# Utilización del Switch del Catalyst 6500/6000 CPU elevada

## Contenido

# Introducción

Este documento describe las causas de la elevada utilización de la CPU en los switches Cisco Catalyst 6500/6000 Series y los sistemas basados en Virtual Switching System (VSS) 1440. Al igual que en los routers Cisco, los switches utilizan el comando **show processes cpu** a fin de mostrar el uso de la CPU para el procesador de Supervisor Engine del switch. Sin embargo, debido a las diferencias en arquitectura y mecanismos de reenvío entre los routers Cisco y los switches, la salida típica del comando **show processes cpu** difiere significativamente. El significado de la salida diferencia también. Este documento aclara estas diferencias y describe la utilización de la CPU en el Switches y cómo interpretar la salida del **comando show processes cpu**.

**Nota:** En este documento, las palabras “conmutan” y el “Switches” refiere al Switches del Catalyst 6500/6000.

# prerrequisitos

## Requisitos

No hay requisitos específicos para este documento.

## Componentes Utilizados

La información en este documento se basa en las versiones de software y hardware para el Switches y el sistema de transferencia virtual (VSS) del Catalyst 6500/6000 1440 sistemas basados.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

**Nota:** El software admitido para el sistema de transferencia virtual (VSS) 1440 sistemas basados es la versión 12.2(33)SXH1 del Cisco IOS ® Software o más adelante.

## Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

# Diferencia entre el software de sistema CatOS y Cisco IOS

**Catalyst OS (CatOS) en el Supervisor Engine y Cisco IOS® Software en la Multilayer Switch Feature Card (MSFC)** (Híbrido): Puede utilizar una imagen de CatOS como software de sistema para ejecutar el Supervisor Engine en switches Catalyst 6500/6000. Si está instalado el MSFC opcional, se utiliza una imagen de software IOS de Cisco separada para ejecutar el MSFC.

**Cisco IOS Software en Supervisor Engine y en MSFC** (Nativo): Puede utilizar una única imagen del software Cisco IOS como software de sistema para ejecutar tanto el Supervisor Engine como la MSFC en switches Catalyst 6500/6000.

**Nota:** Refiérase a Comparación de los Sistemas Operativos Cisco Catalyst y Cisco IOS para Cisco Catalyst 6500 Series Switch para obtener más información.

## Introducción al Uso de CPU en Switches Catalyst 6500/6000

Los routers basados en software Cisco utilizan software a fin de procesar y direccionar paquetes. El uso de CPU en un router Cisco tiende a incrementarse a medida que el router ejecuta más tareas de procesamiento y ruteo de paquetes. Por lo tanto, el comando show processes cpu puede proveer una indicación bastante precisa de la carga de procesamiento de tráfico en el router.

Los Switches Catalyst 6500/6000 no utilizan la CPU de la misma manera. Estos switches toman decisiones de reenvío en el hardware, no en el software. Por lo tanto, cuando los switches efectúan el reenvío o toman decisiones de conmutación para la mayoría de las tramas que pasan a través del switch, el proceso no involucra a la CPU del Supervisor Engine.

Los Switches Catalyst 6500/6000 poseen dos CPU. Una CPU es la CPU del Supervisor Engine, que se denomina Network Management Processor (NMP) o Switch Processor (SP). La otra CPU es la CPU del motor de ruteo de Capa 3, denominada MSFC o Route Processor (RP).

La CPU del SP realiza funciones entre las que se encuentran:

- Colaborar en el aprendizaje y desactualización de direcciones MAC**Nota:** El MAC Address Learning también se llama configuración de la trayectoria.
- Ejecuta protocolos y procesos que proporcionan control de la redAlgunos ejemplos son: Spanning Tree Protocol (STP), Cisco Discovery Protocol (CDP), VLAN Trunk Protocol (VTP), Dynamic Trunking Protocol (DTP) y Port Aggregation Protocol (PAgP).
- Maneja el tráfico de administración de la red que se destina a la CPU del switchAlgunos ejemplos son: tráfico Telnet, HTTP y Simple Network Management Protocol (SNMP).

La CPU del RP realiza funciones entre las que se encuentran:

- Crea y actualiza las tablas de ruteo de Capa 3 y del Address Resolution Protocol (ARP)
- Genera tablas de Cisco Express Forwarding (CEF), Forwarding Information Base (FIB) y de adyacencia; además, descarga las tablas en la Policy Feature Card (PFC) )
- Maneja el tráfico de administración de red con destino al RPAlgunos ejemplos incluyen: tráfico Telnet, HTTP y SNMP.

## Situaciones y Funciones que Hacen que el Tráfico Pase por Software

## Paquetes Destinados al Switch

Cualquier paquete que tiene como destino el switch pasa por software. Tales paquetes incluyen:

- Paquetes de controlLos paquetes de control son recibidos por STP, CDP, VTP, Hot Standby Router Protocol (HSRP), PAgP, Link Aggregation Control Protocol (LACP) y UniDirectional Link Detection (UDLD).
- Actualizaciones del Routing ProtocolAlgunos ejemplos de estos protocolos son: Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP) y Open Shortest Path First Protocol (Protocolo OSPF).
- Tráfico SNMP que tiene como destino el switch
- Telnet y el protocolo secure shell (SSH) trafican al Switch.CPU elevada el ultilization debido a SSH se ve como:
  ```
  00:30:50.793 SGT Tue Mar 20 2012CPU utilization for five seconds: 83%/11%; one minute: 15%;
  five minutes: 8% PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process    3
  6468      8568        754 69.30%  7.90%  1.68%   1 SSH Process
  ```
  Incluya estos comandos en el script EEM para verificar el número de sesiones SSH establecidas cuando pasa a ALTO el CPU:muestre a los usuarioslínea show
- Respuestas ARP a solicitudes ARP

## Paquetes y Condiciones que Requieren Procesamiento Especial

Esta lista proporciona condiciones y tipos de paquetes específicos que obligan a que los paquetes se manejen en el software:

- Paquetes con opciones IP, un Time to Live (TTL) vencido, o encapsulación que no sea del tipo Advanced Research Projects Agency (ARPA)
- Paquetes con un manejo especial, como el de tunelización
- Fragmentación de IP
- Paquetes que requieren mensajes del tipo Internet Control Message Protocol (ICMP) provenientes de RP o de SP
- Error de comprobación de la unidad de transmisión máxima (MTU)
- Paquetes con errores IP, que incluyen errores de longitud y de comprobación de suma IP
- Si los paquetes de entrada vuelven un error de bit (tal como el error de un solo bit (SBE)), los paquetes se envían al CPU para el software que procesa y se corrigen. El sistema afecta un aparato un buffer para ellos y utiliza a los recursos de la CPU para corregirlo.
- Cuando el PBR y la lista de acceso reflexiva están en la trayectoria de un flujo de tráfico, el paquete es conmutado por software, que requiere un ciclo de la CPU adicional.
- Misma interfaz de adyacencia
- ¿Paquetes que fallan el control del reenvío de trayecto inverso (RPF)? **falla de RPF**
- Recopilar/recibir (Glean/receive)"Glean" hace referencia a paquetes que requieren resolución ARP y "receive" a paquetes que llegan a la caja de recepción.
- Tráfico del tipo Internetwork Packet Exchange (IPX) que es conmutado por software en el Supervisor Engine 720, tanto en el Software Cisco IOS como en CatOSTráfico IPX que también se conmute por software en el Supervisor Engine 2/Software Cisco IOS; pero el tráfico se conmuta por hardware en el Supervisor Engine 2/CatOS. Tráfico IPX que se conmuta por hardware en el Supervisor Engine 1A para ambos sistemas operativos.
- Tráfico AppleTalk
- Condiciones completas de recursos de hardwareEntre estos recursos podemos mencionar:

FIB, memoria con direccionamiento por contenido (CAM) y CAM ternaria (TCAM).

## Funciones Basadas en ACL

- Tráfico rechazado por una ACL (lista de control de acceso) con la función direcciones inalcanzables ICMP activada**Nota:** Este es el valor predeterminado.Algunos paquetes rechazados por ACL se filtran a la MSFC si se habilita la función de direcciones IP inalcanzables. Los paquetes que requieran direcciones inalcanzables de ICMP se filtran a una velocidad que puede configurar el usuario. De forma predeterminada, la velocidad es de 500 paquetes por segundo (pps).
- Filtrado IPX en base a parámetros no compatibles, como host de origenEn el Supervisor Engine 720, el proceso del tráfico IPX de Capa 3 IPX siempre se efectúa en el software.
- Access Control Entries (ACE) que requieran registro, con la palabra clave **log**Esto se aplica a las funciones de registro de ACL y VLAN ACL (VACL). ACE en la misma ACL que no requieran registro y que aún se encuentren en proceso en el hardware. El Supervisor Engine 720 con PFC3 es compatible con el límite de velocidad de paquetes que se redireccionan a la MSFC para registro ACL y VACL. El Supervisor Engine 2 con PFC3 es compatible con el límite de velocidad de paquetes que se redireccionan a la MSFC para registro ACL y VACL. La compatibilidad para registro de ACL en el Supervisor Engine 2 está programada para la rama de la versión 12.2S del Cisco IOS Software.
- Tráfico con ruteo por políticas, con el uso de los parámetros **match length**, **set ip precedence** u otros parámetros no compatiblesEl parámetro **set interface** cuenta con soporte en software. Sin embargo, el parámetro **set interface null 0** es una excepción. El tráfico es manejado en el Supervisor Engine 2 con PFC2 y el Supervisor Engine 720 con PFC3.
- ACL de routers que no sean IP ni IPX (RACL)Las RACL no IP se aplican a todos los Supervisor Engines. Las RACL no IPX se aplican al Supervisor Engine 1a con PFC y al Supervisor Engine 2 con PFC2 exclusivamente.
- Tráfico de broadcast que sea rechazado en una RACL
- Tráfico que sea rechazado en una comprobación unicast RPF (uRPF), ACE de ACLEsta comprobación uRPF se aplica al Supervisor Engine 2 con PFC2 y al Supervisor Engine 720 con PFC3.
- Proxy de AutenticaciónLa velocidad de un tráfico sujeto a un proxy de autenticación se puede limitar en el Supervisor Engine 720.
- Seguridad IP (IPsec) del Cisco IOS SoftwareLa velocidad de un tráfico sujeto a cifrado Cisco IOS se puede limitar en el Supervisor Engine 720.

## Funciones Basadas en NetFlow

Las funciones basadas en NetFlow que se describen en esta sección se aplican al Supervisor Engine 2 y al Supervisor Engine 720 exclusivamente.

- Las funciones basadas en NetFlow siempre necesitan ver el primer paquete de un flujo en software. Una vez que el primer paquete del flujo llega al software, los paquetes subsiguientes del mismo flujo se conmutan por hardware.Esta disposición de flujo se aplica a ACL reflexivas, Web Cache Communication Protocol (WCCP) y a Cisco IOS Server Load Balancing (SLB).**Nota:** En el Supervisor Engine 1, el ACL reflexivo confía en las entradas TCAM dinámicas para crear los accesos directos por hardware para un flujo determinado. El principio es el mismo: el primer paquete de un flujo pasa al software. Los paquetes

subsiguientes de ese flujo se conmutan por hardware.
- Con la función TCP Intercept, el contacto triple y el cierre de sesión se manejan por software. El resto del tráfico se maneja por hardware.**Nota:** Sincronice (SYN), SYN reconocen (SYN ACK), y los paquetes ACK comprenden la entrada en contacto de tres vías. El cierre de sesión se materializa con finish (FIN) o reset (RST).
- En el caso de Network Address Translation (NAT), el tráfico se maneja de esta forma:En el Supervisor Engine 720:El tráfico que requiere NAT se maneja por hardware después de la traducción inicial. La traducción del primer paquete de un flujo se ejecuta por software y los paquetes subsiguientes de ese flujo se conmutan por hardware. En el caso de paquetes TCP, se crea un acceso directo de hardware en la tabla NetFlow una vez finalizado el contacto trile TCP.En Supervisor Engine 2 y Supervisor Engine 1:Todo el tráfico que requiera NAT se conmuta por software.
- Context-based Access Control (CBAC) utiliza accesos directos NetFlow para clasificar el tráfico que requiera inspección. Posteriormente, CBAC envía sólo este tráfico a software. El CBAC es una característica software solamente; trafique que está conforme al examen no es conmutado por hardware.**Nota:** Trafique que está conforme al examen puede ser tarifa limitada en el Supervisor Engine 720.

