QUESTION 16
White working with software images, an engineer observes that Cisco DNA Center cannot upload its software image directly from the device. Why is the image not uploading?

A. The device has lost connectivity to Cisco DNA Center.
B. The software image for the device is in bundle mode
C. The software image for the device is in install mode.
D. The device must be resynced to Cisco DNA Center

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

QUESTION 17
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: B
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.

QUESTION 18
Drag and Drop Question
Drag and drop the MPLS VPN concepts from the left onto the correct descriptions on the right.

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

Answer:

multiprotocol BGP
Resource Reservation Protocol
route distinguisher
route target

QUESTION 19
Drag and Drop Question
Drag and drop the address from the left onto the correct IPv6 filter purposes on the right.

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

Answer:

permit ip 2001:D8B:800:200C::c/126 2001:0DBB:800:2010::/64 eq 123
permit ip 2001:D88:800:200C::e/126 2001:0DBB:800:2010::/64 eq 514
permit ip 2001:d8b:800:200c::800 /117 2001:0DBB:800:2010::/64 eq 80
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 20
Which security feature can protect DMVPN tunnels?

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

Answer: A

QUESTION 21
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
Explanation:
https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/software/15_4_1_cg/vrf_cgr1000.html
show ip route vrf vrf-name [connected] [protocol [as- Displays IP routing table number] [list [list-number]] [mobile] [odr] [profile] information associated [static] [summary][supernets-only] with a VRF.

QUESTION 22
Refer to the exhibit. An administrator that is connected to the console does not see debug messages when remote users log in.
Which action ensures that debug messages are displayed for remote logins?

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

A. Enter the transport input ssh configuration command.
B. Enter the terminal monitor exec command.
C. Enter the logging console debugging configuration command.

D. Enter the aaa new-model configuration command.

Answer: C

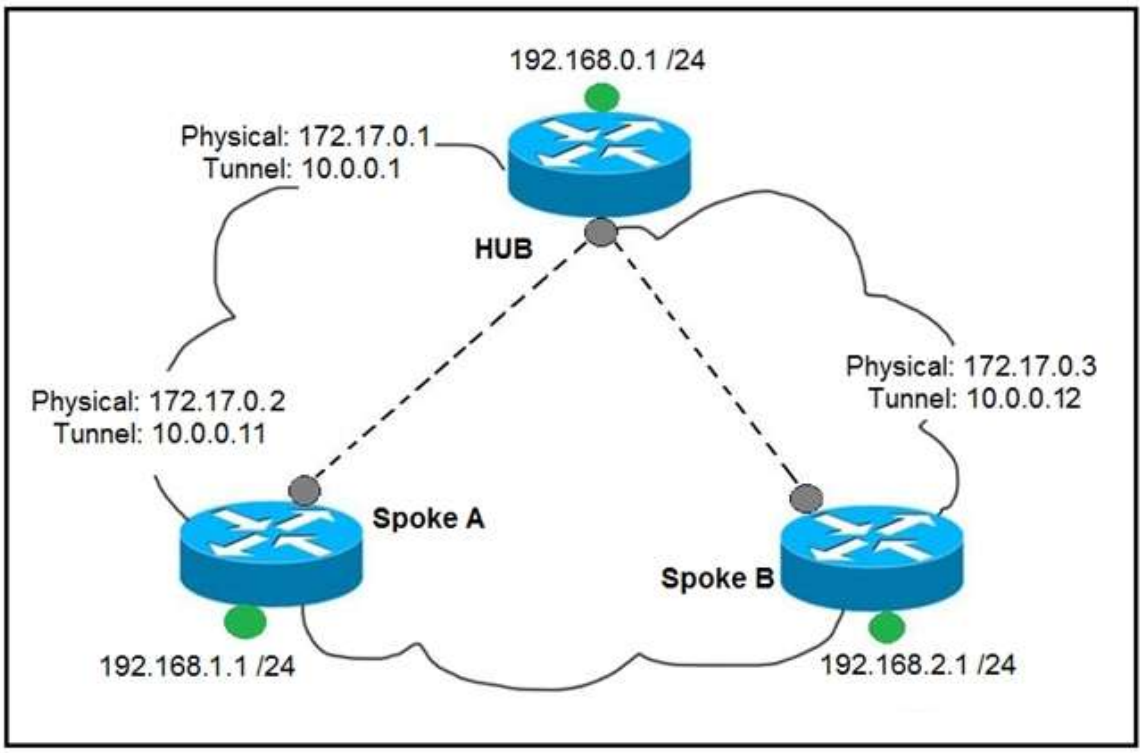
QUESTION 23
Refer to the exhibit. An engineer is trying to block the route to 192.168.2.2 from the routing table by using the configuration that is shown.
The route us still present in the routing table as an OSPF route. Which action blocks the route?

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

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

Answer: C

QUESTION 24
Refer to the exhibit. Which interface configuration must be configured on the spoke A router to enable a dynamic DMVPN tunnel with the spoke B router?



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

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

C.
```
interface Tunnel0
ip address 10.1.0.11 255.255.255.0
ip nhrp network-id 1
tunnel source 1.1.1.10
ip nhrp map 10.0.0.11 172.17.0.2
tunnel mode gre
```

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

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

QUESTION 25
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
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4m-book.pdf

QUESTION 26
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