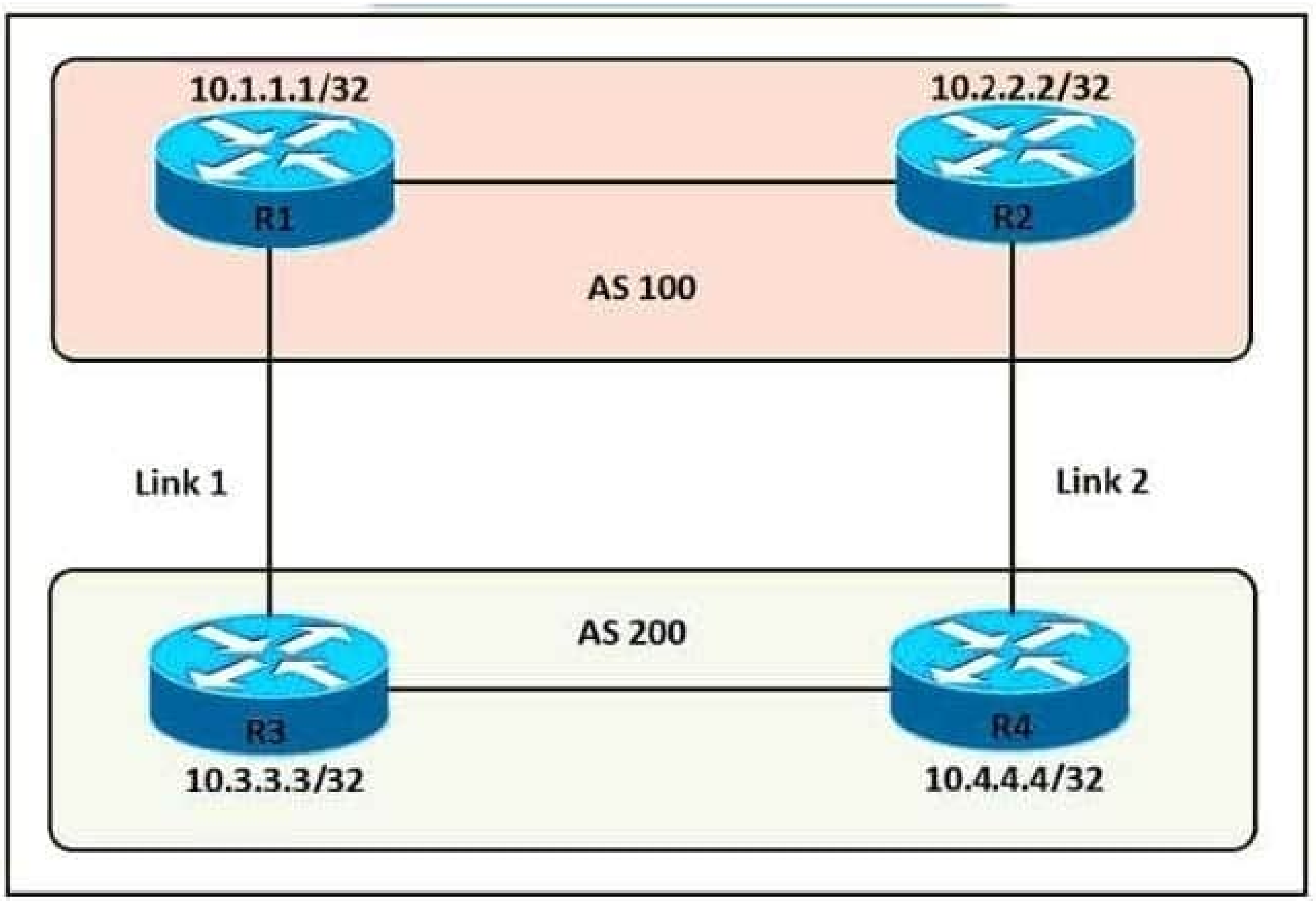
350-401Q&As

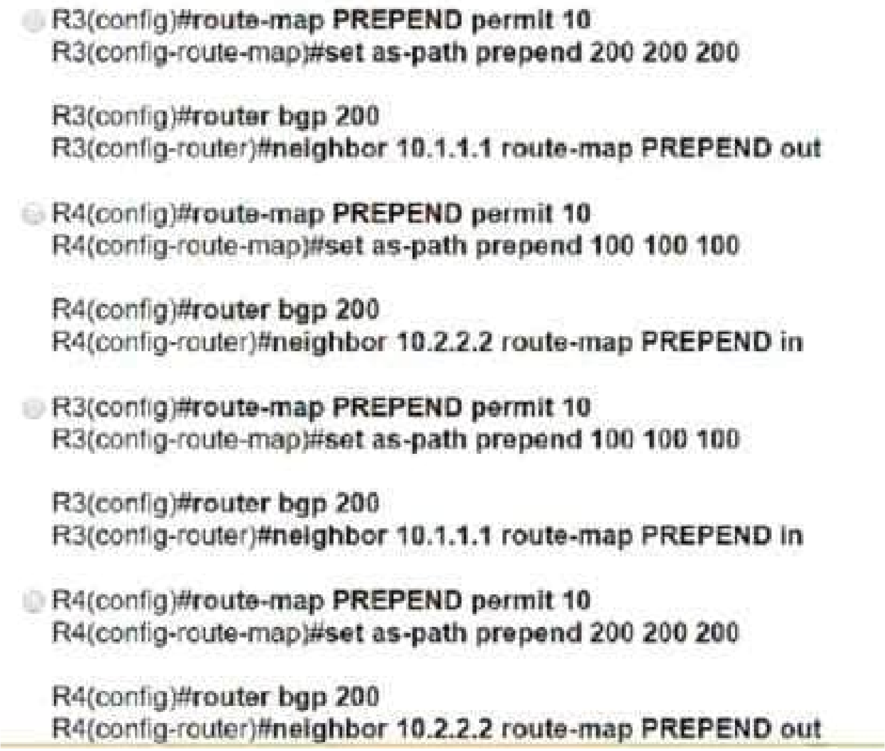
Implementing and Operating Cisco Enterprise Network Core Technologies (ENCOR) & CCIE Enterprise Infrastructure & CCIE Enterprise Wireless

QUESTION 1

Refer to the exhibit.



An engineer must ensure that all traffic leaving AS 200 will choose Link 2 as an entry point. Assuming that all BGP neighbor relationships have been formed and that the attributes have not been changed on any of the routers, which configuration accomplish task?



```
○ R3(config)#route-map PREPEND permit 10
  R3(config-route-map)#set as-path prepend 200 200 200

  R3(config)#router bgp 200
  R3(config-router)#neighbor 10.1.1.1 route-map PREPEND out

○ R4(config)#route-map PREPEND permit 10
  R4(config-route-map)#set as-path prepend 100 100 100

  R4(config)#router bgp 200
  R4(config-router)#neighbor 10.2.2.2 route-map PREPEND in

○ R3(config)#route-map PREPEND permit 10
  R3(config-route-map)#set as-path prepend 100 100 100

  R3(config)#router bgp 200
  R3(config-router)#neighbor 10.1.1.1 route-map PREPEND in

○ R4(config)#route-map PREPEND permit 10
  R4(config-route-map)#set as-path prepend 200 200 200

  R4(config)#router bgp 200
  R4(config-router)#neighbor 10.2.2.2 route-map PREPEND out
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 2

Which PAgP mode combination prevents an Etherchannel from forming?

A. auto/auto

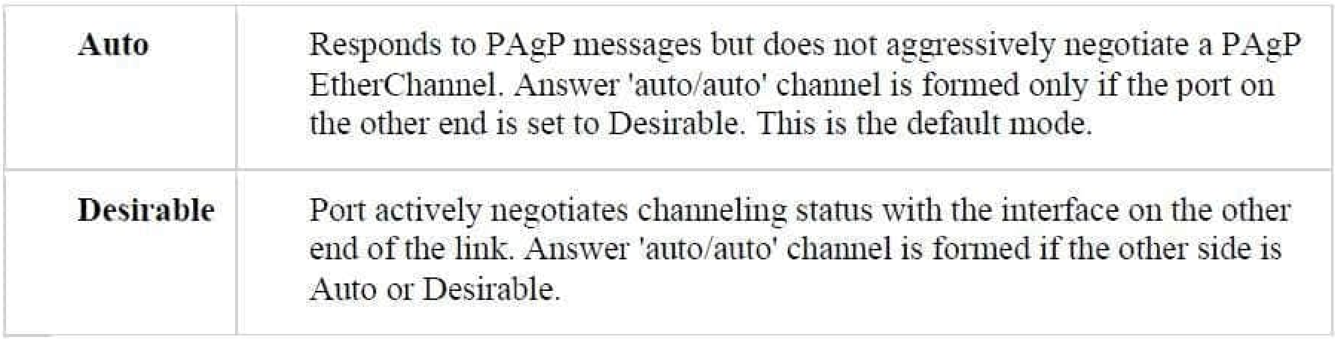
B. desirable/desirable

C. auto/desirable

D. desirable

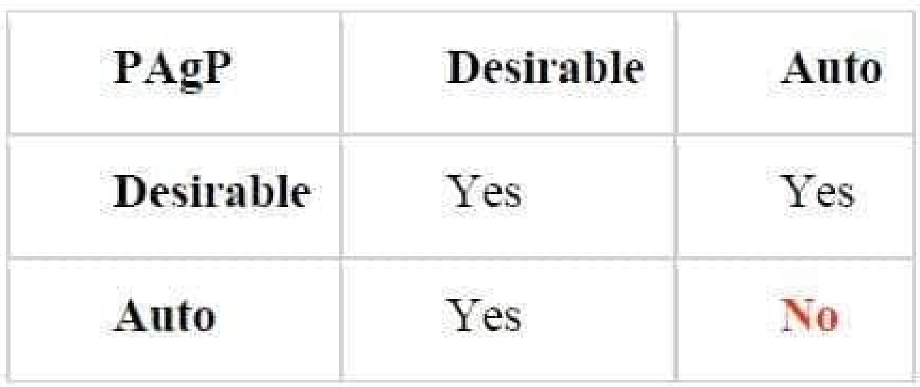
Correct Answer: A

There are two PAgP modes:



Auto	Responds to PAgP messages but does not aggressively negotiate a PAgP EtherChannel. Answer 'auto/auto' channel is formed only if the port on the other end is set to Desirable. This is the default mode.
Desirable	Port actively negotiates channeling status with the interface on the other end of the link. Answer 'auto/auto' channel is formed if the other side is Auto or Desirable.

The table below lists if an EtherChannel will be formed or not for PAgP: Reference: https://www.omnisecu.com/cisco-certified-network-associate-ccna/etherchannel-pagp-and-lacp-modes.php



PAgP	**Desirable**	**Auto**
Desirable	Yes	Yes
Auto	Yes	No

QUESTION 3

An engineer is describing QoS to a client. Which two facts apply to traffic policing? (Choose two.)

A. Policing adapts to network congestion by queuing excess traffic

B. Policing should be performed as close to the destination as possible

C. Policing drops traffic that exceeds the defined rate

D. Policing typically delays the traffic, rather than drops it

E. Policing should be performed as close to the source as possible

Correct Answer: CE

Traffic policing propagates bursts. When the traffic rate reaches the configured maximum rate (or committed information rate), excess traffic is dropped (or remarked). The result is an output rate that appears as a saw-tooth with crests and

troughs.

Unlike traffic shaping, traffic policing does not cause delay. Classification (which includes traffic policing, traffic shaping and queuing techniques) should take place at the network edge. It is recommended that classification occur as close to

the source of the traffic as possible. Also according to this Cisco link, "policing traffic as close to the source as possible".

QUESTION 4

Which algorithms are used to secure REST API from brute attacks and minimize the impact?

A. SHA-512 and SHA-384

B. MD5 algorithm-128 and SHA-384

C. SHA-1, SHA-256, and SHA-512

D. PBKDF2, BCrypt, and SCrypt

Correct Answer: D

One of the best practices to secure REST APIs is using password hash. Passwords must always be hashed to protect the system (or minimize the damage) even if it is compromised in some hacking attempts. There are many such hashing

algorithms which can prove really effective for password security e.g. PBKDF2, bcrypt and scrypt algorithms.

Other ways to secure REST APIs are: Always use HTTPS, Never expose information on URLs (Usernames, passwords, session tokens, and API keys should not appear in the URL), Adding Timestamp in Request, Using OAuth, Input

Parameter Validation.

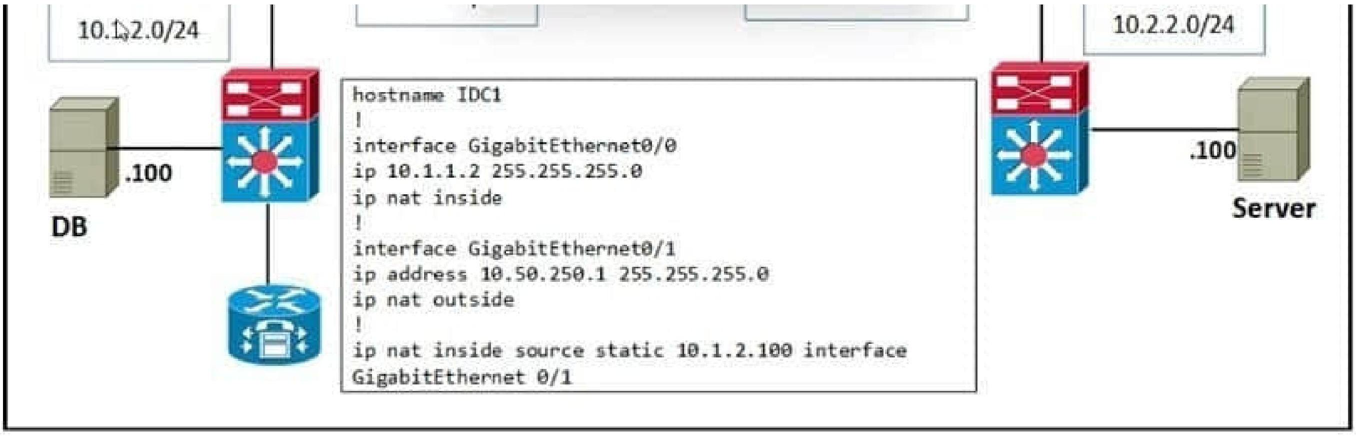
Reference: https://restfulapi.net/security-essentials/

We should not use MD5 or any SHA (SHA-1, SHA-256, SHA-512...) algorithm to hash password as they are not totally secure. Note: A brute-force attack is an attempt to discover a password by systematically trying every possible

combination of letters, numbers, and symbols until you discover the one correct combination that works.

QUESTION 5

Refer to the exhibit.



