Troubleshooting

Troubleshooting

Recovering a Lost Password

This section describes how to recover a lost network administrator password using the console port of the switch.

You can recover the network administrator password using one of two methods:

- From the CLI with a username that has network-admin privileges
- By power cycling the switch

Using the CLI with Network-Admin Privileges

If you are logged in to, or can log into, the switch with a username that has network-admin privileges, follow these steps:

SUMMARY STEPS

1. Verify that your username has network-admin privileges.
2. Assign a new network administrator password if your username has network-admin privileges.
3. Save the configuration.

DETAILED STEPS

Step 1 Verify that your username has network-admin privileges.

Example:

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:dbgusr
        this user account has no expiry date
        roles:network-admin network-operator
```

Step 2 Assign a new network administrator password if your username has network-admin privileges.

Example:

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
```

Step 3 Save the configuration.

Example:

```
switch# copy running-config startup-config
```

Power Cycling the Switch

If you cannot start a session on the switch that has network-admin privileges, you must recover the network administrator password by power cycling the switch.

Caution This procedure disrupts all traffic on the switch.

Note You cannot recover the administrator password from a Telnet or SSH session. You must have access to the local console connection.

To recover the network administrator password by power cycling the switch, follow these steps:

Establish a terminal session on the console port of the supervisor module.

SUMMARY STEPS

1. Power cycle the switch.
2. Press the **Ctrl-]** key sequence from the console port session when the switch begins the Cisco NX-OS software boot sequence to enter the boot prompt mode.
3. Reset the network administrator password.
4. Display the bootflash: contents to locate the Cisco NX-OS software image file.
5. Load the Cisco NX-OS system software image.
6. Log in to the switch using the new administrator password.
7. Reset the new password to ensure that is it is also the SNMP password.
8. Save the configuration.

DETAILED STEPS

Step 1 Power cycle the switch.

Step 2 Press the **Ctrl-]** key sequence from the console port session when the switch begins the Cisco NX-OS software boot sequence to enter the boot prompt mode.

Note In releases of Cisco NX-OS prior to 4.0(1a) the key sequence to enter the boot prompt mode was **Ctrl-Shift-B**.

Example:

```
Ctrl-]
switch(boot)#
```

Step 3 Reset the network administrator password.

Example:

```
switch(boot)# configure terminal
switch(boot-config)# admin-password <new password>
switch(boot-config)# exit
```

Step 4 Display the bootflash: contents to locate the Cisco NX-OS software image file.

Example:

```
switch(boot)# dir bootflash:
```

Step 5 Load the Cisco NX-OS system software image.

Example:

In the following example, the system image filename is nx-os.bin:

```
switch(boot) # load bootflash:nx-os.bin
```

Step 6 Log in to the switch using the new administrator password.

Example:

```
switch login: admin
Password: <new password>
```

Step 7 Reset the new password to ensure that is it is also the SNMP password.

Example:

```
switch# configure terminal
switch(config)# username admin password <new password>
switch(config)# exit
```

Step 8 Save the configuration.

Example:

```
switch# copy running-config startup-config
```

Using Ethanalyzer

Ethanalyzer is a Cisco NX-OS protocol analyzer tool based on the Wireshark (formerly Ethereal) open source code. Ethanalyzer is a command-line version of Wireshark that captures and decodes packets. You can use Ethanalyzer to troubleshoot your network and analyze the control-plane traffic.

To configure Ethanalyzer, use one or more of the following commands:

SUMMARY STEPS

1. switch# **ethanalyzer local interface** *interface*
2. switch# **ethanalyzer local interface** *interface* **brief**
3. switch# **ethanalyzer local interface** *interface* **limit-captured-frames**
4. switch# **ethanalyzer local interface** *interface* **limit-frame-size**
5. switch# **ethanalyzer local interface** *interface* **capture-filter**
6. switch# **ethanalyzer local interface** *interface* **display-filter**
7. switch# **ethanalyzer local interface** *interface* **write**
8. switch# **ethanalyzer local read** *file*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# **ethanalyzer local interface** *interface*	Captures packets sent or received by the supervisor and provides detailed protocol information. **Note** For all commands in this table, interface is inbound-hi (Inbound high-priority interface), inbound-low (Inbound low-priority interface), or mgmt (management interface).
Step 2	switch# **ethanalyzer local interface** *interface* **brief**	Captures packets sent or received by the supervisor and provides a summary of protocol information.
Step 3	switch# **ethanalyzer local interface** *interface* **limit-captured-frames**	Limits the number of frames to capture.
Step 4	switch# **ethanalyzer local interface** *interface* **limit-frame-size**	Limits the length of the frame to capture.
Step 5	switch# **ethanalyzer local interface** *interface* **capture-filter**	Filters the types of packets to capture.
Step 6	switch# **ethanalyzer local interface** *interface* **display-filter**	Filters the types of captured packets to display.
Step 7	switch# **ethanalyzer local interface** *interface* **write**	Saves the captured data to a file.
Step 8	switch# **ethanalyzer local read** *file*	Opens a captured data file and analyzes it.

Ethanalyzer does not capture data traffic that Cisco NX-OS forwards in the hardware.

Ethanalyzer uses the same capture filter syntax as tcpdump. For more information, see the following URL: http://www.tcpdump.org/tcpdump_man.html

For information on the syntax of the display filter, see the following URL: http://wiki.wireshark.org/DisplayFilters

This example shows captured data (limited to four packets) on the management interface:

```
switch# ethanalyzer local interface mgmt brief limit-captured-frames 4
Capturing on eth0
2005-01-25 07:18:08.997132 10.193.24.42 -> 10.200.0.103 TELNET Telnet Data ...
2005-01-25 07:18:09.166266 10.200.0.103 -> 10.193.24.42 TCP 1235 > telnet [ACK] Seq=0 Ack=19
 Win=64129 Len=0
2005-01-25 07:18:09.166830 10.193.24.42 -> 10.200.0.103 TELNET Telnet Data ...
2005-01-25 07:18:09.376250 10.200.0.103 -> 10.193.24.42 TCP 1235 > telnet [ACK] Seq=0 Ack=99
 Win=64049 Len=0
4 packets captured
```

This example shows detailed captured data for one HSRP packet:

```
switch(config)# ethanalyzer local interface mgmt capture-filter "tcp port 23"
limit-captured-frames 1
Capturing on eth0
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Jan 25, 2005 08:49:49.250719000
    [Time delta from previous captured frame: 1106642989.250719000 seconds]
    [Time delta from previous displayed frame: 1106642989.250719000 seconds]
    [Time since reference or first frame: 1106642989.250719000 seconds]
    Frame Number: 1
    Frame Length: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp]
Ethernet II, Src: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00), Dst: 00:0d:ec:6d:81:00
(00:0d:ec:6d:81:00)
    Destination: 00:0d:ec:6d:81:00 (00:0d:ec:6d:81:00)
        Address: 00:0d:ec:6d:81:00 (00:0d:ec:6d:81:00)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00)
        Address: 00:1a:a2:d2:d7:00 (00:1a:a2:d2:d7:00)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Type: IP (0x0800)
    Trailer: 000000000000
Internet Protocol, Src: 10.200.0.103 (10.200.0.103), Dst: 10.193.24.42 (10.193.24.42)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 40
    Identification: 0xa651 (42577)
    Flags: 0x04 (Don't Fragment)
        0... = Reserved bit: Not set
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 127
    Protocol: TCP (0x06)
    Header checksum: 0x2765 [correct]
        [Good: True]
        [Bad : False]
    Source: 10.200.0.103 (10.200.0.103)
    Destination: 10.193.24.42 (10.193.24.42)
Transmission Control Protocol, Src Port: 1288 (1288), Dst Port: telnet (23), Seq: 0, Ack:
0, Len: 0
    Source port: 1288 (1288)
    Destination port: telnet (23)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 0    (relative ack number)
    Header length: 20 bytes
    Flags: 0x10 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 64334
    Checksum: 0x934f [correct]
        [Good Checksum: True]
        [Bad Checksum: False]

1 packets captured
```

For more information on Wireshark, see the following URL: http://www.wireshark.org/docs/.

Troubleshooting Fibre Channel

fctrace

The fctrace feature provides the following capabilities:

- Trace the route followed by data traffic.
- Compute inter-switch (hop-to-hop) latency.

You can invoke fctrace by providing the FC ID, the N port WWN, or the device alias of the destination.

The trace frame is routed normally through the network until it reaches the far edge of the fabric. When the frame reaches the edge of the fabric (the F port connected to the end node with the given port WWN or the FC ID), the frame is looped back (swapping the source ID and the destination ID) to the originator.

