

Chapters 15 – 16: IP Services and VPNs Exam (Answers)

itexamanswers.net/chapters-15-16-ip-services-and-vpns-exam-answers.html

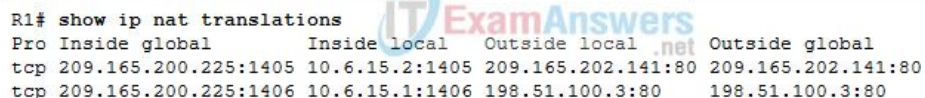
December 18, 2020

CCNPv8 ENCOR (Version 8.0) – IP Services and VPNs Exam

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.

1. Refer to the exhibit. Based on the output that is shown, what type of NAT has been implemented?



```
R1# show ip nat translations
Pro Inside global      Inside local    Outside local    Outside global
tcp 209.165.200.225:1405 10.6.15.2:1405 209.165.202.141:80 209.165.202.141:80
tcp 209.165.200.225:1406 10.6.15.1:1406 198.51.100.3:80    198.51.100.3:80
```

- dynamic NAT with a pool of two public IP addresses
- static NAT with a NAT pool
- **PAT using an external interface**
- static NAT with one entry

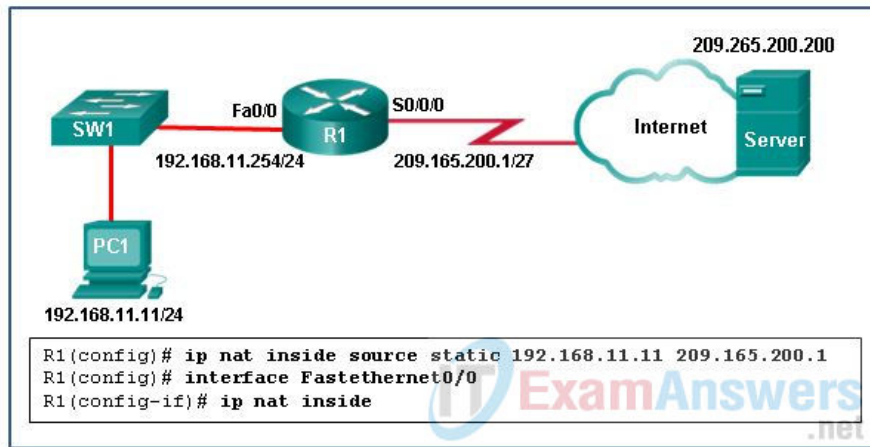
Explanation: The output shows that there are two inside global addresses that are the same but that have different port numbers. The only time port numbers are displayed is when PAT is being used. The same output would be indicative of PAT that uses an address pool. PAT with an address pool is appropriate when more than 4,000 simultaneous translations are needed by the company.

2. Match the steps with the actions that are involved when an internal host with IP address 192.168.10.10 attempts to send a packet to an external server at the IP address 209.165.200.254 across a router R1 that is running dynamic NAT. (Not all options are used.)



Explanation: The translation of the IP addresses from 209.65.200.254 to 192.168.10.10 will take place when the reply comes back from the server.

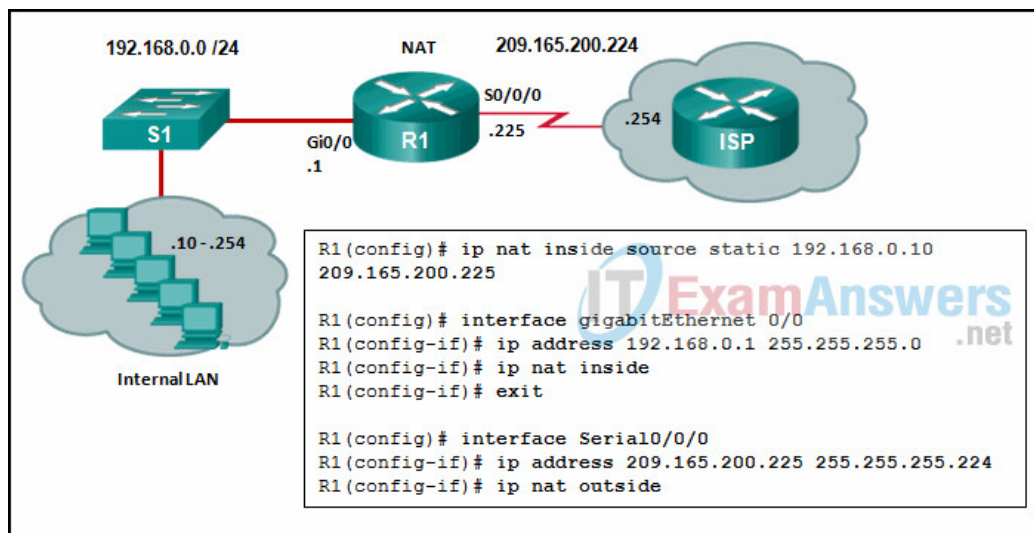
3. Refer to the exhibit. What has to be done in order to complete the static NAT configuration on R1?



