Классификация и маркировка QoS для коммутаторов Catalyst серии 6500/6000 с программным обеспечением CatOS

Содержание

Введение

В этом документе описано, что происходит при маркировке и классификации пакета в различных местах при его прохождении через шасси коммутатора Catalyst 6000. В этом документе рассматриваются особые случаи, ограничения и содержатся краткие практические примеры.

Этот документ не предназначен, чтобы быть полным списком всех команд операционной

системы Catalyst (CatOS) относительно Качества обслуживания (QoS) или маркировки. Для получения дополнительной информации об интерфейсе командной строки (CLI) CatOS обратитесь к следующему документу:

- Настройке функции QoS

Примечание: В данном документе рассматривается только IP-трафик.

Перед началом работы

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Предварительные условия

Для данного документа отсутствуют предварительные условия.

Используемые компоненты

Этот документ допустим для Коммутаторов семейства Catalyst 6000 Family, выполняющих Программное обеспечение CatOS и использующих один из следующих Supervisor Engine:

- SUP1A + PFC
- SUP1A + PFC + MSFC
- SUP1A + PFC + MSFC2
- SUP2 + PFC2
- SUP2 + PFC2 + MSFC2

Все примеры команд были проверены на Catalyst 6506 с ПО SUP1A/PFC версии 6.3.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Терминология

Ниже следует список терминов, использованных в документе:

- Поле кода дифференцирования обслуживания (DSCP) - первые шесть битов из байта вида услуг (ToS) в IP-заголовке. Код DSCP содержится только в IP-пакете.**Примечание:** Также каждому пакету (IP и другим) назначается внутренняя точка DSCP. Более подробно процесс назначения внутренней точки DSCP рассматривается в данном документе позже.
- 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). Он состоит из любых из следующих трех бит:Три бита dot1p в метке dot1q для пакета IEEE dot1q.Три бита, именуемые "User Field" (полем

пользователя) в заголовке межкоммутаторного канала (ISL) для пакета, инкапсулированного в ISL.Отсутствует класс обслуживания в пакете non-dot1q или ISL.
- Классификация: процесс использовал выбирать трафик, который будет отмечен.
- Маркирование: Процесс настройки пакета DSCP уровня 3 (L3). В данном документе определение маркировки расширено и включает задание значений L2 CoS.

Семейство коммутаторов Catalyst 6000 можно классифицировать по следующим трем параметрам:

- DSCP
- Приоритет IP
- CoS

Коммутаторы семейства Catalyst 6000 Family делают классификацию и маркировку в других местах. Ниже показано, что происходит в этих разных местах:

- Входной порт (входная специализированная интегральная схема [ASIC])
- Механизм коммутации (Policy Feature Card - PFC)
- Порт вывода (исходящий трафик ASIC)

Включение QoS

По умолчанию QoS отключено на Catalyst 6000 Switches. QoS может быть включено путем запуска **qos набора команд** CatOS**, включают**.

Когда QoS отключено нет никакой классификации или маркировки сделанного коммутатором и как такового, каждый пакет оставляет коммутатор с приоритетами DSCP/IP, которые это имело при вводе коммутатора.

Обработка входного порта

С точки зрения классификации основной параметр конфигурации для входного порта – trust state. Каждый порт системы может иметь одно из следующих состояний доверия:

- trust ip precedence (приоритет доверенных IP-адресов)
- trust dscp
- trust cos
- недоверяемый

В оставшейся части этой секции описано, как состояния надежности порта влияют на конечную классификацию пакета. Доверительное состояние порта может быть настроено или изменено с помощью следующей команды CatOS:

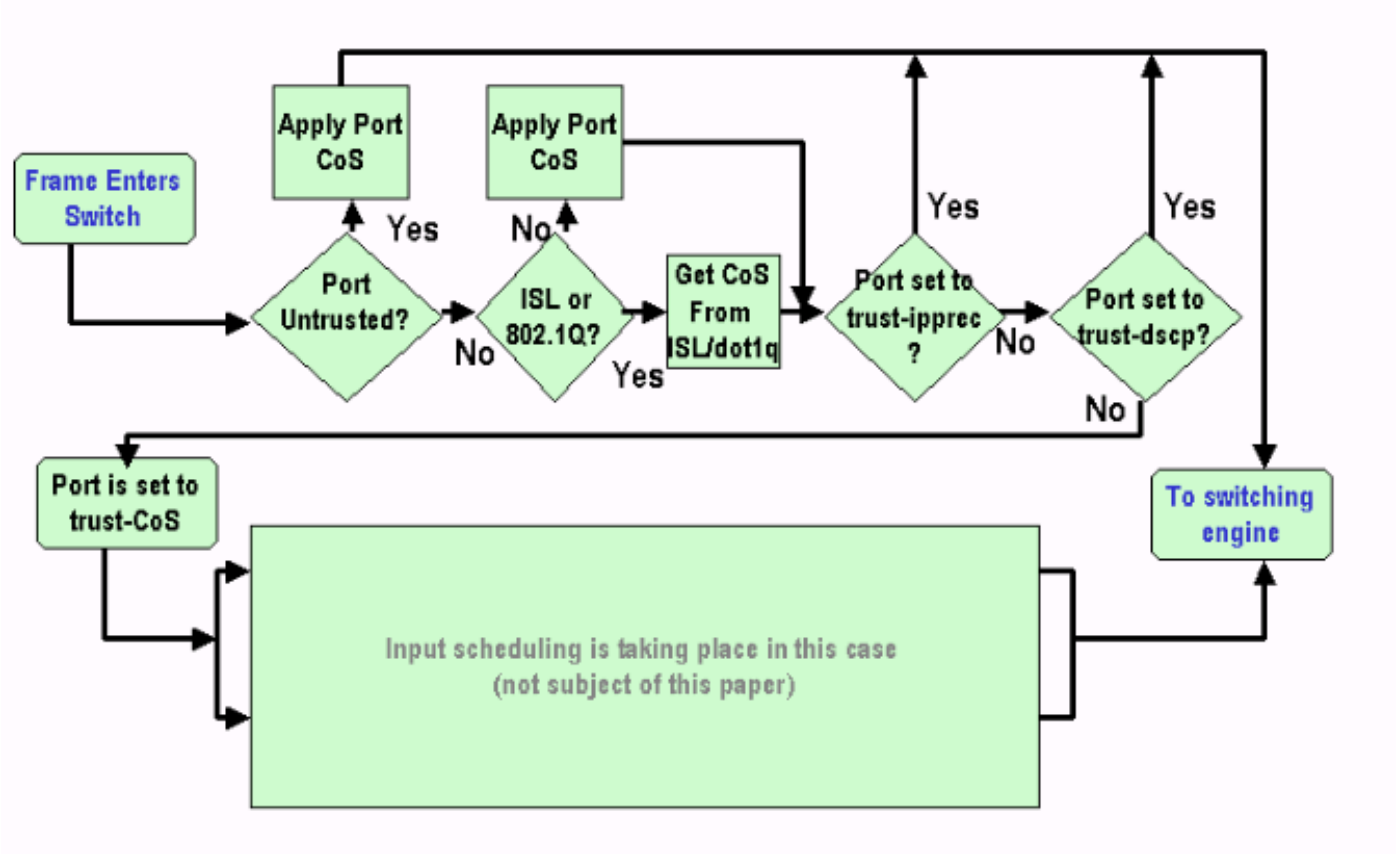
доверие *mod/port* **set port qos {недоверяемый | trust-cos | Trust-ipprec | trust dscp}**

Примечание: По умолчанию все порты находятся в ненадежном состоянии при включении QoS.

На уровне входного порта можно также применить функции CoS для каждого порта, как показано на следующем примере:

mod/port **set port qos, потому что** *cos-value*

Если порт установлен в состояние "ненадежный", просто пометить кадр с CoS порта по умолчанию и передать заголовок на модуль коммутатора (PFC). Если порт установлен в один из режимов доверия, примените порт CoS по умолчанию (если кадр не имеет полученного CoS (dot1q или ISL)), или поддержите CoS, как это (для dot1q и кадров ISL), и передайте кадр к устройству переключения. Классификация ввода изображена на следующей структурной схеме:



Примечание: Как показано в блок-схеме выше, каждый кадр будет иметь назначенный внутренний CoS (либо полученный CoS, либо CoS порта по умолчанию), включая непомеченные кадры, не несущие никакого реального CoS. Этот внутренний CoS и полученный DSCP записываются в заголовок специального пакета и отправляются по шине данных к модулю коммутации. Это происходит на входной линейной плате, и на этом этапе еще не известно, будут ли этот внутренний CoS нести к выходному ASIC и вставлять в исходящий кадр. Это все зависит от того, что PFC делает и далее описан в следующем разделе.

Коммутаторный модуль (PFC)

Когда заголовок достигает модуля коммутатора, с помощью логических схем распознавания закодированных адресов (Encoded Address Recognition Logic, EARL) модуля коммутатора каждому кадру назначается внутренняя точка дифференцированных кодов обслуживания. Внутренний DSCP – это внедренный приоритет, приписанный кадру контроллером последовательности команд и передается коммутатору. Этот код отличается от DSCP в заголовке IPv4. Это выводится из существующего параметра CoS или ToS и используется для сброса CoS или ToS, когда кадр выходит из коммутатора. Этот внутренний DSCP присвоен всем кадрам, обрабатываемым или передаваемым контроллером последовательности команд, даже не IP-кадры.

Четыре возможных источника внутренних значений DSCP

Внутренний DSCP будет наследован из одного из следующих источников:

1. Существующее значение DSCP, установленное до входа фрейма в коммутатор.
2. Принятые биты предшествования IP уже установлены в заголовке IPv4. Поскольку имеется 64 значения DSCP и только восемь значений приоритета IP, администратор настроит сопоставление, используемое коммутатором для установления происхождения DSCP. Если администратор не настроит отображения, действуют отображения по умолчанию.
3. Полученные биты CoS уже установлены для кадра, входящего в коммутатор, или для CoS входящего порта по умолчанию, если во входящем кадре не было CoS. Как и с приоритетом IP-адреса, максимальное число значений CoS равно восьми, каждое из них должно соответствовать одному из 64 значений DSCP. Можно настроить это сопоставление или использовать сопоставление по умолчанию.
4. DSCP может быть установлен для кадра с помощью значения по умолчанию DSCP, обычно назначаемого через запись списка управления доступом (ACL).

Для № 2 и 3 в вышеупомянутом списке используемое статическое отображение по умолчанию, следующим образом:

- Полученный DSCP равен восьми CoS, для привязки CoS к DSCP.
- DSCP производный равен восьми IP старшинству, для IP старшинства DSCP сопоставления.

Это статическое отображение может быть отвергнуто пользователем путем запуска следующих команд:

set qos ipprec-dscp-map <dscp1> <dscp2>... <dscp8>

set qos cos-dscp-map <dscp1> <dscp2>... <dscp8>

Первое значение DSCP, относящегося к сопоставлению CoS (или приоритета IP) равно 0, второе равно 1, и т.д. в этой последовательности.

Какой из четырех возможных источников для внутреннего DSCP будет использоваться?

В разделе изложены правила, определяющие, какой из четырех описанных выше источников будет использоваться для каждого пакета. Это зависит от следующих параметров:

1. Какой список управления доступом к QoS будет применен к пакету? Это определяется следующими правилами:**Примечание:** Каждый пакет проходит запись ACL.Если к входящему порту или VLAN не приписан ни один список ACL, используйте стандартный ACL.При наличии ACL, подключенного к входящему порту или VLAN, и если трафик соответствует одной из записей в ACL, используйте эту запись.*Если список управления доступом (ACL) подключен к входному порту или виртуальной локальной сети (VLAN) и при этом трафик не соответствует одной из записей списка (ACL), используйте список управления доступом (ACL), установленный по умолчанию.*
2. Каждая запись содержит ключевое слово классификации. Ниже приводится список возможных ключевых слов и их описания:Trust-ipprec: Внутренний DSCP будет извлечен из полученного прецедента IP в соответствии со статическим

сопоставлением, независимо от состояния надежности порта.trust dscp: Внутренние значение DSCP будет заимствовано от полученного значения DSCP независимо от состояния доверия порта.trust cos: Внутренняя DSCP будет извлечена из полученной настройки CoS в соответствии со статическим отображением, если порт находится в состоянии доверия (trust-cos, trust-dscp, trust-ipprec). Состояние доверительности порта - trust-xx, DSCP извлекается из порта CoS по умолчанию в соответствии с тем же статическим отображением.*dscp xx:* Внутренняя DSCP зависит от следующих состояний доверия входящего порта:Если порт будет недоверяем, то внутренний DSCP будет установлен в *xx*.Если порт имеет свойство trust-dscp, внутренний DSCP будет получен во входящем пакете.Если порт будет trust-CoS, то внутренний DSCP будет получен из CoS полученного пакета.Если порт является trust-ipprec, внутренний DSCP будет заимствован из значения IP-приоритета полученного пакета.

3. Каждый ACL QoS может быть применен или к порту или к VLAN, но существует параметр дополнительной настройки для принятия во внимание; тип порта ACL. Порт можно настраивать для сети VLAN или по портам. Далее представлено описание двух типов конфигурации:Порт, настроенный, чтобы быть на основе VLAN, будет только смотреть на ACL, применился к VLAN, которой принадлежит порт. Если будет ACL, подключенный к порту, то ACL будет проигнорирован для пакета, входящего на том порту.Если для порта, принадлежащего сети VLAN, настроена конфигурация на основе портов, для поступающего от данного порта трафика это не учитывается, даже если данной сети VLAN назначен список ACL.

Это синтаксис для создания списка управления доступом качества сервиса QoS для маркирования IP трафика:

acl_name **ip acl set qos [xx dscp | trust-cos | trust dscp | Trust-ipprec]** *правило ввода acl*

Следующий ACL, отметит весь IP - трафик, направленный к хосту 1.1.1.1 с DSCP "40", и будет trust dscp для всего другого IP - трафика:

set qos acl TEST_ACL dscp 40 ip any host 1.1.1.1

set qos acl TEST_ACL trust-dscp ip any any

После создания списка управления доступом (ACL) нужно соотнести его с портом или VLAN, для чего выполняется следующая команда:

acl set qos сопоставляет *acl_name* **[модуль/порт | VLAN]**

По умолчанию каждый порт на основе порта для ACL, поэтому если вы хотите подключить ACL к VLAN, необходимо настроить порты этой VLAN как основанные на vlan. Это можно сделать с помощью следующей команды:

основанный на vlan *модуль/порт* **set port qos**

Его также можно вернуть в режим портов при помощи следующей команды:

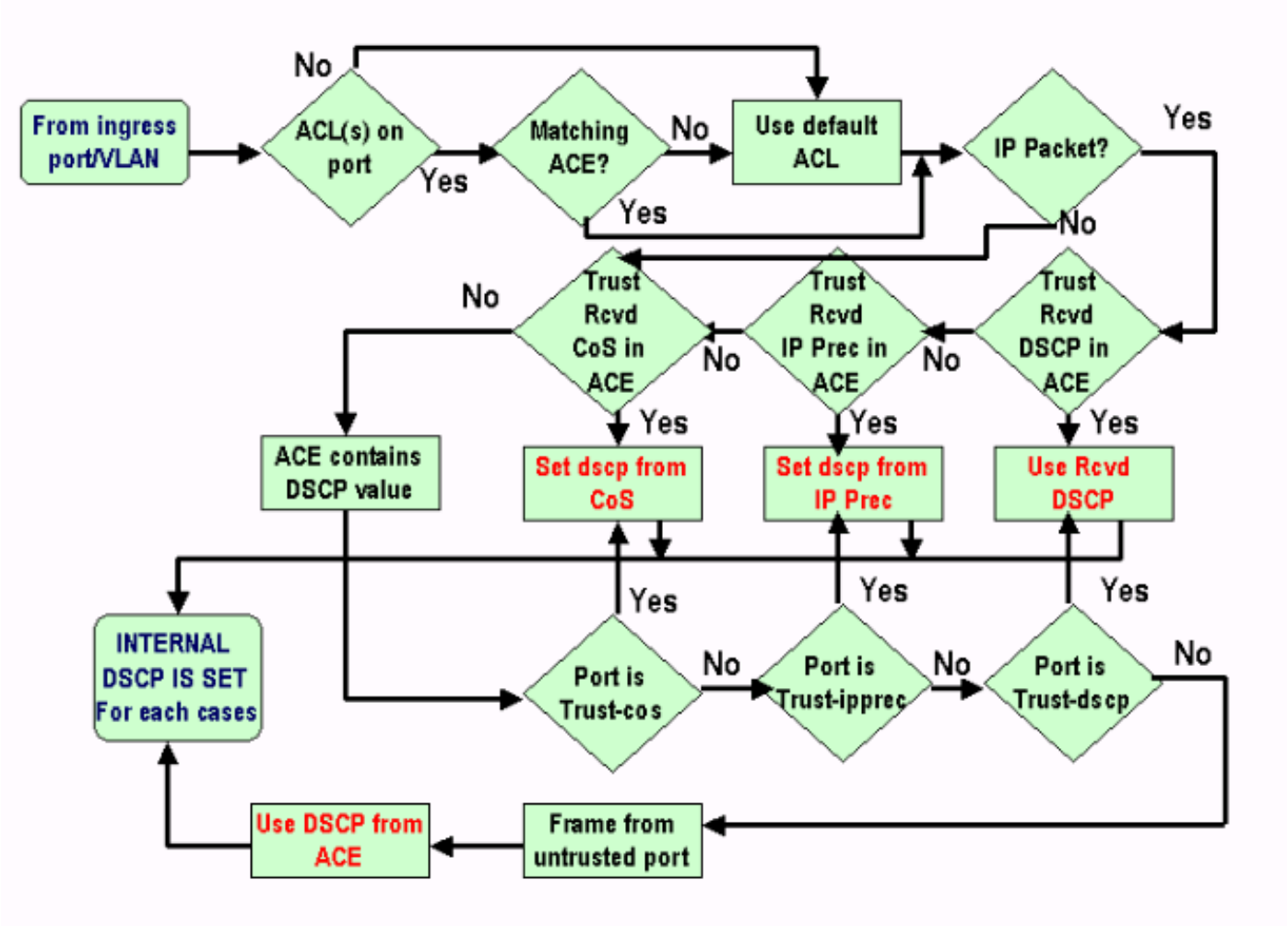
модуль/порт **set port qos на основе порта**

Сводка: Каким образом выбиралась внутренняя DSCP?

Внутренний DSCP зависит от таких факторов:

- состояние доверительности порта
- ACL, присвоенный порту
- список доступа по умолчанию
- На основе виртуальной локальной сети или на основе порта в отношении ACL

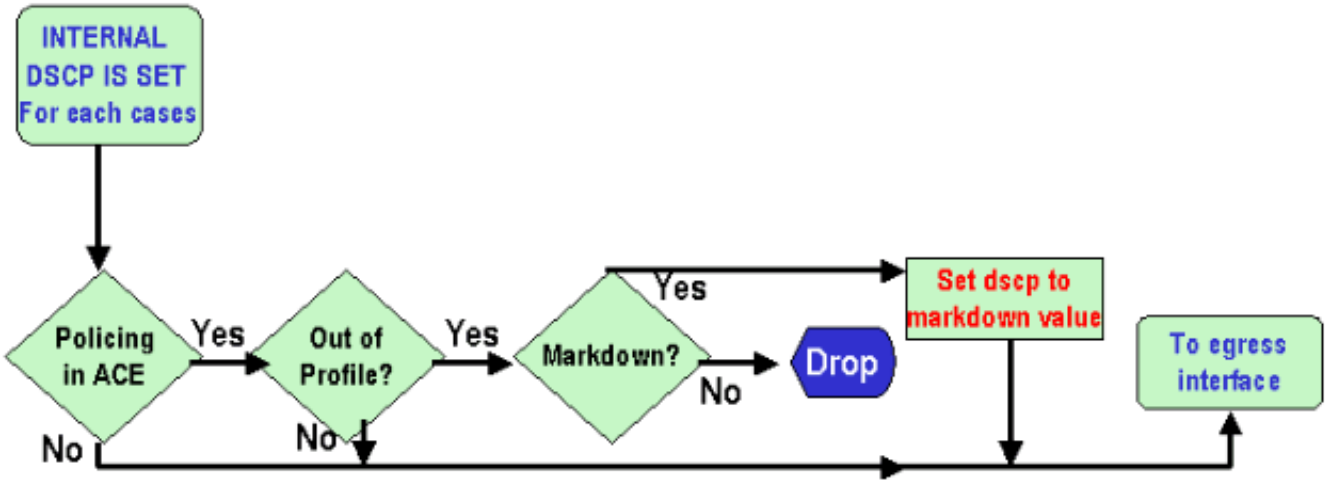
Следующая структурная схема показывает, как выбирается внутреннее дифференцированное обслуживание пунктов связи (DSCP) в зависимости от конфигурации:



PFC также может осуществлять контроль. Результатом может быть снижение внутренней DSCP. Дополнительные сведения о применении политик см. в следующем документе:

- Применение QoS Профилирование (policing) в коммутаторе Catalyst 6000

На следующей блок-схеме изображен процесс использования ограничителя:



Обработка выходного порта

На уровне выходного порта изменить параметры классификации невозможно, однако маркировка пакетов в данном разделе осуществляется в соответствии со следующими правилами:

- Если это пакет IPv4, скопируйте внутреннее поле DSCP, присвоенное коммутатором, в поле ToS заголовка IPv4.
- Если порт вывода настроен для инкапсуляции ISL или dot1q, используйте CoS из внутреннего DSCP и скопируйте в кадр ISL или dot1q.

