Односторонняя лавинная маршрутизация в коммутируемых сетях кампуса

Содержание

Введение

В настоящем документе описаны возможные причины и последствия односторонней лавинной маршрутизации пакетов в коммутируемых сетях.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Определение проблемы

Коммутаторы LAN используют таблицы переадресации (таблицы второго уровня (L2), таблицы ассоциативной памяти (CAM)), чтобы направить трафик на определенные порты на основе номера VLAN и MAC-адреса назначения кадра. Если во входящей VLAN нет записи,

соответствующей MAC-адресу назначения кадра, то (одноадресный) кадр будет направлен на все порты пересылки соответствующей VLAN, что вызывает лавинную маршрутизацию.

Ограниченная лавинная передача является частью нормального процесса коммутации. Бывают, однако, ситуации, когда непрерывная лавинная адресация может привести к неблагоприятному воздействию на производительность сети. В этом документе объяснено, какие проблемы могут возникнуть из-за лавинной адресации, и самые общие причины, по которым некоторые виды трафика могут постоянно переполняться.

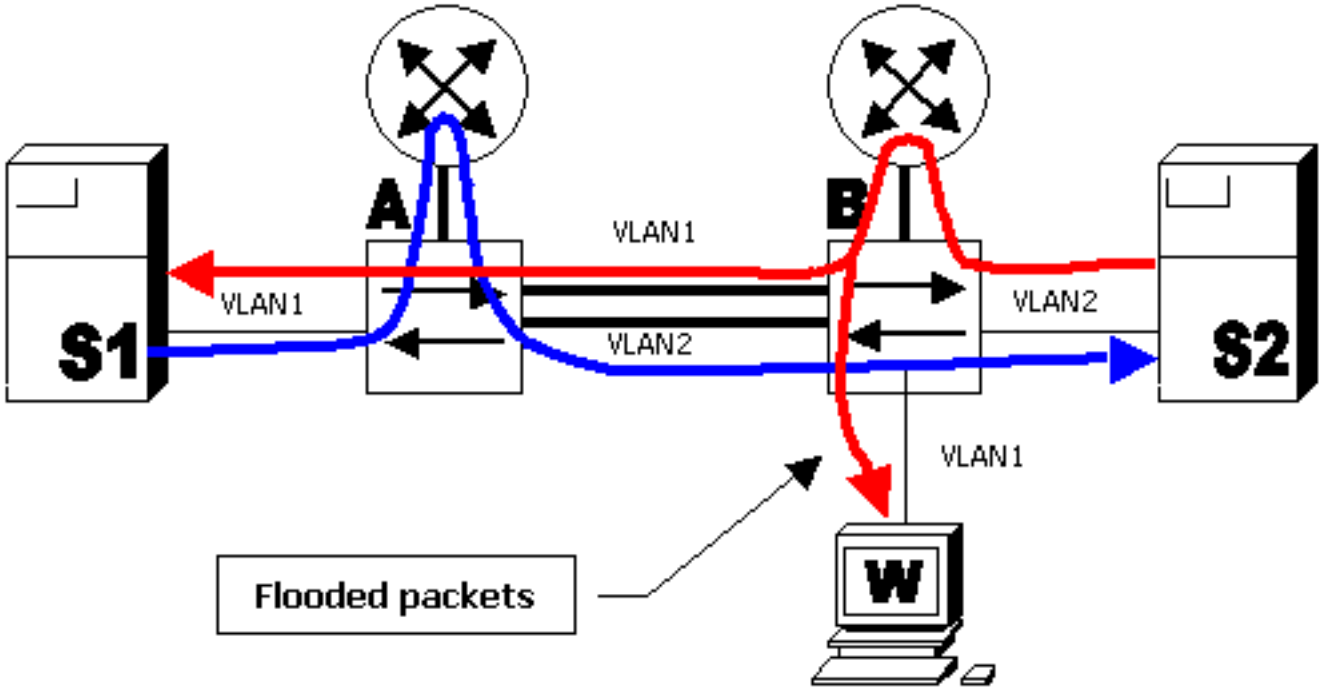
На большинстве современных коммутаторов, включая коммутаторы серии Catalyst 2900 XL, 3500 XL, 2940, 2950, 2970, 3550, 3750, 4500/4000, 5000 и 6500/6000 хранятся таблицы пересылки второго уровня для каждой сети VLAN.

Причины лавинной маршрутизации

Основная причина лавинной маршрутизации заключается в том, что MAC-адрес назначения пакета не находится в таблице пересылки L2 коммутатора. В таком случае, пакет будет направлен на все порты пересылки в своей VLAN (кроме порта получения). В следующих практических примерах отражены наиболее общие причины, по которым MAC-адрес назначения не известен коммутатору.

Причина 1: Асимметричная маршрутизация

Большое количество лавинно распространяющегося трафика может переполнить каналы с низкой пропускной способностью, что вызовет проблемы с производительностью сети или приведет к невозможности соединения с устройствами, подключенными через такие каналы с низкой пропускной способностью. Посмотрите на следующую схему:



На представленной выше схеме, сервер S1 в сети VLAN 1 работает в качестве резервного (тотальная передача данных) для сервера S2 во VLAN 2. Шлюз по умолчанию сервера S1 указывает на интерфейс сети VLAN 1 маршрутизатора A. Шлюз по умолчанию сервера S2

указывает на интерфейс сети VLAN 2 маршрутизатора B. Пакеты из S1 в S2 будут переданы по следующему пути:

- S1--VLAN 1--коммутатор A--маршрутизатор A--VLAN 2--коммутатор B--VLAN 2--S2 (синяя линия)

Пакеты из S2 на S1 направляются по следующему пути:

- S2--VLAN 2--коммутатор B--маршрутизатор B--VLAN 1--коммутатор A--лавинная маршрутизация во VLAN 1--S1 (красная линия)

Учтите, что при такой схеме коммутатор A не будет "видеть" трафик от MAC-адреса S2 в сети VLAN 2 (так как MAC-адрес источника будет переписан маршрутизатором B и пакет достигнет только сети VLAN 1). Это означает, что каждой отправке пакета на MAC-адрес S2 коммутатором A, пакет будет лавинно направляться в VLAN 2. Такая же ситуация будет происходить с MAC-адресом S1 на коммутаторе B.

Такое поведение называется асимметричной маршрутизацией. Пакеты следуют различными путями, в зависимости от направления. Асимметричная маршрутизация – одна из двух наиболее распространенных причин лавинной передачи.

Последствий однонаправленного лавинного потока

Вернемся к описанному примеру. В результате, пакеты передачи данных между S1 и S2 главным образом будут лавинно передаваться во VLAN 2 коммутатора A и в VLAN 1 коммутатора B. Это значит, что каждый подключаемый порт (в данном примере рабочая станция W) в сети VLAN 1 коммутатора B будет получать все пакеты разговоров между S1 и S2. Предположим, резервирование сервера занимает полосу пропускания в 50 Мб/с. Такое количество трафика заполнит каналы в 10 Мбит/сек. Это приведет к полному отключению соединений с компьютерами или значительно замедлит их.

Данная лавинная адресация является следствием асимметричной маршрутизации и может остановиться, когда сервер S1 отправит широковещательный пакет (например, протокол разрешения адреса (ARP)). Коммутатор A перешлет этот пакет в сеть VLAN 1, и коммутатор B получит и запомнит MAC-адрес S1. Если коммутатор не получает трафик постоянно, эта запись переадресации устареет и возобновится лавинная маршрутизация. Такой же процесс происходит с S2.

Существует несколько подходов для ограничения лавинной адресации, вызванной асимметричной маршрутизацией. Дополнительные сведения см. в следующих документах:

- Асимметричная маршрутизация с мостовыми группами на коммутаторах Catalyst 2948G-L3 и 4908G-L3
- Асимметричная маршрутизация и HSRP (чрезмерное количество лавинного одноадресного трафика в сетях с маршрутизаторами под управлением HSRP)

Обычным подходом является сделать время ожидания ARP и время старения таблицы передачи коммутаторов близкими друг другу. Это приведет к широковещательной передаче пакетов ARP. Прежде чем запись таблицы передачи L2 устареет, обязательно должна произойти регенерация.

Типичным сценарием, при котором наблюдается подобная проблема, будет тот, когда зарезервированные коммутаторы уровня 3 (L3) (такие как Catalyst 6000 с платой Mutilayer Switch Feature Card (MSFC)) настроены для распределения нагрузки с помощью протокола

маршрутизатора в горячем резерве (HSRP). В этом случае один коммутатор будет активным для четных VLAN, а другой – для нечетных.

Причина 2: Изменения в топологии протокола связующего дерева

Другая распространенная проблема, вызванная лавинной передачей, - уведомление об изменении топологии STP. Уведомление об изменении топологии предназначено для исправления таблицы передачи после изменения топологии передачи. Это нужно для того, чтобы избежать обрывов соединения, поскольку после изменений топологии некоторые назначения, ранее доступные через отдельные порты, могут стать недоступными через различные порты. TCN сокращает время устаревания таблицы коммутации, чтобы предотвратить переполнение (происходящее в том случае, если адрес не будет установлен заново и устареет).

TCN включаются портом, который переходит в состояние передачи или выходит из него. Если даже определенный MAC-адрес и устарел, после TCN лавинная адресация в большинстве случаев не будет длиться долго, поскольку адрес будет получен повторно. Проблема может возникнуть при постоянном появлении TCN на коротких интервалах. Таблицы пересылки коммутаторов постоянно будут быстро устаревать, поэтому и лавинные потоки будут практически постоянными.

Обычно, в хорошо настроенных сетях, TCN случается редко. Когда порт коммутатора включается или выключается, в итоге появляется сообщение о превышении порога (TCN), как только STP-состояние порта изменяется на переадресацию или с нее. Когда порт перебрасывается, это может вызвать повторяющиеся TCN и лавинную маршрутизацию.

Порты с включенной функцией быстрого порта STP не будут вызывать TCN при входе или выходе из состояния пересылки. Рекомендуется конфигурация PortFast для всех портов конечных устройств (таких как принтеры, компьютеры, серверы и т.д.), ограничивающая TCN низким объемом. См. этот документ для получения дополнительной информации о TCN:

- Изменения топологии протокола Spanning Tree Protocol

Примечание: На плате MSFC IOS работает процесс оптимизации, вызывающий повторное заполнение таблиц ARP интерфейсов VLAN, когда в соответствующей сети VLAN происходит TCN. Это позволяет ограничить лавинную адресацию в случае поступления TCN, т. к. будет осуществляться рассылка ARP, и MAC-адрес хоста будет известен после ответа хоста ARP.

Причина 3: Переполнение таблицы пересылки

Еще одна причина лавинной передачи может заключаться в переполнении таблицы пересылки коммутатора. В данном случае определение новых адресов невозможно, что приводит к лавинной адресации пакетов, направленных на данные адреса, до тех пор, пока в таблице пересылки не появится свободное пространство. Затем будут изучаться новые адреса. Это возможно, но бывает редко, поскольку у большинства современных коммутаторов достаточно большие таблицы пересылки, чтобы разместить MAC-адреса для большинства проектов.

Опустошение таблицы перенаправления также может быть вызвано атакой на сеть, при которой один узел начинает генерировать кадры, в источнике которых указаны различные MAC-адреса. Это сделает невозможным использование всех ресурсов таблицы пересылки.

После заполнения таблиц переадресации происходит наплыв трафика из-за невозможности продолжать анализ. Этот вид атак может быть обнаружен при проверке таблицы пересылки коммутатора. Большинство MAC-адресов будут указывать на один и тот же порт или группу портов. Подобные атаки можно предупредить, ограничив количество MAC-адресов, изученных на ненадежных портах, с помощью функции обеспечения безопасности порта.

Руководства по настройке коммутаторов Catalyst под управлением ПО Cisco IOS® или CatOS содержат раздел "Настройка безопасности порта" или "Настройка контроля трафика на уровне порта". Дополнительные сведения см. в технической документации к своему коммутатору на страницах продукта Коммутаторы Cisco.

Примечание: Если одноадресная лавинная адресация происходит в порту коммутатора, который настроен для Защиты на уровне порта с условием "Restrict" фиксировать затопление, нарушение безопасности является trigerred.

```
Router(config-if)#switchport port-security violation restrict
```

Примечание: То, когда такое нарушение безопасности происходит, затронутые порты, настроенные для, "ограничивают" режим, должно отбросить пакеты с адресами неизвестного источника, пока вы не удаляете достаточное число безопасных MAC-адресов для падения ниже максимального значения. Это вызывает SecurityViolation в противоречии с инкрементом.

Примечание: Вместо этого поведения, если порт коммутатора перемещается в Состояние завершения работы тогда, необходимо настроить `(config-if) #switchport` так, чтобы порт определенного коммутатора был отключен для одноадресной лавинной адресации.

Как обнаружить чрезмерную адресацию

Большинство решений коммутаторов не имеют специальных команд для обнаружения переполнения. **Коммутаторы Catalyst 6500/6000 Supervisor Engine 2 и более новых серий под управлением ПО Cisco IOS (встроенная) версии 12.1(14)E и более новой или системным ПО Cisco CatOS версии 7.5 или более новой выполняют функцию 'защиты от одноадресной лавинной маршрутизации'.** В двух словах, эта функция позволяет коммутатору отслеживать количество лавинной маршрутизации на VLAN и предпринимать указанные заранее действия, если уровень лавинной маршрутизации превышает указанный предел. Такими действиями могут быть – создание записи в системном журнале, ограничение или отключение VLAN. Создание записи в системном журнале – наиболее подходящая мера для обнаружения лавинной маршрутизации. Когда лавинная маршрутизация превышает определенный объем, а указанным заранее действием является создание записи в системном журнале, будет напечатано следующее сообщение:

```
%UNICAST_FLOOD-4-DETECTED: Host 0000.0000.2100 on vlan 1 is flooding
to an unknown unicast destination at a rate greater than/equal to 1 Kfps
```

Указанный MAC-адрес является исходным MAC, их которого пакеты направляются на этот коммутатор. Часто необходимо знать MAC-адреса назначения, на которые коммутатор лавинно направляет пакеты (поскольку коммутатор осуществляет пересылку пакетов согласно MAC-адресу назначения). Cisco IOS (встроенная) версии 12.1(20)E для catalyst 6500/6000 supervisor engine 2 и выше будут способны отображать MAC-адреса, на которые осуществляется лавинная маршрутизация:

```
cat6000#sh mac-address-table unicast-flood
Unicast Flood Protection status: enabled
```

```
Configuration:
 vlan      Kfps         action       timeout
------+----------+-----------------+----------
   55          1             alert      none

Mac filters:
 No.    vlan   souce mac addr.           installed on           time left (mm:ss)
-----+------+----------------+-----------------------------+------------------

Flood details:
 Vlan   souce mac addr.              destination mac addr.
------+---------------+-----------------------------------------------
   55   0000.2222.0000    0000.1111.0029, 0000.1111.0040, 0000.1111.0063
                          0000.1111.0018, 0000.1111.0090, 0000.1111.0046
                          0000.1111.006d
```

Дальнейшее исследование позволит увидеть, действительно ли MAC-адрес 0000.2222.0000 должен отправлять трафик на MAC-адреса, указанные в разделе MAC-адресов назначения. Если трафик допустим, то необходимо установить причину, по которой MAC-адреса назначения неизвестны коммутатору.

Возникновение лавины можно обнаружить по отслеживанию пакетов, видимому на рабочей станции во время снижения темпа или остановки работы. Обычно одноадресные пакеты, не вовлекающие рабочую станцию, не должны повторно отображаться в порте. Если это происходит, возможно, идет лавинная передача. Для различных случаев лавинной маршрутизации содержание записей пакетов может различаться.

При асимметричной маршрутизации возможна отправка направляемых на определенный MAC-адрес пакетов, которые не прекратят поступать лавинообразно даже после ответа получателя. Если используются TCNs, лавинная адресация будет включать множество различных адресов, но наконец остановится и перезагрузится.

При переполнении таблицы пересылки L2 возможно нечто вроде затопления, как при асимметричной маршрутизации. Разница заключается в том, что вероятно появление большого количества странных пакетов или обычных пакетов в нестандартном количестве с разными MAC-адресами источника.

Дополнительные сведения

- Поддержка коммутаторов
- Поддержка технологии коммутации локальных сетей
- Техническая поддержка - Cisco Systems