Tools Used in Troubleshooting

This chapter describes the troubleshooting tools available for the Cisco Nexus 1000V.

Commands

You use the CLI from a local console or remotely using a Telnet or Secure Shell (SSH) session. The command-line interface (CLI) provides a command structure similar to the Cisco NX-OS software, with context-sensitive help, **show** commands, multi-user support, and role-based access control.

Each feature has **show** commands that provide information about the feature configuration, status, and performance. Additionally, you can use the following commands for more information:

- **show system—Provides information on system-level components, including cores, errors, and exceptions. Use the show system error-id command to find details on error codes:**

```
n1000v# copy running-config startup-config
[########################################] 100%
2008 Jan 16 09:59:29 zoom %$ VDC-1 %$ %BOOTVAR-2-AUTOCOPY_FAILED: Autocopy of file
/bootflash/n1000-s1-dk9.4.0.0.837.bin.S8 to standby failed, error=0x401e0008

n1000v# show system error-id 0x401e0008
Error Facility: sysmgr
Error Description: request was aborted, standby disk may be full
```

Ping

The ping utility generates a series of *echo* packets to a destination across a TCP/IP internetwork. When the echo packets arrive at the destination, they are rerouted and sent back to the source. Using ping, you can verify connectivity and latency to a particular destination across an IP routed network.

The ping utility allows you to ping a port or end device. By specifying the IPv4 address, you can send a series of frames to a target destination. Once these frames reach the target, they are looped back to the source and a time stamp is taken. Ping helps you to verify the connectivity and latency to the destination.

Traceroute

Use traceroute to do the following:

- Trace the route followed by the data traffic.

- Compute inter-switch (hop-to-hop) latency.

Traceroute identifies the path taken on a hop-by-hop basis and includes a time stamp at each hop in both directions. You can use traceroute to test the connectivity of ports along the path between the generating switch and the switch closest to the destination.

Enter the **traceroute** command to access this feature.

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

Monitoring Processes and CPUs

The CLI has features that enable you to monitor switch processes and CPU status and utilization.

Identifying the Processes Running and Their States

Use the **show processes command** to identify the processes that are running and the status of each process. (See Example 2-1.) The command output includes the following:

- PID—Process ID.
- State—Process state.
- PC—Current program counter in hex format.
- Start_cnt—How many times a process has been started (or restarted).
- TTY—Terminal that controls the process. A “-” (hyphen) usually means a daemon that is not running on any particular TTY.
- Process—Name of the process.

Process states are as follows:

- D—Uninterruptible sleep (usually I/O).
- R—Runnable (on run queue).
- S—Sleeping.
- T—Traced or stopped.
- Z—Defunct (zombie) process.
- NR—Not-running.
- ER—Should be running but currently not-running.

Note The ER state typically designates a process that has been restarted too many times, which causes the system to classify it as faulty and disable it.

