

Proceso de comprobación de estado del sistema de la plataforma de switch Nexus serie 3500

Contenido

[Introducción](#)

[Supervisar el uso de CPU y memoria](#)

[Comprobar estado de diagnóstico de hardware](#)

[Ver perfil de hardware](#)

[Supervisión de búfer activa](#)

[Supervisar contadores/estadísticas de interfaz](#)

[Supervisar estadísticas de regulación del plano de control](#)

[Realizar comprobación de estado del sistema de archivos Bootflash](#)

[Recopilación de Números de Sistema y Registros de Proceso](#)

[Información Relacionada](#)

Introducción

Este documento describe el proceso general que se utiliza para realizar una verificación del estado del sistema en las plataformas de switches Nexus de Cisco serie 3500 que ejecutan Nexus Operating System (NX-OS) versión 6.0(2).

Supervisar el uso de CPU y memoria

Para recibir una descripción general del uso de la CPU y la memoria del sistema, ingrese el comando **show system resources**:

```
switch# show system resources
Load average:  1 minute: 0.32   5 minutes: 0.13   15 minutes: 0.10
Processes   :   366 total, 2 running
CPU states  :   5.5% user,   12.0% kernel,   82.5% idle
      CPU0 states :   10.0% user,   18.0% kernel,   72.0% idle
      CPU1 states :    1.0% user,    6.0% kernel,   93.0% idle
Memory usage: 4117064K total, 2614356K used, 1502708K free
Switch#
```

Si necesita más detalles sobre los procesos que consumen ciclos de CPU o memoria, ingrese los comandos **show process cpu sort** y **show system internal kernel memory usage**:

```
switch# show process cpu sort
PID      Runtime(ms)   Invoked    uSecs   lSec    Process
-----
3239     55236684     24663045   2239    6.3%   mtc_usd
3376         776         7007     110    2.7%   netstack
  15    26592500 178719270   148    0.9%   kacpid
3441     4173060     29561656   141    0.9%   cfs
3445     7646439     6391217   1196    0.9%   lacp
```

```

3507      13646757  34821232    391    0.9%  hsrp_engine
   1         80564   596043    135    0.0%   init
   2           6     302     20    0.0%  kthreadd
   3        1064   110904     9    0.0%  migration/0
<snip>

```

```
switch# show system internal kernel memory usage
```

```

MemTotal:      4117064 kB
MemFree:      1490120 kB
Buffers:         332 kB
Cached:          1437168 kB
ShmFS:           1432684 kB
Allowed:         1029266 Pages
Free:            372530 Pages
Available:       375551 Pages
SwapCached:      0 kB
Active:          1355724 kB
Inactive:        925400 kB
HighTotal:    2394400 kB
HighFree:     135804 kB
LowTotal:     1722664 kB
LowFree:      1354316 kB
SwapTotal:       0 kB
SwapFree:        0 kB
Dirty:           12 kB
Writeback:       0 kB
AnonPages:       843624 kB
Mapped:          211144 kB
Slab:            98524 kB
SReclaimable:    7268 kB
SUnreclaim:      91256 kB
PageTables:      19604 kB
NFS_Unstable:    0 kB
Bounce:          0 kB
WritebackTmp:    0 kB
CommitLimit:     2058532 kB
Committed_AS:    10544480 kB
VmallocTotal:    284664 kB
VmallocUsed:     174444 kB
VmallocChunk:    108732 kB
HugePages_Total: 0
HugePages_Free:  0
HugePages_Rsvd:  0
HugePages_Surp:  0
Hugepagesize:    2048 kB
DirectMap4k:     2048 kB
DirectMap2M:     1787904 kB
switch#

```

El resultado muestra que la región de **memoria alta** es utilizada por NX-OS, y la región de **memoria baja** es utilizada por el kernel. Los valores **MemTotal** y **MemFree** proporcionan la memoria total disponible para el switch.

Para generar alertas de uso de memoria, configure el switch de manera similar a esto:

```
switch(config)# system memory-thresholds minor 50 severe 70 critical 90
```

Nota: Para este documento, los valores **50**, **70** y **90** se utilizan solamente como ejemplos; seleccione límites de umbral en función de sus necesidades.

Comprobar estado de diagnóstico de hardware

Para verificar el estado del diagnóstico de hardware, ingrese el comando **show diagnostic output all**. Asegúrese de que todas las pruebas pasen y que el **resultado de diagnóstico general sea PASS**.

```
switch# show diagnostic result all
Current bootup diagnostic level: complete
Module 1: 48x10GE Supervisor SerialNo : <serial #>
Overall Diagnostic Result for Module 1 : PASS
Diagnostic level at card bootup: complete
Test results: (. = Pass, F = Fail, I = Incomplete, U = Untested, A = Abort)
  1) TestUSBFlash -----> .
  2) TestSPROM -----> .
  3) TestPCIE -----> .
  4) TestLED -----> .
  5) TestOBFL -----> .
  6) TestNVRAM -----> .
  7) TestPowerSupply -----> .
  8) TestTemperatureSensor -----> .
  9) TestFan -----> .
 10) TestVoltage -----> .
 11) TestGPIO -----> .
 12) TestInbandPort -----> .
 13) TestManagementPort -----> .
 14) TestMemory -----> .
 15) TestForwardingEngine -----> .
<snip>
```

Ver perfil de hardware

Ingrese el comando **show hardware profile status** para verificar el perfil de hardware actual configurado en el switch y el uso de la tabla de hardware:

```
switch# show hardware profile status
Hardware table usage:
Max Host Entries = 65535, Used = 341
Max Unicast LPM Entries = 24576, Used = 92
Max Multicast LPM Entries = 8192, Used (L2:L3) = 1836 (1:1835)
Switch#
```

Asegúrese de que el uso de las entradas **Host Entries** y las entradas **Unicast/Multicast Longest Prefix Match (LPM)** estén dentro del límite especificado.

Nota: Para obtener un rendimiento óptimo del switch, es importante elegir la plantilla de perfil de hardware adecuada.

Si desea que el switch genere un syslog en un nivel de umbral específico, configure el switch de manera similar a esto:

```
switch(config)# hardware profile multicast syslog-threshold ?
<1-100> Percentage

switch(config)# hardware profile unicast syslog-threshold ?
```

<1-100> Percentage

Nota: El valor de umbral predeterminado es del 90% tanto para unidifusión como para multidifusión.

Para obtener más detalles, consulte el artículo [Configuración de PIM Cisco](#), que proporciona detalles de configuración basados en la licencia instalada y las funciones habilitadas. Además, si desea optimizar la tabla de reenvío, consulte los [switches Nexus de Cisco serie 3000: Comprender, configurar y ajustar el artículo de Cisco de la tabla de reenvío](#).

Supervisión de búfer activa

La supervisión de búfer activa (ABM) proporciona los datos de ocupación de búfer granular, lo que permite obtener una mejor perspectiva de los puntos de congestión más activos. Esta función admite dos modos de funcionamiento: Modo **de unidifusión** y **multidifusión**.

En el modo **unidifusión**, ABM monitorea y mantiene los datos de uso del búfer por bloque de búfer, y la utilización del búfer de unidifusión para los 48 puertos. En el modo **Multicast**, monitorea y mantiene los datos de uso del buffer por bloque-buffer, y la utilización del búfer multicast por bloque-buffer.

Nota: Para obtener más información, consulte el artículo de Cisco [Cisco Nexus 3548 Active Buffer Monitoring](#). La figura 4 del artículo muestra que el uso del búfer alcanzó un pico a las **22:15:32** y duró hasta las **22:15:37**. Además, el histograma proporciona evidencia de picos repentinos en el uso y muestra la velocidad a la que se drena el búfer. Si hay un receptor lento (como un receptor de 1 Gbps entre receptores de 10 Gbps), entonces para evitar caídas de paquetes, debe incluir una configuración similar a esta: **perfil de hardware puerto de receptor lento multicast <x>**.

Supervisar contadores/estadísticas de interfaz

Para monitorear la pérdida de tráfico, ingrese el comando **show interface ethernet x/y**. El resultado de este comando proporciona información básica sobre la velocidad del tráfico y también errores/caídas a nivel de puerto.

```
switch# show interface eth1/10
Ethernet1/10 is up
Dedicated Interface
Belongs to Pol
Hardware: 100/1000/10000 Ethernet, address: 30f7.0d9c.3b51
(bia 30f7.0d9c.3b51)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s, media type is 10G
Beacon is turned off
Input flow-control is off, output flow-control is off
Rate mode is dedicated
Switchport monitor is off
EtherType is 0x8100
Last link flapped 3d21h
```

```
Last clearing of "show interface" counters never
14766 interface resets
30 seconds input rate 47240 bits/sec, 68 packets/sec
30 seconds output rate 3120720 bits/sec, 3069 packets/sec
Load-Interval #2: 5 minute (300 seconds)
input rate 50.18 Kbps, 52 pps; output rate 3.12 Mbps, 3.05 Kpps
```

RX

```
4485822 unicast packets 175312538 multicast packets 388443 broadcast
packets
180186040 input packets 9575683853 bytes
0 jumbo packets 0 storm suppression bytes
1 runts 0 giants 1 CRC 0 no buffer
2 input error 0 short frame 0 overrun 0 underrun 0 ignored
0 watchdog 0 bad etype drop 0 bad proto drop 0 if down drop
0 input with dribble 260503 input discard
0 Rx pause
```

