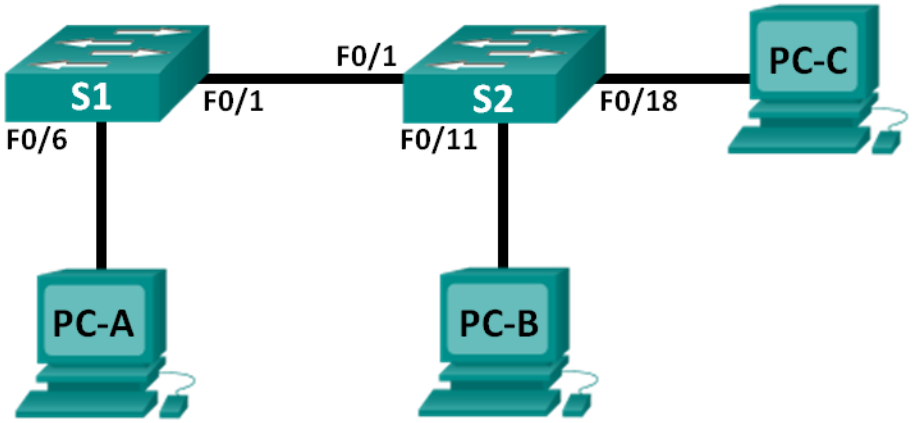
Lab – Implementing VLAN Security

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
PC-A	NIC	172.17.99.3	255.255.255.0	172.17.99.1
PC-B	NIC	172.17.10.3	255.255.255.0	172.17.10.1
PC-C	NIC	172.17.99.4	255.255.255.0	172.17.99.1

VLAN Assignments

VLAN	Name
10	Data
99	Management&Native
999	BlackHole

Objectives

Part 1: Build the Network and Configure Basic Device Settings

Part 2: Implement VLAN Security on the Switches

Background / Scenario

Best practice dictates configuring some basic security settings for both access and trunk ports on switches. This will help guard against VLAN attacks and possible sniffing of network traffic within the network.

In this lab, you will configure the network devices in the topology with some basic settings, verify connectivity and then apply more stringent security measures on the switches. You will examine how Cisco switches behave by using various **show** commands. You will then apply security measures.

Note: The switches used with this lab are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Build the Network and Configure Basic Device Settings

In Part 1, you will configure basic settings on the switches and PCs. Refer to the Addressing Table for device names and address information.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the switches.

Step 3: Configure IP addresses on PC-A, PC-B, and PC-C.

Refer to the Addressing Table for PC address information.

Step 4: Configure basic settings for each switch.

a. Disable DNS lookup.

b. Configure the device names as shown in the topology.

c. Assign **class** as the privileged EXEC mode password.

d. Assign **cisco** as the console and VTY password and enable login for console and vty lines.

e. Configure synchronous logging for console and vty lines.

Step 5: Configure VLANs on each switch.

a. Create and name VLANs according to the VLAN Assignments table.

b. Configure the IP address listed in the Addressing Table for VLAN 99 on both switches.

c. Configure F0/6 on S1 as an access port and assign it to VLAN 99.

d. Configure F0/11 on S2 as an access port and assign it to VLAN 10.

e. Configure F0/18 on S2 as an access port and assign it to VLAN 99.

f. Issue **show vlan brief** command to verify VLAN and port assignments.

To which VLAN would an unassigned port, such as F0/8 on S2, belong?

Step 6: Configure basic switch security.

a. Configure a MOTD banner to warn users that unauthorized access is prohibited.

b. Encrypt all passwords.

c. Shut down all unused physical ports.

d. Disable the basic web service running.

```
S1(config)# no ip http server
S2(config)# no ip http server
```

e. Copy the running configuration to startup configuration.

Step 7: Verify connectivity between devices and VLAN information.

a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

b. From S1, ping the management address of S2. Were the pings successful? Why?

c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

d. From a command prompt on PC-C, ping the management addresses on S1 and S2. Were you successful? Why?

Note: It may be necessary to disable the PC firewall to ping between PCs.

Part 2: Implement VLAN Security on the Switches

Step 1: Configure trunk ports on S1 and S2.

a. Configure port F0/1 on S1 as a trunk port.

```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
```

b. Configure port F0/1 on S2 as a trunk port.

```
S2(config)# interface f0/1
S2(config-if)# switchport mode trunk
```

c. Verify trunking on S1 and S2. Issue the **show interface trunk** command on both switches.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
```

```
Fa0/1       on              802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,99,999
```

Step 2: Change the native VLAN for the trunk ports on S1 and S2.

Changing the native VLAN for trunk ports from VLAN 1 to another VLAN is a good practice for security.

a. What is the current native VLAN for the S1 and S2 F0/1 interfaces?

b. Configure the native VLAN on the S1 F0/1 trunk interface to Management&Native VLAN 99.

```
S1# config t
S1(config)# interface f0/1
S1(config-if)# switchport trunk native vlan 99
```

c. Wait a few seconds. You should start receiving error messages on the console session of S1. What does the %CDP-4-NATIVE_VLAN_MISMATCH: message mean?

d. Configure the native VLAN on the S2 F0/1 trunk interface to VLAN 99.

```
S2(config)# interface f0/1
S2(config-if)# switchport trunk native vlan 99
```

e. Verify that the native VLAN is now 99 on both switches. S1 output is shown below.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       1-4094

Port        Vlans allowed and active in management domain
Fa0/1       1,10,99,999

Port         Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,999
```

Step 3: Verify that traffic can successfully cross the trunk link.

a. From a command prompt on PC-A, ping the management address of S1. Were the pings successful? Why?

b. From the console session on S1, ping the management address of S2. Were the pings successful? Why?

c. From a command prompt on PC-B, ping the management addresses on S1 and S2 and the IP address of PC-A and PC-C. Were your pings successful? Why?

d. From a command prompt on PC-C, ping the management addresses on S1 and S2 and the IP address of PC-A. Were you successful? Why?

Step 4: Prevent the use of DTP on S1 and S2.

Cisco uses a proprietary protocol known as the Dynamic Trunking Protocol (DTP) on its switches. Some ports automatically negotiate to trunking. A good practice is to turn off negotiation. You can see this default behavior by issuing the following command:

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

a. Turn off negotiation on S1.

```
S1(config)# interface f0/1
S1(config-if)# switchport nonegotiate
```

b. Turn off negotiation on S2.

```
S2(config)# interface f0/1
S2(config-if)# switchport nonegotiate
```

c. Verify that negotiation is off by issuing the **show interface f0/1 switchport** command on S1 and S2.

```
S1# show interface f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
<Output Omitted>
```

Step 5: Secure access ports on S1 and S2.

Even though you shut down unused ports on the switches, if a device is connected to one of those ports and the interface is enabled, trunking could occur. In addition, all ports by default are in VLAN 1. A good practice is to put all unused ports in a “black hole” VLAN. In this step, you will disable trunking on all unused ports. You will also assign unused ports to VLAN 999. For the purposes of this lab, only ports 2 through 5 will be configured on both switches.

a. Issue the **show interface f0/2 switchport** command on S1. Notice the administrative mode and state for trunking negotiation.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
<Output Omitted>
```

b. Disable trunking on S1 access ports.

```
S1(config)# interface range f0/2 – 5
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 999
```

c. Disable trunking on S2 access ports.

d. Verify that port F0/2 is set to access on S1.

```
S1# show interface f0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 999 (BlackHole)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
<Output Omitted>
```

e. Verify that VLAN port assignments on both switches are correct. S1 is shown below as an example.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
10   Data                             active
99   Management&Native                active    Fa0/6
999  BlackHole                        active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
1002 fddi-default                       act/unsup
1003 token-ring-default                 act/unsup
1004 fddinet-default                    act/unsup
1005 trnet-default                      act/unsup
Restrict VLANs allowed on trunk ports.
```

By default, all VLANs are allowed to be carried on trunk ports. For security reasons, it is a good practice to only allow specific desired VLANs to cross trunk links on your network.

f. Restrict the trunk port F0/1 on S1 to only allow VLANs 10 and 99.

```
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,99
```

g. Restrict the trunk port F0/1 on S2 to only allow VLANs 10 and 99.

h. Verify the allowed VLANs. Issue a **show interface trunk** command in privileged EXEC mode on both S1 and S2.

```
S1# show interface trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/1       10,99

Port        Vlans allowed and active in management domain
Fa0/1       10,99

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,99
```

What is the result?

Reflection

What, if any, are the security problems with the default configuration of a Cisco switch?