Cisco

200-105 Exam

Cisco Interconnecting Cisco Networking Devices Part 2 Exam

Thank you for Downloading 200-105 exam PDF Demo

You can Buy Latest 200-105 Full Version Download

https://www.certkillers.net/Exam/200-105

Version: 9.2

Question: 1

Which protocol authenticates connected devices before allowing them to access the LAN?

A. 802.1d
B. 802.11
C. 802.1w
D. 802.1x

Answer: D

Explanation:
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Question: 2

What is a difference between TACACS+ and RADIUS in AAA?

A. Only TACACS+ allows for separate authentication.
B. Only RADIUS encrypts the entire access-request packet.
C. Only RADIUS uses TCP.
D. Only TACACS+ couples authentication and authorization.

Answer: A

Explanation:
Authentication and Authorization

RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

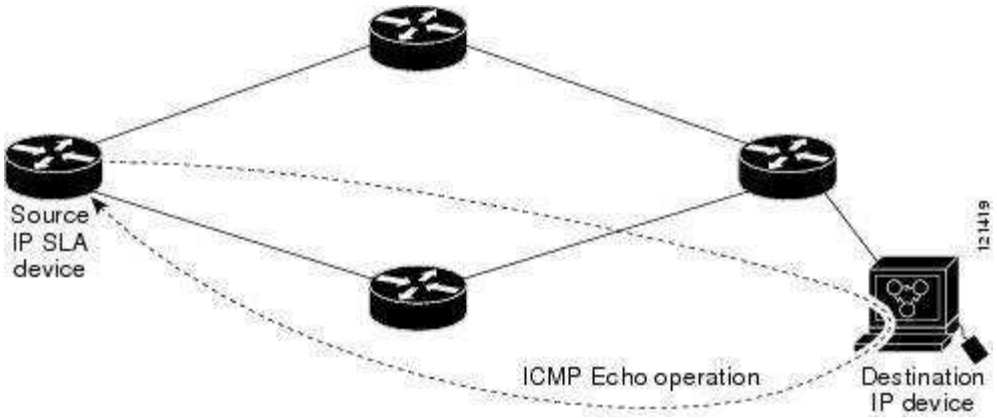
Question: 3

Which statement about the IP SLAs ICMP Echo operation is true?

A. The frequency of the operation .s specified in milliseconds.
B. It is used to identify the best source interface from which to send traffic.
C. It is configured in enable mode.
D. It is used to determine the frequency of ICMP packets.

Answer: D

Explanation:
This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing.
ICMP Echo Operation
The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply.
In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements.
Figure 1. ICMP Echo Operation



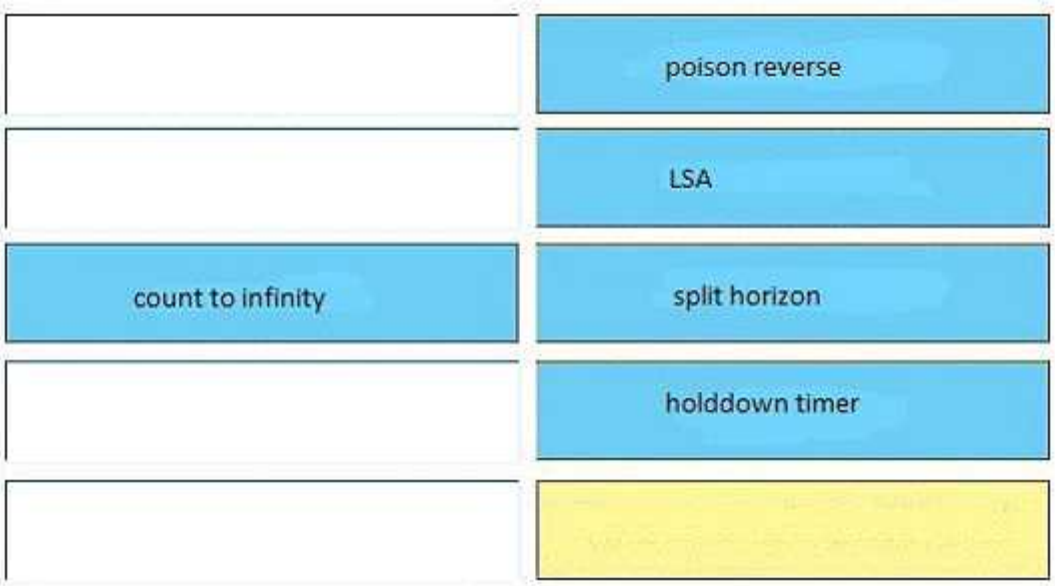
The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times.
Configuring a Basic ICMP Echo Operation on the Source Device
SUMMARY STEPS
1. enable
2. configureterminal
3. ipslaoperation-number
4. icmp-echo{destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interfaceinterface-name]
5. frequencyseconds
6. end

