Send feedback to nexus4K-docfeedback@cisco.com

CHAPTER 35

Troubleshooting

This chapter describes basic troubleshooting methods used to resolve issues with the Cisco Nexus 4001I and 4005I Switch Module for IBM BladeCenter. This chapter includes the following sections:

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

This section includes the following topics:

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, perform the following steps:

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

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

Send feedback to nexus4K-docfeedback@cisco.com

```
user:USERID
        this user account has no expiry date
        roles:network-operator
```

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

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

Step 3 Save the configuration:

```
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, perform the following steps:

Step 1 Establish a terminal session on the console port.

Step 2 Power cycle the switch.

Step 3 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:

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

Step 4 Reset the network administrator password:

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

Step 5 Display the bootflash: contents to locate the Cisco NX-OS software image file:

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

Step 6 Load the Cisco NX-OS system software image.

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

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

Send feedback to nexus4K-docfeedback@cisco.com

Step 7 Log in to the switch using the new administrator password:

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

Step 8 Reset the new password to ensure that is it is also the SNMP password:

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

Step 9 Save the configuration:

```
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, perform one or more of the following tasks:

Command	Purpose
`switch# ethanalyzer local interface`	Captures packets sent or received and provides detailed protocol information.
`switch# ethanalyzer local interface inband`	Captures packets sent or received and provides detailed protocol information in the inband and outband interfaces.
`switch# ethanalyzer local interface mgmt`	Captures packets sent or received and provides detailed protocol information in the management interfaces.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} brief`	Captures packets sent or received and provides a summary of protocol information.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} limit-captured-frames`	Limits the number of frames to capture.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} limit-frame-size`	Limits the length of the frame to capture.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} capture-filter`	Filters the types of packets to capture.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} display-filter`	Filters the types of captured packets to display.
`switch# ethanalyzer local interface {inband | mgmt | mgmt-backplane} decode-internal`	Decodes the internal frame header for Cisco NX-OS. **Note** Do not use this option if you plan to analyze the data using the Wireshark instead of Ethanalyzer.

Send feedback to nexus4K-docfeedback@cisco.com

Command	Purpose
switch# **ethanalyzer local interface** {**inband** | **mgmt** | **mgmt-backplane**} **write**	Saves the captured data to a file.
switch# **ethanalyzer local read**	Opens the 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

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

```
switch# ethanalyzer local interface mgmt brief limit-captured-frames 4
Capturing on eth2
2009-05-19 11:07:06.633801 00:05:ad:00:33:37 -> ff:ff:ff:ff:ff:ff ARP Who has
172.29.231.1?  Tell 172.29.231.177
2009-05-19 11:07:06.813956 172.29.230.3 -> 224.0.0.2    HSRP Hello (state Standby)
2009-05-19 11:07:06.829894 172.29.230.3 -> 224.0.0.2    HSRP Hello (state Standby)
2009-05-19 11:07:06.980957 172.29.230.2 -> 224.0.0.5    OSPF Hello Packet
4 packets captured
```

The following example shows captured data (limited to 2 packets) on the inband interface:

```
switch# ethanalyzer local interface inband brief limit-captured-frames 2
Capturing on inb0
2009-05-19 11:08:42.911357 00:05:ad:00:34:73 -> 01:80:c2:00:00:00 STP RST. Root =
32769/00:05:ad:00:34:71  Cost = 0  Port = 0x8093
2009-05-19 11:08:42.911390 00:05:ad:00:34:73 -> 01:80:c2:00:00:00 STP RST. Root =
32769/00:05:ad:00:34:71  Cost = 0  Port = 0x8093
2 packets captured
```

The following 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 eth2
Frame 1 (74 bytes on wire, 74 bytes captured)
    Arrival Time: May 19, 2009 11:07:52.061847000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 74 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:tcp]
Ethernet II, Src: 00:1a:30:00:bc:00 (00:1a:30:00:bc:00), Dst: 00:05:ad:00:34:5a
(00:05:ad:00:34:5a)
    Destination: 00:05:ad:00:34:5a (00:05:ad:00:34:5a)
        Address: 00:05:ad:00:34:5a (00:05:ad:00:34:5a)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:1a:30:00:bc:00 (00:1a:30:00:bc:00)
        Address: 00:1a:30:00:bc:00 (00:1a:30:00:bc:00)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
```

Send feedback to nexus4K-docfeedback@cisco.com