```
hostname IDC1
!
interface GigabitEthernet0/0
ip 10.1.1.2 255.255.255.0
ip nat inside
!
interface GigabitEthernet0/1
ip address 10.50.250.1 255.255.255.0
ip nat outside
!
ip nat inside source static 10.1.2.100 interface
GigabitEthernet 0/1
```

The server in DC2 is expecting traffic from the database in DC1 to use the source network of 10.50.250.0/24. The server sends the initial request. The inside global IP is configured for 10.50.250.1. What is the result of this configuration?

A. Only the server can initiate communication.

B. The server and the database cannot communicate.

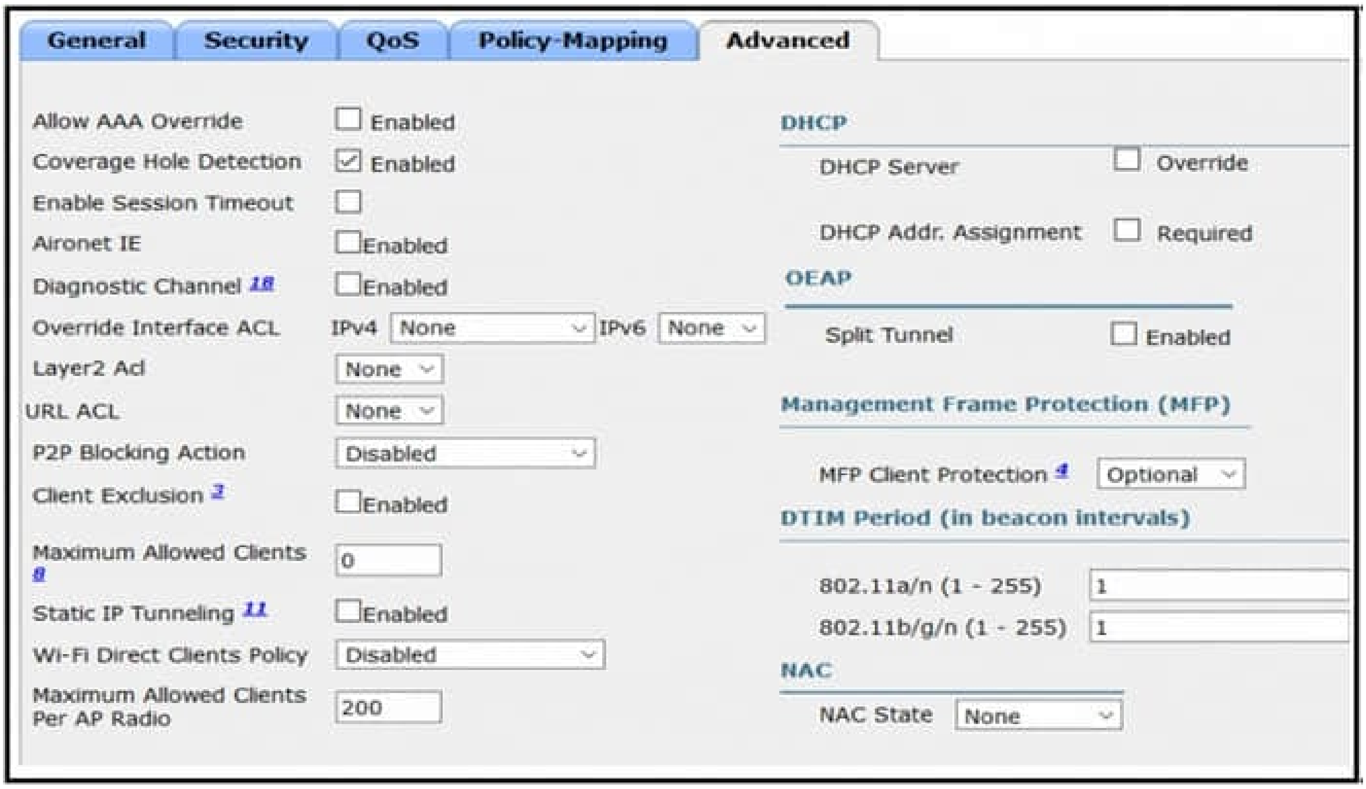
C. The server and the database can initiate communication.

D. Only the database can initiate communication

Correct Answer: C

QUESTION 6

Refer to the exhibit.



Allow AAA Override □ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout □
Aironet IE □Enabled
Diagnostic Channel 18 □Enabled
Override Interface ACL IPv4 None IPv6 None
Layer2 Acl None
URL ACL None
P2P Blocking Action Disabled
Client Exclusion 2 □Enabled
Maximum Allowed Clients 8 0
Static IP Tunneling 11 □Enabled
Wi-Fi Direct Clients Policy Disabled
Maximum Allowed Clients Per AP Radio 200

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

OEAP
Split Tunnel □ Enabled

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

An engineer is investigating why guest users are able to access other guest user devices when the users are connected to the customer guest WLAN. What action resolves this issue?

A. implement MFP client protection

B. implement split tunneling

C. implement P2P blocking

D. implement Wi-Fi direct policy

Correct Answer: C

Reference: 2.3 Ensure `Peer-to-Peer Blocking Action` is set to `Drop\\' for All `Wireless LAN Identifiers\\' (Scored)

Description:

This control determines whether the Wireless LAN Controller is configured to prevent clients connected to the same Wireless Local Area Controller from communicating with each other. Wireless Client Isolation prevents wireless clients from

communicating with each other over the RF. Packets that arrive on the wireless interface are forwarded only out the wired interface of an Access Point. One wireless client could potentially compromise another client sharing the same wireless

network.

QUESTION 7

An engineer uses the Design workflow to create a new network infrastructure in Cisco DNA Center. How is the physical network device hierarchy structured?

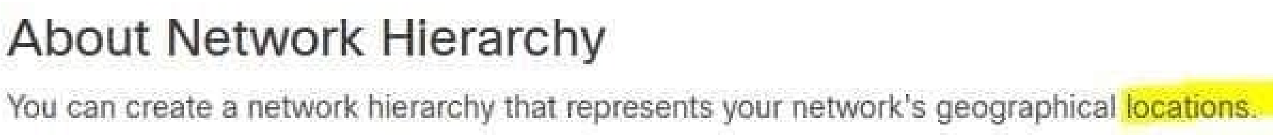
A. by location

B. by role

C. by organization

D. by hostname naming convention

Correct Answer: A



About Network Hierarchy

You can create a network hierarchy that represents your network's geographical locations.

QUESTION 8

Which statement about VXLAN is true?

A. VXLAN uses TCP 35 the transport protocol over the physical data cento network.

B. VXLAN extends the Layer 2 Segment ID field to 24-bits. which allows up to 4094 unique Layer 2 segments over the same network.

C. VXLAN encapsulates a Layer 2 frame in an IP-UDP header, which allows Layer 2 adjacency across router boundaries.

D. VXLAN uses the Spanning Tree Protocol for loop prevention.

Correct Answer: C

802.1Q VLAN identifier space is only 12 bits. The VXLAN identifier space is 24 bits. This doubling in size allows the VXLAN ID space to support 16 million Layer 2 segments -> Answer \\'VXLAN extends the Layer 2 Segment ID field to 24-bits,

which allows up to 4094 unique Layer 2 segments over the same network\\' is not correct.

VXLAN is a MAC-in-UDP encapsulation method that is used in order to extend a Layer 2 or Layer 3 overlay network over a Layer 3 infrastructure that already exists.

Reference:

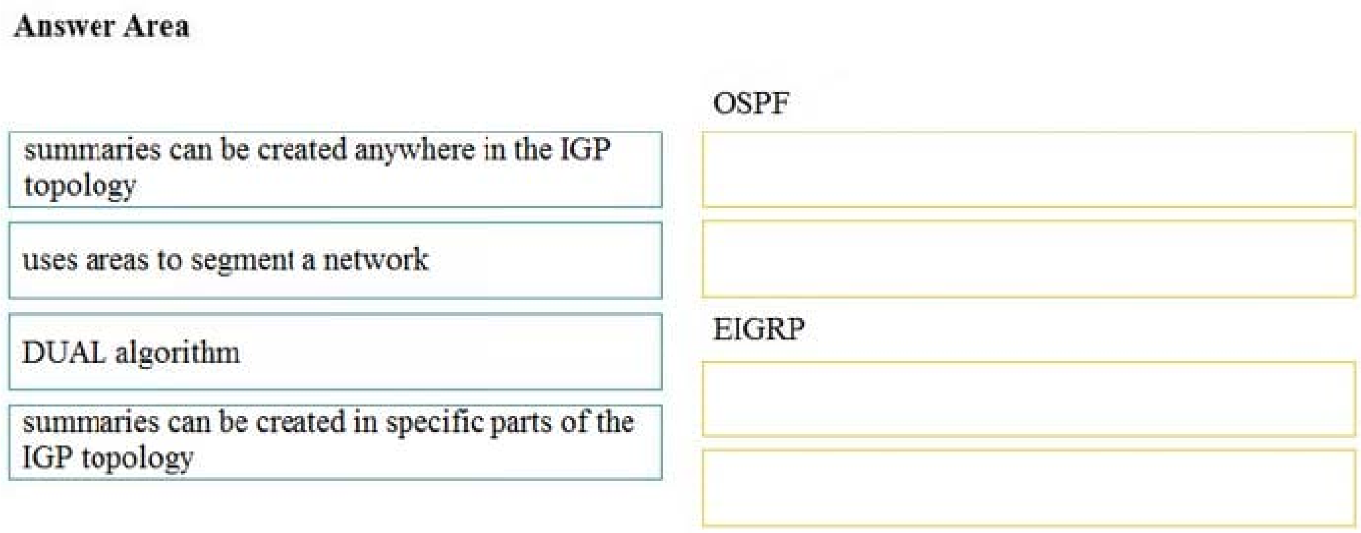
https://www.cisco.com/c/en/us/support/docs/lan-switching/vlan/212682- virtualextensible-lan-and-ethernet-virt.html

QUESTION 9

DRAG DROP

Drag and drop the descriptions from the left onto the routing protocol they describe on the right.

Select and Place:



Answer Area

summaries can be created anywhere in the IGP topology

uses areas to segment a network

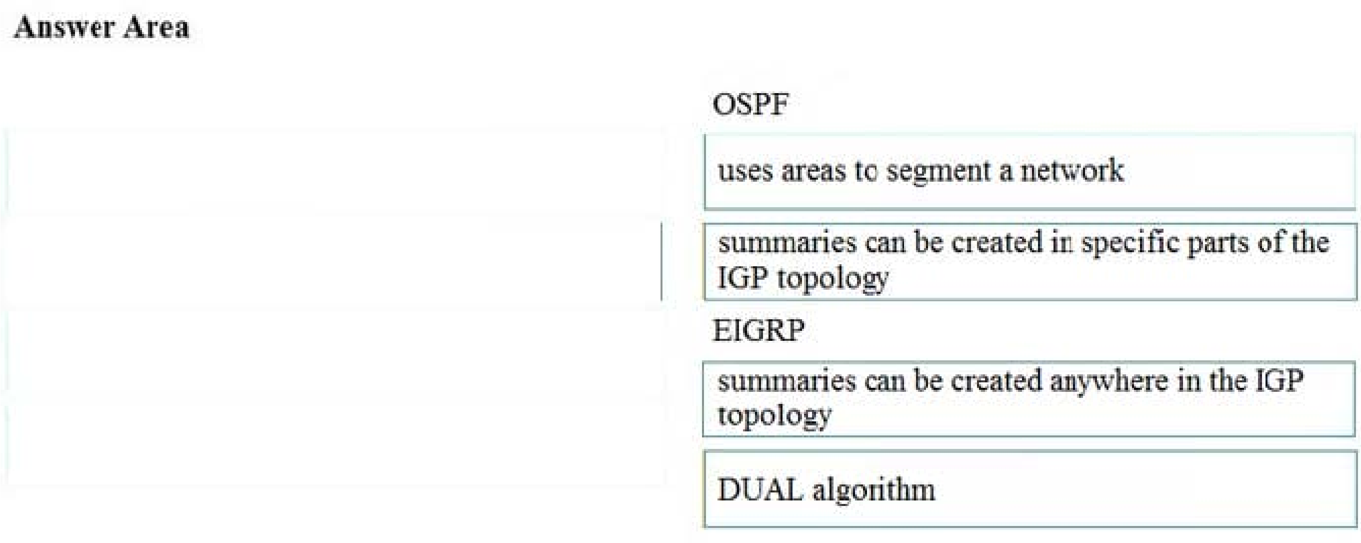
DUAL algorithm

summaries can be created in specific parts of the IGP topology

OSPF

EIGRP

Correct Answer:



Answer Area

OSPF

uses areas to segment a network

summaries can be created in specific parts of the IGP topology

EIGRP

summaries can be created anywhere in the IGP topology

DUAL algorithm

QUESTION 10

Which of the following are features typically only found in a Next Generation (NextGen) firewall? (Choose two.)

A. Network Address Translation (NAT)

B. Secure remote access VPN (RA VPN)

C. Deep packet inspection

D. reputation based malware detection

E. IPSec site-to-site VPN

Correct Answer: CD

QUESTION 11

Which technology provides a secure communication channel for all traffic at Layer 2 of the OSI model?

A. MACsec

B. IPsec

C. SSL

D. Cisco Trustsec

Correct Answer: A

MACsec, defined in 802.1AE, provides MAC-layer encryption over wired networks by using out- ofband methods for encryption keying. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA and MACsec are implemented after successful authentication using the 802.1x Extensible Authentication Protocol (EAP-TLS) or Pre Shared Key (PSK) framework. A switch using MACsec accepts either MACsec or non-MACsec frames, depending on the policy associated with the MKA peer. MACsec frames are encrypted and protected with an integrity check value (ICV). When the switch receives frames from the MKA