
- ip access-group No-Telnet in
- **ipv6 traffic-filter No-Telnet in**

Explanation: The ACL requires an ACE denying Telnet access from all users in the LAN to the file server at 2001:DB8:100:50::15/64. The IPv6 ACL also has an implicit deny, so a permit statement is required to allow all other traffic. With IPv6, the ipv6 traffic filter command is used to bind the ACL to the interface.

6. Refer to the exhibit. An administrator is configuring a prefix list to stop advertising 172.18.100.0/24, a secure Branch network, to the internet. After adding the prefix list, the administrator notices that the branch network is still being advertised. How can the administrator fix the error?

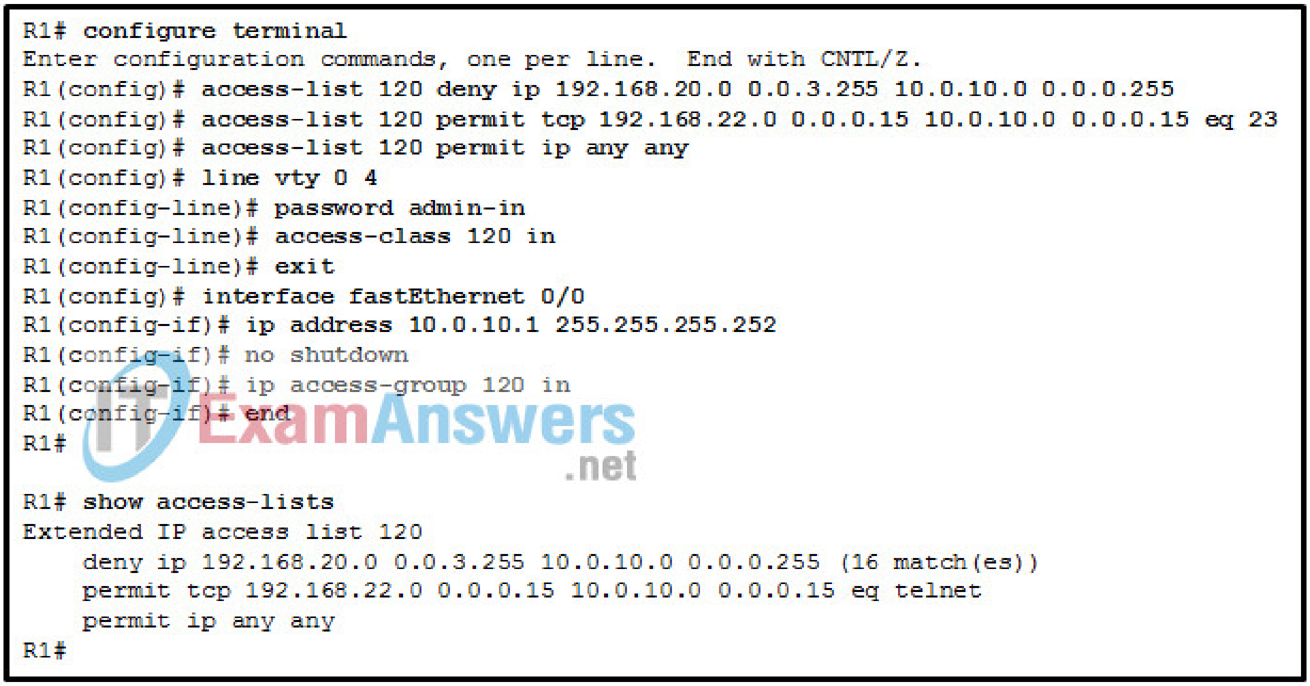


```
R1# show ip prefix-list
 ip prefix-list FILTER_Branch: 2 entries
 seq 10 permit 0.0.0.0/0  le 32
 seq 15 deny 172.18.100.0/24
```

- **Modify the order of the statements so that the deny statement is before the permit statement.**
- The prefix list needs another statement to permit the advertisement of the default route.
- Modify the permit statement to use ge 32 instead of le 32 .
- Modify the entry with sequence number 10 to be sequence number 5.
- Modify the deny statement to seq 15 deny 172.18.0.0/16.

