OSPF & EIGRP Questions

https://www.networktut.com/ospf-eigrp-questions

Question 1

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

Answer: B (?)

Explanation

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 **router-id** *ospf-process-ID* command).

OSPFv3 New-Style OSPF Configuration Commands:

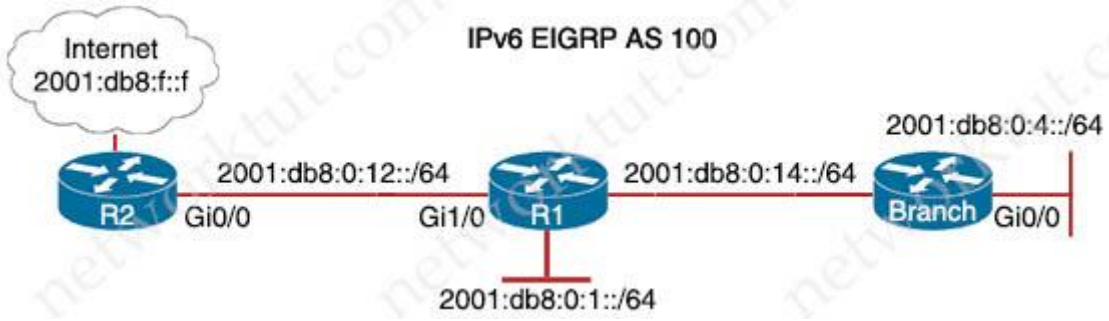
```
R1(config)#ipv6 unicast-routing //although only OSPFv3 for IPv4 is configured but we have to enable IPv6 under global configuration mode
R1(config)#router ospfv3 1
R1(config-router)# router-id 1.1.1.1
R1(config)#interface GigabitEthernet0/1
R1(config-if)#ipv6 enable //although only OSPFv3 for IPv4 is configured but we have to enable IPv6 under interface mode
R1(config-if)#ospfv3 1 ipv4 area 0
```

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)#.

Reference: https://www.ciscopress.com/articles/article.asp?p=2294214&seqNum=4

Question 2

Refer to the exhibit. User in the branch network of 2001:db8:0:4 report 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** EIGRP-IPv6 Topology Table for AS(100)/ID(10.1.12.1) Codes: P – Passive, A – Active, U – Update, Q – Query, R – Rely, 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, GigabitEthernet0/0	Branch#**show ipv6 eigrp topology** EIGRP-IPv6 Topology Table for AS(100)/ID(4.4.4.4) Codes: P – Passive, A – Active, U – Update, Q – Query, R – Rely, 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

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

Answer: B

Explanation

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.

Question 3

Refer to the exhibit. An engineer configuration 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 192.168.12.2,00:33:32, 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

Answer: A

Explanation

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

Question 4

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
Gateway of last resort is not set
```

```
        192.168.1.0/32 is subnetted, 1 subnets
O               192.168.1.1[110/11] via 192.168.12.1,13:32:22, 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

Answer: D

Explanation

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**."

Reference: CCNP Route 642-902 Official Certification Guide

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

+ An example of using the command “summary-address” is shown below:

Recently the RIPv2 domain has been redistributed into our OSPF domain but the administrator wants to configure a summarized route instead of 32 external type-5 LSAs (for 172.16.32.0/24 to 172.16.63.0/24) flooding into the OSPF network. In this case the administrator has to use the “summary-address” command as follows:

Router(config-router)#summary-address 172.16.32.0 255.255.224.0

Note: In this case R1 is the ASBR for OSPF domain.

BGP Questions

https://www.networktut.com/bgp-questions

Question 1

Refer to the exhibit. R2 is a route reflector, and R1 and R3 are route reflector clients. The router R2 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?

```
R2#show ip bgp
BGP table version is 4, local router ID is 209.65.200.225
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
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    ?
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 01:00:18         0
```

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

Answer: D

Explanation

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.

Question 2

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 LIMIT_BGP
 Class BGP
  Average Rate Traffic Shaping
  cir 10000000 (bps)

Policy Map POLICY_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

Answer: D

Explanation

The “conform-action” specifies the action to take on packets that conform to the rate limit and the “exceed-action” specifies the action to be taken on packets when the packet rate is greater than the rate specified in the maximum-burst-bytes argument.

Question 3

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 10.222.10.1?

```
<exhibit missing>
```

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

Answer: ?

Question 4

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, 193843 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, 64484847 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”

Answer: D

Question 5

Refer to the exhibit, in which circumstance does the BGP neighbor remain in the idle condition?

```
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#
```

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

Answer: D

Explanation

Idle (PfxCt) means the session is in the Idle state because the neighbor has sent more prefixes than the configured maximum-prefixes limit.

```
router bgp 100
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 maximum-prefix 10 80
```

In the last command, “10” is the maximum number of prefixes allowed from the neighbor and the router starts to generate a warning message at 80%.

Reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/25160-bgp-maximum-prefix.html

Therefore if the BGP neighbor sent 11 prefixes, the local router will be in Idle (PfxCt) state.

Route-map Questions

https://www.networktut.com/route-map-questions

Question 1

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

```
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 65000
```

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?

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

Answer: A

Explanation

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.

Question 2

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 is still present in the routing table as an OSPF route. Which action blocks the route?

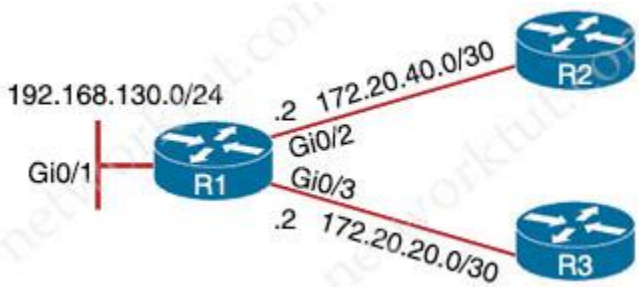
```
Router#show access-lists
Standard IP access list 1
    10 permit 192.168.2.2 (1 match)
Router#
Router#show route-map
route-map RM-OSPF-DL, permit, sequence 10
  Match clauses:
    ip address (access-lists): 1
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
Router#
Router#show running-config | 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

Answer: C

Question 3

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 17.20.20.0/30 network?



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 Gi0/2
ip policy route-map test
!
route-map test permit 10
match ip address 1
set ip next-hop 172.20.20.1

C. 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

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

E. 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 172.20.20.1
```

Answer: E

Explanation

The traffic reaches Gi0/1 interface so we must apply policy ("ip policy route-map test") on this interface. The question requires to reach the destination of 172.20.20.0/30 so the next-hop IP address should be 172.20.20.1.

Redistribution Questions

https://www.networktut.com/redistribution-questions

Question 1

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 ospf 1
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

Answer: B

Question 2

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 list TO-OSPF

Answer: A

Explanation

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-list-name [access-list-number…| access-list-name] | **prefix-list** prefix-list-name [prefix-list-name…]}

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/iproute_pi/command/reference/iri_book/iri_pi1.html

Question 3

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

Answer: A

Explanation

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.

Question 4

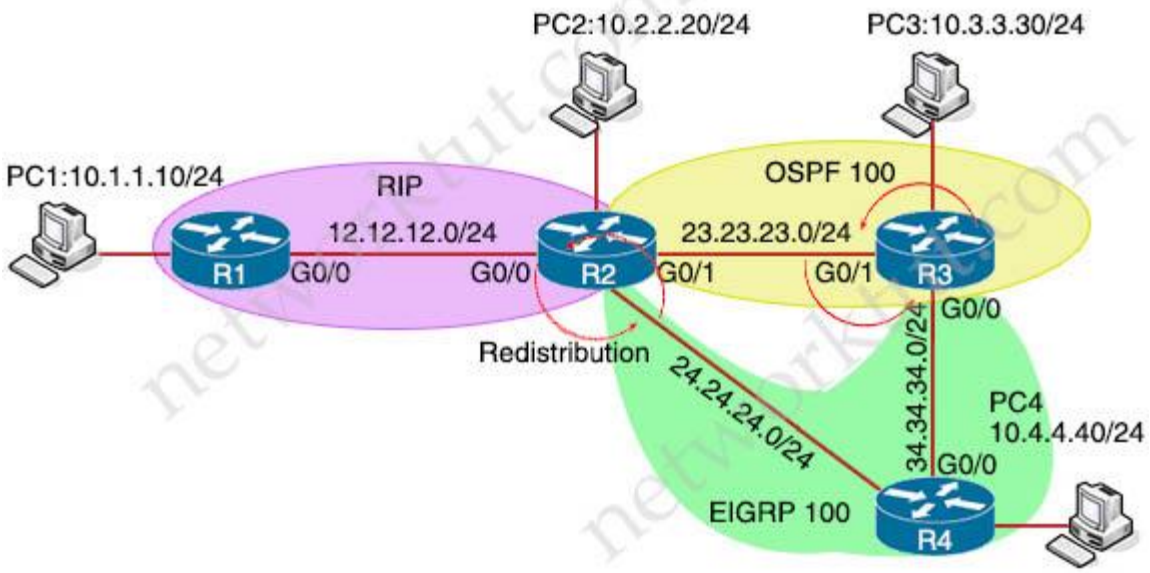
Which two statements about redistributing EIGRP into OSPF are true? (Choose two)

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

Answer: B F

Question 5

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.

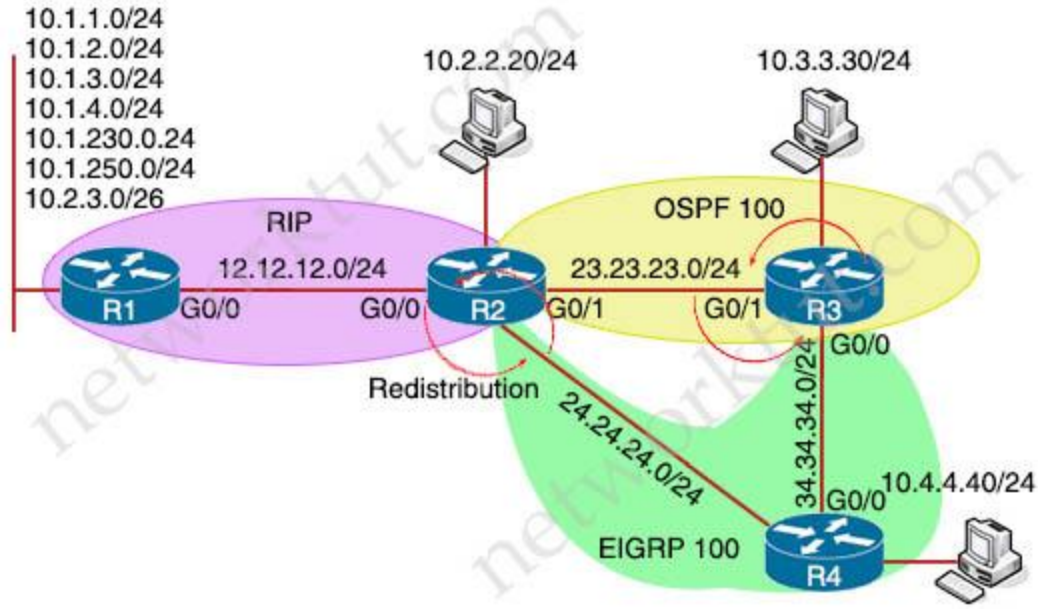
Answer: A

Explanation

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.

Question 6

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 le 24
!
ip prefix-list OSPF-TAG-PRF-1 seq 5 permit 10.2.0.0/18 le 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
B. 10.1.4.0/24
C. 10.1.2.0/24
D. 10.2.3.0/26

Answer: A

Explanation

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 OSPF-TAG-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.

Question 7

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?

```
O E2      10.0.0.0 [110/20] via 192.168.12.2, 00:00:33, Ethernet0/0
O   192.168.3.0/24 [110/20] via 192.168.12.2, 00:00:43, 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

Answer: A

Explanation

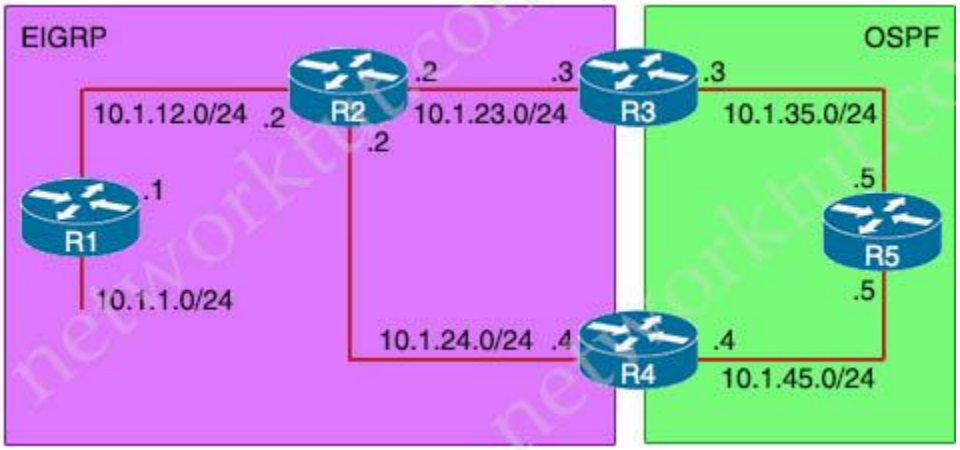
If you configure the redistribution of OSPF into BGP without keywords, only OSPF intra-area and inter-area routes are redistributed into BGP, by default.

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"

Reference: https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/5242-bgp-ospf-redis.html

Question 8

Refer to the exhibit The output of the trace from R5 shows a loop in the network.



R1 router eigrp 1 redistribute connected network 10.1.12.1 0.0.0.0 ——————————— R3 router ospf 1 redistribute eigrp 1 network 10.1.35.3 0.0.0.0 area 0 ——————————— R4 router eigrp 1 redistribute ospf 1 metric 2000000 1 255 1 1500 ! router ospf 1 network 10.1.45.4 0.0.0.0 area 0	R5#traceroute 10.1.1.1 Type escape sequence to abort. Tracing the route to 10.1.1.1 1 10.1.35.3 80 msec 44 msec 20 msec 2 10.1.23.2 44 msec 104 msec 64 msec 3 10.1.24.4 44 msec 64 msec 40 msec 4 10.1.45.5 24 msec 40 msec 20 msec 5 10.1.35.3 92 msec 144 msec 147 msec 6 10.1.23.2 103 msec 77 msec 88 msec —output omitted—

Which configuration prevents this loop?

A. R3
router ospf 1
redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG deny 10
set tag 1
———————————————————————————————-
R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
match tag 1

B. R3
router eigrp 1
redistribute ospf 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
set tag 1

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

R4
router eigrp 1
redistribute ospf 1 metric 2000000 1 255 1 1500 route-map FILTER-TAG
!
route-map FILTER-TAG deny 10
match tag 1
route-map FILTER-TAG permit 20

D. R3
router ospf 1
redistribute eigrp 1 subnets route-map SET-TAG
!
route-map SET-TAG permit 10
set tag 1

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

Answer: B

Explanation

In this topology, we are doing mutual redistribution at multiple points (between OSPF and EIGRP on R3 & R4), which is a very common cause of network problems, especially routing loops so you should use route-map to prevent redistributed routes from redistributing again into the original domain.

In this question, route-map is also used for this purpose. In particular, 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 tag 1 set:

```
R4
route-map FILTER-TAG deny 10
match tag 1
```

MPLS Questions

https://www.networktut.com/mpls-questions

Question 1

Which transport layer protocol is used to form LDP sessions?

A. UDP
B. SCTP
C. TCP
D. RDP

Answer: C

Explanation

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.

Reference: https://tools.ietf.org/html/rfc5036

Question 2

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

Answer: B

Question 3

Which command allows traffic to load-balance in an MPLS Layer 3 VPN configuration?

A. Multi-paths eibgp 2
B. Maximum-paths ibgp 2
C. Multi-paths 2
D. Maximum-paths 2

Answer: D

Explanation

The command "maximum-paths [ibgp] *number-of-paths*" configures the maximum number of multipaths allowed. Use the **ibgp** keyword to configure iBGP load balancing. This question does not tell which BGP load-balance it wants (iBGP or eBGP) so in fact answer B is also correct.

Question 4

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

Answer: D

Explanation

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

Note: pop means "remove the top MPLS label"

Question 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

Answer: A

Explanation

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)

Question 6

What statement about route distinguishes 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

Answer: B

Explanation

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
```

We can see the IP addresses on Gi0/1 & Gi0/2 interfaces are overlapping but there is no problem with it as the RDs are different.

VRF-Lite Questions

https://www.networktut.com/vrf-lite-questions

Question 1

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

Answer: A

Explanation

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
```

Question 2

Which protocol does VRF-Lite support?

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

Answer: C

Question 3

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

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

Answer: B E

Question 4

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

A. It extends the IP address to identify which VRF 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

Answer: A

Explanation

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.

Question 5

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

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

Answer: B

Question 6

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

Answer: C

Explanation

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

DMVPN Questions

https://www.networktut.com/dmvpn-questions

Question 1

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

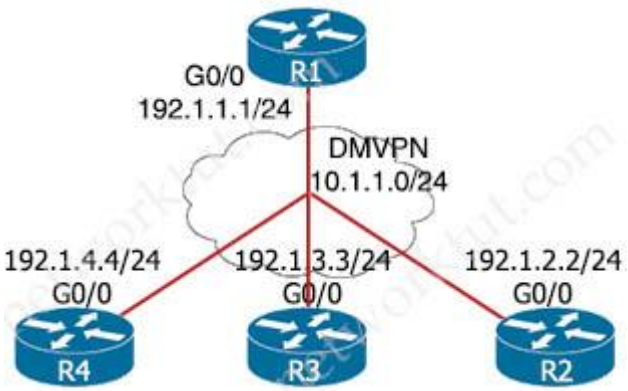
Answer: A

Explanation

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.

Question 2

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



On R2:	On R3:	On R4:
R2(config)#interface tunnel 1 R2(config-if)#ip address 10.1.1.2 255.255 255.0 R2(config-if)#tunnel source FasEthernet0/0 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 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-ff)#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

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 redirect commands is missing on the hub router.
D. The ip shortcut commands is missing on the hub router.
E. The ip nhrp command is missing on the hub router.

Answer: B C

Explanation

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 next-hop value for a remote spoke network from the default initial hub tunnel IP address to the NHRP resolved remote spoke tunnel IP address)

Question 3

Refer to the following output:

```
Router#show ip nhrp detail
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
Type: dynamic, Flags: authoritative unique nat registered used
NBMA address: 10.12.1.2
```

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

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

Answer: A

Explanation

From the output we learn that the logical address 10.2.1.2 is mapped to the NBMA address 10.12.1.2. Type "dynamic" means NBMA address was obtained from NHRP Request packet whilw type "static" means NBMA address is statically configured. The "authoritative" flag means that the NHRP information was obtained from the Next Hop Server (NHS).

Reference:
http://www.cisco.com/c/en/us/td/docs/ios/12_4/ip_addr/configuration/guide/hadnhrp.html

Question 4

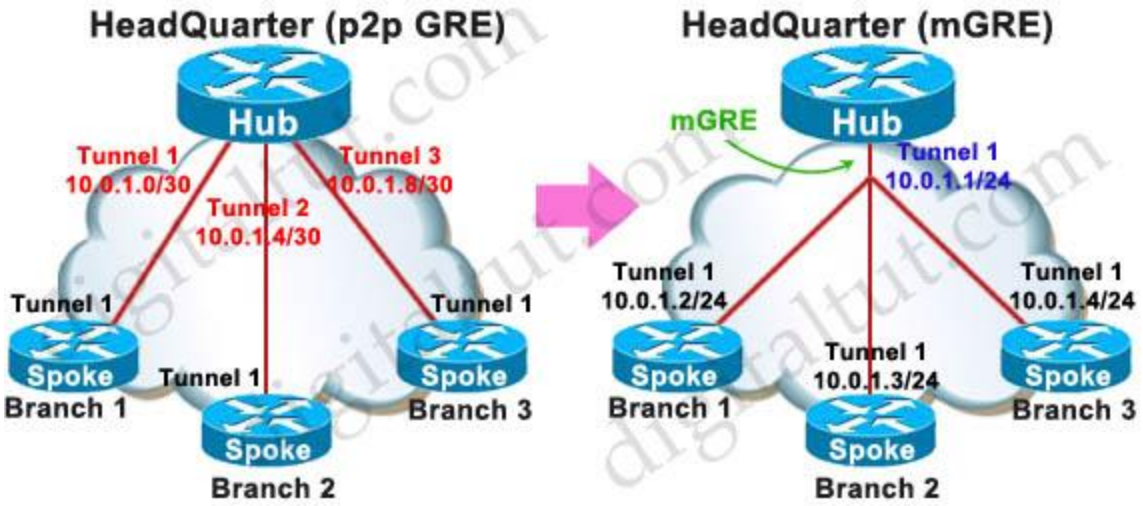
Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?

A. DMVPN
B. GETVPN
C. Cisco Easy VPN
D. FlexVPN

Answer: A

Explanation

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.



mGRE tunnel is treated as a non-broadcast multi-access (NBMA) environment. mGRE tunnel does not have to be configured with a tunnel destination so we need another protocol to take care of the destination addresses. In this case NHRP is used for NBMA environment.

Question 5

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

Answer: D

Explanation

Maybe this question wanted to ask "Which protocol is used in a DMVPN network to **map logical IP address to physical IP addresses**?"

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).

Question 6

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

A. DMVPN
B. MPLS VPN
C. Virtual Tunnel Interface (VTI)
D. SSL VPN
E. PPPoE

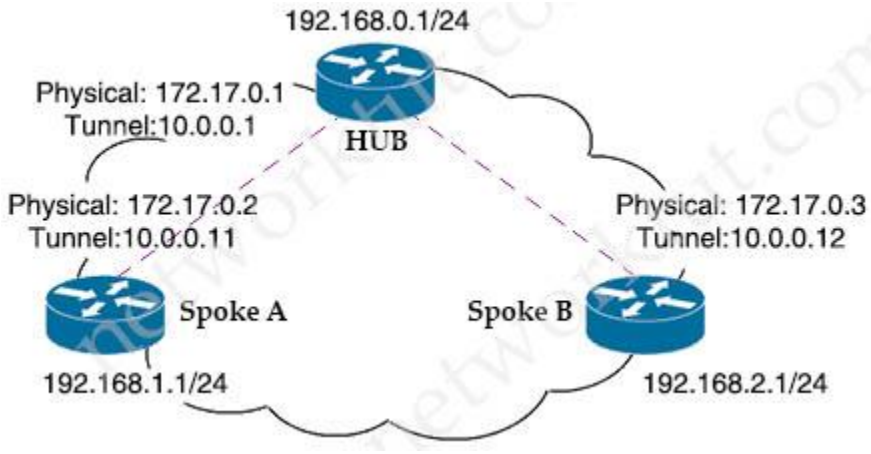
Answer: A C

Explanation

Reference: 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.

Question 7

Refer to the exhibit. Which interface configuration must be configured on the spoke A 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 destination FastEthernet0/0
tunnel mode gre multipoint

B. 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 10.0.0.11 172.17.0.2
tunnel mode gre

C. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp map multicast static
ip nhrp network-id 1
tunnel source 10.0.0.1
tunnel mode gre multipoint

D. interface Tunnel0
ip address 10.0.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source FastEthernet0/0
tunnel mode gre multipoint
ip nhrp nhs 10.0.0.1
ip nhrp map 10.0.0.1 172.17.0.1

Answer: D

Explanation

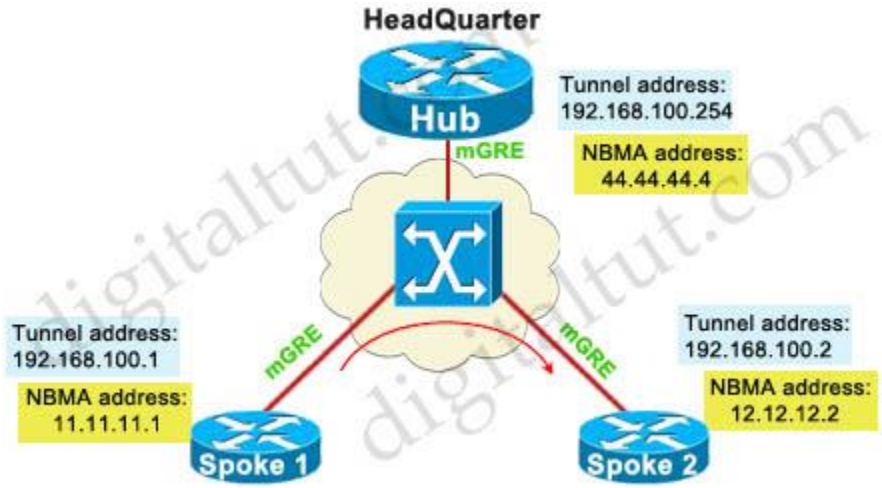
The command "ip nhrp map multicast dynamic" should be only used on Hub router, not spoke. If we are running dynamic routing protocols based on multicast (like RIP, OSPF, EIGRP …) we have to add the command "**ip nhrp map multicast dynamic**" in Hub to replicate all multicast traffic to all dynamic entries 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 B 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 C 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 D is correct. The " tunnel source FastEthernet0/0″ is equivalent to "tunnel source 172.17.0.2", which is the NBMA address of Spoke A.

An example of configuring DMVPN Phase II – Dynamic Mapping is shown below:



DMVPN Phase II – Dynamic Mapping **Hub** interface tunnel 1 ip address 192.168.100.254 255.255.255.0 tunnel source 44.44.44.4 tunnel mode gre multipoint ip nhrp network 10	**Spoke 1** interface tunnel 1 ip address 192.168.100.1 255.255.255.0 tunnel source 11.11.11.1 tunnel mode gre multipoint ip nhrp network 10 ip nhrp map 192.168.100.254 44.44.44.4 ip nhrp nhs 192.168.100.254 !	**Spoke 2** interface tunnel 1 ip address 192.168.100.2 255.255.255.0 tunnel source 12.12.12.2 tunnel mode gre multipoint ip nhrp network 10 ip nhrp map 192.168.100.254 44.44.44.4 ip nhrp nhs 192.168.100.254

If you want to learn more about DMVPN please read our DMVPN Tutorial.

Question 8

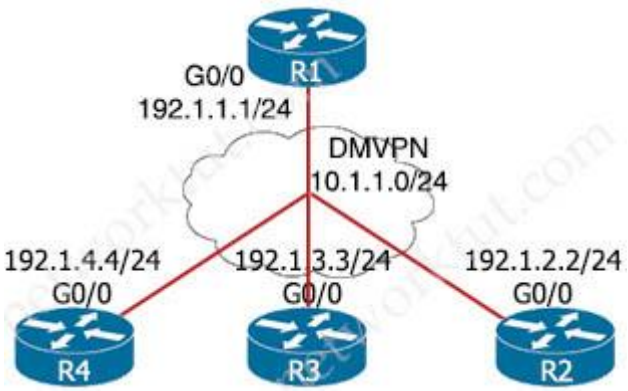
Which security feature can protect DMVPN tunnels?

A. IPsec
B. TACACS+
C. RTBH
D. RADIUS

Answer: A

Question 9

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 resolved the issue? (Choose two)



R2:	**R3:**
R2(config)#crypto isakmp policy 10 R2(config-isakmp)#hash md5 R2(config-isakmp)#authentication pre-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-md5-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 E2(config-if)#tunnel protection ipsec profile TST	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
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

Answer: A B

Explanation

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 <transform-set-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

There is an issue with above configuration in both R2 & R3: both R2 and R3 use the DMVPN tunnel address 10.1.1.1 (in the command "crypto isakmp key cisco address 10.1.1.1". This is the tunnel interface IP address which is not correct. They must use the WAN address 192.1.1.1 instead.

We should configure the key with "address 0.0.0.0 0.0.0.0" (means remote peer is any -> any destination can try to negotiate with this router). While the hub's public IP address is known we must keep in mind that R2 and R3 can build dynamic VPN tunnel between them. Taking into consideration that their public IP address is dynamic it is imperative to use 0.0.0.0 0.0.0.0 for the remote peer.

AAA Questions

https://www.networktut.com/aaa-questions

Question 1

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” in the aaa authentication login Console local command
D. Add the aaa authentication login default none command to the global configuration

Answer: B

Explanation

The keyword “local-case” will use case-sensitive local username for authentication so it will not solve this problem -> Answer A is not correct.

We test answer B on R1, answer C on R2 (also turned on debugging for AAA authentication via the “debug aaa authentication” command):

On R1:

So after adding the “login authentication Console” line under line configuration, AAA will prefer the authentication method listed under specific line configuration, which is “local” in this case.

On R2:

```
R2 con0 is now available



Press RETURN to get started.









User Access Verification

Username:
*Mar  1 00:17:22.743: %AAA-3-BADSERVERTYPEERROR: Cannot process aut
hentication server type tacacs+ (UNKNOWN)
Username: cisco1
Password:

R2#sh run | in aaa
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication login console local
aaa session-id common
R2#sh run | sec line con
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
R2#
```


With two “aaa authentication login” commands, AAA prefers the default login method.

We also tried to put the “aaa authentication login console local” command in front of “aaa authentication login default group tacacs+ local” but the result is still the same.

About answer D, if we add “aaa authentication login default none” to the current configuration then the “aaa authentication login default group tacacs+ local” will be removed -> we can access this device without any authentication.

Question 2

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 (2546660185): 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

Answer: D

Explanation

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.

Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/13864-tacacs-pppdebug.html

NTP Questions

https://www.networktut.com/ntp-questions

Question 1

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 00101AOB015218120622474707lE 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 13:15:26: %SYS-S-CONFIG_I: Configured from console by console
R1#
*Dec 30 13:1S: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

Answer: B

Question 2

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?

```
*Feb 28 12:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Down User reset
*Feb 28 12:41:57: %BGP_SESSION-5-ADJCHANGE : neighbor 192.168.2.2 IPv4 Unicast
topology base removed from session User reset
*Feb 28 12:41:57: %BGP-5-ADJCHANGE: neighbor 192.168.2.2 Up
R1#show clock
*13:42:00.506 CET Feb 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

Answer: C

Explanation

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.

Question 3

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 dock on the device?

A. clock calendar-valid
B. service timestamps log datetime localtime show-timezone
C. service timestamps log uptime
D. dock summer-time mst recurring 2 Sunday mar 2:00 1 Sunday nov 2:00

Answer: B

Explanation

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] [show-timezone] [msec] [year]
```

Below is the output if we entered the command “service timestamps log datetime localtime show-timezone” (without”msec” keyword the output would not show time in milisecond)

```
*Mar  1 00:02:24 UTC: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
```

Note: The command "clock calendar-valid" enables the device to act as a valid time source to which network peers can synchronize. By default, the time maintained on the software clock is not considered to be reliable and will not be synchronized with NTP or VINES time service. To set the hardware clock as a valid time source, use this command.

Access-list Questions

https://www.networktut.com/access-list-questions

Question 1

Refer to the exhibit. 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

Answer: B

Question 2

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
!
int Gi0/0
ipv6 access-map 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
!
int Gi0/0
ipv6 traffic-filter 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 eq telnet
!
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 eq telnet
!
int Gi0/0
ipv6 traffic-filter Deny_Telnet in

Answer: D

Explanation

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.

Control Plane Questions

https://www.networktut.com/control-plane-questions

Question 1

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

Answer: A

Explanation

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:

```
R2# show policy-map control-plane
 Control Plane

  Service-policy input: CoPP_policy

    Class-map: Telnet_class (match-all)
      62 packets, 2866 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group name CoPP_traffic
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 62 packets, 2866 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps

    Class-map: class-default (match-any)
      38 packets, 2944 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

Question 2

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 at least 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

Answer: A

Explanation

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

Question 3

Which option is the best for protecting CPU utilization on a device?

A. fragmentation
B. COPP
C. ICMP redirects
D. ICMP unreachable messages

Answer: B

Explanation

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.

Reference: https://www.ciscopress.com/articles/article.asp?p=1181682&seqNum=10

Question 4

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

Answer: C E

Explanation

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.

Reference: https://www.cisco.com/c/en/us/support/docs/routers/2500-series-routers/15092-copyimage.html

IPv6 Questions

https://www.networktut.com/ipv6-questions

Question 1

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 stateful autoconfiguration addresses in Layer 3 neighbor tables
C. It learns and secures bindings for stateful autoconfiguration addresses in Layer 2 neighbor tables

D. It learns and secures binding for stateless autoconfiguration addresses in Layer 2 neighbor tables

Answer: D

Explanation

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.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ip6-nd-inspect.html

Question 2

Which statement about IPv6 RA Guard is true?

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

Answer: A

Explanation

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.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-xe-3s-book/ip6-ra-guard.html

IP SLA Questions

https://www.networktut.com/ip-sla-questions

Question 1

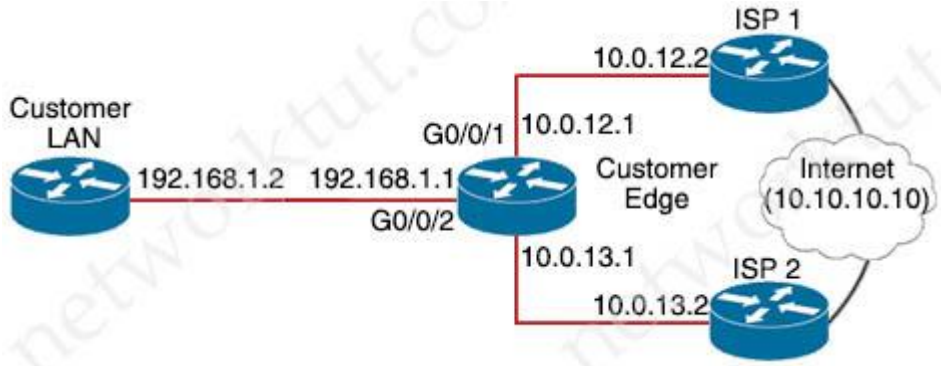
Which command is used to check IP SLA when an interface is suspected to receive lots of traffic with options?

A. show track
B. show threshold
C. show timer
D. show delay

Answer: A

Question 2

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

Answer: A

Explanation

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
```

Question 3

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?

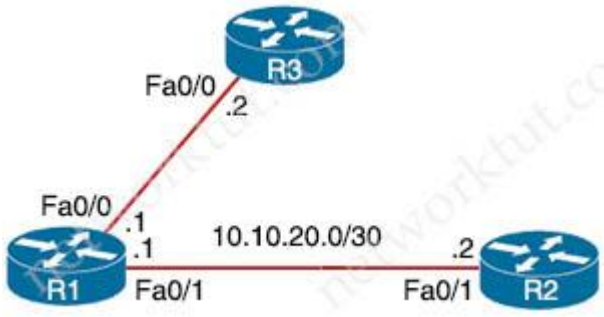
A. show frequency
B. show track
C. show reachability
D. show threshold

Answer: B

Question 4

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

Answer: C

Explanation

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.

SNMP Questions

https://www.networktut.com/snmp-questions

Question 1

Which SNMP verification command shows the encryption and authentication protocols that are used in SNMPv3?

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

Answer: B

Explanation

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.

