Руководство по настройке
Конфигурация ACL и QoS
Ethernet-коммутаторы ЦОД серия QSW-7600

Оглавление

1. НАСТРОЙКА ACL

1.1. Обзор

Список контроля доступа (ACL) также называется списком доступа или брандмауэром. В некоторых документах это даже называется фильтрацией пакетов. ACL определяет правила, определяющие, следует ли пересылать или отбрасывать пакеты данных, прибывающие на интерфейс сети.

ACL классифицируются по функциям на два типа:

- Security ACL: используются для управления потоками данных, которым разрешено проходить через сетевое устройство.
- ACL качества обслуживания (QoS): используются для классификации и обработки потоков данных по приоритету.

ACL настраиваются по многим причинам. К основным причинам относятся:

- Контроль доступа к сети: для обеспечения сетевой безопасности определяются правила, ограничивающие доступ пользователей к некоторым службам (например, разрешен доступ только к WWW и службам электронной почты, а доступ к другим службам, таким как Telnet, запрещен) или пользователей для доступа к службам в указанный период времени, или разрешить доступ к сети только определенным хостам.
- QoS: ACL QoS используются для преимущественной классификации и обработки важных потоков данных. Дополнительные сведения об использовании ACL QoS см. в Настройка QOS.

1.2. Приложения

Приложение	Описание
Контроль доступа в корпоративной сети	В корпоративной сети права доступа к сети каждого отдела, например, права доступа к серверам и разрешения на использование средств общения (таких как QQ и MSN), должны контролироваться в соответствии с требованиями

1.2.1. Контроль доступа в корпоративной сети

1.2.1.1. Сценарий

Интернет-вирусы можно найти повсюду. Поэтому необходимо блокировать порты, которые часто используются вирусами, для обеспечения безопасности сети предприятия следующим образом:

- Разрешить доступ к серверу только внутренним ПК.
- Запретить компьютерам нефинансового отдела доступ к компьютерам финансового отдела и запретить компьютерам неисследовательских отделов доступ к компьютерам отдела исследований и разработок.
- Запретить сотрудникам отдела исследований и разработок использовать средства чата (такие как ICQ и Skype) в рабочее время с 09:00 до 18:00.

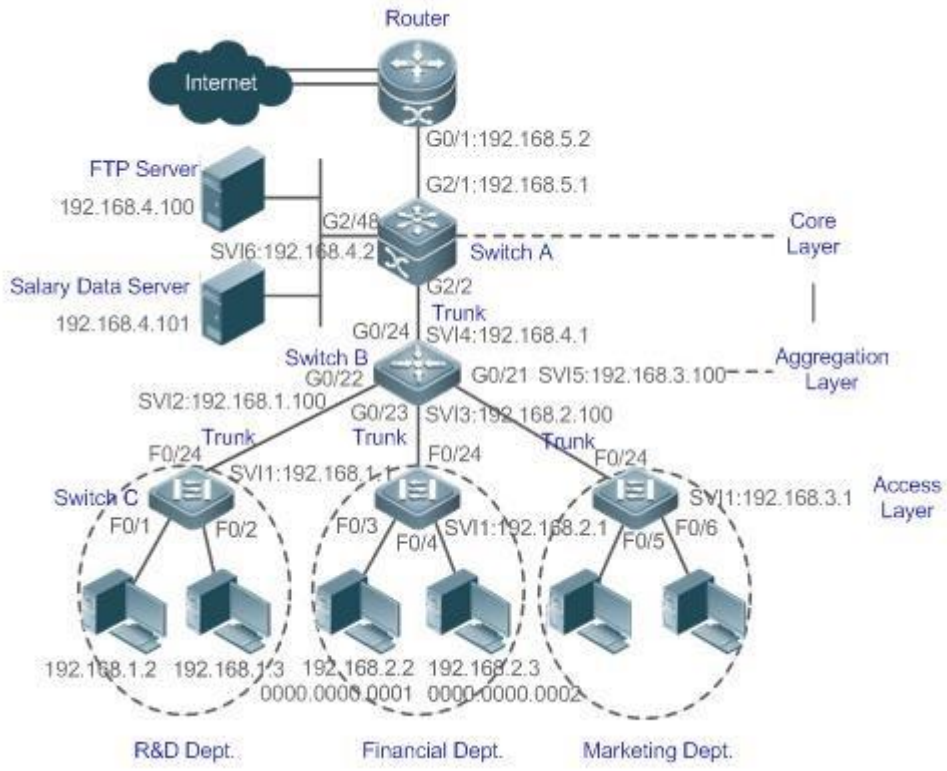

Рисунок 1-1.

Коммутатор C на уровне доступа: подключен к ПК каждого отдела и к коммутатору B на уровне агрегации через гигабитное оптоволокно (режим транка).

Коммутатор B на уровне агрегации: Несколько виртуальных локальных сетей (VLAN) разделены. Одна VLAN определена для одного отдела. Эти VLAN подключены к коммутатору A на уровне ядра через 10-гигабитное оптоволокно (режим транка).

Коммутатор A на уровне ядра: он подключен к различным серверам, таким как сервер File Transfer Protocol (FTP) и сервер Hypertext Transfer Protocol (HTTP), а также к Интернету через брандмауэры.

1.2.1.2. Развертывание

- Настройте расширенный ACL на порт G2/1 для фильтрации пакетов данных, тем самым защитив сеть от вирусов. Этот порт расположен на устройстве базового уровня (коммутатор A) и используется для подключения коммутатора A к uplink-порту G2/1 маршрутизатора.
- Разрешите доступ к серверам только внутренним ПК и запретите доступ к серверам внешним ПК. Определите и примените расширенные списки управления доступом (ACL) IP к G2/2 или виртуальному интерфейсу коммутатора (SVI) 2, который используется для подключения коммутатора A к устройству или серверу уровня агрегации.
- Запретите взаимный доступ между указанными отделами. Определите и примените расширенные списки контроля доступа IP на G0/22 и G0/23 коммутатора B.
- Настройте и примените расширенные IP ACL на основе времени на SVI 2 коммутатора B, чтобы запретить отделу исследований и разработок использовать средства чата (такие как ICQ и Skype) в течение определенного периода времени.

1.3. Функции

1.3.1. Основные понятия

1.3.1.1. ACL

ACL включают базовые ACL и динамические ACL.

При необходимости вы можете выбрать базовые или динамические ACL. Как правило, базовые списки ACL могут соответствовать требованиям безопасности. Однако опытные хакеры могут использовать определенное программное обеспечение для доступа к сети.с помощью подмены IP-адреса. Если используются динамические списки ACL, пользователям предлагается пройти идентификацию перед доступом к сети, что предотвращает вторжение хакеров в сеть. Таким образом, вы можете использовать динамические ACL в некоторых важных областях, чтобы гарантировать сетевую безопасность.

ПРИМЕЧАНИЕ: подмена IP-адреса — неотъемлемая проблема всех ACL-списков, включая динамические ACL-списки. Хакеры могут использовать поддельные IP-адреса для доступа к сети в течение срока действия аутентифицированных идентификаторов пользователей. Для решения этой проблемы доступны два метода. Один из них — установить меньшее время простоя доступа пользователя, что усложняет проникновение в сети. Другой — шифрование сетевых данных с использованием протокола IPSec, который гарантирует, что все данные будут зашифрованы при поступлении на устройство.

ACL обычно настраиваются на следующих сетевых устройствах:

- Устройства между внутренней сетью и внешней сетью (например, Интернет).
- Устройства на границе двух сегментов сети.
- Устройства, подключенные к контролируемым портам.

Утверждения ACL должны выполняться в строгом соответствии с их последовательностью в ACL. Сравнение начинается с первого утверждения. Как только заголовок пакета данных совпадает с утверждением в ACL, последующие утверждения игнорируются и больше не проверяются.

1.3.1.2. ACL ввода/вывода, шаблон поля фильтрации и правила

При получении пакета на интерфейсе устройство проверяет, соответствует ли пакет какой-либо записи управления доступом (ACE) во входном ACL этого интерфейса. Перед отправкой пакета через интерфейс устройство проверяет, соответствует ли пакет какому-либо ACE в выходном ACL этого интерфейса.

Когда определены разные правила фильтрации, все или только некоторые правила могут применяться одновременно. Если пакет соответствует ACE, этот пакет обрабатывается в соответствии с политикой действий (разрешить или запретить), определенной в этом ACE. ACE в ACL идентифицируют пакеты Ethernet на основе следующих полей в пакетах Ethernet:

Поля уровня 2 (L2):

- 48-битный MAC-адрес источника (содержащий все 48 бит).
- 48-битный MAC-адрес назначения (содержащий все 48 бит).
- 16-битное поле типа L2.
- Поля уровня 3 (L3).
- Поле исходного IP-адреса (можно указать все значения исходного IP-адреса или можно использовать подсеть для определения типа потоков данных).

- Поле IP-адреса назначения (можно указать все значения IP-адреса назначения или можно использовать подсеть для определения типа потоков данных).
- Поле типа протокола.
- Поля уровня 4 (L4).
- Указывается исходный или конечный порт TCP, либо оба, либо указан диапазон исходного или конечного порта.
- Указывается либо исходный порт UDP, либо порт назначения, либо оба, либо указан диапазон исходного или конечного порта.

Поля фильтрации относятся к полям в пакетах, которые можно использовать для идентификации или классификации пакетов при создании ACE. Шаблон поля фильтрации представляет собой комбинацию этих полей. Например, при создании ACE пакеты идентифицируются и классифицируются на основе поля IP-адреса назначения в каждом пакете; при создании другого ACE пакеты идентифицируются и классифицируются на основе поля исходного IP-адреса и поля исходного порта UDP в каждом пакете. Два ACE используют разные шаблоны полей фильтрации.

Правила относятся к значениям полей в шаблоне поля фильтрации ACE. Например, содержимое ACE выглядит следующим образом:

```
permit tcp host 192.168.12.2 any eq telnet
```

В этом ACE шаблон поля фильтрации представляет собой комбинацию следующих полей: поле исходного IP-адреса, поле IP-протокола и поле порта назначения TCP. Соответствующие значения (правила) следующие: исходный IP-адрес = Host 192.168.12.2; IP-протокол = TCP; Порт назначения TCP = Telnet.

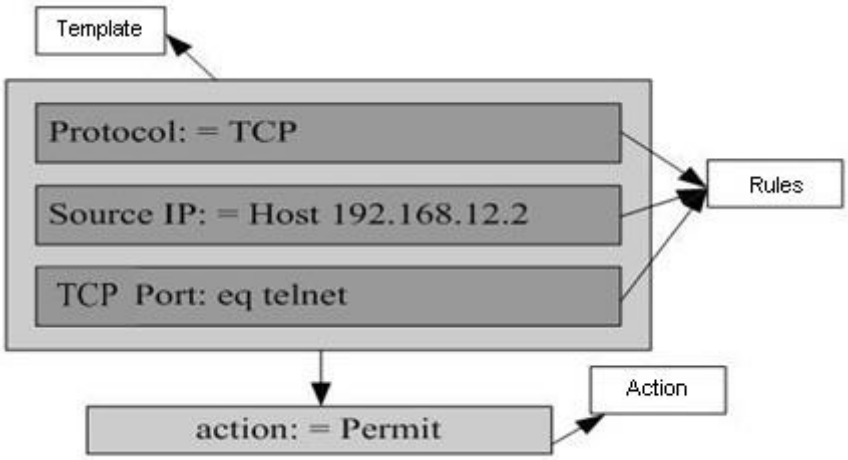

Рисунок 1-2. Анализ ACE: permit tcp host 192.168.12.2 any eq telnet

ПРИМЕЧАНИЯ:

- Шаблон поля фильтрации может быть комбинацией полей L3 и L4 или комбинацией нескольких полей L2. Однако шаблон поля фильтрации стандартного или расширенного ACL не может быть комбинацией полей L2 и L3, комбинацией полей L2 и L4 или комбинацией полей L2, L3 и L4. Чтобы использовать комбинацию полей L2, L3 и L4, вы можете использовать экспертные ACL.
- SVI, связанный со списками ACL в исходящем направлении, поддерживает стандартный IP, расширенный IP, расширенный MAC и экспертный ACL. Если расширенный MAC или экспертный ACL настроены на соответствие MAC-адресу назначения и применяется к исходящему направлении SVI, соответствующий ACE

можно настроить, но он не вступит в силу. Если настроен расширенный IP или экспертный ACL соответствует IP-адресу назначения, но IP-адрес назначения не входит в диапазон IP-адресов подсети связанного SVI, настроенный ACL не может вступить в силу. Например, предположим, что адрес VLAN 1 — **192.168.64.1 255.255.255.0**, создан расширенный IP-список ACL, и ACE — **deny udp any 192.168.65.1 0.0.0.255 eq 255**. Если этот ACL применяется к исходящему интерфейсу VLAN 1, ACL не может вступить в силу, поскольку IP-адрес назначения не находится в IP-адресе подсети диапазон VLAN 1. Если ACE имеет значение **deny udp any 192.168.64.1 0.0.0.255 eq 255**, ACL может вступить в силу, поскольку IP-адрес назначения находится в диапазоне IP-адресов подсети VLAN 1.

- На коммутаторе, если ACL применяются к исходящему направлению физического порта или агрегированного порта (AP), ACL могут фильтровать только хорошо известные пакеты (одноадресные или многоадресные пакеты), но не неизвестные одноадресные пакеты. То есть для неизвестных или широковещательных пакетов ACL, настроенные в исходящем направлении порта, не действуют.
- На коммутаторе, если входной ACL и DOT1X, глобальная привязка IP+MAC, port security и IP source guard являются общими для всех портов, разрешающие и запрещающие по умолчанию ACE не вступают в силу, но другие запрещающие ACE вступают в силу.
- На коммутаторе, если входной ACL и QoS совместно используются, разрешающие ACE не вступают в силу, вступают в силу другие запрещающие ACE, а запрещающие ACE по умолчанию вступает в силу после вступления в силу QoS ACE.
- На коммутаторе вы можете запустить команду **norgos-security compatible**, позволяющую разрешающим и запрещающим ACE вступать в силу одновременно, когда входной ACL и DOT1X на основе порта, глобальная привязка IP + MAC, port security и IP source guard используются совместно.
- Если ACE добавляются в ACL, а затем коммутатор перезапускается после применения ACL к входящему направлению нескольких SVI, ACL может не настроиться на некоторых SVI из-за ограниченной аппаратной емкости.
- Если экспертный ACL-список настроен и применяется к исходящему направлению интерфейса, а некоторые ACE в этом ACL-списке содержат информацию о соответствии L3 (например, IP-адрес и порт L4), non-IP-пакеты, отправляемые на устройство с этого интерфейса, не могут управлятся разрешающими и запрещающими ACE в этом ACL.
- Если ACE ACL (IP ACL или экспертный расширенный ACL) настроены на соответствие полям, отличных от L2 (таким как SIP и DIP), ACL не действует на тегированные пакеты MPLS.

Чтобы пользователи могли лучше изучать текущее состояние ACL на устройстве, вы можете определить, следует ли указывать параметр ведения журнала ACL как требуемый при добавлении ACE. Если указан этот параметр, журналы выводятся при обнаружении пакетов, соответствующих ACE. Журналы ACL отображаются на основе ACE. То есть устройство периодически отображает записи ACE с совпавшими пакетами и количество совпавших пакетов. Пример журнала выглядит следующим образом:

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

Чтобы контролировать количество журналов и частоту вывода, вы можете настроить интервал обновления журнала соответственно для ACL IPv4 и ACL IPv6.

ПРИМЕЧАНИЯ:

- ACE, содержащий параметр ведения журнала ACL, потребляет больше аппаратных ресурсов. Если все настроенные ACE содержат этот параметр, емкость ACE устройства будет уменьшена вдвое.
- По умолчанию интервал обновления журнала равен 0, то есть журнал не выводится. После указания параметра ведения журнала ACL в ACE необходимо настроить интервал обновления журнала для вывода соответствующих журналов.
- Для записи ACE, содержащей параметр ведения журнала ACL, если за указанный интервал не найдено ни одного пакета, журнал сопоставления пакетов, связанный с этой записью ACE, выводиться не будет. Если совпадающие пакеты будут найдены в указанном интервале, журналы сопоставления пакетов, относящиеся к этому ACE, будут выведены по истечении интервала. Количество совпадающих пакетов — это общее количество пакетов, соответствующих ACE в течение заданного интервала, то есть периода от предыдущего вывода журнала до текущего вывода журнала.
- Только коммутаторы поддерживают функцию ведения журнала ACL.

1.3.1.3. Счетчики сопоставления пакетов ACL

Для реализации управления сетью пользователям может потребоваться узнать, есть ли у ACE какие-либо совпадающие пакеты и сколько пакетов совпало. ACL предоставляют счетчики соответствия пакетов на основе ACE. Вы можете включить или отключить счетчики сопоставления пакетов для всех ACE в ACL, который может быть IP ACL, MAC ACL, экспертным ACL или IPv6 ACL. Кроме того, вы можете запустить команду **clear counters access-list** [*acl-id* | *acl-name*] для сброса счетчиков ACL для нового этапа статистики.

ПРИМЕЧАНИЯ:

- Для включения счетчиков ACL требуется больше аппаратных записей. В крайнем случае это сократит вдвое количество ACE, которые можно настроить на устройстве.
- Только коммутаторы поддерживают счетчики сопоставления пакетов ACL.

1.4. Обзор

Особенность	Описание
IP ACL	Контролируйте входящие или исходящие пакеты IPv4 устройства на основе информации L3 или L4 в заголовке пакета IPv4
Расширенный ACL MAC-адресов	Контролируйте входящие или исходящие пакеты L2 устройства на основе информации L2 в заголовке пакета Ethernet
Экспертный расширенный ACL	Объедините IP ACL и расширенный ACL MAC в экспертный расширенный ACL, который контролирует (разрешает или запрещает) входящие или исходящие пакеты устройства, используя одно и то же правило на основе информации L2, L3 и L4 в заголовке пакета

Особенность	Описание
IPv6 ACL	Контролируйте входящие или исходящие пакеты IPv6 устройства на основе информации L3 или L4 в заголовке пакета IPv6
ACL80	Настройте совпадающие поля и маску для сценариев, в которых фиксированные совпадающие поля не соответствуют требованиям
Перенаправление ACL	Перенаправить входящие пакеты устройства, соответствующие ACE, на указанный исходящий интерфейс
Глобальный Security ACL	Сделайте так, чтобы ACL действовал во входящем направлении всех интерфейсов вместо применения ACL к каждому интерфейсу
Канал безопасности	Разрешить пакетам обходить проверку приложений контроля доступа, таких как DOT1X и веб-аутентификация, для удовлетворения требований некоторых особых сценариев
ACL маршрутизатора SVI	Разрешить пользователям в одной VLAN общаться друг с другом
Ведение журнала ACL	Выводить журналы сопоставления пакетов ACL с заданным интервалом в соответствии с требованиями. Журналы помогают пользователям узнать результат сопоставления пакетов с указанным ACE

1.4.1. IP ACL

IP ACL реализует усовершенствованный контроль входящих и исходящих IPv4-пакетов устройства. Вы можете разрешить или запретить ввод определенных пакетов IPv4 в сеть в соответствии с фактическими требованиями для управления доступом IP-пользователей к сетевым ресурсам.

1.4.1.1. Принцип работы

Определите ряд правил IP-доступа в IP ACL, а затем примените IP ACL во входящем или исходящем направлении интерфейса или глобально. Устройство проверяет, соответствуют ли входящие или исходящие пакеты IPv4 правилам, и соответственно пересылает или блокирует эти пакеты.

Чтобы настроить IP ACL, необходимо указать уникальное имя или идентификатор для ACL протокола, чтобы протокол мог однозначно идентифицировать каждый ACL. В следующей таблице перечислены протоколы, которые могут использовать идентификаторы для идентификации ACL, и диапазон идентификаторов.

Протокол	Диапазон идентификаторов
Стандартный IP	1–99, 1300–1999
Расширенный IP	100–199, 2000–2699

Базовые списки ACL включают стандартные IP ACL и расширенные IP ACL. Стандартные правила, определенные в ACL, содержат следующие совпадающие поля:

- исходный IP-адрес;
- IP-адрес получателя;
- номер IP-протокола;
- идентификатор исходного порта L4 или тип ICMP;
- идентификатор порта назначения L4 или код ICMP.

Стандартный IP ACL (диапазон идентификаторов: 1–99, 1300–1999) используется для пересылки или блокировки пакетов на основе исходного IP-адреса, тогда как расширенный IP ACL (диапазон идентификаторов: 100–199, 2000–2699) используется для пересылки или блокировки пакетов на основе комбинации предыдущих совпадающих полей.

Для отдельного ACL можно использовать несколько независимых правил ACL для определения нескольких правил. Все правила ссылаются на один и тот же идентификатор или имя, поэтому эти операторы связаны одним и тем же ACL. Однако большее количество правил означает, что становится все труднее читать и понимать ACL.

ПРИМЕЧАНИЕ: для продуктов маршрутизации поле сопоставления кода ICMP в правиле ACL не действует для пакетов ICPM, тип ICPM которых равен 3. Если код ICPM для сопоставляемых пакетов ICMP настроен в правиле ACL, результат сопоставления ACL для входящих пакетов ICMP устройства, у которого тип ICPM 3, может отличаться от ожидаемого результата.

1.4.1.2. Скрытое правило «Запретить весь трафик»

В конце каждого IP ACL находится скрытое правило «запретить весь трафик». Следовательно, если пакет не соответствует какому-либо правилу, пакет будет отклонен.

Например:

```
access-list 1 permit host 192.168.4.12
```

Этот ACL разрешает только пакеты, отправленные с хоста-источника 192.168.4.12, и запрещает пакеты, отправленные со всех других хостов. Это связано с тем, что в конце этого ACL находится следующее правило: список доступа 1 запрещает все.

Если ACL содержит только следующую инструкцию:

```
access-list 1 deny host 192.168.4.12
```

Пакеты, отправленные с любого хоста, будут отклонены при прохождении через этот порт.

ПРИМЕЧАНИЕ: при определении ACL необходимо учитывать пакеты обновлений маршрутизации. Поскольку в конце ACL существует скрытое правило «запретить весь трафик», все пакеты обновления маршрутизации могут быть заблокированы.

1.4.1.3. Входная последовательность правил

Каждое новое правило добавляется в конец ACL и перед правилом по умолчанию. Входная последовательность правил ACL очень важна. Он определяет приоритет каждого

оператора в ACL. При принятии решения о пересылке или блокировке пакетов, устройство сравнивает пакеты с правилами на основе последовательности, в которой создаются правила. После обнаружения совпадающего правила устройство не проверяет другие правила.

Если правило создано и запрещает весь трафик, все последующие правила не будут проверяться.

Например:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255 eq telnet any
```

Первое правило запрещает все IP-пакеты. Поэтому пакеты Telnet от хоста в сети 192.168.12.0/24 будут отклонены. После того, как устройство обнаружит, что пакеты соответствуют первому правилу, оно больше не проверяет последующие утверждения правила.

1.4.1.4. Связанная конфигурация

Настройка IP ACL

По умолчанию на устройстве не настроен IP ACL.

Запустите команду **ip access-list** { **standard** | **extended** } {*acl-name* | *acl-id*} в режиме глобальной конфигурации, чтобы создать стандартный или расширенный IP ACL и войти в стандартный или расширенный режим IP ACL.

Добавление ACE в IP ACL

По умолчанию вновь созданный IP ACL содержит скрытый ACE, запрещающий все пакеты IPv4. Этот ACE скрыт от пользователей, но вступает в силу, когда ACL применяется к интерфейсу. То есть все пакеты IPv4 будут отброшены. Поэтому, если вы хотите, чтобы устройство получало или отправляло определенные пакеты IPv4, добавьте несколько ACE в ACL.

Для стандартного IP ACL добавьте ACE следующим образом:

- Независимо от того, является ли стандартный IP ACL именованным или числовым ACL, вы можете запустить следующую команду в стандартном режиме IP ACL, чтобы добавить ACE:

[*sn*] **{ permit** | **deny** } {**host** *source*| **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]

- Для нумерованного стандартного IP ACL вы также можете запустить следующую команду в режиме глобальной конфигурации, чтобы добавить ACE:

access-list *acl-id* { **permit** | **deny** } {**host** *source*| **any** | *source source-wildcard* } [**time-range** *tm-rng-name*][**log**]

- Для расширенного IP ACL вы можете добавить записи ACE следующим образом:
- Независимо от того, является ли расширенный IP ACL именованным или нумерованным, вы можете запустить следующую команду в режиме расширенного IP ACL, чтобы добавить ACE:

[*sn*] { **permit** | **deny** } *protocol*{**host** *source*| **any** | *source source-wildcard* } {**host** *destination*| **any** | *destination destination-wildcard* }[[[**precedence** *precedence*] [**tos** *tos*]] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**time-range** *time-range-name*] [**log**]

- Для нумерованного расширенного IP ACL вы также можете запустить следующую команду в режиме глобальной конфигурации, чтобы добавить ACE:

access-list *acl-id* { **permit** | **deny** } *protocol*{**host** *source*| **any** | *source source-wildcard* } {**host** *destination*| **any** | *destination destination-wildcard* }[[[**precedence** *precedence*] [**tos** *tos*]] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**timerange** *time-range-name*] [**log**]

Применение IP ACL

По умолчанию IP ACL не применяется ни к какому интерфейсу, то есть IP ACL не фильтрует входящие и исходящие IP-пакеты устройства.

Запустите команду **ip access-group** { *acl-id* | *acl-name* } { **in**| **out** } в режиме настройки интерфейса для применения стандартного или расширенного IP ACL к указанному интерфейсу.

1.4.2. Расширенный ACL MAC-адресов

Расширенный ACL MAC реализует усовершенствованный контроль над входящими и исходящими пакетами на основе заголовков L2 пакетов. Вы можете разрешать или запрещать вход определенных пакетов L2 в сеть, тем самым защищая сетевые ресурсы от атак или контролируя доступ пользователей к сетевым ресурсам.

1.4.2.1. Принцип работы

Определите серию правил доступа MAC в расширенном ACL MAC, а затем примените ACL к входящему или исходящему направлению интерфейса. Устройство проверяет, соответствуют ли входящие или исходящие пакеты правилам, и соответственно пересылает или блокирует эти пакеты.

Чтобы настроить расширенный ACL MAC, необходимо указать уникальное имя или идентификатор для этого ACL, чтобы однозначно идентифицировать ACL. В следующей таблице перечислены диапазоны идентификаторов, которые идентифицируют расширенные ACL MAC.

Протокол	Диапазон идентификаторов
Расширенный ACL MAC	700–799

Типичные правила, определенные в расширенном ACL MAC, включают:

- исходный MAC-адрес;
- MAC-адрес назначения;
- тип протокола Ethernet.

Расширенный ACL MAC (диапазон идентификаторов: 700–799) используется для фильтрации пакетов на основе MAC-адреса источника или получателя и типа Ethernet в пакетах.

Для отдельного расширенного ACL MAC можно использовать несколько независимых правил ACL для определения нескольких правил. Все правила ссылаются на один и тот же идентификатор или имя, поэтому эти правила связаны одним и тем же ACL. Однако большее количество правил означает, что становится все труднее читать и понимать ACL.

ПРИМЕЧАНИЕ: если ACE в расширенном ACL MAC не определены специально для пакетов IPv6, то есть тип Ethernet не указан или значение поля типа Ethernet не равно 0x86dd, расширенный ACL MAC не фильтрует пакеты IPv6. Если вы хотите фильтровать пакеты IPv6, используйте расширенный ACL IPv6.

1.4.2.2. Скрытое правило «Запретить весь трафик»

В конце каждого расширенного ACL MAC находится скрытое правило «запретить весь трафик». Следовательно, если пакет не соответствует какому-либо правилу, пакет будет отклонен.

Например:

```
access-list 700 permit host 08c6.b300.0001 any
```

Этот ACL разрешает только пакеты от хоста с MAC-адресом 08c6.b300.0001 и запрещает пакеты от всех остальных хостов. Это связано с тем, что в конце этого ACL находится следующее правило: **access-list 700 deny any any**.

1.4.2.3. Связанная конфигурация

Настройка расширенного ACL MAC

По умолчанию на устройстве не настроен расширенный ACL MAC.

Запустите команду **mac access-list extended {***acl-name* **| acl-id }** в режиме глобальной конфигурации для создания расширенного ACL MAC и перехода в режим расширенного ACL MAC.

Добавление ACE в расширенный ACL MAC

По умолчанию вновь созданный расширенный ACL MAC содержит скрытый ACE, запрещающий все пакеты L2. Этот ACE скрыт от пользователей, но вступает в силу, когда ACL применяется к интерфейсу. То есть все пакеты L2 будут отброшены. Поэтому, если вы хотите, чтобы устройство получало или отправляло определенные пакеты L2, добавьте несколько ACE в ACL.

Вы можете добавить ACE в расширенный ACL MAC следующим образом:

- Независимо от того, является ли расширенный ACL MAC именованным или нумерованным ACL, вы можете выполнить следующую команду в режиме расширенного ACL MAC, чтобы добавить ACE:

[*sn*]{ **permit** |**deny** }{**any**|**host** *src-mac-addr*}{**any**|**host** *dst-mac-addr*}[*ethernet-type*][**cos** *cos*] [**inner** *cos*] [**time-range** *tm-rng-name*]

- Для расширенного ACL с нумерованным MAC-адресом вы также можете запустить следующую команду в режиме глобальной конфигурации, чтобы добавить ACE:

access-list *acl-id*{ **permit** |**deny** }{**any**|**host** *src-mac-addr*}{**any**|**host** *dst-mac-addr*}[*ethernet-type*][**cos** *cos*] [**inner** *cos*] [**time-range** *time-range-name*]

Применение расширенного ACL MAC

По умолчанию расширенный ACL MAC не применяется ни к какому интерфейсу, то есть созданный расширенный ACL MAC не фильтрует входящие или исходящие пакеты L2 устройства.

Запустите команду **mac access-group** { *acl-id* | *acl-name* } { **in**| **out** } в режиме конфигурации интерфейса для применения расширенного ACL MAC к указанному интерфейсу.

1.4.3. Экспертный расширенный ACL

Вы можете создать экспертный расширенный ACL для сопоставления информации L2 и L3 в пакетах, используя одно и то же правило. Экспертный расширенный ACL можно рассматривать как комбинацию и расширение IP ACL и расширенного ACL MAC, потому что экспертный расширенный ACL может содержать ACE как в IP ACL, так и в расширенном ACL MAC. Кроме того, VLAN ID можно указать в расширенном экспертном ACL для фильтрации пакетов.

1.4.3.1. Принцип работы

Определите ряд правил доступа в экспертном расширенном ACL, а затем примените ACL во входящем или исходящем направлении интерфейса. Устройство проверяет, соответствуют ли входящие или исходящие пакеты правилам, и соответственно пересылает или блокирует эти пакеты.

Для настройки экспертного расширенного ACL необходимо указать уникальное имя или идентификатор для этого ACL, чтобы протокол мог однозначно идентифицировать каждый ACL. В следующей таблице перечислены диапазоны идентификаторов расширенного экспертного ACL.

Протокол	Диапазон идентификаторов
Экспертный расширенный ACL	2700–2899

Когда создается экспертный расширенный ACL, определенные правила могут применяться ко всем пакетам. Устройство определяет, следует ли пересылать или блокировать пакеты, проверяя, соответствуют ли пакеты этим правилам.

Типичные правила, определенные в экспертном расширенном ACL, включают:

- вся информация в базовом ACL и расширенном ACL MAC;
- идентификатор VLAN.

Экспертный расширенный ACL (диапазон идентификаторов: 2700–2899) представляет собой комбинацию базового ACL и расширенного ACL MAC и может фильтровать пакеты на основе идентификатора VLAN.

Для отдельного расширенного экспертного ACL можно использовать несколько независимых правил для определения нескольких правил. Все правила ссылаются на один и тот же идентификатор или имя, поэтому эти правила связаны одним и тем же ACL.

ПРИМЕЧАНИЕ: если правила в экспертном расширенном ACL не определены специально для пакетов IPv6, то есть не указан тип Ethernet или значение поля типа Ethernet не равно 0x86dd, экспертный расширенный ACL не фильтрует пакеты IPv6. Если вы хотите фильтровать пакеты IPv6, используйте расширенный ACL IPv6.

ПРИМЕЧАНИЕ: поле UDF в экспертном расширенном ACL продукта центра обработки данных является настраиваемым полем. Пользователи должны настроить уровень протокола, смещение (offset), данные и маску.

1.4.3.2. Скрытое правило «Запретить весь трафик»

В конце каждого экспертного расширенного ACL находится скрытое правило «запретить весь трафик». Следовательно, если пакет не соответствует какому-либо правилу, пакет будет отклонен.

Например:

```
access-list 2700 permit 0x0806 any any any any any
```

Этот ACL разрешает только пакеты ARP с типом Ethernet 0x0806 и запрещает все другие типы пакетов. Это связано с тем, что в конце этого списка ACL существует следующий оператор: **access-list 2700 deny any any any any**.

1.4.3.3. Связанная конфигурация

Настройка экспертного расширенного ACL

По умолчанию на устройстве не настроен расширенный экспертный ACL.

Запустите команду **expert access-list extended** {*acl-name* | *acl-id* } в режиме глобальной конфигурации для создания экспертного расширенного ACL и входа в экспертный расширенный ACL-режим.

Добавление ACE в расширенный экспертный ACL

По умолчанию вновь созданный экспертный расширенный ACL содержит скрытый ACE, запрещающий все пакеты. Этот ACE скрыт от пользователей, но вступает в силу, когда ACL применяется к интерфейсу. То есть все пакеты L2 будут отброшены. Поэтому, если вы хотите, чтобы устройство получало или отправляло определенные пакеты L2, добавьте несколько ACE в ACL.

Вы можете добавить ACE в расширенный экспертный ACL следующим образом:

- Независимо от того, является ли расширенный экспертный ACL именованным или пронумерованным, вы можете запустить следующую команду в режиме расширенного экспертного ACL, чтобы добавить ACE:

[*sn*]{ **permit** |**deny** }[*protocol*| [*ethernet-type*][**cos**[*out*] [**inner** *in*]]] [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** source | **any**}{**host** *source-mac-address*|**any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [[**precedence** *precedence*][**tos** *tos*] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**range** *lowerupper*] [[**udf** *udf-id header pos value mask*] | [**int-flag**]] [**time-range** *time-range-name*]]

- Для нумерованного расширенного экспертного ACL вы также можете запустить следующую команду в режиме экспертного расширенного ACL, чтобы добавить ACE:

access-list *acl-id*{ **permit** |**deny** }[*protocol*| [*ethernet-type*][**cos**[*out*] [**inner** *in*]]] [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host** *source* | **any**}{**host** *source-mac-address*|**any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [[**precedence** *precedence*][**tos** *tos*] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**range** *lowerupper*] [[**udf** *udf-id header pos value mask*] | [**int-flag**]] [**time-range** *time-range-name*]]

Применение экспертного расширенного ACL

По умолчанию экспертный расширенный ACL не применяется ни к одному интерфейсу, то есть созданный экспертный расширенный ACL не фильтрует входящие или исходящие пакеты L2 или L3 устройства.

Запустите команду **expert access-group** { *acl-id* | *acl-name* } { **in**| **out** } в режиме настройки интерфейса, чтобы применить экспертный расширенный ACL к указанному интерфейсу.

1.4.4. IPv6 ACL

ACL IPv6 реализует усовершенствованный контроль над входящими и исходящими пакетами IPv6 устройства. Вы можете разрешить или запретить ввод определенных пакетов IPv6 в сеть в соответствии с фактическими требованиями для контроля доступа пользователей IPv6 к сетевым ресурсам.

1.4.4.1. Принцип работы

Определите ряд правил доступа IPv6 в ACL IPv6, а затем примените ACL во входящем или исходящем направлении интерфейса. Устройство проверяет, соответствуют ли входящие или исходящие пакеты IPv6 правилам, и соответственно пересылает или блокирует эти пакеты.

Чтобы настроить ACL IPv6, вы должны указать уникальное имя для этого ACL.

ПРИМЕЧАНИЕ: в отличие от IP ACL, расширенного ACL MAC и экспертного расширенного ACL, вы можете указать только имя, но не идентификатор для созданного ACL IPv6.

ПРИМЕЧАНИЕ: только один IP ACL, или один расширенный ACL MAC, или один экспертный расширенный ACL может быть применен к входящему или исходящему направлению интерфейса. Кроме того, можно применить еще один ACL IPv6.

1.4.4.2. Скрытое правило «Запретить весь трафик»

В конце каждого списка ACL IPv6 находится скрытое правило «запретить весь трафик IPv6». Следовательно, если пакет не соответствует какому-либо правилу, пакет будет отклонен.

Например:

```
ipv6 access-list ipv6_acl
10 permit ipv6 host 200::1 any
```

Этот ACL разрешает только пакеты IPv6 от хоста-источника 200::1 и запрещает пакеты IPv6 от всех остальных хостов. Это связано с тем, что в конце этого списка управления доступом есть следующее правило: **deny ipv6 any any**.

Хотя список управления доступом IPv6 по умолчанию содержит скрытое правило «запретить весь трафик IPv6», он не фильтрует пакеты ND.

1.4.4.3. Входная последовательность правил

Каждое новое правило добавляется в конец ACL и перед оператором правила по умолчанию. Входная последовательность операторов в ACL очень важна. Он определяет приоритет каждого оператора в ACL. При определении того, следует ли пересылать или блокировать пакеты, устройство сравнивает пакеты с правилами на основе последовательности, в которой создаются операторы правил. После обнаружения совпадающего оператора правила устройство не проверяет другие операторы правила.

Если оператор правила создан и разрешает весь трафик IPv6, все последующие операторы не будут проверяться.

Например:

```
pv6 access-list ipv6_acl
10 permit ipv6 any any
20 deny ipv6 host 200::1 any
```

Поскольку первое утверждение правила разрешает все пакеты IPv6, все пакеты IPv6, отправленные с хоста 200::1, не соответствуют последующему правилу отказа с порядковым номером 20 и, следовательно, не будут отклонены. После того, как устройство обнаружит, что пакеты соответствуют первому утверждению правила, оно больше не проверяет последующие утверждения правила.

1.4.4.4. Связанная конфигурация

Настройка ACL IPv6

По умолчанию на устройстве не настроен ACL IPv6.

Запустите команду **ipv6 access-list** *acl-name* в режиме глобальной конфигурации, чтобы создать ACL IPv6 и войти в режим ACL IPv6.

Добавление ACE в ACL IPv6

По умолчанию вновь созданный ACL IPv6 содержит неявный ACE, запрещающий все пакеты IPv6. Этот ACE скрыт от пользователей, но вступает в силу, когда ACL применяется к интерфейсу. То есть все пакеты IPv6 будут отброшены. Поэтому, если вы хотите, чтобы

устройство получало или отправляло определенные пакеты IPv6, добавьте несколько записей ACE в ACL.

Выполните следующую команду в режиме IPv6 ACL, чтобы добавить ACE:

[*sn*] {**permit** | **deny** }*protocol*{*src-ipv6-prefix*/*prefix-len*|**host** *src-ipv6-addr*| **any**}{*dst-ipv6-pfix*/*pfix-len*|**host** *dst-ipv6-addr*|**any**} [**range** *lower upper*] [**dscp** *dscp*][**flow-label** *flow-label*][**fragment**][**time-range** *tm-rng-name*] [**log**]

Применение ACL IPv6

По умолчанию ACL IPv6 не применяется ни к одному интерфейсу, то есть список ACL IPv6 не фильтрует входящие и исходящие пакеты IPv6 устройства.

Запустите команду **ipv6 traffic-filter** *acl-name* { **in| out** } в режиме конфигурации интерфейса для применения ACL IPv6 к указанному интерфейсу.

1.4.5. ACL80

ACL80 относится к экспертному расширенному ACL и также называется пользовательским ACL. Он фильтрует пакеты на основе первых 80 байтов каждого пакета. Среди этих 80 байт поля SMAC, DMAC, SIP, DIP и ETYPE в пакете являются обязательными, а остальные 16 байтов можно указать.

1.4.5.1. Принцип работы

Пакет состоит из нескольких байтов. ACL80 позволяет сопоставлять указанные 16 байтов по битам в первых 80 байтах пакета. Любой бит 16-байтового поля может быть установлен в значение (0 или 1), указывающее, сравнивается ли бит. При фильтрации любого байта учитываются три фактора: содержимое совпадающего поля, маска совпадающего поля и начальная позиция для сопоставления. Биты содержимого совпадающего поля находятся во взаимно однозначном отношении отображения с битами маски совпадающего поля. Правило фильтрации указывает значение фильтруемого поля. Шаблон поля фильтрации указывает, следует ли фильтровать соответствующее поле в правиле фильтрации. (1 указывает, что бит, указанный в правиле фильтрации, должен совпадать; 0 указывает, что бит, указанный в правиле фильтрации, не соответствует.) Следовательно, когда требуется соответствие определенному биту, вы должны установить соответствующий бит в 1 в шаблоне поля фильтрации. Например, если бит установлен в 0 в шаблоне поля фильтрации, ни один бит не соответствует независимо от того, какой бит указан в правиле фильтрации.

Например,

```
QTECH(config)#expert access-list advanced name
QTECH(config-exp-dacl)#permit 08c6b3123456 fffffffffff 0
QTECH(config-exp-dacl)#deny 08c6b3654321 fffffffffff 6
```

Пользовательский ACL сопоставляет любой байт из первых 80 байтов в кадре данных L2 в соответствии с определением пользователя и соответствующим образом фильтрует пакеты. Чтобы правильно использовать пользовательский ACL, вы должны иметь глубокое понимание структуры фрейма данных L2. Ниже показаны первые 64 байта кадра данных L3 (каждая буква представляет собой шестнадцатеричное число, а каждые две буквы представляют один байт):

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

В следующей таблице описано значение и смещение каждой буквы:

Буква	Значение	Смещение	Буква	Значение	Смещение
A	MAC-адрес назначения	0	O	Поле «Time To Live» (TTL)	34
B	Исходный MAC-адрес	6	P	Номер протокола	35
C	Поле тега VLAN	12	Q	IP checksum	36
D	Длина кадра данных	16	R	Исходный IP-адрес	38
E	Поле «Destination service access point» (DSAP)	18	S	IP-адрес получателя	42
F	Поле Source service access point (SSAP)	19	T	TCP-порт источника	46
G	Поле Cntl	20	U	Порт назначения TCP	48
H	Поле Org Code	21	V	Серийный номер	50
I	Инкапсулированный тип данных	24	Wт	Поле подтверждения	54
J	Номер версии IP	26	XY	Длина заголовка IP и зарезервированный бит	58
K	Поле TOS	27	Z	Зарезервированный бит и бит флагов	59
L	Длина IP-пакета	28	a	Поле размера окна	60
M	ID	30	b	Разнообразный	62
N	Поле флагов	32			

В приведенной выше таблице смещение каждого поля — это смещение этого поля в тегированном пакете 802.3 SNAP. В пользовательском ACL вы можете использовать маску

правила и смещение вместе, чтобы извлечь любой байт из первых 80 байтов кадра данных, сравнить байт с правилом, настроенным в ACL, а затем отфильтровать совпадающие кадры данных для дальнейшей обработки. Индивидуальные правила могут быть некоторыми фиксированными атрибутами данных. Например, чтобы получить все пакеты TCP, вы можете определить правило как «06», маску правила как «FF» и смещение как «35». Затем устройство может совместно использовать маску правила и смещение для извлечения содержимого поля номера протокола TCP в полученном кадре данных и сравнения извлеченного содержимого с правилом для получения всех пакетов TCP.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают ACL80.

ПРИМЕЧАНИЕ: ACL80 поддерживает фильтрацию пакетов Ethernet, 803.3 SNAP и 802.3 LLC. Если значения полей от DSAP до cntl установлены на AAAA03, ACL используется для фильтрации пакетов SNAP 803.3. Если значения полей от DSAP до cntl установлены на E0E003, ACL используется для фильтрации пакетов 803.3 LLC. Значение поля cntl нельзя настроить для фильтрации пакетов Ethernet.

ПРИМЕЧАНИЕ: ACL80 можно настроить для сравнения пакетов с любым из 16 байтов. Если 16 байтов уже используются, нельзя настроить ACE для сравнения пакетов с полями в любых других байтах.

1.4.5.2. Связанная конфигурация

Настройка экспертного расширенного ACL

По умолчанию экспертный расширенный ACL не настроен на устройстве.

Запустите команду **expert access-list advanced** *acl-name* в режиме глобальной конфигурации, чтобы создать экспертный расширенный ACL и войти в экспертный расширенный режим ACL.

Добавление записей ACE в экспертный расширенный список ACL

По умолчанию вновь созданный экспертный расширенный ACL содержит скрытое правило ACE, запрещающую все пакеты. Этот ACE скрыт от пользователей, но вступает в силу, когда ACL применяется к интерфейсу. То есть все пакеты L2 будут отброшены. Поэтому, если вы хотите, чтобы устройство получало или отправляло определенные пакеты L2, добавьте несколько записей ACE в ACL.

- Запустите команду [*sn*] { **permit** | **deny** } *hex hex-mask offset* в экспертном расширенном режиме ACL, чтобы добавить ACE в экспертный расширенный ACL.

Применение экспертного расширенного ACL

По умолчанию экспертный расширенный ACL не применяется ни к какому интерфейсу, то есть созданный экспертный расширенный ACL не фильтрует входящие или исходящие пакеты устройства.

Запустите команду **expert access-group** *acl-name* { **in**| **out** } в режиме конфигурации интерфейса, чтобы применить экспертный расширенный ACL к указанному интерфейсу.

1.4.6. Перенаправление ACL

Перенаправление ACL позволяет устройству анализировать полученные пакеты и перенаправлять пакеты на указанный порт для пересылки. Чтобы анализировать определенные входящие пакеты устройства, вы можете настроить функцию перенаправления ACL для перенаправления пакетов, отвечающих правилам, на указанный порт и захвата пакетов на этом порту для анализа.

1.4.6.1. Принцип работы

Привяжите другую политику ACL к интерфейсу и укажите выходной целевой интерфейс для каждой политики. При приеме пакетов на этот интерфейс устройство последовательно ищет политики ACL, привязанные к этому интерфейсу. Если пакеты соответствуют критериям, описанным в определенной политике, устройство перенаправляет пакеты на интерфейс назначения, указанный в политике, тем самым перенаправляя пакеты на основе трафика.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают функцию перенаправления ACL.

ПРИМЕЧАНИЕ: перенаправление ACL действует только во входящем направлении интерфейса.

1.4.6.2. Связанная конфигурация

Настройка ACL

Прежде чем настраивать перенаправление ACL, настройте ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Подробнее о том, как добавлять записи ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Настройка перенаправления ACL

По умолчанию перенаправление ACL на устройстве не настроено.

Запустите команду **redirect destinationinterface** *interface-name* **acl** {*acl-id* | ***acl-name*** } **in** в режиме конфигурации интерфейса для настройки перенаправления ACL.

ПРИМЕЧАНИЕ: функцию перенаправления ACL можно настроить только на интерфейсе Ethernet или точке доступа.

1.4.7. Глобальный Security ACL

Чтобы соответствовать требованиям развертывания безопасности, ACL на основе портов часто настраивается на фильтрацию вирусных пакетов и получение пакетов с определенными характеристиками, например, пакетов, атакующих TCP-порт. В глобальной сетевой среде существуют различные вирусные пакеты, и признаки идентификации вирусных пакетов на каждом порту идентичны или схожи. Поэтому обычно создается ACL. После добавления в ACL запрещающего ACE для сопоставления вирусных сигнатур список ACL на основе портов применяется к каждому порту коммутатора для фильтрации вирусных пакетов.

Неудобно использовать ACL на основе портов в антивирусных сценариях, таким как фильтрация вирусов, по двум причинам. Первая причина заключается в том, что ACL на основе портов необходимо настроить для каждого порта, что приводит к повторяющейся настройке, низкой производительности операций и чрезмерному потреблению ресурсов ACL. Вторая причина заключается в том, что функция управления доступом ACL ослаблена. Поскольку ACL на основе порта используется для фильтрации вирусов, основные функции ACL, такие как ограничение обновления маршрута и ограничение доступа к сети, не могут быть использованы должным образом. Глобальный Security ACL можно использовать для глобального развертывания и защиты от вирусов, не затрагивая ACL на основе портов. Запустив всего одну команду, вы можете заставить глобальный Security ACL действовать на всех интерфейсах L2. Напротив, ACL на основе порта должен быть настроен на каждом интерфейсе.

1.4.7.1. Принцип работы

Глобальный Security ACL действует на всех интерфейсах L2. Если настроены и глобальный Security ACL, и ACL на основе портов, вступают в силу оба. Пакеты, соответствующие глобальному Security ACL, напрямую отфильтровываются как вирусные пакеты. Пакеты, которые не соответствуют глобальному Security ACL, по-прежнему контролируются ACL на основе портов. Вы можете отключить глобальный Security ACL на некоторых портах, чтобы эти порты не контролировались глобальным Security ACL.

ПРИМЕЧАНИЕ: глобальный Security ACL в основном используется для фильтрации вирусов. Таким образом, в ACL, связанном с глобальным Security ACL, вступают в силу только записи ACE с запретом, а списки ACE с разрешениями не действуют.

ПРИМЕЧАНИЕ: в отличие от безопасного ACL, применяемого к порту, глобальный Security ACL не содержит ACE по умолчанию «запретить весь трафик», то есть разрешены все пакеты, не соответствующие ACL.

ПРИМЕЧАНИЕ: глобальный Security ACL может действовать как на порту L2, так и на маршрутизируемом порту. То есть он действует на все следующие типы портов: порт доступа, магистральный порт, порт hibird, маршрутизируемый порт и AP (L2 или L3). Глобальный Security ACL не влияет на SVI.

ПРИМЕЧАНИЕ: вы можете отключить глобальный Security ACL на отдельном физическом порту или AP, но не на порту-участнике AP. Глобальный защищенный ACL поддерживает только связанный стандартный ACL IP, расширенный ACL IP, расширенный ACL MAC и экспертный расширенный ACL.

1.4.7.2. Связанная конфигурация

Настройка ACL

Прежде чем настраивать глобальный Security ACL, настройте ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Дополнительные сведения о том, как добавить записи ACE в ACL, см. в предыдущих описаниях IP ACL.

Настройка Security ACL

По умолчанию на устройстве не настроен глобальный Security ACL.

Запустите команду {**ip |mac** |**Expert** } **access-group** *acl-id* { **in** | **out** } в режиме глобальной конфигурации, чтобы включить глобальный Security ACL.

Настройка эксклюзивного интерфейса глобального Security ACL

По умолчанию эксклюзивный интерфейс для глобального Security ACL на устройстве не настроен.

Запустите команду **no global ip access-group** в конфигурации интерфейса, чтобы отключить глобальный Security ACL на указанном интерфейсе.

1.4.8. Канал безопасности

В некоторых сценариях приложений пакеты, отвечающие некоторым характеристикам, могут нуждаться в обходе проверок приложений управления доступом. Например, перед проверкой подлинности DOT1X пользователям разрешается входить на указанный веб-сайт для загрузки клиента проверки подлинности DOT1X. Для этой цели можно использовать канал Security. Когда команда настройки канала Security выполняется для применения безопасного ACL глобально или к интерфейсу, этот ACL становится каналом Security.

1.4.8.1. Принцип работы

Канал безопасности также является ACL и может быть настроен глобально или для определенного интерфейса. При поступлении на интерфейс пакеты проверяются на канале безопасности. При соблюдении условий соответствия канала безопасности пакеты напрямую поступают на коммутатор без прохождения контроля доступа, такого как безопасность порта, веб-аутентификация, 802.1x и проверка IP-MAC binding. Глобально применяемый канал безопасности действует на всех интерфейсах, кроме эксклюзивных интерфейсов.

ПРИМЕЧАНИЕ: запрещающие ACE в ACL, который применяется к каналу безопасности, не вступают в силу. Кроме того, этот ACL не содержит скрытого правила «запретить весь трафик» в конце ACL. Если пакеты не соответствуют условиям соответствия канала безопасности, они проверяются по правилам управления доступом в соответствии с соответствующим процессом.

ПРИМЕЧАНИЕ: вы можете настроить до восьми эксклюзивных интерфейсов для глобального канала безопасности. Кроме того, на этих эксклюзивных интерфейсах нельзя настроить канал безопасности на основе интерфейса.

ПРИМЕЧАНИЕ: если канал безопасности применяется к интерфейсу, когда существует глобальный канал безопасности, этот глобальный канал безопасности не влияет на этот интерфейс.

ПРИМЕЧАНИЕ: если к интерфейсу применяются и режим мигрируемой аутентификации на основе порта, и канал безопасности, канал безопасности не действует.

ПРИМЕЧАНИЕ: ACL IPv6 нельзя настроить в качестве канала безопасности.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают безопасный канал.

1.4.8.2. Связанная конфигурация

Настройка ACL

Перед настройкой канала безопасности настройте ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Подробнее о том, как добавлять ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC или экспертного расширенного ACL.

Настройка канала безопасности на интерфейсе

По умолчанию на интерфейсе устройства не настроен канал безопасности.

Запустите командум **security access-group** {*acl-id* | ***acl-name*** } в режиме настройки интерфейса для настройки канала безопасности на интерфейсе.

Настройка глобального канала безопасности

По умолчанию на устройстве не настроен глобальный канал безопасности.

Запустите команду **security global access-group** {*acl-id* | ***acl-name*** } в режиме конфигурации интерфейса для настройки глобального канала безопасности.

Настройка эксклюзивного интерфейса для канала глобальной безопасности

По умолчанию эксклюзивный интерфейс для глобального канала безопасности на устройстве не настроен.

Запустите команду **security uplink enable** в режиме настройки интерфейса, чтобы настроить указанный интерфейс в качестве эксклюзивного интерфейса глобального канала безопасности.

1.4.9. ACL маршрутизатора SVI

По умолчанию ACL, применяемый к SVI, также влияет на пакеты L2, пересылаемые внутри VLAN, и пакеты L3, пересылаемые между VLAN. Следовательно, у пользователей в одной и той же VLAN может не получиться общаться друг с другом. Поэтому предусмотрен метод переключения, так что ACL, применяемый к SVI, действует только при маршрутизации пакетов между VLAN.

1.4.9.1. Принцип работы

По умолчанию функция ACL маршрутизатора SVI отключена, и ACL SVI действует на пакеты L3, пересылаемые между VLAN, и пакеты L2, пересылаемые внутри VLAN. После того как функция ACL маршрутизатора SVI включена, ACL SVI действует только на пакеты L3, пересылаемые между VLAN.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают ACL маршрутизатора SVI.

1.4.9.2. Связанная конфигурация

Настройка ACL

Перед настройкой ACL маршрутизатора SVI настройте и примените ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Подробнее о том, как добавлять ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Применение ACL

Дополнительные сведения о том, как применять ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6. Примените ACL в режиме конфигурации SVI.

Настройка ACL маршрутизатора SVI

Запустите команду **svi router-acls enable** в режиме глобальной конфигурации, чтобы включить ACL маршрутизатора SVI, чтобы ACL, применяемый к SVI, действовал только на пакеты, пересылаемые на L3, а не на пакеты, пересылаемые на L2 внутри VLAN.

1.4.10. Ведение журнала ACL

Ведение журнала ACL используется для отслеживания текущего состояния ACE в ACL и предоставления необходимой информации для планового обслуживания, и оптимизации сети.

1.4.10.1. Принцип работы

Чтобы лучше узнать текущее состояние списков ACL на устройстве, вы можете указать, следует ли указывать параметр ведения журнала ACL при добавлении ACE. Если указан этот параметр, журналы выводятся при обнаружении пакетов, соответствующих ACE. Журналы ACL отображаются на основе ACE. То есть устройство периодически отображает записи ACE с совпавшими пакетами и количество совпавших пакетов. Пример журнала выглядит следующим образом:

```
*Sep 9 16:23:06: %ACL-6-MATCH: ACL 100 ACE 10 permit icmp any any, match 78 packets.
```

Чтобы контролировать количество журналов и частоту вывода, вы можете настроить интервал обновления журнала.

ПРИМЕЧАНИЕ: ACE, содержащий параметр ведения журнала ACL, потребляет больше аппаратных ресурсов. Если все настроенные ACE содержат этот параметр, емкость ACE устройства будет уменьшена вдвое.

ПРИМЕЧАНИЕ: по умолчанию интервал обновления журнала равен 0, то есть журнал не выводится. После того, как параметр ведения журнала ACL указан в ACE, вам необходимо настроить интервал обновления журнала для вывода связанных журналов; в противном случае журналы не выводятся.

ПРИМЕЧАНИЕ: для записи ACE, содержащей параметр ведения журнала ACL, если за указанный интервал не найдено ни одного пакета, журнал сопоставления пакетов, связанный с этой записью ACE, выводиться не будет. Если совпадающие пакеты будут найдены в указанном интервале, журналы сопоставления пакетов, относящиеся к этому ACE, будут выведены по истечении интервала. Количество совпадающих пакетов — это общее количество пакетов, соответствующих ACE в течение заданного интервала, то есть периода от предыдущего вывода журнала до текущего вывода журнала.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают функцию ведения журнала ACL.

ПРИМЕЧАНИЕ: параметр ведения журнала ACL можно настроить только для IP ACL или IPv6 ACL.

1.4.10.2. Связанная конфигурация

Настройка ACL

Настройте ACL перед настройкой ACE, содержащих параметр ведения журнала ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Дополнительные сведения о том, как добавить ACE в ACL, см. в предыдущих описаниях IP ACL и IPv6 ACL. Обратите внимание, что параметр ведения журнала ACL должен быть настроен.

Настройка интервала обновления журнала

Запустите команду {**ip | ipv6**} **access-list log-update inerval** *time* в режиме конфигурации для настройки интервала вывода журналов ACL.

Применение ACL

Дополнительные сведения о том, как применять ACL, см. в предыдущих описаниях IP ACL и IPv6 ACL.

1.4.11. Счетчики сопоставления пакетов

В дополнение к журналам ACL счетчики сопоставления пакетов предоставляют еще один вариант для планового обслуживания и оптимизации сети.

1.4.11.1. Принцип работы

Для реализации управления сетью пользователям может потребоваться узнать, есть ли в ACE какие-либо совпадающие пакеты и сколько пакетов совпало. ACL предоставляют счетчики сопоставления пакетов на основе ACE. Вы можете включить или отключить счетчики сопоставления пакетов для всех записей ACE в ACL. Когда пакет соответствует ACE, соответствующий счетчик увеличивается на 1. Вы можете запустить **clear counters access-list** [*acl-id* | *acl-name*] для сброса счетчиков всех ACE в ACL для нового раунда статистики.

ПРИМЕЧАНИЕ: для включения счетчиков ACL требуется больше аппаратных записей. В крайнем случае это сократит вдвое количество ACE, которые можно настроить на устройстве.

ПРИМЕЧАНИЕ: вы можете включить счетчики сопоставления пакетов в IP ACL, MAC ACL, экспертном ACL или IPv6 ACL.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают счетчики сопоставления пакетов ACL.

1.4.11.2. Связанная конфигурация

Настройка ACL

Настройте ACL перед настройкой ACE, содержащих параметр ведения журнала ACL. Дополнительные сведения о настройке ACL см. в предыдущих описаниях настройки ACL.

Добавление ACE в ACL

Дополнительные сведения о том, как добавить записи ACE в ACL, см. в предыдущих описаниях ACL. Обратите внимание, что параметр ведения журнала ACL должен быть настроен.

Включение счетчиков совпадения пакетов

Чтобы включить счетчики сопоставления пакетов в IP ACL, MAC ACL или экспертном ACL, запустите команду {**mac | expert** | **ip**} **access-list counter** { *aclid* | *acl-name* } в режиме глобальной конфигурации.

Чтобы включить счетчики сопоставления пакетов в ACL IPv6, запустите команду **ipv6 access-list counter** *acl-name* в режиме глобальной конфигурации.

Применение ACL

Дополнительные сведения о том, как применять ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Очистка счетчиков совпадения пакетов

Запустите команду **clear counters access-list** [*acl-id* | *acl-name*] в привилегированном режиме EXEC для сброса счетчиков сопоставления пакетов.

1.4.12. Режим сопоставления фрагментированных пакетов

В режиме сопоставления фрагментированных пакетов ACL может осуществлять более точный контроль над фрагментированными пакетами.

1.4.12.1. Принцип работы

IP-пакеты могут быть фрагментированы при передаче по сети. Когда происходит фрагментация, только первый фрагмент пакета содержит информацию L4, такую как номер порта TCP/UDP, тип ICMP и код ICMP, а другие фрагментированные пакеты не содержат информацию L4. По умолчанию, если ACE содержит флаг фрагмента, фильтруются фрагментированные пакеты, кроме первых фрагментов. Если ACE не содержит флага фрагмента, фильтруются все фрагментированные пакеты (включая первые фрагменты). В дополнение к этому режиму сопоставления фрагментированных пакетов по умолчанию предоставляется новый режим сопоставления фрагментированных пакетов. Вы можете переключаться между двумя режимами сопоставления фрагментированных пакетов по мере необходимости в указанном ACL. В новом режиме сопоставления фрагментированных пакетов, если ACE не содержит флага фрагмента и пакеты фрагментированы, первые фрагменты сравниваются со всеми полями сопоставления (включая информацию L3 и L4), определенными в ACE, а другие фрагментированные пакеты сравниваются только с информацией, отличной от L4, определенной в ACE.

ПРИМЕЧАНИЕ: в новом режиме сопоставления фрагментированных пакетов, если ACE не содержит флага фрагмента, а действие «Разрешить», этот тип ACE занимает больше аппаратных записей. В крайнем случае это уменьшит вдвое количество аппаратных записей. Если Установлено (Established) настроено для фильтрации флага TCP в ACE, будет занято больше аппаратных записей.

ПРИМЕЧАНИЕ: ACL временно не действует во время переключения режима сопоставления фрагментированных пакетов.

ПРИМЕЧАНИЕ: в новом режиме сопоставления фрагментированных пакетов, если ACE не содержит флага фрагмента, необходимо сравнить информацию L4 пакетов, и действие «Разрешить», ACE проверяет информацию L3 и L4 первых фрагментов пакетов и проверяет только информацию L3 других фрагментированных пакетов. Если выбрано действие «Запретить», ACE проверяет только первые фрагменты пакетов и игнорирует другие фрагментированные пакеты.

ПРИМЕЧАНИЕ: в новом режиме сопоставления фрагментированных пакетов, если ACE содержит флаг фрагмента, ACE проверяет только фрагментированные пакеты, но не первые фрагменты пакетов, независимо от того, является ли действие в ACE «Разрешить» или «Запретить».

ПРИМЕЧАНИЕ: только расширенный IP ACL и экспертный расширенный ACL поддерживают переключение между двумя режимами сопоставления фрагментированных пакетов.

ПРИМЕЧАНИЕ: только коммутаторы поддерживают фильтрацию фрагментированных пакетов.

1.4.12.2. Связанная конфигурация

Настройка ACL

Подробнее о том, как настроить ACL, см. в предыдущих описаниях IP ACL и экспертного расширенного ACL.

Добавление ACE в ACL

Дополнительные сведения о том, как добавить ACE в ACL, см. в предыдущих описаниях IP ACL и экспертного расширенного ACL. Обратите внимание, что необходимо добавить параметр фрагмента.

Переключение режима сопоставления фрагментированных пакетов

Запустите команду [**no**] {**ip | expert**} **access-list new-fragment-mode** { *acl-id* | *acl-name* } в режиме глобальной конфигурации для переключения режима сопоставления фрагментированных пакетов.

Применение ACL-списка

Подробнее о том, как применять ACL, см. в предыдущих описаниях IP ACL и экспертного расширенного ACL.

1.5. Ограничения

1. В продуктах серии QSW-7600 ACL, примененный к входящему направлению, не поддерживает сопоставление «NEQ» на портах уровня 4 для пакетов TCP и UDP, а ACL, примененный к исходящему направлению, поддерживает только сопоставление «EQ» на портах уровня 4 для пакетов TCP и UDP.
2. ACL IPv6, настроенные на продуктах серии QSW-7600, поддерживают сопоставление по следующим полям: **protocol**, **sip, l4_src**, **dip, l4_dst**, **dscp**, и **flow_label**. ACL IPv6 поддерживает сопоставление только на основе следующих двух групп полей:

- protocol, sip, l4_src, l4_dst, dscp, flow_label, range
- protocol, dip, l4_src, l4_dst, dscp, flow_label, range
- ACL не может использовать все поля для сопоставления. Кроме того, ACL IPv6 не поддерживают ни сопоставление по фрагменту, ни сопоставление по метке потока в исходящем направлении.
- Когда для IP-адреса источника и IP-адреса назначения необходимо сопоставить только старшие 64 бита (длина маски меньше или равна 64), поддерживается сопоставление с помощью IPv6 5-tuple.

3. В продуктах серии QSW-7600 Security ACL, применяемые к SVI, эффективны как для пакетов внутри VLAN, пересылаемых мостами, так и для пакетов маршрутизации между VLAN. В результате пользователи в VLAN не могут обмениваться данными.
4. Продукты серии QSW-7600 не могут идентифицировать поле флага фрагмента в пакетах IPv6. Если ACL IPv6 содержит флаг фрагмента, флаг фрагмента игнорируется при сопоставлении пакетов. Это эквивалентно отсутствию флага фрагмента в списках ACL, и сопоставление выполняется для всех пакетов, включая пакеты первого фрагмента и пакеты не первого фрагмента.
5. Продукты серии QSW-7600 поддерживают переключение режима сопоставления пакетов фрагментов, когда применяются расширенные ACL IP или экспертные расширенные ACL.
6. В продуктах серии QSW-7600 ACL 80 поддерживает только следующие общие поля: MAC-адрес назначения, MAC-адрес источника, VID, ETYPE, номер протокола IP, адрес IPv4 источника, адрес IPv4 назначения, идентификатор порта назначения, идентификатор порта источника, тип ICMP и код ICMP.

1.6. Конфигурация

Элемент конфигурации	Описание и команда	
Настройка IP ACL	(Опционально) Он используется для фильтрации пакетов IPv4	
	ip access-list standard	Настраивает стандартный IP ACL
	ip access-list extended	Настраивает расширенный IP ACL
	permit host any time-range log	Добавляет разрешающий ACE в стандартный IP ACL
	deny host any time-range log	Добавляет запрещающий ACE в стандартный IP ACL
	permit host any host any tos dscp **precedence fragment time-range log**	Добавляет разрешающий ACE в расширенный IP ACL

Элемент конфигурации	Описание и команда	
Настройка IP ACL	**deny host any host any tos dscp precedence fragment time-range log**	Добавляет запрещающий ACE в расширенный IP ACL
	ip access-group in out	Применяет стандартный или расширенный IP ACL
Настройка расширенного ACL MAC	(Опционально) Он используется для фильтрации пакетов L2	
	mac access-list extended	Настраивает расширенный ACL MAC
	permit any host any host cos inner timerange	Добавляет разрешающий ACE в расширенный ACL MAC
	deny any host any host cos inner time-range	Добавляет запрещающий ACE в расширенный ACL MAC
	mac access-group in out	Применяет расширенный ACL MAC
Настройка экспертного расширенного ACL	(Опционально) Он используется для фильтрации пакетов L2 и L3	
	expert access-list extended	Настраивает экспертный расширенный ACL
	permit cos inner VID inner host any host any **host any host any precedence tos fragment** **range time-range**	Добавляет разрешающий ACE в экспертный расширенный ACL
	deny cos inner VID inner host any host any **host any host any precedence tos fragment** **range time-range**	Добавляет запрещающий ACE в экспертный расширенный ACL
	expert access-group in out	Применяет экспертный расширенный ACL

Элемент конфигурации	Описание и команда	
Настройка расширенного ACL IPv6	(Опционально) Используется для фильтрации пакетов IPv6	
	ipv6 access-list	Настраивает ACL IPv6
	permit host any host any range dscp flowlabel fragment time-range log	Добавляет разрешающий ACE в ACL IPv6
	deny host any host any range dscp flowlabel fragment time-rangelog	Добавляет запрещающий ACE в ACL IPv6
	ipv6 traffic-filter in out	Применяет ACL IPv6
Настройка ACL80	(Опционально) Используется для настройки полей для фильтрации пакетов L2 и L3	
	expert access-list advanced	Настраивает экспертный расширенный ACL
	permit	Добавляет разрешающий ACE в экспертный расширенный ACL
	deny	Добавляет запрещающий ACE в экспертный расширенный ACL
	expert access-group in out	Применяет экспертный расширенный ACL
Настройка перенаправления ACL	(Опционально) Используется для перенаправления пакетов, соответствующих правилам, на указанный интерфейс	
	redirect destination interface acl in	Настраивает перенаправление ACL
Настройка глобальной Security ACL	(Опционально) Используется для того, чтобы ACL вступил в силу глобально	
	ip access-group in out	Применяет глобальный Security ACL в режиме глобальной конфигурации

Элемент конфигурации	Описание и команда	
Настройка глобальной Security ACL	**no global ip access-group**	Настраивает интерфейс как эксклюзивный интерфейс глобального Security ACL в режиме настройки интерфейса
Настройка канала безопасности	(Опционально) Используется для того, чтобы пакеты, соответствующие некоторым характеристикам, могли обходить проверки приложений контроля доступа, таких как DOT1X и веб-аутентификация	
	security access-group	Включает канал безопасности в режиме конфигурации интерфейса
	security global access-group	Включает канал безопасности в режиме глобальной конфигурации
	security uplink enable	Настраивает интерфейс как эксклюзивный интерфейс глобального канала безопасности в режиме настройки интерфейса
Настройка комментариев для ACL	(Опционально) Используется для настройки комментариев для ACL или ACE, чтобы пользователи могли легко идентифицировать функции ACL или ACE	
	list-remark	Настраивает комментарий для ACL в режиме конфигурации ACL
	access-list list-remark	Настраивает комментарий для ACL в режиме глобальной конфигурации
	remark	Настраивает комментарий для ACE в режиме конфигурации ACL

1.6.1. Настройка IP ACL

1.6.1.1. Эффект конфигурации

Настройте и примените IP ACL к интерфейсу, чтобы контролировать все входящие и исходящие пакеты IPv4 этого интерфейса. Вы можете разрешить или запретить вход определенных пакетов IPv4 в сеть, чтобы контролировать доступ IP-пользователей к сетевым ресурсам.

1.6.1.2. Шаги настройки

Настройка IP ACL

- (Обязательно) Настройте IP ACL, если вы хотите контролировать доступ пользователей IPv4 к сетевым ресурсам.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. IP ACL действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление записей ACE в IP ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, все входящие IPv4-пакеты устройства по умолчанию отклоняются.

Применение IP ACL

- (Обязательно) Примените IP ACL к указанному интерфейсу, если вы хотите, чтобы этот ACL вступил в силу.
- Вы можете применить IP ACL к указанному интерфейсу устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.1.3. Проверка

- Используйте следующие методы, чтобы проверить влияние конфигурации IP ACL:
- Запустите команду **ping**, чтобы убедиться, что IP ACL действует на указанном интерфейсе. Например, если IP ACL настроен на запрет доступа к хосту с указанным IP-адресом или хостам в указанном диапазоне IP-адресов, запустите команду **ping**, чтобы убедиться, что хосты не могут быть успешно пропингованы.
- Получите доступ к связанным сетевым ресурсам, чтобы убедиться, что IP ACL действует на указанном интерфейсе. Например, доступ в Интернет или доступ к ресурсам FTP в сети через FTP.

1.6.1.4. Связанные команды

Настройка IP ACL

Команда	**ip access-list** { **standard** | **extended** } {*acl-name* | *acl-id* }
Описание параметров	**standard**: указывает, что создан стандартный IP ACL. **extended**: указывает, что создан расширенный IP ACL. *acl-name*: указывает имя стандартного или расширенного IP ACL. Если этот параметр настроен, создается именованный ACL. Имя представляет собой строку от 1 до 99 символов. Имя ACL не может начинаться с цифр (0–9), «in» или «out». *acl-id*: указывает идентификатор, который однозначно идентифицирует стандартный или расширенный IP ACL. Если этот параметр настроен, создается нумерованный ACL. Если создается стандартный IP ACL, диапазон значений *acl-id* составляет 1–99 и 1300–1999. Если создается расширенный IP ACL, диапазон значений *acl-id* составляет 100–199 и 2000–2699
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Запустите эту команду, чтобы настроить стандартный или расширенный IP ACL и войти в режим конфигурации стандартного или расширенного IP ACL. Если вы хотите контролировать доступ пользователей к сетевым ресурсам, проверяя исходный IP-адрес каждого пакета, настройте стандартный IP ACL. Если вы хотите контролировать доступ пользователей к сетевым ресурсам, проверяя IP-адрес источника или получателя, номер протокола и порт источника или получателя TCP/UDP, настройте расширенный список управления доступом IP

Добавление записей ACE в IP ACL

- Добавьте записи ACE в стандартный IP ACL.

Используйте любой из следующих методов для добавления записей ACE в стандартный IP ACL:

Команда	[*sn*] { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**log**]
Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. **host** *source*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что IP-пакеты, отправленные с любого узла, фильтруются. *source source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона. **log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе

Режим команд	Стандартный режим конфигурации IP ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в стандартном режиме настройки IP ACL. ACL может быть именованным или нумерованным ACL

Команда	**access-list** *acl-id* { **permit** | **deny** } {**host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] [**log**]
Описание параметров	*acl-id*: указывает идентификатор пронумерованного ACL. Он однозначно идентифицирует ACL. Диапазон значений *acl-id*: 100–199 и 1300–1999. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. **host** *source*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что IP-пакеты, отправленные с любого узла, фильтруются. *source source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона. **log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе
Режим команд	Стандартный режим конфигурации IP ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в пронумерованный список ACL IP в режиме глобальной конфигурации. Ее нельзя использовать для добавления записей ACE в именованный список ACL IP

- Добавьте записи ACE в расширенный IP ACL.

Используйте любой из следующих методов для добавления записей ACE в расширенный список управления доступом IP:

Команда	[*sn*] { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time range** *time-range-name*] [**log**]

Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрещающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *protocol*: указывает номер IP-протокола. Диапазон значений от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения для замены конкретных номеров протоколов IP, включая eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp и udp. **host** *source*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. *source source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **host** *destination*: указывает, что IP-пакеты, отправляемые на хост с указанным IP-адресом назначения, фильтруются. Если настроено ключевое слово **any**, IP-пакеты, отправляемые на любой хост, фильтруются. *destination destination-wildcard*: указывает, что IP-пакеты, отправляемые на узлы в указанном сегменте IP-сети, фильтруются. **any**: указывает, что IP-пакеты, отправляемые на любой хост или с него, фильтруются. **precedence** *precedence*: указывает, что IP-пакеты с указанным полем приоритета в заголовке фильтруются. **tos** *tos*: указывает, что IP-пакеты с указанным полем типа службы (TOS) в заголовке фильтруются. **dscp** *dscp*: указывает, что IP-пакеты с указанным полем dcsp в заголовке фильтруются. **ecn** *ecn*: указывает, что IP-пакеты с указанным полем ecn в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные IP-пакеты, за исключением первых фрагментов. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона

Описание параметров	**log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе
Режим команд	Расширенный режим конфигурации IP ACL
Руководство по использованию	Запустите эту команду, чтобы добавить ACE в расширенный режим настройки IP ACL. ACL может быть именованным или нумерованным ACL

Команда	**access-list** *acl-id* { **permit** | **deny** } *protocol* {**host** *source* | **any** | *source source-wildcard* } {**host** *destination* | **any** | *destination destination-wildcard* } [[**precedence** *precedence* [**tos** *tos*]] | **dscp** *dscp*] [**fragment**] [**time-range** *time-range-name*] [**log**]
Описание параметров	*acl-id*: указывает идентификатор пронумерованного ACL. Он однозначно идентифицирует ACL. Диапазон значений *acl-id*: 100–199 и 2000–1999. *sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажите порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *protocol*: указывает номер IP-протокола. Значение находится в диапазоне от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения для замены конкретных номеров IP-протокола, включая eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp и udp. **host** *source*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. *source source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **host** *destination*: указывает, что IP-пакеты, отправляемые на хост с указанным IP-адресом назначения, фильтруются. Если настроено ключевое слово **any**, IP-пакеты, отправляемые на любой хост, фильтруются

Описание параметров	*destination destination-wildcard*: указывает, что IP-пакеты, отправляемые на узлы в указанном сегменте IP-сети, фильтруются. **any**: указывает, что IP-пакеты, отправляемые на любой хост или с него, фильтруются. **precedence** *precedence*: указывает, что IP-пакеты с указанным полем приоритета в заголовке фильтруются. **tos** *tos*: указывает, что IP-пакеты с указанным полем типа службы (TOS) в заголовке фильтруются. **dscp** *dscp*: указывает, что IP-пакеты с указанным полем dcsp в заголовке фильтруются. **ecn** *ecn*: указывает, что IP-пакеты с указанным полем ecn в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные IP-пакеты, за исключением первых фрагментов. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона. **log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе
Режим команд	Расширенный режим конфигурации IP ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в пронумерованный список контроля доступа IP в режиме конфигурации расширенного списка контроля доступа IP. Ее нельзя использовать для добавления записей ACE в именованный расширенный список контроля доступа IP

Применение IP ACL

Команда	**ip access-group** { *acl-id* **|** *acl-name* } { **in**	**out** } [**reflect**]
Описание параметров	*acl-id*: указывает, что к интерфейсу будет применяться пронумерованный стандартный или расширенный IP ACL. *acl-name*: указывает, что к интерфейсу будет применен именованный стандартный или расширенный IP ACL. **in**: указывает, что этот ACL контролирует входящие IP-пакеты интерфейса. **out**: указывает, что этот ACL контролирует исходящие IP-пакеты интерфейса. **reflect**: указывает, что рефлексивный ACL включен
Режим команд	Режим конфигурации интерфейса

Руководство по использованию	Эта команда заставляет IP ACL действовать на входящие или исходящие пакеты указанного интерфейса

1.6.1.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Настройка IP ACL для запрета отделам, кроме финансового отдела, на доступ к серверу финансовых данных

Сценарий:

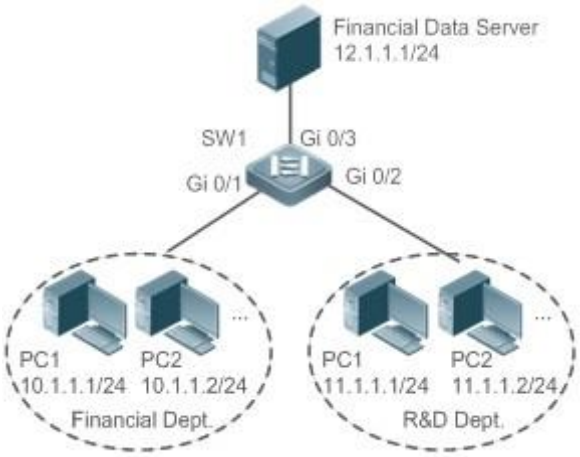

Рисунок 1-3.

Шаги настройки	• Настройте IP ACL. • Добавьте записи ACE в IP ACL. • Примените IP ACL к исходящему направлению интерфейса, соединяющего сервер финансовых данных
SW1	sw1(config)#ip access-list standard 1 sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 out
Проверка	• На ПК отдела исследований и разработок пропингуйте сервер финансовых данных. Убедитесь, что операция проверки связи не удалась. • На ПК финансового отдела пропингуйте сервер финансовых данных. Убедитесь, что операция проверки связи прошла успешно

SW1	sw1(config)#show access-lists ip access-list standard 1 10 permit 10.1.1.0 0.0.0.255 20 deny 11.1.1.0 0.0.0.255 sw1(config)#show access-group ip access-group 1 out Применяется на интерфейсе GigabitEthernet 0/3

1.6.2. Настройка расширенного ACL MAC

1.6.2.1. Эффект конфигурации

Настройте и примените расширенный ACL MAC к интерфейсу, чтобы контролировать все входящие и исходящие пакеты IPv4 этого интерфейса. Вы можете разрешить или запретить ввод определенных пакетов L2 в сеть, чтобы контролировать доступ пользователей к сетевым ресурсам на основе пакетов L2.

1.6.2.2. Шаги настройки

Настройка расширенного ACL MAC

- (Обязательно) Настройте расширенный ACL MAC, если вы хотите контролировать доступ пользователей к сетевым ресурсам на основе заголовка пакета L2, например, MAC-адреса ПК каждого пользователя.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Расширенный ACL MAC действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление записей ACE в расширенный ACL MAC

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, все входящие L2 Ethernet-пакеты устройства по умолчанию отклоняются.

Применение расширенного ACL MAC

- (Обязательно) Примените расширенный ACL MAC к указанному интерфейсу, если вы хотите, чтобы этот ACL вступил в силу.
- Вы можете применить расширенный ACL MAC к указанному интерфейсу устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.2.3. Проверка

- Используйте следующие методы для проверки эффектов конфигурации расширенного ACL MAC:
- Если расширенный ACL MAC настроен на разрешение или запрет некоторых IP-пакетов, запустите команду **ping**, чтобы проверить, действуют ли ACE этого ACL на указанном интерфейсе. Например, расширенный ACL MAC настроен для предотвращения приема IP-пакетов интерфейсом устройства (тип Ethernet — 0x0800), для проверки выполните команду **ping**.

- Если расширенный ACL MAC настроен на разрешение или запрет некоторых пакетов, отличных от IP (например, пакетов ARP), также запустите команду **ping**, чтобы проверить, действуют ли ACE этого ACL на указанном интерфейсе. Например, чтобы отфильтровать пакеты ARP, выполните команду **ping** для проверки.
- Вы также можете создать пакеты L2, отвечающие некоторым указанным характеристикам, чтобы проверить, действует ли расширенный ACL MAC. Как правило, подготовьте два ПК, создайте и отправьте пакеты L2 на одном ПК, включите захват пакетов на другом ПК и проверьте, пересылаются ли пакеты должным образом (пересылаются или блокируются) в соответствии с действием, указанным в ACE.

1.6.2.4. Связанная команда

Настройка расширенного списка контроля доступа MAC

Команда	**mac access-list extended** {*acl-name* | *acl-id* }
Описание параметров	*acl-name*: указывает имя расширенного ACL MAC. Если этот параметр настроен, создается именованный ACL. Имя представляет собой строку от 1 до 99 символов. Имя ACL не может начинаться с цифр (0–9), «in» или «out». *acl-id*: указывает идентификатор, который однозначно идентифицирует расширенный ACL MAC. Если этот параметр настроен, создается нумерованный ACL. Диапазон значений acl-id — 700–799
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить расширенный ACL MAC и войти в режим конфигурации расширенного ACL MAC. Вы можете настроить расширенный ACL MAC для управления доступом пользователей к сетевым ресурсам путем проверки информации L2 Ethernet-пакетов

Добавление ACE в расширенный ACL MAC

Используйте любой из следующих методов для добавления записей ACE в расширенный ACL MAC:

- Добавьте ACE в расширенный режим конфигурации ACL MAC.

Команда	[*sn*] { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней

	записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. **any**: указывает, что пакеты L2, отправляемые с любого хоста, фильтруются. **host** *src-mac-addr*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным MAC-адресом, фильтруются. **any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. **host** *dst-mac-addr*: указывает, что IP-пакеты, отправляемые на хост с указанным MAC-адресом назначения, фильтруются. *ethernet-type*: указывает, что пакеты L2 указанного типа Ethernet фильтруются. **cos** *cos*: указывает, что пакеты L2 с указанным полем класса обслуживания (cos) во внешнем теге фильтруются. **inner** *cos*: указывает, что пакеты L2 с указанным полем cos во внутреннем теге фильтруются. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона.
Режим команд	Расширенный режим конфигурации ACL MAC
Руководство по использованию	Запустите эту команду, чтобы добавить ACE в расширенный режим конфигурации ACL MAC. ACL может быть именованным или нумерованным ACL

- Добавьте ACE в расширенный ACL MAC в режиме глобальной конфигурации.

Команда	**access-list** *acl-id* { **permit** | **deny** } {**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos* [**inner** *cos*]] [**time-range** *tm-rng-name*]
Описание параметров	*acl-id*: указывает идентификатор пронумерованного ACL. Он однозначно идентифицирует ACL. Диапазон значений *acl-id*: 700–799. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. **host** *src-mac-addr*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным MAC-адресом, фильтруются. *hostsource*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным MAC-адресом, фильтруются.

Описание параметров	**any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. **host** *dst-mac-addr*: указывает, что IP-пакеты, отправляемые на хост с указанным MAC-адресом назначения, фильтруются. *ethernet-type*: указывает, что пакеты L2 указанного типа Ethernet фильтруются. **cos** *cos*: указывает, что пакеты L2 с указанным полем cos во внешнем теге фильтруются. **inner** *cos*: указывает, что пакеты L2 с указанным полем cos во внутреннем теге фильтруются. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Для получения подробной информации о временном диапазоне см. в руководстве по настройке временного диапазона
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в расширенный ACL с нумерованным MAC-адресом в режиме глобальной конфигурации. Его нельзя использовать для добавления ACE в именованный расширенный ACL MAC

Применение расширенного ACL MAC

Команда	**mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Описание параметров	*acl-id*: указывает, что к интерфейсу будет применен расширенный нумерованный MAC IP ACL. *acl-name*: указывает, что к интерфейсу будет применен именованный расширенный IP ACL MAC. **in**: указывает, что этот ACL контролирует входящие пакеты L2 интерфейса. **out**: указывает, что этот ACL контролирует исходящие пакеты L2 интерфейса
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эта команда заставляет расширенный ACL MAC действовать на входящие или исходящие пакеты указанного интерфейса

1.6.2.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Настройка расширенного ACL MAC для ограничения ресурсов, доступных посетителям

Сценарий:

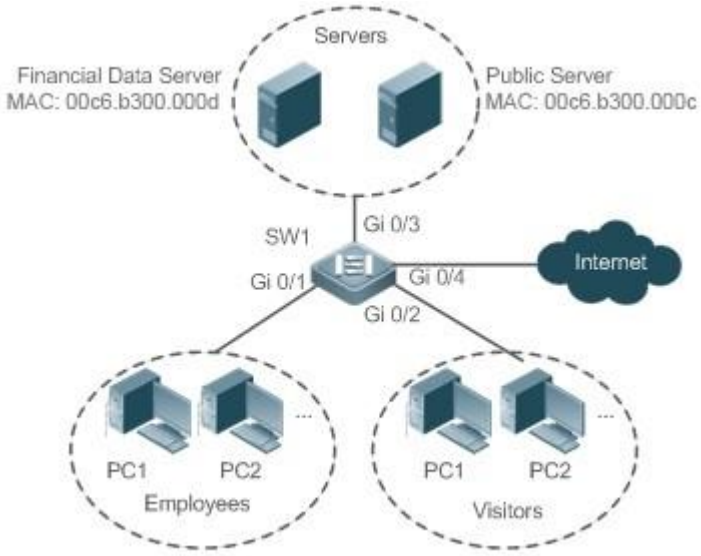

Рисунок 1-4.

Шаги настройки	• Настройте расширенный ACL MAC. • Добавьте ACE в расширенный ACL MAC. • Примените расширенный ACL MAC к исходящему направлению интерфейса, подключенного к зоне для посетителей, чтобы посетителям был разрешен доступ в Интернет и к общедоступному серверу компании, но запрещен доступ к серверу финансовых данных компании. То есть посетители не могут получить доступ к серверу с MAC-адресом 00c6.b300.000d
SW1	sw1(config)#mac access-list extended 700 sw1(config-mac-nacl)#deny any host 00c6.b300.000d sw1(config-mac-nacl)#pemit any any sw1(config-mac-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#mac access-group 700 in
Проверка	• На компьютере посетителя пропингуйте сервер финансовых данных. Убедитесь, что операция проверки связи не удалась • На компьютере посетителя пропингуйте сервер общедоступного ресурса. Убедитесь, что операция проверки связи прошла успешно. • На компьютере посетителя подключитесь к Интернету, например, посетите веб-сайт QTECH. Убедитесь, что веб-страницу можно открыть

SW1	sw1(config)#show access-lists mac access-list extended 700 10 deny any host 00c6.b300.000d etype-any 20 permit any any etype-any sw1(config)#show access-group mac access-group 700 in Applied On interface GigabitEthernet 0/2

1.6.3. Настройка экспертного расширенного ACL

1.6.3.1. Эффект конфигурации

Настройте и примените экспертный расширенный ACL к интерфейсу, чтобы контролировать входящие и исходящие пакеты интерфейса на основе информации L2 и L3, а также разрешать или запрещать ввод определенных пакетов в сеть. Кроме того, вы можете настроить экспертный расширенный ACL для управления всеми пакетами L2 на основе VLAN, чтобы разрешить или запретить доступ пользователей в некоторых сегментах сети к сетевым ресурсам. Как правило, вы можете использовать экспертный расширенный ACL, если вы хотите включить ACE IP ACL и расширенного ACL MAC в один ACL.

1.6.3.2. Шаги настройки

Настройка экспертного расширенного ACL

- (Обязательно) Настройте экспертный расширенный ACL, если вы хотите контролировать доступ пользователей к сетевым ресурсам на основе заголовка пакета L2, например, идентификатора VLAN.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Экспертный расширенный ACL действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление записей ACE в экспертный расширенный ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, все входящие пакеты устройства по умолчанию запрещены.

Применение экспертного расширенного ACL

- (Обязательно) Примените экспертный расширенный ACL к указанному интерфейсу, если вы хотите, чтобы этот ACL вступил в силу.
- Вы можете применить экспертный расширенный ACL во входящем или исходящем направлении указанного интерфейса устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.3.3. Проверка

- Используйте следующие методы для проверки эффектов конфигурации экспертного расширенного ACL:
- Если в экспертном расширенном ACL настроены правила доступа на основе IP для разрешения или запрета некоторых IP-пакетов, запустите команду **ping**, чтобы проверить, действуют ли эти правила.

- Если правила доступа на основе MAC-адресов настроены в экспертном расширенном ACL для разрешения или запрета некоторых пакетов L2 (например, пакетов ARP), также запустите команду **ping**, чтобы проверить, действуют ли ACE этого ACL на указанном интерфейсе. Например, чтобы отфильтровать пакеты ARP, выполните команду **ping** для проверки.
- Если правила доступа на основе идентификатора VLAN настроены в экспертном расширенном ACL для разрешения или запрета некоторых пакетов L2 в некоторых сегментах сети (например, для предотвращения обмена данными между пользователями VLAN 1 и VLAN 2), пропингуйте ПК VLAN 2 на ПК VLAN 1. В случае сбоя операции **ping** правила вступают в силу.

1.6.3.4. Связанная команда

Настройка экспертного расширенного ACL

Команда	**expert access-list extended {***acl-name* | *acl-id* **}**
Описание параметров	*acl-name*: указывает имя экспертного расширенного ACL. Если этот параметр настроен, создается именованный ACL. Имя представляет собой строку от 1 до 99 символов. Имя ACL не может начинаться с цифр (0–9), «in» или «out». *acl-id*: указывает идентификатор экспертного расширенного ACL. Если этот параметр настроен, создается нумерованный ACL. Диапазон значений *acl-id*: 2700–2899
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить расширенный ACL и войти в режим конфигурации экспертных расширенных ACL

Добавление записей ACE в экспертный расширенный ACL

Используйте любой из следующих методов, чтобы добавить записи ACE в экспертный расширенный ACL:

- Добавьте ACE в экспертном расширенном режиме конфигурации ACL.

Команда	[*sn*] { **permit** |**deny** } [*protocol*| [*ethernet-type*] [**cos**[*out*] [**inner** *in*]]] [[**VID** [*out*] [**inner** *in*]]] {*sourcesource wildcard* | **host***source* | **any**}{**host** *source-mac-address*|**any** } {*destination destination-wildcard* | **host** *destination* | **any**} {**host** *destination-mac-address* | **any**} [[**precedence** *precedence*][**tos** *tos*] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**range** *lowerupper*] [[udf udf-id header pos value mask] | [**int-flag**]] [**time-range** *time-range-name*]]
Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней

	записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *protocol*: указывает номер IP-протокола. Диапазон значений от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения для замены конкретных номеров протоколов IP, включая eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp и udp. *ethernet-type*: указывает, что пакеты L2 указанного типа Ethernet фильтруются. **cos** *out*: указывает, что пакеты L2 с указанным полем cos во внешнем теге фильтруются. **cos inner** *in*: указывает, что пакеты L2 с указанным полем cos во внутреннем теге фильтруются. **VID** *out*: указывает, что пакеты L2 с указанным полем VLAN ID во внешнем теге фильтруются. **VID inner** *in*: указывает, что пакеты L2 с указанным полем идентификатора VLAN во внутреннем теге фильтруются. *source source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **host** source: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что IP-пакеты, отправленные с любого узла, фильтруются. **host** *source-mac-address*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным MAC-адресом, фильтруются. **any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. *destination destination-wildcard*: указывает, что IP-пакеты, отправляемые на узлы в указанном сегменте IP-сети, фильтруются. **host** *destination*: указывает, что IP-пакеты, отправляемые на хост с указанным IP-адресом назначения, фильтруются. **any**: указывает, что IP-пакеты, отправляемые на любой хост, фильтруются. **host** *destination-mac-address*: указывает, что IP-пакеты, отправленные на хост с указанным MAC-адресом назначения, фильтруются. **any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. **precedence** *precedence*: указывает, что IP-пакеты с указанным полем приоритета в заголовке фильтруются.

Описание параметров	**tos** *tos*: указывает, что IP-пакеты с указанным полем tos в заголовке фильтруются. **dscp** *dscp*: указывает, что IP-пакеты с указанным полем dcsp в заголовке фильтруются. **ecn** *ecn*: указывает, что IP-пакеты с указанным полем ecn в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные IP-пакеты, за исключением первых фрагментов. **udf** *udf-id header pos value mask*: указывает настраиваемые поля. **int-flag**: указывает, что поле флага int пакетов фильтруется. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона
Режим команд	Экспертный расширенный режим конфигурации ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в экспертном расширенном режиме конфигурации ACL. ACL может быть именованным или нумерованным ACL

- Добавьте ACE в экспертный расширенный ACL в режиме глобальной конфигурации.

Команда	**access-list** *acl-id*{ **permit** |**deny** }[*protocol*| [*ethernet-type*][**cos**[*out*] [**inner** *in*]]] [[**VID** [*out*][**inner** *in*]]] {*source source-wildcard* | **host***source* | **any**}{**host** *source-mac-address*|**any** } {*destination destination wildcard* | **host***destination* | **any**} {**host** *destination-mac-address* | **any**} [[**precedence** *precedence*][**tos** *tos*] | [**dscp** *dscp*] [**ecn** *ecn*]] [**fragment**] [**range** *lowerupper*] [[udf udf-id header pos value mask] | [**int-flag**]] [**time-range** *time-range-name*]]
Описание параметров	*acl-id*: указывает идентификатор пронумерованного ACL. Он однозначно идентифицирует ACL. Диапазон значений acl-id от 2700 до 2899. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE *protocol*: указывает номер IP-протокола. Значение находится в диапазоне от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения для замены конкретных номеров IP-протокола, включая eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp и udp. *ethernet-type*: указывает, что пакеты L2 указанного типа Ethernet фильтруются.

Описание параметров	**cos** *out*: указывает, что пакеты L2 с указанным полем cos во внешнем теге фильтруются. **cos inner** *in*: указывает, что пакеты L2 с указанным полем cos во внутреннем теге фильтруются. **VID** *out*: указывает, что пакеты L2 с указанным полем VLAN ID во внешнем теге фильтруются. **VID inner** *in*: указывает, что пакеты L2 с указанным полем идентификатора VLAN во внутреннем теге фильтруются. ***source*** *source-wildcard*: указывает, что IP-пакеты, отправленные с хостов в указанном сегменте IP-сети, фильтруются. **host** *source*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что IP-пакеты, отправленные с любого узла, фильтруются. **host** *source-mac-address*: указывает, что IP-пакеты, отправленные с хоста с указанным исходным MAC-адресом, фильтруются. **any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. ***destination*** *destination-wildcard*: указывает, что IP-пакеты, отправляемые на узлы в указанном сегменте IP-сети, фильтруются. **host** *destination*: указывает, что IP-пакеты, отправляемые на хост с указанным IP-адресом назначения, фильтруются. **any**: указывает, что IP-пакеты, отправляемые на любой хост, фильтруются. **host** *destination-mac-address*: указывает, что IP-пакеты, отправленные на хост с указанным MAC-адресом назначения, фильтруются. **any**: указывает, что пакеты L2, отправляемые на любой хост, фильтруются. **precedence** *precedence*: указывает, что IP-пакеты с указанным полем приоритета в заголовке фильтруются. **tos** *tos*: указывает, что IP-пакеты с указанным полем tos в заголовке фильтруются. **dscp** *dscp*: указывает, что IP-пакеты с указанным полем dcsp в заголовке фильтруются. **ecn** *ecn*: указывает, что IP-пакеты с указанным полем ecn в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные IP-пакеты, за исключением первых фрагментов. **udf** *udf-id header pos value mask*: указывает настраиваемые поля. **int-flag**: указывает, что поле флага int пакетов фильтруется.

Описание параметров	**time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в нумерованный экспертный расширенный ACL в режиме глобальной конфигурации. Его нельзя использовать для добавления записей ACE в именованный экспертный расширенный ACL

Применение экспертного расширенного ACL

Команда	**expert access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }
Описание параметров	*acl-id*: указывает, что к интерфейсу будет применен нумерованный экспертный расширенный ACL. *acl-name*: указывает, что к интерфейсу будет применен именованный экспертный расширенный ACL. **in**: указывает, что этот ACL контролирует входящие пакеты L2 интерфейса. **out**: указывает, что этот ACL контролирует исходящие пакеты L2 интерфейса
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эта команда заставляет экспертный расширенный ACL действовать на входящие или исходящие пакеты указанного интерфейса

1.6.3.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Настройка экспертного расширенного ACL для ограничения ресурсов, доступных посетителям (требуется, чтобы посетители и сотрудники не могли общаться друг с другом, посетители могли получить доступ к серверу общедоступных ресурсов, но не к серверу финансовых данных компании.)

Сценарий:

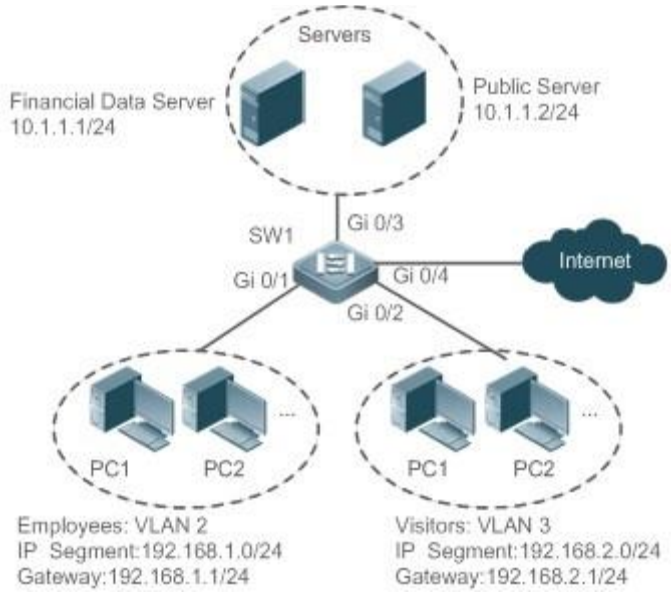

Рисунок 1-5.

Шаги настройки	• Настройте экспертный расширенный ACL. • Добавьте ACE, чтобы запретить пакеты, отправляемые с ПК в зоне для посетителей (VLAN 3) на ПК сотрудников в VLAN 2. • Добавьте ACE, чтобы запретить посетителям доступ к серверу финансовых данных компании. • Добавьте ACE, чтобы разрешить все пакеты. • Примените ACL к входящему направлению интерфейса коммутатора, который подключается к гостевой зоне
SW1	sw1(config)#expert access-list extended 2700 sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any sw1(config-exp-nacl)#pemit any any any any sw1(config-exp-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in
Проверка	• На компьютере посетителя пропингуйте сервер финансовых данных. Убедитесь, что операция проверки связи не удалась. • На компьютере посетителя пропингуйте сервер общедоступного ресурса. Убедитесь, что операция **ping** прошла успешно. • На ПК посетителя пропинговать адрес шлюза 192.168.1.1 сотрудника. Убедитесь, что операция проверки связи не удалась

Проверка	• На компьютере посетителя подключитесь к Интернету, например, посетите веб-сайт QTECH. Убедитесь, что веб-страницу можно открыть
SW1	sw1(config)#show access-lists expert access-list extended 2700 10 deny ip any any 192.168.1.0 0.0.0.255 any 20 deny ip any any host 10.1.1.1 any 30 permit ip any any any any sw1(config)#show access-group expert access-group 2700 in Применяется на интерфейсе GigabitEthernet 0/2

1.6.4. Настройка расширенного ACL IPv6

1.6.4.1. Эффект конфигурации

Настройте и примените ACL IPv6 к интерфейсу, чтобы контролировать все входящие и исходящие пакеты IPv5 этого интерфейса. Вы можете разрешить или запретить вход определенных пакетов IPv6 в сеть, чтобы контролировать доступ пользователей IPv6 к сетевым ресурсам.

1.6.4.2. Шаги настройки

Настройка списка контроля доступа IPv6

- (Обязательно) Настройте IP ACL, если вы хотите, чтобы пользователи IPv4 имели доступ к сетевым ресурсам.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Список ACL IPv6 действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление записей ACE в ACL IPv6

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, все входящие IPv6-пакеты устройства по умолчанию отклоняются.

Применение ACL IPv6

- (Обязательно) Примените ACL IPv6 к указанному интерфейсу на устройстве, если вы хотите, чтобы этот ACL вступил в силу.
- Вы можете применить список управления доступом IPv6 к указанному интерфейсу устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.4.3. Проверка

- Используйте следующие методы, чтобы проверить влияние конфигурации списка управления доступом IPv6:
- Запустите команду **ping**, чтобы убедиться, что список ACL IPv6 действует на указанном интерфейсе. Например, если ACL IPv6 настроен на запрет хосту с

указанным IP-адресом или хостам в указанном диапазоне адресов IPv6 доступ к сети, запустите команду **ping**, чтобы убедиться, что хосты не могут быть успешно пропингованы.

- Получите доступ к сетевым ресурсам, например, посетите веб-сайт IPv6, чтобы проверить, действует ли список ACL IPv6 на указанном интерфейсе.

1.6.4.4. Связанная команда

Настройка списка контроля доступа IPv6

Команда	**ipv6 access-list** *acl-name*
Описание параметров	*acl-name*: указывает имя стандартного или расширенного IP ACL. Имя представляет собой строку от 1 до 99 символов. Имя ACL не может начинаться с цифр (0–9), «in» или «out»
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить ACL IPv6 и войти в режим настройки IPv6

Добавление записей ACE в список ACL IPv6

Чтобы фильтровать пакеты TCP или UDP, добавьте записи ACE в ACL IPv6 следующим образом:

Команда	[*sn*] {**permit** | **deny** } *protocol* {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} {*dst-ipv6-pfix/pfix-len* | **host** *dst-ipv6-addr* | **any**} [*op dstport* | **range** *lower upper*] [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment]** [**time-range***tm-rng-name*][**log**]
Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрещающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *protocol*: указывает номер протокола IPv6. Диапазон значений от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения номеров протоколов IPv6 для замены конкретных номеров протоколов IP, включая icmp, ipv6, tcp и udp.

Описание параметров	*src-ipv6-prefix/prefix-len*: указывает, что IP-пакеты, отправляемые с хостов в указанном сегменте сети IPv6, фильтруются. **host** *src-ipv6-addr*: указывает, что пакеты IPv6, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что пакеты IPv6, отправляемые с любого хоста, фильтруются. *dst-ipv6-pfix/pfix-len*: указывает, что пакеты IPv6, отправленные с хостов в указанном сегменте сети IPv6, фильтруются. **host** *dst-ipv6-addr*: указывает, что пакеты IPv6, отправляемые на хост с указанным IP-адресом назначения, фильтруются. **any**: указывает, что пакеты IPv6, отправляемые на любой хост, фильтруются. ***op*** *dstport*: указывает, что пакеты TCP или UDP фильтруются на основе номера порта назначения L4. Значение параметра **op** может быть **eq** (равно), **neq** (не равно), **gt** (больше) или **lt** (меньше). **range** *lower upper*: указывает, что пакеты TCP или UDP с номером порта назначения L4 в указанном диапазоне фильтруются. **dscp** *dscp*: указывает, что пакеты IPv6 с указанным полем dcsp в заголовке фильтруются. **flow-label** *flow-label*: указывает, что пакеты IPv6 с указанным полем метки потока в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные пакеты IPv6, кроме первых фрагментов. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона. **log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе
Режим команд	Режим конфигурации IPv6 ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в режиме конфигурации ACL IPv6

- Чтобы отфильтровать пакеты IPv6, за исключением пакетов TCP или UDP, добавьте записи ACE в ACL IPv6 следующим образом:

Команда	[*sn*] { **permit** | **deny** } *protocol* { *src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any** } { *dst-ipv6-pfix/pfix len* | **host** *dst-ipv6-addr* | **any** } [**dscp** *dscp*] [**flow-label** *flow-label*] [**fragment**] [**time-range***tm-rng name*] [**log**]

Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен порядковому номеру последнего ACE в текущем ACL плюс число приращения (по умолчанию 10). Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *protocol*: указывает номер протокола IPv6. Значение находится в диапазоне от 0 до 255. Для облегчения использования система предоставляет часто используемые сокращения номеров протоколов IPv6 для замены конкретных номеров протоколов IP, включая icmp, ipv6, tcp и udp. *src-ipv6-prefix/prefix-len*: указывает, что IP-пакеты, отправляемые с хостов в указанном сегменте сети IPv6, фильтруются. **host** *src-ipv6-addr*: указывает, что пакеты IPv6, отправленные с хоста с указанным исходным IP-адресом, фильтруются. **any**: указывает, что пакеты IPv6, отправляемые с любого хоста, фильтруются. *dst-ipv6-pfix/pfix-len*: указывает, что пакеты IPv6, отправленные с хостов в указанном сегменте сети IPv6, фильтруются. **host** *dst-ipv6-addr*: указывает, что пакеты IPv6, отправляемые на хост с указанным IP-адресом назначения, фильтруются. **any**: указывает, что пакеты IPv6, отправляемые на любой хост, фильтруются. **dscp** *dscp*: указывает, что пакеты IPv6 с указанным полем dcsp в заголовке фильтруются. **flow-label** *flow-label*: указывает, что пакеты IPv6 с указанным полем метки потока в заголовке фильтруются. **fragment**: указывает, что фильтруются только фрагментированные пакеты IPv6, кроме первых фрагментов. **time-range** *time-range-name*: указывает, что этот ACE связан с временным диапазоном. ACE вступает в силу только в пределах этого временного диапазона. Подробнее о временном диапазоне см. в руководстве по настройке временного диапазона. **log**: указывает, что журналы будут периодически выводиться, если будут найдены пакеты, соответствующие ACE. Дополнительные сведения о журналах см. в разделе «Ведение журнала ACL» в этом документе

Режим команд	Режим конфигурации IPv6 ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в режиме конфигурации ACL IPv6

Применение ACL IPv6

Команда	**ipv6 traffic-filter** *acl-name* { **in** | **out** }
Описание параметров	*acl-name*: указывает имя ACL IPv6. **in**: указывает, что этот ACL контролирует входящие пакеты IPv6 интерфейса. **out**: указывает, что этот ACL контролирует исходящие пакеты IPv6 интерфейса
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эта команда заставляет ACL IPv6 действовать на входящие или исходящие пакеты указанного интерфейса

1.6.4.5. Пример конфигурации

Настройка ACL IPv6 для запрета доступа отдела исследований и разработок (R&D) к видеосерверу

Сценарий:

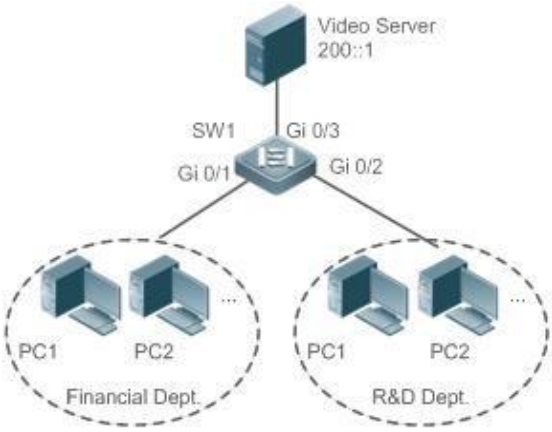

Рисунок 1-6.

Шаги настройки	• Настройте ACL IPv6. • Добавьте ACE в ACL IPv6, чтобы предотвратить доступ к видеосерверу. • Добавьте ACE в ACL IPv6, чтобы разрешить все пакеты IPv6. • Примените ACL IPv6 к входящему направлению интерфейса, подключенного к отделу исследований и разработок

SW1	sw1(config)#ipv6 access-list dev_deny_ipv6video sw1(config-ipv6-nacl)#deny ipv6 any host 200::1 sw1(config-ipv6-nacl)#permit ipv6 any any sw1(config-ipv6-nacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6video in
Проверка	На ПК отдела R&D пропинговать видеосервер. Убедитесь, что операция проверки связи не удалась
SW1	sw1(config)#show access-lists ipv6 access-list dev_deny_ipv6video 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Применяется на интерфейсе GigabitEthernet 0/2

1.6.5. Настройка ACL80

1.6.5.1. Эффект конфигурации

Если IP ACL, расширенный ACL MAC, экспертный расширенный ACL и ACL IPv6 с фиксированными полями сопоставления не могут соответствовать требованиям, настройте ACL80 для настройки полей пакета, которые необходимо сопоставить.

1.6.5.2. Шаги настройки

Настройка экспертного расширенного ACL

- (Обязательно) Настройте экспертный расширенный ACL, если вы хотите реализовать функцию ACL80. Подробнее о том, как настроить экспертный расширенный ACL, см. в соответствующих описаниях.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Экспертный расширенный ACL действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление записей ACE в экспертный расширенный ACL

(Обязательно) Добавьте записи ACE в экспертный расширенный ACL, чтобы настроить соответствующие поля. Если в экспертный расширенный ACL не добавлена ни одна запись ACE, запрещающие записи ACE будут отбрасывать все пакеты по умолчанию. Дополнительные сведения о том, как добавить ACE в экспертный расширенный список ACL, см. в соответствующих описаниях.

Применение экспертного расширенного ACL

- (Обязательно) Примените экспертный расширенный ACL к указанному интерфейсу, если вы хотите, чтобы этот ACL вступил в силу.
- Вы можете применить экспертный расширенный ACL к указанному интерфейсу устройств доступа, агрегации и ядра на основе распределения пользователей.

1.6.5.3. Проверка

- Используйте следующие методы для проверки эффектов конфигурации экспертного расширенного ACL:
- Запустите команду **ping**, чтобы проверить, вступили ли в силу настройки.
- Создайте пакеты, соответствующие ACE, чтобы проверить, действуют ли ACE.

1.6.5.4. Связанные команды

Настройка экспертного расширенного ACL

Команда	**expert access-list advanced** *acl-name*
Описание параметров	*acl-name*: указывает имя экспертного расширенного ACL. Имя представляет собой строку от 1 до 99 символов. Имя ACL не может начинаться с цифр (0–9), «in» или «out»
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить экспертный расширенный ACL и войти в режим конфигурации экспертных расширенных ACL

Добавление записей ACE в экспертный расширенный ACL

Команда	[*sn*] { **permit** | **deny** } *hex hex-mask offset*
Описание параметров	*sn*: указывает порядковый номер ACE. Значение находится в диапазоне от 1 до 2 147 483 647. Этот порядковый номер определяет приоритет этой записи ACE в ACL. Меньший порядковый номер указывает на более высокий приоритет. ACE с более высоким приоритетом будет предпочтительно использоваться для сопоставления пакетов. Если вы не укажете порядковый номер при добавлении ACE, система автоматически присвоит порядковый номер, который равен приращению (по умолчанию 10) плюс порядковый номер последнего ACE в текущем ACL. Например, если порядковый номер последней записи ACE равен 100, порядковый номер вновь добавленной записи ACE будет по умолчанию равен 110. Вы можете настроить приращение с помощью команды. **permit**: указывает, что ACE является разрешающим ACE. **deny**: указывает, что ACE является запрещающим ACE. *hex*: указывает пользовательское правило сопоставления, выраженное в шестнадцатеричном формате, например, 08c6b300. *hex-mask*: указывает соответствующую маску

Описание параметров	*offset*: указывает начальную позицию сопоставления. Например, если совпадающее содержимое — 08c6b300, совпадающая маска — 00ff0000, а начальная позиция — 6, сравнивается MAC-адрес назначения каждого пакета. Все пакеты, у которых второй байт MAC-адреса назначения равен d0, соответствуют этому ACE
Режим команд	Экспертный расширенный режим конфигурации ACL
Руководство по использованию	Запустите эту команду, чтобы добавить записи ACE в экспертный расширенный режим конфигурации ACL

Применение экспертного расширенного ACL

Команда	**expert access-group** *acl-n* { **in** | **out** }
Описание параметров	*acl-id*: указывает, что к интерфейсу будет применяться пронумерованный экспертный расширенный ACL. *acl-name*: указывает, что к интерфейсу будет применяться именованный экспертный расширенный ACL. **in**: указывает, что этот ACL контролирует входящие пакеты L2 интерфейса. **out**: указывает, что этот ACL контролирует исходящие пакеты L2 интерфейса
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эта команда заставляет экспертный расширенный ACL действовать на входящие или исходящие пакеты указанного интерфейса

1.6.5.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Настройка ACL80 для ограничения ресурсов, доступных посетителям (требуется, чтобы посетители и сотрудники не могли общаться друг с другом, посетители могли получить доступ к серверу общедоступных ресурсов, но не к серверу финансовых данных компании).

Сценарий:

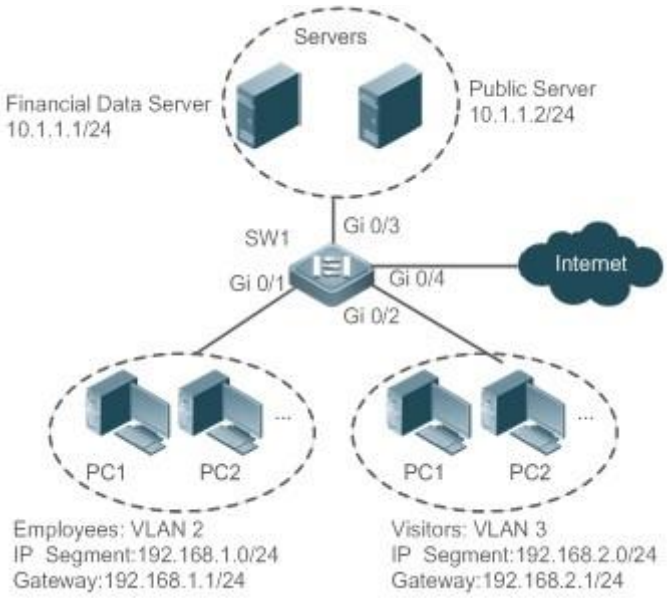

Рисунок 1-7.

Шаги настройки	• Настройте экспертный расширенный ACL. • Добавьте ACE, чтобы запретить пакеты, отправляемые с ПК в зоне для посетителей (VLAN 3) на ПК сотрудников в VLAN 2. • Добавьте ACE, чтобы запретить посетителям доступ к серверу финансовых данных компании. • Добавьте ACE, чтобы разрешить все пакеты. • Примените ACL к входящему направлению интерфейса коммутатора, который подключается к гостевой зоне
SW1	sw1(config)#expert access-list advanced acl80-guest sw1(config-exp-dacl)#deny 08C6B3 FFFFFF 42 sw1(config-exp-dacl)#deny 0A010101 FFFFFFFF 42 sw1(config-exp-dacl)#permit 0806 FFFF 24 sw1(config-exp-dacl)#permit 0800 FFFF 24 sw1(config-exp-dacl)#exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)#expert access-group acl80-guest in
Проверка	• На компьютере посетителя пропингуйте сервер финансовых данных. Убедитесь, что операция проверки связи не удалась. • На компьютере посетителя пропингуйте сервер общедоступного ресурса. Убедитесь, что операция **ping** прошла успешно. • На ПК посетителя пропинговать адрес шлюза 192.168.1.1 сотрудника. Убедитесь, что операция проверки связи не удалась

Проверка	• На компьютере посетителя подключитесь к Интернету, например, посетите веб-сайт QTECH. Убедитесь, что веб-страницу можно открыть
SW1	sw1(config)#show access-lists expert access-list advanced sss 10 deny 08C6B3 FFFFFF 42 20 deny 0A010101 FFFFFFFF 42 30 permit 0806 FFFF 24 40 permit 0800 FFFF 24 expert access-group acl80-guest in Применяется на интерфейсе GigabitEthernet 0/2

1.6.6. Настройка перенаправления ACL

1.6.6.1. Эффект конфигурации

Настройте функцию перенаправления ACL на указанном интерфейсе, чтобы напрямую перенаправлять указанные пакеты на интерфейсе или на всех интерфейсах на указанный порт для дальнейшей пересылки.

1.6.6.2. Шаги настройки

Настройка ACL

- (Обязательно) Чтобы реализовать перенаправление ACL, необходимо сначала настроить ACL, например, расширенный IP-адрес, расширенный MAC-адрес или экспертный расширенный ACL. Дополнительные сведения о настройке ACL см. в соответствующих описаниях.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. ACL IPv6 действует только на локальном устройстве и не влияет на другие устройства в сети.

Добавление ACE в ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, функция перенаправления ACL недоступна. Подробнее о том, как добавить ACE в ACL, см. в соответствующих описаниях.

Настройка перенаправления ACL

- (Обязательно) Включите перенаправление ACL на указанном интерфейсе, если вы хотите реализовать перенаправление ACL.
- Вы можете настроить функцию перенаправления ACL на указанном интерфейсе устройств доступа, агрегации и ядра на основе распределения пользователей.

1.6.6.3. Проверка

Отправьте пакеты, соответствующие ACE, на порт, где включено перенаправление ACL, а затем используйте программное обеспечение для захвата пакетов на порту назначения, чтобы проверить, действует ли функция перенаправления ACL.

1.6.6.4. Связанная команда

Настройка списка контроля доступа

Подробнее о том, как настроить ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Добавление ACE в ACL

Подробнее о том, как добавлять записи ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Настройка перенаправления ACL на интерфейсе

Команда	**redirect destination interface** *interface-name* **acl** {*acl-id* | *acl-name* } **in**
Описание параметров	**interface** *interface-name*: указывает имя порта назначения для перенаправления. *acl-id*: указывает идентификатор ACL. *acl-name*: указывает имя ACL. **in**: указывает, что входящие пакеты интерфейса перенаправляются
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы перенаправить входящие пакеты интерфейса, соответствующие ACE, на порт назначения для дальнейшей пересылки

1.6.6.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Включение перенаправления ACL для перенаправления пакетов, отправленных с хоста 10.1.1.1, на устройство захвата пакетов для анализа

Сценарий:

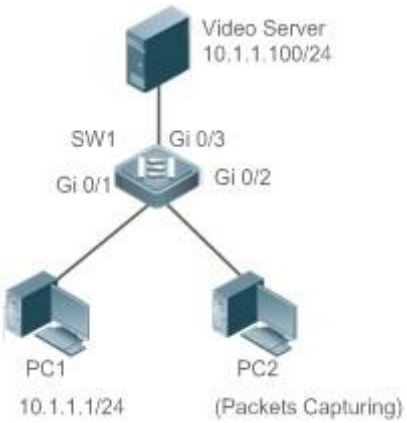

Рисунок 1-8.

Шаги настройки	• Настраивает IP ACL. • Добавьте ACE в IP ACL, чтобы разрешить отправку пакетов с хоста 10.1.1.1. • Включите перенаправление ACL на порту Gi 0/1 и установите порт назначения на Gi 0/2
SW1	sw1(config)#ip access-list standard 1 sw1 (config-std-nacl)#permit host 10.1.1.1 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# redirect destination interface gigabitEthernet 0/2 acl 1
Проверка	Захват пакетов на ПК 2. Пропингуйте видеосервер на ПК 1. Убедитесь, что запросы ICMP, отправленные с ПК 1, перехватываются на ПК 2
SW1	sw1#show access-lists ip access-list standard 1 10 permit host 10.1.1.1 sw1#show redirect interface gigabitEthernet 0/1 acl redirect configuration on interface gigabitEthernet 0/1 redirect destination interface gigabitEthernet 0/2 acl 1 in

1.6.7. Настройка глобальной Security ACL

1.6.7.1. Эффект конфигурации

Настройте глобальный Security ACL, чтобы предотвратить доступ внутренних компьютеров компании к незаконным веб-сайтам или предотвратить атаку вирусов на внутреннюю сеть компании. Вы также можете настроить эксклюзивные интерфейсы, чтобы разрешить определенным отделам компании доступ к внешним веб-сайтам.

1.6.7.2. Шаги настройки

Настройка ACL

- (Обязательно) Настройте IP ACL, если вы хотите глобально защитить внутреннюю сеть. Дополнительные сведения о методе настройки см. в соответствующих описаниях.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Конфигурации действуют только на локальном устройстве и не влияют на другие устройства в сети.

Добавление ACE в ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, это эквивалентно тому, что глобальный Security ACL не существует. Подробнее о том, как добавить ACE в ACL, см. в соответствующих описаниях.

Настройка глобального Security ACL

- (Обязательно) Включите функцию глобальной безопасности, если вы хотите, чтобы глобальный Security ACL вступили в силу.
- Вы можете настроить глобальный Security ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.7.3. Проверка

Во внутренней сети, защищенной глобальным Security ACL, пропингуйте веб-сайт или устройство, запрещенные ACE, чтобы проверить, действует ли глобальный Security ACL.

1.6.7.4. Связанная команда

Настройка AC

Дополнительные сведения о методе настройки см. в предыдущих описаниях ACL.

Добавление ACE в ACL

Дополнительные сведения о методе настройки см. в предыдущих описаниях ACL.

Настройка глобального Security ACL

Команда	{ **ip** | **mac** | expert } **access-group** *acl-id* { **in** | **out** }
Описание параметров	*acl-id*: указывает идентификатор IP ACL. **in**: фильтрует входящие пакеты устройства. **out**: фильтрует исходящие пакеты устройства
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы включить глобальный Security ACL, чтобы ACL действовал на всех интерфейсах L2 устройства

Настройка эксклюзивнго интерфейса глобального Security ACL

Команда	**no global ip access-group**
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы аннулировать глобальный Security ACL на указанном интерфейсе

1.6.7.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Настройка глобального Security ACL для предотвращения доступа отдела исследований и разработок к серверу отдела продаж, но разрешения доступа отдела продаж к этому серверу

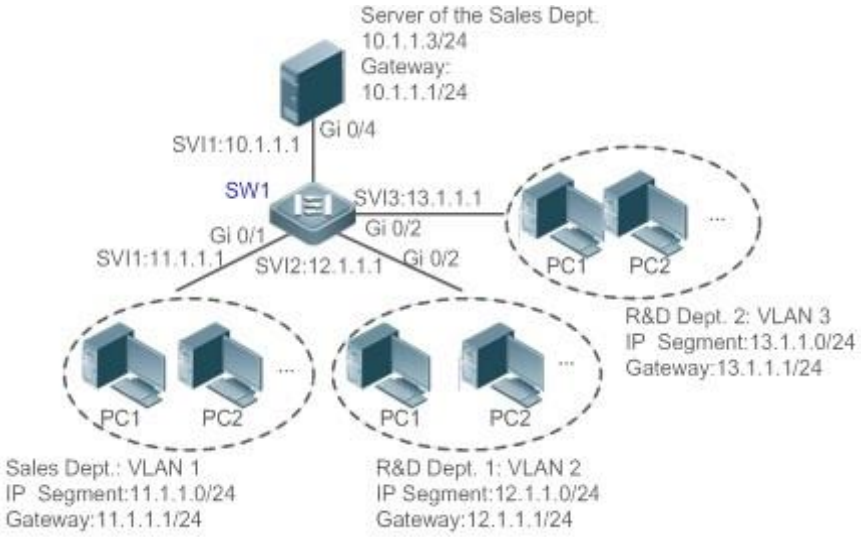

Рисунок 1-9.

Шаги настройки	• Настройте расширенный IP ACL «ip_ext_deny_dst_sale_server». • Добавьте ACE, который запрещает устройству пересылать пакеты на узел назначения 10.1.1.3/24. • Настройте ACL «ip_ext_deny_dst_sale_server» как глобальный Security ACL. • Настройте интерфейс, напрямую связанный с отделом продаж, в качестве эксклюзивного интерфейса глобального Security ACL
SW1	sw1(config)#ip access-list extended ip_ext_deny_dst_sale_server sw1(config-ext-nacl)# deny ip any host 10.1.1.3 sw1(config-ext-nacl)#exit sw1(config)#ip access-group ip_ext_deny_dst_sale_server in sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# no global ip access-group
Проверка	• На ПК отдела продаж пропинговать сервер отдела продаж. Убедитесь, что операция **ping** прошла успешно. • На компьютерах отдела R&D 1 и отдела R&D 2 пропинговать сервер отдела продаж. Убедитесь, что операции проверки связи не выполняются

```
sw1#show access-lists
ip access-list extended ip_ext_deny_dst_sale_server
10 deny ip any host 10.1.1.3
sw1#show running
……
!
ip access-group ip_ext_deny_dst_sale_server in
!
!
!
```

1.6.8. Настройка канала безопасности

1.6.8.1. Эффект конфигурации

Настройте канал безопасности, чтобы пакеты, отвечающие правилам канала безопасности, могли обходить проверки приложений контроля доступа. Настройте канал безопасности, если приложение управления доступом (например, DOT1X) включено на uplink-интерфейсе пользователя, но пользователю должно быть разрешено входить на веб-сайт для загрузки некоторых ресурсов (например, загрузки ПО QTECH) перед аутентификацией DOT1X.

1.6.8.2. Шаги настройки

Настройка ACL

- (Обязательно) Настройте ACL перед настройкой канала безопасности. Дополнительные сведения о методе настройки см. в предыдущих описаниях.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Конфигурации действуют только на локальном устройстве и не влияют на другие устройства в сети.

Добавление ACE в ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен для ACL, это эквивалентно тому, что канал безопасности не вступает в силу. Подробнее о том, как добавить ACE в ACL, см. в соответствующих описаниях.

Настройка канала безопасности на указанном интерфейсе или глобально

- Настройте канал безопасности на интерфейсе, если вы хотите, чтобы этот канал безопасности работал на интерфейсе. Настройте глобальный канал безопасности, если вы хотите, чтобы этот канал безопасности действовал глобально. Вы должны настроить канал безопасности на основе интерфейса или глобальный канал безопасности.
- Вы можете настроить канал безопасности для устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

Настройка эксклюзивного интерфейса для канала глобальной безопасности

(Опционально) Настройте интерфейс как эксклюзивный интерфейс для глобального канала безопасности, если вы не хотите, чтобы глобальный канал безопасности действовал на этом интерфейсе.

Настройка приложения контроля доступа

- (Опционально) Вы можете включить функцию DOT1X или веб-аутентификации для проверки функции канала безопасности.
- Вы можете настроить функцию управления доступом на устройствах доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.8.3. Проверка

На ПК, находящемся под контролем приложения управления доступом, пропингуйте ресурсы (устройства или серверы), которым разрешено обходить проверку приложения управления доступом, чтобы проверить конфигурацию канала безопасности.

1.6.8.4. Связанная команда

Настройка ACL

Подробнее о том, как настроить ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Добавление ACE в ACL

Подробнее о том, как добавлять записи ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Настройка канала безопасности на интерфейсе

Команда	**security access-group** {*acl-id* | *acl-name* }
Описание параметров	*acl-id*: указывает идентификатор ACL, настроенного в качестве канала безопасности. *acl-name*: указывает имя ACL, настроенного в качестве канала безопасности
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы настроить указанный ACL в качестве канала безопасности на указанном интерфейсе

Настройка глобального канала безопасности

Команда	**security global access-group** {*acl-id* | *acl-name* }
Описание параметров	*acl-id*: указывает идентификатор ACL, настроенного в качестве канала безопасности. *acl-name*: указывает имя ACL, настроенного в качестве канала безопасности

Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить указанный ACL в качестве глобального канала безопасности

Настройка эксклюзивного интерфейса для канала глобальной безопасности

Команда	**security uplink enable**
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы настроить указанный интерфейс в качестве эксклюзивного интерфейса глобального канала безопасности

1.6.8.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Включение аутентификации DOT1X и настройка канала безопасности, чтобы пользователи могли загружать программное обеспечение QTECH с сервера до аутентификации

Сценарий:

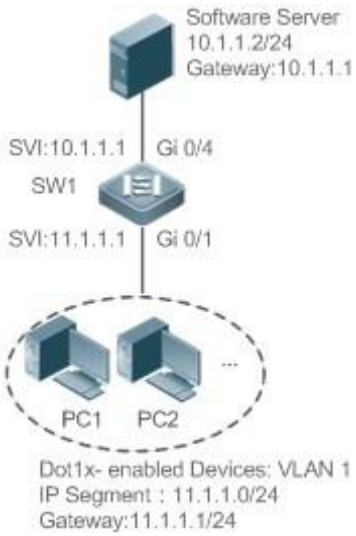

Рисунок 1-10.

Шаги настройки	• Настройте экспертный расширенный ACL "exp_ext_esc". • Добавьте ACE, чтобы разрешить пересылку пакетов на узел назначения 10.1.1.2. • Добавьте ACE, чтобы разрешить пакеты DHCP. • Добавьте ACE, чтобы разрешить пакеты ARP. • На интерфейсе, где включена аутентификация DOT1X, настройте ACL «exp_ext_esc» в качестве канала безопасности

SW1	sw1(config)#expert access-list extended exp_ext_esc sw1(config-exp-nacl)# permit ip any any host 10.1.1.2 any sw1(config-exp-nacl)# permit 0x0806 any any any any any sw1(config-exp-nacl)# permit tcp any any any any eq 67 sw1(config-exp-nacl)# permit tcp any any any any eq 68 sw1(config)#int gigabitEthernet 0/1 sw1(config-if-GigabitEthernet 0/1)# security access-group exp_ext_esc
Проверка	• На ПК отдела продаж пропинговать сервер отдела продаж. Убедитесь, что операция **ping** прошла успешно. • На компьютерах отдела R&D 1 и отдела R&D 2 пропинговать сервер отдела продаж. Убедитесь, что операции проверки связи не выполняются
	sw1#show access-lists expert access-list extended exp_ext_esc 10 permit ip any any host 10.1.1.2 any 20 permit arp any any any any any 30 permit tcp any any any any eq 67 40 permit tcp any any any any eq 68…… sw1#show running-config interface gigabitEthernet 0/1 Конфигурация построения... Текущая конфигурация: 59 байт интерфейс GigabitEthernet 0/1 security access-group exp_ext_esc

1.6.9. Настройка ACE на основе временного диапазона

1.6.9.1. Эффект конфигурации

Настройте ACE на основе временного диапазона, если вы хотите, чтобы некоторые ACE вступали в силу или становились недействительными в указанный период времени, например, в некоторых временных диапазонах в течение недели.

1.6.9.2. Шаги настройки

Настройка ACL

- (Обязательно) Настройте ACL, если вы хотите, чтобы ACE вступали в силу в указанном диапазоне времени. Дополнительные сведения о методе настройки см. в предыдущих описаниях.

- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Конфигурации действуют только на локальном устройстве и не влияют на другие устройства в сети.

Добавление ACE с указанным диапазоном времени

(Обязательно) Укажите временной диапазон при добавлении ACE. Для получения подробной информации о том, как настроить временной диапазон, см. руководство по настройке, связанное с временным диапазоном.

Применение ACL

- (Обязательно) Примените ACL к указанному интерфейсу, если вы хотите, чтобы ACE вступали в силу в указанном диапазоне времени.
- Вы можете применить IP ACL к указанному интерфейсу устройств доступа, агрегации и ядра в зависимости от распределения пользователей.

1.6.9.3. Проверка

В диапазоне времени, в течение которого настроенный ACE вступает в силу или становится недействительным, запустите команду **ping** или создайте пакеты, соответствующие ACE, чтобы проверить, вступает ли ACE в силу или становится недействительным.

1.6.9.4. Связанная команда

Настройка ACL

Дополнительные сведения о командах настройки ACL см. в более ранних описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Добавление ACE с указанным диапазоном времени

Дополнительные сведения о командах настройки ACE см. в более ранних описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Применение ACL

Дополнительные сведения о команде для применения ACL см. в более ранних описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

1.6.9.5. Пример конфигурации

Следующий пример конфигурации описывает только конфигурации, связанные с ACL.

Добавление ACE с указанным временным диапазоном, чтобы разрешить отделу исследований и разработок доступ в Интернет с 12:00 до 13:30 Каждый день

Сценарий:

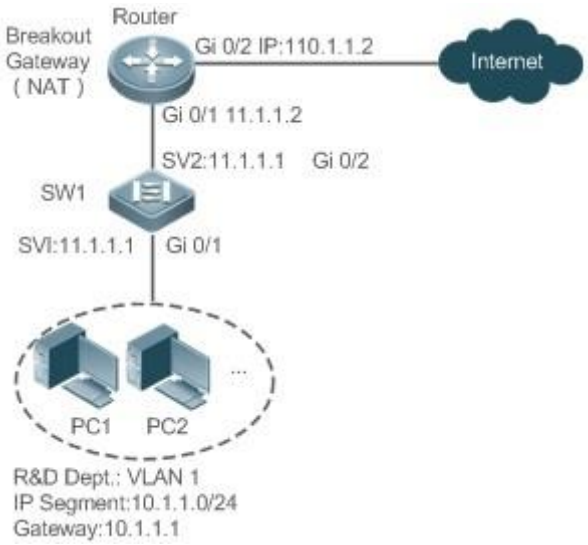

Рисунок 1-11.

Шаги настройки	• Настройте временной диапазон с именем «access-internet» и добавьте запись временного диапазона между 12:00 и 13:30 каждый день. • Настройте IP ACL "ip_std_internet_acl". • Добавьте ACE, чтобы разрешить пакеты с исходным IP-адресом в сетевом сегменте 10.1.1.0/24, и свяжите этот ACE с часовым поясом «access-internet». • Добавьте ACE для запрета пакетов с исходным IP-адресом сегмента сети 10.1.1.0/24. Доступ к Интернету запрещен, кроме как в указанный период времени. • Добавьте ACE, чтобы разрешить все пакеты. • Примените ACL к исходящему направлению интерфейса, подключенного к коммутационному шлюзу
SW1	QTECH(config)# time-range access-internet QTECH(config-time-range)# periodic daily 12:00 to 13:30 QTECH(config-time-range)# exit sw1(config)# ip access-list standard ip_std_internet_acl sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255 sw1(config-std-nacl)# permit any sw1(config-std-nacl)# exit sw1(config)#int gigabitEthernet 0/2 sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl out

Проверка	• В промежутке времени с 12:00 до 13:30 посетите веб-сайт QTECH на ПК отдела исследований и разработок. Убедитесь, что веб-сайт можно открыть в обычном режиме. • Вне диапазона времени с 12:00 до 13:30 посетите веб-сайт QTECH на ПК отдела исследований и разработок. Убедитесь, что веб-сайт не может быть открыт
SW1	sw1#show time-range time-range entry: access-internet (inactive) periodic Daily 12:00 to 13:30 sw1#show access-lists ip access-list standard ip_std_internet_acl 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive) 20 deny 10.1.1.0 0.0.0.255 30 permit any sw1#show access-group ip access-group ip_std_internet_acl out Применяется на интерфейсе GigabitEthernet 0/2

1.6.10. Настройка комментариев для ACL

1.6.10.1. Эффект конфигурации

Если во время обслуживания сети многие ACL настроены без каких-либо комментариев, впоследствии эти списки сложно различить. Вы можете настроить комментарии для ACL, чтобы лучше понять предполагаемое использование ACL.

1.6.10.2. Шаги настройки

Настройка ACL

- (Обязательно) Настройте ACL перед настройкой канала безопасности. Дополнительные сведения о методе настройки см. в предыдущих описаниях.
- Вы можете настроить этот ACL для устройств доступа, агрегации и ядра в зависимости от распределения пользователей. Конфигурации действуют только на локальном устройстве и не влияют на другие устройства в сети.

Настройка комментариев для ACL

(Опционально) Настройте комментарии для ACL, чтобы упростить управление и понимание настроенных ACL.

Добавление ACE в ACL

(Опционально) ACL может содержать ноль или несколько записей ACE. Если ACE не настроен, это эквивалентно тому, что канал безопасности не действует. Подробнее о том, как добавить ACE в ACL, см. в соответствующих описаниях.

Настройка комментариев для ACE

(Опционально) Чтобы облегчить понимание настроенного ACL, вы можете настроить комментарии для ACE в дополнение к комментариям для ACL.

1.6.10.3. Проверка

Запустите на устройстве команду **show access-lists**, чтобы отобразить комментарии, настроенные для ACL.

1.6.10.4. Связанная команда

Настройка ACL

Подробнее о том, как настроить ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Настройка комментария для ACL

Используйте любой из следующих двух методов для настройки комментария для указанного ACE в ACL:

Команда	**[sn] remark** *comment*
Описание параметров	*comment*: указывает комментарий. Значение представляет собой строку от 1 до 100 символов. Комментарий длиннее 100 символов будет обрезан до 100 символов. **sn**: указывает идентификатор ACE
Режим команд	Режим конфигурации ACL
Руководство по использованию	Запустите эту команду, чтобы настроить комментарий для указанной записи ACE в ACL. Если **sn** не настроен, комментарий настраивается для последней ACE

Команда	**access-list** *acl-id* **sn-remark** *comment*
Описание параметров	*acl-id*: указывает идентификатор ACL. *comment*: указывает комментарий. Значение представляет собой строку от 1 до 100 символов. Комментарий длиннее 100 символов будет обрезан до 100 символов. **sn**: указывает идентификатор ACE
Режим команд	Режим конфигурации

Руководство по использованию	Запустите эту команду, чтобы настроить комментарий для указанной записи ACE в ACL. Если **sn** не настроен, комментарий настраивается для последней ACE

Добавление ACE в ACL

Подробнее о том, как добавлять записи ACE в ACL, см. в предыдущих описаниях IP ACL, расширенного ACL MAC, экспертного расширенного ACL или ACL IPv6.

Настройка комментариев для ACE

Используйте любой из следующих двух методов, чтобы настроить комментарий для ACE:

Команда	**remark** *comment*
Описание параметров	*comment*: указывает комментарий. Значение представляет собой строку от 1 до 100 символов. Комментарий длиннее 100 символов будет обрезан до 100 символов
Режим команд	Режим конфигурации ACL
Руководство по использованию	Запустите эту команду, чтобы настроить комментарий для указанного ACE

Команда	**access-list** *acl-id* **remark** *comment*
Описание параметров	*acl-id*: указывает идентификатор ACL. *comment*: указывает комментарий. Значение представляет собой строку от 1 до 100 символов. Комментарий длиннее 100 символов будет обрезан до 100 символов
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить комментарий для указанного ACE

1.7. Мониторинг

1.7.1. Очистка

Описание	Команда
Очищает счетчики сопоставления пакетов ACL	**clear counters access-list** [*acl-id* | *acl-name*]

Описание	Команда
Очищает счетчики пакетов, соответствующих запрещающим ACE	**clear access-list counters [***acl-id* |*acl-name* **]**

1.7.2. Отображение

Описание	Команда
Отображает основные ACL	**show access-lists** [*acl-id* | *acl-ame*] [**summary**]
Отображает записи ACE перенаправления, привязанные к указанному интерфейсу. Если интерфейс не указан, отображаются ACE перенаправления, привязанные ко всем интерфейсам	**show redirect** [**interface** *interface-name*]
Отображает конфигурации ACL, примененные к интерфейсу	**show access-group** [**interface** *interface-name*]
Отображает конфигурации IP ACL, примененные к интерфейсу	**show ip access-group** [**interface** *interface-name*]
Отображает расширенные конфигурации ACL MAC, примененные к интерфейсу	**show mac access-group** [**interface** *interface-name*]
Отображает экспертные расширенные конфигурации ACL, примененные к интерфейсу	**show expert access-group** [**interface** *interface-name*]
Отображает конфигурации ACL IPv6, примененные к интерфейсу	**show ipv6 traffic-filter** [**interface** *interface-name*]
Отображает информацию TCAM или указанную информацию TCAM	**show acl res** [**dev** *dev-num* [**slot** *slot-num*]]

1.7.3. Отладка

Системные ресурсы заняты при выводе отладочной информации. Поэтому отключите отладку сразу после использования.

Описание	Команда
Отладка работающего процесса ACL	**debug acl acld event**
Отладка клиентов ACL	**debug acl acld client-show**

Описание	Команда
Отладка списков ACL, созданные всеми клиентами ACL	**debug acl acld acl-show**

2. НАСТРОЙКА QOS

2.1. Обзор

Качество обслуживания (QoS) позволяет обеспечить хорошие возможности обслуживания для указанной сети с использованием различных технологий инфраструктуры.

Когда пропускная способность сети достаточна, все потоки данных могут быть правильно обработаны; когда происходит перегрузка сети, все потоки данных могут быть отброшены. Чтобы удовлетворить требования пользователей к различным приложениям и различным уровням качества обслуживания, сеть должна иметь возможность распределять и планировать ресурсы на основе требований пользователей и обеспечивать различные уровни качества обслуживания для различных потоков данных. В частности, сеть может обрабатывать важные пакеты данных в режиме реального времени с более высоким приоритетом и обрабатывать пакеты не в реальном времени и общие пакеты данных с более низким приоритетом и даже отбрасывать пакеты данных при перегрузке сети.

Используемый традиционными сетями «лучший» механизм переадресации больше не может удовлетворять требованиям, и тогда возникает QoS. Устройства с поддержкой QoS обеспечивают качество передачи QoS. Приоритет передачи может быть назначен потокам данных типа, чтобы идентифицировать важность потоков данных. Затем устройства предоставляют политики пересылки для различных приоритетов, уменьшения перегрузки и другие механизмы для предоставления специальных услуг передачи для этих потоков данных. Сетевое окружение, настроенное с QoS, может обеспечить предсказуемость производительности сети, эффективное распределение пропускной способности сети и разумное использование сетевых ресурсов.

2.2. Приложения

Приложение	Описание
Ограничение скорости интерфейса + перемаркировка приоритета	Основываясь на различных требованиях к обслуживанию кампусной сети, обеспечьте управление скоростью и приоритетную обработку исходящего трафика учебного корпуса, лабораторий и общежития
Изменение приоритета + планирование очереди	Обеспечить приоритетную обработку и контроль пропускной способности для трафика внутреннего доступа к серверам предприятия

2.2.1. Ограничение скорости интерфейса + перемаркировка приоритета

2.2.1.1. Сценарий

Чтобы соответствовать служебным требованиям нормального обучения, школа выдвигает следующие требования:

- Ограничивайте трафик доступа в Интернет до 100 МБ и отбрасывайте пакеты сверх лимита.
- Ограничивайте исходящий трафик здания общежития до 50M и отбрасывайте пакеты сверх лимита.

- Ограничивайте скорость пакетов с приоритетом DSCP 7, отправленных из лабораторий менее 20M, и измените приоритеты DSCP для этих пакетов, скорость которых превышает 20M, на 16.
- Ограничивайте исходящий трафик учебного корпуса до 30M отбрасывайте пакеты сверх лимита.

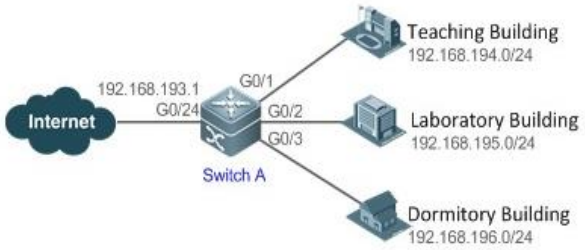

Рисунок 2-1.

Школа подключает GigabitEthernet 0/24 коммутатора A к Интернету в uplink-канале и подключает GigabitEthernet 0/1, GigabitEthernet 0/2 и GigabitEthernet 0/3 коммутатора A к учебному корпусу, лаборатории (192.168.195.0) и корпусу общежития (192.168.196.0) в downlink-канале соответственно.

2.2.1.2. Развертывание

- Настройте ограничение скорости интерфейса QoS для интерфейса G0/24 коммутатора A для подключения к Интернету. Настройте ограничение скорости QoS для пакетов, отправляемых из общежития на коммутаторе A.
- Установите ограничение скорости для пакетов с приоритетом DSCP 7, отправляемых из лаборатории, на 20M и перемаркируйте приоритет DSCP для пакетов, выходящих за пределы ограничения скорости, на 16.
- Настройте ограничение скорости QoS для пакетов, отправляемых из учебного корпуса на коммутаторе A.

2.2.2. Изменение приоритета + планирование очереди

2.2.2.1. Сценарий

Настройте перемаркировку приоритетов и планирование очередей в соответствии со следующими требованиями:

- Когда отдел исследований и разработок и отдел маркетинга получают доступ к серверам, приоритеты пакетов сервера следующие:
  почтовый сервер> файловый сервер> сервер запросов о зарплате.
- Независимо от того, когда отдел кадров получает доступ к Интернету или серверам, коммутатор обрабатывает соответствующие пакеты с наивысшим приоритетом.
- Поскольку при работе коммутатора часто возникает перегрузка сети, для обеспечения бесперебойной работы бизнеса необходимо использовать планирование очереди WRR для планирования IP-пакетов для отделов исследований и разработок, и маркетинга для доступа к почтовой базе данных, файловой базе данных и базе данных запросов о заработной плате на основе соотношения 6:2:1.

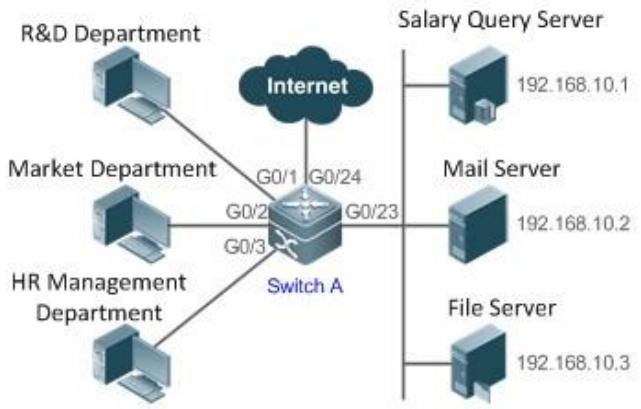

Рисунок 2-2.

Отделы исследований и разработок, маркетинга и управления персоналом получают доступ к интерфейсам GigabitEthernet 0/1, GigabitEthernet 0/2 и GigabitEthernet 0/3 коммутатора A соответственно. Сервер запросов о зарплате, почтовый сервер и файловый сервер подключены к GigabitEthernet 0/23 коммутатора A.

2.2.2.2. Развертывание

- Настройте значения CoS потоков данных для доступа к разным серверам, чтобы гарантировать, что коммутатор обрабатывает пакеты для разных серверов с разными приоритетами.
- Установите значение CoS интерфейса по умолчанию на конкретное значение, чтобы гарантировать, что коммутатор обрабатывает пакеты, отправленные отделом управления персоналом, с наивысшим приоритетом.
- Настройте планирование очереди WRR, чтобы гарантировать, что пакеты данных передаются в определенном соотношении количества.

2.3. Особенности

2.3.1. Основная концепция

2.3.1.1. DiffServ

Режим дифференцированных услуг (DiffServ) — это система IETF, на основе которой QoS реализуется в продуктах QTECH. Система DiffServ классифицирует все пакеты, передаваемые в сети, по разным типам. Информация о классификации включена в заголовки пакетов уровней 2/3, включая приоритеты 802.1P, IP и IP DSCP.

В сети, совместимой с DiffServ, все устройства применяют одну и ту же политику службы передачи к пакетам, содержащим одинаковую информацию о классификации, и применяют разные политики службы передачи к пакетам, содержащим различную информацию о классификации. Информация о классификации пакетов либо назначается хостами или другими устройствами в сети, либо назначается на основе различных политик приложений или различного содержимого пакетов. На основании классификационной информации, содержащейся в пакетах, устройство может предоставлять разные приоритеты передачи для разных потоков пакетов, резервировать полосу пропускания для определенных потоков пакетов, отбрасывать определенные пакеты с более низким приоритетом или выполнять некоторые другие действия.

2.3.1.2. Приоритет 802.1P (PRI)

Приоритет 802.1P расположен в заголовке пакета уровня 2 с заголовком 802.1Q и используется в сценариях, где заголовки уровня 3 не нужно анализировать, а QoS необходимо реализовать на уровне 2.

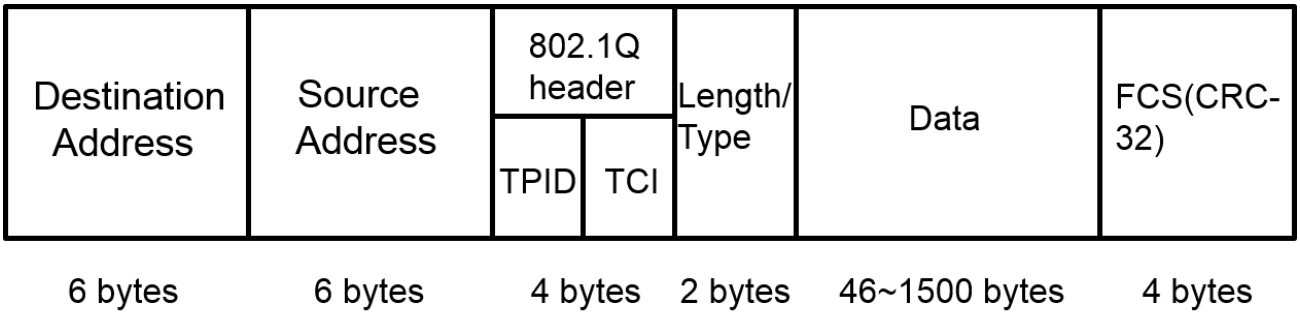

Рисунок 2-3. Структура пакета уровня 2

Как показано на рисунке выше, 4-байтовый заголовок 802.1Q содержит 2-байтовый идентификатор протокола тега (TPID), значение которого равно 0x8100, и 2-байтовую управляющую информацию тега (TCI). Первые три бита TCI указывают приоритет 802.1P.

2.3.1.3. Приоритет IP (IP PRE) и приоритет DSCP

Приоритеты IP-пакетов определяются приоритетами IP PRE и DSCP. Поле типа обслуживания (ToS) заголовка IPv4 состоит из 8 битов; где первые три бита указывают приоритет IP (IP PRE) в диапазоне от 0 до 7. RFC 2474 переопределяет поле ToS заголовка IPv4, которое называется полем дифференцированных услуг (DS). Приоритет точки кода дифференцированных услуг (DSCP) определяется первыми 6 битами (биты от 0 до 5) поля DS и первыми 6 битами поля класса трафика в заголовке IPv6.

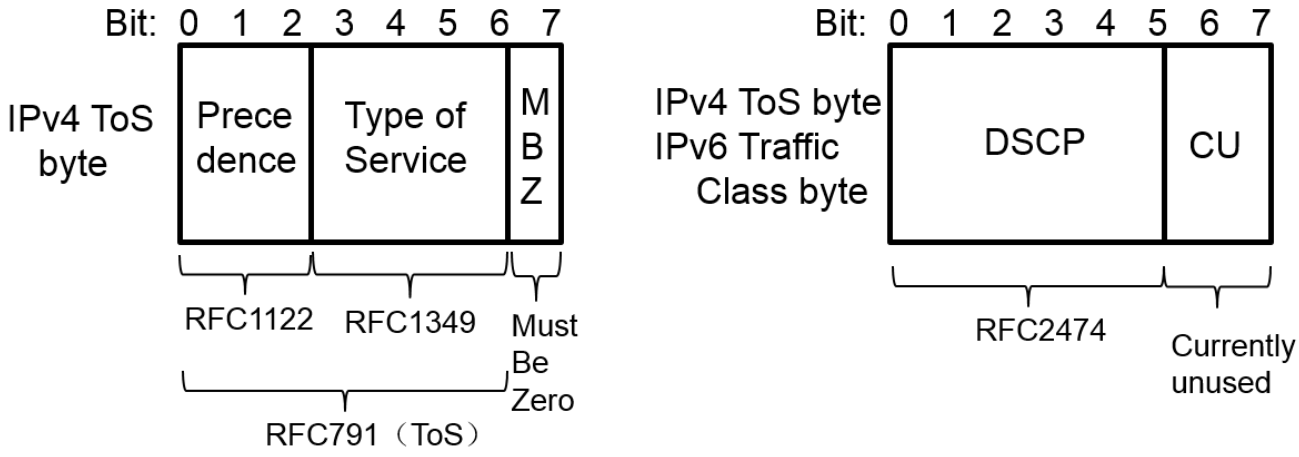

Рисунок 2-4. Расположение приоритетов IP PRE и DSCP в пакетах IPv4/IPv6

2.3.1.4. CoS

Класс обслуживания (CoS). Продукты QTECH преобразуют приоритеты пакетов в значения CoS, чтобы идентифицировать локальные приоритеты пакетов и определять идентификатор входной очереди, когда пакеты отправляются с выходного интерфейса.

2.3.2. Обзор

Особенность	Описание
Классификация потоков	Классификация потоков использует определенные правила для идентификации пакетов с одинаковыми характеристиками и является предпосылкой и основой для различения сетевых служб
Приоритетная маркировка и сопоставление	Помечает приоритеты пакетов указанными значениями и сопоставляет значения с соответствующими значениями CoS
Контроль трафика	Контролирует спецификацию трафика, поступающего в сеть, ограничивает трафик в разумных пределах и отбрасывает трафик за пределами лимита или изменяет приоритет трафика
Управление перегрузками	Определяет последовательность пакетов данных, отправляемых с интерфейса, на основе приоритетов пакетов данных и убеждается, что ключевые услуги могут быть обработаны вовремя, когда возникает перегрузка
Предотвращение перегрузки	Отслеживает использование очереди выходного интерфейса и снижает нагрузку на сеть, активно отбрасывая пакеты и регулируя сетевой трафик при перегрузке сети

2.3.3. Классификация потоков

Классификация потоков использует определенные правила для идентификации пакетов с одинаковыми характеристиками и является предпосылкой и основой для различения сетевых служб. Правила классификации потоков используются для того, чтобы различать разные пакеты в сети и задавать разные параметры QoS для пакетов на разных уровнях обслуживания.

2.3.3.1. Принцип работы

Правилами классификации потоков могут быть сопоставление приоритетов PRE или DSCP IP-пакетов или классификация пакетов путем идентификации содержимого пакета с помощью ACL. Вы можете определить привязку между несколькими потоками и поведением потоков, используя команды для формирования политик, которые можно применять к интерфейсам для классификации и обработки потоков.

Политика качества обслуживания

Политика QoS состоит из трех элементов: класс, поведение потока и политика.

- Класс

Класс идентифицирует потоки и содержит имя класса и правила класса. Вы можете определить правила класса, используя команды для классификации пакетов.

- Поведение потока

Поведение потока определяет действия QoS, предпринимаемые для пакетов, включая маркировку приоритетов и контроль трафика для пакетов.

- Политика

Плитика связывает конкретный класс и конкретное поведение потока и включает имя политики, имена связанных классов и поведение потока. Вы можете связать указанный класс и поведение потока с помощью политики QoS и применить политику к одному или нескольким интерфейсам.

Группа логических интерфейсов QoS

Вы можете указать ряд интерфейсов в качестве группы логических интерфейсов QoS (включая как AP, так и интерфейсы Ethernet) и связать политики с группой логических интерфейсов для обработки QoS. Возьмем, к примеру, ограничение скорости для потокового поведения. Для пакетов, отвечающих условиям ограничения скорости, все интерфейсы в одной группе логических интерфейсов совместно используют полосу пропускания, указанную в политике.

2.3.3.2. Связанная конфигурация

Создание класса

По умолчанию класс не определен.

Вы можете запустить команду **class-map**, чтобы создать класс и войти в режим конфигурации класса.

Соответствие ACL

По умолчанию правила для класса не определены.

В режиме конфигурации класса вы можете запустить команду **match acess-group**, чтобы определить правило класса как соответствующее ACL. Сначала необходимо создать правила ACL.

Создание политики

По умолчанию политика не определена.

Вы можете запустить команду **policy-map**, чтобы создать политику и войти в режим настройки политики.

Связывание класса

По умолчанию политика не связана ни с одним классом.

В режиме конфигурации политики вы можете запустить команду **class**, чтобы связать класс и войти в режим конфигурации класса политики.

Привязка поведения потока

По умолчанию класс не привязан ни к какому поведению потока.

В режиме конфигурации класса политики вы можете запустить команду **set**, чтобы изменить значения CoS, DSCP или VID указанного потока; где значение CoS находится в диапазоне от 0 до 7, значение DSCP — в диапазоне от 0 до 63, а значение VID — в диапазоне от 1 до 4094. Вы можете запустить команду **police**, чтобы ограничить пропускную способность и обрабатывать потоки за пределами ограничения для указанных потоков. Диапазоны ограничений пропускной способности определяются продуктами.

Настройка группы логических интерфейсов

Группа логических интерфейсов не определена, и по умолчанию интерфейс не добавляется ни в одну группу логических интерфейсов.

В режиме глобальной конфигурации вы можете запустить команду **virtual-group** для создания группы логических интерфейсов. В режиме конфигурации интерфейса вы можете запустить команду **virtual-group**, чтобы добавить интерфейс в группу логических интерфейсов. Если эта группа логических интерфейсов не создана, вы можете создать

группу логических интерфейсов и добавить интерфейс в группу. Вы можете создать 128 групп логических интерфейсов в диапазоне от 1 до 128.

Применение политики к интерфейсу

Никакая политика не применяется к интерфейсу по умолчанию.

В режиме конфигурации интерфейса вы можете запустить команду **service-policy**, чтобы применить политику в направлениях ввода/вывода интерфейса. В режиме глобальной конфигурации вы можете запустить команду **service-policy**, чтобы применить политику в направлениях ввода/вывода всех интерфейсов.

2.3.4. Приоритетная маркировка и сопоставление

Приоритеты используются для маркировки запланированных «весов» пакетов или приоритетов пакетов при пересылке. Разные типы пакетов имеют разные типы приоритетов, включая приоритеты 802.1P(PRI), IP PRE и DSCP. Маркировка и сопоставление приоритетов относятся к маркировке приоритетов пакетов указанными значениями и сопоставлению этих значений с соответствующими значениями CoS.

2.3.4.1. Принцип работы

После того, как потоки данных пакетов входят в интерфейс устройства, устройство назначает приоритеты пакетам на основе режима доверия, настроенного для интерфейса. Ниже описаны несколько режимов доверия (trust mode):

- Когда режим доверия интерфейса untrust, что означает недоверие к информации о приоритете, передаваемой в пакетах:

Измените значение CoS в соответствии со значением CoS по умолчанию (0, которое настраивается), таблицей сопоставления CoS-DSCP и таблицей сопоставления DSCP-CoS интерфейса и поместите пакеты в очереди на основе окончательного значения CoS. Для выходных пакетов с тегом 802.1Q приоритет пакета будет изменен на соответствующее значение CoS.

- Когда режим доверия интерфейса trust CoS:

Для пакетов с тегом 802.1Q измените значение CoS в соответствии со значением PRI, таблицей сопоставления CoS-DSCP и таблицей сопоставления DSCP-CoS и поместите пакеты в очереди на основе окончательного значения CoS. Для выходных пакетов с тегом 802.1Q приоритет пакета будет изменен на соответствующее значение CoS.

Для пакетов без тега 802.1Q измените значение CoS в соответствии со значением CoS по умолчанию (0, которое настраивается), таблицей сопоставления CoS-DSCP и таблицей сопоставления DSCP-CoS интерфейса и поместите пакеты в очереди на основе конечного значения CoS. Для выходных пакетов с тегом 802.1Q приоритет пакета будет изменен на соответствующее значение CoS.

- Когда режим доверия интерфейса trust DSCP:

Для пакетов, отличных от IP, обработка такая же, как и для trust CoS.

Для IP-пакетов измените значение CoS в соответствии со значением DSCP пакетов и таблицей сопоставления DSCP-CoS и поместите пакеты в очереди на основе окончательного значения CoS.

- Когда режим доверия интерфейса trust IP PRE:

Для пакетов, отличных от IPv4, обработка такая же, как и для trust CoS.

Для пакетов IPv4 получите и измените приоритет DSCP пакетов в соответствии со значением IP PRE пакетов и таблицей сопоставления IP-PRE-DSCP, получите значение

CoS в соответствии с таблицей сопоставления DSCP-CoS, а затем поместите пакеты в очереди на основе конечного значения CoS.

- Когда режим доверия и применяемая политика интерфейса работают вместе:

Когда режим доверия и применяемая политика интерфейса работают вместе, режим доверия имеет более низкий приоритет, чем политика, и приоритет CoS можно получить в соответствии с таблицей сопоставления DSCP-CoS.

Если к интерфейсу применяется политика, но в политике нет конфигурации для изменения значений DSCP и CoS, обработка будет выполняться на основе режима доверия интерфейса.

2.3.4.2. Связанная конфигурация

Настройка режима доверия интерфейса

Режим доверия интерфейса по умолчанию — недоверие.

В режиме настройки интерфейса запустите команду **mls qos trust**, чтобы изменить режим доверия. Режимом доверия может быть trust CoS, trust DSCP или trust IP PRE.

Настройка значения CoS по умолчанию для интерфейса

Значение CoS по умолчанию для интерфейса равно 0.

В режиме конфигурации интерфейса запустите команду **mls qos cos**, чтобы изменить значение CoS по умолчанию для интерфейса, которое находится в диапазоне от 0 до 7.

Маркировка приоритета потоков

По умолчанию приоритеты потоков не перемаркируются.

В режиме конфигурации класса политики запустите команду **set**, чтобы изменить значения CoS, DSCP и VID потоков. Значение CoS находится в диапазоне от 0 до 7, значение DSCP — в диапазоне от 0 до 63, а значение VID — в диапазоне от 1 до 4094.

Настройка сопоставления CoS-DSCP

По умолчанию значения CoS 0, 1, 2, 3, 4, 5, 6 и 7 отображаются на значения DSCP 0, 8, 16, 24, 32, 40, 48 и 56 соответственно.

Запустите команду **mls qos map cos-dscp**, чтобы настроить сопоставление COS-DSCP. Значение DSCP находится в диапазоне от 0 до 63.

Настройка карты DSCP-CoS

По умолчанию DSCP 0–7 сопоставляются с CoS 0, DSCP 8–15 сопоставляются с CoS 1, DSCP 16–23 сопоставляются с CoS2, DSCP 24–31 сопоставляются с CoS 3, DSCP 32–39 сопоставляются с CoS 4, DSCP 40 до 47 сопоставлены с CoS 5, DSCP 48 до 55 сопоставлены с CoS 6, а DSCP 56 до 63 сопоставлены с CoS 7.

Запустите команду **mls qos map dscp-cos**, чтобы настроить сопоставление DSCP-CoS. Значение CoS находится в диапазоне от 0 до 7, а значение DSCP — в диапазоне от 0 до 63.

2.3.5. Контроль трафика

Контролируйте спецификацию трафика, поступающего в сеть, ограничивайте трафик в разумных пределах и отбрасывайте трафик за пределами лимита или изменяйте приоритет пакетов. Кроме того, можно контролировать общий трафик интерфейса, а трафик за пределами лимита будет отбрасываться.

2.3.5.1. Принцип работы

Контроль трафика используется для отслеживания спецификации трафика, поступающего в сеть, и выполнения предустановленных действий по контролю на основе различных результатов оценки. Эти действия могут быть:

- Пересылка (Forwarding): обычно пересылает пакеты в пределах лимита трафика.
- Отбрасывание (Discarding): отбрасывать пакеты, превышающие лимит трафика.
- Изменение приоритета и переадресация: изменяет приоритеты пакетов за пределами лимита трафика, а затем перенаправляет пакеты.

Напрямую отбрасывать пакеты за пределами общего лимита трафика интерфейса.

2.3.5.2. Связанная конфигурация

Настройка действия при превышении лимита трафика

Никаких действий, которые должны выполняться при превышении лимита трафика, по умолчанию не настроено.

В режиме конфигурации класса политик запустите команду **police**, чтобы настроить действие, которое будет выполняться при превышении лимита трафика, на отбрасывание трафика за лимитом или изменение значения CoS, или значения DSCP. Диапазон ограничения трафика определяется продуктами. Когда трафик превышает лимит, вы можете изменить значение CoS в диапазоне от 0 до 7 и значение DSCP в диапазоне от 0 до 63.

Настройка общего лимита трафика для интерфейса

Общий лимит трафика для интерфейса по умолчанию не настроен.

В режиме настройки интерфейса запустите команду **rate-limit**, чтобы настроить общий лимит трафика для интерфейса в направлениях ввода и вывода. Диапазон ограничения трафика определяется продуктами.

2.3.6. Управление перегрузками

Когда скорость приема пакетов превышает скорость отправки пакетов, на интерфейсе отправки возникает перегрузка. Если для хранения этих пакетов не предоставлен достаточный буфер, пакеты могут быть потеряны. Механизм управления перегрузкой определяет последовательность пакетов данных, которые должны быть отправлены с интерфейса, на основе приоритетов пакетов данных. Функция управления перегрузкой позволяет контролировать перегрузку, повышая приоритеты важных пакетов данных. Когда происходит перегрузка, важные пакеты данных отправляются с более высоким приоритетом, чтобы обеспечить своевременную реализацию ключевых услуг.

2.3.6.1. Принцип работы

Механизм планирования очереди используется для управления перегрузкой, и процесс выглядит следующим образом:

- После того, как каждый пакет проходит всю обработку QoS в коммутаторе, пакет наконец получает значение CoS.
- На выходном интерфейсе устройство классифицирует пакеты по соответствующим очередям отправки на основе значений CoS.
- Выходной интерфейс выбирает пакеты в очереди для отправки на основе различных политик планирования (SP, WRR, DRR, WFQ, SP+WRR, SP+DRR, SP+WFQ).

Политика планирования

Политики планирования очередей включают SP, WRR, DRR, WFQ, SP+WRR, SP+DRR и SP+WFQ.

- Планирование со строгим приоритетом (Strict-Priority (SP)) означает планирование пакетов строго в соответствии с идентификаторами очереди. Каждый раз перед отправкой пакетов проверяйте, есть ли в очереди с первым приоритетом пакеты для отправки. Если да, пакеты в этой очереди отправляются первыми. Если нет, проверьте, есть ли пакеты в очереди со вторым приоритетом. Следуйте тем же правилам для пакетов в других очередях.
- Планирование Weighted Round Robin (WRR) означает планирование очередей по очереди, чтобы гарантировать, что все очереди имеют определенное время обслуживания. Например, интерфейс 1000 Мбит/с имеет 8 выходных очередей. WRR настраивает взвешенное значение (5, 5, 10, 20, 20, 10, 20 и 10, которые указывают пропорции полученных ресурсов) для каждой очереди. Этот метод планирования гарантирует, что очереди с самым низким приоритетом будет назначена полоса пропускания не менее 50 Мбит/с, что позволит избежать обслуживания пакетов в очереди с самым низким приоритетом в течение длительного времени при использовании метода планирования SP.
- Планирование Deficit Round Robin (DRR) похоже на WRR, но применяет весовые значения на основе байтов, а не на основе временных интервалов.
- Планирование Weighted Fair Queueing (WFQ) обеспечивает динамическую и справедливую организацию очереди и применяет взвешенные значения на основе байтов, аналогично DRR. При обнаружении пустой очереди DRR немедленно перейдет к следующей очереди для передачи. Если очередь пропускает свое время передачи, очередь должна ждать следующего раза, что является разницей между WFQ и DRR; следовательно, WFQ больше подходит для обработки пакетов данных переменной длины, чем DRR.
- Планирование SP+WRR означает настройку планирования SP для одной или нескольких очередей отправки и настройку планирования WRR для других очередей. Среди очередей SP только после отправки всех пакетов в очереди SP с первым приоритетом могут быть отправлены пакеты в очереди SP со вторым приоритетом. Среди очередей SP и WRR только после отправки пакетов во всех очередях SP можно отправлять пакеты в очередях WRR.
- Планирование SP+WFQ означает настройку планирования SP для одной или нескольких очередей отправки и настройку планирования DRR для других очередей. Среди очередей SP только после отправки всех пакетов в очереди SP с первым приоритетом могут быть отправлены пакеты в очереди SP со вторым приоритетом. Среди очередей SP и DRR только после отправки пакетов во всех очередях SP можно отправлять пакеты в очередях DRR.
- Планирование SP+WFQ означает настройку планирования SP для одной или нескольких очередей отправки и настройку планирования WFQ для других очередей. Среди очередей SP только после отправки всех пакетов в очереди SP с первым приоритетом могут быть отправлены пакеты в очереди SP со вторым приоритетом. Среди очередей SP и WFQ только после отправки пакетов во всех очередях SP можно отправлять пакеты в очередях WFQ.

2.3.6.2. Многоадресная очередь QoS

В некоторых продуктах очереди интерфейса подразделяются на одноадресные и многоадресные очереди. Есть 8 одноадресных очередей. Все известные одноадресные пакеты попадают в соответствующие одноадресные очереди для пересылки в

соответствии с их приоритетами. Существует от 1 до 8 очередей многоадресной рассылки (в зависимости от продуктов. Некоторые продукты не поддерживают очереди многоадресной рассылки). За исключением известных одноадресных пакетов, все пакеты (например, широковещательные пакеты, многоадресные пакеты, неизвестные одноадресные пакеты и зеркальные пакеты) попадают в соответствующие многоадресные очереди для пересылки в зависимости от их приоритетов. Подобно одноадресным очередям, вы можете настроить сопоставление приоритетов и алгоритмы планирования для многоадресных очередей. Команда **Cos-to-Mc-Queue** может использоваться для настройки сопоставления приоритетов с очередями многоадресной рассылки. В настоящее время многоадресные очереди поддерживают алгоритмы планирования SP, WRR и SP+WRR.

2.3.6.3. Политика планирования и round robin weight для выходных очередей на интерфейсе

Политики планирования и round robin weight для выходных очередей основаны на глобальных конфигурациях. Некоторые продукты поддерживают как глобальные конфигурации, так и конфигурации на основе интерфейса. Конфигурации на основе интерфейса имеют более высокий приоритет, чем глобальные конфигурации. Глобальная политика планирования работает с соответствующим глобальным round robin weight, тогда как интерфейсная политика планирования работает с интерфейсным round robin weight. Если настроена только глобальная политика планирования или политика планирования интерфейса, но не настроены соответствующие round robin weight, round robin weight по умолчанию будут работать с политикой планирования.

2.3.6.4. Пропускная способность очереди

Некоторые продукты позволяют настраивать гарантированную минимальную пропускную способность и ограниченную максимальную пропускную способность для очереди. Очередь, настроенная с гарантированной минимальной пропускной способностью, гарантирует, что пропускная способность для этой очереди не меньше настроенного значения. Очередь, настроенная с ограниченной максимальной пропускной способностью, гарантирует, что пропускная способность для этой очереди не превышает настроенное значение, а пакеты, выходящие за пределы пропускной способности, будут отбрасываться. Ограничения пропускной способности для очередей одноадресной и многоадресной рассылки настраиваются вместе на некоторых продуктах, тогда как на некоторых других продуктах они настраиваются отдельно. Кроме того, некоторые продукты позволяют настраивать пропускную способность только для одноадресных очередей.

2.3.6.5. Очередь ECN

Благодаря сочетанию технологии WRED и технологии явного уведомления о перегрузке (ECN) оконечное устройство может воспринимать перегрузку сети и уведомлять исходное устройство о перегрузке. Получив уведомление, исходное устройство снижает скорость отправки пакетов, чтобы предотвратить перегрузку.

- Обе функции ECN и WRED должны быть настроены для включения функции очереди ECN.
- После включения функции очереди ECN (а именно поле ECN в пакетах установлено в 01 или 10), при перегрузке очереди устройство меняет поле ECN на CE (11), вместо случайного отбрасывания пакетов по шаблону WRED.
- После включения функции очереди ECN устройство устанавливает для поля ECN значение CE только тогда, когда скорость передачи пакетов достигает нижнего порога отбрасывания, указанного в шаблоне WRED.

2.3.6.6. Связанная конфигурация

Настройка сопоставления CoS-очереди

По умолчанию значения CoS 0, 1, 2, 3, 4, 5, 6 и 7 сопоставляются с очередями 1, 2, 3, 4, 5, 6, 7 и 8 соответственно.

Запустите команду **cos-map priority-queue**, чтобы настроить сопоставление CoS-очереди. Значение CoS находится в диапазоне от 0 до 7, а значение очереди — в диапазоне от 1 до 8.

Настройка политики планирования для очереди вывода

По умолчанию политика планирования для глобальной очереди вывода — WRR, а политика планирования для интерфейса не настроена.

Запустите команду **mls qos scheduler**, чтобы настроить политику планирования вывода для очереди. Настраиваемые политики планирования включают SP, WRR и DRR. Вы также можете запустить команду **priority-queue**, чтобы настроить политику планирования как SP.

Настройка round robin weight, соответствующего политике планирования WRR для очереди вывода.

По умолчанию вес глобальной очереди или очереди на основе интерфейса составляет 1:1:1:1:1:1:1:1.

Запустите команду **wrr-queue bandwidth**, чтобы настроить round robin weight, соответствующий политике планирования WRR для выходной очереди. Настраиваемый диапазон веса определяется продуктами.

Более высокий вес означает более длительное время вывода.

Настройка round robin weight, соответствующего политике планирования DRR для очереди вывода

По умолчанию вес глобальной очереди или очереди на основе интерфейса составляет 1:1:1:1:1:1:1:1.

Запустите команду **drr-queue bandwidth**, чтобы настроить round robin weight, соответствующий политике планирования DRR для выходной очереди. Настраиваемый диапазон веса определяется продуктами.

Чем выше вес, тем больше байтов пакета может быть отправлено.

Настройка round robin weight, соответствующего политике планирования WFQ для очереди вывода

По умолчанию вес глобальной очереди или очереди на основе интерфейса составляет 1:1:1:1:1:1:1:1.

Запустите команду **wfq-queue bandwidth**, чтобы настроить round robin weight, соответствующий политике планирования WFQ для выходной очереди. Настраиваемый диапазон веса определяется продуктами.

Чем выше вес, тем больше байтов пакета может быть отправлено.

Настройка пропускной способности для очереди

Запустите команду **qos queue**, чтобы настроить гарантированную минимальную пропускную способность и ограниченную максимальную пропускную способность для каждой очереди. Значение очереди варьируется от 1 до 8, а гарантированная минимальная пропускная способность и ограниченные диапазоны значений максимальной пропускной способности определяются продуктами. Поддерживаемые типы очередей определяются продуктами.

Настройка очереди ECN

Запустите команду **qos queue** *queue_num* **ecn**, чтобы включить ECN для всех очередей. (Диапазон очереди: от 1 до 8).

2.3.7. Предотвращение перегрузки

Отслеживайте использование очереди выходного интерфейса и снижайте нагрузку на сеть, активно отбрасывая пакеты и регулируя сетевой трафик при перегрузке сети.

2.3.7.1. Принцип работы

Уменьшите перегрузку, эффективно отслеживая сетевой трафик и прогнозируя возникновение перегрузки. Пакеты необходимо отбрасывать, чтобы уменьшить перегрузку. Политики отбрасывания включают в себя Tail-Drop, Random Early Detection (RED) и Weighted Random Early Detection (WRED).

2.3.7.2. Tail-Drop

Традиционные политики потери пакетов включают Tail-Drop. Tail-Drop эффективен для всего трафика и не может различать уровни обслуживания. Когда возникает перегрузка, пакеты данных в хвосте очереди будут отбрасываться до тех пор, пока перегрузка не будет устранена.

2.3.7.3. RED и WRED

Хосты, использующие TCP, уменьшат скорость отправки пакетов в ответ на массовую потерю пакетов. После устранения перегрузки хосты увеличивают скорость отправки пакетов. Таким образом, Tail-Drop может вызвать глобальную синхронизацию TCP. Когда очередь одновременно отбрасывает несколько TCP-пакетов, несколько TCP-соединений одновременно входят в состояние уменьшения перегрузки и медленного запуска, а трафик сокращается и корректируется. После устранения заторов могут появиться пики трафика. Процесс постоянно повторяется, сетевой трафик внезапно увеличивается и уменьшается, а линейный трафик всегда колеблется между минимальным и максимальным значениями. Когда происходит глобальная синхронизация TCP, пропускная способность соединения не может быть использована должным образом, что приводит к потере пропускной способности.

Чтобы избежать этого обстоятельства, вы можете использовать политику отбрасывания пакетов RED/WRED. Эта политика обеспечивает механизм случайного отбрасывания пакетов, что позволяет избежать глобальной синхронизации TCP. Когда пакеты TCP-подключения отбрасываются и отправляются с более низкой скоростью, пакеты других TCP-подключений по-прежнему отправляются с более высокой скоростью. Таким образом, всегда есть TCP-соединения, пакеты которых отправляются с более высокой скоростью, что увеличивает использование пропускной способности линии.

При использовании WRED можно установить нижнее пороговое значение и максимальную вероятность отбрасывания для очереди. Когда длина очереди меньше нижнего порогового значения, WRED не отбрасывает пакеты. Когда длина очереди находится между верхним и нижним пороговыми значениями, WRED отбрасывает пакеты случайным образом (чем больше длина очереди, тем выше вероятность отбрасывания пакетов. Существует максимальная вероятность отбрасывания). Когда длина очереди превышает верхнее пороговое значение, WRED отбрасывает пакеты с максимальной вероятностью отбрасывания.

В отличие от RED, WRED использует приоритеты, чтобы различать политики отмены. RED — это особый пример WRED. Когда все значения CoS интерфейса сопоставлены с одними и теми же нижними и высшими пороговыми значениями, WRED становится RED.

2.3.7.4. Связанная конфигурация

Включение функции WRED

Политика отбрасывания пакетов по умолчанию — Tail-Drop.

Вы можете запустить команду **queueing wred**, чтобы включить функцию WRED.

Настройка нижнего порога

Когда поддерживаются 2 группы нижних порогов в процентах, значения по умолчанию равны 100 и 80 (количество групп порогов определяется продуктами). Некоторые продукты поддерживают настройку в ячейках (значение по умолчанию определяется продуктами).

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect min-threshold**, чтобы настроить нижние пороги в процентах для пакетов, отбрасываемых WRED в каждой очереди. Значение очереди находится в диапазоне от 1 до 8. Нижний порог находится в диапазоне от 1 до 100.

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect min-threshold cell**, чтобы настроить нижние пороги в единице ячейки для пакетов, отбрасываемых WRED в каждой очереди. Диапазон значений очереди зависит от продуктов.

Настройка верхнего порога

Когда поддерживаются 2 группы нижних порогов в процентах, значения по умолчанию равны 100 и 100 (количество групп порогов определяется продуктами). Некоторые продукты поддерживают настройку в ячейках (значение по умолчанию определяется продуктами).

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect max-threshold**, чтобы настроить более высокие пороги в процентах для пакетов, отбрасываемых WRED в каждой очереди. Значение очереди находится в диапазоне от 1 до 8. Верхний порог находится в диапазоне от минимального значения нижнего порога до максимального значения верхнего порога.

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect max-threshold cell**, чтобы настроить более высокие пороги в единице ячейки для пакетов, отбрасываемых WRED в каждой очереди. Значение очереди находится в диапазоне от 1 до 8. Верхний порог находится в диапазоне от минимального значения нижнего порога до максимального значения верхнего порога.

Когда длина очереди меньше нижнего порога, WRED не отбрасывает пакеты. Когда длина очереди находится между нижним и верхним пороговыми значениями, WRED отбрасывает пакеты случайным образом.

Настройка максимальной вероятности отбрасывания

Когда поддерживаются 2 группы максимальных вероятностей отбрасывания, значения по умолчанию равны 100 и 80 (количество групп пороговых значений определяется продуктами).

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect probability**, чтобы настроить максимальные вероятности отбрасывания пакетов, отбрасываемых WRED в каждой очереди. Значение очереди находится в диапазоне от 1 до 8. Максимальная вероятность отбрасывания находится в диапазоне от 1 до 100.

Корректировка средней длины очереди для вероятности отбрасывания

Когда пакеты пересылаются, WRED определяет вероятность отбрасывания на основе средней длины выходной очереди.

Когда длина очереди находится между нижним порогом и верхним порогом, WRED начинает случайным образом отбрасывать пакеты. Более длинная очередь приводит к более высокой вероятности отбрасывания, которая меньше максимальной вероятности отбрасывания. Когда длина очереди превышает верхний порог, пакеты отбрасываются с максимальной вероятностью отбрасывания.

По умолчанию средняя длина очереди определяется продуктами. Вы можете настроить интервал выборки и вес отбрасываемых пакетов, чтобы повлиять на результат расчета средней длины очереди.

Вес выборки указывает весовой коэффициент выборочных обновлений данных. Больший вес выборки указывает на более длительный интервал обновления средней длины очереди и большую среднюю длину очереди. В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue random-detect sample-weight**, чтобы настроить весовой коэффициент выборки для каждой очереди. Диапазон значений определяется продуктами.

Настройка сопоставления CoS-порога

По умолчанию все значения CoS сопоставляются с первой группой пороговых значений (количество пороговых групп определяется продуктами).

В режиме конфигурации интерфейса вы можете запустить команду **wrr-queue cos-map**, чтобы настроить сопоставление группы CoS с порогом. Значение CoS находится в диапазоне от 0 до 7, а количество пороговых групп определяется продуктами. Можно настроить несколько групп более низких пороговых значений и максимальных вероятностей отбрасывания. Настроив сопоставление группы CoS с порогом, вы можете выбрать действующую пороговую группу, сопоставленную со значением CoS, например, CoS 0 сопоставляется с первой пороговой группой, а CoS 1 сопоставляется со второй пороговой группой. Если пакеты CoS 0 и 1 добавляются в очередь 1 для планирования, пакеты CoS 0 обрабатываются на основе нижних пороговых значений и максимальных вероятностей отбрасывания в первой группе, а пакеты CoS 1 обрабатываются на основе нижних пороговых значений и максимальных вероятностей отбрасывания во второй группе.

Когда все значения CoS интерфейса сопоставлены с одной и той же группой пороговых значений, включенный WRED становится RED.

2.3.8. Отображение и конфигурация очереди

По умолчанию режим отображения и настройки всех очередей на устройстве — 1–8.

Изменение отображения очереди и режима конфигурации

В режиме глобальной конфигурации вы можете запустить команду **qos-queue compatible enable**, чтобы изменить отображение очереди и режим конфигурации всех очередей на устройстве на 0–7.

2.3.9. Изменение приоритета пакетов

По умолчанию приоритет пакета изменяется на тот, который настроен на устройстве, когда пакет отправляется с устройства. Например, отправляется пакет L2 с приоритетом 4. Направление входа связано с политикой сопоставления (policy-map). Если пакет соответствует политике, значение CoS в пакете устанавливается равным 2. Когда пакет перехватывается на выходе, приоритет пакета равен 2.

Отключение изменения приоритета пакетов

В режиме глобальной конфигурации запустите команду **mls qos comment disabled**, чтобы отключить изменение приоритета пакета, т. е. когда пакет отправляется с устройства, его приоритет такой же, как и при отправке пакета на устройство.

2.4. Ограничения

- Trust mode QoS нельзя настроить на SVI.
- Для продуктов серии QSW-7600 члены группы логических портов должны находиться на одном устройстве.
- Элементы, добавляемые в группу логических портов, должны быть физическими портами или агрегируемыми портами (AP).
- Запрещающая запись в ACL, соответствующая class-map, не действует.
- Продукты серии QSW-7600 не поддерживают модификацию VID.
- Когда QoS применяется к исходящему направлению, продукты серии QSW-7600 изменяют значение DSCP для пакетов, пропускная способность которых превышает ограничение, но сохраняют значение CoS неизменным. Когда QoS применяется к входящему направлению, продукты серии QSW 7600 изменяют значение DSCP и значение CoS для пакетов, пропускная способность которых превышает ограничение.
- Продукты серии QSW-7600 изменяют как значение DSCP, так и значение CoS для пакетов, пропускная способность которых превышает лимит. После установки **none-tos** продукты серии QSW-7600 не изменяют значение DSCP при изменении значения CoS.
- Продукты серии QSW-7600 не поддерживают опцию **none-tos** при настройке CoS.
- В продуктах серии QSW-7600 ограничение пропускной способности основано на фактической пропускной способности, включая нагрузку, создаваемую преамбулой и межкадровым интервалом. Преамбула и межкадровый интервал, передаваемые в каждом пакете, занимают 20 байтов.
- Продукты серии QSW-7600 поддерживают минимальную степень детализации ограничения скорости 8 кбит/с. Степень детализация ограничения скорости зависит от настроек ограничения скорости. В следующей таблице перечислены взаимосвязи между ограничениями скорости и степенью детализации.

Диапазон ограничения скорости	от 64 кбит/с до 2 Гбит/с	от 2 Гбит/с до 4 Гбит/с	от 4 Гбит/с до 8 Гбит/с
Степень детализации	8 кбит/с	16 кбит/с	32 кбит/с
Диапазон ограничения скорости	от 8 Гбит/с до 16 Гбит/с	от 16 Гбит/с до 32 Гбит/с	от 32 Гбит/с до 40 Гбит/с
Степень детализации	64 кбит/с	128 кбит/с	256 кбит/с

- Для второго параметра (всплеск трафика) в политике ограничения скорости QoS, если значение параметра слишком мало, фактическая скорость может быть чрезмерно малой в случае всплеска трафика. Если значение параметра слишком велико, фактическая скорость может быть слишком большой. При необходимости вы можете использовать следующую рекомендуемую конфигурацию:
  - (1) Если настроенное ограничение скорости меньше 1024 кбит/с, рекомендуемое значение размера пакета составляет 1024 кбайт.
  - (2) Если сконфигурированное ограничение скорости меньше 10 240 кбит/с, рекомендуется установить значение размера пакета таким же, как ограничение скорости, или использовать максимальное значение

(допустимое значение размера пакета продуктов может быть меньше чем 10240 кбайт).

- (3) Если настроенный предел скорости превышает 10 240 кбит/с, рекомендуется установить значение размера пакета равным максимально допустимому значению для устройства.

- Для второго параметра в политике ограничения скорости QoS, когда ограничение скорости относительно велико, второй параметр необходимо скорректировать соответствующим образом. В противном случае предел скорости может быть неточным.
- Для портов 10G или 40G рекомендуется установить порог скорости равным 32 или больше.
- Продукты серии QSW-7600 поддерживают применение политик (policy map) к исходящему направлению.
- Когда политика применяется к AP продуктов серии QSW-7600, порты-члены AP должны соответствовать следующему условию, чтобы сконфигурированное ограничение пропускной способности было пропускной способностью, совместно используемой всеми портами-членами AP: порты-члены AP должны принадлежат одному и тому же устройству QSW-7600.
- В продуктах серии QSW-7600 class-map должна быть связана с ACL, поэтому все ограничения, настроенные в ACL, доступны для функции QoS. Подробнее см. Настройка ACL.
- Политики нельзя применять к SVI.
- Политики могут быть настроены в направлении вывода, но не могут быть настроены на AP.
- Политики, настроенные в направлении вывода, не поддерживают перемаркировку значения CoS пакетов. Значение CoS пакетов не перемаркируется при перемаркировке значения DSCP пакетов.
- QoS не поддерживается для групп логических портов в направлении вывода.
- Порты виртуального коммутируемого канала (Virtual Switching Link (VSL)) продуктов серии QSW-7600 используют алгоритм планирования Strict Priority (SP) + Deficit Round Robin (DRR) по умолчанию. Очередь 7 принимает планирование SP, а веса других очередей равны 1, что не может быть изменено пользователями.

Например, порты-участники VLAN 1 содержат Gi0/1, Gi/2, Gi0/33 и Gi0/34, а ограничение скорости QoS в 10 Мбит/с применяется к VLAN 1. Фактическое ограничение скорости пакетов, передаваемых Gi0/1, Gi/2, Gi0/33 и Gi0/34 фактически составляют 20 Мбит/с. Gi0/1 и Gi/2 используют ограничение скорости 10 Мбит/с, а Gi0/33 и Gi0/34 разделяют ограничение скорости еще 10 Мбит/с.

- Вы можете запускать только команду **show run**, чтобы проверить, включена ли функция WRED глобально.
- Нижний порог и максимальная вероятность отбрасывания очереди образуют одну группу конфигурации WRED. Количество поддерживаемых групп конфигурации WRED зависит от ограничения. Продукты серии QSW-7600 поддерживают до 120 групп конфигурации WRED.
- Не рекомендуется, чтобы настроенное количество групп конфигурации WRED превышало 120. Дополнительные группы конфигурации WRED могут привести к неправильной работе.
- Если нижний порог равен 100 %, функция WRED отключена.

- Продукты серии QSW-7600 поддерживают настройку сопоставления физических портов.
- Администраторы могут настроить сопоставления DSCP-CoS и CoS-threshold для реализации сопоставления DSCP-threshold.
- Администраторы могут настроить сопоставления CoS-threshold и CoS-queue для реализации сопоставления queue-threshold.

2.5. Конфигурация

Конфигурация	Описание и команда	
Настройка классификации потоков	(Опционально) Используется для создания информации о классификации потока	
	class-map	Создает класс
	match access-group	Соответствие правилам ACL
	policy-map	Создает политику
	class	Ассоциирует класс
	police	Настраивает лимит пропускной способности для потоков и действие по обработке пакетов за лимитом
	set	Настраивает поведение для изменения значений CoS, DSCP и VID потоков
	virtual-group	Создает группу логических интерфейсов и добавляет интерфейсы в группу логических интерфейсов
	service-policy	Применяет политику к интерфейсу
Настройка маркировки и отображения приоритетов для пакетов	(Опционально) Он используется для настройки trust mode, значения CoS по умолчанию и различных сопоставлений для интерфейса	
	mls qos trust	Изменяет trust mode интерфейс
	mls qos cos	Изменяет значение CoS по умолчанию для интерфейса
	mls qos map cos-dscp	Настраивает сопоставление CoS-DSCP

Конфигурация	Описание и команда	
Настройка маркировки и отображения приоритетов для пакетов	**mls qos map dscp-cos**	Настраивает сопоставление DSCP-CoS
Настройка ограничения скорости интерфейса	(Опционально) Он используется для настройки ограничения скорости для интерфейса	
	rate-limit	Настраивает лимит трафика для интерфейса
Настройка управления перегрузками	(Опционально) Он используется для настройки сопоставления CoS-queue, политик планирования очередей и round robin weight	
	priority-queue cos-map	Настраивает сопоставление CoS-queue
	priority-queue	Настраивает политику планирования вывода для очереди на SP
	mls qos scheduler	Настраивает политику планирования вывода для очереди
	wrr-queue bandwidth	Настраивает round robin weight, соответствующий политике планирования WRR для выходной очереди
	drr-queue bandwidth	Настраивает round robin weight, соответствующий политике планирования DRR для выходной очереди
	wfq-queue bandwidth	Настраивает round robin weight, соответствующий политике планирования WFQ для выходной очереди
	qos queue	Настраивает гарантированную минимальную пропускную способность и ограниченную максимальную пропускную способность для очереди
	qos queue ecn	Включает функцию очереди ECN

Конфигурация	Описание и команда	
Настройка предотвращения перегрузки	(Опционально) Он используется для предотвращения перегрузки сети путем настройки отбрасывания пакетов	
	queueing wred	Включает функцию WRED
	wrr-queue random-detect sample-weight	Настраивает вес выборки пакетов, которые будут отбрасываться WRED
	wrr-queue random-detect min-threshold	Настраивает нижнее пороговое значение для пакетов, отбрасываемых WRED
	wrr-queue random-detect max-threshold	Настраивает верхний порог для пакетов, отбрасываемых WRED (в процентах)
	wrr-queue random-detect min-threshold cell	Настраивает нижний порог для пакетов, отбрасываемых WRED (в ячейках)
	wrr-queue random-detect max-threshold cell	Настраивает более высокий порог для пакетов, отбрасываемых WRED (в ячейках)
	wrr-queue random-detect probability	Настраивает максимальную вероятность отбрасывания пакетов, отбрасываемых WRED
	wrr-queue cos-map	Настраивает сопоставление threshold-CoS
Настройка отображения очереди и режим настройки	(Опционально) Используется для установки режима отображения очереди и настройки всех очередей на устройстве на 0–7	
	qos-queue compatible enable	Включает отображение очереди и режим конфигурации всех очередей на устройстве на 0–7
Отключение изменения приоритета пакетов	(Опционально) Используется для отключения изменения приоритета пакета	
	mls qos remark disable	Отключает изменение приоритета пакетов

2.5.1. Настройка классификации потоков

2.5.1.1. Эффект конфигурации

- Создайте класс и сопоставьте правила классификации.
- Создайте политику, привяжите поведения класса и потока и свяжите с интерфейсом.

2.5.1.2. Примечания

- Имена классов и политик не могут содержать более 31 символа.
- Конфигурации интерфейса допускают только конфигурации интерфейса AP и Ethernet. Некоторые продукты поддерживают политики, применяемые к интерфейсам SVI с помощью команды **service-policy**. Когда и физические интерфейсы, и интерфейсы SVI настроены с помощью политик, приоритет физических интерфейсов выше, чем у интерфейсов SVI.
- Если запустить команду **service-policy** в режиме глобальной конфигурации, политики будут применяться ко всем интерфейсам, которые можно настроить с помощью политик.

2.5.1.3. Шаги настройки

Создание класса и сопоставление правил ACL

- Необязательный.
- Создайте класс. В режиме конфигурации класса сопоставьте ACL, IP PRE или DSCP.

Создание политики

- Необязательный.
- Создайте политику. В режиме конфигурации политики привяжите поведение класса и потока.

Создание группы логических интерфейсов и добавление интерфейсов в группу логических интерфейсов

- Необязательный.
- Создайте группу логических интерфейсов и добавьте интерфейсы в группу логических интерфейсов.

Применение политики к интерфейсу

- Необязательный.
- Свяжите настроенную политику с указанным интерфейсом или группой логических интерфейсов.

2.5.1.4. Проверка

- Запустите команду **show class-map**, чтобы проверить, успешно ли создан класс и успешно ли сопоставлены правила.
- Запустите команду **show policy-map**, чтобы проверить, успешно ли создана политика и успешно ли связаны поведение класса и потока.
- Запустите команду **show mls qos interface**, чтобы проверить, связан ли интерфейс с политикой.
- Запустите команду **show virtual-group**, чтобы проверить интерфейсы в группе логических интерфейсов.

- Запустите команду **show mls qos virtual-group**, чтобы проверить, связана ли группа логического интерфейса с политикой.

2.5.1.5. Связанная команда

Создание класса

Команда	**class-map** *class-map-name*
Описание параметров	*class-map-name*: указывает имя создаваемого класса. Имя не может содержать более 31 символа
Режим команд	Режим глобальной конфигурации

Соответствие ACL

Команда	**match access-group** *access-list-number*
Описание параметров	*access-list-number*: указывает номер списка ACL, который должен быть сопоставлен
Режим команд	Режим конфигурации класса

Создание политики

Команда	**policy-map** *policy-map-name*
Описание параметров	*policy-map-name*: указывает имя создаваемой политики. Имя не может содержать более 31 символа
Режим команд	Режим глобальной конфигурации

Связывание класса

Команда	**class** *class-map-name*
Описание параметров	*class-map-name*: указывает имя класса, который будет связан
Режим команд	Режим конфигурации политики

Привязка поведений для изменения значений CoS, DSCP и VID потоков

Команда	**set** { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**]}
Описание параметров	**ip dscp** *new-dscp*: изменяет значение DSCP потоков на new-dscp в диапазоне от 0 до 63. **cos** *new-cos*: изменяет значение CoS потоков на new-cos в диапазоне от 0 до 7.

	none-tos: не изменяет значение DSCP пакетов при изменении значения CoS пакетов. **vid** *new-vid*: изменяет VLAN ID потоков на new-vid в диапазоне от 1 до 4094
Режим команд	Режим конфигурации класса

Привязка лимита пропускной способности для потоков и действия по обработке пакетов, превышающих лимит

Команда	**police** *rate-bps burst-byte* [**exceed-action** { **drop** | **dscp** *new-dscp* | **cos** *new-cos* [**none-tos**] }]
Описание параметров	*rate-bps*: указывает ограничение пропускной способности в секунду (кбит). Диапазон значений определяется продуктами. *burst-byte*: указывает ограничение на пакетный трафик (кбайт). Диапазон значений определяется продуктами. **drop**: отбрасывает пакеты за пределами пропускной способности. **dscp** *new-dscp*: изменяет значение DSCP для пакетов, выходящих за пределы полосы пропускания, на new-dscp в диапазоне от 0 до 63. **cos** *new-cos*: изменяет значение CoS пакетов, выходящих за пределы полосы пропускания, на new-cos, в диапазоне от от 0 до 7. **none-tos**: не изменяет значение DSCP пакетов при изменении значения CoS пакетов
Режим команд	Режим конфигурации класса

Создание группы логических интерфейсов и добавление интерфейсов в группу логических интерфейсов

Команда	**virtual-group** *virtual-group-number*
Описание параметров	*virtual-group-number*: указывает номер группы логического интерфейса в диапазоне от 1 до 128
Режим команд	Создайте группу логических интерфейсов в режиме глобальной конфигурации, добавьте интерфейс в группу логических интерфейсов в режиме конфигурации интерфейсов. Если группы логических интерфейсов не существует, необходимо сначала создать группу логических интерфейсов, а затем добавить интерфейсы в группу логических интерфейсов

Применение политики к интерфейсу

Команда	**service-policy** { **input** | **output** } *policy-map-name*
Описание параметров	**input**: применение для входящего трафика интерфейса.

	output: применение для исходящего трафика интерфейса. *policy-map-name*: указывает имя политики, примененной к интерфейсу
Режим команд	Режим конфигурации интерфейса/Режим глобальной конфигурации/ Режим группы логических портов

2.5.1.6. Пример конфигурации

Создание четырех классов потоков и сопоставление ACL, IP PRE и DSCP

Шаги настройки	• Создайте правила ACL. • Создайте четыре класса потоков и сопоставьте ACL, IP PRE и DSCP
	QTECH# configure terminal QTECH(config)# access-list 11 permit host 192.168.23.61 QTECH(config)# class-map cmap1 QTECH(config-cmap)# match access-group 11 QTECH(config-cmap)# exit
Проверка	Проверьте правильность созданных правил ACL и правил потокового класса
	QTECH# show access-lists ip access-list standard 11 10 permit host 192.168.23.61 QTECH# show class-map Class Map cmap1 Match access-group 11

2.5.2. Настройка маркировки и отображения приоритетов для пакетов

2.5.2.1. Эффект конфигурации

- Настройте trust mode и значение CoS по умолчанию для интерфейса.
- Настройте сопоставления CoS-DSCP и DSCP-CoS.
- Настройка качества обслуживания

2.5.2.2. Примечания

Конфигурации интерфейса допускают только конфигурации интерфейса AP и Ethernet.

2.5.2.3. Шаги настройки

Настройка trust mode и значения CoS по умолчанию для интерфейса

- Необязательный.

- В режиме конфигурации интерфейса настройте trust mode и значение CoS по умолчанию для интерфейса.

Настройка сопоставлений CoS-DSCP и DSCP-CoS

- Необязательный.
- Настройте различные сопоставления.

2.5.2.4. Проверка

- Запустите команду **show mls qos interface**, чтобы отобразить trust mode и значение CoS по умолчанию для интерфейса.
- Запустите команду **show mls qos maps**, чтобы отобразить сопоставления CoS-to-DSCP и DSCP-to-CoS.

2.5.2.5. Связанная команда

Настройка интерфейса trust mode

Команда	**mls qos trust** { **cos** | **ip-precedence** | **dscp** }
Описание параметров	**cos**: настраивает интерфейса trust mode к CoS. **ip-precedence**: настраивает интерфейса trust mode на IP PRE. **dscp**: настраивает интерфейса trust mode к DSCP
Режим команд	Режим конфигурации интерфейса

Настройка значения CoS по умолчанию для интерфейса

Команда	**mls qos cos** *default-cos*
Описание параметров	*default-cos*: настраивает значение CoS по умолчанию в диапазоне от 0 до 7. Значение по умолчанию — 0
Режим команд	Режим конфигурации интерфейса

Настройка CoS-to-DSCP map

Команда	**mls qos map cos-dscp** *dscp1…dscp8*
Описание параметров	*dscp1….dscp8*: указывает значения DSCP, сопоставленные со значениями CoS. Значения CoS по умолчанию 0–7 отображаются на DSCP 0, 8, 16, 24, 32, 40, 48 и 56 соответственно. Значение DSCP находится в диапазоне от 0 до 63
Режим команд	Режим глобальной конфигурации

Настройка DSCP-to-CoS map

Команда	**mls qos map dscp-cos** *dscp-list* **to** *cos*
Описание параметров	*dscp-list*: указывает список DSCP, сопоставленный со значениями CoS. DSCP 0–7 по умолчанию сопоставляются с CoS 0, DSCP 8–15 сопоставляются с CoS 1, DSCP 16–23 сопоставляются с CoS 2, DSCP 24–31 сопоставляются с CoS 3, DSCP 32–39 сопоставляются с CoS 4, DSCP 40–47 сопоставляется с CoS 5, DSCP 48–55 сопоставляется с CoS 6, а DSCP 56–63 сопоставляется с CoS 7. Значение DSCP находится в диапазоне от 0 до 63. *cos*: указывает значения CoS, сопоставленные с DSCP-списком, в диапазоне от от 0 до 7
Режим команд	Режим глобальной конфигурации

2.5.2.6. Пример конфигурации

Настройка trust mode и значения CoS по умолчанию для интерфейса

Шаги настройки	• Измените trust mode интерфейса gigabitEthernet 0/0 на DSCP. • Измените значение CoS по умолчанию для интерфейса gigabitEthernet 0/1 на 7
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/0 QTECH(config-if-GigabitEthernet 0/0)# mls qos trust dscp QTECH(config-if-GigabitEthernet 0/0)# exit QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# mls qos cos 7 QTECH(config-if-GigabitEthernet 0/1)# exit
Проверка	Убедитесь, что trust mode и значение CoS по умолчанию успешно настроены для интерфейса
	QTECH# show mls qos interface gigabitEthernet 0/0 Interface: GigabitEthernet 0/0 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: Default trust: dscp Default cos: 0 QTECH# show mls qos interface gigabitEthernet 0/1

	Interface: GigabitEthernet 0/1 Ratelimit input: Ratelimit output: Attached input policy-map: Attached output policy-map: Default trust: none Default cos: 7

Настройка сопоставлений CoS-to-DSCP и DSCP-to-CoS

Шаги настройки	• Настройте CoS-to-DSCP для сопоставления CoS 0, 1, 2, 3, 4, 5, 6 и 7 с DSCP 7, 14, 21, 28, 35, 42, 49 и 56 соответственно. • Настройте DSCP-to-CoS для сопоставления DSCP 0, 1, 2, 3 и 4 с CoS 4 и DSCP 11, 12, 13 и 14 с CoS 7
	QTECH# configure terminal QTECH(config)# mls qos map cos-dscp 7 14 21 28 35 42 49 56 QTECH(config)# mls qos map dscp-cos 0 1 2 3 4 to 4 QTECH(config)# mls qos map dscp-cos 11 12 13 14 to 7
Проверка	Проверьте, все ли сопоставления успешно настроены
	QTECH# show mls qos maps cos-dscp cos dscp --- ---- 0 7 1 14 2 21 3 28 4 35 5 42 6 49 7 56

QTECH# show mls qos maps dscp-cos

dscp	cos	dscp	cos	dscp	cos	dscp	cos
0	4	1	4	2	4	3	4
4	4	5	0	6	0	7	0
8	1	9	1	10	1	11	7
12	7	13	7	14	7	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3
28	3	29	3	30	3	31	3
32	4	33	4	34	4	35	4
36	4	37	4	38	4	39	4
40	5	41	5	42	5	43	5
44	5	45	5	46	5	47	5
48	6	49	6	50	6	51	6
52	6	53	6	54	6	55	6
56	7	57	7	58	7	59	7
60	7	61	7	62	7	63	7

2.5.3. Настройка ограничения скорости интерфейса

2.5.3.1. Эффект конфигурации

Настройте лимит трафика для интерфейса.

2.5.3.2. Примечания

Конфигурация поддерживается только интерфейсами Ethernet.

2.5.3.3. Шаги настройки

Настройка лимита трафика для интерфейса

- Необязательный.
- Настройте ограничение на трафик и пакетный трафик для интерфейса.

2.5.3.4. Проверка

Запустите команду **show mls qos rate-limit**, чтобы отобразить информацию об ограничении скорости для интерфейса.

2.5.3.5. Связанная команда

Настройка лимита трафика для интерфейса

Команда	**rate-limit** { **input** | **output** } *bps burst-size*
Описание параметров	**input**: указывает направление ввода интерфейса. **output**: указывает направление вывода интерфейса. *bps*: указывает ограничение пропускной способности в секунду (кбит). Диапазон значений определяется продуктами. *burst-size*: указывает ограничение на всплеск трафика (кбайт). Диапазон значений определяется продуктами
Режим команд	Режим конфигурации интерфейса

2.5.3.6. Пример конфигурации

Типичное применение — ограничение скорости интерфейса + перемаркировка приоритета

Шаги настройки	• Для доступа в Интернет с использованием выходного интерфейса настройте ограничение исходящего трафика на интерфейсе G0/24, а также установите ограничение полосы пропускания на 102 400 кбит/с и ограничение всплеска трафика на 256 кбайт в секунду. • Для здания общежития настройте ограничение входящего трафика на интерфейсе G0/3, а также установите ограничение пропускной способности на 51 200 кбит/с и ограничение всплеска трафика на 256 кбйт в секунду. • Для учебного здания настройте ограничение входящего трафика на интерфейсе G0/1, а также установите ограничение пропускной способности на 30 720 кбит/с и ограничение всплеска трафика на 256 кбайт в секунду. • Для лаборатории создайте класс cmap_dscp7 для соответствия приоритету DSCP 7, создайте политику pmap_test для связи с cmap_dscp7, привяжите поведение потока для изменения значения DSCP для пакетов, скорость которых превышает 20M на 16, примените pmap_test к интерфейсу G0/2, и настройте интерфейс на доверие DSCP
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/24 QTECH(config-if-GigabitEthernet 0/24# rate-limit output 102400 256 QTECH(config-if-GigabitEthernet 0/24)# exit QTECH(config)# interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3# rate-limit input 51200 256 QTECH(config-if-GigabitEthernet 0/3)# exit QTECH(config)# interface gigabitEthernet 0/1

	QTECH(config-if-GigabitEthernet 0/1# rate-limit input 30720 256 QTECH(config-if-GigabitEthernet 0/1)# exit QTECH(config)# class-map cmap_dscp7 QTECH(config-cmap)# match ip dscp 7 QTECH(config-cmap)# exit QTECH(config)# policy-map pmap_test QTECH(config-pmap)# class cmap_dscp7 QTECH(config-pmap-c)# police 20480 128 exceed-action dscp 16 QTECH(config-pmap-c)# exit QTECH(config-pmap)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2# service-policy input pmap_test QTECH(config-if-GigabitEthernet 0/2)# mls qos trust dscp QTECH(config-if-GigabitEthernet 0/2)# exit
Проверка	• Проверьте, успешно ли настроено ограничение скорости интерфейса. • Убедитесь, что класс и политика успешно созданы и успешно применены к интерфейсу
	QTECH# show mls qos rate-limit Interface: GigabitEthernet 0/1 rate limit input Kbps = 30720 burst = 256 Interface: GigabitEthernet 0/3 rate limit input Kbps = 51200 burst = 256 Interface: GigabitEthernet 0/24 rate limit output Kbps = 102400 burst = 256 QTECH# show class-map cmap_dscp7 Class Map cmap_dscp7 Match ip dscp 7 QTECH# show policy-map pmap_test Policy Map pmap_test Class cmap_dscp7 police 20480 128 exceed-action dscp 16 QTECH# show mls qos interface gigabitEthernet 0/2 Interface: GigabitEthernet 0/2

	Ratelimit input: Ratelimit output: Attached input policy-map: pmap_test Attached output policy-map: Default trust: dscp Default cos: 0

2.5.4. Настройка управления перегрузками

2.5.4.1. Эффект конфигурации

- Настройте сопоставление CoS-to-queue.
- Настройте политику планирования и round robin weight для выходной очереди.
- Настройте гарантированную минимальную пропускную способность и ограниченную максимальную пропускную способность для очереди.
- Включите функцию очереди ECN.

2.5.4.2. Примечания

- Конфигурация интерфейса допускается только на интерфейсах AP и Ethernet.
- Обе функции ECN и WRED должны быть настроены для включения функции очереди ECN.

2.5.4.3. Шаги настройки

Конфигурирование сопоставлений CoS-to-unicast и CoS-to-multicast

- Опционально.
- Настройте сопоставления CoS-to-queue. В продуктах, поддерживающих очереди многоадресной рассылки, можно настроить сопоставление CoS-to-multicast.

Настройка политик планирования и round robin weight для одноадресных и многоадресных выходных очередей

- Опционально.
- Настройте политику планирования для очереди вывода и измените round robin weight. В продуктах, поддерживающих очереди многоадресной рассылки, можно настроить политики планирования и коэффициенты round robin weight для очередей многоадресной рассылки.

Настройка гарантированной минимальной пропускной способности и ограниченной максимальной пропускной способности для очереди

- Опционально.
- Настройте гарантированную минимальную пропускную способность и ограниченную максимальную пропускную способность для очереди.

Включение очереди ECN

- Опционально.
- Включите функцию очереди ECN.

2.5.4.4. Проверка

- Запустите команду **show mls qos queuing**, чтобы отобразить информацию об очереди вывода.
- Запустите команду **show mls qos scheduler**, чтобы отобразить политику планирования для очереди вывода.
- Запустите команду **show qos bandwidth**, чтобы отобразить пропускную способность очереди.

2.5.4.5. Связанная команда

Настройка CoS-to-Queue map

Команда	**priority-queue cos-map** *qid cos0* [*cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7*]]]]]]]
Описание параметров	*qid*: указывает идентификатор очереди, который необходимо сопоставить, в диапазоне от 1 до 8. *cos0~cos7*: указывает значения CoS, которые должны быть сопоставлены с qid. Значения CoS по умолчанию 0~7 сопоставляются с очередями 1~8. Диапазон значений от 0 до 7
Режим команд	Режим глобальной конфигурации

Настройка политики планирования для очереди вывода в SP

Команда	**priority-queue**
Режим команд	Режим глобальной конфигурации

Настройка политики планирования для очереди вывода

Команда	**mls qos scheduler** { **sp** | **rr** | **wrr** | **drr** | **wfq** }
Описание параметров	**sp**: устанавливает алгоритм планирования для очереди вывода на SP. **rr**: устанавливает алгоритм планирования для очереди вывода на RR. **wrr**: устанавливает алгоритм планирования для очереди вывода на WRR. **drr**: устанавливает алгоритм планирования для очереди вывода на DRR. **wfq**: устанавливает алгоритм планирования для очереди вывода на WFQ
Режим команд	Глобальный/интерфейсный режим конфигурации

Настройка политики планирования и round robin weight для выходной очереди

Команда	{ **drr-queue** | **wrr-queue | wfq-queue** } **bandwidth** *weight1...weight8*
Описание параметров	**drr-queue**: настраивает round robin weight, соответствующий политике планирования DRR для выходной очереди. **wrr-queue**: настраивает round robin weight, соответствующий политике планирования WRR для выходной очереди. **wfq-queue**: настраивает round robin weight, соответствующий политике планирования WFQ для выходной очереди. *weight1...weight8*: указывает вес очередей с 1 по 8. Диапазон значений определяется продуктами. Значение 0 указывает, что очередь использует алгоритм планирования SP. Вес по умолчанию для глобальных/интерфейсных очередей составляет 1:1
Режим команд	Глобальный/интерфейсный режим конфигурации

Настройка гарантированной минимальной пропускной способности и ограниченной максимальной пропускной способности для очереди

Команда	**qos queue** *queue-id* **bandwidth** { **minimum** | **maximum** } *bandwidth*
Описание параметров	**queue**: настраивает гарантированную минимальную пропускную способность или ограниченную максимальную пропускную способность для устройств, которые позволяют настраивать ограничения пропускной способности как для одноадресной, так и для многоадресной очереди. *queue-id*: указывает идентификатор очереди, который необходимо настроить, в диапазоне от 1 до 8
Описание параметров	**minimum** *bandwidth*: указывает гарантированную минимальную пропускную способность, кбит/с. Диапазон значений определяется продуктами. По умолчанию он не настроен. **maximum** *bandwidth*: указывает ограниченную максимальную пропускную способность, кбит/с. Диапазон значений определяется продуктами. По умолчанию он не настроен
Режим команд	Режим конфигурации интерфейса

Включение очереди ECN

Команда	**qos queue** *queue-id* **ecn**
Описание параметров	*queue-id*: идентификатор очереди. Диапазон: от 1 до 8
Режим команд	Режим конфигурации интерфейса

Руководство по использованию	Обе функции ECN и WRED должны быть настроены для включения функции очереди ECN

2.5.4.6. Пример конфигурации

Настройка сопоставления CoS-to-queue и изменение политики планирования и ее round robin weight

Шаги настройки	• Настройте сопоставление CoS-to-queue на сопоставление значений CoS 0, 1, 2, 3, 4, 5, 6 и 7 с очередями 1, 2, 5, 5, 5, 5, 7 и 8. • Настройте политику планирования вывода для очереди на DRR и round robin weight на 2:1:1:1:6:6:6:8
	QTECH# configure terminal QTECH(config)# priority-queue cos-map 1 2 5 5 5 5 7 8 QTECH(config)# mls qos scheduler drr QTECH(config)# drr-queue bandwidth 2 1 1 1 6 6 6 8
Проверка	Проверьте, успешно ли создано сопоставление CoS-to-queue, а также успешно ли настроены политика планирования выходных данных и round robin weight для очереди
	QTECH# show mls qos scheduler Global Multi-Layer Switching scheduling Deficit Round Robin QTECH# show mls qos queueing CoS-to-queue map: Cos qid --- --- 0 1 1 2 2 5 3 5 4 5 5 5 6 7 7 8 wrr bandwidth weights: qid weights --- ------- 1 1

	2 1 3 1 4 1 5 1 6 1 7 1 8 1 drr bandwidth weights: qid weights --- ------- 1 2 2 1 3 1 4 1 5 6 6 6 7 6 8 8 wfq bandwidth weights: qid weights --- ------- 1 1 2 1 3 1 4 1 5 1 6 1 7 1 8 1

Включение очереди ECN

Шаги настройки	Включите ECN в очереди 1 интерфейса gigabitEthernet 0/1
	QTECH# configure terminal QTECH(config)# queueing wred QTECH(config)# interface gigabitEthernet 0/1

	QTECH(config-if-GigabitEthernet 0/1)# qos queue 1 ecn QTECH(config-if-GigabitEthernet 0/1)# exit
Проверка	Запустите команду **show run**, чтобы проверить результат

Типичное применение — перемаркировка приоритетов + планирование очереди

Шаги настройки	• Создайте ACL для доступа к различным серверам и создайте классы для соответствия этим ACL. • Создайте политики для связи с классами и укажите новые значения CoS для пакетов, обращающихся к различным серверам. Свяжите значения CoS с входными интерфейсами для отделов исследований и разработок, маркетинга и настройте интерфейсы на доверие CoS. • Настройте значение CoS по умолчанию для интерфейса отдела управления персоналом на наивысший приоритет 7, чтобы гарантировать, что пакеты от отдела управления персоналом отправляются с наивысшим приоритетом. • Настройте политику планирования вывода на WR и round robin weight на 1:1:1:2:6:1:1:0 для очередей. Это означает, что алгоритм планирования SP используется для пакетов отдела управления персоналом, а пакеты отдела R&D и отдела маркетинга для доступа к почтовой базе данных, файловой базе данных и базе данных запроса зарплаты планируются на основе соотношения 6:2:1
	QTECH# configure terminal QTECH(config)# ip access-list extended salary QTECH(config-ext-nacl)# permit ip any host 192.168.10.1 QTECH(config-ext-nacl)# exit QTECH(config)# ip access-list extended mail QTECH(config-ext-nacl)# permit ip any host 192.168.10.2 QTECH(config-ext-nacl)# exit QTECH(config)# ip access-list extended file QTECH(config-ext-nacl)# permit ip any host 192.168.10.3 QTECH(config-ext-nacl)# exit QTECH(config)# class-map salary QTECH(config-cmap)# match access-group salary QTECH(config-cmap)# exit QTECH(config)# class-map mail QTECH(config-cmap)# match access-group mail QTECH(config-cmap)# exit

	QTECH(config)# class-map file QTECH(config-cmap)# match access-group file QTECH(config)# policy-map toserver QTECH(config-pmap)# class mail QTECH(config-pmap-c)# set cos 4 QTECH(config-pmap-c)# exit QTECH(config-pmap)# class file QTECH(config-pmap-c)# set cos 3 QTECH(config-pmap-c)# exit QTECH(config-pmap)# class salary QTECH(config-pmap-c)# set cos 2 QTECH(config-pmap-c)# end QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# service-policy input toserver QTECH(config-if-GigabitEthernet 0/1)# mls qos trust cos QTECH(config-if-GigabitEthernet 0/1)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# service-policy input toserver QTECH(config-if-GigabitEthernet 0/2)# mls qos trust cos QTECH(config-if-GigabitEthernet 0/2)# exit QTECH(config)# interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# mls qos cos 7 QTECH(config)#wrr-queue bandwidth 1 1 1 2 6 1 1 0 QTECH(config)#mls qos scheduler wrr
Проверка	• Проверьте, успешно ли созданы списки ACL и успешно ли ассоциированы классы со списками ACL. • Проверьте, успешно ли созданы политики, успешно ли привязаны классы и поведение потоков и успешно ли применены политики к интерфейсам. • Проверьте, успешно ли настроено значение CoS по умолчанию для интерфейса и правильно ли настроены политика планирования и round robin weight
	QTECH# show access-lists

```
ip access-list extended file
 10 permit ip any host 192.168.10.3

ip access-list extended mail
 10 permit ip any host 192.168.10.2

ip access-list extended salary
 10 permit ip any host 192.168.10.1

QTECH# show class-map

Class Map salary
  Match access-group salary
Class Map mail
  Match access-group mail
Class Map file
  Match access-group file

QTECH# show policy-map

Policy Map toserver
  Class mail
   set cos 4
  Class file
   set cos 3
  Class salary
   set cos 2
QTECH# show mls qos interface gigabitEthernet 0/1
Interface: GigabitEthernet 0/1
Ratelimit input:
Ratelimit output:
Attached input policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0
```

```
QTECH# show mls qos interface gigabitEthernet 0/2
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input policy-map: toserver
Attached output policy-map:
Default trust: cos
Default cos: 0

QTECH# show mls qos interface gigabitEthernet 0/3
Interface: GigabitEthernet 0/2
Ratelimit input:
Ratelimit output:
Attached input policy-map:
Attached output policy-map:
Default trust: none
Default cos: 7
QTECH# show mls qos scheduler
Global Multi-Layer Switching scheduling
Weighted Round Robin
QTECH# QTECH#show mls qos queueing
CoS-to-queue map:
Cos  qid
---  ---
0    1
1    2
2    3
3    4
4    5
5    6
6    7
7    8
wrr bandwidth weights:
qid  weights
---  -------
1    1
```

```
2     1
3     1
4     2
5     6
6     1
7     1
8     0
drr bandwidth weights:
qid   weights
---   -------
1     1
2     1
3     1
4     1
5     1
6     1
7     1
8     1
wfq bandwidth weights:
qid   weights
---   -------
1     1
2     1
3     1
4     1
5     1
6     1
7     1
8     1
```

2.5.5. Настройка предотвращения перегрузки

2.5.5.1. Эффект конфигурации

- Настройте нижнее и верхнее пороговое значение для WRED. Когда длина пакетов в очереди меньше нижнего порогового значения, WRED не отбрасывает пакеты.
- Настройте максимальную вероятность отбрасывания. Когда длина пакетов в очереди находится между нижним и верхним пороговыми значениями, WRED отбрасывает пакеты случайным образом. Настраивается максимальная вероятность отбрасывания пакетов.

- Настройте сопоставление CoS-to-threshold.

2.5.5.2. Примечания

Конфигурации интерфейса допускают только конфигурации интерфейса AP и Ethernet.

2.5.5.3. Шаги настройки

Включение функции WRED

- Опционально.
- При необходимости включите функцию WRED.

Настройка нижнего порогового значения

- Опционально.
- При необходимости настройте нижнее пороговое значение.

Настройка верхнего порога

- Опционально.
- При необходимости настройте более высокий порог.

Настройка максимальной вероятности отбрасывания

- Опционально.
- При необходимости настройте максимальную вероятность отбрасывания.

Корректировка средней длины очереди для вероятности отбрасывания

- Опционально.
- При необходимости настройте интервал выборки и вес средней длины очереди.

Настройка сопоставления CoS-to-threshold

- Опционально.
- При необходимости настройте сопоставление CoS-to-threshold.

2.5.5.4. Проверка

- Запустите команду **show queuing wred interface**, чтобы отобразить конфигурацию WRED.
- Запустите команду **show qos wred-ecn statistics**, чтобы отобразить статистику пакетов, отброшенных WRED, и пакетов, помеченных ECN.

2.5.5.5. Связанная команда

Включение функции WRED

Команда	**queueing wred**
Режим команд	Режим глобальной конфигурации

Настройка нижнего порога (в процентах)

Команда	**wrr-queue random-detect min-threshold** *queue_id thr1* [*thr2*]
Описание параметров	*queue_id*: указывает идентификатор очереди для интерфейса в диапазоне от 1 до 8.

	thrN: Поддерживает 2 группы нижних порогов, в диапазоне от 1 до указанного верхнего порога
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Поскольку максимальное значение диапазона конфигурации равно текущему верхнему порогу, необходимо обратить внимание на настройку верхнего порога при настройке нижнего порога. Пороговое значение для пакетов, отбрасываемых WRED, может быть настроено в процентах или ячейках. Преобладает последний сконфигурированный режим

Настройка верхнего порога (в процентах)

Команда	**wrr-queue random-detect max-threshold** *queue_id thr1* [*thr2*]
Описание параметров	*queue_id*: указывает идентификатор очереди на интерфейсе в диапазоне от 1 до 8
Описание параметров	*thrN*: поддерживает 2 группы более высоких порогов, начиная от указанного нижнего порога до 100
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Поскольку минимальное значение настроенного диапазона равно текущему нижнему порогу, необходимо учитывать нижний порог при настройке верхнего порога. Пороговое значение для пакетов, отбрасываемых WRED, может быть настроено в процентах или ячейках. Преобладает последний сконфигурированный режим

Настройка нижнего порога (в ячейках)

Команда	**wrr-queue random-detect cell min-threshold** *queue_id thr1* [*thr2*]
Описание параметров	*queue_id*: указывает идентификатор очереди на интерфейсе в диапазоне от 1 до 8. *thrN*: поддерживает 2 группы нижних порогов, в диапазоне от 1 до указанного верхнего порога. Значение по умолчанию определяется продуктами
Режим команд	Режим конфигурации интерфейса

Руководство по использованию	Доступность этой команды определяется продуктами. Поскольку максимальное значение диапазона конфигурации равно текущему верхнему порогу, необходимо обратить внимание на настройку верхнего порога при настройке нижнего порога. Пороговое значение для пакетов, отбрасываемых WRED, может быть настроено в процентах или ячейках. Преобладает последний сконфигурированный режим

Настройка верхнего порога (в ячейках)

Команда	**wrr-queue random-detect cell max-threshold** *queue_id thr1* [*thr2*]
Описание параметров	*queue_id*: указывает идентификатор очереди на интерфейсе в диапазоне от 1 до 8. *thrN*: поддерживает 2 группы более высоких порогов, начиная от установленного нижнего порога и заканчивая максимально высоким порогом. Значение по умолчанию определяется продуктами
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Доступность этой команды определяется продуктами. Поскольку минимальное значение диапазона конфигурации равно текущему нижнему порогу, необходимо учитывать нижний порог при настройке верхнего порога. Пороговое значение для пакетов, отбрасываемых WRED, может быть настроено в процентах или ячейках. Преобладает последний сконфигурированный режим

Настройка максимальной вероятности отбрасывания

Команда	**wrr-queue random-detect probability** *queue_id prob1* [*prob2*]
Описание параметров	*queue_id*: указывает идентификатор очереди для интерфейса в диапазоне от 1 до 8. *probN*: поддерживает 2 группы максимальных вероятностей отбрасывания в диапазоне от 1 до 100
Режим команд	Режим конфигурации интерфейса

Корректировка средней длины очереди для вероятности отбрасывания – вес выборки

Команда	**wrr-queue random-detect sample-weight** *queue_id weight*
Описание параметров	*queue_id*: указывает идентификатор очереди на интерфейсе в диапазоне от 1 до 8.

	weight: указывает коэффициент веса в диапазоне от 0 до 15. Диапазон значений может варьироваться в зависимости от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Доступность этой команды определяется продуктами. Поскольку настроенный интервал выборки влияет на функцию отбрасывания WRED в режиме конфигурации интерфейса, рекомендуется настроить интервал выборки после верхнего и нижнего порогов для пакетов, которые будут отбрасываться WRED. Используйте эту команду вместе с командой настройки интервала выборки для пакетов, отбрасываемых WRED, чтобы точно настроить функцию отбрасывания WRED

Настройка сопоставления CoS-to-threshold

Команда	**wrr-queue cos-map** *threshold_id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]
Описание параметров	*threshold_id*: указывает идентификатор группы порогов в диапазоне от 1 до 2. Поддерживаются две группы порогов. *cos1…cos8*: указывает значения CoS, которые должны быть сопоставлены с пороговой группой, в диапазоне от 0 до 7. По умолчанию все значения CoS сопоставляются с первой пороговой группой
Режим команд	Режим конфигурации интерфейса

2.5.5.6. Пример конфигурации

Включение функции WRED и настройка нижнего порогового значения, максимальной вероятности отбрасывания и сопоставления CoS-to-threshold (при условии, что для продукта существует 2 группы пороговых значений)

Шаги настройки	• Включите функцию WRED. • Настройте нижние пороговые значения для очереди 2 интерфейса gigabitEthernet 0/2 на 10 и 20. • Настройте более высокие пороговые значения для очереди 2 интерфейса gigabitEthernet 0/2 на 60 и 90. • Настройте максимальные вероятности отбрасывания для очереди 2 интерфейса gigabitEthernet 0/2 на 60 и 80. • Настройте значения CoS 0, 1, 2 и 3 на интерфейсе gigabitEthernet 0/2, чтобы использовать пороговую группу 2
	QTECH# configure terminal QTECH(config)# queueing wred QTECH(config)# interface gigabitEthernet 0/2

	QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect min-threshold 2 10 20 QTECH(config-if-GigabitEthernet 0/2)#wrr-queue random-detect max-threshold 2 60 90 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect probability 2 60 80 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue random-detect probability 2 60 80 QTECH(config-if-GigabitEthernet 0/2)# wrr-queue cos-map 2 0 1 2 3
Проверка	Проверьте, включена ли функция WRED, успешно ли настроены пороговые значения и успешно ли настроено сопоставление CoS-to-threshold
	QTECH# show running-config Building configuration... Current configuration : 1654 bytes version 11.0(1C2B1)(09/11/13 00:16:26 CST -ngcf78) queueing wred QTECH# show queueing wred interface gigabitEthernet 0/2 --- --------- ---------- ----- ----- ------ --------- ---------- ----- Qid max_cell_1 min_cell 1 max_1 min_1 prob_1 max_cell_2 min_cell 2 max_2 min_2 prob_2 --- ---- ----- -- -- -- ------ ----- -- -- -- 1 120000 120000 0 0 0 120000 120000 1 1 1 2 120000 120000 60 10 60 120000 120000 90 20 80 3 120000 120000 0 0 0 120000 120000 1 1 1 4 120000 120000 0 0 0 120000 120000 1 1 1 5 120000 120000 0 0 0 120000 120000 1 1 1 6 120000 120000 0 0 0 120000 120000 1 1 1 7 120000 120000 0 0 0 120000 120000 1 1 1 8 120000 120000 0 0 0 120000 120000 1 1 1 --- --- ------------ cos qid threshold_id --- --- ------------

	0 1 2 1 2 2 2 5 2 3 5 2 4 5 1 5 5 1 6 7 1 7 8 1
	Проверьте пакеты, отброшенные WRED, и пакеты, помеченные ECN. QTECH#show qos wred-ecn statistics Wred ecn stats result: Port WredDropped EcnSended --- TFGigabitEthernet 0/1 0 0 TFGigabitEthernet 0/2 0 0 TFGigabitEthernet 0/3 0 0 TFGigabitEthernet 0/4 0 0 TFGigabitEthernet 0/5 0 0 TFGigabitEthernet 0/6 0 0 TFGigabitEthernet 0/7 0 0 TFGigabitEthernet 0/8 0 0 TFGigabitEthernet 0/9 0 0 TFGigabitEthernet 0/10 0 0 TFGigabitEthernet 0/11 0 0 TFGigabitEthernet 0/12 0 0

2.5.6. Настройка отображения очереди и режим настройки

2.5.6.1. Эффект конфигурации

Настройте отображение очереди и режим конфигурации, чтобы изменить режим отображения и конфигурации всех очередей на устройстве с 1–8 на 0–7.

2.5.6.2. Примечания

После настройки отображения очереди и режима конфигурации настроенные команды, относящиеся к очереди, изменяются автоматически.

2.5.6.3. Шаги настройки

Установка отображения очереди и режима конфигурации на 0–7

- Опционально.
- При необходимости установите отображение очереди и режим конфигурации на 0–7.

2.5.6.4. Проверка

Запустите команду **show running-config**, чтобы отобразить конфигурации.

2.5.6.5. Связанная команда

Установка отображения очереди и режима конфигурации на 0–7

Команда	**qos-queue compatible enable**
Режим команд	Режим глобальной конфигурации

2.5.6.6. Пример конфигурации

Установка отображения очереди и режима конфигурации на 0–7

Шаги настройки	Включить глобальный QOS
	QTECH# configure terminal QTECH(config)# qos-queue compatible enable
Проверка	Проверьте, успешно ли выполнена конфигурация
	QTECH# show running-config Building configuration... Current configuration : 1654 bytes version 11.0(1C2B1)(09/11/13 00:16:26 CST -ngcf78)

2.5.7. Отключение изменения приоритета пакетов

2.5.7.1. Эффект конфигурации

После того, как изменение приоритета пакета отключено, приоритет пакета при его отправке с устройства будет таким же, как при отправке пакета на устройство.

2.5.7.2. Этапы настройки

Отключение изменения приоритета пакетов

- Необязательный.

- Чтобы убедиться, что приоритет пакета при отправке с устройства такой же, как при отправке на устройство, отключите изменение приоритета пакета.

2.5.7.3. Проверка

Запустите команду **show running-config**, чтобы отобразить конфигурации.

2.5.7.4. Связанная команда

Отключение изменения приоритета пакетов

Команда	**mls qos remark disable**
Режим команд	Режим глобальной конфигурации

2.5.7.5. Пример

Отключение изменения приоритета пакетов

Шаги настройки	Отключить изменение приоритета пакетов
	QTECH#configure terminal QTECH(config)#mls qos remark disable

2.6. Мониторинг

2.6.1. Очистка

Описание	Команда
Очистить статистику пакетов, отброшенных WRED, и пакетов, помеченных ECN	**clear qos wred-ecn statistics** [**interfaces** *interface-id*]

2.6.1.1. Отображение

Описание	Команда
Отображает информацию о классификации потоков	**show class-map** [*class-map-name*]
Отображает информацию о политике QoS	**show policy-map** [*policy-map-name* [**class** *class-map-name*]]
Отображает политику, примененную к интерфейсу	**show policy-map interface** *interface-id*

Описание	Команда
Отображает информацию о группе логических интерфейсов	**show virtual-group** [*virtual-group-number* | **summary**]
Отображает политику, примененную к группе логических интерфейсов	**show mls qos virtual-group** [*virtual-group-number* | **policers**]
Отображает различные сопоставления	**show mls qos maps** [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]
Отображает информацию об ограничении скорости интерфейса	**show mls qos rate-limit** [**interface** *interface-id*]
Отображает очередь QoS, политику планирования и информацию о round robin weight	**show mls qos queueing** [**interface** *interface-id*]
Отображает информацию о планировании выходной очереди	**show mls qos scheduler** [**interface** *interface-id*]
Отображает конфигурации WRED	**show queueing wred interface** *interface-id*
Отображает информацию QoS интерфейса	**show mls qos interface** *interface-id* [**policers**]
Отображает информацию о пропускной способности интерфейса	**show qos bandwidth** [**interfaces** *interface-id*]
Отображать статистику пакетов, отброшенных WRED, и пакетов, помеченных ECN	**show qos wred-ecn statistics** [**interfaces** *interface-id*]

2.6.1.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключите отладку сразу после использования.

Описание	Команда
Отлаживает библиотеку QoS	**debug qos lib** [**event** | **message**]
Отлаживает сервер связи QoS	**debug qos server** [**event** | **message**]
Отлаживает обработку пользовательских команд QoS	**debug qos mls**
Отлаживает конфигурации VMSUP	**debug qos vmsup**

3. НАСТРОЙКА MMU

3.1. Обзор

Блок управления памятью (MMU) означает, что буфер микросхемы распределяется разумно, чтобы коммутационное оборудование могло лучше справляться со всеми видами пакетных потоков.

Потоки не стабильны все время, и в сети существуют различные пакетные потоки. При стабильном сетевом потоке и достаточной пропускной способности все потоки данных обрабатываются лучше; когда в сети существуют пакетные потоки, потоки данных могут быть отброшены, даже если средняя скорость потока не превышает пропускную способность.

Пакеты данных, поступающие на коммутационное оборудование, сохраняются в буфере коммутационного оборудования перед пересылкой. Обычно пакеты данных остаются в буфере на короткое время и пересылаются за микросекунды; при наличии пакетного потока, если мгновенная скорость пакетного потока превышает возможности обработки коммутационного оборудования, пакеты данных, которые не могут быть обработаны вовремя, будут накапливаться в коммутационном оборудовании, и потеря пакетов произойдет, как только буфера окажется недостаточно. В этом случае MMU можно использовать для разумной настройки буфера и выделения различных размеров буфера для соответствующих служб с целью оптимизации сети.

3.2. Приложения

Приложение	Описание
Настройка приложения с большим буфером на основе исходящей очереди	Предприятию требуется достаточно большой буфер в службе SkyDrive, чтобы избежать потери пакетов для потока службы

3.2.1. Настройка приложения с большим буфером на основе исходящей очереди

3.2.1.1. Сценарий

Предприятию требуется достаточно большой буфер в службе SkyDrive, чтобы избежать потери пакетов для потока службы.

Как показано на следующем рисунке, оборудование A подключено к 5 клиентам и 35 сервисным серверам, где 15 сервисных серверов виртуализируют 15 интерфейсных серверов.

Основной сервисный поток выглядит следующим образом:

- Клиентский сервер отправляет пакет запроса на фронтенд-сервер.
- Фронтенд-сервер отправляет полученный пакет запроса на сервисный сервер.
- После получения пакета запроса сервисный сервер отправляет ответный пакет фронтенд-серверу.
- Получив ответный пакет, фронтенд-сервер отправляет его клиентскому серверу.
- После получения ответного пакета клиент указывает, что сеанс успешно создан.

В этой сервисной модели существует режим передачи потока «многие к одному» (many-to-one):

- Потоки запросов нескольких клиентов отправляются на один фронтенд-сервер.
- Потоки запросов нескольких фронтенд-серверов отправляются на один сервисный сервер.
- Потоки ответов нескольких сервисных серверов отправляются на один фронтенд-сервер.
- Потоки ответов нескольких фронтенд-серверов отправляются одному клиенту.

Эти потоки передаются в основном через оборудование A, что легко приводит к перегрузке сети. Такую проблему можно исправить, настроив на оборудовании большой буфер.

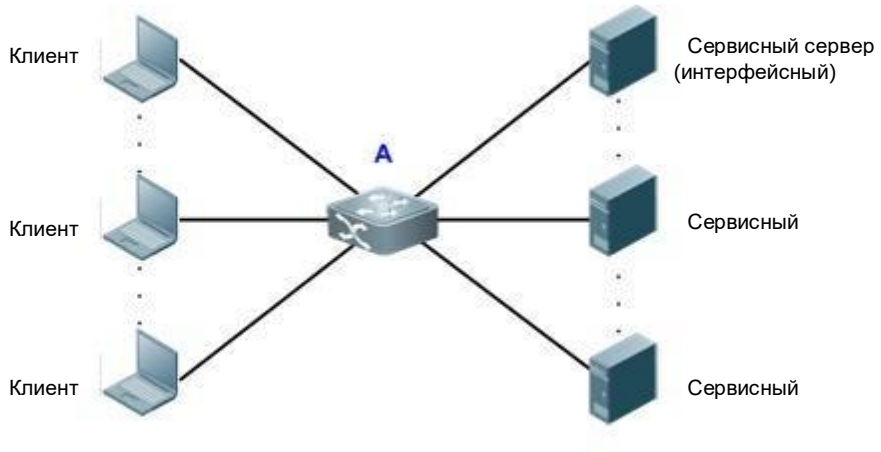

Рисунок 3-1.

3.2.1.2. Развертывание

- Во всех служебных портах (а именно, портах, соединяющих клиентов с серверами) настройте общий буфер очереди, в которой сервис настроен на 100 %.
- Во всех сервисных портах настройте минимальное значение гарантированного буфера неиспользуемой очереди.
- Во всех неиспользуемых портах настройте минимальное значение гарантированных буферов всех очередей.

Конкретную конфигурацию см. в примерах конфигурации в разделе Конфигурация.

3.3. Особенности

3.3.1. Базовые концепты

3.3.1.1. Ячейка (Cell)

Ячейка представляет собой буферную единицу, т. е. минимальную единицу хранения коммутационным оборудованием пакетов. Размер каждой ячейки зависит от продукта. Один пакет может использовать несколько ячеек, а одна ячейка может использоваться только одним пакетом.

3.3.1.2. Группа портов

Все порты, физически принадлежащие одному чипу коммутации, вместе называются группой портов, в группе портов управляется буфер коммутационного оборудования. Возьмем, к примеру, плату, в этой версии две микросхемы переключения, поэтому есть две группы портов. Первые 20 портов принадлежат к группе портов 1, а остальные 20 портов принадлежат к группе портов 2.

3.3.1.3. Исходящая очередь

Очереди на выходе портов делятся на одноадресные и многоадресные очереди (количество очередей зависит от продукта). Логически микросхема переключения делится на вход (ingress) (входящее направление) и выход (egress) (исходящее направление). Выходная очередь находится в направлении выхода. Прежде чем пакеты отправятся из выхода, для них необходимо выполнить операцию постановки в очередь в выходной очереди. В некоторых наших продуктах реализовано управление буфером на основе выходной очереди.

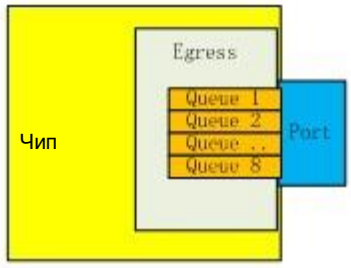

Рисунок 3-2.

В настоящее время существует три типа моделей исходящих очередей:

- На выходе имеется 8 одноадресных очередей и 8 многоадресных очередей. Хорошо известные одноадресные пакеты следуют за одноадресной очередью, а все остальные пакеты следуют за многоадресной очередью.
- На выходе имеется 8 одноадресных очередей и 4 многоадресных очереди. Хорошо известные одноадресные пакеты следуют за одноадресной очередью, а все остальные пакеты следуют за многоадресной очередью.
- На выходе всего 8 очередей, без разграничения на одноадресные и многоадресные очереди.

3.3.2. Обзор

Особенность	Описание
Настройка буфера	Буфер регулируется на основе очереди. Это основа MMU
Настройка мониторинга буфера	Мониторинг буфера фактически означает мониторинг использования емкости буфера, что облегчает настройку буфера
Настройка подсчета очереди	Полученные и отправленные пакеты каждой очереди подсчитываются, чтобы можно было легко отобразить результат настройки буфера

3.3.3. Настройка буфера

Регулировка буфера означает, что очередь каждой службы имеет разные размеры буфера за счет некоторой настройки буфера очереди, так что каждая служба обрабатывается по-разному, а службы с разными приоритетами обслуживаются по-разному.

3.3.3.1. Принцип работы

Рабочий механизм кеширования в аппаратном обеспечении

Что касается аппаратного обеспечения, буфер управляется в направлении ввода и вывода. Механизм обработки показан ниже.

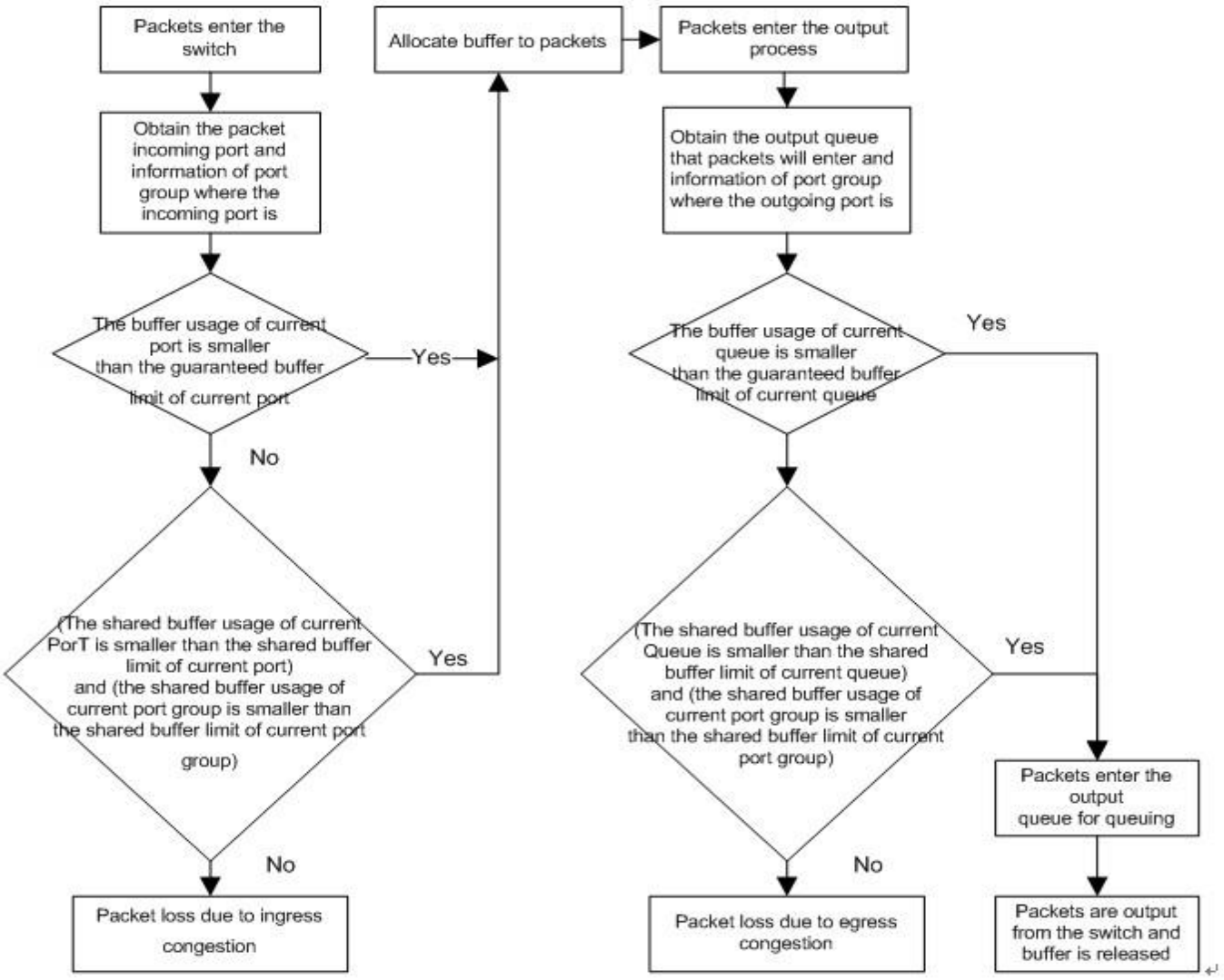

Рисунок 3-3.

Во время управления буфером направление ввода устанавливается на максимальное значение, чтобы предотвратить потерю пакетов в направлении ввода и обеспечить потерю пакетов в направлении вывода. Таким образом, корректировка не открывается для буфера в направлении ввода, а CLI обеспечивает корректировку буфера только в направлении вывода, включая гарантированный буфер очереди и общий буфер очереди. Настройка буфера настраивает гарантированный порог буфера и порог общего буфера очередей, чтобы выделять различные размеры буфера для очередей.

Гарантированный буфер

Гарантированный буфер также называется эксклюзивным буфером. Эта часть буфера распределяется по каждой очереди. Гарантированный буфер очереди может использоваться только этой очередью. По умолчанию для каждой очереди выделяется фиксированный гарантированный буфер. Эта часть очереди позволяет этой очереди пересылать пакеты с нормальной скоростью линии при стабильном потоке.

Совместный буфер (Shared buffer)

В общем буфере группы портов оставшаяся часть представляет собой общий совместный буфер после вычета гарантированного буфера каждой очереди. Совместный буфер может использоваться всеми очередями. Пороговое значение совместных очередей может быть установлено для каждой очереди. Этот порог ограничивает максимальный объем совместного буфера, который может использоваться этой очередью. Когда сумма совместного буфера, настроенная для каждой очереди в группе портов, превышает общую совместную очередь группы портов, применяется механизм заполнения буфера "первым пришел — первым обслужен".

3.3.4. Настройка мониторинга буфера

Мониторинг буфера реализует мониторинг объема использования каждой очереди и совместный буфера с целью обеспечения поддержки данных для оптимизации сети и разумной конфигурации буфера.

3.3.4.1. Принцип работы

Мониторинг буфера использует режим опроса для регулярного считывания объема использования буфера каждой очереди и ситуации использования совместного буфера и отображения ситуации использования буфера текущего оборудования в режиме реального времени.

Порог предупреждения использования буфера группы портов

Когда использование буфера группы портов превышает этот порог, системный журнал будет распечатан, чтобы напомнить пользователю.

Порог предупреждения об использовании буфера очереди

Когда использование буфера очереди превышает этот порог, системный журнал будет распечатан, чтобы напомнить пользователю.

Интервал выборки данных мониторинга буфера

Буферизованные данные мониторинга отбираются с определенным интервалом, который можно настроить в соответствии с требованиями пользователя.

3.3.5. Настройка подсчета очереди

Подсчет очередей отслеживает данные о пересылке и потере пакетов каждой очереди, чтобы обеспечить поддержку данных для оптимизации сети и разумной конфигурации буфера.

3.3.5.1. Принцип работы

Очередь переходит в режим опроса для регулярного считывания количества переадресованных пакетов/количества байтов и количества потерянных пакетов/количества байтов каждой очереди, а затем использует данные для расчета каждого вида статистики очереди.

Оповещение о потере пакетов в очереди

Устройство анализирует статистику по отброшенным пакетам, чтобы определить, происходит ли потеря пакетов в очереди. После потери пакетов в очереди устройство отображает предупреждение о потере пакетов в соответствии с конфигурацией предупреждения о потере пакетов.

Частота оповещения о потере пакетов в очереди

Только N предупреждений о потере пакетов могут отображаться в течение определенного периода T. Вы можете настроить период (T) и количество предупреждений (N), чтобы настроить отображение предупреждений о потере пакетов.

3.4. Конфигурация

Конфигурация	Описание и команда	
Настройка буфера	(Опционально) Он используется для настройки буфера	
	mmu queue-guarantee	Настраивает гарантированный буфер исходящей очереди
	mmu queue-threshold	Настраивает общий буфер исходящей очереди
	mmu pg-guarantee	Настраивает гарантированный входной буфер PG
	mmu ingress-threshold	Настраивает общий буфер входящего PG
	mmu headroom-threshold	Настраивает размер буфера запаса на основе PG
	mmu pg-headroom	Настраивает размер буфера глобального запаса
Настройка мониторинга буфера	(Опционально) Используется для настройки буфера	
	mmu usage-warn-limit	Настраивает пороговое значение оповещения использования буфера
	mmu sample-period	Настраивает интервал выборки данных мониторинга буфера
Настройка режима	**mmu cut-through**	Настраивает режим передачи cut-through

Конфигурация	Описание и команда	
Настройка предупреждения о потере пакетов	**mmu queue-loss-warn {unicast| multicast}**	Настраивает оповещение о потере пакетов в очереди
	mmu queue-loss-warn frequency	Настраивает частоту предупреждений о потере пакетов

3.4.1. Настройка буфера

3.4.1.1. Эффект конфигурации

- Настройте гарантированный буфер, чтобы очередь могла совместно использовать только эту часть буфера.
- Настройте совместный буфер, чтобы контролировать объем использования общего буфера очереди.

3.4.1.2. Примечания

Конфигурация интерфейса может быть выполнена только на физическом порту.

3.4.1.3. Шаги настройки

Настройка гарантированного буфера исходящей очереди

- Опционально.
- В режиме конфигурации интерфейса используйте команду **mmu queue-guarantee**, чтобы настроить гарантированный буфер для каждой очереди и убедиться, что диапазон конфигурации буфера зависит от продукта.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu queue-guarantee output** { **unicast** | **multicast** } [*queue-id1* [*queue-id2* [*queue-idN*]] **set** *value*
Описание параметров	**output**: выполняет управление буфером в исходящей очереди. **unicast**: выполняет управление буфером в исходящей очереди одноадресной передачи. **multicast**: выполняет управление буфером в исходящей очереди многоадресной рассылки. *queue-id*: идентификатор очереди в диапазоне от 1 до 8. *value*: количество гарантированных буферов, в ячейках; диапазон зависит от продукта
По умолчанию	По умолчанию для каждой очереди выделяется фиксированное количество гарантированных буферов. Конкретная конфигурация зависит от продукта
Режим команд	Режим конфигурации интерфейса

Руководство по использованию	Эффективность этой команды зависит от продукта

Настройка совместного буфера исходящей очереди

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu queue-threshold output** { **unicast** | **multicast** } [*queue-id1* [*queue-id2* [*queue-idN*]] **set** *thr%*
Описание параметров	**output**: выполняет управление буфером в исходящей очереди. **unicast**: выполняет управление буфером в исходящей очереди одноадресной рассылки. **multicast**: выполняет управление буфером в исходящей очереди многоадресной рассылки. *queue-id*: идентификатор очереди, в диапазоне от 1 до 8. *thr%*: процент, в диапазон от 1 до 100
По умолчанию	По умолчанию каждой очереди назначается пороговое значение использования совместного буфера. Этот порог представляет собой процент. Метод расчета максимально доступного совместного буфера для очереди следующий: Максимально доступный совместный буфер для очереди = общее количество совместных буферов группы портов * пороговое значение в процентах Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эффективность этой команды зависит от продукта

Настройка входного гарантийного буфера PG

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu pg-guarantee pg** { *priority -id1* [*priority-id2* [*priority -idN*] } *set value*
Описание параметров	*priority -idN*: номер входящей PG. *value*: гарантированное значение конфигурации буфера
По умолчанию	Значение по умолчанию зависит от продукта

Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эффективность этой команды зависит от продукта

Настройка совместного буфера входящего PG

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu ingress-threshold pg [***pg-id0* **[***pg-id1* **[***pg-id N***]] set** *thr%*
Описание параметров	*pg-idN*: идентификатор приоритетной группы. *th%*: общий совместный буфер × пороговое значение в процентах = максимально доступный буфер для очереди
По умолчанию	Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	1. Эффективность этой команды зависит от продукта. 2. Конфигурация вступает в силу, только если управление потоком/управление потоком на основе приоритета (PFC) не включено. 3. Значение, настроенное пользователем, отображается при выполнении команды **show run**, даже если значение, настроенное пользователем, является значением по умолчанию

Настройка запаса входного буфера PG

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu headroom-threshold pg** [*pg-id0* [*pg-id1* [*pg-id N*]] **set** *value*
Описание параметров	*pg-idN*: идентификатор приоритетной группы. *value*: пороговое значение запаса, измеряется в ячейках
По умолчанию	Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	1. Эффективность этой команды зависит от продукта. 2. Значение, настроенное пользователем, отображается при выполнении команды **show run**, даже если значение, настроенное пользователем, является значением по умолчанию

Настройка порога управления потоком

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu xoff-threshold pg** [*pg-id0* [*pg-id1* [*pg-id N*]] **set** *thr%*
Описание параметров	*pg-idN*: идентификатор приоритетной группы. *value*: пороговое значение запаса, измеряется в ячейках
По умолчанию	Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	1. Эффективность этой команды зависит от продукта. 2. Конфигурация вступает в силу, только если включено управление потоком/PFC. 3. Если управление потоком/PFC не включено, порог общего буфера PG соответствует значению **ingress-threshold**. 4. Значение, настроенное пользователем, отображается при выполнении команды **show run**, даже если значение, настроенное пользователем, является значением по умолчанию

Настройка порога восстановления управления потоком

- Необязательный.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu xon-threshold-offset pg** [*pg-id0* [*pg-id1* [*pg-id N*]] **set** *value*
Описание параметров	*pg-idN*: идентификатор приоритетной группы. *value*: пороговое значение запаса, измеряется в ячейках
По умолчанию	Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	1. Эффективность этой команды зависит от продукта. 2. Конфигурация вступает в силу, только если включено управление потоком/PFC. 3. Значение, настроенное пользователем, отображается при выполнении команды **show run**, даже если значение, настроенное пользователем, является значением по умолчанию

Настройка порога глобального запаса

- Опционально.
- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu pg-headroom set** *value*
Описание параметров	*value*: пороговое значение запаса, измеряется в ячейках
По умолчанию	Значение по умолчанию зависит от продукта
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	1. Эффективность этой команды зависит от продукта. 2. Конфигурация вступает в силу, только если включено управление потоком/PFC. 3. Значение, настроенное пользователем, отображается при выполнении команды **show run**, даже если значение, настроенное пользователем, является значением по умолчанию

3.4.1.4. Проверка

Используйте команду **show running**, чтобы проверить, успешно ли настроен MMU под соответствующим интерфейсом.

3.4.2. Настройка мониторинга буфера

3.4.2.1. Эффект конфигурации

- Настройте пороговое значение оповещения использования буфера для группы портов. Журнал предупреждений будет распечатан, когда использование буфера группы портов превысит это настроенное значение.
- Настройте пороговое значение предупреждающего сигнала использования буфера для очереди. Предупреждающий сигнал журнала будет распечатан, когда использование буфера очереди превысит это настроенное значение.
- Настройте интервал выборки данных мониторинга. Нижний слой производит выборку и сообщает данные в соответствии с настроенным интервалом.

3.4.2.2. Примечания

Конфигурация интерфейса может быть выполнена только на физическом порту.

3.4.2.3. Шаги настройки

Настройка порога оповещения об использовании буфера группы портов

- Опционально.
- В режиме глобальной конфигурации используйте команду **mmu usage-warn-limit**, чтобы настроить порог предупреждения об использовании буфера для группы портов.

- Используйте команды **no** или **default**, чтобы восстановить значение буфера по умолчанию.

Команда	**mmu usage-warn-limit set** *value*
Описание параметров	*value*: процент, в диапазоне от 1 до 100
По умолчанию	Значение по умолчанию равно 0, что указывает на то, что предупреждение не сообщается
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эта конфигурация действует для всех групп портов

Настройка порога предупреждения об использовании буфера очереди

- Опционально.
- В режиме конфигурирования интерфейса команду **mmu usage-warn-limit** { **unicast** | **multicast** } [*queue-id1* [*queue-id2* [*queueidN*]] **set** *value* для настройки порога предупреждения об использовании буфера для каждой очереди.
- Используйте команды **no** или **default**, чтобы восстановить настройку по умолчанию.

Команда	**mmu usage-warn-limit** { **unicast** | **multicast** } [*queue-id1* [*queue-id2* [*queue-idN*]] **set** *value*
Описание параметров	**unicast**: выполняет управление буфером в исходящей очереди одноадресной рассылки. **multicast**: выполняет управление буфером в исходящей очереди многоадресной рассылки. *queue-id*: идентификатор очереди в диапазоне от 1 до 8. *value*: процент, в диапазоне от 1 до 100
По умолчанию	Значение по умолчанию равно 0, что указывает на то, что предупреждение не сообщается
Режим команд	Режим конфигурации интерфейса

Настройка интервала выборки данных мониторинга

- Опционально.
- В режиме глобальной конфигурации используйте команду **mmu sample-period { buffer-counter | queue-counter }** *value* для настройки интервала выборки данных мониторинга для каждой очереди.
- Используйте команды **no** или **default**, чтобы восстановить настройку по умолчанию.

Команда	**mmu sample-period** { **buffer-counter | queue-counter** } *value*
Описание параметров	**buffer-counter**: количество занятых буферов. **queue-counter**: количество отправленных и удаленных записей в очереди. *value*: интервал выборки в секундах
По умолчанию	Интервал выборки по умолчанию составляет 5 секунд
Режим команд	Режим глобальной конфигурации

3.4.2.4. Проверка

- Используйте команду **show running**, чтобы проверить, успешно ли настроен MMU под соответствующим интерфейсом.
- Используйте команду **show queue-buffer**, чтобы проверить успешность конфигурации.

3.4.2.5. Примеры конфигурации

Настройка порогового значения предупреждающего сигнала использования буфера на основе группы портов

Шаги настройки	На коммутаторе настройте пороговое значение аварийного сигнала использования буфера для группы портов на 80 %
	QTECH# configure terminal QTECH(config)# mmu usage-warn-limit set 80 QTECH(config)#
Проверка	Проверьте, успешно ли сконфигурирован порог предупреждения использования буфера
	QTECH# show run mmu usage-warn-limit set 80

Настройка предела предупреждения использования буфера на основе исходящей очереди

Шаги настройки	Настройте порог предупреждения использования буфера как 70 % в очередях одноадресной рассылки 6 и 8 порта 1/1 на коммутаторе
	QTECH# configure terminal QTECH(config)# int te1/1 QTECH(config-if)#mmu usage-warn-limit unicast 6 8 set 70

Проверка	Проверьте, правильно ли настроен порог предупреждения использования буфера

QTECH#show queue-buffer interface gigabitEthernet 0/9

Dev/slot	Port-group	Total-shared(%)	Guarantee-used(%)	Share-used(%)	Available(%)	Warn-limit(%)
1/-	1	74.5271	0.0822	14.7615	85.1562	NA

Interface GigabitEthernet 0/9:

Type	Queue	Admin-shared(%)	Total-used(%)	Available(%)	Warn-limit(%)	Peak-usage(%)	Peak-time
Unicast	1	(default)	7.4836	0.0103	NA	7.5041	2015/7/14 20:7:14
Unicast	2	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	3	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	4	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	5	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	6	(default)	0.0000	7.4938	70%	0.0000	NA
Unicast	7	(default)	0.0000	7.4938	NA	0.0000	NA
Unicast	8	(default)	0.0000	7.4938	70%	0.0000	NA
Multicast	1	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	2	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	3	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	4	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	5	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	6	(default)	0.0000	7.4938	NA	0.0000	NA
Multicast	7	(default)	0.0000	7.4938	NA	0.0000	NA

	Multicast 8 (default) 0.0000 7.4938 NA 0.0000 NA

Настройка интервала выборки данных мониторинга

Шаги настройки	Настройте интервал выборки данных мониторинга в режиме глобальной конфигурации
	QTECH# configure terminal QTECH(config)# mmu sample-period buffer-counter 8 QTECH(config)# mmu sample-period queue-counter 10
Проверка	Проверьте, правильно ли настроен интервал выборки
	QTECH# show run mmu sample-period buffer-counter 8 mmu sample-period queue-counter 10

3.4.3. Настройка режима cut-through

3.4.3.1. Эффект конфигурации

Включите функцию cut-through, чтобы уменьшить задержку пересылки пакетов.

3.4.3.2. Примечания

Функцию подключения cut-through можно настроить только на физических портах.

3.4.3.3. Шаги настройки

Настройка гарантийного буфера

- Опционально.
- В режиме конфигурации интерфейса запустите команду **mmu cut-through**, чтобы включить функцию доступа cut-through на интерфейсе.
- Используйте команды **no** или **default**, чтобы восстановить настройку по умолчанию.

Команда	**mmu cut-through**
По умолчанию	По умолчанию режим cut-through отключен
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Эффективность этой команды зависит от продукта

3.4.4. Настройка предупреждения о потере пакетов

3.4.4.1. Эффект конфигурации

- Включить/выключить глобальное предупреждение о потери пакетов очередей для всех интерфейсных очередей.
- Включить/выключить оповещение о потере пакетов в очереди на интерфейсе. Приоритет этой конфигурации выше, чем у глобальной конфигурации.
- Настройте частоту сигналов предупреждения о потере пакетов так, чтобы в период T отображалось только N сигналов тревоги о потере пакетов.

3.4.4.2. Примечания

Эту функцию можно настроить в режиме глобальной конфигурации и в режиме конфигурации интерфейса.

3.4.4.3. Шаги настройки

Настройка оповещения о потере пакетов

- Опционально.
- В режиме глобальной конфигурации или конфигурации интерфейса запустите команду **mmu queue-loss-warn {unicast | multicast} [***qid1 [qid2 [qidN]]* **] {on | off}** для включения/отключения функции оповещения о потере пакетов в очередях.
- Используйте команды **no** или **default**, чтобы восстановить конфигурацию по умолчанию. Функция оповещения о потере пакетов по умолчанию отключена.

Команда	**[no] mmu queue-loss-warn {unicast | multicast } [***qid1 [qid2 [qidN]]* **] {on | off}**
Описание параметров	**unicast**: указывает на одноадресную очередь. **multicast**: указывает очередь многоадресной рассылки. *qid*: указывает идентификатор очереди. **on**: включает сигнализацию о потере пакетов. **off**: отключает оповещение о потере пакетов
По умолчанию	Функция оповещения о потере пакетов по умолчанию отключена
Режим команд	Режим глобальной конфигурации и режим конфигурации интерфейса
Руководство по использованию	Эффективный способ этой команды зависит от продукта

Настройка частоты оповещения о потере пакетов

- Опционально.
- В режиме глобальной конфигурации запустите команду **mmu queue-loss-warn frequency cycle** *value1* **times** *value2*, чтобы настроить частоту оповещения о потере пакетов.
- Используйте команды **no** или **default** для восстановления конфигурации по умолчанию.

Команда	**[no] mmu queue-loss-warn frequency cycle** *value1* **times** *value2*
Описание параметров	*value1*: указывает период отображения тревоги потери пакетов. *value2*: указывает количество аварийных сигналов о потере пакетов, которые могут отображаться за период
По умолчанию	По умолчанию в течение 60 секунд может отображаться до 30 предупреждений о потере пакетов
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эффективность этой команды зависит от продукта

3.5. Мониторинг

3.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команды **clear** во время работы оборудования может привести к прерыванию обслуживания из-за потери важной информации.

Описание	Команда
Очищает значение счетчика очереди	**clear queue-counter**
Очищает историческое пиковое значение буфера исходящей очереди	**clear mmu queue-buffer peaked**
Очищает историческое пиковое значение входного буфера PG	**clear mmu pg-buffer peaked**
Очищает количество раз, когда занятый буфер превышает порог предупреждения	**clear mmu usage-warn-count**

3.5.2. Отображение

Описание	Команда
Отображает информацию об использовании буфера интерфейса панели	**show queue-buffer interface**
Отображает информацию счетчика очереди интерфейса панели	**show queue-counter interface**
Отображает информацию об использовании буфера входного PG	**show pg-buffer interface**

4. ОБЩАЯ ИНФОРМАЦИЯ

4.1. Гарантия и сервис

Процедура и необходимые действия по вопросам гарантии описаны на сайте QTECH в разделе «Поддержка» –> «Гарантийное обслуживание».

Ознакомиться с информацией по вопросам тестирования оборудования можно на сайте QTECH в разделе «Поддержка» –> «Взять оборудование на тест».

Вы можете написать напрямую в службу сервиса по электронной почте sc@qtech.ru.

4.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться разделом технической поддержки пользователей QTECH на нашем сайте www.qtech.ru/support/.

Телефон Технической поддержки +7 (495) 269-08-81

Центральный офис +7 (495) 477-81-18

4.3. Электронная версия документа

Дата публикации 28.02.2025

https://files.qtech.ru/upload/switchers/QSW-7600/QSW-7600_ACL_QoS_config_guide.pdf