peer, it decrypts them and calculates the correct ICV by using session keys provided by MKA. The switch compares that ICV to the ICV within the frame. If they are not identical, the frame is dropped. The switch also encrypts and adds an ICV to any frames sent over the secured port (the access point used to provide the secure MAC service to a MKA peer) using the current session key.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-9/configuration_guide/sec/b_169_sec_9300_cg/macsec_encryption.html

Note: Cisco Trustsec is the solution which includes MACsec.

QUESTION 12

What are three valid HSRP states? (Choose three)

A. INIT

B. listen

C. full

D. learning

E. speak

F. established

Correct Answer: ABE

HSRP StatesWhen in operation, HSRP devices are configured into one of many states:

Active ?This is the state of the device that is actively forwarding traffic.

Init or Disabled ?This is the state of a device that is not yet ready or able to participate in HSRP.

Learn ?This is the state of a device that has not yet determined the virtual IP address and has not yet seen a hello message from an active device.

Listen ?This is the state of a device that is receiving hello messages.

Speak ?This is the state of a device that is sending and receiving hello messages.

Standby ?This is the state of a device that is prepared to take over the traffic forwarding duties from the active device.

QUESTION 13

Which characteristic distinguishes Ansible from Chef?

A. Ansible lacs redundancy support for the master server. Chef runs two masters in an active/active mode.

B. Ansible uses Ruby to manage configurations. Chef uses YAML to manage configurations.

C. Ansible pushes the configuration to the client. Chef client pulls the configuration from the server.

D. The Ansible server can run on Linux, Unix or Windows. The Chef server must run on Linux or Unix.

Correct Answer: C

Ansible works by connecting to your nodes and pushing out small programs, called "Ansible modules" to them. These programs are written to be resource models of the desired state of the system. Ansible then executes these modules (over

SSH by default), and removes them when finished.

Chef is a much older, mature solution to configure management. Unlike Ansible, it does require an installation of an agent on each server, named chef-client. Also, unlike Ansible, it has a Chef server that each client pulls configuration from.

QUESTION 14

How do agent-based versus agentless configuration management tools compare?

A. Agent-based tools do not require a high-level language interpreter such as Python or Ruby on slave nodes

B. Agentless tools require no messaging systems bet-veen master and slaves.

C. Agent-based tools do not require instaltation of additional software packages on the slave nodes

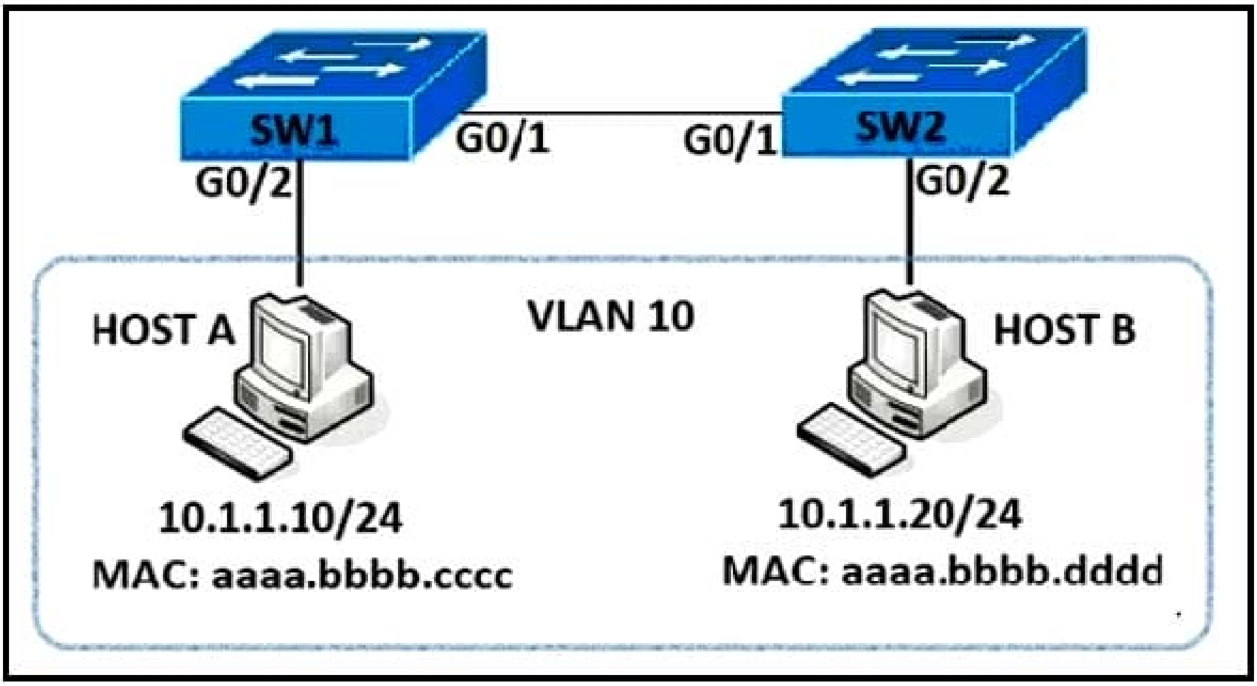
D. Agentless tools use proxy nodes to interface with slave nodes

Correct Answer: A

QUESTION 15

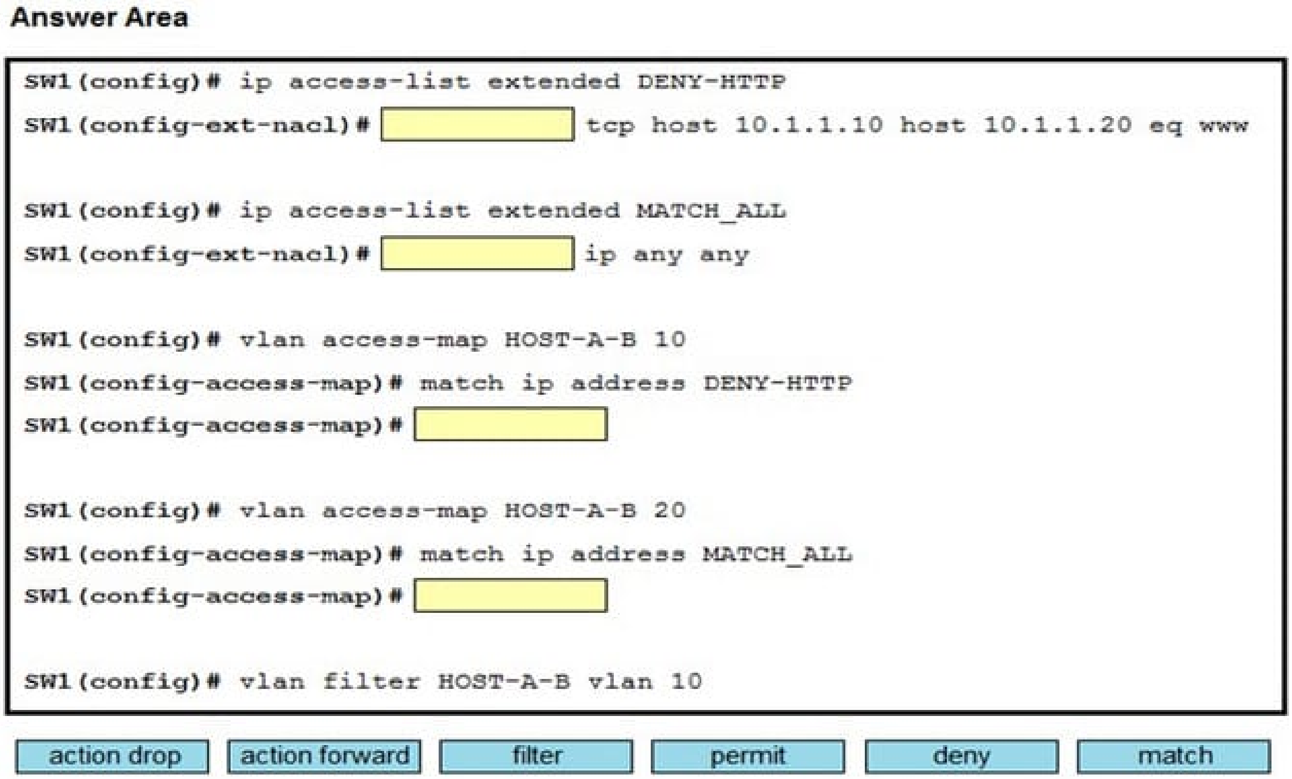
DRAG DROP

Refer to the exhibit. An engineer must deny HTTP traffic from host A to host V while allowing all other communication between the hosts, drag and drop the commands into the configuration to achieve these results.



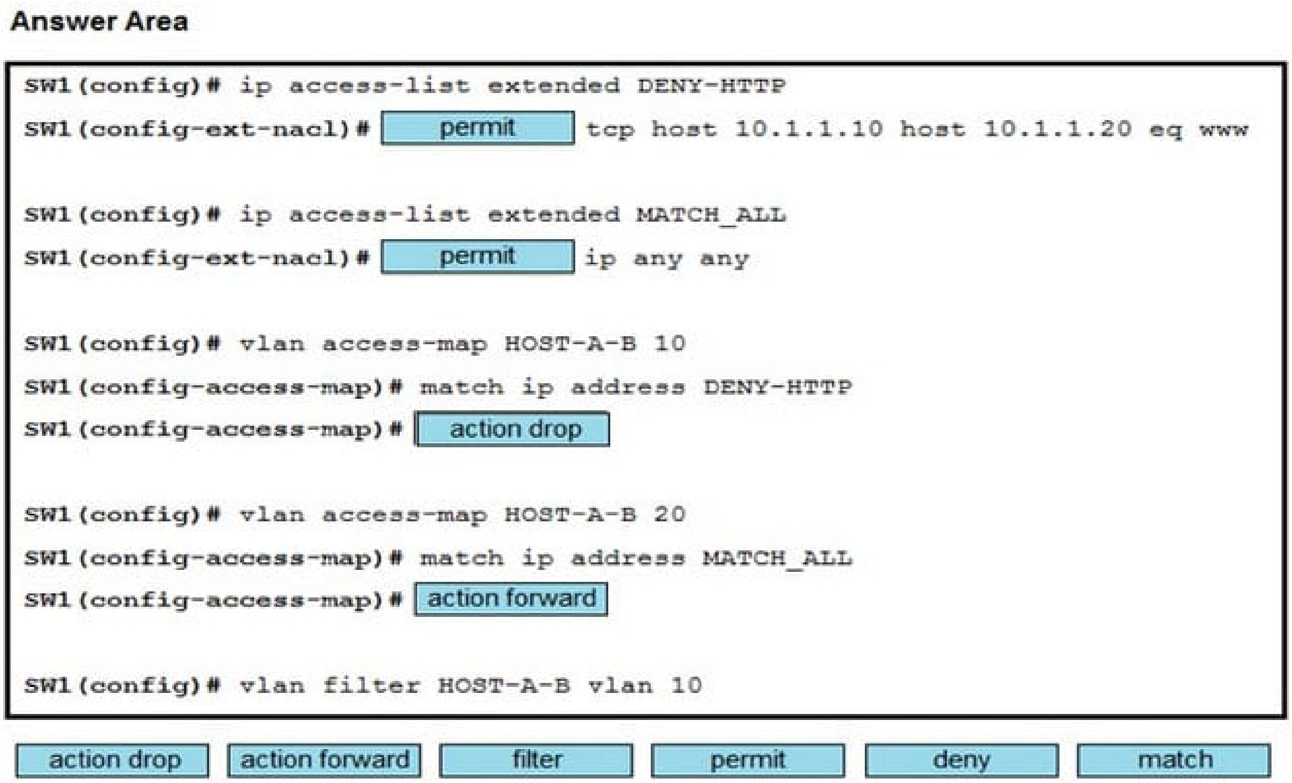
Some commands may be used more than once. Not all commands are used.

Select and Place:


Answer Area

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# __________ tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# __________ ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# __________

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# __________

SW1(config)# vlan filter HOST-A-B vlan 10
```

Correct Answer:



Answer Area

```
SW1(config)# ip access-list extended DENY-HTTP
SW1(config-ext-nacl)# permit tcp host 10.1.1.10 host 10.1.1.20 eq www

SW1(config)# ip access-list extended MATCH_ALL
SW1(config-ext-nacl)# permit ip any any

SW1(config)# vlan access-map HOST-A-B 10
SW1(config-access-map)# match ip address DENY-HTTP
SW1(config-access-map)# action drop

SW1(config)# vlan access-map HOST-A-B 20
SW1(config-access-map)# match ip address MATCH_ALL
SW1(config-access-map)# action forward

SW1(config)# vlan filter HOST-A-B vlan 10
```

When talking about access-lists or prefix-lists associated with *-maps, Permit and Deny take on new meanings.

As we all know, a *-list processes each entry until a match is found.

Once a match is found, processing of the *-list stops.

*-maps operate the same way.

-

If the matched statement is \\'permit,\\' the *-list reports back to the *-map with a match success, which allows the *-map to process the associated action. No further *-map sequences are processed.

-

If the matched statement is \\'deny,\\' the *-list reports back to the *-map with NO MATCH; wherein the *-map will proceed to the next *-map sequence until a *-map match IS found.

-

If NO statement is matched in the *-list, the implicit \\'deny any any\\' is ALWAYS matched. In This case, the *-list will report to the *-map with NO MATCH, and the *-map will proceed to the next sequence until a match IS found.

Latest 350-401 Dumps 350-401 VCE Dumps 350-401 Study Guide