



Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)



EXAMKILLER

Help Pass Your Exam At First Try

Cisco

Exam 300-410

Implementing Cisco Enterprise Advanced Routing and Services (300-410 ENARSI)

Version: 40.0

[Total Questions: 530]

Topic break down

Topic	No. of Questions
Topic 1: Exam Pool A	109
Topic 2: Exam Pool B	115
Topic 3: Exam Pool C	306

Topic 1, Exam Pool A

Question No : 1 - (Topic 1)

Which two protocols can cause TCP starvation? (Choose two)

- A. TFTP
- B. SNMP
- C. SMTP
- D. HTTPS
- E. FTP

Answer: A,B

Question No : 2 - (Topic 1)

Users were moved from the local DHCP server to the remote corporate DHCP server. After the move,

none of the users were able to use the network.

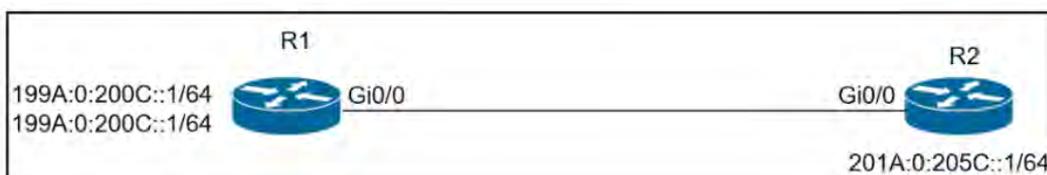
Which two issues will prevent this setup from working properly? (Choose two)

- A. Auto-QoS is blocking DHCP traffic.
- B. The DHCP server IP address configuration is missing locally
- C. 802.1X is blocking DHCP traffic
- D. The broadcast domain is too large for proper DHCP propagation
- E. The route to the new DHCP server is missing

Answer: B,E

Question No : 3 - (Topic 1)

Refer to the exhibit.



Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?

A)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
  ipv6 traffic-filter Deny_Telnet in
!
```

B)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64 eq telnet
!
int Gi0/0
  ipv6 access-map Deny_Telnet in
!
```

C)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
  ipv6 access-map Deny_Telnet in
!
```

D)

```
ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host
201A:0:205C::1/64
!
int Gi0/0
  ipv6 traffic-filter Deny_Telnet in
!
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Question No : 4 - (Topic 1)

Which protocol does VRF-Lite support?

- A. IS-IS
- B. ODR
- C. EIGRP
- D. IGRP

Answer: C

Question No : 5 - (Topic 1)

Refer to the exhibit.

```
R1#show running-config | section dhcp
ip dhcp excluded-address 192.168.1.1 192.168.1.49
ip dhcp pool DHCP
  network 192.168.1.0 255.255.255.0
  default-router 192.168.1.1
  dns-server 8.8.8.8
  lease 0 12
```

Users report that IP addresses cannot be acquired from the DHCP server. The DHCP server is configured as shown. About 300 total nonconcurrent users are using this DHCP server, but none of them are active for more than two hours per day. Which action fixes the issue within the current resources?

- A. Modify the subnet mask to the network 192.168.1.0 255.255.254.0 command in the DHCP pool
- B. Configure the DHCP lease time to a smaller value
- C. Configure the DHCP lease time to a bigger value
- D. Add the network 192.168.2.0 255.255.255.0 command to the DHCP pool

Answer: B

Question No : 6 - (Topic 1)

Refer to the exhibit.

```
R1(config) # do show running-config | section line|username
username cisco secret 5 $1$yb/o$L3G5cXODxpYMSJ70PzEyo0
line con 0
  logging synchronous
line vty 0 4
  login local
  transport input telnet
R1(config) # logging console 7
R1(config) # do debug aaa authentication
R1(config) #
```

An administrator that is connected to the console does not see debug messages when remote users log in. Which action ensures that debug messages are displayed for remote logins?

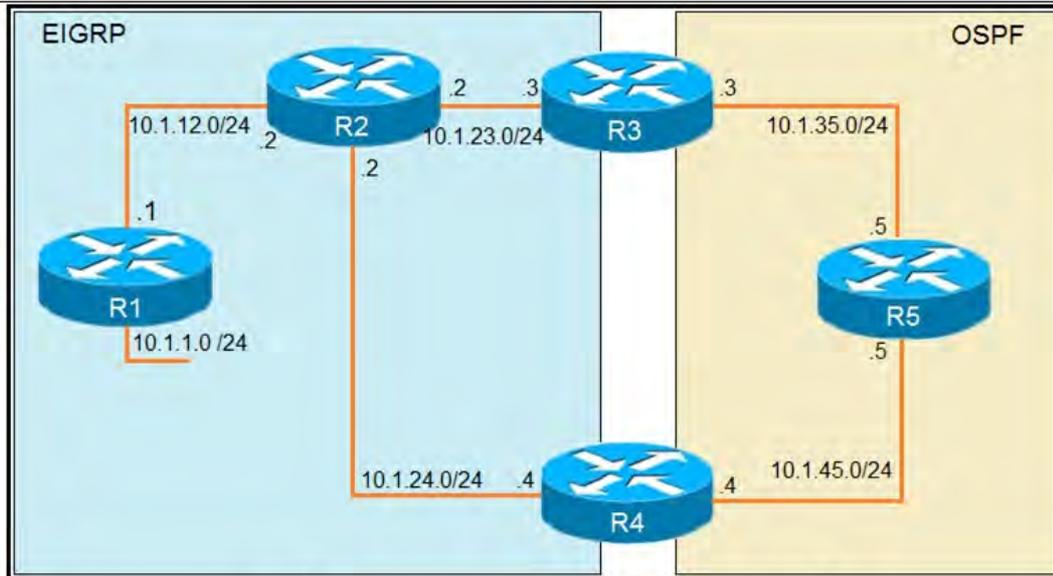
- A. Enter the transport input ssh configuration command.
- B. Enter the terminal monitor exec command.
- C. Enter the logging console debugging configuration command.
- D. Enter the aaa new-model configuration command.

Answer: C

Explanation: The logging console is a default and hidden command.

Question No : 7 - (Topic 1)

Refer to the exhibit.



```

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

 0 10.1.35.3 80 msec 44 msec 20 msec
 1 10.1.23.2 44 msec 104 msec 64 msec
 2 10.1.24.4 44 msec 64 msec 40 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 truncated>

```

The output of the trace route from R5 shows a loop in the network. Which configuration prevents this loop?

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
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: A

Explanation: The reason for the loop is that R2 is forwarding the packets destined to 10.1.1.1 to R4, instead of R1. This is because in the redistribute OSPF statement, BW metric has a higher value and delay has a value of 1. So, R2 chooses R4 over R1 for 10.1.1.0/24 subnet causing a loop. Now, R5 learns 10.1.1.0/24 from R3 and advertises the same route to R4, that R4 redistributes back in EIGRP. If R3 sets a tag of 1 while redistributing EIGRP in OSPF, and R4 denies all the OSPF routes with tag 1 while redistributing, it will not advertise 10.1.1.0/24 back into EIGRP. Hence, the loop will be

broken.

Question No : 8 DRAG DROP - (Topic 1)

Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

IPv6 DHCPv6 Guard	Block a malicious host and permit the router from a legitimate route
IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents.
IPv6 Source Guard	Create a binding table that is based on NS and NA messages.
IPv6 RA Guard	Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.
IPv6 ND Inspection	Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

Answer:

IPv6 DHCPv6 Guard	IPv6 RA Guard
IPv6 Binding Table	IPv6 DHCPv6 Guard
IPv6 Source Guard	IPv6 ND Inspection
IPv6 RA Guard	IPv6 Source Guard
IPv6 ND Inspection	IPv6 Binding Table

Explanation:



Graphical user

interface, chart

Description automatically generated

Question No : 9 - (Topic 1)

Refer to the exhibit.

```

access-list 100 deny tcp any any eq 465
access-list 100 deny tcp any eq 465 any
access-list 100 permit tcp any any eq 80
access-list 100 permit tcp any eq 80 any
access-list 100 permit udp any any eq 443
access-list 100 permit udp any eq 443 any

```

During troubleshooting it was discovered that the device is not reachable using a secure web browser. What is needed to fix the problem?

- A. permit tcp port 443
- B. permit udp port 465
- C. permit tcp port 465
- D. permit tcp port 22

Answer: A

Question No : 10 - (Topic 1)

Refer to the exhibit.

```

R200#show ip bgp summary
BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 26, main routing table version 26
1 network entries using 132 bytes of memory
1 path entries using 52 bytes of memory
2/1 BGP path/bestpath attribute entries using 296 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 2) using 28 bytes of memory
BGP using 508 total bytes of memory
BGP activity 24/23 prefixes, 24/23 paths, scan interval 60 secs
Neighbor    V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
192.0.2.2   4  65100 20335   20329    0  0  0 00:02:04  Idle (PfxCt)
R200#

```

In which circumstance does the BGP neighbor remain in the idle condition?

- A. if prefixes are not received from the BGP peer
- B. if prefixes reach the maximum limit
- C. if a prefix list is applied on the inbound direction

D. if prefixes exceed the maximum limit

Answer: D

Explanation: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/25160-bgp-maximum-prefix.html#b>

Question No : 11 - (Topic 1)

Refer to the exhibit.

```
router eigrp 1
 redistribute ospf 5 match external route-map OSPF-TO-EIGRP
 metric 10000 2000 255 1 1500
 route-map OSPF-TO-EIGRP
 match ip address TO-OSPF
```

Which routes from OSPF process 5 are redistributed into EIGRP?

- A. E1 and E2 subnets matching access list TO-OSPF
- B. E1 and E2 subnets matching prefix list TO-OSPF
- C. only E2 subnets matching access list TO-OSPF
- D. only E1 subnets matching prefix list TO-OS1

Answer: A

Question No : 12 - (Topic 1)

Refer the exhibit.

```
R3#show policy-map control-plane
Control Plane

Service-policy output: R3_CoPP

Class-map: mgmt (match-all)
 361 packets, 73858 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: access-group 120
 police:
   cir 8000 bps, bc 1500 bytes, be 1500 bytes
   conformed 8 packets, 1506 bytes; actions:
     transmit
   exceeded 353 packets, 72352 bytes; actions:
     drop
   violated 0 packets, 0 bytes; actions:
     drop
   conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any)
 124 packets, 10635 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match: any
R3#show access-lists 120
Extended IP access list 120
 10 permit udp any any eq snmptrap (361 matches)
```

Which action resolves intermittent connectivity observed with the SNMP trap packets?

