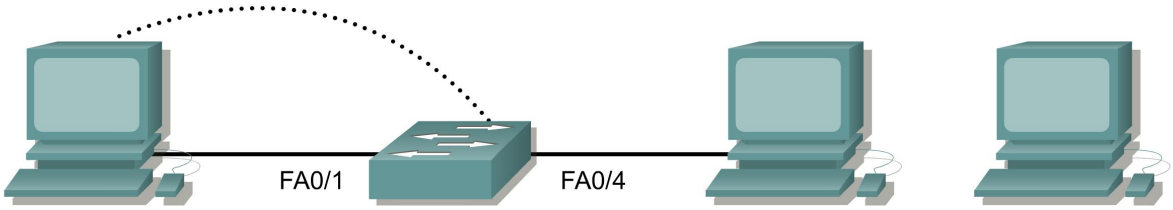
Lab 6.2.6 Add, Move, and Change MAC Addresses



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

Straight-through cable	
Serial cable	
Console (Rollover)	
Crossover cable	

Objective

- Create and verify a basic switch configuration.
- Move a PC from one switch port to another and add a new PC to the switch.

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 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 VLAN 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

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

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. Do not connect this PC to the switch yet.

Step 3 Verify connectivity

a. To verify that the 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 MAC addresses on the hosts

a. To determine and record the layer 2 addresses of the PC network interface cards enter the following.

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. PC4: _____

Step 5 Determine what MAC addresses the switch has learned

a. Determine what MAC addresses the switch has learned by using the **`show mac-address-table`** command 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 MAC table options

To determine the options that the **`mac-address-table`** command has using enter the **`?`** option as follows:

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

Step 7 Set up a static MAC address

To setup a static MAC address on Fast Ethernet interface 0/4 enter the following:

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
```


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 static addresses are there? _____

Step 9 List port security options

a. To determine the options for setting port security on interface Fast Ethernet 0/4. Type **port security ?** from the interface configuration prompt for Fast Ethernet port 0/4.

```
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>
```

b. Allow the switchport on Fast Ethernet 0/4 to accept only one device by typing **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? _____

Step 11 Show the running configuration file

a. In the listing of the running configuration are there statements that directly reflect the security implementation? _____

b. What do those statements mean? _____

_____

Step 12 Limit the number of hosts on each port

a. Enter the following on interface Fast Ethernet 0/4 to set the port security maximum MAC count to 1:

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#switchport port-security maximum 1
```

1900:

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

b. Disconnect the PC that is attached to Fast Ethernet 0/4. Connect to the port that the PC has been given the IP address 192.168.1.7. This PC has not yet been attached to the switch. To generate some traffic ping the switch address 192.168.1.2 with the -n 50 option. For example **`ping 192.168.1.2 –n 50`**, where 50 is the number of pings sent.

Step 13 Move host

a. Take the PC that had previously been connected to Fast Ethernet 0/4 and reconnect it to Fast Ethernet 0/8. The PC has been moved to a new location. This could be to another VLAN but in this instance all switch ports are in VLAN 1 and network 192.168.1.0.

b. From this PC on Fast Ethernet 0/8, **`ping 192.168.1.2 –n 50`**

c. Was the ping successful? _____

d. Why or why not? _____

e. Enter the following to show the **`mac-address-table`**.

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

f. Record observations about the show output. _____

_____

Step 14 Clear MAC table

a. Enter the following to clear the **`mac-address-table`**:

Note: This will unlock the MAC addresses from security and allow a new address to be registered.

```
ALSwitch#clear mac-address-table dynamic
```

b. From the PC on the Fast Ethernet 0/8, **`ping 192.168.1.2 –n 50`**.

c. Was the ping successful? _____

d. If not troubleshoot as necessary.

Step 15 Change security settings

a. Enter the following to show the **mac-address-table**:

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

b. Notice that Fast Ethernet 0/4 is secure. However, that security should be applied to the machine on port 0/8, as this is the machine that was moved from port 0/4. Remove port security from interface Fast Ethernet 0/4 as follows:

```
ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#no switchport port-security
ALSwitch(config-if)#no switchport port-security mac-address sticky
ALSwitch(config-if)#no switchport port-security mac-address sticky
0008.744d.8ee2
ALSwitch(config-if)#shutdown
ALSwitch(config-if)#no shutdown
```

1900:

```
ALSwitch(config)#interface ethernet 0/4
ALSwitch(config-if)#no port secure
```

c. Apply port security with a max-mac-count of 1 to interface Fast Ethernet 0/8 as follows:

```
ALSwitch(config)#interface fastethernet 0/8
ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address sticky
ALSwitch(config-if)#switchport port-security maximum 1
```

1900:

```
ALSwitch(config)#interface ethernet 0/8
ALSwitch(config-if)#port secure max-mac-count 1
```

d. Enter the following to clear the **mac-address-table**.

Note: Clearing individual entries could have also been done.

```
ALSwitch#clear mac-address-table
```

Step 16 Verify the results

a. Verify that the mac-address-table has been cleared.

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

b. Can all PCs still successfully ping each other? _____

c. If not troubleshoot the switch and PCs.

Step 17 Exit the switch

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

```
Switch#exit
```

Once the steps are complete, 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**.

