Catalyst Switches der Serie 4500 - Konfigurationsbeispiel für Wireshark-Funktionen

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration der Wireshark-Funktion für Cisco Catalyst Switches der Serie 4500.

Voraussetzungen

Anforderungen

Um das Wireshark-Feature zu verwenden, müssen Sie die folgenden Bedingungen erfüllen:

- Das System muss einen Cisco Catalyst Switch der Serie 4500 verwenden.
- Auf dem Switch muss die Supervisor Engine 7-E ausgeführt werden (die Supervisor Engine 6 wird derzeit nicht unterstützt).
- Diese Funktion muss über eine bestimmte IP Base- und Enterprise-Services verfügen (derzeit wird keine LAN Base-Unterstützung angeboten).
- Die Switch-CPU kann keine hohe Auslastung aufweisen, da die Wireshark-Funktion CPU-intensiv ist und Software bestimmte Pakete im Erfassungsprozess umschaltet.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Catalyst Switches der Serie 4500, auf denen die Supervisor Engine 7-E ausgeführt wird.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Die Cisco Catalyst Switches der Serie 4500, die die Supervisor Engine 7-E ausführen, verfügen über eine neue integrierte Funktionalität mit Cisco IOS®-XE Version 3.3(0)/151.1 oder höher. Diese integrierte Wireshark-Funktion kann Pakete so erfassen, dass die herkömmliche Verwendung von Switch Port Analyzer (SPAN) durch einen angeschlossenen PC ersetzt wird, um Pakete in einem Fehlerbehebungsszenario zu erfassen.

Konfigurieren

Dieser Abschnitt dient als Kurzanleitung, um mit der Erfassung zu beginnen. Die bereitgestellten Informationen sind sehr allgemein gehalten, und Sie müssen bei Bedarf Filter und Puffereinstellungen implementieren, um die exzessive Erfassung von Paketen zu begrenzen, wenn Sie in einem Produktionsnetzwerk arbeiten.

Gehen Sie wie folgt vor, um die Wireshark-Funktion zu konfigurieren:

1. Überprüfen Sie, ob Sie die Bedingungen erfüllen, um die Erfassung zu unterstützen. (Referenzieren Sie Anforderungen für weitere Informationen.) Geben Sie diese Befehle ein, und überprüfen Sie die Ausgabe:

```
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:

    888844444222222222222222333334444422222222222222255555222222
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. Datenverkehr wird vom Port in TX/RX-Richtung erfasst **Gig. 2/26** in diesem Beispiel. Speichern der Erfassungsdatei auf einem Bootflash in einem **Pappe** Dateiformat zur Prüfung von einem lokalen PC aus, falls erforderlich:**Hinweis**: Stellen Sie sicher, dass Sie die Konfiguration im **Benutzer-EXEC-**Modus durchführen, nicht im **globalen Konfigurationsmodus**.

```
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. Dies erfasst den gesamten ein- und ausgehenden Datenverkehr am Port. **g2/26**. Außerdem wird die Datei in einer Produktionssituation sehr schnell mit nutzlosem Datenverkehr gefüllt, es sei denn, Sie geben die Richtung an und wenden Erfassungsfilter an, um den Umfang des erfassten Datenverkehrs einzugrenzen. Geben Sie diesen Befehl ein, um einen Filter anzuwenden:

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

Hinweis: Dadurch wird sichergestellt, dass Sie nur ICMP-Datenverkehr (Internet Control Message Protocol) in Ihrer Erfassungsdatei erfassen.

4. Sobald die Erfassungsdatei das Timeout überschreitet oder das Größenkontingent ausfüllt, erhalten Sie die folgende Meldung:

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

Geben Sie diesen Befehl ein, um die Erfassung manuell zu beenden:

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

5. Sie können die Erfassung über die CLI anzeigen. Geben Sie den folgenden Befehl ein, um die Pakete anzuzeigen:

```
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
```

Hinweis: Die Detailoption ist am Ende verfügbar, um das Paket im Wireshark-Format anzuzeigen. Außerdem ist die Dump-Option verfügbar, um den Hex-Wert des Pakets anzuzeigen.

6. Die Erfassungsdatei wird übersichtlich, wenn Sie keinen Erfassungsfilter verwenden, wenn Sie mit der Erfassung beginnen. Verwenden Sie in diesem Fall die Option **Display-Filter**, um bestimmten Datenverkehr im Display anzuzeigen. Sie möchten nur den ICMP-Datenverkehr anzeigen, nicht den Hot Standby Router Protocol (HSRP)-, Spanning Tree Protocol (STP)- und Cisco Discovery Protocol (CDP)-Datenverkehr, der in der vorherigen Ausgabe gezeigt

wurde. Der **Anzeigefilter** verwendet das gleiche Format wie Wireshark, sodass Sie die Filtersonnenzeile finden können.

```
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. Übertragen Sie die Datei auf einen lokalen Computer, und betrachten Sie die **pcap-**Datei wie jede andere Standarddatenerfassungsdatei. Geben Sie einen der folgenden Befehle ein, um die Übertragung abzuschließen:

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

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

8. Um die Erfassung zu bereinigen, entfernen Sie die Konfiguration mit den folgenden Befehlen:

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

<no output>

4500TEST#
```

Zusätzliche Einstellungen

Die Größenbeschränkung der Erfassungsdatei beträgt standardmäßig 100 Pakete oder 60 Sekunden in einer linearen Datei. Um die Größenbeschränkung zu ändern, verwenden Sie die Option **limit** in der Monitorerfassungssyntax:

```
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
```

Die maximale Größe des Puffers beträgt 100 MB. Mit dem folgenden Befehl wird diese Einstellung sowie die Einstellung für den runden/linearen Puffer angepasst:

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

Die integrierte Wireshark-Funktion ist ein sehr leistungsstarkes Tool, wenn sie korrekt verwendet wird. Sie spart Zeit und Ressourcen bei der Fehlerbehebung im Netzwerk. Seien Sie jedoch vorsichtig, wenn Sie die Funktion verwenden, da dies die CPU-Auslastung in Situationen mit hohem Datenverkehr erhöhen kann. Konfigurieren Sie das Tool niemals, und lassen Sie es unbeaufsichtigt.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Aufgrund von Hardware-Einschränkungen erhalten Sie möglicherweise Pakete in der Erfassungsdatei, die nicht in der richtigen Reihenfolge sind. Dies ist auf die separaten Puffer zurückzuführen, die für die Erfassung von Ein- und Ausgangs-Paketen verwendet werden. Wenn bei der Erfassung Pakete außerhalb der Reihenfolge aufgezeichnet wurden, legen Sie beide Puffer auf **Eingang** fest. Dadurch wird verhindert, dass die ausgehenden Pakete vor den eingehenden Paketen verarbeitet werden, wenn der Puffer verarbeitet wird.

Wenn Pakete außerhalb der Reihenfolge angezeigt werden, wird empfohlen, die Konfiguration von **beiden** auf **in** beiden Schnittstellen zu ändern.

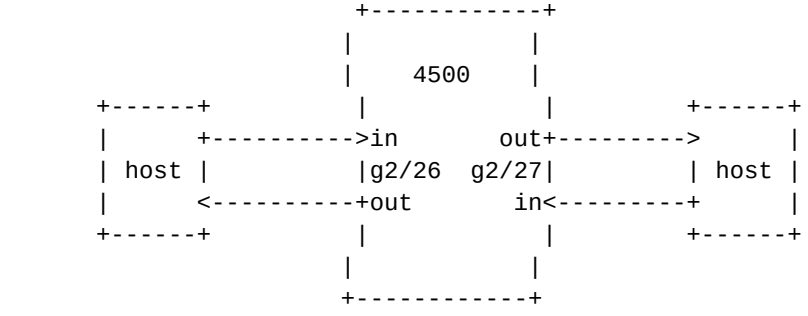
Der vorherige Befehl ist wie folgt:

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

Ändern Sie den Befehl folgendermaßen:

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

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



Zugehörige Informationen

- Catalyst Switch der Serie 4500 - Software-Konfigurationsleitfaden, Version IOS XE 3.3.0SG und IOS 15.1(1)SG - Konfigurieren von Wireshark
- Technischer Support und Dokumentation - Cisco Systems