

CCNP ROUTE

Number: 300-301
Passing Score: 800
Time Limit: 120 min
File Version: 9.0

Cisco 300-101
Implementing Cisco IP Routing
Version: 9.0



Exam A

QUESTION 1

A network administrator executes the command clear ip route. Which two tables does this command clear and rebuild? (Choose two.)

- A. IP routing
- B. FIB
- C. ARP cache
- D. MAC address table
- E. Cisco Express Forwarding table
- F. topology table

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

To clear one or more entries in the IP routing table, use the following commands in any mode:

Command

Purpose

```
clear ip route {* | {route |  
prefix/length}}{next-hop interface}}  
[vrf vrf-name]
```

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 6

Example:

```
switch(config)# clear ip route  
10.2.2.2
```

Clears one or more routes from both the unicast RIB and all the module FIBs. The route options are as follows:

-
- *—All routes.
-
- route**—An individual IP route.
-
- prefix/length**—Any IP prefix.
-
- next-hop**—The next-hop address
-

interface—The interface to reach the next-hop address.

The **vrf-name** can be any case-sensitive, alphanumeric string up to 32 characters.

Reference:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/unicast/5_0_3_N1_1/Cisco_n5k_layer3_ucast_cfg_rel_503_N1_1/l3_manage-routes.html

QUESTION 2

Which switching method is used when entries are present in the output of the command show ip cache?

- A. fast switching
- B. process switching
- C. Cisco Express Forwarding switching
- D. cut-through packet switching

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding. Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching. To display the routing table cache used to fast switch IP traffic, use the “show ip cache” EXEC

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/command/reference/fswtch_r/xfscmd5.html#wp1038133

QUESTION 3

Which two actions must you perform to enable and use window scaling on a router? (Choose two.)

- A. Execute the command ip tcp window-size 65536
- B. Set window scaling to be used on the remote host.
- C. Execute the command ip tcp queuemax
- D. Set TCP options to "enabled" on the remote host.
- E. Execute the command ip tcp adjust-mss

Correct Answer: AB

Section: (none)

Explanation

Explanation/Reference:

The TCP Window Scaling feature adds support for the Window Scaling option in RFC 1323, TCP Extensions for High Performance. A larger window size is recommended to improve TCP performance in network paths with large bandwidth-delay product characteristics that are called Long Fat Networks (LFNs). The TCP Window Scaling enhancement provides that support.

The window scaling extension in Cisco IOS software expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header. The window size can increase to a scale factor of 14. Typical applications use a scale factor of 3 when deployed in LFNs.

The TCP Window Scaling feature complies with RFC 1323. The larger scalable window size will allow TCP to perform better over LFNs. Use **the ip tcp window-size** command in global configuration mode to configure the TCP window size. In order for this to work, the remote host must also support this feature and its window size must be increased.

Reference: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/12-4t/iap-12-4tbook/iap-tcp.html#GUID-BD998AC6-F128-47DD-B5F7-B226546D4B08>

QUESTION 4

Which three TCP enhancements can be used with TCP selective acknowledgments? (Choose three.)

- A. header compression
- B. explicit congestion notification
- C. keepalive
- D. time stamps
- E. TCP path discovery
- F. MTU window

Correct Answer: BCD

Section: (none)

Explanation

Explanation/Reference:

TCP Selective Acknowledgment

The TCP Selective Acknowledgment feature improves performance if multiple packets are lost from one TCP window of data.

Prior to this feature, because of limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per-round-trip time. An aggressive sender could choose to resend packets early, but such re-sent segments might have already been

successfully received.

The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that has been received. In other words, the receiver can acknowledge packets received out of order. The sender can then resend only missing data segments (instead of everything since the first missing packet).

Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would need to be re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 must be re-sent.

TCP selective acknowledgment is used only when multiple packets are dropped within one TCP window. There is no performance impact when the feature is enabled but not used. Use the `ip tcp selective-ack` command in global configuration mode to enable TCP selective acknowledgment. Refer to RFC 2018 for more details about TCP selective acknowledgment.

TCP Time Stamp

The TCP time-stamp option provides improved TCP round-trip time measurements. Because the time stamps are always sent and echoed in both directions and the time-stamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP time-stamp option is disabled. Use the `ip tcp timestamp` command to enable the TCP time-stamp option.

TCP Explicit Congestion Notification

The TCP Explicit Congestion Notification (ECN) feature allows an intermediate router to notify end hosts of impending network congestion. It also provides enhanced support for TCP sessions associated with applications, such as Telnet, web browsing, and transfer of audio and video data that are sensitive to delay or packet loss. The benefit of this feature is the reduction of delay and packet loss in data transmissions. Use the `ip tcp ecn` command in global configuration mode to enable TCP ECN.

TCP Keepalive Timer

The TCP Keepalive Timer feature provides a mechanism to identify dead connections. When a TCP connection on a routing device is idle for too long, the device sends a TCP keepalive packet to the peer with only the Acknowledgment (ACK) flag turned on. If a response packet (a TCP ACK packet) is not received after the device sends a specific number of probes, the connection is considered dead and the device initiating the probes frees resources used by the TCP connection.

Reference: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/xe-3s/asr1000/iap-xe-3s-asr1000-book/iap-tcp.html#GUID-22A82C5F-631F-4390-9838-F2E48FFEEA01>

QUESTION 5

A network administrator uses IP SLA to measure UDP performance and notices that packets on one router have a higher one-way delay compared to the opposite direction. Which UDP characteristic does this scenario describe?

- A. latency
- B. starvation
- C. connectionless communication
- D. nonsequencing unordered packets
- E. jitter

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Cisco IOS IP SLAs provides a proactive notification feature with an SNMP trap. Each measurement operation can monitor against a pre-set performance threshold. Cisco IOS IP SLAs generates an SNMP trap to alert management applications if this threshold is crossed. Several SNMP traps are available: round trip time, average jitter, **one-way latency**, jitter, packet loss, MOS, and connectivity tests.

Here is a partial sample output from the IP SLA statistics that can be seen:

```
router#show ip sla statistics 1
```

```
Round Trip Time (RTT) for Index 55
```

```
Latest RTT: 1 ms
```

```
Latest operation start time: *23:43:31.845 UTC Thu Feb 3 2005
```

```
Latest operation return code: OK
```

```
RTT Values:
```

```
Cisco 300-101 Exam
```

```
"Pass Any Exam. Any Time." - www.actualtests.com 10
```

```
Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds
```

```
Latency one-way time:
```

```
Number of Latency one-way Samples: 0
```

```
Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
```

```
Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
```

Reference:

http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html

QUESTION 6

Under which condition does UDP dominance occur?

- A. when TCP traffic is in the same class as UDP
- B. when UDP flows are assigned a lower priority queue
- C. when WRED is enabled

D. when ACLs are in place to block TCP traffic

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

It is a general best practice to not mix TCP-based traffic with UDP-based traffic (especially Streaming-Video) within a single service-provider class because of the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters throttle back flows when drops are detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and, thus, never lower transmission rates because of dropping.

When TCP flows are combined with UDP flows within a single service-provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance.

TCP starvation/UDP dominance likely occurs if (TCP-based) Mission-Critical Data is assigned to the same service-provider class as (UDP-based) Streaming-Video and the class experiences sustained congestion.

Even if WRED is enabled on the service-provider class, the same behavior would be observed because WRED (for the most part) manages congestion only on TCP-based flows.

Reference:

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 11

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSSRND-Book/VPNQoS.html

QUESTION 7

Prior to enabling PPPoE in a virtual private dialup network group, which task must be completed?

- A. Disable CDP on the interface
- B. Execute the vpdn enable command.
- C. Execute the no switchport command.
- D. Enable QoS FIFO for PPPoE support.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Enabling PPPoE in a VPDN Group

Perform this task to enable PPPoE in a virtual private dial-up network (VPDN) group.

Restrictions

This task applies only to releases prior to Cisco IOS Release 12.2(13)T.

SUMMARY STEPS

1.
enable
2.
configure terminal
3.
vpdn enable
4.
vpdn-group name
5.
request-dialin
6.
protocol pppoe

DETAILED STEPS

Command or Action

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 12

Example:

Router> enable

Enables privileged EXEC mode.

•

Enter your password if prompted.

Step 2

configure terminal

Example:

Router# configure terminal

Enters global configuration mode.

Step 3

vpdn enable

Example:

Router(config)# vpdn enable

Enables virtual private dialup networking.

Step 4

vpdn-group name

Example:

```
Router(config)# vpdn-group group1
```

Associates a VPDN group with a customer or VPDN profile.

Step 5

request-dialin

Example:

```
Router(config-vpdn)# request-dialin
```

Creates a request-dialin VPDN subgroup.

Step 6

protocol pppoe

Example:

```
Router(config-vpdn-req-in)# protocol pppoe
```

Enables the VPDN subgroup to establish PPPoE

Reference:

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftpppoe_support_TSD_Island_of_Content_Chapter.html

QUESTION 8

A network engineer has been asked to ensure that the PPPoE connection is established and authenticated using an encrypted password. Which technology, in combination with PPPoE, can be used for authentication in this manner?

- A. PAP
- B. dot1x
- C. Ipsec
- D. CHAP
- E. ESP



Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

With PPPoE, the two authentication options are PAP and CHAP. When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router. When the remote device receives the challenge packet, it concatenates the ID, the remote device’s password, and the random number, and then encrypts all of it using the remote device’s password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process.

When the access server receives the response, it uses the name it received to retrieve a

password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password—if the result matches the result sent in the response packet, authentication succeeds.

The benefit of using CHAP authentication is that the remote device's password is never transmitted in clear text (encrypted). This prevents other devices from stealing it and gaining illegal access to the ISP's network.

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html

QUESTION 9

A corporate policy requires PPPoE to be enabled and to maintain a connection with the ISP, even if no interesting traffic exists. Which feature can be used to accomplish this task?

- A. TCP Adjust
- B. Dialer Persistent
- C. PPPoE Groups
- D. half-bridging
- E. Peer Neighbor Route

Correct Answer: B

Section: (none)

Explanation



Explanation/Reference:

A new interface configuration command, **dialer persistent**, allows a dial-on-demand routing (DDR) dialer profile connection to be brought up without being triggered by **interesting** traffic.

When configured, the **dialer persistent** command starts a timer when the dialer interface starts up and starts the connection when the timer expires. If interesting traffic arrives before the timer expires, the connection is still brought up and set as persistent. The command provides a default timer interval, or you can set a custom timer interval.

To configure a dialer interface as persistent, use the following commands beginning in global configuration mode:

Command

Purpose

Step 1

```
Router(config)# interface dialer number
```

Creates a dialer interface and enters interface configuration mode.

Step 2

```
Router(config-if)# ip address address mask
```

Specifies the IP address and mask of the dialer interface as a node in the destination network to be called.

Step 3

Router(config-if)# **encapsulation type**

Specifies the encapsulation type.

Step 4

Router(config-if)# **dialer string dial-string class class-name**

Specifies the remote destination to call and the map class that defines characteristics for calls to this destination.

Step 5

Router(config-if)# **dialer pool number**

Specifies the dialing pool to use for calls to this destination.

Step 6

Router(config-if)# **dialer-group group-number**

Assigns the dialer interface to a dialer group.

Step 7

Router(config-if)# **dialer-list dialer-group protocol protocol-name {permit | deny | list access-listnumber}**

Specifies an access list by list number or by protocol and list number to define the interesting packets that can trigger a call.

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 15

Step 8

Router(config-if)# **dialer remote-name user-name**

(Optional) Specifies the authentication name of the remote router on the destination subnetwork for a dialer interface.

Step 9

Router(config-if)# dialer persistent [delay [initial] seconds | max-attempts number]

Forces a dialer interface to be connected at all times, even in the absence of interesting traffic.

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/dial/configuration/guide/12_4t/dia_12_4t_book/dia_dialer_persist.html

QUESTION 10

Which PPP authentication method sends authentication information in clear text?

- A. MS CHAP
- B. CDPCP
- C. CHAP
- D. PAP

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

PAP authentication involves a two-way handshake where the username and password are sent across the link in clear text; hence, PAP authentication does not provide any protection against playback and line sniffing.

CHAP authentication, on the other hand, periodically verifies the identity of the remote node using a three-way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calculated using a one-way hash function. The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

Reference: <http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10241-pppcallin-hostname.html>

QUESTION 11

Which protocol uses dynamic address mapping to request the next-hop protocol address for a specific connection?

- A. Frame Relay inverse ARP
- B. static DLCI mapping
- C. Frame Relay broadcast queue
- D. dynamic DLCI mapping



Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Dynamic address mapping uses Frame Relay Inverse ARP to request the next-hop protocol address for a specific connection, given its known DLCI. Responses to Inverse ARP requests are entered in an address-to-DLCI mapping table on the router or access server; the table is then used to supply the next-hop protocol address or the DLCI for outgoing traffic.

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/12_2/wan/configuration/guide/fwan_c/wcffrely.html

QUESTION 12

Which statement is true about the PPP Session Phase of PPPoE?

- A. PPP options are negotiated and authentication is not performed. Once the link setup is completed, PPPoE functions as a Layer 3 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.
- B. PPP options are not negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 4 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.
- C. PPP options are automatically enabled and authorization is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be encrypted over the PPP link within PPPoE headers.
- D. PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

PPPoE is composed of two main phases:

Reference: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpncli/vpn-pppoe.html>



QUESTION 13

PPPoE is composed of which two phases?

- A. Active Authentication Phase and PPP Session Phase
- B. Passive Discovery Phase and PPP Session Phase
- C. Active Authorization Phase and PPP Session Phase
- D. Active Discovery Phase and PPP Session Phase

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

PPPoE is composed of two main phases:

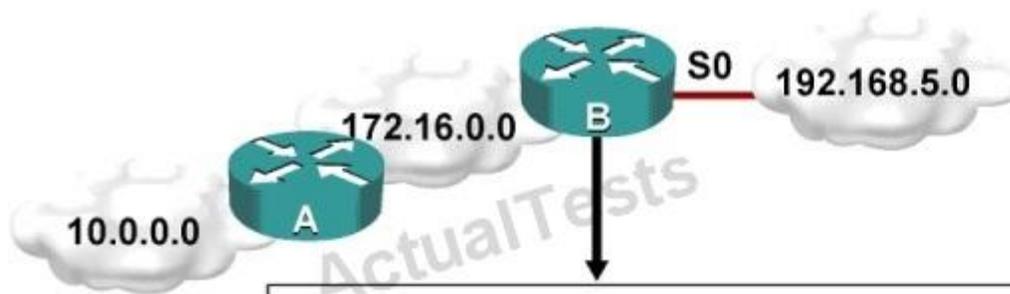
Reference: <http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpncli/vpn-pppoe.html>

QUESTION 14

Which one statement is true?

Exhibit:





```
router eigrp 1
 network 172.16.0.0
 network 192.168.5.0
 distribute-list 7 out s0
!
access-list 7 permit 172.16.0.0 0.0.255.255
```

- A. Traffic from the 172.16.0.0/16 network will be blocked by the ACL.
- B. The 10.0.0.0/8 network will not be advertised by Router B because the network statement for the 10.0.0.0/8 network is missing from Router B.
- C. The 10.0.0.0/8 network will not be in the routing table on Router B.
- D. Users on the 10.0.0.0/8 network can successfully ping users on the 192.168.5.0/24 network, but users on the 192.168.5.0/24 cannot successfully ping users on the 10.0.0.0/8 network.
- E. Router B will not advertise the 10.0.0.0/8 network because it is blocked by the ACL.

Correct Answer: E

Section: (none)

Explanation

Explanation/Reference:

You can filter what individual routes are sent (out) or received (in) to any interface within your EIGRP configuration.

One example is noted above. If you filter outbound, the next neighbor(s) will not know about anything except the 172.16.0.0/16 route and therefore won't send it to anyone else downstream. If you filter inbound, YOU won't know about the route and therefore won't send it to anyone else downstream.

QUESTION 15

A router with an interface that is configured with ipv6 address autoconfig also has a link-local address assigned. Which message is required to obtain a global unicast address when a router is present?

- A. DHCPv6 request
- B. router-advertisement
- C. neighbor-solicitation
- D. redirect

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Autoconfiguration is performed on multicast-enabled links only and begins when a multicast-enabled interface is enabled (during system startup or manually). Nodes (both, hosts and routers) begin the process by generating a link-local address for the interface. It is formed by appending the interface identifier to well-known link-local prefix **FE80::0**. The interface identifier replaces the right-most zeroes of the link-local prefix. Before the link-local address can be assigned to the

interface, the node performs the Duplicate Address Detection mechanism to see if any other node is using the same link-local address on the link. It does this by sending a Neighbor Solicitation message with target address as the "tentative" address and destination address as the solicitednode multicast address corresponding to this tentative address. If a node responds with a Neighbor Advertisement message with tentative address as the target address, the address is a duplicate address and must not be used. Hence, manual configuration is required.

Once the node verifies that its tentative address is unique on the link, it assigns that link-local address to the interface. At this stage, it has IP-connectivity to other neighbors on this link.

The autoconfiguration on the routers stop at this stage, further tasks are performed only by the hosts. The routers will need manual configuration (or stateful configuration) to receive site-local or global addresses.

The next phase involves obtaining Router Advertisements from routers if any routers are present on the link. If no routers are present, a stateful configuration is required. If routers are present, the Router Advertisements notify what sort of configurations the hosts need to do and the hosts receive a global unicast IPv6 address.

Reference: <https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ipv6-statelessautoconfiguration>

QUESTION 16

An engineer has configured a router to use EUI-64, and was asked to document the IPv6 address of the router. The router has the following interface parameters:

mac address C601.420F.0007
subnet 2001:DB8:0:1::/64



Which IPv6 addresses should the engineer add to the documentation?

- A. 2001:DB8:0:1:C601:42FF:FE0F:7
- B. 2001:DB8:0:1:FFFF:C601:420F:7
- C. 2001:DB8:0:1:FE80:C601:420F:7
- D. 2001:DB8:0:1:C601:42FE:800F:7

Correct Answer: A

Section: (none)

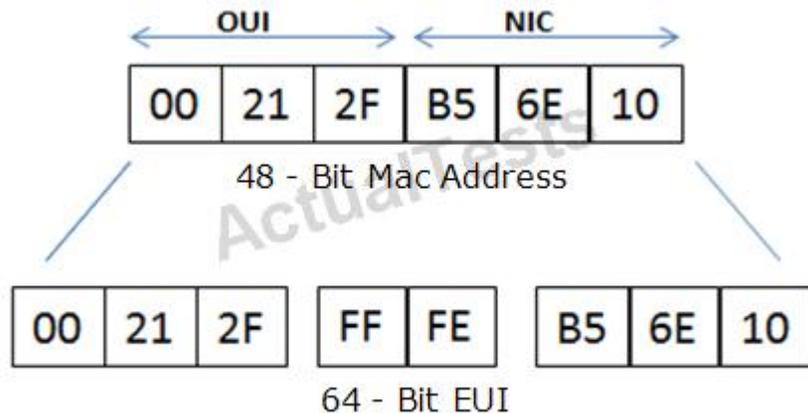
Explanation

Explanation/Reference:

Extended Unique Identifier (EUI), as per RFC2373, allows a host to assign itself a unique 64-Bit IP Version 6 interface identifier (EUI-64). This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4. The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits to form the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC

address.

Here is an example showing how the Mac Address is used to generate EUI0.



Next, the seventh bit from the left, or the universal/local (U/L) bit, needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered. If 0, the address is locally administered and if 1, the address is globally unique. It is worth noticing that in the OUI portion, the globally unique addresses assigned by the IEEE has always been set to 0 whereas the locally created addresses has 1 configured. Therefore, when the bit is inverted, it maintains its original scope (global unique address is still global unique and vice versa). The reason for inverting can be found in RFC4291 section 2.5.1.

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 21

Reference: <https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bitaddress>

QUESTION 17

For security purposes, an Ipv6 traffic filter was configured under various interfaces on the local router. However, shortly after implementing the traffic filter, OSPFv3 neighbor adjacencies were lost. What caused this issue?

- A. The traffic filter is blocking all ICMPv6 traffic.
- B. The global anycast address must be added to the traffic filter to allow OSPFv3 to work properly.
- C. The link-local addresses that were used by OSPFv3 were explicitly denied, which caused the neighbor relationships to fail.
- D. Ipv6 traffic filtering can be implemented only on SVIs.

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

OSPFv3 uses link-local Ipv6 addresses for neighbor discovery and other features, so if any Ipv6 traffic filters are implemented be sure to include the link local address so that it is permitted in the filter list.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/unicast/configuration/guide/l3_cli_nxos/l3_ospfv3.html

QUESTION 18

What is the purpose of the autonomous-system {autonomous-system-number} command?

- A. It sets the EIGRP autonomous system number in a VRF.
- B. It sets the BGP autonomous system number in a VRF.
- C. It sets the global EIGRP autonomous system number.
- D. It sets the global BGP autonomous system number.

Correct Answer: A

Section: (none)

Explanation



Explanation/Reference:

To configure the autonomous-system number for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process to run within a VPN routing and forwarding (VRF) instance, use the **autonomous-system** command in address-family configuration mode. To remove the autonomous-system for an EIGRP routing process from within a VPN VRF instance, use the **no** form of this command.

Autonomous-system autonomous-system-number
no autonomous-system autonomous-system-number

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/iproute_eigrp/command/reference/ire_book/ire_a1.html#wp1062796

QUESTION 19

What is the default OSPF hello interval on a Frame Relay point-to-point network?

- A. 10
- B. 20
- C. 30

D. 40

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

Before you troubleshoot any OSPF neighbor-related issues on an NBMA network, it is important to remember that an NBMA network can be configured in these modes of operation with the **ip ospf network** command:

The Hello and Dead Intervals of each mode are described in this table:

Network Type

Hello Interval (secs)

Dead Interval (secs)

Point-to-Point

10

40

Point-to-Multipoint

30

120

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 23

Broadcast

10

40

Non-Broadcast

30

120

Reference: <http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13693-22.html>

QUESTION 20

Exhibit: Which command only announces the 1.2.3.0/24 network out of FastEthernet 0/0?

Exhibit:

```
access-list 1 permit 1.0.0.0  
0.255.255.255  
access-list 2 permit 1.2.3.0  
0.0.0.255  
!  
router rip
```

- A. distribute list 1 out
- B. distribute list 1 out FastEthernet0/0
- C. distribute list 2 out
- D. distribute list 2 out FastEthernet0/0

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

Access list 2 is more specific, allowing only 1.2.3.0/24, whereas access list 1 permits all 1.0.0.0/8 networks. This question also asks us to apply this distribute list only to the outbound direction of the fast Ethernet 0/0 interface, so the correct command is "distribute list 2 out FastEthernet0/0."

QUESTION 21

Which prefix is matched by the command ip prefix-list name permit 10.8.0.0/16 ge 24 le 24?

- A. 10.9.1.0/24
- B. 10.8.0.0/24
- C. 10.8.0.0/16
- D. 10.8.0.0/23

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

With prefix lists, the ge 24 term means greater than or equal to a /24 and the le 24 means less than or equal to /24, so only a /24 is both greater than or equal to 24 and less than or equal to 24. This translates to any prefix in the 10.8.x.0/24 network, where X is any value in the 0-255 range. Only the choice of 10.8.0.0/24 matches this.

QUESTION 22

Router A and Router B are configured with IPv6 addressing and basic routing capabilities using OSPFv3. The networks that are advertised from Router A do not show up in Router B's routing table. After debugging IPv6 packets, the message "not a router" is found in the output. Why is the routing information not being learned by Router B?

- A. OSPFv3 timers were adjusted for fast convergence.
- B. The networks were not advertised properly under the OSPFv3 process.
- C. An IPv6 traffic filter is blocking the networks from being learned via the Router B interface that is connected to Router A.
- D. IPv6 unicast routing is not enabled on Router A or Router B.

Correct Answer: D

Section: (none)

Explanation

Explanation/Reference:

show ipv6 traffic Field Descriptions

Field

Description

source-routed

Number of source-routed packets.

truncated

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 25

Number of truncated packets.

format errors

Errors that can result from checks performed on header fields, the version number, and packet length.

not a router

Message sent when IPv6 unicast routing is not enabled.

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_16.html

QUESTION 23

After you review the output of the command show ipv6 interface brief, you see that several IPv6 addresses have the 16-bit hexadecimal value of "fffe" inserted into the address. Based on this information, what do you conclude about these IPv6 addresses?

- A. IEEE EUI-64 was implemented when assigning IPv6 addresses on the device.

- B. The addresses were misconfigured and will not function as intended.
- C. IPv6 addresses containing "FFFE" indicate that the address is reserved for multicast.
- D. The IPv6 universal/local flag (bit 7) was flipped.
- E. IPv6 unicast forwarding was enabled, but IPv6 Cisco Express Forwarding was disabled.

Correct Answer: A

Section: (none)

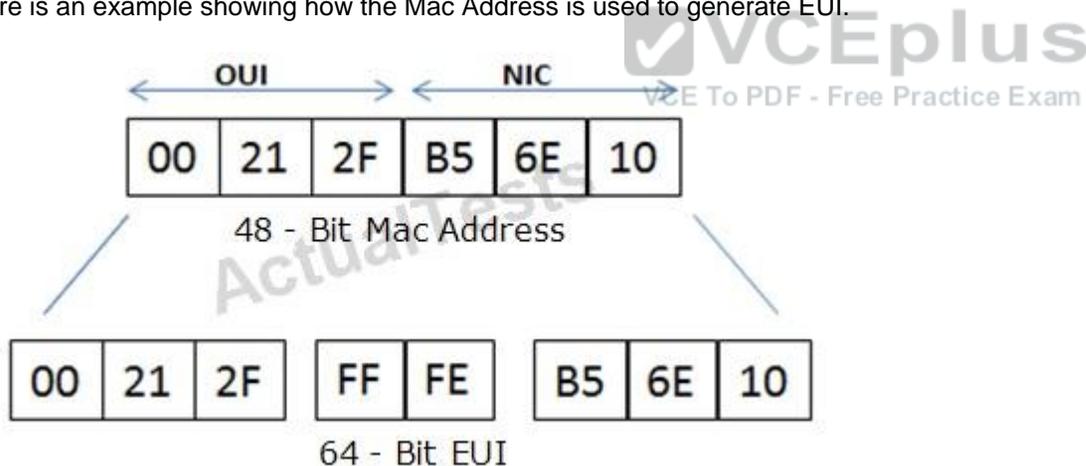
Explanation

Explanation/Reference:

Extended Unique Identifier (EUI), as per RFC2373, allows a host to assign itself a unique 64-Bit IP Version 6 interface identifier (EUI-64). This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4. The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific.

The 16-bit 0xFFFE is then inserted between these two 24-bits to form the 64-bit EUI address. **IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC address.**

Here is an example showing how the Mac Address is used to generate EUI.

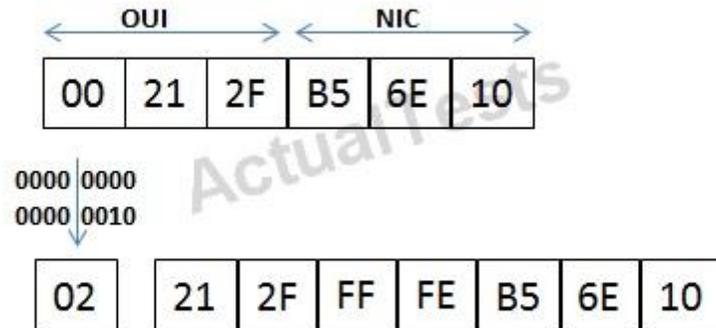


Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 26

Next, the seventh bit from the left, or the universal/local (U/L) bit, needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered. If 0, the address is locally administered and if 1, the address is globally unique. It is worth noticing that in the OUI portion, the globally unique addresses assigned by the IEEE have always been set to 0 whereas

the locally created addresses have 1 configured. Therefore, when the bit is inverted, it maintains its original scope (global unique address is still global unique and vice versa). The reason for inverting can be found in RFC4291 section 2.5.1.



Once the above is done, we have a fully functional EUI-64 address.
Reference: <https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bitaddress>

QUESTION 24

A packet capture log indicates that several router solicitation messages were sent from a local host on the Ipv6 segment. What is the expected acknowledgment and its usage?

- A. Router acknowledgment messages will be forwarded upstream, where the DHCP server will allocate addresses to the local host.
- B. Routers on the Ipv6 segment will respond with an advertisement that provides an external path from the local subnet, as well as certain data, such as prefix discovery.
- C. Duplicate Address Detection will determine if any other local host is using the same Ipv6 address for communication with the Ipv6 routers on the segment.
- D. All local host traffic will be redirected to the router with the lowest ICMPv6 signature, which is statically defined by the network administrator.

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

Router Advertisements (RA) are sent in response to router solicitation messages. Router

solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message. Given that router solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in router solicitation messages is usually the unspecified Ipv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When an RA is sent in response to a router solicitation, the destination address in the RA message is the unicast address of the source of the router solicitation message.

RA messages typically include the following information:

- One or more onlink Ipv6 prefixes that nodes on the local link can use to automatically configure their Ipv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the router should be used as a default router)
- Additional information for hosts, such as the hop limit and MTU a host should use in packets that it

Reference:

http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-addrg_bsc_con.html

QUESTION 25

A company has just opened two remote branch offices that need to be connected to the corporate network. Which interface configuration output can be applied to the corporate router to allow communication to the remote sites?

- A. interface Tunnel0
bandwidth 1536
ip address 209.165.200.230 255.255.255.224
tunnel source Serial0/0
tunnel mode gre multipoint
- B. interface fa0/0
bandwidth 1536
ip address 209.165.200.230 255.255.255.224

- ```
tunnel mode gre multipoint
```
- C. interface Tunnel0  
bandwidth 1536  
ip address 209.165.200.231 255.255.255.224  
tunnel source 209.165.201.1  
tunnel-mode dynamic
- D. interface fa 0/0  
bandwidth 1536  
ip address 209.165.200.231 255.255.255.224  
tunnel source 192.168.161.2  
tunnel destination 209.165.201.1  
tunnel-mode dynamic

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The configuration of mGRE allows a tunnel to have multiple destinations. The configuration of mGRE on one side of a tunnel does not have any relation to the tunnel properties that might exist at the exit points. This means that an mGRE tunnel on the hub may connect to a p2p tunnel on the branch. Conversely, a p2p GRE tunnel may connect to an mGRE tunnel. The distinguishing feature between an mGRE interface and a p2p GRE interface is the tunnel destination. An mGRE interface does not have a configured destination. Instead the GRE tunnel is configured with the command **tunnel mode gre multipoint**. This command is used instead of the **tunnel destination** x.x.x.x found with p2p GRE tunnels. Besides allowing for multiple destinations, an mGRE tunnel requires NHRP to resolve the tunnel endpoints. Note, tunnel interfaces by default are point-to-

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 91

point (p-p) using GRE encapsulation, effectively they have the **tunnel mode gre** command, which is not seen in the configuration because it is the default.

The mGRE configuration is as follows:

```
!
interface Tunnel0
bandwidth 1536
ip address 10.62.1.10 255.255.255.0
tunnel source Serial0/0
tunnel mode gre multipoint
```

Reference:

[http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN\\_and\\_MAN/DMVPDG/DMVPN\\_2\\_Phase2.html](http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG/DMVPN_2_Phase2.html)

**QUESTION 26**

A network engineer executes the show crypto ipsec sa command. Which three pieces of information are displayed in the output? (Choose three.)

- A. inbound crypto map
- B. remaining key lifetime
- C. path MTU
- D. tagged packets
- E. untagged packets
- F. invalid identity packets

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**show crypto ipsec sa**

This command shows IPsec SAs built between peers. The encrypted tunnel is built between 12.1.1.1 and 12.1.1.2 for traffic that goes between networks 20.1.1.0 and 10.1.1.0. You can see the two Encapsulating Security Payload (ESP) SAs built inbound and outbound. Authentication Header (AH) is not used since there are no AH SAs.

This output shows an example of the show crypto ipsec sa command (bolded ones found in answers for this question).

interface: FastEthernet0

**Crypto map tag: test, local addr. 12.1.1.1**

local ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)

remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)

current\_peer: 12.1.1.2

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 92

PERMIT, flags={origin\_is\_acl,}

#pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918

#pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0,

#pkts decompress failed: 0, #send errors 1, #Recv errors 0

local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2

**path mtu 1500, media mtu 1500**

current outbound spi: 3D3

inbound esp sas:

spi: 0x136A010F(325714191)

transform: esp-3des esp-md5-hmac ,  
in use settings ={Tunnel, }  
slot: 0, conn id: 3442, flow\_id: 1443, crypto map: test  
**sa timing: remaining key lifetime (k/sec): (4608000/52)**

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

inbound pcp sas:

outbound esp sas:

spi: 0x3D3(979)

transform: esp-3des esp-md5-hmac ,

in use settings ={Tunnel, }

slot: 0, conn id: 3443, flow\_id: 1444, crypto map: test

sa timing: remaining key lifetime (k/sec): (4608000/52)

IV size: 8 bytes

replay detection support: Y

outbound ah sas:

outbound pcp sas:

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ikeprotocols/5409-ipsec-debug-00.html>



#### QUESTION 27

Refer to the following output:

```
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
Type: Dynamic, Flags: authoritative unique nat registered used
NBMA address: 10.12.1.2
```

What does the authoritative flag mean in regards to the NHRP information?

- A. It was obtained directly from the next-hop server.
- B. Data packets are process switches for this mapping entry.
- C. NHRP mapping is for networks that are local to this router.
- D. The mapping entry was created in response to an NHRP registration request.
- E. The NHRP mapping entry cannot be overwritten.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## Show NHRP: Examples

The following is sample output from the **show ip nhrp** command:

```
Router# show ip nhrp
10.0.0.2 255.255.255.255, tunnel 100 created 0:00:43 expire 1:59:16
Type: dynamic Flags: authoritative
NBMA address: 10.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
Type: static Flags: authoritative
NBMA address: 10.1.1.2
```

The fields in the sample display are as follows:

- The IP address and its network mask in the IP-to-NBMA address cache. The mask is always 255.255.255.255 because Cisco does not support aggregation of NBMA information through NHRP.

- The interface type and number and how long ago it was created (hours:minutes:seconds).

- The time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ip nhrp holdtime** command.

- Type of interface:

- dynamic—NBMA address was obtained from the NHRP Request packet.  Free Practice Exam
- static—NBMA address was statically configured.

**authoritative**—Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination.

Reference:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_4/ip\\_addr/configuration/guide/hadnhrp.html](http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html)

### QUESTION 28

Which common issue causes intermittent DMVPN tunnel flaps?

- A. a routing neighbor reachability issue
- B. a suboptimal routing table
- C. interface bandwidth congestion
- D. that the GRE tunnel to hub router is not encrypted

**Correct Answer:** A

**Section:** (none)

## Explanation

### Explanation/Reference:

## DMVPN Tunnel Flaps Intermittently

### Problem

DMVPN tunnel flaps intermittently.

### Solution

When DMVPN tunnels flap, check the neighborship between the routers as issues with neighborship formation between routers may cause the DMVPN tunnel to flap. In order to resolve this problem, make sure the neighborship between the routers is always up.

Reference: <http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ikeprotocols/29240-dcmvpn.html#Prblm1>

## QUESTION 29

Which encapsulation supports an interface that is configured for an EVN trunk?

- A. 802.1Q
- B. ISL
- C. PPP
- D. Frame Relay
- E. MPLS
- F. HDLC



**Correct Answer:** A

**Section:** (none)

### Explanation

### Explanation/Reference:

## Restrictions for EVN

• **An EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.**

- A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end.
- If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.
- OSPFv3 is not supported; OSPFv2 is supported.

Reference: <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3sbook/evn-overview.pdf>

## QUESTION 30

Which three characteristics are shared by subinterfaces and associated EVNs? (Choose three.)

- A. IP address
- B. routing table
- C. forwarding table
- D. access control lists
- E. NetFlow configuration

**Correct Answer:** ABC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Trunk interface can carry traffic for multiple EVNs. To simplify the configuration process, all the subinterfaces and associated EVNs have the same IP address assigned. In other words, the trunk interface is identified by the same IP address in different EVN contexts. This is accomplished as a result of each EVN having a unique routing and forwarding table, thereby enabling support for overlapping IP addresses across multiple EVNs.

Reference: <http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/xr-3sg/evnoverview.pdf>

### QUESTION 31

A user is having issues accessing file shares on a network. The network engineer advises the user to open a web browser, input a prescribed IP address, and follow the instructions. After doing this, the user is able to access company shares. Which type of remote access did the engineer enable?

- A. EZVPN
- B. Ipsec VPN client access
- C. VPDN client access
- D. SSL VPN client access

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.

After entering the URL, the browser connects to that interface and displays the login screen. If the

user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.  
Reference: <http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-nextgeneration-firewalls/100936-asa8x-split-tunnel-anyconnect-config.html>

### QUESTION 32

Which Cisco IOS VPN technology leverages Ipsec, mGRE, dynamic routing protocol, NHRP, and Cisco Express Forwarding?

- A. FlexVPN
- B. DMVPN
- C. GETVPN
- D. Cisco Easy VPN

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Dynamic Multipoint Virtual Private Network (DMVPN)** is a dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers and Unix-like Operating Systems based on the standard protocols, GRE, NHRP and Ipsec. This DMVPN provides the capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible tunnel end-point peers, including Ipsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol) peers. DMVPN is initially configured to build out a hub-and-spoke network by statically configuring the hubs (VPN headends) on the spokes, no change in the configuration on the hub is required to accept new spokes. Using this initial hub-and-spoke network, tunnels between spokes can be dynamically built on demand (dynamic-mesh) without additional configuration on the hubs or spokes. This dynamic-mesh capability alleviates the need for any load on the hub to route data between the spoke networks.

DMVPN is combination of the following technologies:

Reference: [http://en.wikipedia.org/wiki/Dynamic\\_Multipoint\\_Virtual\\_Private\\_Network](http://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network)

### QUESTION 33

Which traffic does the following configuration allow?

```
Ipv6 access-list cisco
permit ipv6 host 2001:DB8:0:4::32 any eq ssh
line vty 0 4
```

ipv6 access-class cisco in

- A. all traffic to vty 0 4 from source 2001:DB8:0:4::32
- B. only ssh traffic to vty 0 4 from source all
- C. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32
- D. all traffic to vty 0 4 from source all

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Here we see that the Ipv6 access list called “cisco” is being applied to incoming VTY connections to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of 2001:DB8:0:4::32 to connect using SSH only.

#### QUESTION 34

For troubleshooting purposes, which method can you use in combination with the “debug ip packet” command to limit the amount of output data?

- A. You can disable the IP route cache globally.
- B. You can use the KRON scheduler.
- C. You can use an extended access list.
- D. You can use an IOS parser.
- E. You can use the RITE traffic exporter.



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The “debug ip packet” command generates a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks.

Always use with the access-list command to apply an extended ACL to the debug output.

Reference: <http://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpndmvpn/111976-dmvpn-troubleshoot-00.html>

#### QUESTION 35

Refer to the following access list.

Access-list 100 permit ip any any log

After applying the access list on a Cisco router, the network engineer notices that the router CPU utilization has risen to 99 percent. What is the reason for this?

- A. A packet that matches access-list with the "log" keyword is Cisco Express Forwarding switched.
- B. A packet that matches access-list with the "log" keyword is fast switched.
- C. A packet that matches access-list with the "log" keyword is process switched.
- D. A large amount of IP traffic is being permitted on the router.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Logging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices. Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions of the network device. There are two primary factors that contribute to the CPU load increase from ACL logging: process switching of packets that match log-enabled access control entries (ACEs) and the generation and transmission of log messages.

Reference: <http://www.cisco.com/web/about/security/intelligence/acl-logging.html#4>

### QUESTION 36

Which address is used by the Unicast Reverse Path Forwarding protocol to validate a packet against the routing table?

- A. source address
- B. destination address
- C. router interface
- D. default gateway

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects

such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

Reference: [http://www.cisco.com/en/US/docs/ios/12\\_2/security/configuration/guide/scfrpf.html](http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html)

### QUESTION 37

What are the three modes of Unicast Reverse Path Forwarding?

- A. strict mode, loose mode, and VRF mode
- B. strict mode, loose mode, and broadcast mode
- C. strict mode, broadcast mode, and VRF mode
- D. broadcast mode, loose mode, and VRF mode

**Correct Answer:** A

**Section:** (none)

**Explanation**

#### **Explanation/Reference:**

Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded.

**Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode.** Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode will not be covered in this document.

When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the **allow-default** option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.

Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.

Reference: <http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html>

**QUESTION 38**

What does the following access list, which is applied on the external interface FastEthernet 1/0 of the perimeter router, accomplish?

```
Router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
router (config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
router (config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
router (config)#access-list 101 permit ip any any
router (config)#interface fastEthernet 1/0
router (config-if)#ip access-group 101 in
```

- A. It prevents incoming traffic from IP address ranges 10.0.0.0-10.0.0.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 and logs any intrusion attempts.
- B. It prevents the internal network from being used in spoofed denial of service attacks and logs any exit to the Internet.
- C. It filters incoming traffic from private addresses in order to prevent spoofing and logs any intrusion attempts.
- D. It prevents private internal addresses to be accessed directly from outside.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The private IP address ranges defined in RFC 1918 are as follows:

10.0.0.0 — 10.255.255.255

172.16.0.0 — 172.31.255.255

192.168.0.0 — 192.168.255.255

These IP addresses should never be allowed from external networks into a corporate network as they would only be able to reach the network from the outside via routing problems or if the IP addresses were spoofed. This ACL is used to prevent all packets with a spoofed reserved private source IP address to enter the network. The log keyword also enables logging of this intrusion attempt.

**QUESTION 39**

Refer to the following command:

```
router(config)# ip http secure-port 4433
```

Which statement is true?

- A. The router will listen on port 4433 for HTTPS traffic.

- B. The router will listen on port 4433 for HTTP traffic.
- C. The router will never accept any HTTP and HTTPS traffic.
- D. The router will listen to HTTP and HTTPS traffic on port 4433.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

To set the secure HTTP (HTTPS) server port number for listening, use the ip http secure-port command in global configuration mode. To return the HTTPS server port number to the default, use the no form of this command.

**Ip http secure-port port-number**

**no ip http secure-port**

**Syntax Description**

port-number

Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.

Reference: <http://www.cisco.com/en/US/docs/ios-xml/ios/https/command/nm-https-cr-clsh.html#wp3612805529>



**QUESTION 40**

A network engineer is configuring a routed interface to forward broadcasts of UDP 69, 53, and 49 to 172.20.14.225. Which command should be applied to the configuration to allow this?

- A. router(config-if)#ip helper-address 172.20.14.225
- B. router(config-if)#udp helper-address 172.20.14.225
- C. router(config-if)#ip udp helper-address 172.20.14.225
- D. router(config-if)#ip helper-address 172.20.14.225 69 53 49

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

To let a router forward broadcast packet the command ip helper-address can be used. The broadcasts will be forwarded to the unicast address which is specified with the ip helper command.

ip helper-address {ip address}

When configuring the ip helper-address command, the following broadcast packets will be forwarded by the router by default:

- TFTP — UDP port 69

- Domain Name System (DNS) – UDP port 53
- Time service — port 37
- NetBIOS Name Server — port 137
- NetBIOS Datagram Server — port 138
- Bootstrap Protocol (BOOTP) — port 67
- TACACS – UDP port 49

Reference: [http://www.cisco-faq.com/163/forward\\_udp\\_broadcas.html](http://www.cisco-faq.com/163/forward_udp_broadcas.html)

#### QUESTION 41

A network engineer is configuring SNMP on network devices to utilize one-way SNMP notifications. However, the engineer is not concerned with authentication or encryption. Which command satisfies the requirements of this scenario?

- A. `router(config)#snmp-server host 172.16.201.28 traps version 2c CISCORO`
- B. `router(config)#snmp-server host 172.16.201.28 informs version 2c CISCORO`
- C. `router(config)#snmp-server host 172.16.201.28 traps version 3 auth CISCORO`
- D. `router(config)#snmp-server host 172.16.201.28 informs version 3 auth CISCORO`

**Correct Answer:** A

**Section:** (none)

**Explanation**



#### Explanation/Reference:

Most network admins and engineers are familiar with SNMPv2c which has become the dominant SNMP version of the past decade. It's simple to configure on both the router/switch-side and just as easy on the network monitoring server. The problem of course is that the SNMP statistical payload is not encrypted and authentication is passed in cleartext. Most companies have decided that the information being transmitted isn't valuable enough to be worth the extra effort in upgrading to SNMPv3, but I would suggest otherwise.

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 104

Like IPv4 to Ipv6, there are some major changes under the hood. SNMP version 2 uses community strings (think cleartext passwords, no encryption) to authenticate polling and trap delivery. SNMP version 3 moves away from the community string approach in favor of user-based authentication and view-based access control. The users are not actual local user accounts, rather they are simply a means to determine who can authenticate to the device. The view is used to define what the user account may access on the IOS device. Finally, each user is added to a group, which determines the access policy for its users. Users, groups, views.

Reference: <http://www.cnpguide.com/snmp-version-3/>

#### QUESTION 42

When using SNMPv3 with NoAuthNoPriv, which string is matched for authentication?

- A. username
- B. password
- C. community-string
- D. encryption-key

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The following security models exist: SNMPv1, SNMPv2, SNMPv3. The following security levels exist: “noAuthNoPriv” (no authentication and no encryption – noauth keyword in CLI), “AuthNoPriv” (messages are authenticated but not encrypted – auth keyword in CLI), “AuthPriv” (messages are authenticated and encrypted – priv keyword in CLI). SNMPv1 and SNMPv2 models only support the “noAuthNoPriv” model since they use plain community string to match the incoming packets. The SNMPv3 implementations could be configured to use either of the models on per-group basis **(in case if “noAuthNoPriv” is configured, username serves as a replacement for community string)**.

Reference: <http://blog.ine.com/2008/07/19/snmpv3-tutorial/>

**QUESTION 43**

After a recent DoS attack on a network, senior management asks you to implement better logging functionality on all IOS-based devices. Which two actions can you take to provide enhanced logging results? (Choose two.)

- A. Use the msec option to enable service time stamps.
- B. Increase the logging history
- C. Set the logging severity level to 1.
- D. Specify a logging rate limit.
- E. Disable event logging on all noncritical items

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The optional **msec** keyword specifies the date/time format should include milliseconds. This can aid in pinpointing the exact time of events, or to correlate the order that the events happened. To limit syslog messages sent to the router’s history table and to an SNMP network management station based on severity, use the logging history command in global configuration mode. By

default, Cisco devices Log error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher." By increasing the severity level, more granular monitoring can occur, and SNMP messages will be sent by the less severe (5-7) messages.

#### QUESTION 44

A network engineer finds that a core router has crashed without warning. In this situation, which feature can the engineer use to create a crash collection?

- A. secure copy protocol
- B. core dumps
- C. warm reloads
- D. SNMP
- E. NetFlow

**Correct Answer:** B

**Section:** (none)

**Explanation**

#### Explanation/Reference:

When a router crashes, it is sometimes useful to obtain a full copy of the memory image (called a **core dump**) to identify the cause of the crash. Core dumps are generally very useful to your technical support representative.

Four basic ways exist for setting up the router to generate a core dump:

- Using Trivial File Transfer Protocol (TFTP)
- Cisco 300-101 Exam  
"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 106  
Using File Transfer Protocol (FTP)

- Using remote copy protocol (rcp)

- Using a Flash disk

Reference: <http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr19aa.html>

#### QUESTION 45

A network engineer is trying to implement broadcast-based NTP in a network and executes the ntp broadcast client command. Assuming that an NTP server is already set up, what is the result of the command?

- A. It enables receiving NTP broadcasts on the interface where the command was executed.

- B. It enables receiving NTP broadcasts on all interfaces globally.
- C. It enables a device to be an NTP peer to another device.
- D. It enables a device to receive NTP broadcast and unicast packets.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The NTP service can be activated by entering any ntp command. When you use the ntp broadcast client command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.

**Command**

**Description**

ntp broadcast client

Allows the system to receive NTP broadcast packets on an interface.

Reference: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-xe-3se-3850-crbook/bsm-xe-3se-3850-cr-book\\_chapter\\_00.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-xe-3se-3850-crbook/bsm-xe-3se-3850-cr-book_chapter_00.html)

**QUESTION 46**

What is a function of NPTv6?



- A. It interferes with encryption of the full IP payload.
- B. It maintains a per-node state.
- C. It is checksum-neutral.
- D. It rewrites transport layer headers.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

RFC 6296 describes a stateless Ipv6-to-Ipv6 Network Prefix Translation (NPTv6) function, designed to provide address independence to the edge network. It is transport-agnostic with respect to transports that do not checksum the IP header, such as SCTP, and to transports that use the TCP/UDP/DCCP (Datagram Congestion Control Protocol) pseudo-header and checksum. NPTv6 provides a simple and compelling solution to meet the address-independence requirement in Ipv6. The address-independence benefit stems directly from the translation function of the network prefix translator. To avoid as many of the issues associated with NAT44 as possible,

**NPTv6 is defined to include a two-way, checksum-neutral**, algorithmic translation function, and

nothing else.

Reference: <http://tools.ietf.org/html/rfc6296>

#### QUESTION 47

Ipv6 has just been deployed to all of the hosts within a network, but not to the servers. Which feature allows Ipv6 devices to communicate with Ipv4 servers?

- A. NAT
- B. NATng
- C. NAT64
- D. dual-stack NAT
- E. DNS64

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**NAT64** is a mechanism to allow Ipv6 hosts to communicate with Ipv4 servers. The NAT64 server is the endpoint for at least one Ipv4 address and an Ipv6 network segment of 32-bits (for instance 64:ff9b::/96, see RFC 6052, RFC 6146). The Ipv6 client embeds the Ipv4 address it wishes to communicate with using these bits, and sends its packets to the resulting address. The NAT64 server then creates a NAT-mapping between the Ipv6 and the Ipv4 address, allowing them to communicate.

Reference: <http://en.wikipedia.org/wiki/NAT64>

#### QUESTION 48

A network engineer initiates the ip sla responder tcp-connect command in order to gather statistics for performance gauging. Which type of statistics does the engineer see?

- A. connectionless-oriented
- B. service-oriented
- C. connection-oriented
- D. application-oriented

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

## Configuration Examples for IP SLAs TCP Connect Operations

The following example shows how to configure a TCP Connection-oriented operation from Device B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1), as shown in the “TCP Connect Operation” figure in the “Information About the IP SLAs TCP Connect Operation” section. The operation is scheduled to start immediately. In this example, the control protocol is disabled on the source (Device B). IP SLAs uses the control protocol to notify the IP SLAs responder to enable the target port temporarily. This action allows the responder to reply to the TCP Connect operation. In this example, because the target is not a Cisco device and a well-known TCP port is used, there is no need to send the control message.

### Device A (target device) Configuration

configure terminal

```
ip sla responder tcp-connect ipaddress 10.0.0.1 port 23
```

Reference: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mtbook/sla\\_tcp\\_conn.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mtbook/sla_tcp_conn.html)

### QUESTION 49

A network engineer executes the “ipv6 flowset” command. What is the result?

- A. Flow-label marking in 1280-byte or larger packets is enabled.
- B. Flow-set marking in 1280-byte or larger packets is enabled.
- C. Ipv6 PMTU is enabled on the router.
- D. Ipv6 flow control is enabled on the router.



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### Enabling Flow-Label Marking in Packets that Originate from the Device

This feature allows the device to track destinations to which the device has sent packets that are 1280 bytes or larger.

#### SUMMARY STEPS

1. enable
2. configure terminal
3. ipv6 flowset
4. exit
5. clear ipv6 mtu

#### DETAILED STEPS

##### Command or Action

##### Purpose

**Step 1**

enable

**Example:**

Device> enable

Enables privileged EXEC mode.

**Step 2**

configure terminal

**Example:**

Device# configure terminal

Enters global configuration mode.

**Step 3**

ipv6 flowset

**Example:**

Device(config)# ipv6 flowset

**Configures flow-label marking in 1280-byte or larger packets sent by the device.**

Reference: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6\\_basic/configuration/15-mt/ip6b-15-mt-book/ip6-mtu-path-disc.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-mt/ip6b-15-mt-book/ip6-mtu-path-disc.html)

**QUESTION 50**

A network engineer executes the show ip flow export command. Which line in the output indicates that the send queue is full and export packets are not being sent?

- A. output drops
- B. enqueueing for the RP
- C. fragmentation failures
- D. adjacency issues

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Field**

**Description**

Exporting flows to 10.1.1.1 (1000) and 10.2.1.1

Specifies the export destinations and ports. The ports are in parentheses.

Exporting using source IP address 10.3.1.1

Specifies the source address or interface.

Version 5 flow records

Specifies the version of the flow.

11 flows exported in 8 udp datagrams

The total number of export packets sent, and the total number of flows contained within them.

0 flows failed due to lack of export packet

No memory was available to create an export packet.

0 export packets were sent up to process level

The packet could not be processed by CEF or by fast switching, possibly because another feature requires running on the packet.

0 export packets were dropped due to no fib

0 export packets were dropped due to adjacency issues

Indicates that CEF was unable to switch the packet or forward it up to the process level.

0 export packets were dropped due to fragmentation failures

0 export packets were dropped due to encapsulation fixup failures

Indicates that the packet was dropped because of problems constructing the IP packet.

0 export packets were dropped enqueueing for the RP

0 export packets were dropped due to IPC rate limiting

Indicates that there was a problem transferring the export packet between the RP and the line card.

**0 export packets were dropped due to output drops**

**Indicates that the send queue was full while the packet was being transmitted.**

Reference: [http://www.cisco.com/c/en/us/td/docs/ios/12\\_0s/feature/guide/oaggnf.html](http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/oaggnf.html)

#### QUESTION 51

A network engineer is asked to configure a "site-to-site" Ipsec VPN tunnel. One of the last things that the engineer does is to configure an access list (access-list 1 permit any) along with the command ip nat inside source list 1 int s0/0 overload. Which functions do the two commands serve in this scenario?

- A. The command access-list 1 defines interesting traffic that is allowed through the tunnel.
- B. The command ip nat inside source list 1 int s0/0 overload disables "many-to-one" access for all devices on a defined segment to share a single IP address upon exiting the external interface.
- C. The command access-list 1 permit any defines only one machine that is allowed through the tunnel.
- D. The command ip nat inside source list 1 int s0/0 overload provides "many-to-one" access for all devices on a defined segment to share a single IP address upon exiting the external interface.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Configuring NAT to Allow Internal Users to Access the Internet Using Overloading**

## NAT Router

```
interface 116thernet 0
ip address 10.10.10.1 255.255.255.0
```

Cisco 300-101 Exam

"Pass Any Exam. Any Time." - www.actualtests.com 112

```
ip nat inside
```

**!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.**

```
Interface 116thernet 1
ip address 10.10.20.1 255.255.255.0
```

```
ip nat inside
```

**!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.**

```
Interface serial 0
ip address 172.16.10.64 255.255.255.0
```

```
ip nat outside
```

**!--- Defines serial 0 with an IP address and as a NAT outside interface.**

```
Ip nat pool ovrlD 172.16.10.1 172.16.10.1 prefix 24
```

```
!
```

**!--- Defines a NAT pool named ovrlD with a range of a single IP**

**!--- address, 172.16.10.1.**

```
ip nat inside source list 7 pool ovrlD overload
```

```
!
```

```
!
```

```
!
```

**!--- Indicates that any packets received on the inside interface that**

**!--- are permitted by access-list 7 has the source address**

**!--- translated to an address out of the NAT pool named ovrlD.**

**!--- Translations are overloaded, which allows multiple inside**

**!--- devices to be translated to the same valid IP address.**

```
Access-list 7 permit 10.10.10.0 0.0.0.31
```

```
access-list 7 permit 10.10.20.0 0.0.0.31
```

**!--- Access-list 7 permits packets with source addresses ranging from**

**!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.**

Note in the previous second configuration, the NAT pool "ovrlD" only has a range of one address.

The keyword **overload** used in the **ip nat inside source list 7 pool ovrlD overload** command allows NAT to translate multiple inside devices to the single address in the pool.

Reference:

[http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080094e77.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml)

**QUESTION 52**

A network engineer is configuring a solution to allow failover of HSRP nodes during maintenance windows, as an alternative to powering down the active router and letting the network respond accordingly. Which action will allow for manual switching of HSRP nodes?

- A. Track the up/down state of a loopback interface and shut down this interface during maintenance.
- B. Adjust the HSRP priority without the use of preemption.
- C. Disable and enable all active interfaces on the active HSRP node.
- D. Enable HSRPv2 under global configuration, which allows for maintenance mode.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The **standby track** command allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if that router has **standby preempt** enabled. Loopback interfaces can be tracked, so when this interface is shut down the HSRP priority for that router will be lowered and the other HSRP router will then become the active one. Reference: <http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html>

**QUESTION 53**

A network engineer is notified that several employees are experiencing network performance related issues, and bandwidth-intensive applications are identified as the root cause. In order to identify which specific type of traffic is causing this slowness, information such as the source/destination IP and Layer 4 port numbers is required. Which feature should the engineer use to gather the required information?

- A. SNMP
- B. Cisco IOS EEM
- C. NetFlow
- D. Syslog
- E. WCCP

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****NetFlow Flows Key Fields**

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

Reference: <http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-4t/cfg-nflowdata-expt.html>

**QUESTION 54**

An organization decides to implement NetFlow on its network to monitor the fluctuation of traffic that is disrupting core services. After reviewing the output of NetFlow, the network engineer is unable to see OUF traffic on the interfaces. What can you determine based on this information?

- A. Cisco Express Forwarding has not been configured globally.
- B. NetFlow output has been filtered by default.
- C. Flow Export version 9 is in use
- D. The command `ip flow-capture fragment-offset` has been enabled

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

We came across a recent issue where a user setup a router for NetFlow export but was unable to Cisco 300-101 Exam

"Pass Any Exam. Any Time." - [www.actualtests.com](http://www.actualtests.com) 115

see the OUF traffic for the interfaces in NetFlow Analyzer. Every NetFlow configuration aspect was checked and nothing incorrect was found. That is when we noticed the 'no ip cef' command on the router. CEF was enabled at the global level and within seconds, NetFlow Analyzer started showing OUF traffic for the interfaces. This is why this topic is about Cisco Express Forwarding.

**What is switching?**

A Router must make decisions about where to forward the packets passing through. This decisionmaking process is called "switching". Switching is what a router does when it makes the following decisions:

1. Whether to forward or not forward the packets after checking that the destination for the packet is reachable.
2. If the destination is reachable, what is the next hop of the router and which interface will the router use to get to that destination.

**What is CEF?**

CEF is one of the available switching options for Cisco routers. Based on the routing table, CEF

creates its own table, called the Forwarding Information Base (FIB). The FIB is organized differently than the routing table and CEF uses the FIB to decide which interface to send traffic from. CEF offers the following benefits:

1. Better performance than fast-switching (the default) and takes less CPU to perform the same task.
2. When enabled, allows for advanced features like NBAR
3. Overall, CEF can switch traffic faster than route-caching using fast-switching

### How to enable CEF?

CEF is disabled by default on all routers except the 7xxx series routers. Enabling and Disabling CEF is easy. To enable CEF, go into global configuration mode and enter the CEF command.

```
Router# config t
```

```
Router(config)# ip cef
```

```
Router(config)#
```

To disable CEF, simply use the 'no' form of the command, ie. '**no ip cef**'.

### Why CEF Needed when enabling NetFlow ?

CEF is a prerequisite to enable NetFlow on the router interfaces. CEF decides through which interface traffic is exiting the router. Any NetFlow analyzer product will calculate the OUT traffic for an interface based on the **Destination Interface** value present in the NetFlow packets exported from the router. If the CEF is disabled on the router, the NetFlow packets exported from the router will have "Destination interface" as "null" and this leads NetFlow Analyzer to show no OUT traffic for the interfaces. Without enabling the CEF on the router, the NetFlow packets did not mark the destination interfaces and so NetFlow Analyzer was not able to show the OUT traffic for the interfaces.

Reference: <https://blogs.manageengine.com/network-2/netflowanalyzer/2010/05/19/need-for-cefin-netflow-data-export.html>

### QUESTION 55

A network engineer has left a NetFlow capture enabled over the weekend to gather information regarding excessive bandwidth utilization. The following command is entered:

```
switch#show flow exporter Flow_Exporter-1
```

What is the expected output?

- A. configuration of the specified flow exporter
- B. current status of the specified flow exporter
- C. status and statistics of the specified flow monitor
- D. configuration of the specified flow monitor

**Correct Answer:** B

**Section:** (none)

## Explanation

### Explanation/Reference:

show flow exporter exporter-name

### Example:

Device# show flow exporter FLOW\_EXPORTER-1

(Optional) Displays the current status of the specified flow exporter

Reference: <http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-mt/cfg-defnflow-exprts.html>

## QUESTION 56

A company's corporate policy has been updated to require that stateless, 1-to-1, and Ipv6 to Ipv6 translations at the Internet edge are performed. What is the best solution to ensure compliance with this new policy?

- A. NAT64
- B. NAT44
- C. NATv6
- D. NPTv4
- E. NPTv6

**Correct Answer:** E

**Section:** (none)

### Explanation

### Explanation/Reference:

NPTv6 provides a mechanism to translate the private internal organization prefixes to public globally reachable addresses. The translation mechanism is stateless and provides a 1:1 relationship between the internal addresses and external addresses. The use cases for NPTv6 outlined in the RFC include peering with partner networks, multi homing, and redundancy and load sharing.

Reference:

[http://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/August2012/Cisco\\_SBA\\_BN\\_IPv6AddressingGuide-Aug2012.pdf](http://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/August2012/Cisco_SBA_BN_IPv6AddressingGuide-Aug2012.pdf)

## QUESTION 57

Which two functions are completely independent when implementing NAT64 over NAT-PT?

(Choose two.)

- A. DNS
- B. NAT

- C. port redirection
- D. stateless translation
- E. session handling

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Work Address Translation IPv6 to IPv4, or NAT64, technology facilitates communication between IPv6-only and IPv4-only hosts and networks (whether in a transit, an access, or an edge network). This solution allows both enterprises and ISPs to accelerate IPv6 adoption while simultaneously handling IPv4 address depletion. The DnS64 and NAT64 functions are completely separated, which is essential to the superiority of NAT64 over NAT-PT.

Reference: [http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white\\_paper\\_c11-676278.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html)

**QUESTION 58**

Which two methods of deployment can you use when implementing NAT64? (Choose two.)

- A. stateless
- B. stateful
- C. manual
- D. automatic
- E. static
- F. functional
- G. dynamic



**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

While stateful and stateless NAT64 perform the task of translating IPv4 packets into IPv6 packets and vice versa, there are important differences. The following table provides a high-level overview of the most relevant differences.

**Table 2.** Differences Between Stateless NAT64 and Stateful NAT64

**Stateless NAT64**

**Stateful NAT64**

1:1 translation

1:N translation  
No conservation of IPv4 address  
Conserves IPv4 address  
Assures end-to-end address transparency and scalability  
Uses address overloading, hence lacks in end-to-end address transparency  
No state or bindings created on the translation  
State or bindings are created on every unique translation  
Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)  
No requirement on the nature of IPv6 address assignment  
Requires either manual or DHCPv6 based address assignment for IPv6 hosts  
Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC  
Reference: [http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white\\_paper\\_c11-676277.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676277.html)

**QUESTION 59**

Which NetFlow component is applied to an interface and collects information about flows?

- A. flow monitor
- B. flow exporter
- C. flow sampler
- D. flow collector

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Flow monitors are the NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.

Reference:

[http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf\\_book/fnf\\_01.html#wp1314030](http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_01.html#wp1314030)

**QUESTION 60**

Refer to the exhibit

Sampler: mysampler, id : 1, packets matched : 10, mode : random sampling mode

Which statement about the output of the show flow-sampler command is true?

- A. The sampler matched 10 packets, each packet randomly chosen from every group of 100 packets.
- B. The sampler matched 10 packets, one packet every 100 packets
- C. The sampler matched 10 packets, each one randomly chosen from every 100-second interval
- D. The sampler matched 10 packets, one packet every 100 seconds.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The sampling mode determines the algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that Random Sampled NetFlow uses, incoming packets are randomly selected so that one out of each **n** sequential packets is selected **on average** for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th, 120th, 199th, 302nd, and so on packets. This sample configuration provides NetFlow data on 1 percent of total traffic. The **n** value is a parameter from 1 to 65535 packets that you can configure.

Table 2 show flow-sampler Field Descriptions

**Field**

**Description**

Sampler

Name of the flow sampler

id

Unique ID of the flow sampler

packets matched

Number of packets matched for the flow sampler

mode

Flow sampling mode

sampling interval is

Flow sampling interval (in packets)

Reference:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_0s/feature/guide/nfstatsa.html#wp1084291](http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/nfstatsa.html#wp1084291)



**QUESTION 61**

What is the result of the command ip flow-export destination 10.10.10.1 5858?

- A. It configures the router to export cache flow information to IP 10.10.10.1 on port UDP/5858.
- B. It configures the router to export cache flow information about flows with destination IP 10.10.10.1 and port UDP/5858.

- C. It configures the router to receive cache flow information from IP 10.10.10.1 on port UDP/5858.
- D. It configures the router to receive cache flow information about flows with destination IP 10.10.10.1 and port UDP/5858.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

To enable the exporting of information in NetFlow cache entries, use the **ip flow-export destination** command in global configuration mode.

**Syntax Description**

**ip-address**

IP address of the workstation to which you want to send the NetFlow information.

**Udp-port**

UDP protocol-specific port number.

Reference:

[http://www.cisco.com/c/en/us/td/docs/ios/12\\_0s/feature/guide/12s\\_mdnf.html#wp1023091](http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html#wp1023091)

**QUESTION 62**

Which type of traffic does DHCP snooping drop



- A. discover messages
- B. DHCP messages where the source MAC and client MAC do not match
- C. traffic from a trusted DHCP server to client
- D. DHCP messages where the destination MAC and client MAC do not match

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

The switch validates DHCP packets received on the untrusted interfaces of VLANs with DHCP snooping enabled. The switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

- 

The switch receives a packet (such as a DHCP OFFER, DHCP ACK, DHCP NAK, or DHCP LEASE QUERY packet) from a DHCP server outside the network or firewall.

- 

**The switch receives a packet on an untrusted interface, and the source MAC address and**

**the DHCP client hardware address do not match.** This check is performed only if the DHCP snooping MAC address verification option is turned on.

- The switch receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

- The switch receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0. To support trusted edge switches that are connected to untrusted aggregation-switch ports, you can enable the DHCP option-82 on untrusted port feature, which enables untrusted aggregationswitch ports to accept DHCP packets that include option-82 information. Configure the port on the edge switch that connects to the aggregation switch as a trusted port.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html>

### QUESTION 63

Which two commands would be used to troubleshoot high memory usage for a process? (Choose two.)

- A. router#show memory allocating-process table
- B. router#show memory summary
- C. router#show memory dead
- D. router#show memory events
- E. router#show memory processor statistics



**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 64

The following configuration is applied to a router at a branch site:

```
ipv6 dhcp pool dhcp-pool
dns-server 2001:DB8:1:B::1
dns-server 2001:DB8:3:307C::42
domain-name example.com
```

If IPv6 is configured with default settings on all interfaces on the router, which two dynamic IPv6 addressing mechanisms could you use on end hosts to provide end-to-end connectivity? (Choose

two.)

- A. EUI-64
- B. SLAAC
- C. DHCPv6
- D. BOOTP

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 65

The enterprise network WAN link has been receiving several denial of service attacks from both IPv4 and IPv6 sources. Which three elements can you use to identify an IPv6 packet via its header, in order to filter future attacks? (Choose three.)

- A. Traffic Class
- B. Source address
- C. Flow Label
- D. Hop Limit
- E. Destination Address
- F. Fragment Offset



**Correct Answer:** ACD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 66

A network engineer has set up VRF-Lite on two routers where all the interfaces are in the same VRF. At a later time, a new loopback is added to Router 1, but it cannot ping any of the existing interfaces. Which two configurations enable the local or remote router to ping the loopback from any existing interface? (Choose two.)

- A. adding a static route for the VRF that points to the global route table

- B. adding the loopback to the VRF
- C. adding dynamic routing between the two routers and advertising the loopback
- D. adding the IP address of the loopback to the export route targets for the VRF
- E. adding a static route for the VRF that points to the loopback interface
- F. adding all interfaces to the global and VRF routing tables

**Correct Answer:** AB

**Section:** (none)

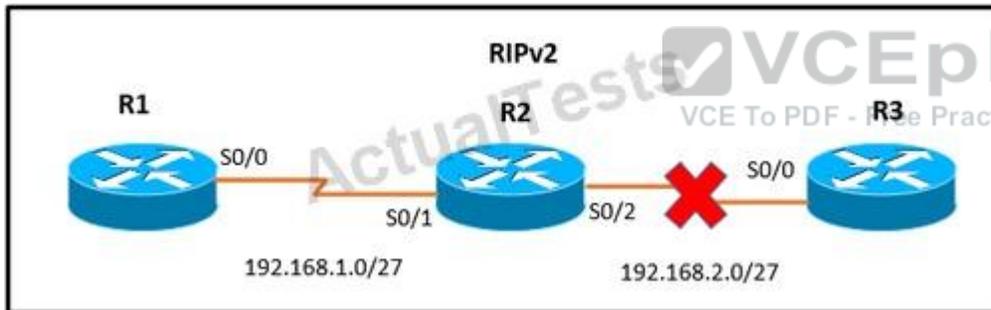
**Explanation**

**Explanation/Reference:**

**QUESTION 67**

Refer to the exhibit. The network setup is running the RIPv2 routing protocol. Which two events will occur following link failure between R2 and R3? (Choose two.)

**Exhibit:**



- A. R2 will advertise network 192.168.2.0/27 with a hop count of 16 to R1
- B. R2 will not send any advertisements and will remove route 192.168.2.0/27 from its routing table.
- C. R1 will reply to R2 with the advertisement for network 192.168.2.0/27 with a hop count of 16.
- D. After communication fails and after the hold-down timer expires, R1 will remove the 192.168.2.0/27 route from its routing table.
- E. R3 will not accept any further updates from R2, due to the split-horizon loop prevention mechanism.

**Correct Answer:** AC

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 68**

Which three benefits does the Cisco Easy Virtual Network provide to an enterprise network?  
(Choose three.)

- A. simplified Layer 3 network virtualization
- B. improved shared services support
- C. enhanced management, troubleshooting, and usability
- D. reduced configuration and deployment time for dot1q trunking
- E. increased network performance and throughput
- F. decreased BGP neighbor configurations

**Correct Answer:** ABC

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 69**

Which technology was originally developed for routers to handle fragmentation in the path between end points?

- A. PMTUD
- B. MSS
- C. windowing
- D. TCP
- E. global synchronization

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:**

**QUESTION 70**

Which traffic characteristic is the reason that UDP traffic that carries voice and video is assigned to the queue only on a link that is at least 768 kbps?

- A. typically is not fragmented
- B. typically is fragmented
- C. causes windowing
- D. causes excessive delays for video traffic

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 71**

A network administrator is troubleshooting a DMVPN setup between the hub and the spoke. Which action should the administrator take before troubleshooting the IPsec configuration?

- A. Verify the GRE tunnels.
- B. Verify ISAKMP.
- C. Verify NHRP.
- D. Verify crypto maps.



**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 72**

To configure SNMPv3 implementation, a network engineer is using the AuthNoPriv security level. What effect does this action have on the SNMP messages?

- A. They become unauthenticated and unencrypted.
- B. They become authenticated and unencrypted.
- C. They become authenticated and encrypted.
- D. They become unauthenticated and encrypted.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 73

A network engineer is investigating the cause of a service disruption on a network segment and executes the debug condition interface fastethernet f0/0 command. In which situation is the debugging output generated?

- A. when packets on the interface are received and the interface is operational
- B. when packets on the interface are received and logging buffered is enabled
- C. when packets on the interface are received and forwarded to a configured syslog server
- D. when packets on the interface are received and the interface is shut down

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**



### QUESTION 74

Refer to the exhibit. The command is executed while configuring a point-to-multipoint Frame Relay interface. Which type of IPv6 address is portrayed in the exhibit?

Exhibit:

```
frame-relay map ipv6 FE80::1C2 102
```

- A. link-local
- B. site-local
- C. global
- D. multicast

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 75**

An engineer executes the ip flow ingress command in interface configuration mode. What is the result of this action?

- A. It enables the collection of IP flow samples arriving to the interface.
- B. It enables the collection of IP flow samples leaving the interface.
- C. It enables IP flow while disabling IP CEF on the interface
- D. It enables IP flow collection on the physical interface and its subinterfaces

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 76**

What is the primary service that is provided when you implement Cisco Easy Virtual Network?

- A. It requires and enhances the use of VRF-Lite.
- B. It reduces the need for common services separation
- C. It allows for traffic separation and improved network efficiency
- D. It introduces multi-VRF and label-prone network segmentation

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 77**

How does an IOS router process a packet that should be switched by Cisco Express Forwarding without an FIB entry?

- A. by forwarding the packet
- B. by dropping the packet

- C. by creating a new FIB entry for the packet
- D. by looking in the routing table for an alternate FIB entry

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 78**

Which statement about dual stack is true?

- A. Dual stack translates IPv6 addresses to IPv4 addresses
- B. Dual stack means that devices are able to run IPv4 and IPv6 in parallel
- C. Dual stack translates IPv4 addresses to IPv6 addresses
- D. Dual stack changes the IP addresses on hosts from IPv4 to IPv6 automatically

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 79**

Which PPP authentication method sends authentication information in cleartext

- A. MS CHAP
- B. CDPCP
- C. CHAP
- D. PAP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 80**

A router receives a routing advertisement for the same prefix and subnet from four different routing protocols. Which advertisement is installed in the routing table?

- A. RIP
- B. OSPF
- C. iBGP
- D. EIGRP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 81**

Refer to the exhibit. When summarizing these routes, which route is the summarized route?

**Exhibit:**

```
OI 2001:DB8:0:7::/64 [110/20]
 via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI 2001:DB8:0:8::/64 [110/100]
 via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
OI 2001:DB8:0:9::/64 [110/20]
 via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
```



- A. OI 2001:DB8::/48 [110/100] via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
- B. OI 2001:DB8::/24 [110/100] via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
- C. OI 2001:DB8::/32 [110/100] via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0
- D. OI 2001:DB8::/64 [110/100] via FE80::A8BB:CCFF:FE00:6F00, Ethernet0/0

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 82**

Which type of BGP AS number is 64591?

- A. a private AS number
- B. a public AS number
- C. a private 4-byte AS number
- D. a public 4-byte AS number

**Correct Answer:** A

**Section:** (none)

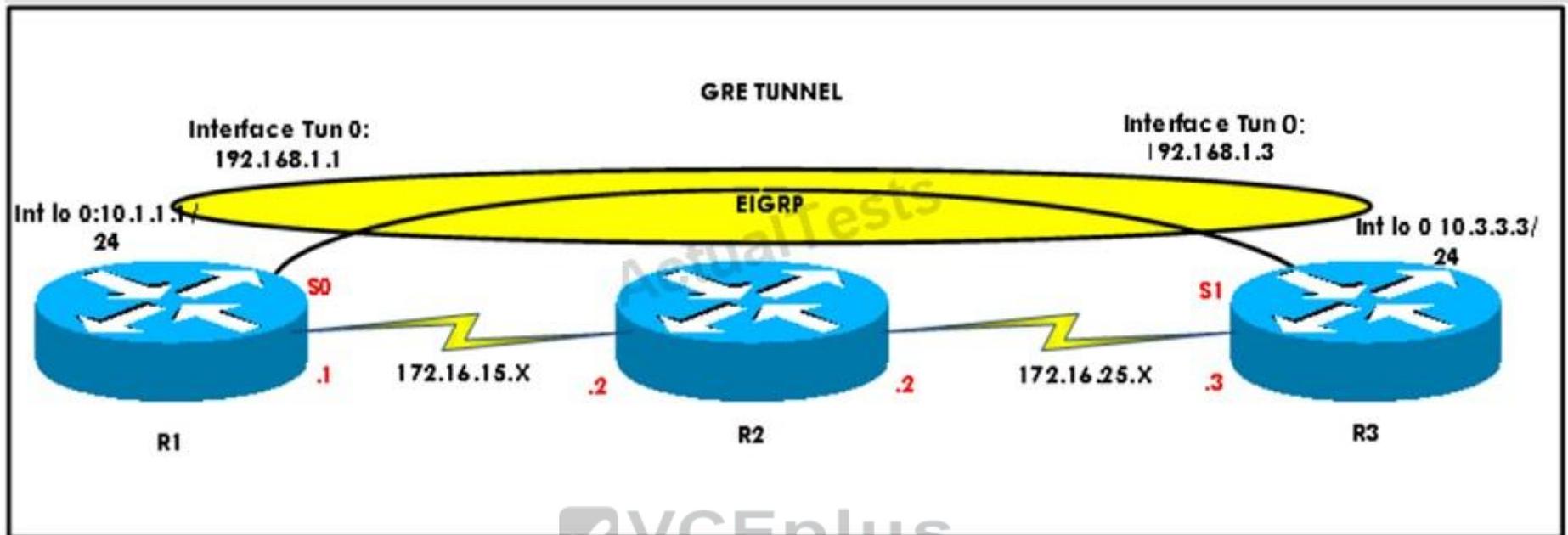
**Explanation**

**Explanation/Reference:**

**QUESTION 83**

Refer to the exhibit. After configuring GRE between two routers running OSPF that are connected to each other via a WAN link, a network engineer notices that the two routers cannot establish the GRE tunnel to begin the exchange of routing updates. What is the reason for this?

**Exhibit:**



- A. Either a firewall between the two routers or an ACL on the router is blocking IP protocol number 47.
- B. Either a firewall between the two routers or an ACL on the router is blocking UDP 57.
- C. Either a firewall between the two routers or an ACL on the router is blocking TCP 47.
- D. Either a firewall between the two routers or an ACL on the router is blocking IP protocol number 57.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 84

Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?

- A. DMVPN

- B. GETVPN
- C. Cisco Easy VPN
- D. FlexVPN

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 85**

Which Cisco VPN technology uses AAA to implement group policies and authorization and is also used for the XAUTH authentication method?

- A. DMVPN
- B. Cisco Easy VPN
- C. GETVPN
- D. GREVPN

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**



#### **QUESTION 86**

Two aspects of an IP SLA operation can be tracked: state and reachability. Which statement about state tracking is true?

- A. When tracking state, an OK return code means that the track's state is up; any other return code means that the track's state is down.
- B. When tracking state, an OK or over threshold return code means that the track's state is up; any other return code means that the track's state is down.
- C. When tracking state, an OK return code means that the track's state is down; any other return code means that the track's state is up.
- D. When tracking state, an OK or over threshold return code means that the track's state is down; any other return code means that the track's state is up.

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 87**

Refer to the exhibit. Which statement about the configuration is true?

**Exhibit:**

```
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip sla monitor 1
 type jitter dest-ipaddr 200.0.10.3 dest-port 65051 num-packets 20
 request-data-size 160
 tos 128
 frequency 30
ip sla monitor schedule 1 start-time after 00:05:00
```

- A. 20 packets are being sent every 30 seconds
- B. The monitor starts at 12:05:00 a.m.
- C. Jitter is being tested with TCP packets to port 65051
- D. The packets that are being sent use DSCP EF

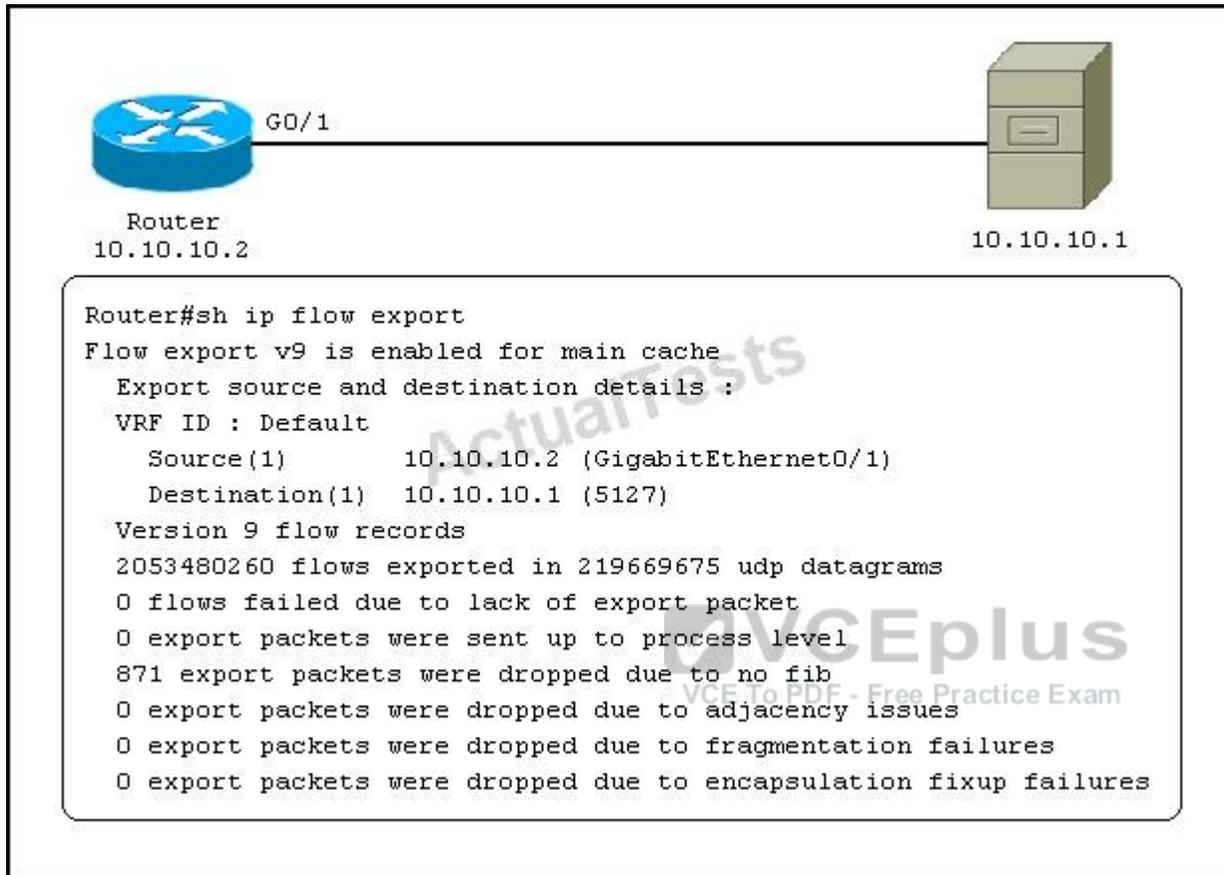
**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 88**

Refer to the exhibit. Which statement about the command output is true?

**Exhibit:**



- A. The router exports flow information to 10.10.10.1 on UDP port 5127.
- B. The router receives flow information from 10.10.10.2 on UDP port 5127
- C. The router exports flow information to 10.10.10.1 on TCP port 5127
- D. The router receives flow information from 10.10.10.2 on TCP port 5127.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 89**

A network engineer is trying to modify an existing active NAT configuration on an IOS router by using the following command:

```
(config)# no ip nat pool dynamic-nat-pool 192.1.1.20 192.1.1.254 netmask 255.255.255.0
```

Upon entering the command on the IOS router, the following message is seen on the console:  
%Dynamic Mapping in Use, Cannot remove message or the %Pool outpool in use, cannot destroy

What is the least impactful method that the engineer can use to modify the existing IP NAT configuration?

- A. Clear the IP NAT translations using the clear ip nat traffic \* " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
- B. Clear the IP NAT translations using the clear ip nat translation \* " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
- C. Clear the IP NAT translations using the reload command on the router, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
- D. Clear the IP NAT translations using the clear ip nat table \* " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 90**

Which IPv6 address type is seen as the next-hop address in the output of the show ipv6 rip RIPv6 database command?

- A. link-local
- B. global
- C. site-local
- D. anycast
- E. multicast

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 91**

Which three items can you track when you use two time stamps with IP SLAs? (Choose three.)

- A. delay
- B. jitter
- C. packet loss
- D. load
- E. throughput
- F. path

**Correct Answer:** ABC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**



**QUESTION 92**

If the total bandwidth is 64 kbps and the RTT is 3 seconds, what is the bandwidth delay product?

- A. 8,000 bytes
- B. 16,000 bytes
- C. 24,000 bytes
- D. 32,000 bytes
- E. 62,000 bytes

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 93**

What are the default timers for RIPng?

- A. Update: 30 seconds Expire: 180 seconds Flush: 240 seconds
- B. Update: 20 seconds Expire: 120 seconds Flush: 160 seconds
- C. Update: 10 seconds Expire: 60 seconds Flush: 80 seconds
- D. Update: 5 seconds Expire: 30 seconds Flush: 40 seconds

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 94**

What is the purpose of the route-target command?

- A. It extends the IP address to identify which VRF instance it belongs to.
- B. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities.
- C. It manages the import and export of routes between two or more VRF instances.
- D. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

A network engineer has configured a tracking object to monitor the reachability of IP SLA 1. In order to update the next hop for the interesting traffic, which feature must be used in conjunction with the newly created tracking object to manipulate the traffic flow as required?

- A. SNMP
- B. PBR
- C. IP SLA

- D. SAA
- E. ACLs
- F. IGP

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### **QUESTION 96**

A route map uses an ACL, if the required matching is based on which criteria?

- A. addressing information
- B. route types
- C. AS paths
- D. metrics

**Correct Answer:** A  
**Section:** (none)  
**Explanation**



**Explanation/Reference:**

#### **QUESTION 97**

Various employees in the same department report to the network engineer about slowness in the network connectivity to the Internet. They are also having latency issues communicating to the network drives of various departments. Upon monitoring, the engineer finds traffic flood in the network. Which option is the problem?

- A. network outage
- B. network switching loop
- C. router configuration issue
- D. wrong proxy configured

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:****QUESTION 98**

Which type of handshake does CHAP authentication use to establish a PPP link?

- A. one-way
- B. two-way
- C. three-way
- D. four-way

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 99**

Which two authentication protocols does PPP support? (Choose two.)

- A. WAP
- B. PAP
- C. CHAP
- D. EAP
- E. RADIUS

**Correct Answer: BC**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 100**

Which statement is a restriction for PPPoE configuration?

- A. Multiple PPPoE clients can use the same dialer interface.
- B. Multiple PPPoE clients can use the same dialer pool

- C. A PPPoE session can be initiated only by the client
- D. A PPPoE session can be initiated only by the access concentrator.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 101

Refer to the exhibit:

Which statement about the configuration is true?

**Exhibit:**

```
interface Ethernet 0
 pppoe-client dial-pool-number 5
 pppoe-client ppp-max-payload 1500
interface Dialer 1
 ip address negotiated
 dialer pool 5
 mtu 1492
```

- A. This configuration is incorrect because the MTU must match the ppp-max-payload that is defined.
- B. This configuration is incorrect because the dialer interface number must be the same as the dialer pool number.
- C. This configuration is missing an IP address on the dialer interface.
- D. This configuration represents a complete PPPoE client configuration on an Ethernet connection.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 102

A company has their headquarters located in a large city with a T3 frame relay link that connects 30 remote locations that each have T1 frame relay connections. Which technology must be configured to prevent remote sites from getting overwhelmed with traffic and prevent packet drops from the headquarters?

- A. traffic shaping
- B. IPsec VPN
- C. GRE VPN
- D. MPLS

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 103

On which two types of interface is Frame Relay switching supported? (Choose two.)

- A. serial interfaces
- B. Ethernet interfaces
- C. fiber interfaces
- D. ISDN interfaces
- E. auxiliary interfaces



**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 104

In IPv6, SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router. How is the prefix advertised?

- A. routing table
- B. router advertisements
- C. routing protocol

D. routing type

**Correct Answer:** B

**Section:** (none)

**Explanation**

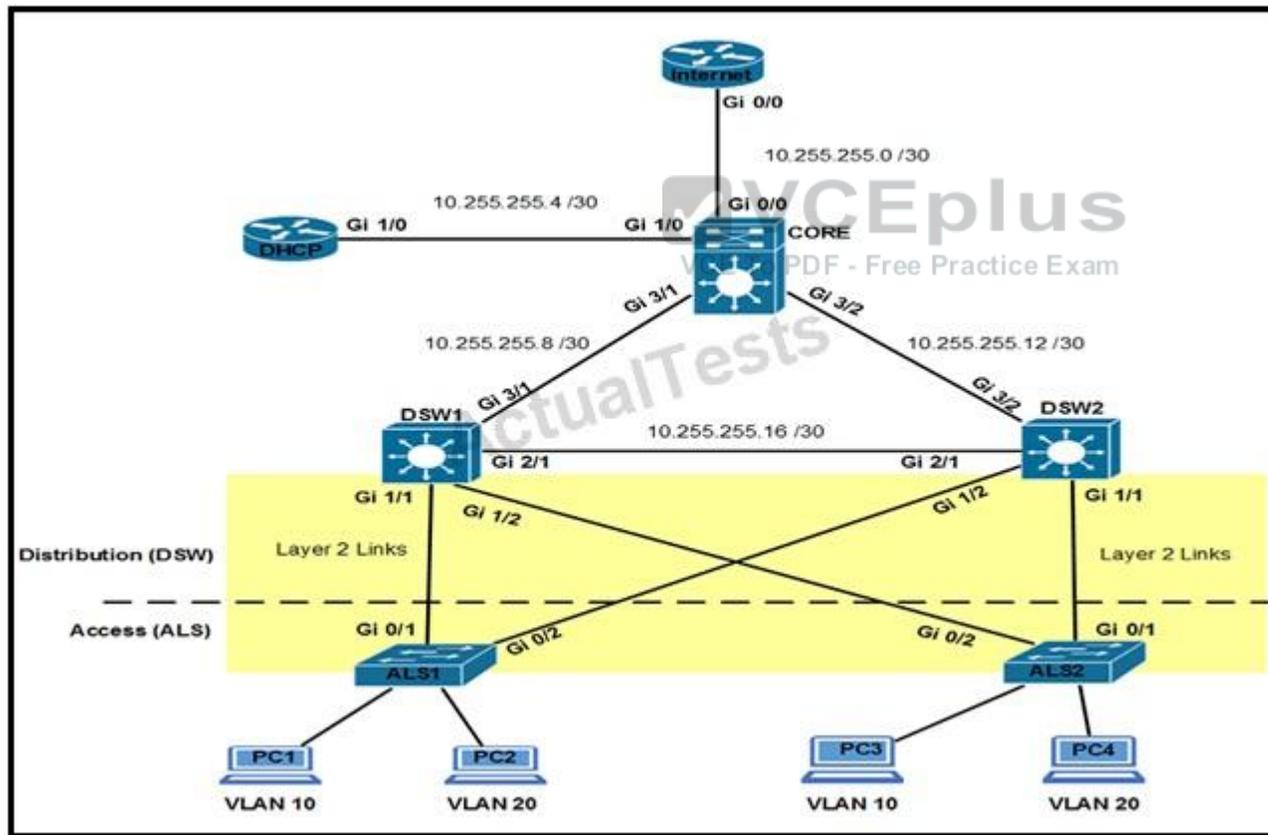
**Explanation/Reference:**

**QUESTION 105**

Refer to the exhibit:

Which option prevents routing updates from being sent to the access layer switches?

**Exhibit:**



- A. DWS1(config-router)# passive-interface default DWS2(config-router)# passive-interface default
- B. ALS1(config-router)# passive-interface default ALS2(config-router)# passive-interface default
- C. DWS1(config-router)# passive-interface gi1/1 DWS1(config-router)# passive-interface gi1/2  
DWS2(config-router)# passive-interface gi1/1 DWS2(config-router)# passive-interface gi1/2
- D. ALS1(config-router)# passive-interface gi0/1 ALS1(config-router)# passive-interface gi0/2  
ALS2(config-router)# passive-interface gi0/1 ALS2(config-router)# passive-interface gi0/2

**Correct Answer:** C

**Section:** (none)

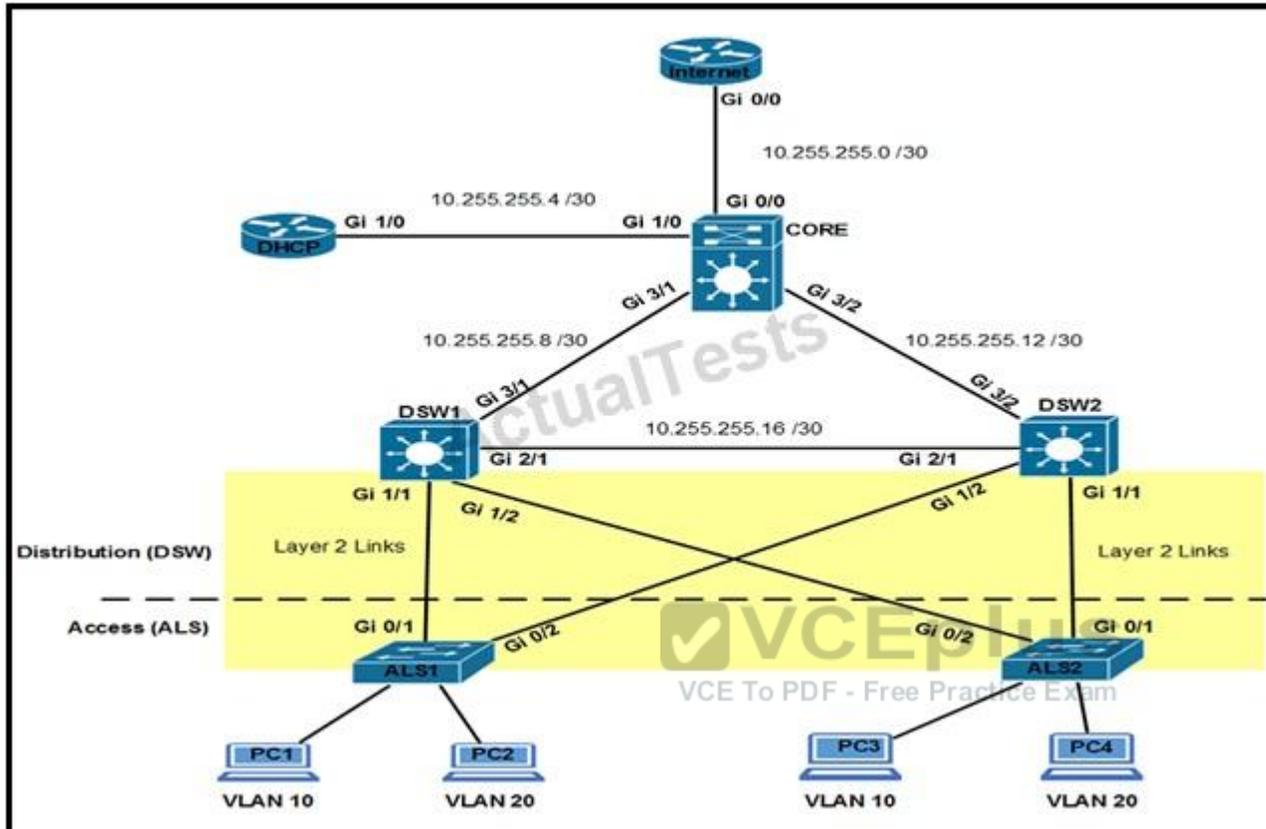
**Explanation**

**Explanation/Reference:**

#### **QUESTION 106**

Which option prevents routing updates from being sent to the DHCP router, while still allowing routing update messages to flow to the Internet router and the distribution switches?

**Exhibit:**



- A. DHCP(config-router)# passive-interface default DHCP(config-router)# no passive-interface Gi1/0 Internet(config-router)# passive-interface Gi0/1 Internet (config-router)# passive-interface Gi0/2
- B. Core(config-router)# passive-interface Gi0/0 Core(config-router)# passive-interface Gi3/1 Core(config-router)# passive-interface Gi3/2 DHCP(config-router)# no passive-interface Gi1/0
- C. Core(config-router)# passive-interface default Core(config-router)# no passive-interface Gi0/0 Core(config-router)# no passive-interface Gi3/1 Core(config-router)# no passive-interface Gi3/2
- D. Internet(config-router)# passive-interface default Core(config-router)# passive-interface default DSW1(config-router)# passive-interface default DSW2(config-router)# passive-interface default

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 107**

A network engineer is considering enabling load balancing with EIGRP. Which consideration should be analyzed?

- A. EIGRP allows a maximum of four paths across for load balancing traffic
- B. By default, EIGRP uses a default variance of 2 for load balancing.
- C. EIGRP unequal path load balancing can result in routing loops.
- D. By default, EIGRP performs equal cost load balancing at least across four equal cost paths.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 108**

The OSPF database of a router shows LSA types 1, 2, 3, and 7 only. Which type of area is this router connected to?

- A. stub area
- B. totally stubby area
- C. backbone area
- D. not-so-stubby area

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 109**

An engineer is configuring a GRE tunnel interface in the default mode. The engineer has assigned an IPv4 address on the tunnel and sourced the tunnel from an Ethernet interface. Which option also is required on the tunnel interface before it is operational?

- A. tunnel destination address
- B. keepalives
- C. IPv6 address
- D. tunnel protection

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 110**

Which protocol is used in a DMVPN network to map physical IP addresses to logical IP addresses?

- A. BGP
- B. LLDP
- C. EIGRP
- D. NHRP

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### **QUESTION 111**

Which two routing protocols are supported by Easy Virtual Network? (Choose two.)

- A. RIPv2
- B. OSPFv2
- C. BGP
- D. EIGRP
- E. IS-IS

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 112**

Which statement is true?

- A. RADIUS uses TCP, and TACACS+ uses UDP
- B. RADIUS encrypts the entire body of the packet
- C. TACACS+ encrypts only the password portion of a packet
- D. TACACS+ separates authentication and authorization

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 113**

Which two statements about AAA implementation in a Cisco router are true? (Choose two.)

- A. RADIUS is more flexible than TACACS+ in router management
- B. RADIUS and TACACS+ allow accounting of commands.
- C. RADIUS and TACACS+ encrypt the entire body of the packet.
- D. RADIUS and TACACS+ are client/server AAA protocols.
- E. Neither RADIUS nor TACACS+ allow for accounting of commands

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 114**

Which option is invalid when configuring Unicast Reverse Path Forwarding?

- A. allow self ping to router
- B. allow default route

- C. allow based on ACL match
- D. source reachable via both

**Correct Answer:** D

**Section:** (none)

**Explanation**

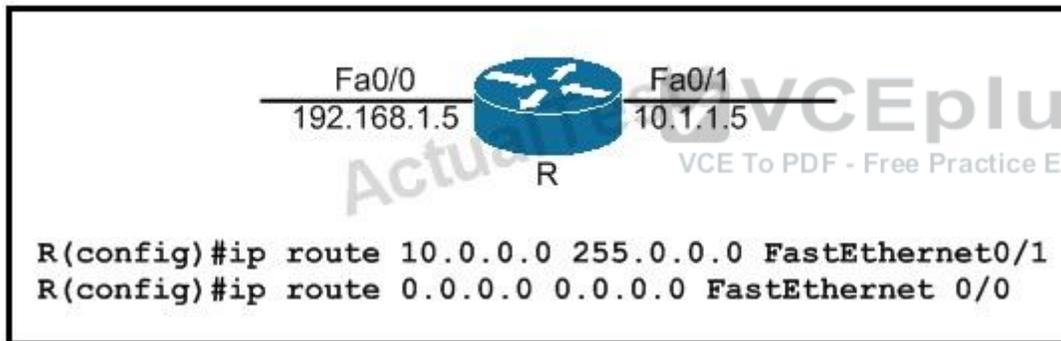
**Explanation/Reference:**

### QUESTION 115

Refer to the exhibit.

Which option represents the minimal configuration that allows inbound traffic from the 172.16.1.0/24 network to successfully enter router R, while also limiting spoofed 10.0.0.0/8 hosts that could enter router R?

**Exhibit:**



- A. (config)#ip cef  
(config)#interface fa0/0  
(config-if)#ip verify unicast source reachable-via rx allow-default
- B. config)#ip cef  
(config)#interface fa0/0  
(config-if)#ip verify unicast source reachable-via rx
- C. (config)#no ip cef  
(config)#interface fa0/0  
(config-if)#ip verify unicast source reachable-via rx
- D. (config)#interface fa0/0  
(config-if)#ip verify unicast source reachable-via any

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### **QUESTION 116**

Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

- A. ip access-list extended 200  
deny tcp host 10.10.10.1 eq 80 any  
permit ip any any
- B. ip access-list extended 10  
deny tcp host 10.10.10.1 any eq 80  
permit ip any any
- C. ip access-list extended NO\_HTTP  
deny tcp host 10.10.10.1 any eq 80
- D. ip access-list extended 100  
deny tcp host 10.10.10.1 any eq 80  
permit ip any any



**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### **QUESTION 117**

Which two statements indicate a valid association mode for NTP synchronization? (Choose two.)

- A. The client polls NTP servers for time
- B. The client broadcasts NTP requests
- C. The client listens to NTP broadcasts.
- D. The client creates a VPN tunnel to an NTP server.
- E. The client multicasts NTP requests.

**Correct Answer:** AC  
**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 118**

Refer to the exhibit.

Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

**Exhibit:**

```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

- A. ip nat inside source list 10 interface FastEthernet0/1 overload
- B. ip nat outside source static 209.165.200.225 10.10.10.0 overload
- C. ip nat inside source list 10 interface FastEthernet0/2 overload
- D. ip nat outside source list 10 interface FastEthernet0/2 overload

**Correct Answer:** A

**Section:** (none)

**Explanation****Explanation/Reference:****QUESTION 119**

Which statement describes what this command accomplishes when inside and outside interfaces are correctly identified for NAT?

```
ip nat inside source static tcp 192.168.1.50 80 209.165.201.1 8080 extendable
```

- A. It allows host 192.168.1.50 to access external websites using TCP port 8080
- B. It allows external clients coming from public IP 209.165.201.1 to connect to a web server at 192.168.1.50.
- C. It allows external clients to connect to a web server hosted on 192.168.1.50
- D. It represents an incorrect NAT configuration because it uses standard TCP ports

**Correct Answer: C**

**Section: (none)**

**Explanation**

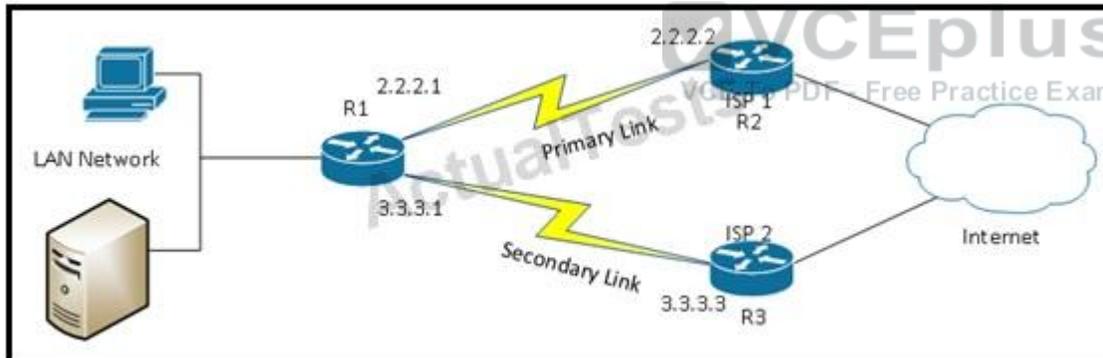
**Explanation/Reference:**

### QUESTION 120

Refer to the exhibit.

Which technology can be employed to automatically detect a WAN primary link failure and failover to the secondary link?

**Exhibit:**



- A. HSRP
- B. VRRP
- C. IP SLA
- D. multicast

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 121**

In which two ways can NetFlow data be viewed? (Choose two.)

- A. CLI
- B. NetFlow
- C. built-in GUI
- D. syslog server interface
- E. web interface

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:****QUESTION 122**

An engineer is asked to monitor the availability of the next-hop IP address of 172.16.201.25 every 3 seconds using an ICMP echo packet via an ICMP echo probe. Which two commands accomplish this task? (Choose two.)

- A. `router(config-ip-sla)#icmp-echo 172.16.201.25 source-interface FastEthernet 0/0`
- B. `router(config-ip-sla-echo)#timeout 3`
- C. `router(config-ip-sla)#icmp-jitter 172.16.201.25 interval 100`
- D. `router(config-ip-sla-echo)#frequency 3`
- E. `router(config-ip-sla)#udp-echo 172.16.201.25 source-port 23`
- F. `router(config-ip-sla-echo)#threshold 3`

**Correct Answer:** AD

**Section:** (none)

**Explanation**

**Explanation/Reference:**