Contenido

Introducción

Este documento describe CPU elevada la utilización en las diversas plataformas Catalyst debido a inundar de los paquetes de detección y de las maneras del módulo de escucha del Multicast IPv6 de atenuar este problema.

Prerrequisitos

No hay requisitos previos.

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en los Cisco Catalyst 6500 Series Switch, los Catalyst 4500 Series Switch y los Catalyst 3850 Series Switch.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada).

Problema

CPU elevada la utilización se puede considerar en algunas Plataformas del Cisco Catalyst debido al tráfico del Multicast IPv6 con la dirección MAC en el rango 3333.xxxx.xxxx que es llevado en batea al CPU.

Según el RFC7042, todos los identificadores del Multicast MAC-48 prefijaron el "33-33" (es decir, 2**32 los identificadores del Multicast MAC en el rango a partir de la 33-33-00-00-00-00 a 33-33-FF-FF-FF-FF) se utilizan como se especifica en [RFC2464] para el Multicast IPv6. Un paquete del IPv6 con un DST de la dirección de destino de Multicast, consistiendo en los dieciséis octetos DST[1] con DST[16], se transmite a la dirección Multicast de los Ethernetes cuyos primeros dos octetos son el valor 3333 hexadecimal y cuyos octetos del último cuatro son los cuatro octetos más recientes de DST tal y como se muestra en del cuadro 1.

Se ha visto en algunas ocasiones que cuando los dispositivos de los host usando cierto indicador luminoso LED amarillo de la placa muestra gravedad menor NIC van al modo de sueño, inundan el tráfico del Multicast IPv6. Este problema no se limita a un vendedor del host determinado, aunque cierto chipsets se ha visto para exhibir este comportamiento más a menudo que otros.

Troubleshooting y solución

Usted puede utilizar los siguientes procedimientos para descubrir si su switch de Catalyst que considera CPU elevada la utilización es afectado por este problema, y para implementar las soluciones respectivas.

Catalyst 3850 Series Switch

En los Catalyst 3850 Switch, el proceso NGWC L2M utiliza el CPU para procesar los paquetes del IPv6. Cuando el snooping de la detección del módulo de escucha del Multicast (MLD) se inhabilita en el Switch, MLD únase a/paquete de la licencia se inundan a todos los puertos de miembro. Y, si hay mucho entrante MLD se une a/los paquetes de la licencia, este proceso consumirá más ciclos de la CPU para enviar los paquetes en todos los puertos de miembro. Se ha visto que cuando ciertos equipos del host van al modo de sueño, pueden enviar varios miles de paquetes/sec MLD del tráfico IGMPv6.

```
3850#show processes cpu detailed process iosd sorted | exc 0.0
Core 0: CPU utilization for five seconds: 43%; one minute: 35%; five minutes: 33%
Core 1: CPU utilization for five seconds: 54%; one minute: 46%; five minutes: 46%
Core 2: CPU utilization for five seconds: 75%; one minute: 63%; five minutes: 58%
Core 3: CPU utilization for five seconds: 48%; one minute: 49%; five minutes: 57%
PID    T C  TID    Runtime(ms) Invoked uSecs  5Sec      1Min     5Min     TTY   Process
12577  L           2766882     2422952 291    23.52     23.67    23.69    34816 iosd
12577  L 3  12577  1911782     1970561 0      23.34     23.29    23.29    34818 iosd
12577  L 0  14135  694490      3264088 0      0.28      0.34     0.36     0     iosd.fastpath
162    I           2832830     6643    0      93.11     92.55    92.33    0     NGWC L2M
```

Solución

Snooping del mld del IPv6 de la configuración en el Switches afectado global para habilitar el **snooping del mld del IPv6**. Esto debe bajar abajo de la utilización de la CPU.

```
3850#conf t
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#ipv6 mld snooping
3850(config)#end
```

Cuando MLD el snooping se habilita, una tabla de direcciones del Multicast IPv6 del por el VLAN se construye en el software y soporte físico. El Switch entonces realiza el bridging basado dirección Multicast del IPv6 en hardware, que previene estos paquetes que se procesarán por el

software.

Haga clic en el link para más información sobre configurar MLD el snooping

En las versiones anteriores de IOS XE, fue encontrado que la cola CPU podría conseguir pegada debido a este problema que pararía todos los paquetes de control en esa cola de ir al CPU. Esto fue reparada con CSCuo14829 en las versiones de IOS 3.3.3 y 3.6.0 y posterior. Refiera por favor este bug para los detalles.

Catalyst 4500 Series Switch

Hardware que reenvía del soporte de los Catalyst 4500 Series Switch del tráfico del Multicast IPv6 usando el Ternary Content Addressable Memory (TCAM). Esto se explica en el Multicast en el Switches de las Cisco Catalyst 4500E y 4500X Series

Cuando se trata del tráfico de la detección del módulo de escucha del Multicast IPv6, necesidades del Switch de realizar la expedición del software (usando los recursos de la CPU). Como se explica en configurar el snooping del IPv6 MLD en los Catalyst 4500 Switch MLD el snooping se puede habilitar o inhabilitar global o por el VLA N. Cuando MLD el snooping se habilita, una tabla del MAC address del Multicast IPv6 del por el VLAN se construye en el software y una tabla de direcciones del Multicast IPv6 del por el VLAN se construye en el software y soporte físico. El Switch entonces realiza el bridging basado dirección Multicast del IPv6 en hardware. Ésta es la conducta esperada en los Catalyst 4500 Series Switch.

¿Para marcar el tipo de paquete que es llevado en batea al CPU que podemos ejecutarnos? ¿**el paquete todo de la plataforma del debug mitiga**? ¿seguido por? ¿**muestre el paquete CPU de la plataforma mitigado**? comando.

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-------------------------------------
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data&colon;
0: 0x60 0x0  0x0  0x0  0x0  0x20 0x0  0x1  0xFE 0x80
10: 0x0  0x0  0x0  0x0  0x0  0x0  0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2  0x0  0x0  0x0  0x0
30: 0x0  0x0  0x0  0x0  0x0  0x1  0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0  0x5  0x2  0x0  0x0  0x1  0x0  0x83 0x0
```

Este paquete llegó en la interfaz Tengigabitethernet1/15 en 214 vlan del MAC Address de origen 44:39:C4:39:5A:4A. El protocolo 0x86DD es IPv6 y el dst MAC 33:33:FF:7F:EB:DB se está utilizando para los Nodos del IPv6 del Multicast MLD en este caso.

Solución

Tenemos dos opciones para reparar CPU elevada el utilización debido a este tráfico.

1. Inhabilite la generación de tráfico de la detección del módulo de escucha del Multicast IPv6 en el host extremo. Esto puede hecho actualizando los driveres NIC o inhabilitando la característica en el BIOS de los host que envían los paquetes del IPv6. Usted puede entrar

en contacto al vendedor de su máquina del cliente que puede ayudar a inhabilitar la característica en el BIOS o a actualizar los driveres NIC.

1. Permita a las Políticas del plano de control (CoPP) para caer la cantidad excesiva de tráfico de la detección del módulo de escucha del Multicast IPv6 que se esté llevando en batea al CPU. Y, estos paquetes son límite del salto de un local del link, así es conducta esperada que estos paquetes serán llevados en batea al CPU.

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-------------------------------------
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data&colon;
0: 0x60 0x0  0x0  0x0  0x0  0x20 0x0  0x1  0xFE 0x80
10: 0x0  0x0  0x0  0x0  0x0  0x0  0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2  0x0  0x0  0x0  0x0
30: 0x0  0x0  0x0  0x0  0x0  0x1  0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0  0x5  0x2  0x0  0x0  0x1  0x0  0x83 0x0
```

En el ejemplo antedicho, estamos limitando la cantidad de tráfico del IPv6 que sea manejado por el CPU a 32000 paquetes por segundo.

Catalyst 6500 Series Switch

Los Catalyst 6500 Switch toman las decisiones de reenvío en hardware usando el TCAM que no necesita normalmente la ayuda CPU mientras el TCAM tenga la entrada de reenvío.

El supervisor Enginet 720 en los Catalyst 6500 Switch tiene dos CPU. Un CPU es el procesador de administración de red (NMP) o el switch processor (SP). El otro CPU es la capa 3 CPU, que se llama el (RP) del Route Processor.

La utilización de la CPU del proceso y de la interrupción se enumera en el **comando show process cpu**. Como se muestra abajo, CPU elevada

```
4500#debug platform packet all buffer
platform packet debugging is on
Cat4500#sh platform cpu packet buffered
Total Received Packets Buffered: 1024
-------------------------------------
Index 0:
33 days 11:42:21:833532 - RxVlan: 214, RxPort: Te1/15
Priority: Normal, Tag: Dot1Q Tag, Event: L2 Router, Flags: 0x40, Size: 90
Eth: Src 44:39:C4:39:5A:4A Dst 33:33:FF:7F:EB:DB Type/Len 0x86DD
Remaining data&colon;
0: 0x60 0x0  0x0  0x0  0x0  0x20 0x0  0x1  0xFE 0x80
10: 0x0  0x0  0x0  0x0  0x0  0x0  0x46 0x39 0xC4 0xFF
20: 0xFE 0x39 0x5A 0x4A 0xFF 0x2  0x0  0x0  0x0  0x0
30: 0x0  0x0  0x0  0x0  0x0  0x1  0xFF 0x7F 0xEB 0xDB
40: 0x3A 0x0  0x5  0x2  0x0  0x0  0x1  0x0  0x83 0x0
```

Marque si cualquier interfaz o capa 3 Vlan está cayendo la mucha cantidad de tráfico. (Caídas de entradas en la cola). Si es así el tráfico puede conseguir llevó en batea al RP de eso vlan.

```
Vlan19 is up, line protocol is up
```

```
 Input queue: 0/75/6303532/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 5 minute input rate 19932000 bits/sec, 26424 packets/sec
 5 minute output rate 2662000 bits/sec, 1168 packets/sec
```

El siguiente comando puede ser utilizado para encontrar todos los paquetes en el buffer de la cola de entrada para la interfaz 19 vlan.

```
Vlan19 is up, line protocol is up
 Input queue: 0/75/6303532/0 (size/max/drops/flushes); Total output drops: 0
 Queueing strategy: fifo
 5 minute input rate 19932000 bits/sec, 26424 packets/sec
 5 minute output rate 2662000 bits/sec, 1168 packets/sec
```

Alternativamente, usted puede utilizar la captura de NetDR para capturar el tráfico que va al CPU en un Catalyst 6500 Switch. Este documento explica cómo interpretar los paquetes capturados usando la captura de NetDR.

```
------- dump of incoming inband packet -------interface Vl16, routine
mistral_process_rx_packet_inlin, timestamp 03:17:56.380dbus info: src_vlan 0x10(16), src_indx
0x1001(4097), len 0x5A(90)  bpdu 0, index_dir 0, flood 1, dont_lrn 0, dest_indx 0x4010(16400)
E8820000 00100000 10010000 5A080000 0C000418 01000008 00000008 4010417Emistral hdr: req_token
0x0(0), src_index 0x1001(4097), rx_offset 0x76(118)  requeue 0, obl_pkt 0, vlan 0x10(16)destmac
33.33.FF.4A.C3.FD, srcmac C8.CB.B8.29.33.62, protocol 86DDprotocol ipv6: version 6, flow
1610612736, payload 32, nexthdr 0, hoplt 1class 0, src FE80::CACB:B8FF:FE29:3362, dst
FF02::1:FF4A:C3FD
```

Solución

Utilice uno o más de las soluciones abajo.

1. Caiga los paquetes del Multicast IPv6 usando la configuración siguiente.

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. Reoriente el tráfico del Multicast IPv6 a un inusitado o los admin apagan la interfaz (Gi1/22 en este ejemplo).

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. Utilice el VLAN Access Control List (VACL) para caer el tráfico del Multicast IPv6.

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. Inhabilite el snooping del IPv6 MLD.

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. Caiga el tráfico del Multicast IPv6 usando las Políticas del plano de control (CoPP)

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

1. Utilice el control de tormentas en las interfaces de ingreso. el tráfico entrante de los monitores de control de tormentas nivela sobre el intervalo del a1 segundo y durante este intervalo compara el nivel de tráficog con el nivel de control de tormentas configurado del tráfico. El nivel de control de tormentas del tráfico es un porcentaje del ancho de banda disponible total del puerto. Cada puerto tiene un solo nivel de control de tormentas del tráfico que se utilice para todos los tipos de tráfico (broadcast, Multicast, y unicast).

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

7. En caso de que si el CPU es alto en SP (Procesador del switch), aplique la solución alternativa abajo.

```
6500(config)#mac-address-table static 3333.FF4A.C3FD vlan <vlan #> drop
```

Si usted no puede determinar la razón basada en la información proporcionada en este documento, abra por favor una petición del servicio TAC de investigar más lejos.