Exemple de configuration des fonctionnalités Wireshark des commutateurs de la gamme Catalyst 4500

Contenu

Introduction

Ce document décrit comment configurer la fonctionnalité Wireshark pour les commutateurs de la gamme Cisco Catalyst 4500.

Conditions préalables

Conditions requises

Pour utiliser la fonctionnalité Wireshark, vous devez remplir les conditions suivantes :

- Le système doit utiliser un commutateur de la gamme Cisco Catalyst 4500.
- Le commutateur doit exécuter Supervisor Engine 7-E (Supervisor Engine 6 n'est pas pris en charge pour le moment).
- La fonctionnalité doit avoir un ensemble IP Base et Enterprise Services (LAN Base n'est pas pris en charge pour le moment).
- Le processeur du commutateur ne peut pas avoir une condition d'utilisation élevée, car la fonction Wireshark est gourmande en CPU et le logiciel commute certains paquets dans le processus de capture.

Components Used

Les informations de ce document sont basées sur les commutateurs de la gamme Cisco Catalyst 4500 qui exécutent Supervisor Engine 7-E.

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.

Informations générales

Les commutateurs de la gamme Cisco Catalyst 4500 qui exécutent Supervisor Engine 7-E ont une nouvelle fonctionnalité intégrée avec Cisco IOS®-XE Versions 3.3(0) / 151.1 ou ultérieures. Cette fonctionnalité Wireshark intégrée permet de capturer des paquets d'une manière qui remplace l'utilisation traditionnelle de l'analyseur de port de commutateur (SPAN) par un PC connecté afin de capturer des paquets dans un scénario de dépannage.

Configuration

Cette section sert de guide de démarrage rapide pour commencer une capture. Les informations fournies sont très générales et vous devez implémenter des filtres et des paramètres de tampon si nécessaire afin de limiter la capture excessive de paquets si vous opérez dans un réseau de production.

Complétez ces étapes afin de configurer la fonctionnalité Wireshark :

1. Vérifiez que vous remplissez les conditions afin de prendre en charge la capture. (Référez-vous à la **Conditions requises** pour plus de détails.) Entrez ces commandes et vérifiez le résultat :

```
4500TEST#show version

Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
 (cat4500e-UNIVERSAL-M), Version 03.03.00.SG RELEASE SOFTWARE (fc3)

<output omitted>

License Information for 'WS-X45-SUP7-E'
 License Level: entservices   Type: Permanent
 Next reboot license Level: entservices

cisco WS-C4507R+E (MPC8572) processor (revision 8)
 with 2097152K/20480K bytes of memory.

Processor board ID FOX1512GWG1

MPC8572 CPU at 1.5GHz, Supervisor 7

<output omitted>

4500TEST#show proc cpu history

History information for system:

    888844444222222222222223333344444222222222222222255555222222
100
```

```
 90
 80
 70
 60
 50
 40
 30
 20
10 ****                                                  ****
0.....5.....1.....1.....2.....2.....3.....3.....4.....4.....5....5
           0     5     0     5     0     5     0     5     0    5

                     CPU% per second (last 60 seconds)
```

2. Le trafic est capturé dans une direction TX/RX à partir du port **gig2/26** dans cet exemple. Stocker le fichier de capture sur bootflash dans un **pcap** format de fichier à consulter à partir d'un PC local, si nécessaire :**Note**: Assurez-vous d'exécuter la configuration à partir du mode **EXEC utilisateur** et non du mode **Configuration globale**.

```
4500TEST#monitor capture MYCAP interface g2/26 both
4500TEST#monitor capture file bootflash:MYCAP.pcap
4500TEST#monitor capture MYCAP match any start

*Sep 13 15:24:32.012: %BUFCAP-6-ENABLE: Capture Point MYCAP enabled.
```

3. Ceci capture tout le trafic entrant et sortant sur le port **g2/26**. Il remplit également le fichier très rapidement avec du trafic inutile dans une situation de production, à moins que vous ne spécifiiez la direction et n'appliquiez des filtres de capture afin de restreindre l'étendue du trafic capturé. Entrez cette commande afin d'appliquer un filtre :

```
4500TEST#monitor capture MYCAP start capture-filter "icmp"
```

Note: Cela garantit que vous ne capturez que le trafic ICMP (Internet Control Message Protocol) dans votre fichier de capture.

4. Une fois que le fichier de capture expire ou remplit le quota de taille, vous recevez ce message :

```
*Sep 13 15:25:07.933: %BUFCAP-6-DISABLE_ASYNC:
 Capture Point MYCAP disabled. Reason : Wireshark session ended
```

Entrez cette commande afin d'arrêter manuellement la capture :

```
4500TEST#monitor capture MYCAP stop
```

5. Vous pouvez afficher la capture à partir de l'interface de ligne de commande. Entrez cette commande afin d'afficher les paquets :

```
4500TEST#show monitor capture file bootflash:MYCAP.pcap

 1   0.000000 44:d3:ca:25:9c:c9 -> 01:00:0c:cc:cc:cc CDP
      Device ID: 4500TEST  Port ID: GigabitEthernet2/26
 2   0.166983 00:19:e7:c1:6a:18 -> 01:80:c2:00:00:00 STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
 3   0.166983 00:19:e7:c1:6a:18 -> 01:00:0c:cc:cc:cd STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
 4   1.067989    14.1.98.2 -> 224.0.0.2    HSRP Hello (state Standby)
 5   2.173987 00:19:e7:c1:6a:18 -> 01:80:c2:00:00:00 STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
```

Note: L’option detail est disponible à la fin afin d’afficher le paquet dans un format Wireshark. En outre, l'option dump est disponible afin de voir la valeur hexadécimale du paquet.

6. Le fichier de capture devient encombré si vous n'utilisez pas de filtre de capture lorsque vous commencez la capture. Dans ce cas, utilisez l'option **display-filter** afin d'afficher le trafic spécifique dans l'affichage. Vous ne voulez afficher que le trafic ICMP, et non le trafic HSRP (Hot Standby Router Protocol), STP (Spanning Tree Protocol) et CDP (Cisco Discovery Protocol) présenté dans la sortie précédente. Le **filtre d'affichage** utilise le même format que Wireshark, pour que vous puissiez trouver les filtres en ligne.

```
4500TEST#show monitor capture file bootflash:MYCAP.pcap display-filter "icmp"

 17   4.936999  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=0/0, ttl=255)
 18   4.936999 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=0/0, ttl=251)
 19   4.938007  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=1/256, ttl=255)
 20   4.938007 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=1/256, ttl=251)
 21   4.938998  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=2/512, ttl=255)
 22   4.938998 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=2/512, ttl=251)
 23   4.938998  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=3/768, ttl=255)
 24   4.940005 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=3/768, ttl=251)
 25   4.942996  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=4/1024, ttl=255)
 26   4.942996 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=4/1024, ttl=251)
```

7. Transférez le fichier sur une machine locale, et regardez le fichier **pcap** comme vous le feriez pour n'importe quel autre fichier de capture standard. Entrez l'une de ces commandes afin de terminer le transfert :

```
4500TEST#copy bootflash: ftp://Username:Password@
```

```
4500TEST#copy bootflash: tftp:
```

8. Afin de nettoyer la capture, supprimez la configuration à l'aide des commandes suivantes :

```
4500TEST#no monitor capture MYCAP
4500TEST#show monitor capture MYCAP

<no output>

4500TEST#
```

Paramètres supplémentaires

Par défaut, la taille limite du fichier de capture est de 100 paquets, soit 60 secondes dans un fichier linéaire. Afin de modifier la limite de taille, utilisez l'option **limit** dans la syntaxe de capture du moniteur :

```
4500TEST#monitor cap MYCAP limit ?

duration       Limit total duration of capture in seconds
packet-length  Limit the packet length to capture
packets        Limit number of packets to capture
```

La taille maximale du tampon est de 100 Mo. Ceci est ajusté, ainsi que le paramètre de tampon circulaire/linéaire, avec cette commande :

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

La fonction Wireshark intégrée est un outil très puissant s'il est utilisé correctement. Il permet de gagner du temps et des ressources lors du dépannage d'un réseau. Cependant, soyez prudent lorsque vous utilisez la fonctionnalité, car elle peut augmenter l'utilisation du CPU dans les situations de trafic élevé. Ne configurez jamais l'outil et laissez-le sans surveillance.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

En raison de limitations matérielles, vous pouvez recevoir des paquets en panne dans le fichier de capture. Ceci est dû aux tampons séparés utilisés pour les captures de paquets d'entrée et de sortie. Si votre capture contient des paquets en panne, définissez les deux tampons sur **entrée**. Cela empêche les paquets en sortie de traiter avant les paquets en entrée lorsque la mémoire tampon est traitée.

Si vous voyez des paquets en panne, il est recommandé de modifier votre configuration des **deux** à **l'entrée** sur les deux interfaces.

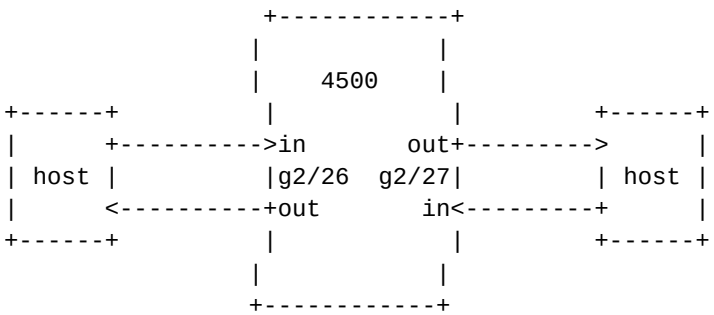
Voici la commande précédente :

```
4500TEST#monitor capture MYCAP interface g2/26 both
```

Remplacez la commande par les commandes suivantes :

```
4500TEST#monitor capture MYCAP interface g2/26 in

4500TEST#monitor capture MYCAP interface g2/27 in
```



Informations connexes

- Guide de configuration du logiciel du commutateur de la gamme Catalyst 4500, version IOS XE 3.3.0SG et IOS 15.1(1)SG - Configuration de Wireshark
- Support et documentation techniques - Cisco Systems