Cisco 350-018 Exam

Volume: 872 Questions

Question No: 1

The computer at 10.10.10.4 on your network has been infected by a bontnet that directs traffic to a malware site at 168.65.201.120 Assuming that filtering will be performed on a Cisco ASA, What command can you use to block all current and future connections from the infected host?

A. ip access-list extended BLOCK_BOT_OUT deny ip any host 10.10.10.4

B. shun 168.65.201.120 10.10.10.4 6000 80

C. ip access-list extended BLOCK_BOT_OUT deny ip host 10.10.10.4 host 168.65.201.120

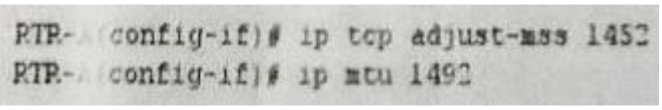
D. shun 10.10.10.4 68.65.201.120 6000 80

Answer: B

Question No: 2

Refer to the exhibit.

Which effect of this configuration is true?



```
RTP-  config-if)# ip tcp adjust-mss 1452
RTP-  config-if)# ip mtu 1492
```

A. The MSS of TCP SYN packets is set to 1452 bytes and the IP MTU of the interface is set to 1942 bytes

B. The maximum size of TCP SYN+ACK packets passing the transient host is set to 1452 bytes and the IP MTU of the interface is set to 1492 bytes

C. The PMTUD values sets itself to 1452 bytes when the interface MTU is set to 1492 bytes

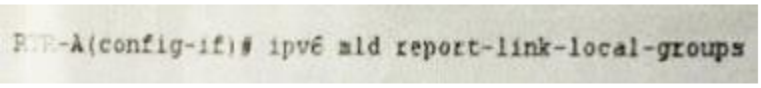
D. SYN packets carries 1452 bytes in the payload when the Ethernet MTU of the interface is to 1492 bytes

E. The maximum size of TCP SYN+ACK packets passing the router is set to 452 bytes and the IP MTU of the interface is set to 1492 bytes

Answer: A

Question No: 3

Refer to the exhibit.
Which effect of this configuration is true?



```
RTR-A(config-if)# ipv6 mld report-link-local-groups
```

A. It configures the node to generate a link-local group report when it joins the solicited-node multicast group

B. It enables local group membership for MLDvl and MLDv2

C. It enables hosts to send MLD report messages for groups in 224.0.0.0/24

D. It enables MLD query messages for all link-local groups

E. It enables the host to send MLD report messages for nonlink local groups

Answer: C

Question No: 4
You have configured an ASA firewall in multiple context mode. If the context are sharing an Interface. What are two of the actions you could take to classify packets to the appropriate Context?(Choose two)

A. Enable DHCP

B. Disable MAC auto-generation and adding unique IP addresses to each interface

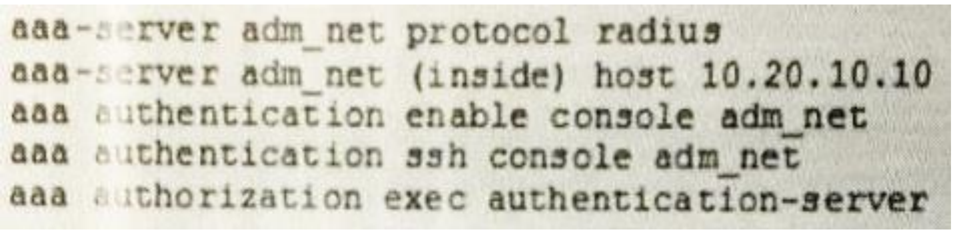
C. Enable MAC auto-generation globally

D. Assign a unique MAC address to each interface

E. Apply QoS to each interface

Answer: CD

Question No: 5
Refer to the exhibit.
What is the effect if the given configuration?



```
aaa-server adm_net protocol radius
aaa-server adm_net (inside) host 10.20.10.10
aaa authentication enable console adm_net
aaa authentication ssh console adm_net
aaa authorization exec authentication-server
```

A. It requires the enable password to be authorized by the LOCAL database

B. It allows users to log in with any user name in the LOCAL database

C. It enables management authorization for a user-authenticated RADIUS server

D. Users will be authenticated against the RADIUS servers defined in the adm_net list

E. It allows SSH connections to console login into the ASA

Answer: D

Question No: 6
What feature enables extended secure access form non-secure physical locations?

A. NEAT

B. 802.1X port-based authentication

C. port security

D. storm-control

E. CBAC

Answer: A

Question No: 7
What are the two technologies that support AFT?(Choose two)

A. NAT-6 to 4

B. NAT-PT

C. DNAT

D. NAT64

E. NAT-PMP

F. SNAT

Answer: BD

Question No: 8
On an ASA firewall in multiple context mode running version 8.X, what is the default number of VPN site-to-site tunnels per context?

A. 2 sessions

B. 4 sessions

C. 1 session

D. 0 sessions

Answer: A

Question No: 9
Which three statements about Unicast RPF in strict mode and loose mode are true?(Choose three)

A. Inadvertent packet loss can occur when loose mode is used with asymmetrical routing

B. Interface in strict mode drop traffic which return routes that point to the Null 0 interface

C. Strict mode requires a default route to be associated with the uplink network interface

D. Loose mode requires the source address to be present in the routing table

E. Both loose and strict modes are configured globally on the router

F. Strict mode is recommended on interfaces that will receive packets only from the same subnet to which the interface is assigned

Answer: BDF

Question No: 10
What are the three scanning engines that the cisco Iron Port dynamic vectoring and Streaming engine can use to protect against malware? (Choose three)

A. Sophos

B. McAfee

C. Symantec

D. F-Secure

E. Webroot

F. TrendMicro

Answer: ABE

Question No: 11
Which feature can you implement to protect against SYN-flooding DoS attacks?

A. TCP intercept

B. a null zero route

C. CAR applied to ICMP packets

D. the ip verify unicast reverse-path command

Answer: A

Question No: 12
What are two advantages of NBAR2 over NBAR? (Choose two)

A. Only NBAR2 allows the administrator to apply individual PDL flies

B. Only NBAR2 supports custom protocols based on HTTP URLS

C. Only NBAR2 supports PDLM to support new protocols

D. Only NBAR2 supports Flexible NetFlow for extracting and exporting fields from the Packet header

E. Only NBAR2 can use Sampled NetFlow to extract pre-defined packet headers for reporting

Answer: BD

Question No: 13
What are two characteristics of RPL ,used in IoT environments? (Choose two)

A. it is distance-vector protocol

B. it is a Interior Gateway Protocol

C. it is link-state protocol

D. it is a hybrid protocol

E. it is an Exterior Gateway Protocol

Answer: AE

Question No: 14
What protocol does IPv6 Router Advertisement use for its messages?

A. ARP

B. TCP

C. ICMPv6

D. UDP

Answer: C

Question No: 15
Which ASA device is designated as the cluster master in the High Availability setup?

A. The ASA configured with the lowest priority value

B. The ASA configured with the highest priority value

C. The ASA with the highest MAC address

D. The ASA with the lowest MAC address

Answer: A

Question No: 16
Refer to the exhibit .
A signature failed to compile and returned the given error messages. What is a possible reason for the problem?

```
%IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5284:0 - compilation of regular expression failed
%IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12023:0 - compiles discontinued for this engine
```

A. Additional signatures must be compiled during the compiling process

B. The signatures belongs to the IOS IPS Basic category

C. The signatures belongs to the IOS IPS Advanced category

D. There is insufficient memory to compile the signature

E. The signature is retired

Answer: D

Question No: 17
Which two statements about PVLAN port types are true? (Choose two)

A. A promiscuous port can send traffic to all ports within a broadcast domain

B. An isolated port can receive traffic t from promiscuous ports in any community on its Broadcast domain, but can send traffic only to ports in its own community

C. An isolated port can send and receive traffic only to and from promiscuous ports

D. A community port can send traffic to promiscuous ports in other communities its Broadcast domain

E. A community port can send traffic to community ports in other communities its Broadcast domain

F. A promiscuous can send traffic to community ports in other Broadcast domains

Answer: AC

Question No: 18
Which statement about the Cisco ASA operation running versions 8.3 is true?

A. NAT control is enabled by default

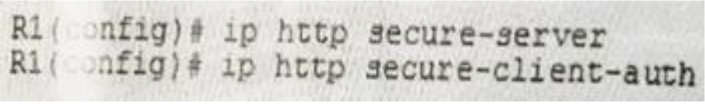
B. The interface and global access lists both can be applied in the input or output direction

C. The static CLI command is used to configure static NAT translation rules

D. The imperfect access list is matched first before the global access list

Answer: D

Question No: 19
Refer to the exhibit.
What is the effect if the given command sequence?



```
R1(config)# ip http secure-server
R1(config)# ip http secure-client-auth
```

A. The server will accept secure HTTP connections from clients with signed security certificates

B. The client profile will match the authorization profile defined in the AAA server

C. The HTTP server and client will negotiate the cipher suite encryption parameters

D. The clients are added to the cipher suite*s profile

E. The server will accept secure HTTP connections from clients defined in the AAA server

Answer: A

Question No: 20
Which two network protocols can operate on the application layer? (Choose two)

A. UDP

B. TCP

C. SMB

D. DNS

E. DCCP

F. NetBIOS

Answer: CD

Question No: 21
When a host initiates a TCP session, what is the numerical range into which the initial sequence number must fall?

A. 1 to 4,294,967,295

B. 0 to 4,294,967,295

C. 1 to 65535

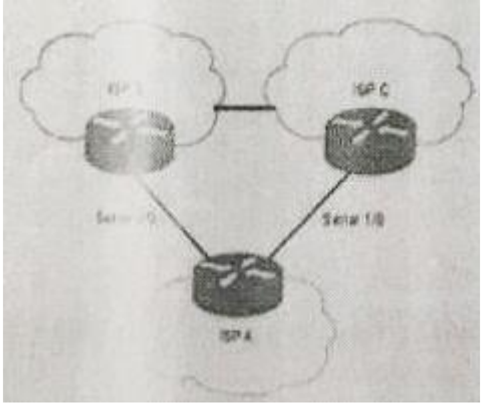
D. 0 to 65535

E. 0 to 1024

F. 1 to 1024

Answer: B

Question No: 22
Refer to the exhibit.
If R1 is connected upstream to R2 and R3 at different ISPs as shown, what action must be taken to prevent Unicast Reverse Path Forwarding(uRPF)from dropping asymmetric traffic?



A. Configure Unicast RPF Strict Mode on R2 and R3 only

B. Configure Unicast RPF loose Mode on R2 and R3 only

C. Configure Unicast RPF Strict Mode on RI only

D. Configure Unicast RPF loose Mode on RI only

E. Configure Unicast RPF Strict Mode on RI,R2 and R3

Answer: A

Question No: 23
What are two features that help to mitigate man-in-the-middle attacks?(Choose two)

A. DHCP snooping

B. dynamic ARP inspection

C. destination MAC ACLS

D. ARP sniffing on specific ports

E. ARP spoofing

Answer: AB

Question No: 24
Which three statements about Dynamic ARP inspection on Cisco series are true? (Choose three)

A. The trusted database can be manually configured using the CLI

B. Dynamic ARP inspection is supported only on access ports

C. Dynamic ARP inspection does no perform ingress security checking

D. DHCP snooping is used to dynamically build the trusted database

E. Dynamic ARP inspection checks ARP packets against the trusted database

F. Dynamic ARP inspection checks ARP packets on trusted and untrusted ports

Answer: ADE

Question No: 25
Which three statements about the SHA-2 algorithm are true?(Choose three)

A. It generates a 160-bit message digest

B. It generates a 512-bit message digest

C. It is the collective term for the SHA-224 ,SHA-256,SHA-384,and SHA-512 algorithms

D. It is used for integrity verification

E. It is provides a fixed-length output using a collision-resistant cryptographic hash

F. It is provides a variable-length output using a collision-resistant cryptographic hash

Answer: CDE

Question No: 26
Why is the IPv6 type 0 routing header vulnerable to attack?

A. It allows the sender to generate multiple NDP requests for each packet

B. It allows the receiver of a packet to control its flow

C. It allows the sender to generate multiple ARP requests for each packet

D. it allows the sender of a packet to control its flow.

E. It allows the receiver of a packet to modify the source IP address

Answer: D

Question No: 27
Which statement about 150/IEC 27001 is true?

A. It is only intended to report security breaches to the management authority

B. It was reviewed by the international Electrotechnical Commission

C. It was reviewed by the international Organization for Standardization

D. It is intended to bring information security under management control

E. It was published by 150/IEC

Answer: D

Question No: 28
What ASA feature can you use to restrict a user to a specific VPN group?

A. a vpn filter

B. MPF

C. a Webtype ACL

D. group-lock

Answer: D

Question No: 29
Which two statements about the send protocol are true?(Choose two)

A. it counters neighbor discovery threats

B. it must be enabled before you can configure IPv6 address

C. It supports numerous custom neighbor discovery messages

D. it supports an auto configuration mechanism

E. it logs IPv6-related threats to an external log server

F. it uses IPsec as baseline mechanism

Answer: AD

Question No: 30
In a Cisco ASA multiple-context mode of operation configuration ,what three session types are resource-limited by default when their context is a member of the default class?(Choose three)

A. ASDM sessions

B. Telnet sessions

C. IPSec sessions

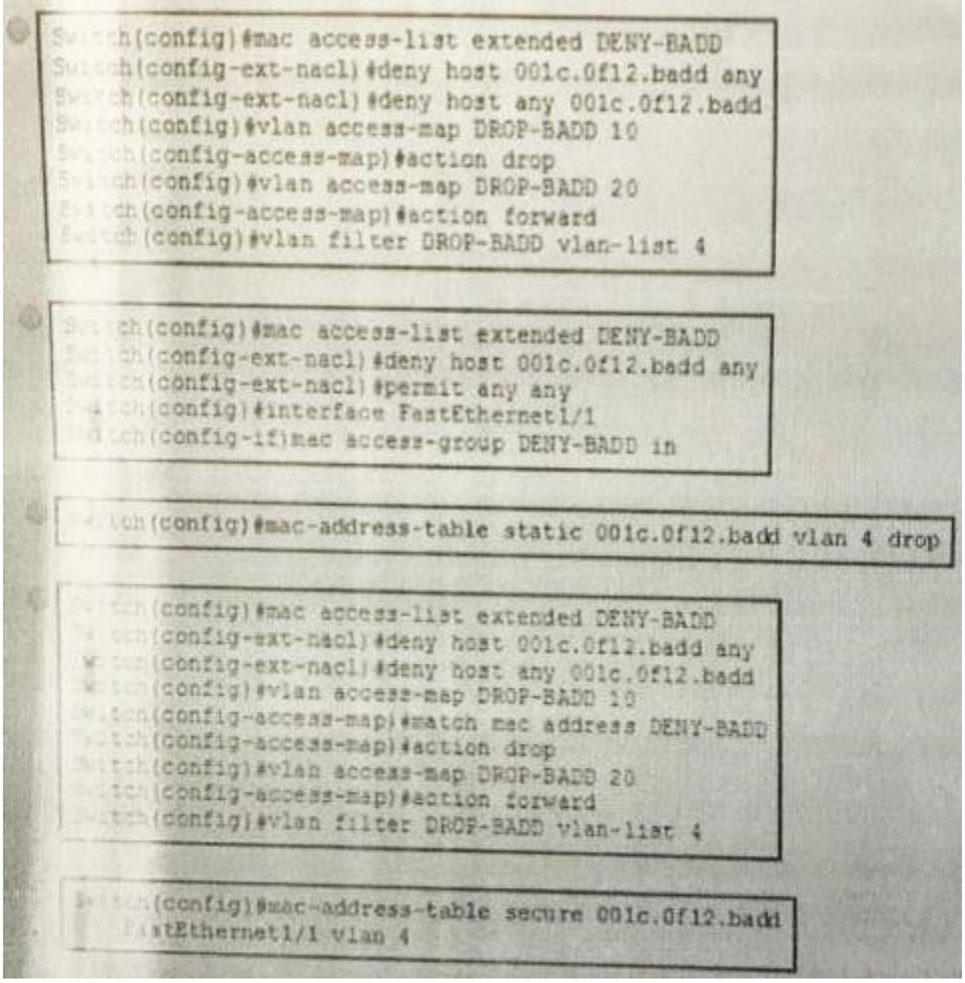
D. SSL VPN sessions

E. TCP sessions

F. SSH sessions

Answer: ABF

Question No: 31
You have discovered an unwanted device with MAC address 001c.of12.badd on port FastEthernet1/1 on VLAN 4.What command or command sequence can enter on the switch to prevent the MAC address from passing traffic on VLAN 4 ?



```
Switch(config)#mac access-list extended DENY-BADD
Switch(config-ext-nacl)#deny host 001c.0f12.badd any
Switch(config-ext-nacl)#deny host any 001c.0f12.badd
Switch(config)#vlan access-map DROP-BADD 10
Switch(config-access-map)#action drop
Switch(config)#vlan access-map DROP-BADD 20
Switch(config-access-map)#action forward
Switch(config)#vlan filter DROP-BADD vlan-list 4
```

```
Switch(config)#mac access-list extended DENY-BADD
Switch(config-ext-nacl)#deny host 001c.0f12.badd any
Switch(config-ext-nacl)#permit any any
Switch(config)#interface FastEthernet1/1
Switch(config-if)mac access-group DENY-BADD in
```

```
Switch(config)#mac-address-table static 001c.0f12.badd vlan 4 drop
```

```
Switch(config)#mac access-list extended DENY-BADD
Switch(config-ext-nacl)#deny host 001c.0f12.badd any
Switch(config-ext-nacl)#deny host any 001c.0f12.badd
Switch(config)#vlan access-map DROP-BADD 10
Switch(config-access-map)#match mac address DENY-BADD
Switch(config-access-map)#action drop
Switch(config)#vlan access-map DROP-BADD 20
Switch(config-access-map)#action forward
Switch(config)#vlan filter DROP-BADD vlan-list 4
```

```
Switch(config)#mac-address-table secure 001c.0f12.badd
  FastEthernet1/1 vlan 4
```

A. Exhibit A

B. Exhibit B

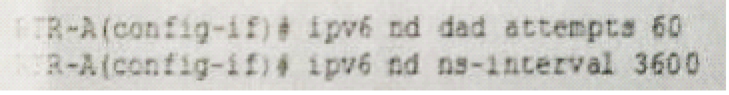
C. Exhibit C

D. Exhibit D

E. Exhibit D

Answer: C

Question No: 32
Refer to exhibit.
What is the effect to the given configuration?



```
R-A(config-if)# ipv6 nd dad attempts 60
R-A(config-if)# ipv6 nd ns-interval 3600
```

A. It sets the duplicated address detection Interval to 60 seconds and sets the IPv6 Neighbor solicitation Interval to 3600 milliseconds.

B. It sets the number of neighbor solicitation messages to 60 while duplicate address detection is performed and sets the neighbor solicitation retransmission interval to 3600 milliseconds.

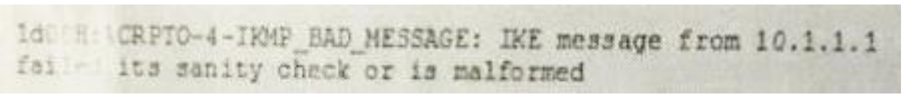
C. It sets the number of neighbor solicitation messages to 60 and sets the duplicate address detection interval to 3600 seconds.

D. It sets duplicate address detection interval to 60 seconds and sets the IPv6 neighbor reachable time to 3600 milliseconds.

E. It sets the number of duplicate address detection attempts to 60 and sets the duplicate address detection interval to 3600 milliseconds.

Answer: B

Question No: 33
Refer to the exhibit.
What is the meaning of the given error message?



```
1d  H: CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 10.1.1.1
fai    its sanity check or is malformed
```

A. The PFS groups are mismatched

B. IKES disabled on the remote peer

C. The pre-shared keys are mismatched

D. The mirrored crypto ACLs are mismatched

Answer: C

Question No: 34
What are three IPv6 extension headers?(Choose three)

A. Hop-by-Hop Options

B. Swgment

C. TTL

D. Source Options

E. Authentication Header

F. Destination Options

Answer: AEF

Question No: 35
Which two statements about PCI DSS are true?(Choose two)

A. it is a criminal act of cardholder information fraud.

B.it is an IETF standard for companies to protect credit, debit ,and ATM cardholder information.

C.it has as one of its objectives to restrict physical access to credit, debit ,and ATM cardholder information.

D. it is a US government standard that defines ISP security compliance

E.it is a proprietary security standard that defines a framework for credit, debit ,and ATM cardholder information.

Answer: CE

Question No: 36
You are developing an application to manage the traffic flow of a switch using an Open Daylight controller Knowing you use a Northbound which statement is true?

A. We must teach our applications about the Southbound protocol(s) used.

B. Different applications ,even in different languages ,cannot use the same functions in a REST API at the same time.

C. The applications are considered to be the clients, and the controller is considered to be the server

D. The server retains client state records

Answer: C

Question No: 37
Which two statements about IKEv2 are true?(Choose two)

A. it uses EAP authentication

B. At minimum. A complete proposal requires one encryption algorithm and one integrity algorithm.

C. The profile contains a repository of symmetric and asymmetric and asymmetric preshared keys.

D. It uses X.509 certificates for authentication

E. The profile is a collection of transforms used to negotiate IKE SAS

F. It supports DPD and NAT-T by default.

Answer: AF

Question No: 38
Which object table contains information about the clients know to the server in Cisco NHRP MIB implementation?

A. NHRP Server NHC Table

B. NHRP Client Statistics Table

C. NHRP Cache Table

D. NHRP Purge Request Table

Answer: A

Question No: 39
Which two options describe the main purpose of EIGRP authentication?(Choose two)

A. to allow faster convergence

B. to identify authorized peers

C. to provide redundancy

D. to provide routing updates confidentiality

E. to prevent injection of incorrect routing information

Answer: BE

Question No: 40
Your IPv6 a CA and trust anchors to implement secure network discovery. What extension must your CA certificates support?

A. id-pe-ipaddrBiocks

B. keyUsage

C. extKeyUsage

D. id-pe-autonomousSyslds

E. ia-ad-classusers

F. nameConstraints

Answer: E

Question No: 41
A cloud service provider is designing a large multitenant data center to support thousands of tenants. The provider is concerned about the scalability the layer 2 network and providing layer 2 segmentation to potentially thousands of tenants .Which layer 2 technology is best suited in this scenario?

A. extended VLAN ranges

B. VXLAN

C. VRF

D. LDP

Answer: B

Question No: 42
Which two statements about the IPv6 Hop-by-Hop Options extension header (EH) are true?(Choose two)

A. The Hop-by-Hop EH is processed in hardware by all intermediate network devices

B. The Hop-by-Hop extension header is processed by the CPU by network devices

C. The Hop-by-Hop EH is encrypted by the Encapsulating Security Header

D. If present, the Hop-by-Hop EH must follow the Mobility EH.

E. If present,network devices must process the Hop-by-Hop EH first

F. The Hop-by-Hop EH is processed in hardware at the source and the destination devices only

Answer: BE

Question No: 43
CCMP(CCM mode Protocol) is based on which algorithm?

A. AES

B. RCS

C. 3DES

D. IDEA

E. Blowfish

Answer: A

Question No: 44
Which MAC address control command enables usage monitoring for A CAM table on a switch?

A. mac-address-table learning

B. mac-address-table synchronize

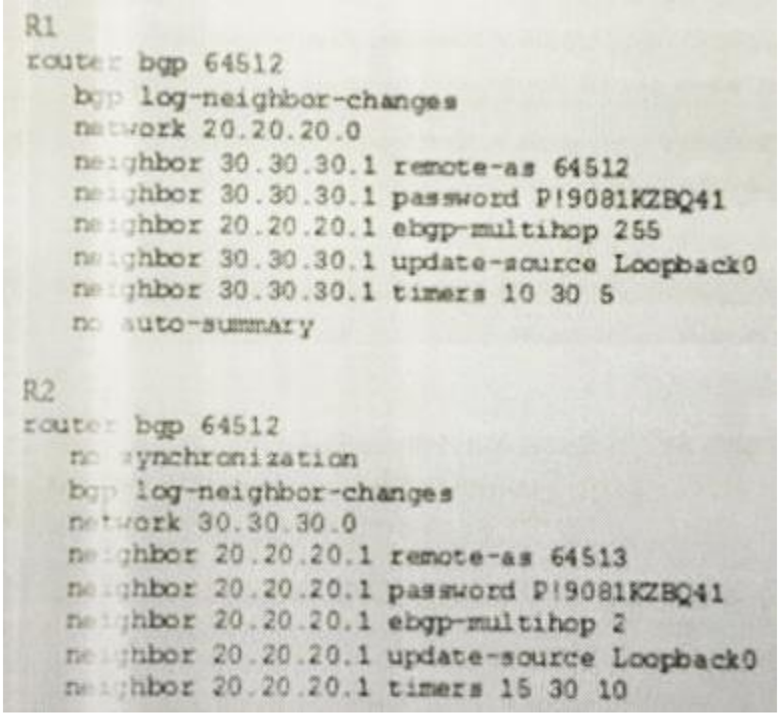
C. mac-address-table secure

D. mac-address-table limit

E. mac-address-table notification threshold

Answer: E

Question No: 45
Refer to the exhibit.



```
R1
router bgp 64512
  bgp log-neighbor-changes
  network 20.20.20.0
  neighbor 30.30.30.1 remote-as 64512
  neighbor 30.30.30.1 password P!9081KZBQ41
  neighbor 20.20.20.1 ebgp-multihop 255
  neighbor 30.30.30.1 update-source Loopback0
  neighbor 30.30.30.1 timers 10 30 5
  no auto-summary

R2
router bgp 64512
  no synchronization
  bgp log-neighbor-changes
  network 30.30.30.0
  neighbor 20.20.20.1 remote-as 64513
  neighbor 20.20.20.1 password P!9081KZBQ41
  neighbor 20.20.20.1 ebgp-multihop 2
  neighbor 20.20.20.1 update-source Loopback0
  neighbor 20.20.20.1 timers 15 30 10
```

R1 and R2 are failing to establish a BGP neighbor relationship.
What is a Possible reason for the problem?

A. The neighbor remote-as command on R2 uses an incorrect AS number

B. The BGP timers on R1 and R2 are different

C. R2 is configured with a private AS

D. The no synchronization command is missing from R1's configuration

E. The dbgp-multihop values on R1 and R2 are different

F. The no auto-summary command is missing from R2's configuration.

Answer: A

Question No: 46
If a cisco ASA firewall that is configured in multiple-context mode of operation receives a packet whose destination MAC address is a multicast address, how is the packet routed?

A. The Packets dropped

B. The packet is duplicated and forwarded to every context

C. The packet is forwarded to the admin context only

D. The packet duplicated and forwarded to every context except admin

Answer: B

Question No: 47
Refer to the exhibit. Which statement about this configuration is true?

A. The ASA injects a static default route into OSPF process 1

B. The ASA injects a static default route into OSPF process 1

C. The ASF stops LSA type 7 packets from flooding into OSPF area 1

D. The ASA redistributes routes from one routing protocol to another