- R1 should be configured with the command `ip nat inside source static 209.165.200.200 192.168.11.11`.
- **Interface So/o/o should be configured with the command `ip nat outside`.**
- Interface Fa0/o should be configured with the command `no ip nat inside`.
- R1 should be configured with the command `ip nat inside source static 209.165.200.1 192.168.11.11`.

Explanation: In order for NAT translations to work properly, both an inside and outside interface must be configured for NAT translation on the router.

4. Refer to the exhibit. Given the commands as shown, how many hosts on the internal LAN off R1 can have simultaneous NAT translations on R1?



- 1
- 255
- 244
- 10

Explanation: The NAT configuration on R1 is static NAT which translates a single inside IP address, 192.168.0.10 into a single public IP address, 209.165.200.225. If more hosts need translation, then a NAT pool of inside global address or overloading should be configured.

5. What is a potential disadvantage when implementing HSRP as compared to GLBP?

- **HSRP does not provide load balancing with multiple active routers.**
- HSRP does not function in a multivendor environment.
- HSRP does not have the capability to support IPv6 addresses.
- HSRP provides default gateway failover only when the active router fails.

Explanation: HSRP is a first-hop redundancy protocol that can utilize a group of routers, where a single router is acting as the default gateway and all other HSRP routers will maintain a backup status. GLBP supports load balancing, where multiple active routers can share the traffic load at a single time. Both HSRP and GLBP are Cisco proprietary. HSRP provides default gateway failover when pre-set conditions are met or when the active router fails, and HSRP can support IPv6 addressing.

6. What are three advantages of using private IP addresses and NAT? (Choose three.)

- creates multiple public IP addresses
- reduces CPU usage on customer routers
- **hides private LAN addressing from outside devices that are connected to the Internet**
- improves the performance of the router that is connected to the Internet
- **conserves registered public IP addresses**
- **permits LAN expansion without additional public IP addresses**

Explanation: Private IP addresses are designed to be exclusively used for internal networks and they cannot be used on the Internet. Thus they are not visible directly from the Internet and they can be used freely by network administrators for internal networks. In order for the internal hosts to access the Internet, NAT is used to translate between private and public IP addresses. NAT takes an internal private IP address and translates it to a global public IP address before the packet is forwarded.

7. A network engineer wants to synchronize the time of a router with an NTP server at the IPv4 address 209.165.200.225. The exit interface of the router is configured with an IPv4 address of 192.168.212.11. Which global configuration command should be used to configure the NTP server as the time source for this router?

- ntp peer 209.165.200.225
- ntp peer 192.168.212.11
- ntp server 192.168.212.11
- **ntp server 209.165.200.225**

Explanation: The global configuration command ntp server server ip-address will set the server at that address as the time source for the router. The ntp peer command which enables a router to both update the time of another similarly configured router, and also synchronize with that router if necessary, is not appropriate in this case.

8. Which router command is required to configure VRRP to support IPv6?

- standby 1 ipv6 FE80::1:1
- **fhrp version vrrp v3**
- standby 6 ipv6 autoconfig
- vrrp 22 address-family ipv6

Explanation: VRRPv3 supports IPv4 and IPv6 and is configured globally using the fhrp version vrrp v3 command before the vrrp instance-id address-family ipv6 interface configuration command is applied. standby 6 ipv6 autoconfig and standby 1 ipv6 FE80::1:1 are HSRP commands.

9. A networking engineer is configuring an NTP client to have access to multiple NTP servers but wants one server to have priority over the others. Which command will achieve this?

- ntp server 2001:DB8:0:0:800:200C:417A version 4h
- ntp max-associations 1
- **ntp server 203.0.113.1 prefer**
- ntp master 1

Explanation: The ntp server 2001:DB8:0:0:800:200C:417A version 4 command configures the NTP client to synchronize with the NTP server at the specified IPv6 address but does not give it priority over other available servers. The command ntp max-associations number sets the maximum number of NTP peer-and-client associations that the router will serve. The command ntp master 1 sets the router to be a stratum level 1 NTP server.

10. What is a feature or purpose of NTP peers?

- NTP peers are NTP clients that share a common NTP server.
- An NTP client that loses connection with an NTP server can synchronize the time with an NTP peer.
- **NTP peers query each other to synchronize their clocks.**

- An NTP peer that loses connection with another NTP peer loses all NTP synchronization.

Explanation: An NTP peer that is configured with an authoritative time source treats its peer as an equal and adjusts its clock to synchronize with that peer.

11. Which two NTP details are displayed by issuing the show ntp associations command on a switch configured to use NTP? (Choose two.)

- reference time
- **NTP server IP address**
- **reference clock IP address**
- “Clock is synchronized” statement
- NTP uptime

Explanation: NTP uptime, “Clock is synchronized” statement, and the reference time are displayed by the show ntp status command.

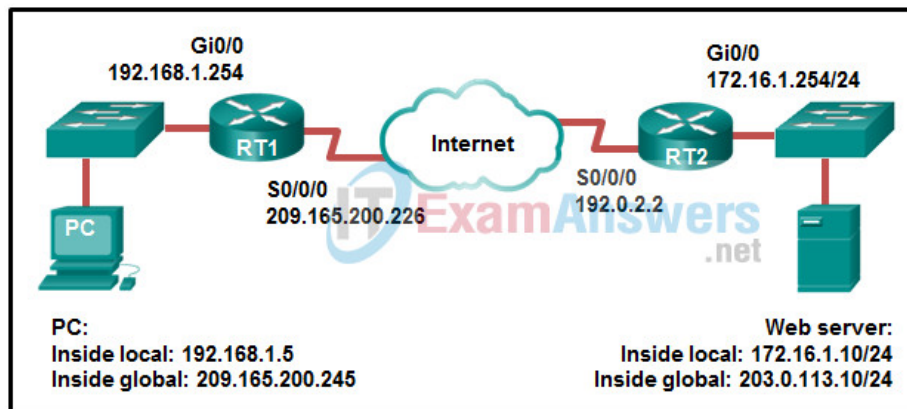
12. Refer to the exhibit. A network administrator has configured R2 for PAT. Why is the configuration incorrect?

```
R2(config)#ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)#access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)#ip nat inside source list 100 pool NAT-POOL2 overload
R2(config)#interface Serial0/0/0
R2(config-if)#ip nat inside
R2(config)#interface Serial0/1/0
R2(config-if)#ip nat outside
```

- The overload keyword should not have been applied.
- The ACL does not define the list of addresses to be translated.
- The static NAT entry is missing.
- **NAT-POOL2 is bound to the wrong ACL.**

Explanation: In the exhibit, NAT-POOL 2 is bound to ACL 100, but it should be bound to the configured ACL 1. This will cause PAT to fail. 100, but it should be bound to the configured ACL 1. This will cause PAT to fail.

13. Refer to the exhibit. NAT is configured on RT1 and RT2. The PC is sending a request to the web server. What IPv4 address is the source IP address in the packet between RT2 and the web server?



- 192.0.2.2
- 172.16.1.10
- 172.16.1.254
- **209.165.200.245**
- 203.0.113.10
- 192.168.1.5

Explanation: Because the packet is between RT2 and the web server, the source IP address is the inside global address of PC, 209.165.200.245.

14. A network administrator would like to ensure that router R1 is always elected the active router for an HSRP group. Which set of commands would ensure the required results?

```
R1(config-if)# ip address 192.168.1.100 255.255.255.0
R1(config-if)# standby 1 ip 192.168.1.1
R1(config-if)# standby 1 priority 150
R1(config-if)# no shutdown
```

```
R1(config-if)# ip address 192.168.1.250 255.255.255.0
R1(config-if)# standby 1 ip 192.168.1.1
R1(config-if)# no shutdown
```

```
R1(config-if)# ip address 192.168.1.100 255.255.255.0
R1(config-if)# standby 1 ip 192.168.1.1
R1(config-if)# standby 1 priority 1
R1(config-if)# no shutdown
```

```
R1(config-if)# ip address 192.168.1.100 255.255.255.0
R1(config-if)# standby 1 ip 192.168.1.1
R1(config-if)# standby 1 priority 255
R1(config-if)# standby 1 preempt
R1(config-if)# no shutdown
```

Explanation: In order to configure HSRP, the standby command is used. The IP address given with the standby command is the virtual IP address used by hosts as a default gateway. A priority number of 255 is the highest that can be assigned and should be configured on the router that is to be the active router.

15. Refer to the exhibit. What two statements describe the NTP status of the router? (Choose two.)

```
Router# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24
reference time is DA27B091.83E37490 (12:09:53.515 UTC Fri Dec 25 2015)
clock offset is -1.5326 msec, root delay is 13.90 msec
root dispersion is 7941.16 msec, peer dispersion is 0.76 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is -0.000000130 s/s
system poll interval is 64, last update was 117 sec ago.
```

- The router is serving as an authoritative time source.
- The software clock for the router must be configured with the set clock command so that NTP will function properly.
- **The router is attached to a stratum 2 device.**
- The router is serving as a time source for the device at 192.168.1.1.
- **The IP address of the time source for the router is 192.168.1.1.**

Explanation: The show ntp status command displays information about how NTP is operating on the device. The output shows that the router clock is synchronized with the NTP server with the address of 192.168.1.1. NTP is hierarchical. The router is a stratum 3 device, therefore its time source is a stratum 2 device. Authoritative time sources in the NTP system are located at stratum 0.

16. Refer to the exhibit. A network administrator has just configured address translation and is verifying the configuration. What three things can the administrator verify? (Choose three.)

```

R1# show ip nat statistics
Total translations: 6 (2 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/2/1
Inside Interfaces: Serial0/2/0 , FastEthernet0/0.10 , FastEthernet0/0.11 ,
FastEthernet0/0.12
Hits: 3 Misses: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool NAT refCount 4
pool NAT: netmask 255.255.255.248
start 209.165.200.228 end 209.165.200.230
type generic, total addresses 3 , allocated 1 (33%), misses 0

```

- **A standard access list numbered 1 was used as part of the configuration process.**
- **Two types of NAT are enabled.**
- One port on the router is not participating in the address translation.
- **Address translation is working.**
- Three addresses from the NAT pool are being used by hosts.
- The name of the NAT pool is refCount.

Explanation: The show ip nat statistics , show ip nat translations , and debug ip nat commands are useful in determining if NAT is working and also useful in troubleshooting problems that are associated with NAT. NAT is working, as shown by the hits and misses count. Because there are four misses, a problem might be evident. The standard access list numbered 1 is being used and the translation pool is named NAT as evidenced by the last line of the output. Both static NAT and NAT overload are used as seen in the Total translations line.

17. Refer to the exhibit. What statement is true about the output of the show standby command?

```

Router# show standby

Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
  Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
  Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec

```

- **The router is currently forwarding packets.**
- This router is tracking two properly operating interfaces.
- The current priority of this router is 120.
- This router is in the HSRP down state because its tracked interfaces are down.

Explanation: The output shows that the active router is local and indicates that this router is the active router and is currently forwarding packets.

18. Match the step number to the sequence of stages that occur during the HSRP failover process. (Not all options are used.)

Step 1	The new forwarding router assumes both the IP and MAC addresses of the virtual router. <input type="text"/>
Step 2	
Step 3	
Step 4	

The host initiates an ARP request.

