



**Exam : 350-001**

**Title : CCIE Cisco Certified  
InterNetworking Expert**

**Version : Demo**

1. What is the purpose of an explicit "deny any" statement at the end of an ACL?

- A. none, since it is implicit
- B. to enable Cisco IOS IPS to work properly; however, it is the deny all traffic entry that is actually required
- C. to enable Cisco IOS Firewall to work properly; however, it is the deny all traffic entry that is actually required
- D. to allow the log option to be used to log any matches
- E. to prevent sync flood attacks
- F. to prevent half-opened TCP connections

Answer: D

2. Which of these is mandatory when configuring Cisco IOS Firewall?

- A. Cisco IOS IPS enabled on the untrusted interface
- B. NBAR enabled to perform protocol discovery and deep packet inspection
- C. a route map to define the trusted outgoing traffic
- D. a route map to define the application inspection rules
- E. an inbound extended ACL applied to the untrusted interface

Answer: E

3. Which statement correctly describes the disabling of IP TTL propagation in an MPLS network?

- A. The TTL field from the IP packet is copied into the TTL field of the MPLS label header at the ingress edge LSR.
- B. TTL propagation cannot be disabled in an MPLS domain.
- C. TTL propagation is only disabled on the ingress edge LSR.
- D. The TTL field of the MPLS label header is set to 255.
- E. The TTL field of the IP packet is set to 0.

Answer: D

4. Two routers configured to run BGP have been connected to a firewall, one on the inside interface and one on the outside interface. BGP has been configured so the two routers should peer, including the

correct BGP session endpoint addresses and the correct BGP session hop-count limit (EBGP multihop).  
What is a good first test to see if BGP will work across the firewall?

- A. Attempt to TELNET from the router connected to the inside of the firewall to the router connected to the outside of the firewall. If telnet works, BGP will work, since telnet and BGP both use TCP to transport data.
- B. Ping from the router connected to the inside interface of the firewall to the router connected to the outside interface of the firewall. If you can ping between them, BGP should work, since BGP uses IP to transport packets.
- C. There is no way to make BGP work across a firewall without special configuration, so there is no simple test that will show you if BGP will work or not, other than trying to start the peering session.
- D. There is no way to make BGP work across a firewall.

Answer: A

5. Spanning Tree Protocol IEEE 802.1s defines the ability to deploy which of these?

- A. one global STP instance for all VLANs
- B. one STP instance for each VLAN
- C. one STP instance per set of VLANs
- D. one STP instance per set of bridges

Answer: C

6. Which two of these are used in the selection of a root bridge in a network utilizing Spanning Tree Protocol IEEE 802.1D? (Choose two.)

- A. Designated Root Cost
- B. bridge ID priority
- C. max age
- D. bridge ID MAC address
- E. Designated Root Priority
- F. forward delay

Answer: BD

7. If a port configured with STP loop guard stops receiving BPDUs, the port will be put into which state?

- A. learning state
- B. listening state
- C. forwarding state
- D. root-inconsistent state

Answer: D

8. What is the purpose of the STP PortFast BPDU guard feature?

- A. enforce the placement of the root bridge in the network
- B. ensure that a port is transitioned to a forwarding state quickly if a BPDU is received
- C. enforce the borders of an STP domain
- D. ensure that any BPDUs received are forwarded into the STP domain

Answer: C

9. When STP UplinkFast is enabled on a switch utilizing the default bridge priority, what will the new bridge priority be changed to?

- A. 8192
- B. 16384
- C. 49152
- D. 65535

Answer: C

10. Which of these best describes the actions taken when a VTP message is received on a switch configured with the VTP mode "transparent"?

- A. VTP updates are ignored and forwarded out all ports.
- B. VTP updates are ignored and forwarded out trunks only.
- C. VTP updates are made to the VLAN database and are forwarded out trunks only.
- D. VTP updates are ignored and are not forwarded.