Example 2-1 show processes Command

```
n1000v# show processes

PID    State  PC        Start_cnt    TTY   Process
-----  -----  --------  -----------  ----  -------------
    1      S  41520eb8            1     -  init
    2      S         0            1     -  kthreadd
```

```
  3      S         0             1      -  migration/0
  4      S         0             1      -  ksoftirqd/0
  5      S         0             1      -  watchdog/0
  6      S         0             1      -  migration/1
  7      S         0             1      -  ksoftirqd/1
  8      S         0             1      -  watchdog/1
  9      S         0             1      -  events/0
 10      S         0             1      -  events/1
 11      S         0             1      -  khelper
 12      S         0             1      -  kblockd/0
 13      S         0             1      -  kblockd/1
 14      S         0             1      -  kacpid
 15      S         0             1      -  kacpi_notify
 16      S         0             1      -  kseriod
 17      S         0             1      -  ata/0
 18      S         0             1      -  ata/1
 19      S         0             1      -  ata_aux
 20      S         0             1      -  ksuspend_usbd
 21      S         0             1      -  khubd
 22      S         0             1      -  pdflush
 23      S         0             1      -  pdflush
 24      S         0             1      -  kswapd0
 25      S         0             1      -  aio/0
 26      S         0             1      -  aio/1
 27      S         0             1      -  nfsiod
 28      S         0             1      -  rpciod/0
 29      S         0             1      -  rpciod/1
 30      S         0             1      -  kirqd
359      S         0             1      -  kjournald
364      S         0             1      -  kjournald
954      S         0             1      -  kjournald
961      S         0             1      -  kjournald
1263     S  4151e5b6             1      -  portmap
1272     S  41520eb8             1      -  rpc.statd
1287     S         0             1      -  lockd
1288     S         0             1      -  nfsd
1289     S         0             1      -  nfsd
1290     S         0             1      -  nfsd
1291     S         0             1      -  nfsd
1292     S         0             1      -  nfsd
1293     S         0             1      -  nfsd
1294     S         0             1      -  nfsd
1295     S         0             1      -  nfsd
1300     S  41520eb8             1      -  rpc.mountd
1323     S  41520eb8             1      -  sysmgr
1675     S  41528053             1      -  httpd
1846     S         0             1      -  mping-thread
1847     S         0             1      -  mping-thread
1875     S         0             1      -  stun_kthread
1876     S         0             1      -  stun_arp_mts_kt
1877     S         0             1      -  stun_packets_re
1878     S         0             1      -  stun_send_packe
1933     S         0             1      -  redun_kthread
1934     S         0             1      -  redun_timer_kth
2269     S         0             1      -  sf_rdn_kthread
2286     S  41520eb8             1      -  xinetd
2287     S  41520eb8             1      -  tftpd
2288     R  4151e5ed             1      -  syslogd
2289     S  41520eb8             1      -  sdwrapd
2290     S  41520eb8             1      -  platform
2299     S         0             1      -  ls-notify-mts-t
2317     S  41520494             1      -  pfm_dummy
2319     S  41520494             1      -  vshd
2320     S  41520eb8             1      -  stun
```

```
2321      S  415c4642           1      -  smm
2322      S  41520eb8           1      -  redun_mgr
2323      S  41520eb8           1      -  psshelper
2324      S  41520eb8           1      -  lmgrd
2325      S  41520494           1      -  licmgr
2326      S  41520eb8           1      -  fs-daemon
2327      S  41520eb8           1      -  feature-mgr
2328      S  41520eb8           1      -  confcheck
2329      S  41520eb8           1      -  cdm
2330      S  41520eb8           1      -  capability
2331      S  41520eb8           1      -  psshelper_gsvc
2350      S  41520eb8           1      -  cisco
2351      S  41523f92           1      -  clis
2353      S  41520eb8           1      -  vem_mgr
2354      S  41523f92           1      -  port-profile
2357      S  41520eb8           1      -  xmlma
2358      S  41520ee7           1      -  vnm_pa_intf
2359      S  41520eb8           1      -  vmm
2360      S  41520eb8           1      -  vdc_mgr
2361      S  41520eb8           1      -  ttyd
2362      R  414f2c20           1      -  sysinfo
2363      S  41520eb8           1      -  sksd
2365      S  415277b3           1      -  res_mgr
2366      S  41520ee7           1      -  plugin
2367      S  415c4642           1      -  npacl
2368      S  41520eb8           1      -  mvsh
2369      S  41520eb8           1      -  mping_server
2370      S  41520eb8           1      -  module
2371      S  41523f92           1      -  fwm
2372      S  41520eb8           1      -  evms
2373      S  41520eb8           1      -  evmc
2374      S  41520eb8           1      -  core-dmon
2375      S  41520eb8           1      -  bootvar
2376      S  41520494           1      -  ascii-cfg
2377      S  41520494           1      -  securityd
2378      S  41523f92           1      -  cert_enroll
2379      S  41520eb8           1      -  aaa
2389      S  415c4642           1      -  l3vm
2390      S  415c4642           1      -  urib
2393      S  41520eb8           1      -  ExceptionLog
2394      S  41520eb8           1      -  ifmgr
2396      S  41520eb8           1      -  tcap
2415      S  41523f92           1      -  snmpd
2432      S  415c4642           1      -  adjmgr
2436      S  415c4642           1      -  u6rib
2461      S  41487a55           1      -  PMon
2467      S  41520eb8           1      -  aclmgr
2475      S  415c4642           1      -  arp
2476      S  414886c1           1      -  icmpv6
2480      S  415c4642           1      -  netstack
2552      S  b7f8757e           1      -  klogd
2571      S  41523f92           1      -  radius
2572      S  41520494           1      -  ip_dummy
2574      S  41520494           1      -  ipv6_dummy
2576      S  41523f92           1      -  ntp
2577      S  41520494           1      -  pktmgr_dummy
2578      S  41520494           1      -  tcpudp_dummy
2579      S  41523f92           1      -  dcos-xinetd
2581      S  41523f92           1      -  ntpd
2582      S  41523f92           1      -  cdp
2754      S  41523f92           1      -  ufdm
2755      S  41523f92           1      -  stp
2756      S  41523f92           1      -  seg_bd
2757      S  41523f92           1      -  sal
```

```
 2758      S  415c4642           1      -  rpm
 2759      S  41523f92           1      -  pltfm_config
 2760      S  41523f92           1      -  monitor
 2761      S  41520eb8           1      -  m2rib
 2762      S  41520eb8           1      -  ipqosmgr
 2763      S  415c4642           1      -  igmp
 2764      S  41523f92           1      -  eth_port_channel
 2765      S  41523f92           1      -  eth-port-sec
 2766      S  41520eb8           1      -  acllog
 2776      S  41520eb8           1      -  lacp
 2778      S  41523f92           1      -  vlan_mgr
 2798      S  41523f92           1      -  ethpm
 2844      S  41520eb8           1      -  msp
 2847      S  41523f92           1      -  vms
 2866      S  41523f92           1      -  vns_agent
 2867      S  41520eb8           1      -  vim
 2868      S  41523f92           1      -  nsmgr
 2869      S  41523f92           1      -  nfm
 2870      S  41523f92           1      -  httpmgr
 2871      S  41520eb8           1      -  cloud_agent
 2872      S  41520eb8           1      -  aclcomp
 2888      S  414f265e           1      -  ExtensibleApiEngine
 2890      S  414f265e           1      -  monitor_eae.sh
 2893      S  41520ee7           1      -  lua
 2903      S  414f265e           1      -  launch_apache.s
 2930      S  41520eb8           1      -  httpd
 2936      S  415ca60e           1      -  rotatelogs
 2938      S  415ca60e           1      -  rotatelogs
 3007      Z         0           1      -  sh
 3065      S  4151957e           1     S0  getty
 3458      S  41520eb8           1      1  vsh
 3607      Z         0           1      -  sh
 5622      Z         0           1      -  sh
16120      S  415293c6           1      -  httpd
16980      S  4151957e           1      1  login
17004      R   804b4d6           1      -  hwclock
17080      S  41523f92           1      -  dcos_sshd
17106      R  414c78d1           1      0  vsh
17211      S  414f2b0b           1      -  sleep
17226      S  414f2b0b           1      -  sleep
17227      S  4151957e           1      0  more
17228      S  41520494           1      0  vsh
17229      R  4151957e           1      -  ps
27264      S  415293c6           1      -  httpd
    -     NR         -           0      -  tacacs
    -     NR         -           0      -  bgp
    -     NR         -           0      -  dhcp_snoop
    -     NR         -           0      -  evb
    -     NR         -           0      -  installer
    -     NR         -           0      -  private-vlan
    -     NR         -           0      -  scheduler
    -     NR         -           0      -  vbuilder
    -     NR         -           0      -  vff
    -     NR         -           0      -  vtracker
```

