

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Поток Трафика с конкретным адресом и Буферизация](#)

[Поток Многоадресного трафика и Буферизация](#)

[Какие причины вводят сброс?](#)

[Пример устранения проблем](#)

[Scenerio 1: входной сброс](#)

[Шаг 1: Определите порты с входным сбросом](#)

[Шаг 2: Идентификация ASIC](#)

[Шаг 3: Определите переполненный порт выхода](#)

[Scenerio 2: входной сброс с HOLB \(головка блокирования линии\)](#)

[Смягчение HOLB: Включите предел VOQ](#)

[Смягчение HOLB: классификация трафика](#)

[Связанные сведения](#)

Введение

Этот документ описывает, как устранить неполадки входного сброса на коммутаторах серии Cisco Nexus 5600/6000. Входной сброс является индикацией относительно превышенного выходного порта. Это также означает подобное отбрасывание трафика с конкретным адресом на том определенном порту. Ниже разделов поможет понимать, как одноадресно переданный и многоадресный трафик буферизован на этой платформе и как входной сброс мог произойти наряду с шагами смягчения.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах

- Cisco Nexus конфигурация серии 6000

Используемые компоненты

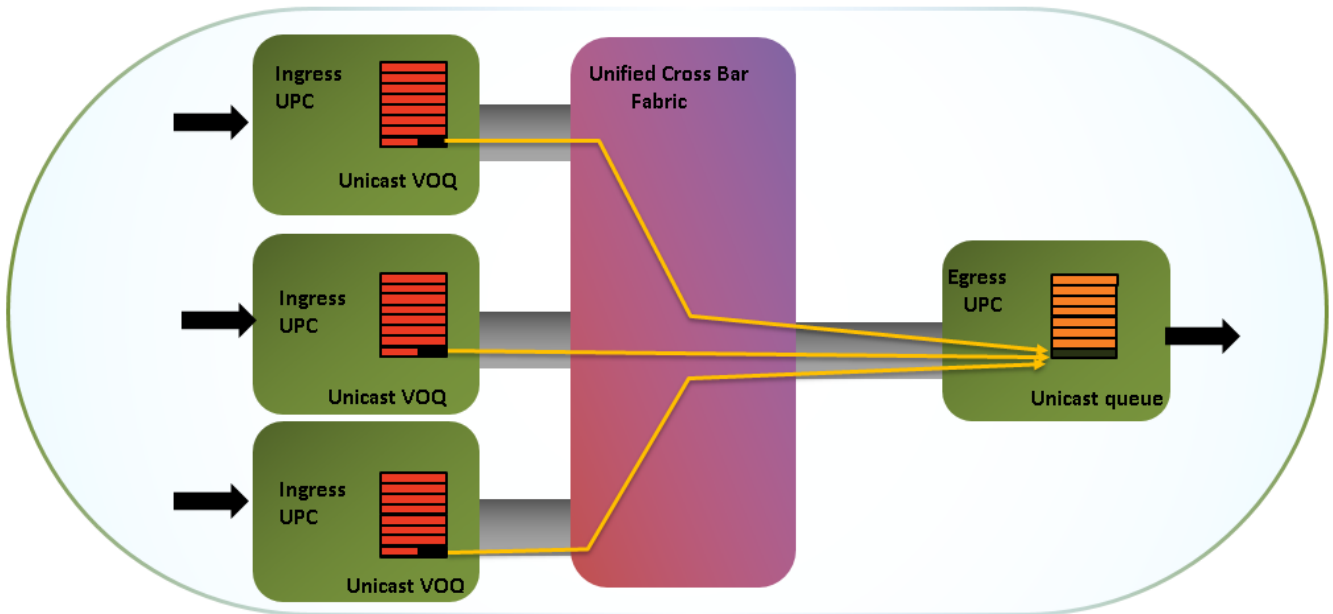
Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco Nexus 6001
- 7.1 (3) N1 (1)

