Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Informations générales](#)
[Configurez](#)
[Configurations supplémentaires](#)
[Vérifiez](#)
[Dépannez](#)
[Informations connexes](#)

Introduction

Ce document décrit comment configurer la caractéristique de Wireshark pour le Commutateurs de la gamme Cisco Catalyst 4500.

Conditions préalables

Conditions requises

Afin d'utiliser la caractéristique de Wireshark, vous devez remplir ces conditions :

- Le système doit utiliser un commutateur de gamme Cisco Catalyst 4500.
- Le commutateur doit exécuter l'engine 7-E de superviseur (l'engine 6 de superviseur est sans support à ce moment).
- La caractéristique doit avoir un IP Base de positionnement et des services d'entreprise (le LAN Base est sans support à ce moment).
- La CPU de commutateur ne peut pas avoir un état d'utilisation élevée, car la caractéristique de Wireshark est certains paquets CPU-intensifs et de logiciel-Commutateurs dans le processus de capture.

Composants utilisés

Les informations dans ce document sont basées sur le Commutateurs de la gamme Cisco Catalyst 4500 qui exécutent l'engine 7-E de superviseur.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le Commutateurs de la gamme Cisco Catalyst 4500 qui exécutent l'engine 7-E de superviseur a une nouvelle fonctionnalité intégrée avec le Cisco IOS? - Versions 3.3(0) XE/151.1 ou plus tard. Cette caractéristique de Wireshark de fonction intégrée a la capacité de capturer des paquets d'une manière dont remplace l'utilisation traditionnelle du Switch Port Analyzer (ENVERGURE) par un PC relié afin de capturer des paquets dans un scénario de dépannage.

Configurez

Cette section sert de guide de démarrage rapide afin de commencer une capture. Les informations fournies sont très générales, et vous devez implémenter des filtres et des configurations de mémoire tampon en tant que nécessaire afin de limiter la capture excessive des paquets si vous fonctionnez dans un réseau de production.

Terminez-vous ces étapes afin de configurer la caractéristique de Wireshark :

1. Vérifiez que vous remplissez les conditions afin de prendre en charge la capture. (Mettez en référence la section de **conditions requises** pour plus de détails.) Sélectionnez ces commandes et vérifiez la sortie :

```
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:

    888844444222222222222223333344444222222222222225555522222
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 du port **gig2/26** dans cet exemple. Enregistrez le fichier de capture sur le bootflash dans un format de fichier de **pcap** pour l'examen d'un ordinateur local, s'il y a lieu :Remarque: Assurez-vous que vous exécutent la configuration du mode d'**Exec de l'utilisateur**, pas mode de **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 tous les d'entrée et de sortie du trafic sur le port **g2/26**. Il remplit également fichier très rapidement de trafic inutile dans une situation de production, à moins que vous spécifiiez la direction et appliquiez des filtres de capture afin de rétrécir la portée du trafic qui est capturé. Sélectionnez cette commande afin d'appliquer un filtre :
`4500TEST#monitor capture MYCAP start capture-filter "icmp"`Remarque: Ceci s'assure que vous capturez seulement le trafic de Protocole ICMP (Internet Control Message Protocol) dans votre fichier de capture.
4. Une fois les minuteries de fichier de capture, ou remplit quota de taille, vous reçoivent ce message : `4500TEST#monitor capture MYCAP start capture-filter "icmp"`Sélectionnez cette commande afin d'arrêter manuellement la capture : `4500TEST#monitor capture MYCAP stop`
5. Vous pouvez visualiser la capture du CLI. Sélectionnez cette commande afin de visualiser 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
```

Remarque: L'option de détail est disponible à l'extrémité afin de visualiser le paquet dans un format de Wireshark. En outre, l'option de vidage mémoire est disponible afin de voir la valeur hexadécimale du paquet.

6. Le fichier de capture devient encombré si vous n'utilisez pas un capture-filtre quand vous commencez la capture. Dans ce cas, utilisez l'option d'affichage-**filtre** afin d'afficher le trafic spécifique dans l'affichage. Vous voulez seulement visualiser le trafic d'ICMP, le trafic pas de Protocole HSRP (Hot Standby Router Protocol), de Protocole Spanning Tree (STP), et de Protocole CDP (Cisco Discovery Protocol) affiché dans la sortie précédente. **L'affichage-filtre** utilise le même format que Wireshark, ainsi vous pouvez trouver le filtersonline.

`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 vers un ordinateur local, et regardez le fichier de **pcap** comme vous n'importe quel autre fichier standard de capture. Sélectionnez une de ces commandes afin de se terminer le transfert :
   ```
   4500TEST#copy bootflash: ftp://Username:Password@<ftp server address>
   4500TEST#copy bootflash: tftp:
   ```
8. Afin de nettoyer la capture, retirez la configuration avec ces commandes :
   ```
   4500TEST#no monitor capture MYCAP
   4500TEST#show monitor capture MYCAP

   <no output>

   4500TEST#
   ```

Configurations supplémentaires

Par défaut, la limite de taille du fichier de capture est 100 paquets, ou de 60 secondes dans un fichier Linéaire. Afin de changer la limite de taille, utilisez l'option de **limite** dans la syntaxe de monitor capture :

```
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 de mémoire tampon est 100 Mo. Ceci est ajusté, aussi bien que configuration circulaire/Linéaire de mémoire tampon, avec cette commande :

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

La caractéristique de Wireshark de fonction intégrée est très un outil puissant si utilisée correctement. Il économise le temps et les ressources quand vous dépannez un réseau. Cependant, attention d'exercice quand vous utilisez la caractéristique, parce qu'elle pourrait augmenter l'utilisation du processeur dans des situations du trafic élevé. Ne configurez jamais l'outil et laissez-le sans surveillance.

Vérifiez

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

Dépannez

En raison des limitations matérielles, vous pourriez recevoir des paquets en panne dans le fichier

de capture. C'est dû aux mémoires tampons distinctes utilisées pour les captures d'entrée et de paquet de sortie. Si vous avez des paquets en panne dans votre capture, placez chacun des deux vos mémoires tampons au **d'entrée**. Ceci empêche les paquets dans le de sortie de traiter avant les paquets d'entrée quand la mémoire tampon est traitée.

Si vous voyez des paquets en panne, il est recommandé que vous changez votre configuration de **chacun des deux** à **dedans** sur les deux interfaces.

Voici la commande précédente :

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

Changez la commande à ces derniers :

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

4500TEST#monitor capture MYCAP interface g2/27 in4500TEST#monitor capture MYCAP interface g2/26
in

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

Informations connexes

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