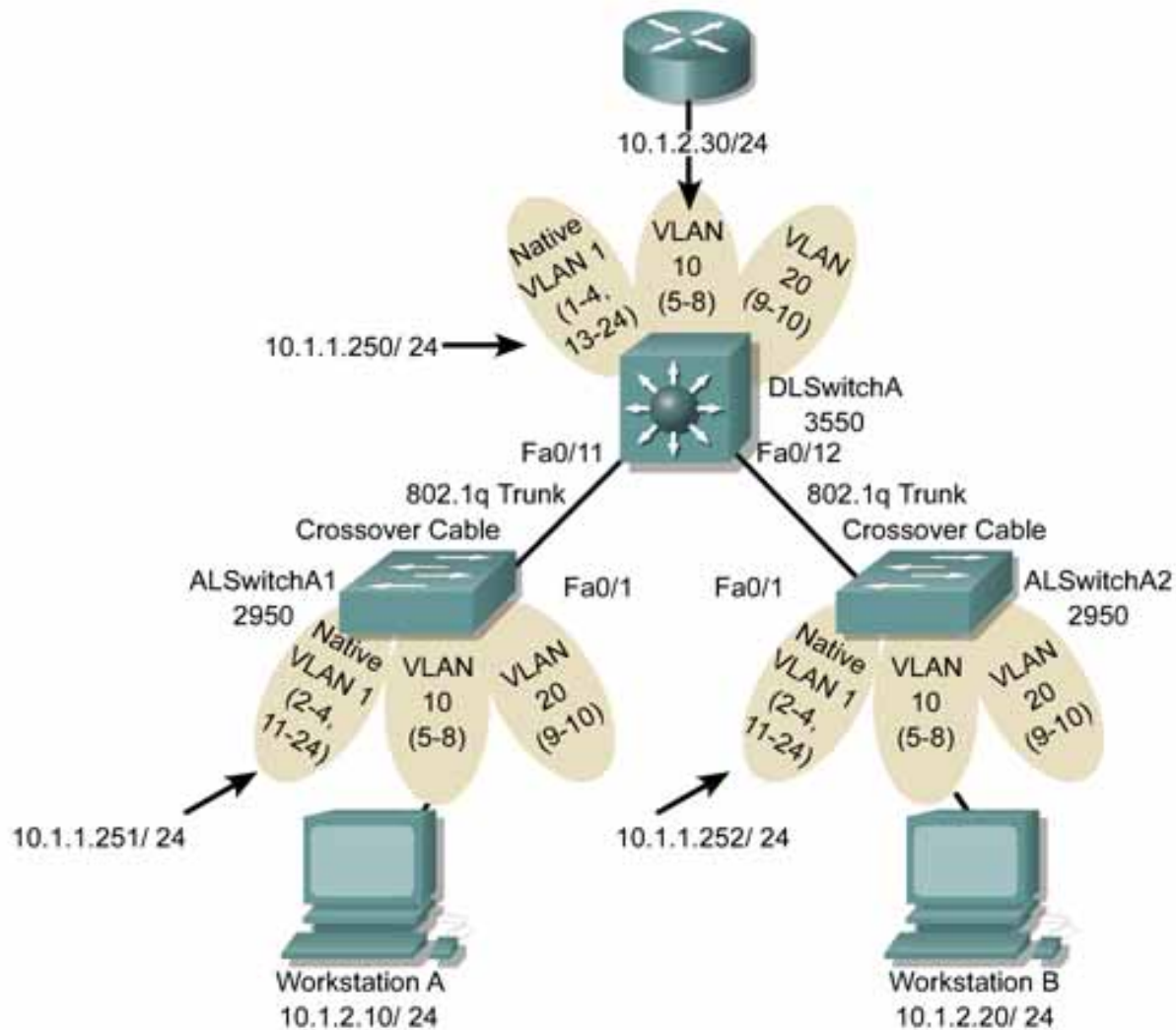




Lab 7.2.5.1 Catalyst 2950 and 3550 Series Intra-VLAN Security



Objective

Configure intra-VLAN security with Access Control Lists (ACLs) using the command-line interface (CLI) mode.

Scenario

This lab will cover how to configure basic intra-VLAN network security on a switch by using Access Control Lists (ACLs).

The 3550 switch with EMI supports three applications of ACLs to filter traffic:

- Router ACLs access-control routed traffic between VLANs and are applied to Layer 3 interfaces. You can apply one router ACL in each direction on an interface.

- Port ACLs access-control traffic entering a Layer 2 interface. The switch does not support port ACLs in the outbound direction. You can apply only one IP access list and one MAC access list to a Layer 2 interface.
- VLAN ACLs or VLAN maps access-control all packets (bridged and routed). You can use VLAN maps to filter traffic between devices in the same VLAN. VLAN maps are configured to provide access-control based on Layer 3 addresses for IP. Unsupported protocols are access-controlled through MAC addresses by using Ethernet ACEs. After a VLAN map is applied to a VLAN, all packets (routed or bridged) entering the VLAN are checked against the VLAN map. Packets can either enter the VLAN through a switch port or through a routed port after being routed.

This lab will implement Port ACL's to filter intra-VLAN IP traffic.

Step 1

If the same switches and setup from Lab 2.9.3 are used, verify connectivity with a **ping** between switches and between workstations. When done, then continue with Step 2.

If different set of switches is used, it is necessary to insure there are no inappropriate VTP, VLAN information, or other configurations present. Disconnect any cables from the switches and power up the switches. Delete the startup configuration and the VLAN database (vlan.dat). Then reload the switches and cable the lab according to the lab diagram. Finally, load the configurations from Lab 2.9.3.

Enable VLAN 1 on all switches with the **no shutdown** interface command.

On DLSwitchA, enter the VTP domain name to enable VTP and pruning. Then reenter the VLAN names as follows:

```
DLSwitchA#vlan database
DLSwitchA(vlan)#vtp domain CORP
Changing VTP domain name from NULL to CORP
DLSwitchA(vlan)#vtp pruning
Pruning switched ON
DLSwitchA(vlan)#vlan 10 name Accounting
VLAN 10 added:
    Name: Accounting
DLSwitchA(vlan)#vlan 20 name Marketing
VLAN 20 added:
    Name: Marketing
DLSwitchA(vlan)#exit
APPLY completed.
Exiting....
```

Although it is not absolutely necessary, reset ALSwitchA1 and ALSwitchA2 to the VTP client mode by issuing the following commands:

```
ALSwitchA1#vlan database
ALSwitchA1(vlan)#vtp client
Setting device to VTP CLIENT mode.
ALSwitchA1(vlan)#exit
In CLIENT state, no apply attempted.
Exiting....

ALSwitchA2#vlan database
ALSwitchA2(vlan)#vtp client
Setting device to VTP CLIENT mode.
ALSwitchA2(vlan)#exit
In CLIENT state, no apply attempted.
Exiting....
```

Verify connectivity with a **ping** between switches and between workstations.

Sample outputs in this lab are based upon the continuation of this lab from Lab 2.9.3 using the same switches and setup. If different switches are used and the Lab 2.9.3 configurations were loaded on these switches, the output may appear slightly different. However, it will not impact successful completion of this lab.

Step 2

Connect a router to port 5 of the DLSwitchA to simulate a file server and configure as follows:

```
Router#configure terminal
Router(config)#hostname Server
Server(config)#ip http server
Server(config)#interface FastEthernet0/0
Server(config-if)#ip address 10.1.2.30 255.255.255.0
Server(config-if)#no shutdown
Server(config-if)#line console 0
Server(config-line)#password cisco
Server(config-line)#login
Server(config-line)#line vty 0 4
Server(config-line)#password cisco
Server(config-line)#login
Server(config-line)#^z
```

Verify connectivity with a **ping** between the Management VLANs of the switches, between workstations, and between the workstations and router. All **ping** attempts should be successful.

```
Server#ping 10.1.2.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.30, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms

Server#ping 10.1.2.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms

Server#ping 10.1.2.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.2.20, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

Step 3

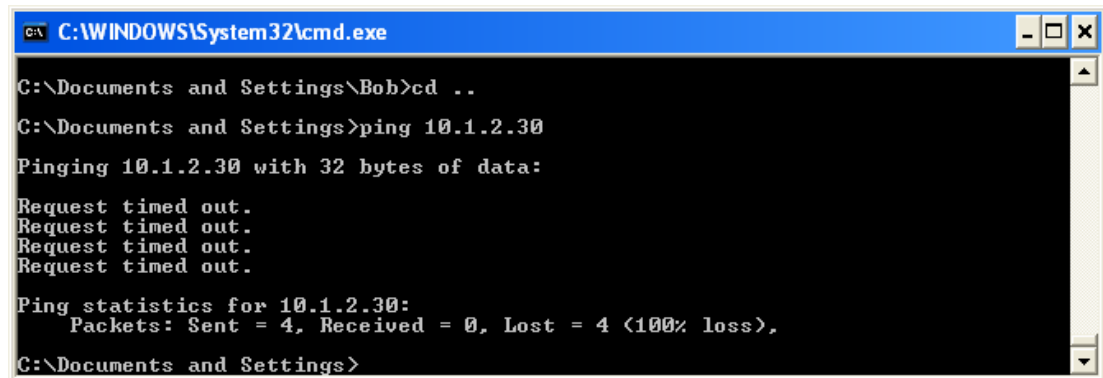
On the DLSwitchA, configure an ACL to deny ICMP **echo-reply** from Workstation A to the Server. Apply the ACL to Fa0/5 as incoming:

```
DLSwitchA#configure terminal
DLSwitchA(config)# access-list 101 deny icmp host 10.1.2.30 host 10.1.2.10
                        echo-reply

DLSwitchA(config)#access-list 101 permit ip any any
DLSwitchA(config)#interface FastEthernet 0/5
DLSwitchA(config-if)#ip access-group 101 in
DLSwitchA(config-if)#^z
```

In the preceding configuration, the ACL can only be applied as inbound on the Fa0/5 interface because a switch does not support an outbound ACL.

The ICMP **ping** traffic from Workstation A to the server should now be blocked.

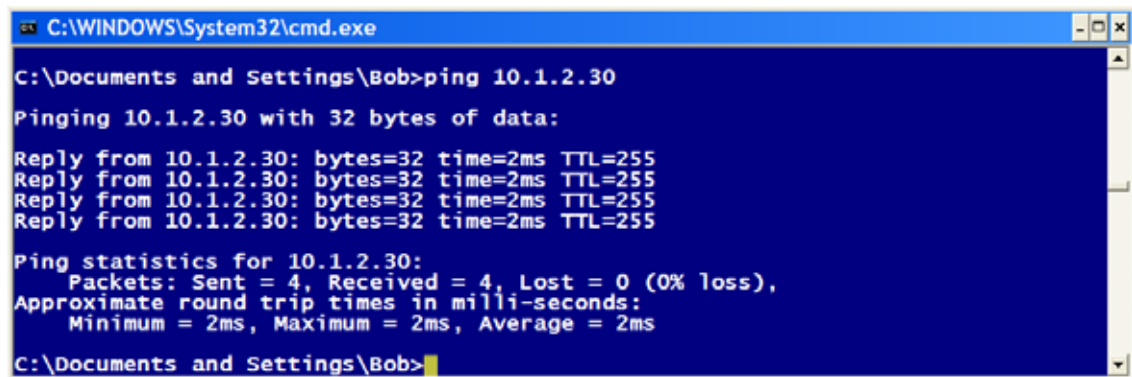


```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Bob>cd ..
C:\Documents and Settings>ping 10.1.2.30
Pinging 10.1.2.30 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.2.30:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Documents and Settings>
```

Verify that a **ping** from Workstation B to the Server is still successful.



```
C:\WINDOWS\System32\cmd.exe

C:\Documents and Settings\Bob>ping 10.1.2.30
Pinging 10.1.2.30 with 32 bytes of data:
Reply from 10.1.2.30: bytes=32 time=2ms TTL=255
Reply from 10.1.2.30: bytes=32 time=2ms TTL=255
Reply from 10.1.2.30: bytes=32 time=2ms TTL=255
Reply from 10.1.2.30: bytes=32 time=2ms TTL=255

Ping statistics for 10.1.2.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
C:\Documents and Settings\Bob>
```

1. Should a **ping** from the server to Workstation A (10.1.2.10) be successful? Why?

Verify with a **ping** from the server to Workstation A (10.1.2.10).

2. Should a **ping** from the server to Workstation B (10.1.2.20) be successful? Why?

Verify with a **ping** from the Server to Workstation B (10.1.2.20).

3. Should a **ping** from Workstation A to Workstation B and another **ping** back from Workstation B to Workstation A be successful? Why?

Verify with a **ping** from Workstation A (10.1.2.10) to Workstation B (10.1.2.20) or with a **ping** from Workstation B (10.1.2.20) to Workstation A (10.1.2.10).

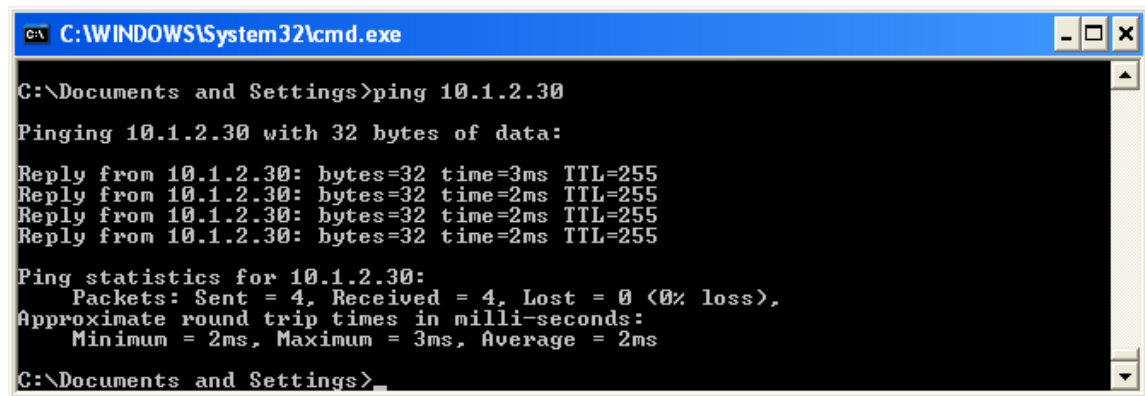
Step 4

Issue the following to remove the first access list from the DLSwitchA. Then create another one that will deny Telnet and HTTP access to the server from Workstation B:

```
DLSwitchA#configure terminal
DLSwitchA(config)#no access-list 101
DLSwitchA(config)#access-list 101 deny tcp host 10.1.2.30 eq telnet host
10.1.2.20
DLSwitchA(config)#access-list 101 deny tcp host 10.1.2.30 eq www host
10.1.2.20
DLSwitchA(config)#access-list 101 permit ip any any
DLSwitchA(config-if))#^z
```

Notice that the ACL denies Telnet and WWW traffic from the source address (10.1.2.30) and not from the destination (10.1.2.20) as it is usually applied. Again, this is because the Fa0/5 interface has the ACL applied as inbound. It is not necessary to reapply the access list to interface FastEthernet 0/5.

A **ping** from Workstation A to the Server (10.1.2.30) should now be successful, because the first access list is no longer applicable. Verify this with a **ping**.



Step 5

Test the new ACL. Attempt to **telnet** from Workstation B to the server (10.1.2.30), then open a web browser and attempt to access the server (10.1.2.30). Both attempts should fail.

1. Should a **ping** from Workstation B to the server (10.1.2.30) be successful? Why?

Verify with a **ping** from Workstation B to the Server (10.1.2.30).

2. Should Telnet and HTTP access to the Server (10.1.2.30) from Workstation A (10.1.2.10) be successful? Why?

Verify by **telnetting** into the server (10.1.2.30) from Workstation B. Then open a browser in Workstation B and access the server (10.1.2.30) by way of HTTP.

Intra-VLAN security with Access Control Lists has now been successfully configured.

Refer to the Catalyst 3550 Multilayer Switch Software Configuration Guide and the Catalyst 2950 Desktop Switch Software Configuration Guide for more information about configuring network security on the Cisco Catalyst WS-C3550 and WS-C2950 switches.