Cisco CCNP Enterprise ENARSI 300-410

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

Todd Lammle
CCNP Enterprise Expert Trainer

TL TODD LAMMLE

Implementing Cisco Enterprise Advanced Routing and Services v1.0 (300-410)

Book Update Version 1.0

This book will dive into the latest practice questions needed before you take the Cisco CCNP exam 300-410.

Chapter 1: Layer 3 Technologies

The objectives covered in this chapter:

35% 1.0 Layer 3 Technologies

1.1 Troubleshoot administrative distance (all routing protocols)

1.2 Troubleshoot route map for any routing protocol (attributes, tagging, filtering)

1.3 Troubleshoot loop prevention mechanisms (filtering, tagging, split horizon, route poisoning)

1.4 Troubleshoot redistribution between any routing protocols or routing sources

1.5 Troubleshoot manual and auto-summarization with any routing protocol

1.6 Configure and verify policy-based routing

1.7 Configure and verify VRF-Lite

1.8 Describe Bidirectional Forwarding Detection

1.9 Troubleshoot EIGRP (classic and named mode)

1.9.a Address families (IPv4, IPv6)

1.9.b Neighbor relationship and authentication

1.9.c Loop-free path selections (RD, FD, FC, successor, feasible successor, stuck in active)

1.9.d Stubs

1.9.e Load balancing (equal and unequal cost)

1.9.f Metrics

1.10 Troubleshoot OSPF (v2/v3)

1.10.a Address families (IPv4, IPv6)

1.10.b Neighbor relationship and authentication

1.10.c Network types, area types, and router types

1.10.c (i) Point-to-point, multipoint, broadcast, nonbroadcast

1.10.c (ii) Area type: backbone, normal, transit, stub, NSSA, totally stub

1.10.c (iii) Internal router, backbone router, ABR, ASBR

1.10.c (iv) Virtual link

1.10.d Path preference

1.11 Troubleshoot BGP (Internal and External)

1.11.a Address families (IPv4, IPv6)

1.11.b Neighbor relationship and authentication

(next-hop, mulithop, 4-byte AS, private AS, route refresh, synchronization, operation, peer group, states and timers)

1.11.c Path preference (attributes and best-path)

1.11.d Route reflector (excluding multiple route reflectors, confederations, dynamic peer)

1.11.e Policies (inbound/outbound filtering, path manipulation)

1. Which of the following sources of route information has the highest (i.e. the least believable) administrative distance?
A. RIP
B. External EIGRP
C. OSPF
D. Internal EIGRP

2. What is the seed metric for EIGRP?
A. 20
B. 1
C. Infinity
D. 0

3. Which of the following is not an option for assigning a metric to a routing protocol?
A. Set a default metric for all routing sources being injected into a routing protocol.
B. Set a metric using a Route Map.
C. Specify a metric as part of the “redistribute” command.
D. Specify a metric with a Route Tag.

4. You wish to redistribute all routes within AS 1 into AS 2 with the exception of 192.168.1.0/24. Which of the following approaches can you use to selectively filter that route?
A. Create an ACL to match the 192.168.1.0/24 network, and reference that ACL under a “route map deny” statement.
B. Use the “filter-list 192.168.1.0/24” option as part of the “redistribute” command.
C. Create an ACL to match the 192.168.1.0/24 network, and reference that network in a “distribute list” command.
D. Use the “distribute-list 192.168.1.0/24” option as part of the “redistribute” command.

5. What route-map configuration mode command is used to set a route tag to a value of 10?
A. create tag 10
B. match tag 10
C. tag mode 10
D. set tag 10

6. When redistributing IPv6 routes, which of the following is true?
A. By default, the “redistribute” command includes connected routes on interfaces enabled for the redistributed protocol.
B. By default, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol.
C. The “redistribute” command is used exclusively for redistributing IPv4 routes, while the “redistribute-v6” command is used for redistributing IPv6 routes.
D. If you wish to set a non-default metric on a redistributed route, the “metric” option must be used as part of the “redistribute” command.

7. Where should Policy Based Routing (PBR) be applied on a router?
A. On a router’s egress interface
B. In a router’s global configuration mode
C. On a router’s ingress interface
D. In a router’s router configuration mode

8. What configuration structure does PBR use to match traffic and specify behavior for that traffic?
A. policy-map
B. route-map
C. class-map
D. access-class

9. Which of the following is true regarding VRF, by default?
A. With VRF, virtual routers share an IP routing table.
B. With VRF, virtual routers have their own IP routing table, but they also see routes in the physical router’s IP routing table.
C. With VRF, all virtual routers must be using the same IP routing protocol.
D. With VRF, all virtual routers have their own independent IP routing tables.

10. In a VRF configuration, you wish view the IP routing table of a virtual router with a VRF instance name of “TENANT-A”. What command would you use?
A. show ip route vrf TENANT-A
B. show address family ip4 TENANT-A
C. show vrf TENANT-A ip route
D. show virtual-instance TENANT-A ip route

11. Which of the following protocols does EIGRP use to ensure delivery of routing updates?
A. STP
B. Dijkstra
C. RTP
D. DUAL

12. Refer to The exhibit. The network administrator must mutually redistribute routes at the Chicago router to the LA and New York routers. The configuration of the Chicago router is this:
After the configuration, the LA router receives all the New York routes, but New York router does
not receive any LA routes. Which set of configurations fixes the problem on the Chicago router?

Chicago:
router ospf 1
redistribute eigrp 100
router eigrp 100
redistribute ospf 1

A.
router ospf 1
  redistribute eigrp 100 metric 20

B.
router eigrp 100
  redistribute ospf 1 metric 10 10 10 10 10

C.
router eigrp 100
  redistribute ospf 1 subnets

D.
```
router ospf 1
  redistribute eigrp 100 subnets
```

13. What is EIGRP's default Hold Time on a LAN interface?
A. 5 seconds
B. 10 seconds
C. 15 seconds
D. 20 seconds

14. By default, EIGRP uses which of the following parameters to calculate its metric?
A. Delay and Load
B. Bandwidth and Delay
C. Bandwidth and Reliability
D. Bandwidth, Delay, Reliability, Load, and MTU

15. What is the name given to an EIGRP backup route that has met the Feasibility Condition?
A. Feasible Successor Route
B. Successor Route
C. Standby Route
D. DUAL Route

16. EIGRP's Feasibility Condition requires a Feasible Successor's Reported Distance to be less than what?
A. The Advertised Distance of the Successor Route
B. The Administrative Distance of the Successor Route
C. The Reported Distance of the Successor Route
D. The Feasible Distance of the Successor Route

17. If an EIGRP router loses its Successor Route to a destination network and it has no Feasible Successor Route, what message does the router send out in an attempt to find an alternate path to the network?
A. Hello
B. Query
C. Open
D. Discover

18. Which of the following is true of EIGRP for IPv4 neighbors?
A. EIGRP neighbors must have matching Variance values
B. EIGRP neighbors must have matching Process IDs (PIDs)
C. EIGRP neighbors must have matching Autonomous System (AS) numbers
D. EIGRP neighbors must have matching Hello and Hold Timers

19. What can be used in an EIGRP Stub Router configuration to allow selected routes to be advertised by the Stub Router?
A. Leak Map
B. Policy Map
C. Class Map
D. Service Policy

20. Under which condition will EIGRP not load balance across a backup path with the Variance feature?
A. The backup path's metric equals, but is not less than, the product of the Variance and the metric of the Successor Route.
B. The backup path does not meet the Feasibility Condition.
C. The Variance value is greater than 4.
D. The backup path uses an interface with a different Hello Timer than the interface used by the Successor Route.

21. What command is used to enable EIGRP's Automatic Summarization feature?
A. Router(config-router)# ip summary-address eigrp [AS]
B. Router(config-if)# auto-summary
C. Router(config-if)# ip summary-address eigrp [AS]
D. Router(config-router)# auto-summary

22. What interface configuration mode command is issued to tell an interface to participate in an EIGRP for IPv6 routing process for Autonomous System (AS) 1?
A. Router(config-if)# ipv6 unicast-routing eigrp 1
B. Router(config-if)# unicast-routing 1
C. Router(config-if)# ipv6 eigrp 1
D. Router(config-if)# eigrp ipv6 1

23. Under what Named EIGRP configuration mode would you configure the Variance option?

A. Address-Family-Topology configuration mode
B. Address-Family configuration mode
C. Address-Family-Interface configuration mode
D. Service-Family configuration mode

24. Which of the following routing protocols support the SHA hashing algorithm?
A. EIGRP for IPv4
B. EIGRP for IPv6
C. Named EIGRP
D. All of the above

25. What is the effect of setting a router's OSPF routing process to a Priority of 0?
A. It causes that router to be elected as a DR.
B. It causes that router to be elected as a BDR.
C. It prevents that router from participating in a DR election.
D. It suspends the OSPF process on that router.

26. By default, if you set an OSPF interface's Hello timer to 10 seconds, what will be the value of the Dead timer?
A. 5 seconds
B. 20 seconds
C. 30 seconds
D. 40 seconds

27. What is the default Reference Bandwidth used by OSPF to calculate Cost?
A. 100 kbps
B. 100 Mbps
C. 1 Gbps
D. 10 Gbps

28. What is the default OSPF Network Type of a non-Frame Relay OSPF interface?
A. Point-to-Point
B. Point-to-Multipoint
C. NBMA
D. Broadcast

29. What LSA Type is used to inject networks from a separate autonomous system (AS) into an OSPF Stub or Totally Stubby Area?
A. Type 3
B. Type 4
C. Type 5
D. Type 7

30. What Cisco IOS command is used to change the default reference-bandwidth of an OSPF-speaking router?
A. reference-bandwidth [bandwidth_amount]
B. interface-cost [bandwidth_amount]
C. auto-metric reference-bandwidth [bandwidth_amount]
D. auto-cost reference-bandwidth [bandwidth_amount]

31. What types of packets are sent over an OSPF Virtual Link?
A. Data packets
B. OSPF packets
C. GRE packets
D. Data, OSPF, and GRE packets

32. What Cisco IOS command is used to perform OSPF route summarization on an ABR?
A. area range
B. prefix-list
C. summary-address
D. distribute-list

33. What OSPFv3 LSA Type is used to advertise an area's Link Local address?
A. Type 4
B. Type 7
C. Type 8
D. Type 9

34. What command is used to create an OSPFv3 routing process with the Address Families configuration approach?
A. router ospfv3 [process-id]
B. ipv6 ospf [process-id]
C. router ipv6 ospf [process-id]

D. ospfv3 [process-id]

35. Which of the following is a hashing option for OSPFv3 Address Families authentication?
A. DES
B. Plain Text
C. AES
D. SHA-1

36. What well-known port is used by BGP when establishing a session?
A. TCP 179
B. TCP 443
C. TCP 137
D. TCP 161

37. In which state does a BGP-enabled router wait for the receipt of a Keepalive message in order to completely establish the BGP session?
A. Active
B. Idle
C. OpenSent
D. OpenConfirm

38. Which BGP command allows us to change interface source address used when establishing a neighbor adjacency?
A. update-interface
B. session-source
C. update-source
D. set-source

39. Which category of BGP attributes must be present in all updates and are passed on to other BGP peers?
A. Well-known discretionary
B. Well-known mandatory
C. Optional transitive
D. Optional nontransitive

40. Which command allows us to disable the default BGP synchronization feature found in older Cisco IOS versions?
A. no suppress

B. no local preference
C. no metric-type internal
D. no synchronization

41. Which mechanism within Multiprotocol BGP (MP-BGP) allows BGP to carry multiple protocols at once?
A. Route reflectors
B. VPNv4
C. Address families
D. L2VPN

42. Which BGP feature allows us to reduce the number of BGP updates created, lowering resource usage on BGP-enabled devices?
A. Peer group
B. Multihop
C. Route reflector
D. Summarization

43. What is the default time-to-live (TTL) value used with external BGP (eBGP)?
A. 0
B. 5
C. 2
D. 1

44. Which BGP mechanism allows all internal BGP (iBGP) neighbors within an autonomous system to learn about all available routes without creating loops in the network, and without using a full-mesh configuration?
A. MP-BGP
B. Communities
C. Route reflectors
D. Filtering

45. Which optional keyword is used to suppress prefixes and present only an aggregate address in the BGP update?
A. no-summary
B. summary-only
C. aggregate-address
D. suppress-update

46. Which BGP command allows for routes to be received even if a router sees its own autonomous system number in the AS-Path section of a BGP update?
A. no-prepend
B. replace-as
C. allowas-in
D. local-as

47. What is the definition of a floating static route?
A. A static route with an administrative distance higher than 0.
B. A static route with an administrative distance higher than 2.
C. A static route with an administrative distance higher than 1.
D. A static route with an administrative distance higher than 10.

48. Refer to the exhibit. A router receiving BGP routing updates from multiple neighbors for routers in
AS 690. What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.1.1?

```
router bgp 100
!
 neighbor 10.222.1.1 route-map SET-WEIGHT in
 neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map SET-WEIGHT permit 10
 match as-path 200
 set local-preference 250
 set weight 200
```

A. The local preference value in another neighbor statement is higher than

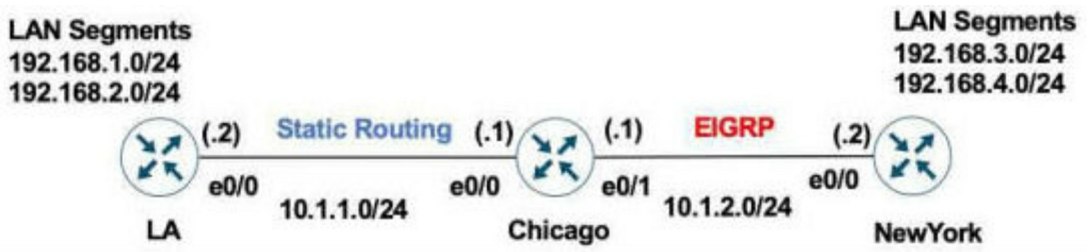
250.
B. The local preference value should be set to the same value as the weight in the route map.
C. The route map is applied in the wrong direction.
D. The weight value in another statement is higher than 200.

49. Refer to the exhibit. What is the result if applying this configuration?

```
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
```

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

50. Refer to the exhibits. A user on the 192.168 1.0/24 network can successfully ping 192.168.3.1,
but the administrator cannot ping 192.168.3.1 from the LA router. Which set of configurations fixes the issue?



Chicago Router
ip route 192.168.1.0 255.255.255.255.0 10.1.1.2
ip route 192.168.2.0 255.255.255.255.0 10.1.1.2
!
router eigrp 100
  redistribute static

LA Router
ip route 0.0.0.0 0.0.0.0 10.1.1.1

A. Chicago Router
router eigrp 100
redistribute static metric 10.10.10.10

B. Chicago Router
router eigrp 100
redistribute connected

C. Chicago Router
ip route 192.168.3.0 255.255.255.0 10.1.2.2
ip route 192.168.4.0 255.255.255.0 10.1.2.2

D. LA Router
ip route 192.168.3.0 255.255.255.0 10.1.1.1
ip route 192.168.4.0 255.255.255.0 10.1.1.1

51. Refer to the exhibit. Which control plan policy limits BGP traffic that is destined to the CPU to 1
Mbps and ignores BGP traffic that is higher rate?

```
Cat3850-Stack-2# show policy-map

Policy Map LIMIT_BGP
  Class BGP
    drop

Policy Map SHAPE_BGP
  Class BGP
    Average Rate Traffic Shaping
    cir 10000000 (bps)

Policy Map POLICE_BGP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action transmit

Policy Map COPP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action drop
```

A. policy-map SHAPE_BGP
B. policy-map LIMIT_BGP
C. policy-map POLICE_BGP
D. policy-map COPP

52. Which configuration enables the VRF that is labeled `'inet" on FastEthernet0/0?
A. R1(config)# ip vrf Inet
R1(config-vrf)#ip vrf FastEthernet0/0

B. R1 (conflg)#ip vrf Inet FastEthernet0/0

C. R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet

D. R1 (config)#router ospf 1 vrf Inet
R1 (config-router)#ip vrf forwarding FastEthernet0/0

53. Which attribute eliminates LFAs that belong to protected paths in situations where links in a
network are connected through a common fiber?
A. Interface-dispoint
B. Shared risk link group-disjoint
C. Linecard-disjoint
D. Lowest-repair-path-metric

54. 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

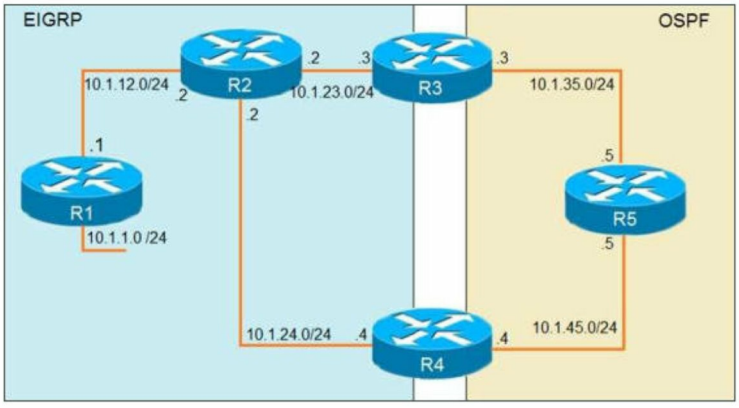
55. R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:
What is the result when the route-map OUT command is applied toward an eBGP neighbor R1
(1.1.1.1) by using the neighbor 1.1.1.1 route-map OUT out command?

ip prefix-list test seq 5 permit 192.168.130.0/24
!
route-map OUT permit 10
match ip address prefix-list test

set as-path prepend 6500

A. R1 sees 192.168.130.0/24 as two hops away instead of one AS hop away
B. R1 does not forward traffic that is destined for 192.168.130.0/24.
C. Network 192.168.130.0/24 is not allowed in the R1 table.
D. R1 does not accept any route other than 192.168.130.0/24.

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



R1
router eirp 1
redistribute connected
network 10.1.12.1 0.0.0.0

R3
router ospf 1
redistribute eigrp 1 subnets
network 10.1.35.0 0.0.0.0 area 0

R4
router eirp 1
redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
network 10.1.45.4 0.0.0.0 area 0
!
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

1 10.1.35.3 80 msec 44 msec 20 msec
2 10.1.23.2.44 44 msec 104 msec 64 msec
3 10.1.24.4.44 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 truncuated>
```

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 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 SET-TAG
!
```

R4
```
router eigrp 1
  redistribute ospf 1 metric 2000000 1 255 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 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 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 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
  match tag 1
```

57. What is the role of a route distinguisher via a VRF-Lite setup implementation?

A. It extends the IP address to identify which VFP instance it belongs to.

B. It manages the import and export of routes between two or more VRF instances.

C. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities.

D. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities.

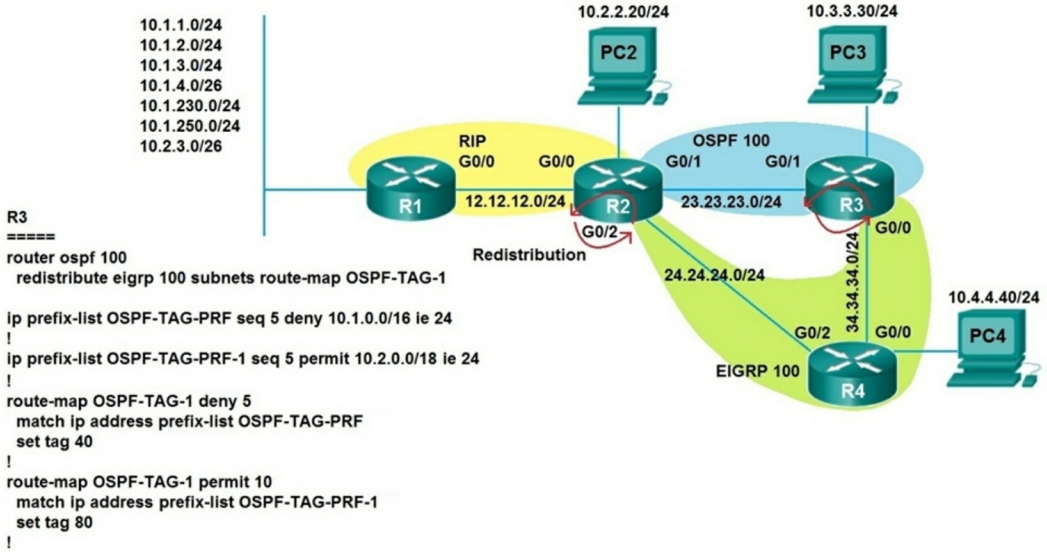
58. Refer to the exhibit. R2 is a route reflector, and R1 and R3 are route reflector clients. The route
reflector learns the route to 172.16.25.0/24 from R1, but it does not advertise to R3. What is the
reason the route is not advertised?

```
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#
```

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

59. Which method changes the forwarding decision that a router makes first changing the routing
table or influencing the IP data plane?
A. Policy-based routing
B. Nonbroadcast multi-access
C. Packet switching
D. Forwarding information base

60. Refer to the exhibit. Which subnet is redistributed from EIGRP to OSPF routing protocols?



A. 10.2.2.0/24
B. 10.1.4.0/24
C. 10.1.2.0/24
D. 10.2.3.0/26

61. Refer to the exhibit. An engineer is trying to redistribute OSPF to BGP, but not all of the routes are redistributed. What is the reason for this issue?

```
Router#sh ip route ospf
<output omitted>
Gateway is last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
   o  E2     10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
   o       192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, Ethernet0/0
Router#

Router#show ip bgp
<output omitted>
     Network          Next Hop      Metric     LocPrf     Weight     Path
>*   192.168.1.1/32   0.0.0.0            0                32768      ?
>*   192.168.3.0      192.168.12.2      20                32768      ?
>*   192.168.12.0     0.0.0.0            0                32768      ?
Router#show running-config | section router bgp
router bgp 65000
 bgp log-neighbor-changes
 redistribute ospf 1
Router#
```

A. By default, only internal OSPF routes are redistributed into BGP
B. By default, only internal routers and external type 1 routes are redistributed into BGP.

C. BGP convergence is slow, so the route will eventually be present in the BGP table.
D. Only classful networks are redistributed from OSPF to BGP.

62. 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

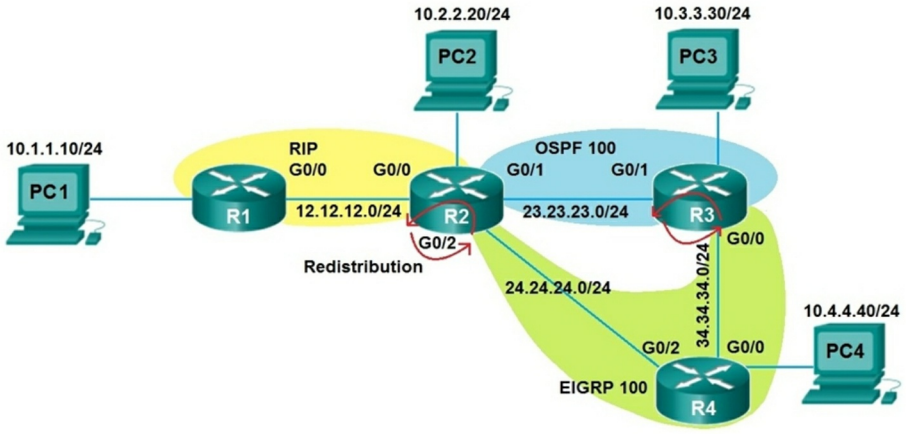
63. Refer to the exhibit. An engineer is trying to generate a summary route in OSPF for network
10.0.0.0/8, but the summary route does not show up in the routing table. Why is the summary
route missing?

```
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 route is not visible on this router, but it is visible on other OSPF routers in the same
area.
B. The summary-address command is used only for summary prefixes between areas.
C. The summary route is visible only in the OSPF database not in the routing table.
D. There is no route for a subnet inside 10.0.0.0/8, so the summary route is not generated.

64. Which is statement about IPv6 inspection is true?
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 3 neighbor tables.
D. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables.

65. Refer to the exhibit. After redistribution is enabled between the routing protocols; PC2, PC3, and
PC4 cannot reach PC1. Which action can the engineer take to solve the issue so that all the PCs are reachable?



A. Filter the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP.
B. Set the administrative distance 100 under the process on R2.
C. Filter the prefix 10.1.1.0/24 when redistributed from RIP to EIGRP.
D. Redistribute the directly connected interfaces on R2.

66. Refer to the exhibit. An engineer configures a static route on a router, but when the engineer
checks the route to the destination, a different next hop is chosen. What is the reason for this?

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Ethernet0/1
         209.165.200.226/32 is directly connected, Ethernet0/1
```

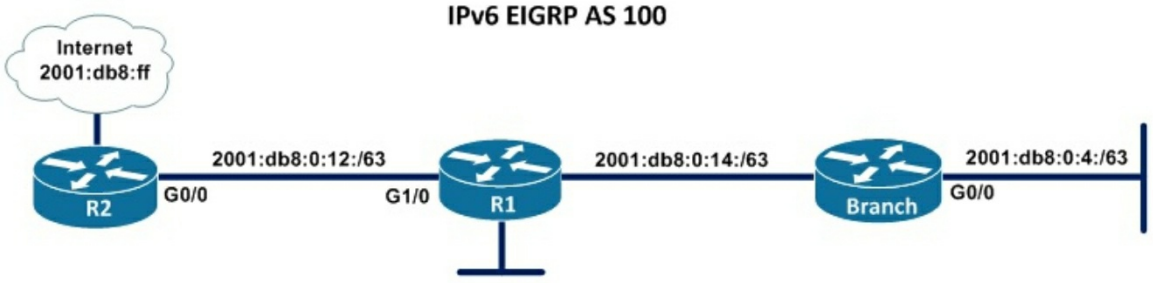
A. The configured AD for the static route is higher than the AD of OSPF.
B. The metric of the OSPF route is lower than the metric of the static route.
C. Dynamic routing protocol always have priority over static routes.
D. The syntax of the static route is not valid do the route is not considered.

67. Refer to the exhibit. An engineer is troubleshooting BGP on a device but discovers that the clock
on the device does not correspond to the time stamp of the log entries. Which action ensures consistency between the two times?

```
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
* Jun 28 14:41:57: %BGP_SESSION-5-ADCHANGE: neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session  User reset
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*15:42:00 506 CET Fri Jun 28 2019
```

A. Configure the logging clock synchronize command in global configuration mode.
B. Configure the service timestamps log uptime command in global configuration mode.
C. Configure the service timestamps log datetime localtime command in global configuration mode.
D. Make sure that the clock on the device is synchronized with an NTP server.

68. Refer to the exhibit. Users in the branch network of 2001:db8:0:4::/64 report that they cannot
access the Internet. Which command is issued in IPv6 router EIGRP 100 configuration mode to



solve this issue?

```
R1#show ipv6 eigrp topology
EIGEP-IPv6 Topology Table for
AS(100)1D(10.1.12.1)
Codes: P-Passive, A-Active, U-Update, Q-
Query, R-Reply
      r-reply Status, s-sia Status
```

```
Branch#show ipv6 eigrp topology
EIGEP-IPv6 Topology Table for
AS(100)1D(4.4.4.4)
Codes: P-Passive, A-Active, U-Update, Q-
Query, R-Reply
      r-reply Status, s-sia Status
```

```
P 2001:DB8:0:4::/64, 1 successors, FD is 28416
     via FE80:C828:DFF:FEF4:1C(28416/2816),
FastEthernet3/0
P 2001:DB8:0:1::/64, 1 successors, FD is 2816
     via Connected, GigabitEthernet0/0
P ::/0, 1 successors, FD is 2816
     via FE80:C821:17FF:FE04:8(2816/256),
GigabitEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is
28160
     via Connected, FastEthernet3/0
P 2001:DB8:0:12::/64, 1 successors, FD is 2816
     via Connected, GigabitEthernet1/0
```

```
P 2001:DB8:0:4::/64, 1 successors, FD is 2816
     via Connected, GigabitEthernet0/0
P 2001:DB8:0:1::/64, 1 successors, FD is 28416
     via FE80:C820:17FF:FE04:54(28416/2816),
FastEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
     via Connected, FastEthernet1/0
P 2001:DB8:0:12::/64, 1 successors, FD is 28416
     via FE80:C820:17FF:FE04:54(28416/2816),
FastEthernet1/0
```

A. Issue the eigrp stub command on R1.
B. Issue the no eigrp stub command on R1.
C. Issue the eigrp stub command on R2.
D. Issue the no eigrp stub command on R2.

69. Which of the following are true statements regarding OSPF adjacency states? (Choose three).
A. 2-way - Routers exchange information with other routers in the multiaccess network.
B. Loading - Each router configures the DBD packets that were received from the other router.
C. ExStart - The network has already elected a DR and a backup BDR.
D. Init - The OSPF router ID of the receiving router was not contained in the hello message.
E. Exchange - The OSPF router ID of the receiving router contained the hello message.

70. Refer to Exhibit. Which statement about redistribution from BGP into OSPF process 10 is true?

```
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
```

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.

71. Which two statements about redistributing EIGRP into OSPF are true? (Choose two)
A. The redistributed EIGRP routes appear as type 3 LSAs in the OSPF database
B. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database
C. The administrative distance of the redistributed routes is 170
D. The redistributed EIGRP routes appear as OSPF external type 1
E. The redistributed EIGRP routes as placed into an OSPF area whose area ID matches the EIGRP
autonomous system number
F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table

72. What is a prerequisite for configuring BFD?
A. All routers in the path between two BFD endpoints must have BFD enabled.
B. Jumbo frame support must be configured on the router that is using BFD.
C. Cisco Express Forwarding must be enabled on all participating BFD endpoints.
D. To use BFD with BGP. the timers 3 9 command must first be configured in the BGP routing
process.

73. Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family
configuration?
A. Router# ospf3 1 address-family ipv4
B. Router(config-router)#ospfv3 1 ipv4 area 0
C. Router(config-router)#ospfv3 3 1
D. Router# ospfv3 1 address-family ipv4 unicast

74. While troubleshooting connectivity issues to a router, these details are noticed:

- Standard pings to all router interfaces, including loopbacks, are successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either or disconnects frequently.

Which command must be configured first to troubleshoot this issue?

A. Show policy-map control-plane
B. Show policy-map
C. Show interface inc drop
D. Show ip route

75. Refer to the exhibit. Which statement about R1 is true?

```
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
```

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

76. Refer to the exhibit. Which routes from OSPF process 5 are redistributed into EIGRP?

```
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
```

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 listTO-OS1

77. What is the output of the following command:

show ip vrf

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

```
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#
```

78. Refer to the exhibit. 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.

79. Refer to the exhibit. An engineer is trying to get 192.168.32.100 forwarded through 10.1.1.1, but it was forwarded through 10.1.1.2. What action forwards the packets through 10.1.1.1?

```
router#show ip route
....
    D 192.168.32.0/19 [90/25789217] via 10.1.1.1
    R 192.168.32.0/24 [120/4] via 10.1.1.2
    O 192.168.32.0/26 [110/229840] via 10.1.1.3
```

A. Configure EIGRP to receive 192.168.32.0 route with lower admin distance.

B. Configure EIGRP to receive 192.168.32.0 route with longer prefix than /19.
C. Configure EIGRP to receive 192.168.32.0 route with lower metric.
D. Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24.

