Chapters 18 – 20: VPNs Exam Answers (CCNPv8 ENARSI)

itexamanswers.net/chapters-18-20-vpns-exam-answers-ccnpv8-enarsi.html

April 8, 2021

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

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

CCNP Enterprise: Advanced Routing (Version 8.0) – VPNs Exam

1. An network administrator has created VRF instances on a router and assigned interfaces to the VRF instances. What command can the administrator issue to verify what IP address is assigned to the interface, what VRF instance the interface is in, and whether the interface is up or down?

- show ip route
- show interface
- **show ip vrf interfaces**
- show ip vrf

Explanation: The `show ip vrf interfaces` command will show each interface that is assigned to a VRF as well as the IP address assigned to the interface, and whether the interface is up.

2. When connectivity over a VRF instance is being verified, what information must be specified as part of the ping command?

- **the VRF instance**
- the source interface
- the source address
- the datagram size

Explanation: When the ping command is issued, the VRF instance must be specified, otherwise the global routing table is used and the ping will fail.

3. Which two components used in MPLS operation are associated with the router data plane? (Choose two.)

- label distribution protocol (LDP)
- **IP forwarding table (FIB)**
- IP routing table (RIB)
- **label forwarding table (LFIB)**
- label information base (LIB)

Explanation: The data plane of a LSR consists of an IP forwarding table (FIB) and a label forwarding table (LFIB). The FIB makes forwarding decisions for unlabeled packets. The LFIB makes forwarding decision for labeled packets.

4. In an MPLS Layer 3 VPN network, which router is responsible for adding both the VPN and the LDP labels to packets?

- egress PE
- CE
- **ingress PE**
- P

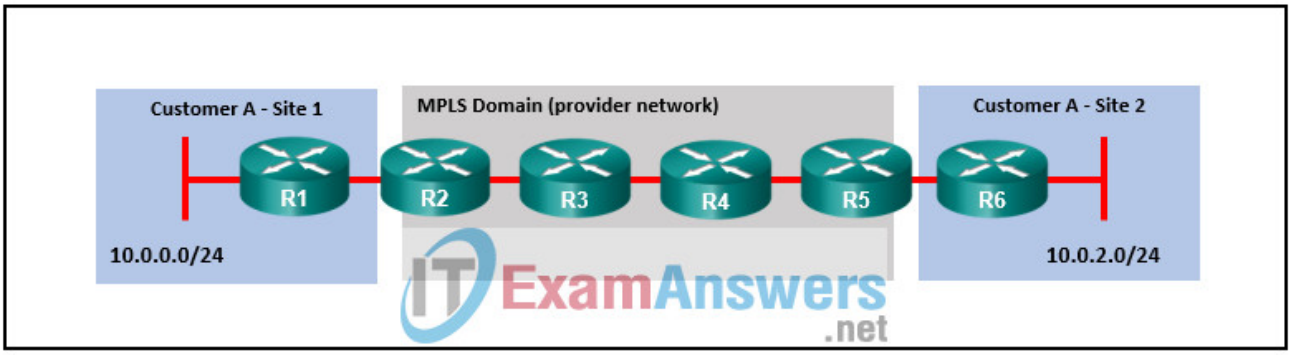
Explanation: When an IP packet arrives at the ingress PE router, it attaches both the VPN and the LDP label.

5. Which database on an LSR is used to make forwarding decisions on labeled packets?

- RIB
- FIB
- LIB
- **LFIB**

Explanation: The data plane of a LSR consists of a IP forwarding table (FIB) and a label forwarding table (LFIB). The FIB makes forwarding decisions for unlabeled packets. The LFIB makes forwarding decision for labeled packets.

6. Refer to the exhibit. Which router will perform penultimate hop popping on packets destined for the 10.0.2.0/24 network?



