Встроенный захват пакета для Cisco IOS и примера конфигурации XE IOS

Содержание

Введение

Этот документ описывает функцию встроенной функции захвата пакетов (EPC) в программном обеспечении Cisco IOS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco IOS Release 12.4 (20) T или позже
- Выпуск 15.2 (4) S - 3.7.0 Cisco IOS XE или позже

Сведения в этом документе были созданы от устройств в лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Если используемая сеть является действующей, убедитесь в понимании возможного влияния любой из применяемых команд.

Общие сведения

Когда включено, маршрутизатор перехватывает пакеты, переданные и полученные. Пакеты являются сохраненными в буфере в DRAM и являются таким образом не персистентными через повторную загрузку. Как только данные перехвачены, они могут быть исследованы в сводке или подробном представлении на маршрутизаторе. Кроме того, данные могут быть экспортированы как захват пакета (PCAP) файл для учета дальнейшего исследования. Программное средство настраивают в режиме EXEC и считают временным программным средством помощи. В результате конфигурация программного средства не сохранена в конфигурации маршрутизатора и не останется на месте после перезагрузки системы.

Программное средство Генератора и Анализатора Config Захвата пакета доступно Клиентам Cisco для способствования конфигурации, перехвату и экстракции захватов пакета.

Пример конфигурации Cisco IOS

Основная конфигурация EPC

1. Определите 'накопительный буфер', который является временным буфером, в котором сохранены захваченные пакеты. Существуют различные варианты, которые могут быть выбраны, когда определен буфер; такой как размер, maxium размер пакета, и круговой/линейный:

   ```
   monitor capture buffer BUF size 2048 max-size 1518 linear
   ```
2. Фильтр может также быть применен для ограничения перехвата заданным трафиком. Определите Список контроля доступа (ACL) в режиме конфигурации и примените фильтр к буферу:

   ```
   ip access-list extended BUF-FILTER
   permit ip host 192.168.1.1 host 172.16.1.1
   permit ip host 172.16.1.1 host 192.168.1.1monitor capture buffer BUF filter access-list
   BUF-FILTER
   ```
3. Определите 'точку перехвата', которая определяет местоположение, где происходит перехват. Точка перехвата также определяет, происходит ли перехват для IPv4 или IPv6 и в котором коммутируемом пути (обрабатывают по сравнению с cef):

   ```
   monitor capture point ip cef POINT fastEthernet 0 both
   ```
4. Подключите буфер к точке перехвата:

   ```
   monitor capture point associate POINT BUF
   ```
5. Запустите перехват:

   ```
   monitor capture point start POINT
   ```
6. Перехват теперь активен. Позвольте набор необходимых данных.

7. Остановите перехват:

   ```
   monitor capture point stop POINT
   ```
8. Исследуйте буфер на модуле:

   ```
   show monitor capture buffer BUF dump
   ```
   Примечание: Эти выходные данные только

показывают шестнадцатеричный дамп пакетных перехватов. Для наблюдения их в человекочитаемом существует два пути.Экспортируйте буфер от маршрутизатора для дальнейшего анализа:

```
monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
```
Совет: CSCuw77601 запроса на расширение был подан для добавления почты - к опции под экспортом, таким образом, можно послать по электронной почте буфер diretly к почтовому идентификатору.Однако, предыдущий способ не всегда практичен, поскольку он потребовал доступа T/FTP к маршрутизатору. В таких ситуациях можно сделать копию шестнадцатеричного дампа и использовать любой онлайновый шестнадцатеричный-pcap преобразователь для просмотра файлов.

9. Как только необходимые данные были собраны, удалите 'точку перехвата' и 'накопительный буфер': `no monitor capture point ip cef POINT fastEthernet 0 both`
`no monitor capture buffer BUF`

Примечания:

- В версиях ранее, чем Cisco IOS Release 15.0 (1) M, размер буфера был ограничен 512K.
- В версиях ранее, чем Cisco IOS Release 15.0 (1) M, размер захваченного пакета был ограничен 1024 байтами.
- Буфер пакетов сохранен в DRAM и не сохранится через повторные загрузки.
- Конфигурация перехвата не сохранена в NVRAM и не сохранится через повторные загрузки.
- Точка перехвата может быть определена для получения в cef или процессах коммутации пути.
- Точка перехвата может быть определена для получения только на интерфейсе или глобально.
- Когда накопительный буфер экспортируется в формате PCAP, информация о L2 (такая как Инкапсуляция Ethernet) не сохранена.
- Методы SeeBest для поиска Дают команду для получения дополнительных сведений о командах, используемых в этом разделе.

Пример конфигурации Cisco IOS XE

Встроенная функция Захвата пакета была представлена в Выпуске 3.7 - 15.2 (4) S Cisco IOS XE. Конфигурация перехвата является другой, чем Cisco IOS, поскольку это добавляет больше опций.

Основная конфигурация EPC

1. Определите местоположение, где произойдет перехват:

```
monitor capture CAP interface GigabitEthernet0/0/1 both
```
2. Привяжите фильтр. Фильтр может быть задан встроенный, или ACL, или на class-map можно сослаться:

```
monitor capture CAP match ipv4 protocol tcp any any
```
3. Запустите перехват:

```
monitor capture CAP start
```

4. Перехват теперь активен. Позвольте ему собирать необходимые данные.

5. Остановите перехват:

```
monitor capture CAP stop
```

6. Исследуйте перехват в итоговом представлении:

```
show monitor capture CAP buffer brief
```

7. Исследуйте перехват в подробном представлении:

```
show monitor capture CAP buffer detailed
```

8. Кроме того, экспортируйте перехват в формате PCAP для дальнейшего анализа:

```
monitor capture CAP export ftp://10.0.0.1/CAP.pcap
```

9. Как только необходимые данные были собраны, удалите перехват:

```
no monitor capture CAP
```

Примечания:

- Перехват может быть выполнен на физических интерфейсах, подчиненных интерфейсах и туннельных интерфейсах.
- Сетевое распознавание приложений (NBAR), основанное фильтры, то использование **команда match protocol** под class-map, в настоящее время не поддерживается.
- Посмотрите Оптимальные методы для поиска Команд для получения дополнительных сведений о командах, используемых в этом разделе.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Для EPC, который работает на Cisco IOS XE, эта команда отладки может использоваться, чтобы гарантировать, что EPC установлен должным образом:

```
no monitor capture CAP
```

Дополнительные сведения

- Встроенный захват пакета - Cisco IOS XE
- Встроенный захват пакета - Cisco IOS
- Cisco Systems – техническая поддержка и документация