Índice

Introdução

Este documento descreve as causas da utilização elevada da CPU nos Cisco Catalyst 6500/6000 Series Switches e nos sistemas com base no Sistema de Switching Virtual (VSS) 1440. Como roteadores Cisco, o Switches usa o **comando show processes cpu** a fim mostrar a utilização CPU para o processador do Supervisor Engine do interruptor. Contudo, devido às diferenças na arquitetura e nos mecanismos de encaminhamento entre roteadores e switches Cisco, as saídas típicas do comando show processes cpu diferem significativamente. O significado da saída difere também. Este documento esclarece estas diferenças e descreve a utilização CPU no Switches e como interpretar a saída do **comando show processes cpu**.

Nota: Neste documento, as palavras “comutam” e o “Switches” refere o Switches do Catalyst 6500/6000.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão de software e hardware para o Switches do Catalyst 6500/6000 e o sistema de switching virtual (VSS) 1440 sistemas baseados.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Nota: O software suportado para o sistema de switching virtual (VSS) 1440 sistemas baseados é a liberação 12.2(33)SXH1 do Cisco IOS ® Software ou mais tarde.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Diferença entre CatOS e software do sistema IOS

OS do catalizador (CatOS) no Supervisor Engine e software de Cisco IOS® no Multilayer Switch Feature Card (MSFC) (híbrido): Você pode usar uma imagem de catos como o software do sistema para executar o Supervisor Engine no Switches do Catalyst 6500/6000. Se o MSFC opcional está instalado, uma imagem de Cisco IOS Software separada é utilizada para executar o MSFC.

Cisco IOS Software em Supervisor Engine e MSFC (Nativo): Você pode usar uma única imagem do Cisco IOS Software como o software do sistema para executar o Supervisor Engine e o MSFC no Switches do Catalyst 6500/6000.

Nota: Consulte o Comparação dos Sistemas Operacionais Cisco Catalyst e Cisco IOS para o Switch Catalyst 6500 Series para obter mais informações.

Compreenda a utilização CPU no Switches do Catalyst 6500/6000

Os roteadores baseado em software de Cisco usam o software a fim processar e os pacotes de rota. A utilização CPU em um roteador Cisco tende a aumentar enquanto o roteador executa mais pacote que processa e que distribui. Portanto, o comando show processes cpu pode oferecer uma indicação regularmente precisa da carga de processamento de tráfego no roteador.

O Switches do Catalyst 6500/6000 não usa o CPU da mesma forma. Este Switches faz decisões de encaminhamento no hardware, não no software. Consequentemente, quando o Switches faz a transmissão ou a decisão de switching para a maioria de quadros que passam através do interruptor, o processo não envolve o CPU de Supervisor Engine.

No Switches do Catalyst 6500/6000, há dois CPU. Um CPU é o CPU de Supervisor Engine, que é chamado o processador de gerenciamento de rede (NMP) ou o switch processor (SP). O outro CPU é o Engine de roteamento CPU da camada 3, que é chamado o MSFC ou o route processor (RP).

O SP CPU executa as funções que incluem:

- Assistências na aprendizagem de endereço MAC e no envelhecimento**Nota:** A aprendizagem de endereço MAC é chamada igualmente instalação do trajeto.
- Protocolos e processos das corridas que fornecem o controle de redeOs exemplos incluem o Spanning Tree Protocol (STP), o Cisco Discovery Protocol (CDP), o protocolo VLAN Trunk (VTP), o Dynamic Trunking Protocol (DTP), e o Port Aggregation Protocol (PAgP).
- Segura o tráfego de gerenciamento de rede que é destinado ao CPU do interruptorOs exemplos incluem o telnet, o HTTP, e o tráfego do Simple Network Management Protocol (SNMP).

O RP CPU executa as funções que incluem:

- As construções e atualizam o roteamento da camada 3 e as tabelas do Address Resolution Protocol (ARP)
- Gera o banco de informação de encaminhamento (FIB) e as tabelas de adjacência do Cisco Express Forwarding (CEF), e transfere as tabelas no Policy Feature Card (o PFC)
- Segura o tráfego de gerenciamento de rede que é destinado ao RPOs exemplos incluem o telnet, o HTTP, e o tráfego SNMP.

Situações e características que tráfego do disparador a ir ao software

Pacotes que são destinados ao interruptor

Todo o pacote que for destinado ao interruptor vai ao software. Tais pacotes incluem:

- Pacotes de controleOs pacotes de controle são recebidos para o STP, o CDP, o VTP, o Hot Standby Router Protocol (HSRP), o PAgP, o protocolo link aggregation control (LACP), e o UniDirectional Link Detection (UDLD).
- Atualizações de protocolo de roteamentoOs exemplos destes protocolos são Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), e abrem o protocolo shortest path first (protocolo de OSPF).
- Tráfego SNMP que é destinado ao interruptor
- O telnet e o protocolo secure shell (SSH) traficam ao interruptor.O ultilization da alta utilização da CPU devido ao SSH é visto como:Inclua estes comandos no script EEM a fim verificar o número de sessões SSH estabelecidas quando o CPU vai altamente:mostre usuáriosshow line
- Reações ARP às requisições ARP

Pacotes e circunstâncias que exigem o processamento especial

Esta lista fornece os tipos de pacote e as circunstâncias específicos que forçam pacotes para ser segurados no software:

- Pacotes com opções IP, um Time to Live expirado (TTL), ou encapsulamento NON-avançado da agência dos projetos de pesquisa (ARPA)
- Pacotes com manipulação especial, tal como o Tunelamento
- Fragmentação de IP
- Pacotes que exigem mensagens do Internet Control Message Protocol (ICMP) do RP ou do SP
- Falha da verificação da unidade de transmissão máxima (MTU)
- Pacotes com erros IP, que incluem a soma de verificação e os erros de comprimento IP
- Se os pacotes de entrada retornam um erro de bit (tal como o erro de um bit (SBE)), os pacotes são enviados ao CPU para o software que processa e corrigidos. O sistema atribui um buffer para eles e usa os recursos do CPU para corrigi-lo.
- Quando o PBR e a lista de acessos reflexiva estão no trajeto de um fluxo de tráfego, o pacote é o software comutado, que exige um ciclo de CPU adicional.
- Adjacência a mesma relação
- Pacotes que falham a verificação do encaminhamento de caminho reverso (RPF)? **falha de RPF**
- Recolha/recebaRecolha refere os pacotes que exigem a resolução ARP, e recebem refere os pacotes que caem no exemplo da recepção.
- Tráfego das Trocas de Pacote Entre Redes IPX (IPX) que é comutado por software no Supervisor Engine 720 no Cisco IOS Software e no CatOSO tráfego IPX é igualmente comutado por software no IOS Software do Supervisor Engine 2/Cisco, mas o tráfego é comutado por hardware no Supervisor Engine 2/CatOS. O tráfego IPX é comutado por hardware no Supervisor Engine 1A para ambos os sistemas operacionais.
- Tráfego do APPLETALK
- Condições completas dos recursos do hardwareEstes recursos incluem MENTEM, a memória de conteúdo endereçável (CAM), e CAM ternário (TCAM).