Explanation: The order of the statements within the prefix list is wrong. Currently, all networks are permitted before the Branch network is denied. The administrator must modify the prefix list to add a sequence 5 with the deny statement to deny network 172.18.100.0/24 and remove the seq 15 statement.

7. Refer to the exhibit. A network administrator is configuring an ACL to limit the connection to R1 vty lines to only the IT group workstations in the network 192.168.22.0/28. The administrator verifies the successful Telnet connections from a workstation with IP 192.168.22.5 to R1 before the ACL is applied. However, after the ACL is applied to the interface Fa0/0, Telnet connections are denied. What is the cause of the connection failure?



```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# access-list 120 deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255
R1(config)# access-list 120 permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq 23
R1(config)# access-list 120 permit ip any any
R1(config)# line vty 0 4
R1(config-line)# password admin-in
R1(config-line)# access-class 120 in
R1(config-line)# exit
R1(config)# interface fastEthernet 0/0
R1(config-if)# ip address 10.0.10.1 255.255.255.252
R1(config-if)# no shutdown
R1(config-if)# ip access-group 120 in
R1(config-if)# end
R1#

R1# show access-lists
Extended IP access list 120
    deny ip 192.168.20.0 0.0.3.255 10.0.10.0 0.0.0.255 (16 match(es))
    permit tcp 192.168.22.0 0.0.0.15 10.0.10.0 0.0.0.15 eq telnet
    permit ip any any
R1#
```

- **The IT group network is included in the deny statement.**
- The login command has not been entered for vty lines.
- The permit ACE specifies a wrong port number.
- The enable secret password is not configured on R1.
- The permit ACE should specify protocol ip instead of tcp.

Explanation: The source IP range in the deny ACE is 192.168.20.0 0.0.3.255, which covers IP addresses from 192.168.20.0 to 192.168.23.255. The IT group network 192.168.22.0/28 is included in the 192.168.20/22 network. Therefore, the connection is denied. To fix it, the order of the deny and permit ACE should be switched.

8. Which two commands can be used to verify the content and placement of access control lists? (Choose two.)

- **show running-config**
- show ip route
- show cdp neighbor
- show processes
- **show access-lists**

Explanation: If troubleshooting or verifying an ACL, an administrator needs to view the access list statements and verify what interface and direction is being used. Two commands that accomplish this task are show access-lists and show running-config .

9. Which prefix-list entry will be used when multiple entries in a prefix list match a given prefix?

- all matching entries
- entry with the largest sequence number
- **entry with the lowest sequence number**
- entry with the longest prefix mask length

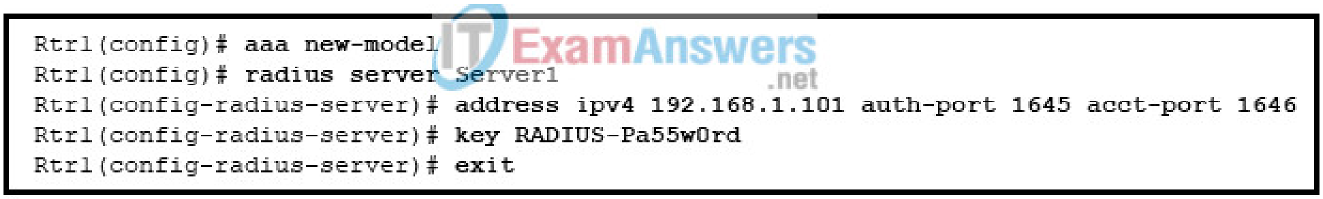
Explanation: A prefix list is made up of various sequences; these sequences are processed sequentially from the top of the prefix list to the bottom of the prefix list, in order of sequence number. A prefix list begins looking for a match using the lowest sequence number first and the very first sequence that matches is the sequence that is used.

10. Which feature is unique to IPv6 ACLs when compared to those of IPv4 ACLs?

- **an implicit permit of neighbor discovery packets**
- the use of named ACL statements
- the use of wildcard masks
- an implicit deny any any statement

Explanation: One of the major differences between IPv6 and IPv4 ACLs are two implicit permit statements at the end of any IPv6 ACL. These two permit statements allow neighbor discovery operations to function on the router interface.

