Uso elevado de la CPU en switches Catalyst 4500 basados en el software Cisco IOS

Contenido

Introducción

Los switches Catalyst 4500 Series, que incluyen los switches Catalyst 4948, tienen una metodología de dirección del paquete sofisticada para el tráfico dirigido hacia la CPU. Un problema comúnmente conocido es la elevada utilización de la CPU de estos switches. Este documento proporciona detalles sobre la arquitectura de dirección del paquete de la CPU y muestra cómo identificar las causas de la elevada utilización de la CPU en estos switches. El documento también enumera algunos escenarios comunes de configuración o de red que causan una elevada utilización de la CPU en las series Catalyst 4500.

Nota: Si ejecuta switches Catalyst 4500/4000 Series basados en Catalyst OS (CatOS), consulte el documento Utilización de CPU en Catalyst 4500/4000, 2948G, 2980G y 4912G Switches que Ejecutan CatOS Software ...

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Catalyst 4500 Series Switch
- Catalyst 4948 Series Switch

Nota: Este documento se aplica solamente a los switches basados en software Cisco IOS® y no a los switches basados en CatOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Antecedentes

Antes de observar la arquitectura de gestión de paquetes de la CPU y solucionar problemas de alto uso de la CPU, debe entender las diferentes formas en las que los switches de reenvío basados en hardware y los routers basados en software de Cisco IOS usan la CPU. El error común es creer que el alto uso de la CPU indica el agotamiento de recursos en un dispositivo y la amenaza de un fallo. Un problema de capacidad es uno de los síntomas de alto uso de la CPU en los routers de Cisco IOS. Sin embargo, un problema de capacidad casi nunca es un síntoma de uso elevado de la CPU con switches de reenvío basados en hardware como el Catalyst 4500. El Catalyst 4500 está diseñado para reenviar paquetes en el circuito integrado específico de la aplicación de hardware (ASIC) y alcanzar velocidades de reenvío de tráfico de hasta 102 millones de paquetes por segundo (Mpps).

La CPU Catalyst 4500 realiza estas funciones:

- Administra protocolos de software configurados, por ejemplo:Spanning Tree Protocol (STP)Protocolo de ruteoProtocolo de detección de Cisco (CDP)Port Aggregation Protocol (PAgP)Protocolo troncal VLAN (VTP)Protocolo de concentración de enlaces dinámico (DTP)
- Programas, configuración/entradas dinámicas a los ASIC de hardware, por ejemplo:Listas de Control de Acceso (ACLs)entradas CEF
- Administra internamente varios componentes, por ejemplo:Tarjetas de línea Power over Ethernet (PoE)Fuentes de alimentaciónBandeja de ventilador
- Administra el acceso al switch, por ejemplo:TELNETConsola‘Protocolo de administración de

red simple (SNMP)
- Reenvía los paquetes a través de la trayectoria del software, por ejemplo:Paquetes enrutados por Internetwork Packet Exchange (IPX), que sólo se admiten en la ruta de softwareFragmentación máxima de la unidad de transmisión (MTU)

Según esta lista, el uso elevado de la CPU puede ser el resultado de la recepción o el proceso de paquetes por parte de la CPU. Algunos de los paquetes que se envían para el proceso pueden ser esenciales para el funcionamiento de la red. Un ejemplo de estos paquetes esenciales es la unidad de datos de protocolo de puente (BPDU) para las configuraciones de topología de árbol de extensión. Sin embargo, otros paquetes pueden ser tráfico de datos reenviados por software. Estos escenarios requieren que los ASIC de conmutación envíen paquetes a la CPU para su procesamiento:

- Paquetes que se copian a la CPU, pero los paquetes originales se conmutan en hardwareUn ejemplo es el aprendizaje de la dirección MAC del host.
- Paquetes que se envían a la CPU para su procesamientoAlgunos ejemplos son:Actualizaciones de Routing ProtocolBPDUInundación intencional o no intencional de tráfico
- Paquetes que se envían a la CPU para su reenvíoUn ejemplo son los paquetes que necesitan ruteo IPX o AppleTalk.

Comprensión de la arquitectura de manejo de paquetes de CPU Catalyst 4500

El Catalyst 4500 tiene un mecanismo de calidad de servicio (QoS) integrado para diferenciar entre tipos de tráfico destinados a la CPU. El mecanismo realiza la diferenciación sobre la base de la información del paquete de Capa 2 (L2)/Capa 3 (L3)/Capa 4 (L4). El Supervisor Packet Engine tiene 16 colas para manejar varios tipos de paquetes o eventos. La figura 1 muestra estas colas. La tabla 1 enumera las colas y los tipos de paquetes que se colocan en cada cola. Las 16 colas permiten al Catalyst 4500 poner en cola los paquetes según el tipo de paquete o la prioridad.

Figura 1: Catalyst 4500 utiliza varias colas de CPU

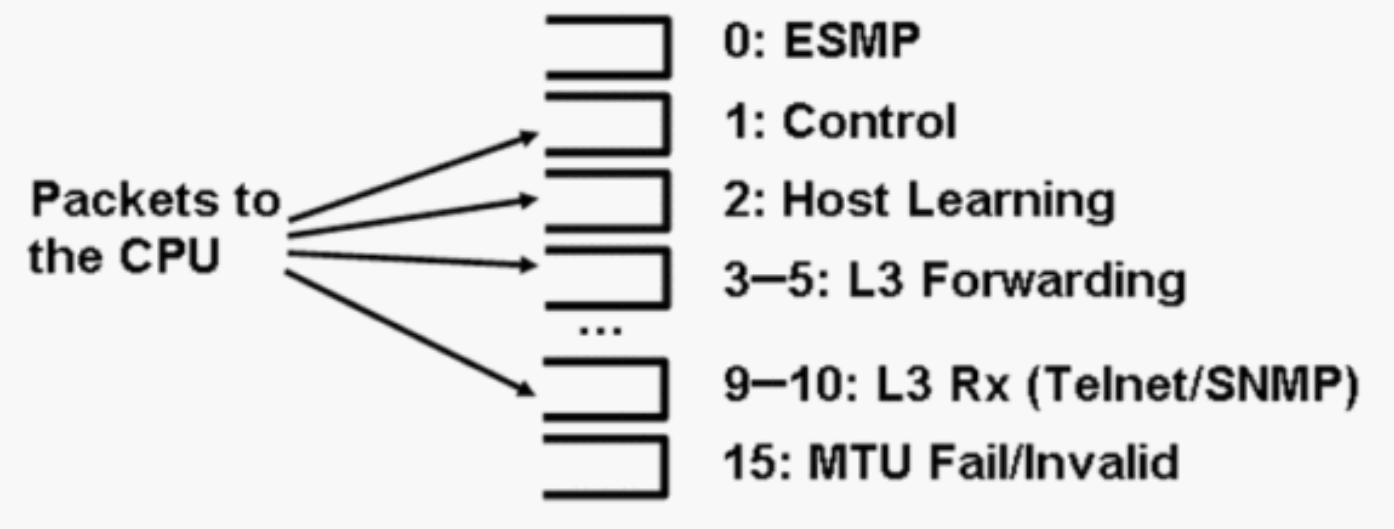


Tabla 1 - Descripción de la Cola Catalyst 4500

Número	Nombre de cola	Paquetes en cola

de cola		
0	Esmp	Paquetes ESMP[1] (paquetes de administración interna) para los ASIC de tarjeta de línea u otra administración de componentes
1	Control	Paquetes de plano de control L2, como STP, CDP, PAgP, LACP[2] o UDLD[3]
2	Aprendizaje de host	Tramas con direcciones MAC de origen desconocidas que se copian a la CPU para construir la tabla de reenvío L2
3, 4, 5	L3 Fwd más alto, L3 Fwd alto/medio, L3 Fwd más bajo	Paquetes que se deben reenviar en el software, como los túneles GRE [4] Si el ARP [5] no se resuelve para la dirección IP de destino, los paquetes se envían a esta cola.
6, 7, 8	L2 Fwd más alto, L2 Fwd alto/medio, L2 Fwd bajo	Paquetes que se reenvían como resultado de la conexión en puente • Los protocolos que no se soportan en el hardware, como los paquetes ruteados IPX y AppleTalk, se puentean con la CPU • petición y respuesta ARP • Los paquetes con una dirección MAC de destino de la interfaz SVI[6]/L3 del switch se puentean si los paquetes no se pueden rutear en hardware debido a: Opciones de encabezado IPTTL[7] vencidoEncapsulación no ARPA
9, 10	L3 Rx Alta, L3 Rx Baja	El tráfico del plano de control L3, por ejemplo, los protocolos de ruteo, que están destinados a las direcciones IP de la CPU Los ejemplos incluyen Telnet, SNMP y SSH [8].
11	Falla de RPF	Paquetes de multidifusión que fallaron la verificación RPF[9]
12	ACL fwd(snooping)	Paquetes que son procesados por las funciones de snooping de DHCP [10], de inspección dinámica ARP o de snooping de IGMP [11].
13	registro ACL, no alcanzar	Paquetes que alcanzan un ACE[12] con la palabra clave **log** o paquetes que fueron descartados debido a una denegación en una ACL de salida o la falta de una ruta al destino Estos paquetes requieren la generación de mensajes ICMP

		inalcanzables.
14	procesamiento de ACL SW	Paquetes impulsados a la CPU debido a la falta de recursos de hardware ACL adicionales, como TCAM[13], para ACL de seguridad
15	Error de MTU/No válido	Paquetes que deben fragmentarse porque el tamaño de MTU de la interfaz de salida es menor que el tamaño del paquete

[1] ESMP = Incluso protocolo simple de administración.

[2] LACP = Link Aggregation Control Protocol .

[3] UDLD = Detección de Link Unidireccional.

[4] GRE = encapsulación de ruteo genérico.

[5] ARP = Protocolo de resolución de direcciones.

[6] SVI = interfaz virtual conmutada.

[7] TTL = Tiempo de vida.

[8] SSH = protocolo de shell seguro.

[9] RPF = Reenvío de Trayectoria Inversa

[10] DHCP = Protocolo de configuración dinámica de host.

[11] IGMP = Internet Group Management Protocol .

[12] ACE = entrada de control de acceso.

[13] TCAM = memoria direccionable de contenido ternario.

Estas colas son colas separadas:

- `L2 Fwd Highest` **O** `L3 Fwd Highest`
- `L2 Fwd High/Medium` **O** `L3 Fwd High/Medium`
- `L2 Fwd Low` **O** `L3 Fwd Low`
- `L3 Rx Alta` **O** `L3 Rx Baja`

Los paquetes se ponen en cola en estas colas en función de la etiqueta de QoS, que es el valor de punto de código de servicios diferenciados (DSCP) del tipo de servicio IP (ToS). Por ejemplo, los paquetes con un DSCP de 63 se colocan en la cola `L3 Fwd Highest` queue. Puede ver los paquetes recibidos y descartados para estas 16 colas en el resultado del comando **show platform cpu packet statistics all**. El resultado de este comando es muy largo. Ejecute el comando **show platform cpu packet statistics** para mostrar solamente los eventos que no son cero. Un comando alternativo es el comando **show platform cpuport**. Utilice solamente el comando **show platform cpuport** si ejecuta Cisco IOS Software Release 12.1(11)EW o anterior. Este comando ha sido obsoleto. Sin embargo, este comando más antiguo formaba parte del comando **show tech-support** en las versiones del software Cisco IOS anteriores a la versión 12.2(20)EWA del software Cisco IOS.

Utilice el comando **show platform cpu packet statistics** para la resolución de problemas.

```
Switch#show platform cpu packet statistics all
!--- Output suppressed. Total packet queues 16 Packets Received by Packet Queue Queue Total 5
sec avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- --------
- --------- ---------- Esmp 0 0 0 0 0 Control 48 0 0 0 0 Host Learning 0 0 0 0 0 L3 Fwd High 0 0
0 0 0 L3 Fwd Medium 0 0 0 0 0 L3 Fwd Low 0 0 0 0 0 L2 Fwd High 0 0 0 0 0 L2 Fwd Medium 0 0 0 0 0
L2 Fwd Low 0 0 0 0 0 L3 Rx High 0 0 0 0 0 L3 Rx Low 0 0 0 0 0 RPF Failure 0 0 0 0 0 ACL
fwd(snooping) 0 0 0 0 0 ACL log, unreach 0 0 0 0 0 ACL sw processing 0 0 0 0 0 MTU Fail/Invalid
0 0 0 0 0 Packets Dropped by Packet Queue Queue Total 5 sec avg 1 min avg 5 min avg 1 hour avg -
---------------------- --------------- --------- --------- --------- ---------- Esmp 0 0 0 0 0
Control 0 0 0 0 0 Host Learning 0 0 0 0 0 L3 Fwd High 0 0 0 0 0 L3 Fwd Medium 0 0 0 0 0 L3 Fwd
Low 0 0 0 0 0 L2 Fwd High 0 0 0 0 0 L2 Fwd Medium 0 0 0 0 0 L2 Fwd Low 0 0 0 0 0 L3 Rx High 0 0
0 0 0 L3 Rx Low 0 0 0 0 0 RPF Failure 0 0 0 0 0 ACL fwd(snooping) 0 0 0 0 0 ACL log, unreach 0 0
0 0 0 ACL sw processing 0 0 0 0 0 MTU Fail/Invalid 0 0 0 0 0
```

La CPU Catalyst 4500 asigna pesos a las diversas colas que enumera la Tabla 1. La CPU asigna los pesos en función de la importancia, o tipo, y en función de la prioridad de tráfico, o DSCP. La CPU presta servicios a la cola en función de los pesos relativos de la cola. Por ejemplo, si un paquete de control, como una BPDU, y una solicitud de eco ICMP están pendientes, la CPU atiende primero el paquete de control. Una cantidad excesiva de tráfico de baja prioridad o menos importante no priva a la CPU de la capacidad de procesar o administrar el sistema. Este mecanismo garantiza que la red sea estable incluso bajo una alta utilización de la CPU. Esta capacidad de la red para permanecer estable es información crítica que debe comprender.

Hay otro detalle de implementación muy importante de la gestión de paquetes de CPU de Catalyst 4500. Si la CPU ya ha prestado servicio a paquetes o procesos de alta prioridad pero tiene más ciclos de CPU de repuesto durante un período de tiempo determinado, la CPU presta servicios a los paquetes de cola de baja prioridad o realiza procesos en segundo plano de menor prioridad. El uso elevado de la CPU como resultado del procesamiento de paquetes de baja prioridad o de los procesos en segundo plano se considera normal porque la CPU constantemente intenta utilizar todo el tiempo disponible. De esta manera, la CPU se esfuerza por lograr el máximo rendimiento del switch y la red sin poner en peligro la estabilidad del switch. El Catalyst 4500 considera que la CPU está infrautilizada a menos que la CPU se utilice al 100% para una sola ranura de tiempo.

Cisco IOS Software Release 12.2(25)EWA2 y posteriores han mejorado el mecanismo y la contabilidad de manejo de procesos y paquetes de la CPU. Por lo tanto, utilice estas versiones en sus implementaciones de Catalyst 4500.

Identificación del motivo del uso elevado de la CPU en Catalyst 4500

Ahora que comprende la arquitectura y el diseño de administración de paquetes de la CPU de Catalyst 4500, es posible que desee identificar por qué su uso de la CPU de Catalyst 4500 es elevado. El Catalyst 4500 tiene los comandos y herramientas necesarios para identificar la causa raíz de la alta utilización de la CPU. Después de identificar el motivo, los administradores pueden realizar cualquiera de estas acciones:

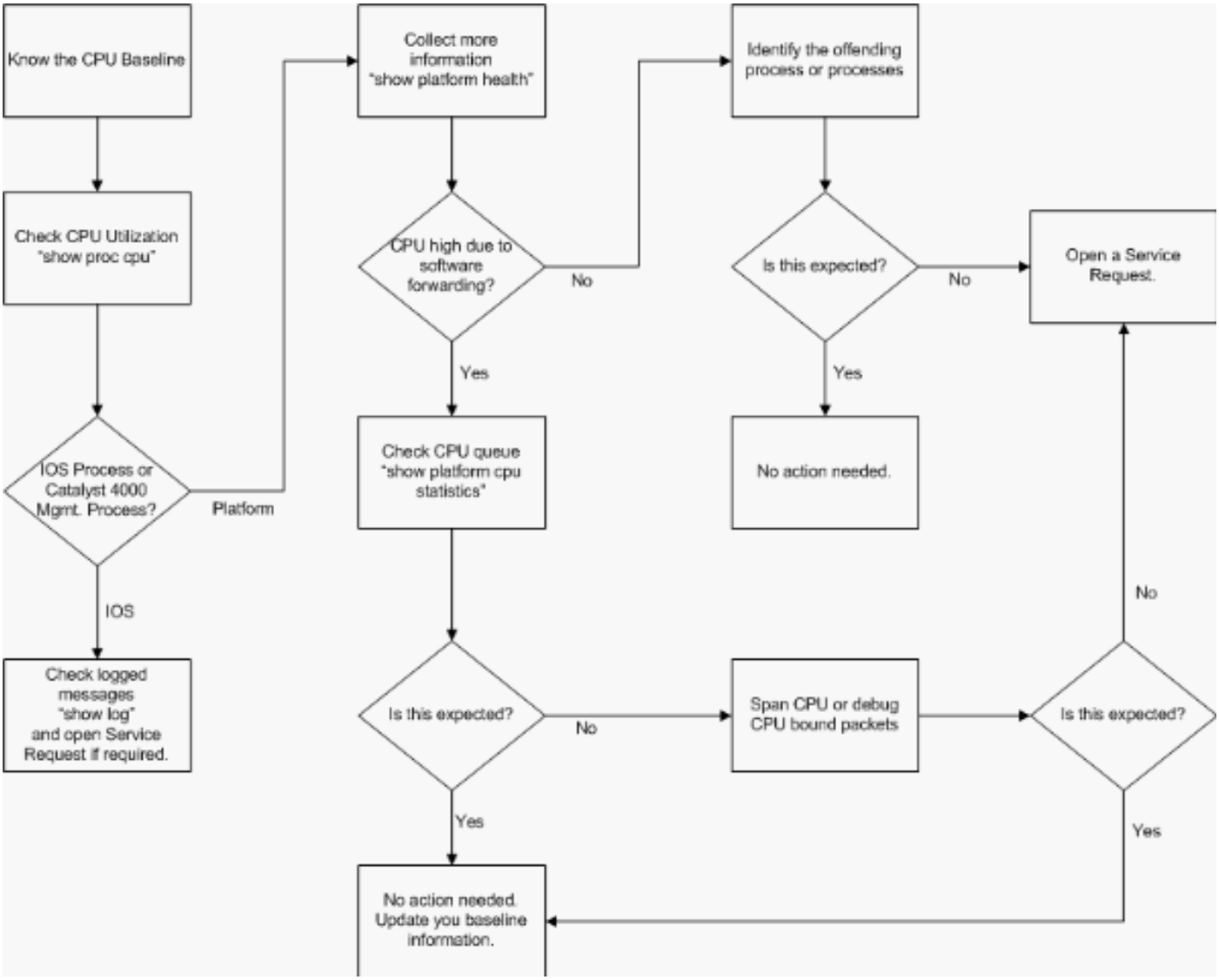
- Acción correctiva: puede incluir cambios en la configuración o en la red, o la creación de una solicitud de servicio de soporte técnico de Cisco para un análisis posterior.
- Sin acción: el Catalyst 4500 funciona según las expectativas. La CPU muestra una alta utilización de la CPU porque Supervisor Engine maximiza los ciclos de la CPU para realizar

todos los trabajos de reenvío de paquetes de software y de fondo necesarios.

Asegúrese de identificar el motivo de la alta utilización de la CPU aunque no sea necesario realizar acciones correctivas en todos los casos. La alta utilización de la CPU puede ser sólo un síntoma de un problema en la red. Puede ser necesaria una resolución de la causa raíz de ese problema para reducir la utilización de la CPU.

La Figura 2 muestra la metodología de troubleshooting que se debe utilizar para identificar la causa raíz de la alta utilización de la CPU del Catalyst 4500.

Figura 2: Metodología de solución de problemas de uso elevado de la CPU en switches Catalyst 4500



Los pasos generales para la resolución de problemas son:

1. Ejecute el comando **show processes cpu** para identificar los procesos de Cisco IOS que consumen ciclos de CPU.
2. Ejecute el comando **show platform health** para identificar aún más los procesos específicos de la plataforma.
3. Si el proceso altamente activo es `K2CpuMan Review`, ejecute el comando **show platform cpu packet statistics** para identificar el tipo de tráfico que llega a la CPU.Si la actividad no se debe al proceso `K2CpuMan Review`, omita el Paso 4 y vaya al Paso 5.
4. Identifique los paquetes que golpean la CPU con el uso de las Herramientas de Troubleshooting para Analizar el Tráfico Destinado a la CPU, si es necesario.Un ejemplo de

las herramientas de solución de problemas que se deben utilizar es el analizador de puertos conmutados (SPAN) de la CPU.

5. Revise este documento y la sección Solución de problemas comunes de uso elevado de la CPU para causas comunes.Si todavía no puede identificar la causa principal, póngase en contacto con el Soporte Técnico de Cisco.

Base del uso de la CPU

El primer paso importante es conocer el uso de la CPU de su switch para su configuración y configuración de red. Utilice el comando **show processes cpu** para identificar la utilización de la CPU en el switch Catalyst 4500. La actualización continua de la utilización de la CPU básica puede ser necesaria a medida que agrega más configuración a la configuración de la red o que cambia el patrón de tráfico de la red. La figura 2 indica este requisito.

Esta salida es de un Catalyst 4507R completamente cargado. La CPU de estado estacionario es de alrededor del 32 a 38 por ciento, lo que es necesario para realizar las funciones de administración para este switch:

```
Switch#show processes cpu
CPU utilization for five seconds: 38%/1%; one minute: 32%; five minutes: 32%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        63          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          60     50074          1  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 Deferred Events
!--- Output suppressed. 27 524 250268 2 0.00% 0.00% 0.00% 0 TTY Background 28 816 254843 3 0.00%
0.00% 0.00% 0 Per-Second Jobs 29 101100 5053 20007 0.00% 0.01% 0.00% 0 Per-minute Jobs 30
26057260  26720902        975 12.07% 11.41% 11.36%   0 Cat4k Mgmt HiPri
  31    19482908  29413060        662 24.07% 19.32% 19.20%   0 Cat4k Mgmt LoPri
  32        4468    162748         27  0.00%  0.00%  0.00%   0 Galios Reschedul
  33           0         1          0  0.00%  0.00%  0.00%   0 IOS ACL Helper
  34           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager
```

El uso de CPU de cinco segundos se expresa como:

x%/*y*%

El *x*% representa la utilización total de la CPU y el *y*% representa la CPU que se gasta en el nivel de interrupción. Cuando resuelva problemas con los switches Catalyst 4500, concéntrese solamente en el uso total de la CPU.

Comprender el comando show processes cpu en los switches Catalyst 4500

Esta salida **show processes cpu** muestra que hay dos procesos que utilizan la CPU: **Cat4k Mgmt HiPri** y **Cat4k Mgmt LoPri** . Estos dos procesos agregan varios procesos específicos de la plataforma que realizan las funciones de administración esenciales en el Catalyst 4500. Estos procesos procesan el plano de control, así como los paquetes de datos que necesitan ser conmutados o procesados por software.

Para ver cuál de los procesos específicos de la plataforma usa la CPU en el contexto de **Cat4k Mgmt HiPri** y **Cat4k Mgmt LoPri**, ejecute el comando **show platform health**.

Cada uno de los procesos específicos de la plataforma tiene un uso objetivo/esperado de la CPU. Cuando ese proceso se encuentra dentro del objetivo, la CPU ejecuta el proceso en el contexto

de alta prioridad. El resultado del comando **show processes cpu** cuenta esa utilización bajo **Cat4k Mgmt HiPri** . Si un proceso excede el objetivo/utilización esperada, ese proceso se ejecuta en el contexto de baja prioridad. El resultado del comando **show processes cpu** cuenta esa utilización adicional bajo **Cat4k Mgmt LoPri**. Este **Cat4k Mgmt LoPri** también se utiliza para ejecutar procesos en segundo plano y otros de baja prioridad, como la verificación de consistencia y la lectura de contadores de interfaz. Este mecanismo permite a la CPU ejecutar procesos de alta prioridad cuando sea necesario, y los ciclos de CPU inactivos que permanecen se utilizan para los procesos de baja prioridad. Superar el uso de CPU objetivo en una cantidad pequeña, o un pico momentáneo en la utilización, no es una indicación de un problema que necesita investigación.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review    3.00   0.29     10      3  100  500    0   0    0  11:15
S2w-JobEventSchedule  10.00   0.32     10      7  100  500    0   0    0  10:14
Stub-JobEventSchedul  10.00  12.09     10      6  100  500   14  13    9  396:35
StatValueMan Update    1.00   0.22      1      0  100  500    0   0    0  6:28
Pim-review             0.10   0.00      1      0  100  500    0   0    0  0:22
Ebm-host-review        1.00   0.00      8      0  100  500    0   0    0  0:05
Ebm-port-review        0.10   0.00      1      0  100  500    0   0    0  0:01
Protocol-aging-revie   0.20   0.00      2      0  100  500    0   0    0  0:00
Acl-Flattener  e       1.00   0.00     10      0  100  500    0   0    0  0:00
KxAclPathMan create/   1.00   0.00     10      5  100  500    0   0    0  0:39
KxAclPathMan update    2.00   0.00     10      0  100  500    0   0    0  0:00
KxAclPathMan reprogr   1.00   0.00      2      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10      0  100  500    0   0    0  0:00
K2CpuMan Review       30.00  10.19     30     28  100  500   14  13    9  397:11
K2AccelPacketMan: Tx  10.00   2.20     20      0  100  500    2   2    1  82:06
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
K2AclCamMan stale en   1.00   0.00     10      0  100  500    0   0    0  0:00
K2AclCamMan hw stats   3.00   1.04     10      5  100  500    1   1    0  39:36
K2AclCamMan kx stats   1.00   0.00     10      5  100  500    0   0    0  13:40
K2AclCamMan Audit re   1.00   0.00     10      5  100  500    0   0    0  13:10
K2AclPolicerTableMan   1.00   0.00     10      1  100  500    0   0    0  0:38
K2L2 Address Table R   2.00   0.00     12      5  100  500    0   0    0  0:00
K2L2 New Static Addr   2.00   0.00     10      1  100  500    0   0    0  0:00
K2L2 New Multicast A   2.00   0.00     10      5  100  500    0   0    0  0:01
K2L2 Dynamic Address   2.00   0.00     10      0  100  500    0   0    0  0:00
K2L2 Vlan Table Revi   2.00   0.00     12      9  100  500    0   0    0  0:01
K2 L2 Destination Ca   2.00   0.00     10      0  100  500    0   0    0  0:00
K2PortMan Review       2.00   0.72     15     11  100  500    1   1    0  37:22
Gigaport65535 Review   0.40   0.07      4      2  100  500    0   0    0  3:38
Gigaport65535 Review   0.40   0.08      4      2  100  500    0   0    0  3:39
K2Fib cam usage revi   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib IrmFib Review    2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib Vrf Default Ro   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib AdjRepop Revie   2.00   0.00     15      0  100  500    0   0    0  0:00
K2Fib Vrf Unpunt Rev   2.00   0.01     15      0  100  500    0   0    0  0:23
K2Fib Consistency Ch   1.00   0.00      5      2  100  500    0   0    0  29:25
K2FibAdjMan Stats Re   2.00   0.30     10      4  100  500    0   0    0  6:21
K2FibAdjMan Host Mov   2.00   0.00     10      4  100  500    0   0    0  0:00
K2FibAdjMan Adj Chan   2.00   0.00     10      0  100  500    0   0    0  0:00
K2FibMulticast Signa   2.00   0.01     10      2  100  500    0   0    0  2:04
K2FibMulticast Entry   2.00   0.00     10      7  100  500    0   0    0  0:00
K2FibMulticast Irm M   2.00   0.00     10      7  100  500    0   0    0  0:00
K2FibFastDropMan Rev   2.00   0.00      7      0  100  500    0   0    0  0:00
K2FibPbr route map r   2.00   0.06     20      5  100  500    0   0    0  16:42
K2FibPbr flat acl pr   2.00   0.07     20      2  100  500    0   0    0  3:24
```

```
K2FibPbr consolidati    2.00    0.01      10       0  100   500     0    0     0  0:24
K2FibPerVlanPuntMan     2.00    0.00      15       4  100   500     0    0     0  0:00
K2FibFlowCache flow     2.00    0.01      10       0  100   500     0    0     0  0:23
K2FibFlowCache flow     2.00    0.00      10       0  100   500     0    0     0  0:00
K2FibFlowCache adj r    2.00    0.01      10       0  100   500     0    0     0  0:20
K2FibFlowCache flow     2.00    0.00      10       0  100   500     0    0     0  0:06
K2MetStatsMan Review    2.00    0.14       5       2  100   500     0    0     0  23:40
K2FibMulticast MET S    2.00    0.00      10       0  100   500     0    0     0  0:00
K2QosDblMan Rate DBL    2.00    0.12       7       0  100   500     0    0     0  4:52
IrmFibThrottler Thro    2.00    0.01       7       0  100   500     0    0     0  0:21
K2 VlanStatsMan Revi    2.00    1.46      15       7  100   500     2    2     1  64:44
K2 Packet Memory Dia    2.00    0.00      15       8  100   500     0    1     1  45:46
K2 L2 Aging Table Re    2.00    0.12      20       3  100   500     0    0     0  7:22
RkiosPortMan Port Re    2.00    0.73      12       7  100   500     1    1     1  52:36
Rkios Module State R    4.00    0.02      40       1  100   500     0    0     0  1:28
Rkios Online Diag Re    4.00    0.02      40       0  100   500     0    0     0  1:15
RkiosIpPbr IrmPort R    2.00    0.02      10       3  100   500     0    0     0  2:44
RkiosAclMan Review      3.00    0.06      30       0  100   500     0    0     0  2:35
MatMan Review           0.50    0.00       4       0  100   500     0    0     0  0:00
Slot 3 ILC Manager R    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 3 ILC S2wMan Re    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 4 ILC Manager R    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 4 ILC S2wMan Re    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 5 ILC Manager R    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 5 ILC S2wMan Re    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 6 ILC Manager R    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 6 ILC S2wMan Re    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 7 ILC Manager R    3.00    0.00      10       0  100   500     0    0     0  0:00
Slot 7 ILC S2wMan Re    3.00    0.00      10       0  100   500     0    0     0  0:00
EthHoleLinecardMan(1    1.66    0.04      10       0  100   500     0    0     0  1:18
EthHoleLinecardMan(2    1.66    0.02      10       0  100   500     0    0     0  1:18
EthHoleLinecardMan(6    1.66    0.17      10       6  100   500     0    0     0  6:38
                      ------------
%CPU Totals           212.80   35.63
```

Comprender el comando show platform health en los switches Catalyst 4500

El comando **show platform health** proporciona mucha información que sólo es relevante para un ingeniero de desarrollo. Para resolver problemas de uso elevado de la CPU, busque un número mayor en la columna `%CPU real` en la salida. Además, asegúrese de echar un vistazo al lado derecho de esa fila para verificar el uso de la CPU de ese proceso en las columnas `promedio %CPU` de 1 minuto y 1 hora. A veces, los procesos llegan a un pico momentáneo pero no retienen la CPU durante mucho tiempo. Parte del uso momentáneamente elevado de la CPU se produce durante la programación de hardware o la optimización de la programación. Por ejemplo, un pico de utilización de CPU es normal durante la programación de hardware de una ACL grande en el TCAM.

En el resultado del comando **show platform health** en la sección Comprender el comando show processes cpu en los switches Catalyst 4500, los procesos **`Stub-JobEventSchedul`** y K2CpuMan Review utilizan un mayor número de ciclos de CPU. La tabla 2 proporciona información básica sobre los procesos específicos de la plataforma común que aparecen en el resultado del comando **show platform health**.

Tabla 2: Descripción de los Procesos Específicos de la Plataforma del Comando show platform health

Nombre de proceso específico	Descripción

de la plataforma	
Revisión Pim	Gestión del estado del chasis/tarjeta de línea
Ebm	Módulo de puente Ethernet, como envejecimiento y supervisión
Acl-Flattener / K2AclMan	Proceso de fusión de ACL
KxAclPathMan - Path TagMan-Review	Administración y mantenimiento del estado de ACL
K2CpuMan Review	El proceso que realiza el reenvío de paquetes de software Si ve un uso elevado de la CPU debido a este proceso, investigue los paquetes que golpean a la CPU con el uso del comando **show platform cpu packet statistics**.
K2AccelPacketMan	El driver que interactúa con el motor de paquetes para enviar paquetes que están destinados desde la CPU
K2AclCamMan	Administra el hardware TCAM de entrada y salida para QoS y funciones de seguridad
K2AclPolicerTableMan	Administra los reguladores de entrada y salida
K2L2	Representa el subsistema de reenvío L2 del software Catalyst 4500 Cisco IOS Estos procesos son responsables del mantenimiento de las diversas tablas L2.
K2PortMan Review	Administra las diversas funciones de programación relacionadas con los puertos
K2Fib	gestión FIB[1]
K2FibFlowCache	Administración de caché de PBR [2]
K2FibAdjMan	Administración de tabla de adyacencia FIB
K2FibMulticast	Administra entradas FIB de multidifusión
K2MetStatsMan Review	Administra estadísticas del [TEM3]
K2QosDblMan Review	Administra QoS DBL[4]
Thro de IrmFibThrottler	módulo de IP Routing
Tabla de antigüedad de K2 L2 Re	Administra la función de envejecimiento L2
GalChassisVp-review	Supervisión del estado del chasis
Programación de eventos de	Administra los protocolos S2W[5] para supervisar el estado de las tarjetas de línea

trabajo S2w	
Stub-JobEventSchedul	Supervisión y mantenimiento de tarjetas de línea basadas en ASIC Stub
Puerto RkiosPortMan Re	Supervisión y mantenimiento del estado del puerto
Estado R del módulo Rkios	Supervisión y mantenimiento de tarjetas de línea
EthHoleLinecardMan	Administra GBICs [6] en cada una de las tarjetas de línea

[1] FIB = Base de Información de Reenvío.

[2] PBR = ruteo basado en políticas.

[3] MET = Tabla de expansión de multidifusión.

[4] DBL = Límite de búfer dinámico.

[5] S2W = serial a cable.

[6] GBIC = Conversor de interfaz Gigabit.

Solución de problemas comunes de uso elevado de la CPU

Esta sección cubre algunos de los problemas comunes de uso elevado de la CPU en los switches Catalyst 4500.

Uso elevado de la CPU debido a paquetes conmutados por proceso

Una de las razones comunes para la alta utilización de la CPU es que la CPU Catalyst 4500 está ocupada con el proceso de paquetes para paquetes reenviados por software o paquetes de control. Ejemplos de paquetes reenviados por software son IPX o paquetes de control, como BPDU. Un pequeño número de estos paquetes se envía típicamente a la CPU. Sin embargo, un número constantemente grande de paquetes puede indicar un error de configuración o un evento de red. Debe identificar la causa de los eventos que llevan al reenvío de paquetes a la CPU para su procesamiento. Esta identificación le permite depurar los problemas de uso elevado de la CPU.

Algunas de las razones comunes para la alta utilización de la CPU debido a los paquetes conmutados por proceso son:

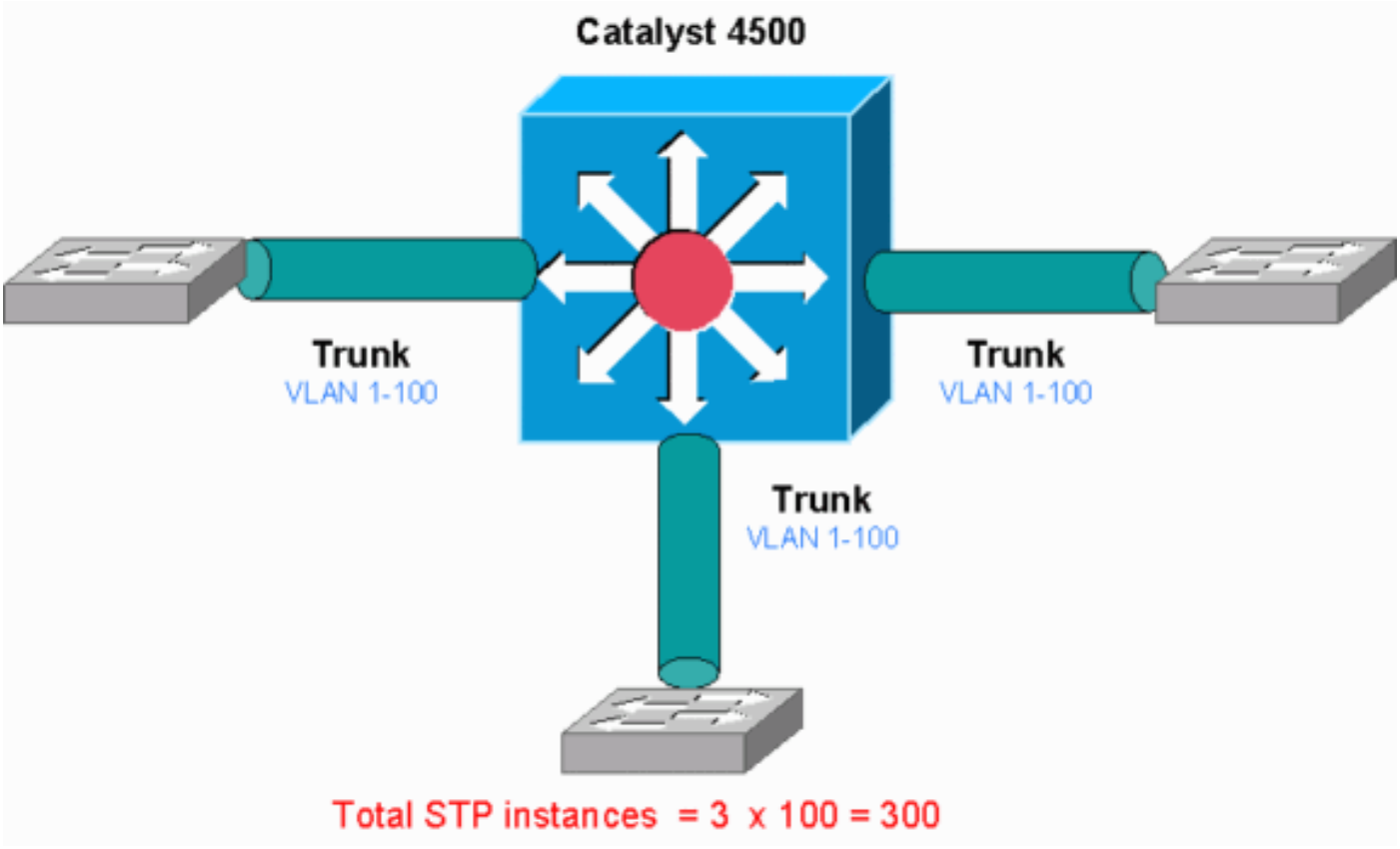
- Un alto número de instancias de puerto de árbol de expansión
- Mensajes de redirección ICMP; paquetes de ruteo en la misma interfaz
- ruteo IPX o AppleTalk
- Aprendizaje de host
- Recursos de hardware (TCAM) para ACL de seguridad
- La palabra clave **log** en ACL
- Loops de reenvío de capa 2

Otras razones para el switch de paquetes a la CPU son:

- Fragmentación de MTU: asegúrese de que todas las interfaces a lo largo de la trayectoria del paquete tengan la misma MTU.
- ACL con indicadores TCP distintos de los **establecidos**
- IP versión 6 (IPv6) Routing: solo se admite a través de la ruta de switching de software.
- GRE: solo se admite a través de la ruta de switching de software.
- Denegación del tráfico en la ACL del router de entrada o salida (RACL)**Nota:** Esto está limitado a la velocidad en Cisco IOS Software Release 12.1(13)EW1 y posteriores.Ejecute el comando **no ip unreachables** bajo la interfaz de la ACL.
- El tráfico ARP y DHCP excesivo llega a la CPU para su procesamiento debido al gran número de hosts conectados directamenteSi sospecha un ataque DHCP, utilice la indagación DCHP para limitar la velocidad del tráfico DHCP desde cualquier puerto host específico.
- Sondeo SNMP excesivo por una estación final legítima o con mal comportamiento

Un alto número de instancias de puerto de árbol de expansión

El Catalyst 4500 admite 3000 instancias de puerto de árbol de extensión o puertos activos en el modo Per VLAN Spanning Tree+ (PVST+). El soporte se encuentra en todos los Supervisor Engines, excepto en el Supervisor Engine II+ y II+TS, y en el Catalyst 4948. El Supervisor Engine II+ y II+TS y el Catalyst 4948 soportan hasta 1500 instancias de puerto. Si excede estas recomendaciones de instancia de STP, el switch muestra una alta utilización de la CPU.



Este diagrama muestra un Catalyst 4500 con tres puertos troncales que llevan VLAN 1 a 100 cada uno. Esto equivale a 300 instancias de puerto de árbol de expansión. En general, puede calcular instancias de puerto de árbol de expansión con esta fórmula:

```
Total number of STP instances = Number of access ports + Sum of all VLANs
that are carried in each of the trunks
```

En el diagrama, no hay puertos de acceso, pero los tres troncales llevan VLAN 1 a 100:

```
Total number of STP instances = 0 + 100 + 100 + 100 = 300
```

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Esta sección revisa los comandos que utiliza un administrador para reducir el problema de uso elevado de la CPU. Si ejecuta el comando **show processes cpu**, puede ver que dos procesos principales, **Cat4k Mgmt LoPri** y **Spanning Tree** , utilizan principalmente la CPU. Con sólo esta información, usted sabe que el proceso del árbol de expansión consume una porción considerable de los ciclos de CPU.