Características ACL-baseadas

- O Access Control List (ACL) - tráfego negado com a característica dos ICMP não alcançável girou sobre**Nota:** Esse é o padrão.Alguns pacotes ACL-negados estão escapados ao MSFC se os inalcançáveis IP são permitidos. Os pacotes que exigem ICMP não alcançável são escapados em uma taxa dos configuráveis pelo usuário. À revelia, a taxa é 500 pacotes por segundo (pps).
- IPX que filtra com base em parâmetros não suportados, tais como o host de origemNo Supervisor Engine 720, o processo de tráfego IPX da camada 3 está sempre no software.
- Entradas de controle de acesso (ACE) que exigem o registo, com a palavra-chave do **log**Isto aplica-se às características do log ACL e do log VLAN ACL (VACL). ACE no mesmo ACL que não exigem o registo ainda do processo no hardware. O Supervisor Engine 720 com PFC3 apoia o limite de taxa dos pacotes que são reorientados ao MSFC para o registo ACL e VACL. O Supervisor Engine 2 apoia o limite de taxa dos pacotes que são reorientados ao MSFC para o registo VACL. O apoio para o ACL que entra o Supervisor Engine 2 é programado para o ramo do Cisco IOS Software Release 12.2S.
- o tráfego Política-roteado, com uso do **comprimento do fósforo**, **ajustou a Precedência IP**, ou os outros parâmetros não suportadosO parâmetro da **relação do grupo** tem o apoio no software. Contudo, o parâmetro do **null0 da relação do grupo** é uma exceção. Este tráfego é segurado no hardware no Supervisor Engine 2 com PFC2 e no Supervisor Engine 720 com PFC3.
- Não-IP e ACLs de roteador NON-IPX (rACLs)O rACLs não-IP aplica-se a todos os motores do supervisor. O rACLs NON-IPX aplica-se ao Supervisor Engine 1A com PFC e ao Supervisor Engine 2 com PFC2 somente.
- Tráfego de broadcast que é negado em um RACL
- Trafique que é negado em uma verificação do unicast RPF (o uRPF), ACL ACEEsta verificação do uRPF aplica-se ao Supervisor Engine 2 com PFC2 e ao Supervisor Engine 720 com PFC3.
- Proxy de autenticaçãoTrafique que é sujeito ao Proxy de autenticação pode ser limite de taxa no Supervisor Engine 720.
- Segurança IP do Cisco IOS Software (IPsec)Trafique que é sujeito ao Cisco IOS que a criptografia pode ser limite de taxa no Supervisor Engine 720.

Características Netflow-baseadas

As características Netflow-baseadas que esta seção descreve aplicam-se ao Supervisor Engine 2 e ao Supervisor Engine 720 somente.

- as características Netflow-baseadas precisam sempre de considerar o primeiro pacote de um fluxo no software. Uma vez que o primeiro pacote do fluxo alcança o software, os pacotes subsequente para o mesmo fluxo são comutados por hardware.Este arranjo do fluxo aplica-se aos ACLs reflexivo, ao Protocolo de Comunicação de Cache da Web (WCCP), e ao Cisco IOS Server Load Balancing (SLB).**Nota:** No Supervisor Engine 1, os ACLs reflexivo confiam em entradas de TCAM dinâmicas para criar atalhos de hardware para um fluxo particular. O princípio é o mesmo: o primeiro pacote de um fluxo vai ao software. Os pacotes subsequente para esse fluxo são comutados por hardware.
- Com os recursos de interceptação de TCP, o fim do cumprimento de três vias e da sessão é segurado no software. O resto do tráfego é segurado no hardware.**Nota:** O sincronizar (SYN), SYN reconhece (SYN ACK), e os pacotes de ACK compreendem o cumprimento de três vias. O fim da sessão ocorre com revestimento (FIN) ou restauração (RST).

- Com Network Address Translation (NAT), o tráfego é segurado desta maneira:No Supervisor Engine 720:Trafique que exige o NAT é segurado no hardware após a tradução inicial. A tradução do primeiro pacote de um fluxo ocorre no software, e os pacotes subsequente para esse fluxo são comutados por hardware. Para pacotes de TCP, um atalho de hardware é criado na tabela do Netflow após conclusão do cumprimento de três vias TCP.No Supervisor Engine 2 e no Supervisor Engine 1:Todo o tráfego que exige o NAT é comutado por software.
- O Context-Based Access Control (CBAC) usa atalhos do Netflow a fim classificar o tráfego que exige a inspeção. Então, o CBAC envia somente este tráfego ao software. O CBAC é uma característica somente software; trafique que é sujeito à inspeção não é comutado por hardware.**Nota:** Trafique que é sujeito à inspeção pode ser limite de taxa no Supervisor Engine 720.

Tráfego multicast

- Espião da transmissão múltipla independente de protocolo (PIM)
- Verificação do Protocolo de Gerenciamento do Grupo da Internet (IGMP) (TTL=1)Este tráfego é destinado certamente ao roteador.
- Espião da descoberta do ouvinte do Multicast (MLD) (TTL=1)Este tráfego é destinado certamente ao roteador.
- MENTIR a falta
- Pacotes de transmissão múltipla para o registo que têm a conexão direta ao origem de transmissão múltiplaEstes pacotes de transmissão múltipla são escavados um túnel ao ponto de reunião.
- Multicast do IP Versão 6 (IPv6)

Outros recursos

- Network-Based Application Recognition (NBAR)
- Inspeção ARP, com CatOS somente
- Segurança de portas, com CatOS somente
- Espião DHCP

Situações do IPv6

- Pacotes com um cabeçalho de opção do salto a salto
- Os pacotes com o mesmo IPv6 do destino endereçam como aquele do Roteadores
- Pacotes que falham a verificação da aplicação do espaço
- Pacotes que excedem o MTU do link da saída
- Pacotes com um TTL que seja inferior ou igual a 1
- Pacotes com uma entrada VLAN que iguale a saída VLAN
- URPF do IPv6O software executa este uRPF para todos os pacotes.
- ACLs reflexivo do IPv6O software segura estes ACLs reflexivo.
- os prefixos 6to4 para o protocolo do endereçamento do túnel automático do Intra-local do IPv6 (ISATAP) escavam um túnelO software segura este Tunelamento. Todo tráfego restante que incorpora um túnel ISATAP é comutado por hardware.

LCP Schedular e módulo de DFC

Em um Distributed Forwarding Card (DFC), o processo `schedular do lcp` que é executado em uma alta utilização da CPU não é uma edição e não levanta nenhum problema à operação. O LCP schedular é parte do código do firmware. Em todos os módulos que não exigem um DFC, o firmware é executado em um processador específico chamado o processador da placa de linha (LCP). Este processador é usado para programar o hardware ASIC e para comunicar-se ao módulo do supervisor central.