11. Refer to the exhibit. The settings to connect to a RADIUS server were issued on router Rtr1. Which conclusion can be drawn if a problem occurs with AAA authentication between Rtr1 and Server1?



```
Rtr1(config)# aaa new-model
Rtr1(config)# radius server Server1
Rtr1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1645 acct-port 1646
Rtr1(config-radius-server)# key RADIUS-Pa55w0rd
Rtr1(config-radius-server)# exit
```

- The RADIUS server configuration requires that port 1813 be used for authentication and port 1812 for authorization.
- The RADIUS server configuration requires that port 49 be used for authentication and authorization.
- **The port numbers configured on the router are not identical to those configured on the RADIUS server.**
- The configuration will not be active until it is saved and Rtr1 is rebooted.

Explanation: RADIUS uses ports 1812 or 1645 (Cisco default) for authentication and 1813 or 1646 (Cisco default) for accounting. Therefore, if the RADIUS server is using ports 1812 and 1813, these same port numbers have to be configured on the Cisco router.

12. Which mitigation technique would prevent rogue servers from providing false IPv6 configuration parameters to clients?

- **enabling DHCPv6 Guard**
- enabling RA Guard
- implementing port security on edge ports
- disabling CDP on edge ports

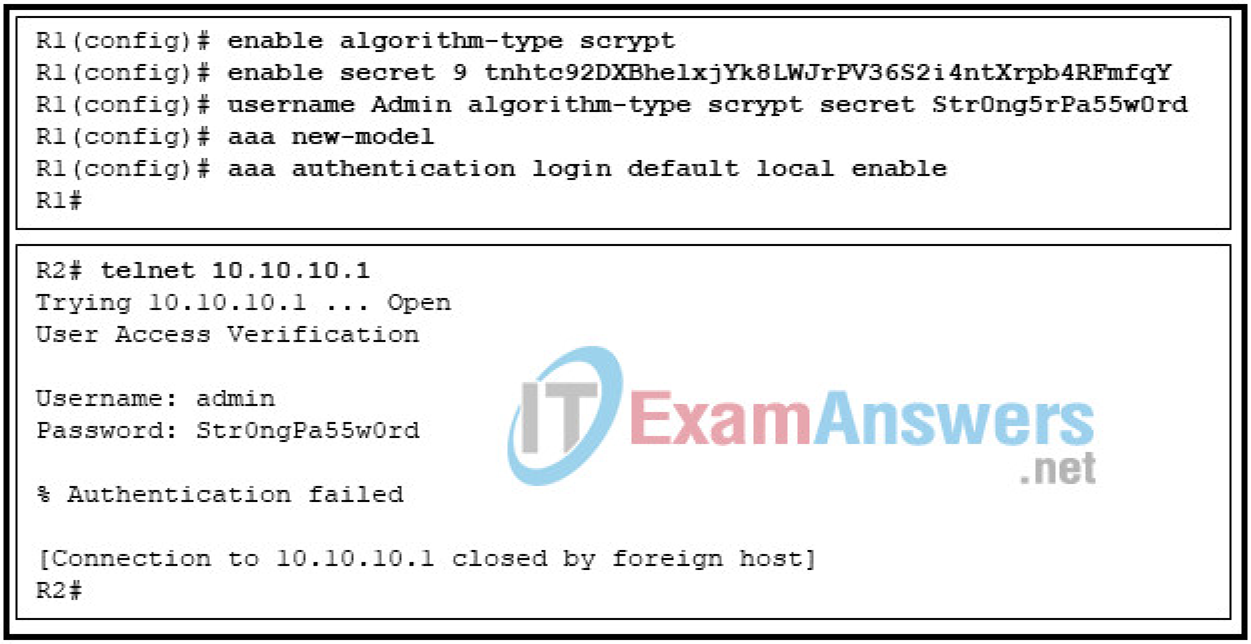
Explanation: DHCPv6 Guard is a feature designed to ensure that rogue DHCPv6 servers are not able to hand out addresses to clients, redirect client traffic, or starve out the DHCPv6 server and cause a DoS attack. DHCPv6 Guard requires a policy to be configured in DHCP Guard configuration mode, and DHCPv6 Guard is enabled on an interface-by-interface basis.

13. Which IPv6 First-Hop Security feature can block IPv6 traffic if this traffic is from an unknown origin?

- RA Guard
- **Source Guard**
- DHCPv6 Guard
- IPv6 ND inspection/snooping

Explanation: IPv6 Source Guard is a Layer 2 snooping interface feature for validating the source of IPv6 traffic. If the traffic arriving on an interface is from an unknown source, IPv6 Source Guard can block it.

14. Refer to the exhibit. Router R1 is configured as shown. An administrative user attempts to use Telnet from router R2 to R1 using the interface IP address 10.10.10.1. However, Telnet access is denied. Which conclusion can be drawn from this scenario?



```
R1(config)# enable algorithm-type scrypt
R1(config)# enable secret 9 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local enable
R1#
```

```
R2# telnet 10.10.10.1
Trying 10.10.10.1 ... Open
User Access Verification

Username: admin
Password: Str0ngPa55w0rd

% Authentication failed

[Connection to 10.10.10.1 closed by foreign host]
R2#
```

- The vty lines must be configured with the login authentication default command.
- **The password was mistyped.**
- The administrative user should use the username Admin .
- The aaa local authentication attempts max-fail command must be set to 2 or higher.

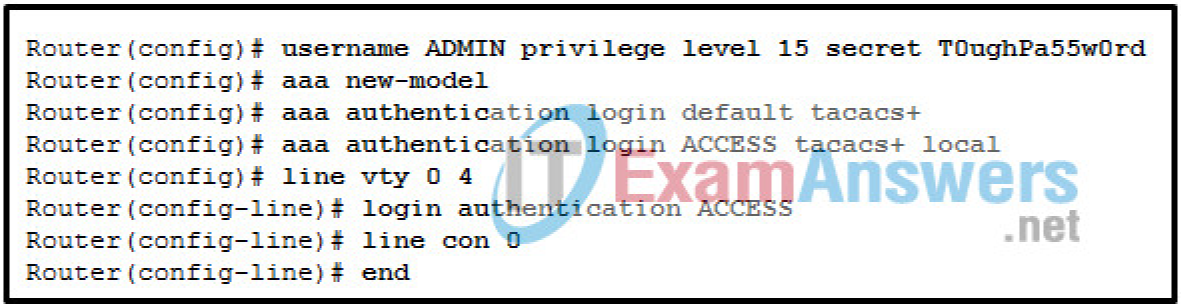
Explanation: The AAA authentication is defined with the list default with two methods. The first method is to use the local database and the second method is to use the enable password. The local keyword indicates that the username and password are not case-sensitive, so the username can be typed as “admin”. The problem is that the password is “Str0ng5rPa55w0rd” and the user typed “Str0ngPa55w0rd”.

15. What happens when a packet does not match any of the defined class maps specified in a policy map?

- The packet is transmitted to a default interface.
- The packet is transmitted to a default gateway.
- The packet is dropped.
- **The packet is subject to the policy defined in a default class.**

Explanation: If a packet does not match any of the defined classes, it is subject to the conditions laid out in the default class.

16. Refer to the exhibit. Which piece of information can be obtained from the AAA configuration commands?



```
Router(config)# username ADMIN privilege level 15 secret T0ughPa55w0rd
Router(config)# aaa new-model
Router(config)# aaa authentication login default tacacs+
Router(config)# aaa authentication login ACCESS tacacs+ local
Router(config)# line vty 0 4
Router(config-line)# login authentication ACCESS
Router(config-line)# line con 0
Router(config-line)# end
```

- If the TACACS+ AAA server is not available, no users can establish a Telnet session with the router.
- The authentication method list used by the console port is named ACCESS.
- **The authentication method list used for Telnet is named ACCESS.**
- The local database is checked first when console and Telnet access to the router is being authenticated.
- If the TACACS+ AAA server is not available, console access to the router can be authenticated using the local database.

Explanation: The login authentication ACCESS command under the line vty 0 4 command configures the AAA authentication for VTY lines access to use the method list named ACCESS. The aaa authentication login ACCESS tacacs+ local command configures the authentication method for ACCESS to use the AAA server with TACACS+ protocol. If the AAA server cannot be connected, then the local user database is used next.

17. A junior engineer is learning how to apply a service policy to a Cisco router control plane. Which piece of information should be considered to perform this configuration?

