

# Processo da verificação de saúdes de sistema da plataforma do 3500 Series Switch do nexo

## Índice

[Introdução](#)

[Monitore o CPU e a utilização de memória](#)

[Verifique o estado dos diagnósticos de hardware](#)

[Veja o perfil de hardware](#)

[Monitoração ativa do buffer](#)

[Monitore contadores de interface/estatísticas](#)

[Monitore estatísticas do Policiamento do plano de controle](#)

[Execute o exame médico completo do sistema de arquivos do bootflash](#)

[Recolha núcleos do sistema e processe logs](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve o processo geral que é usado a fim executar uma verificação de saúdes de sistema nas Plataformas do 3500 Series Switch do nexo de Cisco que executam a liberação do sistema operacional do nexo (NX-OS) 6.0(2).

## Monitore o CPU e a utilização de memória

A fim receber uma vista geral do CPU e a utilização de memória do sistema, incorpore o comando dos **recursos de sistema da mostra**:

```
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#**

Se você exige mais detalhes sobre os processos que consomem ciclos de CPU ou memória, incorpore o **tipo processador central do processo da mostra e mostre a sistema comandos usage da memória de núcleo interna**:

```

switch# show process cpu sort
PID      Runtime(ms)   Invoked    uSecs   1Sec    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#

```

A saída mostra que a região de **memória alta** está usada pelo NX-OS, e a região de **memória baixa** é usada pelo núcleo. Os valores de **MemTotal** e de **MemFree** fornecem a memória total que está disponível para o interruptor.

A fim gerar alertas da utilização de memória, configurar o interruptor similar a este:

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

**Note:** Para este documento, os 50 pés, os 70, e os 90 dos valores são usados somente como exemplos; escolha os limites de limiar baseados em suas necessidades.

## Verifique o estado dos diagnósticos de hardware

A fim verificar o estado dos diagnósticos de hardware, inscreva o comando **all** do resultado de diagnóstico da mostra. Assegure-se de que todos os testes passem, e que o resultado de diagnóstico total é **PASSAGEM**.

```
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>
```

## Veja o perfil de hardware

Inscreva o comando **status** do perfil de hardware da mostra a fim verificar o perfil de hardware atual que é configurado no interruptor, e o uso da tabela do 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#
```

Assegure-se de que o uso das entradas de host e o unicast/as entradas compatibilidade de prefixo mais longo do Multicast (LPM) estejam dentro do limite especificado.

**Note:** Para o desempenho ótimo do interruptor, é importante escolher o molde apropriado do perfil de hardware.

Se você quer o interruptor gerar um Syslog a nível de ponto inicial específico, configurar o interruptor similar a este:

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

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

**Note:** O valor de limiar do padrão é 90 por cento para o unicast e o Multicast.

Para mais detalhes, refira o artigo [configurando PIM](#) Cisco, que fornece os detalhes de configuração baseados na licença instalada e nas características permitidas. Igualmente, se você quer aperfeiçoar a tabela do forwarding, refira os [3000 Series Switch do nexa de Cisco: Compreenda, configurar e ajuste o](#) artigo de Cisco da [tabela do forwarding](#).

## Monitoração ativa do buffer

A monitoração ativa do buffer (ABM) fornece os dados granulados do manutenção do buffer, que permitem a melhor introspecção em pontos ativo da congestão. Este modo dos suportes de recurso dois de operação: **Unicast** e **Modo multicast**.

**No modo de Unicast**, o ABM monitora e mantém os dados do uso de buffer pelo buffer-bloco, e a utilização do buffer do unicast para todas as 48 portas. **No Modo multicast**, monitora e mantém os dados do uso de buffer pelo buffer-bloco, e a utilização do buffer do Multicast pelo buffer-bloco.

**Note:** Para mais informação, proveja o [buffer ativo do nexa 3548 de Cisco que monitora o](#) artigo de Cisco. Figura 4 do artigo mostra que o uso de buffer repicou em **22:15:32** e durou até **22:15:37**. Também, o histograma fornece a evidência de pontos repentinos no uso e mostra a velocidade em que o buffer drena. Se há um receptor lento (tal como um receptor 1-Gbps entre os receptores 10-Gbps), a seguir a fim evitar quedas de pacote de informação, você deve incluir uma configuração similar a esta: **<x> da porta do lento-receptor do Multicast do perfil de hardware**.

## Monitore contadores de interface/estatísticas

A fim monitorar a perda de tráfego, incorpore o comando do **x/y dos Ethernet de interface da mostra**. A saída deste comando fornece a informação de taxa de tráfego básica, e igualmente as gotas do porta-nível/erros.

```
switch# show interface eth1/10  
Ethernet1/10 is up  
Dedicated Interface  
Belongs to Po1  
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#

Se os descartes da **entrada** ou da **saída** mostram valores diferentes de zero, determine se os pacotes descartado são unicast e/ou Multicast:

```

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#

A saída indica que o tráfego descartado não é devido ao Qualidade de Serviço (QoS). Agora você deve verificar as estatísticas do endereço MAC de 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

```

Quando você executa uma pesquisa de defeitos para gotas do tráfego, as opções chaves a verificar são **congestão**, **erros**, e **qos**. A opção do **pktflow** fornece estatísticas de tráfego nos sentidos RX e TX, as escalas específicas do tamanho do pacote.

```

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 -

```

**Note:** O valor hexadecimal **0x3f997** iguala **260503** no formato decimal.

```

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

```

Na saída, o Mensagem de Erro **PORT\_EXCEPTION\_ICBL\_PKT\_DROP** indica que o tráfego recebido na porta tem uma etiqueta do **dot1q** para um VLAN que não seja permitido no interruptor.

Está aqui um outro exemplo, onde a gota do tráfego é considerado devido 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
```

**Note:** A saída indica que **6153699** pacotes estiveram deixados cair na rota de recepção, que é enganadora. Refira a identificação de bug Cisco [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_VLO	00000000005de5e3	11 - <--- Drops for QoS Group 0 in Hex
<snip>			

Em resumo, estão aqui os comandos que são usados a fim capturar quedas de pacote de informação:

- mostre o `x/y` dos Ethernet de interface
- mostre o `x/y` dos Ethernet da interface de enfileiramento
- mostre o `#>` do `<port da porta dos erros do Mac do dispositivo das estatísticas internas do hardware`

## Monitore estatísticas do Policiamento do plano de controle

O Policiamento do plano de controle (CoPP) protege o plano do controle a fim assegurar a estabilidade de rede. Para detalhes adicionais, proveja o artigo [configurando de](#) Cisco do [Policiamento do plano de controle](#).

A fim monitorar as estatísticas de CoPP, incorpore o comando do **controle plano da relação do mapa de política da mostra**:

```
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>

Na saída, os **pacotes compatíveis do hardware (HW)** e do software (**SW**) para o **copp-s-sibilo** são os mesmos. Isto significa que a quantidade de pacotes que é contada pelo **HW** é 30 (enviado toda para o direcionador Inband CPU), e o **SW** conta o mesmo número de pacotes antes que os envie ao CPU. Isto indica que nenhum pacote está deixado cair por CoPP, porque está dentro do limite configurado de 100 p/s.

Quando você olhar a classe **copp-s-recolher**, que combina os pacotes que são destinados ao endereço IP de Um ou Mais Servidores Cisco ICM NT para que a entrada de cache do Address Resolution Protocol (ARP) não está atual, o número de pacotes que é considerado pelo **HW** é **103,088**, quando os fósforos somente **51544 SW**. Isto indica que o CoPP deixou cair **51544** pacotes (de 103088-51544), porque a taxa destes pacotes excede 500 p/s.

Os contadores SW são obtidos do direcionador Inband CPU, e os contadores do HW vêm do Access Control List (ACL) que é programado no HW. Se você encontra uma situação onde os **pacotes compatíveis do HW** iguaem zero, e um valor diferente de zero esta presente para os **pacotes compatíveis SW**, a seguir nenhum ACL esta presente no HW para esse mapa de classe específico, que podem ser normais. É igualmente importante notar que estes dois contadores não puderam ser votados ao mesmo tempo, e você deve somente usar o troubleshoot dos valores de contador se a diferença é significativa.

As estatísticas de CoPP não puderam diretamente ser relacionadas aos pacotes HW-comutados, mas é ainda relevante se os pacotes que devem ser enviados através do interruptor punted ao CPU. Um pacote-pontapé está causado por várias razões, como quando você executa uma adjacência glean.

Esteja ciente que há três tipos de políticas de CoPP: Opte, a camada 2 (L2), e a camada 3 (L3). Escolha a política apropriada baseada no cenário de distribuição, e altere a política de CoPP baseada nas observações. A fim ajustar o CoPP, verifique regularmente, e verificação depois que você obtém serviços/aplicativos novos ou depois que um redesign da rede.

**Note:** A fim cancelar os contadores, inscreva o **comando statistics claro do copp**.

## Execute o exame médico completo do sistema de arquivos do bootflash

A fim executar um exame médico completo no sistema de arquivos do bootflash, incorpore o comando do **bootflash da verificação de saúdes de sistema**:

```
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#
```



**Caution:** O sistema de arquivos é desmontado quando você executa o teste, e está feito uma nova montagem de uma vez que o teste está completo. Assegure-se de que o sistema de arquivos não esteja alcançado quando você executar o teste.

## Recolha núcleos do sistema e processe logs

**Caution:** Assegure-se de que o sistema não experimente nenhumas restaurações ou impactos do processo, e não se gerencia nenhum arquivos principais ou logs do processo quando você tenta usar os comandos que estão mencionados nesta seção.

Incorpore estes comandos a fim recolher os núcleos do sistema e processar logs:

```
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
```

**Note:** Proveja os [arquivos principais de recuperação do](#) artigo de Cisco das [plataformas de switching do nexo de Cisco](#) para mais detalhes sobre este processo.

## Informações Relacionadas

- [Folhas de dados e literatura - 3000 Series Switch do nexo de Cisco](#)
- [Compare modelos - 3000 Series Switch do nexo de Cisco](#)
- [Introdução - 3000 Series Switch do nexo de Cisco](#)
- [Compreender da “o contador de interface do descarte entrada” em Nexus3000 - Cisco apoiam as comunidades](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)