- A. Decrease the committed burst Size of the mgmt class map
- B. Increase the CIR of the mgmt class map
- C. Add a new class map to match TCP traffic
- D. Add one new entry in the ACL 120 to permit the UDP port 161

Answer: B

Question No : 13 - (Topic 1)

Refer to the exhibit.

```

R1(config)#route-map ADD permit 20
R1(config-route-map)#set tag 1

R1(config)#router ospf1
R1(config-router)#redistribute rip subnets route-map ADD
    
```

Which statement about R1 is true?

- A. OSPF redistributes RIP routes only if they have a tag of one.
- B. RIP learned routes are distributed to OSPF with a tag value of one.
- C. R1 adds one to the metric for RIP learned routes before redistributing to OSPF.
- D. RIP routes are redistributed to OSPF without any changes.

Answer: B

Question No : 14 DRAG DROP - (Topic 1)

Drag and drop the MPLS VPN concepts from the left onto the correct descriptions on the right.

route distinguisher	propagates VPN reachability information
route target	distributes labels for traffic engineering
Resource Reservation Protocol	uniquely identifies a customer prefix
multiprotocol BGP	controls the import/export of customer prefixes

Answer:

route distinguisher	multiprotocol BGP
route target	Resource Reservation Protocol
Resource Reservation Protocol	route distinguisher
multiprotocol BGP	route target



Explanation:

Question No : 15 - (Topic 1)

Which command displays the IP routing table information that is associated with VRF-Lite?

- A. show ip vrf
- B. show ip route vrf
- C. show run vrf
- D. show ip protocols vrf

Answer: B

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/50sg/configuration/guide/Wrapper-46SG/vrf.html#wp1045708>

Question No : 16 - (Topic 1)

Refer to the exhibit.

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

Network operations cannot read or write any configuration on the device with this configuration from the operations subnet. Which two configurations fix the issue? (Choose two.)

- 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 access list 1 and allow SNMP in the access list.
- D. Configure SNMP rw permission in addition to version 1.
- E. Configure SNMP rw permission in addition to community ciscotest 1.

Answer: B,E

Question No : 17 - (Topic 1)

Refer to Exhibit.

```
router ospf 10
  router-id 192.168.1.1
  log-adjacency-changes
  redistribute bgp 1 subnets route-map BGP-TO-OSPF
  !
  route-map BGP-TO-OSPF deny 10
    match ip address 50
  route-map BGP-TO-OSPF permit 20
  !
  access-list 50 permit 172.16.1.0 0.0.0.255
```

Which statement about redistribution from BGP into OSPF process 10 is true?

- A. Network 172.16.1.0/24 is not redistributed into OSPF.
- B. Network 10.10.10.0/24 is not redistributed into OSPF
- C. Network 172.16.1.0/24 is redistributed with administrative distance of 1.
- D. Network 10.10.10.0/24 is redistributed with administrative distance of 20.

Answer: A

Question No : 18 - (Topic 1)

Which SNMP verification command shows the encryption and authentication protocols that are used in

SNMPV3?

- A. show snmp group
- B. show snmp user
- C. show snmp
- D. show snmp view

Answer: B

Question No : 19 - (Topic 1)

An engineer is configuring a network and needs packets to be forwarded to an interface for any destination address that is not in the routing table. What should be configured to accomplish this task?

- A. set ip next-hop
- B. set ip default next-hop
- C. set ip next-hop recursive
- D. set ip next-hop verify-availability

Answer: B

The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address **does not exist**, the command policy routes the packet by **sending it to the specified next hop**.

Explanation:

Question No : 20 - (Topic 1)

Which statement about IPv6 RA Guard is true?

- A. It does not offer protection in environments where IPv6 traffic is tunneled.
- B. It cannot be configured on a switch port interface in the ingress direction.
- C. Packets that are dropped by IPv6 RA Guard cannot be spanned.
- D. It is not supported in hardware when TCAM is programmed.

Answer: A

Explanation: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xs-3s/ip6f-xe-3s-book/ip6-ra-guard.html#GUID-589AF00C-7499-439F-AD23-51005D61CAB7

The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xs-16/ip6f-xe-16-book/ip6-ra-guard.pdf

Question No : 21 - (Topic 1)

Refer to the exhibit.

```
Global RADIUS shared secret:*****
retransmission count:5
timeout value:10
following RADIUS servers are configured:
  myradius.cisco.users.com:
    available for authentication on port:1814
    available for accounting on port:1813
  10.1.1.1:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
  10.2.2.3:
    available for authentication on port:1814
    available for accounting on port:1813
    RADIUS shared secret:*****
```

AAA server 10.1.1.1 is configured with the default authentication and accounting settings, but the switch cannot communicate with the server Which action resolves this issue?

- A. Match the authentication port
- B. Match the accounting port
- C. Correct the timeout value.
- D. Correct the shared secret.

Answer: A

Explanation:

Command Default

Accounting port: 1813

Authentication port: 1812

Accounting: enabled

Authentication: enabled

Retransmission count: 1

Idle-time: 0

Server monitoring: disabled

Timeout: 5 seconds

Test username: test

Test password: test

Reference:

https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/radius-server-host.html

By default, RADIUS uses UDP port 1812 for authentication and port 1813 for accounting. In the

exhibit above we see port 1814 is being used for authentication to AAA server at 10.1.1.1 which

is not the default port so we must adjust the authentication port to the default value 1812.

Question No : 22 - (Topic 1)

Refer to the exhibit.

```
R1#show policy-map control-plane
Control Plane
  Service-policy input: CoPP-BGP
    Class-map: BGP (match all)
      2716 packets, 172071 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group name BGP
      drop

    Class-map: class-default (match-any)
      5212 packets, 655966 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

What is the result of applying this configuration?

- A. The router can form BGP neighborships with any other device.
- B. The router cannot form BGP neighborships with any other device.
- C. The router cannot form BGP neighborships with any device that is matched by the access list named "BGP".
- D. The router can form BGP neighborships with any device that is matched by the access list named "BGP".

Answer: C

Explanation: after bgp session are UP.I configured the CoPP to drop 10.3.3.3 bgp traffic (R3).

R3 bgp traffic that matched the ACL 100 is dropped and the state is in IDLE

```
-----  
access-list 100 permit tcp host 10.3.3.3 any eq bgp  
access-list 100 permit tcp host 10.3.3.3 eq bgp any  
!  
class-map match-all class-bgp  
match access-group 100  
!  
policy-map policy-bgp  
class class-bgp  
drop  
!  
control-plane  
service-policy input policy-bgp  
!  
The 10.3.3.3 neighbor goes to IDLE
```

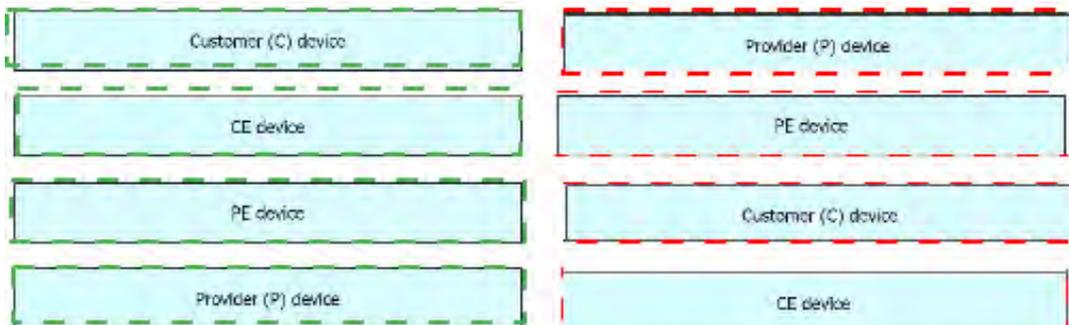
Question No : 23 DRAG DROP - (Topic 1)

Drag and drop the MPLS VPN device types from me left onto the definitions on the right.

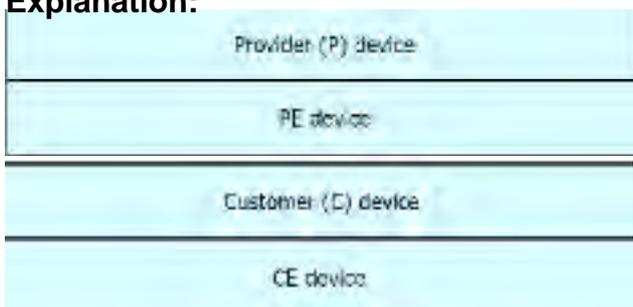
Cisco 300-410 : Practice Test

Customer (C) device	device in the core of the provider network that switches MPLS packets
CE device	device that attaches and detaches the VPN labels to the packets in the provider network
PE device	device in the enterprise network that connects to other customer devices
Provider (P) device	device at the edge of the enterprise network that connects to the SP network

Answer:



Explanation:



Question No : 24 - (Topic 1)

Which component of MPLS VPNs is used to extend the IP address so that an engineer is able to

identify to which VPN it belongs?

- A. VPNv4 address family
- B. RD
- C. RT
- D. LDP

Answer: B

- Specify the correct route distinguisher used for that VPN. This is used to extend the IP address so that you can identify which VPN it belongs to.

Explanation:

`rd <VPN route distinguisher>`

Question No : 25 - (Topic 1)

Refer to the exhibit.