Quando o `lcp schedular` é iniciado, utiliza todo o período disponível do processo. Mas quando um processo novo precisa o tempo do processador, o `lcp schedular` livra acima o tempo do processo para o processo novo. Não há nenhum impacto ao desempenho do sistema no que diz respeito a esta utilização elevada da CPU. O processo agarra simplesmente todos os ciclos de CPU não utilizados, enquanto nenhum processo mais prioritário os exige.

```
DFC#show process cpuPID  Runtime(ms)  Invoked  uSecs    5Sec   1Min   5Min TTY Process  22
0         1      0   0.00%  0.00%  0.00%   0 SCP ChilisLC Lis   23           0         1      0
0.00%  0.00%  0.00%   0 IPC RTTYC Messag   24           0         9      0   0.00%  0.00%  0.00%
0 ICC Slave LC Req   25           0         1      0   0.00%  0.00%  0.00%   0 ICC Async mcast
26           0         2      0   0.00%  0.00%  0.00%   0 RPC Sync           27           0
1      0   0.00%  0.00%  0.00%   0 RPC rpc-master     28           0         1      0   0.00%
0.00%  0.00%   0 Net Input          29           0         2      0   0.00%  0.00%  0.00%   0
Protocol Filteri   30           8       105     76   0.00%  0.00%  0.00%   0 Remote Console P
31          40      1530     26   0.00%  0.00%  0.00%   0 L2 Control Task    32          72
986     73   0.00%  0.02%  0.00%   0 L2 Aging Task      33           4         21    190   0.00%
0.00%  0.00%   0 L3 Control Task    34          12        652     18   0.00%  0.00%  0.00%   0
FIB Control Task   35        9148       165  55442   1.22%  1.22%  1.15%   0 Statistics Task
36           4       413      9   0.00%  0.00%  0.00%   0 PFIB Table Manag   37      655016
64690036     10  75.33% 77.87% 71.10%   0 lcp schedular      38           0       762      0
0.00%  0.00%  0.00%   0 Constellation SP
```

Causas comum e soluções para edições da utilização elevada da CPU

Inalcançáveis IP

Quando um grupo de acesso nega um pacote, o MSFC envia mensagens que não chega a seu destino do ICMP. Esta ação ocorre à revelia.

Com a habilitação do padrão do **comando ip unreachables**, as gotas do Supervisor Engine mais dos pacotes negados no hardware. Então, o Supervisor Engine envia somente um pequeno número de pacotes, um máximo de 10 pps, ao MSFC para a gota. Esta ação gera mensagens que não chega a seu destino do ICMP.

A gota de pacotes e da geração negados de mensagens que não chega a seu destino do ICMP impõe uma carga no MSFC CPU. A fim eliminar a carga, você pode emitir o comando interface configuration do **no ip unreachables**. Este comando desabilita mensagens que não chega a seu destino do ICMP, que permite a gota no hardware de todo o acesso grupo-negado pacotes.

Os mensagens que não chega a seu destino do ICMP não são enviados se um VACL nega um pacote.

Traduções NAT

O NAT utiliza ambo a transmissão do hardware e software. O estabelecimento inicial dos tranlsations NAT deve ser feito no software e uma transmissão mais adicional é feita com

hardware. O NAT igualmente utiliza a tabela do Netflow (máximo 128 KB). Consequentemente, se a tabela do Netflow está completa, o interruptor igualmente começará aplicar a transmissão NAT através do software. Isto normalmente acontece com explosões do tráfego elevado e causará um aumento no CPU de 6500.

Uso do espaço da tabela FIB CEF na tabela de cache do fluxo

O Supervisor Engine 1 tem uma tabela de cache do fluxo que apoie 128,000 entradas. Contudo, com base na eficiência do algoritmo de hashing, estas entradas variam de 32,000 a 120,000. No Supervisor Engine 2, a tabela FIB é gerada e programada no PFC. A tabela guarda tanto como como 256,000 entradas. O Supervisor Engine 720 com PFC3-BXL apoia até 1,000,000 entradas. Uma vez que este espaço é excedido, os pacotes tornam-se comutados no software. Isto pode causar a utilização elevada da CPU no RP. A fim verificar o número de rotas na tabela FIB CEF, use estes comandos:

```
Router#show processes cpuCPU utilization for five seconds:  99.26%                    one
minute: 100.00%                   five minutes: 100.00%PID Runtime(ms) Invoked    uSecs    5Sec
1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- --- -----
----------1   0           0          0          0.74%   0.00%   0.00% -2  Kernel and Idle2   2
245        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0           1          0
0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0          0.00%   0.00%
0.00% -2  L2L3PatchRev   5   653         11737      1000       0.00%   0.00%   0.00% -2  SynDi!-
-- Output is suppressed.26 10576 615970 1000 0.00% 0.00% 0.00% 0 L3Aging 27 47432 51696 8000
0.02% 0.00% 0.00% 0 NetFlow 28 6758259 1060831 501000 96.62% 96.00% 96.00% 0   Fib            29
0           1          0          0.00%   0.00%   0.00% -2  Fib_bg_task  !--- Output is
suppressed.CATOS% show mls cefTotal L3 packets switched:           124893998234Total L3 octets
switched:          530193789624 95Total route entries:                       112579  IP route
entries:                          112578  IPX route entries:                            1  IPM
route entries:                              0IP load sharing entries:                    295IPX
load sharing entries:                         0Forwarding entries:
112521Bridge entries:                                  56Drop entries:
2IOS% show ip cef summaryIP Distributed CEF with switching (Table Version 86771423), flags=0x0
112564 routes, 1 reresolve, 0 unresolved (0 old, 0 new)  112567 leaves, 6888 nodes, 21156688
bytes, 86771426inserts, 86658859invalidations  295 load sharing elements, 96760 bytes, 112359
references  universal per-destination load sharing algorithm, id 8ADDA64A  2 CEF resets, 2306608
revisions of existing leaves  refcounts:  1981829 leaf, 1763584 node!--- You see these messages
if the TCAM space is exceeded:%MLSCEF-SP-7-FIB_EXCEPTION: FIB TCAM exception, Some entries will
be software switched%MLSCEF-SP-7-END_FIB_EXCEPTION: FIB TCAM exception cleared, all CEF entries
will be hardware switched
```

No Supervisor Engine 2, o número de entradas FIB reduz-se à metade se você configurou a verificação RPF nas relações. Esta configuração pode conduzir ao switch de software de mais pacotes e, consequentemente, utilização elevada da CPU.

A fim resolver a edição da utilização elevada da CPU, permita a sumarização de rota. A sumarização de rota pode minimizar a latência em uma rede complexo reduzindo cargas de trabalho do processador, requisitos de memória, e procura da largura de banda.

Refira a compreensão do ACL em Catalyst 6500 Series Switch para obter informações adicionais sobre da utilização de TCAM e da otimização.

Logging ACL aperfeiçoado

O logging ACL aperfeiçoado (OAL) fornece o suporte a hardware para o logging ACL. A menos que você configurar o OAL, o processo de pacotes que exigem o registo ocorre completamente no software no MSFC3. Licenças OAL ou pacotes das gotas no hardware no PFC3. O OAL usa uma rotina aperfeiçoada para enviar a informação ao MSFC3 a fim gerar os mensagens de

registro.

Nota: Para obter informações sobre do OAL, refira o *logging ACL aperfeiçoado com uma* seção *PFC3* compreendendo do apoio do Cisco IOS ACL.