## Tráfico Multicast

- Indagación del tipo Protocol Independent Multicast (PIM)
- Indagación del tipo Internet Group Management Protocol (IGMP) (TTL = 1)De hecho, este tráfico tiene al router como destino.
- Indagación del tipo Multicast Listener Discovery (MLD) (TTL = 1)De hecho, este tráfico tiene al router como destino.
- Omisión FIB
- Paquetes multicast para registro que tengan conexión directa con la fuente multicastEstos paquetes multicast se tunelizan al punto de encuentro.
- Multicast IP Version 6 (IPv6)

## Otras funciones

- Network-Based Application Recognition (NBAR)
- Inspección ARP, sólo con CatOS
- Seguridad de Puertos, sólo con CatOS
- Snooping del DHCP

## Situaciones IPv6

- Paquetes con encabezado de opción hop-by-hop (salto por salto)
- Paquetes con la misma dirección IPv6 destino que la de los routers
- Paquetes que no superan la comprobación de imposición de alcance
- Paquetes que exceden la MTU del enlace de salida
- Paquetes con un valor TTL menor o igual a 1
- Paquetes con un valor VLAN de entrada igual al de VLAN de salida
- IPv6 uRPFEl software ejecuta esta uRPF para todos los paquetes.
- ACL reflexivas IPv6El software administra estas ACL reflexivas.

- Prefijos 6to4 para túneles IPv6 Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)El software administra esta tunelización. Cualquier otro tráfico que ingrese a un túnel ISATAP se conmuta por hardware.

## LCP cedular y módulo DFC

En una Distributed Forwarding Card (DFC), el proceso lcp schedular que se ejecuta con un uso excesivo de CPU no representa un problema para el funcionamiento. El LCP cedular es parte del código del firmware. En todos los módulos que no requieran un DFC, el firmware se ejecuta en un procesador específico llamado el (LCP) del procesador del linecard. Este procesador se utiliza para programar el hardware ASIC y para comunicar al módulo de la central supervisor.

Cuando se inicia lcp schedular, hace uso de todo el tiempo de proceso disponible. Sin embargo, cuando un nuevo proceso necesita tiempo del procesador, lcp schedular libera tiempo de proceso para el nuevo proceso. No se registra impacto alguno sobre el rendimiento del sistema en relación con este uso excesivo de la CPU. EL proceso simplemente se adueña de todos los ciclos de CPU no utilizados, siempre que ningún otro proceso de mayor prioridad los necesite.

```
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 Frecuentes y Soluciones para Problemas de Uso Excesivo de CPU

## Inalcanzables IP

Cuando un grupo de acceso rechaza un paquete, la MSFC envía mensajes de ICMP inalcanzable. Esta acción sucede de forma predeterminada.

Debido a la habilitación predeterminada del comando **ip unreachables**, el Supervisor Engine descarta la mayoría de los paquetes rechazados en hardware. Posteriormente, el Supervisor Engine envía sólo una cantidad reducida de paquetes, con un máximo de 10 pps, a la MSFC para que los descarte. Esta acción genera mensajes de dirección ICMP inalcanzable.

El descarte de paquetes rechazados y la generación de mensajes de ICMP inalcanzable imponen una carga sobre la CPU de la MSFC. A fin de eliminar la carga, puede ejecutar el comando de configuración de interfaz **no ip unreachables**. Este comando deshabilita los mensajes de ICMP inalcanzable, permitiendo así descartar todos los paquetes rechazados por grupos de acceso en hardware.

Los mensajes de ICMP inalcanzable no se envían en caso de que una VACL rechace un paquete.

## Traducciones de NAT

El NAT utiliza ambo la expedición del hardware y software. El establecimiento inicial de los tranlsations NAT debe ser hecho en el software y la expedición adicional se hace con el hardware. El NAT también utiliza la tabla del Netflow (máximo 128 KB). Por lo tanto, si la tabla del Netflow es llena, el Switch también comenzará a aplicar la expedición NAT vía el software. Esto sucede con las explosiones del mucho tráfico y causará normalmente un aumento en el CPU de 6500.

## Uso del Espacio de Tabla CEF FIB en la Tabla de Caché de Flujo

El Supervisor Engine 1 incluye una Tabla de Caché de Flujo que admite 128,000 entradas. Sin embargo, en base de la eficacia del algoritmo de troceo, estas entradas se extienden a partir del 32,000 a 120,000. En el Supervisor Engine 2, la tabla de FIB se genera y se programa en el PFC. La tabla puede albergar hasta 256,000 entradas. El Supervisor Engine 720 con PFC3-BXL admite un máximo de 1,000,000 entradas. Una vez que se excedió el espacio, los paquetes comienzan a conmutarse por software. Esto puede generar un uso excesivo de CPU en el RP. Si desea comprobar la cantidad de rutas en la tabla CEF FIB, emplee estos 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:          53019378962495Total 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
```

En el Supervisor Engine 2, la cantidad de entradas FIB se reduce a la mitad en caso de que haya configurado la comprobación RPF en las interfaces. La configuración puede derivar en la conmutación por software de más paquetes y, en consecuencia, a un uso excesivo de CPU.

Para resolver CPU elevada el problema de la utilización, resumen de Route del permiso. El resumen de Route puede minimizar el tiempo de espera en una red compleja reduciendo las cargas de trabajo del procesador, los requisitos de memoria, y la demanda del ancho de banda.

Consulte Introducción a la ACL en los Catalyst 6500 Series Switches si necesita más información sobre el uso y optimización de TCAM.

## Registro de ACL Optimizado

El Registro de ACL Optimizado (Optimized ACL Logging, OAL) proporciona soporte de hardware para el registro de ACL. A menos que configure OAL, el proceso de paquetes que requieran registro se lleva a cabo íntegramente mediante software en la MSFC3. El OAL admite o descarta paquetes en hardware en la PFC3. El OAL utiliza una rutina optimizada para enviar información a la MSFC3 con el objetivo de generar mensajes de registro.

**Nota:** Para la información sobre el OAL, refiera al *registro de ACL optimizado con una* sección *PFC3* comprensión del soporte del Cisco IOS ACL.

## Límite de Velocidad de Paquetes a la CPU

En el Supervisor Engine 720, los limitadores de velocidad pueden controlar la velocidad con la que los paquetes pueden pasar al software. Este control de velocidad evita ataques de negación de servicio. También puede utilizar algunos de estos limitadores de velocidad en el 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
```

Aquí tiene un ejemplo:

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

Si desea limitar la velocidad de todos los paquetes impulsados por CEF a la MSFC, ejecute el comando que figura en este ejemplo:

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

Si desea reducir la cantidad de paquetes impulsados a la CPU debido a TTL=1, ejecute 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 ejemplo, ésta es la salida de la **captura del netdr**, que muestra que el IPv4 TTL es 1:

```
Source mac    00.00.50.02.10.01  3644Dest mac      AC.A0.16.0A.B0.C0  4092Protocol      0800
4094Interface     Gi1/8              3644Source vlan   0x3FD(1021)        3644Source index
0x7(7)             3644Dest index    0x380(896)         3654 L3  ipv4 source   211.204.66.117
762ipv4 dest     223.175.252.49     3815ipv4 ttl                  1     3656ipv6 source
```

