

# Устранение неисправностей коммутаторов Catalyst 6500 QoS

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Поиск и устранение неполадок QoS](#)

[Пошаговая процедура устранения неполадок](#)

[Рекомендации и ограничения в отношении QoS на коммутаторах Catalyst 6500](#)

[Ограничение QoS TCAM](#)

[Ограничение NBAR](#)

[Отсутствие команд cos-map в супервизоре Supervisor 2](#)

[Ограничения команд service-policy](#)

[Выходные операторы service-policy отсутствуют в выходных данных команды running-config](#)

[Ограничение применения политик](#)

[Проблемы ограничения скорости или применения политик с платой MSFC в гибридной операционной системе](#)

[Команда shape average не поддерживается на интерфейсах VLAN маршрутизатора Cisco 7600](#)

[ОШИБКА QoS: Addition/Modification made to policymap \[строка\] and class \[строка\] is not valid, command is rejected»](#)

[Дополнительные сведения](#)

## Введение

В этом документе изложены основные шаги для поиска и устранения неполадок, ограничения качества обслуживания (QoS), а также приведены сведения, помогающие диагностировать распространенные проблемы QoS в коммутаторах Catalyst 6500. В этом документе также рассматриваются проблемы QoS, возникающие при классификации, маркировке и контроле.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

## Используемые компоненты

Приводимая в настоящем документе информация относится к коммутаторам серии Catalyst 6500.

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.](#)

## Общие сведения

QoS — сетевая функция классификации трафика, обеспечивающая детерминированный механизм доставки. Для иллюстрации процесса QoS опишем его основные шаги:

- **Входная диспетчеризация.** Осуществляется аппаратно заказными микросхемами порта и представляет собой операцию QoS 2-го уровня. Для этой операции не требуется плата функций политик (PFC).
- **Классификация.**—Этот этап выполняется супервизором и/или платой функций политик (PFC) посредством ядра списков контроля доступа (ACL). Супервизор реализует операции QoS на 2-м уровне. Плата PFC реализует операции QoS на 2-м и 3-м уровнях.
- **Применение политик.** Выполняется платой PFC посредством ядра пересылки 3-го уровня. Присутствие PFC является обязательным. Эта плата осуществляет операции QoS на 2-м и 3-м уровнях.
- **Перезапись пакетов.** Осуществляется аппаратно заказными микросхемами портов. Это операция QoS 2-го и 3-го уровней, выполняемая на основе предварительно произведенной классификации.
- **Выходная диспетчеризация.** Осуществляется аппаратно заказными микросхемами портов. Это операция QoS 2-го и 3-го уровней, выполняемая на основе предварительно произведенной классификации.

## Поиск и устранение неполадок QoS

В коммутаторах Catalyst 6500 QoS работает иным образом, чем в маршрутизаторах. Архитектура QoS в коммутаторах Catalyst 6500 весьма сложна. Рекомендуется иметь представление о плате функций коммутатора (MSFC), плате PFC и архитектуре модуля Supervisor Engine в Catalyst 6500. Конфигурация QoS в гибридной операционной системе требует более подробного знания функций CatOS 2-го уровня и платы MSFC 3-го уровня с функциональными возможностями Cisco IOS®. Перед настройкой QoS рекомендуется подробно ознакомиться со следующими документами:

- [Настройка QoS на плате PFC — встроенная реализация IOS](#)
- [Настройка QoS – CatOS](#)

## Пошаговая процедура устранения неполадок

В этом разделе изложена основная пошаговая процедура поиска и устранения неполадок в системе QoS, позволяющая локализовать проблему для ее последующего устранения.

