**Exam : Cisco 350-018**

**Title :** CCIE Pre-Qualification Test for Security

**Update :** Demo

1. How do TCP SYN attacks take advantage of TCP to prevent new connections from being established to a host under attack?

A. These attacks send multiple FIN segments forcing TCP connection release.

B. These attacks fill up a hosts' listen queue by failing to ACK partially opened TCP connections.

C. These attacks take advantage of the hosts transmit backoff algorithm by sending jam signals to the host.

D. These attacks increment the ISN of each segment by a random number causing constant TCP retransmissions.

E. These attacks send TCP RST segments in response to connection SYN+ACK segments forcing SYN retransmissions.

Answer: B

2. What are two key characteristics of VTP? (Choose 2)

A. VTP messages are sent out all switch-switch connections.

B. VTP L2 messages are communicated to neighbors using CDP.

C. VTP manages addition, deletion, and renaming of VLANs 1 to 4094.

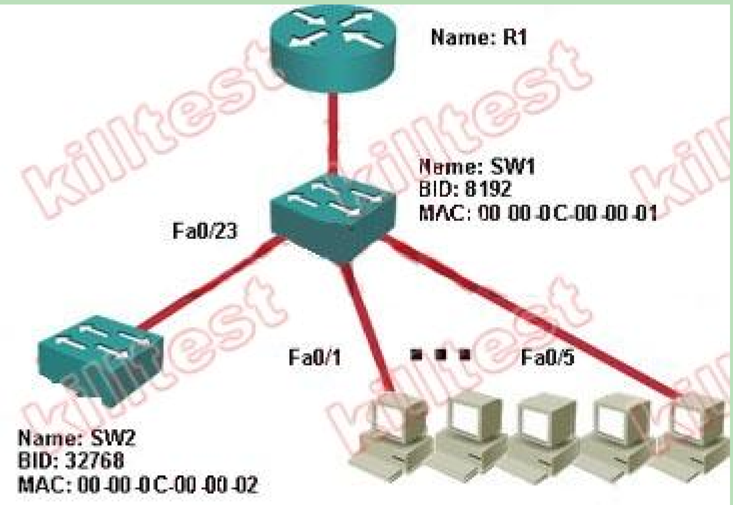
D. VTP pruning restricts flooded traffic, increasing available bandwidth.

E. VTP V2 can only be used in a domain consisting of V2 capable switches.

F. VTP V2 performs consistency checks on all sources of VLAN information.

Answer: DE

3. Refer to the Exhibit. Switch SW2 has just been added to FastEthernet 0/23 on SW1. After a few seconds, interface Fa0/23 on SW1 is placed in the error-disabled state. SW2 is removed from port 0/23 and inserted into SW1 port Fa0/22 with the same result. What is the most likely cause of this problem?



A. The spanning-tree portfast feature has been configured on SW1.

B. BPDU filtering has been enabled either globally or on the interfaces of SW1.

C. The BPDU guard feature has been enabled on the FastEthernet interfaces of SW1.

D. The FastEthernet interfaces of SW1 are unable to auto-negotiate speed and duplex with SW2.

E. PAgP is unable to correctly negotiate VLAN trunk characteristics on the link between SW1 and SW2.

Answer: C

4. What are two important guidelines to follow when implementing VTP? (Choose 2)

A. CDP must be enabled on all switches in the VTP management domain.

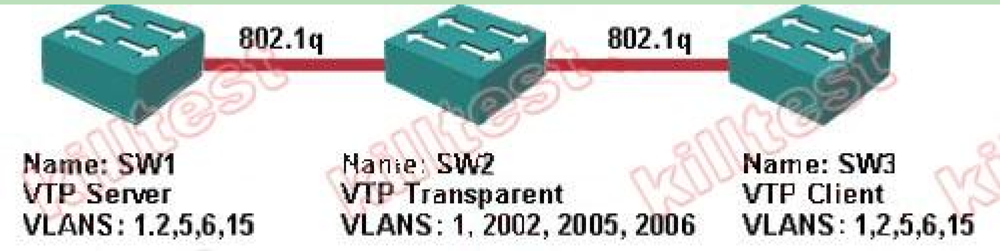
B. All switches in the VTP domain must run the same version of VTP.

C. When using secure mode VTP, only configure management domain passwords on VTP servers.

D. Enabling VTP pruning on a server will enable the feature for the entire management domain. E. Use of the VTP multi-domain feature should be restricted to migration and temporary implementation.

Answer: BD

5. Refer to the Exhibit. The Cisco IOS-based switches are configured with VTP and VLANs as shown. The network administrator wants to quickly add the VLANs defined on SW1 to SW2's configuration and so he copies the vlan.dat file from the flash on SW1 to the flash of SW2. After the file is copied to SW2, it is rebooted. What is the VLAN status of SW2 after the reboot?



A. The VLAN information on SW2 will remain the same since it has been configured for transparent VTP mode.

B. SW2 will clear the vlan.dat file and load its VLAN information from the configuration file stored in NVRAM.

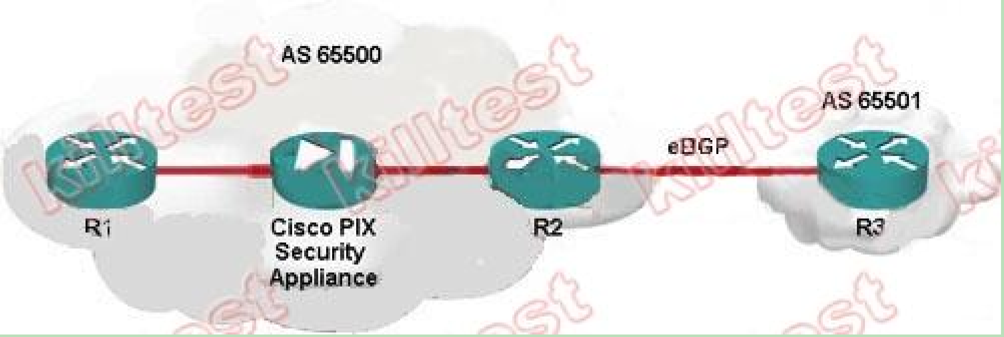
C. A VTP mode mismatch will occur causing the VLANS in the startup config to be ignored and all VLANs above 1005 to be erased.

D. The VLANs in the vlan.dat file will be copied to the running config and merged with the extended VLANs defined in the startup config.

E. All VLANs will be erased and all ports will be moved into the default VLAN 1.

Answer: C

6. Refer to the Exhibit. A Cisco security appliance has been inserted between routers R1 and R2 for security reasons. Unfortunately, BGP stopped working after the appliance was inserted in the network. What three configuration tasks must be completed to restore BGP connectivity? (Choose 3)



A. Configure BGP on the security appliance as an iBGP peer to R1 and R2 in AS 65500.

B. Configure a static NAT translation to allow inbound TCP connections from R2 to R1.

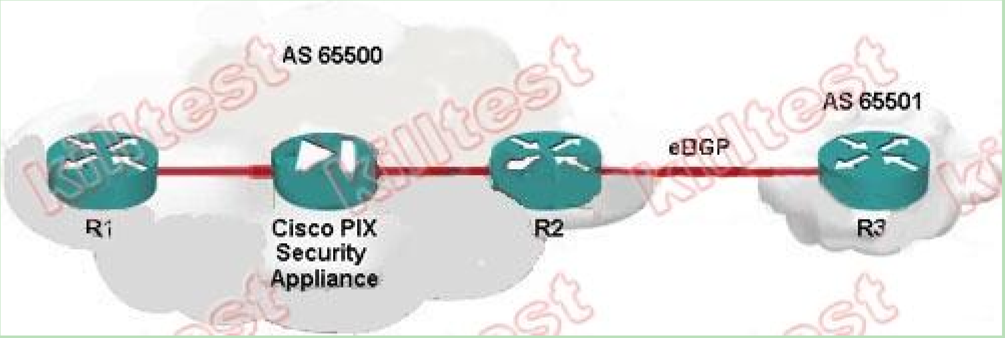
C. Configure an ACL on the security appliance allowing TCP, port 179 between R1 and R2.

D. Configure a static routes on R1 and R2 using the appliance inside and outside interfaces as gateways.

E. Configure the BGP fixup feature on the security appliance to permit BGP TCP connections between R1 and R2.

Answer: BCD

7. Refer to the Exhibit. A Cisco security appliance has been correctly configured and inserted between routers R1 and R2. The security appliance allows iBGP connectivity between R1 and R2 and BGP is fully functional. To increase security, MD5 neighbor authentication is correctly configured on R1 and R2. Unfortunately, BGP stops working after the MD5 configuration is added. What configuration task must be completed on the security appliance to restore BGP connectivity?



A. Configure authentication-proxy on the security appliance.

B. Configure the MD5 authentication key on the security appliance.

C. Add the MD5 key to the security appliance BGP fixup configuration.

D. Add norandomseq to the static NAT translation on the security appliance.

E. Configure a GRE tunnel to allow authenticated BGP connections to traverse the security appliance.

Answer: D

8. According to RFC 3180, what is the correct GLOP address for AS 456?

A. 224.0.4.86

B. 224.4.86.0

C. 233.1.200.0

D. 239.2.213.0

E. 239.4.5.6

Answer: C

9. A network administrator is using a LAN analyzer to troubleshoot OSPF router exchange messages sent to ALL OSPF ROUTERS. To what MAC address are these messages sent?

A. 00-00-1C-EF-00-00

B. 01-00-5E-00-00-05

C. 01-00-5E-EF-00-00

D. EF-FF-FF-00-00-05

E. EF-00-00-FF-FF-FF F. FF-FF-FF-FF-FF-FF

Answer: B

10.Which two IP multicast addresses belong to the group represented by the MAC address of 0x01-00-5E-15-6A-2C?

A. 224.21.106.44

B. 224.25.106.44

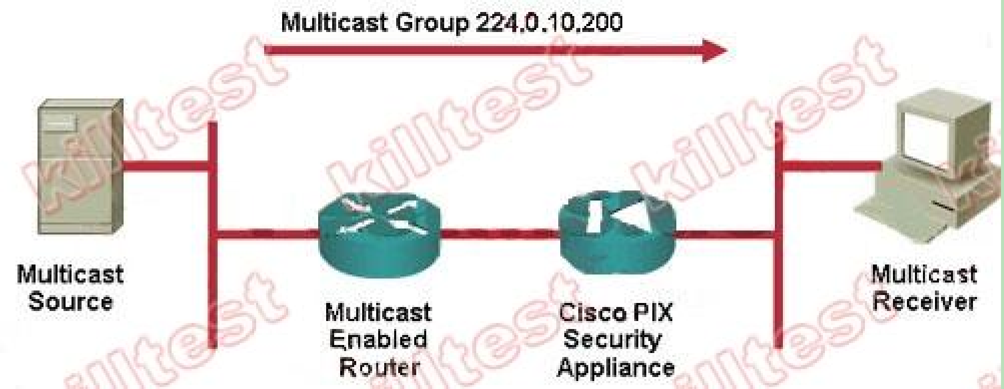
C. 233.149.106.44

D. 236.25.106.44

E. 239.153.106.44

Answer: AC

11. Refer to the Exhibit. A Cisco security appliance has been inserted between a multicast source and its receiver, preventing multicast traffic between them. What is the best solution to address this problem?



A. Configure the security appliance as an IGMP multicast client.

B. Configure a GRE tunnel to allow the multicast traffic to bypass the security appliance.

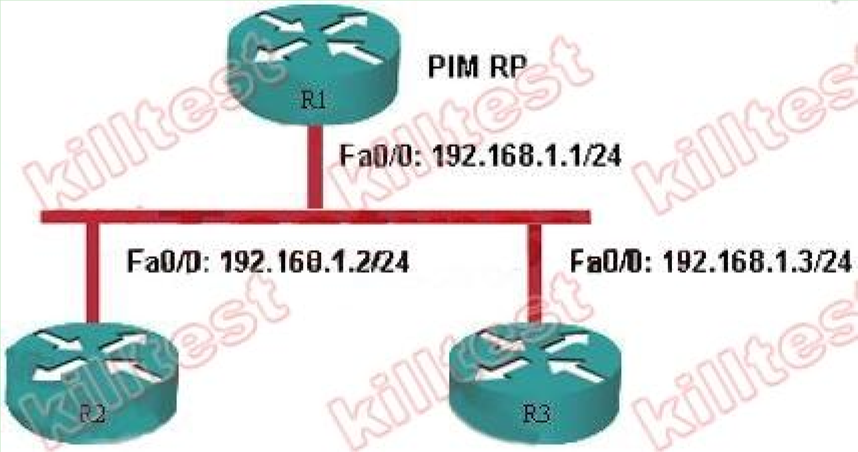
C. Configure the security appliance as the rendezvous point of the multicast network so that all (*,G) trees traverse it.

D. Create a static route on the multicast source and receiver pointing to the outside and inside interfaces of the security appliance respectively.

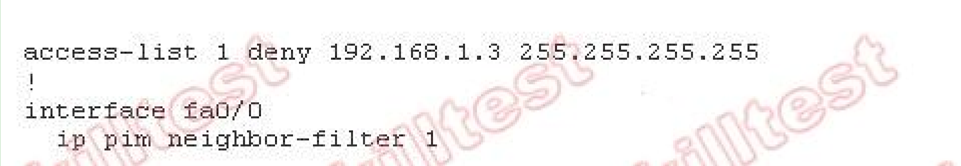
E. Configure SMR so the security appliance becomes an IGMP proxy agent, forwarding IGMP messages from hosts to the upstream multicast router.

Answer: E

12. Refer to the Exhibit. Which of the following R1 router configurations will correctly prevent R3 from becoming a PIM neighbor with rendezvous point R1?

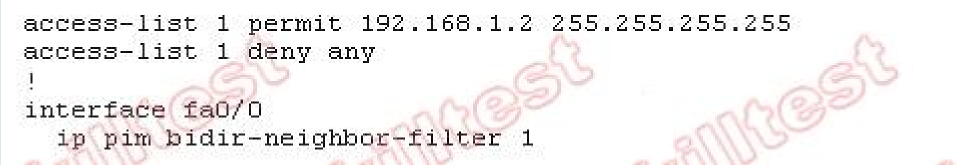


A.



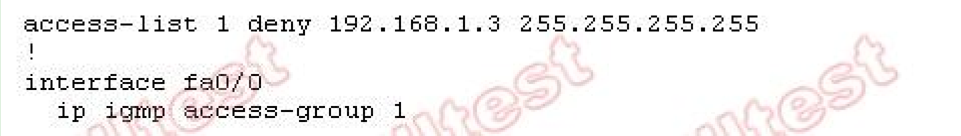
```
access-list 1 deny 192.168.1.3 255.255.255.255
!
interface fa0/0
  ip pim neighbor-filter 1
```

B.



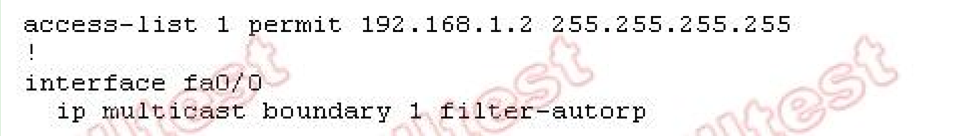
```
access-list 1 permit 192.168.1.2 255.255.255.255
access-list 1 deny any
!
interface fa0/0
  ip pim bidir-neighbor-filter 1
```

C.



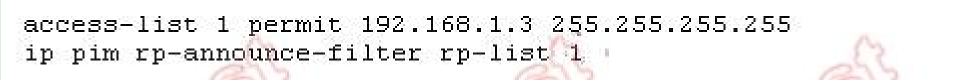
```
access-list 1 deny 192.168.1.3 255.255.255.255
!
interface fa0/0
  ip igmp access-group 1
```

D.



```
access-list 1 permit 192.168.1.2 255.255.255.255
!
interface fa0/0
  ip multicast boundary 1 filter-autorp
```

E.



```
access-list 1 permit 192.168.1.3 255.255.255.255
ip pim rp-announce-filter rp-list 1
```

Answer: A

13. How is the Cisco sensor software version 5.0 different from the version 4.0 release?

A. The monitoring system pulls events from the sensor

B. The sensor supports intrusion prevention functinality

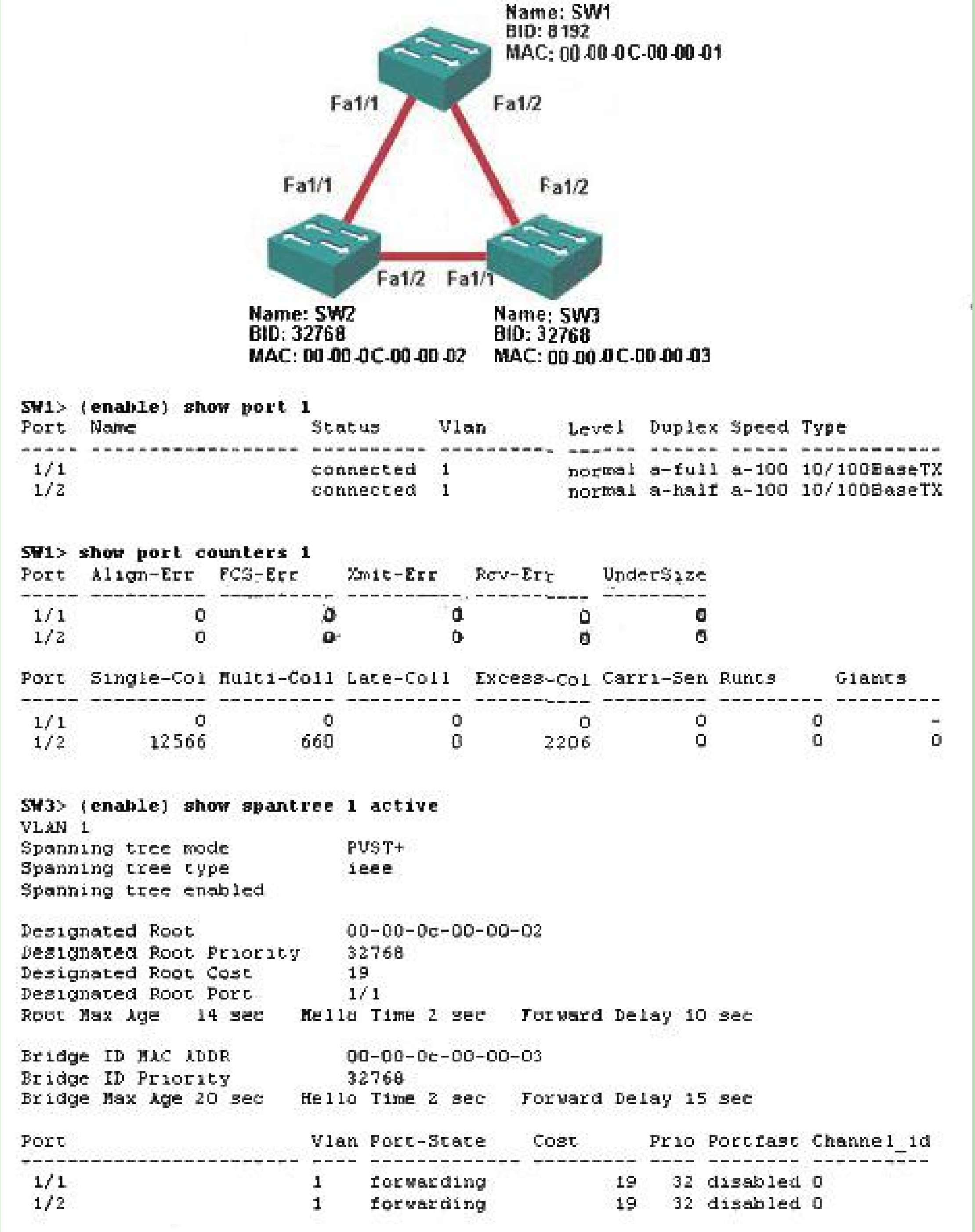
C. The sensor pushes events to the monitoring system

D. The sensor uses RDEP E. The sensor software calculates a Risk Rating for alerts to reduce false

positives
Answer: BE

14. What is SDEE?
A. A Cisco proprietary protocol to transfer IDS events across the network
B. A protocol used by multiple vendors to transmit IDS events across the network
C. A queuing mechanism to store alerts
D. A mechanism to securely encode intrusion events in an event store E. A multi-purpose encryption engine to symmetrically encrpt data across the network
Answer: B

15. Refer to the Exhibit. Under normal conditions, SW1 is spanning tree root and the link between SW2 and SW3 is in the blocking state. This network transports large amounts of traffic and is heavily loaded. After a software upgrade to these switches, users are complaining about slow performance. To troubleshoot, the commands shown in the exhibit are entered. What two are the most likely causes of this



```
SW1> (enable) show port 1
Port  Name               Status     Vlan       Level  Duplex Speed Type
----- ------------------ ---------- ---------- ------ ------ ----- ------------
 1/1                     connected  1          normal a-full a-100 10/100BaseTX
 1/2                     connected  1          normal a-half a-100 10/100BaseTX


SW1> show port counters 1
Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 1/1           0          0          0          0         0
 1/2           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 1/1           0          0          0          0         0         0         -
 1/2       12566        660          0       2206         0         0         0


SW3> (enable) show spantree 1 active
VLAN 1
Spanning tree mode          PVST+
Spanning tree type          ieee
Spanning tree enabled

Designated Root             00-00-0c-00-00-02
Designated Root Priority    32768
Designated Root Cost        19
Designated Root Port        1/1
Root Max Age   14 sec   Hello Time 2 sec   Forward Delay 10 sec

Bridge ID MAC ADDR          00-00-0c-00-00-03
Bridge ID Priority          32768
Bridge Max Age 20 sec   Hello Time 2 sec   Forward Delay 15 sec

Port                     Vlan Port-State    Cost      Prio Portfast Channel_id
------------------------ ---- ------------- --------- ---- -------- ----------
 1/1                     1    forwarding           19   32 disabled 0
 1/2                     1    forwarding           19   32 disabled 0
```

issue?

A. Lack of BPDUs from high priority bridge SW1 causes SW3 to unblock Fa1/1.

B. Duplex mismatch on the link between SW1 and SW3 causing high rate of collisions.

C. The Max Age timers on SW1 and SW2 have been changed and no longer match the MAX Age timer on SW3.

D. UDLD has not been configured between SW1 and SW3 so SW3 errantly sees its link to SW1 as up and operational.

E. The bridge priority of SW1 was changed to be greater than 32768 allowing SW2 to become the new root of the spanning tree.

Answer: AB

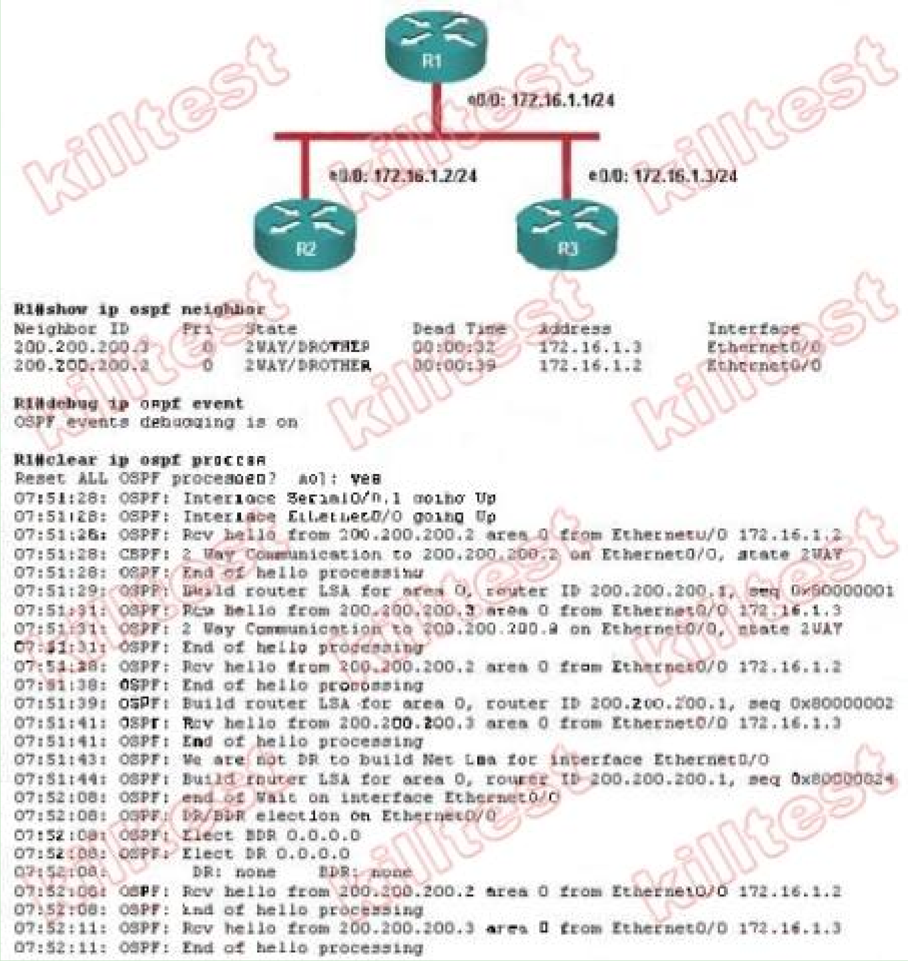
16. What is true about a Pre-Block ACL configured when setting up your sensor to perform IP Blocking?
A. The Pre-Block ACL is overwritten when a blocking action is initiatied by the sensor
B. The blocking ACL entries generated by the sensor override the Pre-Block ACL entries C. The Pre-Block ACL entries override the blocking ACL entries generated by the sensor D. The Pre-Block ACL is replaced by the Post-Block ACL when a blocking action is initiated by the sensor
E. You can not configure a Pre-Block ACL when configuring IP Blocking on your sensor
Answer: C

17. Which of the following is true about the Cisco IOS-IPS functionality? (Choose 2)
A. The signatures available are built into the IOS code.
B. To update signatures you need to install a new IOS image
C. To activate new signatures you download a new Signature Defiition File (SDF) from Cisco's web site
D. Loading and enabling selected IPS signatures is user configurable
E. Cisco IOS only provides Intrusion Detection functionality
F. Cisco IOS-IPS requires a network module installed in your router running sensor software
Answer: CD

18. What is the main reason for using the "ip ips deny-action ips-interface" IOS command? A. To selectively apply drop actions to specific interfaces
B. To enable IOS to drop traffic for signatures configured with the Drop action
C. To support load-balancing configurations in which traffic can arrive via multiple interfaces
D. This is not a valid IOS command
Answer: C

19. By default, to perform IPS deny actions, where is the ACL applied when using IOS-IPS? A. To the ingress interface of the offending packet
B. To the ingress interface on which IOS-IPS is configured
C. To the egress interface on which IOS-IPS is configured
D. To the egress interface of the offending packet
E. To the ingress interface of the offending packet and the ingress interface on which IOS-IPS is configured
Answer: A

20. Refer to the Exhibit. Router R1 is stuck in 2-WAY state with neighbors R2 and R3. As a result R1 has an incomplete routing table. To troubleshoot the issue, the show and debug commands in the exhibit are entered on R1. Based on the output of these commands what is the most likely cause of this problem?



```
R1#show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
200.200.200.3     0   2WAY/DROTHER    00:00:32    172.16.1.3      Ethernet0/0
200.200.200.2     0   2WAY/DROTHER    00:00:39    172.16.1.2      Ethernet0/0

R1#debug ip ospf event
OSPF events debugging is on

R1#clear ip ospf process
Reset ALL OSPF processes? [no]: yes
07:51:28: OSPF: Interface Serial0/0.1 going Up
07:51:28: OSPF: Interface Ethernet0/0 going Up
07:51:28: OSPF: Rcv hello from 200.200.200.2 area 0 from Ethernet0/0 172.16.1.2
07:51:28: OSPF: 2 Way Communication to 200.200.200.2 on Ethernet0/0, state 2WAY
07:51:28: OSPF: End of hello processing
07:51:29: OSPF: Build router LSA for area 0, router ID 200.200.200.1, seq 0x80000001
07:51:31: OSPF: Rcv hello from 200.200.200.3 area 0 from Ethernet0/0 172.16.1.3
07:51:31: OSPF: 2 Way Communication to 200.200.200.3 on Ethernet0/0, state 2WAY
07:51:31: OSPF: End of hello processing
07:51:38: OSPF: Rcv hello from 200.200.200.2 area 0 from Ethernet0/0 172.16.1.2
07:51:38: OSPF: End of hello processing
07:51:39: OSPF: Build router LSA for area 0, router ID 200.200.200.1, seq 0x80000002
07:51:41: OSPF: Rcv hello from 200.200.200.3 area 0 from Ethernet0/0 172.16.1.3
07:51:41: OSPF: End of hello processing
07:51:43: OSPF: We are not DR to build Net Lsa for interface Ethernet0/0
07:51:44: OSPF: Build router LSA for area 0, router ID 200.200.200.1, seq 0x80000024
07:52:08: OSPF: end of Wait on interface Ethernet0/0
07:52:08: OSPF: DR/BDR election on Ethernet0/0
07:52:08: OSPF: Elect BDR 0.0.0.0
07:52:08: OSPF: Elect DR 0.0.0.0
07:52:08:         DR: none    BDR: none
07:52:08: OSPF: Rcv hello from 200.200.200.2 area 0 from Ethernet0/0 172.16.1.2
07:52:08: OSPF: End of hello processing
07:52:11: OSPF: Rcv hello from 200.200.200.3 area 0 from Ethernet0/0 172.16.1.3
07:52:11: OSPF: End of hello processing
```

A. The hello timers on the segment between these routers do not match.

B. All the routers on the Ethernet segment have been configured with "ip ospf priority 0".

C. R1 can not form an adjacency with R2 or R3 because it does not have a matching authentication key.

D. The Ethernet 0/0 interfaces on these routers are missing the "ip ospf network broadcast" command.

E. The Ethernet 0/0 interface on R1 has been configured with the command, "ip ospf network non-broadcast".

Answer: B

21. What two things must you do on the router before generating an SSH key with the "crypto key generate rsa" IOS command?

A. Configure the SSH version that the router will use

B. Configure the host name of the router

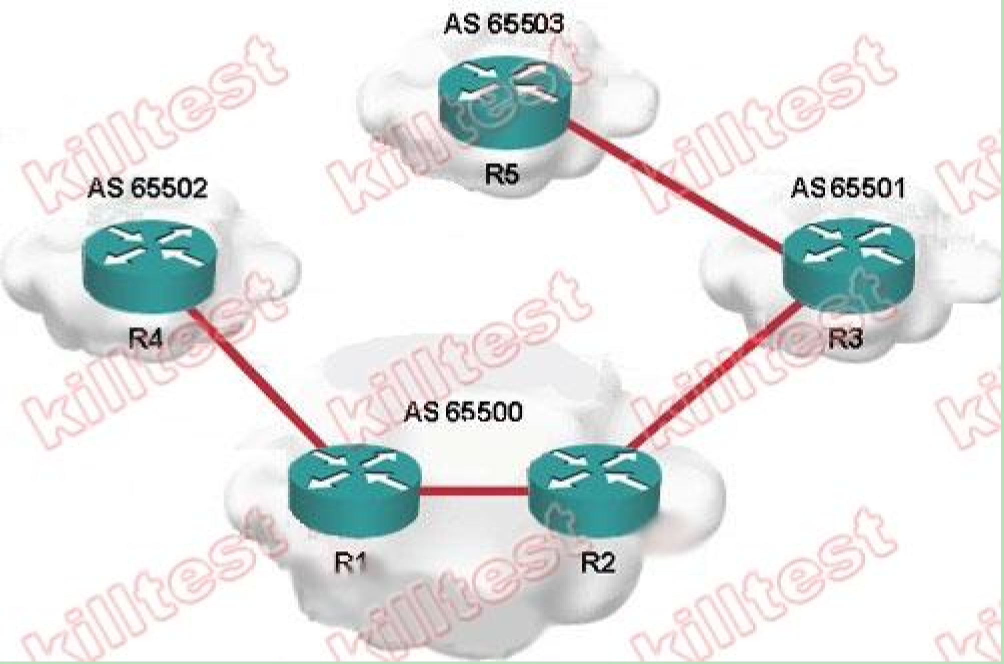
C. Enable AAA Authentication

D. Configure the default IP domain name that the router will use

E. Enable SSH transport support on the vty lines

Answer: BD

22. Refer to the Exhibit. What as-path access-list regular expression should be applied on R2 as a neighbor filter-list to only allow updates with an origin of AS65503?



A. 65503

B. _65503_

C. ^65503$

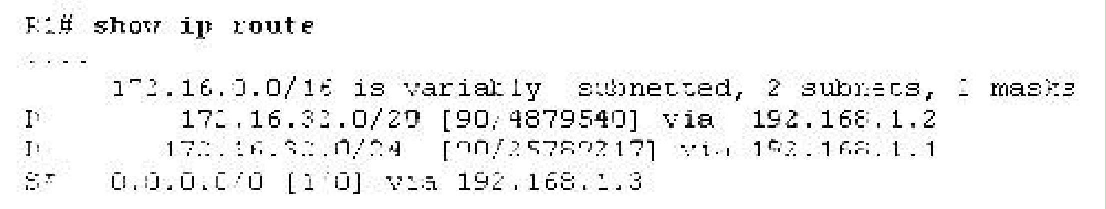
D. _65503$

E. ^65503 .*

F. _65503.?$

Answer: E

23. Refer to the Exhibit. A router running EIGRP with the "no ip classless" command contains the routing table as shown in the exhibit. What will happen to a packet destined for 172.16.254.1?



```
R1# show ip route
....
     172.16.0.0/16 is variably  subnetted, 2 subnets, 2 masks
D        172.16.32.0/20 [90/4879540] via  192.168.1.2
D       172.16.32.0/24  [90/25789217] via 192.168.1.1
S*   0.0.0.0/0 [1/0] via 192.168.1.3
```

A. The packet is forwarded to 192.168.1.1.

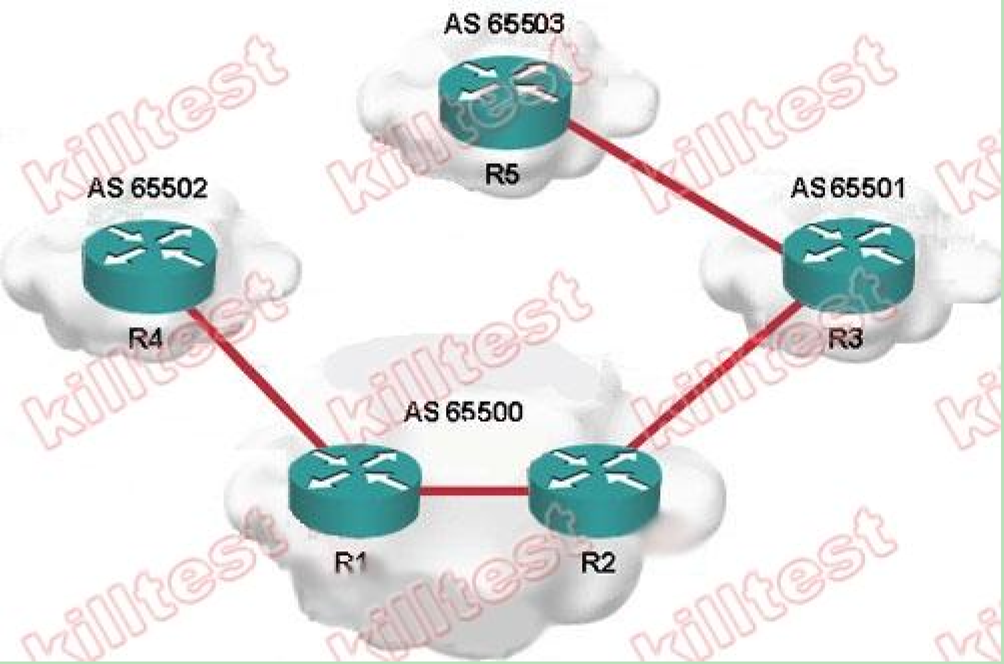
B. The packet is forwarded to 192.168.1.2.

C. The packet is forwarded to 192.168.1.3.

D. The packet is dropped.

Answer: D

24. Refer to the Exhibit. What as-path access-list regular expression should be applied on R2 to only allow updates originated from AS65501 or autonomous systems directly attached to AS65501?



A. _65501_.*

B. _65501_*$

C. ^65501_*$

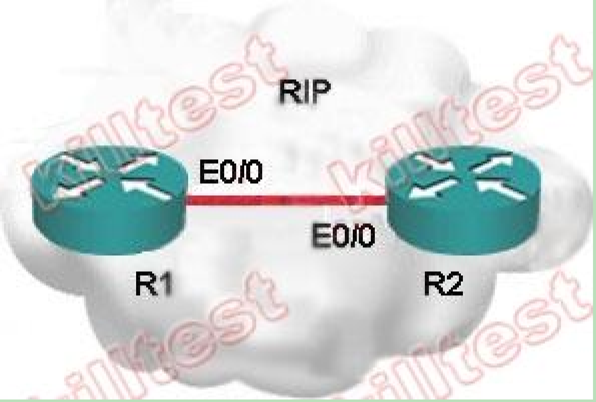
D. _65501+[0.9]$

E. ^65501_[0-9]*$

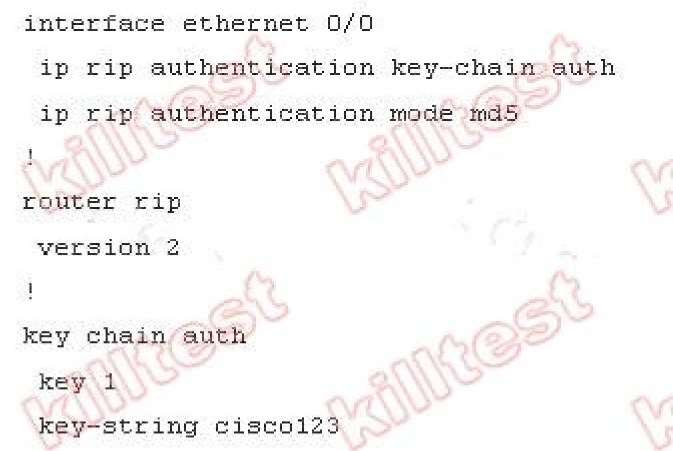
F. \[0-9]*+65501_+\[0-9]$

Answer: E

25. Refer to the Exhibit. What is the correct configuration on R1 to enable message digest authentication between routers R1 and R2?

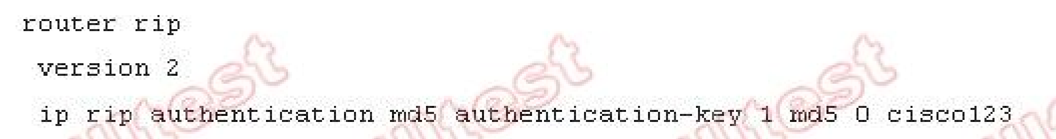


A.



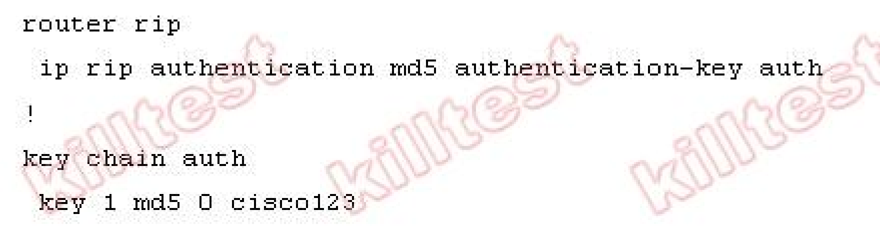
```
interface ethernet 0/0
 ip rip authentication key-chain auth
 ip rip authentication mode md5
!
router rip
 version 2
!
key chain auth
 key 1
 key-string cisco123
```

B.



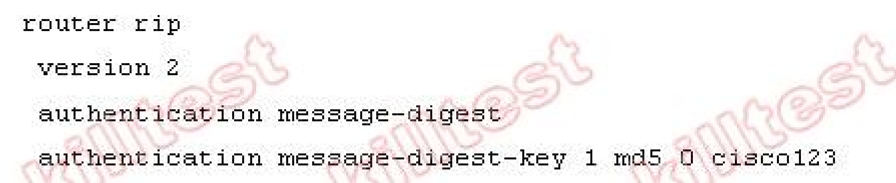
```
router rip
 version 2
 ip rip authentication md5 authentication-key 1 md5 0 cisco123
```

C.



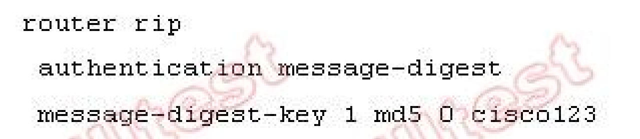
```
router rip
 ip rip authentication md5 authentication-key auth
!
key chain auth
 key 1 md5 0 cisco123
```

D.



```
router rip
 version 2
 authentication message-digest
 authentication message-digest-key 1 md5 0 cisco123
```

E.



```
router rip
 authentication message-digest
 message-digest-key 1 md5 0 cisco123
```

Answer: A

26. When applying MD5 route authentication on routers running RIP or EIGRP, what two important key chain considerations should be accounted for?

A. The lifetimes of the keys in the chain should overlap.

B. No more than three keys should be configured in any single chain.

C. Routers should be configured for NTP to synchronize their clocks.

D. Key 0 of all key chains must match for all routers in the autonomous system.

E. Link compression techniques should be disabled on links transporting any MD5 "hash". Answer: AC

27. Whenever a failover takes place on the ASA running in failover mode, all active connections are dropped and clients must re-establish their connections unless

A. the ASA is configured for Active-Standby failover.

B. the ASA is configured for Active-Active failover.

C. the ASA is configured for Active-Active failover and a state failover link has been configured.

D. the ASA is configured for Active-Standby failover and a state failover link has been configured.

E. the ASA is configured to use a serial cable as the failover link.

F. the ASA is configured for LAN-Based failover.

Answer: CD

28. Which of the following is true with respect to active-active failover on the ASA?

A. Active-active failover is available only for systems running in single context mode

B. Active-active failover is available only for systems running in transparent mode

C. Active-active failover is available only for systems running in routed mode

D. Active-active failover is available only for systems running in multiple context mode

E. Active-active failover is available for systems running in multiple or single context mode Answer: D

29. Whenever a failover takes place on the ASA (configured for failover), all active connections are dropped and clients must re-establish their connections unless: (Choose 2)

A. The ASA is configured for Active-Standby failover.

B. The ASA is configured for Active-Active failover.

C. The ASA is configured for Active-Active failover and a state failover link has been configured.

D. The ASA is configured for Active-Standby failover and a state failover link has been configured.

E. The ASA is configured to use a serial cable as the failover link.

F. The ASA is configured for LAN-Based failover

Answer: CD

30. Which algorithms did TKIP add to the 802.11 specification? (Choose 3)

A. key mixing

B. AES-based encryption

C. anti-replay sequence counter

D. message integrity check

E. cyclic redundancy check

Answer: ACD