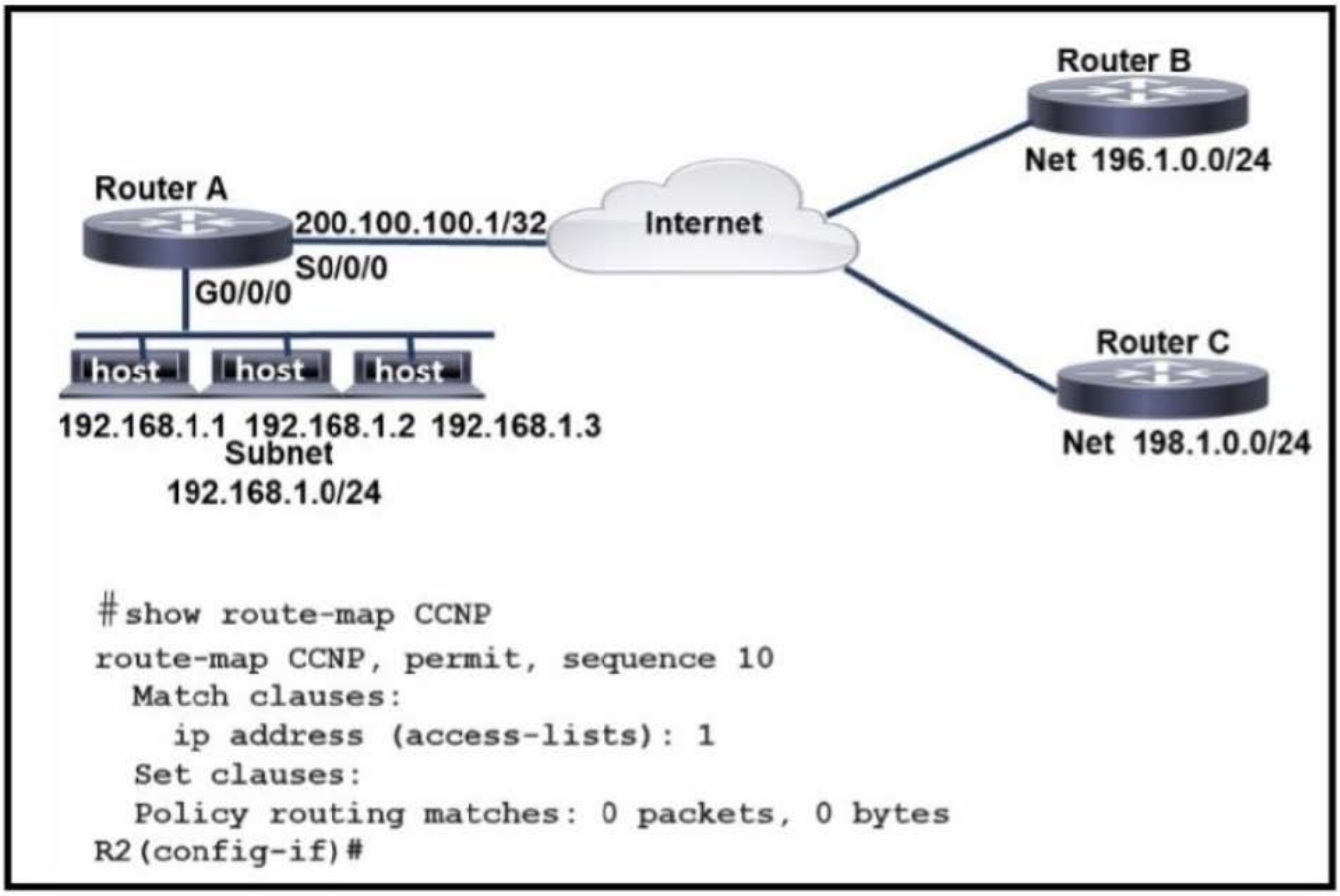
300-410$^{Q\&As}$

Implementing Cisco Enterprise Advanced Routing and Services (ENARSI) (Include 2023 Newest Simulation Labs)

Pass Cisco 300-410 Exam with 100% Guarantee

QUESTION 1

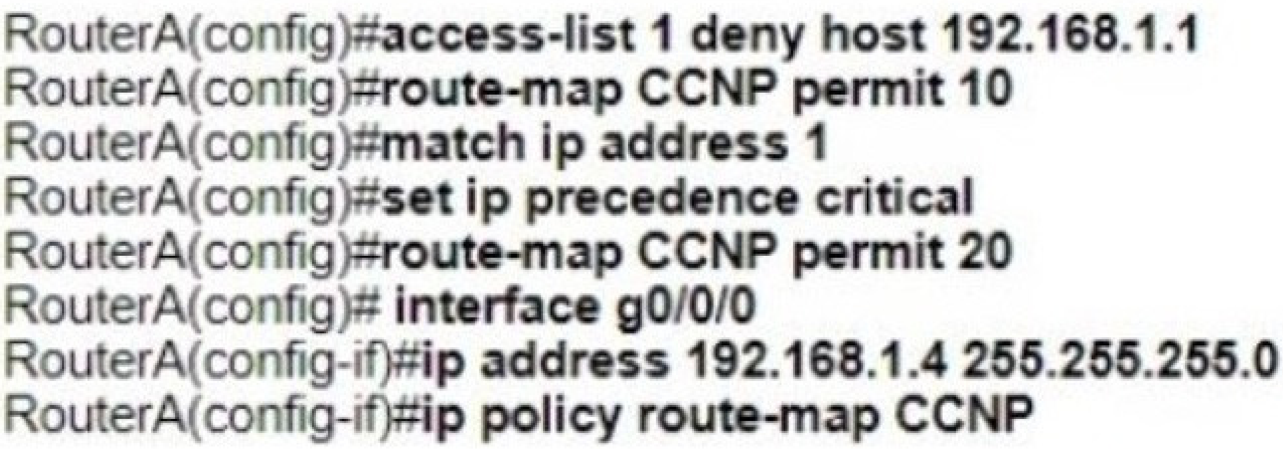
Refer to the exhibit.



```
#show route-map CCNP
route-map CCNP, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
R2(config-if)#
```

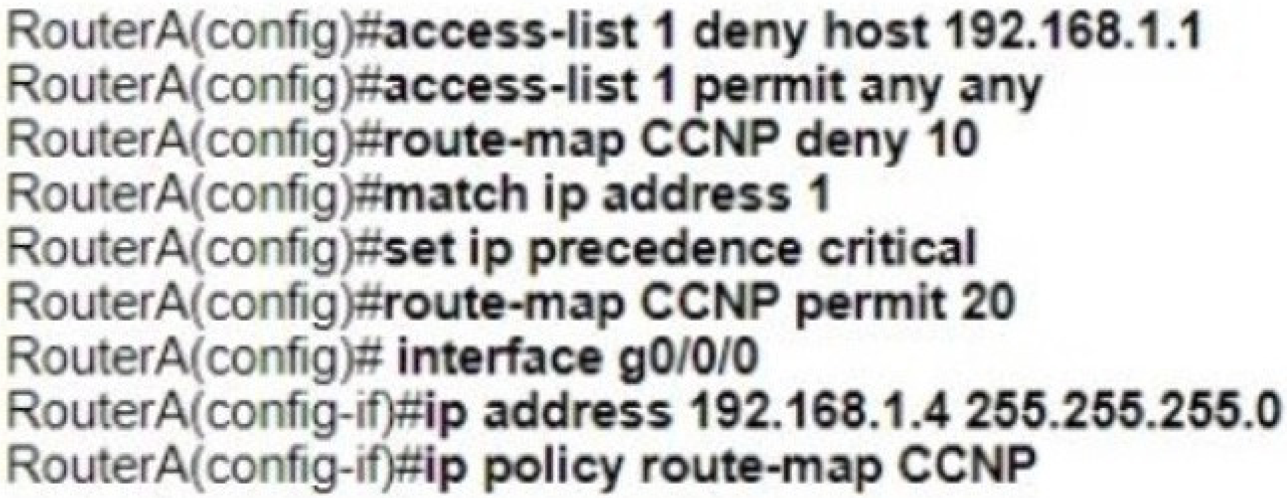
An engineer configures router A to mark all inside to outside traffic from network 192 168 1 0, except from host 192 168 1 1. with critical IP precedence. The policy did not work as expected. Which configuration resolves the issue?

A.



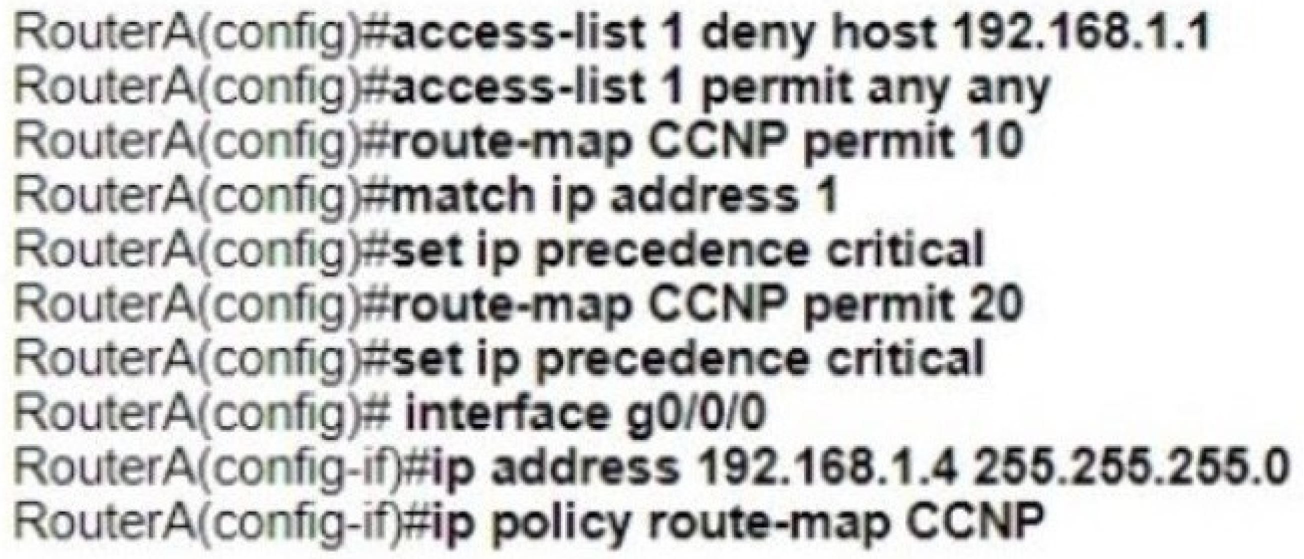
```
RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
```

B.