```
-        0ipv6 dest                  -        0ipv6 hoplt                 -        0ipv6 flow
-        0ipv6 nexthdr               -        0
```

El uso excesivo de CPU también puede deberse a paquetes con TTL = 1 que se filtran a la CPU. Si desea limitar la cantidad de paquetes que se filtran a la CPU, configure un limitador de velocidad por hardware. Los limitadores de velocidad pueden limitar la velocidad de los paquetes que se filtran desde la trayectoria de datos en hardware a la trayectoria de datos en software. Los limitadores de velocidad protegen la trayectoria de control de la congestión al descartar el tráfico que exceda la velocidad configurada. El límite de velocidad se configura con el comando **mls rate-limit all ttl-failure**.

## Fusión Física de VLAN Debido a Cableado Incorrecto

El uso excesivo de CPU también puede ser el resultado de que se fusionen dos o más VLAN debido a cableado incorrecto. Además, si se deshabilita STP en los puertos donde se registra la fusión de las VLAN, se puede generar uso excesivo de CPU.

Para resolver este problema, identifique los errores de cableado y corríjalos. Si sus requisitos lo permiten, también puede habilitar STP en esos puertos.

## Tormenta de broadcast

Se registra una tormenta de broadcast LAN cuando la LAN se ve inundada por paquetes broadcast o multicast. Esta situación genera tráfico excesivo y degrada el rendimiento de la red. Cualquier error en la implementación de la pila de protocolos o en la configuración de la red puede generar una tormenta de broadcast.

Debido al diseño arquitectónico de la plataforma de las Catalyst 6500 Series, los paquetes de broadcast se caen solamente y siempre en el nivel de software.

La supresión de broadcast evita que las interfaces LAN se vean perturbadas por una tormenta de broadcast. La supresión de broadcast utiliza un filtrado que mide la actividad de broadcast en una LAN en un período de 1 segundo y compara la medición con un umbral predefinido. Si se alcanza dicho umbral, se suprime toda actividad de broadcast adicional durante un período de tiempo especificado. La supresión de broadcast está deshabilitada de manera predeterminada.

**Nota:** El cambio VRRP del respaldo a dominar causado por las tormentas de broadcast pudo causar CPU elevada la utilización.

Si desea comprender cómo funciona la supresión de broadcast y cómo habilitar la función, consulte:

- Configuración de la Supresión de Broadcast (software de sistema Cisco IOS)
- Configuración de la Supresión de Broadcast (software de sistema CatOS)

## Seguimiento de la Dirección Next-Hop BGP (Proceso del Escáner BGP)

El proceso del Escáner BGP recorre la tabla BGP y confirma si se pueden alcanzar los próximos saltos. El proceso también verifica el anuncio condicional para poder determinar si BGP debería anunciar prefijos de condición y/o ejecutar amortiguación de rutas. De forma predeterminada, el proceso escanea cada 60 segundos.

Puede esperar que se registre un uso excesivo de CPU durante breves períodos de tiempo debido al proceso del Escáner BGP en un router que transmite una tabla de ruteo de Internet de magnitudes considerables. Una vez por minuto, el Escáner BGP recorre la tabla BGP Routing Information Base (RIB) y ejecuta importantes tareas de mantenimiento. Entre estas tareas se incluyen:

- Comprobación del siguiente salto al que se hace referencia en la tala BGP del router
- Verificación de que se pueden alcanzar los dispositivos next-hop

De este modo, una tabla BGP grande requiere una cantidad de tiempo equivalente para ser transitada y validada. El proceso del Escáner BGP recorre la tabla BGP para poder actualizar cualquier estructura de datos y recorre la tabla de ruteo con fines de redistribución de rutas. Ambas tablas se almacenan separadamente en la memoria del router. Las dos tablas pueden ser muy grandes y, en consecuencia, consumir ciclos de CPU.

Si necesita más información sobre uso de CPU por parte del proceso del Escáner BGP, consulte la sección *Uso Excesivo de CPU Debido a BGP Scanner* de Resolución de Problemas de Uso Excesivo de CPU Causados por el Proceso del Escáner BGP o del Router BGP.

Si necesita más información sobre la función de Seguimiento de Dirección Next-Hop BGP (BGP Next-Hop Address Tracking) y el procedimiento para habilitar/deshabilitar o ajustar el intervalo de la exploración del Escáner, consulte Compatibildad BGP para el Seguimiento de Dirección Next-Hop.

## Tráfico Multicast No RPF

El ruteo multicast (a diferencia del unicast) sólo se preocupa por el origen de un determinado flujo de datos multicast. Esto es, la dirección IP del dispositivo que origina el tráfico multicast. El principio básico es que el dispositivo origen "empuja" el flujo hacia una cantidad indefinida de receptores (dentro de su grupo multicast). Todos los routers crean árboles de distribución, que controlan la trayectoria que adopta el tráfico multicast a través de la red para poder distribuir el tráfico a todos los receptores. Los dos tipos básicos de árboles de distribución multicast son los árboles de origen y los árboles compartidos. RPF es un concepto clave en el reenvío multicast. Permite que los routers reenvíen el tráfico multicast correctamente a través del árbol de distribución. RPF hace uso de la tabla de ruteo unicast existente para determinar los vecinos de flujo ascendente y descendente. Un router reenvía un paquete multicast sólo si es recibido en la interfaz de flujo ascendente. Esta comprobación RPF ayuda a garantizar que el árbol de distribución se encuentre libre de loops.

El tráfico multicast es siempre visible para cualquier router en una LAN puenteada (Capa 2), según la especificación IEEE 802.3 CSMA/CD. En la 802.3 estándar, el bit 0 del primer octeto se utiliza para indicar una trama de broadcast y/o multicast, y se satura cualquier trama de Capa 2 con esta dirección. Esto también ocurre en caso de haberse configurado las indagaciones CGMP o IGMP. Esto se debe a que los routers multicast deben ver el tráfico multicast para poder tomar una decisión de reenvío correcta. Si varios routers multicast poseen interfaces sobre una LAN común, entonces sólo uno reenviará los datos (se lo elige mediante un proceso de selección). Debido a la naturaleza de la saturación de las LAN, el router redundante (el router que no reenvía el tráfico multicast) recibe estos datos en la interfaz de salida para esa LAN. Normalmente, el router redundante descarta este tráfico dado que llegó a la interfaz incorrecta y, en consecuencia, no logra pasar la comprobación RPF. Este tráfico que no logra superar la comprobación RPF se denomina tráfico no RPF o paquetes de error RPF, debido a que fueron transmitidos hacia atrás, en contra del flujo proveniente del origen.

El Catalyst 6500 con una MSFC instalada se puede configurar para funcionar como un router multicast con máximas capacidades. Si se utiliza Multicast Multi-Layer Switching (MMLS), el tráfico suele ser reenviado por el hardware que se encuentra dentro del switch. A los ASIC se les brinda información desde el estado de ruteo multicast (por ejemplo: [*,G] y [S,G]) de modo que se pueda programar un acceso directo de hardware en la tabla Netflow y/o FIB. Este tráfico no RPF todavía es necesario en algunos casos y la CPU de la MSFC requiere de él (en el nivel de proceso) para el mecanismo PIM Assert. De lo contrario, será descartado por la trayectoria de conmutación rápida del software (asumiendo que la conmutación rápida por software no esté deshabilitada en la interfaz RPF).

El Catalyst 6500 que utiliza redundancia no podría manejar eficazmente el tráfico no RPF en ciertas topologías. Por lo general, para este tráfico no RPF, no hay un estado (*,G) o (S,G) en el router redundante y, por lo tanto, no se pueden crear accesos directos de hardware o de software para descartar el paquete. Cada paquete multicast debe ser examinado por el procesador de rutas de la MSFC individualmente; esto se conoce frecuentemente como tráfico de interrupción de CPU (CPU Interrupt). En el caso de conmutación por hardware de Capa 3 y de que existan varias interfaces/redes VLAN conectadas al mismo conjunto de routers, el tráfico no RPF que llega a la CPU de la MSFC redundante ve amplificada su velocidad de origen inicial "N" veces (donde "N" es la cantidad de redes LAN a las que el router está conectado en forma redundante). Si la velocidad del tráfico no RPF excede la capacidad de descarte de paquetes del sistema, se podría generar un uso excesivo de la CPU, desbordamientos de buffer e inestabilidad general en la red.

En el caso del Catalyst 6500, se dispone de un motor de listas de acceso que posibilita que el filtrado se lleve a cabo a la velocidad permitida por el cable. Esta función puede usarse en ciertas situaciones para manejar tráfico no RPF de manera eficiente para los grupos del modo disperso (Sparse Mode). Sólo podrá utilizar el método basado en listas ACL dentro de 'redes stub' del modo disperso, donde no existen routers multicast de flujo descendente (ni sus receptores correspondientes). Además, debido al diseño de reenvío de paquetes de Catalyst 6500, las MSFC redundantes internamente no pueden utilizar esta implementación. Esto se describe en líneas generales en el Id. de error de Cisco CSCdr74908 (sólo para clientes registrados). En grupos que se encuentran en modo denso, se deben ver los paquetes no RPF en el router para que el mecanismo PIM Assert funcione correctamente. Diferentes soluciones, como la limitación de velocidad y QoS basadas en CEF o Netflow, se utilizan para controlar fallas RPF en redes que se encuentren en modo denso y redes de tránsito en modo disperso.

En el caso de Catalyst 6500, se dispone de un motor de listas de acceso que permite que el filtrado se lleve a cabo a la velocidad permitida por el cable. Puede usarse esta función para manejar el tráfico que no es RPF de manera eficiente para los grupos en modo disperso. Con el objetivo de implementar esta solución, ubique una lista de acceso en la interfaz de entrada de la 'red stub' para filtrar el tráfico multicast que no se originó en la 'red stub'. La lista de acceso se empuja hacia abajo al hardware en el Switch. Esta lista de acceso impide que la CPU vea el paquete y permite que el hardware descarte el tráfico no RPF.

**Nota:** No ponga esta lista de acceso en una interfaz del transitar. Está destinada exclusivamente para redes stub (redes con hosts únicamente).

Si desea más información, consulte estos documentos:

- Inconvenientes en Routers Redundantes con Multicast de IP en Redes Stub
- Procesamiento de Tráfico No RPF

## Comandos show

El nivel de utilización de CPU cuando se ejecuta un comando **show** siempre es muy cercano al 100%. Es normal que el uso de CPU sea excesivo cuando se ejecuta un comando **show**, dicho nivel de uso de CPU normalmente se sostiene sólo durante algunos segundos.

Por ejemplo: es normal que el proceso Virtual Exec se eleve cuando se ejecuta un comando **show tech-support** ya que esta salida es una salida impulsada por interrupciones. Su única preocupación deberá ser el uso de CPU excesivo en procesos que no sean comandos **show**.

El comando show cef not-cef-switched muestra porqué los paquetes se llevan en batea al MSFC (reciba, opción del IP, ninguna adyacencia, etc) y cuántos. Por ejemplo:

