



## Checking Port Status and Connectivity

This chapter describes how to check switch port status and connectivity on the Catalyst 4006 switch with Supervisor Engine III.

This chapter includes the following sections:

- [Checking Module Status, page 5-1](#)
- [Checking Interfaces Status, page 5-2](#)
- [Checking MAC Addresses, page 5-2](#)
- [Using Telnet, page 5-3](#)
- [Changing the Logout Timer, page 5-4](#)
- [Monitoring User Sessions, page 5-4](#)
- [Using Ping, page 5-5](#)
- [Using IP Traceroute, page 5-6](#)
- [Configuring ICMP, page 5-7](#)



### Note

For complete syntax and usage information for the commands used in this publication, refer to the *Command Reference for the Catalyst 4006 Switch with Supervisor Engine III* and the publications at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/index.htm>.

## Checking Module Status

The Catalyst 4006 switch with Supervisor Engine III is a multimodule system. You can see which modules are installed, as well as the MAC address ranges and version numbers for each module, by using the **show module** command. You can use the *[mod\_num]* argument to specify a particular module number to see detailed information on that module.

This example shows how to check module status for all modules on your switch:

```
Switch# show module all
```

Mod	Ports	Card Type	Model	Serial No.
1	2	1000BaseX (GBIC) Supervisor Module	WS-X4014	JAB012345AB
5	24	10/100/1000BaseTX (RJ45)	WS-X4424-GB-RJ45	JAB045304EY
6	48	10/100BaseTX (RJ45)	WS-X4148	JAB023402QK

```

M MAC addresses                               Hw  Fw                               Sw                               Stat
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 0004.dd46.9f00 to 0004.dd46.a2ff 0.0 12.1(10r)EW(1.21) 12.1(10)EW(1)      Ok
5 0050.3e7e.1d70 to 0050.3e7e.1d87 0.0                               Ok
6 0050.0f10.2370 to 0050.0f10.239f 1.0                               Ok
Switch#

```

## Checking Interfaces Status

You can view summary or detailed information on the switch ports using the **show interfaces status** command. To see summary information on all of the ports on the switch, enter the **show interfaces status** command with no arguments. Specify a particular module number to see information on the ports on that module only. Enter both the module number and the port number to see detailed information about the specified port.

To apply configuration commands to a particular port, you must specify the appropriate logical module. For more information, see the [“Checking Module Status” section on page 5-1](#).

This example shows how to display the status of all interfaces on a Catalyst 4000 Family switch:

```
Switch#show interfaces status
```

```

Port      Name              Status      Vlan      Duplex  Speed Type
Gi1/1    Gi1/1             notconnect  1         auto    auto No Gbic
Gi1/2    Gi1/2             notconnect  1         auto    auto No Gbic
Gi5/1    Gi5/1             notconnect  1         auto    auto 10/100/1000-TX
Gi5/2    Gi5/2             notconnect  1         auto    auto 10/100/1000-TX
Gi5/3    Gi5/3             notconnect  1         auto    auto 10/100/1000-TX
Gi5/4    Gi5/4             notconnect  1         auto    auto 10/100/1000-TX
Fa6/1    Fa6/1             connected   1         a-full  a-100 10/100BaseTX
Fa6/2    Fa6/2             connected   2         a-full  a-100 10/100BaseTX
Fa6/3    Fa6/3             notconnect  1         auto    auto 10/100BaseTX
Fa6/4    Fa6/4             notconnect  1         auto    auto 10/100BaseTX

```

```
Switch#
```

This example shows how to display the status of interfaces in error-disabled state:

```
Switch# show interfaces status err-disabled
```

```

Port      Name              Status      Reason
Fa9/4    Fa9/4             err-disabled link-flap
informational error message when the timer expires on a cause
-----
5d04h:%PM-SP-4-ERR_RECOVER:Attempting to recover from link-flap err-disable state on Fa9/4
Switch#

```

## Checking MAC Addresses

In addition to displaying the MAC address range for a module using the **show module** command, you can display the MAC address table information of a specific MAC address or a specific interface in the switch using the **show mac-address-table address** and **show mac-address-table interface** commands.