- R1
- R2
- **R4**
- R5
- R6

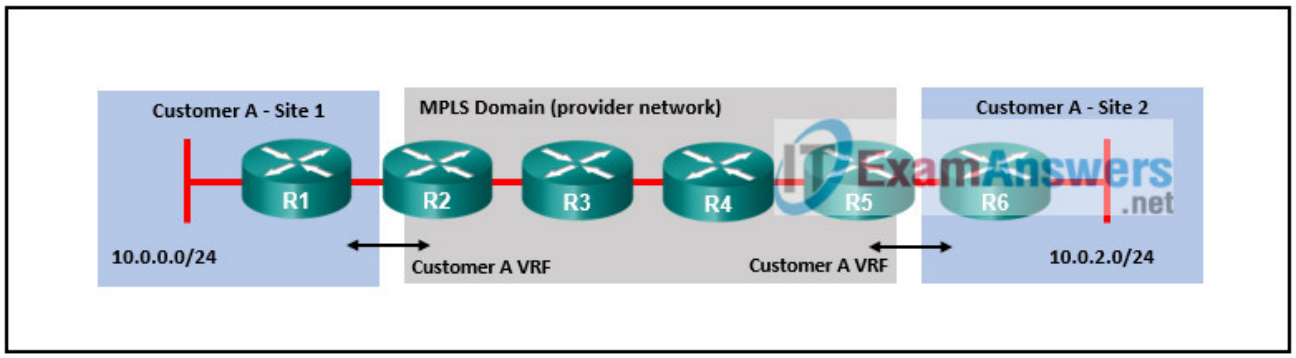
Explanation: With penultimate hop popping, the last provider (P) router, which is router R4 in this example, removes (pops) the label off packets before they reach the provider edge (PE) router, R5.

7. What is a characteristic of CE routers in an MPLS Layer 3 VPN environment?

- They perform penultimate hop popping.
- They run the label distribution protocol to share and distribute labels.
- **They are unaware of MPLS and labels.**
- They remove labels at the end of the label path.

Explanation: CE, or customer edge, routers do not run MPLS. They also are unaware of labels and VRF instances. CE routers are connected to the provider edge (PE) routers of the MPLS service provider.

8. Refer to the exhibit. Which two routers would be participating in MP-BGP? (Choose two.)



- R1
- **R2**
- R3
- R4
- **R5**
- R6

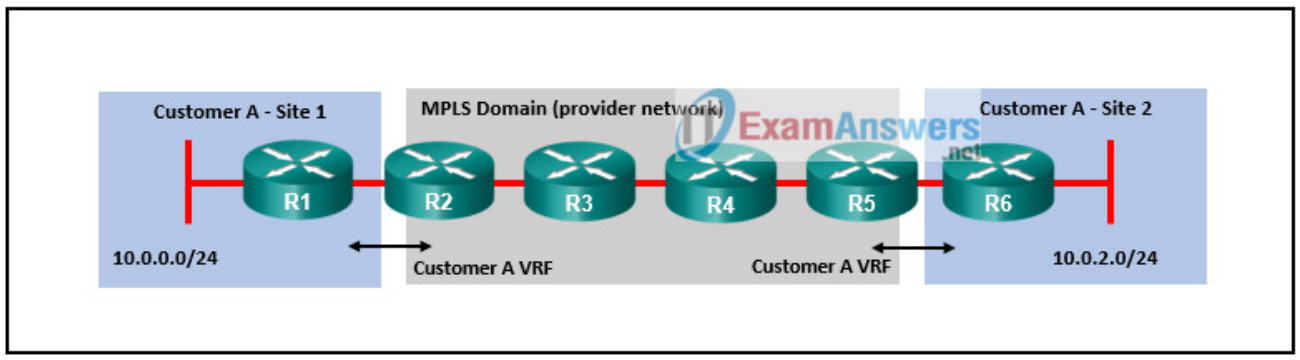
Explanation: The PE routers, R2 and R5, learn routes from the CE routers, R1 and R6, and redistribute the routes into MP-BGP so they can be exchanged with other PE routers. The P routers, R3 and R4, and the customer (CE) routers do not participate in MP-BGP.

9. What addressing method is used by MPLS-enabled routers to forward packets through the MPLS domain?

- **labels**
- destination IP address
- DLCI
- Layer 4 port number

Explanation: Provider MPLS-enabled routers use labels attached to IP packets to forward traffic through the MPLS domain.