TX

```
159370439 unicast packets 6366799906 multicast packets 1111 broadcast
packets
6526171456 output packets 828646014117 bytes
0 jumbo packets
0 output errors 0 collision 0 deferred 0 late collision
0 lost carrier 0 no carrier 0 babble 0 output discard
0 Tx pause
```

switch#

Si los descartes **input** o **output** muestran valores distintos a cero, determine si los paquetes descartados son unidifusión y/o multidifusión:

```
switch# show queuing interface ethernet 1/10
Ethernet1/10 queuing information:
TX Queuing
  qos-group sched-type oper-bandwidth
    0 WRR 100

RX Queuing
Multicast statistics:
  Mcast pkts dropped : 0
Unicast statistics:
  qos-group 0
  HW MTU: 1500 (1500 configured)
  drop-type: drop, xon: 0, xoff: 0
  Statistics:
    Ucast pkts dropped : 0
```

switch#

El resultado indica que el tráfico descartado no se debe a la calidad del servicio (QoS). Ahora debe verificar las estadísticas de dirección MAC del hardware:

```
switch# show hardware internal statistics device mac ?
all Show all stats
congestion Show congestion stats
control Show control stats
errors Show error stats
lookup Show lookup stats
pktflow Show packetflow stats
qos Show qos stats
rates Show packetflow stats
snmp Show snmp stats
```

Cuando realiza una resolución de problemas para caídas de tráfico, las opciones clave para

verificar son **congestión, errores y qos**. La opción **pkflow** proporciona estadísticas de tráfico en las direcciones RX y TX, con rangos de tamaño de paquete específicos.

```
switch# show hardware internal statistics device mac errors port 10
|-----|
| Device: L2/L3 forwarding ASIC   Role:MAC                               |
|-----|
Instance:0
ID      Name                               Value                               Ports
--      -
198    MTC_MB_CRC_ERR_CNT_PORT9              0000000000000002                   10 -
508    MTC_PP_CNT_PORT1_RCODE_CHAIN3         0000000000000002                   10 -
526    MTC_RW_EG_PORT1_EG_CLB_DROP_FCNT_CHAIN3 000000000054da5a                   10 -
3616   MTC_NI515_P1_CNT_TX                   000000000000bed                    10 -
6495   TTOT_OCT                               000000000005f341                   10 -
7365   RTOT                                    0000000000000034                   10 -
7366   RCRC                                    0000000000000001                   10 -
7374   RUNT                                    0000000000000001                   10 -
9511   ROCT                                    00000000000018b9                   10 -
10678 PORT_EXCEPTION_ICBL_PKT_DROP      000000000003f997                   10 -
```

Nota: El valor hexadecimal **0x3f997** es igual a **260503** en formato decimal.

```
switch# show interface eth1/10
Ethernet1/10 is up
<snip> 0 input with dribble
260503 input discard
<snip>
```

En el resultado, el mensaje de error **PORT_EXCEPTION_ICBL_PKT_DROP** indica que el tráfico recibido en el puerto tiene una **etiqueta Dot1Q** para una VLAN que no está habilitada en el switch.

Este es otro ejemplo, donde se ve el tráfico caído debido a QoS:

```
switch# show interface ethernet 1/11

Ethernet1/11 is up
<snip>
TX

<snip>
 0 output errors 0 collision 0 deferred 0 late collision
 0 lost carrier 0 no carrier 0 babble 6153699 output discard
 0 Tx pause
switch#
```

```
switch# show queuing interface ethernet 1/11
```

```
Ethernet1/11 queuing information:
TX Queuing
  qos-group sched-type oper-bandwidth
    0        WRR          100
```

RX Queuing

```
Multicast statistics:
  Mcast pkts dropped : 0
```

```
Unicast statistics:
qos-group 0
HW MTU: 1500 (1500 configured)
drop-type: drop, xon: 0, xoff: 0
Statistics:
    Ucast pkts dropped                : 6153699
```

Nota: La salida indica que se descartaron **6153699** paquetes en la dirección de recepción, lo que es engañoso. Consulte Cisco bug ID [CSCuj20713](#).

```
switch# show hardware internal statistics device mac all | i 11|Port

(result filtered for relevant port)
ID   Name           Value           Ports
<snip>
5596 TX_DROP      00000000005de5e3  11 - <--- 6153699 Tx Drops in Hex
<snip>
10253 UC_DROP_VL0 00000000005de5e3  11 - <--- Drops for QoS Group 0 in Hex
<snip>
```

En resumen, estos son los comandos que se utilizan para capturar las caídas de paquetes:

- **show interface ethernet x/y**
- **show queuing interface ethernet x/y**
- **show hardware internal statistics device mac errors port <port #>**

Supervisar estadísticas de regulación del plano de control

Control Plane Policing (CoPP) protege el plano de control para garantizar la estabilidad de la red. Para obtener más detalles, consulte el artículo [Configuración de Control Plane Policing](#) Cisco.

Para monitorear las estadísticas de CoPP, ingrese el comando **show policy-map interface control-plane**:

```
switch# show policy-map interface control-plane
Control Plane
service-policy input: copp-system-policy

class-map copp-s-ping (match-any)
  match access-group name copp-system-acl-ping
  police pps 100 , bc 0 packets
    HW Matched Packets  30
    SW Matched Packets  30
class-map copp-s-l3destmiss (match-any)
  police pps 100 , bc 0 packets
    HW Matched Packets  76
    SW Matched Packets  74
class-map copp-s-glean (match-any)
  police pps 500 , bc 0 packets
    HW Matched Packets  103088
    SW Matched Packets  51544
<snip>
```

En la salida, el Hardware (HW) y el Software (SW) Paquetes coincidentes para **copp-s-ping** son los mismos. Esto significa que la cantidad de paquetes que se cuenta por el HW es de 30 (todos enviados hacia el controlador de CPU dentro de la banda) y el SW cuenta el mismo número de

paquetes antes de enviarlos a la CPU. Esto indica que CoPP no descarta paquetes porque está dentro del límite configurado de 100 p/s.

Cuando se observa la clase copp-s-glean, que coincide con los paquetes destinados a la dirección IP para la cual no está presente la entrada de caché del protocolo de resolución de direcciones (ARP), el número de paquetes que ve el HW es **103,088**, mientras que el SW coincide sólo con el 1544 ... Esto indica que el CoPP descartó los paquetes **51544** (103088-51544), porque la velocidad de estos paquetes excede los 500 p/s.

Los contadores de SW se obtienen del controlador de banda interna de la CPU y los contadores de hardware provienen de la lista de control de acceso (ACL) que se programa en el hardware. Si se encuentra una situación en la que los **paquetes coincidentes de hardware** son iguales a cero, y un valor distinto de cero está presente para los **paquetes coincidentes de SW**, no hay ninguna ACL presente en el HW para ese mapa de clase específico, que puede ser normal. También es importante tener en cuenta que estos dos contadores podrían no ser sondeados al mismo tiempo, y usted debería utilizar solamente los valores de contador para resolver problemas si la diferencia es significativa.

Es posible que las estadísticas de CoPP no estén directamente relacionadas con los paquetes conmutados por HW, pero sigue siendo relevante si los paquetes que se deben enviar a través del switch se envían a la CPU. Un packet-punt es causado por varias razones, como cuando se ejecuta una adyacencia glean.

Tenga en cuenta que hay tres tipos de políticas CoPP: Predeterminado, Capa 2 (L2) y Capa 3 (L3). Elija la política adecuada en función del escenario de implementación y modifique la política CoPP en función de las observaciones. Para ajustar la CoPP, verifique regularmente y después de obtener nuevos servicios/aplicaciones o después de un rediseño de red.

Nota: Para borrar los contadores, ingrese el comando **clear copp statistics**.

Realizar comprobación de estado del sistema de archivos Bootflash

Para realizar una verificación de estado en el sistema de archivos bootflash, ingrese el comando **system health check bootflash**:

```
switch# system health check bootflash
Unmount successful...
Checking any file system errors...Please be patient...
Result: bootflash filesystem has no errors
done.
Remounting bootflash ...done.
switch#
```

Precaución: El sistema de archivos se desmonta cuando se ejecuta la prueba y se vuelve a montar una vez finalizada la prueba. Asegúrese de que no se tenga acceso al sistema de archivos mientras ejecuta la prueba.

Recopilación de Números de Sistema y Registros de Proceso

Precaución: Asegúrese de que el sistema no experimenta ningún proceso se restablece o se bloquea, y no genera ningún archivo de núcleo o registro de procesos cuando intenta utilizar los comandos mencionados en esta sección.

Ingrese estos comandos para recolectar los núcleos del sistema y los registros de procesos:

```
switch# show cores
Module Instance Process-name PID Date(Year-Month-Day Time)
-----
switch#

switch# show process log
Process PID Normal-exit Stack Core Log-create-time
-----
ethpc 4217 N N N Tue Jun 4 01:57:54 2013
```

Nota: Consulte el artículo [Recuperación de archivos de núcleo de las plataformas de switching Cisco Nexus](#) de Cisco para obtener más detalles sobre este proceso.

Información Relacionada

- [Hojas de datos y documentación: switches Nexus de Cisco serie 3000](#)
- [Comparar modelos: switches Nexus de Cisco serie 3000](#)
- [Introducción: switches Nexus de Cisco serie 3000](#)
- [Introducción al contador de interfaz de "descarte de entrada" en Nexus3000 - Comunidades de soporte de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)