```
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
```

**El ibc de la demostración** y el **ibc de la demostración informan los** comandos show la cola CPU y pueden ser utilizados cuando usted está monitoreando el estatus CPU.

## Procesos Exec

El proceso Exec en Cisco IOS Software es responsable de la comunicación con las líneas TTY (consola, auxiliar, asincrónica) del router. El proceso Virtual Exec (Ejecución virtual) es responsable de las líneas vty (sesiones telnet). Los procesos Exec y Virtual Exec son procesos de prioridad media por lo que, de existir otros procesos con prioridad más alta (Elevada o Crítica), son estos últimos procesos los que consumirán los recursos de la CPU.

En caso de que se transfieran muchos datos a través de estas sesiones, el nivel de utilización de CPU para el proceso Exec se incrementa. Esto se debe a que, cuando el router desea enviar un carácter simple a través de estas líneas, utiliza algunos recursos de la CPU:

- En el caso de la consola (Exec), el router emplea un interruptor por caracter.
- En el caso de la línea VTY (Virtual Exec), la sesión Telnet debe generar un paquete TCP por carácter.

En esta lista se detallan algunos de los posibles motivos para que se registre uso excesivo de CPU en el proceso Exec:

- **Se envían demasiados datos a través del puerto de la consola.**Compruebe si se ha iniciado algún debug en el router con el comando show debugging.Deshabilite el registro de la consola en el router con la forma **no** del comando logging console.Verifique si se imprime una salida extensa en la consola. Por ejemplo: un comando show tech-support o uno show memory.
- **El comando** exec se configura para las líneas asincrónicas y auxiliares.Si por una línea sólo circula tráfico saliente, deshabilite el proceso Exec para esta línea. Debe hacerlo porque, si el dispositivo (por ejemplo, un módem) adjunto a esta línea, envía algunos datos no solicitados, el proceso Exec comenzará en esta línea.Si se utiliza el router como un servidor terminal (para Telnet inversa u otras consolas de dispositivos), le recomendamos que configure el comando **no exec** en las líneas que están conectadas a la consola de los otros dispositivos. De lo contrario, los datos que regresan de la consola podrían dar inicio a un proceso Exec,

proceso que utiliza recursos de la CPU.

Un posible motivo para que se registre un uso excesivo de CPU en el proceso Virtual Exec es el siguiente:

- **Se envían demasiados datos a través de las sesiones Telnet.**El motivo más habitual por el que se registra un uso excesivo de CPU en el proceso Virtual Exec es que se transfieren demasiados datos desde el router a la sesión Telnet. Esto puede darse cuando se ejecutan comandos con salidas extensas como **show tech-support**, **show memory**, entre otros, desde la sesión Telnet. La cantidad de datos transferidos a través de cada sesión VTY se puede verificar con el comando **show tcp vty <line number>**.

## Proceso de desactualización L3

Cuando el proceso de desactualización L3 exporta un gran número de valores del *ifindex* usando la Exportación de datos de NetFlow (NDE), el USO de la CPU pudo golpear el 100%.

Si usted encuentra este problema, marque si estos dos comandos están habilitados:

```
set mls nde destination-ifindex enable

set mls nde source-ifindex enable
```

Si usted habilita estos comandos, el proceso debe exportar todos los valores del ifindex del destino y de la fuente usando el NDE. La utilización del proceso de desactualización L3 pasa a ALTO puesto que debe realizar las operaciones de búsqueda de la BOLA para todos los valores del *ifindex del* destino y de la fuente. Debido a esto, la tabla se convierte por completo, el proceso de desactualización L3 pasa a ALTO, y el USO de la CPU golpea el 100%.

Para resolver este problema, inhabilite estos comandos:

```
set mls nde destination-ifindex disable

set mls nde source-ifindex disable
```

Utilice estos comandos de verificar los valores:

- muestre el resumen del cef de los mls
- muestre las máximo-rutas del cef de los mls

## Tormenta BPDU

El spanning tree mantiene un entorno de Capa 2 libre de loops en redes conmutadas redundantes y puenteadas. Sin el STP, las tramas colocan y/o se multiplican indefinidamente. Esto genera un colapso de la red porque el tráfico elevado interrumpe todos los dispositivos en el dominio de broadcast.

En algunos aspectos, STP es un protocolo antiguo que se desarrolló inicialmente para especificaciones de puente con base en software (IEEE 802.1D); sin embargo, puede resultar complicado implementar exitosamente STP en redes conmutadas de magnitud que cuenten con estas características:

- Muchos VLA N
- Muchos switches en un dominio STP
- Soporte de varios proveedores
- Más nuevas mejoras de IEEE

Si la red debe hacer frente a frecuentes cálculos de spanning tree o el switch debe procesar más BPDU, se puede generar un uso excesivo de CPU y, además, descartes BPDU.

Para poder solucionar estos inconvenientes, recurra a alguno o a todos estos pasos:

1. Separe las VLAN de los switches.
2. Utilice una versión mejorada de STP, como MST.
3. Actualice el hardware del switch.

Además, consulte las recomendaciones de uso para implementar el protocolo Spanning Tree Protocol en la red.

- Mejores prácticas para el Switches de los Catalyst 4500/4000, 5500/5000, y 6500/6000 Series que funciona con la configuración y la Administración de CatOS
- Mejores prácticas para Switches de las 4500/4000 Series de la serie y del Catalyst del Catalyst 6500/6000 que funciona con el Cisco IOS Software

## Sesiones SPAN

En base a la arquitectura de los switches Catalyst 6000/6500 Series, las sesiones SPAN no afectan el rendimiento del switch pero, si la sesión SPAN incluye un puerto de tráfico elevado/uplink o un EtherChannel, puede incrementar la carga del procesador. Si posteriormente aísla una VLAN específica, aumenta aun más la carga de trabajo. Si existe tráfico dañado en el enlace, es posible que la carga de trabajo se incremente aun más.

En algunas situaciones, la función RSPAN puede generar loops y, en consecuencia, la carga del procesador se eleva. Si necesita más información, consulte ¿Por Qué la Sesión SPAN Crea un Loop de Bridging?

El switch puede transferir tráfico en forma habitual porque todo sucede a nivel de hardware, pero es posible que la CPU sufra un nivel excesivo de utilización de recursos si intenta determinar qué tráfico debe enviarse. Le recomendamos que configure sesiones SPAN sólo cuando resulte necesario.

## %CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched

```
%CFIB-SP-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be software switched %CFIB-SP-STBY-7-CFIB_EXCEPTION : FIB TCAM exception, Some entries will be softwareswitched
```

Se recibe este mensaje de error cuando se excede la cantidad de espacio disponible en TCAM. Esto genera uso excesivo de la CPU. Se trata de una limitación FIB TCAM. Una vez que la TCAM se llena, se configurará un indicador y se recibirá una excepción FIB TCAM. De esta manera, se dejan de añadir nuevas rutas a la TCAM. En consecuencia, todo el material se conmutará por software. La eliminación de rutas no ayuda a retomar la conmutación por hardware. Una vez que la TCAM ingresa al estado de excepción, se debe volver a cargar el sistema para salir de ese estado. La cantidad máxima de rutas que se puede instalar en la TCAM se incrementa mediante

el comando **mls cef maximum-routes**.

### El Catalyst 6500/6000 que se ejecuta con CPU elevada tiene un IPv6 ACL con los puertos L4

Unicast del direccionamiento de la compresa acl del IPv6 de los mls del permiso. Este comando es necesario si el IPv6 ACL está correspondiendo con en los números del puerto del protocolo L4. Si este comando no se habilita, el tráfico del IPv6 será llevado en batea al CPU para el proceso del software. Este comando no se configura por abandono.

### Cobre SPF

En el Cisco ME 6500 Series Ethernet Switches, el cobre SFP requiere más interacción del firmware que otros tipos de SFP, que aumenta la utilización de la CPU.

Los algoritmos de software que manejan los SFP de cobre se han mejorado en las versiones del Cisco IOS SXH.

### IOS modular

En los Cisco Catalyst 6500 Series Switch que funcionan con el software IOS modular, la utilización de la CPU normal es un software IOS poco mayor que NON-modular.

El software IOS modular paga un precio por la actividad más que paga un precio por el paquete. El software IOS modular mantiene los procesos consumiendo cierto CPU incluso si no hay mucho los paquetes, así que el consumo de la CPU no se basa en el tráfico real. Sin embargo, cuando van los paquetes procesado alta velocidad, el CPU consumido en el software IOS modular no debe ser más que eso en el software IOS NON-modular.

## Comprobación del Uso de la CPU

Si el uso de la CPU es excesivo, ejecute el comando **show processes cpu** como primera medida. La salida le indicará el nivel de utilización de la CPU en el switch y, además, el consumo de recursos de la CPU por parte de cada proceso.

```
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.
```

En esta ejemplo, la utilización total de recursos de la CPU es del 57% y el uso de CPU por interrupciones es del 48%. Aquí, estos porcentajes aparecen en negrita. El switch de interrupción del tráfico por parte de la CPU causa utilización de recursos de CPU por interrupción. La salida del comando enumera los procesos que causan la diferencia entre ambas utilizaciones. En este caso, el responsable es el proceso SNMP.

En el Supervisor Engine que ejecuta CatOS, la salida tiene el siguiente aspecto:

```
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
```

En esta salida, el primer proceso es Kernel and Idle, que indica la utilización ociosa de recursos de la CPU. Este proceso suele consumir muchos recursos, a menos que otros procesos consuman ciclos de la CPU. En este ejemplo, el proceso SptBpduRx genera uso excesivo de la CPU.

Si el uso de la CPU es excesivo debido a alguno de estos procesos, usted puede diagnosticar el problema y determinar por qué este proceso consume muchos recursos. Pero, si el consumo de recursos de la CPU es excesivo debido a que se impulsa tráfico a la CPU, deberá determinar el motivo de esa situación. Cuando descubra el motivo podrá identificar más fácilmente cuál es el tráfico.

Para resolver problemas, utilice este ejemplo de secuencia de comandos EEM para recoger la salida del Switch cuando usted experimenta CPU elevada la utilización:

```
event manager applet cpu_statsevent snmp oid "1.3.6.1.4.1.9.9.109.1.1.1.1.3.1" get-type exact
entry-op gt entry-val "70"exit-op lt exit-val "50" poll-interval 5action 1.01 syslog msg "------
HIGH CPU DETECTED----, CPU:$_snmp_oid_val%"action 1.02 cli command "enable"action 1.03 cli
command "show clock | append disk0:cpu_stats"action 1.04 cli command "show proc cpu sort |
append disk0:cpu_stats"action 1.05 cli command "Show proc cpu | exc 0.00% | append
disk0:cpu_stats"action 1.06 cli command "Show proc cpu history | append disk0:cpu_stats"action
1.07 cli command "show logging | append disk0:cpu_stats "action 1.08 cli command "show spanning-
tree detail | in ieee|occurr|from|is exec | appenddisk0:cpu_stats"action 1.09 cli command "debug
netdr cap rx | append disk0:cpu_stats"action 1.10 cli command "show netdr cap | append
disk0:cpu_stats"action 1.11 cli command "undebug all"!
```

**Nota:** El comando del **rx de la captura del netdr del debug** es útil cuando el CPU es elevado debido al process switching de los paquetes en vez de hardware. Captura 4096 paquetes entrantes al CPU cuando se funciona con el comando. El comando es totalmente seguro y es la herramienta más conveniente para CPU elevada los problemas en los 6500. No causa la carga adicional al CPU.

## Utilidades y Herramientas para Determinar el Tráfico que se Impulsa a la CPU

En esta sección, se identifican algunas utilidades y herramientas que pueden ayudarlo a analizar este tráfico.

### Software de sistema Cisco IOS

En Cisco IOS Software, el procesador de switch del Supervisor Engine se conoce como SP, y la MSFC se denomina RP.

El comando **show interface** brinda información básica acerca del estado de la interfaz y la velocidad del tráfico en la interfaz. El comando también ofrece contadores de errores.

```
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
```

En esta salida, puede ver que el tráfico entrante se conmuta en la Capa 3 y no en la Capa 2. Esto indica que el tráfico se impulsa a la CPU.

El comando **show processes cpu** le indica si estos paquetes son de tráfico regular o de tráfico de control.