- 1. Разрешение QoS.—Команда `show mls qos` показывает статистику применения политик и состояние QoS (включено/отключено).**  
`Switch#show mls qos` QoS is enabled globally QoS ip packet dscp rewrite enabled globally Input mode for GRE Tunnel is Pipe mode Input mode for MPLS is Pipe mode Vlan or Portchannel(Multi-Earl)policies supported: Yes Egress policies supported: Yes ----- Module [5] ----- QoS global counters: Total packets: 244 IP shortcut packets: 0 Packets dropped by policing: 0 IP packets with TOS changed by policing: 5 IP packets with COS changed by policing: 4 Non-IP packets with COS changed by policing: 0 MPLS packets with EXP changed by policing: 0
- 2. Классификация входящего трафика с использованием доверенного порта. Эта классификация относит входящий трафик к одному из семи значений класса обслуживания (CoS). Входящий трафик может иметь значение CoS, уже назначенное источником. В этом случае нужно настроить порт таким образом, чтобы он доверял значению CoS во входящем трафике. Доверие позволяет коммутатору сохранять значение CoS или тип службы (ToS) из полученного кадра. Эта команда иллюстрирует проверку состояния доверия порта:**  
`Switch#show queueing int fa 3/40` Port QoS is enabled Trust state: trust CoS Extend trust state: not trusted [CoS = 0] Default CoS is 0 !---  
*Output suppressed.* Значение CoS передается только кадрами межкоммутаторной связи (ISL) и dot1q. Кадры, не снабженные метками, не несут значений CoS. Кадры без меток содержат значения ToS, полученные на основе приоритета IP или кода дифференцированного обслуживания (DSCP) из заголовка пакета IP. Для доверия значению ToS необходимо настроить порт в режиме доверия приоритету IP или DSCP. Коды DSCP обратно совместимы с приоритетами IP. Например, если порт коммутатора настроен как порт 3-го уровня, то он не передает кадры dot1q или ISL. В этом случае необходимо настроить данный порт так, чтобы он доверял приоритету IP или коду DSCP.  
`Switch#show queueing interface gigabitEthernet 1/1` Interface GigabitEthernet1/1 queueing strategy: Weighted Round-Robin Port QoS is enabled Trust state: trust DSCP Extend trust state: not trusted [COS = 0] Default CoS is 0 !--- *Output suppressed.*
- 3. Классификация входящего списка с использованием списка контроля доступа и ядер управления приложениями.—Коммутатор можно также настроить для классификации и маркировки трафика. Настройка классификации и маркировки включает в себя следующие шаги: создание списков контроля доступа, карт классов (class-map) и политик (policy-map) и выполнение команды `service-policy input` для применения карты политик к интерфейсу. Можно проверить статистику карты политики, как показано в этом примере:**  
`Switch#show policy-map interface fa 3/13` FastEthernet3/13 Service-policy input: pqos2 class-map: qos1 (match-all) Match: access-group 101 set precedence 5: Earl in slot 5 : 590 bytes 5 minute offered rate 32 bps aggregate-forwarded 590 bytes Class-map: class-default (match-any) 36 packets, 2394 bytes 5 minute offered rate 0 bps, drop rate 0 bps Match: any  
`Switch#show mls qos ip ingress` QoS Summary [IPv4]: (\* - shared aggregates, Mod - switch module) Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By Id Id -----  
`In qos1 40 1 No 10 590 0 All 5 - Default 0 0* No 0 365487 0` Обратите внимание на то, что счетчик AgForward-By, соответствующий карте классов qos1, увеличивается. Если статистика для соответствующей карты классов не отображается, проверьте список контроля доступа, связанный с картой классов.
- 4. Входная диспетчеризация. Для настройки входной диспетчеризации плата PFC не требуется. На одиночном порту 10/100 нельзя настроить команды `rcv-queue threshold` или `set qos drop-threshold`. Это обусловлено тем, что входная диспетчеризация**

обслуживается портами на базе заказных микросхем Coil, рассчитанных на двенадцать портов 10/100. Поэтому входную диспетчеризацию необходимо настраивать группами по 12 портов, например 1–12, 13–24, 25–36, 37–48. Архитектура организации очередей встроена в заказную микросхему и не допускает перенастройки. Для просмотра структуры очередей порта LAN выполните команду **show queueing interface fastethernet слот/порт | include type**.

```
Switch#show queueing interface fastEthernet 3/40 Queueing Mode In
Rx direction: mode-cos Receive queues [type = lq4t]: <----- 1 Queue 4 Threshold Queue
Id Scheduling Num of thresholds ----- 1 Standard 4
queue tail-drop-thresholds ----- 1 50[1] 60[2] 80[3] 100[4] <-----
Threshold levels 50%, 60%, 80% and 100% Packets dropped on Receive: BFDU packets: 0 queue
thresh dropped [cos-map] ----- 1 1 0 [0 1 ] 1
```

2 0 [2 3 ] 1 3 0 [4 5 ] 1 4 0 [6 7 ] !--- Output suppressed. По умолчанию все 4 пороговых значения составляют 100 %. Для настройки пороговых уровней можно применять команду **rcv-queue threshold <код очереди> <порог 1> <порог 2> <порог 3> <порог 4>**. В этом случае при перегрузке трафиком данные, имеющие более высокие значения CoS, не будут отбрасываться первыми в пользу данных с более низким значениями CoS. Switch(config)#interface range fa 3/37 - 48 Switch(config-if-range)#rcv-queue threshold 1 50 60 80 100

5. Привязка. Если порт настроен в режиме доверия CoS, то для привязки полученного значения CoS ко внутреннему значению DSCP следует использовать команду карты **CoS-DSCP**.

```
Switch#show mls qos maps cos-dscp Cos-dscp map: cos: 0 1 2 3 4 5 6 7 -----
----- dscp: 0 8 16 24 32 40 48 56
```

Если порт настроен в режиме доверия приоритету IP, то для привязки получаемого значения приоритета IP ко внутреннему значению DSCP следует использовать таблицу карты **ip-prec-dscp**.

```
Switch#show mls qos maps ip-prec-dscp IpPrecedence-dscp map: ipprec: 0 1 2 3 4 5 6 7 -
----- dscp: 0 8 16 24 32 40 48 56
```

Если порт настроен для доверия DSCP, то полученное значение DSCP будет использоваться в качестве внутреннего значения DSCP. Эти таблицы должны быть одинаковы на всех коммутаторах в сети. Если на любом из коммутаторов привязки в таблице будут отличаться, то требуемый результат получить не удастся. Значения из таблицы можно изменить, как показано ниже: Switch(config)#mls qos map cos-dscp 0 8 16 24 40 48 48 56 Switch(config)#mls qos map ip-prec-dscp 0 8 16 24 40 48 48 56

6. Применение политик.—В коммутаторах Catalyst 6500 существуют два способа применения политик: Агрегированное применение политик.—При агрегированном применении политик контролируется полоса пропускания потока на коммутаторе. Команда **show mls qos aggregate-policies** показывает все настроенные на коммутаторе механизмы применения политик. Статистика по применению политик имеет следующий

```
ВИД:Switch#show mls qos ip fastEthernet 3/13 [In] Policy map is pqos2 [Out] Default. QoS
Summary [IPv4]: (* - shared aggregates, Mod - switch module) Int Mod Dir Class-map DSCP Agg
Trust Fl AgForward-By AgPoliced-By Id Id -----
----- Fa3/13 5 In qos1 0 1* dscp 0 10626 118860 Fa3/13 5 In class-
defa 40 2 No 0 3338 0 Switch#show mls qos QoS is enabled globally QoS ip packet dscp
rewrite enabled globally Input mode for GRE Tunnel is Pipe mode Input mode for MPLS is Pipe
mode Vlan or Portchannel(Multi-Earl) policies supported: Yes Egress policies supported: Yes
----- Module [5] ----- QoS global counters: Total packets: 163 IP shortcut packets: 0
Packets dropped by policing: 120 IP packets with TOS changed by policing: 24 IP packets
with COS changed by policing: 20 Non-IP packets with COS changed by policing: 3 MPLS
```

packets with EXP changed by policing: 0 Применение политик для микропотоков.—В этом режиме применения политик контролируется полоса пропускания потока на каждом интерфейсе коммутатора. По умолчанию механизмы применения политик для микропотоков затрагивают только маршрутизируемый трафик. Чтобы разрешить применение политик для микропотоков к трафику, пересылаемому в режиме моста,

выполните на интерфейсе VLAN команду `mls qos bridged`. Проверить статистику применения политик посредством микропотоков можно следующим образом: `Switch#show mls ip detail`

```

Switch#show mls ip detail
Displaying Netflow entries in Supervisor Earl DstIP SrcIP
Prot:SrcPort:DstPort Src i/f :AdjPtr -----
----- Pkts Bytes Age LastSeen Attributes -----
----- Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST -----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
----- Ig/acli Ig/aclo Ig/qosi Ig/qoso
Fpkt Gemini MC-hit Dirty Diags -----+-----+-----+-----+-----+-----+-----+-----+
--- QoS Police Count Threshold Leak Drop Bucket Use-Tbl Use-Enable -----+-----+-----+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
- :0x0 43 64500 84 21:37:16 L3 - Dynamic 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0x0 0
0 0 NO 1518 NO NO 10.175.50.2 10.175.51.2 icmp:0 :0 -- :0x0 43 64500 84 21:37:16 L3 -
Dynamic 1 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0x0 664832 0 0 NO 1491 NO NO 0.0.0.0
0.0.0.0 0 :0 :0 -- :0x0 1980 155689 1092 21:37:16 L3 - Dynamic 0 1 0 0 1 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0x0 0 0 0 NO 0 NO NO
Switch#show mls qos
QoS is enabled globally
QoS ip packet dscp rewrite enabled globally
Input mode for GRE Tunnel is Pipe mode
Input mode for MPLS is Pipe mode
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes
----- Module [5] -----
QoS global counters: Total packets: 551
IP shortcut packets: 0
Packets dropped by policing: 473
IP packets with TOS changed by policing: 70
IP packets with COS changed by policing: 44
Non-IP packets with COS changed by policing: 11
MPLS packets with EXP changed by policing: 0

```

**Примечание:** Команда `mod/номера типа ip show mls qos` не показывает статистические данные по контролю соблюдения правил для микропотоков. Она показывает только статистику по агрегированному применению политик. Если не удастся получить требуемую статистику по применению политик, проверьте конфигурацию применения политик. [Пример конфигурации см. в документе Применение политик QoS на коммутаторах Catalyst серии 6500/6000. Также см. раздел настоящего документа Рекомендации и ограничения в отношении QoS на коммутаторах Catalyst 6500.](#)

- [Ознакомьтесь с замечаниями к выпуску используемой версии операционной системы и убедитесь в отсутствии ошибок, связанных с конфигурацией QoS.](#)
- Отметьте модель супервизора коммутатора, модель платы PFC, модель платы MSFC и версию Cisco IOS/CatOS. [См. раздел Рекомендации и ограничения в отношении QoS на коммутаторах Catalyst 6500 в контексте характеристик имеющегося оборудования.](#) Убедитесь в том, что ваша конфигурация может действовать.

## [Рекомендации и ограничения в отношении QoS на коммутаторах Catalyst 6500](#)

С QoS связаны некоторые ограничения, о которых необходимо знать, прежде чем настраивать QoS в коммутаторах Catalyst 6500:

- [Общие рекомендации](#)
- [Рекомендации для PFC3](#)
- [Рекомендации для PFC2](#)
- [Ограничения команды class-map](#)
- [Ограничения команды policy-map](#)
- [Ограничения команды policy-map class](#)
- [Рекомендации и ограничения в отношении привязки порогов управления очередями и отбрасыванием](#)
- [ограничения записей ACL trust-cos](#)
- [Ограничения для линейных плат WS-X6248-xx, WS-X6224-xx и WS-X6348-xx](#)
- Платы PFC и PFC2 не предусматривают QoS для трафика WAN. С платами PFC и PFC2 реализация QoS на плате PFC не изменяет байт ToS в трафике WAN.

- Входной трафик LAN, коммутируемый на уровне 3, не проходит через плату MSFC или MSFC2 и сохраняет значение CoS, назначенное ядром коммутации 3-го уровня.
- **QoS не реализует входные перегрузки порта входящим трафиком на портах, настроенных с ключевыми словами `untrusted`, `trust-ipprec` или `trust-dscp`.** Трафик напрямую поступает в модуль коммутатора.
- Для значений CoS, связанных только с очередью, коммутатор применяет порог отбрасывания пакета по превышению очереди. Для значений CoS, связанных с очередью и порогом, коммутатор применяет пороги отбрасывания пакетов на основе случайно взвешенного предварительного обнаружения (WRED).
- При классификации с ядром коммутации 3-го уровня используются значения 2-го, 3-го и 4-го уровней. При маркировке посредством ядра коммутации 3-го уровня используются значения CoS 2-го уровня и значения приоритета IP или кода DSCP 3-го уровня.
- Список контроля доступа `trust-cos` не может восстановить полученное значение CoS в трафике от недоверенных портов. Трафик от недоверенных портов всегда будет иметь значение CoS порта.

**Примечание:** QoS PFC не обнаруживает использование неподдерживаемых команд, пока вы не подключаете карту политик к интерфейсу.

## Ограничение QoS TCAM

Троичная ассоциативная память (TCAM) — специализированный блок памяти, позволяющий ядру ACL на платах PFC, PFC2 и PFC3 выполнять быстрый табличный поиск на основе пакетов, проходящих через коммутатор. Списки контроля доступа обрабатываются аппаратно на коммутаторах Cisco Catalyst серии 6500, именуемых TCAM. При настройке списка контроля доступа список привязывается к QoS, а когда политика QoS применяется на интерфейсе, коммутатор программирует память TCAM. Если все доступное пространство TCAM на коммутаторе уже использовано для QoS, то возникнет сообщение об ошибке:

```
Switch(config)#interface vlan 52 Switch(config-if)#service-policy input test Switch(config-if)#
3w0d: %QM-4-TCAM_ENTRY: Hardware TCAM entry capacity exceeded
```

**Из этого примера выходных данных команды `show tcam count` можно видеть, что пространство масок записей TCAM занято на 95 %.** - QoS %QM-4-TCAM\_ENTRY: .

```
Switch#show tcam count Used Free Percent Used Reserved -----
Labels:(in) 43 4053 1 Labels:(eg) 2 4094 0 ACL_TCAM ----- Masks: 19 4077 0 72 Entries: 95
32673 0 576 QOS_TCAM ----- Masks: 3902 194 95 18 Entries: 23101 9667 70 144 LOU: 0 128 0
ANDOR: 0 16 0 ORAND: 0 16 0 ADJ: 3 2045 0
```

Записи TCAM и метки ACL представляют собой ограниченные ресурсы. Поэтому, в зависимости от конфигурации ACL, могут потребоваться особые меры для предотвращения исчерпания доступных ресурсов. Кроме того, в конфигурациях с крупными списками контроля доступа QoS и списками контроля доступа VLAN (VACL) также следует обратить внимание на пространство энергонезависимой памяти (NVRAM). Объем доступных аппаратных ресурсов различается на модулях супервизора 1а с платой PFC, 2 с платой PFC2 и 720 с платой PFC3.

Модуль супервизора	Память TCAM для QoS	Метки ACL
Супер	2К масок и 16К	512 меток ACL,

визор 1а и плата PFC	шаблонов в общем наборе для списков контроля доступа маршрутизатора (RACL), списков VACL и списков ACL для QoS	общих для разных категорий списков контроля доступа: RACL, VACL и QoS ACL
Супер визор 2 и плата PFC2	4К масок и 32К шаблонов для списков контроля доступа QoS	512 меток ACL, общих для разных категорий списков контроля доступа: RACL, VACL и QoS ACL
Супер визор 720 и плата PFC3	4К масок и 32К шаблонов для списков контроля доступа QoS	512 меток ACL, общих для разных категорий списков контроля доступа: RACL, VACL и QoS ACL

**Примечание:** Независимый от 512 пределов метки ACL, существует дополнительное ограничение ПО в CatOS Cisco 250 QoS на базе списков ACL в масштабе всей системы при использовании (двоичного) режима конфигурации по умолчанию. В текстовом режиме настройки это ограничение снимается. **Командой `set config mode text` можно изменить режим настройки на текстовый.** Текстовый режим обычно использует меньший объем энергонезависимой памяти или флеш-памяти по сравнению с двоичным режимом настройки. **При работе в текстовом режиме для сохранения конфигурации в энергонезависимой памяти необходимо выполнить команду `write memory`.** Командой `set config mode text auto-save` можно автоматически сохранить текстовую конфигурацию в энергонезависимой памяти.

Для проблемы с TCAM существует следующее обходное решение:

- Если на нескольких интерфейсах 2-го уровня, принадлежащих одной сети VLAN, действует команда `service-policy`, то можно реализовать применение политик на основе VLAN вместо применения политик на основе портов коммутатора. Ниже представлен пример:  

```
Switch(config)#interface range fastethernet x/y - Z
Switch(config-if)#mls qos vlan-based
Switch(config-if)#exit
Switch(config)#interface vlan 100
Switch(config-if)#service-policy input Test_Policy
```
- Отключение статистики маркировки QoS. Команда `no mls qos marking statistics` не допускает реализации максимального числа идентификаторов AgID — 1020. Поскольку она выделяет механизм применения политик по умолчанию для механизмов `set dscp`. Недостаток состоит в отсутствии статистики для конкретного механизма применения политик, поскольку все же используется механизм по умолчанию.  

```
Switch(config)#no mls qos marking statistics
```
- Можно попробовать использовать одни и те же списки управления доступом между разными интерфейсами, чтобы уменьшить конкуренцию за ресурсы TCAM.

## Ограничение NBAR

Средство распознавания приложений на основе сети (NBAR) представляет собой механизм классификации, который распознает широкий диапазон приложений, включая протоколы

WWW и другие сложно классифицируемые протоколы, использующие динамическое назначение портов TCP/UDP. После того как приложение определено и классифицировано с помощью средства NBAR, сеть может запускать службы для данного приложения. NBAR классифицирует пакеты и затем применяет QoS к классифицированному трафику, обеспечивая эффективное использование пропускной способности сети. При реализации QoS с использованием NBAR возникает ряд ограничений:

- Плата PFC3 не поддерживает NBAR.
- С модулем управления Supervisor Engine 2, платами PFC2 и MSFC2: Можно настроить NBAR на интерфейсах 3-го уровня вместо PFC QoS. Плата PFC2 реализует аппаратную поддержку входных списков ACL на портах LAN, на которых настроено средство NBAR. При включении QoS на плате PFC трафик через порты LAN, на которых настроено средство NBAR, проходит через входящую и исходящую очереди и пороги отбрасывания. При включении QoS на плате PFC плата MSFC2 устанавливает исходящий класс обслуживания (CoS) равным исходящему приоритету IP в трафике NBAR. После прохождения всего трафика через входную очередь трафик будет обрабатываться программным обеспечением платы MSFC2 на интерфейсах, для которых настроено средство NBAR.

## [Отсутствие команд cos-map в супервизоре Supervisor 2](#)

В выпусках ПО IOS основного режима, начиная с 12.1(8a)EX-12.1(8b)EX5 и 12.1(11b), привязки классов обслуживания QoS для магистральных гигабитных каналов на супервизоре Supervisor2 изменились. Все значения CoS назначены очереди 1 и порогу 1 и допускают изменения.

В следующих выпусках эти команды нельзя настроить на магистральном гигабитном порту Sup2:

```
rcv-queue cos-map priority-queue wrr-queue cos-map
```

Конфигурации QoS ограничены, и применять очередь со строгими приоритетами нельзя. Это затрагивает только гигабитные порты, физически расположенные на модуле Supervisor 2. Порты гигабита на других модулях линейных плат не затрагиваются.

Существует обновление микропрограммы, устраняющее эту проблему. Это обновление можно выполнить программным путем. При необходимости обновления микропрограммы обратитесь в службу технической поддержки. Обратите внимание, что обновление микропрограммы требуется, только если версия оборудования Supervisor2 ниже 4.0. В версиях оборудования Supervisor2 4.0 и выше применение QoS на гигабитных магистральных портах должно быть возможным без обновления микропрограммы. **Для определения уровня микропрограммы можно выполнить команду `show module`. [Эта проблема отмечена в описании идентификатора ошибки Cisco CSCdw89764 \(только для зарегистрированных пользователей\)](#).**

## [Ограничения команд service-policy](#)

Для применения карты политик к интерфейсу выполните команду `service-policy`. Если в карте политики имеется неподдерживаемая команда, то после ее применения посредством команды `service-policy` коммутатор выдаст на консоль сообщения об ошибках. При диагностике проблем, связанных с командой `service-policy`, необходимо обратить внимание



на следующие моменты.

- Не прикрепляйте политику обслуживания к порту, являющемуся членом EtherChannel.
- При установленных платах распределенной пересылки (DFC) плата PFC2 не поддерживает QoS на основе VLAN. **Нельзя выполнить команду `mls qos vlan-based` или прикрепить политики обслуживания к интерфейсам VLAN.**
- PFC QoS поддерживает ключевое слово `output` только с платой PFC3 и только на интерфейсах 3-го уровня (либо портах LAN, настроенных как интерфейсы 3-го уровня, либо интерфейсах VLAN). С платой PFC3 можно прикреплять к интерфейсу 3-го уровня как входную, так и выходную карты политик.
- Реализация QoS платой PFC на основе сетей VLAN или портов на портах 2-го уровня не относится к политикам, прикрепленным к интерфейсам 3-го уровня с ключевым словом `output`.
- Политики, прикрепленные с ключевым словом `output` не поддерживают применение политик для микропотоков.
- **Невозможно прикрепить карту политик, настраивающую доверенное состояние посредством выходных данных команды `service-policy`.**
- Реализация QoS на PFC не поддерживает снижение приоритета на входе с отбрасыванием на выходе или отбрасывание на входе со снижением приоритета на выходе.

### Выходные операторы `service-policy` отсутствуют в выходных данных команды `running-config`

При настройке QoS на мультиканале модуля FlexWan в выходных данных команды `show running-config` не видна команда `service-policy`. Это происходит в том случае, когда на коммутаторе применяется версия Cisco IOS старше 12.2SX. FlexWAN для серии Cisco 7600 поддерживает dLLQ на несвязанных интерфейсах. Он не поддерживает dLLQ на интерфейсах связки MLPPP. Такая поддержка доступна в выпуске ПО Cisco IOS 12.2S.

Способ обойти это ограничение — прикрепить политику обслуживания к несвязанным интерфейсам или модернизировать версию Cisco IOS до 12.2SX или новее, где данная функция поддерживается.

### Ограничение применения политик

Применение политик выполняется на плате PFC аппаратно и не влияет на производительность коммутатора. Применение политик невозможно на платформах 6500 без платы PFC. В гибридной операционной системе применение политик требует настройки на CatOS. При диагностике проблем, связанных с применением политик, необходимо обратить внимание на следующие моменты:

- В случае применения политик к одному и тому же трафику во входящем и исходящем направлениях выполнять снижение приоритета или отбрасывание трафика должны как входная, так и выходная политика. Реализация QoS на PFC не поддерживает снижение приоритета на входе с отбрасыванием на выходе или отбрасывание на входе со снижением приоритета на выходе.
- При настройке механизма применения политик, не использующего ключевое слово `pir`, с параметром `maximum_burst_bytes`, равным параметру `normal_burst_bytes` (эта ситуация

имеет место, если параметр `maximum_burst_bytes` не введен), ключевые слова `exceed-action policed-dscp-transmit` заставляют механизм QoS платы PFC понижать приоритет трафика согласно карте снижения приоритета `policed-dscp max-burst`.

- Если отбрасывание (drop) настроено в качестве действия по превышении предела, то механизм QoS платы PFC будет игнорировать настроенные действия для нарушения.
- Если отбрасывание (drop) настроено в качестве действия для соответствующих пакетов, то механизм QoS платы PFC настраивает отбрасывание как действие для пакетов, превышающих предел или нарушающих условия.
- Возможен конфликт между требованиями масок потоков между механизмами применения политик для микротоков, NetFlow и экспорта данных NetFlow (NDE).

## [Проблемы ограничения скорости или применения политик с платой MSFC в гибридной операционной системе](#)

На коммутаторах Catalyst 6500 под управлением гибридной операционной системы настройка ограничения скорости командой `rate-limit` не дает ожидаемого результата. Например, если команда `rate-limit` настроена в составе команды `interface vlan` на плате MSFC, то она фактически не вызывает ограничения скорости трафика.

```
interface Vlan10
  rate-limit input 256000 2000 2000 conform-action transmit exceed-action drop
  rate-limit output 256000 2000 2000 conform-action transmit exceed-action drop
```

Или:

```
interface Vlan10
  service-policy input Test_Policy
```

Причина состоит в том, что плата MSFC берет на себя только функции управления, а фактическая пересылка трафика осуществляется заказными микросхемами PFC на супервизоре. MSFC составляет информационную базу пересылки (FIB) и таблицы смежности, а также собирает другие сведения для управления и передает их плате PFC для аппаратной реализации. С созданной конфигурацией возможно ограничить скорость только программно коммутируемого трафика, но подобный трафик следует сводить к минимуму (или вовсе его избегать).

Обходное решение — настройка ограничения скорости на супервизоре при помощи интерфейса командной строки (CLI) системы CatOS. [Подробное объяснение настройки механизмов применения политики QoS в системе CatOS см. в разделе Средства QoS в CatOS. Можно обратиться к примеру конфигурации, представленному в документе Применение политик QoS на коммутаторах Catalyst серии 6500/6000.](#)

## [Команда `shape average` не поддерживается на интерфейсах VLAN маршрутизатора Cisco 7600](#)

При применении входной политики обслуживания к интерфейсу Cisco 7600 возникает сообщение об ошибке:

```
7600_1(config)#int Gi 1/40 7600_1(config-if)#service-policy input POLICY_1 shape average command
is not supported for this interface
```

Команда `shape average` для интерфейсов VLAN в Cisco 7600 не поддерживается. Вместо нее необходимо использовать механизмы применения политик.

```
7600_1(config)#policy-map POLICY_1 7600_1(config-pmap)#class TRAFFIC_1 7600_1(config-pmap-
```

```
c)#police <x> <y> conform-action transmit exceed-action drop
```

[Дополнительные сведения о реализации применения политик для ограничения скорости трафика см. в разделе Настройка политики для классов в карте политики.](#)

Поскольку политика обслуживания применяется к интерфейсу VLAN (SVI), то необходимо разрешить QoS на основе VLAN для портов 2-го уровня, принадлежащих этой сети VLAN, в которой должна применяться карта политик.

```
7600_1(config)#interface Gi 1/40 7600_1(config-if)#mls qos vlan-based
```

[Дополнительные сведения см. в документе Активация механизма QoS платы PFC на основе сетей VLAN на портах локальной сети 2-го уровня..](#)

## **ОШИБКА QoS: Addition/Modification made to policymap [строка] and class [строка] is not valid, command is rejected»**

```
QoS-ERROR: Addition/Modification made to policymap vtc-map and class voice-video is not valid, command is rejected
```

Это сообщение об ошибке указывает, что действия, определенные в упомянутом классе, не разрешены в коммутаторах Cisco Catalyst серии 6500. При настройке действий для класса в карте политик существует ряд ограничений.

- В классе карты политик нельзя выполнять одновременно три действия: **Маркировать трафик при помощи команд set** Настраивать доверенное состояние Настраивать применение политик **Можно либо маркировать трафик командами set. Или Настраивать состояние доверия и/или применение политик.**
- Для аппаратно коммутируемого трафика механизм QoS платы PFC не поддерживает команды класса в картах политик: **bandwidth, priority, queue-limit и random-detect.** Эти команды возможно настраивать, поскольку они могут использоваться для программно коммутируемого трафика.
- Механизм QoS платы PFC не поддерживает команды класса в картах политик **set qos-group.**

[Подробнее об этих ограничениях см. в разделе Настройка действий для класса в карте политик.](#)

## **Дополнительные сведения**

- [Классификация QoS и маркирование в коммутаторах Catalyst серии 6500/6000, использующих программное обеспечение Cisco IOS](#)
- [Диспетчеризация исходящих потоков с помощью службы QoS на коммутаторах Catalyst серий 6500/6000 под управлением системы Cisco IOS](#)
- [Применение политик QoS на коммутаторах Catalyst серии 6500/6000](#)
- [Классификация и маркировка QoS для коммутаторов Catalyst серии 6500/6000 с программным обеспечением CatOS](#)
- [Диспетчеризация выходных данных QoS для коммутаторов Catalyst серии 6500/6000 с программным обеспечением CatOS](#)
- [Страницы поддержки продуктов LAN](#)
- [Страница поддержки коммутационных решений для локальной сети](#)
- [Cisco Systems – техническая поддержка и документация](#)