```
    Type: IP (0x0800)
Internet Protocol, Src: 171.69.27.169 (171.69.27.169), Dst: 172.29.231.226
(172.29.231.226)
    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: 60
    Identification: 0x6c57 (27735)
    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: 56
    Protocol: TCP (0x06)
    Header checksum: 0x7b76 [correct]
        [Good: True]
        [Bad : False]
    Source: 171.69.27.169 (171.69.27.169)
    Destination: 172.29.231.226 (172.29.231.226)
Transmission Control Protocol, Src Port: 51225 (51225), Dst Port: telnet (23), Seq: 0,
Len: 0
    Source port: 51225 (51225)
    Destination port: telnet (23)
    Sequence number: 0    (relative sequence number)
    Header length: 40 bytes
    Flags: 0x02 (SYN)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...0 .... = Acknowledgment: Not set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..1. = Syn: Set
        .... ...0 = Fin: Not set
    Window size: 5840
    Checksum: 0xbe6e [correct]
        [Good Checksum: True]
        [Bad Checksum: False]
    Options: (20 bytes)
        Maximum segment size: 1460 bytes
        SACK permitted
        Timestamps: TSval 3876668892, TSecr 0
        NOP
        Window scale: 4 (multiply by 16)

1 packet captured
```

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

show tech-support Command

This section describes the **show tech-support** commands and includes the following topics:

Send feedback to nexus4K-docfeedback@cisco.com

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 Cisco TAC 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.

Tip 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 snmp**
- **show interface brief**
- **show interface**
- **show running-config**
- **show startup-config**

Send feedback to nexus4K-docfeedback@cisco.com

- 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 logging onboard obfl-logs

Send feedback to nexus4K-docfeedback@cisco.com

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.

Tip 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.

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

```
switch# show tech-support brief
Switch Name           : switch
Switch Type           : DS-C9134-K9-SUP
Kickstart Image       : 4.1(2)E1(1) bootflash:///n4000_kickstart.4.1.2.E1.0.175.gbin
System Image          : 4.1(2)E1(1) bootflash:///n4000_system.4.1.2.E1.0.189.bin
IP Address/Mask       : 209.165.200.225/254
Switch WWN            : parsing


--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth1/1        1      eth  access up      none                       10G(D) --
Eth1/2        1      eth  access up      none                       10G(D) --
Eth1/3        1      eth  trunk  up      none                       10G(D) --
Eth1/4        1      eth  access up      none                       10G(D) --
Eth1/5        1      eth  access up      none                       10G(D) --
Eth1/6        1      eth  access up      none                       10G(D) --
Eth1/7        1      eth  access up      none                       10G(D) --
Eth1/8        1      eth  access up      none                       10G(D) --
Eth1/9        1      eth  access up      none                       10G(D) --
Eth1/10       1      eth  access up      none                       10G(D) --
Eth1/11       1      eth  access up      none                       10G(D) --
Eth1/12       1      eth  access up      none                       10G(D) --
Eth1/13       1      eth  access up      none                       10G(D) --
Eth1/14       1      eth  access up      none                       10G(D) --
Eth1/15       1      eth  access down    SFP not inserted           10G(D) --
Eth1/16       1      eth  access down    SFP not inserted           10G(D) --
Eth1/17       1      eth  access down    SFP not inserted           10G(D) --
Eth1/18       1      eth  access down    SFP not inserted           10G(D) --
Eth1/19       1      eth  access down    SFP not inserted           10G(D) --
Eth1/20       monitr eth  access down    SFP not inserted           10G(D) --

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                              Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     209.165.200.225                          1000     1500
mgmt1  --           up     --                                       100      1500
switch#
```

Send feedback to nexus4K-docfeedback@cisco.com

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 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 fwm info pif all**
- **show platform fwm info lif all**
- **show platform fwm info global**
- **show hardware internal cpu-mac mgmt counters**
- **show hardware internal cpu-mac mgmt stats**
- **show hardware internal cpu-mac inband counters**
- **show platform software pfm internal errors**
- **show platform software pfm internal msgs**
- **show platform software pfm internal info**
- **show environment**
- **show sprom all**
- **show module**
- **show hardware internal pci**
- **show system health internal errors**
- **show system health internal messages**
- **show system health internal plog**
- **show chassis summary**

show tech-support platform callhome Command

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

Send feedback to nexus4K-docfeedback@cisco.com

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

- **show hardware internal cpu-mac inband counters**
- **show hardware internal cpu-mac mgmt counters**
- **show hardware internal cpu-mac mgmt stats**
- **show hardware internal xcvr event-history errors**
- **show hardware internal xcvr event-history msgs**
- **show platform software pfm internal errors**
- **show platform software pfm internal msgs**
- **show platform software pfm internal info**
- **show system health internal errors**
- **show system health internal messages**
- **show system health internal plog**
- **show environment**
- **show sprom all**
- **show module**
- **show hardware internal pci**