Классификация QoS и маркирование в коммутаторах Catalyst серии 6500/6000, использующих программное обеспечение Cisco IOS

Содержание

Введение

В этом документе описано, что происходит при маркировании и классификации пакета на

различных стадиях в шасси Cisco Catalyst 6500/6000, использующем ПО Cisco IOS®. В этом документе описаны различные случаи и ограничения, а также короткие примеры.

В документе не представлен исчерпывающий список всех команд программного обеспечения Cisco IOS, связанных с качеством обслуживания или маркированием. Дополнительную информацию об интерфейсе командной строки (CLI) программного обеспечения Cisco IOS см. в документе Конфигурация качества обслуживания PFC.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям оборудования:

- Коммутаторы Catalyst серии 6500/6000 с программным обеспечением Cisco IOS и использующие один из следующих модулей управления Supervisor Engine:Модуль управления Supervisor Engine 1A с платой политик ограничений (PFC; Policy Feature Card) и платой функции многоуровневой коммутации (MSFC; Multilayer Switch Feature Card)Модуль управления Supervisor Engine 1A с PFC и MSFC2Модуль управления Supervisor Engine 2 с PFC2 и MSFC2

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Терминология

Список использованной в документе терминологии:

- Поле кода дифференцирования обслуживания (DSCP) - первые шесть битов из байта вида услуг (ToS) в IP-заголовке. Код DSCP содержится только в IP-пакете.**Примечание:** Коммутатор также назначает внутренний DSCP на каждый пакет, или IP или не-IP. Раздел 4 возможных источника внутреннего поля DSCP данного документа подробно описывает назначение внутреннего поля DSCP.
- IP-приоритетность - первые три бита из байта ToS в IP-заголовке.
- Класс услуг (CoS) - единственное поле, которое может быть использовано для маркирования пакета на уровне 2 (L2). Класс услуг (CoS) состоит из любых из этих трех битов:Три бита IEEE 802.1p (dot1p) в теге IEEE 802.1Q (dot1q) для пакета

dot1q.**Примечание:** По умолчанию коммутаторы Cisco не помечают пакеты собственного VLAN.Три бита, именуемые "User Field" (полем пользователя) в заголовке межкоммутаторного канала (ISL) для пакета, инкапсулированного в ISL.**Примечание:** CoS не присутствует в не-dot1q или пакете ISL.
- Классификация - процесс, используемый для выделения трафика, который должен быть маркирован.
- Маркировка - процесс, устанавливающий в пакете значение DSCP уровня 3 (L3). Этот документ расширяет определение маркировки для того, чтобы включить установку значений CoS уровня L2.

Коммутаторы Catalyst серии 6500/6000 могут выполнять классификацию на основании следующих трех параметров:

- DSCP
- Приоритет IP
- CoS

Коммутаторы Catalyst серий 6500/6000 выполняют классификацию и маркировку на различных стадиях. Вот что происходит в различных местах:

- Входной порт (входная специализированная интегральная схема [ASIC])
- Коммутаторный модуль (PFC)
- Порт вывода (исходящий трафик ASIC)

Обработка входного порта

, , trust. trust:

- trust ip precedence (IP-)
- trust dscp
- trust cos
- untrusted

trust, Cisco IOS interface ():

```
6k(config-if)#mls qos trust ?
  cos            cos keyword
  dscp           dscp keyword
  ip-precedence  ip-precedence keyword
  <cr>
```

Примечание: QoS. **Для включения QoS на Catalyst 6500 с программным обеспечением Cisco IOS, введите команду mls qos в режиме основной конфигурации.**

На уровне входящего порта можно также установить на каждый порт CoS по умолчанию. Например:

```
6k(config-if)#mls qos cos cos-value
```

Этот CoS по умолчанию применяется ко всем пакетам, таким как IP и межсетевой пакетный обмен (IPX; Internetwork Packet Exchange). Можно также применить CoS по умолчанию к любому физическому порту.

untrusted, CoS (PFC). trust, :

- Если кадр не имеет полученного CoS (dot1q или ISL), примените CoS по умолчанию для

порта.
- Для кадров dot1q and ISL не изменяйте CoS.

Затем передайте кадр на модуль коммутатора.

В данном примере представлена входящая классификация и маркировка. В примере показан способ назначения внутреннего CoS для каждого кадра:

Примечание: Как показано в примере каждому кадру назначают внутренний CoS. Назначение основано на полученном CoS или на CoS порта, который установлен по умолчанию. Внутренний CoS включает кадры без тега, которые не имеют никаких реальных CoS. Внутренний CoS записывается в специальный заголовок пакета, который называется заголовок шины данных, и передается в коммутаторный модуль через эту шину данных.

Коммутаторный модуль (PFC)

Когда заголовок достигает коммутирующее устройство, то Enhanced Address Recognition Logic (EARL) коммутирующего устройства назначает каждому фрэйму внутренний DSCP. Этот внутренний DSCP является внутренним приоритетом, который задается PFC фрейму PFC по мере того, как фрейм транзитирует коммутатор. Это не поле DSCP в IP-заголовке версии 4 (IPv4). Внутреннее поле DSCP является результатом установленных настроек CoS или ToS и необходимо для восстановления CoS или ToS, когда кадр выходит из коммутатора. Это внутреннее поле DSCP назначается для всех кадров (даже не IP-кадров), коммутируемых или маршрутируемых PFC.

В разделе описано назначение интерфейсу политики обслуживания для выполнения маркировки. `DSCP,` `trust` .

Настройка политики обслуживания для классификации или маркировки пакета в ПО Cisco IOS версии 12.1(12c)E и более поздних

Выполните следующие действия, чтобы настроить политику обслуживания:

1. Настройте список управления доступом (ACL) для определения трафика, который необходимо рассмотреть.Список управления доступом (ACL) может быть пронумерован или иметь имя, а Catalyst 6500/6000 поддерживает расширенный список ACL. *Введите команду программного обеспечения Cisco IOS access-list xxx, как показано на рисунке:*`(config)#`**`access-list 101 permit ip any host 10.1.1.1`**
2. Сконфигурируйте класс трафика (class map) для того чтобы сравнивать трафик на основании ACP, который вы определили, или на основании полученного DSCP.**Введите команду программного обеспечения Cisco IOS class-map.** QoS PFC не поддерживает более одного выражения совпадения в каждой карте класса. Кроме этого, QoS PFC поддерживает только эти операторы совпадения:**match ip access-groupmatch ip dscpmatch ip precedencematch protocolПримечание: Команда match protocol** позволяет использованию Сетевого распознавания приложений (NBAR) совпасть с трафиком.**Примечание: Из этих вариантов, только match ip dscp и match ip precedence утверждения поддерживаются и работают.** Тем не менее эти операторы не помогают выполнить маркирование или классификацию пакетов. Эти операторы можно использовать, например, для ограничения всех пакетов с определенным полем DSCP. Однако, эта процедура не рассматривается в этом документе.`(config)#`**`class-map`** *`class-`*

name

(config-cmap)#**match {access-group | input-interface | ip dscp}** **Примечание:** Данный пример показывает только три варианта для команды **соответствия**. Но, используя ввод этой команды, можно настроить множество других вариантов.**Примечание:** Любой из вариантов в этой команде **соответствия** выбран для условий соответствия, и другие опции не учтены, согласно входящим пакетам.Например:

```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```

3. Настройте карту ограничения для того, чтобы соотнести стратегию с предварительно определенным вами классом.Карта ограничения содержит:ИмяНабор операторов классаДля каждого оператора класса – действие, применяемое к этом классуПоддерживаемые действия для QoS в PFC1 и PFC2:**trust dscptrust ip precedence (приоритет доверенных IP-адресов)trust cosset ip dscp в программном обеспечении Cisco IOS версии 12.1(12c)E1 и более позднихset ip precedence в программном обеспечении Cisco IOS версии 12.1(12c)E1 и более позднихполитикаПримечание:** Это действие выходит за рамки этого документа.(config)#**policy-map** *policy-name*
(config-pmap)#**class** *class-name*
(config-pmap-c)#**{police | set ip dscp}**
Примечание: Данный пример показывает только два варианта, но можно настроить еще много опций в этом (config-pmap-c) # командная строка.Например:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   set ip dscp 16
```

4. Настройте входные данные политики обслуживания для того, чтобы соотнести предварительно определенную карту ограничения с одним или более интерфейсами.**Примечание:** Можно подключить политику обслуживания или к физическому интерфейсу или к коммутируемому виртуальному интерфейсу (SVI) или интерфейсу виртуальной локальной сети (VLAN). При связывании стратегии обслуживания с VLAN-интерфейсом единственными портами, использующими эту стратегию, являются те, которые принадлежат интерфейсу VLAN и настроены на качество обслуживания (QoS), основанное на VLAN. Если порт не настроен на QoS, основанное на VLAN, порт использует QoS по умолчанию, и смотрит на стратегию обслуживания, которая связана с физическим интерфейсом. test_policy Gigabit Ethernet 1/1:(config) **interface gigabitethernet 1/1**
(config-if)#**service-policy input test_policy**
test_policy VLAN 10, VLAN (QoS):(config) **interface gigabitethernet 1/2**
(config-if)#**switchport mode access**
(config-if)#**switchport access vlan 10**
(config-if)#**mls qos vlan-based**
(config-if)#**exit**
(config-if)#**interface vlan 10**
(config-if)#**service-policy input test_policy**
Примечание: Вы можете совместить раздел 2 и раздел 3 этой процедуры в том случае, если вы пропускаете специфическое определение класса и прилагаете ACL непосредственно к определению карты политик. , TEST police ,
:(config)#**policy-map** *policy-name*
(config-pmap)#**class** *class_name* **{access-group acl_index_or_name | dscp dscp_1 [dscp_2 [dscp_N]] | precedence ipp_1 [ipp_2 [ipp_N]]}**
!--- **Note:** This command should be on one line.

```
policy-map TEST
class TEST police access-group 101
```

Настройка стратегии обслуживания для классификации или маркировки пакета в ПО Cisco IOS версии более ранней, чем 12.1(12c)E

В более ранних версиях программного обеспечения Cisco IOS (более ранних, чем 12.1(12c)E1), нельзя использовать процедуры set ip dscp или set ip precedence в карте ограничения. Таким образом, единственный способ выполнить маркировку определенного трафика, определяемого классом – это настроить ограничитель на очень высокую скорость. Эта скорость, например, должна представлять собой линейную скорость порта или быть достаточно высокой для разрешения трафику достичь ограничителя. *Затем необходимо использовать set-dscp-transmit xx в качестве согласованной процедуры.* Для настройки этой конфигурации выполните следующие действия:

1. Настройте список управления доступом (ACL) для определения трафика, который необходимо рассмотреть.Список управления доступом (ACL) может быть пронумерован или иметь имя, а Catalyst 6500/6000 поддерживает расширенный список ACL. *Введите команду программного обеспечения Cisco IOS access-list xxx, как показано на рисунке:*`(config)#access-list 101 permit ip any host 10.1.1.1`
2. Установите класс трафика (карта класса) для нахождения трафика в соответствии с определенным списком ACL или полученным полем DSCP.**Введите команду программного обеспечения Cisco IOS class-map.** QoS PFC не поддерживает более одного выражения совпадения в каждой карте класса. Кроме этого, QoS PFC поддерживает только эти операторы совпадения:**match ip access-groupmatch ip dscpmatch ip precedencematch protocolПримечание: Команда match protocol** позволяет использованию NBAR совпасть с трафиком.**Примечание:** Из этих операторов только **операторы match ip dscp и match ip precedence** поддерживаются и работают. Тем не менее эти операторы не помогают выполнить маркирование или классификацию пакетов. Эти операторы можно использовать, например, для ограничения всех пакетов с определенным полем DSCP. Однако, эта процедура не рассматривается в этом документе.`(config)#class-map` *`class-name`*
`(config-cmap)#match {access-group | input-interface | ip dscp}`
Примечание: Данный пример показывает только три варианта для команды **соответствия**. Но, используя ввод этой команды, можно настроить множество других вариантов.Например:
```
class-map match-any TEST
 match access-group 101

class-map match-all TEST2
 match ip precedence 6
```
3. Настройте карту ограничения для того, чтобы соотнести стратегию с предварительно определенным вами классом.Карта ограничения содержит:ИмяНабор операторов классаДля каждого оператора класса – действие, применяемое к этом классуПоддерживаемые действия для QoS в PFC1 или PFC2:**trust dscptrust ip precedence (приоритет доверенных IP-адресов)trust cosполитикаНеобходимо использовать оператор police, так как процедуры set ip dscp и set ip precedence не поддерживаются.** Для того, чтобы не управлять трафиком, а только его пометить, используйте ограничитель, определенный для разрешения трафика. То есть, настройте ограничитель для большой скорости и пиков нагрузки. Например, можно

настроить ограничитель с максимально допустимой скоростью и пиками нагрузки. Например:

```
policy-map test_policy
 class TEST
   trust ip precedence
 class TEST2
   police  4000000000 31250000 conform-action
   set-dscp-transmit 16 exceed-action policed-dscp-transmit
```

4. Настройте входные данные стратегии обслуживания для того, чтобы соотнести предварительно определенную карту ограничения с одним или более интерфейсами.**Примечание:** Политика службы может быть приложена как к физическому интерфейсу, так и к интерфейсам SVI или VLAN. При связывании стратегии обслуживания с VLAN-интерфейсом единственными портами, использующими эту стратегию, являются те, которые принадлежат интерфейсу VLAN и настроены на качество обслуживания (QoS), основанное на VLAN. Если порт не настроен на QoS, основанное на VLAN, порт использует QoS по умолчанию, и смотрит на стратегию обслуживания, которая связана с физическим интерфейсом.

```
test_policy    Gigabit Ethernet 1/1:(config) interface gigabitethernet 1/1
(config-if)#service-policy input test_policy
     test_policy       VLAN 10,     VLAN       (QoS):(config) interface gigabitethernet 1/2
(config-if)#switchport mode access
(config-if)#switchport access vlan 10
(config-if)#mls qos vlan-based
(config-if)#exit
(config-if)#interface vlan 10
(config-if)#service-policy input test_policy
```

Четыре возможных источника внутренних значений DSCP

Внутреннее поле DSCP может быть определено следующими факторами:

1. Наличием полученного значения поля DSCP, установленного до того, как кадр вошел в коммутатор**В качестве примера – trust dscp.**
2. Полученными битами IP-приоритетности, уже установленными в заголовке IPv4Поскольку имеется только 64 значения DSCP и только 8 значений IP-приоритетности, администратор настраивает соответствие, которое коммутатор использует для определения поля DSCP. Кроме этого, соответствие настроено по умолчанию, на случай, если администратор не установит соответствие. **В качестве примера – trust ip precedence.**
3. Полученные биты CoS, уже установленные до входа кадра в коммутатор и хранящиеся в заголовке шины данных, или при отсутствии CoS во входящем кадре, из стандартного CoS входящего портаКак и с приоритетом IP-адреса, максимальное число значений CoS равно восьми, каждое из них должно соответствовать одному из 64 значений DSCP. Администратор может настроить эту карту, или коммутатор может использовать карту, уже установленную по умолчанию.
4. Стратегия обслуживания может задать внутреннему полю DSCP определенное значение.

Для номеров 2 и 3 в этом списке статическое маркирование установлено по умолчанию следующим образом:

- Для установления соответствия CoS - DSCP, поле DSCP считается равным CoS, умноженному на восемь.

- Для установления соответствия IP precedence - DSCP, поле DSCP считается равным IP precedence, умноженному на восемь.

Для замены или проверки статического соответствия можно ввести следующие команды:

- *mls qos map ip-prec-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*
- *mls qos map cos-dscp dscp_1 dscp_2 dscp_3 dscp_4 dscp_5 dscp_6 dscp_7 dscp_8*

Первое значение DSCP, соответствующее согласованию с CoS (или IP-приоритетностью), равно 0. Второе значение для CoS (или IP-приоритетности) равно 1 и так далее. Например, эта команда меняет преобразование таким образом, что значение CoS, равное 0, соответствует нулевому значению DSCP, а значение CoS, равное 1 – соответствует значению DSCP, равному 8, и т. д:

```
Cat65(config)#mls qos map cos-dscp 0 8 16 26 32 46 48 54
Cat65#show mls qos maps
CoS-dscp map:
 cos:     0 1  2   3   4   5   6   7
  ---------------------------------
 dscp:    0 8 16  26  32  46  48  54
```

Каким образом выбиралась внутренняя DSCP?

В основе выбора внутреннего поля DSCP лежат следующие параметры:

- Карта ограничения QoS применяется к пакетуКарта ограничения QoS определяют следующие правила:Если ни одна стратегия обслуживания не связана с входящим портом или VLAN, следует использовать настройки по умолчанию.**Примечание:** Это действие по умолчанию должно установить внутренний DSCP в 0.Если стратегия обслуживания связана с входящим портом или VLAN, или если трафик соответствует одному из классов, определяемых стратегией, следует использовать эту запись.Если стратегия обслуживания связана с входящим портом или VLAN, или если трафик не соответствует никакому из классов, определяемых стратегией, следует использовать установки по умолчанию.
- `trust ( "trusting"), :`**Команда set ip dscp или поле DSCP, определяемое для каждого ограничителя в карте ограничения, применяются только в том случае, если порт остался в состоянии untrusted.** `trust, trust DSCP. trust, set ip dscp.`*Команда trust xx в карте ограничения имеет преимущество над состоянием trust порта.* `trust, trust, .`

Следовательно, внутренний DSCP зависит от следующих факторов:

- `trust`
- Политики обслуживания (с использованием списка управления доступом (ACL)), связанной с портом
- Карты ограничения по умолчанию**Примечание:** По умолчанию перезагружает DSCP к 0.
- Основанный на VLAN или на порту по отношению к списку управления доступом

На схеме изображено изменение внутреннего поля DSCP на основании данных конфигураций:

PFC также может осуществлять контроль. В конечном итоге это может сказаться на понижении значения внутреннего поля DSCP. Более подробную информацию об ограничении см. в документе Ограничение QoS в коммутаторах Catalyst серий 6500/6000.

Обработка выходного порта

Изменение классификации на уровне исходящего порта невозможно. Тем не менее, можно маркировать пакет, учитывая следующие правила:

- Если имеется пакет IPv4, скопируйте внутреннее поле DSCP, которое коммутаторный модуль назначил на байт ToS заголовка IPv4.
- Если исходящий порт настроен на ISL или инкапсуляцию dot1q, используйте CoS, полученный из внутреннего поля DSCP. Скопируйте CoS в ISL или в кадр dot1q.

Примечание: CoS получен из внутреннего DSCP согласно помехам. Выполните следующую команду для настройки статики:

```
Router(config)#mls qos map dscp-cos dscp1 [dscp2 [dscp3 [dscp4 [dscp5 [dscp6 [dscp7
[dscp8]]]]]]] to cos_value
!--- Note: This command should be on one line.
```

Стандартные конфигурации появляются. По умолчанию CoS является целой частью поля DSCP, деленного на восемь. Выполните следующую команду для просмотра и проверки согласования:

```
cat6k#show mls qos maps
...
  Dscp-cos map:                                     (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 00 00 00 00 00 00 00 01 01
      1 :    01 01 01 01 01 01 02 02 02 02
      2 :    02 02 02 02 03 03 03 03 03 03
      3 :    03 03 04 04 04 04 04 04 04 04
      4 :    05 05 05 05 05 05 05 05 06 06
      5 :    06 06 06 06 06 06 07 07 07 07
      6 :    07 07 07 07
```

Чтобы изменить данное согласование, введите следующую команду конфигурации в нормальном режиме конфигурации:

```
mls qos map dscp-cos 0 1 2 3 4 5 6 7 to 0
mls qos map dscp-cos 8 9 10 11 12 13 14 15 to 1
mls qos map dscp-cos 16 17 18 19 20 21 22 23 to 2
...
```

После того, как поле DSCP записано в IP-заголовок, а CoS получен из поля DSCP, пакет отправляется в одну из очередей вывода для планирования вывода на основе CoS. Это происходит даже если пакет не является dot1q или ISL. Дополнительную информацию о построении очереди вывода см. в документе Планирование вывода на основе QoS для коммутаторов Catalyst серии 6500/6000 с программным обеспечением системы Cisco IOS.

На схеме изображен процесс обработки пакета относительно маркировки в исходящем порту:

Примечания и ограничения

Стандартный список управления доступом (ACL)

Используемый по умолчанию ACL использует "dscp 0" в качестве ключевого слова классификации. Весь трафик, входящий в коммутатор через порт без доверия и не соответствующий записи в политике обслуживания, маркируются нулевым значением поля DSCP в случае, если QoS включено. В настоящее время нельзя изменить стандартный ACL в программном обеспечении Cisco IOS.

Примечание: В программном обеспечении операционной системы Catalyst (CatOS) можно настроить и изменить это поведение по умолчанию. *Дополнительную информацию см. в разделе Стандартный ACL документа Классификация и маркировка QoS в коммутаторах Catalyst серии 6500/6000 с программным обеспечением CatOS.*

Ограничения линейных плат WS-X61xx, WS-X6248-xx, WS-X6224-xx и WS-X6348-xx

В данном разделе рассматриваются только следующие линейные карты:

- WS-X6224-100FX-MT: Catalyst 6000 24-Port 100 FX Multimode
- WS-X6248-RJ-45: Модуль Catalyst 6000 48-Port 10/100 RJ-45
- WS-X6248-TEL : CATALYST 6000 48-PORT 10/100 TELCO MODULE
- WS-X6248A-RJ-45 : CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6248A-TEL: CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6324-100FX-MM: Catalyst 6000 24-Port 100 FX, Enhanced QoS (улучшенное качество обслуживания), MT
- WS-X6324-100FX-SM: Catalyst 6000 24-Port 100 FX, Enhanced QoS (улучшенное качество обслуживания), MT
- WS-X6348-RJ-45 : CATALYST 6000 48-PORT 10/100, ENHANCED QOS
- WS-X6348-RJ21V: Catalyst 6000 48-Port 10/100, Inline Power (питание по линии)
- WS-X6348-RJ21V: Catalyst 6000 48-Port 10/100, повышенное качество обслуживания, питание по линии
- WS-X6148-RJ21V: Catalyst 6500 48-Port 10/100, Inline Power (питание по линии)
- WS-X6148-RJ45V: Catalyst 6500 48-Port 10/100, Inline Power (питание по линии)

У этих линейных карт имеется ограничение. `trust,` :

- `trust dscp`
- `trust-ipprec`
- `trust cos`

`untrusted.` `trust` :

```
Tank(config-if)#mls qos trust ?
  extend  extend keyword
Tank(config-if)#mls qos trust
% Incomplete command.
Tank(config-if)#mls qos trust cos
                              ^
% Invalid input detected at '^' marker.
Tank(config-if)#mls qos trust ip-pre
                              ^
% Invalid input detected at '^' marker.
```

Чтобы на такую линейную плату поступил кадр с доверием, необходимо связать политику обслуживания с портом или VLAN. Используйте способ в разделе Случай 1: Маркировка на границе данного документа.

Пакеты, поступающие из MSFC1 или MSFC2 на модуль управления Supervisor Engine 1A/PFC

Все пакеты, поступающие из MSFC1 или MSFC2, имеют нулевое значение CoS. Этот пакет может как маршрутироваться программным обеспечением, так и быть сгенерированным MSFC. Это является ограничением PFC, так как это приводит к сбросу CoS всех пакетов, поступающих с MSFC. DSCP и IP-приоритетность все еще поддерживаются. PFC2 не имеет такого ограничения. Исходящий класс обслуживания (CoS) PFC2 идентичен IP-приоритетности пакета.

Краткое описание классификации

В таблицах данного раздела показаны DSCP, которые являются результатом данных классификаций:

-
- Ключевое слово классификации в пределах применяемого ACL (списка управления доступом)

В данной таблице представлены общие итоги для всех портов, кроме WS-X62xx и WS-X63xx:

Ключевое слово согласования для политики **Состояние доверительности порта**	**set-ip-dscp xx или set-dscp-transmit xx**	**trust dscp**	**Trust-ipprec**	**trust cos**
недоверяемый	xx (1)	Принятый 2 DSCP	Получено из принятого ipprec	0
trust dscp	Rx dscp	Rx dscp	Получено из принятого ipprec	Получено из Rx CoS или порта CoS
Trust-ipprec	Получено из принятого ipprec	Rx dscp	Получено из принятого ipprec	Получено из Rx CoS или порта CoS
trust cos	Получено из Rx CoS или порта CoS	Rx dscp	Получено из принятого ipprec	Получено из Rx CoS или порта CoS

(1) Это единственный способ произвести новую пометку кадра.

2 Rx = принятый

В следующей таблице представлена сводка для портов WS-X61xx, WS-X62xx, and WS-X63xx:

Ключевое слово согласования для политики Состояние доверительности порта	set-ip-dscp xx или set-dscp-transmit xx	trust dscp	Trust-ipprec	trust cos
недоверяемый	xx	Rx dscp	Получено из принятого ipprec	0
trust dscp	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается
Trust-ipprec	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается
trust cos	Не поддерживается	Не поддерживается	Не поддерживается	Не поддерживается

Мониторинг и проверка конфигурации

Проверка настройки порта

Введите команду show queuing interface идентификатор интерфейса для проверки настроек и конфигурации порта.

Наряду с другими параметрами, при выполнении данной команды можно выполнить проверку следующих параметров классификации:

- На основе порта или VLAN
- `trust`
- ACL (список управления доступом), связанный с портом

Ниже приведен пример выходных данных этой команды. Важные поля, имеющие отношение к классификации, выделены жирным шрифтом:

```
6500#show queuing interface gigabitethernet 3/2
Interface GigabitEthernet3/2 queuing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Trust state: trust COS
  Default COS is 0
  Transmit queues [type = 1p2q2t]:
```

, trust cos . Кроме этого, значение класса обслуживания (CoS) порта по умолчанию равняется 0.

Проверка заданных классов

Введите команду show class-map для проверки заданных классов. Например:

```
Boris#show class-map
 Class Map match-all test (id 3)
   Match access-group  112

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all voice (id 4)
```

Проверка карты ограничения, применяемой к интерфейсу

Введите следующие команды для проверки карты ограничения, применяемой и имеющей место в предыдущих командах:

- *show mls qos ip interface идентификатор интерфейса*
- *show policy-map interface идентификатор интерфейса*

Ниже представлен пример выходных данных, полученных при выполнении данных команд:

```
Boris#show mls qos ip gigabitethernet 1/1
   [In] Default.   [Out] Default.
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

 Int  Mod Dir  Class-map  DSCP AgId Trust FlId AgForward-Pk AgPoliced-k
 ---------------------------------------------------------------------
 Gi1/1 1  In   TEST       0    0*   No    0    1242120099             0
```

Примечание: Можно посмотреть на эти поля, которые касаются классификации:

- Class-map - , , , , .
- Trust - , trust .
- DSCP - DSCP, , .

```
Tank#show policy-map interface fastethernet 4/4

 FastEthernet4/4

  service-policy input: TEST_aggre2

    class-map: Test_marking (match-all)
      27315332 packets
      5 minute offered rate 25726 pps
      match: access-group 101
      police :
        10000000 bps 10000 limit 10000 extended limit
        aggregate-forwarded 20155529 packets action: transmit
        exceeded 7159803 packets action: drop
        aggregate-forward 19498 pps exceed 6926 pps
```

Практические примеры

В данном разделе содержаться примеры наиболее распространенных конфигураций, использующихся в сетях.

Пример 1: Маркировка на границе

Предположим, что вы настраиваете коммутатор Catalyst 6000, используемый в качестве коммутатора доступа. Большая часть пользователей подключается к слоту 2 коммутатора, в котором установлена линейная плата WS-X6348 (10/100 Мбит/с). Пользователи могут отправлять:

- Normal data traffic (обычный поток данных) — данный вид трафика всегда во VLAN 100 и требует присвоения DSCP со значением 0.
- Voice traffic from an IP phone (голосовой трафик с IP-телефонов) — данный вид трафика всегда в дополнительной голосовой VLAN 101 требует присвоения DSCP со значением 46.
- Mission-critical application traffic (трафик критически важных приложений) — данный трафик также поступает во VLAN 100 и направляется на сервер 10.10.10.20. Этот трафик должен получить значение DSCP, равное 32.

Приложение не помечает какой-либо из этих видов трафика. `untrusted ACL ( ) .` Один ACL применяется для VLAN 100 и другой для VLAN 101. Также необходимо настроить все порты, как основанные на VLAN. Ниже приведен пример конфигурации и результат:

```
Boris(config)#mls qos
Boris(config)#interface range fastethernet 2/1-48
Boris(config-if)#mls qos vlan-based
Boris(config-if)#exit
Boris(config)#ip access-list extended Mission_critical
Boris(config-ext-nacl)#permit ip any host 10.10.10.20
Boris(config)#ip access-list extended Voice_traffic
Boris(config-ext-nacl)#permit ip any any
Boris(config)#class-map voice

Boris(config-cmap)#match access-group Voice_traffic
Boris(config)#class-map Critical

Boris(config-cmap)#match access-group Mission_critical
Boris(config)#policy-map Voice_vlan
Boris(config-pmap)#class voice
Boris(config-pmap-c)#set ip dscp 46
Boris(config)#policy-map Data_vlan
Boris(config-pmap)#class Critical
Boris(config-pmap-c)#set ip dscp 32
Boris(config)#interface vlan 100
Boris(config-if)#service-policy input Data_vlan
Boris(config)#interface vlan 101
Boris(config-if)#service-policy input Voice_vlan
```

Случай 2: Доверие в центральном узле с интерфейсами только Gigabit Ethernet

Предположим, что вы настроили центральный Catalyst 6000 только с интерфейсом Gigabit Ethernet в слоте 1 и 2. Предварительно трафик был корректно помечен коммутаторами доступа. Вам не нужно изменять метки. Несмотря на это, необходимо убедиться, что центральный коммутатор доверяет входящим DSCP. `, .. trust-dscp, :`

```
6k(config)#mls qos
6k(config)#interface range gigabitethernet 1/1-2 , gigabitethernet 2/1-2
6k(config-if)#mls qos trust dscp
```

Дополнительные сведения

- Общие сведение о качестве обслуживания (QoS) для коммутаторов серии Catalyst 6000
- Классификация и маркировка QoS для коммутаторов Catalyst серии 6500/6000 с программным обеспечением CatOS
- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Cisco Systems – техническая поддержка и документация