```
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
```

Si los paquetes se conmutan por proceso, verá que el proceso IP Input consumirá muchos recursos. Ejecute este comando para ver estos paquetes:

show buffers input-interface

```
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
```

Si el tráfico se **conmuta por interrupción**, no podrá ver esos paquetes con el comando **show buffers input-interface**. Si desea ver los paquetes impulsados a RP para que se los conmute por interrupción, puede ejecutar una captura del tipo Switched Port Analyzer (SPAN) del puerto RP.

**Nota:** Refiera a este documento para más información sobre interrupt-switched contra la utilización de la CPU process-switched:

- Sección *Uso Excesivo de la CPU Debido a Interrupciones* de Resolución de Problemas por Uso Excesivo de CPU en Routers Cisco

## SPAN RP-Inband y SP-Inband

Se dispone de un analizador SPAN para el puerto RP o SP en la versión 12.1(19)E de Cisco IOS Software y versiones posteriores.

Ésta es la sintaxis de los comandos:

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

Utilice este sintaxis para el Cisco IOS Software 12.2 versiones SX:

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

**Nota:** Para la versión SXH, usted debe utilizar el **comando monitor session** para configurar una sesión del SPAN local, y después utiliza este comando de asociar a la sesión SPAN al 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 más información sobre estos comandos, refiera a configurar el SPAN local (modo de la configuración de SPAN) en la *guía de configuración de software de la versión 12.2SX del Catalyst 6500*.

A continuación le ofrecemos un ejemplo sobre una consola 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
```

Ahora, el turno de la consola SP. Aquí tiene un ejemplo:

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

**Nota:** En el Cisco IOS 12.2 versiones SX, el comando se han cambiado **para probar el monitor agregan 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:** En el Cisco IOS 12.2 versiones SX, el comando se han cambiado **para probar la demostración 1. del monitor.**

A continuación le ofrecemos un ejemplo sobre una consola 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 de sistema CatOS

En el caso de switches que ejecutan el software de sistema CatOS, el Supervisor Engine ejecuta CatOS y la MSFC ejecuta Cisco IOS Software.

Si ejecuta el comando **show mac**, podrá ver la cantidad de tramas que se impulsan a la MSFC. El puerto 15/1 es la conexión del Supervisor Engine a la MSFC.

**Nota:** El puerto es 16/1 para los motores del supervisor en el slot 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
```

Un incremento veloz en esta cifra indica que los paquetes son impulsados a la MSFC, lo que genera un uso excesivo de la CPU. Entonces, se puede dividir a los paquetes de esta forma:

- Puerto 15/1 o 16/1 de la MSFC del Analizador SPAN
- SPAN sc0

### Puerto 15/1 o 16/1 de la MSFC del Analizador SPAN

Configure una sesión SPAN en la que el origen sea el puerto 15/1 (o el 16/1) de la MSFC y el puerto de destino sea uno Ethernet.

Aquí tiene un ejemplo:

```
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
```

Si usted recoge una traza de sniffer en el puerto 5/10, la traza de sniffer muestra los paquetes que transmiten a y desde el MSFC. Configure a la sesión SPAN como **tx** para capturar los paquetes que se destinan solamente al MSFC, y no del MSFC.

### SPAN sc0

Configure una sesión SPAN con la interfaz **sc0** como origen para poder capturar tramas que se dirijan a la CPU del 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 los módulos Optical Services Modules (OS), usted no puede realizar una captura del SPAN del tráfico.

## Recomendaciones

El uso de la CPU del Supervisor Engine no refleja el rendimiento de reenvío por hardware del switch. Pese a eso, deberá evaluar y controlar el uso de dicha CPU.

1. Evalúe el uso de la CPU del Supervisor Engine para el switch en una red estable con patrones y carga de tráfico normales.Observe qué procesos generan el mayor uso de recursos de la CPU.
2. Cuando resuelva problemas relacionados con el uso de la CPU, tenga en cuenta estas preguntas:¿Qué procesos generan el uso más elevado? ¿Difieren estos procesos de su evaluación inicial?¿El uso de la CPU resulta siempre excesivo y supera la línea de base? ¿O se registran picos de uso excesivo y, posteriormente, se regresa a los niveles iniciales?¿Existen notificaciones del tipo Topology Change Notifications (TCN) en la red?**Nota:** Los puertos inestables o los puertos de host con los minusválidos del STP portfast causan los TCN.¿Se registra tráfico broadcast o multicast excesivo en las subredes/VLAN de administración?¿Se registra tráfico de administración excesivo, como consultas SNMP, en el switch?
3. Durante el alto hora de la CPU (cuando el CPU es el 75% o arriba), recoja la salida de estos comandos:***show clock***show versionmuestre la CPU de los procesos clasificadamuestre el historial CPU del procshow log
4. De ser posible, aísle la VLAN de administración de las VLAN con tráfico de datos de usuario, particularmente en tráfico pesado de broadcast.Entre algunos ejemplos de este tipo de tráfico podemos mencionar: IPX RIP/Service Advertising Protocol (SAP), AppleTalk y otras clases de tráfico broadcast. Este tráfico puede afectar el uso de la CPU del Supervisor Engine y, en casos extremos, interferir con la funcionamiento normal del switch.
5. Si el consumo de recursos de la CPU es excesivo debido a que se impulsa tráfico al RP, determine cuál es el tráfico y por qué se lo impulsa.Para poder hacerlo, emplee las utilidades que describe la sección Utilidades y Herramientas para Determinar el Tráfico que se Impulsa a la CPU.

## Información Relacionada

- Comandos útiles para resolver problemas CPU elevada en el Catalyst 6500's con el Sup720
- Mensajes de Error Comunes de CatOS en Catalyst 6500/6000 Series Switches
- Mensajes de error frecuente en los Catalyst 6500/6000 Series Switch que funcionan con el Cisco IOS Software
- Solución de problemas de hardware y problemas comunes en switches Catalyst Serie 6500/6000 con software de sistema Cisco IOS
- Saturación de unidifusión en redes de oficinas centrales conmutadas
- Soporte de productos de los Cisco Catalyst 6500 Series Switch
- Script EEM para recoger los datos durante CPU elevada el problema intermitente
- Soporte de Producto de LAN
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems