

# Técnicas do filtro para a utilização elevada da CPU devido a DLSw

## Índice

[Introdução](#)

[Diagnostique a utilização elevada da CPU](#)

[Bit-troca os endereços MAC](#)

[Determine os valores-limite SNA](#)

[Filtre nas seivas](#)

[Filtre o tráfego não desejado](#)

[Permita somente os endereços MAC usados para o SNA](#)

## Introdução

Este documento descreve como pesquisar defeitos o utilization da alta utilização da CPU devido ao switching de link de dados (DLSw).

## Diagnostique a utilização elevada da CPU

Termine estas etapas a fim determinar DLSw é a causa da utilização elevada da CPU.

1. Incorpore o comando do **tipo processador central do proc da mostra**.

```
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
```

Nas saídas precedentes, o processo da mensagem de DLSw indica que algum tipo do tráfego que é construído uma ponte sobre em DLSw e em DLSw tenta o enviar a todos os pares. Este pode ser tráfego de explorador real do Systems Network Architecture (SNA), PRESSÃO (protocolo de acesso da sub-rede) molda (o SNA é ponto de acesso ao serviço (SAP) encapsulado), DECNet, ou possivelmente NetBIOS. Mesmo se não é enviado aos pares, é processado por DLSw e toma a utilização CPU, porque o tráfego de DLSw é comutado por processo.

A entrada de hybride é um indício, porque este indica o tráfego Ethernet-construído uma

ponte sobre. O fundo dos Cisco Link Service (CLS) é envolvido igualmente.

2. Inscreva o comando **show proc cpu history** a fim determinar quanto tempo a utilização CPU foi alta.
3. Incorpore o comando do par **SSP-dlx do show dls w** a fim ver demasiado o tráfego no par.

```
CISCO-2821-P1#show dls w 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-troca os endereços MAC

O tráfego pôde incrementar rapidamente nos endereços MAC aprendidos sobre a ponte na interface Ethernet.

```
CISCO-2821-P1#show dls w 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
```

Observe os endereços na saída precedente que não têm uma contagem RX e nenhuma contagem de Tx. Estes são os endereços do problema.

Você pode usar a bit-troca que da [ferramenta do bitswap o](#) MAC endereça em endereços de Ethernet.

- O MAC 0088.a4b1.15b4 em DLSw é o endereço de Ethernet 0011.258D.A82D.
- O MAC 09df.6568.72ee em DLSw é o endereço de Ethernet 90FB.A616.4E77.

- O MAC 4000.7500.0001 em DLSw é o endereço de Ethernet 0200.ae00.0080.

## Determine os valores-limite SNA

Você precisa de saber que endereços e as seivas MAC compreendem os valores-limite SNA. Se tudo é em linha e trabalhos, você pode determinar este com o **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
```

Na saída precedente, o endereço MAC local é o formulário não-canônico (do Token Ring) do MAC address. Isso significa que need bit-para ser trocado a fim ver o MAC address enquanto aparece nos Ethernet. O número no parêntese (04) é SAP que é usado por esta conexão. Todas as estações final na saída precedente usam 0x04. Assim as seivas que são usadas são 0 e 4. SAP 0x0 são usadas para exploradores.

## Filtro nas seivas

Agora, você pode filtrar nas seivas. Você deve permitir pelo menos 0 e 4. É uma boa prática permitir sempre 0, 4, 8, e C.

Para mais informação, refira [técnicas de filtração do DLSw+ SAP/MAC](#).

Supõe que você tem uma configuração como este:

```
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
```

Você precisaria de filtrar primeiramente o que é enviado entre os pares de DLSw, porque este tem o impacto o maior. Você pode obstruir as seivas AA (PRESSÃO), E0 (Novell netware), e F0 (NetBIOS). Esta configuração é segura de executar.

```
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
```

Você poderia usar a versão da **licença do filtro**, se você sabe que SNA cava os usos do cliente e se a lista é pequena. Aqui está um exemplo:

```
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
```

# Tráfego não desejado do filtro

Você pode filtrar o tráfego não desejado no ponte-grupo na interface 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 exemplo usa o permit 0, 4, 8, e C da lista de acesso 200 com um bit da alta ordem (comando/resposta). Este exemplo usa a lista de acesso 201 a fim obstruir a PRESSÃO (protocolo de acesso da sub-rede) e o outro tráfego não desejado.

Aplice os filtros na interface 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
```

Está aqui um exemplo de configuração nos 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
```

Este deve ser tudo que é precisado a fim parar a utilização elevada da CPU pelo DLSw.

## Endereços da licença somente MAC usados para o SNA

Há uma mais etapa que você pode executar a fim permitir somente os endereços MAC que são usados para o SNA da construção de uma ponte sobre. Assegure-se de que todos os dispositivos SNA sejam em linha e trabalho a fim obter uma lista completa com 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
```

Se você ainda tem a utilização elevada da CPU depois que você termina este procedimento, contacte o centro de assistência técnica da Cisco (TAC) a fim de escalar o caso.