300-410Q&As

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

Pass Cisco 300-410 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/300-410.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

QUESTION 1

A network administrator is troubleshooting a failed AAA login issue on a Cisco Catalyst c3560 switch. When the network administrator tries to log in with SSH using TACACS+ username and password credentials, the switch is no longer authenticating and is failing back to the local account. Which action resolves this issue?

A. Configure ip tacacs source-interface GigabitEthernet 1/1

B. Configure ip tacacs source-ip 192.168.100.55

C. Configure ip tacacs-server source-ip 192.168.100.55

D. Configure ip tacacs-server source-interface GigabitEthernet 1/1

Correct Answer: A

R2(config)#ip tacacs so R2(config)#ip tacacs source-interface ? Async Async interface Auto-Template Auto-Template interface BVI Bridge-Group Virtual Interface CDMA-Ix CDMA Ix interface CTunnel CTunnel interface Dialer Dialer interface FastEthernet FastEthernet IEEE 802.3 Lex Lex interface Loopback Loopback interface MFR Multilink Frame Relay bundle interface Multilink Multilink-group interface Null Null interface Port-channel Ethernet Channel of interfaces SSLVPN-VIF SSLVPN Virtual Interface Tunnel Tunnel interface Vif PGM Multicast Host interface Virtual-PPP Virtual PPP interface Virtual-Template Virtual Template interface Virtual-TokenRing Virtual TokenRing vmi Virtual Multipoint Interface

R2(config)#ip tacacs source-interface

QUESTION 2

Refer to the exhibit. An engineer is trying to generate a summary route in OSPF for network 10.0.0.0/8, but the summary route does not show up in the routing table. Why is the summary route missing?

```
Router#show ip route
<output omitted>
Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
O        192.168.1.1 [110/11] via 192.168.12.1, 16:56:40, Ethernet0/0
      192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Loopback0
L        192.168.2.2/32 is directly connected, Loopback0
      192.168.3.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.3.0/24 is directly connected, Ethernet0/1
L        192.168.3.1/32 is directly connected, Ethernet0/1
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.2/32 is directly connected, Ethernet0/0
Router#show running-config | section ospf
router ospf 1
 summary-address 10.0.0.0 255.0.0.0
 redistribute static subnets
 network 192.168.3.0 0.0.0.255 area 0
 network 192.168.12.0 0.0.0.255 area 0
Router#
```

A. The summary-address command is used only for summarizing prefixes between areas.

B. The summary route is visible only in the OSPF database, not in the routing table.

C. There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated.

D. The summary route is not visible on this router, but it is visible on other OSPF routers in the same area.

Correct Answer: C

The summary-address is only used to create aggregate addresses for OSPF at an autonomous system boundary.

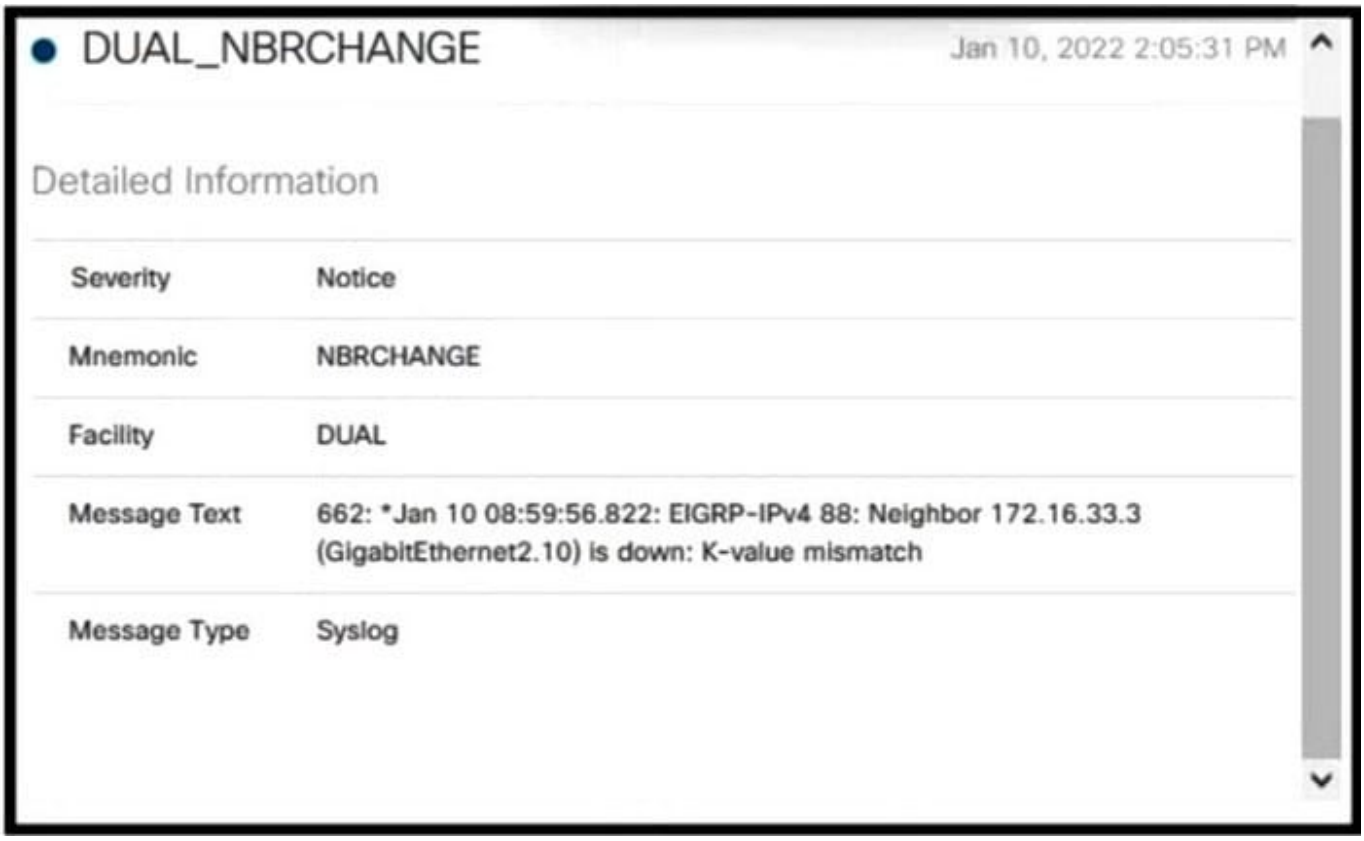
It means this command should only be used on the ASBR when you are trying to summarize externally redistributed routes from another protocol domain or you have a NSSA area. But a requirement to create a summarized route is:

The ASBR compares the summary route\\'s range of addresses with all routes redistributed into OSPF on that ASBR to find any subordinate subnets (subnets that sit inside the summary route range). If at least one subordinate subnet exists,

the ASBR advertises the summary route.

QUESTION 3

Refer to the exhibit.



EIGRP peering was lost.

Which configuration resolves the issue?

A.
```
router EIGRP 88
 metric weights  1 0 1 0 10
```

B.
```
router EIGRP 88
 metric weights 1 1 1 0 0 0
```

C.
```
router EIGRP 88
 metric weights 0 1 1 0 01
```

D.
```
router EIGRP 88
 metric weights 0 1 1 1 0 0
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 4

Which of the following commands enables Unicast Reverse Path forwarding in loose mode?

A. ip verify unicast source reachable-via rx

B. ip verify unicast source reachable-via any

C. ip verify unicast source reachable-via rx allow default

D. ip verify unicast source reachable-via allow default

Correct Answer: B

The command ip verify unicast source reachable-via any enables Unicast Reverse Path Forwarding (RPF) in loose mode. In loose mode, traffic is allowed if the source address is reachable via any interface on the router as indicted in the

routing table. Unicast Reverse Path forwarding uses the source IP address when it validates the packet. Packets are validated when the source address is contained in the routing table and is reachable either via the ingress interface (strict

mode) or via any interface (loose mode).

The command ip verify unicast source reachable-via rx enables Unicast RPF in strict mode, not loose mode. The rx keyword indicates the source must be reachable on the interface where the packet arrived.

The command ip verify unicast source reachable-via rx allow default enables Unicast RPF in strict mode. The inclusion of the allow default keyword indicates the source can be reachable via a default route to be accepted.

The command ip verify unicast source reachable-via allow default is syntactically incorrect. The allow default keyword cannot be present by itself. It must follow either the rx or any keywords.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify router security features

References:

Understanding Unicast Reverse Path Forwarding

Cisco > Cisco IOS Security Command Commands D to L > ip verify unicast source reachable-via

QUESTION 5

An automatic IPv4-compatible IPv6 tunnel exists between two IPv6 networks. The two IPv6 networks belong to different BGP autonomous systems (AS). The tunnel source has the IPv4 address 172.168.111.65/24 and the tunnel destination has the IPv4 address 172.168.222.80/24.

Which of the following statements is TRUE about the tunnel source and tunnel destination IPv6 addresses? (Choose two.)

A. the IPv6 address of the tunnel source is 172.168.111.65::

B. the IPv6 address of the tunnel source is ::172.168.111.65

C. the IPv6 address of the tunnel destination is 172.168.222.80::

D. the IPv6 address of the tunnel destination is ::172.168.222.80

Correct Answer: BD

The IPv6 address of the tunnel source is ::172.168.111.65 and the IPv6 address of the tunnel destination is

::172.168.222.80. These two addresses are IPv4-compatible IPv6 addresses, which are addresses that contain the IPv4 addresses of the tunnel source and destination.

In automatic IPv4-compatible IPv6 tunnel, the IPv4 addresses of the tunnel source and the tunnel destination are used to determine their IPv6 addresses. The IPv4 addresses of the tunnel source/destination are embedded into the least

significant 32 bits of an all-zero unicast IPv6 address. The resultant IPv6 address has zeros in the most significant 96 bits and the IPv4 address of the tunnel source/destination in the remaining 32 bits.

In this case, the source of an automatic IPv4-compatible IPv6 tunnel has the IPv6 address

0:0:0:0:0:0:172.168.111.65, abbreviated as ::2.168.111.65. You can also convert this address into pure hexadecimal format, which would be ACA8:6F41.

Any of the following three addresses could be used to identify the BGP neighbor at 172.168.11.65:

0:0:0:0:0:0:172.168.111.65 ::172.168.111.65 ::ACA8:6F41

Similarly, the tunnel destination has the IPv6 address 0:0:0:0:0:0:172.168.222.80 (abbreviated as ::172.168.222.80). The hexadecimal form of the IPv6 address of the tunnel destination is ::ACA8:DE50.

Any of the following three addresses could be used to identify the BGP neighbor at 172.168.222.80:

0:0:0:0:0:0:172.168.222.80 ::172.168.222.80 ::ACA8:DE50

The other two options state incorrect IPv6 addresses of the tunnel source and the tunnel destination. Both options specify an IPv6 address that has the IPv4 address of the tunnel source/destination in the most significant 32 bits and zeros in

the least significant 96 bits.

Objective:

Network Principles

Sub-Objective:

Recognize proposed changes to the network

References:

Home > Support > Technology Support > IP > IP Version 6 (IPv6) > Configure > Configuration Examples and Technotes > IPv6 Tunnel Through an IPv4 Network > Configure > Configurations (Automatic IPv4-Compatible Mode) Cisco IOS

IPv6 Implementation Guide > Implementing Tunneling for IPv6 Cisco > Support > Technology Support > IP > IP Version 6 (IPv6) > Technology Information > Technology White Paper > IPv6 Deployment Strategies > Selecting a Deployment

Strategy > Deploying IPv6 Over IPv4 Tunnels > Automatic IPv4-Compatible Tunnel