10. Refer to the exhibit. Which two routers are considered P routers? (Choose two.)



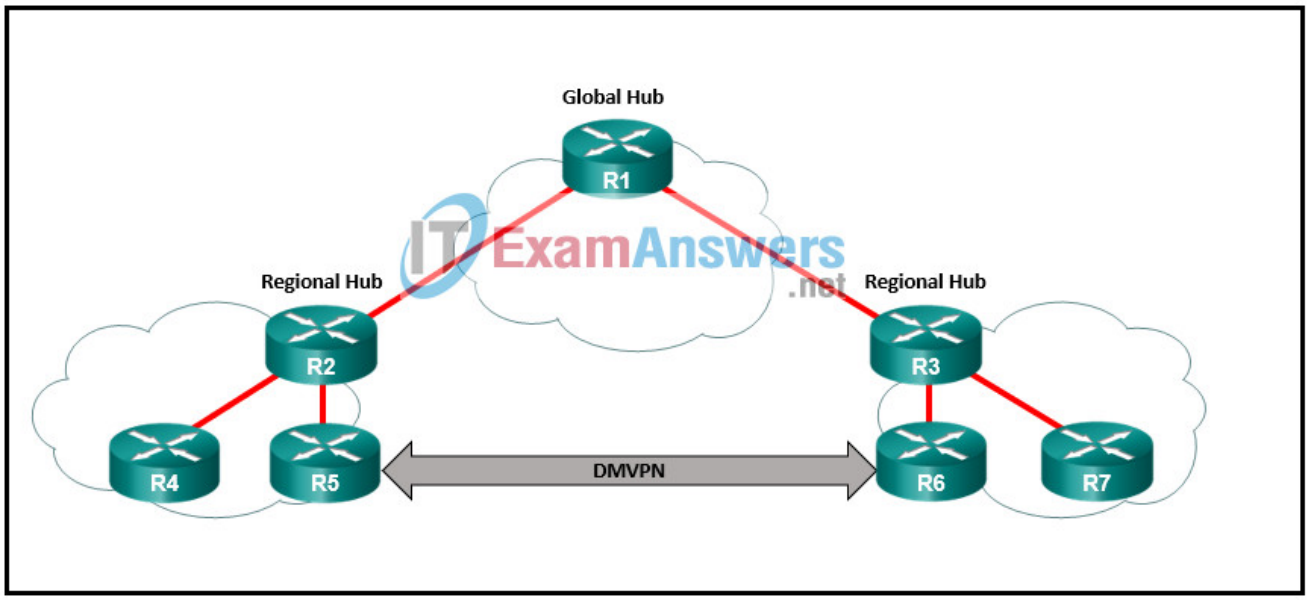
- R1
- R2
- **R3**
- **R4**
- R5
- R6

Explanation: The PE routers, R2 and R5, learn routes from the CE routers. The PE routers label packets from the CE routers and forward the labeled packets to the P routers, R4 and R5.

11. Match the DMVPN tunnel state with the description. (Not all options are used.)
2021-04-16_143624.jpg

- **IPsec** – IPsec security associations are not established.
- **NHRP** – The DMVPN spoke router has not yet successfully registered.
- (Empty) – IPsec tunnels have not established an IKE session.
- **INTF** – The line protocol of the DMVPN tunnel is down.

12. Refer to the exhibit. Which DMVPN phase or phases will support a DMVPN tunnel between R5 and R6?



- Phase 1, 2, or 3
- Phase 1 and 2 only
- Phase 2 and 3 only
- **Phase 3 only**

Explanation: There are three DMVPN phase models: Phase 1, Phase 2, and Phase 3. The first DMVPN implementation is Phase 1. Phase 1 supports only spoke-to-hub tunnels. Traffic between spokes must traverse the hub. Phases 2 and 3 support not only spoke-to-hub tunnels, but also direct spoke-to-spoke tunnels. Only Phase 2 supports spoke-to-spoke communication between DMVPN networks or regions.

13. After how many NHRP registration request re-transmissions is a next-hop server (NHS) declared "down" if a spoke has not received an NHRP registration reply?

- 2
- **3**
- 4
- 5

Explanation: NHRP registration requests are sent by the spoke every NHRP timeout period. If an NHRP registration reply is not received, the spoke will make three additional attempts. If after the third additional attempt a reply is not received, the NHS is declared "down".

14. When implementing IPv6 DMVPN with IPv6 as the tunneling protocol, what IPv6 address type must be assigned to the tunnel interface?

- unique global
- **link-local**
- anycast
- unique local

Explanation: Because IPv6 routing protocols use IPv6 link-local addresses for neighbor discovery, IPv6 DMVPN configuration must assign IPv6 link-local addresses on the tunnel interfaces.

15. Which additional command, beyond DVMPN Phase 1 configuration, is added to spoke routers for Phase 3 DMVPN (Multipoint)?

- ip nhrp nhs
- ip nhrp redirect
- **ip nhrp shortcut**
- ip nhrp map

Explanation: The Phase 3 DMVPN configuration for spoke routers uses the ip nhrp shortcut command on the tunnel interface.

16. Which capability is supported by all three DMVPN phase models?

- **direct spoke-to-hub communication**
- spoke-to-spoke between DMVPN networks
- direct spoke-to-spoke communication
- on-demand VPN tunnels between spokes

Explanation: There are three DMVPN phase models: Phase 1, Phase 2, and Phase 3. The first DMVPN implementation is Phase 1. Phase 1 only supports spoke-to-hub tunnels. Traffic between spokes must traverse the hub. Phases 2 and 3 support not only spoke-to-hub tunnels, but also direct spoke-to-spoke tunnels.

17. Match the NHRP message type with the description.
2021-04-16_144150.jpg

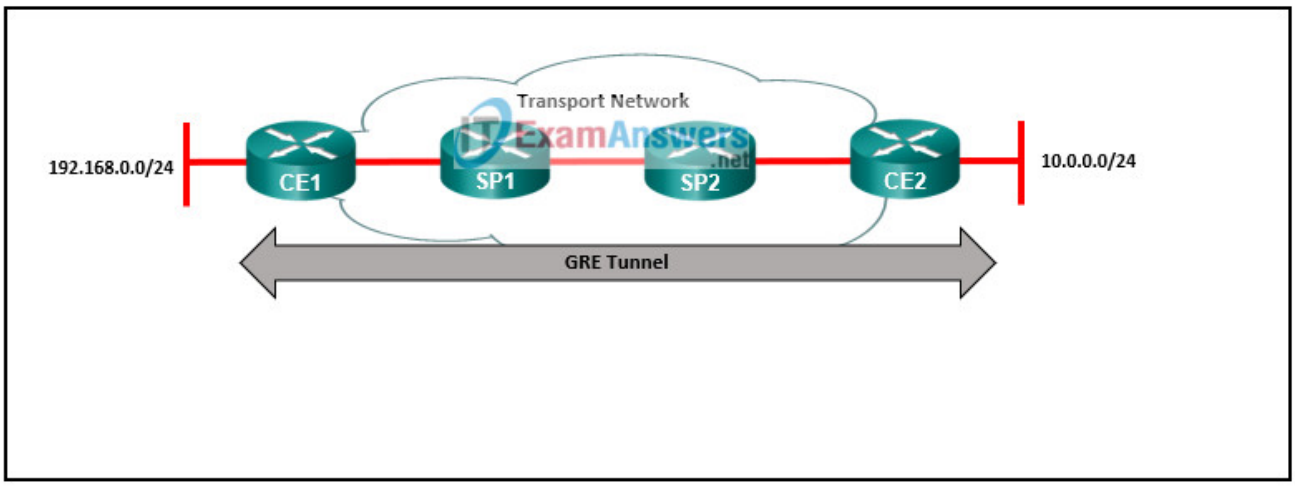
- **resolution** – locates and provides address information of remote spoke
- **redirect** – informs router of more optimal path to a destination
- **registration** – informs hubs of spoke NBMA information
- **purge** – removes cached NHRP entries

18. Which solution would prevent the problem of recursive routing over DMVPN tunnels?

- conditional forwarding
- NHRP
- STP
- **front door VRF**

Explanation: A front door VRF instance occurs when the VRF instance is associated with the DMVPN transport network. It allows the interface associated with the transport network to be associated with a transport VRF that is a different VRF instance from the DMVPN tunnel.

19. Refer to the exhibit. A network administrator has configured a GRE tunnel between routers CE1 and CE2 to connect two corporate sites across the provider network. From the perspective of router CE1, how many hops away is network 10.0.0.0/24?



- 0
- **1**
- 2
- 3

Explanation: The GRE tunnel creates an overlay network through the provider network. The provider routers, SP1 and SP2, do not participate in the routing protocol connecting the two GRE edge routers CE1 and CE2. From the perspective of router CE1, the 10.0.0.0/24 network is only 1 hop away.

20. What is the default NHRP cache holdtime period?

- 60 seconds
- 600 seconds
- 15 minutes
- **2 hours**

Explanation: NHRP entries in the NHRP cache stay valid for 7200 seconds (2 hours) by default. This hold time can be modified using the ip nhrp holdtime command. It is recommended that the hold time for valid entries be modified to 600 seconds.

21. Which component is an element of secure data transport that is concerned with ensuring data is viewable to only authorized users?

