QUESTION 27
An engineer is trying to copy an IOS file from one router to another router by using TFTP.
Which two actions are needed to allow the file to copy? (Choose two.)

A. Configure the TFTP authentication on the source router with the tftp-server authentication local command.
B. Configure a user on the source router with the username tftp password tftp command.
C. Enable the TFTP server on the source router with the tftp-server flash:<filename> command.
D. TFTP is not supported in recent IOS versions, so an alternative method must be used.
E. Copy the file to the destination router with the copy tftp: flash: command

Answer: CE
Explanation:
Below are the steps to follow for copying the Cisco IOS software image from a router acting as TFTP server to another router.
1. Check the image size on Router1 with the show flash command.
2. Check the image size on Router2 with the show flash command to verify if enough space is available on Router2 for the system image file to be copied.
3. Configure Router1 as the TFTP server: Router1(config)#tftp-server flash:/c2500-js-l.122-10b
4. When the TFTP server is configured, download the specified image from Router1 to Router2 using the copy tftp flash command.
Reference: https://www.cisco.com/c/en/us/support/docs/routers/2500-series-routers/15092-copyimage.html

QUESTION 28
Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two.)

A. DMVPN
B. MPLS VPN
C. Virtual Tunnel Interface (VTI)
D. SSL VPN
E. PPPoE

Answer: AC
Explanation:
IP security (IPsec) virtual tunnel interfaces (VTIs) provide a routable interface type for terminating IPsec tunnels and an easy way to define protection between sites to form an overlay network. IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and simplify network management and load balancing.

QUESTION 29

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

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

Answer: D
Explanation:
Next Hop Resolution Protocol (NHRP), defined in RFC 2332, is a Layer 2 address resolution protocol and cache, like Address Resolution Protocol (ARP). NHRP is used by a branch router connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of the "NBMA next hop"; in this case, the headend router or the destination IP address of another branch router.
NHRP is used to map tunnel IP addresses to "physical" or "real" IP addresses, used by endpoint routers. It resolves private addresses (those behind mGRE and optionally IPSEC) to a public address. NHRP is layer 2 resolution protocol and cache, much like Address Resolution Protocol (ARP) or Reverse ARP (Frame Relay).

QUESTION 30
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

Answer: A
Explanation:
An mGRE tunnel inherits the concept of a classic GRE tunnel but an mGRE tunnel does not require a unique tunnel interface for each connection between Hub and spoke like traditional GRE. One mGRE can handle multiple GRE tunnels at the other ends. Unlike classic GRE tunnels, the tunnel destination for a mGRE tunnel does not have to be configured; and all tunnels on Spokes connecting to mGRE interface of the Hub can use the same subnet.

QUESTION 31
Which option is the best for protecting CPU utilization on a device?

A. fragmentation
B. COPP
C. ICMP redirects
D. ICMP unreachable messages

Answer: B
Explanation:
The traffic managed by a device can be divided into three functional components or planes:
+ Data plane
+ Management plane
+ Control plane
The vast majority of traffic flows through the device via the data plane; however, the route processor handles certain traffic, such as routing protocol updates, remote-access services, and network management traffic such as SNMP. This type of traffic is referred to as the control and management plane. The route processor is critical to network operation. Therefore any service disruption or security compromise to the route processor, and hence the control and management planes, can result in network outages that impact regular operations. For example, a DoS attack targeting the route processor typically involves high bursty traffic resulting in excessive CPU utilization on the route processor. Such attacks can be devastating to network stability and availability. The bulk of traffic managed by the route processor is handled by way of the control and management planes.
The CoPP feature is used to protect the aforementioned control and management planes; to ensure stability, reachability, and availability and to block unnecessary or DoS traffic. CoPP uses a dedicated control plane

configuration through the modular QoS CLI (MQC) to provide filtering and rate limiting capabilities for the control plane packets.
Reference: https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=10

QUESTION 32
Which transport layer protocol is used to form LDP sessions?

A. UDP
B. SCTP
C. TCP
D. RDP

Answer: C
Explanation:
LDP uses TCP as a reliable transport for sessions. When multiple LDP sessions are required between two LSRs, there is one TCP session for each LDP session.
Reference: https://tools.ietf.org/html/rfc5036

QUESTION 33
R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:

```
ip prefix-list test seq 5 permit 192.168.130.0/24
!
route-map OUT permit10
match ip address prefix-list test
set as-path prepend 65000
```

What is the result when the route-map OUT command is applied toward an eBGP neighbor R1 (1.1.1.1) by using the neighbor 1.1.1.1 route-map OUT out command?