Displaying CPU Utilization

Enter the **show processes cpu** command to display CPU utilization. (See Example 2-2.) The command output includes the following:

- Runtime(ms)—CPU time that the process has used, expressed in milliseconds.

- Invoked—Number of times that the process has been invoked.
- uSecs—Microseconds of CPU time as an average for each process invocation.
- 1Sec—CPU utilization as a percentage for the last one second.

Example 2-2 show processes cpu Command

```
n1000v# show processes cpu
PID    Runtime(ms)  Invoked   uSecs  1Sec    Process
-----  -----------  --------  -----  ------  -----------
    1        26994    364073     74    0.0%  init
    2            5       214     24    0.0%  kthreadd
    3         5861    174700     33    0.0%  migration/0
    4        17907   3927067      4    0.0%  ksoftirqd/0
    5          703     19374     36    0.0%  watchdog/0
    6         5315    155392     34    0.0%  migration/1
    7        16890   3767036      4    0.0%  ksoftirqd/1
    8           97     19374      5    0.0%  watchdog/1
    9       589280   1297793    454    0.0%  events/0
   10         4107    667550      6    0.0%  events/1
   11           93      1051     88    0.0%  khelper
   12          109      2029     53    0.0%  kblockd/0
   13         1812     44595     40    0.0%  kblockd/1
   14            0         2      0    0.0%  kacpid
   15            0         2      0    0.0%  kacpi_notify
   16            0        12     76    0.0%  kseriod
   17            0         2      9    0.0%  ata/0
   18            0         2      6    0.0%  ata/1
   19            0         2      1    0.0%  ata_aux
   20            0         2      0    0.0%  ksuspend_usbd
...
```

Displaying CPU and Memory Information

Enter the **show system resources** command to display system-related CPU and memory statistics. (See Example 2-3.) The output includes the following:

- The load is defined as the number of running processes. The average reflects the system load over the past 1, 5, and 15 minutes.
- Processes displays the number of processes in the system, and how many processes are actually running when the command is entered.
- CPU states shows the CPU usage percentage in the user mode, kernel mode, and idle time in the last one second.
- Memory usage provides the total memory, used memory, free memory, memory used for buffers, and memory used for cache in kilobytes. Buffers and cache are also included in the used memory statistics.

Example 2-3 show system resources Command

```
n1000v# show system resources
Load average:   1 minute: 0.50   5 minutes: 0.23   15 minutes: 0.13
Processes   :   299 total, 1 running
CPU states  :   1.0% user,   0.0% kernel,   99.0% idle
Memory usage:   4035420K total,   1280048K used,   2755372K free
Current memory status: OK
```

RADIUS

The RADIUS protocol is used for the exchange of attributes or credentials between a head-end RADIUS server and a client device. These attributes relate to three classes of services:

- Authentication
- Authorization
- Accounting

Authentication refers to the authentication of users for access to a specific device. You can use RADIUS to manage user accounts for access to a Cisco Nexus 1000V device. When you try to log in to a device, the Cisco Nexus 1000V validates you with information from a central RADIUS server.

Authorization refers to the scope of access that you have once you have been authenticated. Assigned roles for users can be stored in a RADIUS server with a list of actual devices that the user should have access to. Once the user has been authenticated, the switch can refer to the RADIUS server to determine the extent of access that the user will have within the switch network.

Accounting refers to the log information that is kept for each management session in a switch. This information can be used to generate reports for troubleshooting purposes and user accountability. Accounting can be implemented locally or remotely (using RADIUS).

This example shows how to display accounting log entries:

```
n1000v# show accounting log
Fri Aug 22 10:54:48 2014:type=stop:id=NSMGR:user=root:cmd=
Fri Aug 22 10:54:48 2014:type=start:id=NSMGR:user=root:cmd=
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" (SUCCESS)
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" ; switchport mode trunk (REDIRECT)
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" ; switchport mode trunk (SUCCESS)
Fri Aug 22 10:54:48 2014:type=stop:id=NSMGR:user=root:cmd=
Fri Aug 22 10:54:48 2014:type=start:id=NSMGR:user=root:cmd=
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" (SUCCESS)
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" ; switchport trunk allowed vlan all (REDIRECT)
Fri Aug 22 10:54:48 2014:type=update:id=NSMGR:user=root:cmd=configure terminal ;
 port-profile "vmn_926e4512-f5e5-4639-8e2e-29344caf3dcc_654d375f-80b3-45d7-a8ea-
a370e30f4879" ; switchport trunk allowed vlan all (SUCCESS)
```

Note The accounting log shows only the beginning and ending (start and stop) times for each session.

Syslog

The system message logging software saves messages in a log file or directs the messages to other devices. This feature provides the following capabilities:

- Logging information for monitoring and troubleshooting.
- Selecting the types of logging information to be captured.

- Selecting the destination of the captured logging information.

The syslog software allows you to store a chronological log of system messages locally or send to a central syslog server. Syslog messages can also be sent to the console for immediate use. These messages can vary in detail depending on the configuration that you choose.

Syslog messages are categorized into seven severity levels from *debug to critical* events. You can limit the severity levels that are reported for specific services within the switch.

Log messages are not saved across system reboots. However, a maximum of 100 log messages with a severity level of critical and below (levels 0, 1, and 2) can logged to a local file or server.

Logging Levels

The Cisco Nexus 1000V supports the following logging levels:

- 0—emergency
- 1—alert
- 2—critical
- 3—error
- 4—warning
- 5—notification
- 6—informational
- 7—debugging

By default, the switch logs normal but significant system messages to a log file and sends these messages to the system console. You can specify which system messages should be saved based on the type of facility and the severity level. Messages are time-stamped to enhance real-time debugging and management.

Enabling Logging for Telnet or SSH

System logging messages are sent to the console based on the default or configured logging facility and severity values.

You can disable logging to the console or enable logging to a given Telnet or SSH session as follows:

- To disable console logging, enter the **no logging console** command in global configuration mode.
- To enable logging for Telnet or SSH, enter the **terminal monitor** command in EXEC mode.

Note When logging to a console session that is disabled or enabled, that state is applied to all future console sessions. If you exit and log in again to a new session, the state is preserved. However, when logging to a Telnet or SSH session that is enabled or disabled, that state is applied only to that session. The state is not preserved after you exit the session.

The **no logging console** command that is shown in Example 2-4 disables console logging and is enabled by default.

Example 2-4 no logging console Command

```
n1000v(config)# no logging console
```

The **terminal monitor** command that is shown in Example 2-5 enables logging for Telnet or SSH and is disabled by default.

Example 2-5 terminal monitor Command

```
n1000v# terminal monitor
```

For more information about configuring syslogs, see the *Cisco Nexus 1000V for KVM System Management Configuration Guide, Release 5.x*.