Answer: B

11. Refer to the exhibit. In this network, R1 has been configured to advertise a summary route, 192.168.0.0/22, to R2. R2 has been configured to advertise a summary route, 192.168.0.0/21, to R1. Both

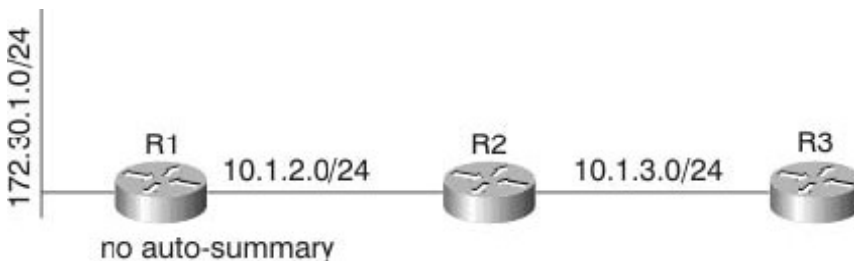
routers have been configured to remove the discard route (the route to null created when a summary route is configured) by setting the administrative distance of the discard route to 255. What will happen if R1 receives a packet destined to 192.168.3.1?



- A. The packet will loop between R1 and R2.
- B. It is not possible to set the administrative distance on a summary to 255.
- C. The packet will be forwarded to R2, where it will be routed to null0.
- D. The packet will be dropped by R1, since there is no route to 192.168.3.1.

Answer: A

12. Refer to the exhibit. In this network, R1 is configured not to perform autosummarization within EIGRP. What routes will R3 learn from R2 through EIGRP?



- A. 172.30.1.0/24 and 10.1.2.0/24; EIGRP only performs autosummarization at the edge between two major networks.
- B. 172.30.0.0/16 and 10.1.2.0/24; R2 will perform autosummarization, although R1 will not.
- C. Since R2 is configured without autosummarization, it will not propagate the 172.30.1.0/24 route.
- D. 172.30.0.0/8 and 10.0.0.0/8.

Answer: A

13. The classic Spanning Tree Protocol (802.1D 1998) uses which sequence of variables to determine the best received BPDU?

- A. 1) lowest root bridge id, 2) lowest sender bridge id, 3) lowest port id, 4) lowest root path cost

B. 1) lowest root path cost, 2) lowest root bridge id, 3) lowest sender bridge id, 4) lowest sender port id  
 C. 1) lowest root bridge id, 2) lowest sender bridge id, 3) lowest root path cost 4) lowest sender port id

D. 1) lowest root bridge id, 2) lowest root path cost, 3) lowest sender bridge id, 4) lowest sender port id  
 Answer: D

14. Which three port states are used by RSTP 802.1w? (Choose three.)

- A. Listening
- B. Learning
- C. Forwarding
- D. Blocking
- E. Discarding
- F. Disabled

Answer: BCE

15. Refer to the exhibit. Catalyst R is the root bridge for both VLAN 1 and VLAN 2. What is the easiest way to load-share traffic across both trunks and maintain redundancy in case a link fails, without using any type of EtherChannel link-bundling?

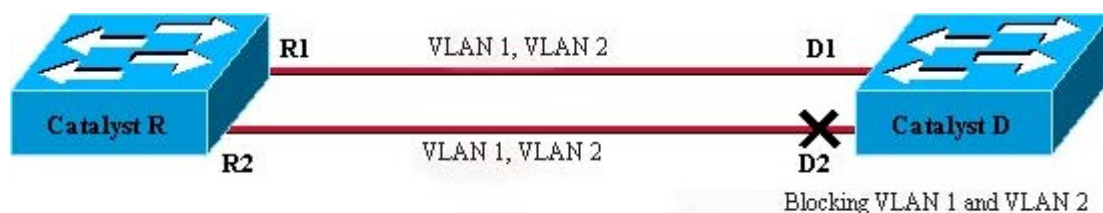


Figure 1

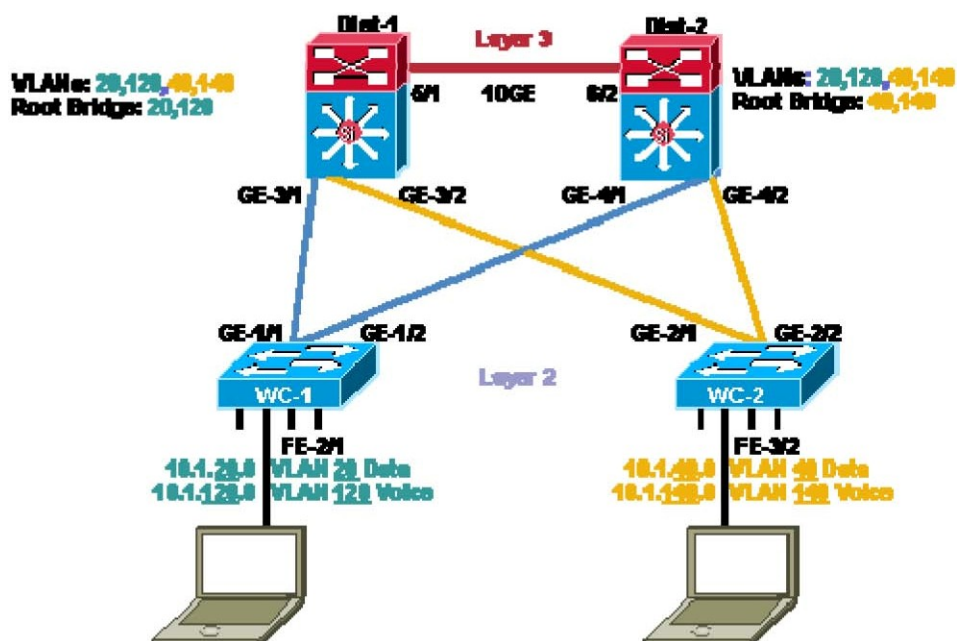
A. Increase the root bridge priority (increasing the numerical priority number) for VLAN 2 on Catalyst D so that port D2 becomes the root port on Catalyst D for VLAN 2.

B. Decrease the port priority on R2 for VLAN 2 on Catalyst R so that port D1 will be blocked for VLAN 2 and port D2 will remain blocked for VLAN 1.

C. Decrease the path cost on R2 on Catalyst R for VLAN 2 so that port D1 will be blocked for VLAN 2 and port D2 will remain blocked for VLAN 1.

D. Increase the root bridge priority (decreasing the numerical priority number) for VLAN 2 on Catalyst R so that R2 becomes the root port on Catalyst D for VLAN 2.

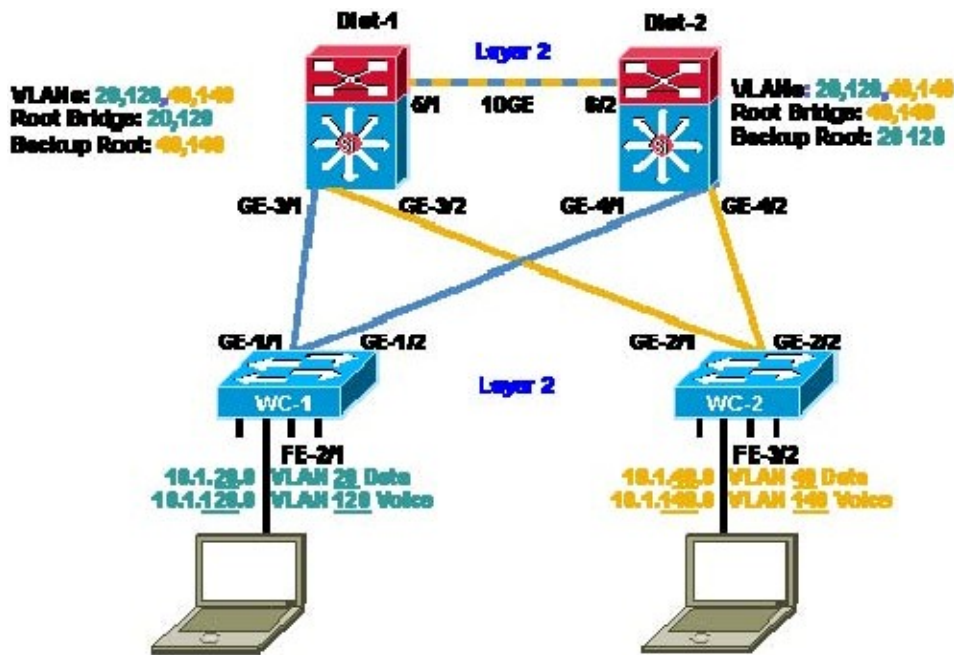
Answer: B 16. Refer to the exhibit. In the diagram, the switches are running IEEE 802.1s MST. Which ports are in the MST blocking state?



- A. GE-1/2 and GE 2/1
- B. GE-1/1 and GE-2/2
- C. GE-3/2 and GE 4/1
- D. no ports are in the blocking state
- E. There is not enough information to determine which ports are in the blocking state.

Answer: D

17. Refer to the exhibit. In the diagram, the switches are running IEEE 802.1w RSTP. On which ports should root guard be enabled in order to facilitate deterministic root bridge election under normal and failure scenarios?



- A. GE-3/1, GE-3/2
- B. FE-2/1, FE-3/2
- C. GE-1/1, GE-1/2
- D. GE-4/1, GE-4/2
- E. GE-2/1, GE-2/2
- F. GE-3/1, GE-3/2, GE-4/1, GE-4/2, FE-2/1, FE-3/2

Answer: F

18. Loop guard and UniDirectional Link Detection both protect against Layer 2 STP loops. In which two ways does loop guard differ from UDLD in loop detection and prevention? (Choose two.)

- A. Loop guard can be used with root guard simultaneously on the same port on the same VLAN while UDLD cannot.
- B. UDLD protects against STP failures caused by cabling problems that create one-way links.
- C. Loop guard detects and protects against duplicate packets being received and transmitted on different ports.
- D. UDLD protects against unidirectional cabling problems on copper and fiber media.
- E. Loop guard protects against STP failures caused by problems that result in the loss of BPDUs from a designated switch port.

Answer: BE

19. Refer to the exhibit. Voice traffic is marked "precedence 5." How much bandwidth is allocated for voice traffic during periods of congestion?

```
!
class-map match-all Signal
  match ip precedence 3
class-map match-any System
  match access-group name Security
  match ip precedence 6
  match ip precedence 7
class-map match-all Bearer
  match ip precedence 5
!
!
policy-map ProviderOut
  class Bearer
    priority 48
  class Signal
    bandwidth 15
  class System
    bandwidth 15
  class class-default
    fair-queue
    random-detect
    shape average 512000
!
interface Ethernet0/1
  description Provider Interface
  ip address dhcp client-id Ethernet0/1
  ip access-group 111 in
  ip nat outside
  full-duplex
  no cdp enable
  service-policy output ProviderOut
!
```

- A. a minimum of 48 kb/s
- B. a maximum of 48 kb/s
- C. a minimum of 48% of the available bandwidth
- D. a maximum of 48% of the available bandwidth

Answer: B

20. Refer to the exhibit. Which of these is applied to the Bearer class?

```
!
class-map match-all Signal
  match ip precedence 3
class-map match-any System
  match access-group name Security
  match ip precedence 6
  match ip precedence 7
class-map match-all Bearer
  match ip precedence 5
!
!
policy-map ProviderOut
  class Bearer
    priority 48
  class Signal
    bandwidth 15
  class System
    bandwidth 15
  class class-default
    fair-queue
    random-detect
    shape average 512000
!
interface Ethernet0/1
  description Provider Interface
  ip address dhcp client-id Ethernet0/1
  ip access-group 111 in
  ip nat outside
  full-duplex
  no cdp enable
  service-policy output ProviderOut
!
```

- A. WRED
- B. traffic shaping
- C. packet marking
- D. packet classification
- E. FIFO queuing within the class

Answer: E