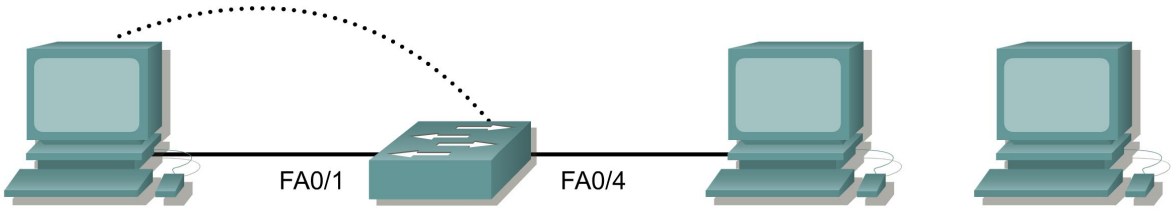
Lab 6.2.5 Configuring Port Security – 2900XL Series



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

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? Yes

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. PC108-00-46-06-FB-B6

c. PC200-08-74-4D-8E-E2

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? 2

c. How many total MAC addresses are there? 51

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

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.

```
2950:
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? 52 (one additional static)

Step 9 List port security options

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

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? 1 static, 1 dynamic

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? Yes

```
interface FastEthernet0/4
switchport mode access
switchport port-security
no ip address
```

b. What do those statements mean? Port security is enabled

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:

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:

2950:

```
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? send a trap

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.


```
Ping was successful.
```

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 up, line protocol is up

```
1900:
ALSwitch#show interface ethernet 0/4
```

c. What is the state of this interface?

Ethernet 0/4 is up, line protocol is up

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** 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.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.2:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```



```
Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum =  0ms, Average =  0ms

C:\>ipconfig /all

Windows 2000 IP Configuration

      Host Name . . . . . . . . . . . . : laptop
      Primary DNS Suffix  . . . . . . . :
      Node Type . . . . . . . . . . . . : Broadcast
      IP Routing Enabled. . . . . . . . : No
      WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

      Connection-specific DNS Suffix  . :
      Description . . . . . . . . . . . : Intel 8255x-based PCI Ethernet
         Adapter (10/100)
      Physical Address. . . . . . . . . : 08-00-46-06-FB-B6
      DHCP Enabled. . . . . . . . . . . : No
      IP Address. . . . . . . . . . . . : 192.168.1.10
      Subnet Mask . . . . . . . . . . . : 255.255.255.0
      Default Gateway . . . . . . . . . : 192.168.1.1
      DNS Servers . . . . . . . . . . . :

C:\>

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.2:
      Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
      Minimum = 0ms, Maximum =  10ms, Average =  2ms

C:\>
C:\>ipconfig /all

Windows 2000 IP Configuration

      Host Name . . . . . . . . . . . . : inspiron1
      Primary DNS Suffix  . . . . . . . : cisco.com
      Node Type . . . . . . . . . . . . : Hybrid
      IP Routing Enabled. . . . . . . . : No
      WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

      Connection-specific DNS Suffix  . :
      Description . . . . . . . . . . . : 3Com 3C920 Integrated Fast
         Ethernet Controller (3C905C-TX Compatible)
```



```
        Physical Address. . . . . . . . . : 00-08-74-4D-8E-E2
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.20
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . :

C:\>

Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname ALSwitch

ALSwitch(config)#enable secret class

ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login

ALSwitch(config-line)#interface Vlan1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config-if)#no shutdown

ALSwitch(config-if)#ip default-gateway 192.168.1.1

ALSwitch(config)#exit


ALSwitch#show mac-address-table
Dynamic Address Count:                   2
Secure Address Count:                    0
Static Address (User-defined) Count:     0
System Self Address Count:               49
Total MAC addresses:                     51
Maximum MAC addresses:                   2048
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0008.744d.8ee2       Dynamic          1  FastEthernet0/4
0800.4606.fbb6       Dynamic          1  FastEthernet0/1

ALSwitch#configure terminal


ALSwitch(config)#mac-address-table ?
  aging-time    Set MAC address table entry maximum age
  dynamic       Configure a dynamic 802.1d address
  notification  Enable/Disable MAC Notification on the switch
  secure        Configure a secure address
  static        Configure a static 802.1d static address

ALSwitch(config)#mac-address-table static 0008.744d.8ee2 fa0/4 vlan 1
ALSwitch(config)#exit

ALSwitch#show mac-address-table
```



```
Dynamic Address Count:                    1
Secure Address Count:                     0
Static Address (User-defined) Count:      1
System Self Address Count:                49
Total MAC addresses:                      51
Maximum MAC addresses:                    2048
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0800.4606.fbb6       Dynamic          1  FastEthernet0/1

Static Address Table:
Destination Address  VLAN  Input Port  Output Ports
-------------------  ----  ----------  -----------------------
0008.744d.8ee2          1  Fa0/1
                        1  Fa0/2
                        1  Fa0/3
                        1  Fa0/4
                        1  Fa0/5
                        1  Fa0/6
                        1  Fa0/7
                        1  Fa0/8
                        1  Fa0/9
                        1  Fa0/10
                        1  Fa0/11
                        1  Fa0/12
                        1  Fa0/13
                        1  Fa0/14
                        1  Fa0/15
                        1  Fa0/16
                        1  Fa0/17
                        1  Fa0/18
                        1  Fa0/19
                        1  Fa0/20
                        1  Fa0/21
                        1  Fa0/22
                        1  Fa0/23
                        1  Fa0/24

ALSwitch#configure terminal

ALSwitch(config)#interface fa0/4
ALSwitch(config-if)#port security ?
  action          action to take for security violation
  aging           Enable Port-security aging
  max-mac-count   maximum mac address count
  <cr>

ALSwitch(config-if)#port security
ALSwitch(config-if)#exit
ALSwitch(config)#exit

ALSwitch#show mac-address-table
Dynamic Address Count:                    1
Secure Address Count:                     0
Static Address (User-defined) Count:      1
System Self Address Count:                49
Total MAC addresses:                      51
Maximum MAC addresses:                    2048
Non-static Address Table:
```



```
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0800.4606.fbb6       Dynamic          1  FastEthernet0/1

Static Address Table:
Destination Address  VLAN  Input Port  Output Ports
-------------------  ----  ----------  -----------------------
0008.744d.8ee2          1  Fa0/1
                        1  Fa0/2
                        1  Fa0/3
                        1  Fa0/4
                        1  Fa0/5
                        1  Fa0/6
                        1  Fa0/7
                        1  Fa0/8
                        1  Fa0/9
                        1  Fa0/10
                        1  Fa0/11
                        1  Fa0/12
                        1  Fa0/13
                        1  Fa0/14
                        1  Fa0/15
                        1  Fa0/16
                        1  Fa0/17
                        1  Fa0/18
                        1  Fa0/19
                        1  Fa0/20
                        1  Fa0/21
                        1  Fa0/22
                        1  Fa0/23
                        1  Fa0/24
```

```
ALSwitch#show port security
Secure Port        Secure Addr     Secure Addr  Security    Security Action
                      Cnt (Current)   Cnt (Max)     Reject Cnt
---------------  -------------  -----------  ----------  ------------------
FastEthernet0/4       0                132          0           Send Trap

ALSwitch#show running-config
Building configuration...

Current configuration:
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ALSwitch
!
enable secret 5 $1$PEwH$P8EQAxXb5Hh/sIsTNvWU6.


!
ip subnet-zero

!
interface FastEthernet0/1
```



```
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
 port security
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface VLAN1
 ip address 192.168.1.2 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
ip default-gateway 192.168.1.1
mac-address-table static 0008.744d.8ee2 FastEthernet0/4 vlan 1
!
line con 0
 password cisco
 login
 transport input none
```



```
 stopbits 1
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
end


ALSwitch#configure terminal

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


ALSwitch#configure terminal

ALSwitch(config)#interface fastethernet 0/4
ALSwitch(config-if)#port security action ?
shutdown shut down the port from which security violation is detected
trap send snmp trap for security violation

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

ALSwitch#show interface fa0/4
FastEthernet0/4 is up, line protocol is up
 Hardware is Fast Ethernet, address is 0004.c075.1504 (bia
   0004.c075.1504)
 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
   reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive not set
 Auto-duplex (Full), Auto Speed (100), 100BaseTX/FX
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input never, output 00:00:01, output hang never
 Last clearing of "show interface" counters never
 Queueing strategy: fifo
 Output queue 0/40, 0 drops; input queue 0/75, 0 drops
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute output rate 0 bits/sec, 0 packets/sec
      93 packets input, 10849 bytes
      Received 78 broadcasts, 0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 6 multicast
      0 input packets with dribble condition detected
      363 packets output, 30381 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      0 babbles, 0 late collision, 0 deferred
      0 lost carrier, 0 no carrier
      0 output buffer failures, 0 output buffers swapped out
```


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#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.

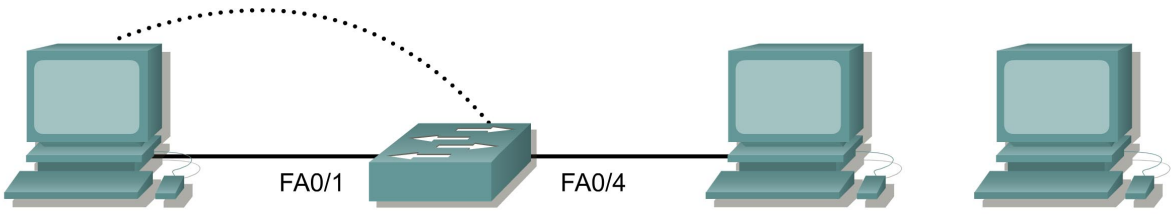
   ```
   #delete nvram
   ```

   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**.

Lab 6.2.5 Configuring Port Security – 2950 Series



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.
- 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? Yes

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. PC18-00-46-06-FB-B6

c. PC200-08-74-4D-8E-E2

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? 2

c. How many total MAC addresses are there? 6

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

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? 5

Step 9 List port security options

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

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? 6

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? Yes

```
interface FastEthernet0/4
switchport mode access
switchport port-security
no ip address
```

b. What do those statements mean? Port security is enabled.

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:

```
   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? protect, restrict

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.

Ping was successful.

Step 14 Show port 0/4 configuration information

d. 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
```

e. What is the state of this interface?

FastEthernet0/4 is up, line protocol is up

1900:

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

f. What is the state of this interface?

Ethernet 0/4 is up, line protocol is up.

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** 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.

```
Switch#
Switch#configure terminal

Switch(config)#hostname ALSwitch

ALSwitch(config)#enable secret class

ALSwitch(config)#line con 0
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 15
ALSwitch(config-line)#password cisco
ALSwitch(config-line)#login

ALSwitch(config-line)#interface Vlan1
ALSwitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSwitch(config-if)#no shutdown
```



```
ALSwitch(config-if)#ip default-gateway 192.168.1.1

ALSwitch(config)#exit

ALSwitch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  All    000a.b772.2b40    STATIC       CPU
  All    0100.0ccc.cccc    STATIC       CPU
  All    0100.0ccc.cccd    STATIC       CPU
  All    0100.0cdd.dddd    STATIC       CPU
  1    0008.744d.8ee2    DYNAMIC     Fa0/4
  1    0800.4606.fbb6    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 6

ALSwitch#configure terminal

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>


ALSwitch(config-if)#switchport mode access
ALSwitch(config-if)#switchport port-security
ALSwitch(config-if)#switchport port-security mac-address stick
ALSwitch(config-if)#exit
ALSwitch(config)#exit

ALSwitch#show mac-address-table
Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
All 000a.b772.2b40 STATIC CPU
All 0100.0ccc.cccc STATIC CPU
All 0100.0ccc.cccd STATIC CPU
All 0100.0cdd.dddd STATIC CPU
1 0008.744d.8ee2 STATIC Fa0/4
1 0800.4606.fbb6 DYNAMIC Fa0/1
Total Mac Addresses for this criterion: 6


ALSwitch#show port-security
  aging         Port-security aging commands
  mac-address   Secure mac address
  maximum       Max secure addrs
  violation     Security Violation Mode
  <cr>



ALSwitch(config-if)#switchport mode access
```



```
ALSwitch(config-if)#switchport port-security mac-address stick
ALSwitch(config-if)#exit
ALSwitch(config)#exit


ALSwitch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  All    000a.b772.2b40    STATIC       CPU
  All    0100.0ccc.cccc    STATIC       CPU
  All    0100.0ccc.cccd    STATIC       CPU
  All    0100.0cdd.dddd    STATIC       CPU
  1    0008.744d.8ee2    STATIC      Fa0/4
  1    0800.4606.fbb6    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 6

ALSwitch#show port-security
Secure Port  MaxSecureAddr CurrentAddr  SecurityViolation  Security Action
                (Count)       (Count)       (Count)
---------------------------------------------------------------------------
Fa0/4            1                0              0               Shutdown
---------------------------------------------------------------------------
Total Addresses in System : 0
Max Addresses limit in System : 1024


ALSwitch#show running-config
Building configuration...

Current configuration : 1791 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ALSwitch
!
enable secret 5 $1$gVST$m6H2rsGkpM4.f9bskK7PE0
enable password cisco
!
ip subnet-zero
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!

interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
```



```
 no ip address
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 no ip address
!
interface FastEthernet0/5
 no ip address
!
interface FastEthernet0/6
 no ip address
!
interface FastEthernet0/7
 no ip address
!
interface FastEthernet0/8
 no ip address
!
interface FastEthernet0/9
 no ip address
!
interface FastEthernet0/10
 no ip address
!
interface FastEthernet0/11
 no ip address
!
interface FastEthernet0/12
 no ip address
!
interface FastEthernet0/13
 no ip address
!
interface FastEthernet0/14
 no ip address
!
interface FastEthernet0/15
 no ip address
!
interface FastEthernet0/16
 no ip address
!
interface FastEthernet0/17
 no ip address
!
interface FastEthernet0/18
 no ip address
!
interface FastEthernet0/19
 no ip address
!
interface FastEthernet0/20
 no ip address
!
interface FastEthernet0/21
 no ip address
!
interface FastEthernet0/22
```



```
 no ip address
!
interface FastEthernet0/23
 no ip address
!
interface FastEthernet0/24
 no ip address
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!

line con 0
 password cisco
 login
line vty 0 4
 password cisco
 login
line vty 5 15
 password cisco
 login
!
mac-address-table static 0008.744d.8ee2 vlan 1 interface FastEthernet0/4
end

ALSwitch#configure terminal

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

ALSwitch(config-if)#end

ALSwitch#show interface fastethernet

FastEthernet0/4 is up, line protocol is up (connected)
 Hardware is Fast Ethernet, address is 000a.b772.2b44 (bia
     000a.b772.2b44)
 MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
 Full-duplex, 100Mb/s
 input flow-control is off, output flow-control is off
 ARP type: ARPA, ARP Timeout 04:00:00
 Last input 00:00:00, output 00:00:01, output hang never
 Last clearing of "show interface" counters never
 Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 Output queue :0/40 (size/max)
 5 minute input rate 0 bits/sec, 0 packets/sec
 5 minute ouxtput rate 0 bits/sec, 0 packets/sec
     161 packets input, 19257 bytes, 0 no buffer
     Received 137 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 5 multicast, 0 pause input
```



```
     0 input packets with dribble condition detected
     349 packets output, 29399 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out

ALSwitch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation Security Action
                (Count)        (Count)       (Count)
-----------------------------------------------------------------------------
Fa0/4            1               1              0               Shutdown
-----------------------------------------------------------------------------
Total Addresses in System : 1
Max Addresses limit in System : 1024

ALSwitch#exit

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.2:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum =  0ms, Average =  0ms


C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255
Reply from 192.168.1.2: bytes=32 time<10ms TTL=255

Ping statistics for 192.168.1.2:
     Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
     Minimum = 0ms, Maximum =  10ms, Average =  2ms
```


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#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**.