Примечание: CoS получен из внутреннего DSCP в соответствии с помехой, настроенной пользователем при выполнении следующей команды:

Примечание: *set qos dscp-cos-map dscp_list: cos_value*

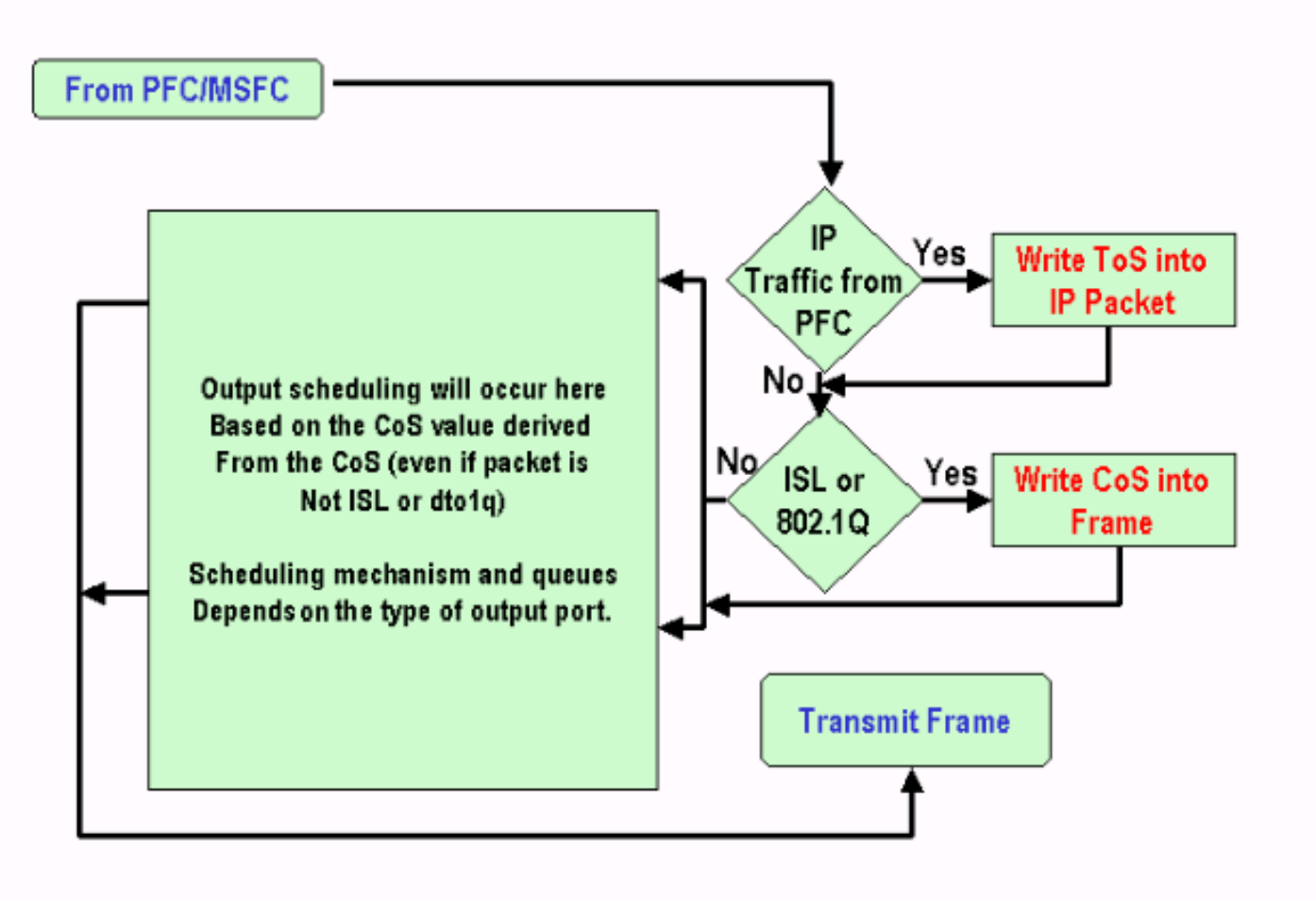
Примечание: Ниже приведены конфигурации по умолчанию. По умолчанию значение CoS рассчитывается путем деления целой части DSCP на восемь:

```
set qos dscp-cos-map 0-7:0
set qos dscp-cos-map 8-15:1
set qos dscp-cos-map 16-23:2
set qos dscp-cos-map 24-31:3
set qos dscp-cos-map 32-39:4
set qos dscp-cos-map 40-47:5
set qos dscp-cos-map 48-55:6
set qos dscp-cos-map 56-63:7
```

Как только DSCP записан в IP-заголовок и CoS получен из DSCP, пакет направляется в одну из выходных очередей для планирования вывода на основе его CoS (даже если это не пакет dot1q или ISL). За более подробной информацией по составлению очереди вывода обратитесь к следующей документации:

- QoS на коммутаторах серии Catalyst 6000: планирование вывода на Catalyst 6000 с PFC или Использованием программного обеспечения CatOS PFC 2

Следующая структурная схема показывает обработку пакета согласно маркеру на порту вывода:



Примечания и ограничения

Стандартный список управления доступом (ACL)

По умолчанию список ACL использует в качестве ключевого слова классификации "dscp 0". Это означает, что весь трафик, вводящий коммутатор через ненадежный порт, будет отмечен DSCP "0", если будет включено QoS. Можно проверить список доступа по умолчанию для IP с помощью следующей команды:

```
Boris-1> (enable) show qos acl info default-action ip set qos acl default-action ----------
---------- ip dscp 0
```

Список доступа по умолчанию может также быть изменен с помощью следующей команды:

ip действия по умолчанию acl set qos [xx dscp | trust-CoS | trust dscp | Trust-ipprec]

ограничения записей ACL trust-cos

Существуют дополнительные ограничения при использовании ключевого слова trust-CoS для входа. CoS является доверенным на входе, только если состояние доверия приема является надежным. При попытке настройки записи с помощью команды trust-CoS выводится следующее предупреждение:

```
Telix  (enable) set qos acl ip test_2 trust-CoS ip any any Warning: ACL trust-CoS should only be
used with ports that are also configured with port trust=trust-CoS test_2 editbuffer modified.
Use 'commit' command to apply changes.
```

Это ограничение является следствием того, что ранее отображалось в разделе “Обработка

выходного порта”. Как видно из блок-схемы этого раздела, если порт ненадежный, кадру немедленно назначается стандартный уровень CoS порта. Таким образом, CoS для входящего трафика не сохраняется и не отсылается на устройство коммутации, что приводит к невозможности доверять данным CoS даже при имеющемся ACL.

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

Сведения этого раздела относятся только к следующим линейным картам:

- 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 100FX, ENH QOS, MT
- WS-X6324-100FX-SM: CATALYST 6000 24-PORT 100FX, ENH QOS, MT
- WS-X6348-RJ-45 : CATALYST 6000 10/100 С 48 ПОРТАМИ, УЛУЧШЕННЫЙ QO
- WS-X6348-RJ21V: Catalyst 6000 48-Port 10/100, Inline Power (питание по линии)
- WS-X6348-RJ21V: CATALYST 6000 48-PORT 10/100, ENH QOS, INLI NE POWER

Однако, эти линейные платы имеют некоторые дополнительные ограничения:

- На уровне порта нельзя применить trust-dscp или trust-ipprec.
- На уровне порта, если состояние надежности порта является trust-CoS, применяются следующие операторы:Получить порог для входного планирования включен. Кроме того, CoS в получить пакете используется для расположения по приоритетам пакетов для доступа к шине.CoS не будут доверять и не будут использовать для получения внутреннего DSCP, пока вы также не настроили ACL для того трафика к trust-cos. Кроме того, для линейных плат недостаточно trust-cos на порте, необходимы ACL с trust-cos для всего трафика.
- Если состояние надежности порта недоверяемо, обычная маркировка произойдет (как со стандартным случаем). Это зависит от списка ACL, примененного к трафику.

Любая попытка настроить надежное состояние на одном из этих портов приведет к выдаче следующих предупреждающих сообщений:

```
telix (enable) set port qos 3/24 trust trust-ipprec
Trust type trust-ipprec not supported on this port.

telix (enable) set port qos 8/4 trust trust-dscp
Trust type trust-dscp not supported on this port.

telix (enable) set port qos 3/24 trust trust-cos
Trust type trust-cos not supported on this port.
Receive thresholds are enabled on port 3/24.
Port  3/24 qos set to untrusted.
```

Краткое описание классификации

В приведенных ниже таблицах показаны итоговые точки дифференцированных кодов обслуживания, распределенные по следующим категориям:

- Состояние доверенности входящего порта.
- Ключевое слово классификации в пределах применяемого ACL (списка управления

доступом).

Сводная таблица для всех портов, кроме WS-X62xx и WS-X63xx

Ключевое слово ACL Состояние доверительности порта	dscp xx	trust dscp	Trust-ipprec	trust cos
Недоверяемый	xx (1)	Rx 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.

Краткое содержание таблицы для *WS-X62xx* или *WS-X63xx*

Ключевое слово ACL Состояние доверительности порта	dscp 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	xx	Rx dscp	получено из принятог	полученный из CoS Rx

			o ipprec	или CoS порта (2)

(2) Это единственный способ сохранить входящее CoS для трафика, идущего от линейной платы 62xx или 63xx.

Проверка и мониторинг конфигурации

Проверка конфигурации порта

Настройки порта и конфигурации можно проверить, применив команду:

модуль/порт **show port qos**

С помощью этой команды можно проверить (среди прочих параметров) следующие параметры классификации:

- основанный на порте или на виртуальной локальной сети (параметр классификации)
- тип доверенного порта
- ACL, присвоенный порту

Ниже приведен пример выходных данных команды с выделенными полями, имеющими отношение к классификации:

```
tamer (enable) show port qos 1/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.


Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------ -------------
 1/1    port-based     port-based COPS local Port TxPort Type RxPort Type Trust Type Trust Type
Def CoS Def CoS config runtime config runtime ----- ------------ ------------ ------------ -----
-------- ------- ------- 1/1 1p2q2t 1p1q4t untrusted untrusted 0 0 (*)Runtime trust type set to
untrusted. Config: Port ACL name Type ----- ------------------------------- ---- 1/1 test_2 IP
Runtime: Port ACL name Type ----- ------------------------------- ---- 1/1 test_2 IP
```

Примечание: Для каждого поля имеется настроенный параметр и рабочий параметр. К пакету применяется динамический параметр.

Проверка ACL

Можно проверить примененный и отображенный предыдущими командами ACL с помощью такой команды:

acl_name **info runtime acl show qos**

```
tamer (enable) show qos acl info run test_2
set qos acl IP test_2
---------------------------------------------
1. dscp 32 ip any host 1.1.1.1 2. trust-dscp any
```

Практические примеры

Следующие примеры - варианты типичных конфигураций, которые встречаются в сети.

Пример 1: Маркировка на границе

Предположим, выполняется настройка Catalyst 6000, который используется как ключ доступа для пользователей, подключенных к слоту 2 с линейной платой WS-X6348 (10/100M). Пользователи могут отправить следующее:

- Нормальный трафик данных: Это всегда находится в VLAN 100 и должно получить DSCP "0".
- Голосовой трафик с IP-телефона: Всегда в дополнительных голосовых VLAN 101, для DSCP необходимо получить значение "40"."
- Критически важный трафик приложения: Поступает также в сеть VLAN 100 и перенаправляется на сервер 10.10.10.20. Этот трафик должен получить значение DSCP, равное 32."

Этот трафик не отмечен приложением, поэтому вы покинете порт как "не пользующийся доверием" и сконфигурируете специальный ACL для классификации трафика. Один ACL будет применен к VLAN 100, и один ACL будет применен к VLAN 101. Также необходимо настроить все порты как на основе VLAN. Пример итоговой конфигурации:

```
set qos enable
set port qos 2/1-48 vlan-based
!--- Not needed, as it is the default. set port qos 2/1-48 trust untrusted set qos acl ip
Data_vlan dscp 32 ip any host 10.10.10.20 !--- Not needed, because if it is not present you
would !--- use the default ACL which has the same effect. Set qos acl ip Data_vlan dscp 0 ip any
any set qos acl ip Voice_vlan dscp 40 ip any any commit qos acl all set qos acl map Data_vlan
100 set qos acl map Voice_vlan 101
```

Случай 2: Доверие к ядру только с гигабитным интерфейсом

Представьте, что вы настраиваете ядро Catalyst 6000 с одним лишь гигабитным интерфейсом в слотах 1 и 2 (в шасси отсутствуют линейные платы 62xx или 63xx). Трафик был правильно маркирован коммутаторами доступа ранее, поэтому повторную маркировку производить не требуется, однако необходимо убедиться в надежности входящего DSCP. Это самый простой случай, поскольку все порты будут отмечены как trust-dscp и этого должно быть достаточно:

```
set qos enable
set port qos 1/1-2 trust trust-dscp
set port qos 2/1-16 trust trust-dscp
...
```

Случай 3: Основная надежность и порт 62xx или 63xx в аппаратном блоке

Предположим, что выполняется настройка центрального устройства или устройства распределения с гигабитным каналом на линейной плате WS-X6416-GBIC (в гнезде 2) и каналом 10/100 на линейной плате WS-X6348 (в гнезде 3). Необходимо также сделать весь входящий трафик доверенным, т. к. он уже проходил маркировку на уровне ключа доступа. Поскольку вы не можете trust dscp на 6348 линейных картах, наилегчайший метод в этом случае должен был бы оставить все порты столь же недоверяемыми и изменить список доступа по умолчанию на trust dscp, как в следующем примере:

```
set qos enable
set port qos 2/1-16 trust untrusted
set port qos 3/1-48 trust untrusted
```

```
set qos acl default-action ip trust-dscp
```

Дополнительные сведения

- Поддержка продуктов для ЛВС
- Поддержка технологии коммутации локальных сетей
- Техническая поддержка - Cisco Systems