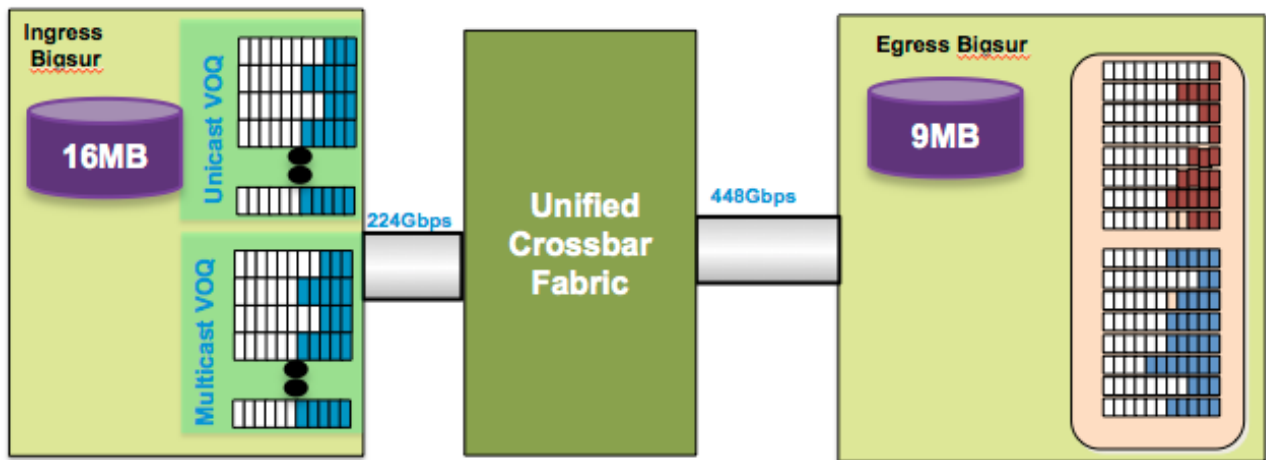
Поток Трафика с конкретным адресом и Буферизация

Трафик с конкретным адресом помещен в очередь в пуле выходного буфера сначала и

затем входной буфер после того, как выходная очередь будет полна.

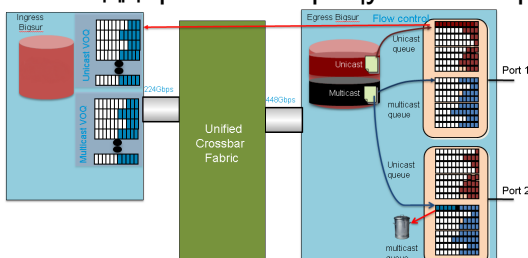


Там действительно ли 16 МБ являются входом? совместно используемый? буфер и выход 9 МБ? совместно используемый? буфер. Буферы разделены между 12 x10gig портами порты OR 3x40 Гб. Совместно используемый буфер хорош для пакетного поглощения. Вот визуальное описание распределения памяти для ссылки (Bigsur является названием Контроллера портов ASIC / Унифицированного Контроллера портов),



Поток Многоадресного трафика и Буферизация

- Пакеты групповой адресации буферизованы и отброшены в выходе
- Понижьте пакет групповой адресации близко к точке перегрузки избегают HOLB
- Поддержите матрицу без потерь для индивидуальной рассылки



В большинстве случаев выходные отбрасывания будут всегда происходить из-за трафика Групповой адресации/широковещательного сообщения/Одноадресного одноадресной.

Какие причины вводят сброс?

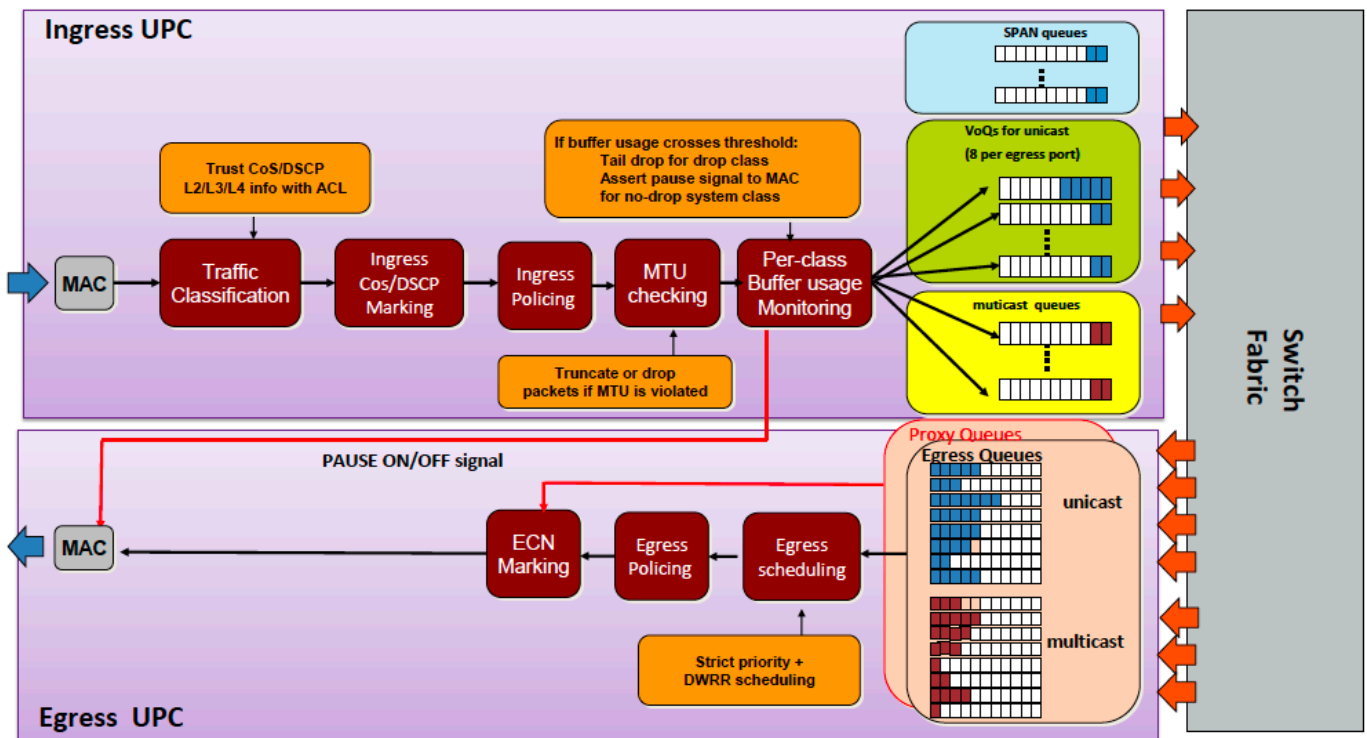
Переполненный выходной порт вызовет выходные буфера, заполнится сначала, и затем он это вызовет обратное давление на входе. Это только для трафика с конкретным адресом. Как только входные буфера полны тогда, мы могли потенциально отбросить трафик на входе, который приводит к входному сбросу.

Это пояснение в очень высоком уровне и легко к дайджесту, но существует немного больше к нему особенно, когда вы смотрите на другой класс трафика, очереди и т.д.

Существует понятие VOQ (Виртуальная очередь вывода), которая часто используется на платформе Nexus. VOQ является выделением входных буферов для каждого класса обслуживания (CoS) IEEE 802.1p на выходной порт. Таким образом, существует 8 VOQ на выходной порт.

Перегрузка на одном выходном порте в одном CoS eventually выйдет за край в переполнение соответствующего VOQ на входном порте. Как только предел достигнут тогда, трафик будет отброшен. Это, однако, не влияет на трафик, предназначенный для другого CoSs или других исходящих интерфейсов, таким образом избегая блокирования заголовка очереди (HOL), которое иначе заставило бы перегрузку распространяться.

Вот визуальное отображение трафика от входа до выходного порта и различных блоков в воспроизведении



Пример устранения проблем

Scenario 1: входной сброс

Лабораторная установка:



Трафик скорости линии egressing e1/3 и возможное превышение подписки

В моделируемой настройке как выше, вы знаете причину превышения подписки, но в производственной настройке, где профиль трафика является пульсирующим, это может быть стимулирующим для определения переполненных выходных портов хотя вышеупомянутые команды.

Перечисленные шаги помогут с определением переполненных выходных портов

Шаг 1: Определите порты с входным сбросом

Входной сброс, замеченный на e1/4 порта

Шаг 2: Идентификация ASIC

? Сопоставьте интерфейс с внутренним ASIC (UPC) форма номера ниже выходных данных.

? Узнайте входной ID ASIC из ID входного порта, на котором мы заметили отбрасывания

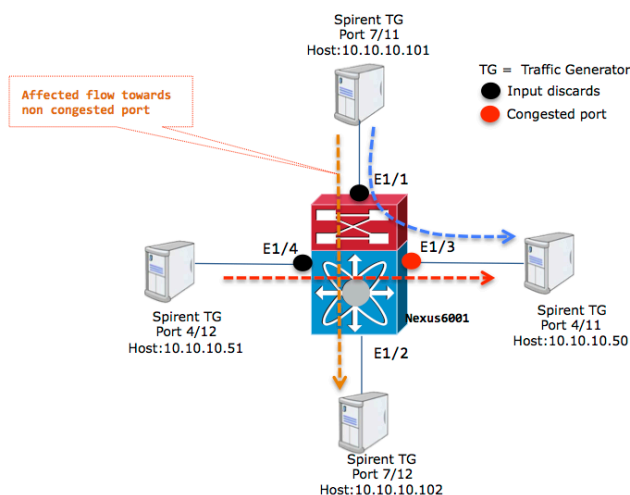
Шаг 3: Определите переполненный порт выхода

? Определение переполненного выходного порта со счетчиками VOQ

? Использовать номер ASIC в? противостоит voq цифре asic? узнать, какой выходной порт способствует отбрасываниям

Scenerio 2: входной сброс с HOLB (головка блокирования линии)

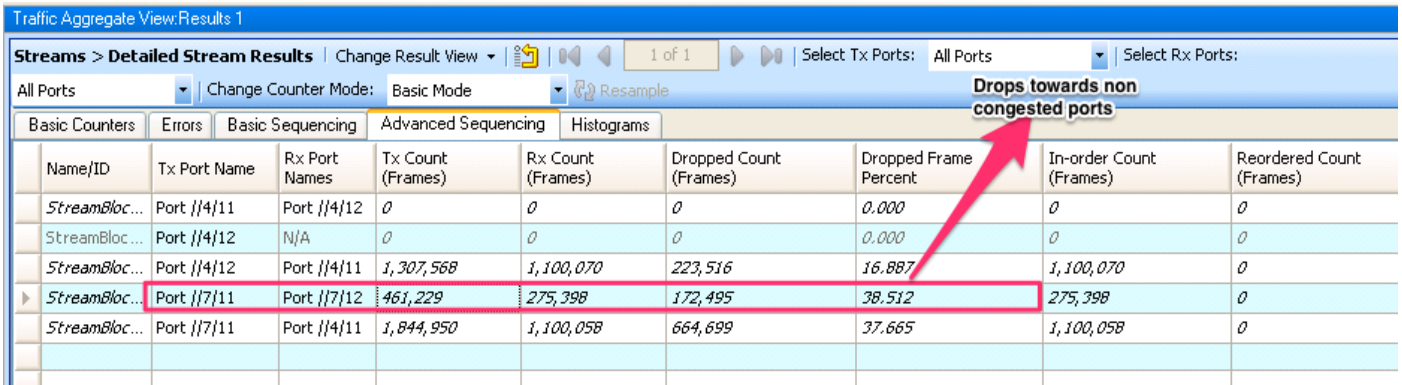
Лабораторная установка:



Основная задача в этом сценарии - определить, какой порт является переполненным или более входных портах, которые передают трафик

входных портах. Это - классическая проблема Головки блокирования линии (HOLB).

Снимок генераторов трафика Spirent показывает отбрасываемые потоки. Номера портов являются номерами портов Spirent.



Traffic Aggregate View: Results 1

Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

Drops towards non congested ports

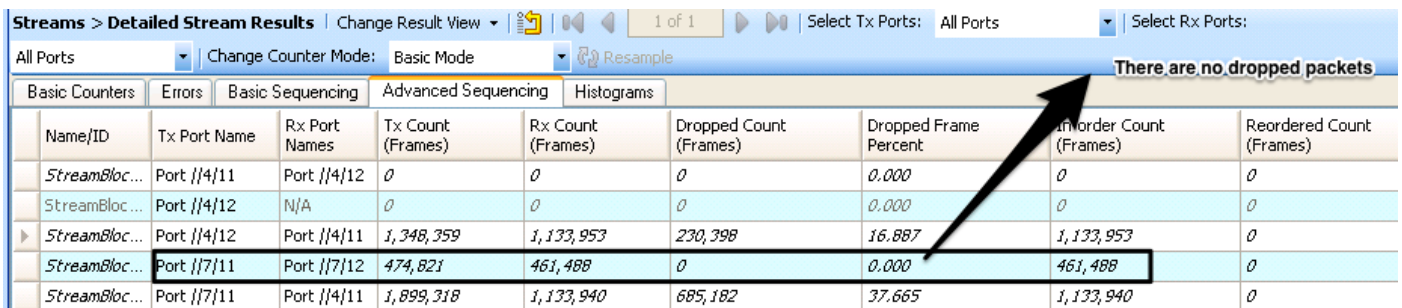
Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,307,568	1,100,070	223,516	16.887	1,100,070	0
StreamBloc...	Port //7/11	Port //7/12	461,229	275,398	172,495	38.512	275,398	0
StreamBloc...	Port //7/11	Port //4/11	1,844,950	1,100,058	664,699	37.665	1,100,058	0

Смягчение HOLB: Включите предел VOQ

Для предотвращения этого сценария VOQ (только для трафика с конкретным адресом) могут быть настроены с порогом набора.

После конфигурации не будут влиять на потоки к переполненным портам поп.

Представление Генератора трафика Spirent после предельного config VOQ



Streams > Detailed Stream Results | Change Result View | 1 of 1 | Select Tx Ports: All Ports | Select Rx Ports: All Ports

Change Counter Mode: Basic Mode | Resample

There are no dropped packets

Name/ID	Tx Port Name	Rx Port Names	Tx Count (Frames)	Rx Count (Frames)	Dropped Count (Frames)	Dropped Frame Percent	In-order Count (Frames)	Reordered Count (Frames)
StreamBloc...	Port //4/11	Port //4/12	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	N/A	0	0	0	0.000	0	0
StreamBloc...	Port //4/12	Port //4/11	1,348,359	1,133,953	230,398	16.887	1,133,953	0
StreamBloc...	Port //7/11	Port //7/12	474,821	461,488	0	0.000	461,488	0
StreamBloc...	Port //7/11	Port //4/11	1,899,318	1,133,940	685,182	37.665	1,133,940	0

Хотя эта конфигурация показывает ясное преимущество в предотвращении отбрасываний из-за HOLB, почему это не config по умолчанию?

Как правило, трафик в производственной среде мог быть пульсирующим по своей природе. Путем отключения порога VOQ мы позволяем входным буферам поглощать трафик микро пакет без того, чтобы быть отброшенным. Пока ситуация не гарантирует потребность включить предел VOQ, рекомендуется использовать по умолчанию, который должен оставить отключенным.

Смягчение HOLB: классификация трафика

Существует другой метод для смягчения HOLB с помощью конфигурации QoS. Начиная с входа discards только влияют на specific VOQ, который в свою очередь является specific классом QoS, можно сопоставить соответствующий трафик с переполненным портом поп другой группе QoS. От ниже выходных данных, входной сброс влияет на QoS Group 0 классов.

Конфигурация ниже сопоставит представляющий интерес трафик с Группой QoS 2.

1. Определите ACL для трафика, который не должен быть отброшен. Цель состоит в том, чтобы классифицировать этот трафик в другую группу QoS, таким образом, это не становится влияемым.

2. Классификация QoS

3. Сетевой config QoS

4. Примените различную политику. В то время как политика классификации может быть применена к одному интерфейсу, сеть QoS в масштабе всей системы.

5. Отбрасывания не замечены для группы QoS 2 класса

Связанные сведения

[Пример конфигурации QoS коммутаторов серии "Catalyst 6000" Nexus](#)