

Técnicas del filtro para CPU elevada el utilización debido a DLSw

Contenido

[Introducción](#)

[Diagnostique CPU elevada la utilización](#)

[Bit-intercambio las direcciones MAC](#)

[Determine los puntos finales SNA](#)

[Filtre en las savias](#)

[Filtre el tráfico no deseado](#)

[Permita solamente las direcciones MAC usadas para el SNA](#)

Introducción

Este documento describe cómo resolver problemas CPU elevada el utlitzation debido al Data-Link Switching (DLSw).

Diagnostique CPU elevada la utilización

Complete estos pasos para determinar DLSw es la causa CPU elevada de la utilización.

1. Ingrese el comando de la **clase CPU del proc de la demostración**.

```
CISCO-2821-P1#show proc cpu sort
CPU utilization for five seconds: 98%/16%; one minute: 98%; five minutes: 98%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
366 40569376 27522064 1474 72.31% 74.57% 74.62% 0 DLSw msg proc
371 2099016 27845490 75 3.83% 3.93% 3.94% 0 HyBridge Input P
13 134172 1263 106232 2.15% 0.27% 0.18% 0 Licensing Auto U
367 779500 27475147 28 1.27% 1.35% 1.35% 0 CLS Background
```

En el ouput anterior, el proceso del mensaje de DLSw indica que una cierta clase de tráfico que se interliga en DLSw y DLSw intenta enviarlo a todos los pares. Éste puede ser tráfico del explorador real de la Arquitectura de red de sistemas (SNA), BROCHE (protocolo de acceso del red secundario) enmarca (el SNA es punto de acceso de servicio (SAP) encapsulado), DECNet, o posiblemente NetBios. Incluso si no se envía a los pares, es procesado por DLSw y toma la utilización de la CPU, porque el tráfico de DLSw es **process-switched**.

La entrada de Hybridge es una pista, porque ésta indica el tráfico Ethernet-interligado. El

fondo de los Servicios de link de Cisco (CLS) también está implicado.

2. Ingrese el **comando show proc cpu history** para determinar cuánto tiempo la utilización de la CPU ha sido alta.
3. Ingrese el comando del par **SSP-dlx del show dlsw** para ver el tráfico en el par también.

```
CISCO-2821-P1#show dlsw peer ssp-dlx
Peer: 192.168.2.1 received transmitted
CUR_ex Can U Reach Explorers 0 3
DATA Data Frame 0 205842
--> DSAP: SNAP (0xAA) 0 205789
--> DSAP: Other 0 53
CAPX Capabilities Exchange 102 111
Total SSP Primatives 102 205956

DLX Peer Test Request 0 347
DLX Peer Test Response 347 0
Last SSP Sent: DATA

Total number of connected peers: 1
Total number of connections: 1
```

Bit-intercambio las direcciones MAC

El tráfico pudo incrementar rápidamente en las direcciones MAC aprendidas sobre el Bridge en la interfaz de Ethernet.

```
CISCO-2821-P1#show dlsw peer ssp-dlx
Peer: 192.168.2.1 received transmitted
CUR_ex Can U Reach Explorers 0 3
DATA Data Frame 0 205842
--> DSAP: SNAP (0xAA) 0 205789
--> DSAP: Other 0 53
CAPX Capabilities Exchange 102 111
Total SSP Primatives 102 205956

DLX Peer Test Request 0 347
DLX Peer Test Response 347 0
Last SSP Sent: DATA

Total number of connected peers: 1
Total number of connections: 1
```

Note los direccionamientos en la salida anterior que tienen una cuenta del rx y ninguna cuenta del tx. Éstos son los direccionamientos del problema.

Usted puede utilizar el bit-intercambio de la [herramienta del bitswap](#) para las direcciones MAC en las direcciones Ethernet.

- El MAC 0088.a4b1.15b4 en DLSw es la dirección Ethernet 0011.258D.A82D.
- El MAC 09df.6568.72ee en DLSw es la dirección Ethernet 90FB.A616.4E77.

- El MAC 4000.7500.0001 en DLSw es la dirección Ethernet 0200.ae00.0080.

Determine los puntos finales SNA

Usted necesita saber qué direcciones MAC y saviás comprenden los puntos finales SNA. Si todo es en línea y trabajos, usted puede determinar esto con el **comando show dlsw circuit**:

```
CISCO-2821-P1#show dlsw cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

En la salida anterior, el MAC Address local es la forma no canónica (del Token Ring) de la dirección MAC. Eso significa que need bit-para ser intercambiado para ver la dirección MAC mientras que aparece en los Ethernetes. El número en paréntesis (04) es SAP que sean utilizados por esta conexión. Todas las estaciones terminales en la salida anterior utilizan 0x04. Las saviás se utilizan que son tan 0 y 4. SAP 0x0 se utilizan para los exploradores.

Filtro en las saviás

Ahora, usted puede filtrar en las saviás. Usted debe permitir por lo menos 0 y 4. Es una práctica adecuada permitir siempre 0, 4, 8, y el C.

Para más información, refiera a las [técnicas de filtrado del DLSw+ SAP/MAC](#).

Suponga que usted tiene una configuración como esto:

```
CISCO-2821-P1#show dlsw cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Usted necesitaría filtrar primero qué se envía entre los pares de DLSw, porque éste tiene el impacto más grande. Usted puede bloquear las saviás AA (BROCHE), E0 (Novell Netware), y F0 (NetBios). Esta configuración es segura de implementar.

```
CISCO-2821-P1#show dlsw cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Usted podría utilizar la versión del **permiso del filtro**, si usted sabe qué SNA socava las aplicaciones del cliente y si la lista es pequeña. Aquí tiene un ejemplo:

```
CISCO-2821-P1#show dlsw cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Tráfico no deseado del filtro

Usted puede filtrar el tráfico no deseado en el bridge-group en la interfaz de Ethernet:

```
CISCO-2821-P1#show dls w cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Note: Este ejemplo utiliza el permit 0, 4, 8, y C de la **lista de acceso 200** para con (comando/respuesta) un bit de alto nivel. Este ejemplo utiliza la **lista de acceso 201** para bloquear la BROCHE (protocolo de acceso del red secundario) y el otro tráfico no deseado.

Aplique los filtros en la interfaz de Ethernet:

```
CISCO-2821-P1#show dls w cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Aquí está un ejemplo de configuración en los Ethernetes:

```
CISCO-2821-P1#show dls w cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

Éste debe ser todo que es necesario para parar CPU elevada la utilización por el DLSw.

Direcciones MAC del permiso solamente usadas para el SNA

Hay un más paso que usted puede realizar para permitir solamente las direcciones MAC que se utilizan para el SNA de ser interligado. Asegúrese de que todos los dispositivos SNA sean en línea y trabajo para obtener una lista completa con este comando:

```
CISCO-2821-P1#show dls w cir
Index local addr(lsap) remote addr(dsap) state uptime
369099416 0088.a4b1.15b4(04) 4000.7500.0001(04) CONNECTED 1d02h
3607102105 09df.6568.72ee(04) 4000.7500.0001(04) CONNECTED 00:57:43
Total number of circuits connected: 2
```

```
MAC 0088.a4b1.15b4 in DLSw is ethernet address 0011.258D.A82D.
MAC 09df.6568.72ee in DLSw is ethernet address 90FB.A616.4E77.
```

```
access-list 701 permit 0011.258D.A82D 0000.0000.0000
```

```
access-list 701 permit 0FB.A616.4E77 0000.0000.0000
```

```
access-list 701 deny 0000.0000.0000 ffff.ffff.ffff
```

```
conf t
```

```
interface GigabitEthernet0/0.1  
bridge-group 1 input-address-list 701  
exit  
wr
```

Si usted todavía tiene CPU elevada utilización después de que usted complete este procedimiento, entre en contacto el Centro de Asistencia Técnica de Cisco (TAC) para extender el caso.