

Routing and Switching Essentials (Version 6.00) - RSE Practice Final

Below is the feedback on items for which you did not receive full credit. Some interactive items may not display your response.

Subscore: Domain Knowledge - Standard Score ▼

5 Which type of static route typically uses the *distance* parameter in the ip route global configuration command?

| Correct Response | Your Response |
|------------------|---------------|
|------------------|---------------|

- ☐ standard static route
- ☐ default static route
- ☒ floating static route
- ☐ summary static route

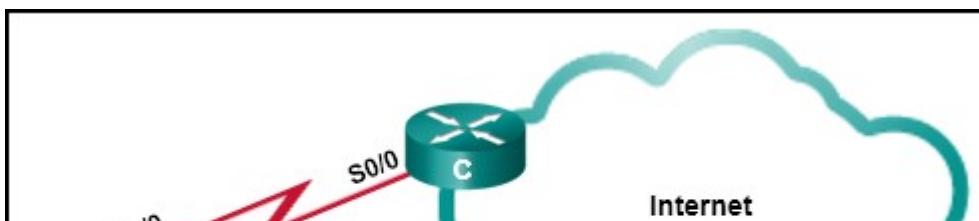
Because a floating static route is not designed to be used as a primary route, its configuration requires a higher administrative distance than the usual default value of 1. When set higher than the administrative distance for the current routing protocol, the *distance* parameter allows the route to be used only when the primary route fails. All other forms of static routes have specific uses as primary routes.

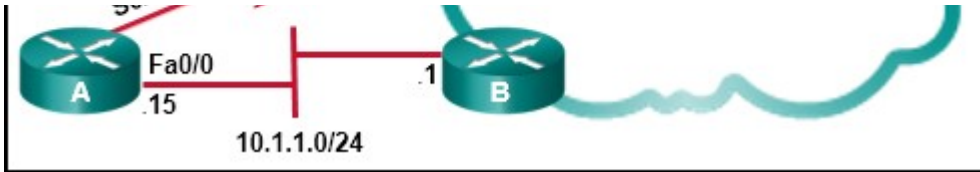
This item references content from the following areas:

Routing and Switching Essentials

2.1.2 Types of Static Routes

9





avoids recursive route lookups and any potential next-hop issues caused by the multiaccess nature of the Ethernet segment with router B. What should the administrator configure?

Correct Response Your Response

- ☐ Create a static route pointing to 10.1.1.1 with an AD of 1.
- ☐ Create a static route pointing to Fa0/0 with an AD of 1.
- ☒ Create a static route pointing to 10.1.1.1 with an AD of 95.
- ☒ Create a fully specified static route pointing to Fa0/0 with an AD of 95.
- ☐ Create a fully specified static route pointing to Fa0/0 with an AD of 1.

A floating static route is a static route with an administrative distance higher than that of another route already in the routing table. If the route in the table disappears, the floating static route will be put into the routing table in its place. Internal EIGRP has an AD of 90, so a floating static route in this scenario would need to have an AD higher than 90. Also, when creating a static route to a multiaccess interface like a FastEthernet segment a fully specified route should be used, with both a next-hop IP address and an exit interface. This prevents the router from doing a recursive lookup, but still ensures the correct next-hop device on the multiaccess segment forwards the packet.


This item references content from the following areas:

Routing and Switching Essentials

2.3.2 Troubleshoot IPv4 Static and Default Route Configuration

15 What is the name of the layer in the Cisco borderless switched network design that would have more switches deployed than other layers in the network design of a large organization?

Correct Response **Your Response**

- ☐ data link
- ☐ core
-  ☐ access
- ☐ network
- ☒ network access

Access layer switches provide user access to the network. End user devices, such as PCs, access points, printers, and copiers, would require a port on a switch in order to connect to the network. Thus, more switches are needed in the access layer than are needed in the core and distribution layers.


This item references content from the following areas:

Routing and Switching Essentials

4.1.1 Converged Networks

16 What is a function of the distribution layer?

Correct Response **Your Response**

- ☒ network access to the user
- ☐ fault isolation
-  ☐ interconnection of large-scale networks in wiring closets
- ☐ high-speed backbone connectivity

The distribution layer interacts between the access layer and the core by aggregating access layer connections in wiring closets, providing intelligent routing and switching, and applying access policies to access the rest of the network. Fault isolation and high-speed backbone connectivity are the primary functions of the core layer. The main function of the access layer is to provide network access to the user.

This item references content from the following areas:

Routing and Switching Essentials

4.1.1 Converged Networks

20 Which statement correctly describes how a LAN switch forwards frames that it receives?

| Correct Response | Your Response |
|---------------------|------------------|
|---------------------|------------------|

- ☐ Only frames with a broadcast destination address are forwarded out all active switch ports.
- ☐ Cut-through frame forwarding ensures that invalid frames are always dropped.
- ☒ Frame forwarding decisions are based on MAC address and port mappings in the CAM table.
- ☐ Unicast frames are always forwarded regardless of the destination MAC address.

Cut-through frame forwarding reads up to only the first 22 bytes of a frame, which excludes the frame check sequence and thus invalid frames may be forwarded. In addition to broadcast frames, frames with a destination MAC address that is not in the CAM are also flooded out all active ports. Unicast frames are not always forwarded. Received frames with a destination MAC address that is associated with the switch port on which it is received are not forwarded because the destination exists on the network segment connected to that port.

This item references content from the following areas:

Routing and Switching Essentials

4.2.1 Frame Forwarding

23 A company security policy requires that all MAC addressing be dynamically learned and added to both the MAC address table and the running configuration on each switch. Which port security configuration will accomplish this?

| Correct Response | Your Response |
|------------------|---------------|
|------------------|---------------|

- ☐ auto secure MAC addresses
- ☒ dynamic secure MAC addresses
- ☐ static secure MAC addresses
- ☒ sticky secure MAC addresses

With sticky secure MAC addressing, the MAC addresses can be either dynamically learned or manually configured and then stored in the address table and added to the running configuration file. In contrast, dynamic secure MAC addressing provides for dynamically learned MAC addressing that is stored only in the address table.

This item references content from the following areas:

Routing and Switching Essentials

5.2.2 Switch Port Security

24 A network technician is configuring port security on switches. The interfaces on the switches are configured in such a way that when a violation occurs, packets with unknown source addresses are dropped and no notification is sent. Which violation mode is configured on the interfaces?

| Correct Response | Your Response |
|------------------|---------------|
|------------------|---------------|

- ☐ off

- ☒ restrict
- ☐ protect
- ☐ shutdown

On a Cisco switch, an interface can be configured for one of three violation modes, specifying the action to be taken if a violation occurs:

Protect - Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. There is no notification that a security violation has occurred.

Restrict - Packets with unknown source addresses are dropped until a sufficient number of secure MAC addresses are removed, or the number of maximum allowable addresses is increased. In this mode, there is a notification that a security violation has occurred.

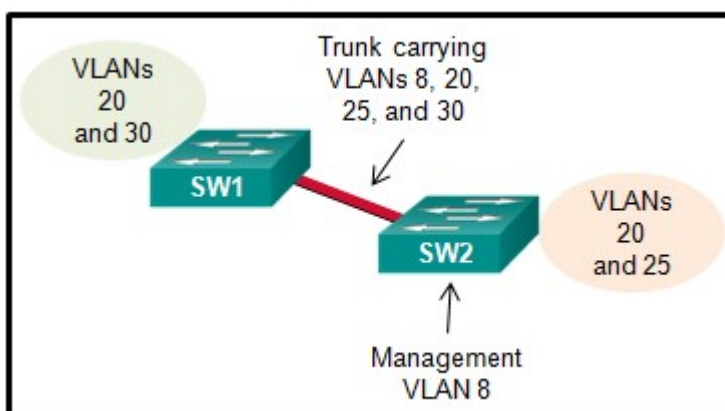
Shutdown - The interface immediately becomes error-disabled and the port LED is turned off.

This item references content from the following areas:

Routing and Switching Essentials

5.2.2 Switch Port Security

26



Refer to the exhibit. A small business uses VLANs 8, 20, 25, and 30 on two switches that have a trunk link between them. What native VLAN should be used on the trunk if Cisco best practices are being implemented?

| Correct Response | Your Response |
|---------------------|------------------|
|---------------------|------------------|

- | | |
|----------------------------------|----|
| <input type="radio"/> | 1 |
| <input checked="" type="radio"/> | 5 |
| <input checked="" type="radio"/> | 8 |
| <input type="radio"/> | 20 |
| <input type="radio"/> | 25 |
| <input type="radio"/> | 30 |

Cisco recommends using a VLAN that is not used for anything else for the native VLAN. The native VLAN should also not be left to the default of VLAN 1. VLAN 5 is the only VLAN that is not used and not VLAN 1.

This item references content from the following areas:

Routing and Switching Essentials

6.1.1 Overview of VLANs

44

```
R1# show ip nat statistics
Total translations: 6 (2 static, 4 dynamic, 4 extended)
Outside Interfaces: Serial0/2/1
Inside Interfaces: Serial0/2/0 , FastEthernet0/0.10 , FastEthernet0/0.11 ,
FastEthernet0/0.12
Hits: 3 Misses: 4
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool NAT refCount 4
  pool NAT: netmask 255.255.255.248
    start 209.165.200.228 end 209.165.200.230
    type generic, total addresses 3 , allocated 1 (33%), misses 0
```

Refer to the exhibit. A network administrator has just configured address translation and is verifying the configuration. What three things can the

| Correct Response | Your Response |
|---------------------|------------------|
|---------------------|------------------|

- | | |
|---------------------------------------|--|
| <input type="checkbox"/> | The name of the NAT pool is refCount. |
| <input checked="" type="checkbox"/> | Three addresses from the NAT pool are being used by hosts. |
| ✓ <input type="checkbox"/> | Two types of NAT are enabled. |
| ✓ <input checked="" type="checkbox"/> | Address translation is working. |
| ✓ <input checked="" type="checkbox"/> | A standard access list numbered 1 was used as part of the configuration process. |
| <input type="checkbox"/> | One port on the router is not participating in the address translation. |

The **show ip nat statistics** , **show ip nat translations** , and **debug ip nat** commands are useful in determining if NAT is working and and also useful in troubleshooting problems that are associated with NAT. NAT is working, as shown by the hits and misses count. Because there are four misses, a problem might be evident. The standard access list numbered 1 is being used and the translation pool is named NAT as evidenced by the last line of the output. Both static NAT and NAT overload are used as seen in the Total translations line.

This item references content from the following areas:

Routing and Switching Essentials

9.3.1 NAT Troubleshooting Commands