If the destination cannot be reached, the path discovery starts, which traces the path up to the point of failure.

Note The fctrace feature works only on TE ports. Make sure that only TE ports exist in the path to the destination. If there is an E port in the path, the fctrace frame is dropped by that switch. Also, fctrace times out in the originator, and path discovery does not start.

To perform the fctrace operation, perform this task:

SUMMARY STEPS

1. switch# **fctrace** {**device-alias** *aliasname* | **fcid** *fcid*} **vsan** *vsan-id* [**timeout** *seconds*]

DETAILED STEPS

switch# **fctrace** {**device-alias** *aliasname* | **fcid** *fcid*} **vsan** *vsan-id* [**timeout** *seconds*]
The device-alias option specifies the device alias name. The fcid specifies the FCID of the destination N port, with the format 0xhhhhhh. The pwwn specifies the PWWN of the destination N port, with the format hh:hh:hh:hh:hh:hh:hh:hh. The vsan option specifies a VSAN ID.

Note By default the period to wait before a time out is 5 seconds and the range is from one through 10 seconds.

This example shows invoking fctrace for the specified FC ID of the destination N port:

```
switch# fctrace fcid 0xd70000 vsan 1
Route present for :  0xd70000

20:00:00:0b:46:00:02:82(0xfffcd5)

Timestamp Invalid.
20:00:00:05:30:00:18:db(0xfffcd7)

Timestamp Invalid.
20:00:00:05:30:00:18:db(0xfffcd7)
```

This example shows invoking fctrace using the pWWN of the destination N port.

```
switch# fctrace pwwn 21:00:00:e0:8b:06:d9:1d vsan 1 timeout 5
Route present for : 21:00:00:e0:8b:06:d9:1d
20:00:00:0b:46:00:02:82(0xfffcd5)

Timestamp Invalid.
20:00:00:05:30:00:18:db(0xfffcd7)

Timestamp Invalid.
20:00:00:05:30:00:18:db(0xfffcd7)
```

This example shows invoking fctrace using the device alias of the destination N port.

```
switch# fctrace device-alias disk1 vsan 1
Route present for : 22:00:00:0c:50:02:ce:f8
20:00:00:05:30:00:31:1e(0xfffca9)
```

fcping

The fcping feature verifies reachability of a node by checking its end-to-end connectivity. You can invoke the fcping feature by providing the FC ID, the destination port WWN, or the device alias information.

To perform a fcping operation, perform this task:

SUMMARY STEPS

1. switch# **fcping** {**device-alias** *aliasname* | **fcid** {*fc-port* | *domain-controller-id*} | **pwwn** *pwwn-id*} vsan *vsan-id* [**[count]** [*number*] [**[timeout]** [*value*] [**[usr-priority]** [*priority*]]]]

DETAILED STEPS

switch# **fcping** {**device-alias** *aliasname* | **fcid** {*fc-port* | *domain-controller-id*} | **pwwn** *pwwn-id*} vsan *vsan-id* [**[count]** [*number*] [**[timeout]** [*value*] [**[usr-priority]** [*priority*]]]]

The device-alias option specifies the device alias name. The fcid specifies the FCID of the destination N port, with the format 0xhhhhhh. The domain-controller-id option verifies connection to the destination switch. The pwwn specifies the PWWN of the destination N port, with the format hh:hh:hh:hh:hh:hh:hh:hh. The vsan option specifies a VSAN ID.

The last three are optional: The count option specifies the number of frames to send in a range of 0 to 2147483647. A value of 0 sends forever. By default, five frames are sent. The timeout option specifies the timeout value in seconds. The range is 1 to 10. The usr-priority option specifies the priority the frame receives in the switch fabric.