A. R1 sees 192.168.130.0/24 as two hops away instead of one AS hop away
B. R1 does not forward traffic that is destined for 192.168.130.0/24.
C. Network 192.168.130.0/24 is not allowed in the R1 table.
D. R1 does not accept any route other than 192.168.130.0/24.

Answer: A
Explanation:
AS-Path prepending is a way to manipulate the AS-Path attribute of a BGP route. It allows prepending multiple entries of AS to a BGP route.

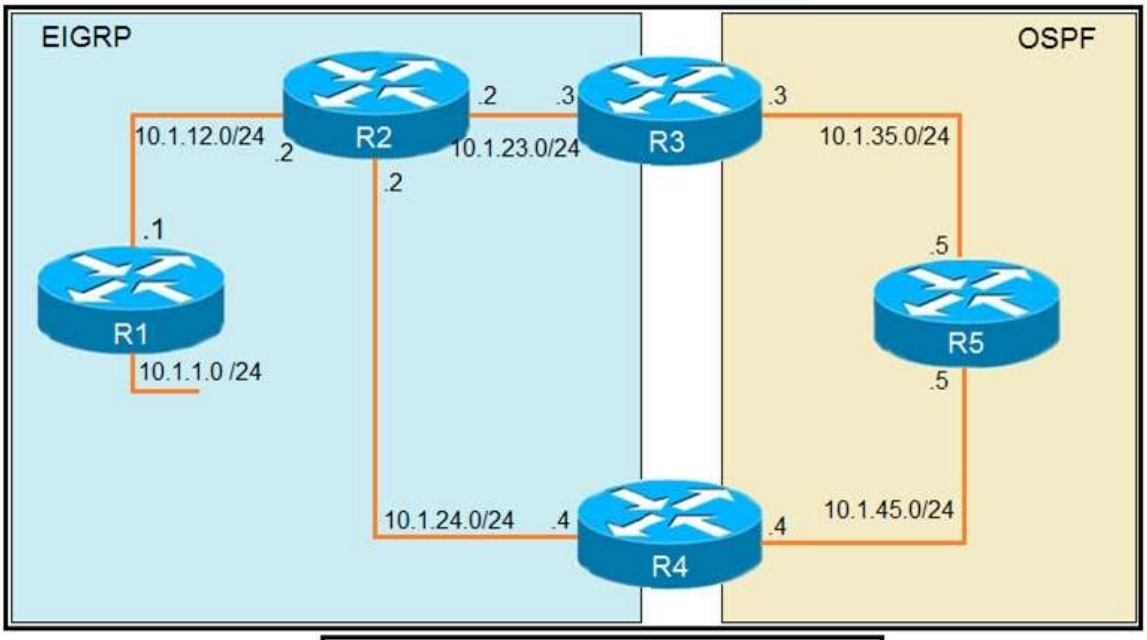
QUESTION 34
Refer to the exhibit. Network operations cannot read or write an configuration on the device with this configuration from the operation subnet. Which two configuration fix the issue? (Choose two.)

```
snmp-server community ciscotest1
snmp-server host 192.168.1.128 ciscotest
snmp-sever enable traps bgp
```

A. Configure SNMP rw permission in addition to community ciscotest.
B. Modify access list 1 and allow operations subnet in the access list.
C. Modify SNMP rw permission in addition to version 1.
D. Configure SNMP rw permission in addition to version 1.
E. Configure SNMP rw permission in addition to community ciscotest 1.

Answer: AB

QUESTION 35
Refer to the exhibit. The output of the trace route from R5 shows a loop in the network.
Which configuration prevents this loop?




```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0

R3
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
 network 10.1.45.4 0.0.0.0 area 0

R5#traceroute 10.1.1.1

Type escape sequence to abort.
Tracing the route to 10.1.1.1

 1 10.1.35.3 80 msec 44 msec 20 msec
 2 10.1.23.2 44 msec 104 msec 64 msec
 3 10.1.24.4 44 msec 64 msec 40 msec
 4 10.1.45.5 24 msec 40 msec 20 msec
 5 10.1.35.3 92 msec 144 msec 148 msec
 6 10.1.23.2 108 msec 76 msec 80 msec
        <output truncuated>
```

A.
```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

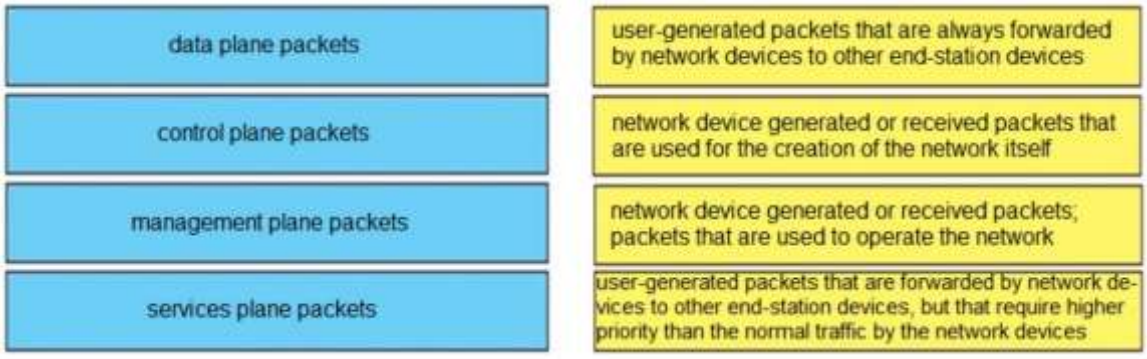
B.
```
R3
router eigrp 1
 redistribute OSPF 1 route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
 network 10.1.24.4 0.0.0.0
!
route-map FILTER-TAG deny 10
 match tag 1
!
route-map FILTER-TAG permit 20
```

C.
```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG permit 10
 match tag 1
```

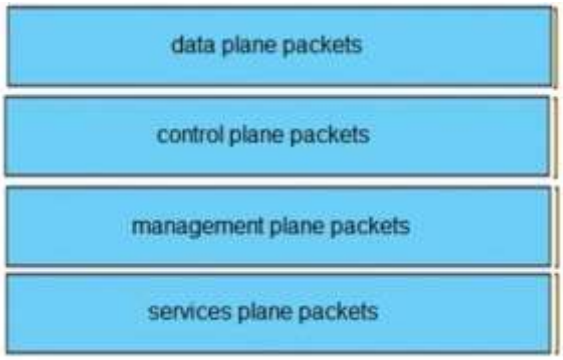
D.
```
R3
router ospf 1
 redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG deny 10
 set tag 1

R4
router eigrp 1
 redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
 match tag 1
```

Answer: A

QUESTION 36
Drag and Drop Question
Drag and drop the packet from the left onto the correct descriptions on the right.

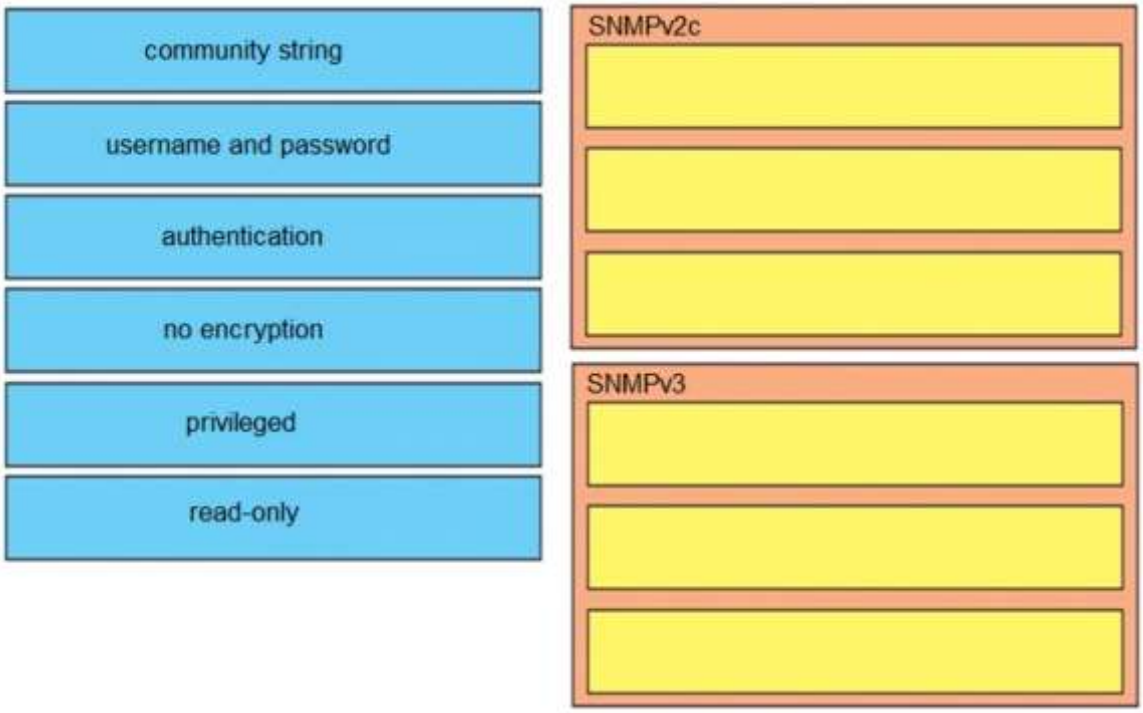


Answer:

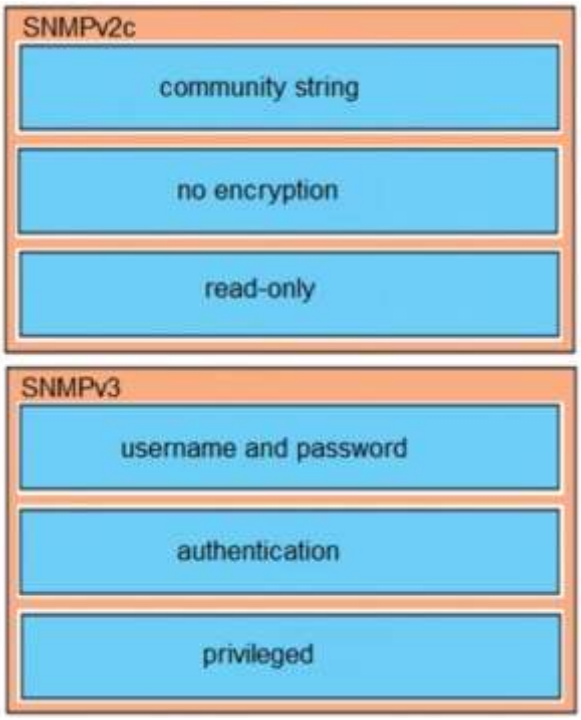


Explanation:
Unlike legacy network technologies such as ISDN, Frame Relay, and ATM that defined separate data and control channels, IP carries all packets within a single pipe. Thus, IP network devices such as routers and switches must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately.
From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
1. Data plane packets – End-station, user-generated packets that are always forwarded by network devices to other end-station devices. From the perspective of the network device, data plane packets always have a transit destination IP address and can be handled by normal, destination IP address-based forwarding processes.
2. Control plane packets – Network device generated or received packets that are used for the creation and operation of the network itself. From the perspective of the network device, control plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as ARP, BGP, OSPF, and other protocols that glue the network together.
3. Management plane packets – Network device generated or received packets, or management station generated or received packets that are used to manage the network. From the perspective of the network device, management plane packets always have a receive destination IP address and are handled by the CPU in the network device route processor. Examples include protocols such as Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network.
4. Services plane packets – A special case of data plane packets, services plane packets are also user-generated packets that are also forwarded by network devices to other end-station devices, but that require high-touch handling by the network device (above and beyond normal, destination IP address-based forwarding) to forward the packet. Examples of high-touch handling include such functions as GRE encapsulation, QoS, MPLS VPNs, and SSL/IPsec encryption/decryption, etc. From the perspective of the network device, services plane packets may have a transit destination IP address, or may have a receive destination IP address (for example, in the case of a VPN tunnel endpoint).
Reference: https://tools.cisco.com/security/center/resources/copp_best_practices

QUESTION 37
Drag and Drop Question
Drag and drop the SNMP attributes in Cisco IOS devices from the onto he correct SNMPv2c or SNMPv3 categories on the right.



Answer:



Explanation:
Both SNMPv1 and v2 did not focus much on security and they provide security based on community string only. Community string is really just a clear text password (without encryption). Any data sent in clear text over a network is vulnerable to packet sniffing and interception. There are two types of community strings in SNMPv2c:
+ Read-only (RO): gives read-only access to the MIB objects which is safer and preferred to other method.
+ Read-write (RW): gives read and write access to the MIB objects. This method allows SNMP Manager to change the configuration of the managed router/switch so be careful with this type.
The community string defined on the SNMP Manager must match one of the community strings on the Agents in order for the Manager to access the Agents.

SNMPv3 provides significant enhancements to address the security weaknesses existing in the earlier versions. The concept of community string does not exist in this version. SNMPv3 provides a far more secure communication using entities, users and groups. This is achieved by implementing three new major features:
+ Message integrity: ensuring that a packet has not been modified in transit.
+ Authentication: by using password hashing (based on the HMAC-MD5 or HMAC-SHA algorithms) to ensure the message is from a valid source on the network.
+ Privacy (Encryption): by using encryption (56-bit DES encryption, for example) to encrypt the contents of a packet.