```
R1#show running-config | include aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login Console local
R1#show running-config | section line
line con 0
  logging synchronous
R1#
```

An engineer is trying to configure local authentication on the console line, but the device is trying to authenticate using TACACS+. Which action produces the desired configuration?

- A. Add the `aaa authentication login default none` command to the global configuration.
- B. Replace the capital "C" with a lowercase "c" in the `aaa authentication login Console local` command.
- C. Add the `aaa authentication login default group tacacs+ local-case` command to the global configuration.
- D. Add the `login authentication Console` command to the line configuration

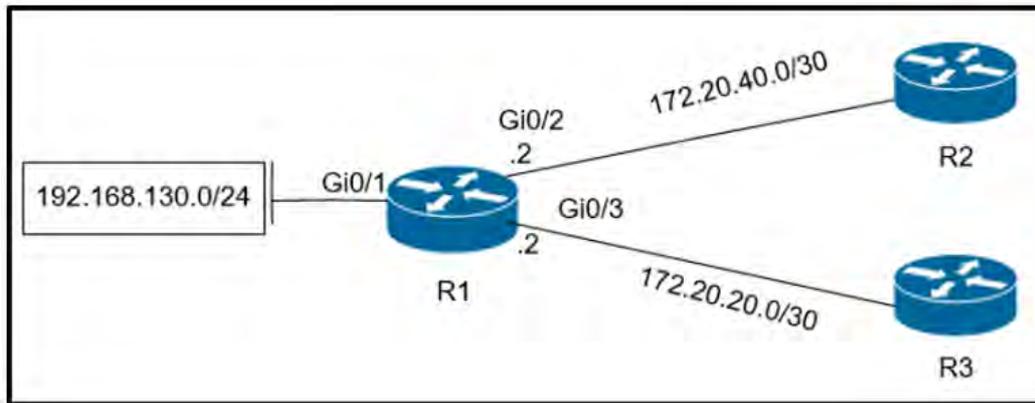
Answer: D

Reference:

<https://community.cisco.com/t5/switching/how-to-define-login-local-for-console-0/td-p/2949493>

Question No : 26 - (Topic 1)

Refer to the exhibit.



Which configuration configures a policy on R1 to forward any traffic that is sourced from the 192.168.130.0/24 network to R2?

- A. **access-list 1 permit 192.168.130.0 0.0.0.255**
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.2
- B. **access-list 1 permit 192.168.130.0 0.0.0.255**
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.2

- C. **access-list 1 permit 192.168.130.0 0.0.0.255**
!
interface Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1
- D. **access-list 1 permit 192.168.130.0 0.0.0.255**
!
interface Gi0/1
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.40.1

- A. Option A
B. Option B
C. Option C
D. Option D

Answer: D

Question No : 27 - (Topic 1)

Refer to the exhibit.

```
R1#show ip ssh
SSH Disabled – version 1.99
%Please create RSA keys to enable SSH (and of atleast 768 bits for SSH v2).
Authentication timeout: 120 secs; Authentication retries: 3
Minimum expected Diffie Hellman key size: 1024 bits
IOS Keys in SECSH format (ssh-rsa, base64 encoded) : NONE
R1#
```

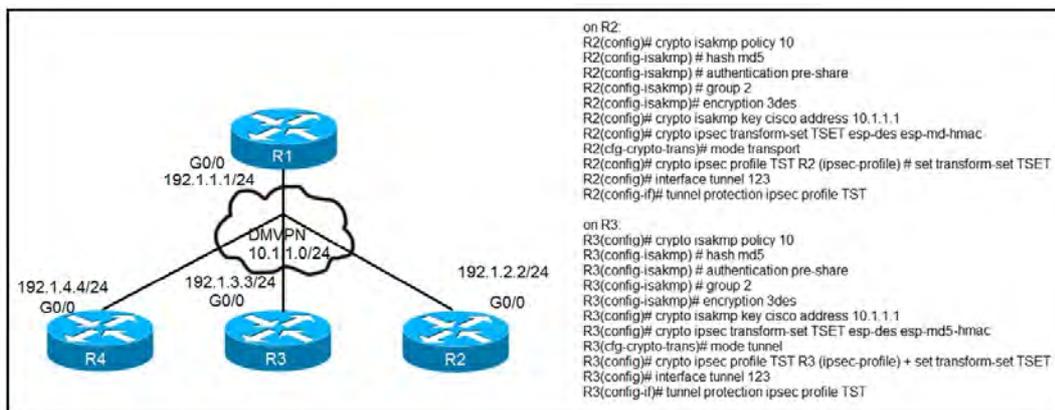
An engineer is trying to connect to a device with SSH but cannot connect. The engineer connects by using the console and finds the displayed output when troubleshooting. Which command must be used in configuration mode to enable SSH on the device?

- A. no ip ssh disable
- B. ip ssh enable
- C. ip ssh version 2
- D. crypto key generate rsa

Answer: D

Question No : 28 - (Topic 1)

Refer to the exhibit.



After applying IPsec, the engineer observed that the DMVPN tunnel went down, and both spoke-to-spoke and hub were not establishing. Which two actions resolve the issue? (Choose two.)

- A. Configure the crypto isakmp key cisco address 192.1.1.1 on R2 and R3
- B. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.
- C. Change the mode from mode tunnel to mode transport on R3
- D. Change the mode from mode transport to mode tunnel on R2.
- E. Remove the crypto isakmp key cisco address 10.1.1.1 on R2 and R3

Answer: A,D

Explanation:

*When using DMVPN with IPsec, it is unnecessary to use tunnel mode. Because DMVPN uses GRE which means that a new IP header is already added by GRE. The GRE

encapsulation happens on the tunnel interface before the encryption process takes place.

Question No : 29 - (Topic 1)

What is an advantage of using BFD?

- A. It detects local link failure at layer 1 and updates routing table.
- B. It detects local link failure at layer 2 and updates routing protocols.
- C. It has sub-second failure detection for layer 1 and layer 3 problems.
- D. It has sub-second failure detection for layer 1 and layer 2 problems.

Answer: D

Question No : 30 - (Topic 1)

Which label operations are performed by a label edge router?

- A. SWAP and POP
- B. SWAP and PUSH
- C. PUSH and PHP
- D. PUSH and POP

Answer: D

Explanation: A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network.

LERs push an MPLS label onto an incoming packet and pop it off an outgoing packet.

Reference:

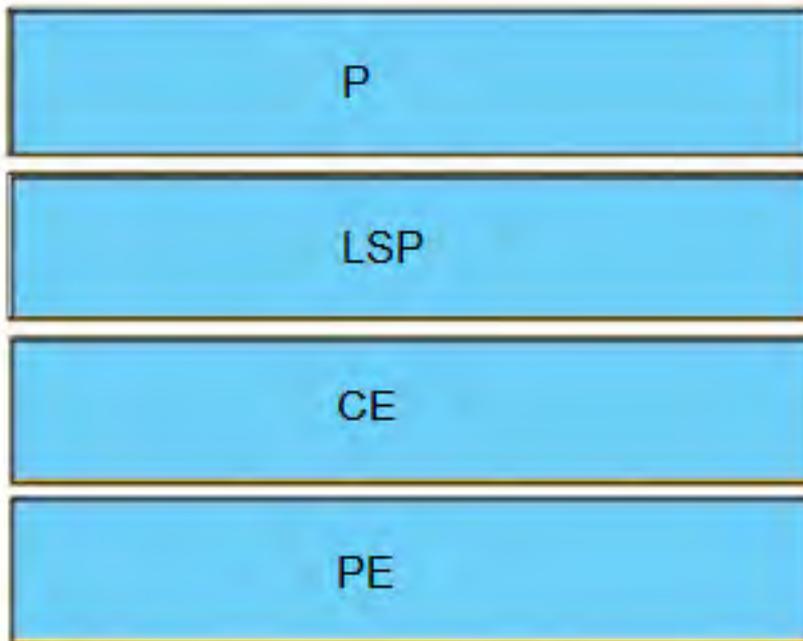
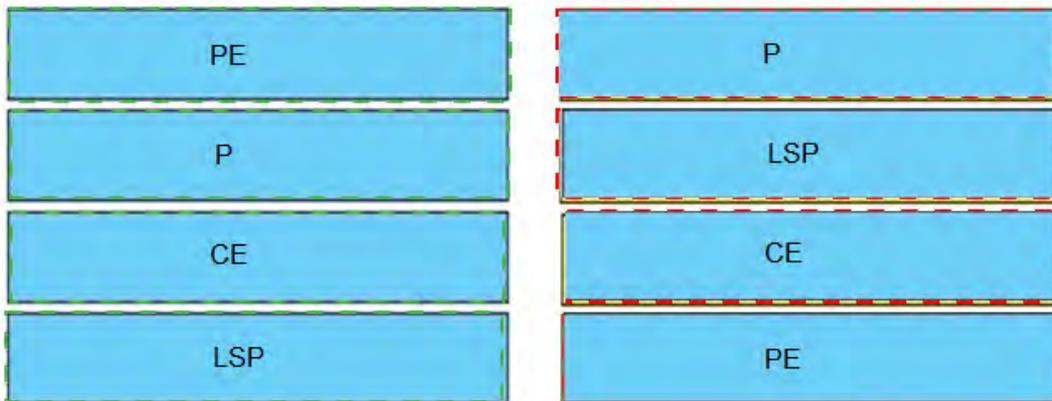
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/mpls/configuration/guide/mpls_cg/mp_mpls_overview.pdf

Question No : 31 DRAG DROP - (Topic 1)

Drag and drop the MPLS terms from the left onto the correct definitions on the right.

PE	device that forwards traffic based on labels
P	path that the labeled packet takes
CE	device that is unaware of MPLS labeling
LSP	device that removes and adds the MPLS labeling

Answer:



Explanation:

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: A,C

Question No : 33 - (Topic 1)

What is a function of IPv6 ND inspection?

- A. It learns and secures bindings for stateless autoconfiguration addresses in Layer 3 neighbor tables
- B. It learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor tables
- C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables.
- D. It learns and secures bindings for stateful autoconfiguration addresses in Layer 3 neighbor tables.

Answer: B

Question No : 34 - (Topic 1)

Refer to the exhibit.

```

R1 #show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 65000
<output omitted>
Neighbor    V AS   MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down  State/PfxRcd
192.168.2.2 4 65000    28    28        22     0    0   00:21:31      0
R1#show ip bgp
BGP table version is 22, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
               r RIB-failure, s stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, C RIB-compressed,
Origin codes: i – IGP, e – EGP, ? – incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop           Metric LocPrf   Weight    Path
* > 172.16.25.0/24    209.165.200.225      0           32768      ?
R1#

```

```

R2 #show ip bgp summary
BGP router identifier 192.168.2.2, local AS number 65000
<output omitted>
Neighbor    V AS   MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down  State/PfxRcd
192.168.1.1 4 65000    29    28         3     0    0   00:22:07      1
192.168.3.3 4 65000     7     8         3     0    0   00:02:55      0
R2#show ip bgp
BGP table version is 3, local router ID is 192.168.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
               r RIB-failure, s stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, C RIB-compressed,
Origin codes: i – IGP, e – EGP, ? – incomplete
RPKI validation codes: V valid, I invalid, N Not found

   Network          Next Hop           Metric LocPrf   Weight    Path
* i 172.16.25.0/24    209.165.200.225      0         100         0      ?
R2#

```

```

R3 #show ip bgp summary
BGP router identifier 192.168.3.3, local AS number 65000
BGP table version is 4, main routing table version 4
Neighbor    V AS   MsgRcvd  MsgSent   Tblver  InQ  OutQ  Up/Down  State/PfxRcd
192.168.2.2 4 65000     8     7         4     0    0   00:03:08      0
R3#

```

R2 is a route reflector, and R1 and R3 are route reflector clients. The route reflector learns the route to 172.16.25.0/24 from R1, but it does not advertise to R3. What is the reason the route is not advertised?

- A. R2 does not have a route to the next hop, so R2 does not advertise the prefix to other clients.
- B. Route reflector setup requires full IBGP mesh between the routers.
- C. In route reflector setup, only classful prefixes are advertised to other clients.
- D. In route reflector setups, prefixes are not advertised from one client to another.

Answer: A

What is the output of the following command:

```
show ip vrf
```

- A. Show's default RD values
- B. Displays IP routing table information associated with a VRF
- C. Show's routing protocol information associated with a VRF.
- D. Displays the ARP table (static and dynamic entries) in the specified VRF

Answer: A

Question No : 36 - (Topic 1)

Refer to the exhibit.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 1.1.1.1
R1(config)# ip route 0.0.0.0 0.0.0.0 2.2.2.2 10
R1(config)# ip sla 1
R1(config)# icmp-echo 1.1.1.1 source-interface FastEthernet0/0
R1(config)# ip sla schedule 1 life forever start-time now

R1(config)# track 1 ip sla 1 reachability
```

An IP SLA is configured to use the backup default route when the primary is down, but it is not working as desired. Which command fixes the issue?

- A. R1(config)# ip route 0.0.0.0.0.0.0.0.2.2.2.2 10 track 1
- B. R1(config)# ip route 0.0.0.0.0.0.0.0.2.2.2.2
- C. R1(config)#ip sla track 1
- D. R1(config)# ip route 0.0.0.0.0.0.0.0.1.1.1.1 track 1

Answer: D

Reference:

Note: By default Static Router AD value-1 hence ip route 0.0.0.0. 0.0.0.0. 1.1.1.1 track 1 means AD-1 which must be less than of back up route AD.

Define the backup route to use when the tracked object is unavailable. !--- The administrative distance of the backup route must be greater than !--- the administrative distance of the tracked route.!--- If the primary gateway is unreachable, that route is removed!--- and the backup route is installed in the routing table!--- instead of the tracked route.

<https://www.cisco.com/c/en/us/support/docs/ip/ip-routing/200785-ISP-Failover-with-default-routes-using-l.html>

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118962-configure-asa-00.html>

Question No : 37 - (Topic 1)

Refer to the exhibit.

```
Router# show tag-switching tdp bindings
(...)
tib entry: 10.10.10.1/32, rev 31
    local binding: tag: 18
    remote binding: tsr: 10.10.10.1:0, tag: imp-null
    remote binding: tsr: 10.10.10.2:0, tag: 18
    remote binding: tsr: 10.10.10.6:0, tag: 21
tib entry: 10.10.10.2/32, rev 22
    local binding: tag: 17
    remote binding: tsr: 10.10.10.2:0, tag: imp-null
    remote binding: tsr: 10.10.10.1:0, tag: 19
    remote binding: tsr: 10.10.10.6:0, tag: 22
```

What does the imp-null tag represent in the MPLS VPN cloud?

- A. Pop the label
- B. Impose the label
- C. Include the EXP bit
- D. Exclude the EXP bit

Answer: A

Explanation: The imp-null (implicit null) tag instructs the upstream router to pop the tag entry off the tag stack before forwarding the packet.

Note: pop means remove the top MPLS label

Question No : 38 - (Topic 1)

Which protocol does MPLS use to support traffic engineering?

- A. Tag Distribution Protocol (TDP)
- B. Resource Reservation Protocol (RSVP)
- C. Border Gateway Protocol (BGP)
- D. Label Distribution Protocol (LDP)

Answer: B

Explanation:

MPLS TE provides a way to integrate TE capabilities (such as those used on Layer 2 protocols like ATM) into Layer 3 protocols (IP). MPLS TE uses an extension to existing protocols (Intermediate System-to-Intermediate System (IS-IS), Resource Reservation Protocol (RSVP), OSPF) to calculate and establish unidirectional tunnels that are set according to the network constraint. Traffic flows are mapped on the different tunnels depending on their destination.

Question No : 39 - (Topic 1)

Refer to the following output:

```
Router#show ip nhrp detail
```

```
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
```

```
TypE. dynamic, Flags: authoritative unique nat registered used
```

```
NBMA address: 10.12.1.2
```

What does the authoritative flag mean in regards to the NHRP information?

- A. It was obtained directly from the next-hop server.
- B. Data packets are process switches for this mapping entry.
- C. NHRP mapping is for networks that are local to this router.
- D. The mapping entry was created in response to an NHRP registration request.
- E. The NHRP mapping entry cannot be overwritten.

Answer: A

Question No : 40 - (Topic 1)

After some changes in the routing policy, it is noticed that the router in AS 45123 is being used as a transit AS router for several service providers. Which configuration ensures that

the branch router in AS 45123 advertises only the local networks to all SP neighbors?

A)

```
ip as-path access-list 1 permit ^45123
|
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

B)

```
ip as-path access-list 1 permit .*
|
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

C)

```
ip as-path access-list 1 permit ^45123$
|
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

D)

```
ip as-path access-list 1 permit ^$
|
router bgp 45123
 neighbor SP-Neighbors filter-list 1 out
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: D

Explanation: By default BGP advertises all prefixes to external BGP neighbors. This means that if you are multi-homed (connected to two or more ISPs) then you might become a transit AS. For example, ISP 2 in AS 200 can send traffic to your router in AS 100 to reach ISP 3 in AS 300 because you advertised prefixes in ISP 3 to ISP 2. This is what will be seen in the BGP routing table of ISP1:

```
ISP1#show ip bgp
--output omitted--
Network          Next Hop          Metric LocPrf Weight Path
....
*> 3.3.3.0/24    192.168.12.1          0 100 300 i
```

Question No : 41 - (Topic 1)

Exhibit:

```
policy-map COPP-7600
class COPP-CRITICAL-7600
  police cir 2000000 bc 62500
  conform-action transmit
  exceed-action transmit
!
class class-default
  police cir 200000 bc 6250
  conform-action transmit
  exceed-action drop
!
class-map match-all COPP-CRITICAL-7600
  match access-group name COPP-CRITICAL-7600
!
ip access-list extended COPP-CRITICAL-7600
  permit ip any any eq http
  permit ip any any eq https
```

BGP is flapping after the Copp policy is applied. What are the two solutions to fix the issue?

(Choose two)

- A. Configure BGP in the COPP-CRITICAL-7600 ACL
- B. Configure a higher value for CIR under the default class to allow more packets during peak traffic
- C. Configure a higher value for CIR under the class COPP-CRITICAL-7600
- D. Configure a three-color policer instead of two-color policer under class COPP-CRITICAL-7600
- E. Configure IP CEF to CoPP policy and BGP to work

Answer: A,B

Explanation: The policy-map COPP-7600 only rate-limit HTTP & HTTPS traffic (based on the ACL

conditions) so any BGP packets will be processed in the class "class-default", which drops exceeded BGP packets. Therefore we have two ways to solve this problem:

+ Add BGP to the ACL with the statement "permit tcp any any eq bgp"

+ Configure higher value for CIR in default class as 2Mbps is too low for web traffic (http & https)

Question No : 42 - (Topic 1)

Refer to the exhibit.

```
R1#show policy-map control-plane
Control Plane
Class-map: NMS (match-all)
500461 packets, 24038351 bytes
5 minute offered rate 1390000 bps, drop rate 0 bps
police:
  cir 50000 bps, bc 5000 bytes
conformed 50444 packets, 24031001 bytes; actions:
transmit
exceeded 990012 packets, 94030134 bytes; actions
drop conformed 4000 bps, exceed 0 bps
R1#
```

A company is evaluating multiple network management system tools. Trending graphs generated by SNMP data are returned by the NMS and appear to have multiple gaps. While troubleshooting the issue, an engineer noticed the relevant output. What solves the gaps in the graphs?

- A. Remove the exceed-rate command in the class map.
- B. Remove the class map NMS from being part of control plane policing.
- C. Configure the CIR rate to a lower value that accommodates all the NMS tools
- D. Separate the NMS class map in multiple class maps based on the specific protocols with appropriate CoPP actions

Answer: D

Reference:

https://tools.cisco.com/security/center/resources/copp_best_practices

The class-map NMS in the exhibit did not classify traffic into specific protocols so many packets

were dropped. We should create some class-map to classify the receiving traffic. It is also a recommendation of CoPP/CP policy:

“Developing a CPP policy starts with the classification of the control plane traffic. To that end,

the control plane traffic needs to be first identified and separated into different class maps.”

Question No : 43 - (Topic 1)

Which two statements about VRF-Lite configurations are true? (Choose two.)

- A. They support the exchange of MPLS labels
- B. Different customers can have overlapping IP addresses on different VPNs
- C. They support a maximum of 512.000 routes
- D. Each customer has its own dedicated TCAM resources
- E. Each customer has its own private routing table.
- F. They support IS-IS

Answer: B,E

Question No : 44 - (Topic 1)

During the maintenance window an administrator accidentally deleted the Telnet-related configuration that permits a Telnet connection from the inside network (Eth0/0) to the outside of the networking between Friday – Sunday night hours only. Which configuration resolves the issue?

A)

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

B)

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic 22:00 to 05:00
```

C)

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

D)

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
access-list 101 permit udp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255
eq telnet time-range changewindow
!
time-range changewindow
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Answer: C

Question No : 45 - (Topic 1)

Refer to the exhibit.

```
BRANCH-RTR#
router eigrp 100
network 10.4.31.0 0.0.0.7
network 10.100.100.1 0.0.0.0
distribute-list route-map FILTER-IN in FastEthernet0/0
eigrp router-id 10.100.100.1
!
ip prefix-list 102 seq 10 permit 10.1.1.100/32
!
route-map FILTER-IN deny 10
match ip address prefix-list 102
!
```

A junior engineer updated a branch router configuration. Immediately after the change, the engineer receives calls from the help desk that branch personnel cannot reach any network destinations. Which configuration restores service and continues to block 10.1.1.100/32?

- A. route-map FILTER-IN deny 5
- B. ip prefix-list 102 seq 15 permit 0.0.0.0/32 le 32