```
Router#show snmp user abcd
User name: abcd
Engine ID: 00000090200000000C025808
storage-type: nonvolatile active access-list: 10
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: 3DES
Group name: VacmGroupName
Group name: VacmGroupName
```

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t2/snmpv3ae.html

Note: 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. Below is an example of this command.

```
R1#show snmp group
groupname: ILMI                                 security model:v1
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active

groupname: ILMI                                 security model:v2c
readview : *ilmi                                writeview: *ilmi
notifyview: <no notifyview specified>
row status: active
```

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_9snmp.html

Question 2

Refer to the exhibit. 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 ciscotest 1
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

Answer: A D

Explanation

The syntax of configuring a SNMP community string is:

snmp-server community *string* [**view** *view-name*] [**ro** | **rw**] [*access-list-number*]

By default, the community string permits read-only (ro) access to all objects. Therefore the first command in the exhibit above means “allow a SNMP manager that matches access-list 1 and use the password “ciscotest” to have Read-Only access to this device.

But the question mentioned that the network operations cannot read or write configuration to this device so there are two issues with above SNMP statement:
+ Maybe ACL 1 did not match the IP address of the network operations so we have to modify ACL 1 to “permit” the operations subnet.
+ This SNMP configuration only allows Read-Only permission so we have to configure the rw

permission by adding the “rw” keyword after the community string (but before the ACL number).

DHCP Questions

https://www.networktut.com/dhcp-questions

Question 1

Users were moved from the local DHCP server to the remote corporate DHCP server. After the move, none of the users were able to use the network. Which two issues will prevent this setup from working property? (Choose two)

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

Answer: B E

Question 2

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

Answer: D

Explanation

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.

DNA Center Questions

https://www.networktut.com/dna-center-questions

Question 1

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 magiev-config update
D. Sudo maglev install config update

Answer: C

Explanation

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.
…

For more information about this procedure, please read https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2/install/b_dnac_install_1_2/b_dnac_install_1_2_chapter_011.html

Question 2

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

Answer: D

Explanation

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."

Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-2-10/user_guide/b_cisco_dna_center_ug_1_2_10/b_dnac_ug_1_2_10_chapter_0111.html

Question 3

While 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

Answer: C

Explanation

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.

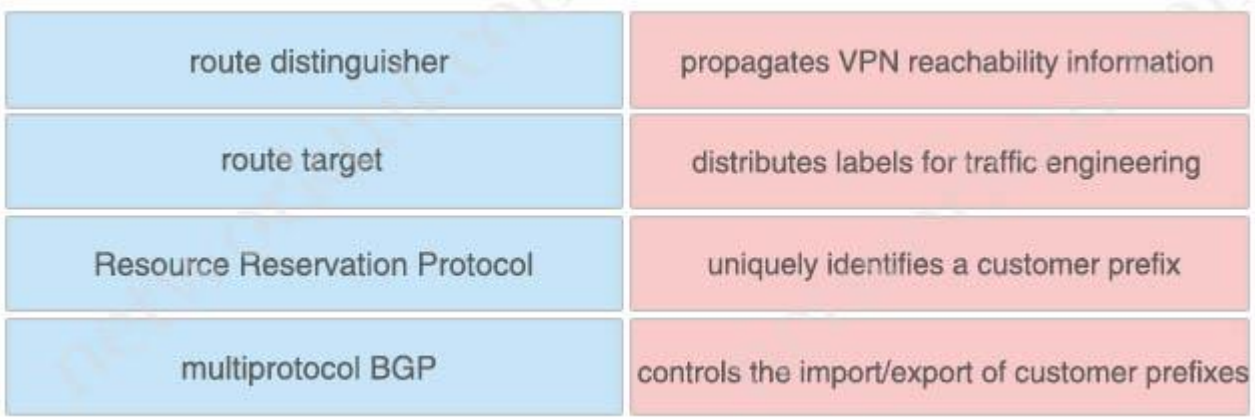
Reference: https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3/user_guide/b_cisco_dna_center_ug_1_3/b_cisco_dna_center_ug_1_3_chapter_0100.html

Drag Drop Questions

https://www.networktut.com/drag-drop-questions

Question 1

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

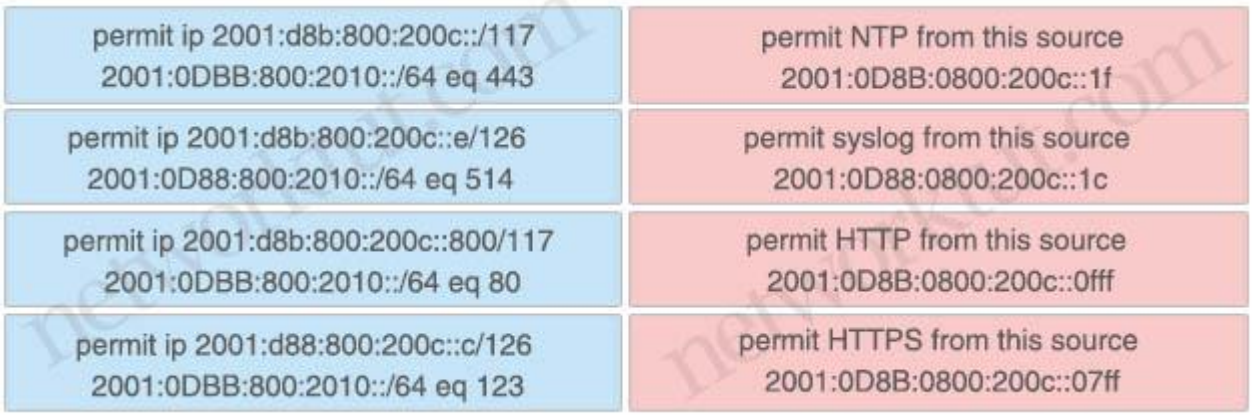


Answer:

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

Question 2

Drag and drop the address from the left onto the correct IPv6 filter purposes on the right.



Answer:

+ permit NTP from this source 2001:0D88:0800:200c::1f – **permit ip 2001:d88:800:200c::c/126 2001:0DBB:800:2010::/64 eq 123**
+ permit syslog from this source 2001:0D88:0800:200c::1c – **permit ip 2001:D88:800:200c::e/126 2001:0DBB:800:2010::/64 eq 514**
+ permit HTTP from this source 2001:0D8B:0800:200c::0fff – **permit ip 2001:d8b:800:200c::800/117 2001:0DBB:800:2010::/64 eq 80**
+ permit HTTPS from this source 2001:0D8B:0800:200c::07ff – **permit ip 2001:d8b:800:200c::/117 2001:0DBB:800:2010::/64 eq 443**

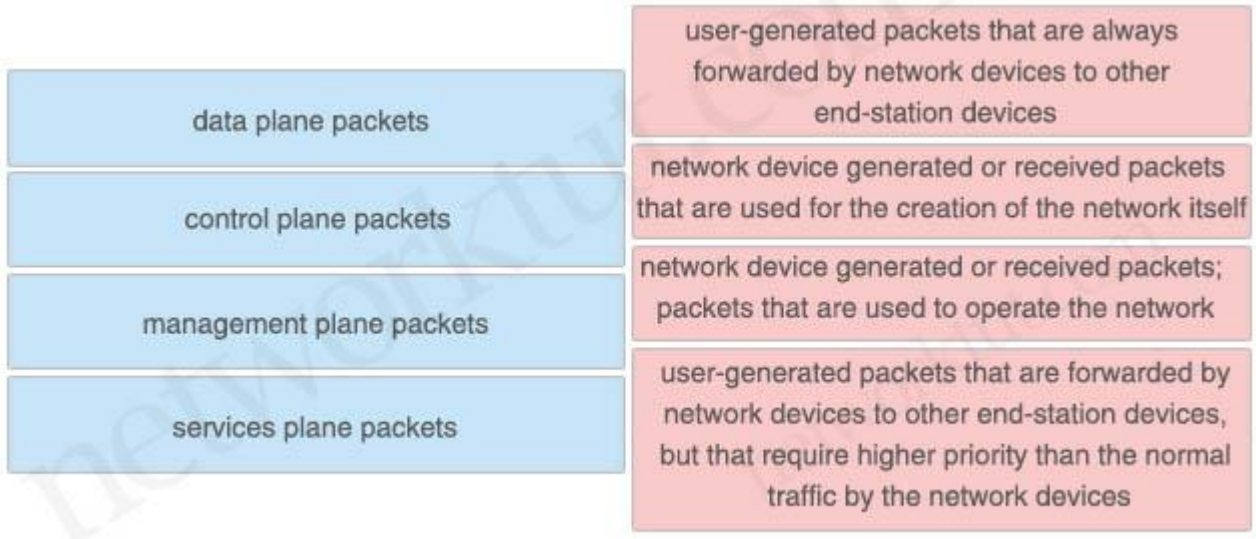
Explanation

HTTP and HTTPs run on TCP port 80 and 443, respectively and we have to remember them.

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**.

Question 3

Drag and drop the packet from the left onto the correct descriptions on the right.



Answer:

+ user-generated packets that are always forwarded by network devices to other end-station devices: **data plane packets**

+ network device generated or received packets that are used for the creation of the network itself: **control plane packets**
+ network device generated or received packets; packets that are used to operate the network: **management plane packets**
+ user-generated packets that are forwarded by network devices to other end-station devices, but that require higher priority than the normal traffic by the network devices: **services plane packets**

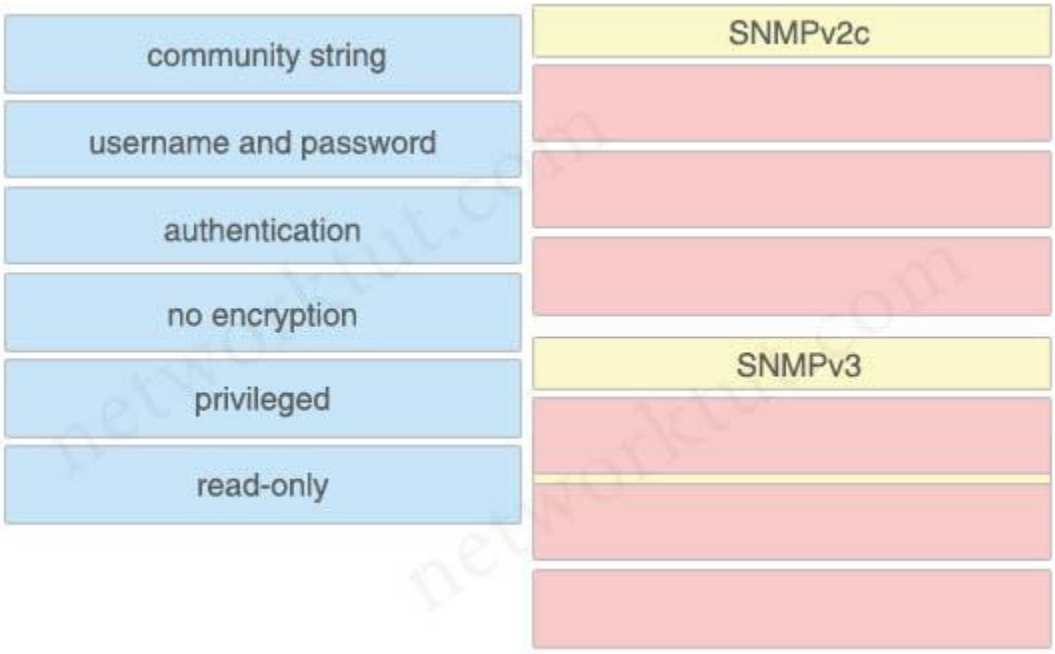
Explanation

Unlike legacy network technologies such as ISDN, Frame Relay, and ATM that defined separate data and control channels, IP carries all packets within a single pipe. Thus, IP network devices such as routers and switches must be able to distinguish between data plane, control plane, and management plane packets to treat each packet appropriately.
From an IP traffic plane perspective, packets may be divided into four distinct, logical groups:
1. **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.
2. **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.
3. **Management plane packets** – Network device generated or received packets, or management station generated or received packets that are used to manage the network. From the perspective of the network device, management 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 Telnet, Secure Shell (SSH), TFTP, SNMP, FTP, NTP, and other protocols used to manage the device and/or network.
4. **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).

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

Question 4

Drag and drop the SNMP attributes in Cisco IOS devices from the onto the correct SNMPv2c or SNMPv3 categories on the right.



Answer:

SNMPv2c:
+ community string
+ no encryption
+ read-only

SNMPv3:
+ username and password
+ authentication
+ privileged

Explanation

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.

Question 5

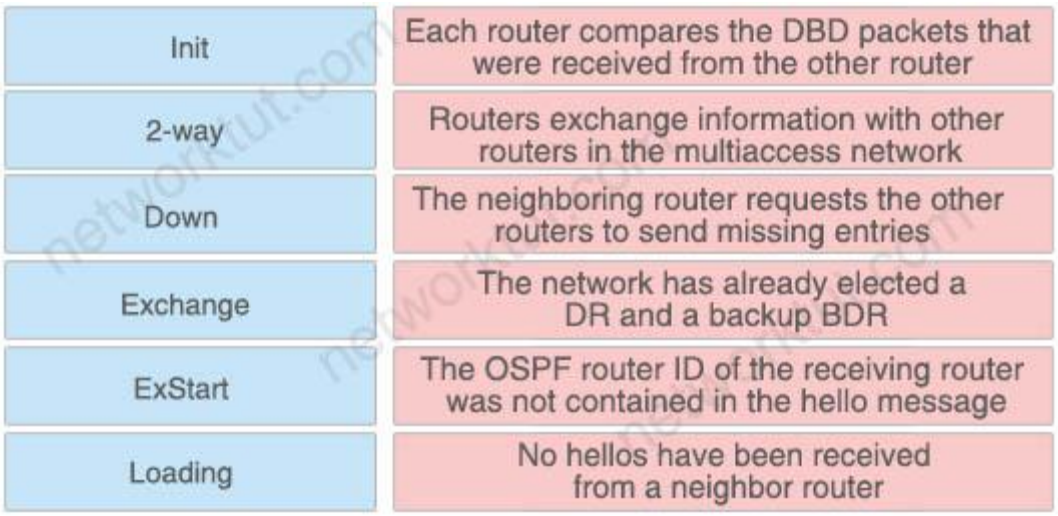
Drag and drop the MPLS terms from the left onto the correct definitions on the right.

Answer:

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

Question 6

Drag and drop the OSPF adjacency states from the left onto the correct descriptions on the right



Answer:

+ Each router compares the DBD packets that were received from the other router: Exchange
+ Routers exchange information with other routers in the multiaccess network: 2-way
+ The neighboring router requests the other routers to send missing entries: Loading
+ The network has already elected a DR and a backup BDR: Exstart
+ The OSPF router ID of the receiving router was not contained in the hello message: Init
+ No hellos have been received from a neighbor router: Down

Explanation

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

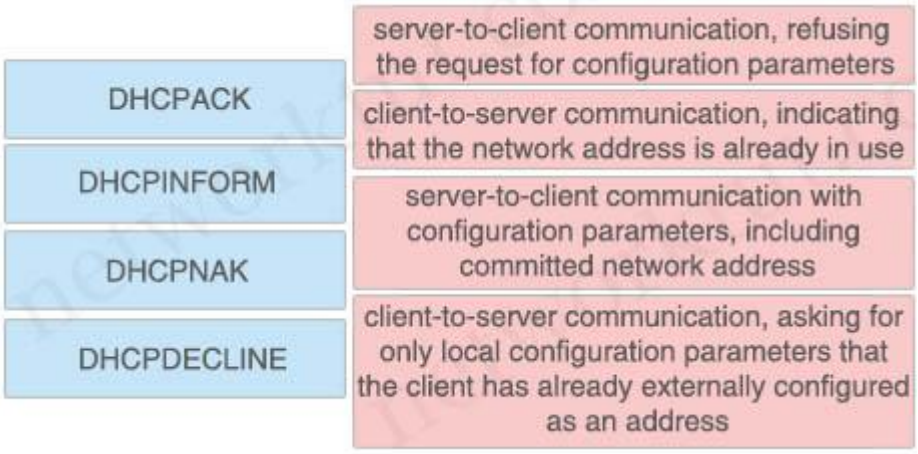
Loading: In this state, the actual exchange of link state information occurs. Outdated or missing entries are also requested to be resent.

Full: routers are fully adjacent with each other

(Reference: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f0e.shtml)

Question 7

Drag and drop the DHCP messages from the left onto the correct uses on the right.



Answer:

+ server-to-client communication, refusing the request for configuration parameters: DHCPNAK
+ client-to-server communication, indicating that the network address is already in use: DHCPDECLINE
+ server-to-client communication with configuration parameters, including committed network address: DHCPACK
+ client-to-server communication, asking for only local configuration parameters that the client has already externally configured as an address: DHCPINFORM

Explanation

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.

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.

DHCPACK: After the DHCP server receives the DHCPREQUEST, it acknowledges the request with a DHCPACK message, thus completing the initialization process.

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.

Reference: https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html

Miscellaneous Questions

https://www.networktut.com/miscellaneous-questions

Question 1

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

Answer: C

Explanation

Bidirectional Forwarding Detection (BFD) is a detection protocol that is designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols.

Prerequisites for Bidirectional Forwarding Detection:
+ Cisco Express Forwarding and IP routing must be enabled on all participating routers.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_bfd/configuration/15-mt/irb-15-mt-book/irb-bi-fwd-det.html

Question 2

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

A. TFTP
B. SNMP

C. SMTP
D. HTTPS
E. FTP

Answer: A B

Explanation

It is a general best practice to not mix TCP-based traffic with UDP-based traffic (especially Streaming-Video) within a single service-provider class because of the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters throttle back flows when drops are detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and, thus, never lower transmission rates because of dropping.

When TCP flows are combined with UDP flows within a single service-provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance.

TCP starvation/UDP dominance likely occurs if TCP-based applications is assigned to the same service-provider class as UDP-based applications and the class experiences sustained congestion.
Granted, it is not always possible to separate TCP-based flows from UDP-based flows, but it is beneficial to be aware of this behavior when making such application-mixing decisions within a single service-provider class.

Reference:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/VPNQoS.html

Therefore two UDP protocols that can cause TCP starvation are TFTP (UDP port 69) and SNMP (UDP port 161 & 162).

Question 3

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

Answer: D

Question 4

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

Answer: B

Explanation

Traditionally, link state protocols despite of having full view of the database, never calculated a backup route. Loop-Free Alternate (LFA) aims to calculate a backup route that can be used to route traffic, in case of a failure of a directly connected link or node on primary path.

Shared Risk Link Groups (SRLG) refer to situations in which links in a network **share a common fiber** (or a common physical attribute). These links have a shared risk: when one link fails, other links in the group might also fail. Topology-Independent Loop-Free Alternate (TI-LFA) SRLG protection attempts to find the post-convergence backup path that excludes the SRLG of the protected link. All local links that share any SRLG with the protecting link are excluded.

Reference: https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k-r6-3/segment-routing/configuration/guide/b-segment-routing-cg-asr9000-63x/b-segment-routing-cg-asr9000-63x_chapter_01001.pdf

Note:

+ **Linecard-disjoint**: This prefers a backup route from an interface that is on another line card. This is also a special case of SRLG
+ **Interface-disjoint**: This means that repair path is over a different interface as compared to the interface used to reach destination via primary path. In case of point-to-point links, this condition is always met.

Question 5

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 loggings?

```
R1(config)#do show running-config | section line|username
username cisco secret 5 $l$^e/o$I3G5cXODxpYMSJ70PzEyoO
line con 0
logging synchronous
```

```
line vty 0 4
login local
transport input telnet
R1(config)# logging console 7
R1(config)# do debug 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

Answer: C (?)

Explanation

The "logging console" is a default and hidden command. This command only appears if it is disabled (no logging console) so in fact it is currently enabled in this question.

But other questions are not correct either. The "terminal monitor" command enables logging on your virtual terminal connection (telnet), not the console line. So if we have to choose one answer, answer C is the best one.

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.

Answer: A

Explanation

Flow exporters are created as separate components in a router's configuration. Exporters are assigned to flow monitors to export the data from the flow monitor cache to a remote system such as a NetFlow collector.

As we can see the "flow exporter EXPORTER-1" was defined but it has not been used. We can use it inside a flow monitor. For example:

```
flow monitor FLOW-MONITOR-1
 record v4_r1
 exporter EXPORTER-1
 exit
```