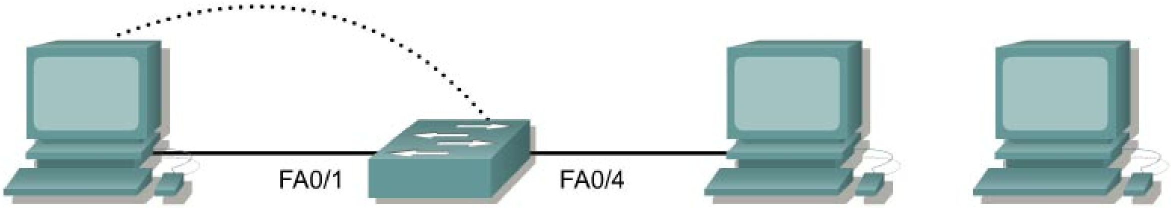
CISCO NETWORKING ACADEMY PROGRAM

Lab 6.2.5 Configuring Port Security



Switch Designation	Switch Name	Enable Secret Password	Enable, VTY, and Console Passwords	VLAN 1 IP Address	Default Gateway IP Address	Subnet Mask
Switch 1	AL Switch	class	cisco	192.168.1.2	192.168.1.1	255.255.255.0

Straight-through cable	────────
Serial cable	───Z───
Console (Rollover)	••••••••••••
Crossover cable	– – – – – – –

Objective

- Create and verify a basic switch configuration.
- Configure port security on individual FastEthernet ports.

Background/Preparation

Cable a network similar to the one in the diagram. The configuration output used in this lab is produced from a 2950 series switch. Any other switch used may produce different output. The following steps are intended to be executed on each switch unless specifically instructed otherwise. Instructions are also provided for the 1900 Series switch, which initially displays a User Interface Menu. Select the “Command Line” option from the menu to perform the steps for this lab.

Start a HyperTerminal session.

> **Note:** Go to the erase and reload instructions at the end of this lab. Perform those steps on all switches in this lab assignment before continuing.

Step 1 Configure the switch

Configure the hostname, access and command mode passwords, as well as the management LAN settings. These values are shown in the chart. If problems occur while performing this configuration, refer to the Basic Switch Configuration lab.

Step 2 Configure the hosts attached to the switch

a. Configure the hosts to use the same IP subnet for the address, mask, and default gateway as on the switch.

b. There is a third host needed for this lab. It needs to be configured with the address 192.168.1.7. The subnet mask is 255.255.255.0 and the default gateway is 192.168.1.1.

Note: Do not connect this PC to the switch yet.

Step 3 Verify connectivity

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

b. Were the pings successful? ____

c. If the answer is no, troubleshoot the hosts and switch configurations.

Step 4 Record the host MAC addresses

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

If running Windows 98, check by using **Start** > **Run** > **`winipcfg`**. Click on **`More info`**.

If running Windows 2000, check by using **Start** > **Run** > **`cmd > ipconfig /all`**.

b. PC1____

c. PC2____

Step 5 Determine what MAC addresses that the switch has learned

a. Determine what MAC addresses the switch has learned by using the **`show mac-address-table`** command, as follows, at the privileged exec mode prompt:

```
ALSwitch#show mac-address-table
```

b. How many dynamic addresses are there? ______________________________________

c. How many total MAC addresses are there? ____________________________________

d. Do the MAC addresses match the host MAC addresses? __________________________

Step 6 Determine the show MAC table options

a. Enter the following to determine the options the **`mac-address-table`** command has use the **`?`** option:

```
ALSwitch(config)#mac-address-table ?
```

Step 7 Setup a static MAC address

Setup a static MAC address on FastEthernet interface 0/4 as follows:

Note: Use the address that was recorded for PC4 in Step 4. The MAC address 00e0.2917.1884 is used in the example statement only.

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

2900:

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

1900:

```
ALSwitch(config)#mac-address-table permanent 00e0.2917.1884 ethernet
0/4
```

Step 8 Verify the results

a. Enter the following to verify the **mac-address table** entries.

```
ALSwitch#show mac-address-table
```

b. How many total MAC addresses are there now? ____

Step 9 List port security options

a. Determine the options for setting port security on interface FastEthernet 0/4. Type **port security ?** from the interface configuration prompt for FastEthernet port 0/4 as follows:

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#switchport port-security ?
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addrs
  violation     Security Violation Mode
  <cr>
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#port secure ?
max-mac-count  Maximum number of addresses allowed on the port
<cr>
```

2950:

```
ALSwitch(config-if)#switchport port-security  ?
aging         Port-security aging commands
mac-address   Secure mac address
maximum       Max secure addrs
violation     Security Violation Mode
<cr>
```

b. To allow the switchport FastEthernet 0/4 to accept only one device enter **port security** as follows:

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

1900:

```
ALSwitch(config-if)#port secure
```

Step 10 Verify the results

a. Enter the following to verify the mac –address table entries:

```
ALSwitch#show mac-address-table
```

b. How are the address types listed for the two MAC addresses? ____________________________

c. Show port security settings

```
ALSwitch#show port-security
```

1900:

```
ALSwitch#show mac-address-table security
```

Step 11 Show the running configuration file

a. Are there statements that directly reflect the security implementation in the listing of the running configuration? ____

b. What do those statements mean?

____

Step 12 Limit the number of hosts per port

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

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#port security max-mac-count 1
```

1900:

```
ALSwitch(config)#interface Ethernet 0/4
ALSwitch(config-if)#port secure max-mac-count 1
```

2950:

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

b. Disconnect the PC attached to FastEthernet 0/4. Connect to the port on the PC that has been given the IP address 192.168.1.7. This PC 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.

c. Record any observations. ____

____

Step 13 Configure the port to shut down if there is a security violation

a. It has been decided that in the event of a security violation the interface should be shut down. Enter the following to make the port security action to shutdown:

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

2900XL:

```
ALSwitch(config-if)#port security action shutdown
```

1900:

```
The default action upon address violation is "suspend"
```

b. What other action options are available with port security? ________________________________

c. If necessary, ping the switch address 192.168.1.2 from the PC 192.168.1.7. This PC is now connected to interface FastEthernet 0/4. This ensures that there is traffic from the PC to the switch.

d. Record any observations.

____

____

Step 14 Show port 0/4 configuration information

a. To see the configuration information for just FastEthernet port 0/4, type **`show interface fastethernet 0/4, as follows,`** at the privileged exec mode prompt:

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

1900:

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

b. What is the state of this interface?

FastEthernet0/4 is ____________________________, line protocol is _______________________

1900:

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

c. What is the state of this interface?

Ethernet 0/4 is ____________________________, line protocol is __________________________

Step 15 Reactivate the port

a. If a security violation occurs and the port is shut down, use the **`no shutdown`** command to reactivate it.

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, type the **`no shutdown`** command on the interface and ping using the DOS window. The **`ping`** will have to be repeated multiple times or use the **`ping 192.168.1.2 -n 200`** command. This will set the number of ping packets to 200 instead of 4. Then switch hosts and try again.

Step 16 Exit the switch

Type **`exit`**, as follows, to leave the switch welcome screen:

```
Switch#exit
```

Once the steps are completed, logoff by typing **`exit`**, and turn all the devices off. Then remove and store the cables and adapter.

Erasing and Reloading the Switch

For the majority of the labs in CCNA 3 and CCNA 4 it is necessary to start with an unconfigured switch. Use of a switch with an existing configuration may produce unpredictable results. These instructions allow preparation of the switch prior to performing the lab so previous configuration options do not interfere. The following is the procedure for clearing out previous configurations and starting with an unconfigured switch. Instructions are provided for the 2900, 2950, and 1900 Series switches.

2900 and 2950 Series Switches

1. Enter into the privileged EXEC mode by typing **`enable`**.

   If prompted for a password, enter **class** (if that does not work, ask the instructor).

   ```
   Switch>enable
   ```

2. Remove the VLAN database information file.

   ```
   Switch#delete flash:vlan.dat
   Delete filename [vlan.dat]?[Enter]
   Delete flash:vlan.dat? [confirm] [Enter]
   ```

   If there was no VLAN file, this message is displayed.

   ```
   %Error deleting flash:vlan.dat (No such file or directory)
   ```

3. Remove the switch startup configuration file from NVRAM.

   ```
   Switch#erase startup-config
   ```

   The responding line prompt will be:

   ```
   Erasing the nvram filesystem will remove all files! Continue? [confirm]
   ```

   Press **Enter** to confirm.

   The response should be:

   ```
   Erase of nvram: complete
   ```

4. Check that VLAN information was deleted.

   Verify that the VLAN configuration was deleted in Step 2 using the **`show vlan`** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present it will be necessary to power cycle the switch (hardware restart) instead of issuing the **`reload`** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it. Then plug it back in.

   If the VLAN information was successfully deleted in Step 2, go to Step 5 and restart the switch using the **`reload`** command.

5. Software restart (using the **`reload`** command)

Note: This step is not necessary if the switch was restarted using the power cycle method.

a. At the privileged EXEC mode enter the command `reload`.

```
Switch(config)#reload
```

The responding line prompt will be:

```
System configuration has been modified. Save? [yes/no]:
```

b. Type **n** and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response will be:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt will be:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

c. Type **n** and then press **Enter**.

The responding line prompt will be:

```
Press RETURN to get started! [Enter]
```

1900 Series Switches

1. Remove VLAN Trunking Protocol (VTP) information.

```
#delete vtp
This command resets the switch with VTP parameters set to factory
defaults.
All other parameters will be unchanged.

Reset system with VTP parameters set to factory defaults, [Y]es or
[N]o?
```

Enter **y** and press **Enter**.

2. Remove the switch startup configuration from NVRAM.

```
#delete nvram
```

This command resets the switch with factory defaults. All system parameters will revert to their default factory settings. All static and dynamic addresses will be removed.

Reset system with factory defaults, [**Y**]es or [**N**]o?

Enter **y** and press **Enter**.