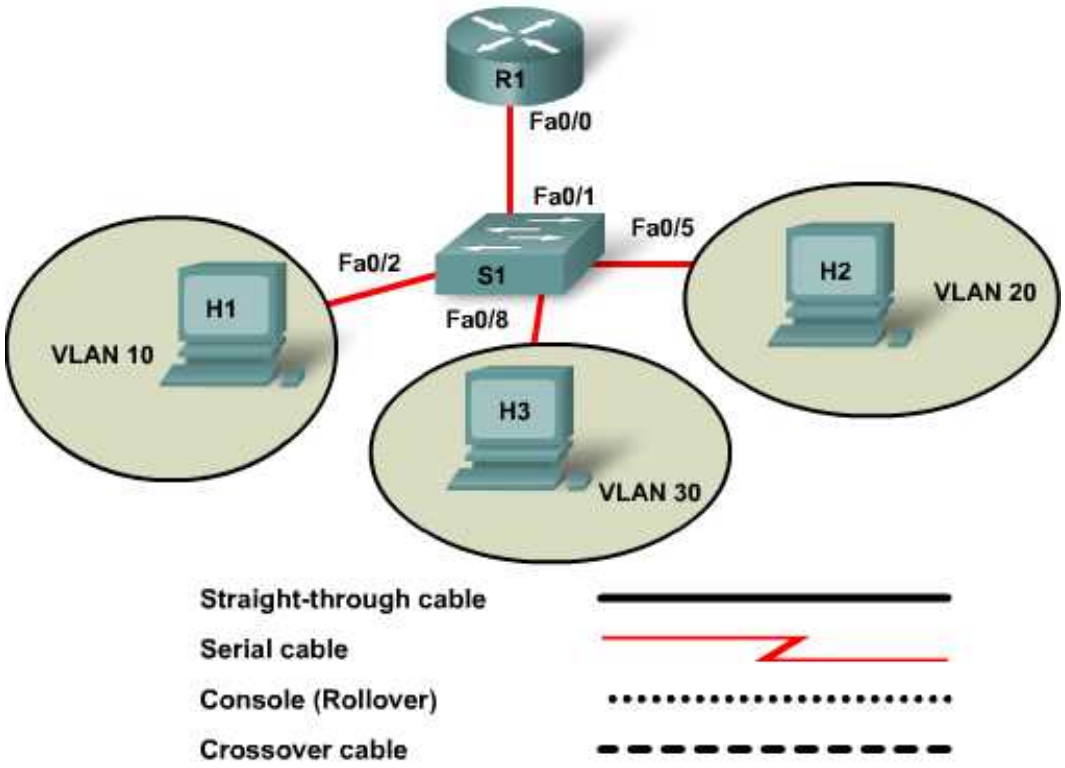
Lab 8.4.5 Configuring and Verifying ACLs to filter Inter-VLAN Traffic



Device	Host Name	FastEthernet IP Address	Default Gateway IP Address	VLAN Names and Numbers	Switch Port Assignments	Enable Secret Password	Enable, vty, and Console Password
Router 1	R1	Fa0/0: none Fa0/0.1: 192.168.1.1/24 Fa0/0.2: 192.168.2.1/24 Fa0/0.3: 192.168.3.1/24 Fa0/0.4: 192.168.4.1/24				class	cisco
Switch 1	S1	192.168.1.2/24	192.168.1.1	VLAN 1 Native VLAN 10 Servers VLAN 20 Users1 VLAN 30 Users2	Fa0/1 Fa0/2 Fa0/5 Fa0/8	class	cisco
Host 1	H1	192.168.2.10/24	192.168.2.1				
Host 2	H2	192.168.3.10/24	192.168.3.1				
Host 3	H3	192.168.4.10/24	192.168.4.1				

Objectives

- Configure VLANs on a switch.
- Configure and verify trunking.
- Configure a router for inter-VLAN routing.
- Configure, apply, and test an ACL to filter inter-VLAN traffic.

Background / Preparation

Cable a network similar to the one shown in the diagram. Any router that meets the interface requirements displayed on the topology diagram may be used. For example, router series 800, 1600, 1700, 1800, 2500, 2600, 2800, or any combination can be used.

The information in this lab applies to the 1841 router. Other routers may also work; however, the command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 or comparable switch
- One Cisco 1841 or comparable router
- Three Windows-based PCs, each with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switch
- Four straight-through Ethernet cables

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect the Fa0/0 interface of Router 1 to the Fa0/1 port of Switch 1 using a straight-through cable.

b. Connect PCs with console cables to perform configurations on the router and switch.

c. Connect the host PCs with straight-through cables to the following switch ports: Host 1, to Fa0/2; Host 2, to Fa0/5; Host 3, to Fa0/8.

Step 2: Perform basic configuration on Router 1

Step 3: Configure R1 to support inter-VLAN traffic

The FastEthernet 0/0 interface on R1 will be subinterfaced to route traffic from each of the three VLANs. Each subinterface IP address will become the default gateway for its designated VLAN.

```
R1#configure terminal
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-subif)#interface fastethernet 0/0.2
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.2.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.3
R1(config-subif)#encapsulation dot1q 20
R1(config-subif)#ip address 192.168.3.1 255.255.255.0
R1(config-subif)#interface fastethernet 0/0.4
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.4.1 255.255.255.0
R1(config-subif)#end
R1#copy running-config startup-config
```

Why is the **no shutdown** command performed only on interface FastEthernet 0/0?

_____

Why is it necessary to specify the encapsulation type on each subinterface?

_____

Step 4: Perform basic configuration on Switch 1

Step 5: Create, name, and assign ports to three VLANs on S1

This network contains one VLAN for the server farm and two VLANs for user groups.

Why is it good practice to place the server farm in a separate VLAN?

_____

a. Enter the following commands to create the three VLANs:

```
S1(config)#vlan 10
S1(config)#name Servers
S1(config)#vlan 20
S1(config)#name Users1
S1(config)#vlan 30
S1(config)#name Users2
```

b. Assign a port to each VLAN, according to the addressing table.

```
S1#configure terminal
S1(config)#interface fastethernet0/2
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 10

S1(config)#interface fastethernet0/5
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 20

S1(config)#interface fastethernet0/8
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 30
```

NOTE: For the purposes of this lab, only one representative interface is assigned to each VLAN. When assigning multiple ports to a VLAN, use the **range** parameter. For example, if assigning ports 0/2 through 0/4 to VLAN 10, use this command sequence:

```
S1(config)#interface range fastethernet 0/2 - 4
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 10
```

Step 6: Create the trunk on S1

Enter the following command to establish interface Fa0/1 as a trunk port:

```
S1(config)#interface fastethernet 0/1
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

Why is it not necessary to specify which trunking protocol (dot1q, ISL) will be used?

_____

Step 7: Configure the hosts

Configure each host with the proper IP address, subnet mask, and default gateway according to the addressing table.

Predict: If the configurations are correct, to which devices should a user at PC1 be able to ping successfully?

_____

Step 8: Verify that the network is functioning

a. From each attached host, ping the other two hosts and each of the router sub-interface IP addresses.

Were the pings successful? _____

If the answer is no, troubleshoot the router, switch and host configurations to find the error.

b. From the switch S1, ping the router default gateway 192.168.1.1.

Were the pings successful? _____

c. Use the command **show ip interfaces brief** and check the status of each interface or sub-interface.

What is the state of the interfaces?

R1:

FastEthernet 0/0: _____

FastEthernet 0/0.1: _____

FastEthernet 0/0.2: _____

FastEthernet 0/0.3: _____

FastEthernet 0/0.4: _____

S1:

Interface VLAN1: _____

d. Ping again until successful.

Step 9: Configure, apply, and test an Extended ACL to filter inter-VLAN traffic

Members of the Users1 VLAN should not be able to reach the server farm, but members of the other VLAN should be able to reach each other and the router. Users1 should be able to reach VLANs other than the server farm.

a. Create the extended ACL statements:

```
R1(config)#access-list 100 deny ip 192.168.3.0 0.0.0.255 192.168.2.0
0.0.0.255
R1(config)#access-list 100 permit ip any any
```

R1 has a FastEthernet 0/0 interface and four subinterfaces. Where should this ACL be placed, and in which direction? Why?

_____

b. Apply the ACL, and test by pinging from PC2 to PC1 and to PC3.

If the ACL is working properly, pings from PC2 to PC1 should fail. All other pings should succeed. If results fail to meet these criteria, troubleshoot the ACL syntax and placement.

Step 10: Reflection

a. Why is it good practice to perform and verify basic and VLAN-related configurations before creating and applying an ACL?

_____

_____

b. What results would have been produced if the ACL had been placed on subinterface FastEthernet 0/0.3 going out and PC2 pinged PC3?

_____