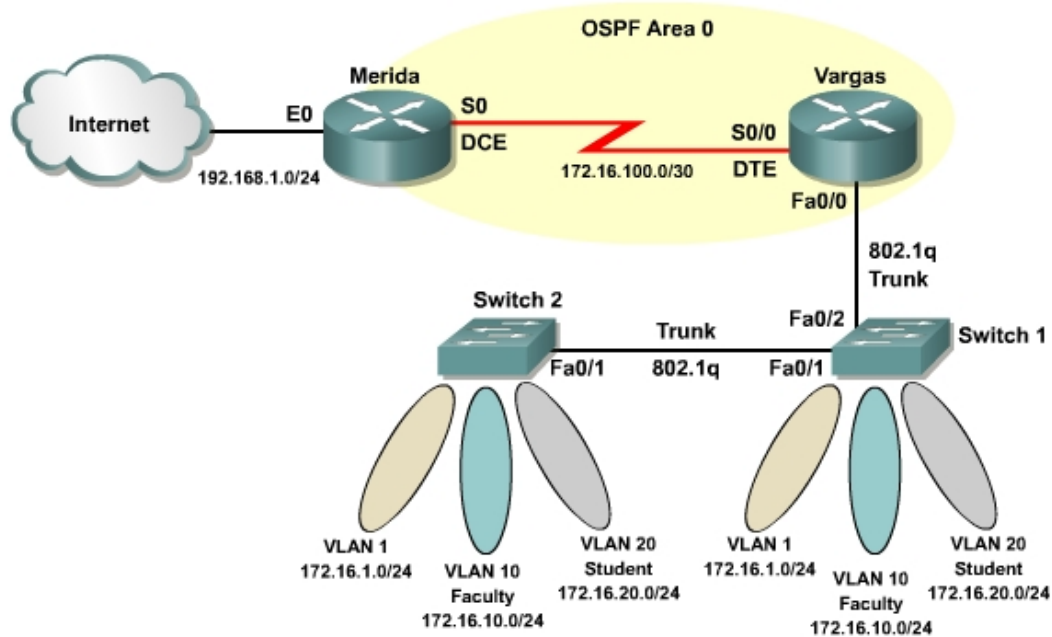


CCNA3 Student Skills-Based Assessment



| | VLAN 10 | VLAN 20 | VLAN 1 | IP Address | Trunk |
|----------|---------------|---------------|---------------------|---------------|--------------|
| Switch 1 | Fa0/5 – Fa0/6 | Fa0/7 – Fa0/8 | All Remaining Ports | 172.16.1.2/24 | Fa0/1, Fa0/2 |
| Switch 2 | Fa0/5 – Fa0/6 | Fa0/7 – Fa0/8 | All Remaining Ports | 172.16.1.3/24 | Fa0/1 |

Notes to Students

Review the following points before the start of the lab exam:

- Depending upon the router model, the interfaces may differ. For example, on some routers Serial0 may be Serial0/0 and Ethernet0 may be FastEthernet0/0.
- The exam is 75 minutes. 15 minutes has been allotted to read the entire lab exam. Then, use the remaining 60 minutes to configure all the requirements.

Objectives

Complete the following tasks throughout the exam:

- Configure OSPF
- Configure OSPF authentication
- Configure a default route
- VLAN configuration on Vargas
- Basic switch configuration
- Configure VLANs on the switches
- Configure VLAN trunking
- Configure VTP

- Configure switch port security
- Verify connectivity

Preconfigurations

The following items have been preconfigured on the routers and switches:

- Hostnames on all routers and switches
- Serial interface IP addresses, subnet masks, and the `no shutdown` command
- The console, telnet, and privileged passwords on all routers and switches
- Clock rates on DCE interfaces
- The topology cabling

Following are the actual commands already configured on the devices:

Merida Router

```

config t
hostname Merida
enable secret cisco
line con 0
  password cisco
  login
  exec-timeout 0 0
line vty 0 4
  password cisco
  login
interface Ethernet0
  ip address 192.168.1.1 255.255.255.0
  no shutdown
interface Serial0
  ip address 172.16.100.2 255.255.255.252
  clockrate 56000
  no shutdown

```

Vargas Router

```

config t
hostname Vargas
enable secret cisco
line con 0
  password cisco
  login
  exec-timeout 0 0
line vty 0 4
  password cisco
  login
interface Serial0/0
  ip address 172.16.100.1 255.255.255.252
  no shutdown

```

Switch 1

```

config t
hostname Switch1
enable secret cisco
line con 0
  password cisco
  login

```

```
    exec-timeout 0 0
line vty 0 15
  password cisco
  login
```

Switch 2

```
config t
hostname Switch2
enable secret cisco
line con 0
  password cisco
  login
  exec-timeout 0 0
line vty 0 15
  password cisco
  login
```

Configuration Tasks

Configure OSPF

Use the following values to configure OSPF on the routers:

- Configure Merida with the OSPF router ID of 10.10.10.1.
- Configure Vargas with the OSPF router ID of 10.10.10.2.
- Configure OSPF on Merida and Vargas.
- Configure OSPF so only the following 172.16.0.0 subnets will be routed. In other words, if another 172.16.0.0 interface were enabled on Merida or Vargas, such as 172.16.3.0/24, those subnets would not be propagated with OSPF. The only 172.16.0.0 subnets to be routed are:
 - 172.16.1.0/24
 - 172.16.10.0/24
 - 172.16.20.0/24
 - 172.16.100.0/30
- Apply OSPF cost values to reflect the actual 64k link between Merida and Vargas.

Configure OSPF Authentication

Authenticate OSPF packets between Merida and Vargas using MD5 encryption.

Configure a Default Route

Configure a default route to the Internet on the Merida router and propagate the default route to Vargas using OSPF.

VLAN Configuration on Vargas

Configure the Vargas Fa0/0 interface to trunk for VLAN 1, VLAN 10, and VLAN 20 with 802.1Q encapsulation.

Basic Switch Configuration

Use the following IP addresses to configure the switches:

- Configure Switch 1 with the VLAN 1 IP address of 172.16.1.2/24.
- Configure Switch 2 with the VLAN 1 IP address of 172.16.1.3/24.
- Configure both switches with the default gateway address of 172.16.1.1.

Configure VLANs on the Switches

Use the following values to configure VLANs on Switch 1:

- On Switch 1 configure the interfaces Fa0/5 and Fa0/6 on VLAN 10.
- On Switch 1 configure the interfaces Fa0/7 and Fa0/8 on VLAN 20.
- All other interfaces on Switch 1 are in VLAN1.

Use the following values to configure VLANs on Switch 2:

- On Switch 2 configure the interfaces Fa0/5 and Fa0/6 on VLAN 10.
- On Switch 2 configure the interfaces Fa0/7 and Fa0/8 on VLAN 20.
- All other interfaces on Switch 2 are in VLAN 1.

Configure VLAN Trunking

Use the following values to configure VLAN trunking on Switch 1 and 2:

- Configure trunking between Switch 1 and Switch 2 with 802.1Q encapsulation using port Fa0/1 on both switches.
- Configure Switch 1 for trunking between Switch 1 and Vargas with 802.1Q encapsulation using port Fa0/2.

Configure VTP

Use the following values to configure VTP on Switch 1 and 2:

- Configure both Switch 1 and Switch 2 as part of VTP domain Group1.
- Configure Switch 1 as the VTP server and Switch 2 as the VTP client.
 - Create VLAN 10 with the name faculty.
 - Create VLAN 20 with the name student.

Configure Switch Port Security

Configure port security on ports Fa0/5 through Fa0/8 to allow only one host. If the port security is violated then shutdown the port.

Verify Connectivity

All routers and switches should be able to ping the interfaces of the other devices.