Limite de taxa dos pacotes ao CPU

No Supervisor Engine 720, os limitadores da taxa podem controlar a taxa em que os pacotes podem ir ao software. Este controle de taxa ajuda a impedir ataques de recusa de serviço. Você pode igualmente usar alguns destes limitadores da taxa no Supervisor Engine 2:

```
Router#show mls rate-limit   Rate Limiter Type       Status     Packets/s   Burst--------------
------   ----------   ---------   -----         MCAST NON RPF   Off                  -       -
MCAST DFLT ADJ   On              100000     100      MCAST DIRECT CON   Off                  -
-        ACL BRIDGED IN   Off                  -       -       ACL BRIDGED OUT   Off
-       -           IP FEATURES   Off                  -       -          ACL VACL LOG   On
2000       1           CEF RECEIVE   Off                  -       -             CEF GLEAN   Off
-       -      MCAST PARTIAL SC   On              100000     100        IP RPF FAILURE   On
500      10           TTL FAILURE   Off                  -       -ICMP UNREAC. NO-ROUTE   On
500      10ICMP UNREAC. ACL-DROP   On                 500      10         ICMP REDIRECT   Off
-       -           MTU FAILURE   Off                  -       -           LAYER_2 PDU   Off
-       -            LAYER_2 PT   Off                  -       -             IP ERRORS   On
500      10           CAPTURE PKT   Off                  -       -            MCAST IGMP   Off
-       -Router(config)#mls rate-limit ?  all        Rate Limiting for both Unicast and
Multicast packets  layer2     layer2 protocol cases  multicast  Rate limiting for Multicast
packets  unicast    Rate limiting for Unicast packets
```

Aqui está um exemplo:

```
Router(config)#mls rate-limit layer2 l2pt 3000
```

O taxa-limite todos os pacotes CEF-punted ao MSFC, emite o comando que está neste exemplo:

```
Router(config)#mls ip cef rate-limit 50000
```

A fim reduzir o número de pacotes punted ao CPU devido ao TTL=1, emita este comando:

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

Por exemplo, esta é a saída da **captação do netdr**, que mostra que o IPv4 TTL é 1:

```
Router(config)#mls rate-limit all ttl-failure 15!--- where 15 is the number of packets per
second with TTL=1. !--- The valid range is from 10 to 1000000 pps.
```

A alta utilização da CPU pode igualmente ser devido aos pacotes com TTL=1 que são escapados ao CPU. A fim limitar o número de pacotes que são escapados ao CPU, configurar um limitador da taxa do hardware. Os limitadores da taxa podem os pacotes do taxa-limite que são escapados do trajeto de dados de hardware até o trajeto de dados do software. Os limitadores da taxa protegem o trajeto do controle de software da congestão deixando cair o tráfego que excede a taxa configurada. O limite de taxa é configurado usando o taxa-**limite dos mls todo o** comando da TTL-**falha**.

Fusão física dos VLAN devido ao cabeamento incorreto

A utilização elevada da CPU igualmente pode resultar da fusão junto de dois ou mais VLAN devido à expedição de cabogramas imprópria. Também, se o STP é desabilitado naquelas portas onde o combinador de VLAN acontece, a utilização elevada da CPU pode ocorrer.

A fim resolver este problema, identifique os erros de expedição de cabogramas e corrija-os. Se

sua exigência reserva, você pode igualmente permitir o STP naquelas portas.

Tempestade de transmissão

Uma tempestade de transmissão LAN ocorre quando a transmissão ou os pacotes de transmissão múltipla inundam o LAN, que cria o tráfego excessivo e degrada o desempenho da rede. Os erros na aplicação do protocol stack ou na configuração de rede podem causar uma tempestade de transmissão.

Devido à concepção arquitetónica da plataforma do Catalyst 6500 Series, os pacotes de transmissão são deixados cair somente e sempre a nível de software.

A supressão de transmissão impede o rompimento das interfaces de LAN por uma tempestade de transmissão. A supressão de transmissão usa a filtração dessas medidas da atividade de transmissão em um LAN durante um período de tempo 1-second e compara a medida com um limiar pré-definido. Se o ponto inicial é alcançado, uma atividade de transmissão mais adicional está suprimida para a duração de um período especificado. A supressão de transmissão é desabilitada à revelia.

Nota: O flapping VRRP do backup a dominar causado por tempestades de transmissão pôde causar a utilização elevada da CPU.

A fim compreender como a supressão de transmissão dos trabalhos e para permitir a característica, refere:

- Configurando a supressão de transmissão (software do sistema do Cisco IOS)
- Configurando a supressão de transmissão (software do sistema de CatOS)

Seguimento do endereço de próximo salto BGP (processo do scanner de BGP)

O processo do scanner de BGP anda a tabela de BGP e confirma a alcançabilidade dos saltos seguintes. Este processo igualmente verifica o anúncio condicional a fim determinar se o BGP deve anunciar prefixos de condição e/ou executar o retardar da rota. À revelia, o processo faz a varredura de cada 60 segundos.

Você pode esperar durações da utilização elevada da CPU para breve devido ao processo do scanner de BGP em um roteador que leve uma grande tabela de roteamento da Internet. Uma vez pelo minuto, o scanner de BGP anda a tabela da base de informação de roteamento de BGP (RIB) e executa tarefas de manutenção importantes. Estas tarefas incluem:

- Uma verificação do salto seguinte que é provido na tabela do roteador BGP
- Verificação que os dispositivos de próximo salto podem ser alcançados

Portanto, uma ampla tabela de BGP demora um bom tempo para ser examinada e validada. O processo do scanner de BGP anda a tabela de BGP a fim atualizar todas as estruturas de dados e anda a tabela de roteamento para finalidades da redistribuição de rota. Ambas as tabelas são armazenadas separadamente na memória de roteador. Ambas as tabelas podem ser muito grandes e, assim, consumir ciclos de CPU.

Para obter mais informações sobre da utilização CPU pelo processo do scanner de BGP, refira a *alta utilização da CPU devido à* seção do *scanner de BGP da* alta utilização da CPU do Troubleshooting causada pelo scanner de BGP ou pelo processo de roteador BGP.

Para obter mais informações sobre dos recursos de tracking do endereço de próximo salto BGP e do procedimento a permitir/desabilite ou ajuste o intervalo da varredura, referem o suporte do BGP para o seguimento do endereço de próximo salto.

Tráfego multicast NON-RPF

O roteamento de transmissão múltipla (ao contrário do roteamento do unicast) é estado relacionado somente com a fonte de um córrego de dados de transmissão múltipla dado. Isto é, o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo que origina o tráfego multicast. O princípio básico é que o dispositivo de origem “empurra” o córrego para fora para um número indeterminado de receptores (dentro de seu grupo de transmissão múltipla). Todos os Multicast Router criam as árvores de distribuição, que controlam o trajeto que o tráfego multicast toma através da rede a fim entregar o tráfego a todos os receptores. Os dois tipos básicos de árvores de distribuição do Multicast são árvores e árvores compartilhadas da fonte. O RPF é um conceito chave no Multicast Forwarding. Permite o tráfego multicast do Roteadores corretamente para a frente abaixo da árvore de distribuição. O RPF utiliza a tabela de roteamento unicast existente para determinar os vizinhos de fluxo acima e fluxo abaixo. Um roteador para a frente um pacote de transmissão múltipla somente se é recebido na relação ascendente. Esta verificação RPF ajuda a garantir que a árvore de distribuição é sem loop.

O tráfego multicast é sempre visível por cada roteador (camada 2) em um LAN construído uma ponte sobre, de acordo com a especificação da IEEE 802.3 CSMA/CD. Nos 802.3 padrão, o bit 0 do primeiro octeto é usado para indicar uma transmissão e/ou um frame de transmissão múltipla, e todo o quadro da camada 2 com este endereço é inundado. Este é igualmente o caso mesmo se o CGMP ou o IGMP Snooping são configurados. Isto é porque os Multicast Router devem ver o tráfego multicast, se são esperados fazer uma decisão de encaminhamento apropriada. Se múltiplo os Multicast Router cada um têm relações em um LAN comum, então somente um roteador para a frente os dados (escolhidos por um processo de eleição). Devido à natureza da inundação dos LAN, o roteador redundante (roteador que não envia o tráfego multicast) recebe estes dados na interface externa para esse LAN. O roteador redundante deixa cair normalmente este tráfego, porque chegou na interface errada e falha consequentemente a verificação RPF. Este tráfego que falha a verificação RPF é chamado tráfego não-RPF ou pacotes da falha de RPF, porque foram transmitidos para trás contra o fluxo da fonte.