- If the direction is not applied to a service policy, the direction is input by default.
- Policy map names are not case-sensitive.
- **There are Cisco IOS versions which do not support output CoPP.**
- The service policy specified in the policy map needs to be attached to a high bandwidth Ethernet interface.

Explanation: Policy map names are case-sensitive. The service policy needs to be attached to the correct interface, the control plane interface. CoPP can be applied to packets entering or leaving the control plane interface. Not all Cisco IOS versions support output CoPP.

18. What is the recommended action when troubleshooting scenarios for CoPP, where specific source and destination IP addresses are used in the ACL?

- Use the destination IP address as the source IP address and vice-versa.
- Change the IP addresses in the ACL with respective IP broadcast addresses for both source and destination IP addresses.
- Replace the extended ACL with an standard ACL.

- **Change the IP addresses in the ACL to any / any .**

Explanation: When troubleshooting ACLs for CoPP, one recommended action if specific source and destination IP addresses are used is changing the IP addresses in the ACL to any / any . If the match is successful, then there is an issue with the original IP addresses. If not, the IP addresses were likely not the problem.

19. Which action is necessary to provide encrypted transfer of data between a RADIUS server and a AAA-enabled router?

- **Configure the preshared key exactly the same way on the server and the router.**
- Encrypt usernames and passwords that will be used between the router and the RADIUS server.
- Use identical reserved ports on the server and the router.
- Create a VPN tunnel between the server and the router.

Explanation: The key command configures the preshared key on a RADIUS server that is used for encryption. The keys must be identical on the router and on the RADIUS server. The creation of a VPN tunnel is unnecessary. The configuration of ports does not have any effect on encryption.

20. A teacher is explaining uRPF to network students in a classroom. Which two statements are accurate about uRPF operation on a Cisco router? (Choose two.)

- **It only works if Cisco Express Forwarding is enabled on a router.**
- With uRPF, any packets generated by the router and destined to the router are considered valid by default.
- **The feature helps eliminate spoofed IP packets on a network by examining the source IP address of an ingress packet.**
- It has two possible operation modes: strict and loose.
- The uRPF feature helps limit spoofed IP packets on a network by examining the source and the destination IP addresses of an ingress packet.

Explanation: Unicast Reverse Path Forwarding (uRPF) helps limit or even eliminate spoofed IP packets on a network. This is accomplished by examining the source IP address of an ingress packet and determining whether the packet is valid. Cisco Express Forwarding must be enabled on the IOS device for uRPF to work. The feature uRPF can operate in three different modes: strict, loose, and VRF. With uRPF, any packets generated by the router and destined to the router are discarded by default.

21. A network administrator is configuring SSH on a router. When verifying the configuration, the administrator notices that the SSH connection requests fail, but the Telnet connection requests from the same workstation are successful.

Which two parts of the router configuration should be checked to try to locate the problem? (Choose two.)

- **The transport input command is incorrect on the vty lines.**
- **An extended ACL that is referencing the port argument for SSH is misconfigured.**
- The ip access-class command is missing.
- The password is misconfigured on the console line.
- A standard ACL is possibly blocking the workstation from access to the router.

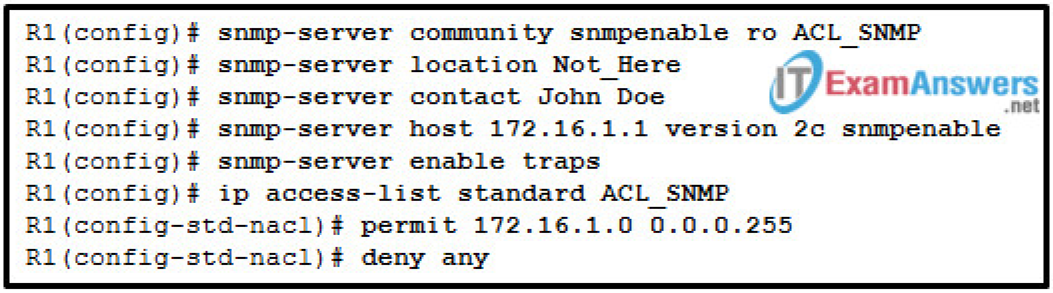
Explanation: There are several possible configuration issues to account for why SSH connections are failing. Among them are (1) the VTY lines should accept SSH connections by the transport input all or transport input ssh command; and (2) if there is an extended ACL to protect access to the vty lines, the port (either by the word ssh or the numeric number) should be included in the permit ACE. Because Telnet works, the connectivity to the vty line can be established, and thus the option that the standard ACL is blocking the workstation from access to the router does not apply. The option that the ip access-class command is missing does not apply because if the command is missing, no ACL will be applied to filter the access to vty lines. (Although the statement might be true in the router configuration, it is not a reason why SSH is not successful.) Finally the option that the password is misconfigured on the console line does not apply because SSH connects to vty lines, not to the console line.

22. A network technician is configuring SNMPv3 and has set a security level of auth . What is the effect of this setting?

- authenticates a packet by using either the HMAC MD5 or HMAC SHA algorithms and encrypts the packet with either the DES, 3DES or AES algorithms
- authenticates a packet by a string match of the username or community string
- authenticates a packet by using the SHA algorithm only
- **authenticates a packet by using either the HMAC with MD5 method or the SHA method**

Explanation: For enabling SNMPv3 one of three security levels can be configured:
1) noAuth
2) auth
3) priv
The security level configured determines which security algorithms are performed on SNMP packets. The auth security level uses either HMAC with MD5 or SHA.

23. Refer to the exhibit. A SNMP manager has IP address 172.16.1.120. The SNMP manager is unable to change configuration variables on the R1 SNMP agent. What could be the problem?

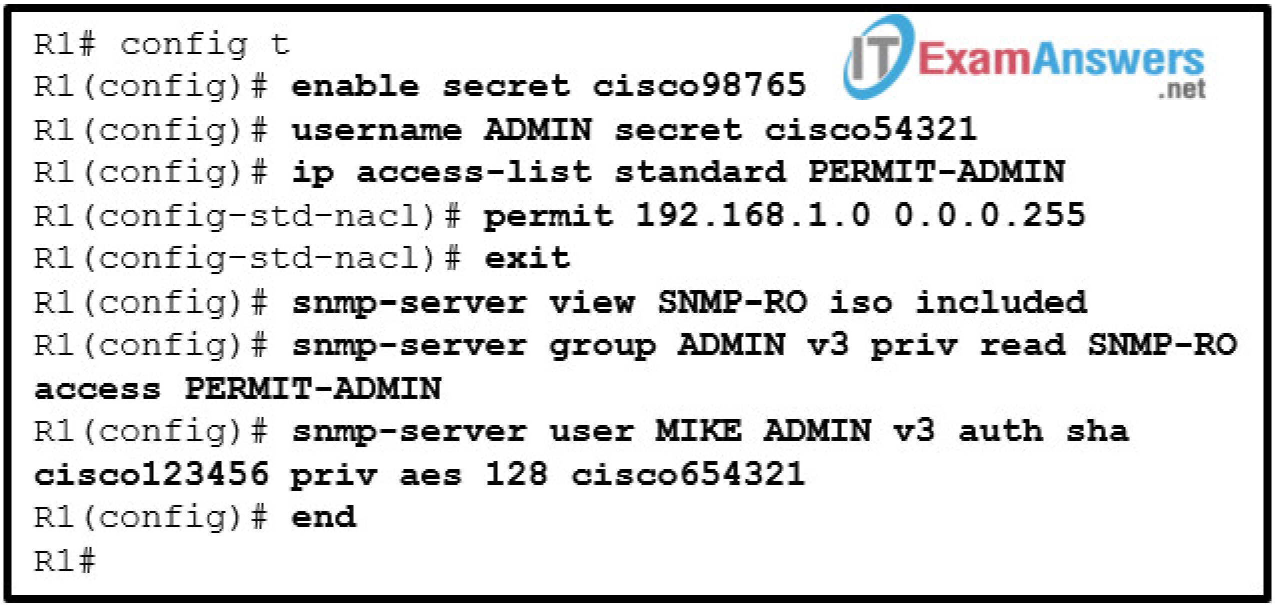


```
R1(config)# snmp-server community snmpenable ro ACL_SNMP
R1(config)# snmp-server location Not_Here
R1(config)# snmp-server contact John Doe
R1(config)# snmp-server host 172.16.1.1 version 2c snmpenable
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard ACL_SNMP
R1(config-std-nacl)# permit 172.16.1.0 0.0.0.255
R1(config-std-nacl)# deny any
```

- **The SNMP agent is not configured for write access.**
- The SNMP agent should have traps disabled.
- The IP address of the SNMP manager must be 172.16.1.1.
- The ACL of ACL_SNMP has not been implemented on an interface yet.

Explanation: Because the SNMP manager is able to access the SNMP agent, the problem is not related to the ACL configuration. The SNMP agent configuration should have an access level configured of rw to support the SNMP manager set requests. The SNMP manager cannot change configuration variables on the SNMP agent R1 with only ro access. The IP address of the SNMP manager does not have to be 172.16.1.1 to make changes to the SNMP agent. The SNMP agent does not have to have traps disabled.

24. Refer to the exhibit. Which SNMP authentication password must be used by the member of the ADMIN group that is configured on router R1?



```
R1# config t
R1(config)# enable secret cisco98765
R1(config)# username ADMIN secret cisco54321
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)# snmp-server group ADMIN v3 priv read SNMP-RO
access PERMIT-ADMIN
R1(config)# snmp-server user MIKE ADMIN v3 auth sha
cisco123456 priv aes 128 cisco654321
R1(config)# end
R1#
```

- cisco654321
- cisco54321
- cisco98765
- **cisco123456**

Explanation: The syntax for the configuration of a SNMPv3 user with a corresponding authentication and encryption password is:
Router(config)# snmp-server user username group-name v3 auth {md5 | sha} auth-password priv {des | 3des | aes {128 | 192 | 256}} privpassword

25. A computer technician is monitoring traffic on a network where users are complaining about slow network performance. The technician is curious as to whether the new network management software is causing the slowdown. Which two port numbers would the technician be looking for in the captured packets for SNMP traffic? (Choose two.)

- **162**
- 80
- **161**
- 67
- 443
- 68

Explanation: SNMP uses UDP ports 161 and 162.

26. Which two types of probes can be configured to monitor traffic by IP SLA within a network environment? (Choose two.)

- SNMP traps
- syslog messages
- website upload time
- **packet loss**
- **voice quality scores**

Explanation: IP SLA is a tool that allows for the continuous monitoring of various aspects of the network. Different types of probes can be configured to monitor traffic within a network environment:

Delay
Jitter (directional)
Packet loss (directional)
Packet sequencing (packet ordering)
Path (per hop)
Connectivity (directional)
Server or website download time
Voice quality scores

27. A network administrator has issued the snmp-server user admin1 admin v3 encrypted auth md5 abc789 priv des 256 key99 command. What are two features of this command? (Choose two.)

- **It uses the MD5 authentication of the SNMP messages.**
- It restricts SNMP access to defined SNMP managers.
- It forces the network manager to log into the agent to retrieve the SNMP messages.
- It allows a network administrator to configure a secret encrypted password on the SNMP server.
- **It adds a new user to the SNMP group.**

Explanation: The command snmp-server user admin1 admin v3 encrypted auth md5 abc789 priv des 256 key99 creates a new user and configures authentication with MD5. The command does not use a secret encrypted password on the server. The command snmp-server community string access-list-number-or-name restricts SNMP access to defined SNMP managers.

28. When configuring SSH on a router to implement secure network management, a network engineer has issued the login local and transport input ssh line vty commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)

- **Create a valid local username and password database.**
- Set the user privilege levels.
- Manually enable SSH after the RSA keys are generated.
- **Generate the asymmetric RSA keys.**
- **Configure the correct IP domain name.**
- Configure role-based CLI access.

Explanation: SSH is automatically enabled after the RSA keys are generated. Setting user privilege levels and configuring role-based CLI access are good security practices but are not a requirement of implementing SSH.

29. A technician configured a switch with console, enable secret, and VTY passwords. The service password-encryption command was then used to encrypt all unencrypted passwords. What happens if the technician issues the no service password-encryption command?

- Only the enable secret password will remain encrypted.
- All passwords, including the enable secret password, will be shown in clear text.
- The switch will issue an ‘Invalid Error’ message.
- **The passwords will still be encrypted.**

Explanation: After the service password-encryption command was issued, there is no way to present the passwords again in clear text. The no service password-encryption command stops any new passwords from being encrypted.

