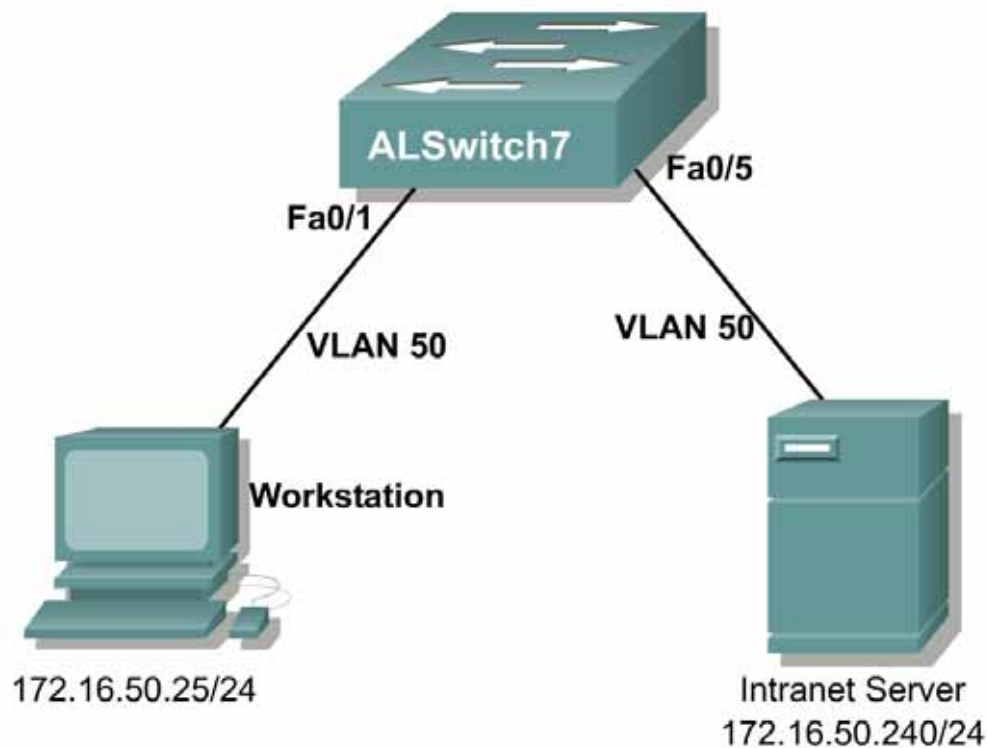


Lab 7.2.5.2 Configuring VLAN Maps



Objective

In this lab, students will configure VLAN Access Control Lists (ACLs) for IP addresses in a common VLAN.

Equipment

The following equipment will be needed to complete this lab:

- Catalyst 3550 series switch
- IOS 12.1(11)EA1
- Network capable workstation with a Web browser application
- Network capable system with Web server application or router to simulate a Web server

Scenario

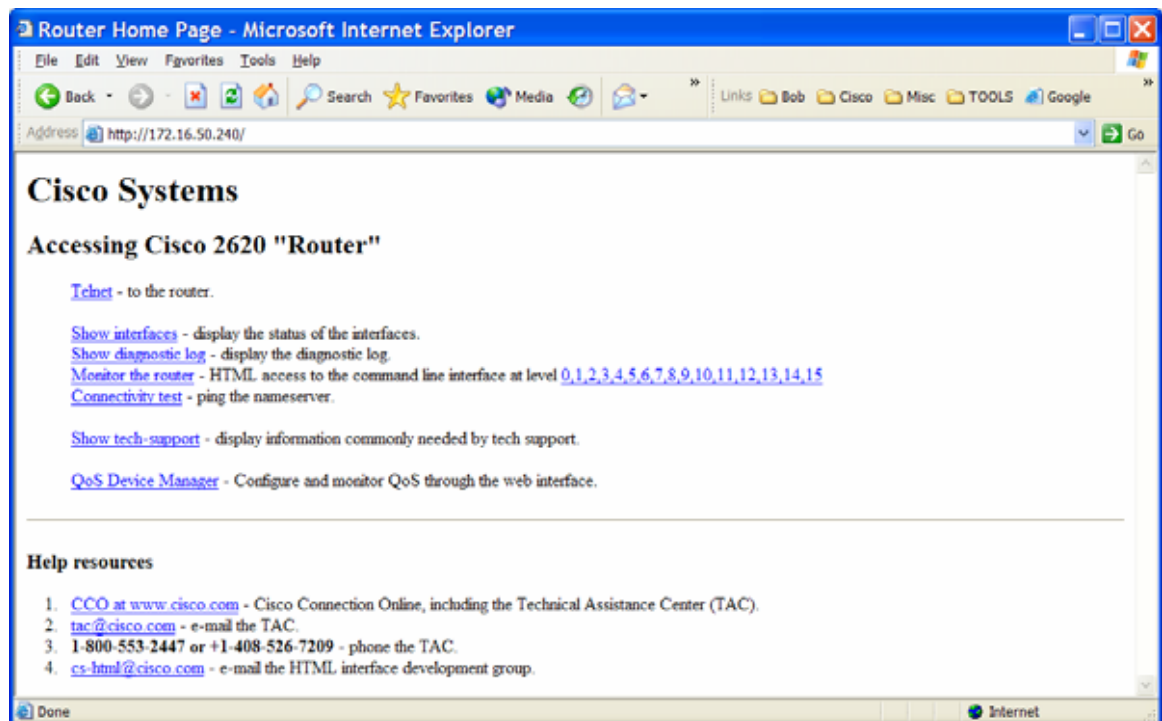
The Human Resources (HR) Director has decided to improve security by implementing VLAN ACLs. This will make it possible to control user traffic within the Human Resources department VLAN. The switch handling all of the HTTP traffic for the HR department must be configured to control access to the HR intranet server, limiting it to a small range of IP addresses.

All of the client machines in the HR subnet are allocated an address by Dynamic Host Configuration Protocol (DHCP) from the pool 172.16.50.1 to 172.16.50.127 / 24. Only hosts in the range 172.16.50.16 to 172.16.50.31 are allowed to access the web server.

Step 1 Configure the network

Build and configure the network according to the diagram. Create VLAN 50 with the name "HR" and assign interfaces FastEthernet 0/1 through 0/5 to VLAN 50.

The HR client at 172.16.50.25 /24 should be able to access the HR Intranet server at 172.16.50.240 /24. In the following sample output, a router was used to simulate the Web Server.



Step 2 Create the access list

Using the information provided in the network diagram, create a named extended access list called **HRServerAllowed** that matches the profile of the authorized traffic. Be as specific as possible with the ACL so other traffic flows are not affected.

```
ALSwitch7(config)#ip access-list extended HRServerAllowed
ALSwitch7(config-ext-nacl)#permit tcp 172.16.50.16 0.0.0.15 host
172.16.50.240 eq www
ALSwitch7(config-ext-nacl)#end
```

Verify the ACL configuration:

```
ALSwitch7#show access-lists
Extended IP access list HRServerAllowed
    permit tcp 172.16.50.16 0.0.0.15 host 172.16.50.240 eq www
ALSwitch7#
```

Now create another extended named access list called **HRServerBlocked** that matches the profile of all of the traffic that must be blocked. Include all traffic from the network 172.16.50.0 /25 to be as specific as possible with the ACL so other traffic flows are not affected.

```
ALSwitch7(config)#ip access-list extended HRServerBlocked
ALSwitch7(config-ext-nacl)#permit tcp 172.16.50.0 0.0.0.127 host
172.16.50.240 eq www
ALSwitch7(config-ext-nacl)#end
```

Verify the ACL configuration:

```
ALSwitch7#show ip access-list
Extended IP access list HRServerAllowed
    permit tcp 172.16.50.16 0.0.0.15 host 172.16.50.240 eq www
Extended IP access list HRServerBlocked
    permit tcp 172.16.50.0 0.0.0.127 host 172.16.50.240 eq www
ALSwitch7#
```

