Содержание

Введение

Когда пакеты лавинно рассылают LAN, создавая избыточный трафик и ухудшающуюся производительность сети, шторм трафика происходит. Можно использовать функцию управления штормом трафика для предотвращения разрушений на портах Уровня 2 широковещанием, передать в многоадресном режиме, или шторм трафика с конкретным адресом на физических интерфейсах.

Управление штормом трафика (также названный подавлением трафика) позволяет вам контролировать уровни широковещания поступления, передавать в многоадресном режиме, и трафик с конкретным адресом по интервалу с 10 миллисекундами. Во время этого интервала уровень трафика, который является процентом от общей доступной пропускной способности порта, по сравнению с уровнем управления штормом трафика, который вы настроили. Когда входной трафик достигает уровня управления штормом трафика, который настроен на порту, управление штормом трафика отбрасывает трафик, пока не заканчивается интервал.

Величины порога управления штормом трафика и временной интервал позволяют алгоритму управления штормом трафика работать с разными уровнями глубины

детализации. Более высокое пороговое значение позволяет большему количеству пакетов проходить.

По умолчанию, когда трафик превышает настроенный уровень, программное обеспечение Cisco Nexus Operating System (NX-OS) не принимает мер по ликвидации последствий. Однако можно настроить действие Встроенного управления событиями (EEM) к отключению из-за ошибки интерфейс, если трафик не спадает (опуститесь ниже порога) в определенном периоде времени

Рекомендации и ограничения для управления штормом трафика

При настройке уровня управления штормом трафика обратите внимание на следующие рекомендации и ограничения:

- Можно настроить управление штормом трафика на интерфейсе порт-канала.
- Не настраивайте управление штормом трафика на интерфейсах, которые являются участниками интерфейса порт-канала. Управление штормом трафика Настройки на интерфейсах, которые настроены в качестве участников канала порта, помещает порты в состояние ожидания.
- Задайте уровень как процент от общей пропускной способности интерфейса: Уровень может быть от 0 до 100.Дополнительная часть уровня может быть от 0 до 99. 100 процентов означают управление штормом "no traffic" (нета трафика). 0 процентов подавляют весь трафик.

Из-за аппаратных ограничений и метода, которым посчитаны пакеты других размеров, процент уровня является приближением. В зависимости от размеров кадров, которые составляют входящий трафик, фактический вынужденный уровень мог бы отличаться от настроенного уровня на несколько процентных пунктов.

Настройки по умолчанию для управления штормом трафика

Параметры	По умолчанию
Управление штормом трафика	Отключенный
Threshold percentage	100

Управление штормом трафика Настройки

Можно установить процент от общей доступной пропускной способности, которую может использовать управляемый трафик.

1. configure terminal
2. интерфейс { ethernet | номер port-channel
3. storm-control { | групповая адресация | индивидуальная рассылка процент уровня [.fraction]

Примечание: Управление штормом трафика использует интервал с 10 миллисекундами, который может влиять на поведение управления штормом трафика.

Проверка конфигурации управления штормом трафика

Для отображения сведений о конфигурации управления штормом трафика выполните одну из следующих задач:

Команда	Цель
show interface [ethernet | номер port-channel противостоит storm-control	Отображает конфигурацию управления штормом трафика для интерфейсов.
show running-config interface	Отображает конфигурацию управления штормом трафика.

Мониторинг счетчиков управления штормом трафика

Можно контролировать счетчики, которые устройство Cisco NX-OS поддерживает для действия управления штормом трафика.

Управление штормом Nexus 7000: Выбор соответствующих значений подавления

Чтобы помочь клиенту выбирать соответствующее пороговое значение, этот раздел предоставляет понимание на логике позади использования пороговых значений.

Примечание: информация, представленная здесь, не предоставляет номеров оптимального метода, но клиент может прийти к логическому решению после прохождения через информации.

Используемые компоненты

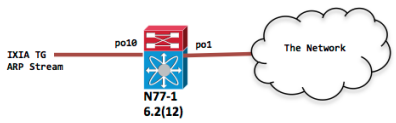
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Nexus 7700 с выпуском 6. 2.1(2) и более поздние версии.
- Линейная карта серии F3.

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.

Лабораторное испытание

Управление штормом является подавлением трафика mechnicm, который применен к входному трафику на определенном порте.



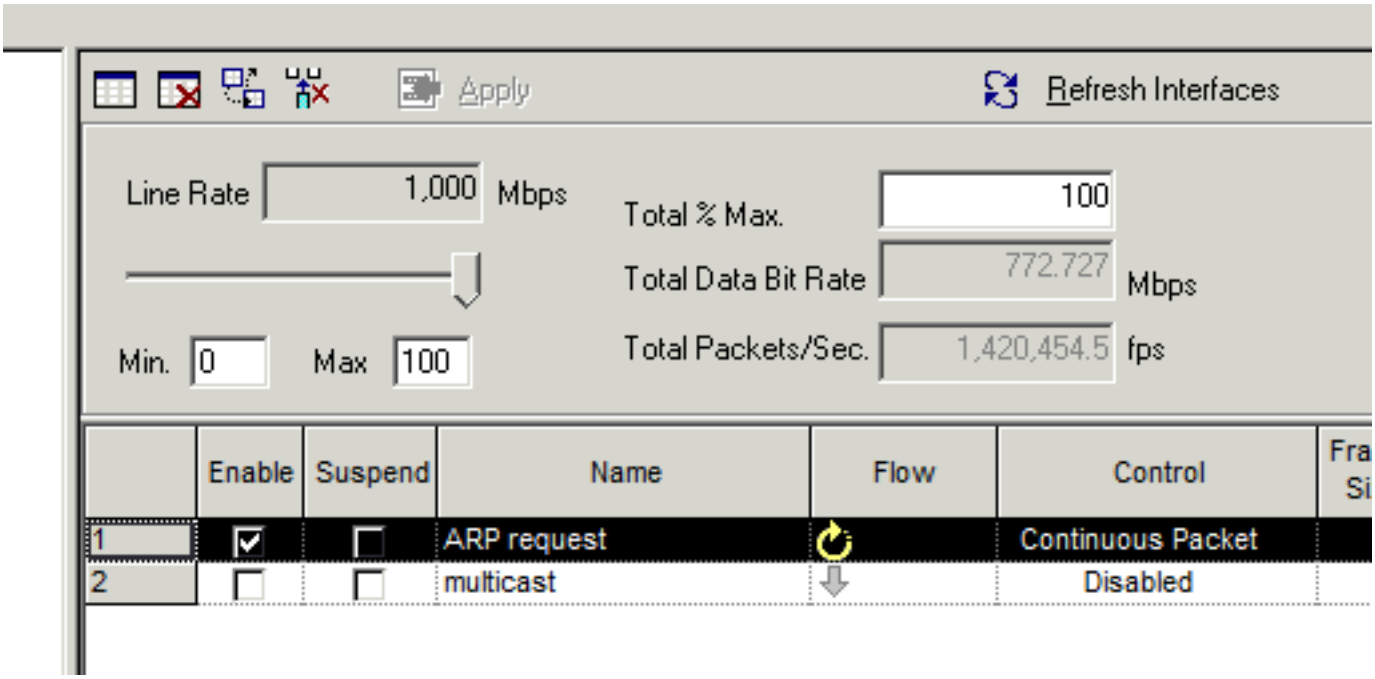
Scenerio 1: скорость Supression составляет 0.01%

Скорость входного трафика установлена в 1 Гбит/с трафика запроса ARP

Config

интерфейсный-порт-channel10
storm-control передавал уровень 0.01

Снимок IXIA для ссылки




```
N77-1(config-if)# sh int po10 | in rate | in "30 sec"  30 seconds input rate 954649416 bits/sec,
1420607 packets/sec  30 seconds output rate 1856 bits/sec, 0 packets/secinput rate 954.82 Mbps,
1.42 Mpps; output rate 1.97 Kbps, 0 pps N77-1(config-if)# sh int po1 | in rate | in "30 sec"  30
seconds input rate 8656 bits/sec, 8 packets/sec  30 seconds output rate 853632 bits/sec, 1225
packets/sec >>>> Output rate is ~ 1200 ppsinput rate 8.74 Kbps, 8 pps; output rate 875.32 Kbps,
1.22 Kpps N77-1# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port       UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
--------------------------------------------------------------------------------
Po10            100.00         100.00           0.01          67993069388
```

Отбрасывания управления штормом показывают для ссылки.

Scenerio 2: скорость Supression составляет 0.1%

Скорость входного трафика установлена в 1 Гбит/с трафика запроса ARP

Config

интерфейсный-порт-channel10
storm-control передавал уровень 0.10

Только переходить показывает исходящий интерфейс, так как входной интерфейс po10

имеет ту же скорость входящего трафика 1 Гбит/с

```
N77-1(config-if)# sh int po1 | in rate | in "30 sec"
  30 seconds input rate 8840 bits/sec, 8 packets/sec
  30 seconds output rate 8253392 bits/sec, 12271 packets/sec >>>> Output rate is ~ 12k pps
```

Scenerio 3: скорость Supression составляет 1%

Скорость входного трафика установлена в 1 Гбит/с трафика запроса ARP

Config

интерфейсный-порт-channel10

storm-control передавал уровень 1

Только переходить показывает исходящий интерфейс, так как входной интерфейс po10 имеет ту же скорость входящего трафика 1 Гбит/с

```
N77-1(config-if)# sh int po1 | in rate
  30 seconds input rate 8784 bits/sec, 7 packets/sec
  30 seconds output rate 86601056 bits/sec, 129293 packets/sec >>>> Output rate is ~ 120k pps
  input rate 8.78 Kbps, 7 pps; output rate 86.60 Mbps, 129.29 Kpps
```

Scenerio 4: скорость Supression составляет 10%

Скорость входного трафика установлена в 1 Гбит/с трафика запроса ARP

Config

интерфейсный-порт-channel10

storm-control передавал уровень 10.00

```
 N77-1(config-if)# sh int po1 | in rate
  30 seconds input rate 8496 bits/sec, 7 packets/sec
  30 seconds output rate 839570968 bits/sec, 1249761 packets/sec >>>> Output rate is ~ 1.2mil
pps
  input rate 8.50 Kbps, 7 pps; output rate 839.57 Mbps, 1.25 Mpps
```

Сводка:

Все вышеупомянутые сценарии имеют дело с длительным потоком трафика, возможно вызванным из-за петли или неправильно функционирующего NIC. Управление штормом является эффективным при этом сценарии в ограничении скорости трафик, прежде чем это будет введено в сеть. Другие уровни подавления говорят как, сколько трафика вы будете вводить в свою сеть.

Когда управление штормом существует, оно заставило бы обычный ARP быть отброшенным при хранении порога на агрессивном уровне?

Существует несколько вещей рассмотреть

1. Прежде всего, если ARP действительно становится отброшенным первоначально всегда существуют повторные попытки, инициируемые уровнем приложения, таким образом, возможности ARP, решаемого во время последующих повторных попыток, выше и приведут к успешному IP к разрешению MAC.
2. Управление штормом является ограничителем входа, и оно должно быть применено максимально близко к краю. Так вы, возможно, имея дело с физическими хостами или кластером VM. Если один хост тогда количество ARPs не является действительно проблемой во время обычного рабочего сценария. Если это - кластер VM, то у вас может быть определенное число хостов, но снова ничто, что укажет на целый слой 2 домена позади порта Edge.
3. Если вы применяетесь, config управления штормом на базовых портах тогда знают, как широковещательный трафик может быть объединен, прежде чем это достигнет магистрального уровня.

Возвращение к нашим тестам? поскольку пульсирующий трафик ARP здесь является некоторыми тестами -

Тест 1: 5000 пакетных пакетов 5000pps одиночный пакет

Уровень Supression 0.01%

Config

интерфейсный-порт-channel10

storm-control передавал уровень 0.01

```
N77-1# sh int po10
port-channel10 is up
admin state is up
RX
  12985158 unicast packets 27 multicast packets 5000 broadcast packets
  12990674 input packets 1091154042 bytes
  0 jumbo packets 2560 storm suppression packets

N77-1#Sh int po1
port-channel1 is up
admin state is up
TX
  0 unicast packets 507 multicast packets 2440 broadcast packets

N77-1(config-if)# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port      UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
--------------------------------------------------------------------------------
Po10            100.00        100.00           0.01                2560
```

Вышеупомянутое показывает 2560 отброшенных пакетов ARP. Конечно, если у вас есть 5000 хостов позади одного интерфейса тогда, половина из них проходит во время первой итерации, и вторая половина пройдет во время следующего или и так далее. Если ваше приложение только передает один запрос ARP для получения IP к разрешению MAC тогда, приложение, возможно, должно модифицироваться, чтобы повторно передать запросы ARP если никакой ответ. В этом случае сверьтесь с поставщиком приложений для помощи в изменении этого поведения.

Тест 2: 5000 пакетных пакетов 50000pps одиночный пакет

Уровень Supression 0.01%

Config

интерфейсный-порт-channel10

storm-control передавал уровень 0.01

```
N77-1(config-if)# sh int po10
port-channel10 is up
admin state is up
RX
  0 unicast packets 19 multicast packets 5000 broadcast packets
  5019 input packets 435550 bytes
  0 jumbo packets 3771 storm suppression packets

N77-1(config-if)# sh int po1
port-channel1 is up
admin state is up
TX
  0 unicast packets 712 multicast packets 1229 broadcast packets

N77-1(config-if)# sh int po10 counters storm-control
--------------------------------------------------------------------------------
Port      UcastSupp %    McastSupp %    BcastSupp %    TotalSuppDiscards
--------------------------------------------------------------------------------
Po10            100.00         100.00           0.01                3771
```

В вышеупомянутых выходных данных существует более высокое количество отбрасываний из-за более высокой скорости блока пакетов.

Похожие результаты замечены, поскольку скорость pps увеличена для 5000 блоков пакетов 100kpps до скорости передачи пакетов на 1 Гбит/с

Следующие опции доступны для обнаружения штормового условия.

Предупреждение в плоскости данных:

- Управление штормом Настройки генерирует сообщение системного журнала для предупреждений, и можно связать EEM, чтобы генерировать Перехваты простого протокола управления сетью (SNMP) или завершить работу порта как профилактического действия.

Предупреждение в Уровне управления:

- Настройте 'опцию' порога отбрасывания регистрации:

На Nexus 7k существует policy-map по умолчанию - уровень управления:

Эта карта политик регулирует, какой трафик проходит к ЦП. В этом policy-map вы видите класс, который регулирует, сколько ARP переходит к ЦП.

Настройка 'порог отбрасывания регистрации' под этим классом сообщит о любых нарушениях в системном журнале, можно далее использовать EEM для генерации trap-сообщения SNMP.

- Контроль уровня управления (CoPP) опрос MIB

Запускаясь в NX-OS 6.2 (2), CoPP поддерживает Cisco на основе классов, MIB QoS (cbQoSMIB) и все его элементы могут быть проверены с помощью SNMP

Заключение

Управление штормом является полезной возможностью, которая предотвращает разрушения на портах Уровня 2 широковещанием, групповой адресацией или штормом трафика с конкретным адресом на физических интерфейсах. Эта функция управляет штормом в плоскости данных, прежде чем это повлияет на уровень управления и CoPP.