80. An engineer configured a leak-map command to summarize EIGRP routes and advertise
specifically loopback 0 with an IP of 10.1.1.1.255.255.255.252 along with the summary route.
After finishing configuration, the customer complained not receiving summary route with specific
loopback address.
Which two configurations will fix it? (Choose two).
A. Configure access-list 1 permit 10.1.1.0.0.0.0.3.
B. Configure access-list 1 permit 10.1.1.1.0.0.0.252.
C. Configure access-list 1 and match under route-map Leak-Route.
D. Configure route-map Leak-Route permit 10 and match access-list 1.
E. Configure route-map Leak-Route permit 20.
81. 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 provides.
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
```

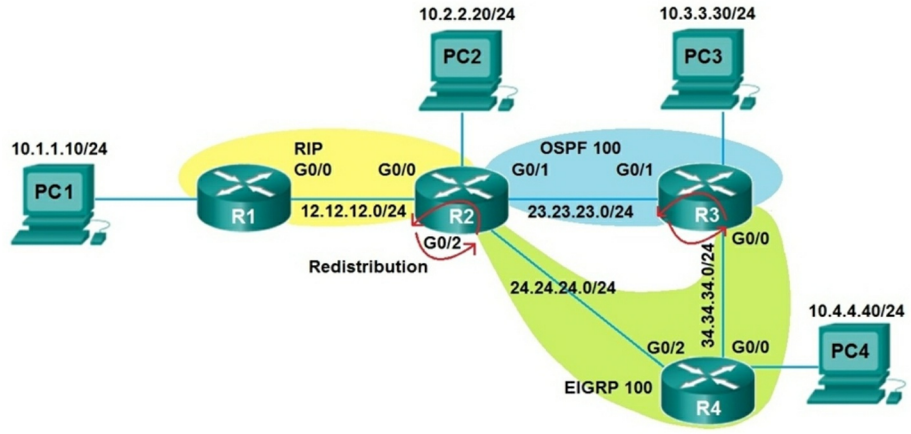
C.

```
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

82. Refer to the exhibit. Redistribution is enabled between the routing protocols, and now PC2 PC3,
and PC4 cannot reach PC1. What are the two solutions to fix the problem? (Choose two).



A. Filter RIP routes back into RIP when redistributing into RIP in R2
B. Filter OSPF routes into RIP FROM EIGRP when redistributing into RIP in R2.
C. Filter all routes except RIP routes when redistributing into EIGRP in R2.
D. Filter RIP AND OSPF routes back into OSPF from EIGRP when redistributing into OSPF in R2

E. Filter all routes except EIGRP routes when redistributing into OSPF in R3.

83. Refer to the exhibit. The network administrator configured VRF lite for customer A. The technician
at the remote site misconfigured VRF on the router. Which configuration will resolve connectivity
for both sites of customer a?

Router Configuration:

```
ip vrf customer_a
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
interface FastEthernet0.1
 encapsulation dot1Q 2
 ip vrf forwarding customer_a
 ip address 192.168.4.1 255.255.255.
!
router ospf 1
 log-adjacency-changes
 !
router ospf 2 vrf customer_a
 log-adjacency-changes
 network 192.168.4.0 0.0.0.255 area (
 !
end
```

A. ip vrf customer_a
rd 1:1
route-target export 1:2
route-target import 1:2

B. ip vrf customer_a
rd 1:1
route-target export 1:1
route-target import 1:2

C. ip vrf customer_a
rd 1:2
route-target both 1:2

D. ip vrf customer_a
rd 1:2
route-target both 1:1

84. 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.

85. An engineer configured a company's multiple area OSPF head office router and Site A cisco
routers with VRF lite. Each site router is connected to a PE router of an MPLS backbone.
After finishing both site router configurations, none of the LSA 3,4 5, and 7 are installed at Site A
router.
Which configuration resolves this issue?
A. configure capability vrf-lite on Site A and its connected PE router under router ospf 1 vrf abc
B. configure capability vrf-lite on Head Office and its connected PE router under router ospf 1 vrf abc
C. configure capability vrf-lite on both PE routers connected to Head Office and Site A routers

under router ospf 1 vrf abc
D. configure capability vrf-lite on Head Office and Site A routers under router ospf 1 vrf abc

86. What destination addresses does EIGRP use when feasible? (Choose two).
A. IP address 224.0.0.9
B. IP address 224.0.0.10
C. IP address 224.0.0.8
D. MAC address 01:00:5E:00:00:0A
E. MAC address 0C:15:C0:00:00:01

87. You just discovered that a ping packet sent from one of the devices to another took a different
path in the return than it did on its way to the destination. What behavior caused this?
A. Windowing
B. Global synchronization
C. MSS
D. Asymmetric routing

88. The OSPF dead interval defaults to how many times the hello interval?
A. Two
B. Three
C. Four
D. Five

89. You need to resolve a route-selection problem in a redistributed network by increasing the
administrative distance to several networks for a protocol, other than EIGRP or BGP, so that
these routes will not be used. You create access list 5 to identify the relevant networks, and
access the routing protocol configuration prompt.
Which command will set the administrative distance to these networks to 220 for the selected
protocol?
A. Router(config-router)#list 5 distance 220
B. Router(config-router)#admin 220 access-list 5

C. Router(config-router)#distance 220 0.0.0.0 255.255.255.255 5
D. Router(config-router)#increase 0.0.0.0 255.255.255.255 admin 220 list 5

90. The OSPF database of a router shows LSA types 1, 2, 7, and 3 default router only.
Which type of area is this router connected to?
A. stub area
B. totally stubby area
C. NSSA totally stub
D. NSSA

91. A network administrator notices that the BGP state drops and logs are generated for missing
BGP hello keepalives. What is the potential problem?
A. Incorrect neighbor options
B. Hello timer mismatch
C. BGP path MTU enabled
D. MTU mismatch

92. Which task do you need to perform first when you configure IP SLA to troubleshoot a network
connectivity issue?
A. Specify the test frequency
B. Enable the ICMP echo operation
C. Schedule the ICMP echo operation
D. Verify the ICMP echo operation

93. Which protocol does VRF-Lite support?
A. IS-IS
B. ODR
C. EIGRP
D. IGRP

94. Which two features are provided by EIGRP for IPv6? (choose two)
A. Backbone areas
B. SPF algorithm
C. Partial updates
D. Area border router
E. Scaling

95. What happens when two EIGRP peers have mismatched K values?
A. The two devices are unable to correctly perform equal-cost routing
B. The two devices fail to perform EIGRP graceful shutdown when one device goes down
C. The two devices fail to from an adjacency
D. The two devices are unable to correctly perform unequal-cast load balancing

96. Refer to the exhibit. The server for the finance department is not reachable consistently on
the 200.30.40.0/24 network and after every second month it gets a new IP address.
Which two actions must be taken to resolve this Issue? (Choose two).

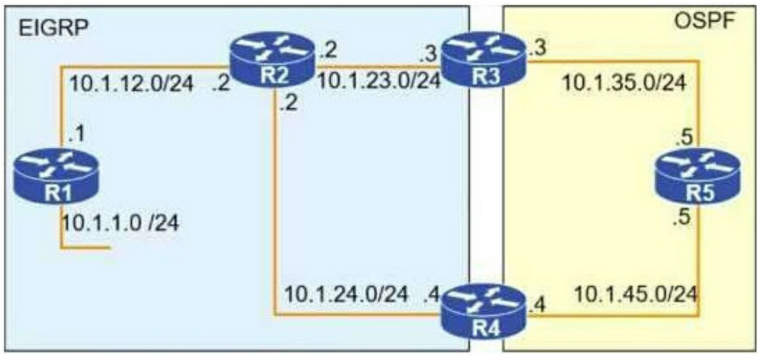
```
ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!
```

A. Configure the server to use DHCP on the network with default gateway 200 30.40.100.
B. Configure the server with a static IP address and default gateway.
C. Configure the router to exclude a server IP address.
D. Configure the server to use DHCP on the network with default gateway 200 30.30.100.
E. Configure the router to exclude a server IP address and default gateway.

97. 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

98. Refer to the exhibit. To provide reachability to network 10.1.1.0 /24 from R5, the network
administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a path through R5 to reach 10.1.1.0/24 network. Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?



R1	R3
router eigrp 1 redistribute connected network 10.1.12.1 0.0.0.0 default-metric 1000000 10 255 1 1500	router eigrp 1 network 10.1.23.3 0.0.0.0 ! router ospf 1 redistribute eigrp 1 subnets network 10.1.35.3 0.0.0.0 area 0

A. Change the administrative distance of the external EIGRP to 90.
B. Apply the outbound distribution list on R5 toward R4 in OSPF.
C. Change the administrative distance of OSPF to 200 on R5.
D. Redistribute OSPF into EIGRP on R4.

99. Refer to the Router output. An engineer wanted to set a tag of 30 to route 10.1.80.65/32 but it failed. How is the issue fixed?

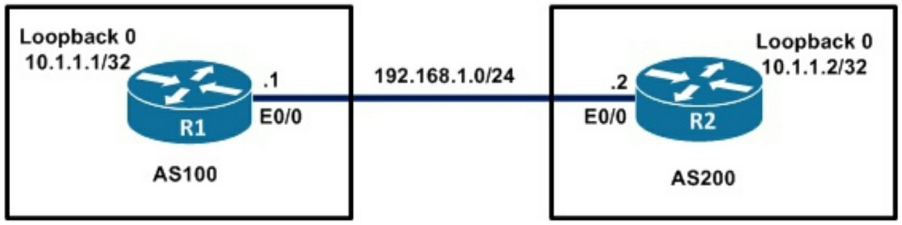
R1

```
ip prefix-list ccnp1 seq 5 permit 10.1.48.9/024 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.9/024 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.9/024 le 24

route-map ospf-to-eigrp permit 10
   match ip address prefix-list ccnp1
   set tag 30
route-map ospf-to-eigrp permit 20
   match ip address prefix-list ccnp2
   set tag 20
route-map ospf-to-eigrp permit 30
   match ip address prefix-list ccnp3
   set tag 10
```

A. Modify prefix-list ccnp3 to add 10.1.64.0/20 ge 32.
B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.
C. Modify prefix-list ccnp3 to add 10.1.64.0/20 le 24.
D. Modify route-map ospf-to-eigrp permit 30 and match prefix-list ccnp2.

100. An engineer needs dynamic routing between two routers and is unable to establish OSPF
adjacency. The output of the show ip ospf neighbor command shows that the neighbor state is
EXSTART/EXCHANGE. Which action should be taken to resolve this issue?
A. match the passwords
B. match the hello timers
C. match the MTUs
D. match the network types

101. Refer to the exhibit. The neighbor is not coming up. Which two sets of configurations bring the neighbors up? (Choose two).



The R1 and R2 configurations are as follows:

R1
router bgp 100
neighbor 10.1.1.2 remote-as 200

R2
router bgp 200
neighbor 10.1.1.1 remote-as 100

A.
R2
ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
neighbor 10.1.1.1 disable-connected-check
neighbor 10.1.1.1 disable-source loopback 0

B.
R2
ip route 10.1.1.1 255.255.255.255 192.168.1.1
!
router bgp 200
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.1 update-source loopback 0

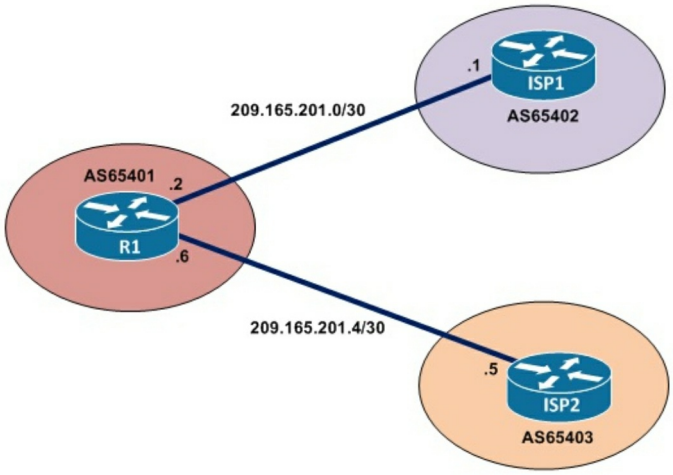
C.
R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2

!
router bgp 100
neighbor 10.1.1.2 disable-connected-check
neighbor 10.1.1.2 disable-source loopback 0

D.
R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.1 ttl-security hops 1
neighbor 10.1.1.2 update-source loopback 0

E.
R2
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.2 ttl-security hops 1
neighbor 10.1.1.2 update-source loopback 0

102. Refer to the exhibit. A company with an autonomous has obtained IP system number AS6401 and an address block of 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer with ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 resolves the issue?



R1#
interface GigabitEthernet0/0
  ip address 209.165.201.2 255.255.255.252
!
interface GigabitEthernet0/1
  ip address 209.165.201.6 255.255.255.252
!
router bgp 65401
bgp log-neighbor-changes
redistribute static
neighbor 209.165.201.1 remote-as 65402
neighbor 209.165.201.5 remote-as 65403
!
ip route 209.165.203.224 255.255.255.224 Null0
ip route 209.165.202.128 255.255.255.224 Null0
!

A.
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 out

B.
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 in

C.
ip route 209.165.200.224 255.255.255.224 209.165.201.1
ip route 209.165.200.128 255.255.255.224 209.165.201.5

D.
ip route 0.0.0.0 0.0.0.0 209.165.201.1
ip route 0.0.0.0 0.0.0.0 100 209.165.201.5

103. Refer to the exhibit. All the serial links between R1, R2, and R3 have the same bandwidth. Users on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path, it shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up. What must the network administrator to fix the slowness?

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, Ethernet0/0
L   192.168.1.1/32 is directly connected, Ethernet0/0
D   192.168.2.0/24 [90/2297856] via 192.168.12.2, 00:02:14, Serial1/1
S   192.168.3.0/24 [1/0] via 192.168.12.2
  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/24 is directly connected, Serial1/1
L   192.168.12.1/32 is directly connected, Serial1/1
  192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.13.0/24 is directly connected, Serial1/0
L   192.168.12.1/32 is directly connected, Serial1/0
D   192.168.23.0/24 [90/2681856] via 192.168.13.3, 00:06:38, Serial1/0
            [90/2681856] via 192.168.12.2., 00:06:38, Serial1/1
D   192.168.24.0/24 [90/2195456] via 192.168.12.2, 00:06:38, Serial1/1
```

A. Change the Administrative Distance of EIGRP to 5.
B. Add a static route on R1 using the next hop of R3.
C. Remove the static route on R1.
D. Redistribute the R1 route to EIGRP

Chapter 1: Answers

1. Which of the following sources of route information has the highest (i.e.

the least believable) administrative distance?

B. External EIGRP

The administrative distance (AD) of RIP is 120. The AD of External EIGRP (i.e. routes injected into EIGRP from a different autonomous system) is 170. OSPF's AD is 110, and Internal EIGRP (i.e. routes learned within an EIGRP autonomous system) has an AD of 90.

2. What is the seed metric for EIGRP?

C. Infinity

A seed metric is assigned to a redistributed route by default if you don't configure a different metric for your redistributed route. The seed metric for OSPF is 20, while the seed metric of RIP and EIGRP is Infinity.

3. Which of the following is not an option for assigning a metric to a routing protocol?

D. Specify a metric with a Route Tag.

All of the options are valid for setting a metric for a routing protocol other than "Specify a metric with a Route Tag." A Tag can be assigned to a route, but it acts as a label rather than a metric.

4. You wish to redistribute all routes within AS 1 into AS 2 with the exception of 192.168.1.0/24. Which of the following approaches can you use to selectively filter that route?

A. Create an ACL to match the 192.168.1.0/24 network, and reference that ACL under a "route map deny" statement.

A common way to filter a route from being redistributed is to match the network with an ACL. Then, that ACL can be referenced as part of a "route map deny" statement. For example, let's say you enter the "access-list 1 permit 192.168.1.0 0.0.0.255" command to create an ACL with a number of 1. Then, you can create a route map with a command such as "route-map DEMO deny 10". Then, in route-map configuration mode, you can reference ACL 1 with the command "match ip address 1". However, to allow other routes to be redistributed, you should follow-up the initial "route-map"

command with another “route-map” command having a higher sequence number, permitting all other routes, such as “route-map permit 20”.

5. What route-map configuration mode command is used to set a route tag to a value of 10?

D. set tag 10

You can set a tag on a route with the route-map configuration mode command “set tag 10”. Then, you can use the route-map configuration mode command “match tag 10” to recognize (and possibly deny) routes that are marked with a tag of 10.

6. When redistributing IPv6 routes, which of the following is true?

B. By default, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol.

Unlike redistributing IPv4 routes, when redistributing IPv6 routes, the “redistribute” command does not include connected routes on interfaces enabled for the redistributed protocol. However, you could instruct the “redistribute” command to redistribute those routes with the “redistribute [routing_source] connected-interfaces” command.

7. Where should Policy Based Routing (PBR) be applied on a router?

C. On a router’s ingress interface

Although “Local PBR” can be applied in a router’s global configuration mode, PBR is applied on a router’s ingress interface.

8. What configuration structure does PBR use to match traffic and specify behavior for that traffic?

B. route-map

A policy-map and class-map are used for quality of service (QoS). An access-class is used to limit incoming connections to a router’s management plane. However, a route-map can match traffic and dictate how that matched traffic should be treated, and it’s a route-map that’s used by Policy Based Routing (PBR).

9. Which of the following is true regarding VRF, by default?

D. With VRF, all virtual routers have their own independent IP routing tables.

With Virtual Routing and Forwarding (VRF), each virtual router maintains its own unique IP routing table. Therefore, different virtual routers running on the same physical router can run different routing protocols. Also, by default, virtual routers cannot see routes in the physical router's IP routing table. However, it is possible to configure "leak maps" to allow specific routers in the physical router's IP routing table to appear in the IP routing table of a virtual router.

10. In a VRF configuration, you wish view the IP routing table of a virtual router with a VRF instance name of "TENANT-A". What command would you use?

A. show ip route vrf TENANT-A

The "show ip route vrf TENANT-A" command is the appropriate command to view the IP routing table of the VRF instanced named "TENANT-A."

11. Which of the following protocols does EIGRP use to ensure delivery of routing updates?

C. RTP

EIGRP uses the Reliable Transport Protocol (RTP) to ensure delivery of routing updates to its neighbors. However, RTP is not used to confirm receipt of Hello messages. Spanning Tree Protocol (STP) is used to prevent a Layer 2 topological loop. The Dijkstra Algorithm is used by OSPF to select the shortest path to a destination network. The Diffusing Update Algorithm (DUAL) is used by EIGRP to select Successor and Feasible Successor routes.

12. Refer to The exhibit. The network administrator must mutually redistribute routes at the Chicago router to the LA and New York routers. The configuration of the Chicago router is this:
After the configuration, the LA router receives all the New York routes, but New York router does
not receive any LA routes. Which set of configurations fixes the problem on

the Chicago router?

Chicago:
router ospf 1
redistribute eigrp 100
router eigrp 100
redistribute ospf 1

B.
router eigrp 100
redistribute ospf 1 metric 10 10 10 10 10

"LA router receives all the NewYork routes but it does not receive any LA routes" because when
redistributing into EIGRP, we must configure the default metric.

13. What is EIGRP's default Hold Time on a LAN interface?

C. 15 seconds

On a LAN interface, EIGRP's default Hello Time is 5 seconds, and its default Hold Time is 15 seconds.

14. By default, EIGRP uses which of the following parameters to calculate its metric?

B. Bandwidth and Delay

By default, EIGRP uses Bandwidth and Delay to calculate its metric. However, EIGRP's K-values can be adjusted for its metric calculation causing the calculation to also include Reliability and Load. Although Maximum Transmission Unit (MTU) size does not factor into EIGRP's metric calculation directly, MTU size can be used as a tie breaker between two routes with equal metrics.

15. What is the name given to an EIGRP backup route that has met the Feasibility Condition?

A. Feasible Successor Route

An EIGRP Successor Route is the preferred route to a destination network, while an EIGRP Feasible Successor Route is a backup route that has met the Feasibility condition.

16. EIGRP's Feasibility Condition requires a Feasible Successor's Reported Distance to be less than what?

D. The Feasible Distance of the Successor Route

EIGRP's Feasibility Condition requires a Feasible Successor's Reported Distance (RD) to be less than the Feasible Distance (FD) of the Successor Route (i.e. the preferred route).

17. If an EIGRP router loses its Successor Route to a destination network and it has no Feasible Successor Route, what message does the router send out in an attempt to find an alternate path to the network?

B. Query

EIGRP sends out a Query message in an attempt to find an alternate route to a network if it loses its Successor Route to that network and it has no Feasible Successor Route. In earlier versions of Cisco IOS, if the Query Reply was dropped on its way back to the sending router, the sending router might think that one or more downstream routers were unavailable. This resulted in a Stuck-In-Active (SIA) condition.

18. Which of the following is true of EIGRP for IPv4 neighbors?

C. EIGRP neighbors must have matching Autonomous System (AS) numbers

EIGRP neighbors do not need matching Variance values. Also, OSPF uses Process IDs, EIGRP does not. Instead, EIGRP must have matching Autonomous System (AS) numbers. Finally, while having matching Hello and Hold Timers is considered a best practice, it is not required for EIGRP. However, OSPF does require matching timer values.

19. What can be used in an EIGRP Stub Router configuration to allow selected routes to be advertised by the Stub Router?

A. Leak Map

A Route Map can be configured to identify specific routes. Then, that Route Map can be reference by a Leak Map in a Stub Router configuration to allow selected routes (i.e. the routes specified by the Route Map) to be advertised by the Stub Router.

20. Under which condition will EIGRP not load balance across a backup path with the Variance feature?

B. The backup path does not meet the Feasibility Condition.

EIGRP's Variance feature will load balance across one or more backup paths if those backup paths have a metric that is equal to or less than the product of the Variance value and the metric (i.e. the Feasible Distance) of the Successor Route. However, a backup path will not be used for load balancing if it did not meet the Feasibility Condition.

21. What command is used to enable EIGRP's Automatic Summarization feature?

D. Router(config-router)# auto-summary

EIGRP's Auto Summarization feature causes EIGRP to advertise classful networks, rather than the subnets within those classful networks. This feature is enabled in router configuration mode with the "auto-summary" command.

22. What interface configuration mode command is issued to tell an interface to participate in an EIGRP for IPv6 routing process for Autonomous System (AS) 1?

C. Router(config-if)# ipv6 eigrp 1

The "ipv6 eigrp [AS]" command is issued in interface configuration mode to cause an interface to participate in an EIGRP for IPv6 routing process.

23. Under what Named EIGRP configuration mode would you configure the Variance option?

A. Address-Family-Topology configuration mode

With Named EIGRP, you can configure topology-wide features such as Route Redistribution and Variance under Address-Family-Topology configuration mode.

24. Which of the following routing protocols support the SHA hashing algorithm?

C. Named EIGRP

While Named EIGRP supports both the MD5 and SHA hashing algorithms, EIGRP for IPv4 and EIGRP for IPv6 only support the MD5 hashing algorithm.

25. What is the effect of setting a router's OSPF routing process to a Priority of 0?

C. It prevents that router from participating in a DR election.

On an OSPF network segment that elects a Designated Router (DR) and Backup Designated Router (BDR), the router on the network segment with the highest Priority is elected as the DR. If the Priority values on all routers are the same, the router with the highest Router ID wins the DR election. However, if you do not wish for a router to participate in the DR election, you can set its Priority to 0.

26. By default, if you set an OSPF interface's Hello timer to 10 seconds, what will be the value of the Dead timer?

D. 40 seconds

By default, an OSPF interface's Dead timer is four times the Hello timer. Therefore, if an OSPF interface's Hello timer is 10 seconds, its Dead timer would be 40 seconds (i.e. 10 * 4 = 40).

27. What is the default Reference Bandwidth used by OSPF to calculate Cost?

B. 100 Mbps

OSPF calculates the Cost of an interface by dividing the interface's speed by

OSPF's Reference Bandwidth. The default Reference Bandwidth used by OSPF is 100 Mbps. Since Cost must be an integer, interfaces speeds of 100 Mbps or greater all have a cost of 1 by default. Therefore, a best practice recommendation is to set OSPF's Reference Bandwidth to at least the bandwidth amount of the highest speed interface being used by OSPF.

28. What is the default OSPF Network Type of a non-Frame Relay OSPF interface?

A. Point-to-Point

The default OSPF Network Type on an Ethernet interface is Broadcast. The default OSPF Network Type on a non-Frame Relay interface is Point-to-Point, and the default OSPF Network Type on a Frame Relay physical interface is NBMA (Non-Broadcast Multiple Access).

29. What LSA Type is used to inject networks from a separate autonomous system (AS) into an OSPF Stub or Totally Stubby Area?

D. Type 7

Type 5 LSAs are typically used to inject networks from a separate AS into OSPF. However, an OSPF Stub or Totally Stubby Area cannot have Type 5 LSAs. As a result, Type 7 LSAs are used to inject those networks.

30. What Cisco IOS command is used to change the default reference-bandwidth of an OSPF-speaking router?

B. interface-cost [bandwidth_amount]

OSPF's default Reference Bandwidth is 100 Mbps. Therefore, this value should typically be changed to a higher value, in order to calculate different Cost values for interface speeds greater than 100 Mbps. To set a non-default Reference Bandwidth, in router configuration mode you can used the command: auto-cost reference-bandwidth [bandwidth_amount], where the unit of measure for bandwidth_amount is Mbps.

31. What types of packets are sent over an OSPF Virtual Link?

B. OSPF packets

An OSPF Virtual Link can be used to logically connect a discontiguous

OSPF Area to a Backbone Area. While an OSPF Virtual Link is a type of tunnel, it is not a GRE tunnel, and no GRE packets are sent. Only OSPF packets are logically sent over the Virtual Link, with the Data packets traveling over physical links.

32. What Cisco IOS command is used to perform OSPF route summarization on an ABR?

A. area range

Unlike EIGRP, which can perform route summarization on any router, OSPF can only perform route summarization on an Area Border Router (ABR) or an Autonomous System Boundary Router (ASBR). The command used to perform OSPF route summarization on an ABR is the “area range” command, and the command used to perform OSPF route summarization on an ASBR is the “summary-address” command.

33. What OSPFv3 LSA Type is used to advertise an area’s Link Local address?

C. Type 8

OSPFv3 adds a couple of LSA types to those seen with OSPFv2. Specifically, Type 8 and Type 9 LSA types are added. A Type 8 LSA (a.k.a. a “Link LSA”) is used to advertise Link Local addresses within an OSPF area, while a Type 9 LSA (a.k.a. an “Intra Area Prefix LSA”) is used to advertise networks within an OSPF area.

34. What command is used to create an OSPFv3 routing process with the Address Families configuration approach?

A. router ospfv3 [process-id]

The “ipv6 router ospf [process-id]” command is used to create an OSPFv3 routing process using the Traditional Configuration approach. However, the “router ospfv3 [process-id]” command is used to create an OSPFv3 routing process using the Address Families configuration approach.

35. Which of the following is a hashing option for OSPFv3 Address Families authentication?

D. SHA-1

Secure Hash Algorithm 1 (“SHA-1” or “sha1”) and Message Digest 5 (“MD5”) are the only hashing algorithms supported for OSPFv3 Address Families authentication.

36. What well-known port is used by BGP when establishing a session?

A. TCP 179

BGP neighbor adjacencies are established using a manual configuration, pointing to a peer router. This communication takes place over TCP port 179. TCP allows BGP to handle fragmentation, sequencing, and provide reliability.

37. In which state does a BGP-enabled router wait for the receipt of a Keepalive message in order to completely establish the BGP session?

D. OpenConfirm

In the OpenConfirm state, BGP waits for the receipt of either a Keepalive or Notification message. If no Keepalive message arrives, the state will move back to Idle. If there is the receipt of a neighbor’s Keepalive message, the BGP session moves to the final Established state.

38. Which BGP command allows us to change interface source address used when establishing a neighbor adjacency?

C. update-source

The “update-source” command allows us to change the interface source address used when establishing a BGP session. By default, when establishing a neighbor adjacency with another BGP-enabled router, the session is formed using the IP address of the outgoing interface nearest to the neighbor. It’s common to create a loopback interface on a router and set this instead as the source of a BGP session. This helps guard against outages, in a case where there may be redundant links between BGP routers. If there are redundant links and one link goes down, the BGP session will also momentarily go down and establish a second session with the redundant interface, creating a network outage during this transition. Using a loopback interface as the source address ensures a seamless transition in a case such as this.

39. Which category of BGP attributes must be present in all updates and are passed on to other BGP peers?

B. Well-known mandatory

Well-known mandatory attributes must be present and understood by all BGP peers, and they are required to exist in the BGP update message. These attributes can be seen in the output of the “show ip bgp” command, and include attributes such as the origin, the autonomous system path, and the next-hop address.

40. Which command allows us to disable the default BGP synchronization feature found in older Cisco IOS versions?

D. no synchronization

A BGP router with synchronization enabled will only advertise a route learned from an internal BGP (iBGP) peer to an external BGP (eBGP) peer when there is an exact match of that route learned from an IGP (such as EIGRP or OSPF) in the routing table. The “no synchronization” command will specifically disable this feature, although by default this is already disabled in newer Cisco IOS versions.

41. Which mechanism within Multiprotocol BGP (MP-BGP) allows BGP to carry multiple protocols at once?

C. Address families

Address families allow MP-BGP to carry multiple protocols at once. BGP will default to an IPv4 address family if none is indicated, dedicated to carrying IPv4 routes. Other address families can be defined for other protocols depending on the IOS platform in use, including IPv6, VPNv4 and VPNv6 address families.

42. Which BGP feature allows us to reduce the number of BGP updates created, lowering resource usage on BGP-enabled devices?

A. Peer group

BGP peer groups allow us to group neighbors together in order to share configurations and policies. When BGP creates updates, a separate update is

created for each neighbor. Peer groups can simplify our configuration and use less device resources, since updates will be processed for the peer group as a whole rather than for each separate neighbor.

43. What is the default time-to-live (TTL) value used with external BGP (eBGP)?

D. 1

External BGP (eBGP) by default requires two BGP-enabled routers to be directly connected to one another in order to properly establish a neighbor adjacency. This is because the default TTL value is 1 when using eBGP. The BGP multihop feature can be used to overcome this, allowing us to configure a higher TTL value.

44. Which BGP mechanism allows all internal BGP (iBGP) neighbors within an autonomous system to learn about all available routes without creating loops in the network, and without using a full-mesh configuration?

C. Route reflectors

Internal BGP (iBGP) neighbors do not add their own autonomous system number to the BGP update messages sent out. For this reason, any routes learned from another iBGP neighbor will not be advertised to any other iBGP neighbor, which would require a full-mesh network to overcome. An alternative to this a BGP route reflector, which allows us to point to other iBGP routers in order to specifically forward routes that would not normally be sent.

45. Which optional keyword is used to suppress prefixes and present only an aggregate address in the BGP update?

B. summary-only

BGP can advertise a summarized route through the “aggregate-address” command. By default, the summary address, along with all other prefixes, will be advertised in the BGP updates sent out to peers. These prefixes can be suppressed so that BGP updates only send out the summarized route to peers by appending the “summary-only” keyword when configuring the aggregate address.

46. Which BGP command allows for routes to be received even if a router sees its own autonomous system number in the AS-Path section of a BGP update?

C. allowas-in

The Allow AS feature overrides the default behavior where a BGP router will discard a prefix in which its own autonomous system number is seen in the AS-Path. This is a built-in loop prevention mechanism that can be overridden with the “allowas-in” command.

47. What is the definition of a floating static route?

C. A static route with an administrative distance higher than 1.

The default administrative distance of a static route is 1. By manually configuring a static route with an administrative distance higher than 1, we are creating a floating static route. This is useful in cases where we want to provide a static backup route for a primary link. An example of this would be configuring two ISP connections and using tracking objects to automatically switch between those in the case of a failure.

48. Refer to the exhibit. A router receiving BGP routing updates from multiple neighbors for routers in
AS 690. What is the reason that the router still sends traffic that is destined to AS 690 to a neighbor other than 10.222.1.1?

```
router bgp 100
!
  neighbor 10.222.1.1 route-map SET-WEIGHT in
  neighbor 10.222.1.1 remote-as 1
!
ip as-path access-list 200 permit ^690$
ip as-path access-list 200 permit ^1800
!
route-map SET-WEIGHT permit 10
  match as-path 200
  set local-preference 250
  set weight 200
```

D. The weight value in another statement is higher than 200.

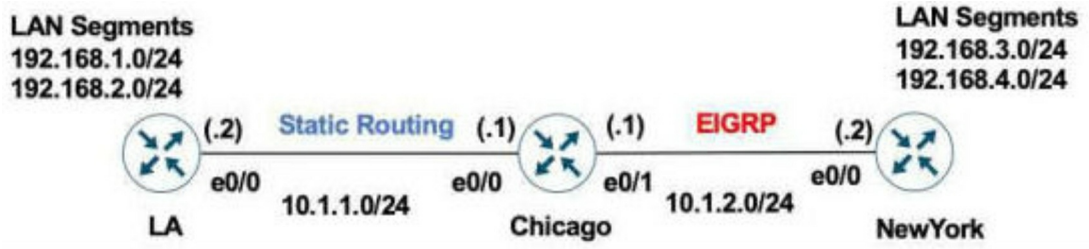
From the configuration above, we learn that the local-preference and weight in BGP updates received from neighbor 10.222.1.1 are updated to 250 and 200, respectively (provided that it matches the AS-PATH in ACL 200). The local-preference attribute is used to influence the routing decision on the neighbor IBGP router while the weight attribute is used to influence the routing decision on the local router (it is only used locally in a router). In this scenario, the weight attribute is used.

49. Refer to the exhibit. What is the result if applying this configuration?

```
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
```

A. The router can form BGP neighborships with any other device.

50. Refer to the exhibits. A user on the 192.168 1.0/24 network can successfully ping 192.168.3.1,
but the administrator cannot ping 192.168.3.1 from the LA router. Which set of configurations fixes the issue?



Chicago Router

ip route 192.168.1.0 255.255.255.255.0 10.1.1.2
ip route 192.168.2.0 255.255.255.255.0 10.1.1.2
!
router eigrp 100
  redistribute static

LA Router
ip route 0.0.0.0 0.0.0.0 10.1.1.1

A. Chicago Router
router eigrp 100
redistribute static metric 10.10.10.10

51. Refer to the exhibit. Which control plan policy limits BGP traffic that is destined to the CPU to 1
Mbps and ignores BGP traffic that is higher rate?

```
Cat3850-Stack-2# show policy-map

Policy Map LIMIT_BGP
  Class BGP
    drop

Policy Map SHAPE_BGP
  Class BGP
    Average Rate Traffic Shaping
    cir 10000000 (bps)

Policy Map POLICE_BGP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action transmit

Policy Map COPP
  Class BGP
    police cir 1000k bc 1500
      conform-action transmit
      exceed-action drop
```

D. policy-map COPP

52. Which configuration enables the VRF that is labeled `'inet" on FastEthernet0/0?

C. R1(config)# ip vrf Inet
R1(config-vrf)#interface FastEthernet0/0
R1(config-if)#ip vrf forwarding Inet

The first command “R1(config)# ip vrf Inet” creates vrf Inet while the two last commands
associate the VRF with interface Fa0/0.

53. Which attribute eliminates LFAs that belong to protected paths in situations where links in a
network are connected through a common fiber?

B. Shared risk link group-disjoint

Shared Risk Link Group (SRLG)-disjoint—Eliminates LFAs that belong to any of the protected
path SRLGs. SRLGs refer to situations where links in a network share a common fiber (or a
common physical attribute). If one link fails, other links in the group may also fail. Therefore, links
in a group share risks.

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

B. show ip route vrf

To display the IP routing table information associated with a VRF, use the following command:
show ip route vrf vrf-name [connected] [protocol [as- Displays IP routing table number] [list
[list-number]] [mobile] [odr] [profile] information associated [static] [summary][supernetsonly] with a VRF.

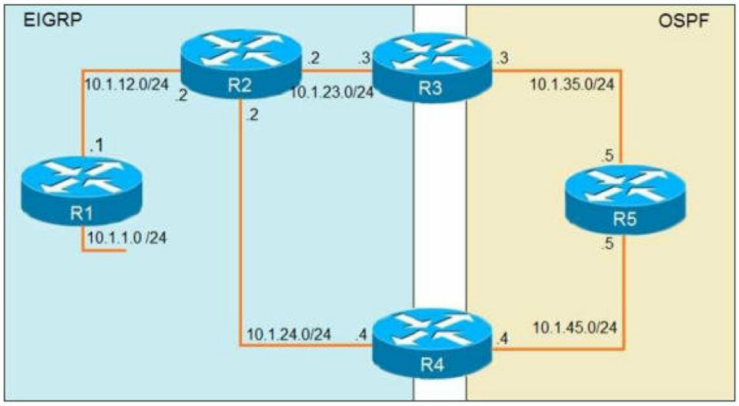
55. R2 has a locally originated prefix 192.168.130.0/24 and has these configurations:

What is the result when the route-map OUT command is applied toward an eBGP neighbor R1
(1.1.1.1) by using the neighbor 1.1.1.1 route-map OUT command?

A. R1 sees 192.168.130.0/24 as two hops away instead of one AS hop away

AS-Path prepending is a way to manipulate the AS-Path attribute of a BGP route. It allows
prepending multiple entries of AS to a BGP route.

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



R1
router eirp 1
redistribute connected
network 10.1.12.1 0.0.0.0

R3
router ospf 1
redistribute eigrp 1 subnets
network 10.1.35.0 0.0.0.0 area 0

R4
router eirp 1
redistribute ospf 1 metric 2000000 1 255 1 1500
!
router ospf 1
network 10.1.45.4 0.0.0.0 area 0
!
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

1 10.1.35.3 80 msec 44 msec 20 msec
2 10.1.23.2.44 44 msec 104 msec 64 msec
3 10.1.24.4.44 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 truncuated>

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 1500 route-map
FILTER-TAG
!
route-map FILTER-TAG deny 10
  match tag 1
!
route-map FILTER-TAG permit 20
```

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.

57. What is the role of a route distinguisher via a VRF-Lite setup implementation?

A. It extends the IP address to identify which VFP instance it belongs to.

In VRF-Lite, Route distinguisher (RD) identifies the customer routing table and “allows customers

to be assigned overlapping addresses". The below example shows overlapping IP addresses
configured on two interfaces which belong to two different VPNs:

```
Router(config)#ip vrf VRF_BLUE
Router(config-vrf)# rd 100:1
Router(config-vrf)# exit
Router(config)#ip vrf VRF_GREEN
Router(config-vrf)# rd 100:2
Router(config-vrf)# exit
Router(config)# interface GigabitEthernet0/1
Router(config-if)# ip vrf forwarding VRF_BLUE
Router(config-if)# ip address 10.0.0.1 255.0.0.0
Router(config-vrf)# exit
Router(config)# interface GigabitEthernet0/2
Router(config-if)# ip vrf forwarding VRF_GREEN
Router(config-if)# ip address 10.0.0.1 255.0.0.0
```

In this example, the RD will be added to the beginning of the IP address. For example with
VRF_BLUE (rd 100:1), an IP address will be seen like this: 100:1:10.0.0.1/8 so that it is unique in
the routing table.

58. Refer to the exhibit. 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?

```
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#
```

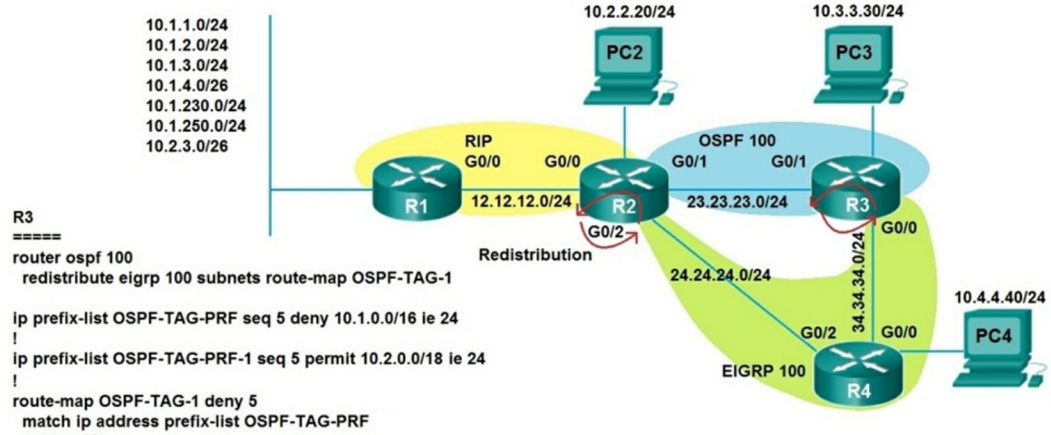
D. R2 does not have a route to the next hop, so R2 does not advertise the prefix to the clients.

With route reflector (RR), we only need to establish a BGP session from the RR to each internal
peer -> Answer A is not correct.
We can advertise both classful and classless prefix to other clients, provided that the prefix
satisfies the RR forwarding rules -> Answer B and answer C are not correct.
Therefore only answer D is left. Maybe we are missing an IGP in our topology so R2 did not know
how to reach the next hop reported by the prefix.

59. Which method changes the forwarding decision that a router makes first changing the routing
table or influencing the IP data plane?

A. Policy-based routing

60. Refer to the exhibit. Which subnet is redistributed from EIGRP to OSPF routing protocols?




```
R3
=====
router ospf 100
  redistribute eigrp 100 subnets route-map OSPF-TAG-1

ip prefix-list OSPF-TAG-PRF seq 5 deny 10.1.0.0/16 ie 24
!
ip prefix-list OSPF-TAG-PRF-1 seq 5 permit 10.2.0.0/18 ie 24
!
route-map OSPF-TAG-1 deny 5
  match ip address prefix-list OSPF-TAG-PRF
  set tag 40
!
route-map OSPF-TAG-1 permit 10
  match ip address prefix-list OSPF-TAG-PRF-1
  set tag 80
!
```

A. 10.2.2.0/24

Only the subnet that matches prefix-list OSPF-TAG-PRF-1 will be redistributed into OSPF (as
indicated by “route-map OSPF-TAG-1 permit 10”). This subnet must match the prefix-list OSPFTAG-PRF-1 so it must be 10.2.0.0/18 to 10.2.0.0/24. Only the subnet 10.2.2.0/24 matches this
requirement.

61. Refer to the exhibit. An engineer is trying to redistribute OSPF to BGP, but not all of the routes are redistributed. What is the reason for this issue?

```
Router#sh ip route ospf
<output omitted>
Gateway is last resort is not set

      10.0.0.0/24 is subnetted, 1 subnets
   o  E2     10.0.0.0 [110/20] via 192.168.12.2, 00:00:10, Ethernet0/0
   o       192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:50, Ethernet0/0
Router#

Router#show ip bgp
<output omitted>
      Network          Next Hop      Metric     LocPrf     Weight     Path
>*    192.168.1.1/32   0.0.0.0            0                32768      ?
>*    192.168.3.0      192.168.12.2      20                32768      ?
>*    192.168.12.0     0.0.0.0            0                32768      ?
Router#show running-config | section router bgp
router bgp 65000
 bgp log-neighbor-changes
 redistribute ospf 1
Router#
```

A. By default, only internal OSPF routes are redistributed into BGP.

If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and
inter-area routes are redistributed into BGP, by default.
You can redistribute both internal and external (type-1 & type-2) OSPF routes via this command:
“Router(config-router)#redistribute ospf 1 match internal external 1 external 2”

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

B. Different customers can have overlapping IP addresses on different VPNs.

E. Each customer has its own private routing table.

VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but a Layer 3 interface cannot belong to more than one VRF at any time.

63. 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#
```

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

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

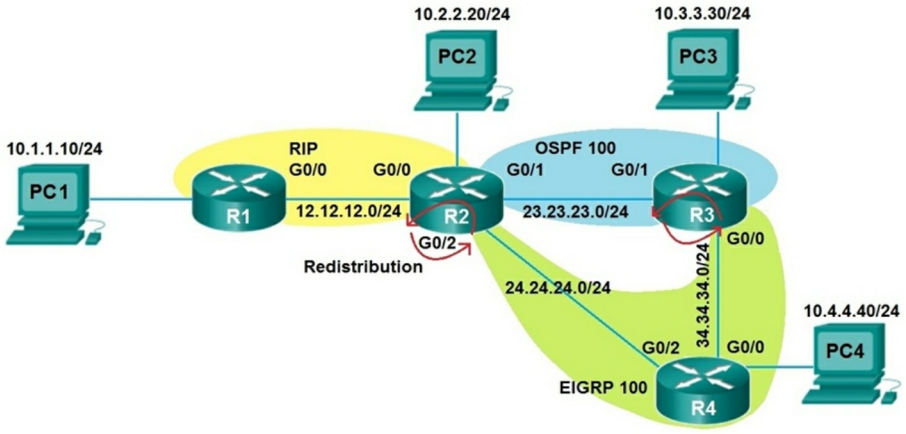
to summarize externally redistributed routes from another protocol domain or you have a NSSA
area. But a requirement to create a summarized route is:
"The ASBR compares the summary route’s range of addresses with all routes redistributed into
OSPF on that ASBR to find any subordinate subnets (subnets that sit inside the summary route
range). If at least one subordinate subnet exists, the ASBR advertises the summary route."
But in this case, we found no prefix that belongs to 10.0.0.0/8. Therefore, a summarized route for
this subnet could not be created.
Note:
+ If a prefix of this subnet exists in the routing table, then, after the summarization is performed, we
will see such an entry:
Router# show ip route
— output omitted —
0 10.0.0.0/8 is a summary via null0

64. Which is statement about IPv6 inspection is true?

**B. It learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor
tables.**

IPv6 Neighbor Discovery (ND) inspection learns and secures bindings for stateless
autoconfiguration addresses in Layer 2 neighbor tables. IPv6 ND inspection analyzes ND
messages in order to build a trusted binding table. IPv6 ND messages that do not have valid
bindings are dropped.

65. Refer to the exhibit. After redistribution is enabled between the routing protocols; PC2, PC3, and
PC4 cannot reach PC1. Which action can the engineer take to solve the issue so that all the PCs are reachable?



A. Filter the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP.

It seems there is a loop because of mutual redistributions among RIP, OSPF and EIGRP
domains. So, we should filter out the prefix 10.1.1.0/24 when redistributed from OSPF to EIGRP
(the second redistribution point) to prevent routing loop.
66. Refer to the exhibit. An engineer configures a static route on a router, but when the engineer
checks the route to the destination, a different next hop is chosen. What is the reason for this?

```
Router#show running-config | include ip route
ip route 192.168.2.2 255.255.255.255 209.165.200.225 130
Router#show ip route

<output omitted>

Gateway of last resort is not set

      192.168.1.0/32 is subnetted, 1 subnets
C        192.168.1.1 is directly connected, Loopback0
      192.168.2.0/32 is subnetted, 1 subnets
O        192.168.2.2[110/11] via 192.168.12.2, 00:52:09, Ethernet0/0
      192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.12.0/24 is directly connected, Ethernet0/0
L        192.168.12.1/32 is directly connected, Ethernet0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.0/24 is directly connected, Ethernet0/1
         209.165.200.226/32 is directly connected, Ethernet0/1
```

A. The configured AD for the static route is higher than the AD of OSPF.

The AD of static route is manually configured to 130 which is higher than the AD of OSPF router
which is 110.

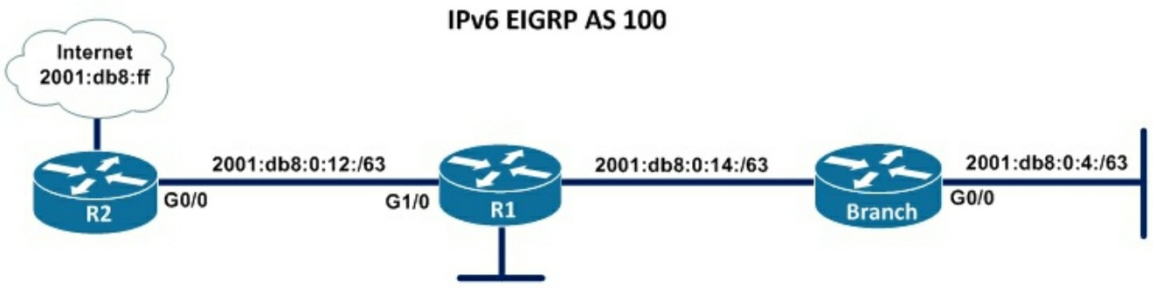
67. Refer to the exhibit. An engineer is troubleshooting BGP on a device but discovers that the clock
on the device does not correspond to the time stamp of the log entries. Which action ensures consistency between the two times?

```
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
* Jun 28 14:41:57: %BGP_SESSION-5-ADCHANGE: neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session  User reset
* Jun 28 14:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*15:42:00 506 CET Fri Jun 28 2019
```

C. Configure the service timestamps log datetime localtime command in global configuration mode.

Even we had a synchronized clock but it may show different timezone so we should set the
“localtime” keyword (which uses local time zone for timestamps) so that the time of logging
messages is matched with our clock.

68. Refer to the exhibit. Users in the branch network of 2001:db8:0:4::/64 report that they cannot
access the Internet. Which command is issued in IPv6 router EIGRP 100 configuration mode to



solve this issue?

R1#show ipv6 eigrp topology
EIGEP-IPv6 Topology Table for AS(100)1D(10.1.12.1)
Codes: P-Passive, A-Active, U-Update, Q-Query, R-Reply
r-reply Status, s-sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 28416
via FE80:C828:DFF:FEF4:1C(28416/2816), FastEthernet3/0
P 2001:DB8:0:1::/64, 1 successors, FD is 2816
via Connected, GigabitEthernet0/0
P ::/0, 1 successors, FD is 2816
via FE80:C821:17FF:FE04:8(2816/256), GigabitEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
via Connected, FastEthernet3/0
P 2001:DB8:0:12::/64, 1 successors, FD is 2816
via Connected, GigabitEthernet1/0

Branch#show ipv6 eigrp topology
EIGEP-IPv6 Topology Table for AS(100)1D(4.4.4.4)
Codes: P-Passive, A-Active, U-Update, Q-Query, R-Reply
r-reply Status, s-sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 2816
via Connected, GigabitEthernet0/0
P 2001:DB8:0:1::/64, 1 successors, FD is 28416
via FE80:C820:17FF:FE04:54(28416/2816), FastEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
via Connected, FastEthernet1/0
P 2001:DB8:0:12::/64, 1 successors, FD is 28416
via FE80:C820:17FF:FE04:54(28416/2816), FastEthernet1/0

B. Issue the no eigrp stub command on R1.

In the output of R1, we see R1 has a default route to the Internet via G1/0, which is correct but R2
does not have this route. One reasonable answer of this issue is R1 has been configured as a

stub router so it only advertised connected and summary routes. In Branch router output, we also
see routes that are directly connected to R1 only.
Note: In this topology, only Branch router should be configured as stub, not R1 router.

69. Which of the following are true statements regarding OSPF adjacency states? (Choose three).

A. 2-way - Routers exchange information with other routers in the multiaccess network.

C. ExStart - The network has already elected a DR and a backup BDR.

D. Init - The OSPF router ID of the receiving router was not contained in the hello message.

When OSPF adjacency is formed, a router goes through several state changes before it becomes
fully adjacent with its neighbor. The states are Down -> Attempt (optional) -> Init -> 2-Way ->
Exstart -> Exchange -> Loading -> Full. Short descriptions about these states are listed below:
Down: no information (hellos) has been received from this neighbor.
Attempt: only valid for manually configured neighbors in an NBMA environment. In Attempt state,
the router sends unicast hello packets every poll interval to the neighbor, from which hellos have
not been received within the dead interval.
Init: specifies that the router has received a hello packet from its neighbor, but the receiving
router’s ID was not included in the hello packet
2-Way: indicates bi-directional communication has been established between two routers.
Exstart: Once the DR and BDR are elected, the actual process of exchanging link state
information can start between the routers and their DR and BDR.
Exchange: OSPF routers exchange and compare database descriptor (DBD) packets

Loading: In this state, the actual exchange of link state information occurs. Outdated or missing
entries are also requested to be resent.
Full: routers are fully adjacent with each other.

70. Refer to Exhibit. Which statement about redistribution from BGP into OSPF process 10 is true?

```
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
```

A. Network 172.16.1.0/24 is not redistributed into OSPF.

The first statement of the above route-map (route-map BGP-TO-OSPF deny 10) will prevent
network 172.16.1.0/24 from being redistributed into OSPF.

71. Which two statements about redistributing EIGRP into OSPF are true? (Choose two)

B. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database
autonomous system number

F. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table.

72. What is a prerequisite for configuring BFD?

C. Cisco Express Forwarding must be enabled on all participating BFD endpoints.

*Cisco Express Forwarding (CEF) and IP routing must be enabled on all participating routers.

*You must enable Cisco Parallel eXpress Forwarding (PXF) on the Cisco 10720 Internet router in order for BFD to operate properly. PXF is enabled by default and is generally not turned off.

*One of the IP routing protocols supported by BFD must be configured on the routers before BFD is deployed. You should implement fast convergence for the routing protocol that you are using. See the IP routing documentation for your version of Cisco IOS software for information on configuring fast convergence. See the "Restrictions for Bidirectional Forwarding Detection" section for more information on BFD routing protocol support in Cisco IOS software.

73. Which configuration adds an IPv4 interface to an OSPFv3 process in OSPFv3 address family
configuration?

B. Router(config-router)#ospfv3 1 ipv4 area 0

The newest OSPFv3 configuration approach utilizes a single OSPFv3 process. It is capable of
supporting IPv4 and IPv6 within a single OSPFv3 process. OSPFv3 builds a single database with
LSAs that carry IPv4 and IPv6 information. The OSPF adjacencies are established separately for
each address family. Settings that are specific to an address family (IPv4/IPv6) are configured
inside that address family router configuration mode.
Running single OSPFv3 for both IPv4 and IPv6 is supported since Cisco IOS Software Release
15.1(3)S.
The new-style OSPFv3 process is enabled using the router ospfv3 process-number command.
Within the OSPF process configuration mode, the OSPF process ID is defined (using the routerid ospf-process-ID command).
OSPFv3 New-Style OSPF Configuration Commands:

Therefore, answer B is the best answer here but in this answer, the configuration mode is not
correct. It should be interface mode (config-if)#, not router mode (config-router)#.

74. While troubleshooting connectivity issues to a router, these details are noticed:
- Standard pings to all router interfaces, including loopbacks, are successful.
- Data traffic is unaffected.
- SNMP connectivity is intermittent.
- SSH is either or disconnects frequently.
Which command must be configured first to troubleshoot this issue?

A. Show policy-map control-plane

The “show policy-map control-plane” is used to display the service-policy associated to the
control-plane. It also shows the packets that matched the class-map. An example of the output of this command is shown below:

75. Refer to the exhibit. Which statement about R1 is true?

```
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
```

B. RIP learned routes are distributed to OSPF with a tag value of one.

If a metric is not specified, OSPF puts a default value of 20 when redistributing routes from all protocols except Border Gateway Protocol (BGP) routes, which get a metric of 1.

76. Refer to the exhibit. Which routes from OSPF process 5 are redistributed into EIGRP?

```
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
```

A. E1 and E2 subnets matching access list TO-OSPF

Use the external keyword along with the redistribute command to redistribute OSPF external
routes. In order to use an prefix-list in a “match” statement, we have to use the command “match ip
address prefix-list …”. The syntax of a “match” statement is as follows:
match ip address {access-list-number [access-list-number… | access-list-name…] | access-listname [access-list-number…| access-list-name] | prefix-list prefix-list-name [prefix-list-name…]}

77. What is the output of the following command:

show ip vrf

A. Shows default RD values

An example of the “show ip vrf” is shown below:

```
Router#show ip vrf
Name                 Default RD          Interfaces
SiteA2               103:30              Serial1/0.20
SiteB                103:11              Serial1/0.100
SiteX                103:20              Ethernet0/0
```

```
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#
```

78. Refer to the exhibit. In which circumstance does the BGP neighbor remain in the idle condition?

D. If prefixes exceed the maximum limit.

The neighbor will remain in the Idle state until the session is manually restarted with the command clear ip bgp [ip address]. If the neighbor is still sending the same number of prefixes and the maximum prefixes limit hasn't been changed, it will quickly return to the Idle (PfxCt) state.

79. Refer to the exhibit. An engineer is trying to get 192.168.32.100 forwarded through 10.1.1.1, but it was forwarded through 10.1.1.2. What action forwards the packets through 10.1.1.1?

```
router#show ip route
....
     D 192.168.32.0/19 [90/25789217] via 10.1.1.1
     R 192.168.32.0/24 [120/4] via 10.1.1.2
     O 192.168.32.0/26 [110/229840] via 10.1.1.3
```

D. Configure EIGRP to receive 192.168.32.0 route with equal or longer prefix than /24.

When a packet arrives on a router interface the route it choose to send the packet to depends on the prefix length, or the number of bits set in the subnet mask. Longer prefixes are always preferred over shorter ones when forwarding a packet.

80. An engineer configured a leak-map command to summarize EIGRP routes and advertises
specifically loopback 0 with an IP of 10.1.1.1.255.255.255.252 along with the summary route.
After finishing configuration, the customer complained not receiving summary route with specific
loopback address. Which two configurations will fix it? (Choose two).

A. Configure access-list 1 permit 10.1.1.0.0.0.0.3.

D. Configure route-map Leak-Route permit 10 and match access-list 1.

When you configure an EIGRP summary route, all networks that fall within the range of your
summary are suppressed and no longer advertised on the interface. Only the summary route is
advertised. But if we want to advertise a network that has been suppressed along with the
summary route then we can use leak-map feature. The below commands will fix the configuration
in this question:
R1(config)#access-list 1 permit 10.1.1.0 0.0.0.3
R1(config)#route-map Leak-Route permit 10 // this command will also remove the "route_map
Leak-Route deny 10" command.
R1(config-route-map)#match ip address 1

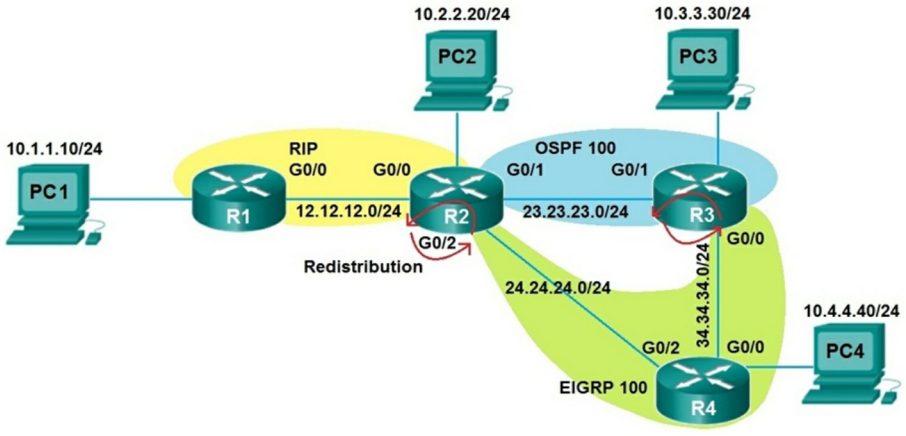
81. After some changes in the routing policy, it is noticed that the router in AS 45123 is being used as a transit AS router for several service provides. Which configuration ensures that the branch router in AS 45123 advertises only the local networks to all SP neighbors?

D.
ip as-path access-list 1 permit ^$
!
router bgp 45123
neighbor SP-Neighbors filter-list 1 out

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  1
```

82. Refer to the exhibit. Redistribution is enabled between the routing protocols, and now PC2 PC3,
and PC4 cannot reach PC1. What are the two solutions to fix the problem? (Choose two).



A. Filter RIP routes back into RIP when redistributing into RIP in R2.

B. Filter OSPF routes into RIP FROM EIGRP when redistributing into RIP in R2.

Even PC2 cannot reach PC1 so there is something wrong with RIP redistribution in R2. Because
RIP has higher Administrative Distance (AD) value than OSPF and EIGRP so it will be looped
when doing mutual redistribution.

83. Refer to the exhibit. The network administrator configured VRF lite for customer A. The technician
at the remote site misconfigured VRF on the router. Which configuration will resolve connectivity
for both sites of customer a?

Router Configuration:

```
ip vrf customer_a
 rd 1:1
 route-target export 1:1
 route-target import 1:1
!
!
interface FastEthernet0.1
 encapsulation dot1Q 2
 ip vrf forwarding customer_a
 ip address 192.168.4.1 255.255.255.
!
router ospf 1
 log-adjacency-changes
 !
router ospf 2 vrf customer_a
 log-adjacency-changes
 network 192.168.4.0 0.0.0.255 area (
 !
end
```

D. ip vrf customer_a
rd 1:2
route-target both 1:1

From the exhibit, we learned:
+ VRF customer_a was exported with Route target (RT) of 1:1 so at the remote site it must be
imported with the same RT 1:1.
+ VRF customer_a was imported with Route target (RT) of 1:1 so at the remote site it must be
exported with the same RT 1:1.
Therefore, at the remote site we must configure the command "route-target both 1:1" (which is
equivalent to two commands "route-target import 1:1" & "route-target export 1:1".

84. What is an advantage of using BFD?

D. It has sub-second failure detection for layer 1 and layer 2 problems.

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.

85. An engineer configured a company's multiple area OSPF head office router and Site A cisco
routers with VRF lite. Each site router is connected to a PE router of an MPLS backbone.
After finishing both site router configurations, none of the LSA 3,4 5, and 7 are installed at Site A
router. Which configuration resolves this issue?

C. Configure capability vrf-lite on both PE routers connected to Head Office and Site A routers
under router ospf 1 vrf abc.

86. What destination addresses does EIGRP use when feasible? (Choose

two).

B. IP address 224.0.0.10
D. MAC address 01:00:5E:00:00:0A

The EIGRP transport mechanism uses a mix of multicast and unicast packets, using reliable delivery when necessary. All transmissions use IP with the protocol type field set to 88. The IP multicast address used is 224.0.0.10. When an EIGRP multicast packet is encapsulated into an Ethernet frame, the destination MAC address is 01-00-5E-00-00-0A.

87. You just discovered that a ping packet sent from one of the devices to another took a different
path in the return than it did on its way to the destination. What behavior caused this?

C. MSS

The TCP Maximum Segment Size (MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IPv4 datagram. This TCP/IPv4 datagram might be fragmented at the IPv4 layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.

88. The OSPF dead interval defaults to how many times the hello interval?

C. Four

The default values are 10 seconds for the hello time, and 40 seconds for the dead time. The usual rule of thumb with OSPF is to keep the dead time value four times the hello interval.

89. You need to resolve a route-selection problem in a redistributed network by increasing the
administrative distance to several networks for a protocol, other than EIGRP or BGP, so that
these routes will not be used. You create access list 5 to identify the relevant

networks, and
access the routing protocol configuration prompt.
Which command will set the administrative distance to these networks to 220 for the selected
protocol?

C. Router(config-router)#distance 220 0.0.0.0 255.255.255.255 5

The correct command is Router(config-router)# distance 220 0.0.0.0 255.255.255.255 5. This command instructs the router to change the AD for any networks specified in the access list 5 to 220.

90. The OSPF database of a router shows LSA types 1, 2, 7, and 3 default router only.
Which type of area is this router connected to?

D. NSSA

The OSPF not-so-stubby area (NSSA) feature is described by RFC 1587 was first introduced in Cisco IOS® Software release 11.2. It is a non-proprietary extension of the existing stub area feature that allows the injection of external routes in a limited fashion into the stub area. Redistribution into an NSSA area creates a special type of link-state advertisement (LSA) known as type 7, which can only exist in an NSSA area. An NSSA autonomous system boundary router (ASBR) generates this LSA and an NSSA area border router (ABR) translates it into a type 5 LSA, which gets propagated into the OSPF domain. There are two flavors in NSSA, just like in stub areas. There are NSSAs that block type 5 and type 4 LSAs, but allow type 3 LSAs, and there are NSSA totally stub areas, which allow only summary default routes and filters everything else.

91. A network administrator notices that the BGP state drops and logs are generated for missing
BGP hello keepalives. What is the potential problem?

D. MTU mismatch

BGP neighbors form; however, at the time of prefix exchange, the BGP state drops and the logs
generate missing BGP hello keepalives or the other peer terminates the

session.
Here are some possible causes:
*The interface MTU on both routers do not match.
*The interface MTU on both routers match, but the Layer 2 domain over which the BGP session
is formed does not match.
*Path MTU discovery determined the incorrect max datasize for the TCP BGP session.
*The BGP Path Maximum Transmission Unit Discovery (PMTUD) could be failing due to PMTUD
ICMP packets blocked (firewall or ACL)

92. Which task do you need to perform first when you configure IP SLA to troubleshoot a network
connectivity issue?

B. Enable the ICMP echo operation

IP Service Level Agreements(SLAs)Internet Control Message Protocol(ICMP) Path Echo operation is used to monitor end-to-end and hop-by-hop response time between a Cisco device and other devices using IP. ICMP Path Echo is useful for determining network availability and for troubleshooting network connectivity issues.

93. Which protocol does VRF-Lite support?

C. EIGRP

You can use most routing protocols (BGP, OSPF, EIGRP, RIP and static routing) between the CE and the PE. External BGP (EBGP) is recommended. VRF-lite does not support IGRP and ISIS.

94. Which two features are provided by EIGRP for IPv6? (Choose two).

C. Partial updates
E. Scaling

EIGRP provides the following features:

* Increased network width--With Routing Information Protocol (RIP), the largest possible width of your network is 15 hops. When EIGRP is enabled,

the largest possible width is 224 hops. Because the EIGRP metric is large enough to support thousands of hops, the only barrier to expanding the network is the transport layer hop counter.
* Fast convergence--The DUAL algorithm allows routing information to converge as quickly as any other routing protocol.
* Partial updates--EIGRP sends incremental updates when the state of a destination changes, instead of sending the entire contents of the routing table. This feature minimizes the bandwidth required for EIGRP packets.
* Neighbor discovery mechanism--This is a simple hello mechanism used to learn about neighboring devices. It is protocol-independent.
* Arbitrary route summarization.
* Scaling--EIGRP scales to large networks.
* Route filtering--EIGRP for IPv6 provides route filtering using the distribute-list prefix-listcommand. Use of the route-map command is not supported for route filtering with a distribute list.

95. What happens when two EIGRP peers have mismatched K values?

C. The two devices fail to from an adjacency.

The K-values must be the same on all of the EIGRP routers in one autonomous system in order to prevent routing problems when different routers use different metric calculations.

96. Refer to the exhibit. The server for the finance department is not reachable consistently on
the 200.30.40.0/24 network and after every second month it gets a new IP address.
Which two actions must be taken to resolve this Issue? (Choose two).

```
ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!
```

B. Configure the server with a static IP address and default gateway.

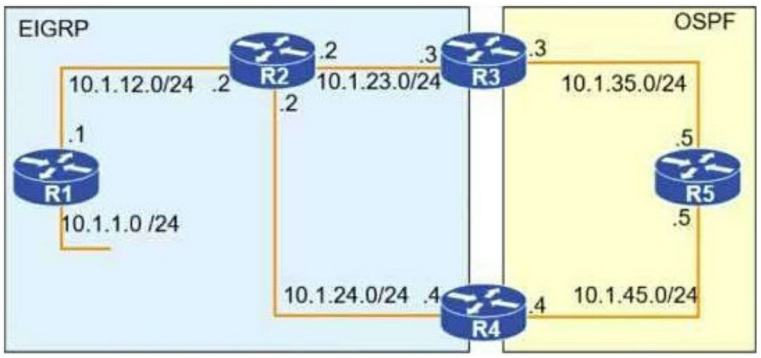
C. Configure the router to exclude a server IP address.

97. 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?

B. set ip default next-hop

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.

98. Refer to the exhibit. To provide reachability to network 10.1.1.0 /24 from R5, the network
administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a path through R5 to reach 10.1.1.0/24 network. Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?



R1
router eigrp 1
redistribute connected
network 10.1.12.1 0.0.0.0
default-metric 1000000 10 255 1 1500

R3
router eigrp 1
network 10.1.23.3 0.0.0.0
!
router ospf 1
redistribute eigrp 1 subnets
network 10.1.35.3 0.0.0.0 area 0

A. Change the administrative distance of the external EIGRP to 90.

When two sources give us information about the exact same network, a decision is made using administrative distance. The lower the better. EIGRP has a lower administrative distance (90) than OSPF (110) so EIGRP will be used.

99. Refer to the Router output. An engineer wanted to set a tag of 30 to route 10.1.80.65/32 but it failed. How is the issue fixed?

R1
ip prefix-list ccnp1 seq 5 permit 10.1.48.9/024 le 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.9/024 le 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.9/024 le 24

route-map ospf-to-eigrp permit 10
 match ip address prefix-list ccnp1
 set tag 30
route-map ospf-to-eigrp permit 20
 match ip address prefix-list ccnp2
 set tag 20
route-map ospf-to-eigrp permit 30
 match ip address prefix-list ccnp3
 set tag 10

B. Modify route-map ospf-to-eigrp permit 10 and match prefix-list ccnp2.

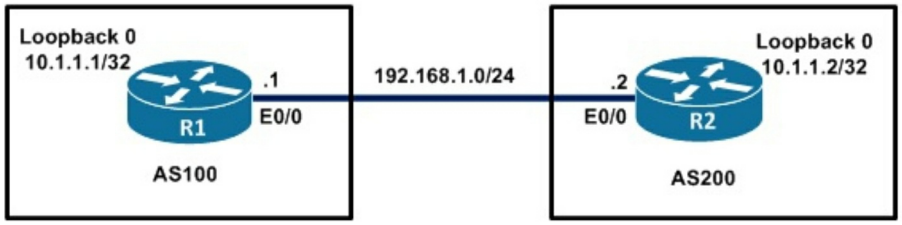
100. An engineer needs dynamic routing between two routers and is unable to establish OSPF

adjacency. The output of the show ip ospf neighbor command shows that the neighbor state is
EXSTART/EXCHANGE. Which action should be taken to resolve this issue?

C. match the MTUs

The problem occurs most frequently when attempting to run OSPF between a Cisco router and another vendor's router. The problem occurs when the maximum transmission unit (MTU) settings for neighboring router interfaces don't match. If the router with the higher MTU sends a packet larger that the MTU set on the neighboring router, the neighboring router ignores the packet.

101. Refer to the exhibit. The neighbor is not coming up. Which two sets of configurations bring the neighbors up? (Choose two).



The R1 and R2 configurations are as follows:

R1
router bgp 100
neighbor 10.1.1.2 remote-as 200

R2
router bgp 200
neighbor 10.1.1.1 remote-as 100

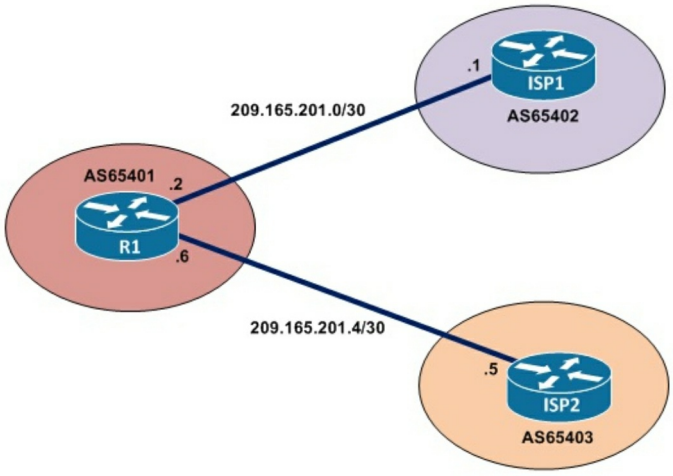
A.
R2
ip route 10.1.1.1 255.255.255.255 192.168.1.1
!

router bgp 200
neighbor 10.1.1.1 disable-connected-check
neighbor 10.1.1.1 disable-source loopback 0

C.
R1
ip route 10.1.1.2 255.255.255.255 192.168.1.2
!
router bgp 100
neighbor 10.1.1.2 disable-connected-check
neighbor 10.1.1.2 disable-source loopback 0

The neighbor disable-connected-check command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

102. Refer to the exhibit. A company with an autonomous has obtained IP system number AS6401 and an address block of 209.165.200.224/27 from ARIN. The company needed more IP addresses and was assigned block 209.165.202.128/27 from ISP2. An engineer with ISP1 reports they are receiving ISP2 routes from AS65401. Which configuration on R1 resolves the issue?



```
R1#
interface GigabitEthernet0/0
  ip address 209.165.201.2 255.255.255.252
!
interface GigabitEthernet0/1
  ip address 209.165.201.6 255.255.255.252
!
router bgp 65401
bgp log-neighbor-changes
redistribute static
neighbor 209.165.201.1 remote-as 65402
neighbor 209.165.201.5 remote-as 65403
!
ip route 209.165.203.224 255.255.255.224 Null0
ip route 209.165.202.128 255.255.255.224 Null0
!
```

A.
access-list 10 deny 209.165.202.128 0.0.0.31
access-list 10 permit any
!
router bgp 65401
neighbor 209.165.201.1 distribute-list 10 out

If you only want to accept routes that are directly connected to the service providers, you must filter the routes that they send to you, as well as the routes that you advertise. This access list and route map permit only locally originated routes; use it to filter outbound routing updates.

103. Refer to the exhibit. All the serial links between R1, R2, and R3 have the same bandwidth. Users on the 192.168.1.0/24 network report slow response times while they access resource on network 192.168.3.0/24. When a traceroute is run on the path, it shows that the packet is getting forwarded via R2 to R3 although the link between R1 and R3 is still up. What must the network administrator to fix the slowness?

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.1.0/24 is directly connected, Ethernet0/0
L   192.168.1.1/32 is directly connected, Ethernet0/0
D   192.168.2.0/24 [90/2297856] via 192.168.12.2, 00:02:14, Serial1/1
S   192.168.3.0/24 [1/0] via 192.168.12.2
  192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.12.0/24 is directly connected, Serial1/1
L   192.168.12.1/32 is directly connected, Serial1/1
  192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.13.0/24 is directly connected, Serial1/0
L   192.168.12.1/32 is directly connected, Serial1/0
D   192.168.23.0/24 [90/2681856] via 192.168.13.3, 00:06:38, Serial1/0
            [90/2681856] via 192.168.12.2., 00:06:38, Serial1/1
D   192.168.24.0/24 [90/2195456] via 192.168.12.2, 00:06:38, Serial1/1
```

C. Remove the static route on R1.

Chapter 2: VPN Technologies

The objectives covered in this chapter:

20% 2.0 VPN Technologies

2.1 Describe MPLS operations (LSR, LDP, label switching, LSP)

2.2 Describe MPLS Layer 3 VPN

2.3 Configure and verify DMVPN (single hub)

2.3.a GRE/mGRE

2.3.b NHRP

2.3.c IPsec

2.3.d Dynamic neighbor

2.3.e Spoke-to-spoke

1. Which protocol is used to automatically generate and exchange labels between multiprotocol label switching (MPLS) routers?
A. LFIB
B. LIB
C. LDP
D. LSR

2. Which structure within an MPLS Layer 3 VPN configuration determines which Virtual Routing and Forwarding (VRF) instance a VPNv4 route will be imported into?
A. Route Distinguisher
B. Route Target
C. Next Hop
D. VPN Label

3. Which protocol is used to dynamically scale a network through use with Dynamic Multipoint VPNs?

A. NHRP
B. NBMA
C. NHC
D. DNS

4. When configuring a DMVPN hub, which command enables the router to support multicast traffic over the tunnel interfaces?
A. ip nhrp multicast tunnel
B. ip nhrp int tun0 multicast
C. ip nhrp traffic-type multicast
D. ip nhrp map multicast dynamic

5. Which list defines the contents of an MPLS label?
A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL.
B. 32-bit label; 3-bit flow label; 1-bit bottom stack; 8-bit hop limit.
C. 20-bit label; 3-bit flow label: 1-bit bottom stack; 8-bit hop limit
D. 32-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL

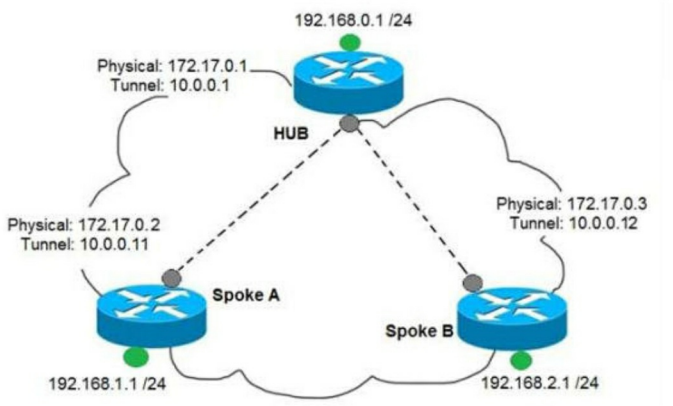
6. What statement about route distinguishers in an MPLS network is true?
A. Route distinguishers make a unique VPNv4 address across the MPLS network.
B. Route distinguishers allow multiple instances of a routing table to coexist within the edge router.
C. Route distinguishers are used for label bindings
D. Route distinguishers define which prefixes are imported and exported on the edge router

7. Refer to the exhibit. What does the imp-null tag represent in the MPLS VPN cloud?

```
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
```

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

8. Refer to the exhibit. Which interface configuration must be configured on the spoke A router to
enable a dynamic DMVPN tunnel with the spoke B router?



A. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel description FastEthernet 0/0
tunnel mode gre multipoint

B. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1

tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1

C. interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.1 172.17.0.1
tunnel mode gre

D. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 1.1.1.10
tunnel mode gre multipoint

9. Which statement about MPLS LDP router ID is true?
A. The force keyword changes the router ID to the specific address causing any impact.
B. The loopback with the highest IP address is selected as the router ID.
C. If not configured, the operational physical interface is chosen as the router ID even if a loopback
is configured.
D. If MPLS LDP router ID must match the IGP router ID.

10. 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

11. Which protocol is used in a DMVPN network to map logical IP address to physical IP addresses?

A. BGP
B. LLDP
C. EIGRP
D. NHRP

12. Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface
on the hub, to support multiple connections from multiple spoke devices?
A. DMVPN
B. GETVPN
C. Cisco Easy VPN
D. FlexVPN

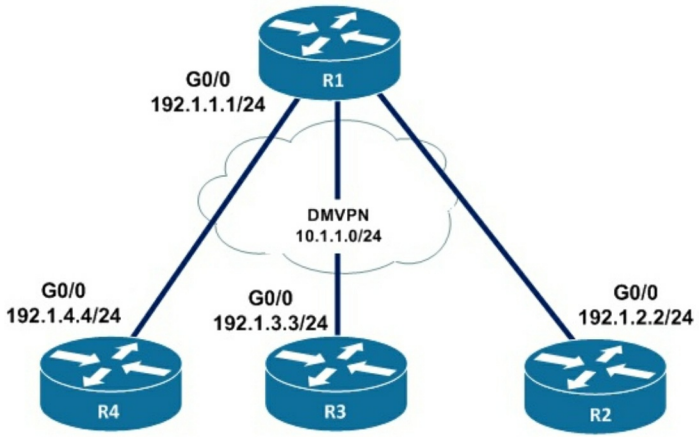
13. Which transport layer protocol is used to form LDP sessions?
A. UDP
B. SCTP
C. TCP
D. RDP

14. 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 regard 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.

15. Refer to the exhibits. Phase-3 tunnels cannot be established between spoke-to-spoke in DMWN.
Which two commands are missing? (Choose two).



R1(config)#interface tunnel 1
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#tunnel source 192.1.1.1
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#ip nhrp network-id 111

R2(config)#interface tunnel 1
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#tunnel source FastEthernet0/0
R2(config-if)#tunnel mode gre multipoint
R2(config-if)#ip nhrp network-id 222
R2(config-if)#ip nhrp nhs 10.1.1.1
R2(config-if)#ip nhrp map 10.1.1.1 192.1.1.1

R3(config)#interface tunnel 1
R3(config-if)#ip address 10.1.1.3 255.255.255.0
R3(config-if)#tunnel source FastEthernet0/0

R4(config)#interface tunnel 1
R4(config-if)#ip address 10.1.1.4 255.255.255.0
R4(config-if)#tunnel source FastEthernet0/0

R3(config-if)#tunnel mode gre multipoint	R4(config-if)#tunnel mode gre multipoint
R3(config-if)#ip nhrp network-id 333	R4(config-if)#ip nhrp network-id 444
R3(config-if)#ip nhrp nhs 10.1.1.1	R4(config-if)#ip nhrp nhs 10.1.1.1
R3(config-if)#ip nhrp map 10.1.1.1 192.1.1.1	R4(config-if)#ip nhrp map 10.1.1.1 192.1.1.1

A. The ip nhrp redirect command is missing on the spoke routers.
B. The ip nhrp shortcut command is missing on the spoke routers.
C. The ip nhrp redirect commands is missing on the hub router.
D. The ip nhrp shortcut commands is missing on the hub router.
E. The ip nhrp command is missing on the hub router.

16. Which protocol is used to determine the NBMA address on the other end of a tunnel when mGRE
is used?
A. NHRP
B. IPsec
C. MP-BGP
D. OSPF

17. 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

18. Identify the true statements the MPLS VPN device types. (Choose three).

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

A. 1, 2, 3
B. 2, 3, 4

C. 1, 3, 4
D. 1, 2, 4

19. 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

20. How are packets forwarded in an MPLS domain?
A. Using the destination IP address of the packet
B. Using the source IP address of the packet
C. Using a number that has been specified in a label
D. Using the MAC address of the frame

21. How long is the default NHRP cache timer?
A. 2 hours
B. 1 hour
C. 30 minutes
D. 15 minutes

22. Which of the following are performed on a Label Switch Router? (Choose two).
A. Performs penultimate hop popping.
B. Assigns labels to unlabeled packets.
C. Reads the labels and forwards the packet based on the labels.
D. Handles traffic between multiple VPNs

23. How are customer routes isolated on PE routers in an MPLS Layer 3 VPN?
A. By using VRF
B. By using VDCs
C. By using MP-BGP
D. By using LDP

24. You are implementing WAN access for an enterprise network while running applications that

require a fully meshed network, which two design standards are appropriate for such an
environment? (Choose two)
A. A centralized DMVPN solution to simplify connectivity for the enterprise
B. A dedicated WAN distribution layer to consolidate connectivity to remote sites
C. A collapsed core and distribution layer to minimize costs
D. Multiple MPLS VPN connections with static routing
E. Multiple MPLS VPN connections with dynamic routing
25. Which protocol is used in a DMVPN network to map physical IP addresses to logical IP
addresses?
A. BGP
B. LLDP
C. EIGRP
D. NHRP

26. Refer to the exhibit. An engineer has configured DMVPN on a spoke router.
What is the WAN IP address of another spoke router within the DMVPN network?

```
Spoke#show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- ---------- ------
1 172.18.16.2 192.168.1.1 UP 01:05:35 S
1 172.18.46.2 192.168.1.4 UP 09:00:25 S
```

A. 172.18.46.2
B. 192.168.1.4
C. 172.18.16.2
D. 192.168.1.1

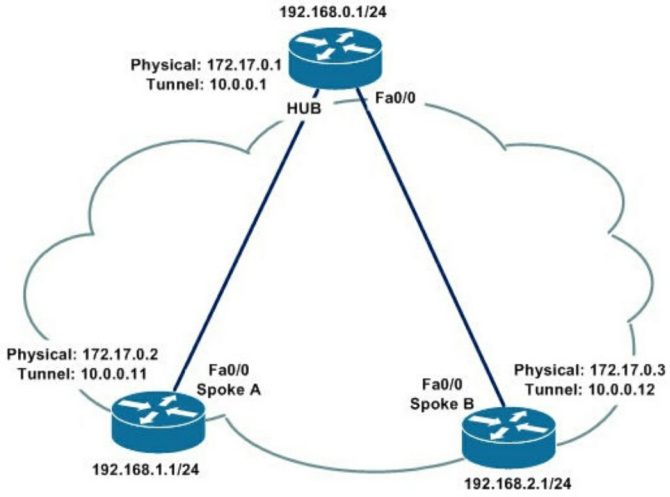
27. Which protocol does MPLS use to support traffic engineering?
A. Tag Distribution Protocol
B. Resource Reservation Protocol
C. Border Gateway Protocol

D. Label Distribution Protocol

28. Which IGPs are supported by the MPLS LDP autoconfiguration feature?
A. ISIS and RIPv2
B. RIPv2 and OSPF
C. OSPF and IS-IS
D. OSPF and EIGRP

29. What does the PE router convert the IPv4 prefix to within an MPLS VPN?
A. 48-bit route combining the IP and PE router-id
B. VPN-IPv4 prefix combined with the 64-bit route distinguisher
C. eBGP path association between the PE and CE sessions
D. prefix that combines the ASN, PE router-id, and IP prefix

30. Refer to the exhibit. Which interface configuration must be configured on the HUB router to
enable MVPN with mGRE mode?



A. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.1.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 172.17.0.1
ip nhrp map 10.0.0.11 172.17.0.2
ip nhrp map 10.0.0.12 172.17.0.3
tunnel mode gre

B. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic

ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint

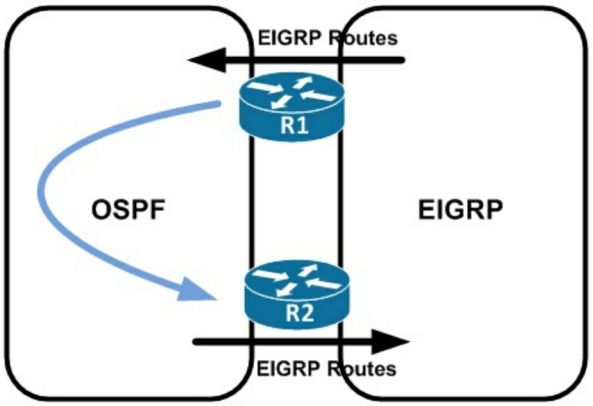
C. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp network-id 1
tunnel source 172.17.0.1
tunnel mode gre multipoint

D. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel destination 172.17.0.2
tunnel mode gre multipoint

31. How are MPLS Layer 3 VPN services deployed?
A. The RD and RT values must match under the VRR
B. The RD and RT values under a VRF must match on the remote PE router
C. The import and export RT values under a VRF must always be the same.
D. The label switch path must be available between the local and remote PE routers.

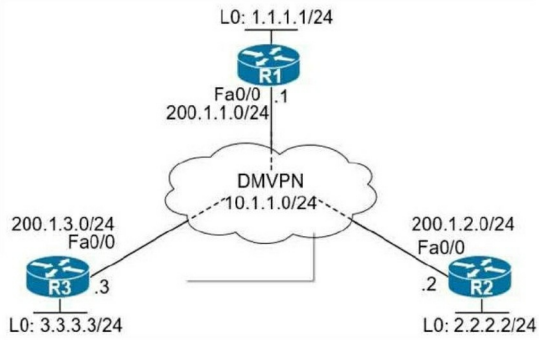
32. What are two functions of LDP? (Choose two).
A. It is defined in RFC 3038 and 3039.
B. It requires MPLS Traffic Engineering.
C. It advertises labels per Forwarding Equivalence Class.
D. It must use Resource Reservation Protocol.
E. It uses Forwarding Equivalence Class

33. Refer to the exhibit. A network administrator configured mutual redistribution on R1 and R2
routers, which caused instability in the network. Which action resolves the issue?



A. Set a tag in the route map when redistributing EIGRP into OSPF on R1. and match the same tag
on R2 to allow when redistributing OSPF into EIGRP.
B. Apply a prefix list of EIGRP network routes in OSPF domain on R1 to propagate back into the
EIGRP routing domain.
C. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag
on R2 to deny when redistributing OSPF into EIGRP.
D. Advertise summary routes of EIGRP to OSPF and deny specific EIGRP routes when redistributing
into OSPF.

34. Refer to the exhibits. When DMVPN is configured, which configuration allows spoke-to-spoke
communication using loopback as tunnel source?



A. Configure crypto isakmp key cisco address 0.0.0.0 on the hub.
B. Configure crypto isakmp key Cisco address 200.1.0.0 255.255.0.0 on the hub.
C. Configure crypto isakmp key cisco address 200.1.0.0 255.255.0.0 on the spokes.
D. Configure crypto isakmp key cisco address 0.0.0.0 on the spokes.

35.
Match the MPLS VPN concepts with its correct definition.
A.
Route Distinguisher = Controls the import/export of customer prefixes
Route Target = Uniquely identifies a customer prefix
Resource Reservation Protocol = Propagates VPN reachability information
Multiprotocol BGP = Distributes labels for traffic engineering

B.
Route Distinguisher = Uniquely identifies a customer prefix
Route Target = Controls the import/export of customer prefixes
Resource Reservation Protocol = Distributes labels for traffic engineering
Multiprotocol BGP = Propagates VPN reachability information

C.
Route Distinguisher = Propagates VPN reachability information
Route Target = Distributes labels for traffic engineering
Resource Reservation Protocol = Controls the import/export of customer prefixes
Multiprotocol BGP = Uniquely identifies a customer prefix

D.
Route Distinguisher = Distributes labels for traffic engineering
Route Target = Propagates VPN reachability information
Resource Reservation Protocol = Uniquely identifies a customer prefix
Multiprotocol BGP = Controls the import/export of customer prefixes

36. Which of the following is the correct definition for the MPLS term "P"?
A. A device that removes and adds the MPLS labeling.
B. A device that forwards traffic based on labels.
C. A path that the label packet takes.
D. A device that is unaware of MPLS labeling.

37. Which of the following is the correct definition for the MPLS term "LSP"?
A. A device that removes and adds the MPLS labeling.
B. A device that forwards traffic based on labels.
C. A path that the label packet takes.
D. A device that is unaware of MPLS labeling.

38. Which of the following is the correct definition for the MPLS term "CE"?
A. A device that removes and adds the MPLS labeling.
B. A device that forwards traffic based on labels.
C. A path that the label packet takes.
D. A device that is unaware of MPLS labeling.

39. Which of the following is the correct definition for the MPLS term "PE"?
A. A device that removes and adds the MPLS labeling.
B. A device that forwards traffic based on labels.
C. A path that the label packet takes.
D. A device that is unaware of MPLS labeling.

40. Which of the following are performed on a Label Switch Router?

(Choose two).
A. Reads the labels and forwards the packet based on the labels.
B. Handles traffic between multiple VPNs
C. Performs penultimate hop popping.
D. Assigns labels to unlabeled packets.

Chapter 2: Answers

1. Which protocol is used to automatically generate and exchange labels between multiprotocol label switching (MPLS) routers?

C. LDP

Label Distribution Protocol (LDP) allows an MPLS router to generate labels for its prefixes, which are advertised to MPLS neighbors. LDP first establishes a neighbor adjacency with another LDP-capable device before exchanging labels. These labels allow MPLS-enabled routers to determine how data is forwarded in the network, rather than basing those decisions on IP addressing information.

2. Which structure within an MPLS Layer 3 VPN configuration determines which Virtual Routing and Forwarding (VRF) instance a VPNv4 route will be imported into?

B. Route Target

A Route Target (RT) is an 8-byte value added to a prefix within MPLS Layer 3 VPNs. The typical format is the autonomous system number followed by the customer site number, separated by a colon (e.g. 65100:1). The RT is attached to a prefix, creating a VPNv4 route that is sent over MP-BGP to a peer. The RT informs the receiving peer about which VRF the VPNv4 route should be imported into.

3. Which protocol is used to dynamically scale a network through use with Dynamic Multipoint VPNs?

A. NHRP

The next-hop resolution protocol (NHRP) is functionally similar to how DNS works. This is an ARP-like protocol that allows DMVPN spokes to directly communicate with one another. This is a client-server model where the DMVPN hub maintains an NHRP database for each spoke, allowing for the spokes to build direct tunnels between themselves.

4. When configuring a DMVPN hub, which command enables the router to support multicast traffic over the tunnel interfaces?

D. ip nhrp map multicast dynamic

The command “ip nhrp map multicast dynamic” allows the next-hop resolution protocol (NHRP) to automatically add routers to the multicast NHRP mappings. This is used when spoke routers need to initiate mGRE and IPsec tunnels to register their NHRP mappings.

5. Which list defines the contents of an MPLS label?

A. 20-bit label; 3-bit traffic class; 1-bit bottom stack; 8-bit TTL.

MPLS uses a 32-bit label field that contains the information that follows:
+ 20-bit label (a number)
+ 3-bit class of service (or experimental field, typically used to carry IP precedence value)
+ 1-bit bottom-of-stack indicator (indicates whether this is the last label before the IP header)
+ 8-bit TTL (equal to the TTL in the IP header)

6. What statement about route distinguishers in an MPLS network is true?

A. Route distinguishers make a unique VPNv4 address across the MPLS network.

MPLS-based VPNs employ BGP to communicate between PEs to facilitate customer routes. This is made possible through extensions to BGP that carry addresses other than IPv4 addresses. A notable extension is called the route distinguisher (RD). The purpose of the route distinguisher (RD) is to make the prefix value unique across the backbone.

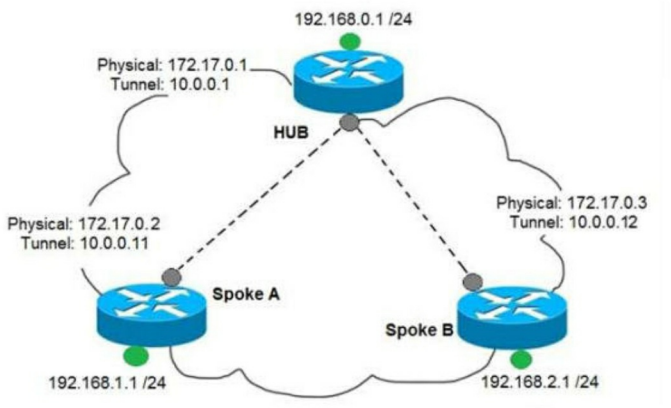
7. Refer to the exhibit. What does the imp-null tag represent in the MPLS VPN cloud?

