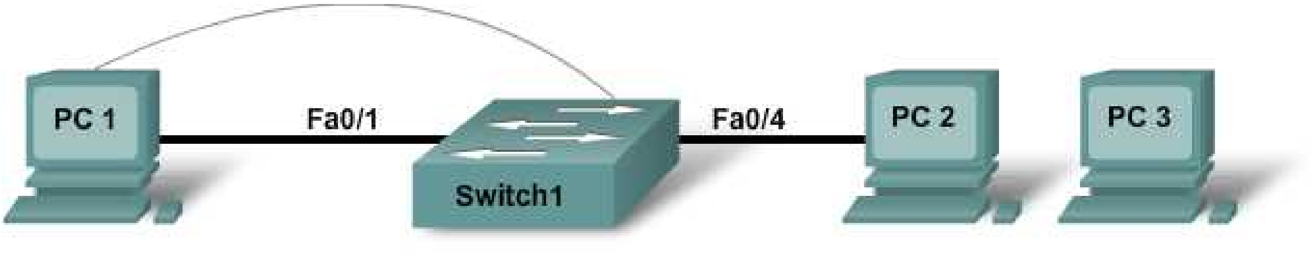
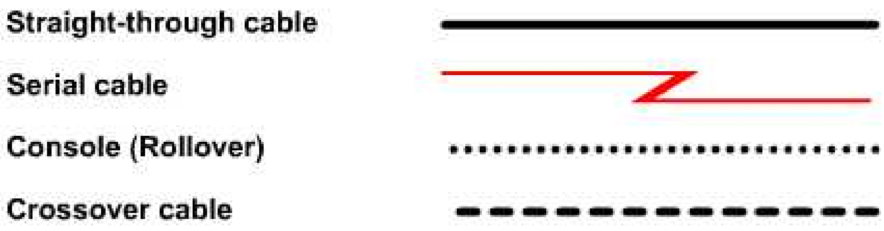
Lab 3.1.4 Applying Basic Switch Security





Device Designation	IP Address	Subnet Mask	Default Gateway	Enable Secret Password	vty and Console Password
PC 1	192.168.1.3	255.255.255.0	192.168.1.1		
PC 2	192.168.1.4	255.255.255.0	192.168.1.1		
PC 3	192.168.1.5	255.255.255.0	192.168.1.1		
Switch1	192.168.1.2	255.255.255.0	192.168.1.1	class	cisco

Objectives

- Configure passwords to ensure that access to the CLI is secured.
- Configure a switch to remove http server status for security.
- Configure port security.
- Disable unused ports.
- Test security configuration by connecting unspecified hosts to secure ports.

Background / Preparation

Set up a network similar to the one in the topology diagram.

The following resources are required:

- One Cisco 2960 or comparable switch
- Three Windows-based PCs, at least one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable

- Two straight-through Ethernet cables (PC1 and PC2 to switch)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

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

Step 1: Connect PC1 to the switch

a. Connect PC1 to Fast Ethernet switch port Fa0/1. Configure PC1 to use the IP address, mask, and gateway shown in the table.

b. Establish a terminal emulation session to the switch from PC1.

Step 2: Connect PC2 to the switch

a. Connect PC2 to Fast Ethernet switch port Fa0/4.

b. Configure PC2 to use the IP address, mask, and gateway shown in the table.

Step 3: Configure PC3 but do not connect

A third host is needed for this lab.

a. Configure PC3 using IP address 192.168.1.5. The subnet mask is 255.255.255.0, and the default gateway is 192.168.1.1.

b. Do not connect this PC to the switch yet. It will be used for testing security.

Step 4: Perform an initial configuration on the switch

a. Configure the hostname of the switch as **Switch1**.

```
Switch>enable
Switch#config terminal
Switch(config)#hostname Switch1
```

b. Set the privileged EXEC mode password to **cisco**.

```
Switch1(config)#enable password cisco
```

c. Set the privileged EXEC mode secret password to **class**.

```
Switch1(config)#enable secret class
```

d. Configure the console and virtual terminal lines to use a password and require it at login.

```
Switch1(config)#line console 0
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#line vty 0 15
Switch1(config-line)#password cisco
Switch1(config-line)#login
Switch1(config-line)#end
```

e. Exit from the console session and log in again.

Which password was required to enter privileged EXEC mode? ______________________________

Why? ____

Step 5: Configure the switch management interface on VLAN 1

a. Enter the interface configuration mode for VLAN 1.

```
Switch1(config)#interface vlan 1
```

b. Set the IP address, subnet mask, and default gateway for the management interface.

```
Switch1(config-if)#ip address 192.168.1.2 255.255.255.0
Switch1(config-if)#no shutdown
Switch1(config-if)#exit
Switch1(config)#ip default-gateway 192.168.1.1
Switch1(config)#end
```

Why does interface VLAN 1 require an IP address in this LAN?

____

What is the purpose of the default gateway?

____

Step 6: Verify the management LANs settings

a. Verify that the IP address of the management interface on the switch VLAN 1 and the IP address of PC1 and PC2 are on the same local network. Use the **show running-config** command to check the IP address configuration of the switch.

b. Verify the interface settings on VLAN 1.

```
Switch1#show interface vlan 1
```

What is the bandwidth on this interface? ____

What are the VLAN states?

VLAN 1 is __________ and line protocol is __________.

Step 7: Disable the switch from being an http server

Turn off the feature of the switch being used as an http server.

```
Switch1(config)#no ip http server
```

Step 8: Verify connectivity

a. To verify that hosts and switch are correctly configured, ping the switch IP address from the hosts.

Were the pings successful? ___________________________

If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host and switch configurations.

b. Save the configuration.

Step 9: Record the host MAC addresses

Determine and record the Layer 2 addresses of the PC network interface cards. From the command prompt of each PC, enter **ipconfig /all**.

PC1 ____

PC2 ____

PC3 ____

Step 10: Determine what MAC addresses the switch has learned

Determine what MAC addresses the switch has learned by using the **show mac-address-table** command at the privileged EXEC mode prompt.

```
Switch1#show mac-address-table
```

How many dynamic addresses are there? ____________

How many total MAC addresses are there? ___________

Do the MAC addresses match the host MAC addresses? ___________

Step 11: View the show mac-address-table options

View the options that the **show mac-address-table** command has available.

```
Switch1(config)#show mac-address-table ?
```

What options are available? ____

____

Step 12: Set up a static MAC address

Set up a static MAC address on FastEthernet interface 0/4. Use the address that was recorded for PC2 in Step 9. The MAC address 00e0.2917.1884 is used in this example statement only.

```
Switch1(config)#mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Step 13: Verify the results

a. Verify the MAC address table entries.

```
Switch1#show mac-address-table
```

How many dynamic MAC addresses are there now? _________

How many static MAC addresses are there now? ____________

b. Remove the static entry from the MAC Address Table.

```
Switch1(config)#no mac-address-table static 00e0.2917.1884 vlan 1
interface fastethernet 0/4
```

Step 14: List port security options

a. Determine the options for setting port security on interface FastEthernet 0/4.

```
Switch1(config)#interface fastethernet 0/4
Switch1(config-if)#switchport port-security ?
```

What are some available options? ____

b. To allow the switch port FastEthernet 0/4 to accept only one device, configure port security.

```
Switch1(config-if)#switchport mode access
Switch1(config-if)#switchport port-security
Switch1(config-if)#switchport port-security mac-address sticky
```

c. Exit configuration mode and check the port security settings.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1            0                0            Shutdown
---------------------------------------------------------------------------
```

If a host other than PC2 attempts to connect to Fa0/4, what will happen?

____

Step 15: Limit the number of hosts per port

a. On interface FastEthernet 0/4, set the port security maximum MAC count to 1.

```
Switch1(config-if)#switchport port-security maximum 1.
```

b. Disconnect the PC attached to FastEthernet 0/4. Connect PC3 to FastEthernet 0/4. PC3 has been given the IP address of 192.168.1.5 and has not yet been attached to the switch. It may be necessary to ping the switch address 192.168.1.2 to generate some traffic.

Record any observations. ____

____

Step 16: Configure the port to shut down if there is a security violation

a. In the event of a security violation, the interface should be shut down. To make the port security shut down, enter the following command:

```
Switch1(config-if)#switchport port-security violation shutdown
```

What other action options are available with port security? ______________________________

____

b. If necessary, ping the switch address 192.168.1.2 from the PC3 192.168.1.5. This PC is now connected to interface FastEthernet 0/4. This ensures that there is traffic from the PC to the switch.

c. Record any observations.

____

____

d. Check the port security settings.

```
Switch1#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4        1             1                0            Shutdown
---------------------------------------------------------------------------
```

Step 17: Show port 0/4 configuration information

To see the configuration information for FastEthernet port 0/4 only, enter **show interface fastethernet 0/4** at the privileged EXEC mode prompt.

```
Switch1#show interface fastethernet 0/4
```

What is the state of this interface?

FastEthernet0/4 is __________ and line protocol is __________.

Step 18: Reactivate the port

a. If a security violation occurs and the port is shut down, use the **shutdown** / **no shutdown** commands to reactivate the port.

b. Try reactivating this port a few times by switching between the original port 0/4 host and the new one. Plug in the original host, enter the **no shutdown** command on the interface, and ping using the command prompt.

The ping will have to be repeated multiple times; alternately, use the **ping 192.168.1.2 –n 200** command. This command sets the number of ping packets to 200 instead of 4. Then switch hosts and try again.

Step 19: Disable unused ports

Disable any ports not being used on the switch.

```
Switch1(config)#interface range Fa0/2 – 3
Switch1(config-if-range)#shutdown
Switch1(config-if-range)#exit
Switch1(config)#interface range Fa0/5 – 24
Switch1(config-if-range)#shutdown

Switch1(config)#interface range gigabitethernet0/1 - 2
Switch1(config-if-range)#shutdown
```

Step 20: Reflection

a. Why would port security be enabled on a switch? ____

____

b. Why should unused ports on a switch be disabled? ____

____