Содержание

Введение

Этот документ описывает, как настроить функцию Wireshark коммутаторов Cisco Catalyst серии 4500.

Предварительные условия

Требования

Для использования функции Wireshark необходимо удовлетворить этим условиям:

- Система должна использовать коммутатор Cisco Catalyst серии 4500.
- Коммутатор должен выполнить Supervisor Engine 7-E (Supervisor Engine 6 является неподдерживаемым в это время).
- Функция должна иметь Ядро IP набора, и Корпоративное обслуживание (Ядро LAN является неподдерживаемым в это время).
- ЦП коммутатора не может иметь условия высокого коэффициента использования, как функция Wireshark с высокой загрузкой ЦПУ и программные коммутаторы определенные пакеты в процессе перехвата.

Используемые компоненты

Сведения в этом документе основываются на коммутаторах Cisco Catalyst серии 4500, которые выполняют Supervisor Engine 7-E.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Коммутаторы Cisco Catalyst серии 4500, которые выполняют Supervisor Engine 7-E, имеют новую встроенную функциональность с Cisco IOS? - Версии XE 3.3 (0) / 151.1 или позже. Эта встроенная функция Wireshark имеет способность перехватить пакеты в пути, который заменяет традиционное использование Анализатора коммутируемых портов (SPAN) с присоединенным ПК для получения пакетов в сценарии устранения проблем.

Настройка

Этот раздел служит руководством по быстрому началу работы для начала перехвата. Предоставленная информация является очень общей, и необходимо внедрить фильтры и буферные параметры настройки по мере необходимости для ограничения чрезмерного перехвата пакетов, если вы действуете в рабочей сети.

Выполните эти шаги для настройки функции Wireshark:

1. Проверьте, что вы удовлетворяете условиям для поддержки перехвата. (Сошлитесь на раздел **Требований** для получения дополнительной информации.) Вводят эти команды и проверяют выходные данные:

```
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:

    888844444222222222222223333344444222222222222222555552222222
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. Трафик перехвачен в направлении TX/RX от порта gig2/26 в данном примере. Сохраните перехват файла на загрузочной флэш-памяти в **pcap** формате файла для анализа от локального компьютера, если необходимый:**Примечание:** Гарантируйте выполнение конфигурации от **Пользовательского режима EXEC**, не **Режима глобальной конфигурации**.`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. Это перехватывает весь вход трафика и выход на порту g2/26. Это также заполняет файл очень быстро бесполезным трафиком в производственной ситуации, пока вы не задаете направление и применяете фильтры перехвата для сужения области трафика, который перехвачен. Введите эту команду для применения фильтра:
`4500TEST#monitor capture MYCAP start capture-filter "icmp"`**Примечание:** Это гарантирует, что вы только перехватываете трафик Протокола ICMP в своем перехвате файла.
4. Как только перехват файла испытывает таймаут или заполняет квоту размера, вы получаете это сообщение: `4500TEST#monitor capture MYCAP start capture-filter "icmp"`Введите эту команду для ручной остановки перехвата: `4500TEST#monitor capture MYCAP stop`
5. Можно просмотреть перехват от CLI. Введите эту команду для просмотра пакетов:
`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
```

Примечание: Подробная опция доступна в конце для просмотра пакета в формате Wireshark. Кроме того, опция дампа доступна для наблюдения Шестнадцатеричного значения пакета.
6. Если вы не используете фильтр перехвата при начале перехвата, перехват файла становится нарушенным. В этом случае используйте опцию **фильтра дисплейного отображения** для показа определенного трафика в показе. Вы только хотите просмотреть трафик ICMP, не Протокол HSRP, Протокол STP (STP) и трафик протокола CDP, показанный в предыдущих выходных данных. **Фильтр дисплейного отображения** использует тот же формат в качестве Wireshark, таким образом, можно найти 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. Передайте файл локальному компьютеру и посмотрите на pcap файл, поскольку вы были бы любой другой стандартный перехват файла. Введите одну из этих команд для завершения передачи:
```
4500TEST#copy bootflash: ftp://Username:Password@<ftp server address>
4500TEST#copy bootflash: tftp:
```
8. Для очистки перехвата удалите конфигурацию с этими командами:
```
4500TEST#no monitor capture MYCAP
4500TEST#show monitor capture MYCAP

<no output>

4500TEST#
```

Дополнительные параметры настройки

По умолчанию ограничение размера перехвата файла является 100 пакетами, или 60 секунд в линейном файле. Для изменения ограничения размера используйте предельную опцию в синтаксисе 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
```

Буферный максимальный размер составляет 100 МБ. Это отрегулировано, а также круговая/линейная буферная установка, с этой командой:

```
4500TEST#monitor cap MYCAP buffer ?

circular circular buffer
size     Size of buffer
```

Встроенной функцией Wireshark является очень мощное программное средство, если используется правильно. Это экономит время и ресурсы при устранении проблем сети. Однако проявите осторожность при использовании функции потому что это могло бы увеличить загрузку ЦПУ в ситуациях большого объема трафика. Никогда не настраивайте программное средство и оставляйте его необслуживаемым.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Из-за аппаратных ограничений, вы могли бы получить поврежденные пакеты в перехвате

файла. Это происходит из-за отдельных буферов, используемых для перехватов исходящего пакета и входа. Если вы имеете поврежденные пакеты в своем перехвате, устанавливаете оба из ваших буферов к **входу**. Когда буфер обработан, это предотвращает пакеты в выходе от обработки перед входящими пакетами.

Если вы видите поврежденные пакеты, рекомендуется изменить конфигурацию от **обоих** до **в** на обоих интерфейсах.

Вот предыдущая команда:

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

Измените команду на них:

```
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
```

Дополнительные сведения

- Руководство по конфигурации программного обеспечения коммутатора серии Catalyst 4500, XE IOS выпуска 3.3.0SG и IOS 15.1 (1) SG - Wireshark Настройки
- Cisco Systems – техническая поддержка и документация