CHAPTER 10

Management Tools for Usability

This chapter describes Cisco NX-OS software features that are recommended for managing a device. The topics covered include changing the configuration, verifying the supervisor module status, or replacing hardware.

This chapter includes the following sections:

Implementing Configuration Changes

This section includes recommended procedural best practices when modifying the Cisco NX-OS configuration.

Configuration Rollback

Introduced: Cisco NX-OS Release 4.0(1)

The configuration rollback feature allows an administrator to create configuration checkpoints that allow for a configuration to be easily rolled back in the event the new configuration changes don't operate as expected. We recommend that you use the configuration rollback feature to create a configuration checkpoint prior to making changes in a production network during change-control procedures. This allows the original configuration to be re-applied with one command if there are any unforeseen issues. Beginning in Cisco NX-OS Release 4.2(1) auto-checkpoints are created if a feature is disabled (manually or by license expiration). VDC removal due to license expiration will not generate an auto-checkpoint. Beginning in Cisco NX-OS Release 4.2(1) checkpoints are saved to the standby supervisor as long as they are not created using the **checkpoint file** command. The following example demonstrates the procedure for basic checkpoint and rollback operation.

```
n7000# checkpoint ospf-change-control
.....Done
```

```
n7000(config)# interface ethernet x/x
n7000(config-if)# ip address x.x.x.x/xx
n7000(config-if)# ip router ospf 10 area 0
n7000(config-if)# no shutdown

n7000# show run interface ethernet x/x

interface Ethernetx/x
  ip address x.x.x.x/xx
  ip router ospf 10 area 0.0.0.0
  no shutdown

n7000# rollback running-config checkpoint ospf-change-control
Note: Applying config parallelly may fail Rollback verification
Collecting Running-Config
Generating Rollback Patch
Executing Rollback Patch
Generating Running-config for verification
Generating Patch for verification

n7000# show run interface ethernet x/x
```

Session Manager

Introduced: Cisco NX-OS Release 4.0(1)

Session Manger allows ACL and QoS configurations to be applied to the running-configuration in batch mode. This is useful for verifying hardware resources such as TCAM space is available before applying the configuration. The Session Manager should always be used when applying ACLs or configuring QoS. The following example illustrates the process for configuring, verifying and applying an ACL to an interface.

```
n7000# configure session apply-acl
Config Session started, Session ID is 1
Enter configuration commands, one per line.  End with CNTL/Z.
n7000(config-s)# ip access-list inbound-acl
n7000(config-s-acl)# deny ip 10.0.0.0/8 any
n7000(config-s-acl)# deny ip 172.16.0.0/12 any
n7000(config-s-acl)# deny ip 192.168.0.0/16 any
n7000(config-s-acl)# interface ethernet x/x
n7000(config-s-if)# ip access-group inbound-acl in
n7000(config-s-if)# verify
Verification Successful
n7000(config-s)# commit
Commit Successful
```

Supervisor Redundancy

To ensure high availability, we recommend that you have two supervisor modules installed per chassis. This section contains information for verifying the status of a redundant supervisor modules and performing a manual supervisor switchover if necessary.

Verifying Supervisor Status

Introduced: Cisco NX-OS Release 4.0(1)

When two supervisor modules are present, one supervisor module should be in an “Active with HA standby”state, and other supervisor module should be in an “HA Standby” state during normal operation of the switch.

```
n7000# show system redundancy status

Redundancy mode
---------------
      administrative:    HA
         operational:    HA

This supervisor (sup-1)
-----------------------
    Redundancy state:    Active
    Supervisor state:    Active
    Internal state:      Active with HA standby

Other supervisor (sup-2)
------------------------
    Redundancy state:    Standby
    Supervisor state:    HA standby
```

Manual Switchover

Introduced: Cisco NX-OS Release 4.0(1)

This section was included for reference and may not be required.

A supervisor switchover can be manually initiated in a chassis with two supervisor modules present. Once the switchover is performed, the previous active supervisor reloads and come back online as the standby supervisor. You cannot manually perform a switchover if the Standby supervisor is not in an “HA standby” state.

```
n7000# system switchover
```

Locator LED

Introduced: Cisco NX-OS Release 4.0(1)

Cisco NX-OS software supports a Locator LED feature that is useful when physically identifying hardware components (chassis, fans, fabrics, modules, power-supplies) and ports on Ethernet I/O modules. The Locator LED feature should be used when working with remote-hands support teams that are responsible for performing physical tasks such as replacing hardware or working with Ethernet ports (adds, moves, etc.). Use the **no locator-led** command to disable the locator LED for a chassis component or interface.

```
n7000# locator-led chassis
n7000# locator-led fan 1
n7000# locator-led module 1
n7000# locator-led powersupply 1
n7000# locator-led xbar 1

n7000(config)# interface ethernet 1/1
n7000(config-if)# beacon
```

```
n7000# show locator-led status
Component        Locator LED Status
-------------------------------------
Chassis          ON
Module  1        ON
Module  2        off
Module  5        off
Xbar  1          ON
Xbar  2          off
Xbar  3          off
PowerSupply  1   ON
PowerSupply  2   off
PowerSupply  3   off
Fan  1           ON
Fan  2           off
Fan  3           off
```

Note The Cisco NX-OS CLI syntax changed in Cisco NX-OS Release 4.1(2). The **locator-led** command replaced the deprecated **blink** command. Ethernet ports on an I/O module do not display their status in the output of the **show locator-led status** command. Use the **show interface** command or view the running-configuration to determine if a port Locator LED (Beacon) is enabled or disabled.

Ethanalyzer

Introduced: Cisco NX-OS Release 4.0(1)

The Ethernet Analyzer should be used when troubleshooting control plane protocols and high CPU utilization. Ethernet Analyzer allows the administrator to capture packets sent to and from the supervisor module CPU. Brief or detailed information per packet can be captured and viewed using the CLI or exported to a protocol analyzer such as Wireshark. When troubleshooting, a brief capture should be performed to identify the interesting packets, and a detailed capture should be performed to dissect the interesting packets in more detail. Captures can be redirected to files and stored locally using the **write** or **>** option. Ethanalyzer will capture 10 frames by default. The **limit-captured-frames <0-2147483647>** option can be used to increase the frame count. A value of **0** means there is no limit and a 10MB circular buffer is created.

Brief Capture:

```
n7000# ethanalyzer local interface inband
Capturing on inband
2010-06-02 20:44:40.327808 192.168.20.1 -> 224.0.0.5    OSPF Hello Packet
2010-06-02 20:44:41.480658 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730633 192.168.20.2 -> 207.68.169.104 DNS Standard query A
print.cisco.com
2010-06-02 20:44:41.730638 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com
2010-06-02 20:44:42.480586 192.168.20.2 -> 65.54.238.85 DNS Standard query A
print.cisco.com

<Text Omitted>
```

Detailed Capture:

```
n7000# ethanalyzer local interface inband limit-captured-frames 100 detail
Capturing on inband
Capturing on inband
```

```
Frame 1 (60 bytes on wire, 60 bytes captured)
    Arrival Time: Oct  2, 2010 22:07:57.150394000
    [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: 60 bytes
    Capture Length: 60 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:llc:stp]
IEEE 802.3 Ethernet
    Destination: 01:80:c2:00:00:00 (01:80:c2:00:00:00)
        Address: 01:80:c2:00:00:00 (01:80:c2:00:00:00)

<Text Omitted>
```

Writing a Brief Capture to a File:

```
n7000# ethanalyzer local interface inband write bootflash:cpu.
```

Reading a Capture File:

```
n7000# ethanalyzer local read bootflash:cpu.txt
```

Redirecting a Detailed Capture to a File:

```
n7000# ethanalyzer local interface detail > cpu-1.txt
```

Reading a Capture File:

```
n7000# show file bootflash:cpu-1.txt
```

Note The **inband** option captures packets on the I/O modules, and the **mgmt** option captures packets on the supervisor module mgmt0 port.

Note The CLI syntax has changed slightly from Cisco NX-OS Release 4.x to Release 5.x. This CLI output is captured from NX-OS Release 5.1(1).

Switched Port Analyzer

Introduced: Cisco NX-OS Release 4.0(1)

Switched Port Analyzer (SPAN) can be used to mirror traffic from a source to a destination when troubleshooting or for providing data for network services such as Intrusion Prevention Systems (IPS). While this document does not cover SPAN in detail, We recommend that you disable local and ERSPAN sessions with the **shut** command if they are not required to be active after troubleshooting. This preserves hardware resources by preventing unnecessary traffic from being flooded across the fabric. The ERSPAN feature was introduced in Cisco NX-OS Release 5.1(1).

Local SPAN:

```
n7000(config)# monitor session 1
n7000(config-monitor)# shut
```

Encapsulated Remote (ERSPAN):

```
n7000(config)# monitor session 1 type erspan-source
n7000(config-erspan-src)# shut
```

```
n7000(config)# monitor session 1 type erspan-destination
n7000(config-erspan-dst)# shut
```

Performing a Debug

This section contains the Cisco NX-OS recommended best practices for performing a debug. Always use caution when executing a debug command since network performance can be impacted.

Redirecting Output to a File

Introduced: Cisco NX-OS Release 4.0(1)

By default, debug output is logged to the console and monitor sessions (SSH/Telnet), which can impact network performance. When performing a debug, the output should be redirected to a file as opposed to the console or a terminal session to reduce processing overhead on the supervisor module CPU. In the following example, the debug output is redirected to a file for analysis. The redirected debug output is saved in the log: directory. Once the debug output is redirected to a file, the output can be viewed and/or copied to a remote destination. The pipe option can be used to parse the log file. The **show debug** command displays the current debug status and the **no debug all** command will disable all debugging.

Note Do not leave an unintended debug running that is not required.

```
n7000# debug logfile cdp-debug
n7000# debug cdp all
n7000# no debug cdp all

n7000# dir log:cdp-debug
      14560    Nov 01 22:05:18 2010  cdp-debug

n7000# show debug logfile cdp-debug
2010 Nov  1 22:02:02.948577 cdp: Going to send CDP version 2 pkt on Ethernet7/3
2010 Nov  1 22:02:02.948662 cdp: Sent CDP packet untagged on interface 0x1a30200
0
2010 Nov  1 22:02:02.948696 cdp: Going to send CDP version 2 pkt on Ethernet10/1
8

<Text Omitted>

n7000# show debug logfile cdp-debug | include Ethernet10/1
```