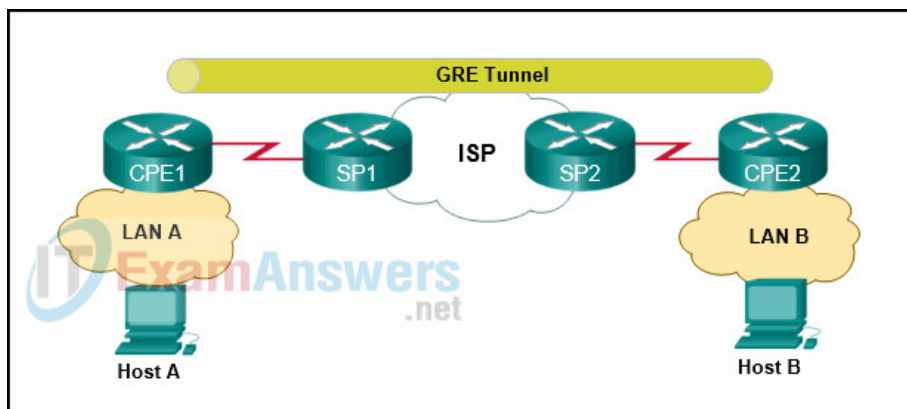
The standby router assumes the role of the forwarding router.

The forwarding router fails.

The standby router stops seeing hello messages from the forwarding router.

Explanation: Hot Standby Router Protocol (HSRP) is a Cisco-proprietary protocol that is designed to allow for transparent failover of a first-hop IPv4 device.

19. Refer to the exhibit. An organization has two remote sites which are connected by a GRE tunnel through an ISP cloud network. The organization has two routers (CPE1 and CPE2) at each of the remote sites which connect to the ISP routers, SP1 and SP2. Which two nodes are the GRE tunnel endpoints to connect the two remote sites? (Choose two.)



- Host A
- CPE1
- SP1
- SP2
- CPE2
- Host B

Explanation: The GRE tunnel is a private tunnel set up by the organization to connect the two remote sites across the ISP network. The organization would need to configure the two routers at the remote sites, CPE1 and CPE2, to the tunnel endpoints of the tunnel.

20. Which protocol creates a virtual point-to-point connection to tunnel unencrypted traffic between Cisco routers from a variety of protocols?

- GRE
- IKE
- OSPF
- IPsec

Explanation: Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that encapsulates multiprotocol traffic between remote Cisco routers. GRE does not encrypt data. OSPF is an open source routing protocol. IPsec is a suite of protocols that allow for the exchange of information that can be encrypted and verified. Internet Key Exchange (IKE) is a key management standard used with IPsec.

21. How many bytes of overhead are added to each IP packet while it is transported through a GRE tunnel?

- 8
- 32
- 16
- **24**

Explanation: A packet that is sent over a GRE tunnel is encapsulated with a GRE header and the tunneling IP header, which combined add an additional 24 bytes to the original packet.

22. Refer to the exhibit. Which IP address is configured on the physical interface of the CORP router?

```
CORP# show interface Tunnel1
Tunnel1 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 10.1.1.1/30
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 209.165.202.133, destination 209.165.202.134
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
<output omitted>
```

- 10.1.1.2
- 209.165.202.134
- **209.165.202.133**
- 10.1.1.1

Explanation: The tunnel source and tunnel destination addresses reference the IP addresses of the physical interfaces on the local and remote routers respectively.

23. What is an IPsec protocol that provides data confidentiality and authentication for IP packets?

- IKE
- RSA
- **ESP**
- AH

Explanation: AH (Authentication Header) does not provide confidentiality for IP packets but rather provides data authentication and integrity. ESP (Encapsulating Security Payload) does provide confidentiality and authentication by encrypting the IP packet. RSA is a cryptosystem used in IKE (Internet Key Exchange).

24. What two encryption algorithms are used in IPsec VPNs? (Choose two.)

- PSK
- **3DES**
- IKE
- DH
- **AES**

Explanation: Advanced Encryption Algorithm (AES) and Triple DES (3DES) are encryption algorithms used for IPsec. Diffie-Hellman (DH), Pre-shared Keys (PSK), and Internet Key Exchange (IKE) are all encryption key mechanisms.

25. Which two identification methods are used by LISP instead of traditional IP addresses? (Choose two.)

- xTR
- **RLOCs**
- MRs
- PxTRs
- **EIDs**

Explanation: As part of the routing architecture, LISP separates IP addresses into endpoint identifiers (EIDs) and routing locators (RLOCs) so that endpoints can roam from site to site and only the RLOC changes. The EID stays the same.

26. Which LISP header is used to provide a secure boundary between multiple organizations?

- outer LISP UDP header
- outer LISP IP header
- **Instance ID**
- RLOC

Explanation: The 24-bit Instance ID field is a value used to provide device- and path-level network virtualization to prevent IP address duplication within a LISP site or provide a secure boundary between multiple organizations.

27. How is routing handled within a LISP site?

- through the use of virtual tunnels
- through the use of virtual controllers
- **through the use of an interior routing protocol**
- through the use of RLOCs

Explanation: With any one particular LISP site, the process of routing packets between devices at that site is handled by any interior routing protocol such as RIP, OSPF, or EIGRP.

28. What is the purpose of a VNI when a company is using VXLANs?

- to map Layer 2 to Layer 3 packets
- to facilitate the discovery of underlay Layer 3 networks
- **to uniquely identify overlay networks**
- to create a database of EID-to-RLOC mappings

Explanation: A 24-bit VXLAN network identifier (VNI) allows up to 16 million VXLAN segments, also known as overlay networks, to coexist within the same infrastructure.

29. What is the purpose of VTEPs when using VXLANs?

- propagate map replies to end devices
- **originate or terminate tunnels**
- identify virtual segments within an organization

- provide replies to internal devices when an external device is cloud-based

Explanation: Virtual tunnel endpoints (VTEPs) originate or terminate VXLAN tunnels and map Layer 2 and Layer 3 packets to the VNI to be used in the overlay network.

30. What are three characteristics of the generic routing encapsulation (GRE) protocol? (Choose three.)

- Developed by the IETF, GRE is a secure tunneling protocol that was designed for Cisco routers.
- **By default, GRE does not include any flow control mechanisms.**
- GRE provides encapsulation for a single protocol type that is traveling through the VPN.
- **GRE tunnels support multicast traffic.**
- GRE uses AES for encryption unless otherwise specified.
- **GRE creates additional overhead for packets that are traveling through the VPN.**

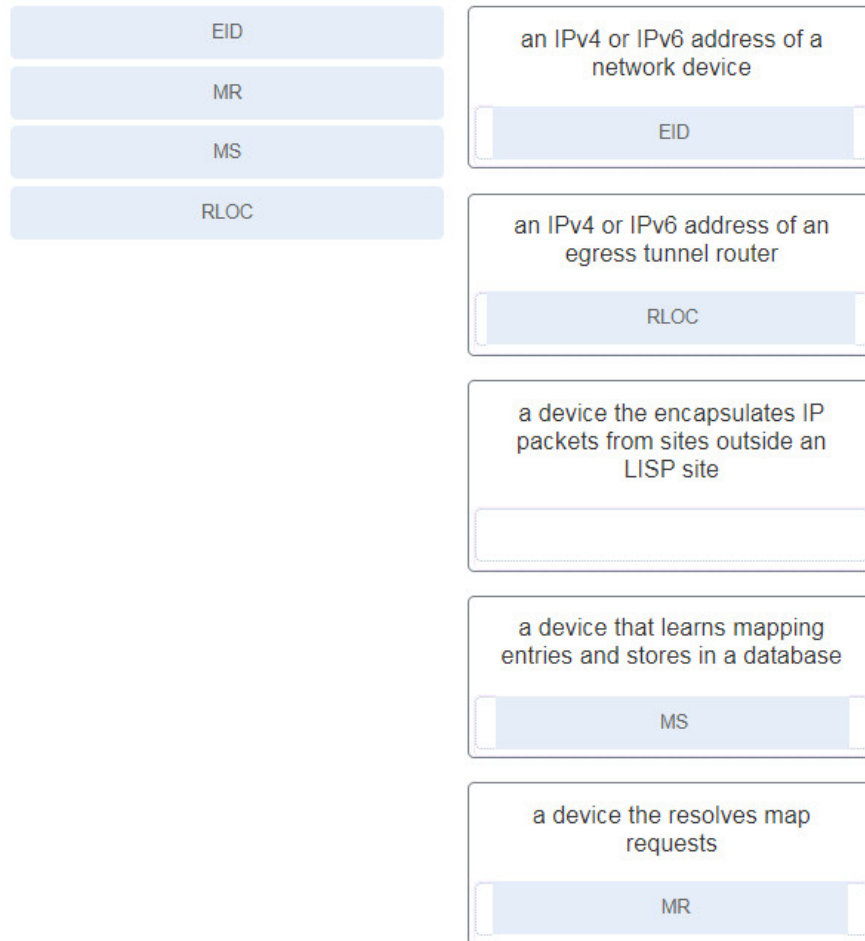
Explanation: GRE was developed by Cisco and encapsulates a wide variety of protocol packet types inside IP tunnels. GRE is stateless and does not include any flow control mechanisms by default. GRE is defined in an IETF standard. GRE does not include any strong security mechanisms to protect the traffic that crosses the site-to-site VPN. GRE supports routing protocols by using multicast traffic as a carrier protocol. GRE headers and the tunneling IP header create additional overhead for tunneled packets. GRE provides encapsulation for multiple protocol types inside an IP tunnel.

31. By the use of sequence numbers, which function of the IPsec security services prevents spoofing by verifying that each packet is non-duplicated and unique?

- **anti-replay protection**
- confidentiality
- authentication
- data integrity

Explanation: Anti-replay protection is the ability to detect and reject replayed packets. By comparing sequence numbers, it helps prevent spoofing by verifying that each packet is unique and not duplicated. Authentication verifies the identity of the source of the data that is sent. Confidentiality is the process of taking all the data that one computer is sending to another and encoding it into a form that only the other computer will be able to decode. Data integrity is achieved by IPsec because the receiver can verify that the data was transmitted through the Internet without being changed or altered in any way.

32. Match the LISP term to the definition. (Not all options are used.)



33. What is the purpose of a proxy ETR used with LISP?

- to communicate with a non-LISP site
- to send map request packets to the MR on behalf of an ETR
- to perform a DNS lookup for any EID within an LISP site
- to register any EID addresses that are not within the mapping database

Explanation: A proxy egress tunnel router (PETR) is a router that connects to a non-LISP site such as to the Internet or a data center when a LISP site needs to communicate to a non-LISP site.

34. Which algorithm is considered insecure for use in IPsec encryption?

- AES
- **3DES**
- SHA-1
- RSA

Explanation: Both DES and 3DES are considered to be too insecure to be used in IPsec encryption. AES is the recommended encryption algorithm. SHA-1 is a hashing algorithm and RSA is used during the initial key exchange.

35. Refer to the exhibit. What algorithm is being used to provide public key exchange?

```
Router1(config)# crypto isakmp policy 1
Router1(config-isakmp)# hash sha
Router1(config-isakmp)# authentication pre-share
Router1(config-isakmp)# group 24
Router1(config-isakmp)# lifetime 3600
Router1(config-isakmp)# encryption aes 256
Router1(config-isakmp)# end
```

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

Explanation: The IPsec framework uses various protocols and algorithms to provide data confidentiality, data integrity, authentication, and secure key exchange. DH (Diffie-Hellman) is an algorithm used for key exchange. DH is a public key exchange method and allows two IPsec peers to establish a shared secret key over an insecure channel.

36. What is the first step in establishing an IPsec VPN?

- creation of a secure tunnel to negotiate a security association policy
- **detection of interesting traffic**
- negotiation of ISAKMP policies
- creation of an IPsec tunnel between two IPsec peers

Explanation: Before an IPsec tunnel can be configured, interesting traffic must be detected. Interesting traffic is defined by an access list permit statement. Once interesting traffic is detected, by matching the access list, IKE phase 1 negotiations can begin that will establish the tunnel.