This example shows invoking fcping for the specified FCID of the destination:

```
switch# fcping fcid 0xd70000 vsan 1
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

This example shows invoking fcping using the count option:

```
switch# fcping fcid 0xd70000 vsan 1 count 10
28 bytes from  0xd70000  time = 730 usec
28 bytes from  0xd70000  time = 165 usec
28 bytes from  0xd70000  time = 262 usec
28 bytes from  0xd70000  time = 219 usec
28 bytes from  0xd70000  time = 228 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 230 usec
28 bytes from  0xd70000  time = 225 usec
28 bytes from  0xd70000  time = 229 usec
28 bytes from  0xd70000  time = 183 usec
10 frames sent, 10 frames received, 0 timeouts
Round-trip min/avg/max = 165/270/730 usec
```

This example shows invoking fcping with a timeout value:

```
switch# fcping fcid 0xd500b4 vsan 1 timeout 10
28 bytes from  0xd500b4  time = 1345 usec
...
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 340/581/1345 usec
```

This example shows invoking fcping for the specified device alias of the destination:

```
switch# fcping device-alias disk1 vsan 1
28 bytes from 22:00:00:0c:50:02:ce:f8 time = 1883 usec
28 bytes from 22:00:00:0c:50:02:ce:f8 time = 493 usec
28 bytes from 22:00:00:0c:50:02:ce:f8 time = 277 usec
28 bytes from 22:00:00:0c:50:02:ce:f8 time = 391 usec
28 bytes from 22:00:00:0c:50:02:ce:f8 time = 319 usec
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 277/672/1883 usec
```

This example shows invoking the fcping command when there is resource exhaustion at the N port:

```
switch# fcping fcid 0x010203 vsan 1
No response from the N port.
switch# fcping pwwn 21:00:00:20:37:6f:db:dd vsan 1
28 bytes from 21:00:00:20:37:6f:db:dd time = 1454 usec
...
5 frames sent, 5 frames received, 0 timeouts
Round-trip min/avg/max = 364/784/1454 usec
```

Note The command returns a "No response from the N port" message even when the N port is active. Retry the command a few seconds later.

Verifying Switch Connectivity

You can verify connectivity to a destination switch.

Note The FC ID variable used in this procedure is the domain controller address; it is not a duplication of the domain ID.

To verify connectivity to a destination switch, perform this task:

SUMMARY STEPS

1. switch# **show fcdomain domain-list vsan 200** **0xda**(218) 20:c8:00:05:30:00:87:9f [Local]
2. switch# **fcping fcid 0xFFFCDA vsan 200**

DETAILED STEPS

	Command or Action	Purpose

Step 1	switch# **show fcdomain domain-list vsan 200**
	0xda(218) 20:c8:00:05:30:00:87:9f [Local]
	
	Example:
	`Number of domains: 7`
	`Domain ID WWN`
	`--------- ----------`
	`0x01(1) 20:c8:00:05:30:00:59:df [Principal]`
	`0x02(2) 20:c8:00:0b:5f:d5:9f:c1`
	`0x6f(111) 20:c8:00:05:30:00:60:df`
	`0x06(6) 20:c8:00:0b:46:79:f2:41`
	`0x04(4) 20:c8:00:05:30:00:86:5f`
	`0x6a(106) 20:c8:00:05:30:00:f8:e3`
		Displays the destination switch's domain ID.
		To obtain the domain controller address, concatenate the domain ID with FFFC. For example, if the domain ID is 0xda(218), the concatenated ID is 0xfffcda.

Step 2	switch# **fcping fcid 0xFFFCDA vsan 200**
	
	Example:
	`28 bytes from 0xFFFCDA time = 298 usec`
	`28 bytes from 0xFFFCDA time = 260 usec`
	`28 bytes from 0xFFFCDA time = 298 usec`
	`28 bytes from 0xFFFCDA time = 294 usec`
	`28 bytes from 0xFFFCDA time = 292 usec`
	`5 frames sent, 5 frames received, 0 timeouts`
	`Round-trip min/avg/max = 260/288/298 usec`
		Verifies reachability of the destination switch by checking its end-to-end connectivity.

show tech-support Command