- **confidentiality**
- availability
- integrity
- accountability

Explanation: The three elements of data security are as follows:

- Confidentiality, which ensures data is viewable to only authorized users
- Integrity, which ensures data can only be modified by authorized users and has not been changed
- Availability, which ensures that the network is always available allowing the secure transport of the data

22. What element of security is ensured by data confidentiality?

- Data is accurate and has not been changed in transit.
- Data can be modified only by authorized users.
- **Data is viewable to only authorized users.**
- Data is always available for users.

Explanation: The three elements of data security are as follows:

- Confidentiality, which ensures data is viewable to only authorized users
- Integrity, which ensures data can only be modified by authorized users and has not been changed
- Availability, which ensures that the network is always available allowing the secure transport of the data

23. Which security mechanism is used to ensure data integrity?

- preshared keys
- encryption algorithms
- **hashing algorithms**
- digital certificates

Explanation: Hashing algorithms ensure data integrity by using a checksum to compare the transported data with the original data.

24. What protection is provided by IPsec perfect forward secrecy?

- ensuring that packets are not modified in transit
- **ensuring a compromised session key does not lead to the compromise of future keys**
- providing protection against hackers trying to capture and insert network traffic
- creating new security keys between endpoints on a specified time interval

Explanation: With perfect forward secrecy each session key is derived independently of the previous key so that a compromise of one key does not mean compromise of future keys.

25. What is a characteristic of the IPsec Encapsulation Security Payload protocol?

- functions only in transport mode
- does not encrypt the original payload of the packet
- **provides data confidentiality, integrity, and authentication**
- uses protocol number 51 located in the IP header

Explanation: IPsec uses two protocols to provide data integrity and confidentiality, the IP Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH, which uses IP protocol number 51, provides integrity and authentication but does not provide encryption. ESP provides data confidentiality, integrity, and authentication. ESP ensures confidentiality by encrypting the payload and adding a new set of headers during transport across a public network.

26. What are two characteristics of IPsec ESP tunnel mode? (Choose two.)

- **It adds a new IPsec header.**
- It encrypts and authenticates only the original packet payload.
- It encrypts the IPsec and ESP headers.
- **It encrypts the entire original packet.**
- It routes packets based on the original IP header.

Explanation: There are two modes of ESP operation, tunnel mode and transport mode. In ESP tunnel mode the entire original packet is encrypted and a new IPsec header is added which is used to route the packet.

27. What is a characteristic of the DMVPN IPsec tunnel mode?

- It encrypts both the GRE and ESP headers.
- It encrypts and authenticates only the original packet payload.
- It uses the original IP header to routes packets.
- **It encrypts the entire original packet and the GRE IP header.**

Explanation: There are two modes of DMVPN IPsec operation, tunnel mode and transport mode. In ESP tunnel mode the entire original packet and the GRE IP header are encrypted and a new IPsec IP header is added which is used to route the packet.

28. What algorithm is used with IPsec to provide data confidentiality?

- SHA
- MD5
- **AES**
- RSA
- Diffie-Hellman

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. Two popular algorithms that are used to ensure that data is not intercepted and modified (data integrity) are MD5 and SHA. AES is an encryption protocol and provides data confidentiality. DH (Diffie-Hellman) is an algorithm that is used for key exchange. RSA is an algorithm that is used for authentication.

29. What can be configured with DMVPN tunnels to provide confidentiality and integrity to data transported over the Internet?

- digital certificates
- **IPsec**
- SSH
- SSL

Explanation: Data confidentiality and integrity can be accomplished by adding IPsec encryption to DMVPN tunnels that use the Internet as a transport.

30. Which algorithm is used to support ESP encryption?

- **AES**
- SHA
- MD5
- HMAC

Explanation: The Advanced Encryption Standard (AES) and the Galois Counter Mode (GCM) encryption algorithms are used to provide encryption for IPsec ESP.

31. What two protocols provide data authentication and integrity for IPsec? (Choose two.)

- **AH**
- L2TP

- GRE
- **ESP**
- PPTP

Explanation: IPsec uses two protocols to provide data integrity and confidentiality, the IP Authentication Header (AH) and the Encapsulating Security Payload (ESP). AH provides integrity and authentication but does not provide encryption. AH can ensure that the original data packet has not been modified during transport but it does not encrypt data to ensure it is viewable only by authorized users. ESP provides confidentiality, integrity, and authentication.

32. Which NHRP message flag indicates that a specific mapping entry in the NHRP cache was used to forward data packets within the past 60 seconds?

- nhop
- implicit
- **used**
- rib