



Checking Port Status and Connectivity

This chapter describes how to check switch port status and connectivity on the Catalyst enterprise LAN switches.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Catalyst 5000 Family Command Reference*.

This chapter consists of these sections:

- [Checking Module Status, page 21-1](#)
- [Checking Port Status, page 21-3](#)
- [Checking Port Capabilities, page 21-5](#)
- [Using Telnet, page 21-6](#)
- [Using Secure Shell Encryption for Telnet Sessions, page 21-7](#)
- [Monitoring User Sessions, page 21-7](#)
- [Using Ping, page 21-9](#)
- [Using Layer 2 Traceroute, page 21-11](#)
- [Using IP Traceroute, page 21-12](#)

Checking Module Status

The Catalyst enterprise LAN switches are multimodule systems. You can see what modules are installed, as well as the MAC address ranges and version numbers for each module, using the **show module** [*mod_num*] command. Specify a particular module number to see detailed information on that module.



Note

For detailed information on the output of the **show module** command, see the *Catalyst 5000 Family Command Reference*.

This example shows how to check module status on a Catalyst 5000 family switch. The output shows that there are two supervisor engine modules (one in standby mode), four additional modules (including an RSM/VIP2 in slots 4 and 5 and a two-slot 10BASE-T Ethernet module in slots 9 and 10), and a LightStream 1010 ASP installed in the chassis.

```

Console> (enable) show module
Mod Slot Ports Module-Type           Model           Status
-----
1  1    4    100BaseFX MMF Supervisor  WS-X5530       ok
2  2    4    100BaseFX MMF Supervisor  WS-X5530       standby
4  4    4    Route Switch Ext Port
5  5    1    Route Switch              WS-X5302       ok
7  7    1    Network Analysis/RMON     WS-X5380       ok
8  8    1    MM OC-3 ATM               WS-X5155       ok
9  9    1    10/100BaseTX Ethernet Ext WS-X5238
10 10   48   10/100BaseTX Ethernet     WS-X5238       ok
13 13    1    ASP/SRP

Mod Module-Name           Serial-Num
-----
1
2
4
5
7
8
9
10

Mod MAC-Address(es)           Hw    Fw    Sw
-----
1  00-e0-4f-ac-b0-00 to 00-e0-4f-ac-b3-ff 1.3  3.1.2  5.1(1)
1  00-e0-1e-9b-2e-00 to 00-e0-1e-9b-31-ff 1.3  3.1.2  5.1(1)
5  00-e0-1e-91-d5-14 to 00-e0-1e-91-d5-15 5.0  20.7   11.3 (3a)WA4 (5)
7  00-e0-14-10-18-00          0.100 4.1.1  4.3 (0.31)
8  00-e0-1e-a9-20-b9          1.2   1.3   3.2 (7)
10 00-50-0f-08-c3-f0 to 00-50-0f-08-c4-1f 0.1   5.3 (1)B 5.1 (1)

Mod Sub-Type Sub-Model Sub-Serial Sub-Hw
-----
1  NFFC      WS-F5521  0011462777 1.1
1  uplink    WS-U5538  0011464723 2.0
2  NFFC      WS-F5521  0008936340 1.1
2  uplink    WS-U5538  0007464204 2.0
Console> (enable)

```

This example shows how to check module status on a specific module:

```

Console> (enable) show module 4
Mod Slot Ports Module-Type           Model           Status
-----
4  4    12   100BaseFX MM Ethernet     WS-X5201R      ok

Mod Module-Name           Serial-Num
-----
4  Backbone Links          00007285650

Mod MAC-Address(es)           Hw    Fw    Sw
-----
4  00-e0-1e-38-48-cc to 00-e0-1e-38-48-d7 0.2   4.1 (0.53-E 5.1 (1)
Console> (enable)

```

Checking Port Status

You can see summary or detailed information on the switch ports using the **show port** [*mod*[/*port*]] command. To see summary information on all of the ports on the switch, enter the **show port** 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.



