640-811

Interconnecting Cisco Networking Devices

DEMO

QUESTION NO: 1

What is the purpose of the OSPF router ID in a DR/BDR election?

A. It is used with the OSPF priority values to determine which OSPF router will become the DR or BDR in a point-to-point network.
B. It is used with the OSPF priority values to determine which interface will be used to form a neighbor relationship with another OSPF router.
C. It is used to determine which interfaces will send Hello packets to neighboring OSPF routers.
D. It is used with the OSPF priority values to determine which router will become the DR or BDR in a multiaccess network.

Answer: D

Explanation:
The router ID is the highest IP address or the highest IP address among loopback addresses (if one is configured) on the Cisco router or can be configured manually by "router-id x.x.x.x". Once the router ID is chosen, it will not be changed unless the OSPF process is reset(clear ip ospf process xx) or the router is reloaded. The IP address of router ID doesn't need to be reachable, but it is used to determine which will router will become the DR or BDR in a multi-access network.

QUESTION NO: 2

Which wild card mask will enable a network administrator to permit access to the Internet for only hosts that are assigned an address in the range of 192.168.8.0 through 192.168.15.255?

A. 0.0.0.0
B. 0.0.3.255
C. 0.0.7.255
D. 0.0.255.255
E. 0.0.0.255

Answer: C

Explanation:
Wildcard masks are used with access lists to specify an individual host, a network, or a certain range of a network or networks. To understand a wildcard mask, you need to understand what a block size is; block sizes are used to specify a range of addresses. Some of the different block sizes available are 64, 32, 16, 8, and 4.
When you need to specify a range of addresses, you choose the next-largest block size for your needs. For example, if you need to specify 34 networks, you need a block size of 64. If you want to specify 18 hosts, you need a block size of 32. If you only specify 2 networks, then a block size of 4 would work. You use wildcards with the host or network address to tell the router a range of available addresses to filter. To specify a host, the address would look like this: 172.16.30.5

0.0.0.0
The four zeros represent each octet of the address. Whenever a zero is present, it means that octet in the address must match exactly. To specify that an octet can be any value, the value of 255 is used. As an example, her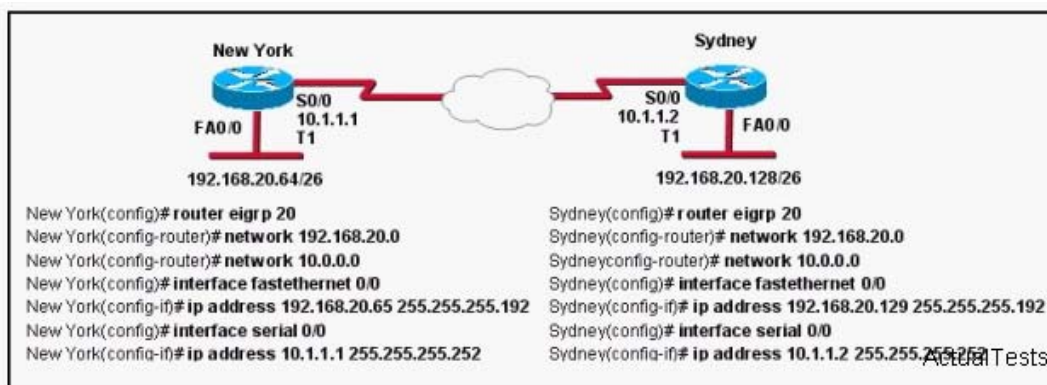e's how a /24 subnet is specified with a wildcard: 172.16.30.0 0.0.0.255 This tells the router to match up the first three octets exactly, but the fourth octet can be any value.

Now, that was the easy part. What if you want to specify only a small range of subnets? This is where the block sizes come in. You have to specify the range of values in a block size. In other words, you can't choose to specify 20 networks. You can only specify the exact amount as the block size value. For example, the range would either have to be 16 or 32, but not 20.

Let's say that you want to block access to part of network that is in the range from 172.16.8.0 through 172.16.15.0. That is a block size of 8. Your network number would be 172.16.8.0, and the wildcard would be 0.0.7.255. Whoa! What is that?!? The 7.255 is what the router uses to determine the block size. The network and wildcard tell the router to start at 172.16.8.0 and go up a block size of eight addresses to network 172.16.15.0.

QUESTION NO: 3

Why has the network shown in the exhibit failed to converge?

New York(config)# router eigrp 20
New York(config-router)# network 192.168.20.0
New York(config-router)# network 10.0.0.0
New York(config)# interface fastethernet 0/0
New York(config-if)# ip address 192.168.20.65 255.255.255.192
New York(config)# interface serial 0/0
New York(config-if)# ip address 10.1.1.1 255.255.255.252

Sydney(config)# router eigrp 20
Sydney(config-router)# network 192.168.20.0
Sydneyconfig-router)# network 10.0.0.0
Sydney(config)# interface fastethernet 0/0
Sydney(config-if)# ip address 192.168.20.129 255.255.255.192
Sydney(config)# interface serial 0/0
Sydney(config-if)# ip address 10.1.1.2 255.255.255.252

A. The autonomous system number has not been properly configured.
B. The no auto-summary command needs to be applied to the routers.
C. The network numbers have not been properly configured on the routers.
D. The bandwidth values have not been properly configured on the serial interfaces.
E. The subnet masks for the network numbers have not been properly configured.

Answer: B

Explanation:
To restore the default behavior of automatic summarization of subnet routes into network-level routes, use the auto-summary command in router configuration mode. To disable this function and transmit subprefix routing information across classful network boundaries, use the no form of this command.
auto-summary

no auto-summary

QUESTION NO: 4

Refer to the exhibit. Switch-1 needs to send data to a host with a MAC address of 00b0.d056.efa4.
What will Switch-1 do with this data?

```
Switch-1# show mac address-table
Dynamic Addresses Count:            3
Secure Addresses (User-defined) Count:  0
Static Addresses (User-defined) Count:  0
System Self Addresses Count:        41
Total Mac addresses:                50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
0010.0de0.e289       Dynamic       1     FastEthernet0/1
0010.7b00.1540       Dynamic       2     FastEthernet0/3
0010.7b00.1545       Dynamic       2     FastEthernet0/2
```

A. Switch-1 will flood the data out all of its ports except the port from which the data originated.
B. Switch-1 will forward the data to its default gateway.
C. Switch-1 will send an ARP request out all its ports except the port from which the data originated.
D. Switch-1 will drop the data because it does not have an entry for that MAC address.

Answer: A

Explanation:

Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port.

Machines may have been removed from a port, turned off, or moved to another port on the same switch or a different switch.

This could cause confusion in frame forwarding.

The MAC address entry is automatically discarded or aged out after 300 seconds

If there is not MAC address of destination host in MAC table, switch sends broadcast to all ports except the source to findout the destination host.

In output there is no MAC address of give host so switch floods to all ports except source port.

QUESTION NO: 5