This example shows how to display MAC address table information for a specific MAC address:

```
Switch# show mac-address-table address 0050.3e8d.6400
vlan  mac address      type      protocol  qos      ports
-----+-----+-----+-----+-----+-----
200  0050.3e8d.6400  static   assigned  --      Switch
100  0050.3e8d.6400  static   assigned  --      Switch
  5  0050.3e8d.6400  static   assigned  --      Switch
  4  0050.3e8d.6400  static          ipx  --      Switch
  1  0050.3e8d.6400  static          ipx  --      Switch
  1  0050.3e8d.6400  static   assigned  --      Switch
  4  0050.3e8d.6400  static   assigned  --      Switch
  5  0050.3e8d.6400  static          ipx  --      Switch
100  0050.3e8d.6400  static          ipx  --      Switch
200  0050.3e8d.6400  static          ipx  --      Switch
100  0050.3e8d.6400  static     other  --      Switch
200  0050.3e8d.6400  static     other  --      Switch
  5  0050.3e8d.6400  static     other  --      Switch
  4  0050.3e8d.6400  static          ip   --      Switch
  1  0050.3e8d.6400  static          ip   --      Route
  1  0050.3e8d.6400  static     other  --      Switch
  4  0050.3e8d.6400  static     other  --      Switch
  5  0050.3e8d.6400  static          ip   --      Switch
200  0050.3e8d.6400  static          ip   --      Switch
100  0050.3e8d.6400  static          ip   --      Switch
Switch#
```

This example shows how to display MAC address table information for a specific interface:

```
Switch# show mac-address-table interface gigabit 1/1
Multicast Entries
vlan  mac address      type      ports
-----+-----+-----+-----
  1  ffff.ffff.ffff  system  Switch,Gi6/1,Gi6/2,Gi6/9,Gi1/1
Switch#
```

## Using Telnet

You can access the switch command-line interface (CLI) using Telnet. In addition, you can use Telnet from the switch to access other devices in the network. You can have up to eight simultaneous Telnet sessions.

Before you can open a Telnet session to the switch, you must first set the IP address (and in some cases the default gateway) for the switch. For information about setting the IP address and default gateway, see [Chapter 3, “Configuring the Switch for the First Time.”](#)



### Note

To **telnet** to a host using the hostname, configure and enable DNS.

To **telnet** to another device on the network from the switch, enter this command in privileged EXEC mode:

Command	Purpose
Switch# <b>telnet</b> <i>host</i> [ <i>port</i> ]	Opens a Telnet session to a remote host.

This example shows how to **telnet** from the switch to the remote host named labsparc:

```
Switch# telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:
```

## Changing the Logout Timer

The logout timer automatically disconnects a user from the switch when the user is idle for longer than the specified time. To set the logout timer, enter the following command in privileged EXEC mode:

Command	Purpose
Switch# <b>logoutwarning</b> <i>number</i>	Changes the logout timer value (a timeout value of 0 prevents idle sessions from being disconnected automatically). Use the <b>no</b> keyword to return to the default value.

## Monitoring User Sessions

You can display the currently active user sessions on the switch using the **show users** command. The command output lists all active console port and Telnet sessions on the switch.

To display the active user sessions on the switch, enter the following command in privileged EXEC mode:

Command	Purpose
Switch# <b>show users</b> [ <b>all</b> ]	Displays the currently active user sessions on the switch.

This example shows the output of the **show users** command when local authentication is enabled for console and Telnet sessions (the asterisk [\*] indicates the current session):

```
Switch#show users
  Line      User      Host(s)      Idle      Location
*  0 con 0      idle         00:00:00

  Interface  User      Mode          Idle      Peer Address

Switch#show users all
  Line      User      Host(s)      Idle      Location
*  0 con 0      idle         00:00:00
  1 vty 0      idle         00:00:00
  2 vty 1      idle         00:00:00
  3 vty 2      idle         00:00:00
  4 vty 3      idle         00:00:00
  5 vty 4      idle         00:00:00
```

```

Interface      User      Mode      Idle      Peer Address
Switch#

```

To disconnect an active user session, enter the following command in privileged EXEC mode:

Command	Purpose
Switch# <b>disconnect</b> {console   ip_addr}	Disconnects an active user session on the switch.

This example shows how to disconnect an active console port session and an active Telnet session:

```

Switch> disconnect console
Console session disconnected.
Console> (enable) disconnect tim-nt.bigcorp.com
Telnet session from tim-nt.bigcorp.com disconnected. (1)
Switch# show users
  Session  User      Location
  -----  -
telnet    jake      jake-mac.bigcorp.com
* telnet  suzy      suzy-pc.bigcorp.com
Switch#

```

## Using Ping

These sections describe how to use IP ping:

- [Understanding How Ping Works, page 5-5](#)
- [Running Ping, page 5-6](#)

## Understanding How Ping Works

You can use the **ping** command to verify connectivity to remote hosts. If you attempt to ping a host in a different IP subnetwork, you must define a static route to the network or configure a router to route between those subnets.

The **ping** command is configurable from normal executive and privileged EXEC mode. Ping returns one of the following responses:

- Normal response—The normal response (*hostname is alive*) occurs in 1 to 10 seconds, depending on network traffic.
- Destination does not respond—If the host does not respond, a No Answer message is returned.
- Unknown host—If the host does not exist, an Unknown Host message is returned.
- Destination unreachable—If the default gateway cannot reach the specified network, a Destination Unreachable message is returned.
- Network or host unreachable—If there is no entry in the route table for the host or network, a Network or Host Unreachable message is returned.

To stop a ping in progress, press **Ctrl-C**.

## Running Ping

To ping another device on the network from the switch, enter the following command in normal or privileged EXEC mode:

Command	Purpose
Switch# <b>ping</b> <i>host</i>	Checks connectivity to a remote host.

This example shows how to ping a remote host from normal executive mode:

```
Switch# ping labsparc
labsparc is alive
Switch> ping 72.16.10.3
12.16.10.3 is alive
Switch#
```

This example shows how to enter a **ping** command in privileged EXEC mode specifying the number of packets, the packet size, and the timeout period:

```
Switch# ping
Target IP Address []: 12.20.5.19
Number of Packets [5]: 10
Datagram Size [56]: 100
Timeout in seconds [2]: 10
Source IP Address [12.20.2.18]: 12.20.2.18
!!!!!!!!!!

----12.20.2.19 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 1/1/1
Switch
```

## Using IP Traceroute

These sections describe how to use IP traceroute feature:

- [Understanding How IP Traceroute Works, page 5-6](#)
- [Running IP Traceroute, page 5-7](#)

## Understanding How IP Traceroute Works

You can use IP traceroute to identify the path that packets take through the network on a hop-by-hop basis. The command output displays all network layer (Layer 3) devices, such as routers, that the traffic passes through on the way to the destination.

Layer 2 switches can participate as the source or destination of the **trace** command but will not appear as a hop in the **trace** command output.

The **trace** command uses the Time To Live (TTL) field in the IP header to cause routers and servers to generate specific return messages. Traceroute starts by sending a User Datagram Protocol (UDP) datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it

drops the datagram and sends back an Internet Control Message Protocol (ICMP) Time-Exceeded message to the sender. Traceroute determines the address of the first hop by examining the source address field of the ICMP Time-Exceeded message.

To identify the next hop, traceroute sends a UDP packet with a TTL value of 2. The first router decrements the TTL field by 1 and sends the datagram to the next router. The second router sees a TTL value of 1, discards the datagram, and returns the Time-Exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host or until the maximum TTL is reached.

To determine when a datagram reaches its destination, traceroute sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP Port Unreachable error message to the source. The Port Unreachable error message indicates to traceroute that the destination has been reached.

## Running IP Traceroute

To trace the path that packets take through the network, enter the following command in EXEC or privileged EXEC mode:

Command	Purpose
Switch# <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]	Runs IP traceroute to trace the path that packets take through the network.

This example shows use the **trace** command to display the route a packet takes through the network to reach its destination:

```
Switch# trace ip ABA.NYC.mil

Type escape sequence to abort.
Tracing the route to ABA.NYC.mil (26.0.0.73)
 0 DEBRIS.CISCO.COM (192.180.1.6) 1000 msec 8 msec 4 msec
 1 BARRNET-GW.CISCO.COM (192.180.16.2) 8 msec 8 msec 8 msec
 2 EXTERNAL-A-GATEWAY.STANFORD.EDU (192.42.110.225) 8 msec 4 msec 4 msec
 3 BB2.SU.BARRNET.NET (192.200.254.6) 8 msec 8 msec 8 msec
 4 SU.ARC.BARRNET.NET (192.200.3.8) 12 msec 12 msec 8 msec
 5 MOFFETT-FLD-MB.in.MIL (192.52.195.1) 216 msec 120 msec 132 msec
 6 ABA.NYC.mil (26.0.0.73) 412 msec 628 msec 664 msec
Switch#
```

## Configuring ICMP

Internet Control Message Protocol (ICMP) provides many services that control and manage IP connections. ICMP messages are sent by routers or access servers to hosts or other routers when a problem is discovered with the Internet header. For detailed information on ICMP, refer to RFC 792.

## Enabling ICMP Protocol Unreachable Messages

If the Cisco IOS software receives a nonbroadcast packet that uses an unknown protocol, it sends an ICMP Protocol Unreachable message back to the source.

Similarly, if the software receives a packet that it is unable to deliver to the ultimate destination because it knows of no route to the destination address, it sends an ICMP Host Unreachable message to the source. This feature is enabled by default.

To enable the generation of ICMP Protocol Unreachable and Host Unreachable messages, enter the following command in interface configuration mode:

Command	Purpose
Switch (config-if)# [no] ip unreachable	Enables ICMP destination unreachable messages. Use the <b>no</b> keyword to disable the ICMP destination unreachable messages.

To limit the rate that Internet Control Message Protocol (ICMP) destination unreachable messages are generated, enter the following command in global configuration mode:

Command	Purpose
Switch (config)# [no] ip icmp rate-limit unreachable [df] <i>milliseconds</i>	Limits the rate that ICMP destination messages are generated. Use the <b>no</b> keyword to remove the rate limit and reduce the CPU usage.

## Enabling ICMP Redirect Messages

Data routes are sometimes less than optimal. For example, it is possible for the router to be forced to resend a packet through the same interface on which it was received. If this occurs, the Cisco IOS software sends an ICMP Redirect message to the originator of the packet telling the originator that the router is on a subnet directly connected to the receiving device, and that it must forward the packet to another system on the same subnet. The software sends an ICMP Redirect message to the packet's originator because the originating host presumably could have sent that packet to the next hop without involving this device at all. The Redirect message instructs the sender to remove the receiving device from the route and substitute a specified device representing a more direct path. This feature is enabled by default.

However, when Hot Standby Router Protocol (HSRP) is configured on an interface, ICMP Redirect messages are disabled (by default) for the interface. For more information on HSRP, refer to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt1/1cdip.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt1/1cdip.htm)

To enable the sending of ICMP Redirect messages if the Cisco IOS software is forced to resend a packet through the same interface on which it was received, enter the following command in interface configuration mode:

Command	Purpose
Switch (config-if)# [no] ip redirects	Enables ICMP Redirect messages. Use the <b>no</b> keyword to disable the ICMP Redirect messages and reduce CPU usage.

## Enabling ICMP Mask Reply Messages

Occasionally, network devices must know the subnet mask for a particular subnetwork in the internetwork. To obtain this information, devices can send ICMP Mask Request messages. These messages are responded to by ICMP Mask Reply messages from devices that have the requested information. The Cisco IOS software can respond to ICMP Mask Request messages if the ICMP Mask Reply function is enabled.

To have the Cisco IOS software respond to ICMP mask requests by sending ICMP Mask Reply messages, use the **ip mask-reply** interface configuration command.

Command	Purpose
Switch (config-if)# [ <b>no</b> ] <b>ip mask-reply</b>	Enables response to ICMP destination mask requests. Use the <b>no</b> keyword to disable this functionality.