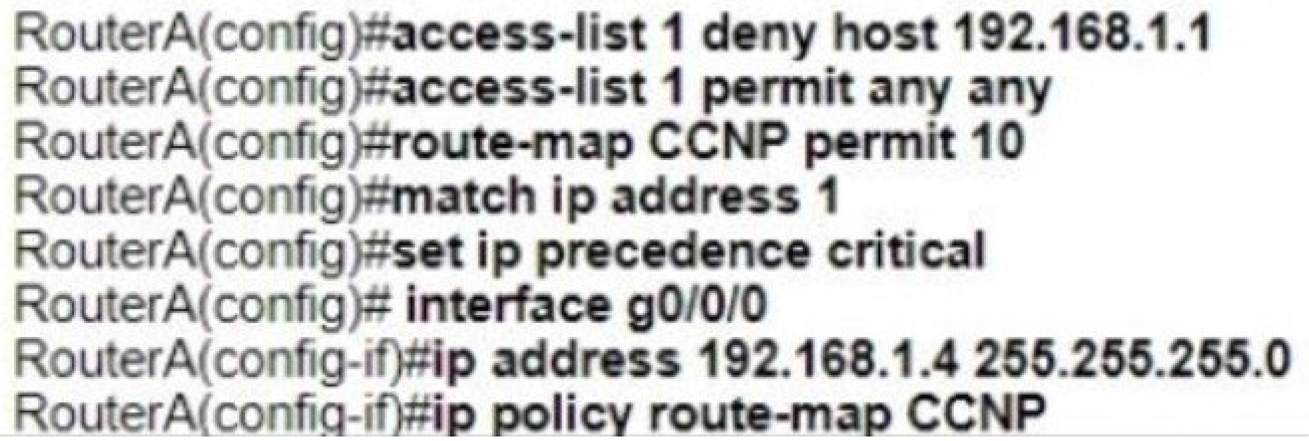
```
RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP deny 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
```

C.



```
RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)#route-map CCNP permit 20
RouterA(config)#set ip precedence critical
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
```

D.



```
RouterA(config)#access-list 1 deny host 192.168.1.1
RouterA(config)#access-list 1 permit any any
RouterA(config)#route-map CCNP permit 10
RouterA(config)#match ip address 1
RouterA(config)#set ip precedence critical
RouterA(config)# interface g0/0/0
RouterA(config-if)#ip address 192.168.1.4 255.255.255.0
RouterA(config-if)#ip policy route-map CCNP
```

