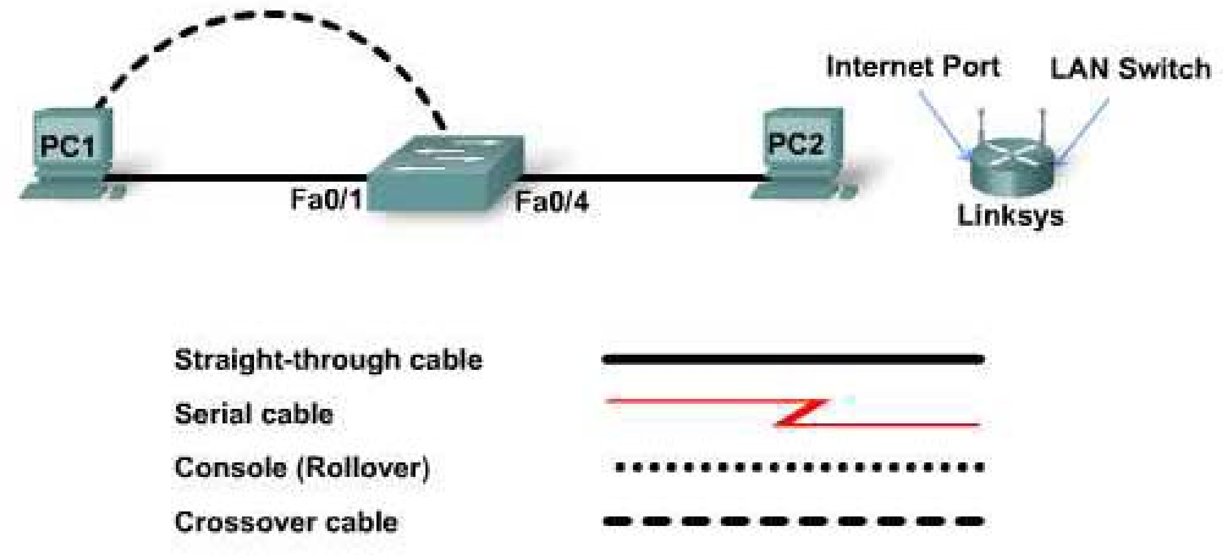
Lab 1.4.6B Implementing Port Security



Device Designation	Device Name	VLAN 1 Address	Subnet mask
S1	FC-ASW-1	10.0.0.2	255.255.255.0
PC1	Host 1	10.0.0.254	255.255.255.0
PC2	Host 2	10.0.0.253	255.255.255.0
Linksys Internet Port	Intruder	10.0.0.252	255.255.255.0

Objectives

- Configure port security on individual FastEthernet ports on a switch.
- Test and confirm the configured switch port security.

640-802 CCNA Exam Objectives

This lab contains skills that relate to the following CCNA exam objectives:

- Perform and verify initial switch configuration tasks, including remote access management.
- Verify network status and switch operation using basic utilities (including: ping, traceroute, Telnet, SSH, arp, ipconfig), and **show** and **debug** commands.
- Implement basic switch security (including port security, trunk access, management VLAN other than VLAN 1, etc.).

Expected Results and Success Criteria

Before starting this lab, read through the tasks that you are expected to perform. What do you expect the result of performing these tasks will be?

____

____

____

Why do you think that network administrators implement port security in their network?

____

____

____

How will a network administrator know if port security is working properly?

____

____

____

Background / Preparation

Network security is an important responsibility for network administrators and network designers. Access Layer switch ports are accessible through the structured cabling at wall outlets. Anyone can plug in a PC, laptop, or wireless Access Point at one of these outlets. These outlets are potential entry points to the network by unauthorized users.

Switches provide a feature called *port security*. With port security, it is possible to limit the number of MAC addresses that can be learned on an interface. The switch can be configured to take an action [shut down], if this number is exceeded. The number of MAC addresses per port can be limited, commonly to 1. The first address dynamically learned by that switch for that port becomes the secure address.

Using the given topology, this lab configures a switch to provide network access to only 2 PCs and tests this security by attempting to connect an "intruder" device, the Linksys Wireless Router, to the secure port.

Task 1: Configure and Test the Switch Connectivity

Step 1: Prepare the switch for configuration

NOTE: If the PCs used in this lab are also connected to your Academy LAN or to the Internet, ensure that you record the cable connections and TCP/IP settings so these can be restored at the conclusion of the lab.

a. Referring to the topology diagram, connect the console (or rollover) cable to the console port on the switch and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Ensure that power has been applied to both the host computer and switch.

b. Establish a console terminal session from PC1 to switch S1.

c. Prepare the switch for lab configuration by ensuring that all existing VLAN and general configurations are removed.

1) Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

2) Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

d. Power cycle the switch and exit the initial configuration setup when the switch restarts.

Step 2: Configure the switch

Configure the hostname and VLAN 1 interface IP address as shown in the table.

Step 3: Configure the hosts attached to the switch

a. Configure the two PCs to use the same IP subnet for the address and mask as shown in the table.

b. Connect PC1 to switch port Fa0/1 and PC2 to switch port Fa0/4. The Linksys device is not connected at this stage of the lab.

Step 4: Verify host connectivity

Ping between all PCs and the switch to verify correct configuration. If any ping was not successful, troubleshoot the hosts and switch configurations.

Step 5: Record the host MAC addresses

Determine and record the Layer 2 addresses of the PC network interface cards.

(For Windows 2000, XP, or Vista, check by using **`Start > Run > cmd > ipconfig /all`**.)

PC1 MAC Address: ________________________________

PC2 MAC Address: ________________________________

Step 6: Determine what MAC addresses the switch has learned

a. At the privileged EXEC mode prompt, issue the **`show mac-address-table`** command to display the PC MAC addresses that the switch has learned.

```
FC-ASW-1#show mac-address-table
```

Record the details displayed in the table.

____

____

b. Note the MAC addresses shown and the associated switch ports. Confirm that these addresses and ports match the connected PCs.

   How were these MAC addresses and port associations learned?

   ____

   ____

Task 2 Configure and Test the Switch for Dynamic Port Security

Step 1: Set port security options

a. Disconnect all PCs Ethernet cables from the switch ports.

b. Ensure that the MAC address table is clear of entries. To confirm this, issue the **`clear mac-address-table dynamic`** and **`show mac-address-table`** commands.

a. Clear the MAC address table entries.

```
FC-ASW-1#clear mac-address-table dynamic
```

b. Issue the **`show mac-address-table`** command.

   Record the table entries.

   ____

   ____

   ____

   ____

c. Determine the options for setting port security on interface FastEthernet 0/4. From the global configuration mode, enter **`interface fastethernet 0/4`**.

```
FC-ASW-1(config)#interface fa 0/4
```

   Enabling switch port security provides options, such as specifying what happens when a security setting is violated.

d. To configure the switch port FastEthernet 0/4 to accept only the first device connected to the port, issue the following commands from the configuration mode:

```
FC-ASW-1(config-if)#switchport mode access
FC-ASW-1(config-if)#switchport port-security
```

e. In the event of a security violation, the interface should be shut down. Set the port security action to **`shutdown`**:

```
FC-ASW-1(config-if)#switchport port-security violation shutdown
FC-ASW-1(config-if)#switchport port-security mac-address sticky
```

   What other action options are available with port security?

   ____

f. Exit the configuration mode.

Step 2: Verify the configuration

a. Display the running configuration.

   What statements in the configuration directly reflect the security implementation?

____

____

____

____

b. Show the port security settings.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Record the details displayed in the table.

____

____

____

____

____

____

____

____

Step 3: Verify the port security

a. Connect PC1 to switch port Fa0/1 and PC2 to switch port Fa0/4.

b. From the command prompt ping from PC1 to PC2.

Was this successful? __________

c. From the command prompt ping from PC2 to PC1.

Was this successful? __________

d. From the console terminal session, issue the **`show mac-address-table`** command.

Record the details displayed in the table.

____

____

e. Show the port security settings.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Record the details displayed in the table.

____

____

____

____

____

____

____

____

Note the difference in entries recorded in Step 2 b.

____

____

____

f. Confirm the status of the switch port.

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

What is the state of this interface?

FastEthernet0/4 is __________ and line protocol is __________

Step 4: Test the port security

a. Disconnect PC2 from Fa0/4

b. Connect PC2 to the Linksys using one of the ports on the Linksys LAN switch.

c. Use the Basic Setup tab to configure the Internet IP address on the Linksys device to the address and mask, as shown in the table.

d. Configure PC2 to get an IP address using DHCP. Verify that PC2 receives an IP address from the Linksys device.

e. Connect the Internet port on the Linksys to Fa0/4.

f. Ping from PC1 to PC2.

Was this successful? __________

g. Ping from PC2 to PC1.

Was this successful? __________

Record the output displayed on the console screen at the switch command line.

____

____

____

h. Issue the **`show mac-address-table`** command.

Record the details displayed in the table.

____

____

i. Show the port security settings.

```
FC-ASW-1#show port-security interface fastethernet 0/4
```

Record the details displayed in the table.

____

____

____

____

____

____

____

Note the difference in entries recorded in Step 3 e.

____

____

____

j. Confirm the status of the switch port.

```
FC-ASW-1#show interface fastethernet 0/4
```

What is the state of this interface?

FastEthernet0/4 is __________ and line protocol is __________

Step 5: Reactivate the port

a. If a security violation occurs and the port is shut down, enter interface Fa0/4 configuration mode, disconnect the offending device, and use the **shutdown** command to temporarily disable the port.

b. Disconnect the Linksys and reconnect PC2 to port Fa0/4. Issue the **no shutdown** command on the interface.

c. Ping from PC1 to PC2. This may have to be repeated multiple times before success.

List reasons why multiple ping attempts may be necessary before success is achieved.

____

____

____

Step 6: Discuss switch port security using dynamic MAC address assignment

Advantages:

____

____

____

____

Disadvantages:

____

____

____

____

Step 7: Clean up

Erase the configurations and reload the switches. Disconnect and store the cabling. For PC hosts that are normally connected to other networks (such as the school LAN or to the Internet), reconnect the appropriate cabling and restore the TCP/IP settings.

Task 3: Reflection

When considering designing a typical enterprise network, it is necessary to think about points of security vulnerability at the Access Layer. Discuss which Access Layer switches should have port security and those for which it may not be appropriate. Include possible future issues in regard to wireless and guest access to the network.