Применение политик QoS на коммутаторах Catalyst серии 6500/6000

Содержание

Введение

Применение политик QoS в сети определяет соответствие сетевого трафика заданному профилю (контракту). Функция применения политик может сбрасывать непрофильный трафик или понижать значение трафика, устанавливая для него другое значение кода дифференцированных услуг DSCP, для обеспечения уровня обслуживания, обусловленного контрактом. (DSCP — показатель уровня QoS для фрейма.).)

Следует различать применение политик к трафику и формирование трафика. В обоих случаях трафик остается в рамках параметров профиля (контракта). При применении политик к трафику, непрофильные пакеты не помещаются в буфер. Поэтому это не влияет на задержку передачи. Трафик либо сбрасывается, либо понижается до более низкого уровня QoS (снижение кода DSCP). Напротив, при формировании трафика происходит буферизация непрофильного трафика и сглаживание пульсаций объема трафика. Это влияет на задержку и колебания задержки. Формирование трафика применяется только к выходному интерфейсу. Применение политик возможно как к входному, так и к выходному интерфейсам.

Платы Catalyst 6500/6000 Policy Feature Card (PFC) и PFC2 поддерживают применения политик только для входящего трафика. PFC3 поддерживает применение политик как для входящего, так и для исходящего трафика. Формирование трафика поддерживается только на определенных модулях WAN для Catalyst серии 6500/7600, например на модулях оптических служб OSM и FlexWAN. См. Примечания Конфигурации модуля маршрутизатора Cisco серии 7600 для получения дополнительной информации

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Параметры QoS Профилирование (policing)

Чтобы настроить контроль, необходимо определить диспетчеры политик и применить их к портам (QoS на основе портов) или VLAN (QoS на основе VLAN). Каждый ограничитель определяет имя, тип, скорость, размер пакета и действия для профильного и внепрофильного трафика. Ограничители скорости на Supervisor Engine II также поддерживают параметры превышения скорости. Существуют два типа средств ограничения скорости: ограничитель микропотоков и общий ограничитель скорости.

- **Диспетчер политик для микропотоков — регулирует трафик для каждого порта и VLAN индивидуально, в зависимости от потока.**
- **Общий диспетчер политик — регулирует трафик для всех портов и VLAN.**

Каждый ограничитель можно использовать для нескольких портов или VLAN. Поток определяется следующими параметрами:

- iP-адрес ОТПРАВИТЕЛЯ
- iP-адрес ПОЛУЧАТЕЛЯ
- Протокол уровня 4 (такой как Протокол датаграммы пользователя [UDP])
- номер исходного порта
- номер порта назначения

Можно сказать, что пакеты, которые совпадают с определенным набором определенных параметров, принадлежат тому же потоку. (Эта концепция потока, по существу, аналогична концепции, используемой коммутацией NetFlow.).)

Например, если настраивается диспетчер политик для микропотока для ограничения TFTP трафика значением 1 Мбит/с в VLAN 1 и VLAN 3, тогда скорость 1 Мбит/с разрешена для каждого потока в VLAN 1 и 1 Мбит/с — для каждого потока в VLAN 3. Другими словами, если в VLAN 1 существуют три потока, а в VLAN 3 — четыре потока, то диспетчер политик микропотока разрешает каждому из этих потоков скорость 1 Мбит/с. При настройке общего диспетчера политик он ограничивает TFTP трафик для всех потоков в VLAN 1 и VLAN 3 значением 1 Мбит/с.

Если действуют и общий диспетчер политик, и диспетчер политик для микропотока, QoS

всегда применяет наиболее жесткое действие из установленных диспетчеров. Например, если один диспетчер указывает сбросить пакет, а другой — понизить значение DSCP пакета, то пакет сбрасывается.

По умолчанию диспетчеры политик для микропотоков действуют только для маршрутизируемого трафика (уровень 3 [L3]). Чтобы контролировать также и мостовой трафик (уровень 2 [L2]), необходимо включить применение политик для мостовых микропотоков. На Supervisor Engine II необходимо включить применение политик для мостовых микропотоков даже для контроля микропотоков L3.

Функция применения политик учитывает протокол. Весь трафик делится на три типа:

- IP
- Межсетевой пакетный обмен (IPX)
- Другой

Применение политик внедрено на Catalyst 6500/6000 согласно понятию "алгоритма дырявое ведро". Маркеры, соответствующие пакетам входящего трафика, помещаются в ведро. (Каждый маркер представляет один бит, поэтому большой пакет представлен большим числом маркеров, по сравнению с маленьким пакетом.). С постоянным интервалом определенное число маркеров удаляется из ведра и отправляется по маршруту. Если в ведре нет места для приема входящих пакетов, эти пакеты считаются непрофильными. Они или сбрасываются или получают более низкий приоритет, в зависимости от настроенного действия политики.

Примечание: Трафик не буферизован в блоке, как это может появиться в образе выше. Реальный трафик вообще не проходит через ведро; ведро используется только для определения соответствия или несоответствия пакета профилю.

Вычислите параметры

Несколько параметров управляют использованием алгоритма Token bucket, как показано здесь:

- **Скорость определяет количество маркеров, удаляемых с каждым интервалом.** Этот параметр фактически задает скорость упорядочения трафика. Весь трафик, укладывающийся в норму, считается профильным.
- **Интервал определяет частоту удаления маркеров из ведра.** Для интервала установлено фиксированное значение 0,00025 с, что соответствует удалению маркеров из выделенного сегмента памяти ("ведра") 4000 раз в секунду. Менять интервал нельзя.
- **Пакет** — определяет максимальное число маркеров, которые блок может держать в любой момент. Для поддержания заданной скорости трафика, блок должен быть не меньше количества маркеров, удаляемых за каждый интервал. Другое допущение состоит в том, что пакет максимального размера должен умещаться в ячейке.

Определить параметр блочной передачи кадров поможет следующее уравнение:

- *Блок = (Скорость [бит/с] * 0,00025 [сек/интервал]) или (максимальный размер пакета [бит]), выбрав большее из этих значений.*

Например, чтобы вычислить минимальный размер блока, необходимый для поддержания скорости 1 Мбит/с в сети Ethernet, эта скорость определяется как 1 Мбит/с, а максимальный размер пакета Ethernet считается равным 1518 байтам. Получаем выражение:

- *Блок = (1000000 бит/с * 0,00025) или (1518 байт * 8 бит/байт) = 250 или 12144.*

Большим значением является 12144, которое округляется до 13 Кбит/с.

Примечание: В программном обеспечении Cisco IOS ограничение скорости определено в битах в секунду (бит/с), в противоположность кбит/с в операционной системе Catalyst (CatOS). Кроме того, в ПО Cisco IOS размер блока определяется в байтах, а не в килобитах как в CatOS.

Примечание: Из-за глубины детализации политики аппаратного обеспечения, точного значения скорости передачи и пакета округлен к самому близкому поддерживаемому значению. Следует выбирать размер блока не меньше максимального размера пакета. В противном случае все пакеты, превышающие размеры пакетной передачи, отбрасываются.

Например, если попытаться установить размер блока равным 1518 в ПО Cisco IOS, это значение будет округлено до 1000. Это приведет к тому, что все кадры, размер которых превышает 1000 байт, будут сброшены. Решением будет установить размер блока равным 2000.

При настройке скорости блоков примите во внимание тот факт, что некоторые протоколы (например, TCP) используют механизм управления потоком, реагирующий на потери пакетов. Например, TCP уменьшает окно кадрирования в два раза при каждой потере пакета. В результате, фактическое использование канала ниже настроенной ограничительной скорости. Можно увеличить пакет, чтобы добиться лучшего использования. Для начала можно увеличить размер блока в два раза. (Для этого примера размер блока увеличивается с 13 Кбит/с до 26 Кбит/с.). Затем оцените производительность и сделайте дальнейшие настройки при необходимости.

По этой причине не рекомендуется использовать трафик на основе соединений для сравнительной оценки функционирования диспетчера политик. Как правило, в этом случае производительность ниже той, которую обеспечивает диспетчер политик.

Действия полиции по наведению порядка

Как упомянуто во Введении, ограничитель может сделать одну из двух вещей к внепрофильному пакету:

- отбросьте пакет (параметр `drop` в конфигурации)
- отметьте пакет к более низкому DSCP (параметр `policed-dscp` в конфигурации)

Для отмечания пакета необходимо модифицировать охраняемую Карту DSCP. Значение кода DSCP из схемы политик устанавливается по умолчанию для пометки пакета этим DSCP. (Понижение не происходит.).)

Примечание: Если "внепрофильные" пакеты отмечены к DSCP, который сопоставлен в другую очередь вывода, чем исходный DSCP, некоторые пакеты могут быть переданы не в порядке. По этой причине, если важен порядок отправки пакетов, рекомендуется понижать непрофильные пакеты до значения DSCP, сопоставленного с той очередью исходящих пакетов, в которой находятся профильные пакеты.

Для модуля Supervisor Engine II, поддерживающего превышение скорости, возможны два триггера:

- Когда трафик превышает обычную норму

- Объем трафика превышает максимальную скорость

Один пример приложения превышения скорости должен отметить пакеты, которые превышают обычную норму и пакеты отбрасывания, которые превышают превышение скорости.

Функции применения политик, поддерживаемые Catalyst 6500/6000

Как упоминалось в разделе Общие сведения, PFC1 на Supervisor Engine 1a и PFC2 на Supervisor Engine 2 поддерживают контроль только входящего трафика (входной интерфейс). PFC3 на Supervisor Engine 720 поддерживает применение политик как для входящего, так и для исходящего трафика (выходной интерфейс).

Catalyst 6500/6000 поддерживает до 63 ограничителей микропотока и до 1023 общих ограничителей.

Supervisor Engine 1a поддерживает применение политик к входящему трафику, начиная с ПО CatOS Release 5.3(1) и ПО Cisco IOS Release 12.0(7)XE.

Примечание: Дочерняя плата PFC или PFC2 требуется для применения политик с Supervisor Engine 1A.

Supervisor Engine 2 поддерживает применение политик к входящему трафику, начиная с ПО CatOS Release 6.1(1) и ПО Cisco IOS Release 12.1(5c)EX. Supervisor Engine II поддерживает параметр диспетчера политик превышения скорости.

Конфигурации с платами распределенной пересылки (DFC) поддерживают только схемы политик на основе портов. Кроме того, общий диспетчер политик подсчитывает трафик только на основе модулей пересылки, а не на основе систем. DFC и PFC являются модулями пересылки; если модуль (линейная плата) не имеет DFC, он использует PFC в качестве модуля пересылки.

Новые функции применения политик для Supervisor Engine 720

Примечание: Если вы незнакомы с политиками QoS Catalyst 6500/6000, несомненно, считают Параметры политик QoS и Характеристики назначения и контроля выполнения политик (правил), Поддерживаемые разделами Catalyst 6500/6000 этого документа.

Supervisor Engine 720 предоставляет новые функции применения политик QoS:

- **Применение политик к исходящему трафику.** Supervisor Engine 720 поддерживает применение политик для входящего трафика на порту или интерфейсе VLAN. Он поддерживает применение политик для исходящего трафика на порту или интерфейсе маршрутизации L3 (при использовании системного ПО Cisco IOS). Работа всех портов в VLAN осуществляется с применением политик для исходящего трафика независимо от режима QoS портов (QoS на основе портов или на основе VLAN). Применение политик для микропотоков не поддерживается для исходящего трафика. Примеры конфигураций приведены в разделах Настройка и мониторинг применения политик в ПО CatOS и

Настройка и мониторинг применения политик в ПО Cisco IOS данного документа.

- **Применение политик для микропотоков для каждого пользователя.** Supervisor 720 поддерживает новую функцию применения политик для микропотоков, называемую применение политик для микропотоков для каждого пользователя. Эта функция поддерживается только при использовании системного ПО Cisco IOS. Она позволяет предоставлять определенную полосу пропускания каждому пользователю (на каждый IP-адрес) после конкретных интерфейсов. Это достигается путем задания маски потока в политике обслуживания. Маска потока определяет информацию, используемую для отличия потоков. Например, если указать маску потока только источника, весь трафик с одного IP-адреса считается одним потоком. Используя этот способ, можно контролировать трафик для каждого пользователя на некоторых интерфейсах (где настроена соответствующая политика обслуживания), а на других интерфейсах продолжать использовать маску потока по умолчанию. Допускается одновременное использование не более двух различных масок потоков QoS в системе. С одной маской потока можно связать только один класс. В политике можно использовать не более двух различных масок.

Другим важным изменением в функции применения политик на Supervisor Engine 720 является ее способность подсчитывать трафик по длине L2 фрейма. Supervisor Engine 2 и Supervisor Engine 1 подсчитывают IP и IPX фреймы по их длине L3. В некоторых приложениях, длины L2 и L3 могут отличаться. Один из примеров – небольшой пакет L3 внутри большого кадра L2. В этом случае ограничиваемая диспетчером политик скорость трафика, отображаемая Supervisor Engine 720, может отличаться от значения скорости, полученного Supervisor Engine 1 и Supervisor Engine 2.

Настройка и мониторинг функции применения политик в ПО CatOS

Настройка функции применения политик в ПО CatOS состоит из трех основных этапов:

1. Определение диспетчеров политик — нормальная скорость трафика, максимальная скорость (если используется), блок и действие политики.
2. Создание QoS ACL для выбора контролируемого трафика и присоединение диспетчера политик к этому ACL.
3. Применение QoS ACL ко всем нужным портам или VLAN.

Этот пример демонстрирует, как на порту 2/8 ограничить весь трафик трафиком UDP-порта 111.

Для Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_port dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates QoS ACL to select traffic and
attaches !--- the policer to the QoS ACL. commit qos acl
all !--- This compiles the QoS ACL. set qos acl map
udp_qos_port 2/8 !--- This maps the QoS ACL to the
switch port.
```

Следующий пример аналогичен предыдущему. Однако в этом примере диспетчер политик присоединяется к VLAN. Порт 2/8 принадлежит VLAN 20.

Примечание: Необходимо изменить QoS порта на `vlan` режим. **Для этого используйте команду set port qos.**

Этот диспетчер политик оценивает трафик со всех портов в VLAN, настроенных для режима QoS на основе VLAN:

Для Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 drop !--- This defines a
policer. For the calculation of rate and burst, !---
refer to Calculate Parameters. set qos acl ip
udp_qos_vlan dscp 0 aggregate udp_1mbps udp any any eq
111 !--- This creates the QoS ACL to select traffic and
attaches !--- the policer to QoS ACL. commit qos acl all
!--- This compiles the QoS ACL. set port qos 2/8 vlan-
based !--- This configures the port for VLAN-based QoS.
set qos acl map udp_qos_vlan 20 !--- This maps QoS ACL
to VLAN 20.
```

Далее, вместо сбрасывания непрофильных пакетов с DSCP 32 понизим значение DSCP до 0 (наилучшее решение).

Для Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Этот пример демонстрирует настройку применения политик для исходящего трафика только на Supervisor Engine 720. Он иллюстрирует способ применения политик для всего исходящего IP-трафика на VLAN 3 общей скоростью 10 Мбит/с.

Для Catalyst 6500/6000

```
set qos enable
!--- This enables QoS. set qos policer aggregate
udp_1mbps rate 1000 burst 13 policed-dscp !--- This
defines a policer. For the calculation of rate and
burst, !--- refer to Calculate Parameters. set qos acl
ip udp_qos_md trust-ipprec aggregate udp_1mbps udp any
any eq 111 dscp-field 32 !--- Note: The above command
should be on one line. !--- This creates the QoS ACL to
```

```
select traffic and attaches !--- the policer to the QoS
ACL.

commit qos acl all
!--- This compiles the QoS ACL. set qos policed-dscp-map
32:0 !--- This modifies the policed DSCP map to mark
down DSCP 32 to DSCP 0. set port qos 2/8 vlan-based !---
This configures the port for VLAN-based QoS. set qos acl
map udp_qos_md 20 !--- This maps the QoS ACL to VLAN 20.
```

Используйте команду show qos maps runtime policed-dscp-map для просмотра текущей схемы политик DSCP.

Используйте команду show qos policer runtime {policer_name | all} для проверки параметров диспетчера политики. Также можно просмотреть QoS ACL, к которому присоединен диспетчер политик.

Примечание: С Supervisor Engine 1 и 1a, не возможно иметь статистику применения политик для отдельных общих ограничителей скорости. Чтобы просмотреть статистику о применении политик по системам, используйте эту команду:

```
Cat6k> (enable) show qos statistics l3stats
Packets dropped due to policing: 1222086
IP packets with ToS changed: 27424
IP packets with CoS changed: 3220
Non-IP packets with CoS changed: 0
```

Чтобы просмотреть статистику о диспетчере политик для микропотоков, используйте эту команду:

```
Cat6k> (enable) show mls entry qos short
Destination-IP  Source-IP Port  DstPrt SrcPrt Uptime  Age
--------------- --------------- ----- ------ ------ -------- --------

IP bridged entries:
239.77.77.77 192.168.10.200UDP   63 6300:22:02 00:00:00
Stat-Pkts : 165360
Stat-Bytes : 7606560
Excd-Pkts : 492240
Stat-Bkts : 1660
239.3.3.3192.168.11.200UDP  888 77700:05:38 00:00:00
Stat-Pkts : 42372
Stat-Bytes : 1949112
Excd-Pkts : 126128
Stat-Bkts : 1628

Only out of the profile MLS entries are displayed
Cat6k> (enable)
```

При использовании Supervisor Engine II можно просмотреть статистику о применении политик для отдельных общих диспетчеров политик, используя команду show qos statistics aggregate-policer.

В этом примере, генератор трафика прикреплен к порту 2/8. Он отправляет UDP трафик 17 Мбит/с в порт назначения 111. Ожидается, что диспетчер политик сбрасывает 16/17 трафика и пропускает только 1 Мбит/с:

```
Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
```

```
------------------------------ ------------- ------------- -------------
udp_1mbps58243997321089732108

Cat6k> (enable) show qos statistics aggregate-policer udp_1mbps
QoS aggregate-policer statistics:
Aggregate policerAllowed packet Packets exceed Packets exceed
                count        normal rate       excess rate
------------------------------ ------------- ------------- -------------
udp_1mbps58250497331989733198
```

Примечание: Заметьте, что позволенный пакеты увеличились на 65, и избыточные пакеты увеличились на 1090. Это означает, что ограничитель отбросил 1090 пакетов и позволил 65 проходить. Простое вычисление 65 / (1090 + 65) = 0,056 дает, приблизительно, 1/17. Следовательно, диспетчер политик работает правильно.

Настройка и мониторинг применения политик в ПО Cisco IOS

Настройка применения политик в ПО Cisco IOS состоит из следующих этапов:

1. Определение диспетчера политик.
2. Создание ACL для выбора контролируемого трафика.
3. Определение схемы класса для выбора трафика с ACL и/или DSCP/IP-приоритета.
4. Создание политики обслуживания, использующей класс, и применение диспетчера политик к заданному классу.
5. Применение политики обслуживания к порту или VLAN.

Рассмотрим пример, приведенный в разделе Настройка и мониторинг применения политик в ПО CatOS, но теперь с использованием ПО Cisco IOS. В этом примере, генератор трафика прикреплен к порту 2/8. Он отправляет UDP трафик 17 Мбит/с в порт назначения 111:

Для Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

В ПО Cisco IOS существуют два типа общих диспетчеров политик: **именованный и для каждого интерфейса.** Именованный общий диспетчер политик контролирует общий трафик со всех интерфейсов, к которым он применяется. Диспетчер этого типа использован в вышеприведенном примере. Диспетчер для каждого интерфейса контролирует трафик отдельно на каждом входном интерфейсе, к которому он применяется. Поведение интерфейсного диспетчера политик определяется в конфигурации карты политик. Рассмотрим следующий пример с общим диспетчером политик для ограничения скорости

по каждому интерфейсу:

Для Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Диспетчеры политик для микропотоков определяются в конфигурации схемы политик, как и общие диспетчеры политик для каждого интерфейса. В следующем примере каждый поток от узла 192.168.2.2, приходящий в VLAN 2, ограничен скоростью 100 Кбит/с. Весь трафик от 192.168.2.2 ограничен общей скоростью 500 Кбит/с. VLAN 2 включает интерфейсы fa4/11 и fa4/12:

Для Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Следующий пример демонстрирует настройку применения политик для исходящего трафика на Supervisor Engine 720. Устанавливает ограничение всего исходящего трафика на интерфейсе Gigabit Ethernet 8/6 значением 100 Кбит/с:

Для Catalyst 6500/6000

```
mls qos
!--- This enables QoS. mls qos aggregate-policer
udp_1mbps 1000000 2000 conform-action transmit exceed-
action drop !--- Note: The above command should be on
one line. !--- This defines a policer. For the
calculation of rate and burst, !--- refer to Calculate
```

```
Parameters. !--- Note: The burst is 2000 instead of
1518, due to hardware granularity.

access-list 111 permit udp any any eq 111
!--- This defines the ACL to select traffic. class-map
match-all udp_qos match access-group 111 !--- This
defines the traffic class to police. policy-map
udp_policy class udp_qos police aggregate udp_1mbps !---
This defines the QoS policy that attaches the policer to
the traffic class. interface GigabitEthernet2/8
switchport service-policy input udp_policy !--- This
applies the QoS policy to an interface.
```

Следующий пример демонстрирует настройку функции применения политик для каждого пользователя на Supervisor Engine 720. Устанавливается ограничение трафика, передаваемого от каждого пользователя после порта 1/1 в Интернет, значением 1 Мбит/с. Трафик, передаваемый из Интернета пользователям, ограничен значением 5 Мбит/с для каждого пользователя:

Для Catalyst 6500/6000

```
mls qos
!--- This enables QoS. access-list 111 permit ip any any
!--- This defines the ACL to select user traffic. class-
map match-all cl_out match access-group 111 !--- This
defines the traffic class for policing. policy-map
pol_out class cl_out police flow mask src-only 1000000
32000 conform-act transmit exceed-act drop
!--- Only the source IP address is considered for flow
creation !--- on interfaces with this policy attached.
interface gigabit 1/1 !--- 1/1 is the uplink toward the
users. service-policy input pol_out !--- Traffic comes
in from users, so the policy is attached !--- in the
input direction. class-map match-all cl_in match access-
group 111 policy-map pol_in class cl_in police flow mask
dest-only 5000000 32000 conform-act transmit exceed-act
drop
!--- Only the destination IP address is considered for
flow creation !--- on interfaces with this policy
attached. interface gigabit 1/2 !--- 1/2 is the uplink
to the Internet. service-policy input pol_in
```

Для мониторинга применения политик можно использовать следующие команды:

```
bratan# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS global counters:
Total packets: 10779
IP shortcut packets: 0
Packets dropped by policing: 2110223
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0

bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127451  2129602
```

```
bratan# show mls qos ip gigabitethernet 2/8
[In] Policy map is udp_policy [Out] Default.
QoS Summary [IP]: (* - shared aggregates, Mod - switch module)

Int   Mod Dir Class-map DSCP AgId Trust FlId AgForward-Pk AgPoliced-Pk
--------------------------------------------------------------------------------
Gi2/8 1   In  udp_qos   0    1*   No0 127755  2134670
```

Примечание: Позволенные пакеты увеличились на 304, и избыточные пакеты увеличились на 5068. Это означает, что ограничитель отбросил 5068 пакетов и позволил 304 проходить. При скорости входящего трафика 17 Мбит/с диспетчер политик должен пропускать 1/17 долю трафика. Если сравнить число сброшенных и пересланных пакетов, можно в этом убедиться: 304 / (304 + 5068) = 0,057 или, приблизительно, 1/17. Возможно некоторое незначительное отклонение из-за дискретности настроек ограничений для аппаратного обеспечения.

Чтобы просмотреть статистику диспетчера политик для микропотоков, используйте команду show mls ip detail:

```
Orion# show mls ip detail
IP Destination IP Source        Protocol L4 Ports     Vlan Xtag L3-protocol
--------------+---------------+--------+-------------+----+----+-----------+
192.168.3.33192.168.2.2udp555 / 5550   1ip
192.168.3.3192.168.2.2udp63 / 630   1ip

[IN/OUT] Ports Encapsulation RW-Vlan RW-MACSourceRW-MACDestinationBytes
--------------+-------------+-------+--------------+-----------------+------------+
Fa4/11 - ----ARPA3    0030.7137.1000  0000.3333.3333314548
Fa4/11 - ----ARPA3    0030.7137.1000  0000.2222.2222314824

Packets     Age   Last SeenQoS      Police Count ThresholdLeak
------------+-----+---------+-----------+------------+---------+-----------+
6838     36   18:50:090x80  34619762*2^5 3*2^0
6844     36   18:50:090x80  34669562*2^5 3*2^0

Drop Bucket  Use-Tbl Use-Enable
----+-------+-------+----------+
YES   1968     NONO
YES   1937     NONO
```

Примечание: показывает количество охраняемых пакетов на поток.

Дополнительные сведения

- Настройке функции QoS
- Общие сведение о качестве обслуживания (QoS) для коммутаторов серии Catalyst 6000
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация