Захват VACL для точного анализа трафика с Cisco Catalyst 6000/6500 под управлением ПО Cisco IOS

Содержание

Введение

В данном документе приводится пример конфигурации для использования функции порта захвата ACL VLAN (VACL) для более точного анализа трафика сети. В данном документе также объясняются преимущества использования порта захвата VACL по сравнению с использованием SPAN на основе VLAN (VSPAN).

Чтобы настроить функцию порта захвата VACL на Cisco Catalyst 6000/6500 под управлением ПО Catalyst OS, см. раздел Захват VACL для точного анализа трафика с Cisco Catalyst 6000/6500 под управлением ПО CatOS Software.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Списки IP-доступа: см. раздел Настройка списков IP-доступа для дополнительных сведений.
- Виртуальная сеть LAN: для получения дополнительных сведений см. раздел Протокол магистрального соединения виртуальных сетей LAN/VLAN (VLAN/VTP) - Введение.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного и аппаратного обеспечения: коммутатор Cisco Catalyst серии 6506, на котором установлено ПО Cisco IOS® версии 12.2(18)SXF8.

Данные для этого документа были получены при тестировании указанных устройств в специально созданных лабораторных условиях. Все устройства, описанные в данном документе, обладают ненастроенной (заданной по умолчанию) конфигурацией. При работе в действующей сети необходимо изучить все возможные последствия каждой команды.

Соответствующие продукты

Данная конфигурация также может использоваться при работе с коммутаторами Cisco Catalyst серии 6000 / 6500, на которых установлено ПО Cisco IOS версии 12.1(13)E и более поздних версий.

Условные обозначения

Более подробные сведения о применяемых в документе обозначениях см. в документе Условные обозначения, используемые в технической документации Cisco.

Общие сведения

SPAN на основе VLAN

SPAN (анализатор коммутируемых портов) копирует трафик из одного или более портов-источников в сети VLAN или из одной или более сетей VLAN в порт назначения для анализа. Локальный SPAN поддерживает порты-источники, исходные сети VLAN и порты назначения на одном и том же коммутаторе Catalyst серии 6500.

Исходная сеть VLAN является сетью VLAN, которая контролируется для анализа трафика. SPAN на основе VLAN (VSPAN) использует VLAN в качестве исходного SPAN. Все порты в исходных сетях VLAN становятся исходными портами. Исходный порт является портом, контролируемым для анализа трафика сети. Магистральные порты можно настроить в качестве портов-источников в сочетании с немагистральными портами-источниками, но SPAN не копирует инкапсуляцию из магистрального порта-источника.

Для сеансов VSPAN с настроенными входными и выходными портами направляются два пакета из порта назначения, если пакеты коммутируются в одной и той же сети VLAN (один пакет в качестве входящего трафика из входящего порта и другой пакет в качестве исходящего трафика из исходящего порта).

VSPAN контролирует только трафик, который поступает или исходит из портов уровня 2 в сети VLAN.

- При настройке сети VLAN в качестве источника входящего трафика, и если трафик передается в контролируемую сеть VLAN, переданный трафик не контролируется, так как никогда не отображается в качестве входящего трафика, который поступает на порт уровня 2 в сети VLAN.

- При настройке сети VLAN в качестве источника исходящего трафика, и если маршрут трафика выходит за пределы контролируемой сети VLAN, передаваемый трафик не контролируется, так как он не отображается в качестве исходящего трафика, отправляемого из порта уровня 2 в сети VLAN.

Для получения дополнительных сведений об исходных сетях VLAN см. раздел Характеристики исходной сети VLAN.

ACL VLAN

Порты VACL обеспечивают контроль доступа для всех пакетов, передаваемых по мостовому соединению в сети VLAN или направляемых в/из интерфейса сети VLAN или WAN для захвата VACL. В отличие от стандартного Cisco IOS или расширенных списков ACL, которые настраиваются только на интерфейсах маршрутизаторов и применяются только к маршрутизируемым пакетам, порты VACL применяются ко всем пакетам и могут быть применены к интерфейсу VLAN или WAN. VACL обрабатываются в оборудовании. VACL используют ACL Cisco IOS. Порты VACL пропускают поля ACL Cisco IOS, которые не поддерживаются в оборудовании.

Порты VACL можно настроить для трафика IP, IPX и MAC-Layer. Порты VACL, примененные к интерфейсам WAN, поддерживают только IP-трафик для захвата VACL.

При настройке порта VACL и его применении в сети VLAN все пакеты, поступающие в сеть VLAN, проходят проверку данного VACL. Если применяется VACL к сети VLAN и список ACL к маршрутизируемому интерфейсу в сети VLAN, пакет, поступающий в сеть VLAN, сначала проходит проверку VACL и при получении разрешения проходит затем проверку во входном ACL перед его обработкой маршрутизируемым интерфейсом. Если пакет передается в другую сеть VLAN, он сначала проходит проверку в выходном ACL, который применен к переданному интерфейсу и при получении разрешения применяется порт VACL, настроенный для сети назначения VLAN. Если VACL настроен для определенного типа пакета, и пакет данного типа не соответствует VACL, по умолчанию действие отклоняется.

Преимущества использования VACL по сравнению с использованием VSPAN

Существует несколько ограничений использования VSPAN для анализа трафика:

- Происходит захват всего трафика уровня 2, который поступает в сеть VLAN. Это увеличивает количество данных, которое необходимо проанализировать.
- Количество сеансов SPAN, которое может быть настроено на коммутаторах Catalyst серии 6500, ограничено. Дополнительные сведения см. в разделе Ограничения сеансов локальных SPAN и RSPAN.
- Порт назначения получает копии отправленного и полученного трафика для всех контролируемых портов-источников. Если лимит порта назначения превышен, он может быть перегружен. Такая перегрузка может повлиять на передачу трафика на один или несколько портов-источников.

Функция захвата с помощью портов VACL позволяет преодолеть некоторые из данных ограничений. VACL изначально не предназначались для контроля трафика, но благодаря широкому диапазону функций по классификации трафика была введена функция порта захвата для упрощения анализа трафика сети. Ниже приведены преимущества использования портов захвата VACL по сравнению с использованием VSPAN:

- Точный анализ трафикаПорты VACL могут совпадать в зависимости от IP-адреса источника, IP-адреса назначения, типа протокола уровня 4, портов-источников и портов назначения уровня 4, а также других данных. Эта особенность делает порты VACL чрезвычайно полезными для точной идентификации и фильтрации трафика.
- Количество сеансовПорты VACL применяются в оборудовании; количество записей контроля доступа (ACE), которое можно создать, зависит от устройства TCAM, доступного на коммутаторах.
- Перегрузка порта назначенияТочная идентификация трафика позволяет сократить количество кадров, которое необходимо направить на порт назначения, и таким образом сводит к минимуму риск перегрузки.
- Пропускная способностьПорты VACL применяются в оборудовании; при применении портов VACL к сети VLAN на коммутаторах Cisco Catalyst серии 6500 пропускная способность не снижается

Настройка

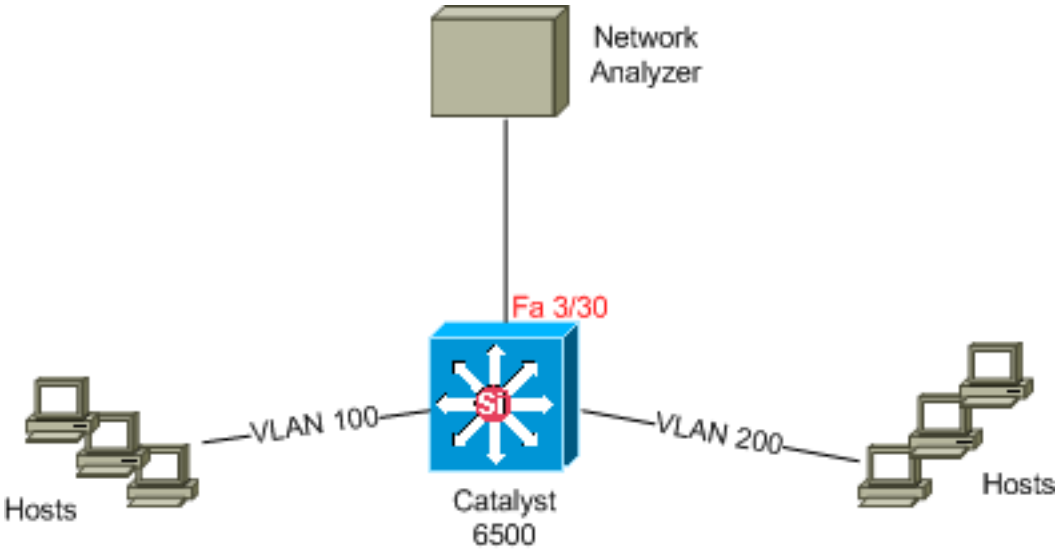
В этом разделе приводится информация по настройке функций, описанных в данном документе.

- Настройка со SPAN на основе VLAN
- Настройка с VACL

Примечание. Чтобы получить дополнительную информацию о применяемых в данном документе командах, используйте Средство поиска команд (только для зарегистрированных пользователей).

Схема сети

В данном документе используется следующая настройка сети.



Конфигурация со SPAN на основе VLAN

В данном примере конфигурации описываются действия, которые необходимо выполнить для захвата всего трафика уровня 2, который поступает в сеть VLAN 100 и VLAN 200, а также для его отправки устройству анализа сети:

1. Укажите соответствующий трафик. В приведенном примере это трафик, который поступает в сеть VLAN 100 и в сеть VLAN 200.
```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>

!---        ,

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```
2. Указать порт назначения для захваченного трафика.
```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

Если заданы эти значения, весь трафик уровня 2, который относится к VLAN 100 и к VLAN 200, копируется и передается на порт Fa3/30. Если порт назначения составляет часть той же сети VLAN, трафик которой контролируется, исходящий трафик из порта назначения не захватывается.

Проверьте конфигурацию SPAN с помощью команды **show monitor**.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
    TX Only        : None
    Both           : 100,200
Source RSPAN VLAN  : None
Destination Ports  : Fa3/30
Filter VLANs       : None
Dest RSPAN VLAN    : None
```

Конфигурация VACL

В данном примере конфигурации существуют многочисленные требования администратора сети:

- Трафик HTTP, поступающий из многочисленных хостов (10.20.20.128/25) в сети VLAN 200 на определенный сервер (10.10.10.101) в сети VLAN 100, должен быть захвачен.
- Трафик многоадресного протокола датаграмм пользователя (UDP) в направлении передачи, предназначенный для группового адреса 239.0.0.100, должен быть захвачен из сети VLAN 100.

1. Укажите соответствующий трафик.
```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```

2. Определите карту доступа VLAN.
```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config-access-map)#exit
```
3. Примените карту доступа VLAN к соответствующим сетям VLAN.
```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
```
4. Настройте порт захвата.
```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

Проверка

Используйте этот раздел, чтобы убедиться в исправной работе конфигурации.

Средство Интерпретатор выходных данных (только для зарегистрированных клиентов) (OIT) поддерживает некоторые команды **show**. Используйте OIT для просмотра аналитики выходных данных команды **show**.

- Команда **show vlan access-map** отображает содержимое карт доступа VLAN.
```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
```
- Команда **show vlan filter** отображает сведения о фильтрах VLAN.
```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

Поиск и устранение неполадок

Для этой конфигурации отсутствуют сведения об устранении неполадок.

Дополнительные сведения

- Захват VACL для точного анализа трафика с Cisco Catalyst 6000/6500 под управлением ПО Cisco IOS
- Поддержка коммутаторов Cisco Catalyst серии 6500
- Поддержка продуктов для LAN
- Техническая поддержка коммутационных решений для LAN
- Cisco Systems - техническая поддержка и документация