The **show tech-support** command is useful when collecting a large amount of information about the switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command varies depending on your configuration. Use the **show tech-support** command in EXEC mode to display general information about the switch when reporting a problem.

You can choose to have detailed information for each command. You can specify the output for a particular interface, module, or VSAN. Each command output is separated by line and the command precedes the output.

Note Explicitly set the **terminal length** command to 0 (zero) to disable auto-scrolling and enable manual scrolling. Use the **show terminal** command to view the configured the terminal size. After obtaining the output of this command, remember to reset your terminal length as required.

You can save the output of this command to a file by appending > (left arrow) and the filename to the **show tech-support** command. If you save this file, verify you have sufficient space to do so—each of these files may take about 1.8 MB. However, you can zip this file using the **gzip** *filename* command. Copy the zipped file to the required location using the **copy** command and unzip the file using the **gunzip** command.

The default output of the **show tech-support** command includes the output of the following commands:

- **show switchname**

- **show system uptime**
- **show interface mgmt0**
- **show interface mgmt1**
- **show system resources**
- **show version**
- **dir bootflash:**
- **show inventory**
- **show diagnostic result all**
- **show logging log**
- **show module**
- **show environment**
- **show sprom backplane**
- **show clock**
- **show callhome**
- **show cfs application**
- **show cfs lock**
- **show snmp**
- **show interface brief**
- **show interface**
- **show running-config**
- **show startup-config**
- **show ip route**
- **show arp**
- **show monitor session all**
- **show accounting log**
- **show process**
- **show process cpu**
- **show process log**
- **show process memory**
- **show processes log details**
- **show logging log**
- **show license host-id**
- **show license**

- **show license usage**
- **show system reset-reason**
- **show logging nvram**
- **show install all status**
- **show install all failure-reason**
- **show system internal log install**
- **show system internal log install details**
- **show cores**
- **show topology**
- **show kernel internal aipc**
- **show tech-support acl**
- **show vlan**
- **show vlan access-map**
- **show mac-address-table**
- **show spanning-tree summary**
- **show spanning-tree active**
- **show interface trunk**
- **show aclmgr status**
- **show aclmgr internal dictionaries**
- **show aclmgr internal log**
- **show aclmgr internal ppf**
- **show aclmgr internal state-cache**
- **show access-lists**
- **show platform software ethpm internal info all**
- **show object-group**
- **show logging onboard obfl-logs**

show tech-support brief Command

Use the **show tech-support brief** command to obtain a quick, condensed review of the switch configurations. This command provides a summary of the current running state of the switch (see the following example).

The **show tech-support brief** command is useful when collecting information about the switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

You can save the output of this command to a file by appending > (left arrow) and the filename to the **show tech-support brief** command.

This example shows how to display a condensed view of the switch configurations:

```
switch# show tech-support brief
Switch Name           : switch
Switch Type            :
Kickstart Image       : 4.0(0) bootflash:///nuova-or-kickstart-nsg.4.0.0.001.bin
System Image         : 4.0(0) bootflash:/nuova-or-system-nsg.4.0.0.001.binnms-or-47
IP Address/Mask     : 172.16.24.47/24
Switch WWN           : 20:00:00:0d:ec:6b:cd:c0
No of VSANs           : 1
Configured VSANs   : 1
VSAN    1:    name:VSAN0001, state:active, interop mode:default
              domain id:0xa6(166), WWN:20:01:00:0d:ec:6b:cd:c1 [Principal]
              active-zone:<NONE>, default-zone:deny
--------------------------------------------------------------------------------
Interface  Vsan   Admin  Admin   Status          SFP    Oper  Oper   Port
                  Mode   Trunk                         Mode  Speed  Channel
                         Mode                                (Gbps)
--------------------------------------------------------------------------------
fc3/1      1      auto   on      down            swl    --           --
fc3/2      1      auto   on      sfpAbsent       --     --           --
fc3/3      1      auto   on      down            swl    --           --
fc3/4      1      auto   on      sfpAbsent       --     --           --
fc3/5      1      auto   on      down            swl    --           --
fc3/6      1      auto   on      sfpAbsent       --     --           --
fc3/7      1      auto   on      down            swl    --           --
fc3/8      1      auto   on      down            swl    --           --
--------------------------------------------------------------------------------
Interface               Status     IP Address        Speed    MTU   Port
                                                                   Channel
--------------------------------------------------------------------------------
Ethernet1/1             sfpIsAbsen --                --       1500  --
Ethernet1/2             sfpIsAbsen --                --       1500  --
Ethernet1/3             up         --                10000    1500  --
Ethernet1/4             sfpIsAbsen --                --       1500  --
Ethernet1/5             sfpIsAbsen --                --       1500  --
Ethernet1/6             sfpIsAbsen --                --       1500  --
Ethernet1/7             sfpIsAbsen --                --       1500  --
Ethernet1/8             sfpIsAbsen --                --       1500  --
Ethernet1/9             sfpIsAbsen --                --       1500  --
Ethernet1/10            sfpIsAbsen --                --       1500  --
Ethernet1/11            sfpIsAbsen --                --       1500  --
Ethernet1/12            sfpIsAbsen --                --       1500  --
Ethernet1/13            sfpIsAbsen --                --       1500  --
Ethernet1/14            sfpIsAbsen --                --       1500  --
Ethernet1/15            notConnect --                --       1500  --
Ethernet1/16            sfpIsAbsen --                --       1500  --
Ethernet1/17            sfpIsAbsen --                --       1500  --
Ethernet1/18            sfpIsAbsen --                --       1500  --
Ethernet1/19            notConnect --                --       1500  --
Ethernet1/20            sfpIsAbsen --                --       1500  --
Ethernet1/21            sfpIsAbsen --                --       1500  --
Ethernet1/22            sfpIsAbsen --                --       1500  --
Ethernet1/23            sfpIsAbsen --                --       1500  --
Ethernet1/24            sfpIsAbsen --                --       1500  --
Ethernet1/25            sfpIsAbsen --                --       1500  --
Ethernet1/26            sfpIsAbsen --                --       1500  --
Ethernet1/27            sfpIsAbsen --                --       1500  --
Ethernet1/28            sfpIsAbsen --                --       1500  --
Ethernet1/29            sfpIsAbsen --                --       1500  --
Ethernet1/30            sfpIsAbsen --                --       1500  --
Ethernet1/31            sfpIsAbsen --                --       1500  --
Ethernet1/32            sfpIsAbsen --                --       1500  --
Ethernet1/33            sfpIsAbsen --                --       1500  --
Ethernet1/34            sfpIsAbsen --                --       1500  --
Ethernet1/35            up         --                10000    1500  --
Ethernet1/36            sfpIsAbsen --                --       1500  --
Ethernet1/37            sfpIsAbsen --                --       1500  --
Ethernet1/38            sfpIsAbsen --                --       1500  --
Ethernet1/39            sfpIsAbsen --                --       1500  --
Ethernet1/40            sfpIsAbsen --                --       1500  --
--------------------------------------------------------------------------------
Interface               Status     IP Address        Speed    MTU
```

```
--------------------------------------------------------------------------------
mgmt0                  up         172.16.24.47      100      1500
```

show tech-support fc Command

Use the **show tech-support fc** command to obtain information about the FC configuration on your switch.

The output of the **show tech-support fc** command includes the output of the following commands:

- **show interface brief**
- **show interface**
- **show port internal info all**
- **show port internal event-history lock**
- **show port internal event-history msgs**
- **show port internal event-history errors**
- **show port internal mem-stats detail**
- **show san-port-channel internal event-history all**
- **show san-port-channel internal event-history errors**
- **show san-port-channel internal event-history msgs**
- **show san-port-channel internal event-history lock**
- **show san-port-channel internal mem-stats detail**
- **show san-port-channel usage**
- **show san-port-channel summary**
- **show san-port-channel consistency detail**
- **show tech-support device-alias**
- **show fcdomain domain-list**
- **show tech-support fcns**
- **show fcns database vsan 1-4093**
- **show fcns database detail vsan 1-4093**
- **show fcns database local vsan 1-4093**
- **show fcns database local detail vsan 1-4093**
- **show fcns statistics vsan 1-4093**
- **show fcns statistics detail vsan 1-4093**
- **show fcns internal info vsan 1-4093**
- **show fcns internal event-history**
- **show fcns internal event-log**
- **show fcroute unicast**

- **show fcs database**
- **show fcs ie**
- **show fctimer**
- **show flogi database**
- **show flogi internal info**
- **show fspf**
- **show fspf database**
- **show tech-support rscn**
- **show rscn internal vsan 1-4093**
- **show rscn internal event-history**
- **show rscn internal mem-stats detail**
- **show rscn internal session-history vsan 1-4093**
- **show rscn internal merge-history vsan 1-4093**
- **show rscn statistics vsan 1-4093**
- **show rscn scr-table vsan 1-4093**
- **show rscn session status vsan 1-4093**
- **show vsan**
- **show vsan membership**
- **show tech-support zone**
- **show zone status vsan 1-4093**
- **show zoneset active vsan 1-4093**
- **show zoneset vsan 1-4093**
- **show zone vsan 1-4093**
- **show fcalias vsan 1-4093**
- **show zone-attribute-group vsan 1-4093**
- **show zone policy vsan 1-4093**
- **show zoneset pending active vsan 1-4093**
- **show zoneset pending vsan 1-4093**
- **show zone pending vsan 1-4093**
- **show zone pending active vsan 1-4093**
- **show fcalias pending vsan 1-4093**
- **show zone policy pending vsan 1-4093**
- **show zone pending-diff vsan 1-4093**

- **show zone analysis active vsan 1-4093**
- **show zone analysis vsan 1-4093**
- **show zone ess vsan 1-4093**
- **show zone internal vsan 1-4093**
- **show zone internal change event-history vsan 1-4093**
- **show zone internal ifindex-table vsan 1-4093**
- **show zone internal merge event-history vsan 1-4093**
- **show zone internal event-history**
- **show zone internal event-history errors**
- **show zone internal tcam event-history vsan 1-4093**
- **show zone statistics vsan 1-4093**
- **show system default zone**
- **show zone internal ddas-table**
- **show zone internal sdv-table vsan 1-4093**
- **show zone internal mem-stats**
- **show zone internal mem-stats detail**
- **show zone internal transit-table received vsan 1-4093**
- **show zone internal transit-table forwarded vsan 1-4093**
- **show zone internal transit-table rejected vsan 1-4093**

You can save the output of this command to a file by appending > (left arrow) and the filename to the **show tech-support zone** command.

show tech-support platform Command

Use the **show tech-support platform** command to obtain information about the platform configuration of your switch.

The output of the **show tech-support platform** command includes the output of the following commands:

- **show platform fwm mem-stats detail**
- **show platform fwm info global**
- **show platform fwm info pif all verbose**
- **show platform fwm info lif all verbose**
- **show platform fwm info vlan all verbose**
- **show platform fwm info error stats**
- **show platform fwm info error history**
- **show platform fwm info stm-stats**

- **show platform fwm info pc all verbose**
- **show platform fwm info ppf**
- **show platform fwm info pss all**
- **show platform hardware fwm info vlan all**
- **show platform hardware fwm info pif all**
- **show platform hardware fwm info lif all**
- **show platform hardware fwm info global**
- **show platform software zschk internal info**
- **show platform software zschk internal msgs**
- **show platform software statsclient msgs**
- **show hardware internal gatos detail**
- **show hardware internal gatos all-ports detail**
- **show hardware internal altos detail**
- **show hardware internal altos event-history errors**
- **show hardware internal altos event-history messages**
- **show platform fcfib fcflow**
- **show platform fcfib event-history all**
- **show platform fcfib unicasts**
- **show platform fcfib unicasts forwarding-configuration**
- **show platform fcfib vsan**
- **show platform fcfib san-port-channel**
- **show platform software fcfib devices**
- **show platform software fcfib multipath**
- **show platform software fcfib vsanidxtable**
- **show platform software fcfib domainidxtable**
- **show platform hardware fcfib pathselecttable**
- **show platform hardware fcfib pathselecttable all**
- **show platform software fcfib fctable-check**
- **show fc2 internal event-history errors**
- **show system internal liod liod_db**
- **show system internal liod queues**
- **show system internal liod state**
- **show system internal liod time_db**

- **show system internal rib domain**
- **show system internal rib system-attributes**
- **show system internal rib unicast**
- **show system internal rib vsan-attributes**
- **show system internal fcfwd fwidxmap if_index**
- **show system internal fcfwd idxmap interface-to-port**
- **show system internal fcfwd pcmap**
- **show platform afm info global**
- **show platform afm info attachment brief**
- **show platform afm info group-cfg all**
- **show platform afm info lop all**
- **show platform software altos detail**
- **show platform software altos event-history errors**
- **show platform software altos event-history msgs**
- **show platform software altos ports all**
- **show platform hardware altos counters all**
- **show platform hardware altos counters interrupts all**
- **show platform hardware altos interrupts all detail**

Default Settings for Troubleshooting Features

The following table lists the default settings for the features included in this chapter.

Table 1: Default Settings for Troubleshooting Features

Parameters	Default
Timeout period to invoke fctrace	5 seconds
Number of frame sent by the fcping feature	5 frames
Remote capture connection protocol	TCP
Remote capture connection mode	Passive
Local capture frame limits	10 frames
FC ID allocation mode	Auto mode