Question: 4

DRAG DROP
Drag the term on the left to its definition on the right. (Not all options are used.)
Select and Place:

holddown timer	A router learns from its neighbor that a route is down, and the router sends an update back to the neighbor with an infinite metric to that route
poison reverse	The packets flooded when a topology change occurs, causing network routers to update their topological databases and recalculate routes
count to infinity	This prevents sending information about a route back out the same interface that originally learned about the route
LSA	For a given period, this causes the router to ignore any updates with poorer metrics to a lost network
split horizon	

Answer:

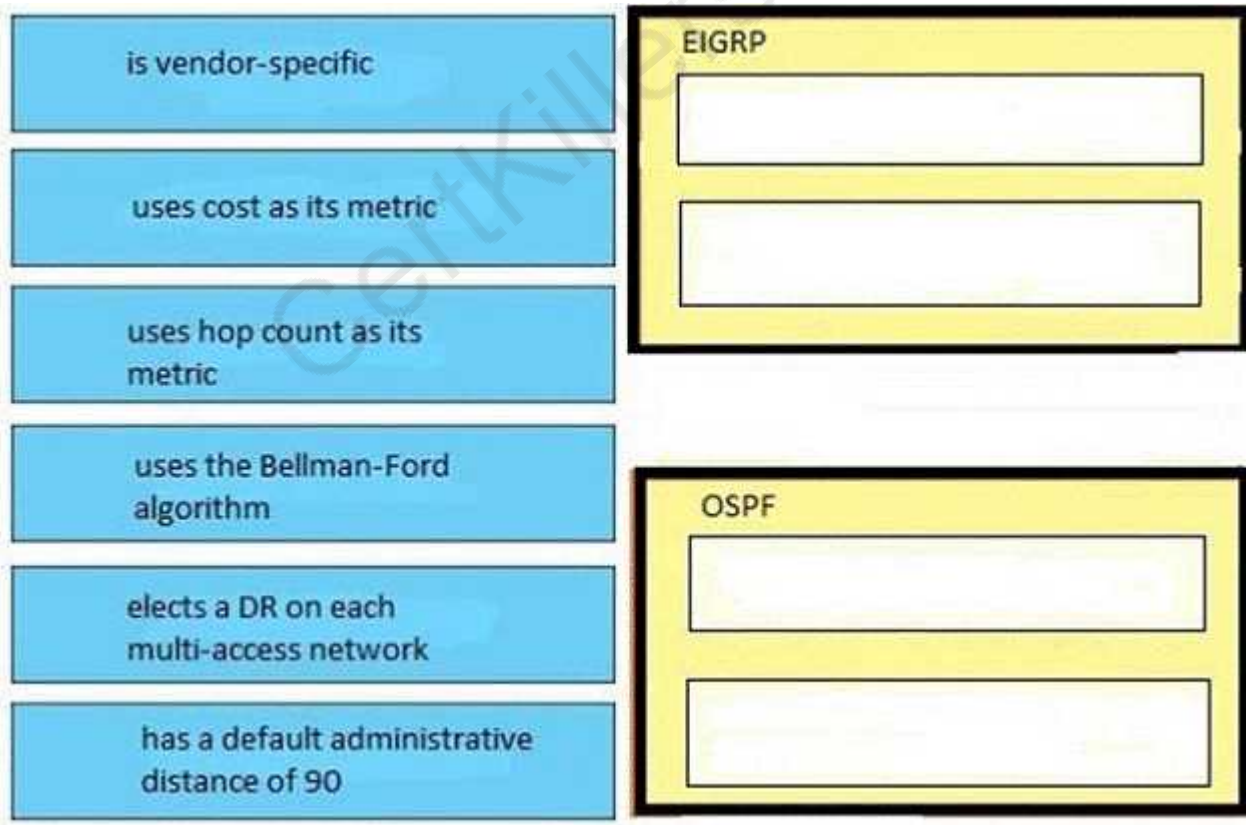


Question: 5

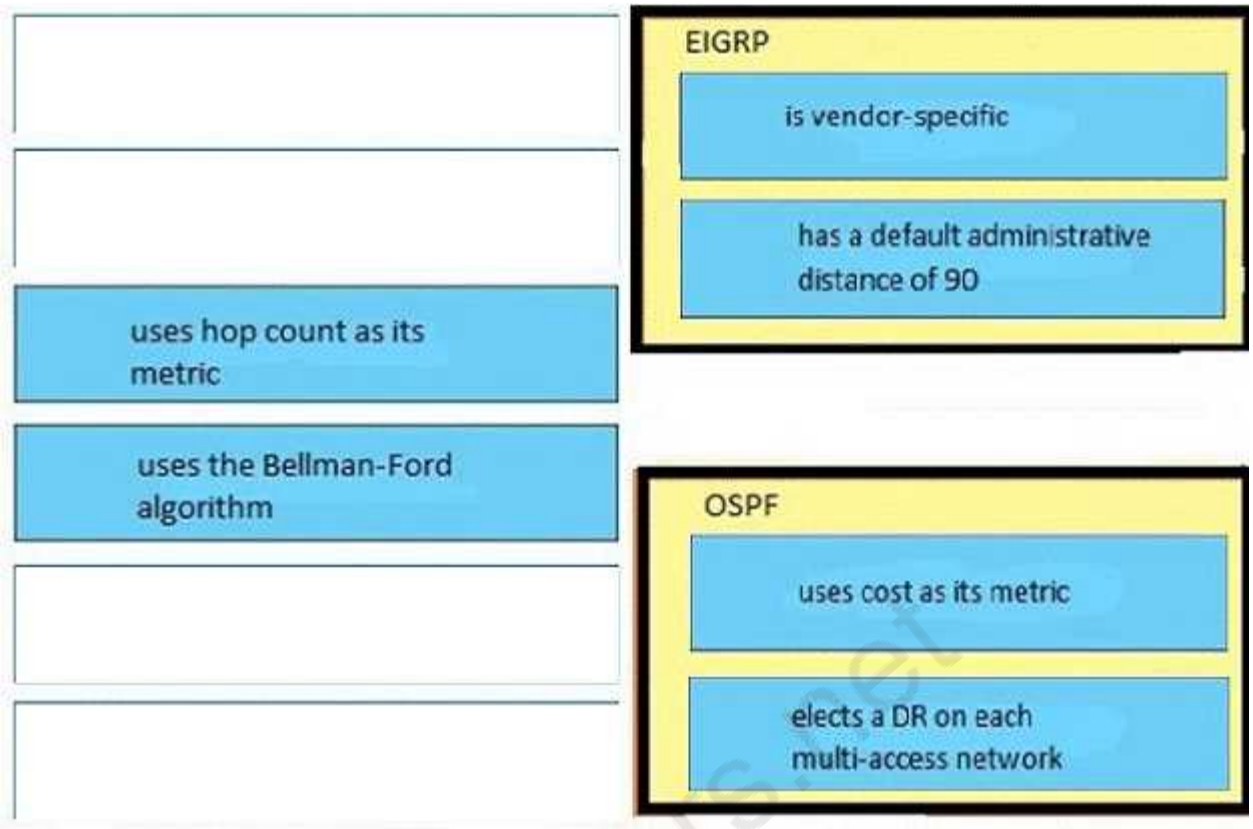
DRAG DROP

Drag the description on the left to the routing protocol on the right. (Not all options are used.)

Select and Place:



Answer:



Question: 6

What is the first step you perform to configure an SNMPv3 user?