30. Which statement correctly describes how an ACL can be used with the access-class command to filter vty access to a router?

- **An extended ACL can be used to restrict vty access based on specific source addresses and protocol but the destination can only specify the keyword any .**
- It is only possible to apply a standard ACL to the vty lines.
- An extended ACL can be used to restrict vty access based on specific source addresses, destination addresses, and protocol.
- An extended ACL can be used to restrict vty access based on specific source and destination addresses but not on protocol.

Explanation: By design, the access-class command only matches the source IP address. Therefore, if an extended access list is used, the any parameter must be used as the destination IP address or the configuration will not work.

31. A network administrator is configuring a prefix list with the ip prefix-list command. Which entry is valid?

- **ip prefix-list LIST1 seq 5 permit 192.168.0.0/14 ge 24 le 28**
- ip prefix-list LIST1 seq 10 permit 192.168.10.0/15 le 23 ge 27
- ip prefix-list LIST1 seq 1 permit 10.18.0.0/16 ge 12
- ip prefix-list LIST1 seq 10 permit 12.16.10.0/12 le 22 ge 24

Explanation: Prefix lists are configured with the global configuration command ip prefix-list prefix-listname [seq sequence-number] { permit | deny } high-order-bit-pattern / high-order-bit-count [ge ge-value] [le le-value]. IOS and IOS XE require that the ge-value be greater than the high-order bit count and that the le-value be greater than or equal to the ge-value, that is, high-order-bit-count — ge-value — le-value .

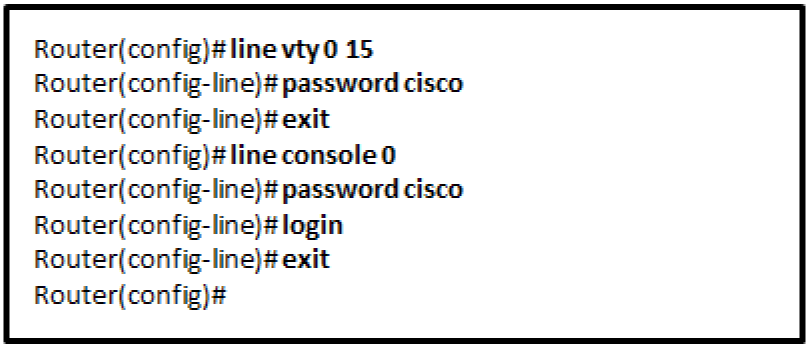
32. A network administrator configures uRPF on a Cisco router interface with the ip verify unicast source reachable-via rx allow-default command to eliminate spoofed IP packets on a network. Which conclusion can be drawn from this configuration?

- The security feature uRPF is configured with loose mode, and the route for return traffic is chosen based on a default route.
- **The security feature uRPF is configured with strict mode ,and the return path is associated with an interface chosen based on a default route.**

- The security feature uRPF is configured with loose mode, and return traffic will take a route other than one based on a default route.
- The security feature uRPF is configured with strict mode, and the return path is associated with an interface other than a default route.

Explanation: The uRPF configuration is applied on an interface-by-interface basis with the ip verify unicast source reachable-via { rx | any } [allow-default] [allow-self-ping] [list] command. For strict mode, the rx option should be used, and for loose mode the any option should be used. The allow-default option is used when the return path is associated with an interface that is chosen based on a default route.

33. Refer to the exhibit. The administrator configured the access to the console and the vty lines of a router. Which conclusion can be drawn from this configuration?



```
Router(config)#line vty 0 15
Router(config-line)#password cisco
Router(config-line)#exit
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#
```

- Access to the vty lines will not be allowed via Telnet by anyone.
- **Because the IOS includes the login command on the vty lines by default, access to the device via Telnet will require authentication.**
- Unauthorized individuals can connect to the router via Telnet without entering a password.
- Because the login command was omitted, the password cisco command is not applied to the vty lines.

Explanation: By default, the IOS includes the login command on the vty lines. This prevents Telnet access to the device without authentication. If, by mistake, the no login command is set, which removes the requirement for authentication, unauthorized persons could connect across the network to the line through Telnet. This would be a major security risk.