

New Features for Catalyst 2900 Series XL Switches

Description

Cisco IOS Release 11.2(8) SA provides software support for the Catalyst 2900 series XL switches, hereafter referred to as the Catalyst 2900 switches. This chapter describes how this release incorporates the following switch features: assigning IP information to the switch, managing the MAC-address table, configuring port features, and enabling the Spanning-Tree Protocol Port Fast feature.

Note Catalyst 2900 switches are preconfigured and begin forwarding packets as soon as they are attached to compatible devices.

Benefits

Cisco IOS Release 11.2(8) SA brings the switching functionality described in this chapter to the Cisco IOS command-line interface (CLI).

List of Terms

Vlan1 is the name of the switch itself when configuring global parameters such as Spanning-Tree Protocol and IP.

Types of Memory

The Catalyst 2900 Series XL uses Flash memory to store the Cisco IOS software image, the startup configuration file, and helper files.

Platforms

The following platforms are supported:

- Catalyst 2908 XL
- Catalyst 2916M XL

Configuration Tasks

This section describes the following tasks:

- Assigning Internet Protocol (IP) information to the switch
- Setting and displaying switch port features such as Switched Port Analyzer (SPAN), Fast EtherChannel, and flooding controls
- Managing the switch MAC-address table
- Entering the speed and duplex settings for a port
- Entering Spanning-Tree Protocol parameters

Assigning IP Information to the Switch

If no IP information has been defined, the switch prompts you for the IP address, subnet mask, and default gateway. Beginning in privileged EXEC mode, follow these steps to enter this same information from the CLI:

Task	Command
Step 1 Enter configuration mode.	configure terminal
Step 2 Define the IP address of the default router.	ip default-gateway <i>ip_address</i>
Step 3 Enter the interface to which the IP information is assigned. VLAN1 is the switch interface.	interface <i>vlan1</i>
Step 4 Assign the IP address and subnet mask.	ip address <i>ip_address subnet_mask</i>
Step 5 Return to EXEC mode.	end
Step 6 Verify that the information was entered correctly by displaying the running configuration. If the information is incorrect, repeat the procedure.	show running-config

Setting Port Features

The **port** command controls switch features that manage packet flooding, port security, Fast EtherChannel port groups, and SPAN. This section describes how to use the **port** command to complete the following tasks:

- Blocking flooded unicast and multicast packets
- Enabling broadcast-storm control
- Enabling port security

Blocking Unicast and Multicast Flooding

By default, the switch floods unknown unicast and multicast packets to all ports. This flooding ensures that packets always reach their destinations, but it is unnecessary in configurations where there are no unknown addresses. Flooding is unnecessary, for example, when a workstation is connected to a port.

Beginning in privileged EXEC mode, complete these tasks to disable the flooding of multicast and unicast packets to a port:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter interface configuration mode and define the interface to configure.	interface <i>interface</i>
Step 3 Enter the port block command and the multicast option to block multicast forwarding to the port.	port block multicast
Step 4 Repeat the command with the unicast option to block unicast flooding to the port.	port block unicast
Step 5 Return to EXEC mode to verify the entry.	end
Step 6 Verify the entries by using the show port block command. Enter the command once for the multicast option and once for the unicast option.	show port block [multicast unicast] <i>interface</i>

Enabling Broadcast-Storm Control on a Port

Broadcast-storm control blocks the forwarding of packets created by broadcast storms, the bursts of broadcast traffic that ports can sometimes generate. When you enable broadcast-storm control on a port, two threshold parameters define the beginning and the end of a broadcast storm. The **rising** parameter determines when the forwarding of broadcast packets from the port is blocked. The **falling** parameter determines when normal forwarding resumes. You can set the port to generate a trap when these thresholds are crossed, and you can disable the port during a broadcast storm.

Beginning in privileged EXEC mode, follow these steps to enable broadcast storm control:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter interface configuration mode and define the interface to configure.	interface <i>interface</i>
Step 3 Enter the port storm-control command and the two threshold parameters.	port storm-control threshold [rising <i>number</i> falling <i>number</i>]
Step 4 Return to EXEC mode to verify the entry.	end
Step 5 Verify that the parameters were entered correctly by using the show command.	show port storm-control <i>interface</i>

Enabling Port Security

Secured ports limit the forwarding of traffic to secure addresses entered in the MAC address table. You can manually enter these addresses, or the switch can learn them. Blocking the flooding of unicast and multicast packets to a port ensures that the port is completely secure.

When you secure a port, you can also define the number of addresses that it can learn. The switch does not learn addresses on this port after it has reached this number.

Beginning in privileged EXEC mode, follow these steps to enable security on a port:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter interface configuration mode, and define the interface to configure.	interface <i>interface</i>
Step 3 Define the maximum number of addresses this port can learn.	port security max-mac-count <i>address-number</i>
Step 4 Define the action to take in the event of an address violation.	port security action {shutdown trap}
Step 5 Return to EXEC mode to verify the entry.	end
Step 6 Verify the entry by using the show command.	show port security <i>interface</i>

Managing the Switch Address Table

The Catalyst 2900 address table contains the MAC addresses of devices that have forwarded packets to the switch. The switch stores each address in the address table and associates it with the port on which it was received. With this information—the MAC address and its associated port—the switch can forward packets to the correct destination port.

You can also manually enter addresses and their ports in the address table. Catalyst 2900 series XL switches support three kinds of addresses:

Dynamic addresses are MAC addresses that are learned by the switch but dropped (aged) when not used.

Secure addresses are MAC addresses that do not age and are retained when the switch is reset. The port can learn secure addresses, or you can manually enter them.

Static addresses are MAC addresses that are manually entered into the address table and that are accompanied by a *forwarding map* that the switch uses to make forwarding decisions.

This section describes how to use the CLI to complete the following address-table tasks:

- Adding secure addresses to the address table
- Adding static addresses to the address table
- Defining the number of secure addresses a port can learn
- Defining the aging time for the address table
- Displaying the contents of the address table

Adding Secure Addresses to the Address Table

Secure addresses do not age and can either be manually entered into the address table or learned. Beginning in privileged EXEC mode, complete these tasks to enter a secure address for a port:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the MAC address and the interface with which it is associated.	mac-address-table secure <i>hw-addr interface</i>
Step 3 Return to EXEC mode to verify the entry.	end
Step 4 Verify the entry by using the show command to display the secure address in the address table.	show mac-address-table secure

Adding Static Addresses to the Address Table

Static addresses are entered in the address table with an *in-port* and an *out-port-list*. Packets received from the *in-port* can be forwarded to ports listed in the *out-port-list*. Beginning in privileged EXEC mode, complete the following tasks to enter a static address in the address table:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the MAC address, the input port, and the port to which it can be forwarded.	mac-address-table static <i>hw-addr in-port out-port-list</i>
Step 3 Return to EXEC mode to verify the entry.	end
Step 4 Verify the entry by using the show command to display the static address in the address table.	show mac-address-table static

Defining the Number of Secure Addresses a Port Can Learn

When port security is enabled on a port, you can manually enter addresses for the port or let the port learn addresses up to a number you define. Although these addresses are learned, they do not age and are not lost when the switch resets. Beginning in privileged EXEC mode, complete these tasks to enter the number of secure addresses a secure port can learn:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter interface configuration mode and define the interface to configure.	interface <i>interface</i>
Step 3 Enter the number of addresses that the port can learn. You can enter a value from 1 to 132.	port security max-mac-count <i>address-number</i>
Step 4 Return to EXEC mode to verify the entry.	end
Step 5 Verify the entry by using the show command.	show port security <i>interface max-sec-cnt</i>

Defining the Aging time for the Address Table

The address table retains dynamic addresses for a configurable amount of time (the aging time). This value is valid for all dynamic addresses. Beginning in privileged EXEC mode, complete the following tasks to define the aging time for the address table.

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Enter the number of seconds that dynamic addresses are to be retained in the address table. You can enter from 1 to 1,000,000.	mac-address-table aging-time <i>seconds</i>
Step 3 Return to EXEC mode to verify the entry.	end
Step 4 Verify your entry by using the show command.	show mac-address-table aging-time

Displaying the Contents of the Address Table

To display the contents of the address table, enter the **show mac-address-table** command in EXEC mode:

```
switch# show mac-address-table
Switch#show mac-address-table
Dynamic Addresses Count:                20
Secure Addresses (User-defined) Count:  2
Static Addresses (User-defined) Count:  0
System Self Addresses Count:            29
Total MAC addresses:                    51
Non-static Address Table:
Destination Address  Address Type  Destination Port
-----
0000.0c5c.e176      Dynamic      FastEthernet0/8
0010.5478.eed7      Dynamic      FastEthernet0/8
0060.2f35.0068      Dynamic      FastEthernet0/6
0060.5cf4.0076      Dynamic      FastEthernet0/6
0060.5cf4.0077      Dynamic      FastEthernet0/5
0060.70cb.f301      Dynamic      FastEthernet0/5
0060.8337.a7d1      Dynamic      FastEthernet0/5
```

Entering the Speed and Duplex Settings for a Port

You can manually enter the speed (10 Mbps or 100 Mbps) and duplex (half or full) settings for a port, or you can let the switch configure the port by using the IEEE 802.3u autonegotiation protocol.

Autonegotiation is still enabled when one of the parameters has been manually set. The mix of autonegotiation and explicitly set parameters can produce unexpected results that affect performance. To maximize the performance of your switch, follow these guidelines when setting the speed and duplex parameters:

- Let both ends of a connection autonegotiate the speed and duplex parameters.
- or
- Manually set both parameters at both ends of the connection.

Beginning in privileged EXEC mode, complete these tasks to set the speed and duplex parameters on a port:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Define the interface to be configured.	interface <i>interface</i>
Step 3 Set the speed parameter for the interface.	speed { 10 100 auto }
Step 4 Set the duplex parameter for the interface.	duplex { full half auto }
Step 5 Return to EXEC mode to verify the entry.	end
Step 6 Verify your entry by using the show command.	show running-config

Entering Spanning-Tree Protocol Parameters

Spanning-Tree Protocol (STP) is enabled by default on the switch. You can use the **spantree** command to change the global and port-based STP parameters. The following parameters can be set for the entire switch and are entered in interface configuration mode with Vlan1 (the switch) as the interface:

- disable
- forward-time
- hello-time
- max-age
- priority
- protocol

The following parameters can be entered on a per-port basis in interface configuration mode:

- cost
- portfast
- priority

Enabling PortFast on a Port

The PortFast option is a simplified version of Spanning-Tree Protocol that accelerates the process of bringing a port into the forwarding state. Use this option when a port is connected to a workstation or server and cannot contribute to bridging loops.



Caution Enabling this option on a port connected to a switch or hub could prevent Spanning-Tree Protocol from detecting and disabling loops in your network.

Disable PortFast on a port with the **no** version of this command. Beginning in privileged EXEC mode, follow these steps to enable PortFast on a port:

Task	Command
Step 1 Enter global configuration mode.	configure terminal
Step 2 Define the interface to be configured.	interface <i>interface</i>
Step 3 Enable the PortFast feature for the interface.	spantree portfast
Step 4 Return to EXEC mode to verify the entry.	end
Step 5 Verify your entry by entering the show running-config command.	show running-config