O Catalyst 6500 com um MSFC instalado, pode ser configurado para atuar como o Multicast Router desenvolvido. Utilizando o interruptor da Multi-camada do Multicast (MMLS), o tráfego RPF é enviado geralmente pelo hardware dentro do interruptor. Os ASIC são dados a informação do estado do roteamento de transmissão múltipla (por exemplo, (*, G) e (S, G)), de modo que um atalho de hardware possa ser programado no Netflow e/ou na tabela FIB. Este tráfego não-RPF é ainda necessário em alguns casos, e é exigido pelo MSFC CPU (a nível de processo) para o PIM afirma o mecanismo. Se não, é deixado cair então pelo caminho de switching rápido do software (a suposição é que o switching rápido do software não está desabilitado na relação RPF).

O Catalyst 6500 que usa a Redundância não pôde segurar o tráfego não-RPF eficientemente em determinadas topologias. Para o tráfego não-RPF, há geralmente nenhum (*, G) ou (S, G) estado no roteador redundante, e consequentemente nenhuns hardware ou atalhos de software pode ser criado para deixar cair o pacote. Cada pacote de transmissão múltipla deve ser examinado pelo processador de rotas MSFC individualmente, e este é referido frequentemente enquanto tráfego da interrupção CPU. Com switching de hardware da camada 3 e interfaces múltiplas/VLAN que conectam o mesmo conjunto de roteador, o tráfego não-RPF que bate o CPU do MSFC redundante é “N amplificado” cronometra a taxa da fonte original (onde “N” é o número de LAN a que o roteador é conectado redundantemente). Se a taxa do tráfego não-RPF excede a

capacidade deixando cair do pacote do sistema, a seguir pôde causar a utilização elevada da CPU, os excessos de buffer e a instabilidade de rede total.

Com o Catalyst 6500, há um motor da lista de acessos que permita a filtração a ocorrer na taxa do fio. Esta característica pode ser usada para segurar eficientemente o tráfego não-RPF para grupos de modo escassos, em determinadas situações. Você pode somente usar o método ACL-baseado dentro redes stub do modo escasso as “, onde não há nenhum Multicast Router a jusante (e receptores correspondentes). Adicionalmente, devido ao projeto do encaminhamento de pacote do Catalyst 6500, os MSFC internamente redundantes não podem usar esta aplicação. Isto é esboçado dentro da identificação de bug Cisco CSCdr74908 (clientes registrados somente). Para grupos do modo denso, os pacotes NON-RPF devem ser vistos no roteador para o PIM afirmam o mecanismo para funcionar corretamente. As soluções diferentes, tais como o CEF ou a taxa limite e QoS baseados Netflow são usadas para controlar falhas de RPF em redes do modo denso e em redes do trânsito do modo escasso.

No Catalyst 6500 há um motor da lista de acessos que permita a filtração a ocorrer na taxa do fio. Esse recurso pode ser usado para controlar o tráfego não-RPF para grupos de modos esparsos eficientemente. A fim executar esta solução, coloque uma lista de acessos na interface de entrada da “rede stub” para filtrar o tráfego multicast que não originou da “rede stub”. A lista de acessos é abaixada para o hardware no interruptor. Esta lista de acessos impede o CPU considere nunca o pacote e permite que o hardware deixe cair o tráfego não-RPF.

Nota: Não coloque esta lista de acessos em uma relação do trânsito. Pretende-se somente para as redes stub (redes com anfitriões somente).

Consulte estes documentos para obter outras informações:

- Edições do roteador redundante com o Protocolo IP multicast nas redes stub
- Processamento do tráfego não-RPF

comandos show

A utilização CPU quando você emite um **comando show** é sempre quase 100%. É normal ter a utilização elevada da CPU quando você emite um **comando show** e permanece normalmente por somente alguns segundos.

Por exemplo, é normal para o processo de EXEC virtual ir altamente quando você emite um **comando show tech-support** porque esta saída é uma saída conduzida interrupção. Seu somente interesse que tem a alta utilização da CPU em outros processos diferentes dos **comandos show**.

O comando show cef not-cef-switched mostra porque os pacotes punted ao MSFC (receba, opção IP, nenhuma adjacência, etc.) e quanto. Por exemplo:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Os comandos show que do **resumo do ibc da mostra** e do **ibc da mostra o** CPU se enfileira e se pode ser usado quando você monitorar o estado CPU.

Processos do executivo

O processo do executivo no Cisco IOS Software é responsável para uma comunicação nas linhas TTY (console, auxiliar, assíncronos) do roteador. O processo Virtual Exec é responsável pelas linhas de vty (sessões de telnet). O executivo e os processos de EXEC virtuais são processos da prioridade média, assim que se há outros processos que têm uma prioridade mais alta (alta ou crítica), os processos mais prioritários obtêm os recursos do CPU.

Se há muitos dados transferidos com estas sessões, a utilização CPU para o processo do executivo aumenta. Isto é porque quando o roteador quer enviar um caractere simples através destas linhas, o roteador usa alguns recursos do CPU:

- Para o console (executivo), o roteador usa uma interrupção pelo caráter.
- Para a linha VTY (EXEC virtual), a sessão de Telnet tem que construir um pacote de TCP pelo caráter.

Esta lista detalha algumas das razões possíveis para a utilização elevada da CPU no processo do executivo:

- **Há demasiados dados enviados através da porta de Console.**Verifique para ver se algum debuga foi começado no roteador com o comando show debugging.Desabilite o console que entra o roteador com **nenhum** formulário do comando logging console.Verifique se umas saídas longas são imprimidas no console. Por exemplo, um tecnologia-apoio da mostra ou um comando show memory.
- O comando exec **é configurado para linhas assíncronas e auxiliares.**Se uma linha tem somente o tráfego de saída, desabilite o processo do executivo para esta linha. Isto é porque se o dispositivo (por exemplo, um modem) anexado a esta linha envia alguns dados não solicitados, o processo do executivo começa nesta linha.Se o roteador está usado como um servidor terminal (para o telnet reverso aos consoles do outro dispositivo), recomenda-se que você configura o **comando no exec nas** linhas que são conectadas ao console dos outros dispositivos. Os dados que voltam do console puderam de outra maneira começar um processo do executivo, que usasse recursos do CPU.

Uma razão possível para a utilização elevada da CPU no processo de EXEC virtual é:

- **Há demasiados dados enviados através das sessões de Telnet.**A maioria de motivo comum para a utilização elevada da CPU no processo de EXEC virtual é que demasiados dados estão transferidos do roteador à sessão de Telnet. Isto pode acontecer quando os comandos com saídas longas tais como o tecnologia-**apoio da mostra**, **memória da mostra**, são executados e assim por diante da sessão de Telnet. A quantidade de dados transferidos através de cada sessão de VTY pode ser verificada com o comando **vty do** *number> do <line* **tcp da mostra**.

Processo de envelhecimento L3

Quando o processo de envelhecimento L3 exporta um grande número *ifindex* avalia usar a exportação de dados de Netflow (NDE), o USO de CPU pôde bater 100%.

Se você encontra este problema, verifique se estes dois comandos estejam permitidos:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
```

```
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Se você permite estes comandos, o processo deve exportar todos os valores do ifindex do destino e da fonte usando o NDE. A utilização do processo de envelhecimento L3 vai altamente desde que deve executar MENTE a consulta para todos os valores do *ifindex do* destino e da fonte. Devido a isto, a tabela torna-se completamente, o processo de envelhecimento L3 vai altamente, e o USO de CPU bate 100%.

A fim resolver esta edição, desabilite estes comandos:

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0Switch#show cef not-cef-switchedCEF Packets passed on to next switching
layerSlot  No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222
0         136        0    60122        0        0        05          0       0           0
0        0        0        0        0IPv6 CEF Packets passed on to next switching layerSlot
No_adj No_encap Unsupp'ted Redirect  Receive  Options   Access      MTURP         0       0
0        0        0        0        0        0
```

Use estes comandos verificar os valores:

- mostre o sumário do cef dos mls
- mostre máximo-rotas do cef dos mls

Tempestade BPDU

Medida - a árvore mantém um ambiente sem loop da camada 2 na comutada redundante e constrói uma ponte sobre redes. Sem STP, os quadros dão laços e/ou multiplicam indefinidamente. Esta ocorrência causa uma sobrecarga de rede porque o tráfego elevado interrompe todos os dispositivos no domínio de transmissão.

Em alguns aspectos, o STP é um protocolo adiantado que seja desenvolvido inicialmente para especificações com base no software lentas da ponte (IEEE 802.1D), mas o STP pode ser complicado a fim executá-lo com sucesso nas grandes redes comutadas que têm estas características:

- Muitos VLAN
- Muito Switches em um domínio de STP
- apoio do Multi-vendedor
- Aprimoramentos de IEEE mais novos

Se a rede enfrenta a medida frequente os cálculos da árvore ou o interruptor têm que processar mais BPDU, pode conduzir à alta utilização da CPU, assim como o BPDU deixa cair.

A fim trabalhar em torno destas edições, execute algumas ou todas estas etapas:

1. Pode fora dos VLAN do Switches.
2. Use uma versão aprimorada do STP, tal como o MST.

3. Promova o hardware do interruptor.

Igualmente refira melhores prática executar o Spanning Tree Protocol na rede.

- Melhores prática para o catalizador 4500/4000, 5500/5000 de, e o Switches do 6500/6000 Series que executa a configuração e o Gerenciamento de CatOS
- Melhores prática para Switches do 4500/4000 Series da série e do catalizador do Catalyst 6500/6000 que executa o Cisco IOS Software

Sessões span

Baseado na arquitetura de Series Switch do Catalyst 6000/6500, as sessões span não afetam o desempenho do interruptor, mas, se a sessão span inclui um tráfego elevado/porta de uplink ou um EtherChannel, pode aumentar a carga no processador. Se escolhe então um VLAN específico, aumenta a carga de trabalho ainda mais. Se há um tráfego ruim no link, aquele pode um aumento mais ulterior a carga de trabalho.

Em algumas encenações, a característica RSPAN pode causar laços, e a carga nos tiros do processador acima. Para mais informação, refira porque faz a sessão span criam um Loop de Bridging?

O interruptor pode passar o tráfego como de costume desde que tudo está no hardware, mas o CPU pode tomar uma batida se tenta figurar para fora que traficam para enviar completamente. Recomenda-se que você configura sessões span somente quando se exige.

%CFIB-SP-STBY-7-CFIB_EXCEPTION: MENTIR a exceção TCAM, algumas entradas será software comutado

```
Switch#show cef not-cef-switchedCEF Packets passed on to next switching layerSlot  No_adj
No_encap Unsupp'ted Redirect  Receive  Options   Access     FragRP      6222       0         136
0    60122        0        0        05          0       0           0        0        0        0
0        0IPv6 CEF Packets passed on to next switching layerSlot  No_adj No_encap Unsupp'ted
Redirect  Receive  Options   Access      MTURP         0       0           0        0        0
0        0        0
```

Este Mensagem de Erro é recebido quando a quantidade do espaço disponível no TCAM é excedida. Isto conduz à alta utilização da CPU. Esta é uma limitação MENTIR TCAM. Uma vez que o TCAM está completo, uma bandeira estará ajustada e MENTIR a exceção TCAM é recebido. Isto para de adicionar rotas novas ao TCAM. Consequentemente, tudo será software comutado. A remoção das rotas não ajuda a recomeçar o switching de hardware. Uma vez que o TCAM incorpora o estado da exceção, o sistema deve ser recarregado para sair desse estado. As rotas do máximo que podem ser instaladas no TCAM são aumentadas pelo **comando maximum routes do cef dos mls**.

O Catalyst 6500/6000 que é executado com alta utilização da CPU tem um IPv6 ACL com portas L4

Permita o **unicast do endereço da compressa acl do IPv6 dos mls**. Este comando é precisado se o IPv6 ACL está combinando em números de porta do protocolo L4. Se este comando não é permitido, o tráfego do IPv6 punted ao CPU para o processamento do software. Este comando não é configurado à revelia.

Cobre SPF

Em Cisco EU Switch Ethernet do 6500 Series, o cobre SFP exige mais interação do firmware do que outros tipos de SFP, que aumenta a utilização CPU.

Os algoritmos de software que controlam os SFP de cobre foram melhorados nas liberações do Cisco IOS SXH.

IO modulares

Nos Cisco Catalyst 6500 Series Switch que executam o IOS Software modular, a utilização CPU normal é um IOS Software pouco maior do que NON-modular.

O IOS Software modular paga um preço pela atividade mais do que paga um preço pelo pacote. O IOS Software modular mantém os processos consumindo determinado CPU mesmo se não há nenhum muito pacotes, assim que o consumo de CPU não é baseado no tráfego real. Contudo, quando os pacotes processado vão taxa alta, o CPU consumido no IOS Software modular não deve ser mais do que aquele no IOS Software NON-modular.

Verifique a utilização CPU

Se a utilização CPU é alta, emita o **comando show processes cpu** primeiramente. A saída mostra-lhe a utilização CPU no interruptor assim como o consumo de CPU por cada processo.

```
Router#show processes cpu CPU utilization for five seconds: 57%/48%; one minute: 56%; five
minutes: 48% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    1
0         5          0  0.00%  0.00%  0.00%   0 Chunk Manager       2          12     18062
0  0.00%  0.00%  0.00%   0 Load Meter          4      164532     13717      11994  0.00%  0.21%
0.17%   0 Check heaps         5          0         1          0  0.00%  0.00%  0.00%   0 Pool
Manager     !--- Output is suppressed. 172 0 9 0 0.00% 0.00% 0.00% 0 RPC aapi_rp 173      243912
2171455        112  9.25%  8.11%  7.39%   0 SNMP ENGINE       174          68       463
146  0.00%  0.00%  0.00%   0 RPC pm-mp  !--- Output is suppressed.
```

Nesta saída, a utilização total de CPU é 57 por cento e a utilização CPU da interrupção é 48 por cento. Aqui, estas porcentagens aparecem no texto em negrito. O interruptor de interrupção do tráfego pelo CPU causa a utilização CPU da interrupção. O comando output lista os processos que causam a diferença entre as duas utilizações. Neste caso, a causa é o processo SNMP.

No Supervisor Engine que executa CatOS, a saída olha como esta:

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

Nesta saída, o primeiro processo é `núcleo e quietude`, que mostra a utilização CPU inativa. Este processo é normalmente alto, a menos que alguns outros processos consumirem ciclos de CPU. Neste exemplo, o processo de `SptBpduRx` causa a utilização elevada da CPU.

Se a utilização CPU é alta devido a um destes processos, você pode pesquisar defeitos e determinar porque este processo é executado altamente. Mas, se o CPU é alta devido traficar ser punted ao CPU, você precisa de determinar porque o tráfego punted. Esta determinação pode ajudá-lo a identificar o que o tráfego é.

Para pesquisar defeitos, use este exemplo de script EEM a fim recolher a saída do interruptor quando você experimenta a utilização elevada da CPU:

```
Switch> (enable) show processes cpuCPU utilization for five seconds:  99.72%
one minute: 100.00%                    five minutes: 100.00%PID Runtime(ms) Invoked    uSecs
5Sec    1Min    5Min    TTY Process--- ----------- ---------- -------- ------- ------- ------- -
-- ---------------1   0           0          0          0.28%   0.00%   0.00% -2  Kernel and
Idle2   2           261        1000       0.00%   0.00%   0.00% -2  Flash MIB Updat3   0
1          0          0.00%   0.00%   0.00% -2  L2L3IntHdlr    4   0           1          0
0.00%   0.00%   0.00% -2  L2L3PatchRev   !--- Output is suppressed.61 727295 172025 18000 0.82%
0.00% 0.00% -2 SptTimer 62  18185410    3712736    106000    22.22%  21.84%  21.96% -2
SptBpduRx      63  845683      91691      105000     0.92%   0.00%   0.00% -2  SptBpduTx
```

Nota: O comando da **captação RX do netdr debugar** é útil quando o CPU é alta devido processar o interruptor dos pacotes em vez do hardware. Captura 4096 pacotes entrantes ao CPU quando o comando é executado. O comando é completamente seguro e é a ferramenta a mais conveniente para edições da alta utilização da CPU nos 6500. Não causa a carga extra ao CPU.

Utilidades e ferramentas para determinar o tráfego que Punted ao CPU

Esta seção identifica algumas utilidades e ferramentas que podem o ajudar a olhar este tráfego.

Software do sistema Cisco IOS

No Cisco IOS Software, o processador de switch no Supervisor Engine é referido como o SP, e o MSFC é chamado o RP.

O comando show interface dá a informação básica no estado da relação e a taxa de tráfego na relação. O comando igualmente fornece contadores de erros.

```
Router#show interface gigabitethernet 4/1GigabitEthernet4/1 is up, line protocol is up
(connected)  Hardware is C6k 1000Mb 802.3, address is 000a.42d1.7580 (bia 000a.42d1.7580)
Internet address is 100.100.100.2/24  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255  Encapsulation ARPA, loopback not set  Keepalive
set (10 sec)  Half-duplex, 100Mb/s  input flow-control is off, output flow-control is off  Clock
mode is auto  ARP type: ARPA, ARP Timeout 04:00:00  Last input 00:00:00, output 00:00:00, output
hang never  Last clearing of "show interface" counters never  Input queue: 5/75/1/24075
(size/max/drops/flushes); Total output drops: 2  Queueing strategy: fifo  Output queue: 0/40
(size/max)  30 second input rate 7609000 bits/sec, 14859 packets/sec  30 second output rate 0
bits/sec, 0 packets/sec  L2 Switched: ucast: 0 pkt, 184954624 bytes - mcast: 1 pkt, 500 bytes
L3 in Switched: ucast: 2889916 pkt, 0 bytes - mcast: 0 pkt, 0 bytes mcast  L3 out Switched:
ucast: 0 pkt, 0 bytes mcast: 0 pkt, 0 bytes     2982871 packets input, 190904816 bytes, 0 no
buffer     Received 9 broadcasts, 0 runts, 0 giants, 0 throttles     1 input errors, 1 CRC, 0
frame, 28 overrun, 0 ignored     0 input packets with dribble condition detected     1256
packets output, 124317 bytes, 0 underruns     2 output errors, 1 collisions, 2 interface resets
0 babbles, 0 late collision, 0 deferred     0 lost carrier, 0 no carrier     0 output buffer
failures, 0 output buffers swapped out
```

Nesta saída, você pode ver que o tráfego de entrada é a camada 3-switched em vez da camada 2-switched. Isto indica que o tráfego punted ao CPU.

O comando show processes cpu diz-lhe se estes pacotes são pacotes ou pacotes de controle do tráfego regular.

```
Router#show processes cpu | exclude 0.00              CPU utilization for five seconds: 91%/50%;
one minute: 89%; five minutes: 47% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY
Process   5      881160     79142      11133  0.49%  0.19%  0.16%   0 Check heaps       98
```

```
121064   3020704         40 40.53% 38.67% 20.59%   0 IP Input          245      209336    894828
233  0.08%  0.05%  0.02%   0 IFCOM Msg Hdlr
```

Se os pacotes são comutados por processo, você vê que o `processo de entrada IP` é executado altamente. Emita este comando a fim ver estes pacotes:

mostre a interface de entrada dos bufferes

```
Router#show buffers input-interface gigabitethernet 4/1 packetBuffer information for Small
buffer at 0x437874D4  data_area 0x8060F04, refcount 1, next 0x5006D400, flags 0x280  linktype 7
(IP), enctype 1 (ARPA), encsize 14, rxtype 1  if_input 0x505BC20C (GigabitEthernet4/1),
if_output 0x0 (None)  inputtime 00:00:00.000 (elapsed never)  outputtime 00:00:00.000 (elapsed
never), oqnumber 65535  datagramstart 0x8060F7A, datagramsize 60, maximum size 308  mac_start
0x8060F7A, addr_start 0x8060F7A, info_start 0x0  network_start 0x8060F88, transport_start
0x8060F9C, caller_pc 0x403519B4  source: 100.100.100.1, destination: 100.100.100.2, id: 0x0000,
ttl: 63,  TOS: 0 prot: 17, source port 63, destination port 6308060F70:
000A 42D17580            ..BQu.08060F80: 00000000 11110800 4500002E 00000000
........E.......08060F90: 3F11EAF3 64646401 64646402 003F003F  ?.jsddd.ddd..?.?08060FA0:
001A261F 00010203 04050607 08090A0B  ..&.............08060FB0: 0C0D0E0F 101164
......d
```

Se o tráfego é **interrupção comutada**, você não pode ver aqueles pacotes com o **comando show buffers input-interface**. A fim ver os pacotes que punted ao RP para o switching de interrupção, você pode executar uma captação do Switched Port Analyzer (SPAN) da porta RP.

Nota: Refira este documento para obter informações adicionais sobre do interrupção-comutado contra a utilização CPU comutado por processo:

- *Utilização elevada da CPU devido à* seção das *interrupções da* utilização elevada da CPU do Troubleshooting em roteadores Cisco

PERÍODO RP-Inband e SP-Inband

UM PERÍODO para a porta RP ou SP no Cisco IOS Software está disponível no Cisco IOS Software Release 12.1(19)E e Mais Recente.

Esta é a sintaxe de comando:

```
test monitor session 1-66 add {rp-inband | sp-inband} [rx | tx | both]
```

Use esta sintaxe para o Cisco IOS Software 12.2 liberações SX:

```
test monitor add {1..66} {rp-inband | sp-inband} {rx | tx | both}
```

Nota: Para a liberação SXH, você deve usar o **comando monitor session** a fim configurar uma sessão do SPAN local, e usa então este comando associar a sessão span com o CPU:

```
source {cpu {rp | sp}} | single_interface | interface_list | interface_range |
mixed_interface_list | single_vlan | vlan_list | vlan_range | mixed_vlan_list} [rx | tx | both]
```

Nota: Para obter mais informações sobre destes comandos, refira configurar o SPAN local (modo da configuração de span) no *manual de configuração do software da liberação 12.2SX do Catalyst 6500*.

Está aqui um exemplo em um console RP:

```
Router#monitor session 1 source interface fast 3/3!--- Use any interface that is
administratively shut down.Router#monitor session 1 destination interface 3/2
```

Agora, vá ao console SP. Aqui está um exemplo:

```
Router-sp#test monitor session 1 add rp-inband rx
```

Nota: No Cisco IOS 12.2 liberações SX, o comando foram mudadas **para testar o monitor adicionam 1 RX RP-inband**.

```
Router#show monitor Session 1---------Type : Local SessionSource Ports :Both : Fa3/3Destination
Ports : Fa3/2SP console:Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1
Egress Source Ports: 3/3 Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans:
<empty>Destination Ports: 3/2
```

Nota: No Cisco IOS 12.2 liberações SX, o comando foram mudadas **para testar a mostra 1. do monitor.**

Está aqui um exemplo em um console SP:

```
Router-sp#test monitor session 1 showIngress Source Ports: 3/3 15/1 Egress Source Ports: 3/3
Ingress Source Vlans: <empty>Egress Source Vlans: <empty>Filter Vlans: <empty>Destination Ports:
3/2
```

Software do sistema de CatOS

Para o Switches que executa o software do sistema de CatOS, o Supervisor Engine executa CatOS e o MSFC executa o Cisco IOS Software.

Se você emite o **comando show mac**, você pode ver o número de quadros que punted ao MSFC. A porta 15/1 é a conexão do Supervisor Engine ao MSFC.

Nota: A porta é 16/1 para os motores do supervisor no entalhe 2.

```
Console> (enable) show mac 15/1Port     Rcv-Unicast          Rcv-Multicast        Rcv-Broadcast-
------- -------------------- -------------------- --------------------15/1
193576                    0                   1Port     Xmit-Unicast         Xmit-Multicast
Xmit-Broadcast-------- -------------------- -------------------- --------------------15/1
3                    0                    0Port     Rcv-Octet            Xmit-Octet-------- ----
---------------- --------------------15/1                 18583370                    0MAC
Dely-Exced MTU-Exced  In-Discard Out-Discard-------- ---------- ---------- ---------- ----------
-15/1              0          -          0           0
```

Um aumento rápido neste número indica que os pacotes punted ao MSFC, que causa a utilização elevada da CPU. Você pode então olhar os pacotes nestas maneiras:

- Porta 15/1 ou 16/1 do PERÍODO MSFC
- PERÍODO sc0

Porta 15/1 ou 16/1 do PERÍODO MSFC

Estabelecer uma sessão span em que a fonte é a porta 15/1 (ou 16/1) MSFC e o destino é uma porta Ethernet.

Aqui está um exemplo:

```
Console> (enable) set span 15/1 5/10Console> (enable) show spanDestination     : Port 5/10Admin
Source    : Port 15/1Oper Source     : NoneDirection       : transmit/receiveIncoming Packets:
disabledLearning        : enabledMulticast       : enabledFilter          : -Status          :
active
```

Se você recolhe um farejador de rastreamento na porta 5/10, o farejador de rastreamento mostra os pacotes que transmitem a e do MSFC. Configurar a sessão span como o **TX** a fim capturar os pacotes que são destinados somente ao MSFC, e não do MSFC.

MEÇA sc0

Estabelecer uma sessão span com a relação **sc0** como a fonte a fim capturar os quadros que vão ao CPU de Supervisor Engine.

```
Console> (enable) set span ?  disable                    Disable port monitoring  sc0
Set span on interface sc0  <mod/port>                 Source module and port numbers  <vlan>
Source VLAN numbers
```

Nota: Para os módulos Optical Services Modules (OS), você não pode executar uma captação do PERÍODO do tráfego.

Recomendações

A utilização do CPU de Supervisor Engine não reflete o desempenho do encaminhamento de hardware do interruptor. Ainda, você deve linha de base e para monitorar a utilização do CPU de Supervisor Engine.

1. Linha de base a utilização do CPU de Supervisor Engine para o interruptor em uma rede de estado estacionário com padrões de tráfego normais e carga.Note que processos geram a utilização CPU a mais alta.
2. Quando você pesquisa defeitos a utilização CPU, considere estas perguntas:Que processos geram a utilização mais elevada? São estes processos diferentes de sua linha de base?O CPU é elevado consistentemente, sobre a linha de base? Ou há uns pontos da utilização elevada, e então um retorno aos níveis de linha de base?Há as notificações da alteração de topologia (TCN) na rede?**Nota:** As portas não sincronizadas ou as portas de host com enfermos do STP portfast causam TCN.Há um broadcast excessivo ou um tráfego multicast no Gerenciamento subnets/VLAN?Há tráfego de gerenciamento excessivo, tal como o polling snmp, no interruptor?
3. Durante a alta utilização da CPU - o tempo (quando o CPU é 75% ou acima), recolhe a saída destes comandos:***show clock***show version**mostre o processador central dos processos classificadomostre a história processador central do procshow log**
4. Se possível, isole o VLAN de gerenciamento dos VLAN com tráfego de dados do usuário, particularmente tráfego de broadcast pesado.Os exemplos deste tipo de tráfego incluem o protocolo de propaganda IPX RIP/Service (SAP), o APPLETALK, e o outro tráfego de broadcast. Tal tráfego pode impactar a utilização do CPU de Supervisor Engine e, em casos extremos, pode interferir com a operação normal do interruptor.
5. Se o CPU executa alta devido ao pontapé do tráfego ao RP, determine o que esse tráfego é e porque o tráfego punted.A fim fazer esta determinação, use as utilidades que as utilidades e as ferramentas para determinar o tráfego que Punted à seção CPU descrevem.

Informações Relacionadas

- Comandos úteis para pesquisando defeitos a alta utilização da CPU no catalizador 6500's com Sup720
- Mensagens de erro comuns de CatOS em Switches da série Catalyst 6500 ou 6000
- Mensagens de erro comum no Catalyst 6500/6000 series switch que executa o Cisco IOS Software
- Troubleshooting de Falhas Comuns e de Hardware em Catalyst 6500/6000 Series Switches

Executando o Cisco IOS System Software

- Inundação de Unicast em Redes de Campus Comutadas
- Sustentação do produto dos Cisco Catalyst 6500 Series Switch
- O script EEM para recolher dados durante a alta utilização da CPU intermitente emite
- Suporte a Produtos de LAN
- Suporte de tecnologia de switching de LAN
- Suporte Técnico e Documentação - Cisco Systems