Techniques de filtre pour l'utilisation du CPU élevé due à DLSw

Contenu

Introduction

Ce document décrit comment dépanner l'utlitization élevé CPU dû au Data-Link Switching (DLSw).

Diagnostiquez l'utilisation du CPU élevé

Terminez-vous ces étapes afin de déterminer DLSw est la cause de l'utilisation du CPU élevé.

1. Sélectionnez la commande de **tri CPU de show proc**.

```
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
```

Dans la sortie précédente, le processus de message de DLSw indique qu'un certain genre de trafic qui pont dans DLSw et DLSw essaye de l'envoyer à tous les pairs. Ceci peut être le vrai trafic d'exploration du Systems Network Architecture (SNA), SNAP (protocole d'accès de sous-réseau) encadre (la SNA est point d'accès services (SAP) encapsulé), DECNet, ou probablement Netbios. Même si il n'est pas envoyé aux pairs, il est traité par DLSw et prend l'utilisation du processeur, parce que le trafic de DLSw est **commuté par processus**.

Le HyBridge Input est un indice, parce que ceci indique le trafic Ethernet-jeté un pont sur. Le fond des services de lien de Cisco (CLS) est également impliqué.

2. Sélectionnez la commande d'**historique CPU de show proc** afin de déterminer combien de temps l'utilisation du processeur a été élevée.

3. Sélectionnez la commande de **ssp-dlx de pair de dlsw d'exposition** afin de voir le trafic sur le pair aussi.

```
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-échange les adresses MAC

Le trafic pourrait incrémenter rapidement sur les adresses MAC apprises au-dessus de la passerelle sur l'interface 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
```

Notez les adresses dans la sortie précédente qui n'ont un compte de Rx et aucun compte de Tx. Ce sont les adresses de problème.

Vous pouvez utiliser le bit-échange d'outil de Bitswap que les adresses MAC dans des Ethernets adresse.

- Le MAC 0088.a4b1.15b4 dans DLSw est l'adresse 0011.258D.A82D d'Ethernets.
- Le MAC 09df.6568.72ee dans DLSw est l'adresse 90FB.A616.4E77 d'Ethernets.
- Le MAC 4000.7500.0001 dans DLSw est l'adresse 0200.ae00.0080 d'Ethernets.

Déterminez les points finaux SNA

Vous devez connaître quelles adresses MAC et sèves comportent les points finaux SNA. Si tout est en ligne et des travaux, vous pouvez déterminer ceci avec la commande de **circuit de dlsw d'exposition** :

```
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
```

Dans la sortie précédente, l'adresse MAC locale est la forme non-canonique (d'Anneau à jeton) de l'adresse MAC. Cela signifie qu'il neeed pour être bit-troqué afin de voir l'adresse MAC pendant qu'il apparaît sur les Ethernets. Le nombre dans la parenthèse (04) est SAP qui est utilisée par cette connexion. Toutes les stations d'extrémité dans la sortie précédente utilisent 0x04. Ainsi les sèves qui sont utilisées sont 0 et 4. SAP 0x0 est utilisées pour des explorateurs.

Filtre sur les sèves

Maintenant, vous pouvez filtrer sur les sèves. Vous devez permettre au moins 0 et 4. D'il est conseillé de autorisation toujours 0, 4, 8, et C.

Le pour en savoir plus, se rapportent à des techniques de filtrage DLSw+ SAP/MAC.

Supposez que vous avez une configuration comme ceci :

```
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
```

Vous devriez filtrer d'abord ce qui est envoyé entre les pairs de DLSw, parce que ceci a la plus grande incidence. Vous pouvez bloquer les sèves aa (SNAP), E0 (Novell NetWare), et F0 (Netbios). Il est sûre implémenter cette configuration.

```
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
```

Vous pourriez utiliser la version d'**autorisation du** filtre, si vous savez quelle SNA sape les utilisations de client et si la liste est petite. Voici un exemple :

```
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
```

Le trafic non désiré de filtre

Vous pouvez filtrer le trafic non désiré au passerelle-groupe sur l'interface Ethernet :

```
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
```

> **Note**: Cet exemple utilise le pemit de la **liste d'accès 200** 0, 4, 8, et C avec (commande/réponse) un bit d'ordre élevé. Cet exemple emploie la **liste d'accès 201** afin de bloquer le SNAP (protocole d'accès de sous-réseau) et tout autre trafic non désiré.

Appliquez les filtres sur l'interface Ethernet :

```
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
```

Voici un exemple de configuration sur les Ethernets :

```
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
```

Ceci devrait être tout ce qui est nécessaire afin d'arrêter l'utilisation du CPU élevé par le DLSw.

Adresses MAC d'autorisation seulement utilisées pour la SNA

Il y a une davantage étape que vous pouvez exécuter afin de permettre seulement les adresses MAC qui sont utilisées pour la SNA de l'pont. Assurez-vous que toutes les unités SNA sont en ligne et travail afin d'obtenir une liste complète avec cette commande :

```
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

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 vous avez toujours l'utilisation du CPU élevé après que vous remplissiez cette procédure, entrez en contact avec le centre d'assistance technique Cisco (TAC) afin de faire suivre le cas.