Note

For detailed information on the output of the **show port** command, see the *Catalyst 5000 Family Command Reference* publication for your switch.

This example shows how to see information on the ports on a specific module only:

```
Console> (enable) show port 3
```

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
3/1		connected	10	normal	full	1000	1000BaseSX
3/2		connected	10	normal	full	1000	1000BaseSX
3/3		connected	20	normal	full	1000	1000BaseSX
3/4		connected	40	normal	full	1000	1000BaseSX
3/5		notconnect	1	normal	full	1000	No GBIC
3/6		notconnect	1	normal	full	1000	No GBIC

Port	Security	Secure-Src-Addr	Last-Src-Addr	Shutdown	Trap	IfIndex
3/1	disabled			No	disabled	15
3/2	disabled			No	disabled	16
3/3	disabled			No	disabled	17
3/4	disabled			No	disabled	18
3/5	disabled			No	disabled	19
3/6	disabled			No	disabled	20

Port	Send FlowControl admin	oper	Receive FlowControl admin	oper	RxPause	TxPause	Unsupported opcodes
3/1	desired	on	desired	on	0	0	0
3/2	desired	on	desired	on	0	0	0
3/3	desired	on	desired	on	0	0	0
3/4	desired	on	desired	on	0	0	0
3/5	desired	off	off	off	0	0	0
3/6	desired	off	off	off	0	0	0

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
3/1	connected	off	not channel		
3/2	connected	off	not channel		
3/3	connected	off	not channel		
3/4	connected	off	not channel		
3/5	notconnect	off	not channel		
3/6	notconnect	off	not channel		

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
3/1	-	0	0	0	0
3/2	-	0	0	0	0
3/3	-	0	0	0	0
3/4	-	0	0	0	0
3/5	-	0	0	0	0
3/6	-	0	0	0	0

Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants
3/1	0	0	0	0	0	0	0
3/2	0	0	0	0	0	0	0
3/3	0	0	0	0	0	0	0
3/4	0	0	0	0	0	0	0
3/5	0	0	0	0	0	0	0
3/6	0	0	0	0	0	0	0

Last-Time-Cleared

 Fri Apr 30 1999, 18:54:17
 Console> (enable)

This example shows how to see information on an individual port:

Console> (enable) **show port 2/1**

Port	Name	Status	Vlan	Level	Duplex	Speed	Type
2/1		connected	trunk	normal	full	1000	1000BaseSX

Port	Security	Secure-Src-Addr	Last-Src-Addr	Shutdown	Trap	IfIndex
2/1	disabled			No	disabled	9

Port	Send FlowControl admin	FlowControl oper	Receive FlowControl admin	FlowControl oper	RxPause	TxPause	Unsupported opcodes
2/1	desired	off	off	off	0	0	0

Port	Status	Channel mode	Channel status	Neighbor device	Neighbor port
2/1	connected	auto	not channel		

Port	Align-Err	FCS-Err	Xmit-Err	Rcv-Err	UnderSize
2/1	-	0	0	0	0

Port	Single-Col	Multi-Coll	Late-Coll	Excess-Col	Carri-Sen	Runts	Giants
2/1	0	0	0	0	0	0	0

Last-Time-Cleared

 Tue Dec 8 1998, 13:26:01
 Console> (enable)

Checking Port Capabilities

You can display the capabilities of any port in a switch using the **show port capabilities** *[[mod][port]]* command.

This example shows you how to display the port capabilities for switch ports:

```
Console> (enable) show port capabilities 1
Model                WS-X5509
Port                 1/1
Type                 100BaseTX
Speed                100
Duplex               half,full
Trunk encap type     ISL
Trunk mode           on,off,desirable,auto,nonegotiate
Channel              1/1-2
Broadcast suppression percentage(0-100)
Flow control         no
Security             yes
Membership           static,dynamic
Fast start           yes
Rewrite              no
```

```
-----
Model                WS-X5509
Port                 1/2
Type                 100BaseTX
Speed                100
Duplex               half,full
Trunk encap type     ISL
Trunk mode           on,off,desirable,auto,nonegotiate
Channel              1/1-2
Broadcast suppression percentage(0-100)
Flow control         no
Security             yes
Membership           static,dynamic
Fast start           yes
Rewrite              no
```

```
Console> (enable) show port capabilities 7/1
Model                WS-X5014
Port                 7/1
Type                 10BaseT
Speed                10
Duplex               half,full
Trunk encap type     no
Trunk mode           off
Channel              no
Broadcast suppression percentage(0-100)
Flow control         no
Security             yes
Membership           static,dynamic
Fast start           yes
Rewrite              no
```

```
Console> (enable) show port capabilities 8
Model                WS-X5155
Port                 8/1
Type                 OC3 MMF ATM
Speed                155
Duplex               full
Trunk encap type     LANE
Trunk mode           on
Channel              no
Broadcast suppression no
```

```

Flow control          no
Security              no
Membership            static
Fast start            no
Rewrite               no
Console> (enable)

```

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. Up to eight simultaneous Telnet sessions are possible.

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 IP Address and Default Gateway.”](#)

To use Telnet to connect to another device on the network from the switch, perform this task in privileged mode:

Task	Command
Open a Telnet session with a remote host.	telnet <i>host</i> [<i>port</i>]

This example shows how to connect from the switch to a remote host using Telnet:

```

Console> (enable) telnet labsparc
Trying 172.16.10.3...
Connected to labsparc.
Escape character is '^]'.

UNIX(r) System V Release 4.0 (labsparc)

login:

```

To change the logout timer value (the number of minutes after which an idle session is disconnected), perform this task in privileged mode:

Task	Command
Change the logout timer value (a timeout value of 0 prevents idle sessions from being disconnected automatically).	set logout <i>timeout</i>

This example shows how to set the logout timer value to 10 minutes:

```

Console> (enable) set logout 10
Sessions will be automatically logged out after 10 minutes of idle time.
Console> (enable)

```

This example shows how to set the logout timer value to 0, preventing idle sessions from being disconnected automatically:

```

Console> (enable) set logout 0
Sessions will not be automatically logged out.
Console> (enable)

```

Using Secure Shell Encryption for Telnet Sessions



Note

To use the Secure Shell encryption feature commands you must be running an encryption image. Encryption commands are: **set crypto key rsa**, **clear crypto key rsa**, and **show crypto key**. See [Chapter 33, “Working with System Software Images,”](#) for the software image naming conventions used for the encryption images.

The secure shell encryption feature provides security for Telnet sessions to the switch. Secure shell encryption is supported for remote logins to the switch only. Telnet sessions initiated from the switch cannot be encrypted. To use this feature, you must install the application on the client accessing the switch, and you must configure secure shell encryption on the switch.

The current implementation of Secure Shell encryption supports SSH version 1, both the DES and 3DES encryption methods, and can be used with RADIUS and TACACS+ authentication. To configure authentication with secure shell encryption, use the **telnet** keyword in the **set authentication** commands.



Note

If you are using Kerberos to authenticate to the switch, you will not be able to use the secure shell encryption feature.

To enable secure shell encryption on the switch, perform this task in privileged mode:

Task	Command
Create the RSA host key.	set crypto key rsa <i>nbits</i> [<i>force</i>]

This example shows how to create the RSA host key:

```
Console> (enable) set crypto key rsa 1024
Generating RSA keys.... [OK]
Console> (enable)
```

The *nbits* value specifies the RSA key size. Valid key size range is 512 to 2048 bits. A key size with a larger number provides higher security but takes longer to generate.

Monitoring User Sessions

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

To display the active user sessions on the switch, perform this task in privileged mode:

Task	Command
Display the currently active user sessions on the switch.	show users [<i>noalias</i>]

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):

```
Console> (enable) show users
  Session  User          Location
  -----  -
  console
  telnet           sam-pc.bigcorp.com
  * telnet         jake-mac.bigcorp.com
Console> (enable)
```

This example shows the output of the **show users** command when TACACS+ authentication is enabled for console and Telnet sessions:

```
Console> (enable) show users
  Session  User          Location
  -----  -
  console  sam
  telnet   jake          jake-mac.bigcorp.com
  telnet   tim           tim-nt.bigcorp.com
  * telnet suzy         suzy-pc.bigcorp.com
Console> (enable)
```

This example shows how to display information about user sessions using the **noalias** keyword to display the IP addresses of connected hosts:

```
Console> (enable) show users noalias
  Session  User          Location
  -----  -
  console
  telnet           10.10.10.12
  * telnet         10.10.20.46
Console> (enable)
```

To disconnect an active user session, perform this task in privileged mode:

Task	Command
Disconnect an active user session on the switch.	disconnect {console ip_addr}

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

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

Using Ping

These sections describe how to use IP ping:

- [Understanding How Ping Works, page 21-9](#)
- [Executing Ping, page 21-10](#)

Understanding How Ping Works

You can use IP ping to test connectivity to remote hosts. If you attempt to ping a host in a different IP subnet, 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 executive mode. In normal executive mode, the **ping** command supports the **-s** parameter, which allows you to specify the packet size and packet count. In privileged executive mode, the **ping** command allows you to specify the packet size, packet count, and the wait time.

Table 21-1 lists the ping default values.

Table 21-1 Ping Default Values

	Ping	Ping-s
Number of Packets	5	0=continuous ping
Packet Size	56	56
Wait Time	2	2
Source Address	Host IP Address	–

Ping will return 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**.

Executing Ping

To ping another device on the network from the switch, perform one of these tasks in normal or privileged mode:

Task	Command
Ping a remote host.	ping <i>host</i>
Ping a remote host using ping options.	ping -s <i>host</i> [<i>packet_size</i>] [<i>packet_count</i>]

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

```
Console> ping labsparc
labsparc is alive
Console> ping 72.16.10.3
12.16.10.3 is alive
Console>
```

This example shows how to ping a remote host using the ping -s option:

```
Console> ping -s 12.20.5.3 800 10
PING 12.20.2.3: 800 data bytes
808 bytes from 12.20.2.3: icmp_seq=0. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=1. time=3 ms
808 bytes from 12.20.2.3: icmp_seq=2. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=3. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=4. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=5. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=6. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=7. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=8. time=2 ms
808 bytes from 12.20.2.3: icmp_seq=9. time=3 ms

----17.20.2.3 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 2/2/3
Console>
```

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

```
Console> (enable) 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
Console> (enable)
```

Using Layer 2 Traceroute

These sections describe how to use Layer 2 traceroute:

- [Understanding Layer 2 Traceroute, page 21-11](#)
- [Configuration Guidelines, page 21-11](#)
- [Executing Layer 2 Traceroute, page 21-12](#)

Understanding Layer 2 Traceroute

The Layer 2 traceroute utility allows you to identify the physical path that a packet takes when going from a source to a destination. The Layer 2 traceroute utility determines the path by looking at the forwarding engine tables of the switches in the path.

Information is displayed about all Catalyst 5000 family switches that are in the path from the source to the destination.

Configuration Guidelines

Follow these configuration guidelines when using the Layer 2 traceroute utility:

- The Layer 2 traceroute utility works for unicast traffic only.
- CDP must be enabled on all of the Catalyst 5000 family switches in the network. (See [Chapter 22, “Configuring CDP”](#) for information about enabling CDP.) If any devices in the path are transparent to CDP, the **l2trace** command will not trace the path through those devices.
- You can use this utility from a switch that is not in the Layer 2 path between the source and the destination; however, all of the switches in the path, including the source and destination, must be reachable from the switch.
- All switches in the path must be reachable from each other.
- You can trace a Layer 2 path by specifying the source and destination IP addresses (or IP aliases) or the MAC addresses. If the source and destination belong to multiple VLANs and you specify MAC addresses, you can also specify a VLAN.
- The source and destination switches must belong in the same VLAN.
- The maximum number of hops an **l2trace** command query tries is 10; this number includes hops involved in source tracing.
- Layer 2 traceroute does not work with Token Ring VLANs, or when multiple devices are attached to one port through hubs, or when there are multiple neighbors on a port.

Executing Layer 2 Traceroute

To identify a Layer 2 path, perform one of these tasks in privileged mode.

Task	Command
(Optional) Trace a Layer 2 path using MAC addresses.	l2trace { <i>src-mac-addr</i> } { <i>dest-mac-addr</i> } [<i>vlan</i>] [detail]
(Optional) Trace a Layer 2 path using IP addresses or IP aliases.	l2trace { <i>src-ip-addr</i> } { <i>dest-ip-addr</i> } [detail]

This example shows the source and destination MAC addresses specified, with no VLAN specified, and the **detail** option specified. For each Catalyst 5000 family switch found in the path, the output shows the device type, device name, device IP address, in port name, in port speed, in port duplex mode, out port name, out port speed, and out port duplex mode.

```
Console> (enable) l2trace 00-01-22-33-44-55 10-22-33-44-55-66 detail
```

```
l2trace vlan number is 10.
```

```
00-01-22-33-44-55 found in C5500 named wiring-1 on port 4/1 10Mb half duplex
C5500:wiring-1:192.168.242.10:4/1 10Mb half duplex -> 5/2 100MB full duplex
C5000:backup-wiring-1:192.168.242.20:1/1 100Mb full duplex -> 3/1 100MB full duplex
C5000:backup-core-1:192.168.242.30:4/1 100 MB full duplex -> 1/1 100MB full duplex
C6000:core-1:192.168.242.40:1/1 100MB full duplex -> 2/1 10MB half duplex.
10-22-33-44-55-66 found in C6000 named core-1 on port 2/1 10MB half duplex.
Console> (enable)
```

Using IP Traceroute

These sections describe how to use IP traceroute:

- [Understanding IP Traceroute, page 21-12](#)
- [Executing IP Traceroute, page 21-13](#)

Understanding IP Traceroute

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.

Switches can participate as the source or destination of the **traceroute** command but will not appear as a hop in the **traceroute** command output.

The **traceroute** 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. The traceroute facility 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 to the source. This message indicates to the traceroute facility that it has reached the destination.

Executing IP Traceroute

To trace the path that packets take through the network, perform this task in privileged mode:

Task	Command
Execute IP traceroute to trace the Layer 3 path that packets take through the network.	traceroute [-n] [-w <i>wait_time</i>] [-i <i>initial_ttl</i>] [-m <i>max_ttl</i>] [-p <i>dest_port</i>] [-q <i>nqueries</i>] [-t <i>tos</i>] <i>host</i> [<i>data_size</i>]

This example shows how to use the **traceroute** command:

```
Console> (enable) traceroute 10.1.1.100
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 40 byte packets
 1 10.1.1.1 (10.1.1.1)  1 ms  2 ms  1 ms
 2 10.1.1.100 (10.1.1.100)  2 ms  2 ms  2 ms
Console> (enable)
```

This example shows how to perform a **traceroute** with six queries to each hop with packets of 1400 bytes each:

```
Console> (enable) traceroute -q 6 10.1.1.100 1400
traceroute to 10.1.1.100 (10.1.1.100), 30 hops max, 1440 byte packets
 1 10.1.1.1 (10.1.1.1)  2 ms  2 ms  2 ms  1 ms  2 ms  2 ms
 2 10.1.1.100 (10.1.1.100)  2 ms  4 ms  3 ms  3 ms  3 ms  3 ms
Console> (enable)
```