1. Why is the ACL HRServerBlocked using a **permit** statement?

Now create a third extended named access list called **HRServerDefaults** to allow all other IP traffic through the VLAN map.

```
ALSwitch7(config)#ip access-list extended HRServerDefaults
ALSwitch7(config-ext-nacl)#permit ip any any
ALSwitch7(config-ext-nacl)#end
```

Verify the ACL configuration:

```
ALSwitch7#show ip access-list
Extended IP access list HRServerAllowed
    permit tcp 172.16.50.16 0.0.0.15 host 172.16.50.240 eq www
Extended IP access list HRServerBlocked
    deny tcp 172.16.50.0 0.0.0.127 host 172.16.50.240 eq www
Extended IP access list HRServerDefaults
    permit ip any any
```

Step 3 Create and configure the VLAN access map

Create a VLAN access map named **HRServerMap** with a sequence number of 10:

```
ALSwitch7(config)#vlan access-map HRServerMap 10
```

Bind the access list **HRServerAllowed** to the VLAN access map **HRServerMap 10**. Set the action to forward packets matching the ACL, then return to global configuration mode:

```
ALSwitch7(config-access-map)#match ip address HRServerAllowed
```

```
ALSwitch7(config-access-map)#action forward
ALSwitch7(config-access-map)#exit
ALSwitch7(config)#
```

Add to the VLAN access map with a sequence number of 20, binding the access list **HRServerBlocked** to the VLAN access map **HRServerMap**. Set the action to drop packets matching the ACL, then return to global configuration mode:

```
ALSwitch7(config)#vlan access-map HRServerMap 20
ALSwitch7(config-access-map)#match ip address HRServerBlocked
ALSwitch7(config-access-map)#action drop
ALSwitch7(config-access-map)#exit
ALSwitch7(config)#
```

Bind the access list **HRServerDefault** to the VLAN access-map **HRServerMap** using a sequence number of 30. Set the action to forward packets matching the ACL, then return to privileged mode:

```
ALSwitch7(config)#vlan access-map HRServerMap 30
ALSwitch7(config-access-map)#match ip address HRServerDefaults
ALSwitch7(config-access-map)#action forward
ALSwitch7(config-access-map)#end
ALSwitch7#
```

Verify the VLAN access-map configuration so far:

```
ALSwitch7#show vlan access-map
Vlan access-map "HRServer" 10
  Match clauses:
    ip address: HRServerAllowed
  Action:
    forward
Vlan access-map "HRServerMap" 20
  Match clauses:
    ip address: HRServerBlocked
  Action:
    drop
Vlan access-map "HRServerMap" 30
  Match clauses:
    ip address: HRServerDefaults
  Action:
    forward
ALSwitch7#
```

Step 4 Apply the VLAN access map to the HR VLAN

Enable VLAN filtering on VLAN 50 using the newly created VLAN access map.

2. What is the command to apply the VLAN access-map **HRServerMap** to the HR VLAN?

Return to privileged mode, and verify the VLAN filter configuration:

```
ALSwitch7#show vlan filter
VLAN Map HRServerMap is filtering VLANs:
 50
ALSwitch7#
```

Step 5 Test connectivity from an allowed host

Verify connectivity between the workstation and the HR Intranet server (172.16.50.240) using a Web browser. Troubleshoot if necessary.

3. Can the workstation connect to the web server running on the HR Intranet server? Explain:

Step 6 Test connectivity from a blocked host

Close the Web browser window and change the IP address on the client workstation to 172.16.50.125/24.

Verify connectivity between the workstation and the HR Intranet server (172.16.50.240) using a new Web browser window. It is important that a new Web browser window be used since the browser could return the webpage cached from memory, leading to false assumptions. Troubleshoot if necessary.

4. Can the workstation connect to the web server running on the HR Intranet server? Explain: