QUESTION 207
Refer to the exhibit. Bangkok is using ECMP to reach to the 192.168.5.0/24 network.
The administrator must configure Bangkok in such a way that Telnet traffic from 192.168.3.0/24 and192.168.4.0/24 networks uses the HongKong router as the preferred router.
Which set of configurations accomplishes this task?
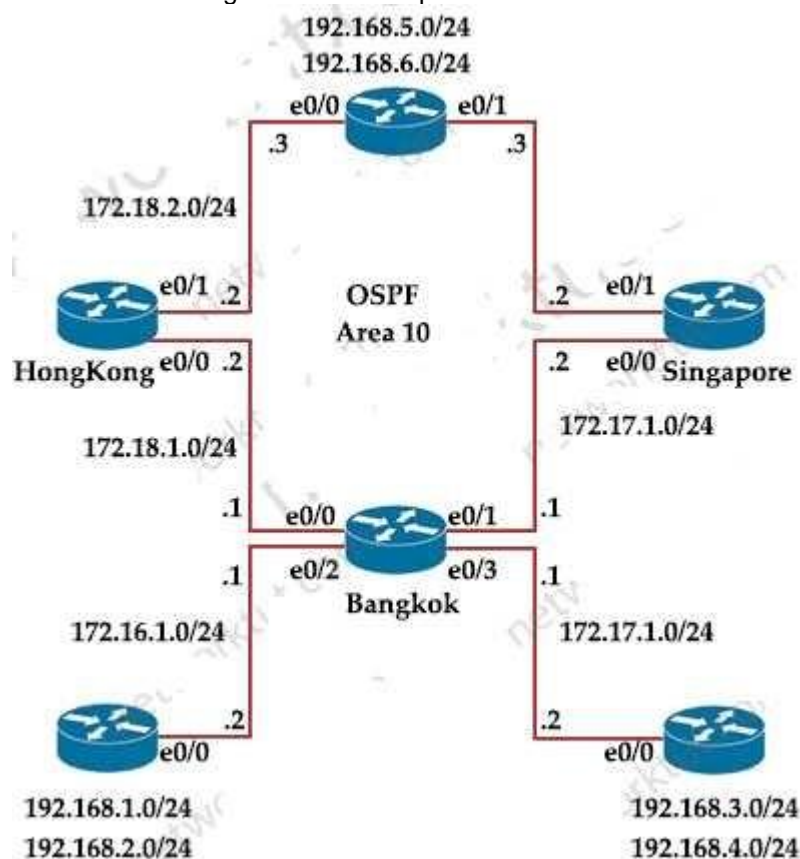
A. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
   access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 !
   route-map PBR1 permit 10
   match ip address 101
   set ip next-hop 172.18.1.2
   interface Ethernet0/3
   ip policy route-map PBR1
B. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
   access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 !
   route-map PBR1 permit 10
   match ip address 101
   set ip next-hop 172.18.1.2
   interface Ethernet0/1
   ip policy route-map PBR1
C. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23
   access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 eq 23 !
   route-map PBR1 permit 10
   match ip address 101
   set ip next-hop 172.18.1.2
   !
   interface Ethernet0/3
   ip policy route-map PBR1
D. access-list 101 permit tcp 192.168.3.0 0.0.0.255 192.168.5.0 0.0.0.255
   access-list 101 permit tcp 192.168.4.0 0.0.0.255 192.168.5.0 0.0.0.255 !
   route-map PBR1 permit 10
   match ip address 101
   set ip next-hop 172.18.1.2
   !
   interface Ethernet0/1
   ip policy route-map PBR1

Answer: C
Explanation:
We need to use Policy Based Routing (PBR) here on Bangkok router to match the traffic from 192.168.3.0/24 & 192.168.4.0/24 and "set ip next-hop" to HongKong router(172.18.1.2 in this case). Note: Please notice that we have to apply the PBR on incoming interface e0/3 to receive traffic from

192.168.3.0/24 and 192.168.4.0/24.

QUESTION 208
Refer to the exhibit. Which action resolves the authentication problem?

```
11:27:07.532: AAA/BIND (00000055): Bind i/
11:27:07.532: AAA/AUTHEN/LOGIN (00000055): Pick method list 'default'
11:27:07.532: TPLUS: Queuing AAA Authentication request 85 for processing
11:27:07.532: TPLUS (00000055) login timer started 1020 sec timeout
11:27:07.532: TPLUS: processing authentication start request id 85
11:27:07.532: TPLUS: Authentication start packet created for 85()
11:27:07.532: TPLUS: Using server 10.106.60.182
11:27:07.532: TPLUS (00000055)/0/NB_WAIT/225FE2DC: Started 5 sec timeout
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: socket event 2
11:27:07.532: TPLUS (00000055)/0/NB_WAIT: wrote entire 38 bytes request
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: Would block while reading
11:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: react entire 12 header bytes (expect 6 bytes data)
13:27:07.532: TPLUS (00000055)/0/READ: socket event 1
11:27:07.532: TPLUS (00000055)/0/READ: read entire 18 bytes response
11:27:07.532: TPLUS (00000055)/0/225FE2DC: Processing the reply packet
11:27:07.532: TPLUS: received bad AUTHEN packet: length = 6, expected 43974
11:27:07.532: TPLUS: Invalid AUTHEN packet (check keys).
```

A. Configure the user name on the TACACS+ server
B. Configure the UDP port 1812 to be allowed on the TACACS+ server
C. Configure the TCP port 49 to be reachable by the router
D. Configure the same password between the TACACS+ server and router.
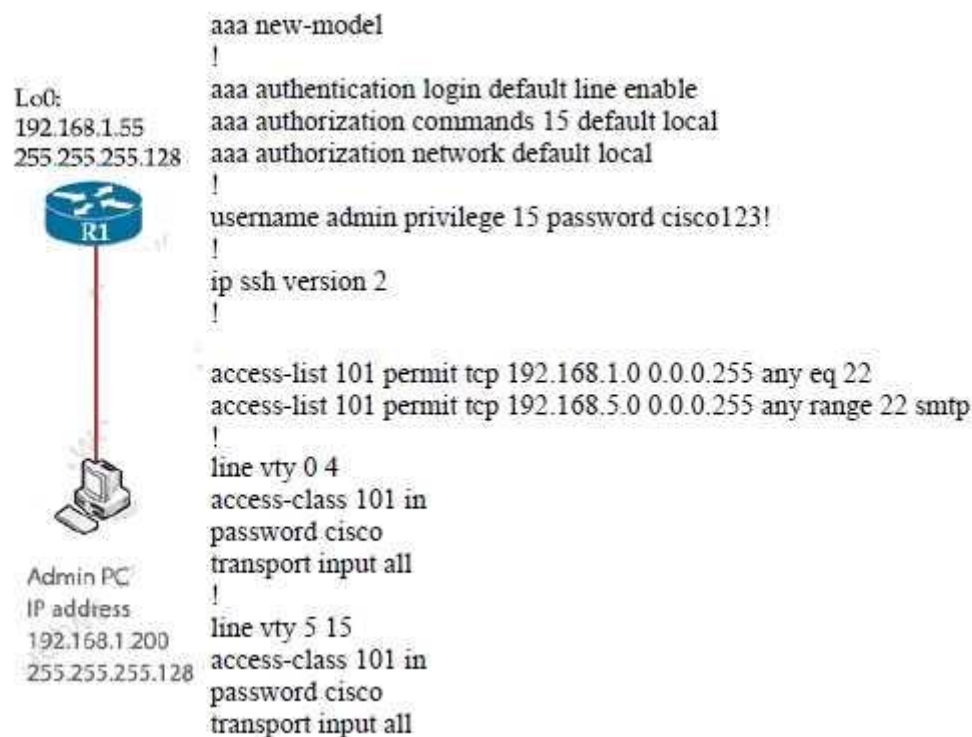
Answer: D
Explanation:
From the last line of the output, we notice that the result was "Invalid AUTHEN packet". Therefore something went wrong with the username or password.
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/200467-Troubleshoot-TACACS-Authentication-Issue.html

QUESTION 209
Refer to the exhibit. The administrator successfully logs into R1 but cannot access privileged mode commands. What should be configured to resolve the issue?


```
aaa new-model
!
aaa authentication login default line enable
aaa authorization commands 15 default local
aaa authorization network default local
!
username admin privilege 15 password cisco123!
!
ip ssh version 2
!
access-list 101 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 101 permit tcp 192.168.5.0 0.0.0.255 any range 22 smtp
!
line vty 0 4
access-class 101 in
password cisco
transport input all
!
line vty 5 15
access-class 101 in
password cisco
transport input all
```

Lo0:
192.168.1.55
255.255.255.128

R1

Admin PC
IP address
192.168.1.200
255.255.255.128

A. aaa authorization reverse-access
B. secret cisco123! at the end of the username command instead of password cisco123!
C. matching password on vty lines as cisco123!
D. enable secret or enable password commands to enter into privileged mode

Answer: D

QUESTION 210
Which two protocols work in the control plane of P routers across the MPLS cloud? (choose two)
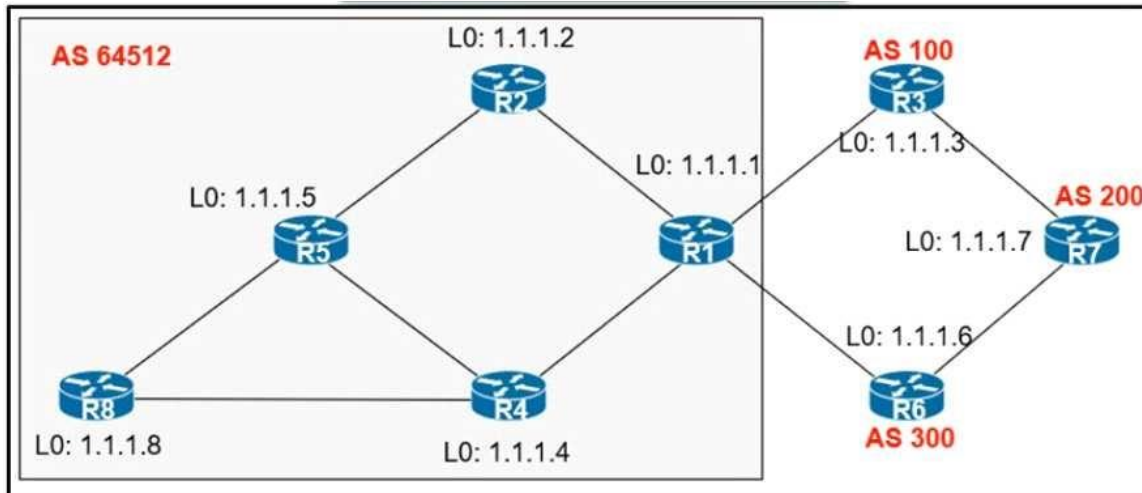
A. LSP
B. RSVP
C. ECMP
D. LDP
E. MPLS OAM

Answer: BD

QUESTION 211

Refer to the exhibit. An engineer configured R2 and R5 as route reflectors and noticed that not all routes are sent to R1 to advertise to the eBGP peers. Which iBGP routers must be configured as route reflectors to advertise all routes to restore reachability across all networks?

A. R1 and R4
B. R1 and R5
C. R4 and R5
D. R2 and R5

Answer: C
Explanation:
When R2 & R5 are route reflectors (RRs), routes from R4 & R8 are advertised to R5 and R5 advertises to R2. But R2 would drop them as R2 is also a RR. Thereforesome routes are missing on R1 to advertise to eBGP peers.
Route reflectors (RR) must be fully iBGP meshed so we cannot configure RR on both R1 and R5. We should choose routers at the center of the topology RRs, in this case R4 & R5.

QUESTION 212
Refer to exhibit. Routing protocols are mutually redistributed on R3 and R1. Users report intermittent connectivity to services hosted on the 10.1.1.0/24 prefix. Significant routing update changes are noticed on R3 when the show ip route profile command is run. How must the services be stabilized?
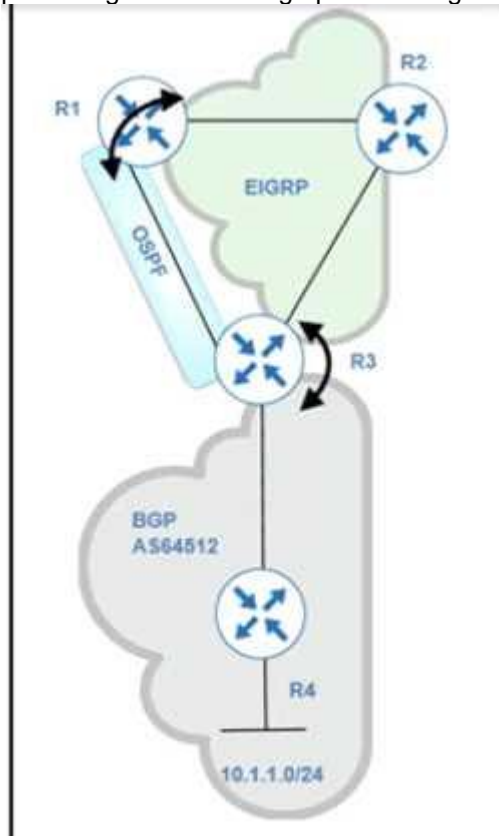
A. The issue with using BGP must be resolved by using another protocol and redistributing it into EIGRP on R3
B. The routing loop must be fixed by reducing the admin distance of iBGP from 200 to 100 on R3
C. The routing loop must be fixed by reducing the admin distance of OSPF from 110 to 80 on R3
D. The issue with using iBGP must be fixed by running eBGP between R3 and R4
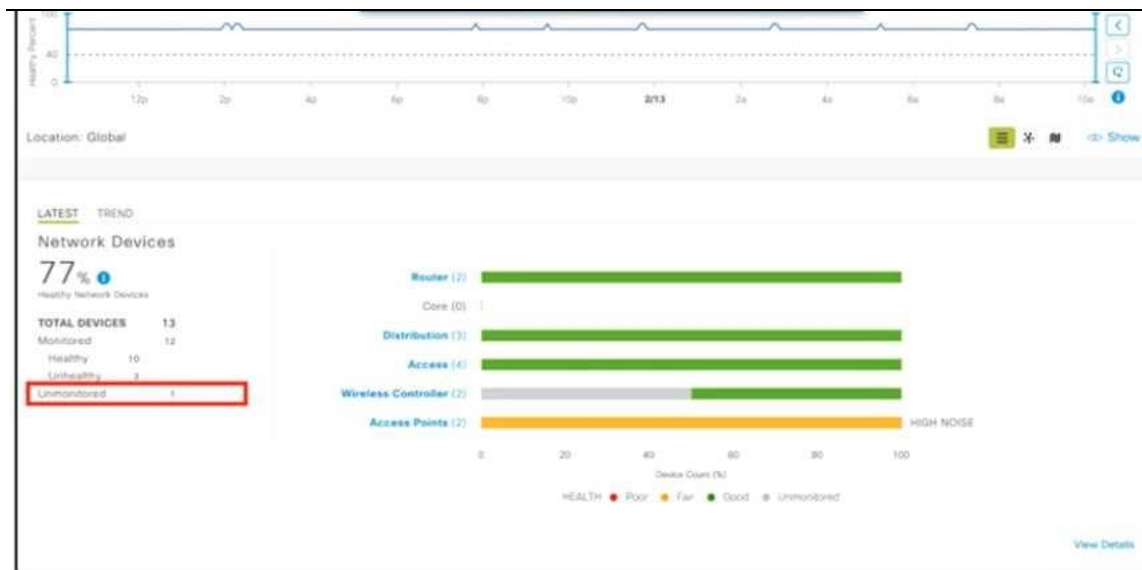
Answer: B
Explanation:
After redistribution, R3 learns about network 10.1.1.0/24 via two paths:+ Internal BGP (IBGP):
advertised from R4 with AD of 200 (and metric of 0)+ OSPF: advertised from R1 with AD of 110 (O E2) (and metric of 20)Therefore R3 will choose the path with the lower AD via OSPF But this is a looped path which is received from R3 -> R2 -> R1 -> R3. So when the advertised route from R4 is expired, the looped path is also expired soon and R3 willreinstall the main path from R4. This is the cause of intermittent connectivity.In order to solve this issue, we can lower the AD of iBGP to a value which is lower than 110 so that it is preferred over OSPF-advertised route.

QUESTION 213
Refer to Exhibit. A network administrator added one router in the Cisco DNA Center and checked its discovery and health from the Network Health Dashboard.
The network administratorobserved that the router is still showing up as unmonitored. What must be configured on the router to mount it in the Cisco DNA Center?

A. Configure router with NetFlow data
B. Configure router with the telemetry data
C. Configure router with routing to reach Cisco DNA Center
D. Configure router with SNMPv2c or SNMPv3 traps

Answer: B
Explanation:
Unmonitored: Unmonitored devices are devices for which Assurance did not receive any telemetry data during the specified time range.

QUESTION 214
Refer to the exhibit. NTP is configured across the network infrastructure and Cisco DNA Center. An NTP issue was reported on the Cisco DNA Center at 17:15. Which action resolves the issue?
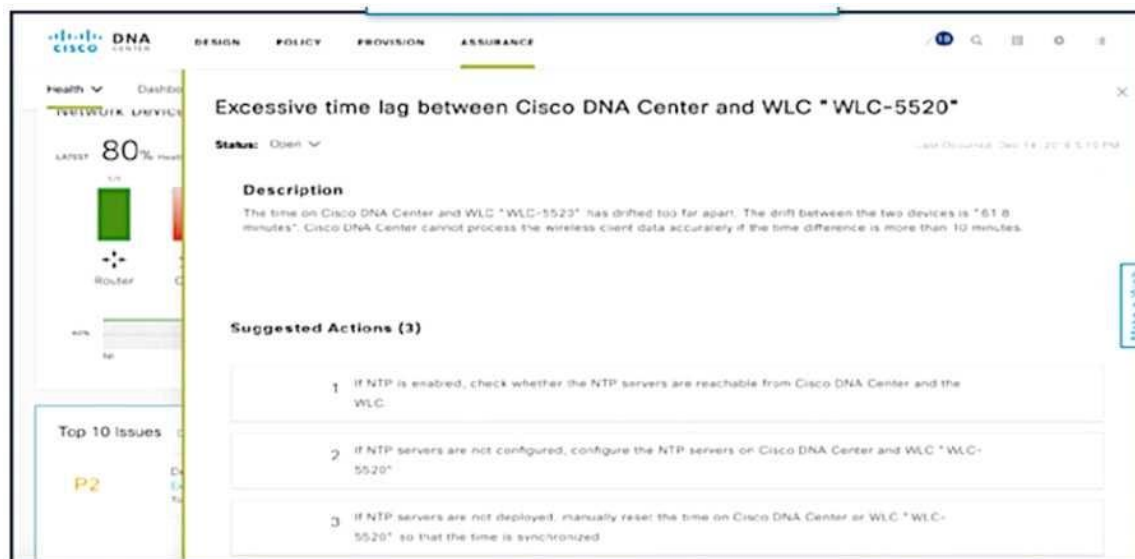
A. Check and resolve reachability between the WLC and the NTP server
B. Reset the NTP server to resolve any synchronization issues tor all devices
C. Check and resolve reachability between Cisco DNA Center and the NTP server
D. Check and configure NTP on the WLC and synchronize with Cisco DNA Center

Answer: D
Explanation:
Excessive time lag between Cisco DNA Center and device: The time difference between Cisco DNA Center and the device IP Address has drifted too far apart. CiscoDNA Center cannot process the device data accurately if the time difference is more than 3 minutes.
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/1-2-10/b_cisco_dna_assurance_1_2_10_ug/b_cisco_dna_assurance_1_2_10_ug_chapter_01101.html

QUESTION 215
Refer to Exhibit. A network administrator enables DHCP snooping on the Cisco Catalyst 3750-X switch and configures the uplink port (Port-channel2) as a trusted port. Clients are not receiving an IP address, but when DHCP snooping is disabled, clients start receiving IP addresses.
Which global command resolves the issue?

```
Jan 9 15:29:29.713: DHCP_SNOOPING: process new DHCP packet, message type: DHCPINFORM, input interface:
Po2, MAC da: ffff.ffff.ffff, DHCP yiaddr: 0.0.0.0, DHCP siaddr: 0.0.0.0, DHCP giaddr: 0.0.0.0
Jan 9 15:29:29.713: DHCP_SNOOPING_SW: bridge packet get invalid mat entry: FFFF.FFFF.FFFF, packet is
flooded to ingress VLAN: (1)
Jan 9 15:29:29.722: DHCP_SNOOPING_SW: bridge packet send packet to cpu port: Vlan1.
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Vl1 for pak. Was Po2
Jan 9 15:29:31.509: DHCPSNOOP(hlfm_set_if_input): Setting if_input to Po2 for pak. Was Vl1Jan 9
15:29:31.517: DHCP_SNOOPING: received new DHCP packet from input interface (Port-channel2)
```

A. No ip dhcp snooping information option
B. ip dhcp snooping
C. ip dhcp relay information trust portchannel2
D. ip dhcp snooping trust

Answer: A

QUESTION 216
Which configuration feature should be used to block rogue router advertisements instead of using the IPv6 Router Advertisement Guard feature?

A. VACL blocking broadcast frames from nonauthorized hosts
B. PVLANs with promiscuous ports associated to route advertisements and isolated ports for nodes
C. PVLANs with community ports associated to route advertisements and isolated ports for nodes
D. IPv4 ACL blocking route advertisements from nonauthorized hosts

Answer: D
Explanation:
The IPv6 Router Advertisement Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue router advertisement guard messages that arrive at the network device platform. Router Advertisements are used by devices to announce themselves on the link. The IPv6 Router Advertisement Guard feature analyzes these router advertisements and filters out router advertisements that are sent by unauthorized devices. Certain switch platforms can already implement some level of rogue RA filtering by the administrator configuring Access Control Lists (ACLs) that block RA ICMP messages that might be inbound on "user" ports.
Reference: https://datatracker.ietf.org/doc/html/rfc6104

QUESTION 217
Refer to Exhibit. AS 111 wanted to use AS 200 as the preferred path for 172.20.5.0/24 and AS 100 as the backup. After the configuration, AS 100 is not used for any other routes. Whichconfiguration resolves the issue?
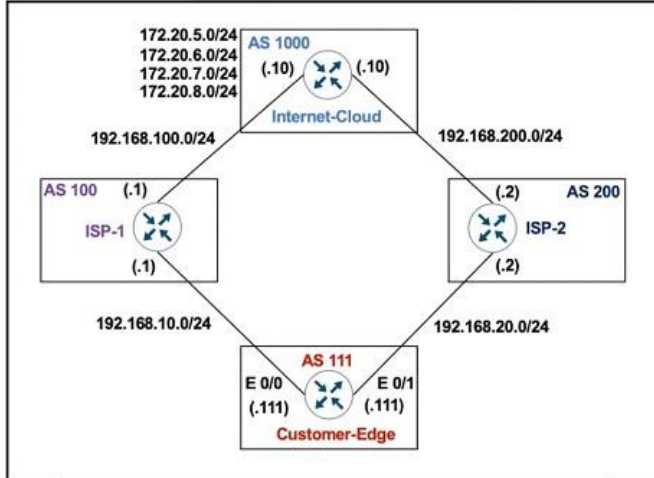
A. route-map SETLP permit 10
   match ip address prefix-list PLIST1
   set local-preference 110
   route-map SETLP permit 20
B. route-map SETLP permit 10
   match ip address prefix-list PLIST1
   set local-preference 99
   route-map SETLP permit 20
C. router bgp 111
   no neighbor 192.168.10.1 route-map SETLP in
   neighbor 192.168.20.2 route-map SETLP in
D. router bgp 111
   no neighbor 192.169.10.1 route-map SETLP in
   neighbor 192.168.10.1 route-map SETLP out

Answer: B
Explanation:
There is an implicit deny all at the end of any route-map so all other traffic that does not match 172.20.5.0/24 would be dropped. Therefore we have to add a permitsequence at the end of the route-map to allow other traffic.
The default value of Local Preference is 100 and higher value is preferred so we have to set the local preference of AS100 lower than that of AS200.

QUESTION 218
Refer to the exhibit. The Math and Science departments connect through the corporate IT router but users in the Math department must not be able to reach the Science department and vice versa Which configuration accomplishes this task?
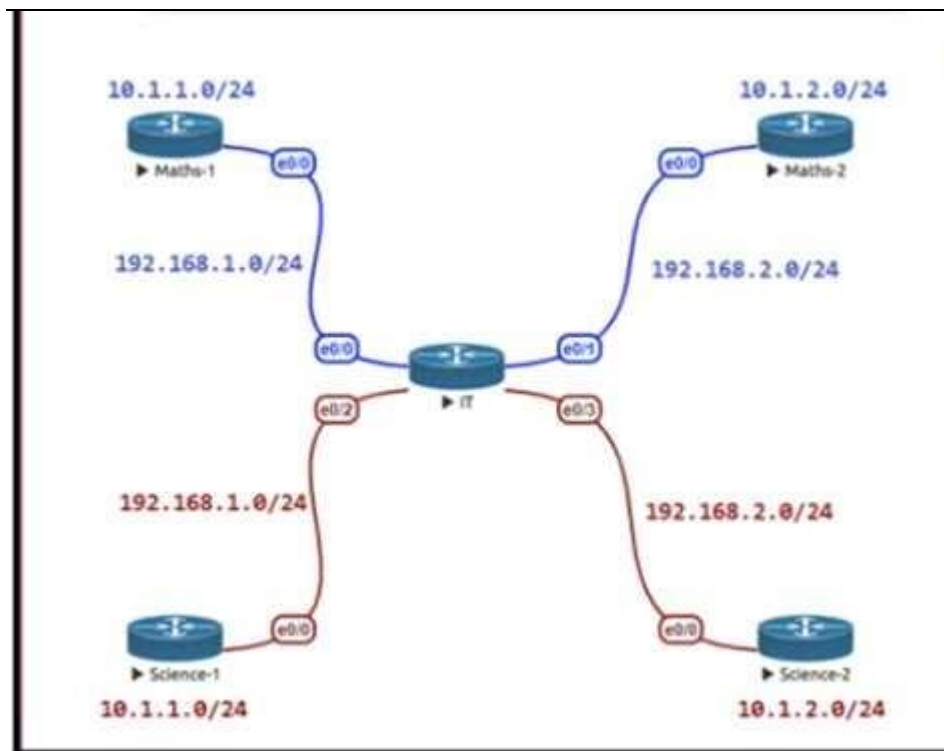
A. ○ vrf definition Science
    address-family ipv4
    !
    interface E 0/2
    vrf forwarding Science
    ip address 192.168.1.1 255.255.255.0
    no shut
    !
    interface E 0/3
    vrf forwarding Science
    ip address 192.168.2.1 255.255.255.0
    no shut

B. ○ vrf definition Science
    address-family ipv4
    !
    interface E 0/2
    ip address 192.168.1.1 255.255.255.0
    no shut
    !
    interface E 0/3
    ip address 192.168.2.1 255.255.255.0
    no shut

C. ○ vrf definition Science
    !
    interface E 0/2
    ip address 192.168.1.1 255.255.255.0
    no shut
    !
    interface E 0/3
    ip address 192.168.2.1 255.255.255.0
    no shut

D. ○ vrf definition Science
    address-family ipv4
    !
    interface E 0/2
    ip address 192.168.1.1 255.255.255.0
    vrf forwarding Science
    no shut
    !
    interface E 0/3
    ip address 192.168.2.1 255.255.255.0
    vrf forwarding Science
    no shut

Answer: D

QUESTION 219
An engineer configured Reverse Path Forwarding on an interface and noticed that the routes are dropped when a route lookup fails on that interface for a prefix that is available in the routing table Which interface configuration resolves the issue?

A. ip verify unicast source reachable-via rx
B. ip verify unicast source reachable-via any
C. ip verify unicast source reachable-via allow-default
D. ip verify unicast source reachable-via 12-src

Answer: C

QUESTION 220
Refer to the exhibit. The neighbor relationship is not coming up. Which two configurations bring the adjacency up? (Choose two)

```
NY
router ospf 1
 network 192.168.12.0 0.0.0.255 area 0
 network 172.16.2.0 0.0.0.255 area 0
!
interface E 0/0
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 Cisco123
```

☐ NY
    interface E 0/0
     no ip ospf message-digest-key 1 md5 Cisco123
     ip ospf authentication-key Cisco123

☑ LA
    router ospf 1
     area 0 authentication message-digest

☑ NY
    router ospf 1
     area 0 authentication message-digest

☐ LA
    interface E 0/0
     ip ospf authentication-key Cisco123

☐ LA
    interface E 0/0
     ip ospf message-digest-key 1 md5 Cisco123

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

Answer: BC

QUESTION 221
Refer to the exhibit. SanFrancisco and Boston routers are choosing slower links to reach each other despite the direct links being up. Which configuration fixes the issue?

```
L    172.1.12.3/32 is directly connected, Ethernet0/0
C    172.1.13.0/24 is directly connected, Ethernet0/1
L    172.1.13.3/32 is directly connected, Ethernet0/1
O    192.168.1.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O    192.168.2.0/24 [110/2] via 172.1.12.1, 00:04:44, Ethernet0/0
O    192.168.3.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
O    192.168.4.0/24 [110/2] via 172.1.13.2, 00:04:44, Ethernet0/1
     192.168.5.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.5.0/24 is directly connected, Loopback0
L    192.168.5.1/32 is directly connected, Loopback0
     192.168.6.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.6.0/24 is directly connected, Loopback1
L    192.168.6.1/32 is directly connected, Loopback1
```

◉ **Boston Router**

    router ospf 1
    auto-cost reference-bandwidth 1000

◉ **SanFrancisco Router**

    router ospf 1
    auto-cost reference-bandwidth 1000

◉ **All Routers**

    router ospf 1
    auto-cost reference-bandwidth 100

◉ **All Routers**

    router ospf 1
    auto-cost reference-bandwidth 1000

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

Answer: D

QUESTION 222
Refer to the exhibit. A network administrator logs into the router using TACACS+ username and password credentials, but the administrator cannot run any privileged commands. Which action resolves the issue?

```
Debug output:
username: USER55
password:
Aug 26 12:39:23.813: TPLUS: Queuing AAA Authentication request 4950 for processing
Aug 26 12:39:23.813: TPLUS(00001356) login timer started 1020 sec timeout
Aug 26 12:39:23.813: TPLUS: processing authentication continue request id 4950
Aug 26 12:39:23.813: TPLUS: Authentication continue packet generated for 4950
Aug 26 12:39:23.813: TPLUS(00001356)/0/WRITE/3A72C8D0: Started 5 sec timeout
!
!----- output omitted -----!
!
Aug 26 12:40:01.241: TAC+: using previously set server 192.168.1.3 from group tacacs+
Aug 26 12:40:01.241: TAC+: Opening TCP/IP to 192.168.1.3/49 timeout=5
Aug 26 12:40:01.249: TAC+: Opened TCP/IP handle 0x3BE31D1C to 192.168.1.3/49
Aug 26 12:40:01.249: TAC+: Opened 192.168.1.3 index=1
Aug 26 12:40:01.250: TAC+: 192.168.1.3 (3653537180) AUTHOR/START queued
Aug 26 12:40:01.449: TAC+: (3653537180) AUTHOR/START processed
Aug 26 12:40:01.449: TAC+: (-641430116): received author response status = FAIL
Aug 26 12:40:01.450: TAC+: Closing TCP/IP 0x3BE31D1C connection to 192.168.1.3/49
```

A. Configure TACACS+ synchronization with the Active Directory admin group
B. Configure the username from a local database
C. Configure full access for the username from TACACS+ server
D. Configure an authorized IP address for this user to access this router

Answer: C

QUESTION 223
Refer to the exhibit. When monitoring an IPv6 access list, an engineer notices that the ACL does not have any hits and is causing unnecessary traffic to pass through the interface. Which command must be configured to resolve the issue?

```
ipv6 access-list INTERNET
 permit ipv6 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA14::/64
 permit tcp 2001:DB8:AD59:BA21::/64 2001:DB8:C0AB:BA13::/64 eq telnet
 permit tcp 2001:DB8:AD59:BA21::/64 any eq http
 permit ipv6 2001:DB8:AD59::/48 any
 deny ipv6 any any log
```

A. access-class INTERNET in
B. ipv6 traffic-filter INTERNET in
C. ipv6 access-class INTERNET in
D. ip access-group INTERNET in

Answer: B

QUESTION 224
Refer to the exhibit. The network administrator configured redistribution on an ASBR to reach to all WAN networks but failed. Which action resolves the issue?

```
router ospf 1
 redistribute eigrp 1 subnets route-map EIGRP->OSPF
!
router eigrp 1
 network 10.0.106.0 0.0.0.255
!
route-map EIGRP->OSPF permit 10
 match ip address WAN_PREFIXES
route-map EIGRP->OSPF permit 20
 match ip address LOCAL_PREFIXES
route-map EIGRP->OSPF permit 30
 match ip address VPN_PREFIXES
!
ip prefix-list LOCAL_PREFIXES seq 5 permit 172.16.0.0/12 le 24
ip prefix-list VPN_PREFIXES seq 5 permit 192.168.0.0/16 le 24
ip prefix-list WAN_PREFIXES seq 5 permit 10.0.0.0/8 le 24
!
```

A. The route map must have the keyword prefix-list to evaluate the prefix list entries
B. The OSPF process must have a metric when redistributing prefixes from EIGRP.
C. The route map EIGRP->OSPF must have the 10.0.106.0/24 entry to exist in one of the three prefix lists to pass

D. EIGRP must redistribute the 10.0.106.0/24 route instead of using the network statement

Answer: D

QUESTION 225
How does an MPLS Layer 3 VPN function?

A. set of sites use multiprotocol BGP at the customer site for aggregation
B. multiple customer sites interconnect through service provider network to create secure tunnels between customer edge devices
C. set of sites interconnect privately over the Internet for security
D. multiple customer sites interconnect through a service provider network using customer edge to provider edge connectivity

Answer: B

QUESTION 226
Refer to the exhibit. Which action resolves the failed authentication attempt to the router?

```
Configuration Output:
aaa new-model
!
aaa authentication login default local
aaa authentication login VTY_AUTH local
aaa authorization exec default none
aaa authorization exec VTY_AUTH local
aaa accounting exec default start-stop group radius
!


password 7 K0AyUubDrfOgO4s
authorization exec VTY_AUTH
login authentication VTY_AUTH


!

Debug Output:
AAA/AUTHEN/LOGIN (000004B6): Pick method list 'default'
AAA/AUTHOR (0x4B6): Pick method list 'VTY_AUTH'
AAA/AUTHOR/EXEC(000004B6): Authorization FAILED
```

A. Configure aaa authorization login command on line vty 0 4
B. Configure aaa authorization login command on line console 0
C. Configure aaa authorization console global command
D. Configure aaa authorization console command on line vty 0 4

Answer: A

QUESTION 227
A customer reports to the support desk that they cannot pnnt from their PC to the local printer id:401987778. Which tool must be used to diagnose the issue using Cisco DNA Center Assurance?

A. application trace
B. path trace
C. ACL trace
D. device trace

Answer: B

QUESTION 228
When determining if a system is capable of support, what is the minimum time spacing required for a BFD control packet to receive once a control packet is arrived?

A. Desired Min TX Interval
B. Detect Mult
C. Required Min RX Interval
D. Required Min Echo RX Interval

Answer: C

QUESTION 229
Refer to the exhibit. Troubleshoot and ensure that branch B only ever uses the MPLS B network to reach HQ. Which action achieves this requirement?
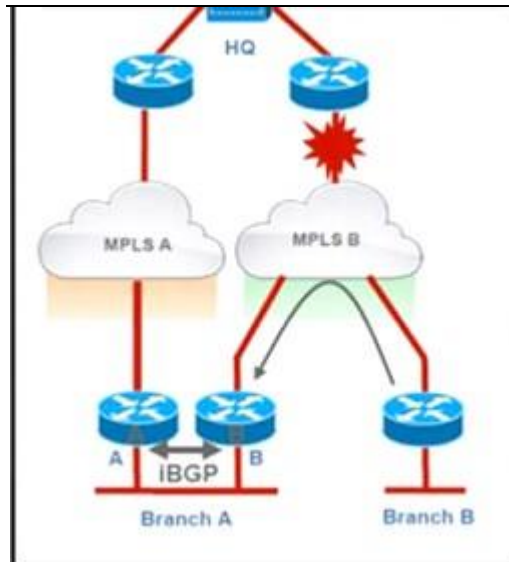
A. Introduce an AS path filter on branch A routers so that only local prefixes are advertised into BGP
B. increase the local preference for all HQ prefixes received at branch B from the MPLS B network to be higher than the local preferences used on the MPLS A network
C. Introduce AS path prepending on the branch A MPLS B network connection so that any HQ advertisements from branch A toward the MPLS B network are prepended three times
D. Modify the weight of all HQ prefixes received at branch B from the MPLS B network to be higher than the weights used on the MPLS A network

Answer: A

QUESTION 230
Refer to the exhibit. The OSPF routing protocol is redistributed into the BGP routing protocol, but not all the OSPF routes are distributed into BGP. Which action resolves the issue?


```
Router# show ip route

     2.0.0.0/24 is subnetted, 1 subnets
C      2.2.2.0 is directly connected, Ethernet0/0
C   3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
     131.108.0.0/24 is subnetted, 2 subnets
O      131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA   131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0

Router# show ip bgp

  Network        Next Hop        Metric LocPrf Weight Path
*> 2.2.2.0/24     0.0.0.0             0         32768 ?
*> 131.108.1.0/24 2.2.2.2            84         32768 ?
*> 131.108.2.0/24 2.2.2.2            74         32768 ?
```

A. Include the word external in the redistribute command
B. Use a route-map command to redistribute OSPF external routes defined in an access list
C. Include the word internal external in the redistribute command
D. Use a route-map command to redistribute OSPF external routes defined in a prefix list.

Answer: B

QUESTION 231
Refer to the exhibit. PC-2 failed to establish a Telnet connection to the terminal server.
Which configuration resolves the issue?
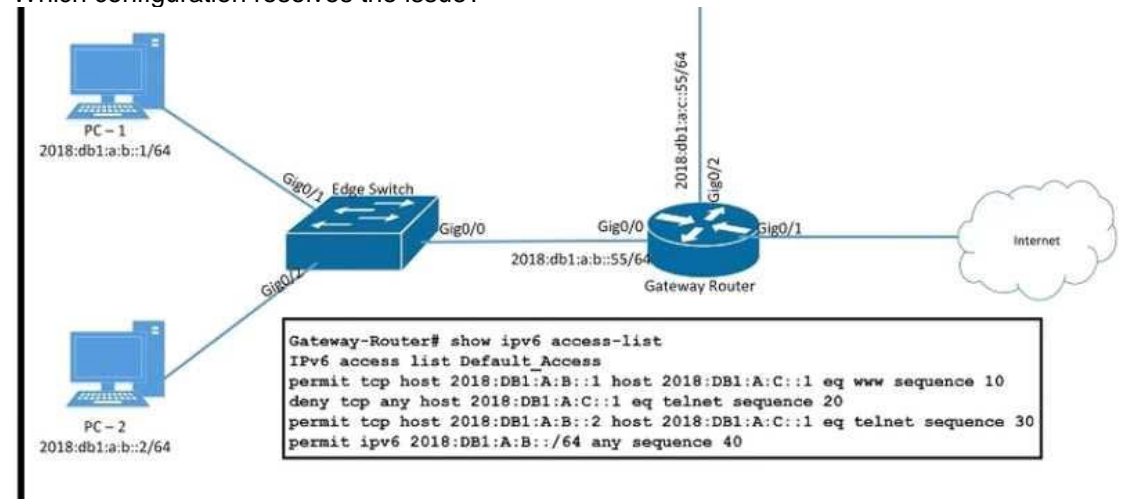

```
Gateway-Router# show ipv6 access-list
IPv6 access list Default_Access
permit tcp host 2018:DB1:A:B::1 host 2018:DB1:A:C::1 eq www sequence 10
deny tcp any host 2018:DB1:A:C::1 eq telnet sequence 20
permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet sequence 30
permit ipv6 2018:DB1:A:B::/64 any sequence 40
```

300-410 Exam Dumps 300-410 Exam Questions 300-410 PDF Dumps 300-410 VCE Dumps

https://www.braindump2go.com/300-410.html

○ Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**sequence 15 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

○ Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

○ Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**no sequence 20**
Gateway-Router(config-ipv6-acl)#**sequence 5 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

⊙ Gateway-Router(config)#**ipv6 access-list Default_Access**
Gateway-Router(config-ipv6-acl)#**sequence 25 permit tcp host 2018:DB1:A:B::2 host 2018:DB1:A:C::1 eq telnet**

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

Answer: D

QUESTION 232
Drag and Drop Question
Drag and drop the MPLS concepts from the left onto the descriptions on the right.

label edge router	allows an LSR to remove the label before forwarding the packet
label switch router	accepts unlabeled packets and imposes labels
forwarding equivalence class	group of packets that are forwarded in the same manner
penultimate hop popping	receives labeled packets and swaps labels

Answer:

penultimate hop popping
label edge router
forwarding equivalence class
label switch router

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. LERspush an MPLS label onto an incoming packet and pop it off an outgoing packet.
A forwarding equivalence class (FEC) is a term.

QUESTION 233
Drag and Drop Question
Drag and drop the LDP features from the left onto the descriptions on the right.

implicit null label	provides ways of improving load balancing by eliminating the need for DPI at transit LSRs
explicit null label	LSR receives an MPLS header with the label set to 3
inbound label binding filtering	packet is encapsulated in MPLS with the option of copying the IP precedence to EXP bits
entropy label	controls the amount of memory used to store LDP label bindings advertised by other devices

Answer:

entropy label
explicit null label
inbound label binding filtering
implicit null label