A. Option A

B. Option B

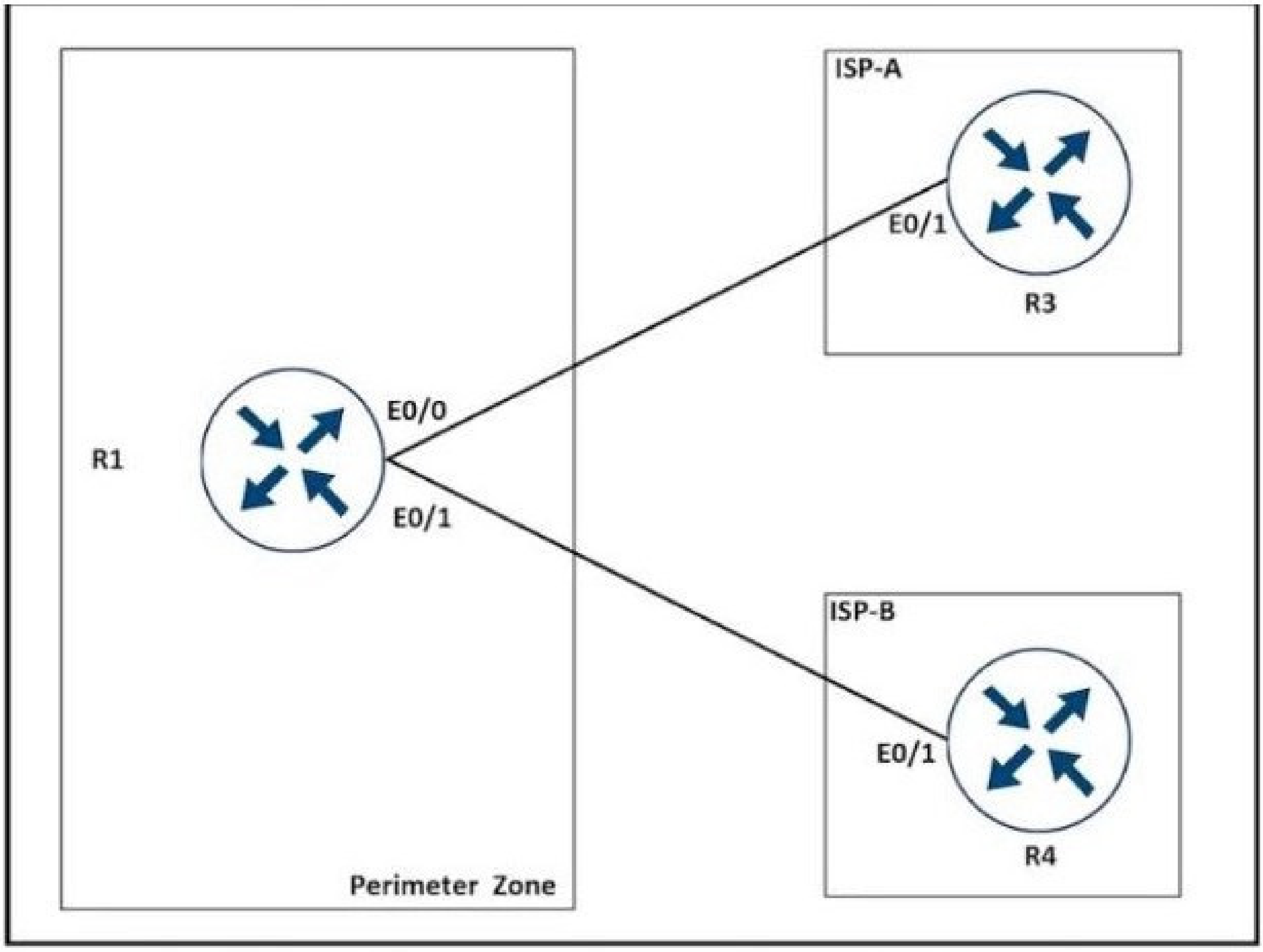
C. Option C

D. Option D

Correct Answer: A

QUESTION 2

Refer to the exhibit.



A network is under a cyberattack. A network engineer connected to R1 by SSH and enabled the terminal monitor via SSH session to find the source and destination of the attack. The session was flooded with messages, which made it impossible for the engineer to troubleshoot the issue. Which command resolves this issue on R1?

A. #terminal no monitor

B. (config)#terminal no monitor

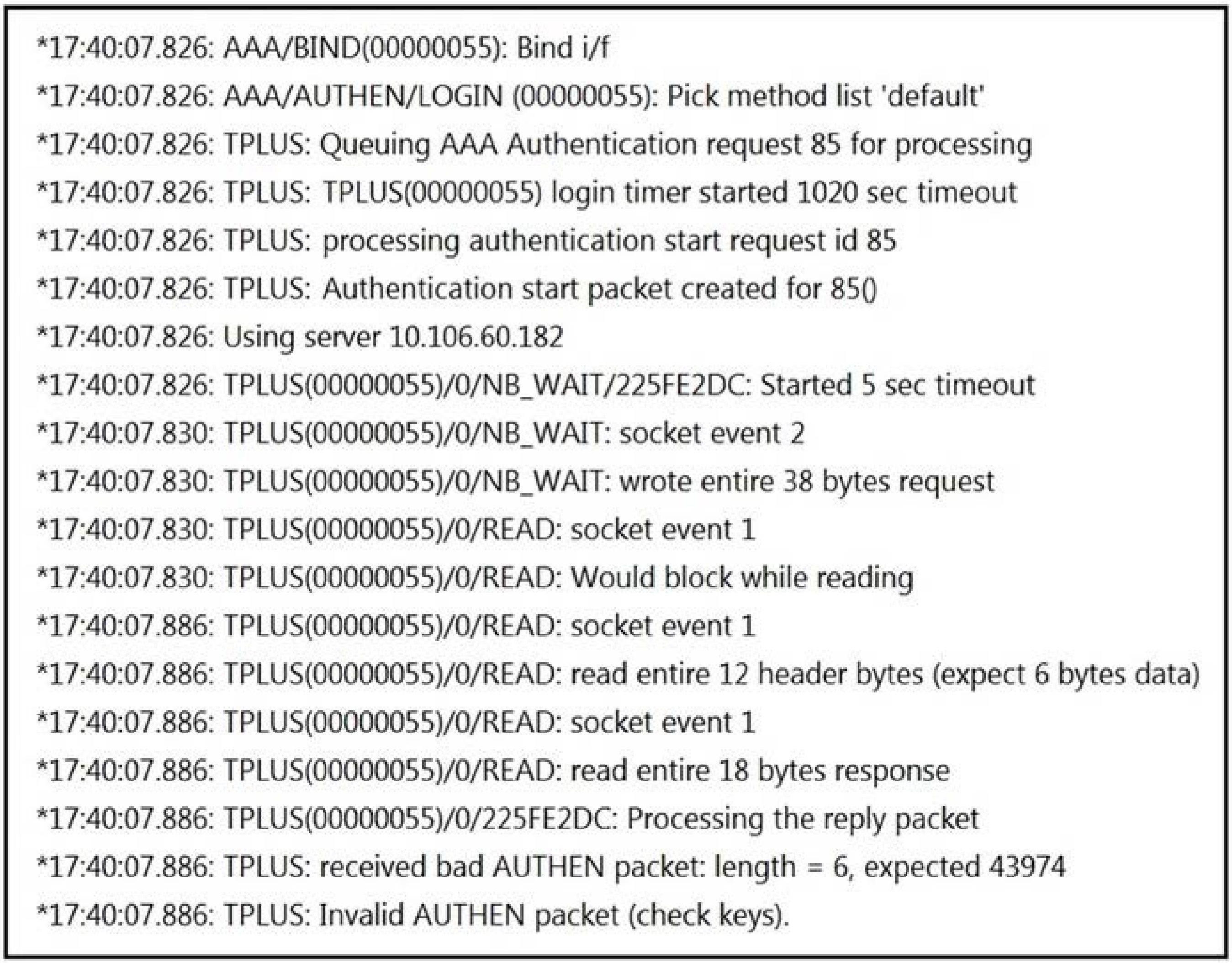
C. #no terminal monitor

D. (config)#no terminal monitor

Correct Answer: A

QUESTION 3

Refer to the exhibit. An engineer is troubleshooting a TACACS problem. Which action resolves the issue?



```
*17:40:07.826: AAA/BIND(00000055): Bind i/f
*17:40:07.826: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
*17:40:07.826: TPLUS: Queuing AAA Authentication request 85 for processing
*17:40:07.826: TPLUS: TPLUS(00000055) login timer started 1020 sec timeout
*17:40:07.826: TPLUS: processing authentication start request id 85
*17:40:07.826: TPLUS: Authentication start packet created for 85()
*17:40:07.826: Using server 10.106.60.182
*17:40:07.826: TPLUS(00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: socket event 2
*17:40:07.830: TPLUS(00000055)/0/NB_WAIT: wrote entire 38 bytes request
*17:40:07.830: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.830: TPLUS(00000055)/0/READ: Would block while reading
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 12 header bytes (expect 6 bytes data)
*17:40:07.886: TPLUS(00000055)/0/READ: socket event 1
*17:40:07.886: TPLUS(00000055)/0/READ: read entire 18 bytes response
*17:40:07.886: TPLUS(00000055)/0/225FE2DC: Processing the reply packet
*17:40:07.886: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
*17:40:07.886: TPLUS: Invalid AUTHEN packet (check keys).
```