```
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
```

D. Pop the label

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”

8. Refer to the exhibit. Which interface configuration must be configured on the spoke A router to
enable a dynamic DMVPN tunnel with the spoke B router?



B. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet 0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1

The command “ip nhrp map multicast dynamic” should be only used on Hub router, not spoke. If
we are running dynamic routing protocols based on multicast (like RIP, OSPF, EIGRP …) we
have to add the command “ip nhrp map multicast dynamic” in Hub to replicate all multicast traffic
to all dynamic entries in the NHRP table (multicast will be proceeded as unicast traffic) -> Answer

A is not correct. Also another error in this answer is the “tunnel source” IP address. It should be
the NBMA address of the Spoke interface: 172.17.0.2.
Answer C is not correct as the “tunnel source 1.1.1.10”, “ip nhrp map 10.0.0.11 172.17.0.2” and
“tunnel mode gre” are wrong.
Answer D is not correct as there is no “ip nhrp map multicast static” command, only the “ip nhrp
map multicast <static-IP>” command is available. The “tunnel source 10.0.0.1” is not correct
either.
Answer B is correct. The ” tunnel source FastEthernet0/0″ is equivalent to “tunnel source
172.17.0.2”, which is the NBMA address of Spoke A.

9. Which statement about MPLS LDP router ID is true?

B. The loopback with the highest IP address is selected as the router ID.

The router determines the LDP router ID as follows:
If the mpls ldp router-id command is not executed,
1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

10. Which two methods use IPsec to provide secure connectivity from the branch office to the
headquarters office? (Choose two).

A. DMVPN
C. Virtual Tunnel Interface (VTI)

IP security (IPsec) virtual tunnel interfaces (VTIs) provide a routable interface type for terminating
IPsec tunnels and an easy way to define protection between sites to form an overlay network.

IPsec VTIs simplify configuration of IPsec for protection of remote links, support multicast, and
simplify network management and load balancing.

11. Which protocol is used in a DMVPN network to map logical IP address to physical IP addresses?

D. NHRP

Next Hop Resolution Protocol (NHRP), defined in RFC 2332, is a Layer 2 address resolution
protocol and cache, like Address Resolution Protocol (ARP). NHRP is used by a branch router
connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of
the “NBMA next hop”; in this case, the headend router or the destination IP address of another
branch router.
NHRP is used to map tunnel IP addresses to “physical” or “real” IP addresses, used by endpoint
routers. It resolves private addresses (those behind mGRE and optionally IPSEC) to a public
address. NHRP is layer 2 resolution protocol and cache, much like Address Resolution Protocol
(ARP) or Reverse ARP (Frame Relay).

12. Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface
on the hub, to support multiple connections from multiple spoke devices?

A. DMVPN

An mGRE tunnel inherits the concept of a classic GRE tunnel but an mGRE tunnel does not
require a unique tunnel interface for each connection between Hub and spoke like traditional
GRE. One mGRE can handle multiple GRE tunnels at the other ends. Unlike classic GRE
tunnels, the tunnel destination for a mGRE tunnel does not have to be

configured; and all tunnels
on Spokes connecting to mGRE interface of the Hub can use the same subnet.

13. Which transport layer protocol is used to form LDP sessions?

C. TCP

LDP uses TCP as a reliable transport for sessions. When multiple LDP sessions are required
between two LSRs, there is one TCP session for each LDP session.

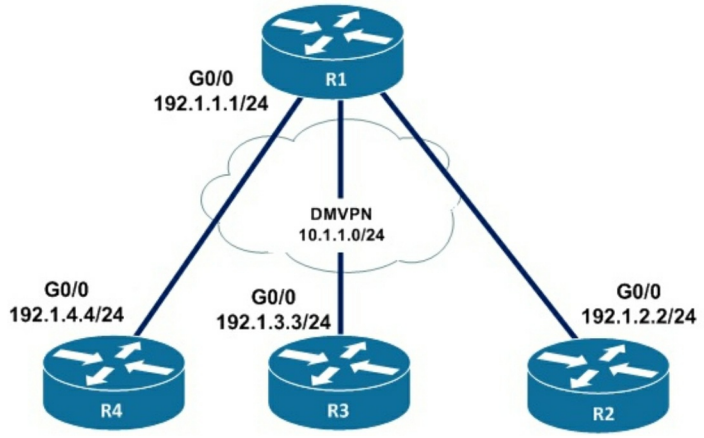
14. Refer to the following output:

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 regard to the NHRP information?

A. It was obtained directly from the next-hop server.

15. Refer to the exhibits. Phase-3 tunnels cannot be established between spoke-to-spoke in DMWN.
Which two commands are missing? (Choose two).



R1(config)#interface tunnel 1
R1(config-if)#ip address 10.1.1.1 255.255.255.0
R1(config-if)#tunnel source 192.1.1.1
R1(config-if)#tunnel mode gre multipoint
R1(config-if)#ip nhrp network-id

R2(config)#interface tunnel 1
R2(config-if)#ip address 10.1.1.2 255.255.255.0
R2(config-if)#tunnel source FastEthernet0/0
R2(config-if)#tunnel mode gre multipoint
R2(config-if)#ip nhrp network-id

111	222 R2(config-if)#ip nhrp nhs 10.1.1.1 R2(config-if)#ip nhrp map 10.1.1.1 192.1.1.1
R3(config)#interface tunnel 1 R3(config-if)#ip address 10.1.1.3 255.255.255.0 R3(config-if)#tunnel source FastEthernet0/0 R3(config-if)#tunnel mode gre multipoint R3(config-if)#ip nhrp network-id 333 R3(config-if)#ip nhrp nhs 10.1.1.1 R3(config-if)#ip nhrp map 10.1.1.1 192.1.1.1	R4(config)#interface tunnel 1 R4(config-if)#ip address 10.1.1.4 255.255.255.0 R4(config-if)#tunnel source FastEthernet0/0 R4(config-if)#tunnel mode gre multipoint R4(config-if)#ip nhrp network-id 444 R4(config-if)#ip nhrp nhs 10.1.1.1 R4(config-if)#ip nhrp map 10.1.1.1 192.1.1.1

B. The ip nhrp shortcut command is missing on the spoke routers.

C. The ip nhrp redirect commands is missing on the hub router.

DMVPN Phase III is same as Phase 2 but removes some restrictions and complexities of Phase
2. Also allows greater variety of DMVPN network designs we use:
+ ip nhrp redirect in hub: tells the initiator spoke to look for a better path to the destination spoke
than through the Hub. Upon receiving the NHRP redirect message the spokes communicate with
each other over the hub and they have their NHRP replies for the NHRP Resolution Requests
that they sent out.
+ ip nhrp shortcut in spokes: overwrite the CEF table on the spoke. It basically overrides the nexthop value for a remote spoke network from the default initial hub tunnel IP address to the NHRP
resolved remote spoke tunnel IP address)

16. Which protocol is used to determine the NBMA address on the other end

of a tunnel when mGRE
is used?

A. NHRP

NHRP is used to map tunnel IP addresses to “physical” or “real” IP addresses (NBMA
addresses), used by endpoint routers. It resolves private addresses (those behind mGRE and
optionally IPsec) to a public address.

17. Which label operations are performed by a label edge router?

D. PUSH and POP

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.

18. Identify the true statements the MPLS VPN device types. (Choose three).

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

C. 1, 3, 4

1, 3, and 4 are correct. #2 is incorrect because a CE device is a device in the enterprise network that connects to other customer devices.

19. 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?

B. RD

Route Distinguishers are used to create VPN-IPv4 addresses, as specified in [RFC4364]. The RDs are structured so that every service provider can administer its own "numbering space" (i.e., can make its own assignments of RDs), without conflicting with the RD assignments made by any other service provider. An RD consists of three fields: a type field, an administrator field, and an assigned number field.

20. How are packets forwarded in an MPLS domain?

C. Using a number that has been specified in a label.

MPLS works with layer 3 routing protocols that integrate network layer routing with label switching. An MPLS FEC contains packets that are forwarded in the same manner by a given label-switching router (LSR).

21. How long is the default NHRP cache timer?

A. 2 hours

NBMA addresses that are advertised as valid means how long the Cisco IOS XE software tells other routers to keep the address mappings it is providing in NHRP responses. The default length of time is 7200 seconds (2 hours). This configuration controls how long a spoke-to-spoke shortcut path will stay up after it is no longer used or how often the spoke-to-spoke short-cut path mapping entry will be refreshed if it is still being used.

22. Which of the following are performed on a Label Switch Router? (Choose two).

B. Assigns labels to unlabeled packets.
D. Handles traffic between multiple VPNs

23. How are customer routes isolated on PE routers in an MPLS Layer 3 VPN?

A. By using VRF

Customer isolation is achieved on a PE router by using virtual routing tables or instances called virtual routing and forwarding tables/instances (VRFs). It is similar to maintaining multiple dedicated routers for customers connecting

into the provider network.

24. You are implementing WAN access for an enterprise network while running applications that
require a fully meshed network, which two design standards are appropriate for such an
environment? (Choose two)

A. A centralized DMVPN solution to simplify connectivity for the enterprise

B. A dedicated WAN distribution layer to consolidate connectivity to remote sites

With DMVPN phase 2 and 3, spokes can speak with each other directly like they are directly
connected in a meshed network. This simplifies the connectivity for the enterprise ->
Answer A is correct. Another way to run applications that require a fully meshed network is through a WAN distribution layer that is connected to all remote sites. Therefore these sites can communicate with each other via this WAN distribution layer.

25. Which protocol is used in a DMVPN network to map physical IP addresses to logical IP
addresses?

D. NHRP

The Next Hop Resolution Protocol (NHRP) is used to map tunnel IP addresses to “physical” or “real” IP addresses. It resolves private addresses to a public address. NHRP is used by a branch router connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of the “NBMA next hop”.

26. Refer to the exhibit. An engineer has configured DMVPN on a spoke router.
What is the WAN IP address of another spoke router within the DMVPN network?

```
Spoke#show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- ---------------- --------------- ----- ---------- ------
1 172.18.16.2 192.168.1.1 UP 01:05:35 S
1 172.18.46.2 192.168.1.4 UP 09:00:25 S
```

A. 172.18.46.2

27. Which protocol does MPLS use to support traffic engineering?

B. Resource Reservation Protocol

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone by using RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth.

28. Which IGPs are supported by the MPLS LDP autoconfiguration feature?

C. OSPF and IS-IS

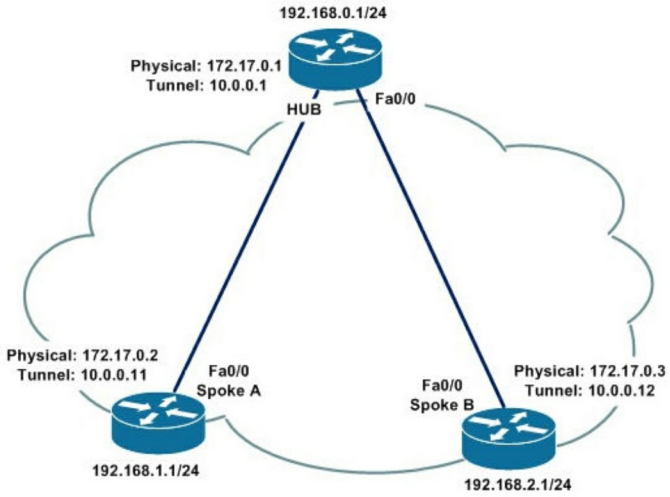
The MPLS LDP Autoconfiguration feature enables you to globally enable LDP on every

29. What does the PE router convert the IPv4 prefix to within an MPLS VPN?

D. prefix that combines the ASN, PE router-id, and IP prefix

When a PE router receives an IPv4 route from a device within a VPN, it converts it into a VPN-IPv4 route by adding the route distinguisher prefix to the route. The VPN-IPv4 addresses are used only for routes exchanged between PE routers.

30. Refer to the exhibit. Which interface configuration must be configured on the HUB router to
enable MVPN with mGRE mode?



B. interface Tunnel0
description mGRE - DMVPN Tunnel
ip address 10.0.0.1 255.255.255.0
ip nhrp map multicast dynamic
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint

Before a multipoint GRE (mGRE) and IPsec tunnel can be established, you must define an Internet Key Exchange (IKE) policy by using the crypto isakmp policy command.

31. How are MPLS Layer 3 VPN services deployed?

D. The label switch path must be available between the local and remote PE routers.

A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network

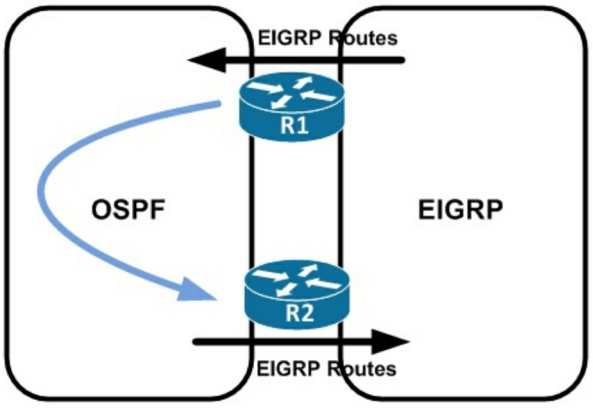
(VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. This module provides the conceptual and configuration information for MPLS Layer 3 VPNs on Cisco IOS XR software.

32. What are two functions of LDP? (Choose two).

C. It advertises labels per Forwarding Equivalence Class.
E. It uses Forwarding Equivalence Class

Label Switched Path (LSP)—A route through an MPLS network, defined by a signaling protocol such as LDP or the Border Gateway Protocol (BGP). The path is set up based on criteria in the forwarding equivalence class (FEC). Forwarding Equivalence Class (FEC)—A set of packets with similar characteristics that might be bound to the same MPLS label. An FEC tends to correspond to a label switched path (LSP); however, an LSP might be used for multiple FECs.

33. Refer to the exhibit. A network administrator configured mutual redistribution on R1 and R2
routers, which caused instability in the network. Which action resolves the issue?



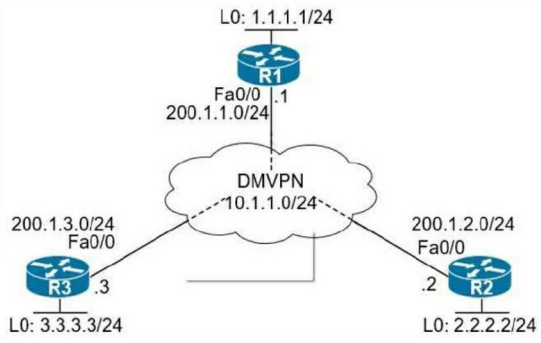
C. Set a tag in the route map when redistributing EIGRP into OSPF on R1, and match the same tag on R2 to deny when redistributing OSPF into EIGRP.

When doing mutual redistribution at multiple points (between OSPF and EIGRP on R1 & R2), we
may create routing loops so we should use route-map to prevent redistributed routes from
redistributing again into the original domain. In the below example, the route-map "SET-TAG" is used to prevent any routes that have been redistributed into EIGRP from redistributed again into OSPF domain by tagging these routes with tag 1:

R3
route-map SET-TAG permit 10
set tag 1
These routes are prevented from redistributed again by route-map FILTER_TAG by denying any routes with the tag1 set:

R4
Route-map FILTER-TAG deny 10
match tag 1

34. Refer to the exhibits. When DMVPN is configured, which configuration allows spoke-to-spoke
communication using loopback as tunnel source?



A. Configure crypto isakmp key cisco address 0.0.0.0 on the hub.

35.
Match the MPLS VPN concepts with its correct definition.

B.
Route Distinguisher = Uniquely identifies a customer prefix
Route Target = Controls the import/export of customer prefixes
Resource Reservation Protocol = Distributes labels for traffic engineering
Multiprotocol BGP = Propagates VPN reachability information

36. Which of the following is the correct definition for the MPLS term "P"?

B. A device that forwards traffic based on labels.

In Multiprotocol Label Switching (MPLS), a P Router or Provider Router is a Label Switch Router (LSR) that functions as a transit router of the core network.

37. Which of the following is the correct definition for the MPLS term "LSP"?

C. A path that the label packet takes.

A label-switched path (LSP) is a path through an MPLS network, set up by the NMS or by a signaling protocol such as LDP, RSVP-TE, BGP (or the now deprecated CR-LDP).

38. Which of the following is the correct definition for the MPLS term "CE"?

D. A device that is unaware of MPLS labeling.

A CE router (customer edge router) is a router located on the customer premises that provides an Ethernet interface between the customer's LAN and the provider's core network.

39. Which of the following is the correct definition for the MPLS term "PE"?

A. A device that removes and adds the MPLS labeling.

The PE (Provider Edge) router or network element is the interface between the customer-facing network and the MPLS core, and the point where customer data is given an MPLS label and/or the label is removed.

40. Which of the following are performed on a Label Switch Router? (Choose two).

A. Reads the labels and forwards the packet based on the labels.
C. Performs penultimate hop popping.

A label switching router is a router or switch that supports the forwarding of MPLS-encapsulated packets based solely on the incoming interface and the information in the shim header.

Chapter 3: Infrastructure Security

The objectives covered in this chapter:

20% 3.0 Infrastructure Security

3.1 Troubleshoot device security using IOS AAA (TACACS+, RADIUS, local database)

3.2 Troubleshoot router security features

3.2.a IPv4 access control lists (standard, extended, time-based)

3.2.b IPv6 traffic filter

3.2.c Unicast reverse path forwarding (uRPF)

3.3 Troubleshoot control plane policing (CoPP) (Telnet, SSH, HTTP(S), SNMP, EIGRP, OSPF, BGP)

3.4 Describe IPv6 First Hop security features (RA guard, DHCP guard, binding table, ND inspection/snooping, source guard)

1. Which command will require the VTY line connections to authenticate a user with the local database of the router?
A. R1(config-line)# local authentication
B. R1(config-line)# vty local
C. R1(config-line)# login local
D. R1(config-line)# aaa login local

2. Which command allows us to configure a router to use a loopback address as the source for TACACS+ communication?
A. R1(config)# tacacs+ source Loopback 0
B. R1(config)# tacacs session source Loopback 0

C. R1(config)# ip tacacs source-interface Loopback 0
D. R1(config-tacacs)# source-interface Loopback 0

3. Which standard port is used by RADIUS for authentication purposes?
A. 1812
B. 1813
C. 1642
D. 1643

4. Which Cisco IOS command will display the hours during which a time-based ACL named AFTER-WORK is configured to be active?
A. R1# show acl periodic AFTER-WORK
B. R1# show periodic AFTER-WORK
C. R1# show active AFTER-WORK
D. R1# show time-range AFTER-WORK

5. Which command is correct when applying an IPv6 ACL named FILTER to an interface in the inbound direction?
A. R1(config-if)# ipv6 traffic-filter FILTER in
B. R1(config-if)# ipv6 access-list FILTER in
C. R1(config-if)# ipv6 access-group FILTER in
D. R1(config-if)# ipv6 FILTER access-list in

6. Which Unicast Reverse Path Forwarding (uRPF) mode verifies that a packet source IP arrives on the same interface the router would use to reach the IP address?
A. Verbose Mode
B. Loose Mode
C. Strict Mode
D. Asymmetric Mode

7. Which structure within a Control Plane Policing (CoPP) configuration is used to define the action which should be taken against policed traffic?
A. Policy Map
B. ACL
C. Class Map
D. Service Policy

8. The IPv6 RA Guard feature filters out which type of router advertisements

in an IPv6 network?
A. Broadcast
B. Multicast
C. Unicast
D. Frame Relay

9. Where can we apply an IPv6 DHCPv6 guard policy?
A. Only on interface
B. Only a VLAN
C. On either an interface or a VLAN
D. Only globally

10. What is used by IPv6 nodes to discover the presence and link-layer addresses of other nodes which reside on the same link?
A. STP
B. LDP
C. NDP
D. ARP

11. Which feature allows us to filter inbound traffic on L2 switch ports that are not found in the IPv6 binding table?
A. IPv6 RA Guard
B. DHCPv6 Guard
C. IPv6 ND Inspection
D. IPv6 Source Guard

12. Which command will allow an administrator to connect to a Cisco device's VTY line only over port 22?
A. R1(config-line)# transport input telnet
B. R1(config-line)# transport input 22
C. R1(config-line)# transport input all
D. R1(config-line)# transport input ssh

13. When switching a router configuration from SSHv1 to SSHv2, which command is necessary in order to provide secure access?
A. R1(config)# crypto key generate rsa
B. R1(config)# generate rsa key
C. R1(config)# secure-access crypto key
D. R1(config)# input password rsa

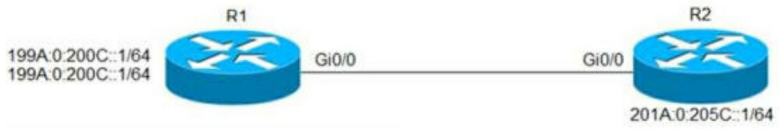
14. Which version of SNMP added the “inform” command in order to provide positive acknowledgement of message receipt?
A. SNMPv1
B. SNMPv1.5
C. SNMPv2c
D. SNMPv3

15. When Cisco IOS command configures a remote user to receive traps using communication configured for authentication without privacy?
A. R1(config)# snmp-server host 10.1.1.50 v3 priv
B. R1(config)# snmp-server host 10.1.1.50 v3 auth
C. R1(config)# snmp-server host 10.1.1.50 v3 noauth
D. R1(config)# snmp-server host 10.1.1.50 v3 authnopriv

16. A device within our network that has a statically configured IP address has begun having communication issues. From a Cisco router acting as a DHCP server, how can we verify an issue with the IP address?
A. R1# show ip dhcp conflict
B. R1# show dhcp conflict
C. R1# show dhcp binding
D. R1# show excluded-address

17. Under what condition would the DHCP Relay Agent feature be required in order to make sure our network hosts are able to obtain an IP address through DHCP?
A. The host and DHCP server are in the same broadcast domain.
B. The hosts and DHCP server are in different broadcast domains.
C. The hosts and DHCP server are directly connected.
D. The hosts and DHCP server are not directly connected.

18. Refer to the exhibit. Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?



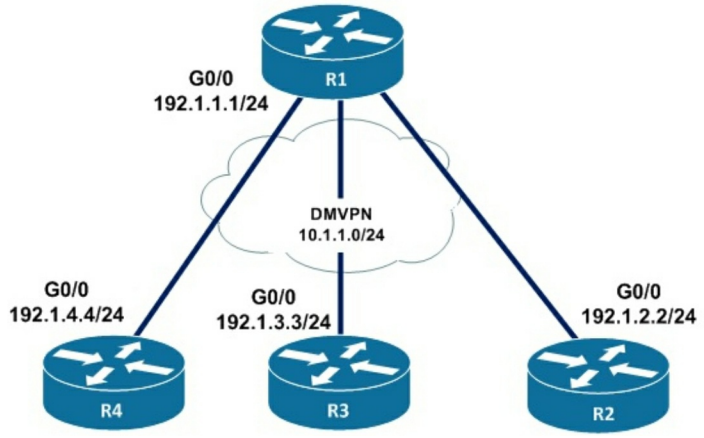
A. ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64 eq telnet
!
int Gi0/0
ipv6 traffic-filter Deny_Telnet in
!

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
!

19. 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).



R2 R2(config)#crypto isakmp policy 10 R2(config-isakmp)#hash md5 R2(config-isakmp)#authentication share R2(config-isakmp)#group 2 R2(config-isakmp)#encryption 3des R2(config)#crypto isakmp key cisco address 10.1.1.1 R2(config)#crypto ipsec transform set TSET esp-des esp-hmac R2(cfg-crypto-trans)#mode transport R2(config)#crypto ipsec profile TST R2 (ipsec-profile) # set transform-set TSET	R3 R3(config)#crypto isakmp policy 10 R3(config-isakmp)#hash md5 R3(config-isakmp)#authentication pre-share R3(config-isakmp)#group 2 R3(config-isakmp)#encryption 3des R3(config)#crypto isakmp key cisco address 10.1.1.1 R3(config)#crypto ipsec transform-set TSET esp-des esp-md5-hmac R3(cfg-crypto-trans)#mode tunnel R3(config)#crypto ipsec profile TST R3 (ipsec-profile) + set transform-set TSET

R2(config)#interface tunnel 123 R2(config-if)#tunnel protection ipsec profile TST	R3(config)#interface tunnel 123 R3(config-if)#tunnel protection ipsec profile TST

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

20. Which security feature can protect DMVPN tunnels?
A. IPsec
B. TACACS+
C. RTBH
D. RADIUS

21. Refer to the exhibit. An engineer is trying to block the route to 192.168.2.2 from the routing table
by using the configuration that is shown. The route us still present in the routing table as an OSPF route. Which action blocks the route?

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#|
```

A. Add this statement to the route map route-map RM-OSPF-DL deny 20
B. Use a prefix list instead of an access list in the route map.
C. Change sequence 10 in the route-map command from permit to deny.
D. Use an extended access list instead of a standard access list.

22. 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.

23. Which option is the best for protecting CPU utilization on a device?
A. fragmentation
B. COPP
C. ICMP redirects
D. ICMP unreachable messages

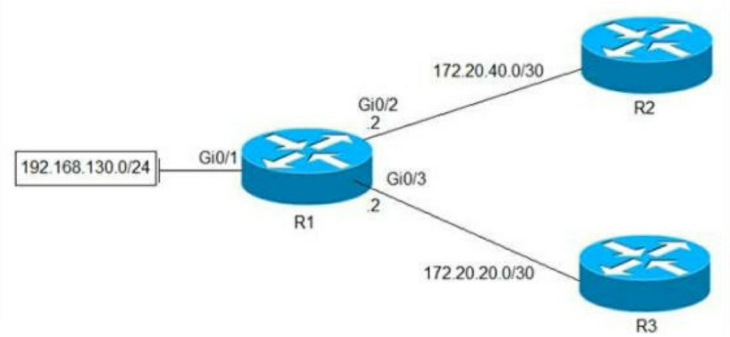
24. Refer to the router output. Network operations cannot read or write an configuration on the device with this configuration from the operation subnet. Which two configuration fix the issue? (Choose two).

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

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 SNMP rw permission in addition to version 1.
D. Configure SNMP rw permission in addition to version 1.
E. Configure SNMP rw permission in addition to community ciscotest 1.

25. 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

26. 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

27. Which two protocols can cause TCP starvation? (Choose two)
A. TFTP
B. SNMP
C. SMTP
D. HTTPS
E. FTP

28. Refer to the exhibit. Why is user authentication being rejected?

```
TAC+: TCP/IP open to 171.68.118.101/49 failed -
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (256660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

A. The TACACS+ server expects "user" but the NT client sends "domain\user"
B. The TACACS+ server refuses the user because the user is set up for

CHAP
C. The TACACS+ server is down and the user is in the local database
D. The TACACS+ server is down and the user is not in the local database

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

```
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#
```

A. crypto key generate rsa
B. ip ssh enable
C. no ip ssh disable
D. ip ssh version 2
30. Refer to the exhibit. 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?

```
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#
```

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

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

32. Refer to the exhibit. 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?

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

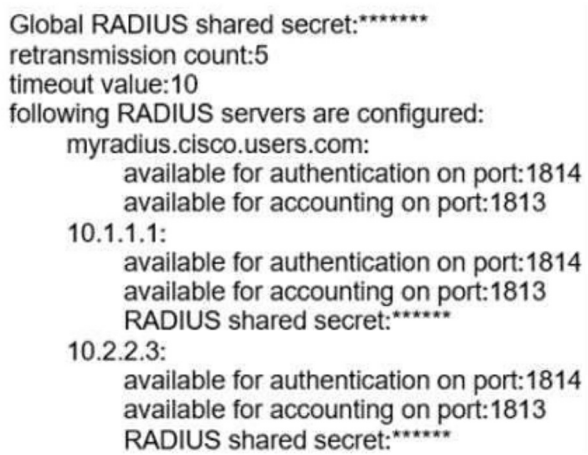
C. ip prefix-list 102 seq 5 permit 0.0.0.0/32 le 32
D. route-map FILTER-IN permit 20

33. Refer to the exhibit. 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?

```
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. 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

34. Refer to the exhibit. 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.

35. 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.

36. Refer the exhibit. BGP is flapping after the COPP policy is applied. What are the two solutions to fix the issue? (Choose two).

```
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
```

A. Configure a three-color policer instead of two-color policer under Class COPP-CRIT1CAL-
7600
B. Configure IP CEF for CoPP policy and BGP to work
C. Configure a higher value for CIR under the default class to allow more packets during peak
traffic
D. Configure a higher value for CIR under the Class COPP-CRIT1CAL-7600
E. Configure BGP in the COPP-CRIT1CAL-7600 ACL

37. Refer the exhibit. Which action resolves intermittent connectivity observed with the SNMP trap
packets?

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

        Service-policy output: R3_CoPP


        Class-map: mgmt (match-all)
            361 packets, 73858 bytes
            4 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, exceeded 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 acceess-list 10
Extended IP access list 120
    10 permit udp any any eq snmptrap (361 matches)
```

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

38. 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 0.0.0.255 172.16.10.0 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 0.0.0.255 172.16.10.0 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 0.0.0.255 172.16.10.0 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 0.0.0.255 172.16.10.0 0.0.0.255 eq telnet
time-range changewindow
!
time-range changewindow

39. Refer to the exhibit. The ACL is placed on the inbound Gigabit 0/1 interface of the router. Host 192.168.10.10 cannot SSH to host 192.168.100.10 even though the flow is permitted. Which action resolves the issue without opening full access to this router?

```
ip access-list extended FILTER
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 22
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 23
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 80
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 443
permit tcp host 192.168.10.10 host 192.168.100.10 eq ssh
permit ip any any
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group FILTER in
!
```

A. Move the SSH entry to the beginning of the ACL
B. Temporarily move the permit ip any any line to the beginning of the ACL

to see if the flow
works
C. Temporarily remove the ACL from the interface to see if the flow works
D. Run the show access-list FILTER command to view if the SSH entry has any hit statistic
associated with it

40. Refer to the exhibit. Which option represents the minimal configuration that allows inbound
traffic from the 172.16.1.0/24 network to successfully enter router R, while also limiting spoofed 10.0.0.0/8 hosts that could enter router R?


```
R(config)#ip route 10.0.0.0 255.0.0.0 FastEthernet0/1
R(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet 0/0
```

A.
R(config)#ip cef
R(config)#interface fa0/0
R(config-if)#ip verify unicast source reachable-via rx allow-default

B.
R(config)#ip cef
R(config)#interface fa0/0
R(config-if)#ip verify unicast source reachable-via rx

C.
R(config)#no ip cef
R(config)#interface fa0/0
R(config-if)#ip verify unicast source reachable-via rx

D.
R(config)#interface fa0/0
R(config-if)#ip verify unicast source reachable-via any

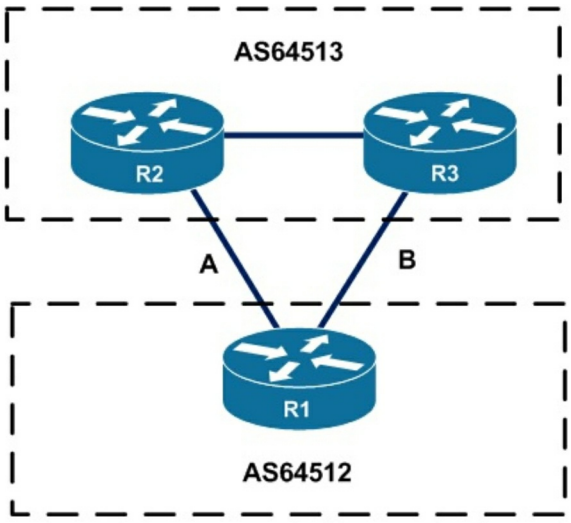
41. Which traffic does the following configuration allow?

ipv6 access-list cisco
permit ipv6 host 2001:DB8:0:4::32 any eq ssh
line vty 0 4
ipv6 access-class cisco in

A. all traffic to vty 0 4 from source 2001:DB8:0:4::32
B. only ssh traffic to vty 0 4 from source all
C. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32
D. all traffic to vty 0 4 from source all

42. Which access list entry checks for an ACK within a packet header?
A. access-list 49 permit ip any any eq 21 tcp-ack
B. access-list 49 permit tcp any any eq 21 tcp-ack
C. access-list 149 permit tcp any any eq 21 established
D. access-list 49 permit tcp any any eq 21 established

43. Refer to the exhibit. A network engineer for AS64512 must remove the inbound and outbound
traffic from link A during maintenance without closing the BGP session so that there is a backup link over link A toward the ASN. Which BGP configuration on R1 accomplishes this goal?



A.
route-map link-a-in permit 10
set weight 200
route-map link-a-out permit 10
set as-path prepend 64512
route-map link-b-in permit 10
set weight 100
route-map link-b-out permit 10

B.
route-map link-a-in permit 10
set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
set weight 100
route-map link-b-out permit 10
set as-path prepend 64512

C.
route-map link-a-in permit 10
set local-preference 200
route-map link-a-out permit 10
route-map link-b-in permit 10
route-map link-b-out permit 10
set as-path prepend 64512

D.
route-map link-a-in permit 10
route-map link-a-out permit 10
set as-path prepend 64512
route-map link-b-in permit 10
set local-preference 200
route-map link-b-out permit 10

44. Refer to the exhibit. R1 is being monitored using SNMP and monitoring devices are getting only
partial information. What action should be taken to resolve this issue?

```
R1#show policy-map control-plane
 Control Plane

        Service-policy output:  CoPP

          Class-map: SNMP-Out (match-all)
            124 packets, 3693 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name SNMP
            police:
                cir 8000 bps, bc 1500 bytes
              conformed 0 packets, 0 bytes; actions:
                transmit
              exceeded 0 packets, 0 bytes; actions:
                drop
              conformed 0000 bps, exceeded 0000 bps

          Class-map: class-default (match-any)
            10 packets, 1003 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
R1#show ip access-list SNMP
Extended IP access list SNMP
        10 permit udp any eq snmp any
```

A. Modify the CoPP policy to increase the configured exceeded limit for SNMP.
B. Modify the access list to include snmptrap.
C. Modify the CoPP policy to increase the configured CIR limit for SNMP.

D. Modify the access list to add a second line to allow udp any any eq snmp.

45. Refer to the exhibit. A client is concerned that passwords are visible when running this show
archive log config all. Which router configuration is needed to resolve this issue?

```
MASS-RTR#show running config
!
hostname MASS-RTR
!
aaa new-model
!
aaa autentication login default local
aaa autentication exec default local
aaa autentication commands 15 default local
!
username admin privilege 15 password 7 023624481115F3348
username cisco privilege 15 password 7 0607072C49A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
 idx   sess    user@lir Logged command
   1      1    console@ |interface GigabitEthernet0/0
   2      1    console@ | no shutdown
   3      1    console@ | ip address dhcp
   4      2    admin@\ |username cisco privilege 15 password cisco
   5      2    admin@\ |!config: USER TABLE MODIFIED
```

A. MASS-RTR(config-archive-log-cfg)#hidekeys
B. MASS-RTR(config-archive-log-cfg)#password encryption aes
C. MASS-RTR(config)#service password-encryption
D. MASS-RTR(config)#aaa authentication arap

46. Refer to the exhibit. An engineer receives this error message when trying to access another
router in-band from the serial interface connected to the console of R1.
Which configuration is needed on R1 to resolve this issue?

```
R1# show run | begin line

line con 0
      exec-timeout 0 0
      privilege level 15
      logging synchronous
      transport preferred telnet
      transport output none
      sstop bits 0 4

line vty 0 4
      login
      transport referred telnet
      transport input none
      transport output telnet

R1#

R1#ssh -1 cisco 192.168.12.2
% ssh connections not permitted from this terminal

R1#
```

A. R1(config)#line console 0
R1(config-line)# transport output ssh

B. R1(config)#line console 0
R1(config-line)# transport preferred ssh

C. R1(config)#line vty 0
R1(config-line)# transport output ssh
R1(config-line)# transport preferred ssh

D. R1(config)#line vty 0
R1(config-line)# transport output ssh

47. Refer to the exhibit. Which two actions should be taken to access the server? (Choose two).

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny sequence 10
    Match clauses:
        ip address (access-lists): 1
    Set Clauses:
    Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config |section ospf
router ospf 1
    network 192.168.1.1 0.0.0.0 area 0
    network 192.168 12.0 0.0.0.255 area 0
    distribute-list route-map RM-OSPF-DL in
Router#
```

A. Modify the access list to add a second line of permit ip any.
B. Modify the access list to deny the route to 192.168.2.2.
C. Modify distribute list seq 10 to permit the route to 192.168.2.2.
D. Add a sequence 20 in the route map to permit access list 1.
E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than
OSPF

48. Refer to the exhibit. A user cannot SSH to the router. What action must be taken to resolve this issue?

```
router#show running-config
Building configuration…
!
<output omitted…...!>
!
hostname R1
!
ip domain-name cisco.com
!
crypto key generate rsa modulus 2048
!
username admin privilege 15 secret cisco123
!
access-list 1 permit 1 10.1.1.0 0.0.0.255
access-list 1 deny any log
!
line vty 0 15
access-class in
login local
!
<output omitted…...!>
!
end
```

A. Configure transport input ssh
B. Configure transport output ssh

C. Configure ip ssh version 2
D. Configure ip ssh source-interface loopback0

49. Refer to the exhibit. An IT staff member comes into the office during normal office hours and
cannot access devices through SSH. Which action should be taken to resolve this issue?

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-range Office-hour
```

A. Modify the access list to use the correct IP address.
B. Configure the correct time range.
C. Modify the access list to correct the subnet mask.
D. Configure the access list in the outbound direction.

50. Refer to the exhibit. A network administrator configured an IPv6 access list to allow TCP return traffic only, but it is not working as expected. Which changes resolve this issue?

```
ipv6 access-list inbound
permit tcp any any
deny ipvy any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```

A. ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log

!
interface gi0/0
ipv6 traffic-filter inbound out

B. ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

C. ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0
ipv6 traffic-filter inbound in

D. ipv6 access-list inbound
permit tcp any any established
deny ipv6 any any log
!
interface g0/0
ipv6 traffic-filter inbound out

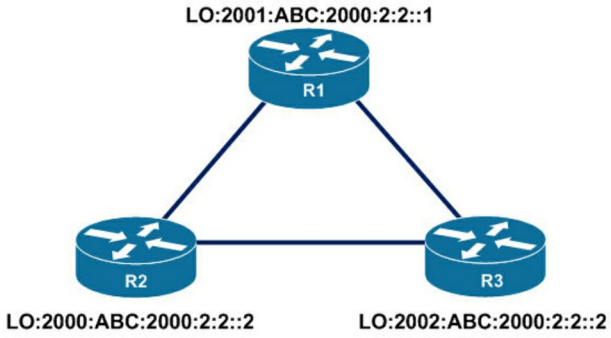
51. What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be
forwarded?
A. ACE
B. ACLS
C. DHCP
D. Binding Table

52. An engineer configured a Cisco router to send reliable and encrypted notifications for any events to the management server. It was noticed that the notification messages are reliable but not encrypted. Which action resolves the issue?
A. Configure all devices for SNMPv3 informs with priv.
B. Configure all devices for SNMPv3 informs with auth.

C. Configure all devices for SNMPv3 traps with auth.
D. Configure all devices for SNMPv3 traps with priv.

53. Which feature drops packets if the source address is not found in the snooping table?
A. IPv6 Source Guard
B. IPv6 Destination Guard
C. IPv6 Prefix Guard
D. Binding Table Recovery

54. Refer to the exhibit. An IPv6 network was newly deployed in the environment and the help desk
reports that R3 cannot SSH to the R2s Loopback interface. Which action resolves the issue?



IPv6 access list PERMIT_SSH
10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
70 deny ipv6 any any

A. Modify line 10 of the access list to permit instead of deny

B. Remove line 60 from the access list.
C. Modify line 30 of the access list to permit instead of deny.
D. Remove line 70 from the access list.

55. An engineer configured SNMP notifications sent to the management server using authentication
and encrypting data with DES. An error in the response PDU is received as "UNKNOWNUSERNAME.
WRONGDIGEST". Which action resolves the issue?
A. Configure the correct authentication password using SNMPv3 authPriv .
B. Configure the correct authentication password using SNMPv3 authNoPriv.
C. Configure correct authentication and privacy passwords using SNMPv3 authNoPriv.
D. Configure correct authentication and privacy passwords using SNMPv3 authPriv.

56. What are two functions of IPv6 Source Guard? (Choose two).
A. It uses the populated binding table for allowing legitimate traffic.
B. It works independent from IPv6 neighbor discovery.
C. It denies traffic from unknown sources or unallocated addresses.
D. It denies traffic by inspecting neighbor discovery packets for specific pattern.
E. It blocks certain traffic by inspecting DHCP packets for specific sources.

57. An engineer configured access list NON-CISCO in a policy to influence routes
What are the two effects of this route map configuration? (Choose two).
A. Packets are not evaluated by sequence 10.
B. Packets are evaluated by sequence 10.
C. Packets a e forwarded to the default gateway.
D. Packets a e forwarded using normal route lookup.
E. Packets are dropped by the access list.

58. Refer to the exhibit. Which two actions restrict access to router R1 by SSH? (Choose two).

```
R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
    Class-map: PERMIT (match-all)
        50 packets, 3811 bytes
        5 minute offered rate 0000 bps
        Match: access-group 100
    Class-map: ANY (match-all)
        210 packets, 19104 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: access-group 199
        drop
    Class-map: class-default (match-any)
        348 packets, 48203 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: any

R1#show access-list 100
Extended IP access list 100
    10 permit udp any any eq 23 (100 matches)
    20 permit tcp any any telnet any (50 matches)
    30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
    10 deny tcp any eq telnet any (50 matches)
    50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
    login
    transport input telnet ssh
    transport output telnet ssh
```

A. Configure transport input ssh on line vty and remove sequence 30 from access list 100.

B. Configure transport output ssh on line vty and remove sequence 20 from access list 100.
C. Remove class-map ANY from service-policy CoPP
D. Configure transport output ssh on line vty and remove sequence 10 from access list 199.
E. Remove sequence 10 from access list 100 and add sequence 20 deny tcp any any eq telnet to
access list 199

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

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

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

60. Which IPv6 filter purpose matches the correct IPv6 address?

Permit syslog from this source:
2001:0D8B:0800:200c::1c

A. permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443
B. permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
C. permit 2001:d8b:800:200c:800/117 2001:0DBB:800:2010::/64 eq 80
D. permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123

61. Which IPv6 filter purpose matches the correct IPv6 address?

Permit HTTPS from this source:
2001:0D8B:0800:200c::07ff

A. permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443
B. permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
C. permit 2001:d8b:800:200c:800/117 2001:0DBB:800:2010::/64 eq 80
D. permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123

62. What is the correct definition for Data Plane packets?
A. User-generated packets that are always forwarded by network devices to other end-station devices.
B. Network device generated or received packets that are used for the creation of the network itself.
C. Network device generated or received packets: packets that are used to operate the network.
D. User-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than normal traffic by the network devices.

63. What is the correct definition for Control Plane packets?
A. User-generated packets that are always forwarded by network devices to other end-station devices.
B. Network device generated or received packets that are used for the creation of the network itself.
C. Network device generated or received packets: packets that are used to operate the network.
D. User-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than normal traffic by the network devices.

64. What is the correct definition for Service Plane packets?
A. User-generated packets that are always forwarded by network devices to other end-station devices.
B. Network device generated or received packets that are used for the creation of the network itself.
C. Network device generated or received packets: packets that are used to operate the network.
D. User-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than normal traffic by the network devices.

65. Which of the following SNMP attributes belong to the SNMPv2

category? (Choose three).
A. Community String
B. Username and password
C. Authentication
D. No encryption
E. Privileged
F. Read-only

66. Which of the following SNMP attributes belong to the SNMPv3 category? (Choose three).
A. Community String
B. Username and password
C. Authentication
D. No encryption
E. Privileged
F. Read-only

67. What is the correct order to configure a policy to avoid following packet forwarding based on the normal routing path?

1. Configure route map instances.
2. Configure set commands.
3. Configure fast switching for PBR.
4. Configure ACLs.
5. Configure match commands.
6. Configure PBR on the interface.

A. 1, 5, 3, 2, 6, 4
B. 4, 6, 5, 1, 3, 2
C. 2, 4, 1, 3, 5, 6
D. 2, 5, 6, 4, 1, 3
E. 4, 1, 5, 2, 6, 3

68. Which IPv6 filter purpose matches the correct IPv6 address?

Permit NTP from this source:
2001:0D8B:0800:200c::1f

A. permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443
B. permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514

C. permit 2001:d8b:800:200c:800/117 2001:0DBB:800:2010::/64 eq 80
D. permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123

Chapter 3: Answers

1. Which command will require the VTY line connections to authenticate a user with the local database of the router?

C. R1(config-line)# login local

While under line configuration mode, the command “login local” configures the lines to authenticate incoming sessions to the local user database on the router.

2. Which command allows us to configure a router to use a loopback address as the source for TACACS+ communication?

C. R1(config)# ip tacacs source-interface Loopback 0

While under global configuration mode, the command “ip tacacs source-interface” allows us to specify a particular interface as the source address for TACACS logging messages. It’s a best practice to set the source to a local loopback interface, so that log messages are more easily interpreted.

3. Which standard port is used by RADIUS for authentication purposes?

A. 1812

RADIUS commonly uses port 1812 for authentication and 1813 for accounting, as defined by the Internet Engineering Task Force (IETF). Some RADIUS servers also use 1645 for authentication and 1646 for accounting, so this the server configuration should be verified when implementing RADIUS in a network. It is possible to change these values when configuring RADIUS within Cisco IOS.

4. Which Cisco IOS command will display the hours during which a time-based ACL named AFTER-WORK is configured to be active?

D. R1# show time-range AFTER-WORK

The command “show time-range” followed by the name of a particular ACL will display the hours during which it is configured to be active. The output

will show the days and times during which the ACL will be enforced.

5. Which command is correct when applying an IPv6 ACL named FILTER to an interface in the inbound direction?

A. R1(config-if)# ipv6 traffic-filter FILTER in

When applying an IPv6 ACL to an interface, rather than using the "access-group" command as we do with IPv4 ACLs, we instead need to use the "ipv6 traffic-filter" command.

6. Which Unicast Reverse Path Forwarding (uRPF) mode verifies that a packet source IP arrives on the same interface the router would use to reach the IP address?

C. Strict Mode

Using strict mode in uRPF means that the router will verify that the same interface on which the packet was received can be used to reach the packet's source IP address. If this is true, and there is a route in the routing table for the source, the packet will be permitted. By contrast, loose mode only checks to see if there is a route available in the routing table, and is not concerned with which interface is used to reach the source.

7. Which structure within a Control Plane Policing (CoPP) configuration is used to define the action which should be taken against policed traffic?

A. Policy Map

With a CoPP configuration, an ACL is used to identify particular traffic, which is classified and grouped using a Class Map. A Policy Map is used to define actions which should be taken against the traffic, such as rate-limiting or dropping. A Service Policy is then used to enable policing on the control plane interface.

8. The IPv6 RA Guard feature filters out which type of router advertisements in an IPv6 network?

B. Multicast

In IPv6 networks, devices periodically send out router advertisement (RA) messages via multicast. These help network nodes determine information

about the LAN, including the default gateway, network prefix lists, and more. The IPv6 RA Guard feature can filter these more specifically so that rogue advertisements cannot be introduced into the network.

9. Where can we apply an IPv6 DHCPv6 guard policy?

C. On either an interface or a VLAN

DHCPv6 guard uses a policy, similar to the way that IPv6 RA Guard works. This can be applied on a per-interface basis or at the VLAN level, applying the policy itself to the selected interfaces.

10. What is used by IPv6 nodes to discover the presence and link-layer addresses of other nodes which reside on the same link?

C. NDP

Neighbor Discovery Protocol (NDP) is used for IPv6 traffic, and it allows different nodes on the same link to advertise themselves to neighboring devices. It also allows them to learn information from these neighbors. These NDP messages are unsecure and susceptible to attacks, which is a case where we would use IPv6 ND Inspection/Snooping for protection. By snooping these messages, we can build a reference table called a DHCPv6 Snooping Binding Table which will help protect against things such as cache poisoning, DoS, and redirect attacks.

11. Which feature allows us to filter inbound traffic on L2 switch ports that are not found in the IPv6 binding table?

D. IPv6 Source Guard

IPv6 Source Guard is a first-hop security feature used for IPv6 networks that filters inbound traffic on a L2 switch. It references the IPv6 binding table, which is populated by an inspection feature such as ND inspection or IPv6 snooping. If the inbound traffic is not found in the binding table, the traffic will be denied, helping to protect against spoofing and DoS attacks.

12. Which command will allow an administrator to connect to a Cisco device’s VTY line only over port 22?

D. R1(config-line)# transport input ssh

SSH uses standard TCP port 22 for communication. Although the “transport input all” command will allow all methods of connection to the VTY line, in order to only allow SSH we would need to say “transport input ssh” under line configuration mode. It’s a best practice to disallow less secure telnet connections in this manner.

13. When switching a router configuration from SSHv1 to SSHv2, which command is necessary in order to provide secure access?

A. R1(config)# crypto key generate rsa

While under global configuration mode, the command “crypto key generate rsa” will create an RSA key used for secure access within SSHv2. Entering this command will prompt you for the key modulus size in bits. SSHv2 requires the RSA key pair size to be greater than or equal to 768 bits.

14. Which version of SNMP added the “inform” command in order to provide positive acknowledgement of message receipt?

C. SNMPv2c

The key advantage of SNMPv2c over SNMPv1 is the addition of the “informs” command. The original version of SNMP uses TRAP messages which are sent between SNMP entities without any acknowledgement or confirmation of receipt, meaning you have no assurance that the TRAP was received. SNMPv2c added an INFORM message, which is essentially a TRAP message that requires an entity to acknowledge that the TRAP was received.

15. When Cisco IOS command configures a remote user to receive traps using communication configured for authentication without privacy?

B. R1(config)# snmp-server host 10.1.1.50 v3 auth

The “auth” keyword configures a remote user to receive traps at the “authNoPriv” security level when using the SNMPv3 security model, meaning that authentication is used but encryption for privacy is not. SNMPv3 added both authentication and encryption, which can be used together or individually.

16. A device within our network that has a statically configured IP address

has begun having communication issues. From a Cisco router acting as a DHCP server, how can we verify an issue with the IP address?

A. R1# show ip dhcp conflict

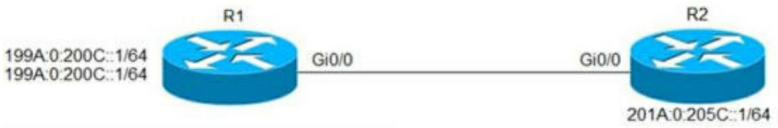
"show ip dhcp conflict" command will display information about any IP address conflicts detected during DHCP negotiation. If we have a statically assigned IP address on a host that is within the range of our DHCP pool, it's possible that this IP address can also be assigned by the DHCP server, particularly if we fail to create an IP address exclusion within the DHCP pool to reserve the address.

17. Under what condition would the DHCP Relay Agent feature be required in order to make sure our network hosts are able to obtain an IP address through DHCP?

B. The hosts and DHCP server are in different broadcast domains.

DHCP negotiation starts when a client sends out a broadcast message in order to obtain IP addressing. If the hosts and DHCP server lie within two different broadcast domains (e.g. different subnets), the broadcast messages will not be able to reach the DHCP server. This can be overcome with the DHCP Relay Agent feature of IOS (ip helper-address), which allows a router to forward DHCP messages from hosts towards the DHCP server, and vice versa.

18. Refer to the exhibit. Which configuration denies Telnet traffic to router 2 from 198A:0:200C::1/64?

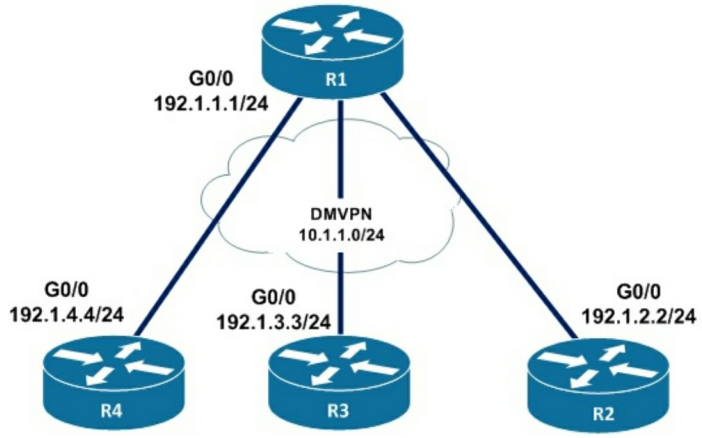


A. ipv6 access-list Deny_Telnet sequence 10 deny tcp host 198A:0:200C::1/64 host 201A:0:205C::1/64 eq telnet
!
int Gi0/0
ipv6 traffic-filter Deny_Telnet in

!

When assigning an IPv4 access list to an interface you used the ip access-list ACL_NAME in|out
command in interface configuration mode. To assign an IPv6 ACL to an interface you'll use the
ipv6 traffic-filter ACL_NAME in|out command in interface configuration mode.
We should also specific which port (telnet in this case) we want to deny or we will drop all TCP
traffic to the destination.
Note: In fact there is an error with all of the above commands as we cannot use subnet mask
(/64) with keyword "host". We must remove the subnet mask before applying the ACL statement.

19. 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).



R2
R2(config)#crypto isakmp policy 10
R2(config-isakmp)#hash md5
R2(config-isakmp)#authentication share
R2(config-isakmp)#group 2
R2(config-isakmp)#encryption 3des
R2(config)#crypto isakmp key cisco address 10.1.1.1
R2(config)#crypto ipsec transform set TSET esp-des esp-hmac
R2(cfg-crypto-trans)#mode transport
R2(config)#crypto ipsec profile TST R2 (ipsec-profile) # set transform- set TSET
R2(config)#interface tunnel 123
R2(config-if)#tunnel protection ipsec profile TST R3

R3(config)#crypto isakmp policy 10
R3(config-isakmp)#hash md5
R3(config-isakmp)#authentication pre-share
R3(config-isakmp)#group 2
R3(config-isakmp)#encryption 3des
R3(config)#crypto isakmp key cisco address 10.1.1.1
R3(config)#crypto ipsec transform-set TSET esp-des esp-md5-hmac
R3(cfg-crypto-trans)#mode tunnel
R3(config)#crypto ipsec profile TST R3 (ipsec-profile) + set transform-set TSET
R3(config)#interface tunnel 123
R3(config-if)#tunnel protection ipsec profile TST

A. Configure the crypto isakmp key cisco address 0.0.0.0 on R2 and R3.

D. Configure the mode from mode tunnel to mode transport on R3.

The first six commands are used to configure IPSec Phase 1 (ISAKMP Policy). Here is the details
of each command used above:
+ crypto isakmp policy 10 – This command creates ISAKMP policy number 10. You can create
multiple policies, for example 7, 8, 9 with different configuration. Routers

participating in Phase 1
negotiation tries to match a ISAKMP policy matching against the list of policies one by one. If any
policy is matched, the IPSec negotiation moves to Phase 2.
+ hash md5– MD5 algorithm will be used.
+ authentication pre-share – Authentication method is pre-shared key.
+ group 2 – Diffie-Hellman group to be used is group 2.
+ encryption 3des – 3DES encryption algorithm will be used for Phase 1.
+ crypto isakmp key cisco address 10.1.1.1 – The Phase 1 password is cisco and remote peer IP
address is 10.1.1.1
The next two command lines are used to configure IPSec Phase 2 (Transform Set):
+ crypto ipsec transform-set <transform-set-name> – Creates transform-set called <transformset-name>
+ esp-des – ESP IPSec protocol with the 56-bit Data Encryption Standard (DES) encryption
algorithm will be used
+ esp-md5-hmac – ESP with the MD5 (HMAC variant) authentication algorithm will be used.
+ mode transport: only encrypts the payload and ESP trailer
or
+ mode tunnel: encrypts the IP header of the ENTIRE packet

20. Which security feature can protect DMVPN tunnels?

A. IPsec

The IPSec protocol provides authentication and encryption to IP packets in the network.

21. Refer to the exhibit. An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown. The route us still present in the routing table as an OSPF route. Which action blocks the route?

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
        ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | section ospf
router ospf 1
  network 192.168.1.1 0.0.0.0 area 0
  network 192.168.12.0 0.0.0.255 area 0
  distribute-list route-map RM-OSPF-DL in
Router#|
```

C. Change sequence 10 in the route-map command from permit to deny.

22. Which statement about IPv6 RA Guard is true?

A. It does not offer protection in environments where IPv6 traffic is tunneled.

Restrictions for IPv6 RA Guard
+ The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is
tunneled.
+ This feature is supported only in hardware when the ternary content addressable memory
(TCAM) is programmed.
+ This feature can be configured on a switch port interface in the ingress

direction.
+ This feature supports host mode and router mode.
+ This feature is supported only in the ingress direction; it is not supported in the egress direction.
+ This feature is not supported on EtherChannel and EtherChannel port members.
+ This feature is not supported on trunk ports with merge mode.
+ This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of
PVLANs, primary VLAN features are inherited and merged with port features.
+ Packets dropped by the IPv6 RA Guard feature can be spanned.
+ If the platform ipv6 acl icmp optimize neighbor-discovery command is configured, the IPv6 RA
Guard feature cannot be configured and an error message will be displayed. This command adds
default global Internet Control Message Protocol (ICMP) entries that will override the RA guard
ICMP entries.

23. Which option is the best for protecting CPU utilization on a device?

B. CoPP

The traffic managed by a device can be divided into three functional components or planes:
+ Data plane
+ Management plane
+ Control plane
The vast majority of traffic flows through the device via the data plane; however, the route
processor handles certain traffic, such as routing protocol updates, remote-access services, and
network management traffic such as SNMP. This type of traffic is referred to as the control and
management plane. The route processor is critical to network operation. Therefore any service
disruption or security compromise to the route processor, and hence the

control and management
planes, can result in network outages that impact regular operations. For example, a DoS attack
targeting the route processor typically involves high bursty traffic resulting in excessive CPU
utilization on the route processor. Such attacks can be devastating to network stability and
availability. The bulk of traffic managed by the route processor is handled by way of the control
and management planes.
The CoPP feature is used to protect the aforementioned control and management planes; to
ensure stability, reachability, and availability and to block unnecessary or DoS traffic. CoPP uses
a dedicated control plane configuration through the modular QoS CLI (MQC) to provide filtering
and rate limiting capabilities for the control plane packets.

24. Refer to the router output. Network operations cannot read or write an configuration on the device with this configuration from the operation subnet. Which two configuration fix the issue? (Choose two).

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

A. Configure SNMP rw permission in addition to community ciscotest.

B. Modify access list 1 and allow operations subnet in the access list.

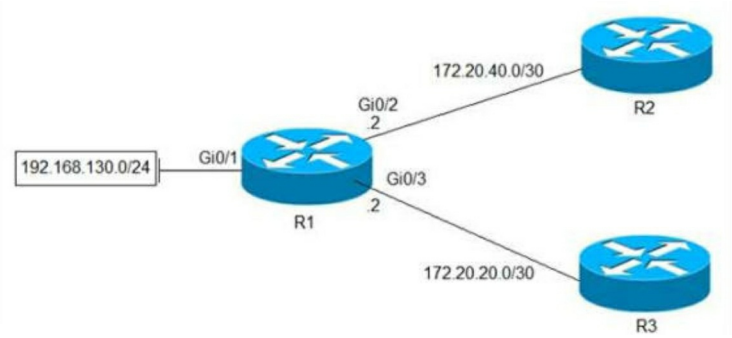
25. Which SNMP verification command shows the encryption and authentication protocols that are
used in SNMPV3?

B. show snmp user

The command “show snmp user” displays information about the configured characteristics of

SNMP users. The following example specifies the username as abcd with authentication method
of MD5 and encryption method of 3DES. The command “show snmp group” displays the names of groups on the router and the security model, the status of the different views, and the storage type of each group.

26. 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?



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

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

A. TFTP
B. SNMP

TCP starvation/UDP dominance likely occurs if TCP-based applications are assigned to the same service-provider class as UDP-based applications and the class experiences sustained congestion. TFTP (runs on UDP port 69) and SNMP (runs on UDP port 161/162) are two protocols which run on UDP so they can cause TCP starvation.

28. Refer to the exhibit. Why is user authentication being rejected?

```
TAC+: TCP/IP open to 171.68.118.101/49 failed -
Destination unreachable; gateway or host down
AAA/AUTHEN (2546660185): status = ERROR
AAA/AUTHEN/START (2546660185): Method=LOCAL
AAA/AUTHEN (256660185): status = FAIL
As1 CHAP: Unable to validate Response. Username chapuser: Authentication failure
```

D. The TACACS+ server is down and the user is not in the local database.

In the output we noticed that the “Destination unreachable; gateway or host down” notification
while trying to communicate with the TACACS+ server. This means the TACACS+ server went
down. So the next authentication method is via the local database (“Method=LOCAL”). But the
authentication was failed again because of bad username, bad password or both.

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

```
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#
```

A. crypto key generate rsa

We see the notification “% Please create RSA keys to enable SSH” so we have to create RSA
keys with the command:
R1(config)#crypto key generate rsa

30. Refer to the exhibit. 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?

```
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#
```

B. Add the login authentication Console command to the line configuration

Use the ***login authentication default*** command which applies the authentication list to a line or set of lines. Router(config-line)#login authentication default

31. What is a limitation of IPv6 RA Guard?

B. It does not offer protection in environments where IPv6 traffic is tunneled.

Restrictions for IPv6 RA Guard
- The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is
tunneled.
- This feature is supported only in hardware when the ternary content addressable memory
(TCAM) is programmed.
- This feature can be configured on a switch port interface in the ingress direction.
- This feature supports host mode and router mode.

- This feature is supported only in the ingress direction; it is not supported in the egress direction.
- This feature is not supported on EtherChannel and EtherChannel port members.
- This feature is not supported on trunk ports with merge mode.
- This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of
PVLANs, primary VLAN features are inherited and merged with port features.
- Packets dropped by the IPv6 RA Guard feature can be spanned.

32. Refer to the exhibit. 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?

```
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
!
```

D. route-map FILTER-IN permit 20

By using "deny" keyword in a route-map, we can filter out the prefix specified in the prefix- list.
But there is an implicit "deny all" statement in the prefix-list so we must permit other prefixes
with "permit" keyword in the route-map.

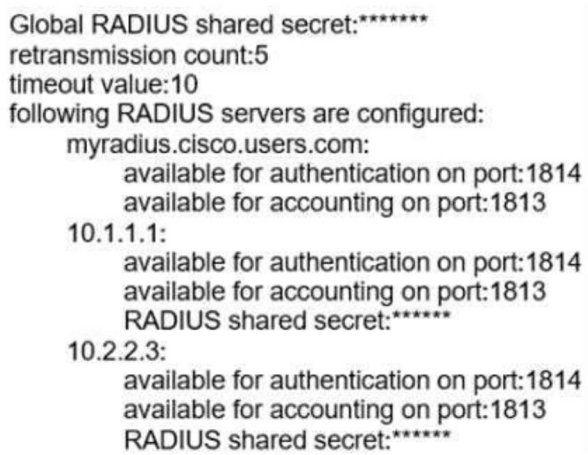
33. Refer to the exhibit. A company is evaluating multiple network management system tools.
Trending graphs generated by SNMP data are returned by the NMS and appear to have multiple
gaps. While troubleshooting the issue, an engineer noticed the relevant output. What solves the
gaps in the graphs?

```
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#
```

**D. Separate the NMS class map in multiple class maps based on the specific protocols with
appropriate CoPP actions.**

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/CPP 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.”

34. Refer to the exhibit. 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

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.

35. What is a function of IPv6 ND inspection?

**B. It learns and secures bindings for stateless autoconfiguration addresses in Layer 2 neighbor
tables.**

IPv6 Neighbor Discovery (ND) inspection analyzes ND messages in order to build a trusted binding table. IPv6 ND messages that do not have valid bindings are dropped.

36. Refer the exhibit. BGP is flapping after the COPP policy is applied. What are the two solutions to fix the issue? (Choose two).

```
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
```

C. Configure a higher value for CIR under the default class to allow more packets during peak
Traffic.

E. Configure BGP in the COPP-CRIT1CAL-7600 ACL.

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)

37. Refer the exhibit. Which action resolves intermittent connectivity observed with the SNMP trap
packets?

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

        Service-policy output: R3_CoPP


        Class-map: mgmt (match-all)
            361 packets, 73858 bytes
            4 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, exceeded 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 acceess-list 10
Extended IP access list 120
    10 permit udp any any eq snmptrap (361 matches)
```

D. Add one new entry in the ACL 120 to permit the UDP port 161.

38. 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?

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 0.0.0.255 172.16.10.0 0.0.0.255 eq telnet time-range changewindow
!
time-range changewindow
periodic Friday Saturday Sunday 22:00 to 05:00
```

39. Refer to the exhibit. The ACL is placed on the inbound Gigabit 0/1 interface of the router.
Host 192.168.10.10 cannot SSH to host 192.168.100.10 even though the flow is permitted. Which action resolves the issue without opening full access to this router?

```
ip access-list extended FILTER
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 22
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 23
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 80
deny tcp 192.168.10.0.0.0.255 192.168.100.0 0.0.0.255 eq 443
permit tcp host 192.168.10.10 host 192.168.100.10 eq ssh
permit ip any any
!
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip access-group FILTER in
!
```

A. Move the SSH entry to the beginning of the ACL.

The host 192.168.10.10 is denied access because the ACL analyses packets beginning at the top of the ACL statements. By moving the permit statement to the beginning of the ACL, the host is permitted, while all others are denied.

40. Refer to the exhibit. Which option represents the minimal configuration that allows inbound
traffic from the 172.16.1.0/24 network to successfully enter router R, while also limiting spoofed 10.0.0.0/8 hosts that could enter router R?


```
R(config)#ip route 10.0.0.0 255.0.0.0 FastEthernet0/1
R(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet 0/0
```

A.
R(config)#ip cef
R(config)#interface fa0/0
R(config-if)#ip verify unicast source reachable-via rx allow-default

41. Which traffic does the following configuration allow?

ipv6 access-list cisco
permit ipv6 host 2001:DB8:0:4::32 any eq ssh
line vty 0 4
ipv6 access-class cisco in

C. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32

Here we see that the Ipv6 access list called "cisco" is being applied to incoming VTY connections

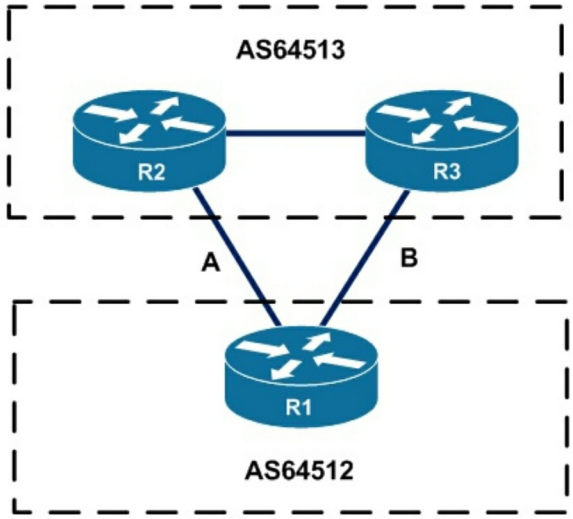
to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of
2001:DB8:0:4::32 to connect using SSH only.

42. Which access list entry checks for an ACK within a packet header?

C. access-list 149 permit tcp any any eq 21 established

The "established" keyword is used only for the TCP protocol to indicate an established connection. A match occurs if the TCP datagram has the ACK or RST bits set, which indicates that the packet belongs to an existing connection.

43. Refer to the exhibit. A network engineer for AS64512 must remove the inbound and outbound
traffic from link A during maintenance without closing the BGP session so that there is a backup link over link A toward the ASN. Which BGP configuration on R1 accomplishes this goal?



D.
route-map link-a-in permit 10
route-map link-a-out permit 10
set as-path prepend 64512
route-map link-b-in permit 10
set local-preference 200
route-map link-b-out permit 10

44. Refer to the exhibit. R1 is being monitored using SNMP and monitoring devices are getting only
partial information. What action should be taken to resolve this issue?

```
R1#show policy-map control-plane
  Control Plane

        Service-policy output:  CoPP

          Class-map: SNMP-Out (match-all)
            124 packets, 3693 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: access-group name SNMP
            police:
                cir 8000 bps, bc 1500 bytes
              conformed 0 packets, 0 bytes; actions:
                transmit
              exceeded 0 packets, 0 bytes; actions:
                drop
              conformed 0000 bps, exceeded 0000 bps

          Class-map: class-default (match-any)
            10 packets, 1003 bytes
            5 minute offered rate 0000 bps, drop rate 0000 bps
            Match: any
R1#show ip access-list SNMP
Extended IP access list SNMP
        10 permit udp any eq snmp any
```

B. Modify the access list to include snmptrap.

45. Refer to the exhibit. A client is concerned that passwords are visible when running this show
archive log config all. Which router configuration is needed to resolve this issue?

```
MASS-RTR#show running config
!
hostname MASS-RTR
!
aaa new-model
!
aaa autentication login default local
aaa autentication exec default local
aaa autentication commands 15 default local
!
username admin privilege 15 password 7 023624481115F3348
username cisco privilege 15 password 7 0607072C49A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
 idx   sess    user@lir Logged command
   1      1    console@ |interface GigabitEthernet0/0
   2      1    console@ | no shutdown
   3      1    console@ | ip address dhcp
   4      2    admin@\ |username cisco privilege 15 password cisco
   5      2    admin@\ |!config: USER TABLE MODIFIED
```

A. MASS-RTR(config-archive-log-cfg)#hidekeys

This command (Device(config-archive-log-config)#hidekeys) is Optional. It suppresses the displayof password information in the configuration log files. Enabling the hidekeys command increases security by preventing password information from being displayed in configuration log files.

46. Refer to the exhibit. An engineer receives this error message when trying to access another
router in-band from the serial interface connected to the console of R1.
Which configuration is needed on R1 to resolve this issue?

```
R1# show run | begin line

line con 0
      exec-timeout 0 0
      privilege level 15
      logging synchronous
      transport preferred telnet
      transport output none
      sstop bits 0 4

line vty 0 4
      login
      transport referred telnet
      transport input none
      transport output telnet

R1#

R1#ssh -1 cisco 192.168.12.2
% ssh connections not permitted from this terminal

R1#
```

A. R1(config)#line console 0
R1(config-line)# transport output ssh

Transport output ssh must be set to the console 0.

47. Refer to the exhibit. Which two actions should be taken to access the server? (Choose two).

```
Router#show access-lists
Standard IP access list 1
        10 permit 192.168.2.2 (1match)
Router#
Router#show route-map
route-map RM-OSPF-DL, deny sequence 10
    Match clauses:
        ip address (access-lists): 1
    Set Clauses:
    Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config |section ospf
router ospf 1
    network 192.168.1.1 0.0.0.0 area 0
    network 192.168 12.0 0.0.0.255 area 0
    distribute-list route-map RM-OSPF-DL in
Router#
```

B. Modify the access list to deny the route to 192.168.2.2.

E. Add a floating static route to reach to 192.168.2.2 with administrative distance higher than OSPF.

48. Refer to the exhibit. A user cannot SSH to the router. What action must be taken to resolve this issue?

```
router#show running-config
Building configuration…
!
<output omitted…...!>
!
hostname R1
!
ip domain-name cisco.com
!
crypto key generate rsa modulus 2048
!
username admin privilege 15 secret cisco123
!
access-list 1 permit 1 10.1.1.0 0.0.0.255
access-list 1 deny any log
!
line vty 0 15
access-class in
login local
!
<output omitted…...!>
!
end
```

A. Configure transport input ssh

The “transport input ssh” must be configured on the console lines to allow

only ssh connections into the device.

49. Refer to the exhibit. An IT staff member comes into the office during normal office hours and
cannot access devices through SSH. Which action should be taken to resolve this issue?

```
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip access-group 101 in
!
time-range Office-hour
periodic weekdays 08:00 to 17:00
!
access-list 101 permit tcp 10.0.0.0 0.0.0.0 172.16.1.0 0.0.0.255 eq ssh time-range Office-hour
```

A. Modify the access list to use the correct IP address.

To ACL should be permit tcp 101 10.1.1.1 0.0.0.0

50. Refer to the exhibit. A network administrator configured an IPv6 access list to allow TCP return traffic only, but it is not working as expected. Which changes resolve this issue?

```
ipv6 access-list inbound
permit tcp any any
deny ipvy any any log
!
interface gi0/0
ipv6 traffic-filter inbound out
```

C. ipv6 access-list inbound
permit tcp any any syn
deny ipv6 any any log
!
interface gi0/0

ipv6 traffic-filter inbound in

Optional TCP access list and the access conditions are as follows: ack—Acknowledgment bit set; fin—Finished bit set; no more data from sender; neq {port | protocol}—Matches only packets that are not on a given port number; psh—Push function bit set; range {port | protocol}—Matches only packets in the port number range; rst—Reset bit set; syn—Synchronize bit set; urg—Urgent pointer bit set.

51. What does IPv6 Source Guard utilize to determine if IPv6 source addresses should be
forwarded?

D. Binding Table

52. An engineer configured a Cisco router to send reliable and encrypted notifications for any events to the management server. It was noticed that the notification messages are reliable but not encrypted. Which action resolves the issue?

A. Configure all devices for SNMPv3 informs with priv.

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the
receiver does not send acknowledgments when this device receives traps."Send reliable and encrypted notifications for any events" so it is SNMP notifications. For encryption we need to
configure "priv".

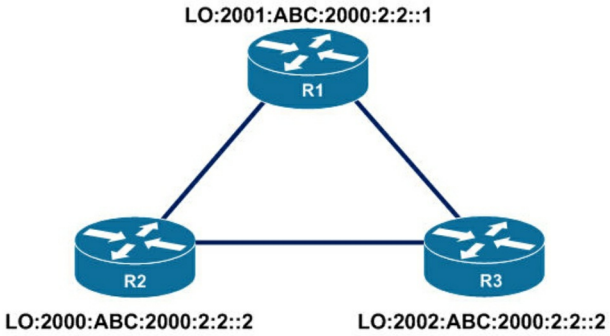
53. Which feature drops packets if the source address is not found in the snooping table?

A. IPv6 Source Guard

IPv6 Source Guard and IPv6 Prefix Guard are Layer 2 snooping features that validate the source of IPv6 traffic. IPv6 Source Guard blocks any data traffic from an unknown source.

54. Refer to the exhibit. An IPv6 network was newly deployed in the environment and the help desk
reports that R3 cannot SSH to the R2s Loopback interface. Which action

resolves the issue?



IPv6 access list PERMIT_SSH
10 deny tcp 2001:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
20 permit tcp 2001:ABC:2000:2:2::/64 host 2000:ABC:20:2:2::2 eq 22
30 deny tcp 2002:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
40 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 22
50 permit tcp 2000:ABC:2000::/36 host 2000:ABC:20:2:2::2 eq 23
60 permit tcp host 2002:ABC:2000:2:2::2 host 2000:ABC:20:2:2::2 eq 22
70 deny ipv6 any any

C. Modify line 30 of the access list to permit instead of deny.

A deny statement in the ACL will drop packets when matched. A permit statement will allow packets to process through the interface.

55. An engineer configured SNMP notifications sent to the management server using authentication
and encrypting data with DES. An error in the response PDU is received as "UNKNOWNUSERNAME.
WRONGDIGEST". Which action resolves the issue?

A. Configure the correct authentication password using SNMPv3 authPriv .

There are three SNMP security levels (for SNMPv1, SNMPv2c, and

SNMPv3):
+ noAuthNoPriv: Security level that does not provide authentication or encryption.
+ authNoPriv: Security level that provides authentication but does not provide encryption.
+ authPriv: Security level that provides both authentication and encryption.
For SNMPv3, "noAuthNoPriv" level uses a username match for authentication.

56. What are two functions of IPv6 Source Guard? (Choose two).

A. It uses the populated binding table for allowing legitimate traffic.

C. It denies traffic from unknown sources or unallocated addresses.

IPv6 source guard can deny traffic from unknown sources or unallocated addresses, such as traffic from sources not assigned by a DHCP server. When traffic is denied, the IPv6 address glean feature is notified so that it can try to recover the traffic by querying the DHCP server or by using IPv6 ND.

57. An engineer configured access list NON-CISCO in a policy to influence routes.
What are the two effects of this route map configuration? (Choose two).

B. Packets are evaluated by sequence 10.

C. Packets a e forwarded to the default gateway.

58. Refer to the exhibit. Which two actions restrict access to router R1 by SSH? (Choose two).

```
R1#show policy-map control-plane
Control Plane
Service-policy input: CoPP
    Class-map: PERMIT (match-all)
        50 packets, 3811 bytes
        5 minute offered rate 0000 bps
        Match: access-group 100
    Class-map: ANY (match-all)
        210 packets, 19104 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: access-group 199
        drop
    Class-map: class-default (match-any)
        348 packets, 48203 bytes
        5 minute offered rate 0000 bps, drop rate 0000 bps
        Match: any

R1#show access-list 100
Extended IP access list 100
    10 permit udp any any eq 23 (100 matches)
    20 permit tcp any any telnet any (50 matches)
    30 permit tcp any eq telnet any (10 matches)

R1#show access-list 199
Extended IP access list 199
    10 deny tcp any eq telnet any (50 matches)
    50 permit ip any any (1 match)

R1#show running-config | section line vty
line vty 0 4
    login
    transport input telnet ssh
    transport output telnet ssh
```

A. Configure transport input ssh on line vty and remove sequence 30 from access list 100.

B. Configure transport output ssh on line vty and remove sequence 20 from access list 100.

To only allow SSH to R1, we have to: + Deny Telnet in ACL 100 because the action of class-map:
PERMIT is "permit" + Permit Telnet in ACL 199 because the action of class-map: ANY is "drop"
But:
+ In ACL 100 there is a permit statement for Telnet traffic "20 permit tcp any any eq telnet (5
matches)" which is not correct so we must remove this statement.
+ In ACL 199 there is an ACL statement "10 deny tcp any eq telnet any (50 matches)". This
statement is aimed for Telnet traffic leaving R1 which is not correct so we must remove this
statement. + The command "transport output telnet ssh" allows telnet and SSH from this device (to other devices).
+ Telnet is TCP port 23. + When using Telnet on source port, it affects Telnet traffic leaving from
R1.

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

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

B. permit tcp port 443

60. Which IPv6 filter purpose matches the correct IPv6 address?

Permit syslog from this source:
2001:0D8B:0800:200c::1c

B. permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514

Syslog runs on UDP port 514 while NTP runs on UDP port 123 so if we remember them we can
find out the matching answers easily. But maybe there is some typos in this question as
2001:d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f.
Same for 2001:D88:800:200c::e/126, which also ranges from 2001:d88:800:200c:0:0:0:c to
2001:d88:800:200c:0:0:0:f and does not cover host 2001:0D88:0800:200c::1c.

61. Which IPv6 filter purpose matches the correct IPv6 address?

Permit HTTPS from this source:
2001:0D8B:0800:200c::07ff

A. permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443

HTTP and HTTPs run on TCP port 80 and 443, respectively and we have to remember them.
But maybe there is some typos in this question as 2001:d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f. Same for 2001:D88:800:200c::e/126, which also ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f and does not cover host 2001:0D88:0800:200c::1c.

62. What is the correct definition for Data Plane packets?

A. User-generated packets that are always forwarded by network

devices to other end-station devices.

From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
Data plane packets – End-station, user-generated packets that are always forwarded by
network devices to other end-station devices. From the perspective of the network device, data
plane packets always have a transit destination IP address and can be handled by normal,
destination IP address-based forwarding processes.

63. What is the correct definition for Control Plane packets?

B. Network device generated or received packets that are used for the creation of the network itself.

From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
Control plane packets – Network device generated or received packets that are used for the
creation and operation of the network itself. From the perspective of the network device, control
plane packets always have a receive destination IP address and are handled by the CPU in the
network device route processor. Examples include protocols such as ARP, BGP, OSPF, and
other protocols that glue the network together.

64. What is the correct definition for Service Plane packets?

D. User-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than normal traffic by the network devices.

From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
Services plane packets – A special case of data plane packets, services plane packets are
also user-generated packets that are also forwarded by network devices to

other end-station
devices, but that require high-touch handling by the network device (above and beyond normal,
destination IP address-based forwarding) to forward the packet. Examples of high-touch handling
include such functions as GRE encapsulation, QoS, MPLS VPNs, and SSL/IPsec
encryption/decryption, etc. From the perspective of the network device, services plane packets
may have a transit destination IP address, or may have a receive destination IP address (for
example, in the case of a VPN tunnel endpoint).

65. Which of the following SNMP attributes belong to the SNMPv2 category? (Choose three).

A. Community String
D. No encryption
F. Read-only

Both SNMPv1 and v2 did not focus much on security and they provide security based on
community string only. Community string is really just a clear text password (without encryption).
Any data sent in clear text over a network is vulnerable to packet sniffing and interception. There
are two types of community strings in SNMPv2c:
+ Read-only (RO): gives read-only access to the MIB objects which is safer and preferred to other
method.
+ Read-write (RW): gives read and write access to the MIB objects. This method allows SNMP
Manager to change the configuration of the managed router/switch so be careful with this type.
The community string defined on the SNMP Manager must match one of the community strings
on the Agents in order for the Manager to access the Agents.
SNMPv3 provides significant enhancements to address the security

weaknesses existing in the
earlier versions. The concept of community string does not exist in this version. SNMPv3 provides
a far more secure communication using entities, users and groups. This is achieved by
implementing three new major features:
+ Message integrity: ensuring that a packet has not been modified in transit.
+ Authentication: by using password hashing (based on the HMAC-MD5 or HMAC-SHA
algorithms) to ensure the message is from a valid source on the network.
+ Privacy (Encryption): by using encryption (56-bit DES encryption, for example) to encrypt the
contents of a packet.

66. Which of the following SNMP attributes belong to the SNMPv3 category? (Choose three).

B. Username and password
C. Authentication
E. Privileged

Both SNMPv1 and v2 did not focus much on security and they provide security based on
community string only. Community string is really just a clear text password (without encryption).
Any data sent in clear text over a network is vulnerable to packet sniffing and interception. There
are two types of community strings in SNMPv2c:
+ Read-only (RO): gives read-only access to the MIB objects which is safer and preferred to other
method.
+ Read-write (RW): gives read and write access to the MIB objects. This method allows SNMP
Manager to change the configuration of the managed router/switch so be careful with this type.
The community string defined on the SNMP Manager must match one of the community strings
on the Agents in order for the Manager to access the Agents.

SNMPv3 provides significant enhancements to address the security weaknesses existing in the
earlier versions. The concept of community string does not exist in this version. SNMPv3 provides
a far more secure communication using entities, users and groups. This is achieved by
implementing three new major features:
+ Message integrity: ensuring that a packet has not been modified in transit.
+ Authentication: by using password hashing (based on the HMAC-MD5 or HMAC-SHA
algorithms) to ensure the message is from a valid source on the network.
+ Privacy (Encryption): by using encryption (56-bit DES encryption, for example) to encrypt the
contents of a packet.

67. What is the correct order to configure a policy to avoid following packet forwarding based on the normal routing path?

1. Configure route map instances.
2. Configure set commands.
3. Configure fast switching for PBR.
4. Configure ACLs.
5. Configure match commands.
6. Configure PBR on the interface.

E. 4, 1, 5, 2, 6, 3

Step.1: Configure ACLs.
Permit statement in ACL is what will be matched. You don't want to permit everything, by default the implicit deny at the bottom of the ACL and just create an ACL that permits what you going to take action on in the route-map.

Step.2: Configure route map instances.
Route maps are similar to Access Control Lists (ACLs), but have these enhanced capabilities - Modifying certain fields in the packet; Forwarding packets in a specified manner; Filtering and modifying the attributes of a route.

Step.3: Configure match commands.
PBR allows the user to match packets based on the length and characteristics of a packet, using a standard or extended ACL.

Step.4: Configure set commands.
Define the action to be taken on the packets that match the criteria using set command.

Step.5: Configure PBR on the interface.
you need to apply this policy/route-map to the interface where the traffic is coming in.

Step.6: (Optional) Configure local PBR.
Packets that are generated by the router are not normally policy routed. To enable PBR for packets generated by the router, issue the
ip local policy route-map <Route map name> command.

68. Which IPv6 filter purpose matches the correct IPv6 address?

Permit NTP from this source:
2001:0D8B:0800:200c::1f

D. permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123

Syslog runs on UDP port 514 while NTP runs on UDP port 123 so if we remember them we can
find out the matching answers easily. But maybe there is some typos in this question as
2001:d88:800:200c::c/126 only ranges from 2001:d88:800:200c:0:0:0:c to 2001:d88:800:200c:0:0:0:f (4 hosts in total). It does not cover host 2001:0D88:0800:200c::1f.
Same for 2001:D88:800:200c::e/126, which also ranges from
2001:d88:800:200c:0:0:0:c to
2001:d88:800:200c:0:0:0:f and does not cover host
2001:0D88:0800:200c::1c.

Chapter 4: Infrastructure Services

The objectives covered in this chapter:

25% 4.0 Infrastructure Services

4.1 Troubleshoot device management

4.1.a Console and VTY

4.1.b Telnet, HTTP, HTTPS, SSH, SCP

4.1.c (T)FTP

4.2 Troubleshoot SNMP (v2c, v3)

4.3 Troubleshoot network problems using logging (local, syslog, debugs, conditional debugs, timestamps)

4.4 Troubleshoot IPv4 and IPv6 DHCP (DHCP client, IOS DHCP server, DHCP relay, DHCP options)

4.5 Troubleshoot network performance issues using IP SLA (jitter, tracking objects, delay, connectivity)

4.6 Troubleshoot NetFlow (v5, v9, flexible NetFlow)

4.7 Troubleshoot network problems using Cisco DNA Center assurance (connectivity, monitoring, device health, network health)

1. Which section of Cisco DNA Center is dedicated to proactive issue detection?
A. Design
B. Assurance

C. Policy
D. Provision

2. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?
A. Analytics
B. Contextual Insight
C. Path Trace
D. Network Health

3. Which well-known port number is commonly used to move files and images between a Cisco router and a TFTP server?
A. TCP 69
B. UDP 69
C. TCP 121
D. UDP 121

4. Which Syslog command will configure a Cisco device for logging at the Warning level, and also those levels considered to be more severe?
A. R1(config)# logging level 2
B. R1(config)# logging level 3
C. R1(config)# logging level 4
D. R1(config)# logging level 5

5. What is the general rule of thumb when using Cisco debug commands?
A. Use a debug command that is as general as possible.
B. Use a debug command on a device as close to the source as possible.
C. Use a debug command on a device as close to the destination as possible.
D. Use a debug command that is as specific as possible.

6. Which Cisco IOS command allows us to specifically turn off conditional debugging that has been put in place for the GigabitEthernet 0/1 interface of a router?
A. R1# debug off interface gig 0/1
B. R1# no debug all
C. R1# no debug condition interface gig 0/1
D. R1# undebug interface gig 0/1

7. Below is a section of an IP SLA configuration that does not appear to be

working properly. What should be done in order to correct the issue with the IP SLA probe?

R1# show ip sla con 1

***
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 10.1.1.50/0.0.0.0
Target port/Source port: 16500/0
Codec Packet size: 32
Control Packets: enabled
Schedule:
    Operation frequency (seconds): 5
    Next scheduled start time: Pending trigger
    Group scheduled: FALSE
    Life (seconds): Forever
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE

        ***

A. Configure a source port.
B. Configure a source address.
C. Configure the start time.
D. Configure an ageout time.

8. Which version of NetFlow features a fixed packet format?
A. NetFlow v4
B. NetFlow v7
C. NetFlow v5
D. NetFlow v9

9. Which version of NetFlow would be preferred in a network using multicast media applications where ingress and egress monitoring is desired?
A. NetFlow v9
B. NetFlow v7
C. NetFlow v5
D. NetFlow v4

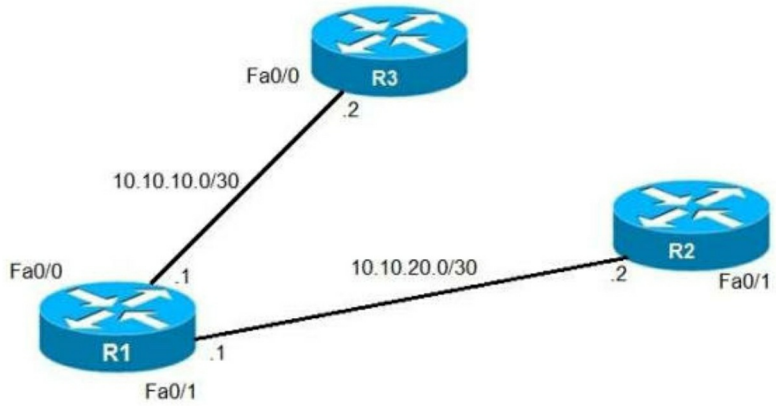
10. Which version of NetFlow allows us to use multiple flow monitors and exporters simultaneously on the same traffic?
A. NetFlow v9
B. NetFlow v10
C. IPFIX
D. Flexible NetFlow

11. Which section of Cisco DNA Center is dedicated to proactive issue detection?
A. Design
B. Assurance
C. Policy
D. Provision

12. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?
A. Analytics
B. Contextual Insight
C. Path Trace
D. Network Health

13. A network engineer is investigating a flapping (up/down) interface issue on a core switch that is
synchronized to an NTP server. Log output does not show the time of the flap. Which command allows on the switch the time of the flap according to the clock on the device?
A. clock calendar-valid
B. service timestamps log datetime localtime show-timezone
C. service timestamps log uptime
D. clock summer-time mst recurring 2 Sunday mar 2:00 1 sunday nov 2:00

14. Refer to the exhibit. An IP SLA was configured on router R1 that allows the default route to be
modified in the event that Fa0/0 losses reachability with the router R3 Fa0/0 interface. The route has changed to flow through route R2. Which debug command is used to troubleshoot this issue?



A. debug ip flow
B. debug ip sla error
C. debug ip routing
D. debug ip packet

15. Refer to the exhibit. 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?

```
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
```

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

16. When provisioning a device in Cisco DNA Center, the engineer sees the error message "Cannot
select the device. Not compatible with template.". What is the reason for the error?
A. The software version of the template is different from the software version of the device
B. The changes to the template were not committed
C. The template has an incorrect configuration.
D. The tag that was used to filter the templates does not match the device tag.

17. White working with software images, an engineer observes that Cisco DNA Center cannot upload
its software image directly from the device. Why is the image not uploading?
A. The device has lost connectivity to Cisco DNA Center.
B. The software image for the device is in bundle mode
C. The software image for the device is in install mode.
D. The device must be resynced to Cisco DNA Center

18. Refer to the exhibit. 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?

```
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) #
```

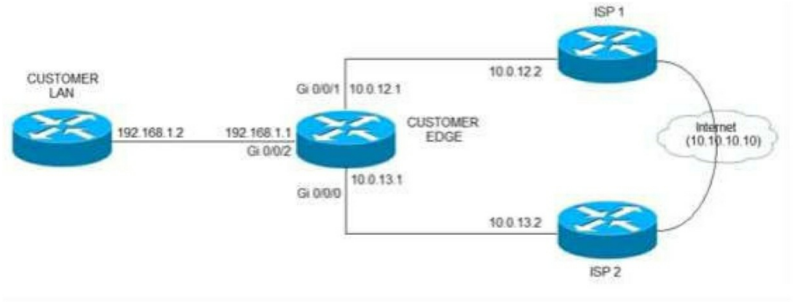
A. Enter the transport input ssh configuration command.
B. Enter the terminal monitor exec command.
C. Enter the logging console debugging configuration command.
D. Enter the aaa new-model configuration command.

19. An engineer is trying to copy an IOS file from one router to another router by using TFTP.
Which two actions are needed to allow the file to copy? (Choose two).
A. Configure the TFTP authentication on the source router with the tftp-server authentication local
command.
B. Configure a user on the source router with the username tftp password tftp command.
C. Enable the TFTP server on the source router with the tftp-server flash: <filename> command.
D. TFTP is not supported in recent IOS versions, so an alternative method must be used.
E. Copy the file to the destination router with the copy tftp: flash: command

20. A network engineer needs to verify IP SLA operations on an interface that shows on indication of excessive traffic. Which command should the engineer use to complete this action?
A. show frequency
B. show track
C. show reachability
D. show threshold

21. An engineer configured the wrong default gateway for the Cisco DNA center enterprise interface
during the install. Which command must the engineer run to correct the configuration?
A. Sudo update config install
B. Sudo maglev reinstall
C. Sudo maglev-config update
D. Sudo maglev install config update
22. Refer to the exhibit. ISP 1 and ISP 2 directly connect to the internet. A customer IS tracking both ISP links to achieve redundancy and cannot see the Cisco IP SLA tracking output on the router console. Which command is

missing from the IP SLA configuration?



A. Start-time now
B. Start-time 00:00
C. Start-time 0
D. Start-time immediately

23. Refer to the exhibit. An administrator noticed that after a change was made on R1, the timestamps on the system logs did not match the clock. What is the reasons for this error?

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101A0B01521812062247470 71E 7
ntp server 10.10.10.10

R1#show clock
*06:13:44.045 MST Sun Dec 30 2018

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config) #logging host 10.10.10.20
R1(config) #end
R1#
*Dec 30 13:15:28: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Dec 30 13:15:28: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.10.20 port 514
started – CLI initiated
```

A. The keyword localtime is defined on the timestamp service command.
B. The NTP server is in an different time zone.
C. An authentication error with the NTP server results in an incorrect timestamp.
D. The system clock is set incorrectly to summer-time hours

24. 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

25. Which command is used to check IP SLA when an interface is suspected to receive lots of traffic
with options?
A. show track
B. show threshold
C. show timer
D. show delay

26. Refer to the exhibit. Why is the remote NetFlow server failing to receive the NetFlow data?

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
ip cef
!
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

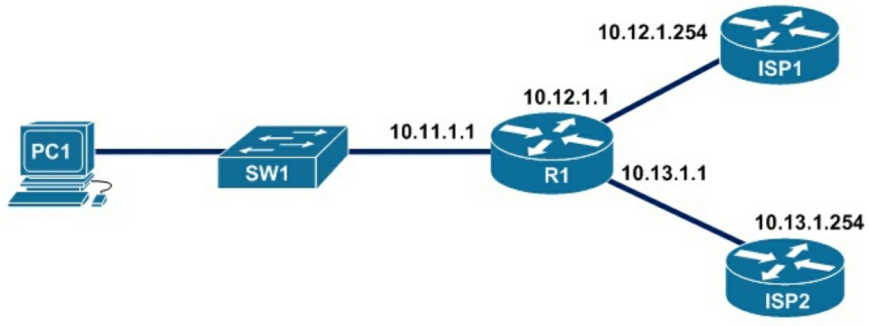
A. The flow exporter is configured but is not used.
B. The flow monitor is applied in the wrong direction.
C. The flow monitor is applied to the wrong interface.
D. The destination of the flow exporter is not reachable.

27. Refer to the exhibit. 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?

```
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
```

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

28. Refer to the exhibit. An engineer is monitoring reachability of the configured default routes to ISP1 and ISP2. The default route from ISP1 is preferred if available. How is this issue resolved?



A. Use the icmp-echo command to track both default routes.
B. Use the same AD for both default routes.
C. Start IP SLA by matching numbers for track and ip sla commands.
D. Start IP SLA by defining frequency and scheduling it.

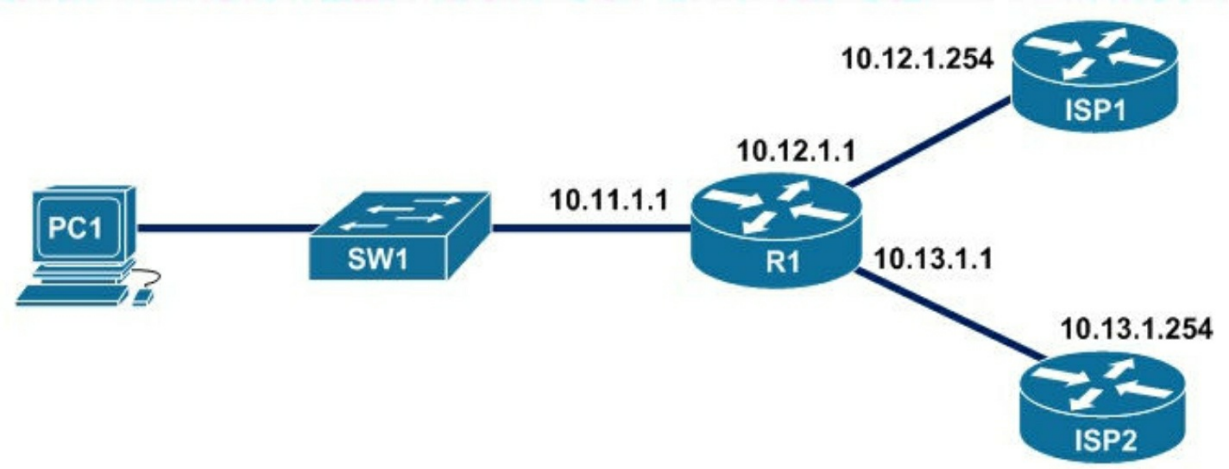
29. Which of the following is the correct use for the DHCPINFORM message?
A. Server-to-client communication refusing the request for configuration parameters.
B. Client-to-server communication, indicating that the network address is already in use.
C. Server-to client communication parameters, including committed network address.
D. Client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address.

30. Which three IP SLA performance metrics can you use to monitor enterprise-class networks?
(Choose three.)
A. Packet loss
B. Delay
C. bandwidth
D. Connectivity
E. Reliability
F. traps

31. Which IP SLA operation can be used to simulate voice traffic on a network?
A. TCP connect
B. UDP-jitter
C. ICMP-echo
D. ICMP-jitter

32. Which location within the network is preferred when using a dedicated route for Cisco IP SLA
operations?
A. user edge
B. provider edge
C. access edge

D. distribution edge



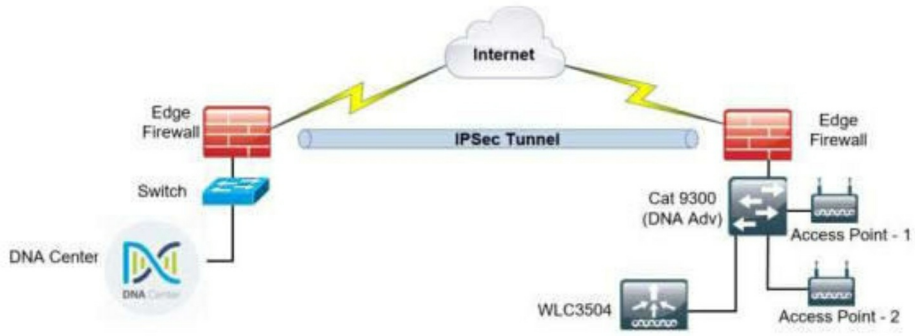
33. Refer to the exhibit. R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?

R1
ip sla 100
icmp-echo 10.12.1.254
!
track 10 ip sla 100 reachability
!
ip route 0.0.0.0 0 0.0.0.0 10.12.1.254 track 10
ip route 0.0.0.0 0 0.0.0.0 10.13.1.254 10
!
R1#show ip route
(output omitted)
Gateway of last resort is 10.13.1.254 to network 0.0.0.0
S* 0.0.0.0/0 [10/0] via 10.13.1.254
10.0.0.0 is variably subnetted, 6 subnets, 2 masks
C 10.11.1.0/24 is directly connected, GigabitEthernet0/1
L 10.11.1.1/24 is directly connected, GigabitEthernet0/1
C 10.12.1.0/24 is directly connected, GigabitEthernet0/0

L 10.12.1.1/24 is directly connected, GigabitEthernet0/1
C 10.13.1.0/24 is directly connected, GigabitEthernet0/2
L 10.13.1.0/24 is directly connected, GigabitEthernet0/2

A. Fix route dampening configured on the router.
B. Replace the SFP module because it is not supported.
C. Fix IP Event Dampening configured on the interface.
D. Correct the IP SLA probe that failed.

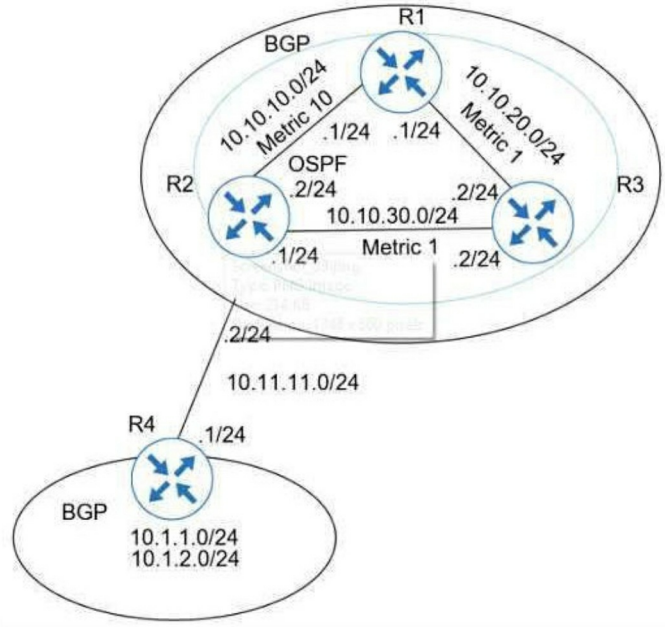
34. Refer to the exhibit. A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [error "uncontactable" when the administrator tries to add it in Cisco DNA Center. Which action discovers WLC in Cisco DNA Center successfully?



A. Copy the .cert file from the Cisco DNA Center on the USB and upload it to the WLC 3504.
B. Delete the WLC 3504 from Cisco DNA Center and add it to Cisco DNA Center again.
C. Add the WLC 3504 under the hierarchy of the Catalyst 9300 connected devices.
D. Copy the .pern file from the Cisco DNA Center on the USB and upload it

to the WLC 3504.

35. Refer to the exhibit. A user has set up an IP SLA probe to test if a non SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?



ip sla 10
tcp connect 10.1.1.80
ip sla schedule 10 life 30 start time now

A. Re-issue the ip sla schedule command.
B. Add icmp-echo command for the host.
C. Add the control disable option to the tcp connect.

D. Modify the ip sla schedule frequency to forever.

36. Refer to the output. The administrator can see the traps for the failed login attempts, but cannot
see the traps of successful login attempts. What command is needed to resolve the issue?

login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog

snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog

A. Configure logging history 2
B. Configure logging history 3
C. Configure logging history 4
D. Configure logging history 5

37. Which of the following is the correct use for the DHCPACK message?
A. Server-to-client communication refusing the request for configuration parameters.
B. Client-to-server communication, indicating that the network address is already in use.
C. Server-to client communication parameters, including committed network address.
D. Client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address.

38. Which of the following is the correct use for the DHCPDECLINE message?
A. Server-to-client communication refusing the request for configuration parameters.
B. Client-to-server communication, indicating that the network address is

already in use.
C. Server-to client communication parameters, including committed network address.
D. Client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address.

39. Which of the following is the correct use for the DHCPNAK message?
A. Server-to-client communication refusing the request for configuration parameters.
B. Client-to-server communication, indicating that the network address is already in use.
C. Server-to client communication parameters, including committed network address.
D. Client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address.

Chapter 4: Answers

1. Which section of Cisco DNA Center is dedicated to proactive issue detection?

B. Assurance

With telemetry capabilities across the broadest sources of inputs, IT can proactively monitor and be notified of network conditions that require attention, helping ensure that the network operation is delivering on the intent of services, policies, and security.

2. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?

A. Analytics

Cisco DNA Assurance collects streaming telemetry from devices around the network and uses AI and machine learning to help ensure alignment of network operations with business intent. In doing this, Cisco DNA Assurance optimizes network performance,

3. Which well-known port number is commonly used to move files and images between a Cisco router and a TFTP server?

B. UDP 69

Trivial File Transfer Protocol (TFTP) is a standard used for transferring files. This protocol uses UDP communication over well-known port 69, as opposed to File Transfer Protocol (FTP) which uses TCP for communication over well-known port 21. The UDP communication used with TFTP makes this a faster method of file transfer.

4. Which Syslog command will configure a Cisco device for logging at the Warning level, and also those levels considered to be more severe?

C. R1(config)# logging level 4

Syslog levels range from most severe Level 0 (Emergency) through

informational Level 7 (Debugging). Warning conditions are specified as Level 4 severity. Configuring a Cisco device for Syslog Level 4 (Warning) logging means that messages at Level 4 and those numerically lower are logged. This means that Levels 0-4 are collected, ranging from Emergency to Warning.

5. What is the general rule of thumb when using Cisco debug commands?

D. Use a debug command that is as specific as possible.

Debug commands have the ability to overwhelm system resources, because they can generate lots of information very quickly. It's a best practice to be as specific as possible when using debug commands, so as to limit the output to pertinent information.

6. Which Cisco IOS command allows us to specifically turn off conditional debugging that has been put in place for the GigabitEthernet 0/1 interface of a router?

C. R1# no debug condition interface gig 0/1

The command "no debug condition interface gig 0/1" will specifically remove conditional debugging that has been configured for the GigabitEthernet 0/1 interface. Although "no debug all" will also remove the condition, this also turns off all possible debugging in a global manner.

7. Below is a section of an IP SLA configuration that does not appear to be working properly. What should be done in order to correct the issue with the IP SLA probe?

R1# show ip sla con 1

***
Operation timeout (milliseconds): 5000
Type of operation to perform: udp-jitter
Target address/Source address: 10.1.1.50/0.0.0.0
Target port/Source port: 16500/0
Codec Packet size: 32
Control Packets: enabled
Schedule:

Operation frequency (seconds): 5
Next scheduled start time: Pending trigger
Group scheduled: FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE

***

C. Configure the start time.

The output snippet indicates that this probe has not yet started, as evidenced by the “Next scheduled start time: Pending Trigger” section. The probe needs to be started by either specifying a specific start time, or by using the “start-time now” option to immediately trigger the probe.

8. Which version of NetFlow features a fixed packet format?

D. NetFlow v9

NetFlow v5 has a fixed packet format that is always the same. This makes v5 compatible with most all NetFlow collection device and software packages. NetFlow v5 is the most popular version for this reason, although NetFlow v9 continues to gain popularity. NetFlow v9 features a dynamic packet format and uses templates to inform the NetFlow collector about the format of the flows being exported.

9. Which version of NetFlow would be preferred in a network using multicast media applications where ingress and egress monitoring is desired?

A. NetFlow v9

NetFlow v9 adds the ability to report on multicast traffic, both ingress and egress monitoring. Using NetFlow v9 allows you to add policies such as bandwidth restriction and quality of service rules to restrict multicast traffic.

10. Which version of NetFlow allows us to use multiple flow monitors and exporters simultaneously on the same traffic?

D. Flexible NetFlow

Flexible NetFlow allows for the exportation of multiple types of flow records

against the same traffic. This is useful in cases where two different departments might be interested in monitoring separate aspects of the network traffic, while keeping the flow records as concise as possible.

11. Which section of Cisco DNA Center is dedicated to proactive issue detection?

B. Assurance

The Assurance section of Cisco DNA Center uses artificial intelligence and machine learning to try and predict services issues in the network in a proactive manner. This works by collecting network telemetry from devices under the control of DNA Center in order to gain insights into the network.

12. Which tool within Cisco DNA Center Assurance allows us to collect network topology and routing data from discovered devices?

C. Path Trace

The Path Trace tool within Cisco DNA Center Assurance allows us to create a visual representation of the path between two hosts or Layer 3 interfaces. This essentially works as a graphical version of the traceroute command, displaying the path through our known topology.

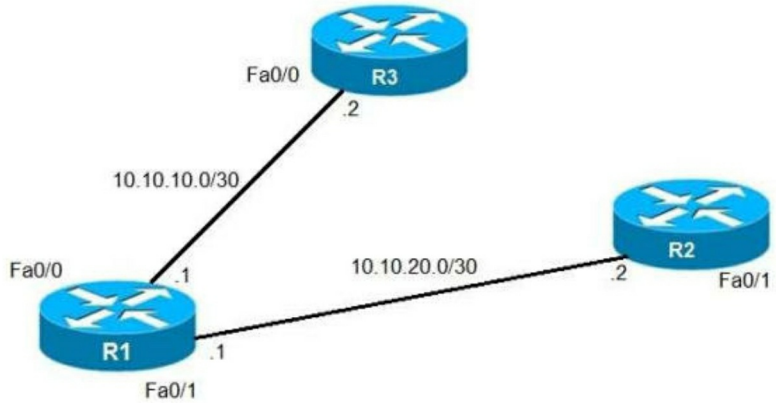
13. A network engineer is investigating a flapping (up/down) interface issue on a core switch that is
synchronized to an NTP server. Log output does not show the time of the flap.
Which command allows on the switch the time of the flap according to the clock on the device?

B. service timestamps log datetime localtime show-timezone

By default, Catalyst switches add a simple uptime timestamp to logging messages. This is a
cumulative counter that shows the hours, minutes, and seconds since the switch has been
booted up. For example:
20w2d: %LINK-3-UPDOWN: Interface FastEthernet1/0/27, changed state to down

21w3d: %SYS-5-CONFIG_I: Configured from console by vty0 (172.25.15.246)
At exactly what date and time did that occur? Who knows!
Instead, you can configure the switch to add accurate clock-like timestamps that are easily
interpreted. you can use the following command to begin using the switch clock as an accurate
timestamp for syslog messages:
Switch(config)# service timestamps log datetime [localtime] [showtimezone] [msec] [year]
Below is the output if we entered the command “service timestamps log datetime localtime showtimezone” (without”msec” keyword the output would not show time in milliseconds)
*Mar 1 00:02:24 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Loopback4, changed state to up

14. Refer to the exhibit. An IP SLA was configured on router R1 that allows the default route to be
modified in the event that Fa0/0 losses reachability with the router R3 Fa0/0 interface. The route has changed to flow through route R2. Which debug command is used to troubleshoot this issue?



C. debug ip routing

The “debug ip routing” command enables debugging messages related to the routing table. Since
the routing table is normally stable, you will only see debug messages when there are any
changes in the routing table.

15. Refer to the exhibit. 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?

```
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
```

D. Configure the DHCP lease time to a smaller value

The command “lease 0 12” set the duration of the lease (the time during which a client computer
can use an assigned IP address). The syntax is “lease {days[hours] [minutes] | infinite}”. In this
case the lease is (0 day) 12 hours.
We also notice that the pool of IP addresses that can issue to the clients are rather small as the
network 192.168.1.0/24 only supports 253 assignable IP addresses. But the first 49 IP addresses
were excluded so we only have 253 – 49 = 204 assignable IP addresses < 300 users.
Therefore the best solution is here to reduce the time of each issued IP address (to 2 hours
instead of 12 hours) as they only need to use in 2 hours per day, thus increasing the chance of
reuse the IP addresses for the clients.

16. When provisioning a device in Cisco DNA Center, the engineer sees the error message "Cannot
select the device. Not compatible with template.". What is the reason for the error?

D. The tag that was used to filter the templates does not match the device tag.

If you use tags to filter the templates, you must apply the same tags to the device to which you
want to apply the templates. Otherwise, you get the following error during provisioning: “Cannot
select the device. Not compatible with template.”

17. White working with software images, an engineer observes that Cisco DNA Center cannot upload
its software image directly from the device. Why is the image not uploading?

C. The software image for the device is in install mode.

When a device is in Install Mode, Cisco DNA Center is unable to upload its software image
directly from the device. When a device is in install mode, you must first manually upload the
software image to the Cisco DNA Center repository before marking the image as golden.

18. Refer to the exhibit. 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?

```
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) #
```

C. Enter the logging console debugging configuration command.

The logging console is a default and hidden command.

19. An engineer is trying to copy an IOS file from one router to another router by using TFTP.
Which two actions are needed to allow the file to copy? (Choose two).

C. Enable the TFTP server on the source router with the tftp-server flash:<filename> command.

E. Copy the file to the destination router with the copy tftp: flash: command

Below are the steps to follow for copying the Cisco IOS software image from a router acting as
TFTP server to another router.
1. Check the image size on Router1 with the show flash command.
2. Check the image size on Router2 with the show flash command to verify if enough space is
available on Router2 for the system image file to be copied.
3. Configure Router1 as the TFTP server: Router1(config)#tftp-server flash:/c2500-js-l.122-10b
4. When the TFTP server is configured, download the specified image from Router1 to Router2
using the copy tftp flash command.

20. A network engineer needs to verify IP SLA operations on an interface that shows on indication of excessive traffic. Which command should the engineer use to complete this action?

B. show track

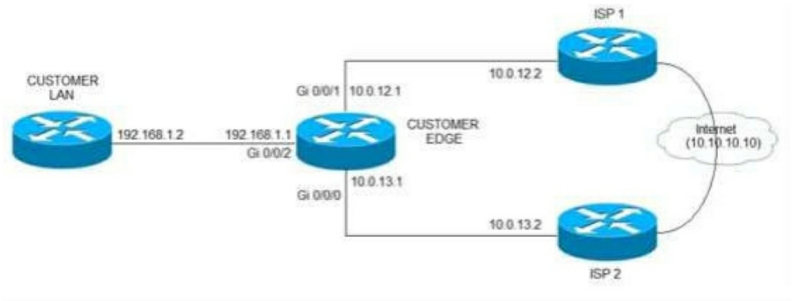
Use the show track command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

21. An engineer configured the wrong default gateway for the Cisco DNA center enterprise interface
during the install. Which command must the engineer run to correct the configuration?

C. Sudo maglev-config update

Once the appliance is configured, you cannot use the Configuration Wizard to change all Cisco
DNA Center appliance settings. Changes are restricted to the following settings only:
+ Host IP address of the appliance
+ DNS server IP addresses
+ Default gateway IP address
Procedure
Using a Secure Shell (SSH) client, log into the IP address of the Enterprise port of the Cisco DNA
Center appliance that needs to be reconfigured, on port 2222. For example:
ssh maglev@Enterprise-port's-IP-address -p 2222
Step 2
When prompted, enter the Linux Password.
Step 3
Enter the following command to access the Configuration Wizard.
$ sudo maglev-config update
If prompted for the Linux Password, enter it again.

22. Refer to the exhibit. ISP 1 and ISP 2 directly connect to the internet. A customer IS tracking both ISP links to achieve redundancy and cannot see the Cisco IP SLA tracking output on the router console. Which command is missing from the IP SLA configuration?



A. Start-time now

Although the IP SLA tracking has been configured but it needs to activate with the “start-time
now” keyword. An example of configuring IP SLA for ICMP echo and start it immediately is
shown below:
ip sla 2
icmp-echo 10.10.10.10
!
ip sla schedule 2 start-time now

23. Refer to the exhibit. An administrator noticed that after a change was made on R1, the timestamps on the system logs did not match the clock. What is the reasons for this error?

```
service timestamps debug datetime msec
service timestamps log datetime
clock timezone MST -7 0
clock summer-time MST recurring
ntp authentication-key 1 md5 00101A0B01521812062247470 71E 7
ntp server 10.10.10.10

R1#show clock
*06:13:44.045 MST Sun Dec 30 2018

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config) #logging host 10.10.10.20
R1(config) #end
R1#
*Dec 30 13:15:28: %SYS-5-CONFIG_I: Configured from console by console
R1#
*Dec 30 13:15:28: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.10.20 port 514
started – CLI initiated
```

A. The keyword localtime is defined on the timestamp service

command.

By default, syslog and debug messages are stamped by UTC, regardless of the time zone that
device configured. You should append localtime key word to "service timestamp {log | debug}
datetime msec" global command to change that behavior.

24. 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).

B. The DHCP server IP address configuration is missing locally.
E. The route to the new DHCP server is missing.

25. Which command is used to check IP SLA when an interface is suspected to receive lots of traffic
with options?

A. show track

Use the show track command to display information about objects that are tracked by the tracking process. When no arguments or keywords are specified, information for all objects is displayed.

26. Refer to the exhibit. Why is the remote NetFlow server failing to receive the NetFlow data?

```
config t
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exit
!
ip cef
!
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

A. The flow exporter is configured but is not used.

The exporter is not configured under the flow monitor.

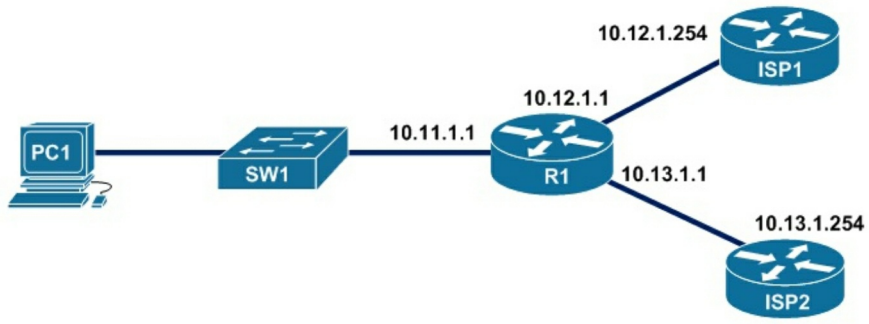
27. Refer to the exhibit. An IP SLA is configured to use the backup default route when the primary is down, but it is not working as desired. Which command fixes the issue?

```
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
```

D. R1(config)# ip route 0.0.0.0.0.0.0.1.1.1.1 track 1

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.

28. Refer to the exhibit. An engineer is monitoring reachability of the configured default routes to ISP1 and ISP2. The default route from ISP1 is preferred if available. How is this issue resolved?



D. Start IP SLA by defining frequency and scheduling it.

In the above configuration we have not had activated our IP SLA operation. We can start it with
this command:
R1(config)#ip sla schedule 100 life forever start-time now
Also we should specific the rate of ICMP echo:
R1(config-ip-sla-echo)#frequency 5 // Send ICMP echo every 5 seconds

29. Which of the following is the correct use for the DHCPINFORM message?

D. Client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address.

DHCPINFORM: If a client has obtained a network address through some other means or has a
manually configured IP address, a client workstation may use a DHCPINFORM request message
to obtain other local configuration parameters, such as the domain name and Domain Name
Servers (DNSs). DHCP servers receiving a DHCPINFORM message construct a DHCPACK
message with any local configuration parameters appropriate for the client

without allocating a
new IP address. This DHCPACK will be sent unicast to the client.

30. Which three IP SLA performance metrics can you use to monitor enterprise-class networks?
(Choose three.)

A. Packet loss
B. Delay
D. Connectivity

Performance metrics collected by IP SLAs operations include the following
* Delay (both round-trip and one-way)
* Jitter (directional)
*Packet loss (directional)
*Packet sequencing (packet ordering)
* Path (per hop)
*Connectivity (directional)
*Server or website download time
* Voice quality scores

31. Which IP SLA operation can be used to simulate voice traffic on a network?

B. UDP-jitter

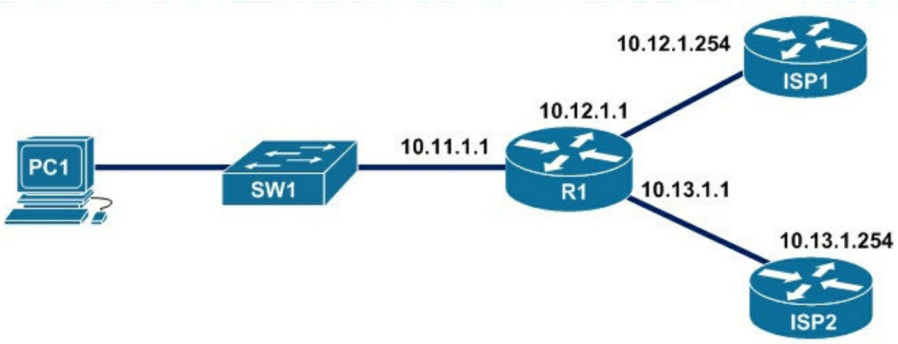
The IP SLA VoIP UDP jitter operation can simulate voice traffic by using common codecs and UDP traffic that are similar to real VoIP traffic.

32. Which location within the network is preferred when using a dedicated route for Cisco IP SLA
operations?

D. distribution edge

The dedicated or SLAs router is used exclusively for Cisco IOS IP SLA operations and is connected to the edge routers to simulate the customer network traffic. Cisco IP SLA routers are particularly useful for Point-Of-Presence (POP) or hub sites to gain access to router monitoring, which requires thousands of Cisco IOS IP SLA probes.

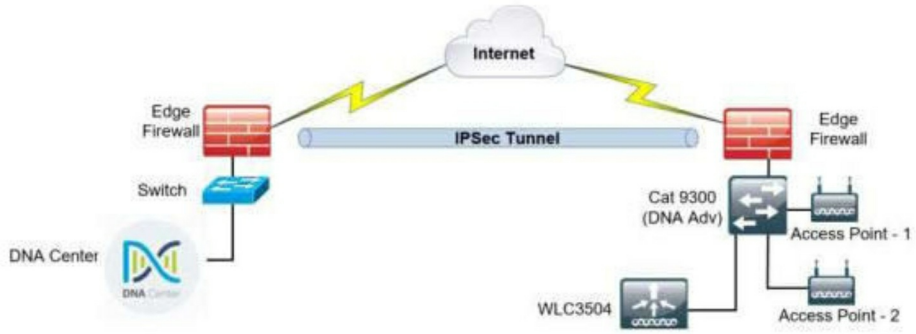
33. Refer to the exhibit. R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?



R1
ip sla 100
icmp-echo 10.12.1.254
!
track 10 ip sla 100 reachability
!
ip route 0.0.0.0 0 0.0.0.0 10.12.1.254 track 10
ip route 0.0.0.0 0 0.0.0.0 10.13.1.254 10
!
R1#show ip route
(output omitted)
Gateway of last resort is 10.13.1.254 to network 0.0.0.0
S* 0.0.0.0/0 [10/0] via 10.13.1.254
10.0.0.0 is variably subnetted, 6 subnets, 2 masks
C 10.11.1.0/24 is directly connected, GigabitEthernet0/1
L 10.11.1.1/24 is directly connected, GigabitEthernet0/1
C 10.12.1.0/24 is directly connected, GigabitEthernet0/0
L 10.12.1.1/24 is directly connected, GigabitEthernet0/1
C 10.13.1.0/24 is directly connected, GigabitEthernet0/2
L 10.13.1.0/24 is directly connected, GigabitEthernet0/2

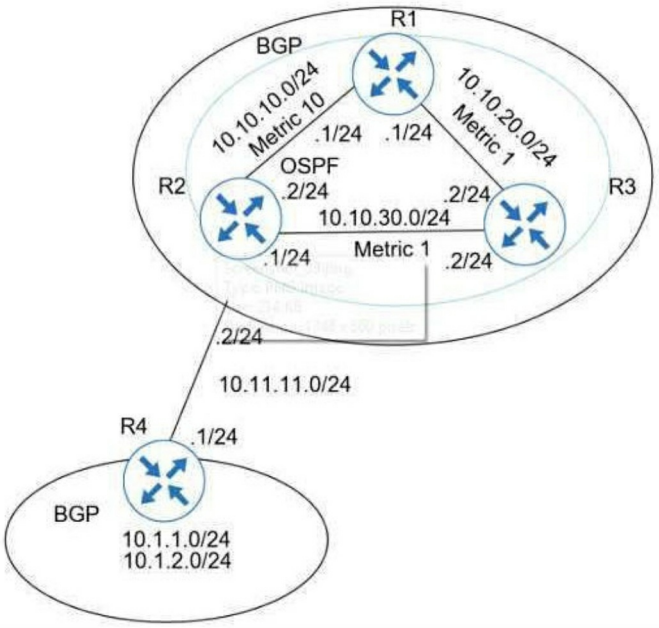
C. Fix IP Event Dampening configured on the interface.

34. Refer to the exhibit. A network administrator is discovering a Cisco Catalyst 9300 and a Cisco WLC 3504 in Cisco DNA Center. The Catalyst 9300 is added successfully However the WLC is showing [error "uncontactable" when the administrator tries to add it in Cisco DNA Center. Which action discovers WLC in Cisco DNA Center successfully?



D. Copy the .pern file from the Cisco DNA Center on the USB and upload it to the WLC 3504.

35. Refer to the exhibit. A user has set up an IP SLA probe to test if a non SLA host web server on IP address 10.1.1.1 accepts HTTP sessions prior to deployment. The probe is failing. Which action should the network administrator recommend for the probe to succeed?



ip sla 10
tcp connect 10.1.1.80
ip sla schedule 10 life 30 start time now

A. Re-issue the ip sla schedule command.

When the group is scheduled to run, based on the scheduler, one IP SLAs operation is created for each destination address in the endpoint list. The operation type depends on the template in the group. If the group is deleted or unscheduled, the created IP SLAs operations are removed and must be re-issued.

36. Refer to the output. The administrator can see the traps for the failed login

attempts, but cannot
see the traps of successful login attempts. What command is needed to resolve the issue?

login block-for 15 attempts 10 within 120
login on-failure log
login on-success log
archive
log config
logging enable
logging size 300
notify syslog

snmp-server enable traps syslog
snmp-server host 172.16.17.1 public syslog

D. Configure logging history 5

By default, the maximum severity sent as a syslog trap is warning. That is why you see syslog
traps for login failures. Since a login success is severity 5 (notifications), those syslog messages
will not be converted to traps. To fix this, configure: login block-for seconds attempts tries within seconds.

37. Which of the following is the correct use for the DHCPACK message?

C. Server-to client communication parameters, including committed network address.

DHCPACK: After the DHCP server receives the DHCPREQUEST, it acknowledges the request
with a DHCPACK message, thus completing the initialization process.

38. Which of the following is the correct use for the DHCPDECLINE message?

B. Client-to-server communication, indicating that the network address is already in use.

DHCPDECLINE: The client receives the DHCPACK and will optionally

perform a final check on
the parameters. The client performs this procedure by sending Address Resolution Protocol
(ARP) requests for the IP address provided in the DHCPACK. If the client detects that the
address is already in use by receiving a reply to the ARP request, the client will send a
DHCPDECLINE message to the server and restart the configuration process by going into the
Requesting state.

39. Which of the following is the correct use for the DHCPNAK message?

A. Server-to-client communication refusing the request for configuration parameters.

DHCPNAK: If the selected server is unable to satisfy the DHCPREQUEST message, the DHCP
server will respond with a DHCPNAK message. When the client receives a DHCPNAK message,
or does not receive a response to a DHCPREQUEST message, the client restarts the
configuration process by going into the Requesting state. The client will retransmit the
DHCPREQUEST at least four times within 60 seconds before restarting the Initializing state.