A. Configure server traps.
B. Configure the server group.
C. Configure the server host.
D. Configure the remote engine ID.

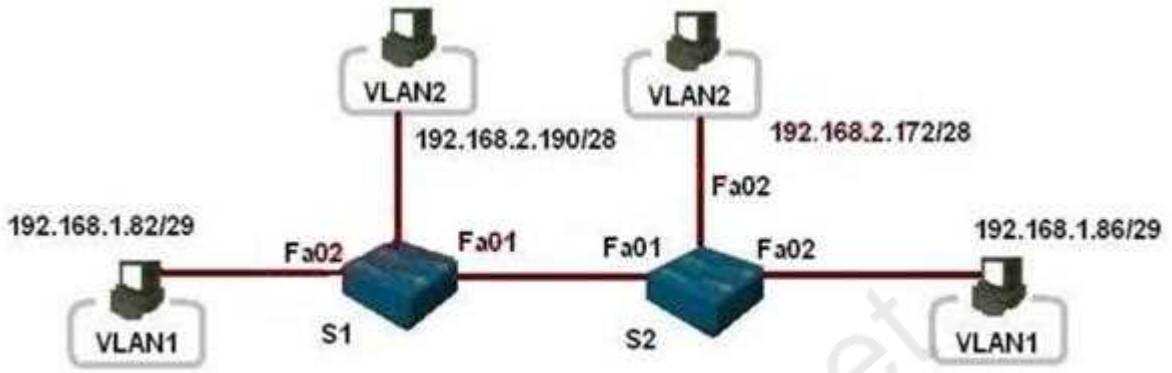
Answer: B

Explanation:
The first task in configuring SNMPv3 is to define a view. To simplify things, we'll create a view that allows access to the entire internet subtree:
router(config)#snmp-server view readview internet included
This command creates a view called readview. If you want to limit the view to the system tree, for example, replace internet with system. The included keyword states that the specified tree should be included in the view; use excluded if you wanted to exclude a certain subtree.
Next, create a group that uses the new view. The following command creates a group called readonly ; v3 means that SNMPv3 should be used. The auth keyword specifies that the entity should authenticate packets without encrypting them; readreadview says that the view named readview should be used whenever members of the readonly group access the router.

router(config)#snmp-server group readonly v3 auth read readview

Question: 7

Refer to the exhibit. A frame on VLAN 1 on switch S1 is sent to switch S2 where the frame is received on
VLAN 2.
What causes this behavior?



```
S1#show interface trunk
Port      Mode    Encapsulation Status      Network vlan
Fa0/1     on      802.1q        inuking             1

Port      Vlans allowed a trunk
Fa0/1     1.1005

Port      Vlans allowed and active in management domain
Fa0/1     12

S2#show interface trunk
Port      Mode    Encapsulation Status      Network vlan
Fa0/1     on      802.1q        inuking             2

Port      Vlans allowed a trunk
Fa0/1     1.1005

Port      Vlans allowed and active in management domain
Fa0/1     12
```

A. trunk mode mismatches
B. allowing only VLAN 2 on the destination
C. native VLAN mismatches
D. VLANs that do not correspond to a unique IP subnet

Answer: C

Question: 8

How can you disable DTP on a switch port?

A. Configure the switch port as a trunk.
B. Add an interface on the switch to a channel group.
C. Change the operational mode to static access.
D. Change the administrative mode to access.

Answer: D

Question: 9

If host Z needs to send data through router R1 to a storage server, which destination MAC address does host Z use to transmit packets?

A. the host Z MAC address
B. the MAC address of the interface on R1 that connects to the storage server
C. the MAC address of the interface on R1 that connects to host Z
D. the MAC address of the storage server interface

Answer: C

Question: 10

Which Cisco platform can verify ACLs?

A. Cisco Prime Infrastructure
B. Cisco Wireless LAN Controller
C. Cisco APIC-EM
D. Cisco IOS-XE

Answer: C

Thank You for trying 200-105 PDF Demo

To Buy Latest 200-105 Full Version Download visit link below

https://www.certkillers.net/Exam/200-105

Start Your 200-105 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your 200-105 preparation with actual exam questions.