Ch. 7/ Mod. 6
Switch Configuration

CCNA 3 version 3.0
Overview

- Identify the major components of a Catalyst switch
- Monitor switch activity and status using LED indicators
- Examine the switch bootup output using HyperTerminal
- Use the help features of the command line interface
- List the major switch command modes
- Verify the default settings of a Catalyst switch
- Set an IP address and default gateway for the switch to allow connection and management over a network
- View the switch settings with a Web browser
- Set interfaces for speed and duplex operation
- Examine and manage the switch MAC address table
- Configure port security
- Manage configuration files and IOS images
- Perform password recovery on a switch
- Upgrade the IOS of a switch
Physical startup of the Catalyst switch

- Switches are dedicated, specialized computers;
  - Central Processing Unit (CPU)
  - Random Access Memory (RAM)
  - Operating System.
- A switch can be managed by connecting to the console port to view and make changes to the configuration.
- Switches typically have no power switch to turn them on and off.
- They simply connect or disconnect from a power source.
Switch LED indicators
Switch LED indicators

- The front panel of a switch has several lights to help monitor system activity and performance.
- These lights are called light-emitting diodes (LEDs).
- The front of the switch has the following LEDs:
  - System LED
    - Whether the system is receiving power and functioning correctly.
  - Remote Power Supply (RPS) LED
    - Whether or not the remote power supply is in use
  - Port Mode LED
    - Indicates the current state of the Mode button.
    - The modes are used to determine how the Port Status LEDs are interpreted.
  - Port Status LEDs
    - Has different meanings, depending on the current value of the Mode LED.
# Switch LED indicators: Port Status LED

<table>
<thead>
<tr>
<th>Mode LED</th>
<th>Color</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAT</td>
<td>Off</td>
<td>No link</td>
</tr>
<tr>
<td>Solid Green</td>
<td>Link operational</td>
<td></td>
</tr>
<tr>
<td>Flashing Green</td>
<td>Port is sending or receiving data</td>
<td></td>
</tr>
<tr>
<td>Alternating green/amber</td>
<td>Link fault</td>
<td></td>
</tr>
<tr>
<td>Solid amber</td>
<td>Port is not forwarding because it was disabled by management or address violation, or blocked by Spanning/Tree Protocol.</td>
<td></td>
</tr>
<tr>
<td>UTL</td>
<td>Off</td>
<td>Each LED that is off indicates a reduction by half of the total bandwidth. The LEDs are turned off from right to left. If the right-most LED is off, then the switch is using less than 50% of total bandwidth. If the two right-most LEDs are off, the switch is using less than 25% of total bandwidth. If all LEDs are green, the switch is using 50% or more of total bandwidth.</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FDUP</td>
<td>Off</td>
<td>Port is operating in half-duplex mode.</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td>Port is operating in full-duplex mode.</td>
</tr>
<tr>
<td>100</td>
<td>Off</td>
<td>Port is operating at 10 Mbps.</td>
</tr>
<tr>
<td>Green</td>
<td></td>
<td>Port is operating at 100 Mbps.</td>
</tr>
</tbody>
</table>
Port LEDs during switch POST – System LED

System LED

The System LED indicates the success or failure of POST.
• If the System LED is off but the switch is plugged in, then POST is running.
• If the System LED is green, then POST was successful.
• If the System LED is amber, then POST failed.

• Once the power cable is connected, the switch initiates a series of tests called the power-on self test (POST).
• If the System LED is **green**, then POST was successful.
• If the System LED is **amber**, then POST failed. POST failure is considered to be a fatal error.
Port LEDs during switch POST – Port Status LED

- The Port Status LEDs also change during switch POST.
- The Port Status LEDs turn **amber** for about 30 seconds as the switch discovers the network topology and searches for loops.
- If the Port Status LEDs turn **green**, the switch has established a link between the port and a target, such as a computer.
- If the Port Status LEDs turn **off**, the switch has determined that nothing is plugged into the port.
Viewing initial bootup output from the switch

- The switch may be configured manually with or without the assistance of the System Configuration dialog.
- The System Configuration dialog on the switch is simpler than that on a router.
The command-line interface (CLI) for Cisco switches is very similar to the CLI for Cisco routers.
Switch command modes

<table>
<thead>
<tr>
<th>Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Gives version information for software and hardware. Used to see exactly which modules and software are in use.</td>
</tr>
<tr>
<td>show running-config</td>
<td>Displays the current configuration file of the switch.</td>
</tr>
<tr>
<td>show interface</td>
<td>Displays the administrative and operational status of a switching port, packets in/out, and errors.</td>
</tr>
<tr>
<td>show interface status</td>
<td>Display the operational mode of the port.</td>
</tr>
<tr>
<td>show controllers ethernet-controller</td>
<td>Gives discarded frames, deferred frames, alignment errors, collisions, and so on.</td>
</tr>
<tr>
<td>show post</td>
<td>Tells if the switch passed the Power-On Self Test (POST).</td>
</tr>
</tbody>
</table>

- The **enable** command is used to change from User EXEC mode to Privileged EXEC mode. Privileged EXEC mode is also recognized by its prompt, which ends in a pound-sign character (#).
show running-config

Switch#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 Switch
!
!<OUTPUT OMITTED>
!
interface VLAN1
no ip directed-broadcast
show interface

Switch# show interface FastEthernet0/1
FastEthernet0/1 is down, line protocol is down
   Hardware is Fast Ethernet, address is 0008.e32e.e501 (bia 0008.e32.e.e601)
   MTU 1500 bytes, BW 0 Kbit, DLY 100 usec,
       reliability 255/25, txlead 1/255, rxlead 1/255
Encapsulation ARPA, Loopback not set
Keepalive not set
Auto-duplex, AutoSpeed , 100BaseTX/TX
ARP type: ARPA, ARP TImeout 04:00:00
Last Input never, output 00:31:54, output hang never
   Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue o/75, 0 drops
   5 minute input rate 0 bits/sec, 0 packets/sec
# show vlan

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Name</th>
<th>Status</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>active</td>
<td>Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12</td>
</tr>
<tr>
<td>1002</td>
<td>fddi-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1003</td>
<td>token-ring-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1004</td>
<td>fddinet-default</td>
<td>active</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>trnet-default</td>
<td>active</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VLAN</th>
<th>Type</th>
<th>SAID</th>
<th>MTU</th>
<th>Parent</th>
<th>RingNo</th>
<th>BridgeNo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>enet</td>
<td>100001</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1002</td>
<td>fddi</td>
<td>101002</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>1003</td>
<td>tr</td>
<td>101003</td>
<td>1500</td>
<td>1005</td>
<td>0</td>
<td>-</td>
</tr>
<tr>
<td>1004</td>
<td>fdnet</td>
<td>101004</td>
<td>1500</td>
<td>-</td>
<td>-</td>
<td>1</td>
</tr>
</tbody>
</table>
show flash

Switch#show flash or Switch#dir flash:
Directory of flash:/

```
  2  -rw-x  1674921  Apr 30 2001 15:09:51  c2950-c3h2s-mz.120-5.3.WC.1.bin
  3  -rw-x     269  Jan 01 1970 00:00:57  env_vars
  4  drwx    10240  Apr 30 2001 15:09:52  html
```

7741440 bytes total (4780544 bytes free)
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-C3H2S-M), Version 12.0(5.3)WC(1), MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Mon 30-Apr-01 07:56 by devgoyal
Image text-base: 0x80010000, data-base: 0x8031A000

ROM: Bootstrap program is CALHOUN boot loader

Switch uptime is 1 hour, 24 minutes
System returned to ROM by power-on
System image file is "flash:c2950-c3h2s-mz.120-5.3.WC.1.bin"
cisco WS-C2950-12 (RC32300) processor (revision B0) with 22260K bytes of memory.
Processor board ID FOC0605W0BH
Reset all Switch Configurations & Reload

The following steps will ensure that a new configuration will completely overwrite any existing configuration:

- Remove any existing VLAN information by deleting the VLAN database file vlan.dat from the flash directory
- Erase the back up configuration file startup-config
- Reload the switch

Catalyst 2950

Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?  
Delete flash:vlan.dat? [confirm]
Switch#erase startup-config
<output omitted>
Switch#reload

Catalyst 1900

Switch#delete nvram
Security, documentation, and management

Switch(config)#hostname ALSwitch
ALSwitch(config)#line con 0
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
ALSwitch(config-line)#line vty 0 4
ALSwitch(config-line)#password <your-choice>
ALSwitch(config-line)#login
Set IP Address and Default Gateway

To allow the switch to be accessible by Telnet and other TCP/IP applications, IP addresses and a default gateway should be set.

By default, VLAN 1 is the management VLAN. (more later)

In a switch-based network, all internetworking devices should be in the management VLAN.

This will allow a single management workstation to access, configure, and manage all the internetworking devices.

```
ALSswitch(config)#interface VLAN1
ALSswitch(config-if)#ip address 192.168.1.2 255.255.255.0
ALSswitch(config)#ip default-gateway 192.168.1.1

Catalyst 1900

ALSswitch(config)#ip address 192.168.1.2 255.255.255.0
ALSswitch(config)#ip default-gateway 192.168.1.1
```
Set Port Speed and Duplex Settings

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

- The Fast Ethernet switch ports default to:
  - auto-speed
  - auto-duplex.
- This allows the interfaces to negotiate these settings.
- When a network administrator needs to ensure an interface has particular speed and duplex values, the values can be set manually.

- More later…
HTTP Service and Port

A web browser can access this service using the IP address and port 80, the default port for http.

The HTTP service can be turned on or off, and the port address for the service can be chosen.
The GUI Interface

Cisco Systems

Accessing Cisco WS-C2950-12 "Switch"

Cluster Management Suite or Visual Switch Manager

Telnet - To the Switch.

Show interfaces - Display the status of the interfaces.
Show diagnostic log - Display the diagnostic log.
Web Console - HTML access to the command line interface at level 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15

Show tech-support - Display information commonly needed by tech support.
Managing the MAC address table

- Switches learn the MAC addresses of PCs or workstations that are connected to their switch ports by examining the source address of frames that are received on that port.
- Machines may have been removed from a port, turned off, or moved to another port on the same switch or a different switch.
- This could cause confusion in frame forwarding.
- The MAC address entry is automatically discarded or aged out after 300 seconds.

```
Switch#show mac-address-table
Dynamic Address Count: 2
Secure Address Count: 0
Static Address (User-defined) Count: 0
System Self Address Count: 13
Total MAC addresses: 15
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address Address Type VLAN Destination Port
------------------ ------------- ---- ----------------
0010.7a60.ad7e Dynamic 1 FastEthernet0/2
00e0.2917.1884 Dynamic 1 FastEthernet0/5
```
Managing the MAC address table

Rather than wait for a dynamic entry to age out, the administrator has the option to use the privileged EXEC command `clear mac-address-table`. 

```
Switch#clear mac-address-table
Switch#show mac-address-table
Dynamic Address Count: 0
Secure Address Count: 0
Static Address (User-defined) Count: 0
System Self Address Count: 13
Total MAC addresses: 14
Maximum MAC addresses: 8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
---------------------------------  -------------  ----  -----------------
```
Configuring static MAC addresses

The reasons for assigning a permanent MAC address to an interface include:
- The MAC address will not be aged out automatically by the switch.
- A specific server or user workstation must be attached to the port and the MAC address is known.
- Security is enhanced.

To set a static MAC address entry for a switch:
```
Switch(config)#mac-address-table static <mac-address of host> interface FastEthernet <Ethernet number> vlan
```
Configuring port security

- Anyone can plug in a PC or laptop into one of these outlets.
- This is a potential entry point to the network by unauthorized users.
- Switches provide a feature called port security.
- It is possible to limit the number of addresses that can be learned on an interface.
- The switch can be configured to take an action if this is exceeded. Secure MAC addresses can be set statically.
- However, securing MAC addresses statically can be a complex task and prone to error.
- To verify port security status the command `show port security` is entered.

```
Switch(config)#interface FastEthernet0/2
Switch(config-if)#port security
    action action to take for security violation
    max-mac-count maximum mac address count
<cr>
Switch(config-if)#port security action
    shutdown shut down the port from which security violation is detected
    trap send snmp trap for security violation

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

Differs on 1900, 2900XL, and 2950 Switches.
Configuring Port Security

- www.cisco.com
- You can use the port security feature to restrict input to an interface by limiting and identifying MAC addresses of the stations allowed to access the port.
- When you assign secure MAC addresses to a secure port, the port does not forward packets with source addresses outside the group of defined addresses.
- If you limit the number of secure MAC addresses to one and assign a single secure MAC address, the workstation attached to that port is assured the full bandwidth of the port.
- If a port is configured as a secure port and the maximum number of secure MAC addresses is reached, when the MAC address of a station attempting to access the port is different from any of the identified secure MAC addresses, a security violation occurs.
- Also, if a station with a secure MAC address configured or learned on one secure port attempts to access another secure port, a violation is flagged.
Secure MAC Addresses

- A secure port can have from 1 to 132 associated secure addresses. After you have set the maximum number of secure MAC addresses on a port, the secure addresses are included in an address table in one of these ways:
  1. You can configure all secure MAC addresses by using the `switchport port-security mac-address mac-address` interface configuration command.
  2. You can allow the port to dynamically configure secure MAC addresses with the MAC addresses of connected devices.
  3. You can configure a number of addresses and allow the rest to be dynamically configured.

- Once the maximum number of secure MAC addresses is configured, they are stored in an address table.

- Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.
Secure MAC Addresses

- The switch supports these types of secure MAC addresses:
  1. Static secure MAC addresses—These are manually configured by using the `switchport port-security mac-address mac-address` interface configuration command, stored in the address table, and added to the switch running configuration.
  2. Dynamic secure MAC addresses—These are dynamically configured, stored only in the address table, and removed when the switch restarts.
  3. *Sticky* secure MAC addresses—These are dynamically configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, when the switch restarts, the interface does not need to dynamically reconfigure them.
Switch(config-if)#switchport mode access
  • Set the interface mode as access; an interface in the default mode (dynamic desirable) cannot be configured as a secure port.

Switch(config-if)# switchport port-security
  • Enable port security on the interface

Switch(config-if)# switchport port-security maximum value
  • (Optional) Set the maximum number of secure MAC addresses for the interface. The range is 1 to 132; the default is 1.

Switch(config-if)# switchport port-security mac-address mac-address
  • (Optional) Enter a static secure MAC address for the interface, repeating the command as many times as necessary.
  • You can use this command to enter the maximum number of secure MAC addresses. If you configure fewer secure MAC addresses than the maximum, the remaining MAC addresses are dynamically learned.
  • **Note** If you enable sticky learning after you enter this command, the secure addresses that were dynamically learned are converted to sticky secure MAC addresses and are added to the running configuration.
2950 Configuration

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

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

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

```
2950:
ALSwith(config-if)#switchport port-security maximum 1
```

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:

```
ALSwith(config-if)#switchport port-security violation shutdown
```
Copying IOS from TFTP Server

ALS witch# copy tftp flash
Address or name of remote host []? 192.168.1.3
Source filename []? c2950-c3h2s-mz.120-5.3.WC.1.bin
Destination filename [c2950-c3h2s-mz.120-5.3.WC.1.bin]? [enter]
%Warning: There is a file already existing with this name

Do you want to over write? [confirm] [enter]
Accessing tftp://192.168.1.3/c2950-c3h2s-mz.120-5.3.WC.1.bin...
Loading c2950-c3h2s-mz.120-5.3.WC.1.bin from 192.168.1.3 (via VLAN1):

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1674921 bytes]
1674921 bytes copied in 51.732 secs (32841 bytes/sec)
ALS witch#
Erasing and Reloading the Switch

Remove the VLAN database information file.

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

Switch#**erase startup-config**

Switch(config)#**reload**

The responding line prompt will be:

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

Type n and then press Enter.
The responding line prompt will be:

Proceed with reload? [confirm] [Enter]
Labs

Required Labs:
• 6.2.1 Verifying Default Switch Configuration
• 6.2.2 Basic Switch Configuration
• 6.2.3 Managing the MAC Address Tables
• 6.2.4 Configuring Static MAC Addresses
• 6.2.5 Configuring Port Security
• 6.2.6 Add, Move, and Change MAC Addresses
• 6.2.7a Managing Switch Operating System Files
• 6.2.7b Managing Switch Startup Configuration Files
Ch. 7/ Mod. 6
Switch Configuration

CCNA 3 version 3.0