A. Configure a matching TACACS server IP.

B. Configure a matching preshared key.

C. Generate authentication from a relative source interface.

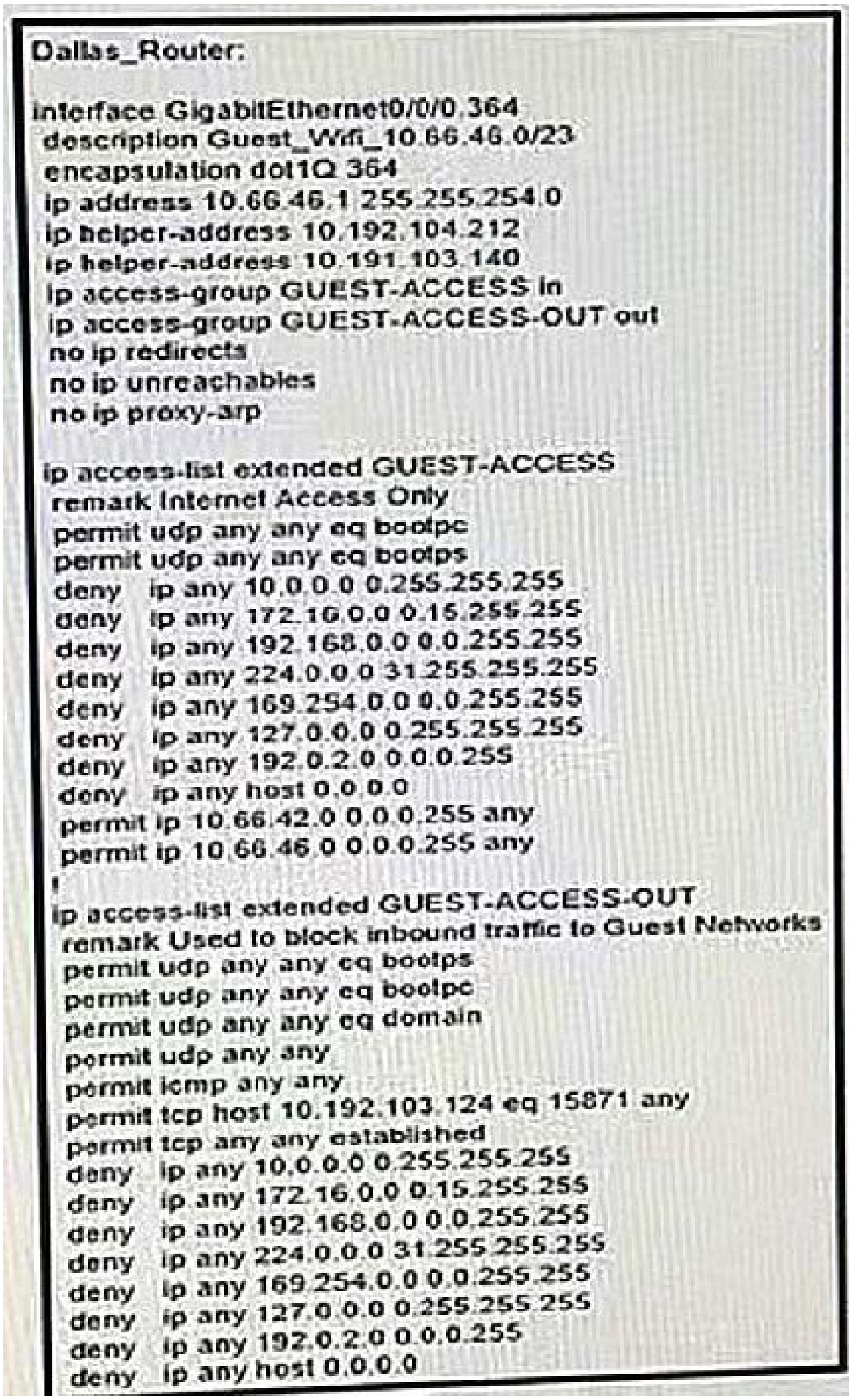
D. Apply a configured AAA profile to the VTY.

Correct Answer: B

https://community.cisco.com/t5/network-access-control/bad-invalid-authentication-packet/td-p/824682

QUESTION 4

Refer to the exhibit.



```
Dallas_Router:

interface GigabitEthernet0/0/0.364
 description Guest_Wifi_10.66.46.0/23
 encapsulation dot1Q 364
 ip address 10.66.46.1 255.255.254.0
 ip helper-address 10.192.104.212
 ip helper-address 10.191.103.140
 ip access-group GUEST-ACCESS in
 ip access-group GUEST-ACCESS-OUT out
 no ip redirects
 no ip unreachables
 no ip proxy-arp

ip access-list extended GUEST-ACCESS
 remark Internet Access Only
 permit udp any any eq bootpc
 permit udp any any eq bootps
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
 permit ip 10.66.42.0 0.0.0.255 any
 permit ip 10.66.46.0 0.0.0.255 any
!
ip access-list extended GUEST-ACCESS-OUT
 remark Used to block inbound traffic to Guest Networks
 permit udp any any eq bootps
 permit udp any any eq bootpc
 permit udp any any eq domain
 permit udp any any
 permit icmp any any
 permit tcp host 10.192.103.124 eq 15871 any
 permit tcp any any established
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 deny   ip any 224.0.0.0 31.255.255.255
 deny   ip any 169.254.0.0 0.0.255.255
 deny   ip any 127.0.0.0 0.255.255.255
 deny   ip any 192.0.2.0 0.0.0.255
 deny   ip any host 0.0.0.0
```

After a new regional office is set up,not all guests can access the internet via guest WiFi. Clients are getting the correct IP address from guest Wi-Fi VLAN 364.

Which action resolves the issue ?

A. Allow 10.66.46.0/23 in the outbound ACL

B. Allow DNS traffic through the outbound ACL

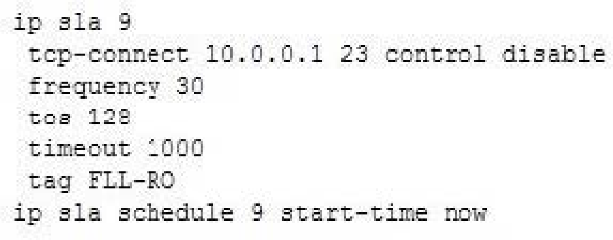
C. Allow DNS traffic through the inbound ACL

D. Allow 10.66.46.0/23 in the inbound ACL

Correct Answer: C

QUESTION 5

You configured a device as an IP SLA responder using the following configuration:



```
ip sla 9
 tcp-connect 10.0.0.1 23 control disable
 frequency 30
 tos 128
 timeout 1000
 tag FLL-RO
ip sla schedule 9 start-time now
```

Which line indicates that the device is not a Cisco device?

A. frequency 30

B. timeout 1000

C. tcp-connect 10.0.0.1 23 control disable

D. tag FLL-RO

Correct Answer: C

The IP SLA TCP connect operation is used to gather statistics on connection-oriented services. The tcp- connect 10.0.0.1 23 control disable command specifies the IP address to which the responder should respond, the port number on

which to respond and it disables the control protocol normally used to inform the responder to temporarily enable the port specified .by the configuration in the sender. When the responder is a non-Cisco device, a well-known port number

must be chosen and the control protocol should be disabled on the responder. When a Cisco device is the responder, then any port number can be chosen and the control protocol should be left enabled.

The frequency 30 command specifies how often the test should occur in seconds. It is not changed in any way as a result of the responder being a non-Cisco device.

The timeout 1000 command specifies in milliseconds the amount of time an IP SLAs operation waits for a response from its request packet. It is not changed in any way as a result of the responder being a non-Cisco device.

The tag FLL-RO command simply applies a user-specified identifier to the IP SLAs operation and is changed in any way as a result of the responder being a non-Cisco device.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify IP SLA

References:

IP SLAs Configuration Guide, Cisco IOS Release 15MandT > Configuring IP SLAs TCP Connect Operations Cisco > Cisco IOS IP SLAs Command Reference > tcp-connect