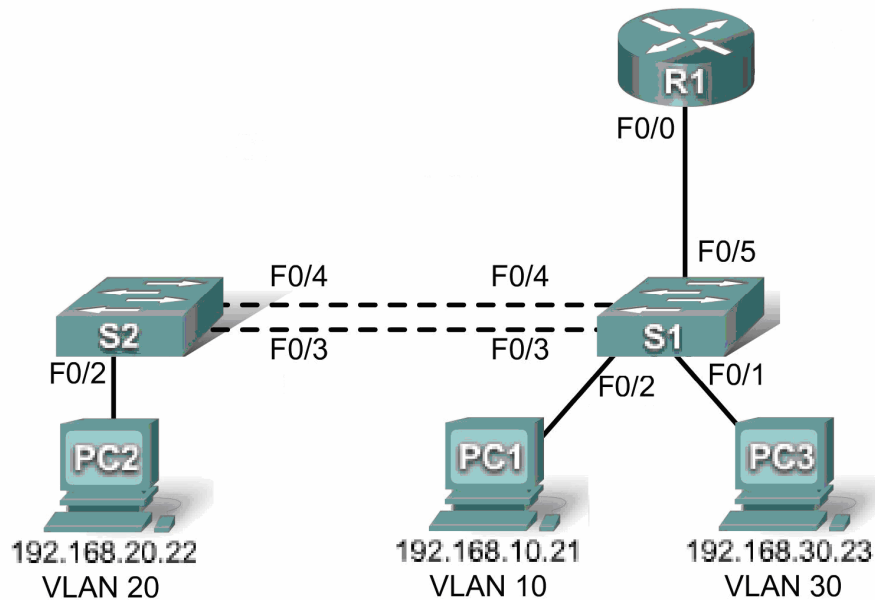


Lab 6: Inter-VLAN Routing

Topology Diagram



Addressing Table

Device (Hostname)	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	192.168.99.11	255.255.255.0	192.168.99.1
S2	VLAN 99	192.168.99.12	255.255.255.0	192.168.99.1
S3	VLAN 99	192.168.99.13	255.255.255.0	192.168.99.1
R1	Fa 0/0	See Subinterface Configuration Table		N/A
PC1	NIC	192.168.10.21	255.255.255.0	192.168.10.1
PC2	NIC	192.168.20.22	255.255.255.0	192.168.20.1
PC3	NIC	192.168.30.23	255.255.255.0	192.168.30.1

Subinterface Configuration Table – Router 1

Router Interface	Assignment	IP Address
Fa0/0.1	VLAN1	192.168.1.1
Fa0/0.10	VLAN 10	192.168.10.1
Fa0/0.20	VLAN 20	192.168.20.1
Fa0/0.30	VLAN 30	192.168.30.1
Fa0/0.99	VLAN 99	192.168.99.1

Task 1: Prepare the Network

Step 1: Cable a network that is similar to the one in the topology diagram.

Note that Ethernet (10Mb) LAN interfaces on routers do not support trunking, and Cisco IOS software earlier than version 12.3 may not support trunking on Fast Ethernet router interfaces.

Set up console connections to all three switches and to the router.

Step 2: Clear any existing configurations on the switches if persistent.

Clear NVRAM, delete the vlan.dat file and reload the switches. Refer to Lab 2.2.1 if necessary for the procedure. After the reload is complete, use the **show vlan** command to confirm that only default VLANs exist and that all ports are assigned to VLAN 1.

Step 3: Disable all ports using the shutdown command.

Ensure that the initial switch port states are inactive by disabling all ports. Use the **interface-range** command to simplify this task.

Step 4: Re-enable the active user ports on switches in access mode.

Use the **no shutdown** command, and configure them as access ports.

Task 2: Perform Basic Switch Configurations

Configure the S1 and S2 switches according to the addressing table and the following guidelines:

- Configure the switch hostname.
- Disable DNS lookup.
- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.
- Configure the default gateway on each switch.

Task 3: Configure the Ethernet Interfaces on host PCs

Configure the Ethernet interfaces of PC1, PC2, PC3 with the IP addresses from the addressing table. Connect these devices using the correct cables and interfaces.

Task 4: Configure VTP on the Switches

Step 1: Configure VTP on the switches.

Use the following table to configure the switches. Remember that VTP domain names and passwords are case-sensitive.

Switch Name	VTP Operating Mode	VTP Domain	VTP Password
S1	Client	Lab6	cisco
S2	Server	Lab6	cisco

Step 2: Configure trunking ports on switches and designate the native VLAN for the trunks.

Configure Fa0/3 through Fa0/4 as trunking ports, and designate VLAN 99 as the native VLAN for these trunks. Use the **interface range** command in global configuration mode to simplify this task.

Step 3: Configure VLANs on the VTP server.

Configure the following VLANs on the VTP server.

VLAN	VLAN Name
VLAN 99	Management
VLAN 10	R&D
VLAN 20	Engineering
VLAN 30	Sales

Verify that the VLANs have been created on S2 with the **show vlan brief** command.

Step 4: Verify that the VLANs created on S2 have been distributed to S1.

Use the **show vlan brief** command on S1 to verify that the four VLANs have been distributed to the client switch.

Step 5: Configure the Management interface address on all switches.

Refer to the addressing table at the beginning of the lab to assign the management IP address on all switches.

Verify that the switches are correctly configured by pinging between them. From S1, ping the Management interface on S2. From S2, ping the Management interface on S1.

Were the pings successful? _____

If not, troubleshoot the switch configurations and resolve.

Step 6: Assign switch ports to appropriate VLANs.

Refer to the topology diagram at the beginning of the lab to assign ports to VLANs.

Step 7: Check connectivity between VLANs.

Ping from PC1 (192.168.10.21) to PC2 (192.168.20.22). Ping from PC2 to PC3 (192.168.30.23).

Are the pings successful? _____

If not, why do these pings fail? _____

Task 5: Configure the Router

Step 1: Clear the configuration on the router and reload.

Step 2: Create a basic configuration on the router.

- Configure the router with hostname R1.
- Disable DNS lookup.

- Configure an EXEC mode password of **class**.
- Configure a password of **cisco** for console connections.
- Configure a password of **cisco** for vty connections.

Step 3: Configure the trunking interface on R1.

You have demonstrated that connectivity between VLANs requires routing at the network layer, exactly like connectivity between any two remote networks. There are a couple of options for configuring routing between VLANs.

The first is something of a brute force approach. An L3 device, either a router or a Layer 3 capable switch, is connected to a LAN switch with multiple connections—a separate connection for each VLAN that requires inter-VLAN connectivity. Each of the switch ports used by the L3 device are configured in a different VLAN on the switch. After IP addresses are assigned to the interfaces on the L3 device, the routing table has directly connected routes for all VLANs, and inter-VLAN routing is enabled. The limitations to this approach are the lack of sufficient Fast Ethernet ports on routers, under-utilization of ports on L3 switches and routers, and excessive wiring and manual configuration. The topology used in this lab does not use this approach.

An alternative approach is to create one or more Fast Ethernet connections between the L3 device (the router) and the distribution layer switch, and to configure these connections as dot1q trunks. This allows all inter-VLAN traffic to be carried to and from the routing device on a single trunk. However, it requires that the L3 interface be configured with multiple IP addresses. This can be done by creating “virtual” interfaces, called subinterfaces, on one of the router Fast Ethernet ports and configuring them to dot1q aware.

Using the subinterface configuration approach requires these steps:

- Enter subinterface configuration mode
- Establish trunking encapsulation
- Associate a VLAN with the subinterface
- Assign an IP address from the VLAN to the subinterface

The commands are as follows:

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no shutdown
R1(config-if)#interface fastethernet 0/0.1
R1(config-subif)#encapsulation dot1q 1
R1(config-subif)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#interface fastethernet 0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#interface fastethernet 0/0.20
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#interface fastethernet 0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.1 255.255.255.0
R1(config-if)#interface fastethernet 0/0.99
R1(config-subif)#encapsulation dot1q 99 native
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
```

Note the following points in this configuration:

- The physical interface is enabled using the **no shutdown** command, because router interfaces are down by default. The virtual interfaces are up by default.

- The subinterface can use any number that can be described with 32 bits, but it is good practice to assign the number of the VLAN as the interface number, as has been done here.
- The native VLAN is specified on the L3 device so that it is consistent with the switches. Otherwise, VLAN 1 would be the native VLAN by default, and there would be no communication between the router and the management VLAN on the switches.

Step 4: Verify the routing configuration.

At this point, there should be five networks configured on R1. Verify that you can route packets to all five by checking the routing table on R1.

If your routing table does not show all five networks, troubleshoot your configuration and resolve the problem before proceeding.

Step 5: Verify inter-VLAN routing

From PC1, verify that you can ping the other two hosts (192.168.20.22 and 192.168.30.23). It may take a couple of pings before the end-to-end path is established.

Are the pings successful? _____

If not, troubleshoot your configuration. Check to make sure the default gateways have been set on all PCs and all switches.

At this point, you should be able to ping any node on any of the five networks configured on your LAN, including the switch management interfaces.

Task 6: Clean Up

Erase the configurations. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.