```
Switch#show processes cpu
CPU utilization for five seconds: 74%/1%; one minute: 73%; five minutes: 50%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4       198         20  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       290         13  0.00%  0.00%  0.00%   0 Load Meter
!--- Output suppressed. 25 488 33 14787 0.00% 0.02% 0.00% 0 Per-minute Jobs 26 90656 223674 405
6.79% 6.90% 7.22% 0 Cat4k Mgmt HiPri  27      158796     59219       2681 32.55% 33.80% 21.43%
0 Cat4k Mgmt LoPri
  28          20      1693         11  0.00%  0.00%  0.00%   0 Galios Reschedul
  29           0         1          0  0.00%  0.00%  0.00%   0 IOS ACL Helper
  30           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager
!--- Output suppressed. 41 0 1 0 0.00% 0.00% 0.00% 0 SFF8472 42 0 2 0 0.00% 0.00% 0.00% 0 AAA
Dictionary R  43       78564     20723       3791 32.63% 30.03% 17.35%   0 Spanning Tree
  44         112       999        112  0.00%  0.00%  0.00%   0 DTP Protocol
  45           0       147          0  0.00%  0.00%  0.00%   0 Ethchnl
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

Para entender qué proceso específico de la plataforma consume la CPU, ejecute el comando **show platform health**. A partir de este resultado, puede ver que el proceso **K2CpuMan Review, un trabajo para manejar paquetes enlazados a la CPU, utiliza la CPU:**

```
Switch#show platform health
%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                  Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
!--- Output suppressed. TagMan-RecreateMtegR 1.00 0.00 10 0 100 500 0 0 0 0:00 K2CpuMan Review
30.00  37.62     30     53  100  500   41  33    1  2:12
K2AccelPacketMan: Tx  10.00   4.95     20      0  100  500    5   4    0  0:36
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Ejecute el comando **show platform cpu packet statistics** para verificar qué cola de la CPU recibe el paquete enlazado a la CPU. El resultado de esta sección muestra que la cola de control recibe un montón de paquetes. Utilice la información de la Tabla 1 y la conclusión que extrajo en el Paso 1. Puede determinar que los paquetes que procesa la CPU y la razón de la alta utilización de la CPU es el procesamiento de BPDU.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Total packet queues 16 Packets Received by Packet Queue Queue Total 5
sec avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- --------
```

```
- --------- ---------- Esmp 202760 196 173 128 28 Control                          388623
2121      1740       598         16

Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
----------------------- --------------- --------- --------- --------- ----------
Control                             17918         0        19        24          3
```

Paso 4: Identifique la causa raíz.

Ejecute el comando **show spanning-tree summary**. Puede verificar si la recepción de las BPDU se debe a un gran número de instancias de puerto de árbol de expansión. El resultado identifica claramente la causa raíz:

```
Switch#show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
!--- Output suppressed. Name Blocking Listening Learning Forwarding STP Active -----------------
----- -------- --------- -------- ---------- ---------- 2994 vlans                    0
0        0       5999       5999
```

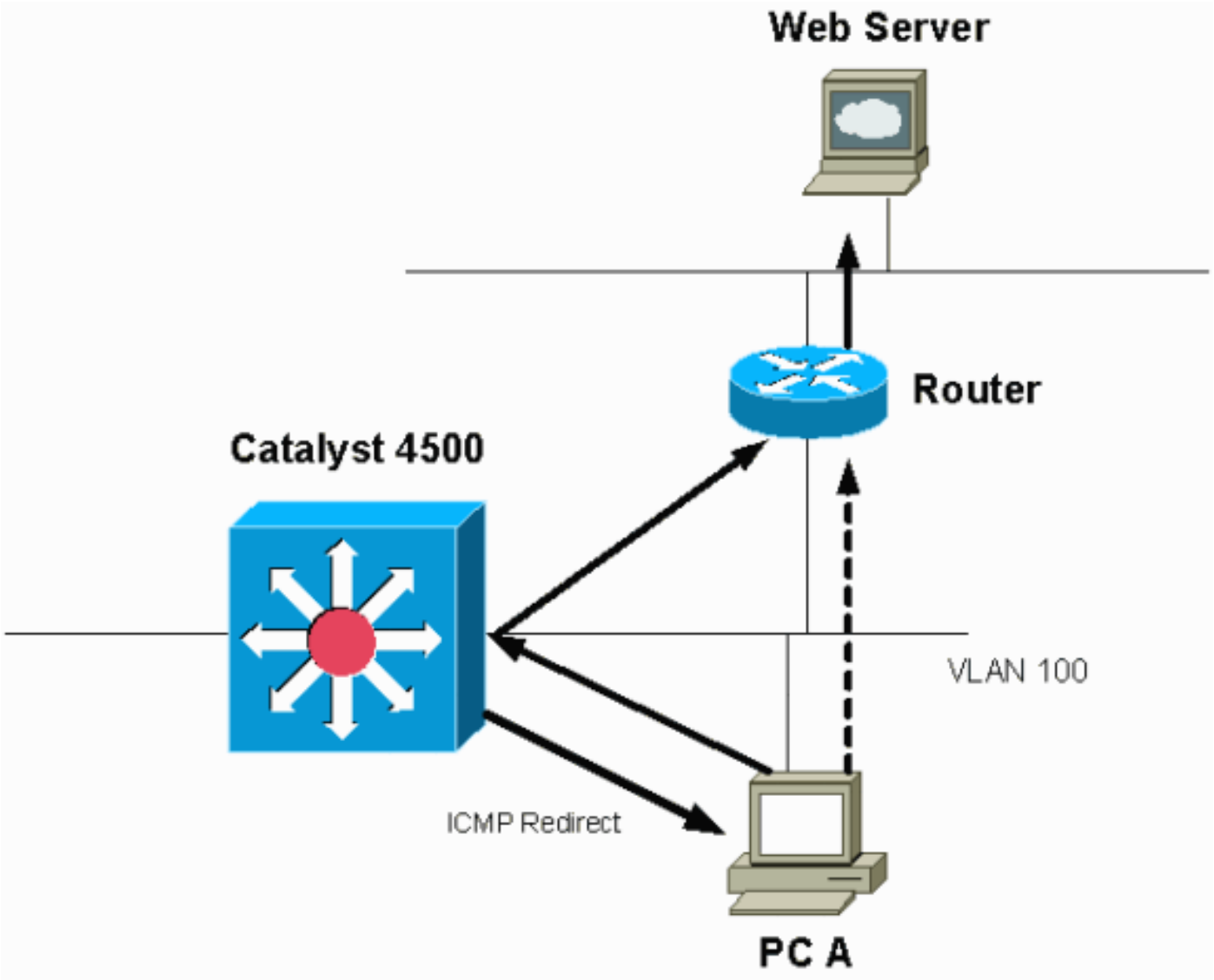
Hay un gran número de VLAN con la configuración del modo PVST+. Para resolver el problema, cambie el modo STP a Árbol de extensión múltiple (MST). En algunos casos, el número de instancias STP es alto porque se reenvía un número elevado de VLAN en todos los puertos trunk. En este caso, elimine manualmente las VLAN que no son necesarias del tronco para dejar caer el número de puertos activos STP muy por debajo del valor recomendado.

Sugerencia: Asegúrese de que no configura los puertos del teléfono IP como puertos troncales. Esta es una configuración errónea común. Configure los puertos del teléfono IP con una configuración de VLAN de voz. Esta configuración crea un pseudo tronco, pero no requiere que recorte manualmente las VLAN innecesarias. Para obtener más información sobre cómo configurar los puertos de voz, refiérase a la guía de configuración del software Configuración de Interfaces de Voz. Los teléfonos IP que no son de Cisco no admiten esta configuración VLAN de voz o VLAN auxiliar. Debe eliminar manualmente los puertos con teléfonos IP que no sean de Cisco.

Mensajes de redirección ICMP; Enrutamiento de paquetes en la misma interfaz

Los paquetes de ruteo en la misma interfaz, o el ingreso y egreso del tráfico en la misma interfaz L3, pueden resultar en una redirección ICMP por parte del switch. Si el switch sabe que el dispositivo de salto siguiente al destino final está en la misma subred que el dispositivo de envío, el switch genera una redirección ICMP al origen. Los mensajes de redirección indican al origen que envíe el paquete directamente al dispositivo de salto siguiente. Los mensajes indican que el dispositivo de salto siguiente tiene una mejor ruta al destino, una ruta de un salto menos que este switch.

En el diagrama de esta sección, PC A se comunica con el servidor web. El gateway predeterminado del PC A señala a la dirección IP de la interfaz VLAN 100. Sin embargo, el router de salto siguiente que habilita el Catalyst 4500 para alcanzar el destino está en la misma subred que el PC A. La mejor trayectoria en este caso es enviar directamente al "Router". Catalyst 4500 envía un mensaje de redirección ICMP al PC A. El mensaje indica a la PC A que envíe los paquetes destinados al servidor web a través del router, en lugar de a través de Catalyst 4500. Sin embargo, en la mayoría de los casos, los dispositivos finales no responden a la redirección ICMP. La falta de respuesta hace que el Catalyst 4500 gaste muchos ciclos de CPU en la generación de estas redirecciones ICMP para todos los paquetes que el Catalyst reenvía a través de la misma interfaz que los paquetes de ingreso.



De forma predeterminada, la redirección ICMP está habilitada. Para inhabilitarlo, utilice el comando **no ip icmp redirects**. Ejecute el comando bajo la interfaz SVI o L3 pertinente.

Nota: Dado que **ip icmp redirects** es un comando predeterminado, no está visible en el resultado del comando **show running-configuration**.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu**. Puede ver que dos procesos principales, `Cat4k Mgmt LoPri` y `IP Input` , utilizan principalmente la CPU. Con sólo esta información, usted sabe que el proceso de los paquetes IP gasta una porción considerable de la CPU.

```
Switch#show processes cpu
CPU utilization for five seconds: 38%/1%; one minute: 32%; five minutes: 32%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        63          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2          60     50074          1  0.00%  0.00%  0.00%   0 Load Meter
   3           0         1          0  0.00%  0.00%  0.00%   0 Deferred Events
!--- Output suppressed. 27 524 250268 2 0.00% 0.00% 0.00% 0 TTY Background 28 816 254843 3 0.00%
0.00% 0.00% 0 Per-Second Jobs 29 101100 5053 20007 0.00% 0.01% 0.00% 0 Per-minute Jobs 30
26057260 26720902 975 5.81% 6.78% 5.76% 0 Cat4k Mgmt HiPri 31    19482908  29413060        662
19.64% 18.20% 20.48%   0 Cat4k Mgmt LoPri
!--- Output suppressed. 35 60 902 0 0.00% 0.00% 0.00% 0 DHCP Snooping 36   504625304 645491491
781 72.40% 72.63% 73.82%   0 IP Input
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

El resultado del comando **show platform health** confirma el uso de la CPU para procesar los paquetes enlazados a la CPU.

```
Switch#show platform health
%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                  Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
--- Output suppressed. TagMan-RecreateMtegR 1.00 0.00 10 0 100 500 0 0 0 0:00 K2CpuMan Review
330.00 19.18 150 79 25 500 20 19 18 5794:08 K2AccelPacketMan: Tx 10.00 4.95 20 0 100 500 5 4 0
0:36 K2AccelPacketMan: Au 0.10 0.00 0 0 100 500 0 0 0 0:00 K2AclMan-taggedFlatA 1.00 0.00 10 0
100 500 0 0 0 0:00
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Ejecute el comando **show platform cpu packet statistics** para verificar qué cola de la CPU recibe el paquete enlazado a la CPU. Puede ver que la cola `L3 Fwd Low` recibe bastante tráfico.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue Queue Total 5 sec avg 1 min avg 5 min
avg 1 hour avg ---------------------- --------------- --------- --------- --------- ----------
Esmp 48613268 38 39 38 39 Control 142166648 74 74 73 73 Host Learning 1845568 2 2 2 2 L3 Fwd
High 17 0 0 0 0 L3 Fwd Medium 2626 0 0 0 0 L3 Fwd Low                   4717094264      3841
3879      3873       3547
L2 Fwd Medium                         1         0         0         0          0
L3 Rx High                       257147         0         0         0          0
L3 Rx Low                       5325772        10        19        13          7
RPF Failure                         155         0         0         0          0
ACL fwd(snooping)              65604591        53        54        54         53
ACL log, unreach               11013420         9         8         8          8
```

Paso 4: Identifique la causa raíz.

En este caso, use el SPAN de la CPU para determinar el tráfico que llega a la CPU. Para obtener información sobre el SPAN de CPU, vea la Herramienta 1: Monitoree el Tráfico de CPU con SPAN—Cisco IOS Software Release 12.1(19)EW y Posterior de este documento. Complete un análisis del tráfico y una configuración con el uso del comando **show running-configuration**. En este caso, un paquete se rutea a través de la misma interfaz, lo que lleva al problema de una redirección ICMP para cada paquete. Esta causa raíz es una de las razones comunes para el uso elevado de la CPU en el Catalyst 4500.

Puede esperar que el dispositivo de origen actúe en la redirección ICMP que envía el Catalyst 4500 y cambie el salto siguiente para el destino. Sin embargo, no todos los dispositivos responden a una redirección ICMP. Si el dispositivo no responde, el Catalyst 4500 debe enviar redirecciones para cada paquete que el switch recibe del dispositivo de envío. Estas redirecciones pueden consumir una gran cantidad de recursos de CPU. La solución es inhabilitar la redirección ICMP. Ejecute el comando **no ip redirects** bajo las interfaces.

Este escenario puede ocurrir cuando también ha configurado direcciones IP secundarias. Cuando habilita las direcciones IP secundarias, la redirección IP se inhabilita automáticamente. Asegúrese de que no habilita manualmente las redirecciones IP.

Como este ICMP Redirige; La sección Ruteo de Paquetes en la Misma Interfaz ha indicado que la mayoría de los dispositivos finales no responden a las redirecciones ICMP. Por lo tanto, como práctica general, inhabilite esta función.

Ruteo IPX o AppleTalk

El Catalyst 4500 soporta el ruteo IPX y AppleTalk solamente a través de la trayectoria de reenvío de software. Con la configuración de tales protocolos, una mayor utilización de la CPU es normal.

Nota: La conmutación del tráfico IPX y AppleTalk en la misma VLAN no requiere la conmutación del proceso. Sólo los paquetes que necesitan rutear requieren reenvío de trayectoria de software.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu** para verificar qué proceso del IOS de Cisco consume la CPU. En este resultado del comando, observe que el proceso principal es el **Cat4k Mgmt LoPri**:

```
witch#show processes cpu
CPU utilization for five seconds: 87%/10%; one minute: 86%; five minutes: 87%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4         53         75  0.00%  0.00%  0.00%   0 Chunk Manager
!--- Output suppressed. 25 8008 1329154 6 0.00% 0.00% 0.00% 0 Per-Second Jobs 26 413128 38493
10732 0.00% 0.02% 0.00% 0 Per-minute Jobs 27 148288424 354390017 418 2.60% 2.42% 2.77% 0 Cat4k
Mgmt HiPri 28   285796820 720618753        396 50.15% 59.72% 61.31%   0 Cat4k Mgmt LoPri
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

El resultado del comando **show platform health** confirma el uso de la CPU para procesar los paquetes enlazados a la CPU.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
!--- Output suppressed. TagMan-RecreateMtegR 1.00 0.00 10 4 100 500 0 0 0 0:00 K2CpuMan Review
30.00  27.39     30     53  100  500   42  47   42  4841:
K2AccelPacketMan: Tx  10.00   8.03     20      0  100  500   21  29   26  270:4
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Para determinar el tipo de tráfico que llega a la CPU, ejecute el comando **show platform cpu**

packet statistics.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue Queue Total 5 sec avg 1 min avg 5 min
avg 1 hour avg ---------------------- --------------- --------- --------- --------- ----------
Esmp 48613268 38 39 38 39 Control 142166648 74 74 73 73 Host Learning 1845568 2 2 2 2 L3 Fwd
High 17 0 0 0 0 L3 Fwd Medium 2626 0 0 0 0 L3 Fwd Low 1582414 1 1 1 1 L2 Fwd Medium 1 0 0 0 0 L2
Fwd Low                    576905398      1837      1697      1938      1515
L3 Rx High                    257147         0         0         0         0
L3 Rx Low                    5325772        10        19        13         7
RPF Failure                      155         0         0         0         0
ACL fwd(snooping)            65604591        53        54        54        53
ACL log, unreach             11013420         9         8         8         8
```

Paso 4: Identifique la causa raíz.

Dado que el administrador ha configurado el ruteo IPX o AppleTalk, la identificación de la causa raíz debe ser sencilla. Pero para confirmar, ejecute SPAN el tráfico de la CPU y asegúrese de que el tráfico que ve sea el tráfico esperado. Para obtener información sobre el SPAN de CPU, vea la Herramienta 1: Monitoree el Tráfico de CPU con SPAN—Cisco IOS Software Release 12.1(19)EW y Posterior de este documento.

En este caso, el administrador debe actualizar la CPU de línea de base al valor actual. La CPU Catalyst 4500 se comporta como se espera cuando la CPU procesa los paquetes conmutados por software.

Aprendizaje de host

El Catalyst 4500 aprende las direcciones MAC de varios hosts, si la dirección MAC no está ya en la tabla de direcciones MAC. El motor de conmutación reenvía una copia del paquete con la nueva dirección MAC a la CPU.

Todas las interfaces VLAN (capa 3) utilizan la dirección de hardware base del chasis como dirección MAC. Como resultado, no hay una entrada en la tabla de direcciones MAC y los paquetes destinados a estas interfaces VLAN no se envían a la CPU para su procesamiento.

Si hay un número excesivo de direcciones MAC nuevas que el switch puede aprender, puede producirse un uso elevado de la CPU.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu** para verificar qué proceso del IOS de Cisco consume la CPU. En este resultado del comando, observe que el proceso principal es el **Cat4k Mgmt LoPri**:

```
Switch#show processes cpu
CPU utilization for five seconds: 89%/1%; one minute: 74%; five minutes: 71%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4        53         75  0.00%  0.00%  0.00%   0 Chunk Manager
!--- Output suppressed. 25 8008 1329154 6 0.00% 0.00% 0.00% 0 Per-Second Jobs 26 413128 38493
10732 0.00% 0.02% 0.00% 0 Per-minute Jobs 27 148288424 354390017 418 26.47% 10.28% 10.11% 0
Cat4k Mgmt HiPri 28   285796820 720618753        396 52.71% 56.79% 55.70%   0 Cat4k Mgmt LoPri
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

El resultado del comando **show platform health** confirma el uso de la CPU para procesar los paquetes enlazados a la CPU.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
!--- Output suppressed. TagMan-RecreateMtegR 1.00 0.00 10 4 100 500 0 0 0 0:00 K2CpuMan Review
30.00  46.88     30     47  100  500   30  29   21  265:01
K2AccelPacketMan: Tx  10.00   8.03     20      0  100  500   21  29   26  270:4
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Para determinar el tipo de tráfico que llega a la CPU, ejecute el comando **show platform cpu packet statistics**.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Received by Packet Queue Queue Total 5 sec avg 1 min avg 5 min
avg 1 hour avg ---------------------- --------------- --------- --------- --------- ----------
Esmp 48613268 38 39 38 39 Control 142166648 74 74 73 73 Host Learning                  1845568
1328      1808      1393       1309
L3 Fwd High                          17         0         0         0          0
L3 Fwd Medium                      2626         0         0         0          0
L3 Fwd Low                      1582414         1         1         1          1
L2 Fwd Medium                         1         0         0         0          0
L2 Fwd Low                    576905398        37         7         8          5
L3 Rx High                       257147         0         0         0          0
L3 Rx Low                       5325772        10        19        13          7
RPF Failure                         155         0         0         0          0
ACL fwd(snooping)              65604591        53        54        54         53
ACL log, unreach               11013420         9         8         8          8
```

Paso 4: Identifique la causa raíz.

El resultado del comando **show platform health** muestra que la CPU ve muchas direcciones MAC nuevas. Esta situación es a menudo el resultado de la inestabilidad de la topología de red. Por ejemplo, si cambia la topología del árbol de extensión, el switch genera notificaciones de cambio de topología (TCN). El problema de los TCN reduce el tiempo de envejecimiento a 15 segundos en el modo PVST+. Las entradas de dirección MAC se vacian si las direcciones no se aprenden de nuevo en el período de tiempo. En el caso del STP rápido (RSTP) (IEEE 802.1w) o MST (IEEE 802.1s), las entradas se desactualizan inmediatamente si la TCN proviene de otro switch. Esta antigüedad hace que las direcciones MAC se aprendan de nuevo. Este no es un problema importante si los cambios de topología son raros. Pero puede haber un número excesivo de cambios de topología debido a un link inestable, un switch defectuoso o puertos host que no están habilitados para PortFast. Se puede producir un gran número de vaciados de la tabla MAC y posterior reaprendizaje. El siguiente paso en la identificación de la causa raíz es resolver problemas de la red. El switch funciona como se esperaba y envía los paquetes a la CPU para el aprendizaje de la dirección del host. Identifique y corrija el dispositivo defectuoso que da lugar a TCN excesivos.

La red puede tener muchos dispositivos que envían tráfico en ráfagas, lo que hace que las direcciones MAC se desactualicen y se vuelvan a aprender posteriormente en el switch. En este caso, aumente el tiempo de envejecimiento de la tabla de direcciones MAC para proporcionar algún alivio. Con un tiempo de envejecimiento más largo, los switches retienen las direcciones MAC del dispositivo en la tabla durante un período más largo antes de que se agote el tiempo de

espera.

Precaución: Realice este cambio de edad sólo después de una cuidadosa consideración. El cambio puede conducir a un agujero negro del tráfico si tiene dispositivos en su red que sean móviles.

Recursos de hardware (TCAM) para ACL de seguridad

El Catalyst 4500 programa las ACL configuradas con el uso de Cisco TCAM. TCAM permite la aplicación de las ACL en la trayectoria de reenvío de hardware. No hay impacto en el rendimiento del switch, con o sin ACL en el trayecto de reenvío. El rendimiento es constante a pesar del tamaño de la ACL porque el rendimiento de las búsquedas de ACL es a velocidad de línea. Sin embargo, TCAM es un recurso finito. Por lo tanto, si configura un número excesivo de entradas de ACL, excede la capacidad de TCAM. La tabla 3 muestra el número de recursos TCAM disponibles en cada uno de los Catalyst 4500 Supervisor Engines y switches.

Tabla 3: Capacidad de TCAM en Catalyst 4500 Supervisor Engines/Switches

Producto	TCAM de funciones (por dirección)	TCAM de QoS (por dirección)
Supervisor Engine II+/II+TS	8192 entradas con máscaras 1024	8192 entradas con máscaras 1024
Supervisor Engine III/IV/V y Catalyst 4948	16 384 entradas con máscaras 2048	16 384 entradas con máscaras 2048
Supervisor Engine V-10GE y Catalyst 4948-10GE	16 384 entradas con 16 384 máscaras	16 384 entradas con 16 384 máscaras

El switch utiliza la función TCAM para programar la ACL de seguridad, como RACL y VLAN ACL (VACL). El switch también utiliza la función TCAM para funciones de seguridad como IP Source Guard (IPSG) para ACL dinámicas. El switch utiliza la TCAM de QoS para programar la clasificación y las ACL del regulador.

Cuando el Catalyst 4500 se queda sin recursos TCAM durante la programación de una ACL de seguridad, una aplicación parcial de la ACL ocurre a través de la trayectoria de software. Los paquetes que afectan a esas ACE se procesan en el software, lo que causa una alta utilización de la CPU. La ACL se programa desde arriba hacia abajo. En otras palabras, si la ACL no encaja en la TCAM, es probable que la ACE en la parte inferior de la ACL no esté programada en la TCAM.

Este mensaje de advertencia aparece cuando se produce un desbordamiento de TCAM:

```
%C4K_HWACLMAN-4-ACLHWPROGERRREASON: (Suppressed 1times) Input(null, 12/Normal)
Security: 140 - insufficient hardware TCAM masks.
%C4K_HWACLMAN-4-ACLHWPROGERR: (Suppressed 4 times) Input Security: 140 - hardware TCAM
limit, some packet processing will be software switched.
```

Puede ver este mensaje de error en el resultado del comando **show logging**. El mensaje indica de manera concluyente que se llevará a cabo cierto procesamiento de software y, en consecuencia, puede haber una alta utilización de la CPU.

Nota: Si cambia una ACL grande, puede ver este mensaje brevemente antes de que la ACL cambiada se programe de nuevo en la TCAM.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu**. Puede ver que la utilización de la CPU es alta porque el proceso **Cat4k Mgmt LoPri** toma la mayor parte de los ciclos de la CPU.

```
Switch#show processes cpu
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 99%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        11          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9716    632814         15  0.00%  0.00%  0.00%   0 Load Meter
   3         780       302       2582  0.00%  0.00%  0.00%   0 SpanTree Helper
!--- Output suppressed. 23 18208 3154201 5 0.00% 0.00% 0.00% 0 TTY Background 24 37208 3942818 9
0.00% 0.00% 0.00% 0 Per-Second Jobs 25 1046448 110711 9452 0.00% 0.03% 0.00% 0 Per-minute Jobs
26 175803612 339500656 517 4.12% 4.31% 4.48% 0 Cat4k Mgmt HiPri   27   835809548 339138782
2464 86.81% 89.20% 89.76%   0 Cat4k Mgmt LoPri
  28       28668   2058810         13  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

Ejecute el comando **show platform health**. Puede ver que **K2CpuMan Review**, un trabajo para manejar paquetes enlazados a la CPU, utiliza la CPU.

```
Switch#show platform health
%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                    Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll               1.00   0.01      2      0  100  500    0   0    0  13:45
GalChassisVp-review    3.00   0.20     10     16  100  500    0   0    0  88:44
S2w-JobEventSchedule  10.00   0.57     10      7  100  500    1   0    0  404:22
Stub-JobEventSchedul  10.00   0.00     10      0  100  500    0   0    0  0:00
StatValueMan Update    1.00   0.09      1      0  100  500    0   0    0  91:33
Pim-review             0.10   0.00      1      0  100  500    0   0    0  4:46
Ebm-host-review        1.00   0.00      8      4  100  500    0   0    0  14:01
Ebm-port-review        0.10   0.00      1      0  100  500    0   0    0  0:20
Protocol-aging-revie   0.20   0.00      2      0  100  500    0   0    0  0:01
Acl-Flattener          1.00   0.00     10      5  100  500    0   0    0  0:04
KxAclPathMan create/   1.00   0.00     10      5  100  500    0   0    0  0:21
KxAclPathMan update    2.00   0.00     10      6  100  500    0   0    0  0:05
KxAclPathMan reprogr   1.00   0.00      2      1  100  500    0   0    0  0:00
TagMan-InformMtegRev   1.00   0.00      5      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10     14  100  500    0   0    0  0:18
K2CpuMan Review       30.00  91.31     30     92  100  500  128 119   84  13039:02
K2AccelPacketMan: Tx  10.00   2.30     20      0  100  500    2   2    2  1345:30
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Debe comprender mejor qué cola de la CPU y, por lo tanto, qué tipo de tráfico llega a la cola de la CPU. Ejecute el comando **show platform cpu packet statistics**. Puede ver que la cola de `procesamiento de ACL sw` recibe un número elevado de paquetes. Por lo tanto, el desbordamiento de TCAM es la causa de este problema de uso elevado de la CPU.

```
Switch#show platform cpu packet statistics
```

```
!--- Output suppressed. Packets Received by Packet Queue Queue Total 5 sec avg 1 min avg 5 min
avg 1 hour avg ---------------------- -------------- --------- --------- --------- ----------
Control 57902635 22 16 12 3 Host Learning 464678 0 0 0 0 L3 Fwd Low 623229 0 0 0 0 L2 Fwd Low
11267182 7 4 6 1 L3 Rx High 508 0 0 0 0 L3 Rx Low 1275695 10 1 0 0 ACL fwd(snooping) 2645752 0 0
0 0 ACL log, unreach 51443268 9 4 5 5 ACL sw processing            842889240      1453      1532
1267       1179

Packets Dropped by Packet Queue

Queue                   Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
L2 Fwd Low                       3270         0         0         0          0
ACL sw processing               12636         0         0         0          0
```

Paso 4: Resolver el problema.

En el Paso 3, se determinó la causa raíz en este escenario. Quite la ACL que provocó el desbordamiento o minimice la ACL para evitar el desbordamiento. Además, revise la guía de configuración Configuración de Seguridad de Red con ACL para optimizar la configuración y programación de ACL en el hardware.

La palabra clave de registro en ACL

El Catalyst 4500 admite el registro de detalles de paquetes que afectan a cualquier entrada ACL específica, pero un registro excesivo puede causar una alta utilización de la CPU. Evite el uso de palabras clave **de registro**, excepto durante la etapa de detección de tráfico. Durante la etapa de detección del tráfico, se identifica el tráfico que fluye a través de la red para el que no se han configurado ACE explícitamente. No utilice la palabra clave **log** para recopilar estadísticas. En Cisco IOS Software Release 12.1(13)EW y posteriores, los mensajes **log** están limitados por velocidad. Si utiliza mensajes **de registro** para contar el número de paquetes que coinciden con la ACL, el conteo no es preciso. En su lugar, utilice el comando **show access-list** para obtener estadísticas precisas. La identificación de esta causa raíz es más fácil porque una revisión de la configuración o de los mensajes **de registro** puede indicar el uso de la función de registro de ACL.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu** para verificar qué proceso del IOS de Cisco consume la CPU. En este resultado de comando, se encuentra que el proceso superior es el **Cat4k Mgmt LoPri**:

```
Switch#show processes cpu
CPU utilization for five seconds: 99%/0%; one minute: 99%; five minutes: 99%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0        11          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9716    632814         15  0.00%  0.00%  0.00%   0 Load Meter
!--- Output suppressed. 26 175803612 339500656 517 4.12% 4.31% 4.48% 0 Cat4k Mgmt HiPri   27
835809548 339138782       2464 86.81% 89.20% 89.76%   0 Cat4k Mgmt LoPri
  28       28668   2058810         13  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

Verifique el proceso específico de la plataforma que utiliza la CPU. Ejecute el comando **show platform health**. En el resultado, observe que el proceso **K2CpuMan Review** utiliza la mayoría de los ciclos de CPU. Esta actividad indica que la CPU está ocupada mientras procesa los paquetes destinados a ella.

```
Switch#show platform health
                      %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                    Target Actual Target Actual   Fg    Bg 5Sec Min Hour  CPU
Lj-poll               1.00   0.01      2      0  100   500    0   0    0  13:45
GalChassisVp-review    3.00   0.20     10     16  100   500    0   0    0  88:44
S2w-JobEventSchedule  10.00   0.57     10      7  100   500    1   0    0  404:22
Stub-JobEventSchedul  10.00   0.00     10      0  100   500    0   0    0  0:00
StatValueMan Update    1.00   0.09      1      0  100   500    0   0    0  91:33
Pim-review             0.10   0.00      1      0  100   500    0   0    0  4:46
Ebm-host-review        1.00   0.00      8      4  100   500    0   0    0  14:01
Ebm-port-review        0.10   0.00      1      0  100   500    0   0    0  0:20
Protocol-aging-revie   0.20   0.00      2      0  100   500    0   0    0  0:01
Acl-Flattener          1.00   0.00     10      5  100   500    0   0    0  0:04
KxAclPathMan create/   1.00   0.00     10      5  100   500    0   0    0  0:21
KxAclPathMan update    2.00   0.00     10      6  100   500    0   0    0  0:05
KxAclPathMan reprogr   1.00   0.00      2      1  100   500    0   0    0  0:00
TagMan-InformMtegRev   1.00   0.00      5      0  100   500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10     14  100   500    0   0    0  0:18
K2CpuMan Review       30.00  91.31     30     92  100   500  128 119   84  13039:02
K2AccelPacketMan: Tx  10.00   2.30     20      0  100   500    2   2    2  1345:30
K2AccelPacketMan: Au   0.10   0.00      0      0  100   500    0   0    0  0:00
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU.

Para determinar el tipo de tráfico que llega a la CPU, ejecute el comando **show platform cpu packet statistics**. En este resultado de comando, puede ver que la recepción de paquetes se debe a la palabra clave **ACL log**:

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Total packet queues 16 Packets Received by Packet Queue Queue Total 5
sec avg 1 min avg 5 min avg 1 hour avg ----------------- -------------------- --------- --------
- --------- ---------- Control 1198701435 35 35 34 35 Host Learning 874391 0 0 0 0 L3 Fwd High
428 0 0 0 0 L3 Fwd Medium 12745 0 0 0 0 L3 Fwd Low 2420401 0 0 0 0 L2 Fwd High 26855 0 0 0 0 L2
Fwd Medium 116587 0 0 0 0 L2 Fwd Low 317829151 53 41 31 31 L3 Rx High 2371 0 0 0 0 L3 Rx Low
32333361 7 1 2 0 RPF Failure 4127 0 0 0 0 ACL fwd (snooping) 107743299 4 4 4 4 ACL log, unreach
1209056404      1987      2125      2139       2089

Packets Dropped by Packet Queue

Queue              Total                 5 sec avg 1 min avg 5 min avg 1 hour avg
------------------ --------------------- --------- --------- --------- ----------
ACL log, unreach              193094788       509       362       437        394
```

Paso 4: Resolver el problema.

En el Paso 3, se determinó la causa raíz en este escenario. Para evitar este problema, quite la palabra clave **log** de las ACL. En la versión 12.1(13)EW1 y posteriores del software del IOS de Cisco, los paquetes están limitados por la velocidad, de modo que la utilización de la CPU no se vuelva demasiado alta. Utilice los contadores de la lista de acceso como una forma de realizar un seguimiento de los resultados de ACL. Puede ver los contadores de la lista de acceso en el resultado del comando **show access-list** ***acl_id.***

Loops de reenvío de capa 2

Los loops de reenvío de capa 2 pueden ser causados por una implementación deficiente del protocolo de árbol de extensión (STP) y varios problemas que pueden afectar al STP.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu

Esta sección revisa los comandos que utiliza un administrador para reducir el problema de uso elevado de la CPU. Si ejecuta el comando **show processes cpu**, puede ver que dos procesos principales, **Cat4k Mgmt LoPri** y **Spanning Tree** , utilizan principalmente la CPU. Con sólo esta información, usted sabe que el proceso del árbol de expansión consume una porción considerable de los ciclos de CPU.

```
Switch#show processes cpu
CPU utilization for five seconds: 74%/1%; one minute: 73%; five minutes: 50%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4       198         20  0.00%  0.00%  0.00%   0 Chunk Manager
   2           4       290         13  0.00%  0.00%  0.00%   0 Load Meter
!--- Output suppressed. 25 488 33 14787 0.00% 0.02% 0.00% 0 Per-minute Jobs 26 90656 223674 405
6.79% 6.90% 7.22% 0 Cat4k Mgmt HiPri  27      158796     59219       2681 32.55% 33.80% 21.43%
0 Cat4k Mgmt LoPri
  28          20      1693         11  0.00%  0.00%  0.00%   0 Galios Reschedul
  29           0         1          0  0.00%  0.00%  0.00%   0 IOS ACL Helper
  30           0         2          0  0.00%  0.00%  0.00%   0 NAM Manager
!--- Output suppressed. 41 0 1 0 0.00% 0.00% 0.00% 0 SFF8472 42 0 2 0 0.00% 0.00% 0.00% 0 AAA
Dictionary R  43       78564     20723       3791 32.63% 30.03% 17.35%   0 Spanning Tree
  44         112       999         112  0.00%  0.00%  0.00%   0 DTP Protocol
  45           0       147           0  0.00%  0.00%  0.00%   0 Ethchnl
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health

Para entender qué proceso específico de la plataforma consume la CPU, ejecute el comando **show platform health**. A partir de este resultado, puede ver que el proceso **K2CpuMan Review, un trabajo para manejar paquetes enlazados a la CPU, utiliza la CPU:**

```
Switch#show platform health
%CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                  Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
!--- Output suppressed. TagMan-RecreateMtegR 1.00 0.00 10 0 100 500 0 0 0 0:00 K2CpuMan Review
30.00  37.62     30     53  100  500   41  33    1  2:12
K2AccelPacketMan: Tx  10.00   4.95     20      0  100  500    5   4    0  0:36
K2AccelPacketMan: Au   0.10   0.00      0      0  100  500    0   0    0  0:00
K2AclMan-taggedFlatA   1.00   0.00     10      0  100  500    0   0    0  0:00
```

Paso 3: Verifique la cola de la CPU que recibe el tráfico para identificar el tipo de tráfico dirigido a la CPU

Ejecute el comando **show platform cpu packet statistics** para verificar qué cola de la CPU recibe el paquete enlazado a la CPU. El resultado de esta sección muestra que la cola de control recibe un montón de paquetes. Utilice la información de la Tabla 1 y la conclusión que extrajo en el Paso 1. Puede determinar que los paquetes que procesa la CPU y la razón de la alta utilización de la CPU es el procesamiento de BPDU.

```
Switch#show platform cpu packet statistics
!--- Output suppressed. Total packet queues 16 Packets Received by Packet Queue Queue Total 5
sec avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- --------
- --------- ---------- Esmp 202760 196 173 128 28 Control                          388623
2121      1740       598         16

Packets Dropped by Packet Queue
```

```
Queue                  Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Control                            17918         0        19        24          3
```

Paso 4: Identificar la causa raíz y solucionar el problema

Por lo general, puede completar estos pasos para resolver problemas (dependiendo de la situación, algunos pasos no son necesarios):

1. Identificar el loop.
2. Descubra el alcance del bucle.
3. Interrumpa el loop.
4. Corrija la causa del loop.
5. Restaure la redundancia.

Cada uno de los pasos se explica en detalle en Resolución de problemas de loops de reenvío - Resolución de problemas de STP en switches Catalyst que ejecutan el software del sistema Cisco IOS.

Paso 5: Implemente funciones avanzadas de STP

- **Protección BDPU**: protege el STP de los dispositivos de red no autorizados conectados a los puertos habilitados para portfast. Refiérase a Mejora de la Protección PortFast BPDU del Spanning Tree para obtener más información.
- **Protección de loop**: aumenta la estabilidad de las redes de capa 2. Refiérase a Mejoras del Spanning-Tree Protocol usando las Funciones de Protección de Loops y Detección de Desviación de BPDU para obtener más información.
- **Protección de raíz**: aplica la ubicación del puente raíz en la red. Consulte Mejora de Protección de Raíz en Spanning-Tree Protocol para obtener más información.
- **UDLD**: detecta links unidireccionales y evita loops de reenvío. Refiérase a Comprensión y Configuración de la Función Unidirectional Link Detection Protocol para obtener más información.

Otras causas de la alta utilización de la CPU

Estas son algunas otras causas conocidas de uso excesivo de la CPU:

- Inundaciones de link excesivas
- Aumento en el uso de la CPU debido a la verificación de consistencia de FIB
- Uso elevado de la CPU en el proceso **K2FibAdjMan Host Move**
- Uso elevado de la CPU en el proceso **RkiosPortMan Port Review**
- Uso elevado de la CPU cuando se conecta a un teléfono IP con el uso de puertos troncales
- Uso elevado de la CPU con paquetes de control RSPAN y Capa 3
- Spike durante la programación de ACL de gran tamañoEl pico en el uso de la CPU ocurre durante la aplicación o la remoción de una ACL grande de una interfaz.

Inestabilidad de link excesiva

El Catalyst 4500 muestra una alta utilización de la CPU cuando uno o más de los links conectados comienzan a producirse una inestabilidad excesiva. Esta situación ocurre en las

versiones del software Cisco IOS anteriores a la versión 12.2(20)EWA del software Cisco IOS.

Paso 1: Verifique el proceso de Cisco IOS con el comando show processes cpu.

Ejecute el comando **show processes cpu** para verificar qué proceso del IOS de Cisco consume la CPU. En este resultado del comando, observe que el proceso principal es el **Cat4k Mgmt LoPri**:

```
Switch#show processes cpu
CPU utilization for five seconds: 96%/0%; one minute: 76%; five minutes: 68%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0         4          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        9840    463370         21  0.00%  0.00%  0.00%   0 Load Meter
   3           0         2          0  0.00%  0.00%  0.00%   0 SNMP Timers
!--- Output suppressed. 27 232385144 530644966 437 13.98% 12.65% 12.16% 0 Cat4k Mgmt HiPri   28
564756724 156627753       3605 64.74% 60.71% 54.75%   0 Cat4k Mgmt LoPri
  29        9716   1806301          5  0.00%  0.00%  0.00%   0 Galios Reschedul
```

Paso 2: Verifique el proceso específico de Catalyst 4500 con el comando show platform health.

La salida del comando **show platform health** indica que el proceso **KxAclPathMan create** utiliza la CPU. Este proceso es para la creación de la ruta interna.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.03      2      0  100  500    0   0    0  9:49
GalChassisVp-review    3.00   1.11     10     62  100  500    0   0    0  37:39
S2w-JobEventSchedule  10.00   2.85     10      8  100  500    2   2    2  90:00
Stub-JobEventSchedul  10.00   5.27     10      9  100  500    4   4    4  186:2
Pim-review             0.10   0.00      1      0  100  500    0   0    0  2:51
Ebm-host-review        1.00   0.00      8      4  100  500    0   0    0  8:06
Ebm-port-review        0.10   0.00      1      0  100  500    0   0    0  0:14
Protocol-aging-revie   0.20   0.00      2      0  100  500    0   0    0  0:00
Acl-Flattener          1.00   0.00     10      5  100  500    0   0    0  0:00
KxAclPathMan create/   1.00  69.11     10      5  100  500   42  53   22  715:0
KxAclPathMan update    2.00   0.76     10      6  100  500    0   0    0  86:00
KxAclPathMan reprogr   1.00   0.00      2      1  100  500    0   0    0  0:00
TagMan-InformMtegRev   1.00   0.00      5      0  100  500    0   0    0  0:00
TagMan-RecreateMtegR   1.00   0.00     10    227  100  500    0   0    0  0:00
K2CpuMan Review       30.00   8.05     30     57  100  500    6   5    5  215:0
K2AccelPacketMan: Tx  10.00   6.86     20      0  100  500    5   5    4  78:42
```

Paso 3: Identifique la causa raíz.

Habilite el registro para los mensajes de link activo/inactivo. Este registro no está habilitado de forma predeterminada. La habilitación le ayuda a reducir los enlaces ofensivos muy rápidamente. Ejecute el comando **logging event link-status** bajo todas las interfaces. Puede utilizar el comando **interface range** para habilitar convenientemente en un rango de interfaces, como muestra este ejemplo:

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface range gigabitethernet 5/1 - 48
Switch(config-if-range)#logging event link-status
Switch(config--if-range)#end
```

```
Switch#show logging
!--- Output suppressed. 3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to
down 3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to up 3w5d: %LINK-3-
UPDOWN: Interface GigabitEthernet5/24, changed state to down 3w5d: %LINK-3-UPDOWN: Interface
GigabitEthernet5/24, changed state to up 3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24,
changed state to down 3w5d: %LINK-3-UPDOWN: Interface GigabitEthernet5/24, changed state to up
```

Después de identificar la interfaz defectuosa o inestable, apague la interfaz para resolver el problema de uso elevado de la CPU. Cisco IOS Software Release 12.2(20)EWA y posteriores han mejorado el comportamiento de Catalyst 4500 para esta condición de links inestables. Por lo tanto, el impacto en la CPU no es tan grande como antes de la mejora. Recuerde que este proceso es un proceso de fondo. La alta utilización de la CPU debido a este problema no causa efectos adversos en los switches Catalyst 4500.

Aumento en el uso de la CPU debido a la verificación de coherencia de FIB

El Catalyst 4500 puede mostrar picos momentáneos en el uso de la CPU durante una verificación de consistencia de la tabla FIB. La tabla FIB es la tabla de reenvío L3 que crea el proceso CEF. La verificación de consistencia mantiene la consistencia entre la tabla FIB del software del IOS de Cisco y las entradas de hardware. Esta consistencia asegura que los paquetes no se enruten mal. La verificación se produce cada 2 segundos y se ejecuta como proceso de fondo de baja prioridad. Este proceso es un comportamiento normal y no interfiere con otros procesos o paquetes de alta prioridad.

La salida del comando **show platform health** muestra que **K2Fib Consistency Ch** consume la mayor parte de la CPU.

Nota: El uso promedio de la CPU para este proceso es insignificante durante un minuto o una hora, lo que confirma que la verificación es un breve examen periódico. Este proceso de fondo sólo utiliza los ciclos de CPU inactivos.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review    3.00   0.29     10      3  100  500    0   0    0  11:15
!--- Output suppressed. K2Fib cam usage revi 2.00 0.00 15 0 100 500 0 0 0 0:00 K2Fib IrmFib
Review 2.00 0.00 15 0 100 500 0 0 0 0:00 K2Fib Vrf Default Ro 2.00 0.00 15 0 100 500 0 0 0 0:00
K2Fib AdjRepop Revie 2.00 0.00 15 0 100 500 0 0 0 0:00 K2Fib Vrf Unpunt Rev 2.00 0.01 15 0 100
500 0 0 0 0:23 K2Fib Consistency Ch 1.00 60.40 5 2 100 500 0    0    0 100:23
K2FibAdjMan Stats Re   2.00   0.30     10      4  100  500    0   0    0  6:21
K2FibAdjMan Host Mov   2.00   0.00     10      4  100  500    0   0    0  0:00
K2FibAdjMan Adj Chan   2.00   0.00     10      0  100  500    0   0    0  0:00
K2FibMulticast Signa   2.00   0.01     10      2  100  500    0   0    0  2:04
```

Uso elevado de la CPU en el proceso de movimiento de host K2FibAdjMan

El Catalyst 4500 puede mostrar un uso elevado de la CPU en el proceso **K2FibAdjMan Host Move**. Esta alta utilización aparece en la salida del comando **show platform health**. Muchas direcciones MAC caducan con frecuencia o se aprenden en los nuevos puertos, lo que provoca esta elevada utilización de la CPU. El valor predeterminado de mac-address-table aging-time es de 5 minutos o 300 segundos. La solución temporal para este problema es aumentar el tiempo de envejecimiento de la dirección MAC, o puede diseñar la red para evitar el gran número de movimientos de dirección MAC. Cisco IOS Software Release 12.2(18)EW y posteriores han mejorado este comportamiento de proceso para consumir menos CPU. Consulte Cisco bug ID

CSCed15021 (sólo clientes registrados) .

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review    3.00   0.29     10      3  100  500    0   0    0  11:15
S2w-JobEventSchedule  10.00   0.32     10      7  100  500    0   0    0  10:14
!--- Output suppressed. K2FibAdjMan Stats Re 2.00 0.30 10 4 100 500 0 0 0 6:21 K2FibAdjMan Host
Mov   2.00  18.68     10      4  100  500   25  29   28  2134:39
K2FibAdjMan Adj Chan   2.00   0.00     10      0  100  500    0   0    0  0:00
K2FibMulticast Signa   2.00   0.01     10      2  100  500    0   0    0  2:04
K2FibMulticast Entry   2.00   0.00     10      7  100  500    0   0    0  0:00
```

Puede modificar el tiempo máximo de envejecimiento de una dirección MAC en el modo de configuración global. La sintaxis del comando es **mac-address-table aging-time seconds** para un router y **mac-address-table aging-time seconds [*vlan vlan-id*]** para un switch Catalyst. Para obtener más información, consulte la Guía de Referencia de Comandos de Servicios de Switching de Cisco IOS.

Uso elevado de la CPU en el proceso de revisión de puertos RkiosPortMan

El Catalyst 4500 puede mostrar un uso elevado de la CPU en el proceso de **Revisión de puertos RkiosPortMan** en la salida del comando **show platform health** en Cisco IOS Software Release 12.2(25)EWA y 12.2(25)EWA1. El Id. de bug Cisco CSCeh08768 (sólo clientes registrados) causa la alta utilización, que el Cisco IOS Software Release 12.2(25)EWA2 resuelve. Este proceso es un proceso en segundo plano y no afecta la estabilidad de los switches Catalyst 4500.

```
Switch#show platform health
                     %CPU   %CPU    RunTimeMax   Priority  Average %CPU  Total
                     Target Actual Target Actual   Fg   Bg 5Sec Min Hour  CPU
Lj-poll                1.00   0.02      2      1  100  500    0   0    0  1:09
GalChassisVp-review    3.00   0.29     10      3  100  500    0   0    0  11:15
S2w-JobEventSchedule  10.00   0.32     10      7  100  500    0   0    0  10:14
!--- Output suppressed. K2 Packet Memory Dia 2.00 0.00 15 8 100 500 0 1 1 45:46 K2 L2 Aging
Table Re 2.00 0.12 20 3 100 500 0 0 0 7:22 RkiosPortMan Port Re   2.00  87.92     12      7  100
500   99  99   89  1052:36
Rkios Module State R   4.00   0.02     40      1  100  500    0   0    0  1:28
Rkios Online Diag Re   4.00   0.02     40      0  100  500    0   0    0  1:15
```

Uso elevado de la CPU cuando se conecta a un teléfono IP con el uso de puertos troncales

Si se configura un puerto tanto para la opción de VLAN de voz como para la opción de VLAN de acceso, el puerto actúa como puerto de acceso de VLAN múltiple. La ventaja es que sólo se conectan mediante troncales las VLAN configuradas para las opciones de VLAN de voz y acceso.

Las VLAN que se enlazan al teléfono aumentan el número de instancias STP. El switch administra las instancias STP. La administración del aumento en las instancias STP también aumenta la utilización de CPU STP.

El trunking de todas las VLAN también hace que el tráfico de difusión innecesario, multidifusión y unidifusión desconocida llegue al link del teléfono.

```
Switch#show processes cpu
CPU utilization for five seconds: 69%/0%; one minute: 72%; five minutes: 73%
```

```
 PID Runtime(ms)    Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           4        165         24  0.00%  0.00%  0.00%   0 Chunk Manager
   2       29012     739091         39  0.00%  0.00%  0.00%   0 Load Meter
   3       67080      13762       4874  0.00%  0.00%  0.00%   0 SpanTree Helper
   4           0          1          0  0.00%  0.00%  0.00%   0 Deferred Events
   5           0          2          0  0.00%  0.00%  0.00%   0 IpSecMibTopN
   6     4980144     570766       8725  0.00%  0.09%  0.11%   0 Check heaps
  26   539173952  530982442       1015 13.09% 13.05% 13.20%   0 Cat4k Mgmt HiPri
  27   716335120  180543127       3967 17.61% 18.19% 18.41%   0 Cat4k Mgmt LoPri
  33     1073728      61623      17424  0.00%  0.03%  0.00%   0 Per-minute Jobs
  34  1366717824  231584970       5901 38.99% 38.90% 38.92%   0 Spanning Tree
  35     2218424   18349158        120  0.00%  0.03%  0.02%   0 DTP Protocol
  36        5160     369525         13  0.00%  0.00%  0.00%   0 Ethchnl
  37      271016    2308022        117  0.00%  0.00%  0.00%   0 VLAN Manager
  38      958084    3965585        241  0.00%  0.01%  0.01%   0 UDLD
  39        1436      51011         28  0.00%  0.00%  0.00%   0 DHCP Snooping
  40         780      61658         12  0.00%  0.00%  0.00%   0 Port-Security
  41     1355308   12210934        110  0.00%  0.01%  0.00%   0 IP Input
```

Uso elevado de la CPU con paquetes de control RSPAN y Capa 3

Los paquetes de control de Capa 3 capturados con RSPAN están destinados a la CPU en lugar de sólo a la interfaz de destino de RSPAN, lo que causa un uso excesivo de la CPU. Los paquetes de control L3 son capturados por entradas CAM estáticas con acción de CPU reenviada. Las entradas CAM estáticas son globales para todas las VLAN. Para evitar inundaciones innecesarias de la CPU, utilice la función Per-VLAN Control Traffic Intercept, disponible en las versiones 12.2(37)SG y posteriores del software del IOS de Cisco.

```
Switch(config)# access-list hardware capture mode vlan
```

Las ACL estáticas se instalan en la parte superior de la función de entrada TCAM para capturar los paquetes de control destinados a direcciones IP multicast conocidas en el rango 224.0.0.*. Las ACL estáticas se instalan en el momento del inicio y aparecen antes que cualquier ACL configurada por el usuario. Las ACL estáticas siempre se activan primero e interceptan el tráfico de control a la CPU en todas las VLAN.

La función Per-VLAN Control Traffic Intercept proporciona el modo selectivo administrado por trayectoria VLAN para capturar el tráfico de control. Las entradas CAM estáticas correspondientes en la función de entrada TCAM se invalidan en el nuevo modo. Los paquetes de control se capturan mediante ACL específica de función conectada a VLAN en las que se habilitan las funciones de snooping o routing. No hay ninguna ACL específica de función conectada a RSPAN VLAN. Por lo tanto, todos los paquetes de control de capa 3 recibidos de la VLAN RSPAN no se reenvían a la CPU.

Solución de problemas de herramientas para analizar el tráfico destinado a la CPU

Como se ha mostrado en este documento, el tráfico destinado a la CPU es una de las principales causas del uso elevado de la CPU en el Catalyst 4500. El tráfico destinado a la CPU puede ser intencional debido a la configuración o no intencional debido a una configuración incorrecta o a un ataque de denegación de servicio. La CPU tiene un mecanismo de QoS integrado para evitar cualquier efecto adverso en la red debido a este tráfico. Sin embargo, identifique la causa raíz del tráfico enlazado a la CPU y elimine el tráfico si no es deseable.

Herramienta 1: Monitoreo del Tráfico de CPU con SPAN—Cisco IOS Software

Release 12.1(19)EW y Posteriores

El Catalyst 4500 permite el monitoreo del tráfico dirigido a la CPU, ya sea de entrada o de salida, con el uso de la función SPAN estándar. La interfaz de destino se conecta a un monitor de paquetes o a un portátil administrador que ejecuta el software de rastreo de paquetes. Esta herramienta ayuda a analizar de forma rápida y precisa el tráfico que procesa la CPU. La herramienta proporciona la capacidad de monitorear las colas individuales que están enlazadas al motor de paquetes de la CPU.

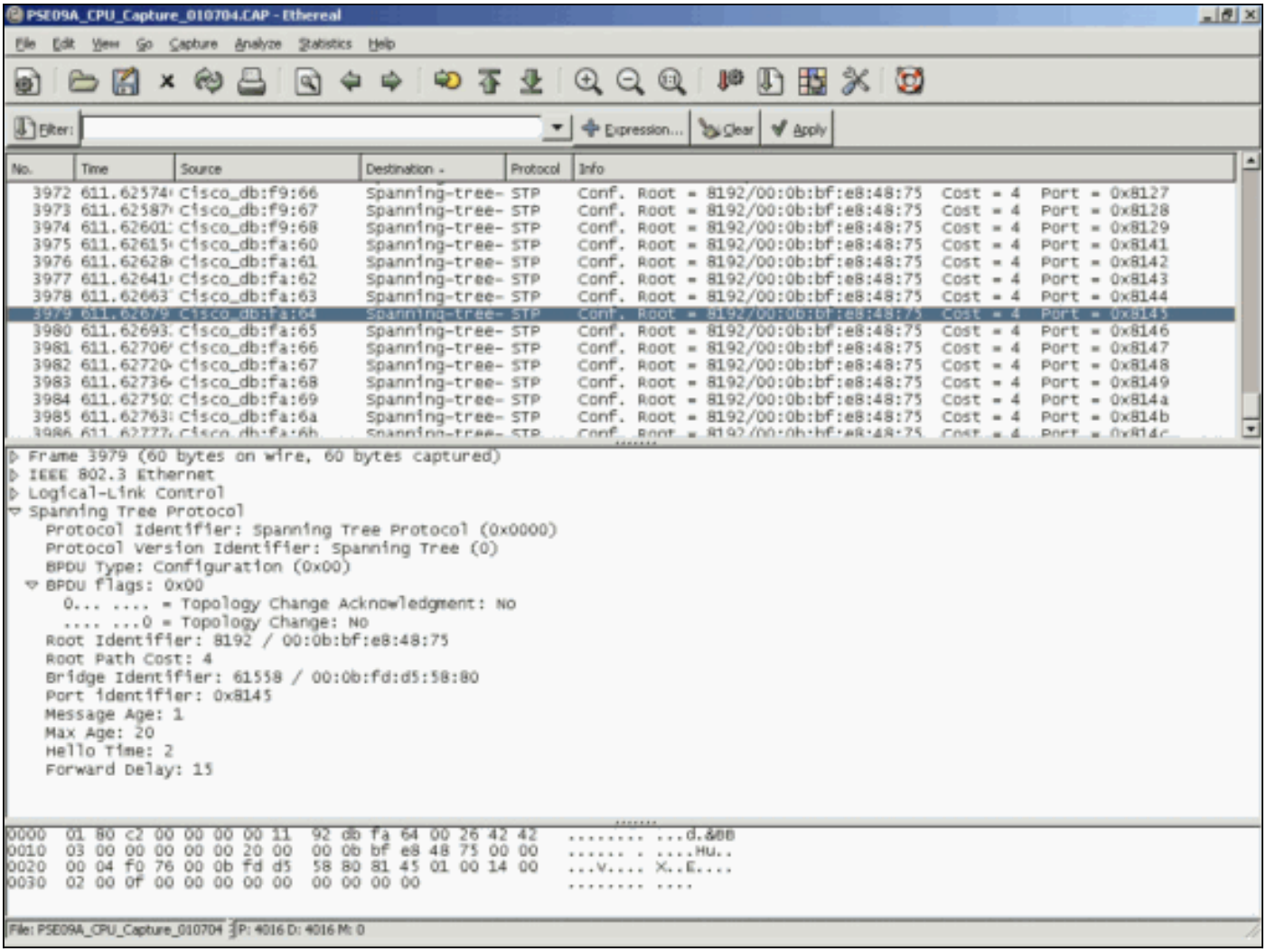
Nota: El motor de conmutación tiene 32 colas para el tráfico de la CPU y el motor de paquetes de la CPU tiene 16 colas.

```
Switch(config)#monitor session 1 source cpu ?
  both   Monitor received and transmitted traffic
  queue  SPAN source CPU queue
  rx     Monitor received traffic only
  tx     Monitor transmitted traffic only
  <cr>
Switch(config)#monitor session 1 source cpu queue ?
  <1-32>          SPAN source CPU queue numbers
  acl             Input and output ACL [13-20]
  adj-same-if     Packets routed to the incoming interface [7]
  all             All queues [1-32]
  bridged         L2/bridged packets [29-32]
  control-packet  Layer 2 Control Packets [5]
  mtu-exceeded    Output interface MTU exceeded [9]
  nfl             Packets sent to CPU by netflow (unused) [8]
  routed          L3/routed packets [21-28]
  rpf-failure     Multicast RPF Failures [6]
  span            SPAN to CPU (unused) [11]
  unknown-sa      Packets with missing source address [10]
Switch(config)#monitor session 1 source cpu queue all rx
Switch(config)#monitor session 1 destination interface gigabitethernet 1/3
Switch(config)#end
4w6d: %SYS-5-CONFIG_I: Configured from console by console

Switch#show monitor session 1
Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : CPU
Destination Ports : Gi1/3
    Encapsulation : Native
          Ingress : Disabled
        Learning  : Disabled
```

Si conecta un PC que ejecuta un programa de sabueso, puede analizar rápidamente el tráfico. En el resultado que aparece en la ventana de esta sección, puede ver que la causa del uso elevado de la CPU es un número excesivo de BPDU STP.

Nota: Las BPDU STP en el analizador de CPU es normal. Pero si ve más de lo esperado, puede que haya superado los límites recomendados para su Supervisor Engine. Vea la sección Un Alto Número de Instancias de Puerto de Spanning Tree de este documento para obtener más información.



Herramienta 2: Sensor de CPU integrado: Cisco IOS Software Release 12.2(20)EW y posterior

El Catalyst 4500 proporciona un rastreador y descodificador de CPU integrado para identificar rápidamente el tráfico que afecta a la CPU. Puede habilitar esta función con el comando **debug**, como se muestra en el ejemplo de esta sección. Esta función implementa un búfer circular que puede retener 1024 paquetes a la vez. A medida que llegan nuevos paquetes, sobrescriben los paquetes más antiguos. Esta función es segura de usar cuando resuelve problemas de uso elevado de la CPU.

```
Switch#debug platform packet all receive buffer
platform packet debugging is on
Switch#show platform cpu packet buffered
Total Received Packets Buffered: 36
--------------------------------------
Index 0:
7 days 23:6:32:37214 - RxVlan: 99, RxPort: Gi4/48
Priority: Crucial, Tag: Dot1Q Tag, Event: Control Packet, Flags: 0x40, Size: 68
Eth: Src 00-0F-F7-AC-EE-4F Dst 01-00-0C-CC-CC-CD Type/Len 0x0032
Remaining data:
 0: 0xAA 0xAA 0x3  0x0  0x0  0xC  0x1  0xB  0x0  0x0
10: 0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16 0x63 0x28
20: 0x62 0x0  0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16
30: 0x63 0x28 0x62 0x80 0xF0 0x0  0x0  0x14 0x0  0x2
40: 0x0  0xF  0x0  0x0  0x0  0x0  0x0  0x2  0x0  0x63
Index 1:
```

```
7 days 23:6:33:180863 - RxVlan: 1, RxPort: Gi4/48
Priority: Crucial, Tag: Dot1Q Tag, Event: Control Packet, Flags: 0x40, Size: 68
Eth: Src 00-0F-F7-AC-EE-4F Dst 01-00-0C-CC-CC-CD Type/Len 0x0032
Remaining data:
 0: 0xAA 0xAA 0x3  0x0  0x0  0xC  0x1  0xB  0x0  0x0
10: 0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16 0x63 0x28
20: 0x62 0x0  0x0  0x0  0x0  0x80 0x0  0x0  0x2  0x16
30: 0x63 0x28 0x62 0x80 0xF0 0x0  0x0  0x14 0x0  0x2
40: 0x0  0xF  0x0  0x0  0x0  0x0  0x0  0x2  0x0  0x63
```

Nota: La utilización de la CPU cuando ejecuta un comando **debug** siempre es casi del 100%. Es normal tener un uso elevado de la CPU cuando se ejecuta un comando **debug**.

Herramienta 3: Identificación de la Interfaz que Envía el Tráfico a la CPU—Cisco IOS Software Release 12.2(20)EW y Posteriores

Catalyst 4500 proporciona otra herramienta útil para identificar las principales interfaces que envían tráfico/paquetes para el procesamiento de CPU. Esta herramienta le ayuda a identificar rápidamente un dispositivo de comando que envía un gran número de ataques de broadcast u otros ataques de denegación de servicio a la CPU. Esta función también es segura de usar cuando resuelve problemas de uso elevado de la CPU.

```
Switch#debug platform packet all count
platform packet debugging is on
Switch#show platform cpu packet statistics
!--- Output suppressed. Packets Transmitted from CPU per Output Interface Interface Total 5 sec
avg 1 min avg 5 min avg 1 hour avg ---------------------- --------------- --------- --------- --
------- ---------- Gi4/47 1150 1 5 10 0 Gi4/48 50 1 0 0 0 Packets Received at CPU per Input
Interface

Interface              Total           5 sec avg 1 min avg 5 min avg 1 hour avg
---------------------- --------------- --------- --------- --------- ----------
Gi4/47                           23130         5        10        50         20
Gi4/48                              50         1         0         0          0
```

Nota: La utilización de la CPU cuando ejecuta un comando **debug** siempre es casi del 100%. Es normal tener un uso elevado de la CPU cuando se ejecuta un comando **debug**.

Summary

Los switches Catalyst 4500 gestionan una alta velocidad de reenvío de paquetes IP versión 4 (IPv4) en hardware. Algunas de las funciones o excepciones pueden causar el reenvío de algunos paquetes a través de la trayectoria de proceso de la CPU. El Catalyst 4500 utiliza un sofisticado mecanismo de QoS para manejar los paquetes enlazados a la CPU. Este mecanismo asegura la fiabilidad y estabilidad de los switches y, al mismo tiempo, maximiza la CPU para el reenvío de software de los paquetes. Cisco IOS Software Release 12.2(25)EWA2 y posteriores proporcionan mejoras adicionales para la gestión de paquetes/procesos, así como para la contabilidad. El Catalyst 4500 también tiene suficientes comandos y herramientas potentes para ayudar en la identificación de la causa raíz de los escenarios de uso elevado de la CPU. Sin embargo, en la mayoría de los casos, el uso elevado de la CPU en Catalyst 4500 no es causa de inestabilidad de la red ni causa preocupación.

Información Relacionada

- Utilización de CPU en switches Catalyst 4500/4000, 2948G, 2980G y 4912G que ejecutan el software CatOS
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems