Руководство по настройке
Конфигурация коммутации Ethernet
Ethernet-коммутаторы ЦОД
серия QSW-6900

Оглавление

1. НАСТРОЙКА ИНТЕРФЕЙСОВ

1.1. Обзор

Интерфейсы важны для реализации коммутации данных на сетевых устройствах. Устройства QTECH поддерживают два типа интерфейсов: физические порты и логические интерфейсы. Физический порт — это аппаратный порт на устройстве, например, интерфейс 100M Ethernet и интерфейс Gigabit Ethernet. Логический интерфейс не является аппаратным портом на устройстве. Логический интерфейс, такой как loopback-интерфейс и туннельный интерфейс, может быть связан с физическим портом или не зависеть от какого-либо физического порта. Для сетевых протоколов физические порты и логические интерфейсы выполняют одну и ту же функцию.

1.2. Приложения

Приложение	Описание
Коммутация данных L2 через физический интерфейс Ethernet	Реализовать передачу данных уровня 2 (L2) сетевых устройств через физический интерфейс L2 Ethernet
Маршрутизация L3 через физический интерфейс Ethernet	Реализовать передачу данных уровня 3 (L3) сетевых устройств через физический интерфейс L3 Ethernet

1.2.1. Коммутация данных L2 через физический интерфейс Ethernet

1.2.1.1. Сценарий

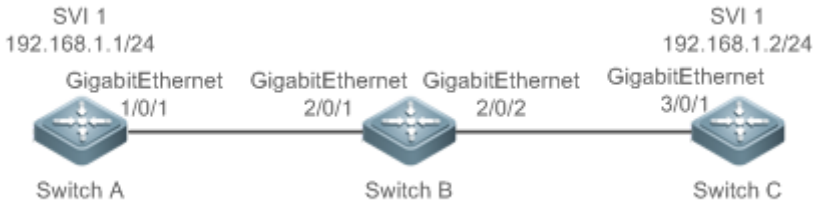


Рисунок 1-1.

Как показано на Рисунке 1-1, Коммутатор A, Коммутатор B и Коммутатор C образуют простую сеть передачи данных L2.

1.2.1.2. Развертывание

- Подключите коммутатор A к коммутатору B через физические порты GigabitEthernet 1/0/1 и GigabitEthernet 2/0/1.
- Подключите коммутатор B к коммутатору C через физические порты GigabitEthernet 2/0/2 и GigabitEthernet 3/0/1.
- Настройте GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2 и GigabitEthernet3/0/1 в качестве магистральных портов.

- Создайте виртуальный интерфейс коммутатора (SVI), SVI 1, на коммутаторе A и коммутаторе C соответственно, и настройте IP-адреса из сетевого сегмента для двух SVI. IP-адрес SVI 1 на коммутаторе A — 192.168.1.1/24, а IP-адрес SVI 1 на коммутаторе C — 192.168.1.2/24.
- Запустите команду **ping 192.168.1.2** на коммутаторе A и команду **ping 192.168.1.1** на коммутаторе C, чтобы реализовать переключение данных через коммутатор B.

1.2.2. Маршрутизация L3 через физический интерфейс Ethernet

1.2.2.1. Сценарий

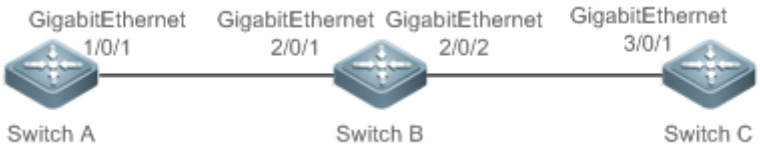


Рисунок 1-2.

Как показано на Рисунке 1-2, Коммутатор A, Коммутатор B и Коммутатор C образуют простую сеть передачи данных L3.

1.2.2.2. Развертывание

- Подключите коммутатор A к коммутатору B через физические порты GigabitEthernet 1/0/1 и GigabitEthernet 2/0/1.
- Подключите коммутатор B к коммутатору C через физические порты GigabitEthernet 2/0/2 и GigabitEthernet 3/0/1.
- Настройте GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2 и GigabitEthernet3/0/1 в качестве маршрутизируемых портов L3.
- Настройте IP-адреса из сегмента сети для GigabitEthernet 1/0/1 и GigabitEthernet 2/0/1. IP-адрес GigabitEthernet 1/0/1 — 192.168.1.1/24, а IP-адрес GigabitEthernet 2/0/1 — 192.168.1.2/24.
- Настройте IP-адреса из сегмента сети для GigabitEthernet 2/0/2 и GigabitEthernet 3/0/1. IP-адрес GigabitEthernet 2/0/2 — 192.168.2.1/24, а IP-адрес GigabitEthernet 3/0/1 — 192.168.2.2/24.
- Настройте запись статического маршрута на коммутаторе C, чтобы коммутатор C мог напрямую обращаться к сетевому сегменту 192.168.1.0/24. Настройте запись статического маршрута на коммутаторе A, чтобы коммутатор C мог напрямую обращаться к сегменту сети 192.168.1.0/24.
- Запустите команду **ping 192.168.2.2** на коммутаторе A и команду **ping 192.168.1.1** на коммутаторе C, чтобы реализовать маршрутизацию L3 через коммутатор B.

1.3. Функции

1.3.1. Базовые определения

Классификация интерфейсов

1. Интерфейсы на устройствах QTECH делятся на три категории:
   - Интерфейс L2 (коммутаторы или межсетевой мост)
   - Интерфейс L3 (поддерживается устройствами L3)

2. Общие интерфейсы L2 подразделяются на следующие типы:
   - Порт коммутации
   - Агрегируемый порт L2 (L2 AP)
3. Общие интерфейсы L3 подразделяются на следующие типы:
   - Маршрутизируемый порт
   - Порт агрегации L3 (L3 AP)
   - SVI
   - Loopback-интерфейс
   - Туннельный интерфейс

Порт коммутации (Switch Port)

Порт коммутации — это отдельный физический порт на устройстве, реализующий только функцию коммутации L2. Порт коммутации используется для управления физическими портами и протоколами L2, связанными с физическими портами.

Порт агрегации L2 (L2 AP Port)

Порт агрегации формируется путем объединения нескольких физических портов. Несколько физических каналов могут быть связаны вместе, чтобы сформировать простой логический канал. Этот логический канал называется портом AP.

Для коммутации L2 порт AP эквивалентен порту коммутации, который объединяет пропускную способность нескольких портов, тем самым увеличивая пропускную способность соединения. Кадры, отправленные через порт AP L2, распределяются между портами-участниками AP L2. В случае сбоя одного канала-участника порт AP L2 автоматически передает трафик по неисправному каналу на другие каналы-участники, повышая надежность соединений.

SVI

SVI можно использовать как интерфейс управления локальным устройством, через который администратор может управлять устройством. Вы также можете создать SVI в качестве интерфейса шлюза, который сопоставляется с виртуальным интерфейсом каждой VLAN для реализации маршрутизации через VLAN между устройствами L3. Вы можете запустить команду **interface vlan**, чтобы создать SVI и назначить IP-адрес этому интерфейсу для настройки маршрута между VLAN'ами.

Как показано на Рисунке 1-3, хосты в VLAN 20 могут напрямую общаться друг с другом без участия устройств L3. Если хост A в VLAN 20 хочет установить связь с хостом B в VLAN 30, необходимо использовать SVI 1 из VLAN 20 и SVI 2 из VLAN 30.

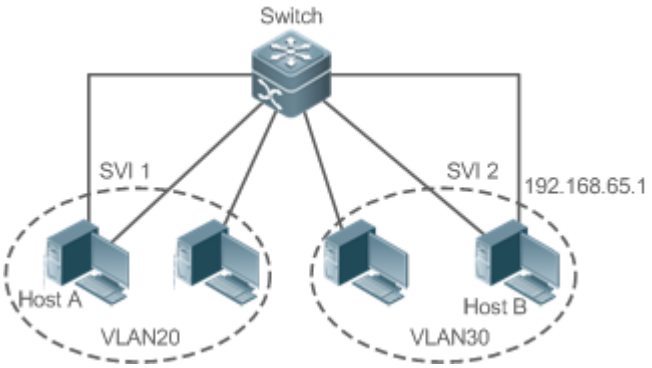


Рисунок 1-3.

Маршрутизируемый порт (Routed Port)

Физический порт на устройстве L3 можно настроить как маршрутизируемый порт, который работает как интерфейс шлюза для коммутации L3. Маршрутизируемый порт не связан с конкретной VLAN. Вместо этого это просто порт доступа. Маршрутизируемый порт нельзя использовать для коммутации L2. Вы можете запустить команду **no switchport**, чтобы изменить порт коммутации на маршрутизируемый порт и назначить IP-адрес этому порту для настройки маршрута. Обратите внимание, что перед выполнением команды **no switchport** необходимо удалить все функции L2 порта коммутации.

ПРИМЕЧАНИЕ: если порт является портом-участником AP L2 или портом DOT1X, который не прошел аутентификацию, вы не можете запустить команду **switchport** или **no switchport** для настройки порта коммутации или маршрутизируемого порта.

Порт AP L3 (L3 AP Port)

Как и порт AP L2, порт AP L3 — это логический порт, объединяющий несколько физических портов-участников. Агрегированные порты должны быть портами L3 того же типа. Порт AP функционирует как интерфейс шлюза для коммутации L3. Несколько физических каналов объединяются в один логический, что увеличивает пропускную способность канала. Кадры, отправленные через порт AP L3, распределяются между портами-участниками AP L3. В случае сбоя одного канала-участника порт AP L3 автоматически передает трафик неисправного канала на другие каналы-участники, повышая надежность соединений.

Порт AP L3 нельзя использовать для коммутации L2. Вы можете запустить команду **no switchport**, чтобы изменить порт AP L2, который не содержит портов-участников, на порт AP L3, добавить несколько маршрутизируемых портов к этому порту AP L3, а затем назначить IP-адрес этому порту AP L3 для настройки маршрута.

Loopback-интерфейс

Интерфейс loopback — это локальный логический интерфейс L3, моделируемый программным обеспечением, который всегда находится в состоянии UP. Пакеты, отправленные на loopback-интерфейс, обрабатываются на устройстве локально, включая информацию о маршруте. IP-адрес loopback-интерфейса может использоваться в качестве идентификатора устройства протокола маршрутизации Open Shortest Path First (OSPF) или в качестве исходного адреса, используемого протоколом пограничного шлюза (BGP) для установки TCP-соединения. Процедура настройки loopback-интерфейса аналогична настройке интерфейса Ethernet, и вы можете рассматривать loopback-интерфейс как виртуальный интерфейс Ethernet.

Туннельный интерфейс (Tunnel Interface)

Туннельный интерфейс реализует функцию туннеля. По туннельному интерфейсу протоколы передачи (например, IP) могут использоваться для передачи пакетов любого протокола. Как и другие логические интерфейсы, туннельный интерфейс также является виртуальным интерфейсом системы. Вместо указания какого-либо протокола передачи или протокола загрузки туннельный интерфейс обеспечивает стандартный режим передачи «точка-точка» (P2P). Следовательно, туннельный интерфейс должен быть настроен для каждого отдельного канала.

1.3.1.1. Обзор

Особенность	Описание
Команды настройки интерфейса	Вы можете настроить атрибуты, связанные с интерфейсом, в режиме конфигурации интерфейса. Если вы войдете в режим настройки несуществующего логического интерфейса, интерфейс будет создан
Описание интерфейса и административный статус	Вы можете настроить имя для интерфейса, чтобы идентифицировать интерфейс и помочь вам запомнить функции интерфейса. Вы также можете настроить административный статус интерфейса
MTU	Вы можете настроить максимальную единицу передачи (MTU) порта, чтобы ограничить длину кадра, который может быть получен или отправлен через этот порт
Пропускная способность	Вы можете настроить пропускную способность интерфейса
Интервал загрузки	Вы можете указать интервал для расчета нагрузки интерфейса
Carrier Delay	Вы можете настроить Carrier Delay для интерфейса, чтобы отрегулировать задержку, после которой статус интерфейса изменится с Down на Up или с Up на Down
Политика Link Trap	Вы можете включить или отключить функцию Link Trap на интерфейсе
Постоянство индекса интерфейса	Вы можете включить функцию сохранения индекса интерфейса, чтобы индекс интерфейса оставался неизменным после перезапуска устройства
Маршрутизируемый порт	Вы можете настроить физический порт на устройстве L3 как маршрутизируемый порт, который работает как интерфейс шлюза для коммутации L3
Агрегируемый порт L3	Вы можете настроить порт AP на устройстве L3 как порт AP L3, который функционирует как интерфейс шлюза для коммутации L3

Особенность	Описание
Скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования	Вы можете настроить скорость, дуплексный режим, режим управления потоком и режим автосогласования интерфейса
Автоматическое определение модуля	Если для скорости интерфейса установлено значение «Авто», скорость интерфейса может регулироваться автоматически в зависимости от типа вставленного модуля
Защищенный порт	Вы можете настроить некоторые порты как защищенные порты, чтобы отключить связь между этими портами. Вы также можете отключить маршрутизацию между защищенными портами
Порт восстановления Errdisable	После отключения порта из-за нарушения вы можете запустить команду восстановления errdisable в режиме глобальной конфигурации, чтобы восстановить все порты в состоянии errdisable и включить эти порты
Защита портов от нестабильности (flapping)	Вы можете настроить функцию защиты портов от flapping'a, чтобы система могла автоматически перевести порт в режим нарушения, когда на порту происходит flapping

1.3.2. Команды настройки интерфейса

Запустите команду **interface** в режиме глобальной конфигурации для входа в режим конфигурации интерфейса. Вы можете настроить атрибуты, связанные с интерфейсом, в режиме конфигурации интерфейса.

1.3.2.1. Принцип работы

Запустите команду **interface** в режиме глобальной конфигурации, чтобы войти в режим конфигурации интерфейса. Если вы войдете в режим настройки несуществующего логического интерфейса, интерфейс будет создан. Вы также можете запустить команду **interface range** или **interface range macro** в режиме глобальной конфигурации, чтобы настроить диапазон (идентификаторы) интерфейсов. Интерфейсы, определенные в одном диапазоне, должны быть одного типа и иметь одинаковые функции.

Вы можете запустить команду **no interface** в режиме глобальной конфигурации, чтобы удалить указанный логический интерфейс.

Правила нумерации интерфейсов

В автономном режиме идентификатор физического порта состоит из двух частей: идентификатора слота и идентификатора порта на слоте. Например, если идентификатор слота порта равен 2, а идентификатор порта в слоте равен 3, идентификатор интерфейса равен 2/3.

Правила нумерации слотов следующие: Идентификатор статического слота равен 0, тогда как идентификатор динамического слота (подключаемого модуля или линейной карты)

находится в диапазоне от 1 до количества слотов. Предположим, что вы стоите лицом к панели устройства. Динамические слоты нумеруются от 1 последовательно спереди назад, слева направо и сверху вниз.

Идентификатор порта в слоте находится в диапазоне от 1 до количества портов в слоте и нумеруется последовательно слева направо.

Идентификатор порта AP находится в диапазоне от 1 до количества портов AP, поддерживаемых устройством.

Идентификатор SVI — это VID VLAN, соответствующей этому SVI.

Настройка интерфейсов в диапазоне

Вы можете запустить команду **interface range** в режиме глобальной конфигурации, чтобы одновременно настроить несколько интерфейсов. Атрибуты, настроенные в режиме конфигурации интерфейса, применяются ко всем этим интерфейсам.

Команда **interface range** может использоваться для указания нескольких диапазонов интерфейсов.

Параметр **macro** используется для настройки макроса, соответствующего диапазону. Дополнительные сведения см. в разделе "Настройка макросов диапазонов интерфейса" ниже.

Диапазоны могут быть разделены запятыми (,).

Типы интерфейсов во всех диапазонах, указанных в команде, должны быть одинаковыми.

Обратите внимание на формат параметра **range** при запуске команды **interface range**.

Допустимы следующие форматы диапазонов интерфейсов:

- **FastEthernet** устройство/слот/{первый порт} - {последний порт};
- **GigabitEthernet** устройство/слот/{первый порт} - {последний порт};
- **TenGigabitEthernet** устройство/слот/{первый порт} - {последний порт};
- **FortyGigabitEthernet** устройство/слот/{первый порт} - {последний порт};
- **AggregatePort** *Aggregate-port ID* (идентификатор AP находится в диапазоне от 1 до максимального количества портов AP, поддерживаемых устройством.)
- **vlan** *vlan-ID-vlan-ID* (идентификатор VLAN находится в диапазоне от 1 до 4094.)
- **Loopback** *loopback-ID* (идентификатор loopback находится в диапазоне от 1 до 2 147 483 647.)
- **Tunnel** *tunnel-ID* (идентификатор туннеля находится в диапазоне от 0 до максимального количества туннельных интерфейсов, поддерживаемых устройством, минус 1).

Интерфейсы в диапазоне интерфейсов должны быть одного типа, а именно, FastEthernet или GigabitEthernet.

Настройка макросов диапазонов интерфейса

Вы можете определить некоторые макросы для замены диапазонов интерфейса. Прежде чем использовать параметр **macro** в команде **interface range**, вы должны сначала запустить команду **define interface-range** в режиме глобальной конфигурации, чтобы определить эти макросы.

Запустите команду **no define interface-range macro_name** в режиме глобальной конфигурации, чтобы удалить настроенные макросы.

1.3.3. Описание интерфейса и административный статус

Вы можете настроить имя для интерфейса, чтобы идентифицировать интерфейс и помочь вам запомнить функции интерфейса.

Вы можете войти в режим конфигурации интерфейса, чтобы включить или отключить интерфейс.

1.3.3.1. Принцип работы

Описание интерфейса

Вы можете настроить имя интерфейса в зависимости от назначения интерфейса. Например, если вы хотите назначить GigabitEthernet 1/1 для исключительного использования пользователем A, вы можете описать интерфейс как «Port for User A» (Порт для пользователя A).

Административный статус интерфейса

Вы можете настроить административный статус интерфейса, чтобы отключить интерфейс по мере необходимости. Если интерфейс отключен, кадры не будут приниматься или отправляться через этот интерфейс, и интерфейс потеряет все свои функции. Вы можете включить отключенный интерфейс, настроив административный статус интерфейса. Определены два типа административного статуса интерфейса: Up и Down. Административный статус интерфейса — Down, если интерфейс отключен, и Up, если интерфейс включен.

1.3.4. MTU

Вы можете настроить MTU порта, чтобы ограничить длину кадра, который может быть получен или отправлен через этот порт.

1.3.4.1. Принцип работы

Когда через порт передается большой объем данных, могут существовать кадры большего размера, чем стандартный кадр Ethernet. Этот тип кадра называется Jumbo Frame. MTU — это длина сегмента действительных данных в кадре. Он не включает накладные расходы на инкапсуляцию Ethernet.

Если порт получает или отправляет кадр, длина которого превышает MTU, этот кадр будет отброшен.

MTU находится в диапазоне от 64 байт до 9 216 байт с шагом в четыре байта. MTU по умолчанию составляет 1500 байт.

ПРИМЕЧАНИЕ: команда **mtu** действует только на физическом порту или AP-порту.

1.3.5. Пропускная способность

1.3.5.1. Принцип работы

Команду **bandwidth** можно настроить таким образом, чтобы некоторые протоколы маршрутизации (например, OSPF) могли вычислять метрику маршрута, а протокол резервирования ресурсов (RSVP) мог вычислять зарезервированную полосу пропускания. Изменение пропускной способности интерфейса не повлияет на скорость передачи данных физического порта.

ПРИМЕЧАНИЕ: команда **bandwidth** является параметром маршрутизации и не влияет на пропускную способность физического канала.

1.3.6. Интервал загрузки

1.3.6.1. Принцип работы

Вы можете запустить команду **load-interval**, чтобы указать интервал для расчета нагрузки интерфейса. Как правило, интервал составляет 10 секунд.

1.3.7. Задержка пересылки

1.3.7.1. Принцип работы

Задержка пересылки относится к задержке, после которой сигнал обнаружения пересылки данных (DCD) изменяется с Down на Up или с Up на Down. Если статус DCD изменится во время задержки, система проигнорирует это изменение, чтобы избежать согласования на верхнем канальном уровне. Если для этого параметра установлено большое значение, почти каждое изменение DCD не будет обнаружено. Наоборот, если параметр установлен на 0, каждое изменение сигнала DCD будет обнаруживаться, что приведет к плохой стабильности.

ПРИМЕЧАНИЕ: если пересылка DCD прерывается в течение длительного времени, следует установить задержку пересылки на меньшее значение для ускорения сходимости топологии или маршрута. Наоборот, если время прерывания пересылки DCD меньше времени сходимости топологии или маршрута, задержка пересылки должна быть установлена на большее значение, чтобы избежать flapping'а топологии или маршрута.

1.3.8. Политика Link Trap

Вы можете включить или отключить функцию Link Trap на интерфейсе.

1.3.8.1. Принцип работы

Когда функция Link Trap на интерфейсе включена, простой протокол управления сетью (SNMP) отправляет Link Trap'ы при изменении состояния связи на интерфейсе.

1.3.9. Постоянство индекса интерфейса

Как и имя интерфейса, индекс интерфейса также идентифицирует интерфейс. При создании интерфейса система автоматически присваивает интерфейсу уникальный индекс. Индекс интерфейса может измениться после перезагрузки устройства. Вы можете включить функцию сохранения индекса интерфейса, чтобы индекс интерфейса оставался неизменным после перезапуска устройства.

1.3.9.1. Принцип работы

После включения сохранения индекса интерфейса индекс интерфейса остается неизменным после перезапуска устройства.

1.3.10. Маршрутизируемый порт

1.3.10.1. Принцип работы

Физический порт на устройстве L3 можно настроить как маршрутизируемый порт, который работает как интерфейс шлюза для коммутации L3. Маршрутизируемый порт нельзя использовать для коммутации L2. Вы можете запустить команду **no switchport**, чтобы изменить порт коммутации на маршрутизируемый порт и назначить IP-адрес этому порту для настройки маршрута. Обратите внимание, что перед выполнением команды **no switchport** необходимо удалить все функции L2 порта коммутации.

1.3.11. Агрегируемый порт L3

1.3.11.1. Принцип работы

Как и в случае с маршрутизируемым портом уровня 3, вы можете запустить команду **no switchport**, чтобы изменить порт агрегации уровня 2 на порт агрегации уровня 3 на устройстве уровня 3, а затем назначить IP-адрес этому порту агрегации для настройки маршрута. Обратите внимание, что вы должны удалить все функции L2 порта AP перед запуском команды **no switchport**.

ПРИМЕЧАНИЕ: порт AP L2 с одним или несколькими портами-участниками не может быть настроен как порт AP L3. Точно так же порт AP L3 с одним или несколькими портами-участниками нельзя изменить на порт AP L2.

1.3.12. Скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования

Вы можете настроить скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования физического порта Ethernet или порта AP.

1.3.12.1. Принцип работы

Скорость

Как правило, скорость физического порта Ethernet определяется путем согласования с peer-устройством. Согласованная скорость может быть любой скоростью в пределах возможностей интерфейса. Вы также можете настроить любую скорость в пределах возможностей интерфейса для физического порта Ethernet.

Когда вы настраиваете скорость порта AP, конфигурация влияет на все его порты-участники. (Все эти порты-участники являются физическими портами Ethernet.)

Дуплексный режим

- Дуплексный режим физического порта Ethernet или порта AP можно настроить следующим образом:
- Установите дуплексный режим интерфейса на полнодуплексный, чтобы интерфейс мог получать пакеты во время отправки пакетов.
- Установите дуплексный режим интерфейса на полудуплексный, чтобы интерфейс мог получать или отправлять пакеты одновременно.
- Установите дуплексный режим интерфейса на автосогласование, чтобы дуплексный режим интерфейса определялся посредством автосогласования между локальным интерфейсом и peer-интерфейсом.
- Когда вы настраиваете дуплексный режим порта AP, конфигурация влияет на все его порты-участники. (Все эти порты-участники являются физическими портами Ethernet.)

Управление потоком

Для интерфейса определены два режима управления потоком:

- Симметричный режим управления потоком: как правило, после включения управления потоком на интерфейсе интерфейс обрабатывает полученные кадры управления потоком и отправляет кадры управления потоком, когда на интерфейсе возникает перегрузка. Полученные и отправленные кадры управления потоком обрабатываются одинаково. Это называется симметричным режимом управления потоком.

- Асимметричный режим управления потоком: в некоторых случаях ожидается, что интерфейс на устройстве будет обрабатывать полученные кадры управления потоком, чтобы гарантировать, что ни один пакет не будет отброшен из-за перегрузки, и не отправлять кадры управления потоком, чтобы избежать снижения скорости сети. В этом случае необходимо настроить асимметричный режим управления потоком, чтобы отделить процедуру получения кадров управления потоком от процедуры отправки кадров управления потоком.
- Когда вы настраиваете режим управления потоком порта AP, конфигурация влияет на все его порты-участники. (Все эти порты-участники являются физическими портами Ethernet.)

Как показано на Рисунке 1-4, Порт A устройства является портом uplink, а порты B, C и D — портами downlink. Предположим, что порт A включен с функциями отправки и получения кадров управления потоком. Порт B и порт C подключены к разным медленным сетям. Если большой объем данных отправляется через порт B и порт C, порт B и порт C будут перегружены, и, следовательно, перегрузка произойдет во входящем направлении порта A. Таким образом, порт A отправляет кадры управления потоком. Когда uplink-устройство отвечает на кадры управления потоком, оно уменьшает поток данных, отправляемых на порт A, что косвенно снижает скорость сети на порту D. В это время вы можете отключить функцию отправки кадров управления потоком на порте A для обеспечения использования пропускной способности всей сети.

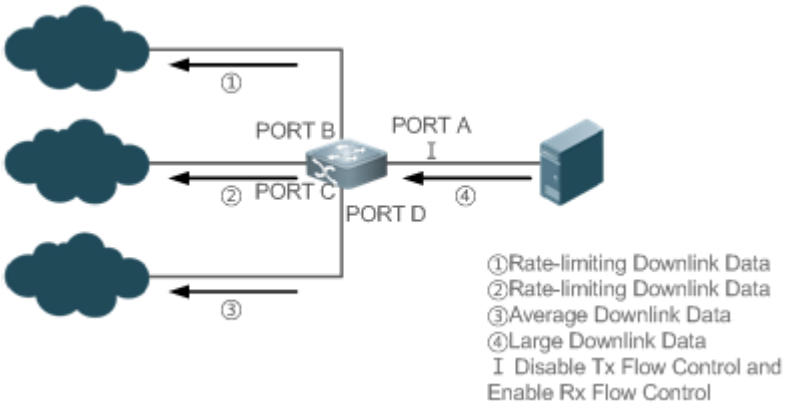


Рисунок 1-4.

Режим автоматического согласования

- Режим автосогласования интерфейса может быть включен или выключен. Состояние автосогласования интерфейса не полностью эквивалентно режиму автосогласования. Состояние автосогласования интерфейса совместно определяется скоростью интерфейса, дуплексным режимом, режимом управления потоком и режимом автосогласования.
- Когда вы настраиваете режим автоматического согласования порта AP, конфигурация вступает в силу на всех его портах-участниках. (Все эти порты-участники являются физическими портами Ethernet.)

ПРИМЕЧАНИЕ: как правило, если скорость интерфейса, дуплексный режим и режим управления потоком установлены на автоматический режим или режим автосогласования интерфейса включен, состояние автосогласования интерфейса включено, т. е. функция автоматического согласования интерфейса включена. Если ни для скорости интерфейса, ни для режима дуплекса, ни для режима управления потоком не задано значение auto, а режим автосогласования интерфейса выключен, состояние автосогласования интерфейса равно Off, т. е. функция автосогласования интерфейса выключена.

ПРИМЕЧАНИЕ: для 100-мегабитного оптоволоконного порта функция автосогласования всегда отключена, то есть состояние автосогласования 100-мегабитного оптоволоконного порта всегда отключено. Для гигабитного медного порта функция автосогласования всегда включена, то есть состояние автосогласования гигабитного медного порта всегда включено.

1.3.13. Автоматическое определение модуля

Если для скорости интерфейса установлено значение Auto, скорость интерфейса может регулироваться автоматически в зависимости от типа вставленного модуля.

1.3.13.1. Принцип работы

В настоящее время функцию автоматического обнаружения модулей можно использовать для обнаружения только модулей SFP и SFP+. SFP — это гигабитный модуль, тогда как SFP+ — это 10-гигабитный модуль. Если вставленный модуль SFP, интерфейс работает в гигабитном режиме. Если вставленный модуль SFP+, интерфейс работает в 10-гигабитном режиме.

ПРИМЕЧАНИЕ: функция автоматического обнаружения модуля действует только тогда, когда для скорости интерфейса установлено значение Auto.

1.3.14. Защищенный порт (Protected Port)

В некоторых средах приложений требуется, чтобы связь между некоторыми портами была отключена. Для этого вы можете настроить некоторые порты как защищенные порты. Вы также можете отключить маршрутизацию между защищенными портами.

1.3.14.1. Принцип работы

Защищенный порт

После того, как порты настроены как защищенные порты, защищенные порты не могут взаимодействовать друг с другом, но могут взаимодействовать с незащищенными портами.

Защищенные порты работают в любом из двух режимов. В первом режиме коммутация L2 заблокирована, но разрешена маршрутизация между защищенными портами. Во втором режиме коммутация L2 и маршрутизация заблокированы между защищенными портами. Если защищенный порт поддерживает оба режима, по умолчанию используется первый режим.

Когда два защищенных порта настроены как пара зеркальных (mirroring) портов, кадры, отправленные или полученные исходным портом, могут быть зеркалированы на порт назначения.

В настоящее время в качестве защищенного порта можно настроить только физический порт Ethernet или порт AP. Когда порт AP настроен как защищенный порт, все его порты-участники настраиваются как защищенные порты.

Блокировка маршрутизации L3 между защищенными портами

По умолчанию маршрутизация L3 между защищенными портами не блокируется. В этом случае вы можете запустить команду **protected-ports route-deny**, чтобы заблокировать маршрутизацию между защищенными портами.

1.3.15. Порт восстановления Errdisable

Некоторые протоколы поддерживают функцию восстановления после сбоя порта для обеспечения безопасности и стабильности сети. Например, в протоколе безопасности порта, когда вы включаете защиту порта и настраиваете максимальное количество

адресов безопасности для порта, событие нарушения порта генерируется, если количество адресов, полученных на этом порту, превышает максимальное количество адресов безопасности. Другие протоколы, такие как протокол связующего дерева (STP), DOT1X, REUP и частый flapping портов, поддерживают аналогичные функции, и порт, нарушающий правила, будет автоматически закрыт для обеспечения безопасности.

1.3.15.1. Принцип работы

После отключения порта из-за нарушения вы можете запустить команду **errdisable recovery** в режиме глобальной конфигурации, чтобы восстановить все порты в состоянии errdisable и включить эти порты. Вы можете восстановить порт вручную или автоматически в назначенное время.

1.3.16. Разделение и объединение портов 100G

1.3.16.1. Принцип работы

Порт 100G Ethernet — это порт с высокой пропускной способностью. Он в основном используется на устройствах на уровне конвергенции или на уровне ядра для увеличения пропускной способности порта. Разделение порта 100G означает, что порт 100G разделен на четыре порта 25G. В это время порт 100G становится недоступным, а четыре порта 25G пересылают данные независимо друг от друга. Комбинация портов 100G означает, что четыре порта 25G объединены в порт 100G. В это время четыре порта 25G становятся недоступными, и только порт 100G передает данные. Вы можете гибко настраивать пропускную способность, комбинируя или разделяя порты.

1.3.17. SVI или субинтерфейсная выборка

По умолчанию SVI или субинтерфейс не поддерживает статистику пакетов. Такая информация, как количество пакетов, полученных или отправленных через SVI или субинтерфейс, а также скорость отправки/получения пакетов, не может быть отображена. Вы можете включить выборку SVI или субинтерфейса для отображения этой статистики.

1.3.18. Защита портов от нестабильности (flapping)

Когда на порту происходит flapping, возникает много аппаратных прерываний, потребляющих много ресурсов ЦП. С другой стороны, частый flapping порта повреждает порт. Вы можете настроить функцию защиты от flapping’а для защиты портов.

1.3.18.1. Принцип работы

По умолчанию функция защиты портов от flapping’а включена. При необходимости вы можете отключить эту функцию. Когда на порту происходит flapping, порт определяет flapping каждые 2 или 10 секунд. Если в течение 2 секунд на порту происходит flapping шесть раз, устройство отображает подсказку. Если непрерывно отображаются 10 подсказок, т. е. в течение 20 секунд постоянно обнаруживается flapping портов, порт переходит в режим нарушения (причину нарушения показывает Link Dither). Если в течение 10 секунд на порту происходит flapping 10 раз, устройство отображает подсказку, не переводя порт в режим нарушения.

1.3.19. Syslog (системный журнал)

Вы можете включить или отключить функцию системного журнала, чтобы определить, отображать ли информацию об изменениях или исключениях интерфейса.

1.3.19.1. Принцип работы

При необходимости вы можете включить или отключить функцию системного журнала. По умолчанию эта функция включена. Когда интерфейс становится ненормальным, например, изменяется статус интерфейса, или интерфейс получает кадры ошибок, или происходит flapping, система отображает подсказки для уведомления пользователей.

1.3.20. Глобальный MTU

Пользователи могут установить глобальный MTU для управления максимальной длиной кадров, которые могут быть отправлены и получены через все порты.

1.3.20.1. Принцип работы

Когда обмен данными с большой пропускной способностью осуществляется через порт, могут существовать кадры, длина которых больше, чем у стандартного кадра Ethernet, и эти кадры называются jumbo-кадрами. MTU указывает длину допустимых полей данных в кадре, за исключением служебных данных инкапсуляции Ethernet.

Если длина кадра, полученного или отправленного портом, превышает значение MTU, кадр будет отброшен.

Значение MTU находится в диапазоне от 64 до 9216 байт. Шаг составляет четыре байта. Значение по умолчанию — 1500 байт.

ПРИМЕЧАНИЕ: IP MTU автоматически изменяется на значение MTU канала интерфейса при изменении глобально установленного MTU канала.

ПРИМЕЧАНИЕ: MTU интерфейса имеет приоритет над глобальным MTU. После настройки глобального MTU для MTU интерфейса нельзя установить значение по умолчанию.

1.3.21. MAC-адрес интерфейса

1.3.21.1. Принцип работы

По умолчанию каждый интерфейс Ethernet имеет глобально уникальный MAC-адрес. При необходимости MAC-адреса интерфейсов Ethernet можно изменить. Однако MAC-адреса в одной и той же локальной сети должны быть уникальными.

Чтобы настроить MAC-адрес интерфейса Ethernet, выполните команду **mac-address** в режиме настройки интерфейса:

ПРИМЕЧАНИЕ: конфигурация MAC-адресов может повлиять на внутреннюю связь в локальной сети. Поэтому пользователям рекомендуется не настраивать MAC-адреса самостоятельно, если в этом нет необходимости.

1.3.21.2. Связанная конфигурация

Настройка MAC-адресов для интерфейсов

По умолчанию каждый интерфейс имеет глобально уникальный MAC-адрес.

Вы можете запустить команду **mac-address** *mac-address* в режиме конфигурации интерфейса, чтобы изменить MAC-адрес интерфейса.

1.3.22. Флаг инкапсуляции VLAN на интерфейсах

1.3.22.1. Принцип работы

Виртуальная локальная сеть (VLAN) представляет собой логическую сеть, разделенную на физическую сеть, и соответствует сети уровня 2 в модели OSI. В 1999 году IEEE выпустила проект протокола 802.1Q для стандартизации решения по реализации VLAN.

Технология VLAN позволяет сетевому администратору разделить физическую локальную сеть на несколько широковещательных доменов (или VLAN). Каждая VLAN содержит группу рабочих станций с одинаковыми требованиями, и каждая VLAN имеет те же атрибуты, что и физическая LAN. Так как виртуальные сети логически разделены, рабочие станции в одной и той же виртуальной сети не обязательно размещать в одном и том же физическом пространстве, то есть эти рабочие станции могут принадлежать к разным физическим сегментам локальной сети. Многоадресный и одноадресный трафик в VLAN не будет перенаправляться в другие VLAN. Это помогает контролировать трафик, сокращать инвестиции в устройства, упрощает управление сетью и повышает безопасность сети.

VLAN — это протокол, используемый для решения проблем широковещательной (broadcast) передачи и безопасности Ethernet. Во время передачи пакета к кадрам Ethernet добавляется заголовок VLAN. Кроме того, идентификаторы VLAN используются для классификации пользователей по разным рабочим группам, чтобы ограничить обмен на уровне 2 между пользователями в разных рабочих группах. Каждая рабочая группа представляет собой сеть VLAN. Сети VLAN можно использовать для ограничения области широковещательной рассылки и формирования виртуальных рабочих групп для динамического управления сетями.

Чтобы обеспечить связь с хостами в VLAN, пользователи могут настроить флаг инкапсуляции VLAN 802.1Q (протокол VLAN) на интерфейсе или субинтерфейсе Ethernet. В этом случае при отправке пакетов через интерфейс Ethernet соответствующий заголовок VLAN будет инкапсулирован. При получении пакетов заголовок VLAN будет удален из пакета.

1.3.22.2. Связанная конфигурация

Настройка флага инкапсуляции VLAN для интерфейсов

По умолчанию протокол инкапсуляции 802.1Q отключен для интерфейсов.

Вы можете запустить команду **encapsulation dot1Q VlanID** в интерфейсном режиме для инкапсуляции 802.1Q для интерфейса. **VlanID** указывает инкапсулированный идентификатор VLAN.

1.3.23. Режим FEC интерфейса

1.3.23.1. Принцип работы

Прямое исправление ошибок (FEC) — это метод исправления кода ошибки, использующий следующий принцип работы: отправитель добавляет избыточный код исправления ошибок к данным для отправки. Приемник выполняет обнаружение ошибок в данных на основе кода исправления ошибок. Если обнаружена ошибка, получатель исправляет ошибку. FEC улучшает качество сигнала, но также вызывает задержку сигнала. Пользователи могут включать или отключать эту функцию в зависимости от реальной ситуации.

Различные типы портов поддерживают разные режимы FEC. Порт 25 Гбит/с поддерживает режим BASE-R, а порт 100 Гбит/с поддерживает режим RS.

1.3.23.2. Связанная конфигурация

Настройка режима FEC интерфейса

По умолчанию режим FEC отключен для порта 25 Гбит/с, а включение или отключение режима FEC для порта 100 Гбит/с определяется вставленным оптическим модулем.

Запустите режим **fec mode {rs | base-r | none | auto}** в режиме интерфейса для настройки режима FEC на интерфейсе.

1.3.24. Цикл выборки статистики по портам Ethernet

1.3.24.1. Принцип работы

Цикл выборки статистики портов Ethernet по умолчанию составляет 5 секунд, что означает, что статистика интерфейса обновляется каждые 5 секунд. В сценариях с высокими требованиями к статистике в реальном времени можно продлить цикл выборки.

ПРИМЕЧАНИЕ: более короткий цикл выборки указывает на более высокое потребление производительности системы. Поэтому цикл выборки должен быть скорректирован по мере необходимости. Если количество физических портов превышает 500, рекомендуется установить цикл выборки более 10 секунд.

1.3.24.2. Связанная конфигурация

Настройка цикла выборки статистики на портах Ethernet

Цикл выборки статистики портов Ethernet по умолчанию составляет 5 секунд.

Запустите команду **ethernet-port counter sample-period [** *seconds* **]** в режиме глобальной конфигурации, чтобы настроить цикл выборки на портах Ethernet.

1.4. Ограничения

- Оптические порты продуктов серии QSW-6900 не поддерживают скорость 100 Мбит/с.
- Оптический порт 10G: когда оптический трансивер 10G вставляется в оптический порт 10G, режим автосогласования отключается. Когда оптический трансивер 1000M вставлен в оптический порт 10G, режим автосогласования включен по умолчанию.
- Оптический порт 40G: когда оптический трансивер вставляется в оптический порт 40G, режим автосогласования отключается. Когда медный кабель подключен к оптическому порту 40G, включается режим автосогласования.
- Для продуктов серии QSW-6900 MTU преобразуется в длину пакета для расчета в чипах. Преобразованная длина пакета, используемая для расчета, на 26 байт (включая 14-байтовый заголовок Ethernet, 4-байтовый FCS и два тега) больше настроенного MTU.
- Когда переключение режимов настроено на портах 25G QSW-6900-56F (**port speed-mode 10G/25G**), режимы четырех последовательных портов настроенного порта изменяются одновременно, и скорость не может быть настроена для портов 25G.
- Убедитесь, что IP MTU, IPv6 MTU и Link MTU интерфейсов уровня 3 установлены правильно и IP/IPv6 MTU не превышает MTU интерфейса. Интерфейсы уровня 3 включают в себя порты маршрутизации, порты агрегации уровня 3 и SVI.

1.5. Конфигурация

Конфигурация	Описание и команда	
Выполнение основных конфигураций	(Опционально) Используется для управления конфигурациями интерфейса, например, для создания/удаления интерфейса или настройки описания интерфейса	
	interface	Создает интерфейс и входит в режим конфигурации созданного интерфейса или заданного интерфейса
	interface range	Вводит диапазон интерфейсов, создает этот интерфейс (если не создан) и входит в режим настройки интерфейса
	define interface-range	Создает макрос для указания диапазона интерфейса
Выполнение основных конфигураций	**snmp-server if-index persis**	Включает функцию сохранения индекса интерфейса, чтобы индекс интерфейса оставался неизменным после перезапуска устройства
	description	Настраивает описание интерфейса до 80 символов в режиме конфигурации интерфейса
	snmp trap link-status	Настраивает, отправлять ли link trap'ы интерфейса
	shutdown	Закрывает интерфейс в режиме конфигурации интерфейса
	split interface	Разделяет порт 40G в режиме глобальной конфигурации
	physical-port dither protect	Настраивает защиту интерфейса от flapping'а в режиме глобальной конфигурации
	logging [link-updown | error-frame | linkdither | res-lack-frame]	Позволяет вносить в журналы информацию о состоянии интерфейса в режиме глобальной конфигурации

Конфигурация	Описание и команда	
Настройка атрибутов интерфейса	(Опционально) Он используется для настройки атрибутов интерфейса	
	bandwidth	Настраивает пропускную способность интерфейса в режиме конфигурации интерфейса
	carrier-delay	Настраивает carrier delay интерфейса в режиме конфигурации интерфейса
	load-interval	Настраивает интервал расчета нагрузки интерфейса
	duplex	Настраивает дуплексный режим интерфейса
	flowcontrol	Включает или отключает управление потоком интерфейса
Настройка атрибутов интерфейса	**mtu**	Настраивает MTU интерфейса
	negotiation mode	Настраивает режим автосогласования интерфейса
	speed	Настраивает скорость интерфейса
	port speed-mode	Настраивает скоростной режим для порта 25G
	switchport	Настраивает интерфейс как интерфейс L2 в режиме настройки интерфейса. (Выполните команду **no switchport**, чтобы настроить интерфейс как интерфейс L3.)
	switchport protected	Настраивает порт как защищенный порт
	protected-ports routedeny	Блокирует маршрутизацию L3 между защищенными портами в режиме глобальной конфигурации
	errdisable recovery [cause link-state]	Восстанавливает порт в состоянии errdisable в режиме глобальной конфигурации

Конфигурация	Описание и команда	
Настройка атрибутов интерфейса	**route-sample enable**	Включает функцию выборки SVI/субинтерфейса в режиме конфигурации интерфейса
	mtu forwarding	Устанавливает глобальный MTU и IP MTU
	mac-address	Устанавливает MAC-адрес интерфейса
	encapsulation dot1Q	Устанавливает тег VLAN для интерфейса
	fec mode	Настраивает режим FEC для интерфейса
	ethernet-port counter sample-period	Настраивает период выборки статистики для порта Ethernet

1.5.1. Выполнение основных конфигураций

1.5.1.1. Эффект конфигурации

- Создайте указанный логический интерфейс и войдите в режим конфигурации этого интерфейса или войдите в режим конфигурации существующего физического или логического интерфейса.
- Создайте несколько указанных логических интерфейсов и войдите в режим конфигурации интерфейса или войдите в режим конфигурации нескольких существующих физических или логических интерфейсов.
- Индексы интерфейса остаются неизменными после перезагрузки устройства.
- Настройте описание интерфейса, чтобы пользователи могли напрямую узнавать информацию об интерфейсе.
- Включите или отключите функцию link trap интерфейса.
- Включить или отключить интерфейс.
- Разделите порт 100G или объедините четыре порта 25G в порт 100G.

1.5.1.2. Примечания

- Форма команды **no** может использоваться для удаления указанного логического интерфейса или логических интерфейсов в указанном диапазоне, но не может использоваться для удаления физического порта или физических портов в указанном диапазоне.
- Форму команды **default** можно использовать в режиме настройки интерфейса для восстановления настроек по умолчанию указанного физического или логического интерфейса или интерфейсов в указанном диапазоне.

1.5.1.3. Шаги настройки

Настройка указанного интерфейса

- Необязательный.

- Запустите эту команду, чтобы создать логический интерфейс или войти в режим настройки физического порта или существующего логического интерфейса.

Команда	**interface** *interface-type interface-number*
Описание параметров	*interface-type interface-number*: указывает тип и номер интерфейса. Интерфейс может быть физическим портом Ethernet, AP-портом, SVI или петлевым интерфейсом
Командный режим	Режим глобальной конфигурации
Руководство по использованию	• Если логический интерфейс еще не создан, запустите эту команду, чтобы создать этот интерфейс и войти в режим настройки этого интерфейса. • Для физического порта или существующего логического интерфейса выполните эту команду, чтобы войти в режим настройки этого интерфейса. • Используйте форму команды **no**, чтобы удалить указанный логический интерфейс. • Используйте форму команды **default** для восстановления настроек интерфейса по умолчанию в режиме конфигурации интерфейса

Настройка интерфейсов в диапазоне

- Опционально.
- Запустите эту команду, чтобы создать несколько логических интерфейсов или войти в режим конфигурации нескольких физических портов или существующих логических интерфейсов.

Команда	**interface range** { *port-range* | **macro** *macro_name* }
Описание параметров	*port-range*: указывает тип и идетификатор диапазона интерфейсов. Эти интерфейсы могут быть физическими портами Ethernet, AP-портам, SVI или петлевыми интерфейсами. *macro_name*: указывает имя макроса диапазона интерфейса
Командный режим	Режим глобальной конфигурации
Руководство по использованию	• Если логические интерфейсы еще не созданы, запустите эту команду, чтобы создать эти интерфейсы и войти в режим настройки интерфейса. • Для нескольких физических портов или существующих логических интерфейсов запустите эту команду, чтобы войти в режим настройки интерфейса.

Руководство по использованию	• Используйте форму команды default, чтобы восстановить настройки этих интерфейсов по умолчанию в режиме конфигурации интерфейса. • Перед использованием макроса запустите команду define interface-range, чтобы определить диапазон интерфейса как имя макроса в режиме глобальной конфигурации, а затем запустите команду interface range macro macro_name, чтобы применить макрос

Настройка сохранения индекса интерфейса

- Опционально.
- Запустите эту команду, когда индексы интерфейса должны оставаться неизменными после перезапуска устройства.

Команда	**snmp-server if-index persist**
По умолчанию	По умолчанию сохранение индекса интерфейса отключено
Командный режим	Режим глобальной конфигурации
Руководство по использованию	После выполнения этой команды текущие индексы всех интерфейсов будут сохранены, а после перезапуска устройства индексы не изменятся. Вы можете использовать форму **no** или форму команды **default**, чтобы отключить функцию сохранения индекса интерфейса

Настройка описания интерфейса

- Опционально.
- Запустите эту команду, чтобы настроить описание интерфейса.

Команда	**description** *string*
Описание параметров	*string*: обозначает строку длиной до 80 символов
По умолчанию	По умолчанию нет описания
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для настройки описания интерфейса. Вы можете использовать форму **no** или форму команды **default**, чтобы удалить описание интерфейса

Настройка функции Link Trap интерфейса

- Опционально.
- Запустите эту команду, чтобы получить link trap'ы через SNMP.

Команда	**snmp trap link-status**
По умолчанию	По умолчанию функция Link Trap включена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для настройки функции Link Trap на интерфейсе. Когда эта функция включена, SNMP отправляет link trap'ы при изменении состояния связи на интерфейсе. Вы можете использовать форму **no** или форму команды **default**, чтобы отключить функцию Link Trap

Настройка административного статуса интерфейса

- Опционально.
- Запустите эту команду, чтобы включить или отключить интерфейс.
- Интерфейс не может отправлять или получать пакеты после его отключения.

Команда	**shutdown**
По умолчанию	По умолчанию административный статус интерфейса Up
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Вы можете запустить команду **shutdown**, чтобы отключить интерфейс, или команду **no shutdown**, чтобы включить интерфейс. В некоторых случаях, например, когда интерфейс находится в состоянии errdisable, вы не можете запустить команду **no shutdown** на интерфейсе. Вы можете использовать форму **no** или форму команды **default**, чтобы включить интерфейс

Разделение порта 100G или объединение четырех портов 25G в один порт 100G

- Опционально.
- Запустите эту команду, чтобы разделить порт 100G или объединить четыре порта 25G в один порт 100G.

Команда	[**no**] **split interface** *interface-type interface-number*
Описание параметров	*interface-type interface-number*: указывает тип и номер порта. Порт должен быть портом 100G
По умолчанию	По умолчанию порты объединены
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Вы можете запустить команду **split**, чтобы разделить порт 100G, или команду **no split**, чтобы объединить разделенный порт 100G. После настройки этой команды обычно требуется перезапустить линейную карту или все устройство, чтобы конфигурация вступила в силу

Настройка SVI или функции выборки субинтерфейса

- Опционально.
- Запустите эту команду, чтобы включить функцию выборки SVI или субинтерфейса.

Команда	[**no**] **route-sample enable**
По умолчанию	По умолчанию SVI или субинтерфейс не поддерживают выборку
Командный режим	Режим конфигурации интерфейса

Настройка защиты от flapping'а портов

- Опционально.
- Запустите эту команду, чтобы защитить порт от flapping'а.

Команда	**physical-port dither protect**
По умолчанию	По умолчанию защита от flapping'а портов включена
Командный режим	Режим глобальной конфигурации

Настройка функции системного журнала

- Опционально.
- Запустите эту команду, чтобы включить или отключить функцию системного журнала на интерфейсе.

Команда	[**no**] **logging** [**link-updown** | **error-frame** | **link-dither** | **res-lack-frame**]
Описание параметров	**link-updown**: печатает информацию об изменении состояния. **error-frame**: печатает информацию об ошибке. **link-dither**: выводит информацию о переключении портов. **res-lack-frame**: печатает информацию об ошибке, полученной интерфейсом, из-за нехватке ресурса
По умолчанию	По умолчанию функция системного журнала включена на интерфейсе
Командный режим	Режим глобальной конфигурации

1.5.1.4. Проверка

Настройка указанного интерфейса

- Запустите команду **interface**. Если вы можете войти в режим конфигурации интерфейса, конфигурация выполнена успешно.
- Для логического интерфейса после выполнения команды **no interface** запустите команду **show running** или **show interfaces**, чтобы проверить, существует ли логический интерфейс. В противном случае логический интерфейс удаляется.
- После выполнения команды **default interface** запустите команду **show running**, чтобы проверить, восстановлены ли настройки по умолчанию для соответствующего интерфейса. Если да, то операция прошла успешно.

Настройка интерфейсов в диапазоне

- Запустите команду **interface range**. Если вы можете войти в режим конфигурации интерфейса, конфигурация выполнена успешно.
- После выполнения команды **default interface range** запустите команду **show running**, чтобы проверить, восстановлены ли настройки по умолчанию для соответствующих интерфейсов. Если да, то операция прошла успешно.

Настройка сохранения индекса интерфейса

- После выполнения команды **snmp-server if-index persist** запустите команду **write**, чтобы сохранить конфигурацию, перезапустите устройство и запустите команду **show interface**, чтобы проверить индекс интерфейса. Если индекс интерфейса остается прежним после перезапуска, включается сохранение индекса интерфейса.

Настройка функции Link Trap интерфейса

- Удалите, а затем вставьте сетевой кабель в физический порт и включите сервер SNMP. Если сервер SNMP получает link trap'ы, функция Link Trap активирована.
- Запустите форму **no** команды **snmp trap link-status**. Извлеките, а затем вставьте сетевой кабель в физический порт. Если сервер SNMP не получает link trap'ы, функция Link Trap отключена.

Настройка административного статуса интерфейса

- Вставьте сетевой кабель в физический порт, включите порт и выполните команду **shutdown** на этом порту. Если на консоли отображается системный журнал, указывающий на то, что состояние порта изменяется на Down, а индикатор порта не горит, порт отключен. Запустите команду **show interfaces** и убедитесь, что состояние интерфейса изменилось на Administratively Down. Затем запустите команду **no shutdown**, чтобы включить порт. Если на консоли отображается системный журнал, указывающий, что состояние порта изменяется на Up, а индикатор на порте горит, порт включен.

Разделение или объединение порта 100G

- Запустите команду **split** на порту 100G в режиме глобальной конфигурации. Убедитесь, что соответствующий системный журнал отображается на консоли. Запустите команду **write**, чтобы сохранить конфигурацию, и перезапустите устройство или линейную карту в соответствии с методом, описанным в системном журнале. Четыре порта 25G можно настроить как порты L2 или L3, но разделенный порт 100G нельзя настроить как порт L2 или L3.
- Запустите команду **no split** на разделенном порту 100G. Убедитесь, что соответствующий системный журнал отображается на консоли. Запустите команду **write**, чтобы сохранить конфигурацию, и перезапустите устройство или линейную карту в соответствии с методом, описанным в системном журнале.

Четыре порта 25G нельзя настроить как порты L2 или L3, но комбинированный порт 100G можно настроить как порт L2 или L3.

Настройка SVI или функции выборки субинтерфейса

Запустите команду **route-sample enable** в режиме конфигурации SVI или субинтерфейса. Затем запустите команду **show interface** и убедитесь, что отображается количество отправленных или полученных пакетов и скорость отправки/получения пакетов. Запустите команду **no route-sample enable**. Затем запустите команду **show interface** и убедитесь, что количество отправленных или полученных пакетов и скорость отправки/получения пакетов не отображаются.

Настройка защиты от переключения портов

Запустите команду **physical-port dither protect** в режиме глобальной конфигурации. Часто извлекайте и вставляйте сетевой кабель в физический порт, чтобы имитировать переключение порта. Убедитесь, что системный журнал, указывающий на переключение портов, отображается на консоли. После того, как такой syslog появится несколько раз, система предложит перевести порт в режим нарушения.

1.5.1.5. Пример конфигурации

Настройка основных атрибутов интерфейсов

Сценарий:

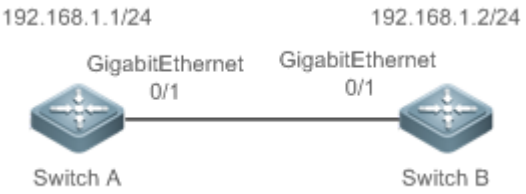


Рисунок 1-5.

Шаги настройки	• Подключите два устройства через порты коммутатора. • Настройте SVI соответственно на двух устройствах и назначьте IP-адреса из сегмента сети двум SVI. • Включите сохранение индекса интерфейса на двух устройствах. • Включите функцию Link Trap на двух устройствах. • Настройте административный статус интерфейса на двух устройствах
A	A# configure terminal A(config)# snmp-server if-index persist A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# snmp trap link-status A(config-if-GigabitEthernet 0/1)# shutdown

	A(config-if-GigabitEthernet 0/1)# end A# write
B	B# configure terminal B(config)# snmp-server if-index persist B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface gigabitethernet 0/1 B(config-if-GigabitEthernet 0/1)# snmp trap link-status B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Проверка	Выполните проверку на коммутаторе A и коммутаторе B следующим образом: • Запустите команду **shutdown** для порта GigabitEthernet 0/1 и проверьте, отключены ли GigabitEthern 0/1 и SVI 1. • Запустите команду **shutdown** на порту GigabitEthernet 0/1 и проверьте, отправляется ли Trap-сообщение, указывающее, что этот интерфейс отключен. • Перезапустите устройство и проверьте, совпадает ли индекс GigabitEthernet 0/1 с индексом до перезапуска
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is administratively down , line protocol is DOWN Hardware is GigabitEthernet, address is 08c6.b3.de9b (bia 08c6.b3.de9b) Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0

	4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns , 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP , line protocol is DOWN Hardware is VLAN, address is 08c6.b3.33af (bia 08c6.b3.33af) Interface address is: 192.168.1.1/24 ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is administratively down , line protocol is DOWN

Hardware is GigabitEthernet
Interface address is: no ip address, address is 08c6.b3.de9b (bia 08c6.b3.de9b)
MTU 1500 bytes, BW 1000000 Kbit
Encapsulation protocol is Bridge, loopback not set
Keepalive interval is 10 sec , set
Carrier delay is 2 sec
Rxload is 1/255, Txload is 1/255

Queue	Transmitted packets	Transmitted bytes	Dropped packets	Dropped bytes
0	0	0	0	0
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	4	440	0	0

Switchport attributes:
interface's description:""
lastchange time:0 Day:20 Hour:15 Minute:22 Second
Priority is 0

admin duplex mode is AUTO, oper duplex is Unknown
admin speed is AUTO, oper speed is Unknown
flow control admin status is OFF, flow control oper status is Unknown
admin negotiation mode is OFF, oper negotiation state is ON
Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
Port-type: access
Vlan id: 1
10 seconds input rate 0 bits/sec, 0 packets/sec
10 seconds output rate 0 bits/sec, 0 packets/sec
4 packets input, 408 bytes, 0 no buffer, 0 dropped
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
4 packets output, 408 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1

	Index(dec):4097 (hex):1001 VLAN 1 is UP , line protocol is DOWN Hardware is VLAN, address is 08c6.b3.33af (bia 08c6.b3.33af) Interface address is: 192.168.1.2/24 ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec , set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255

1.5.2. Настройка атрибутов интерфейса

1.5.2.1. Эффект конфигурации

- Разрешите устройству подключаться и обмениваться данными с другими устройствами через порт коммутации или маршрутизируемый порт.
- Настройте различные атрибуты интерфейса на устройстве.

1.5.2.2. Шаги настройки

Настройка маршрутизируемого порта

- Опционально.
- Запустите эту команду, чтобы настроить порт как маршрутизируемый порт L3.
- После того, как порт настроен как маршрутизируемый порт L3, протоколы L2, работающие на порту, не вступают в силу.
- Эта команда применима к порту коммутации L2.

Команда	**no switchport**
По умолчанию	По умолчанию физический порт Ethernet является портом коммутации L2
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	На устройстве L3 вы можете запустить эту команду, чтобы настроить порт коммутации L2 в качестве маршрутизируемого порта L3. Вы можете запустить команду **switchport**, чтобы изменить маршрутизируемый порт L3 на порт коммутации L2

Настройка порта AP L3

- Необязательный.
- Запустите команду **no switchport** в режиме конфигурации интерфейса, чтобы настроить порт AP L2 в качестве порта AP L3. Запустите команду **switchport**, чтобы настроить порт AP L3 в качестве порта AP L2.

- После того, как порт настроен как маршрутизируемый порт L3, протоколы L2, работающие на порту, не вступают в силу.
- Эта команда применима к порту AP L2.

Команда	**no switchport**
По умолчанию	По умолчанию порт AP является портом AP L2
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	После входа в режим конфигурации порта AP L2 на устройстве L3 вы можете запустить эту команду, чтобы настроить порт AP L2 как порт AP L3. После входа в режим конфигурации порта AP L3 вы можете запустить команду **switchport**, чтобы изменить порт AP L3 на порт AP L2

Настройка скорости интерфейса

- Опционально.
- Flapping портов может произойти, если настроенная скорость порта изменится.
- Эта команда применима к физическому порту Ethernet или порту AP.
- Один и тот же режим скорости должен быть настроен на четырех последовательных портах 25 Гбит/с.

Команда	**speed [10 | 100 | 1000 | 10G | 40G | 100G | auto]**
Описание параметров	**10**: указывает, что скорость интерфейса составляет 10 Мбит/с. **100**: указывает, что скорость интерфейса составляет 100 Мбит/с. **1000**: указывает, что скорость интерфейса составляет 1000 Мбит/с. **10G**: указывает, что скорость интерфейса составляет 10 Гбит/с. **40G**: указывает, что скорость интерфейса составляет 40 Гбит/с. **100G**: указывает, что скорость интерфейса составляет 100 Гбит/с
По умолчанию	По умолчанию скорость интерфейса установлена автоматически
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Если интерфейс является портом-участником AP, скорость этого интерфейса определяется скоростью порта AP. Когда интерфейс выходит из порта AP, он использует собственную конфигурацию скорости. Вы можете запустить **show interfaces** для отображения конфигураций скорости. Параметры скорости, доступные для интерфейса, зависят от типа интерфейса. Например, вы не можете установить скорость интерфейса SFP на 10 Мбит/с. **ПРИМЕЧАНИЕ:** скорость физического порта 40G может быть установлена только на 40 Гбит/с или автоматически

Команда	**port speed-mode [10G | 25G]**
Описание параметров	**10G**: указывает, что скорость интерфейса составляет 10 Гбит/с. **25G**: указывает, что скорость интерфейса составляет 25 Гбит/с
По умолчанию	Скорость интерфейса по умолчанию 25G
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Только порты 25 Гбит/с поддерживают этот режим скорости. Один и тот же режим скорости должен быть настроен на четырех последовательных портах 25 Гбит/с. **ПРИМЕЧАНИЕ:** только порты 25 Гбит/с с одинаковым скоростным режимом могут присоединяться к одной и той же группе агрегации. **ПРИМЕЧАНИЕ:** запуск команды **default interface** не очищает конфигурацию режима скорости на портах 25 Гбит/с

Настройка дуплексного режима интерфейса

- Опционально.
- Flapping порта может произойти, если настроенный дуплексный режим порта изменяется.
- Эта команда применима к физическому порту Ethernet или порту AP.

Команда	**duplex { auto | full | half }**
Описание параметров	**auto**: указывает на автоматическое переключение между полным дуплексом и полудуплексом. **full**: указывает на полный дуплекс. **half**: указывает на полудуплекс
По умолчанию	По умолчанию дуплексный режим интерфейса — автоматический

Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Дуплексный режим интерфейса связан с типом интерфейса. Вы можете запустить **show interfaces** для отображения конфигураций дуплексного режима

Настройка режима управления потоком интерфейса

- Опционально.
- Как правило, режим управления потоком интерфейса по умолчанию отключен. Для некоторых продуктов режим управления потоком включен по умолчанию.
- После включения управления потоком на интерфейсе кадры управления потоком будут отправляться или приниматься для регулировки объема данных, когда на интерфейсе возникает перегрузка.
- Flapping порта может произойти, если настроенный режим управления потоком порта изменяется.
- Эта команда применима к физическому порту Ethernet или порту AP.

Команда	**flowcontrol { auto | off | on }**
Описание параметров	**auto**: указывает на автоматическое управление потоком. **off**: указывает, что управление потоком отключено. **on**: указывает, что управление потоком включено
По умолчанию	По умолчанию управление потоком на интерфейсе отключено
Командный режим	Режим конфигурации интерфейса

Настройка режима автосогласования интерфейса

- Опционально.
- Flapping порта может произойти, если настроенный режим автосогласования порта изменяется.
- Эта команда применима к физическому порту Ethernet или порту AP.

Команда	**negotiation mode { on | off }**
Описание параметров	**on**: указывает, что режим автосогласования включен. **off**: указывает, что режим автосогласования выключен
По умолчанию	По умолчанию режим автосогласования выключен
Командный режим	Режим конфигурации интерфейса

Настройка MTU интерфейса

- Опционально.
- Вы можете настроить MTU порта, чтобы ограничить длину кадра, который может быть получен или отправлен через этот порт.
- Эта команда применима к физическому порту Ethernet или SVI.

Команда	**mtu** *num*
Описание параметров	*num*: 64–9216
По умолчанию	По умолчанию MTU интерфейса составляет 1500 байт
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для настройки MTU интерфейса, то есть максимальной длины кадра данных на канальном уровне. В настоящее время вы можете настроить MTU только для физического порта или порта AP, который содержит один или несколько портов-участников

Настройка глобального MTU

- Опционально.
- Пользователи могут установить глобальный MTU и IP MTU, чтобы контролировать максимальную длину кадров, которые могут быть отправлены и получены через все порты.
- Поддержка физического порта Ethernet.

Команда	**mtu forwarding** *num*
Описание параметров	*num*: 64–9216
По умолчанию	По умолчанию MTU интерфейса составляет 1500 байт
Командный режим	Режим глобальной конфигурации
Руководство по использованию	IP MTU автоматически изменяется на значение MTU канала интерфейса при изменении глобально установленного MTU канала

Настройка пропускной способности интерфейса

- Опционально.
- Как правило, пропускная способность интерфейса равна скорости интерфейса.

Команда	**bandwidth** *kilobits*
Описание параметров	*kilobits*: значение находится в диапазоне от 1 до 2 147 483 647. Единицей является килобит
По умолчанию	Как правило, пропускная способность интерфейса соответствует типу интерфейса. Например, пропускная способность по умолчанию для физического порта Gigabit Ethernet составляет 1 000 000, а для физического порта 10G Ethernet — 10 000 000
Командный режим	Режим конфигурации интерфейса

Настройка задержки пересылки (Carrier Delay) для интерфейса

- Опционально.
- Если сконфигурированная задержка пересылки велика, изменение состояния протокола при изменении физического состояния интерфейса занимает много времени. Если для задержки пересылки установлено значение 0, состояние протокола изменяется сразу же после изменения физического состояния интерфейса.

Команда	**carrier-delay** {[**milliseconds**] *num* | **up** [**milliseconds**] *num* **down** [**milliseconds**] *num*}
Описание параметров	*num*: значение находится в диапазоне от 0 до 60. Единицей является секунда. **milliseconds**: указывает задержку пересылки. Диапазон значений от 0 до 60 000. Единицей измерения является миллисекунда. **up**: указывает задержку, после которой состояние DCD изменяется с Down на Up. **down**: указывает задержку, после которой состояние DCD изменяется с Up на Down
По умолчанию	По умолчанию задержка пересылки для интерфейса составляет 2 секунды
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если в качестве единицы измерения используется миллисекунда, сконфигурированная задержка пересылки должна быть целым числом, кратным 100 миллисекундам

Настройка интервала загрузки интерфейса

- Опционально.
- Настроенный интервал загрузки влияет на вычисление средней скорости передачи пакетов на интерфейсе. Если настроенный интервал загрузки короткий,

средняя скорость передачи пакетов может точно отражать изменения трафика в реальном времени.

Команда	**load-interval** *seconds*
Описание параметров	seconds: значение находится в диапазоне от 5 до 600. Единицей является секунда
По умолчанию	По умолчанию интервал загрузки интерфейса составляет 10 секунд
Командный режим	Режим конфигурации интерфейса

Настройка защищенного порта

- Опционально.
- Пакеты L2 не могут пересылаться между защищенными портами.
- Эта команда применима к физическому порту Ethernet или порту AP.

Команда	**switchport protected**
По умолчанию	По умолчанию защищенный порт не настроен
Командный режим	Режим конфигурации интерфейса

Блокировка маршрутизации L3 между защищенными портами

- Опционально.
- После настройки этой команды маршрутизация L3 между защищенными портами блокируется.

Команда	**protected-ports route-deny**
По умолчанию	По умолчанию функция блокировки маршрутизации L3 между защищенными портами отключена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию маршрутизация L3 между защищенными портами не блокируется. В этом случае вы можете запустить эту команду, чтобы заблокировать маршрутизацию между защищенными портами

Настройка восстановления портов errdisable

- Опционально.
- По умолчанию порт будет отключен и не будет восстановлен после нарушения. После настройки восстановления порта errdisable порт в состоянии errdisable будет восстановлен и включен.

Команда	**errdisable recovery** [**interval** *time* | **cause** *link-state*]
Описание параметров	*time*: указывает время автоматического восстановления. Значение колеблется от 30 до 86 400. Единица секунды. *link-state*: восстанавливает порт, который был установлен в состояние errdisable функцией отслеживания состояния REUP
По умолчанию	По умолчанию восстановление порта errdisable отключено
Командный режим	Режим глобальной конфигурации
Руководство по использованию	По умолчанию порт в состоянии errdisable не восстанавливается. Вы можете восстановить порт вручную или запустить эту команду для автоматического восстановления порта

Настройка MAC-адресов для интерфейсов

- Опционально.
- Если эта функция требуется, запустите команду **mac-address** в режиме настройки интерфейса.
- По умолчанию MAC-адреса интерфейсов имеют фиксированные значения.

Команда	**mac-address** *mac-address*
Описание параметров	*mac-address*: указывает действительный MAC-адрес
Командный режим	Режим конфигурации интерфейса

Настройка флага инкапсуляции VLAN для интерфейсов

- Опционально.
- Если эта функция требуется, запустите команду **encapsulation dot1Q** в режиме конфигурации интерфейса.
- По умолчанию протокол инкапсуляции VLAN отключен для интерфейсов.

Команда	**encapsulation dot1Q** *VlanID*
Описание параметров	*VlanID*: указывает идентификатор VLAN. Диапазон значений от 1 до 4094
Командный режим	Режим конфигурации интерфейса

Настройка режима FEC интерфейса

- Опционально.

- По умолчанию режим FEC отключен для порта 25 Гбит/с, а включение или отключение режима FEC для порта 100 Гбит/с определяется вставленным оптическим модулем.

Команда	**fec mode** {**rs** | **base-r** | **none** | **auto**}
Описание параметров	**rs**: включить режим FEC с помощью rs. Поддерживается портом 100 Гбит/с. **base-r**: включить режим FEC с помощью base-r. Поддерживается портом 25 Гбит/с. **none**: включить функцию FEC. **auto**: включен или выключен режим FEC, определяется вставленным оптическим модулем. Поддерживается портом 100 Гбит/с
Командный режим	Режим конфигурации интерфейса

Настройка цикла выборки статистики на порту Ethernet

- Опционально.
- Цикл выборки статистики портов Ethernet по умолчанию составляет 5 секунд.

Команда	**ethernet-port counter sample-period** [**seconds**]
Описание параметров	**seconds**: единица измерения цикла выборки
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Более короткий цикл выборки указывает на более высокое потребление производительности системы. Поэтому цикл выборки должен быть скорректирован по мере необходимости

1.5.2.3. Проверка

- Запустите команду **show interfaces**, чтобы отобразить конфигурации атрибутов интерфейсов.

Команда	**show interfaces** [*interface-type interface-number*] [**description** | **switchport** | **trunk**]
Описание параметров	*interface-type interface-number*: указывает тип и номер интерфейса. **description**: указывает описание интерфейса, включая статус соединения. **switchport**: указывает информацию об интерфейсе L2. Этот параметр действует только для интерфейса L2

Описание параметров	**trunk**: указывает информацию о магистральном порте. Этот параметр действует для физического порта или порта AP
Командный режим	Привилегированный режим EXEC
Руководство по использованию	Используйте эту команду без каких-либо параметров для отображения основной информации об интерфейсе
	SwitchA#show interfaces GigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is DOWN, line protocol is DOWN Hardware is Broadcom 5464 GigabitEthernet, address is 08c6.b3.de9b (bia 08c6.b3.de9b) Interface address is: no ip address Interface IPv6 address is: No IPv6 address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Medium-type is Copper Admin duplex mode is AUTO, oper duplex is Unknown Admin speed is AUTO, oper speed is Unknown Flow receive control admin status is OFF,flow send control admin status is OFF Flow receive control oper status is Unknown,flow send control oper status is Unknown Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Port-type: trunk Native vlan:1 Allowed vlan lists:1-4094 //Allowed VLAN list of the Trunk port

	Active vlan lists:1, 3-4 //Active VLAN list (indicating that only VLAN 1, VLAN 3, and VLAN 4 are created on the device) Rxload is 1/255,Txload is 1/255 5 minutes input rate 0 bits/sec, 0 packets/sec 5 minutes output rate 0 bits/sec, 0 packets/sec 0 packets input, 0 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 0 packets output, 0 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

- Запустите команду **show eee interfaces status**, чтобы отобразить статус EEE интерфейса.

Команда	**show eee interfaces** { *interface-type interface-number* | **status** }
Описание параметров	*interface-type interface-number*: указывает тип и номер интерфейса. **status**: указывает статус EEE всех интерфейсов
Командный режим	Привилегированный режим EXEC
Руководство по использованию	Если интерфейс указан, отображается статус EEE указанного интерфейса; в противном случае отображается состояние EEE всех интерфейсов
	1. Отображение статуса EEE GigabitEthernet 0/1. QTECH#show eee interface gigabitEthernet 0/1 Interface : Gi0/1 EEE Support : Yes Admin Status : Enable Oper Status : Disable Remote Status : Disable Trouble Cause : Remote Disable

Interface	Указывает информацию об интерфейсе
EEE Support	Указывает, поддерживается ли EEE
Admin Status	Указывает административный статус
Oper Status	Указывает на рабочее состояние
Trouble Cause	Указывает причину, по которой состояние EEE интерфейса является ненормальным

2. Отображение статуса EEE всех интерфейсов.

```
QTECH#show eee interface status
Interface  EEE Support  Admin Status  Oper Status  Remote Status
                Trouble Cause
---------  -------      --------      --------     --------  --------
Gi0/1      Yes          Enable        Disable      Disable   Remote
Disable
Gi0/2      Yes          Enable        Disable      Unknown   None
Gi0/3      Yes          Enable        Enable       Enable    None
Gi0/4      Yes          Enable        Enable       Enable    None
Gi0/5      Yes          Enable        Enable       Enable    None
Gi0/6      Yes          Enable        Enable       Enable    None
Gi0/7      Yes          Enable        Enable       Enable    None
Gi0/8      Yes          Enable        Enable       Enable    None
Gi0/9      Yes          Enable        Enable       Enable    None
Gi0/10     Yes          Enable        Enable       Enable    None
```

Interface	Указывает информацию об интерфейсе
EEE Support	Указывает, поддерживается ли EEE
Admin Status	Указывает административный статус
Oper Status	Указывает на рабочее состояние
Trouble Cause	Указывает причину, по которой состояние EEE интерфейса является ненормальным

1.5.2.4. Пример конфигурации

Настройка атрибутов интерфейса

Сценарий:

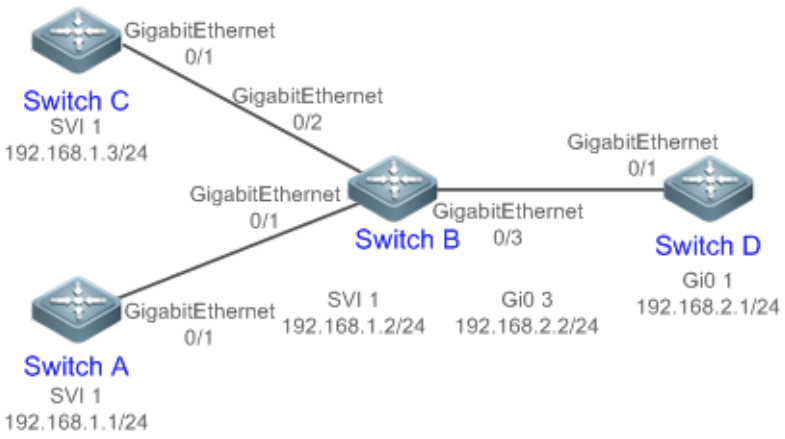


Рисунок 1-6.

Шаги настройки	• На коммутаторе A настройте GigabitEthernet 0/1 в качестве режима доступа, а идентификатор VLAN по умолчанию — 1. Настройте SVI 1, назначьте IP-адрес SVI 1 и настройте маршрут к коммутатору D. • На коммутаторе B настройте GigabitEthernet 0/1 и GigabitEthernet 0/2 в качестве транковых портов, а идентификатор VLAN по умолчанию — 1. Настройте SVI 1 и назначьте IP-адрес SVI 1. Настройте GigabitEthernet 0/3 в качестве маршрутизируемого порта и назначить этому порту IP-адрес из другого сегмента сети. • На коммутаторе C настройте GigabitEthernet 0/1 в качестве порта доступа, а идентификатор VLAN по умолчанию — 1. Настройте SVI 1 и назначьте IP-адрес для SVI 1. • На коммутаторе D настройте GigabitEthernet 0/1 в качестве маршрутизируемого порта, назначьте этому порту IP-адрес и настройте маршрут к коммутатору A
A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode access A(config-if-GigabitEthernet 0/1)# switchport access vlan 1 A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0 A(config-if-VLAN 1)# exit A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# switchport mode trunk B(config-if-GigabitEthernet 0/1)# exit B(config)# interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)# switchport mode trunk B(config-if-GigabitEthernet 0/2)# exit B(config)# interface vlan 1 B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0 B(config-if-VLAN 1)# exit B(config)# interface GigabitEthernet 0/3 B(config-if-GigabitEthernet 0/3)# no switchport B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0 B(config-if-GigabitEthernet 0/3)# exit

C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Проверка	Выполните проверку на коммутаторе A, коммутаторе B, коммутаторе C и коммутаторе D следующим образом: • На коммутаторе A пропингуйте IP-адреса интерфейсов трех других коммутаторов. Убедитесь, что у вас есть доступ к трем другим коммутаторам на коммутаторе A. • Убедитесь, что коммутатор B и коммутатор D могут быть пропингованы взаимно. • Убедитесь, что статус интерфейса правильный
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de90 (bia 08c6.b3.de90) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48

	Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Port-type: access Vlan id: 1 Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de91 (bia 08c6.b3.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full

	Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: Port-type: trunk Native vlan: 1 Allowed vlan lists: 1-4094 Active vlan lists: 1 Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de92 (bia 08c6.b3.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON

	Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 08c6.b3.de93 (bia 08c6.b3.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped

	0 output errors, 0 collisions, 0 interface resets

1.6. Мониторинг

1.6.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает счетчики указанного интерфейса	**clear counters** [*interface-type interface-number*]
Сбрасывает оборудование интерфейса	**clear interface** *interface-type interface-number*
Очищает статистику изменения статуса канала	**clear link-state-change statistics** [*interface-type interface-number*]

1.6.2. Отображение

Отображение конфигураций интерфейса и статуса

Описание	Команда
Отображает всю информацию о состоянии и конфигурации указанного интерфейса	**show interfaces** [*interface-type interface-number*]
Отображает состояние интерфейса	**show interfaces** [*interface-type interface-number*] **status**
Отображает статус errdisable интерфейса	**show interfaces** [*interface-type interface-number*] **status err-disable**
Отображает время изменения состояния соединения и количество указанных портов	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Отображает административное и рабочее состояние портов коммутации (немаршрутизируемых портов)	**show interfaces** [*interface-type interface-number*] **switchport**
Отображает описание и состояние указанного интерфейса	**show interfaces** [*interface-type interface-number*] **description**

Описание	Команда
Отображает счетчики указанного порта, среди которых отображаемая скорость может иметь погрешность ± 0,5 %	**show interfaces** [*interface-type interface-number*] **counters**
Отображает количество пакетов, увеличенных за интервал загрузки	**show interfaces** [*interface-type interface-number*] **counters increment**
Отображает статистику о пакетах ошибок	**show interfaces** [*interface-type interface-number*] **counters error**
Отображает скорость отправки/ получения пакетов интерфейса	**show interfaces** [*interface-type interface-number*] **counters rate**
Отображает скорость отправки/ получения пакетов интерфейса на физическом уровне. Скорость отправки/приема пакетов на физическом уровне относится к скорости отправки/приема пакетов, содержащих межкадровый интервал	**show interfaces** [*interface-type interface-number*] **counters rate physical-layer**
Отображает сводку информации об интерфейсе	**show interfaces** [*interface-type interface-number*] **counters summary**
Отображает использование пропускной способности интерфейса	**show interfaces** [*interface-type interface-number*] **usage**
Отображает глобальную информацию о MTU	**show interface** [*interface-type interface-number*] **mtu forwarding**
Отображает информацию об интерфейсе SubVLAN	**show vlans**

Отображение информации об оптическом модуле

Описание	Команда
Отображает основную информацию об оптическом модуле указанного интерфейса	**show interfaces** [*interface-type interface-number*] **transceiver**
Отображает аварийные сигналы о неисправности оптического модуля на указанном интерфейсе. Если ошибок нет, отображается «None»	**show interfaces** [*interface-type interface-number*] **transceiver alarm**

Описание	Команда
Отображает диагностические значения оптического модуля указанного интерфейса	**show interfaces** [*interface-type interface-number*] **transceiver diagnosis**

2. НАСТРОЙКА SINGLE FIBER

2.1. Обзор

Single Fiber (SF) — это функция, разработанная для удовлетворения особых требований только к приему пакетов, но не к отправке пакетов. В обычных случаях, когда стандартные устройства Ethernet взаимодействуют друг с другом с помощью оптических приемопередатчиков, необходимо использовать двухволоконные оптические приемопередатчики, чтобы соединение стало активным и пакеты пересылались нормально. Недостатком, однако, является то, что физическая изоляция не может быть гладко достигнута в направлении передачи, когда стандартные устройства Ethernet отправляют данные через двужильное волокно. В результате peer-коммутатор может получать непредсказуемые пакеты, влияющие на безопасность коммутатора. Для этого режим SF может быть настроен на физическую изоляцию данных в направлении передачи для обеспечения безопасности данных. Применение портов режима SF не соответствует спецификациям каналов связи портов устройств Ethernet. Следовательно, для реализации приема SF необходимо подключить одножильное оптоволокно к Rx-концу порта коммутатора, чтобы данные с Tx-конца peer оптического приемопередатчика могли приниматься нормально.

2.2. Приложения

Приложение	Описание
SF-прием	Конец Rx порта коммутатора соединяется с концом Tx оптического сплиттера через одножильное волокно

2.2.1. SF-прием

2.2.1.1. Сценарий

Конец Rx порта коммутатора подключен к концу Tx оптического сплиттера через одножильное волокно, а конец Rx оптического сплиттера не подключен к концу Tx подключенного коммутатора для обеспечения физической изоляции.

Рисунок 2-1.

2.2.1.2. Развертывание

Коммутатор может только получать пакеты от оптического сплиттера, но не может отправлять пакеты на оптический сплиттер.

2.3. Конфигурация

Конфигурация	Описание и команда	
Настройка режима SF	(Обязательно) Используется для настройки режима SF	
	transport mode { rx }	Настраивает режим SF Rx
	no transport mode	Восстанавливает режим по умолчанию, т. е. двунаправленный режим Rx/Tx с двумя волокнами

2.3.1. Настройка режима SF

2.3.1.1. Эффект конфигурации

Настройте порт коммутации для поддержки только режима SF и направления Rx.

2.3.1.2. Шаги настройки

Настройка режима SF

- Обязательный.
- Режим SF следует настроить на порту, для которого требуется функция SF Rx, если не указано иное.

Команда	**transport mode {rx}**
Описание параметров	**rx**: указывает режим, в котором принимаются только пакеты
По умолчанию	По умолчанию режим SF отключен
Командный режим	Режим конфигурации интерфейса

2.3.1.3. Проверка

Проверьте конфигурацию SF:

- Проверьте, нормально ли работает порт, на котором настроена функция SF Rx.
- Проверьте, отключена ли функция излучения света для порта, на котором настроена функция SF Rx.
- Убедитесь, что порт, на котором настроена функция SF Rx, может только получать пакеты, но не может отправлять пакеты.

2.4. Мониторинг

2.4.1. Отображение

Описание	Команда
Отображает информацию о порте, на котором настроена функция SF Rx	**show transport mode {rx}**

3. НАСТРОЙКА MAC-АДРЕСА

3.1. Обзор

Таблица MAC-адресов содержит MAC-адреса, номера интерфейсов и идентификаторы VLAN устройств, подключенных к локальному устройству.

Когда устройство пересылает пакет, оно находит выходной порт в своей таблице MAC-адресов в соответствии с MAC-адресом получателя и идентификатором VLAN пакета.

После этого пакет становится unicast, multicast или broadcast.

ПРИМЕЧАНИЕ: этот документ охватывает динамические MAC-адреса, статические MAC-адреса и отфильтрованные MAC-адреса. Сведения об управлении многоадресными (multicast) MAC-адресами см. в разделе Multicast Configuration.

3.1.1. Протоколы и стандарты

- IEEE 802.3: множественный доступ carrier sense с обнаружением столкновений (CSMA/CD), метод доступа и спецификации физического уровня.
- IEEE 802.1Q: локальные сети с виртуальным мостом.

3.2. Приложения

Приложение	Описание
Изучение MAC-адреса	Пересылка unicast-пакетов с помощью изучения MAC-адресов
Уведомление об изменении MAC-адреса	Отслеживайте изменение устройств, подключенных к сетевому устройству, с помощью уведомления об изменении MAC-адреса

3.2.1. Изучение MAC-адреса

3.2.1.1. Сценарий

Обычно устройство поддерживает таблицу MAC-адресов путем динамического изучения MAC-адресов. Принцип работы описывается следующим образом:

Как показано на следующем Рисунке, таблица MAC-адресов коммутатора пуста. Когда пользователь A связывается с пользователем B, он отправляет пакет на порт GigabitEthernet 0/2 коммутатора, а коммутатор узнает MAC-адрес пользователя A и сохраняет его в таблице. Поскольку таблица не содержит MAC-адреса пользователя B коммутатор транслирует пакет на порты всех подключенных устройств, кроме пользователя A, включая пользователя B и пользователя C.

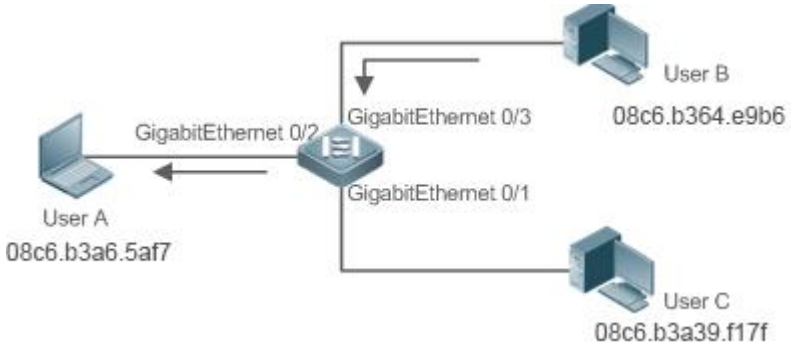


Рисунок 3-1. Шаг 1. Изучение MAC-адреса

Таблица 1. Таблица MAC-адресов 1

Статус	VLAN	MAC-адрес	Интерфейс
Динамический	1	08c6.b3.5af7	GigabitEthernet 0/2

Когда пользователь B получает пакет, он отправляет ответный пакет пользователю A через порт GigabitEthernet 0/3 на коммутаторе. Поскольку MAC-адрес пользователя A уже находится в таблице MAC-адресов, коммутатор отправляет ответный unicast-пакет на порт GigabitEthernet 0/2 и узнает MAC-адрес пользователя B. пользователь C не получает ответный пакет от пользователя B для пользователя A.

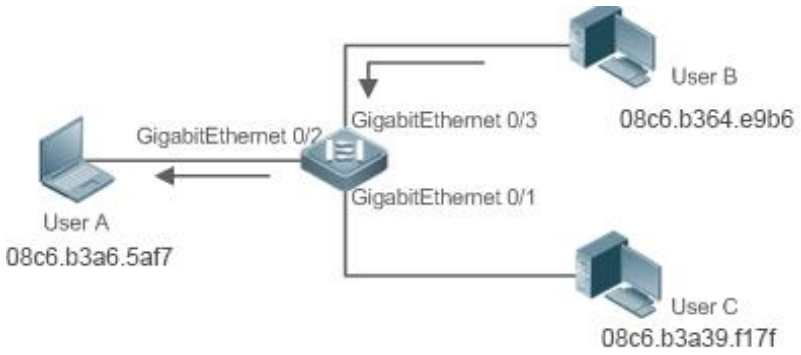


Рисунок 3-2. Шаг 2. Изучение MAC-адреса

Таблица 2. Таблица MAC-адресов 2

Статус	VLAN	MAC-адрес	Интерфейс
Динамический	1	08c6.b3.5af7	GigabitEthernet 0/2
Динамический	1	08c6.b3.e9b6	GigabitEthernet 0/3

Благодаря взаимодействию между пользователем A и пользователем B коммутатор узнает MAC-адреса пользователя A и пользователя B. После этого пакеты между пользователем A и пользователем B будут передаваться по unicast-рассылке без получения пользователем C.

3.2.1.2. Развертывание

Благодаря изучению MAC-адресов коммутатор уровня 2 пересылает пакеты через unicast-рассылку, уменьшая количество broadcast-пакетов и нагрузку на сеть.

3.2.2. Уведомление об изменении MAC-адреса

Уведомление об изменении MAC-адреса предоставляет механизм для системы управления сетью (NMS) для отслеживания смены устройств, подключенных к сетевому устройству.

3.2.2.1. Сценарий

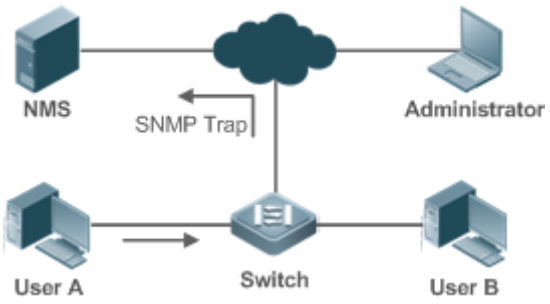


Рисунок 3-3. Уведомление об изменении MAC-адреса

После того, как на устройстве включено уведомление об изменении MAC-адреса, устройство генерирует сообщение уведомления, когда устройство узнает новый MAC-адрес или завершает устаревание изученного MAC-адреса, и отправляет сообщение в сообщении SNMP Trap в указанную NMS.

Уведомление о добавлении MAC-адреса указывает на то, что новый пользователь получает доступ к сети, а уведомление об удалении MAC-адреса указывает на то, что пользователь не отправляет пакеты в течение времени устаревания и обычно пользователь выходит из сети.

Когда сетевое устройство подключено к нескольким устройствам, за короткое время может произойти множество изменений MAC-адресов, что приведет к увеличению трафика. Для уменьшения трафика вы можете настроить интервал отправки уведомлений об изменении MAC-адреса. По истечении интервала все уведомления, созданные в течение этого интервала, инкапсулируются в сообщение.

Когда уведомление генерируется, оно сохраняется в таблице истории уведомлений об изменении MAC-адреса. Администратор может узнать последние изменения MAC-адреса, проверив таблицу истории уведомлений даже без NMS.

ПРИМЕЧАНИЕ: уведомление об изменении MAC-адреса генерируется только для динамического MAC-адреса.

3.2.2.2. Развертывание

Включите уведомление об изменении MAC-адреса на коммутаторе уровня 2, чтобы отслеживать изменение устройств, подключенных к сетевому устройству.

3.3. Функции

3.3.1. Базовые определения

Динамический MAC-адрес

Динамический MAC-адрес — это запись MAC-адреса, созданная в процессе изучения MAC-адреса устройством.

Устаревание адреса

Устройство запоминает только ограниченное количество MAC-адресов, а неактивные записи удаляются по мере устаревания адреса.

Устройство начинает процесс устаревания MAC-адреса, когда изучит его. Если устройство не получит пакет, содержащий MAC-адрес источника, оно удалит MAC-адрес из таблицы MAC-адресов по истечении времени.

Переадресация через unicast-рассылку

Если устройство находит в своей таблице MAC-адресов запись, содержащую MAC-адрес и VLAN ID пакета, а выходной порт уникален, оно отправит пакет напрямую через порт.

Пересылка через broadcast-рассылку

Если устройство получает пакет, содержащий адрес назначения ffff.ffff.ffff или неопознанный адрес назначения, оно отправит пакет через все порты в VLAN, откуда пришел пакет, кроме входного порта.

3.3.1.1. Обзор

Особенность	Описание
Лимит динамических адресов для VLAN	Ограничевает количество динамических MAC-адресов в VLAN
Лимит динамических адресов для интерфейса	Ограничевает количество динамических MAC-адресов на интерфейсе

3.3.2. Лимит динамических адресов для VLAN

3.3.2.1. Принцип работы

Таблица MAC-адресов с ограниченной емкостью используется всеми VLAN. Настройте максимальное количество динамических MAC-адресов для каждой VLAN, чтобы одна VLAN не исчерпала пространство таблицы MAC-адресов.

VLAN может изучить только ограниченное количество динамических MAC-адресов после настройки ограничения. Пакеты, превышающие лимит, передаются в broadcast-режиме.

ПРИМЕЧАНИЕ: если количество изученных MAC-адресов превышает лимит, устройство прекратит изучение MAC-адресов из VLAN и не начнет изучение снова, пока число не упадет ниже лимита после устаревания адреса.

ПРИМЕЧАНИЕ: на MAC-адреса, скопированные в конкретную VLAN, лимит не распространяется.

3.3.3. Лимит динамических адресов для интерфейса

3.3.3.1. Принцип работы

Интерфейс может изучить только ограниченное количество динамических MAC-адресов после того, как лимит настроено. Пакеты, превышающие лимит, передаются в broadcast-режиме.

ПРИМЕЧАНИЕ: если количество изученных MAC-адресов превышает лимит, устройство прекратит изучение MAC-адресов с интерфейса и не начнет изучение снова, пока число не упадет ниже лимита после устаревания адреса.

3.4. Ограничения

Продукты серии QSW-6900 не изучают и не пересылают пакеты, у которых MAC-адреса источника и MAC-адреса назначения равны 0.

3.5. Конфигурация

Конфигурация	Описание и команда	
Настройка динамического MAC-адреса	(Необязательный) Он используется для включения изучения MAC-адреса	
	mac-address-learning	Настраивает изучение MAC-адресов глобально или на интерфейсе
	mac-address-table aging-time	Настраивает время устаревания для динамического MAC-адреса
Настройка статического MAC-адреса	(Опционально) Он используется для привязки MAC-адреса устройства к порту коммутации	
	mac-address-table static	Настраивает статический MAC-адрес
Настройка MAC-адреса для фильтрации пакетов	(Опционально) Он используется для фильтрации пакетов	
	mac-address-table filtering	Настраивает MAC-адрес для фильтрации пакетов
Настройка уведомления об изменении MAC-адреса	(Опционально) Он используется для отслеживания смены устройств, подключенных к сетевому устройству	
	mac-address-table notification	Глобально настраивает уведомление об изменении MAC-адреса

Конфигурация	Описание и команда	
Настройка уведомления об изменении MAC-адреса	**snmp trap mac-notification**	Настраивает уведомление об изменении MAC-адреса на интерфейсе
Настройка VLAN управления для порта AP	(Опционально) Он используется для настройки VLAN управления для порта AP	
	aggregateport-admin vlan	Настраивает VLAN управления для порта AP
Настройка функции регистрации аварийных сигналов для смещения MAC-адреса	(Опционально) Используется для настройки функции регистрации аварийных сигналов при обнаружении смещения MAC-адреса	
	mac-address-table flapping-logging	
Настройка максимального количества изученных MAC-адресов	(Опционально) Используется для настройки максимального количества изученных MAC-адресов	
	max-dynamic-mac-count *count*	
Настройка отбрасывания пакетов, когда количество изученных MAC-адресов превышает лимит адресов	(Опционально) Используется для настройки метода обработки пакетов, когда количество изученных MAC-адресов превышает лимит адресов	
	max-dynamic-mac-count exceed-action *forward* | *discard*	

3.5.1. Настройка динамического MAC-адреса

3.5.1.1. Эффект конфигурации

Изучайте MAC-адреса динамически и пересылайте пакеты через unicast-рассылку.

3.5.1.2. Шаги настройки

Настройка изучения глобального MAC-адреса

- Опционально.
- Вы можете выполнить эту настройку, чтобы отключить глобальное изучение MAC-адресов.
- Конфигурация:

Команда	**mac-address-learning** { **enable** | **disable** }
Описание параметров	**enable**: включает изучение глобального MAC-адреса. **disable**: отключает изучение глобального MAC-адреса
По умолчанию	Изучение глобального MAC-адреса включено по умолчанию
Командный режим	Режим глобальной конфигурации

ПРИМЕЧАНИЕ: по умолчанию изучение глобального MAC-адреса включено. Когда глобальное изучение MAC-адресов включено, конфигурация изучения MAC-адресов на интерфейсе вступает в силу; когда функция отключена, MAC-адреса не могут быть изучены глобально.

Настройка изучения MAC-адреса на интерфейсе

- Опционально.
- Вы можете выполнить эту настройку, чтобы отключить изучение MAC-адреса на интерфейсе.
- Конфигурация:

Команда	**mac-address-learning**
По умолчанию	Изучение MAC-адресов включено по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Выполните эту настройку на интерфейсе уровня 2, например, на порту коммутации или порту AP

ПРИМЕЧАНИЕ: по умолчанию изучение MAC-адресов включено. Если DOT1X, IP SOURCE GUARD, или функция безопасности порта настроена для порта, изучение MAC-адреса не может быть включено. Управление доступом не может быть включено на порту с отключенным изучением MAC-адреса.

Настройка времени устаревания для динамического MAC-адреса

- Опционально.
- Настройте время устаревания для динамических MAC-адресов.
- Конфигурация:

Команда	**mac-address-table aging-time** *value*
Описание параметров	*value*: указывает время устаревания. Значение равно либо 0, либо находится в диапазоне от 10 до 1 000 000
По умолчанию	По умолчанию 300 секунд

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если установлено значение 0, устаревание MAC-адресов отключено, и изученные MAC-адреса не будут устаревать

ПРИМЕЧАНИЕ: фактическое время устаревания может отличаться от настроенного значения, но не более чем в два раза от настроенного значения.

3.5.1.3. Проверка

- Проверьте, запоминает ли устройство динамические MAC-адреса.
- Запустите команду **show mac-address-table dynamic** для отображения динамических MAC-адресов.
- Запустите команду **show mac-address-table aging-time**, чтобы отобразить время устаревания для динамических MAC-адресов.

Команда	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Описание параметров	**address** *mac-address*: отображает информацию о конкретном динамическом MAC-адресе. **interface** *interface-id*: указывает физический интерфейс или порт AP. **vlan** *vlan-id*: отображает динамические MAC-адреса в определенной VLAN
Командный режим	Привилегированный режим EXEC/Режим глобальной конфигурации/ Режим настройки интерфейса

```
QTECH# show mac-address-table dynamic
Vlan   MAC Address       Type            Interface
---- ------------ ------- -----------------
1      0000.0000.0001    DYNAMIC     GigabitEthernet 1/1
1      0001.960c.a740    DYNAMIC     GigabitEthernet 1/1
1      0007.95c7.dff9    DYNAMIC     GigabitEthernet 1/1
1      0007.95cf.eee0    DYNAMIC     GigabitEthernet 1/1
1      0007.95cf.f41f    DYNAMIC     GigabitEthernet 1/1
1      0009.b715.d400    DYNAMIC     GigabitEthernet 1/1
1      0050.bade.63c4    DYNAMIC     GigabitEthernet 1/1
```

Поле	Описание
Vlan	Указывает VLAN, в которой находится MAC-адрес
MAC-адрес	Указывает MAC-адрес

	Тип	Указывает тип MAC-адреса
	Интерфейс	Указывает интерфейс, на котором находится MAC-адрес

Команда	**show mac-address-table aging-time**
Командный режим	Привилегированный режим EXEC/Режим глобальной конфигурации/ Режим настройки интерфейса
	QTECH# show mac-address-table aging-time Aging time : 300

3.5.1.4. Пример конфигурации

Настройка динамического MAC-адреса

Сценарий:

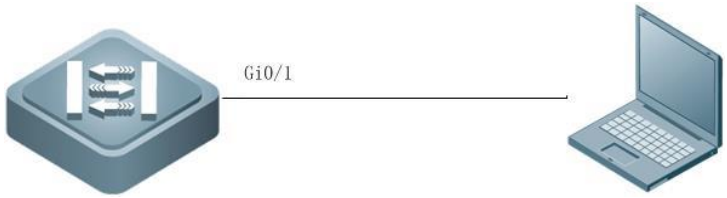


Рисунок 3-4.

Шаги настройки	• Включите изучение MAC-адреса на интерфейсе. • Настройте время устаревания для динамических MAC-адресов на 180 секунд. • Удалите все динамические MAC-адреса в VLAN 1 на порту GigabitEthernet 0/1
	QTECH# configure terminal QTECH(config-if-GigabitEthernet 0/1)# mac-address-learning QTECH(config-if-GigabitEthernet 0/1)# exit QTECH(config)# mac aging-time 180 QTECH# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Проверка	• Проверьте изучение MAC-адреса на интерфейсе. • Показать временя устаревания для динамических MAC-адресов. • Показать все динамические MAC-адреса в VLAN 1 на порту GigabitEthernet 0/1

```
QTECH# show mac-address-learning
GigabitEthernet 0/1      learning ability: enable
QTECH# show mac aging-time
Aging time : 180 seconds
QTECH# show mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1
Vlan       MAC Address          Type         Interface
---------- -------------------- -------- --------------------
1          08c6.b3.1001         STATIC       GigabitEthernet 1/1
```

3.5.1.5. Распространенные ошибки

Настройте изучение MAC-адресов на интерфейсе, прежде чем настраивать интерфейс как интерфейс уровня 2, например, как порт коммутации или порт AP.

3.5.2. Настройка статического MAC-адреса

3.5.2.1. Эффект конфигурации

Свяжите MAC-адрес сетевого устройства с портом коммутации.

3.5.2.2. Шаги настройки

Настройка статического MAC-адреса

- Опционально.
- Свяжите MAC-адрес сетевого устройства с портом коммутации.
- Конфигурация:

Команда	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*
Описание параметров	**address** *mac-address*: указывает MAC-адрес. **vlan** *vlan-id*: указывает VLAN, в которой находится MAC-адрес. **interface** *interface-id*: указывает физический интерфейс или порт AP
По умолчанию	По умолчанию статический MAC-адрес не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Когда коммутатор получает пакет, содержащий указанный MAC-адрес в указанной VLAN, пакет пересылается на связанный интерфейс

3.5.2.3. Проверка

- Запустите команду **show mac-address-table static**, чтобы проверить, вступила ли в силу конфигурация.

Команда	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Описание параметров	**address** *mac-address*: указывает MAC-адрес. **interface** *interface-id*: указывает физический интерфейс или порт AP. **vlan** *vlan-id*: указывает VLAN, в которой находится MAC-адрес
Командный режим	Привилегированный режим EXEC/Режим глобальной конфигурации/ Режим настройки интерфейса
	QTECH# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ----------------- 1 08c6.b3.1001 STATIC GigabitEthernet 1/1 1 08c6.b3.1002 STATIC GigabitEthernet 1/1 1 08c6.b3.1003 STATIC GigabitEthernet 1/1

3.5.2.4. Пример конфигурации

Настройка статического MAC-адреса

В приведенном выше примере взаимосвязь MAC-адресов, VLAN и интерфейсов показана в следующей таблице.

Роль	MAC-адрес	Идентификатор VLAN	Идентификатор интерфейса
Веб-сервер	08c6.b332.0001	VLAN2	Gi0/10
Сервер базы данных	08c6.b332.0002	VLAN2	Gi0/11
Администратор	08c6.б332.1000	VLAN2	Gi0/12

Сценарий:

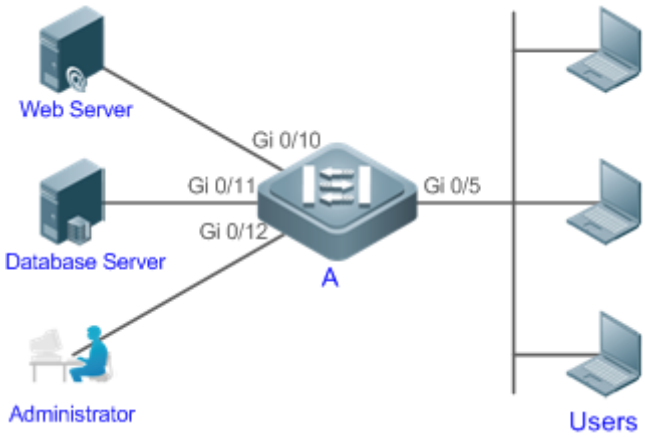


Рисунок 3-5.

Шаги настройки	• Укажите MAC-адреса назначения (*mac-address*). • Укажите VLAN (*vlan-id*), где находятся MAC-адреса. • Укажите идентификаторы интерфейсов (*interface-id*)
A	A# configure terminal A(config)# mac-address-table static 08c6.b3.3232.0001 vlan 2 interface gigabitEthernet 0/10 A(config)# mac-address-table static 08c6.b3.3232.0002 vlan 2 interface gigabitEthernet 0/11 A(config)# mac-address-table static 08c6.b3.3232.1000 vlan 2 interface gigabitEthernet 0/12
Проверка	Отображение конфигурации статического MAC-адреса на коммутаторе
A	A# show mac-address-table static Vlan MAC Address Type Interface ---------- ---------- ---------- 2 08c6.b3.3232.0001 STATIC GigabitEthernet 0/10 2 08c6.b3.3232.0002 STATIC GigabitEthernet 0/11 2 08c6.b3.3232.1000 STATIC GigabitEthernet 0/12

3.5.2.5. Распространенные ошибки

Настройте статический MAC-адрес перед настройкой определенного порта в качестве интерфейса уровня 2, например, порта коммутатора или порта AP.

3.5.3. Настройка MAC-адреса для фильтрации пакетов

3.5.3.1. Эффект конфигурации

Если устройство получает пакеты, содержащие MAC-адрес источника или MAC-адрес назначения, указанный в качестве отфильтрованного MAC-адреса, пакеты отбрасываются.

3.5.3.2. Шаги настройки

Настройка MAC-адреса для фильтрации пакетов

- Опционально.
- Выполните эту настройку для фильтрации пакетов.
- Конфигурация:

Команда	**mac-address-table filtering** *mac-address* **vlan** *vlan-id*
Описание параметров	**address** *mac-address*: указывает MAC-адрес. **vlan** *vlan-id*: указывает VLAN, где находится MAC-адрес
По умолчанию	По умолчанию фильтруемый MAC-адрес не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если устройство получает пакеты, содержащие MAC-адрес источника или MAC-адрес назначения, указанный в качестве отфильтрованного MAC-адреса, пакеты отбрасываются

3.5.3.3. Проверка

- Запустите команду **show mac-address-table filter**, чтобы отобразить отфильтрованный MAC-адрес.

Команда	**show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]
Описание параметров	**address** *mac-address*: указывает MAC-адрес. **vlan** *vlan-id*: указывает VLAN, в которой находится MAC-адрес
Командный режим	Привилегированный режим EXEC/Режим глобальной конфигурации/ Режим настройки интерфейса
	QTECH# show mac-address-table filtering Vlan MAC Address Type Interface ------ ------------------ -------- ----------- 1 0000.2222.2222 FILTER

3.5.3.4. Пример конфигурации

Настройка MAC-адреса для фильтрации пакетов

Шаги настройки	• Укажите MAC-адрес назначения (*mac-address*) для фильтрации. • Укажите VLAN, в которой находятся MAC-адреса
	QTECH# configure terminal QTECH(config)# mac-address-table static 08c6.b3.3232.0001 vlan 1
Проверка	Отобразите отфильтрованную конфигурацию MAC-адреса
	QTECH# show mac-address-table filter Vlan MAC Address Type Interface ---------- -------------------- -------- ------------------- 1 08c6.b3.3232.0001 FILTER

3.5.4. Настройка уведомления об изменении MAC-адреса

3.5.4.1. Эффект конфигурации

Отслеживайте смену устройств, подключенных к сетевому устройству.

3.5.4.2. Шаги настройки

Настройка NMS

- Опционально.
- Выполните эту настройку, чтобы позволить NMS получать уведомления об изменении MAC-адреса.
- Конфигурация:

Команда	**snmp-server host** *host-addr* **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*
Описание параметров	**host** *host-addr*: указывает IP-адрес получателя. **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: указывает версию сообщений SNMP TRAP. Вы также можете указать аутентификацию и уровень безопасности для пакетов Версии 3. *community-string*: указывает имя аутентификации
По умолчанию	По умолчанию функция отключена
Командный режим	Режим глобальной конфигурации

Включение SNMP Trap

- Опционально.

- Выполните эту настройку для отправки сообщений SNMP Trap.
- Конфигурация:

Команда	**snmp-server enable traps**
По умолчанию	По умолчанию функция отключена
Командный режим	Режим глобальной конфигурации

Настройка уведомления об изменении глобального MAC-адреса

- Опционально.
- Если уведомление об изменении MAC-адреса отключено глобально, оно будет отключено на всех интерфейсах.
- Конфигурация:

Команда	**mac-address-table notification**
По умолчанию	По умолчанию уведомление об изменении MAC-адреса отключены глобально
Командный режим	Режим глобальной конфигурации

Настройка уведомления об изменении MAC-адреса на интерфейсе

- Опционально.
- Выполните эту настройку, чтобы включить уведомление об изменении MAC-адреса на интерфейсе.
- Конфигурация:

Команда	**snmp trap mac-notification { added | removed }**
Описание параметров	**added**: генерирует уведомление при добавлении MAC-адреса. **removed**: генерирует уведомление при удалении MAC-адреса
По умолчанию	По умолчанию уведомление об изменении MAC-адреса на интерфейсе отключено
Командный режим	Режим конфигурации интерфейса

Настройка интервала генерации уведомлений об изменении MAC-адреса и объема истории уведомлений

- Опционально.
- Выполните эту настройку, чтобы изменить интервал генерации уведомлений об изменении MAC-адреса и объем истории уведомлений.
- Конфигурация:

Команда	**mac-address-table notification** { **interval** *value* | **history-size** *value* }
Описание параметров	**interval** *value*: (Необязательно) указывает интервал для создания уведомлений об изменении MAC-адреса. Диапазон значений от 1 до 3600 секунд. **history-size** *value*: указывает максимальное количество записей в таблице истории уведомлений. Диапазон значений от 1 до 200
По умолчанию	Интервал по умолчанию составляет 1 секунду. Максимальное количество уведомлений по умолчанию — 50
Командный режим	Режим глобальной конфигурации

3.5.4.3. Проверка

- Запустите команду **show mac-address-table notification**, чтобы проверить, получает ли NMS уведомления об изменении MAC-адреса.

Команда	**show mac-address-table notification** [**interface** [*interface-id*] | **history**]
Описание параметров	**interface**: отображает конфигурацию уведомления об изменении MAC-адреса на всех интерфейсах. *interface-id*: отображает конфигурацию уведомления об изменении MAC-адреса на указанном интерфейсе. **history**: отображает историю уведомлений об изменении MAC-адреса
Командный режим	Привилегированный режим EXEC/Режим глобальной конфигурации/ Режим настройки интерфейса
Руководство по использованию	Отображение конфигурации уведомления об изменении глобального MAC-адреса. QTECH#show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0

Поле	Описание
Interval(Sec)	Указывает интервал генерации уведомлений об изменении MAC-адреса
Maximum History Size	Указывает максимальное количество записей в таблице истории уведомлений

	Current History Size	Указывает текущее количество записей в таблице истории уведомлений

3.5.4.4. Пример конфигурации

Сценарий:

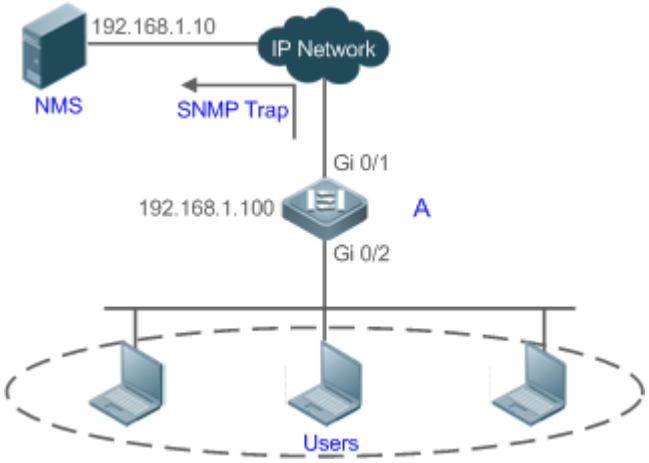


Рисунок 3-6.

На Рисунке показана интрасеть предприятия. Пользователи подключаются к A через порт Gi0/2.

Выполните настройку для достижения следующих эффектов:

Когда порт Gi0/2 узнает новый MAC-адрес или завершает устаревание изученного MAC-адреса, генерируется уведомление об изменении MAC-адреса.

Тем временем A отправляет уведомление об изменении MAC-адреса в сообщении SNMP Trap в указанную NMS.

В сценарии, где A подключен к нескольким пользователям, конфигурация может предотвратить всплеск уведомлений об изменении MAC-адреса за короткое время, чтобы уменьшить сетевой поток.

Шаги настройки	• Включите глобальное уведомление об изменении MAC-адреса на A и настройте уведомление об изменении MAC-адреса на порту Gi0/2. • Настройте IP-адрес узла NMS и включите A с SNMP Trap. A связывается с NMS через маршрутизацию. • Настройте интервал отправки уведомлений об изменении MAC-адреса на 300 секунд (по умолчанию 1 секунда)
A	QTECH# configure terminal QTECH(config)# mac-address-table notification QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added QTECH(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed QTECH(config-if-GigabitEthernet 0/2)# exit

	QTECH(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 QTECH(config)# snmp-server enable traps QTECH(config)# mac-address-table notification interval 300
Проверка	• Проверьте, включено ли глобально уведомление об изменении MAC-адреса. • Проверьте, включено ли уведомление об изменении MAC-адреса на интерфейсе. • Отобразите MAC-адреса интерфейсов и запустите команду **clear mac-address-table dynamic** для имитации устаревших динамических MAC-адресов. • Проверьте, включено ли глобальное уведомление об изменении MAC-адреса. • Отобразите историю уведомлений об изменении MAC-адреса
A	QTECH# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0 QTECH# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap ---------- ---------- ---------- GigabitEthernet 0/2 Enabled Enabled QTECH# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ---------- ---------- -------- ---------- 08c6.b332.0001 DYNAMIC GigabitEthernet 0/2 QTECH# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 QTECH# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683 MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 08c6.b332.0003 GigabitEthernet 0/2

3.5.5. Настройка VLAN управления для порта AP

3.5.5.1. Эффект конфигурации

Включите порт AP для обработки пакетов из VLAN управления как пакеты управления, а из VLAN, не относящейся к управлению, как пакеты данных.

3.5.5.2. Шаги настройки

Настройка VLAN управления для порта AP

- Опционально.
- Выполните эту настройку, чтобы порт AP мог отличать пакеты управления от пакетов данных.
- Конфигурация:

Команда	**aggregateport-admin vlan** *vlan-list*
Описание параметров	*vlan-list*: указывает VLAN или диапазон VLAN, разделенных знаком «-»
По умолчанию	По умолчанию VLAN управления не настроен для порта AP
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Порт AP обрабатывает пакеты, полученные из VLAN управления, как пакеты управления

3.5.5.3. Проверка

Порт AP обрабатывает пакеты из VLAN управления как пакеты управления, а пакеты из VLAN, не относящейся к управлению, — как пакеты данных.

3.5.5.4. Пример конфигурации

Настройка VLAN управления для порта AP

Шаги настройки	Укажите VLAN управления для порта AP
	QTECH# configure terminal QTECH(config)# aggregateport-admin vlan 1-20
Проверка	Запустите команду **show running**, чтобы отобразить конфигурацию

3.5.6. Настройка проверки переключения MAC-адресов

3.5.6.1. Эффект конфигурации

Печатать предупреждение системного журнала, когда происходит flapping MAC-адресов, то есть MAC-адрес попадает на более чем один порт за короткое время в VLAN.

3.5.6.2. Шаги настройки

Настройка проверки Flapping'а MAC-адресов

- Опционально.
- Настройте эту конфигурацию для печати аварийного сигнала системного журнала при изменении MAC-адреса.
- Конфигурация:

Команда	**mac-address-table flapping-logging**
По умолчанию	По умолчанию функция отключена
Командный режим	Режим глобальной конфигурации

3.5.6.3. Проверка

- Запустите команду **show run**, чтобы отобразить конфигурацию.
- Распечатайте системный журнал, чтобы проверить flapping MAC-адресов.

3.5.6.4. Пример конфигурации

- Настройка печати системного журнала при flapping'е MAC-адреса

Шаги настройки	Включить печать системного журнала при flapping'е MAC-адреса
	QTECH# configure terminal QTECH(config)# mac-address-table flapping-logging
Проверка	Запустите команду **show running**, чтобы отобразить конфигурацию

3.5.7. Настройка политики защиты от Flapping'а MAC-адресов

3.5.7.1. Эффект конфигурации

Когда flapping MAC-адресов обнаружен на порту с настроенной политикой защиты от Flapping'а MAC-адресов, порт будет отключен.

3.5.7.2. Примечания

Должна быть включена функция обнаружения Flapping'а MAC-адресов.

3.5.7.3. Шаги настройки

Настройка политики защиты от Flapping'а MAC-адресов

- Опционально.
- Выполните эту операцию, чтобы предотвратить flapping MAC-адресов между разными портами.
- Выполните эту операцию на коммутаторе.

Команда	**mac-address-table flapping action** [**error-down** | **priority** *priotiry-num*]
Описание параметров	**error-down**: указывает политику, согласно которой порт отключается, если на порту обнаруживается flapping MAC-адресов. **priority** *priotiry-num*: указывает приоритет политики закрытия порта. Значение по умолчанию — 0 (самый низкий приоритет). Значение варьируется от 0 до 5. Большее значение указывает на более высокий приоритет
По умолчанию	По умолчанию функция защиты от Flapping'а MAC-адресов отключена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Сначала должна быть включена функция проверки Flapping'а MAC-адресов. В противном случае конфигурация не вступит в силу

3.5.7.4. Проверка

Запустите **show run**, чтобы запросить результат конфигурации.

3.5.7.5. Пример конфигурации

Настройка политики защиты от Flapping'а MAC-адресов

Шаги настройки	Включите функцию обнаружения Flapping'а MAC-адресов
	QTECH# configure terminal QTECH(config)# mac-address-table flapping-logging
	Настройте политику защиты от Flapping'а MAC-адресов. QTECH(config)# interface GigabitEthernet 1/1 QTECH(config-if-GigabitEthernet 1/1)# mac-address-table flapping action error-down QTECH(config-if-GigabitEthernet 1/1)# mac-address-table flapping action priority 2
Проверка	Запустите **show running** на коммутаторе, чтобы запросить конфигурацию

3.5.8. Настройка максимального количества MAC-адресов, изученных портом

3.5.8.1. Эффект конфигурации

Только ограниченное количество динамических MAC-адресов может быть изучено портом.

3.5.8.2. Шаги настройки

Настройка максимального количества MAC-адресов, изученных портом

- Опционально
- Выполните эту операцию на коммутаторе.

Команда	**max-dynamic-mac-count** *count*
Описание параметров	*count*: указывает максимальное количество MAC-адресов, изученных портом
По умолчанию	По умолчанию количество MAC-адресов, изученных портом, не ограничено. После ограничения количества MAC-адресов, изученных портом, и после превышения максимального количества MAC-адресов, пакеты с исходных MAC-адресов пересылаются по умолчанию
Командный режим	Режим конфигурации интерфейса

3.5.8.3. Проверка

Запустите **show run**, чтобы запросить результат конфигурации.

3.5.8.4. Пример конфигурации

Настройка максимального количества MAC-адресов, изученных портом

Шаги настройки	Настройте максимальное количество MAC-адресов, изученных портом
	Настройте максимальное количество MAC-адресов, изученных портом, и меры противодействия в случае, если количество MAC-адресов превышает лимит. QTECH(config)# interface GigabitEthernet 1/1 QTECH(config-if-GigabitEthernet 1/1)# max-dynamic-mac-count 100 QTECH(config-if-GigabitEthernet 1/1)# max-dynamic-mac-count exceed-action discard
Проверка	Запустите **show running** на коммутаторе, чтобы запросить конфигурацию

3.5.9. Настройка максимального количества MAC-адресов, изученных VLAN

3.5.9.1. Эффект конфигурации

VLAN может изучить только ограниченное количество динамических MAC-адресов.

3.5.9.2. Шаги настройки

Настройка максимального количества MAC-адресов, изученных VLAN

- Опционально
- Выполните эту операцию на коммутаторе.

Команда	**max-dynamic-mac-count exceed-action** *forward* | *discard*
Описание параметров	*forward* | *discard*: указывает, что пакеты пересылаются или отбрасываются, когда количество MAC-адресов, изученных VLAN, превышает предел
По умолчанию	По умолчанию количество MAC-адресов, изученных VLAN, не ограничено. После того, как количество MAC-адресов, изученных VLAN, будет ограничено, а максимальное количество MAC-адресов превысит лимит, пакеты с исходных MAC-адресов пересылаются по умолчанию
Командный режим	Режим конфигурации VLAN

3.5.9.3. Проверка

Запустите **show run**, чтобы запросить результат конфигурации.

3.5.9.4. Пример конфигурации

- Настройка максимального количества MAC-адресов, изученных VLAN

Шаги настройки	Настройте максимальное количество MAC-адресов, изученных VLAN
	Настройте максимальное количество MAC-адресов, изученных VLAN, и меры противодействия в случае, если количество MAC-адресов превышает предел. QTECH(config)# vlan 2 QTECH(config-vlan)#max-dynamic-mac-count 100 QTECH(config-vlan)# max-dynamic-mac-count exceed-action discard
Проверка	Запустите **show running** на коммутаторе, чтобы запросить конфигурацию

3.6. Мониторинг

3.6.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере важной информации и прерыванию работы служб.

Описание	Команда
Очищает динамические MAC-адреса	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

3.6.2. Отображение

Описание	Команда
Отображает таблицу MAC-адресов	**show mac-address-table** { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Отображает время устаревания для динамических MAC-адресов	**show mac-address-table aging-time**
Отображает максимальное количество динамических MAC-адресов	**show mac-address-table max-dynamic-mac-count**
Отображает конфигурацию и историю уведомлений об изменении MAC-адреса	**show mac-address-table notification** [**interface** [*interface-id*] | **history**]

3.6.3. Отладка

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

Описание	Команда
Отладка работы MAC-адреса	**debug bridge mac**

4. НАСТРОЙКА АГРЕГИРОВАННОГО ПОРТА

4.1. Обзор

Агрегированный порт (AP) используется для объединения нескольких физических каналов в один логический канал для увеличения пропускной способности канала и повышения надежности соединения.

Порт AP поддерживает балансировку нагрузки, то есть равномерно распределяет нагрузку между элементами соединения. Кроме того, порт AP обеспечивает резервирование канала. Когда участник канала порта AP отключен, нагрузка, переносимая каналом, автоматически распределяется между другими функциональными участниками канала. Участник канала не пересылает broadcast- или multicast-пакеты другим участникам канала.

Например, соединение между двумя устройствами поддерживает максимальную пропускную способность 1000 Мбит/с. Когда служебный трафик, передаваемый по каналу, превышает 1000 Мбит/с, избыточный трафик будет отбрасываться. Для решения проблемы можно использовать агрегацию портов. Например, вы можете соединить два устройства сетевыми кабелями и объединить несколько каналов для формирования логического канала, способного передавать данные со скоростью, кратной 1000 Мбит/с.

Например, есть два устройства, соединенных сетевым кабелем. Когда связь между двумя портами устройств отключена, сервисы, передаваемые по каналу, будут прерваны. После объединения подключенных портов сервисы не будут затронуты, пока остается подключенным один канал.

4.1.1. Протоколы и стандарты

IEEE 802.3ad

4.2. Приложения

Приложения	Описание
Агрегация каналов AP и балансировка нагрузки	Между устройством агрегации и устройством ядра передается большое количество пакетов, что требует большей пропускной способности. Чтобы выполнить это требование, вы можете объединить физические каналы связи между устройствами в один логический канал, чтобы увеличить пропускную способность канала, и настроить правильный алгоритм балансировки нагрузки для равномерного распределения рабочей нагрузки на каждый физический канал, тем самым улучшая использование полосы пропускания

4.2.1. Агрегация каналов AP и балансировка нагрузки

4.2.1.1. Сценарий

На Рисунке 4-1 коммутатор взаимодействует с маршрутизатором через порт AP. Все устройства в интрасети (например, два ПК слева) используют маршрутизатор в качестве шлюза. Все устройства в экстрасети (например, два ПК справа) отправляют пакеты на интернет-устройства через маршрутизатор с MAC-адресом шлюза в качестве исходного MAC-адреса. Чтобы распределить нагрузку между маршрутизатором и другими хостами

на другие каналы, настройте балансировку нагрузки на основе MAC-адресов назначения. На коммутаторе настройте балансировку нагрузки на основе MAC-адреса источника.

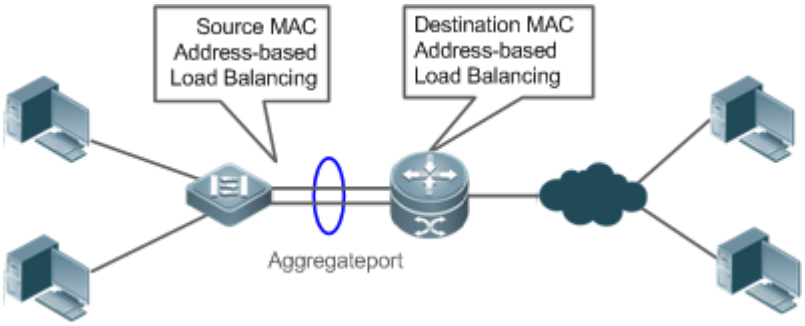


Рисунок 4-1. Агрегация каналов AP и балансировка нагрузки

4.2.1.2. Развертывание

- Настройте напрямую подключенные порты между коммутатором и маршрутизатором как порт статический AP или порт AP протокола управления агрегацией каналов (LACP).
- На коммутаторе настройте алгоритм балансировки нагрузки на основе MAC-адреса источника.
- На маршрутизаторе настройте алгоритм балансировки нагрузки на основе MAC-адреса назначения.

4.3. Функции

4.3.1. Базовые определения

Статический AP

Режим статического AP — это режим агрегации, в котором физические порты напрямую добавляются в группу агрегации AP посредством ручной настройки, чтобы позволить физическим портам пересылать пакеты, когда порты находятся в правильном состоянии в состоянии канала и состоянии протокола.

Порт AP в режиме статического AP называется статическим AP, а его порты-участники называются портами-участниками статического AP.

LACP

LACP — это протокол динамической агрегации каналов. Он обменивается информацией с подключенным устройством через блоки данных LACP (LACPDU).

Порт AP в режиме LACP называется портом AP LACP, а его порты-участники называются портами-участниками AP LACP.

Режим порта-участника AP

Доступны три режима агрегации, а именно активный, пассивный и статический.

Порты-участники AP в активном режиме инициируют согласование LACP. Порты-участники AP в пассивном режиме отвечают только на полученные LACPDU. Порты-участники AP в статическом режиме не отправляют LACPDU для согласования. В следующей таблице перечислены требования для режима peer-порта.

Режим порта	Режим peer-порта
Активный режим	Активный или пассивный режим
Пассивный режим	Активный режим
Статический режим	Статический режим

Состояние порта-участника AP

Доступны два типа состояния порта-участника AP:

- Когда порт-участник находится в состоянии Down, порт не может пересылать пакеты. Отображается состояние Down.
- Когда порт-участник находится в состоянии Up и протокол связи готов, порт может пересылать пакеты. Отображается состояние Up.

Существует три вида состояния порта-участника LACP:

- Когда канал порта отключен, порт не может пересылать пакеты. Отображается состояние Down.
- Когда канал порта находится в состоянии Up и порт добавляется в группу агрегации, отображается состояние bndl.
- Когда канал порта находится в состоянии Up, но порт приостановлен из-за того, что peer end не включен с LACP или атрибуты портов несовместимы с атрибутами master-порта, отображается состояние susp. (Порт в состоянии susp не пересылает пакеты.)

ПРИМЕЧАНИЕ: только полнодуплексные порты поддерживают агрегацию LACP.

ПРИМЕЧАНИЕ: агрегация LACP может быть реализована только тогда, когда скорости, подходы к управлению потоком, типы среды и атрибуты уровня 2/3 портов-участников согласованы.

ПРИМЕЧАНИЕ: если вы измените предыдущие атрибуты порта-участника в группе агрегации, агрегация LACP завершится ошибкой.

ПРИМЕЧАНИЕ: порты, которым запрещено присоединяться или выходить из порта AP, не могут быть добавлены или удалены из статического порта AP или порта LACP AP.

Режим емкости AP

Максимальное количество портов-участников является фиксированным и равно максимальному количеству портов AP, умноженному на максимальное количество портов-участников, поддерживаемых одним портом AP. Если вы хотите увеличить максимальное количество портов AP, необходимо уменьшить максимальное количество портов-участников, поддерживаемых одним портом AP, и наоборот. Это касается концепции режима пропускной способности AP. Некоторые устройства поддерживают настройку режима емкости AP. Например, если система поддерживает 16 384 порта-участника, вы можете выбрать режимы 1024 x 16, 512 x 32 и другие режимы пропускной способности AP (Максимальное количество портов AP, умноженное на максимальное количество портов-участников, поддерживаемых одним портом AP).

Идентификатор системы LACP

По умолчанию все порты LACP на устройстве принадлежат одной и той же системе агрегации LACP.

Одно устройство может быть настроено только с одной системой агрегации LACP. Система идентифицируется идентификатором системы, и каждая система имеет приоритет, который является настраиваемым значением. Идентификатор системы состоит из системного приоритета LACP и MAC-адреса устройства. Более низкий приоритет системы указывает на более высокий приоритет идентификатора системы. Если системные приоритеты одинаковы, меньший MAC-адрес устройства указывает на более высокий приоритет идентификатора системы. Система с идентификатором более высокого приоритета определяет состояние порта. Состояние порта системы с идентификатором более низкого приоритета соответствует состоянию порта более высокого приоритета.

Идентификатор системы LACP можно настроить, когда LACP-порты нескольких (максимум четырех) независимых устройств должны согласовываться с LACP-портом определенного устройства (например, LACP-порты двух независимых ASW должны согласовываться с LACP-портом устройства NC). Вы можете установить системные идентификаторы портов LACP независимых устройств на один и тот же MAC-адрес и настроить разные идентификаторы устройств для реализации нормального согласования.

Идентификатор устройства LACP

Идентификатор устройства LACP можно настроить, когда LACP-порты нескольких независимых устройств должны согласоваться с LACP-портом определенного устройства. Он должен быть настроен вместе с идентификатором системы.

Идентификатор порта LACP

Каждый порт имеет независимый приоритет порта LACP, который является настраиваемым значением. Идентификатор порта состоит из приоритета порта LACP и номера порта. Меньший приоритет порта указывает на более высокий приоритет идентификатора порта. Если приоритеты портов совпадают, меньший номер порта указывает на более высокий приоритет идентификатора порта.

Master-порт LACP

Когда динамические порты-участники находятся в состоянии Up, LACP выбирает один из этих портов в качестве master-порта на основе скоростей и дуплексных режимов, приоритетов идентификаторов портов в группе агрегации и состояния объединения портов-участников в состоянии Up. Только порты, имеющие те же атрибуты, что и master-порт, находятся в состоянии Bundle и участвуют в пересылке данных. Когда атрибуты портов изменяются, LACP повторно выбирает master-порт. Когда новый master-порт не находится в состоянии Bundle, LACP дезагрегирует порты-участники и снова выполняет агрегирование.

Минимальное количество портов-участников AP

AP может быть настроена с минимальным количеством портов-участников AP. Когда порт-участник выходит из группы агрегации AP, в результате чего количество портов-участников становится меньше минимального числа, другие порты-участники в группе разделяются (состояние «Down»). Когда порт-участник снова присоединяется к группе, в результате чего количество портов-участников превышает минимальное число, порты-участники в группе автоматически объединяются (состояние Up).

Независимые порты LACP

В обычных случаях независимые порты LACP используются для взаимодействия между коммутаторами доступа и серверами с двумя сетевыми адаптерами. Если ОС не предварительно установлена при запуске сервера с двумя сетевыми картами, ОС необходимо установить через устройство удаленной установки PXE OS. До установки ОС сервер с двумя сетевыми адаптерами не может выполнять согласование LACP с устройством доступа, и может работать только один сетевой адаптер. В этом случае порт

на устройстве доступа должен иметь возможность автоматически изменяться на общий физический порт Ethernet, чтобы обеспечить нормальную связь между сервером и удаленным устройством установки PXE OS. После того, как ОС будет установлена и оба сетевых адаптера смогут запускать LACP, порт на устройстве доступа должен иметь возможность снова включить LACP для согласования.

ПРИМЕЧАНИЕ: независимые порты LACP могут работать только на уровне 2. После включения независимого порта LACP, если независимый порт LACP не получает пакеты LACP, он автоматически переключается на общий порт Ethernet, который автоматически копирует скорость, режим дуплекса, управление потоком и конфигурацию VLAN с порта AP, чтобы обеспечить возможности переадресации портов.

ПРИМЕЧАНИЕ: независимый порт LACP автоматически переключается на общий порт Ethernet только в том случае, если он не получает пакеты LACP в течение установленного периода ожидания. После того, как порт получает пакеты LACP, он снова становится портом-участником LACP.

4.3.1.1. Обзор

Обзор	Описание
Агрегация канала	Статическое или динамическое объединение физических каналов для реализации расширения пропускной способности и резервного копирования канала
Балансировка нагрузки	Гибко распределяет нагрузку внутри группы агрегации, используя различные методы балансировки нагрузки

4.3.2. Агрегация канала

4.3.2.1. Принцип работы

Существует два типа агрегации каналов AP. Один — статический AP, а другой — динамическая агрегация через LACP.

Статический AP

Конфигурация статического AP проста. Запустите команду, чтобы добавить указанный физический порт к порту AP. После присоединения к группе агрегации порт-участник может получать и передавать данные и участвовать в балансировке нагрузки внутри группы.

Динамический AP (LACP)

Порт с поддержкой LACP отправляет LACPDU для объявления своего системного приоритета, системного MAC-адреса, приоритета порта, номера порта и операционного ключа. При получении LACPDU от peer end устройство сравнивает системные приоритеты обоих концов на основе идентификатора системы в пакете. Конец с более высоким приоритетом идентификатора системы устанавливает порты в группе агрегации в состояние Bundle на основе приоритетов идентификатора порта в порядке убывания и отправляет обновленный LACPDU. При получении LACPDU peer end устанавливает соответствующие порты в состояние Bundle, чтобы обе стороны поддерживали согласованность, когда порт выходит из группы агрегации или присоединяется к ней. Физический канал может пересылать пакеты только после динамического объединения портов на обоих концах.

После объединения каналов порты-участники LACP периодически обмениваются LACPDU. Когда порт не получает LACPDU в указанное время, происходит тайм-аут, и каналы разгруппировываются. В этом случае порты-участники не могут пересылать пакеты. Есть два режима тайм-аута: длинный тайм-аут и короткий тайм-аут. В режиме длительного тайм-аута порт отправляет пакет каждые 30 секунд. Если он не получает пакет от peer end в течение 90 секунд, происходит тайм-аут. В режиме короткого тайм-аута порт отправляет пакет каждую 1 секунду. Если он не получает пакет от peer end в течение 3 секунд, происходит тайм-аут. (Время тайм-аута по умолчанию в режиме короткого тайм-аута LACP составляет 3 секунды. Это значение можно изменить.)

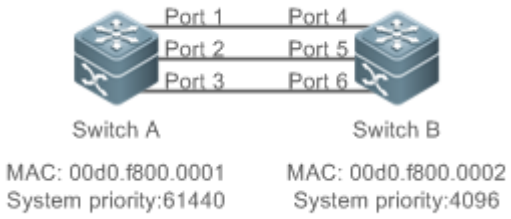


Рисунок 4-2. LACP-согласование

На Рисунке 4-2 коммутатор A подключен к коммутатору B через три порта. Установите системные приоритеты коммутатора A и коммутатора B на 61 440 и 4096 соответственно. Включите LACP на портах 1–6, установите режим агрегации в активный режим и установите для приоритета порта значение по умолчанию 32 768.

При получении LACPDU от коммутатора A коммутатор B обнаруживает, что он имеет более высокий приоритет идентификатора системы, чем коммутатор A (системный приоритет коммутатора B выше, чем у коммутатора A). Коммутатор B устанавливает порт 4, порт 5 и порт 6 в состояние Bundle в зависимости от порядка приоритетов идентификаторов портов (или в порядке возрастания номеров портов, если приоритеты портов совпадают). При получении обновленного LACPDU от коммутатора B коммутатор A обнаруживает, что коммутатор B имеет более высокий приоритет системного идентификатора и устанавливает порт 4, порт 5 и порт 6 в состояние Bundle. Затем коммутатор A также устанавливает порт 1, порт 2 и порт 3 в состояние Bundle.

4.3.3. Балансировка нагрузки

4.3.3.1. Принцип работы

Порты AP разделяют потоки пакетов с помощью алгоритмов балансировки нагрузки, основанных на характеристиках пакетов, таких как MAC-адреса источника и получателя, IP-адреса источника и получателя, а также номера портов источника и получателя уровня 4. Поток пакетов с функцией согласованности передается по одному каналу-участнику, а разные потоки пакетов равномерно распределяются по каналам-участникам. Например, при балансировке нагрузки на основе исходных MAC-адресов пакеты распределяются по каналам-участникам на основе исходных MAC-адресов пакетов. Пакеты с разными исходными MAC-адресами равномерно распределяются по каналам-участникам. Пакеты с идентичным исходным MAC-адресом пересылаются по одному каналу-участнику.

В настоящее время существует несколько режимов балансировки нагрузки AP:

- MAC-адрес источника или MAC-адрес назначения
- MAC-адрес источника + MAC-адрес назначения
- IP-адрес источника или IP-адрес назначения

- IP-адрес источника + IP-адрес назначения
- Номер исходного порта уровня 4 или номер порта назначения уровня 4
- Номер исходного порта уровня 4 + номер порта назначения уровня 4
- IP-адрес источника + номер порта источника уровня 4
- IP-адрес источника + номер порта назначения уровня 4
- IP-адрес назначения + номер порта источника уровня 4
- IP-адрес назначения + номер порта назначения уровня 4
- IP-адрес источника + номер порта источника уровня 4 + номер порта назначения уровня 4
- IP-адрес назначения + номер порта источника уровня 4 + номер порта назначения уровня 4
- IP-адрес источника + IP-адрес назначения + номер порта источника уровня 4
- IP-адрес источника + IP-адрес назначения + номер порта назначения уровня 4
- IP-адрес источника + IP-адрес назначения + номер порта источника уровня 4 + номер порта назначения уровня 4
- Порт панели для входящих пакетов
- Метки пакетов многопротокольной коммутации по меткам (MPLS)
- Опрос порта члена агрегации
- Расширенный режим

ПРИМЕЧАНИЕ: балансировка нагрузки на основе IP-адресов или номеров портов применима только к пакетам уровня 3. Когда устройство, для которого включен этот метод балансировки нагрузки, получает пакеты уровня 2, оно автоматически переключается на метод балансировки нагрузки по умолчанию.

ПРИМЕЧАНИЕ: все методы балансировки нагрузки используют алгоритм нагрузки (алгоритм хеширования (hash-алгоритм)) для расчета каналов-участников на основе входных параметров методов. Входные параметры включают MAC-адрес источника, MAC-адрес назначения, MAC-адрес источника + MAC-адрес назначения, IP-адрес источника, IP-адрес назначения, IP-адрес источника + IP-адреса назначения, IP-адрес источника + IP-адрес назначения + номер порта уровня 4 и так далее. Алгоритм гарантирует, что пакеты с разными входными параметрами равномерно распределяются по каналам-участникам. Это не означает, что эти пакеты всегда распределяются по разным каналам-участникам. Например, при балансировке нагрузки на основе IP-адресов два пакета с разными исходными и целевыми IP-адресами могут быть распределены по одному и тому же каналу-участнику посредством вычислений.

ПРИМЕЧАНИЕ: разные продукты могут поддерживать разные алгоритмы балансировки нагрузки.

Расширенная балансировка нагрузки

Расширенная балансировка нагрузки позволяет комбинировать несколько полей в разных типах пакетов. Эти поля включают **src-mac, dst-mac, l2-protocol** и **src-port** в пакетах уровня 2, **src-ip, dst-ip, protocol, l4-src-port, l4-dst-port** и **src-port** в пакетах IPv4, **src-ip, dst-ip, protocol, l4-src-port, l4-dst-port** и **src-port** в пакетах IPv6; **top-label, 2nd-label, 3rd-label, src-ip, dst-ip, vlan, src-port, src-mac, dst-mac, protocol, l4-src-port, l4-dst-port** и **l2-etype** в пакетах MPLS; и **vlan, src-port, src-id, rx-id, ox-id, fabric-id** и **dst-id** в пакетах FCoE.

Устройство с расширенной балансировкой нагрузки сначала определяет тип передаваемых пакетов и выполняет балансировку нагрузки на основе указанных полей в пакетах. Например, порт AP выполняет балансировку нагрузки на основе исходного IP-адреса для пакетов, содержащих постоянно меняющийся исходный IPv4-адрес.

ПРИМЕЧАНИЕ: все методы балансировки нагрузки применимы к портам AP уровня 2 и уровня 3. Вам необходимо настроить правильные методы распределения нагрузки на основе различных сетевых сред, чтобы полностью использовать пропускную способность сети.

ПРИМЕЧАНИЕ: выполнять расширенную балансировку нагрузки на основе **src-mac, dst-mac** и поля **vlan** в пакетах уровня 2, а также поле **src-ip** в пакетах IPv4. Если входящий пакет представляет собой пакет IPv4 с постоянно меняющимся исходным MAC-адресом, улучшенный алгоритм балансировки не действует, поскольку устройство будет выполнять балансировку нагрузки только на основе поля **src-ip** в пакете IPv4, обнаружив, что он пакет IPv4.

ПРИМЕЧАНИЕ: в расширенной балансировке нагрузки алгоритм балансировки MPLS действует только для пакетов VPN уровня 3 MPLS, но не действует для пакетов VPN уровня 2 MPLS.

Управление балансировкой хеш-нагрузки

Балансировка хеш-нагрузки позволяет пользователям гибко управлять балансировкой нагрузки в различных сценариях. В настоящее время QTECH применяет следующие функции управления балансировкой хеш-нагрузки:

- Фактор нарушения хеширования: трафик через порты AP хешируется для балансировки. Для двух устройств одного типа будет рассчитан один и тот же путь для балансировки нагрузки для одного и того же потока. При развертывании ECMP один и тот же поток двух устройств может быть сбалансирован для одного и того же целевого устройства, что приводит к хеш-поляризации. Фактор нарушения хеширования используется для воздействия на алгоритм балансировки нагрузки. Различные факторы нарушений настраиваются для разных устройств, чтобы обеспечить разные пути для одного и того же потока.
- Хеш-синхронизация: для обеспечения безопасности сети между внутренней и внешней сетями развертывается кластер брандмауэра для очистки трафика. Это требует, чтобы uplink- и downlink-трафик сеанса передавались на одно и то же устройство в кластере брандмауэра для обработки. IP-адреса источника и получателя, содержащиеся в uplink- и downlink-потоках сеанса, меняются местами. Потоки uplink- и downlink-каналов будут направляться на разные брандмауэры в кластере брандмауэров на основе традиционного алгоритма хеширования. Функция хеш-синхронизации гарантирует, что uplink- и downlink-потоки сеанса передаются по одному и тому же пути.
- Режим хеш-алгоритма: примените наиболее подходящий режим хеш-алгоритма к различному трафику, чтобы при изменении трафика можно было сохранить баланс. Например, если MAC-адреса источника и получателя потока увеличиваются на 1 одновременно, настройте алгоритм, основанный на том, что MAC-адреса источника и получателя не могут поддерживать баланс потока. На данный момент необходимо применить подходящий режим хеш-алгоритма.
- Режим получения хеш-фактора: в заголовке каждого пакета VXLAN, GRE и других туннельных пакетов есть внутренний и внешний уровни. Можно указать, чтобы получить хеш-фактор из внутреннего или внешнего уровня для достижения лучшего эффекта балансировки. Например, в некоторых сценариях туннельные пакеты имеют один и тот же внешний IP-адрес, но разные внутренние IP-адреса. В этом случае внутренний IP-адрес можно указать в качестве хеш-фактора для оптимизации балансировки трафика.

4.3.4. Обнаружение BFD порта участника

4.3.4.1. Принцип работы

Обнаружение двунаправленной пересылки (BFD) — это протокол, обеспечивающий быстрое обнаружение сбоев пути. Согласно RFC7130, протоколу LACP требуется 3 секунды для обнаружения отказов канала даже в режиме короткого тайм-аута. Пакеты, переданные неисправному каналу в течение 3-секундного периода, будут потеряны. BFD обеспечивает более быстрое обнаружение сбоев. Вы можете настроить BFD на портах-участниках, чтобы обнаруживать сбой канала и переключать нагрузку на другие каналы-участники в случае сбоя канала.

Поскольку BFD — это протокол уровня 3, вам необходимо настроить BFD на портах AP уровня 3. BFD подразделяется на обнаружение IPv4 и обнаружение IPv6, которые обнаруживают пути IPv4 и IPv6 соответственно. Когда BFD обнаруживает, что путь к порту-участнику не работает, пакеты не будут распределяться на порт-участник.

После включения BFD на порту AP сеансы BFD устанавливаются на его портах-участниках в состоянии пересылки независимо.

4.4. Ограниченичения

- Каждый AP продуктов серии QSW-6900 содержит до восьми портов-участников, и каждое устройство по умолчанию поддерживает до 256 AP.
- Для продуктов серии QSW-6900 можно установить любой из следующих режимов емкости AP: 255×16, 127×32, 63×64 и 31×128. В этих режимах максимальное количество портов-участников, поддерживаемых каждым AP, составляет 16, 32, 64 и 128 соответственно, а максимальное количество поддерживаемых AP — 255, 127, 63 и 31 соответственно. Конфигурация по умолчанию — 255×16.
- Когда продукты серии QSW-6900 используют балансировку нагрузки, основанную на MAC-адресе источника, MAC-адресе получателя или MAC-адресе источника + MAC-адресе получателя, устройства также используют поле типа Ethernet и поле VLAN unicast-пакетов в качестве коэффициентов балансировки по умолчанию.
- В продуктах серии QSW-6900 используется нерасширенный режим балансировки нагрузки. При включенном отслеживании протокола управления группами Интернета (IGMP snooping) или multicast-маршрутизации ключевыми словами для балансировки нагрузки multicast-пакетов являются src-ip, dst-ip или src-ip+dst-ip. Ключевые слова для балансировки нагрузки других multicast-пакетов, неизвестных unicast-пакетов и broadcast-пакетов: src-mac, dst-mac или src-mac+dst-mac. Например, когда пакеты уровня 3 (неизвестные unicast-, multicast- и broadcast-пакеты) пересылаются на уровне 2, балансировка нагрузки не может выполняться на основе src-ip или dst-ip. В этом случае можно использовать расширенный режим, поскольку балансировка нагрузки в этом режиме выполняется на основе типа пакета.
- В режиме балансировки нагрузки на основе src-dst-ip-l4port изменения L4port в продуктах серии QSW-6900 действительны только для unicast-пакетов.
- Продукты серии QSW-6900 поддерживают алгоритмы балансировки нагрузки на основе AP. Алгоритмы балансировки нагрузки на основе AP поддерживают балансировку нагрузки только на основе SMAC, DMAC, SMAC+DMAC, SIP, DIP и SIP+DIP.
- Продукты серии QSW-6900 не поддерживают алгоритм балансировки нагрузки Round Robin (RR).

- Расширенные шаблоны балансировки нагрузки продуктов серии QSW-6900 поддерживают следующие поля:
  - Шаблон L2: src-mac dst-mac vlan l2-protocol src-port
  - Шаблон IPv4: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port
  - Шаблон IPv6: src-ip dst-ip protocol vlan l4-src-port l4-dst-port src-port

4.5. Конфигурация

Конфигурация	Описание и команда	
Настройка статических портов AP	(Обязательно) Используется для ручной настройки агрегации каналов	
	interface aggregateport	Создает порт AP Ethernet
	interface san-port-channel	Создает порт FC AP
	port-group	Настраивает статические порты-участники AP
Настройка портов LACP AP	(Обязательно) Используется для динамической настройки агрегации каналов	
	port-group mode	Настраивает порты-участники LACP
	lacp system-priority	Настраивает системный приоритет LACP
	lacp short-timeout period	Настраивает время тайм-аута системы LACP в режиме короткого тайм-аута
	lacp port-priority	Настраивает приоритет порта
	lacp short-timeout	Настраивает режим короткого тайм-аута на порту
Включение LinkTrap	(Опционально) Используется для включения LinkTrap	
	snmp trap link-status	Включает объявление LinkTrap для порта AP
	aggregateport member linktrap	Включает LinkTrap для портов-участников AP

Конфигурация	Описание и команда	
Настройка режима балансировки нагрузки	(Опционально) Используется для настройки режима балансировки нагрузки для агрегированного канала	
	aggregateport load-balance	Настраивает алгоритм балансировки нагрузки для порта AP или портов-участников AP
	(Опционально) Используется для настройки профиля улучшенной балансировки нагрузки	
	load-balance-profile	Переименовывает профиль улучшенной балансировки нагрузки
	l2 field	Настраивает режим балансировки нагрузки для пакетов уровня 2
	ipv4 field	Настраивает режим балансировки нагрузки для пакетов IPv4
	ipv6 field	Настраивает режим балансировки нагрузки для пакетов IPv6
	mpls field	Настраивает режим балансировки нагрузки для пакетов MPLS
	trill field	Настраивает режим балансировки нагрузки для пакетов TRILL
	fcoe field	Настраивает режим балансировки нагрузки для пакетов FCoE
	(Опционально) Используется для управления политикой балансировки нагрузки	
	aggregateport hash-elasticity enable	Настраивает гибкий хеш
	hash-disturb *string*	Настраивает коэффициент помех (нарушений) хеша
	hash-symmetrical [ipv4 | ipv6 | fcoe| on]	Настраивает хеш-синхронизацию

Конфигурация	Описание и команда	
Настройка режима балансировки нагрузки	**aggregateport hash-header {inner | outer | inner-outer}**	Настраивает режим получения коэффициента балансировки для туннельного пакета
Настройка режима емкости AP	(Опционально) Используется для настройки режима пропускной способности AP	
	aggregateport capacity mode	Настраивает режим пропускной способности AP в режиме глобальной конфигурации
Включение BFD для портов-участников AP	(Опционально) Он используется для включения BFD для портов-участников AP	
	aggregate bfd-detect ipv4	Включает IPv4 BFD для портов-участников AP
Настройка предпочтительного порта-участника AP	(Опционально) Он используется для настройки порта-участника AP в качестве предпочтительного порта	
	aggregateport primary-port	Настраивает порт-участник AP в качестве предпочтительного порта
Настройка минимального количества портов-участников AP	**Aggregateport member minimum**	Настраивает минимальное количество портов-участников AP
Настройка минимального количества портов-участников AP (действие)	**Aggregateport member minimum action**	Запускает действие, когда количество портов-участников AP в состоянии Up меньше минимального количества портов-участников AP
Включение функции независимого порта LACP	**lacp individual enable**	Включает функцию независимого порта LACP

4.5.1. Настройка статических портов AP

4.5.1.1. Эффект конфигурации

- Настройте несколько физических портов в качестве портов-участников AP для реализации агрегации каналов.
- Пропускная способность канала агрегации равна сумме пропускных способностей каналов-участников.

- Когда канал-участник порта AP отключен, нагрузка, переносимая каналом, автоматически распределяется между другими функциональными каналами-участниками.

4.5.1.2. Примечания

- К порту AP можно добавить только физические порты.
- Порты разных типов медиа или режимов портов не могут быть добавлены к одному и тому же порту AP.
- Порты уровня 2 можно добавить только к порту AP уровня 2, а порты уровня 3 можно добавить только к порту AP уровня 3. Атрибуты уровня 2/3 порта AP, которые содержат порты-участники, не могут быть изменены.
- После добавления порта к порту AP атрибуты порта заменяются атрибутами порта AP.
- После удаления порта из порта AP атрибуты порта восстанавливаются.

ПРИМЕЧАНИЕ: после добавления порта к порту AP атрибуты порта согласуются с атрибутами порта AP. Поэтому не выполняйте настройку портов-участников AP и не применяйте настройку к конкретному порту-участнику AP. Однако некоторые конфигурации (команды выключения и отсутствия выключения) можно настроить на портах-участниках AP. При использовании портов-участников AP проверьте, может ли функция, которую вы хотите настроить, воздействовать на конкретный порт-участник AP, и правильно выполните эту настройку.

4.5.1.3. Шаги настройки

Создание порта AP Ethernet

- Обязательный.
- Выполните эту настройку на устройстве с поддержкой AP.

Команда	**interface aggregateport** *ap-number*
Описание параметров	*ap-number*: указывает количество портов AP
По умолчанию	По умолчанию портов AP не создано
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы создать порт AP Ethernet, запустите команду **interfaces aggregateport** в режиме глобальной конфигурации. Чтобы удалить указанный порт AP Ethernet, запустите команду **no interfaces aggregateport** *ap-number* в режиме глобальной конфигурации

ПРИМЕЧАНИЕ: запустите **port-group**, чтобы добавить физический порт к порту статической AP в режиме конфигурации интерфейса. Если порт AP не существует, он будет создан автоматически.

ПРИМЕЧАНИЕ: запустите **port-group mode**, чтобы добавить физический порт к порту LACP AP в режиме конфигурации интерфейса. Если порт AP не существует, он будет создан автоматически.

ПРИМЕЧАНИЕ: функция AP должна быть настроена на устройствах на обоих концах канала, а режим AP должен быть одинаковым (статический AP или LACP AP).

Настройка портов-участников статического AP

- Обязательный.
- Выполните эту настройку на устройствах с поддержкой AP.

Команда	**port-group** *ap-number*
Описание параметров	*ap-number*: указывает номер порта AP
По умолчанию	По умолчанию никакие порты не добавляются ни к одному статическому AP
Командный режим	Режим настройки интерфейса указанного порта Ethernet
Руководство по использованию	Чтобы добавить порты-участники к порту AP, запустите **port-group** в режиме настройки интерфейса. Чтобы удалить порты-участники из порта AP, запустите **no port-group** в режиме конфигурации интерфейса

ПРИМЕЧАНИЕ: статические порты-участники AP, настроенные на устройствах на обоих концах канала, должны быть согласованы.

ПРИМЕЧАНИЕ: после того, как порт-участник выходит из порта AP, настройки по умолчанию порта-участника восстанавливаются. Различные функции по-разному обрабатывают настройки портов-участников по умолчанию. Рекомендуется проверять и подтверждать настройки порта после того, как порт-участник выходит из порта AP.

ПРИМЕЧАНИЕ: после того, как порт-участник выходит из порта AP, порт отключается с помощью команды **shutdown**, чтобы избежать образования петель. После того, как вы подтвердите, что топология нормальная, запустите **no shutdown** в режиме конфигурации интерфейса, чтобы снова включить порт.

Преобразование AP уровня 2 в AP уровня 3

- Опционально.
- Если вам нужно включить маршрутизацию уровня 3 на порте AP, например, для настройки IP-адресов или записей статического маршрута, преобразуйте порт AP уровня 2 в порт AP уровня 3 и включите маршрутизацию на порте AP уровня 3.
- Выполните эту настройку на устройствах с поддержкой AP, которые поддерживают функции уровней 2 и 3, таких как коммутаторы уровня 3 или контроллеры беспроводного доступа (AC).

Команда	**no switchport**
По умолчанию	По умолчанию порты AP являются портами уровня 2
Командный режим	Режим настройки интерфейса указанного порта AP
Руководство по использованию	Функция AP уровня 3 поддерживается только устройствами уровня 3

ПРИМЕЧАНИЕ: порт AP, созданный на устройстве уровня 3, которое не поддерживает функцию уровня 2, является портом AP уровня 3. В противном случае порт AP является портом AP уровня 2.

Создание субинтерфейса AP Ethernet

- Опционально.
- На устройстве, поддерживающем конфигурацию субинтерфейса, запустите **interface aggregateport** *sub-ap-number*, чтобы создать субинтерфейс.
- Выполните эту настройку на устройствах с поддержкой AP, которые поддерживают функции уровня 2 и уровня 3, например, коммутаторы уровня 3.

Команда	**interface aggregateport** *sub-ap-number*
Описание параметров	*sub-ap-number*: указывает номер субинтерфейса AP
По умолчанию	По умолчанию никакие субинтерфейсы не созданы
Командный режим	Режим настройки интерфейса указанного порта AP
Руководство по использованию	Вам необходимо преобразовать master-порт порта AP в порт уровня 3 перед созданием субинтерфейса

4.5.1.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show aggregateport summary**, чтобы отобразить конфигурацию AP.

Команда	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Описание параметров	*aggregate-port-number*: указывает номер порта AP. **load-balance**: отображает алгоритм балансировки нагрузки. **summary**: отображает сводку по каждому каналу
Командный режим	Любой режим

Руководство по использованию	Информация обо всех портах AP отображается, если вы не укажете номер порта AP
	QTECH# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- Ag1 8 Enabled ACCESS dst-mac Gi0/2

4.5.1.5. Пример конфигурации

Настройка порта статической AP Ethernet

Сценарий:

Рисунок 4-3.

Шаги настройки	• Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A к порту 3 статического AP. • Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B к порту 3 статического AP
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3
Проверка	Запустите **show aggregateport summary**, чтобы проверить, содержит ли порт AP 3 порты-участники GigabitEthernet 1/1 и GigabitEthernet 1/2
Коммутатор A	SwitchA# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- Ag3 8 Enabled ACCESS Gi1/1,Gi1/2

Коммутатор B	SwitchB# show aggregateport summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- Ag3 8 Enabled ACCESS Gi2/1,Gi2/2

4.5.2. Настройка портов LACP AP

4.5.2.1. Эффект конфигурации

- Подключенные устройства выполняют автосогласование через LACP для реализации динамического объединения каналов.
- Пропускная способность канала агрегации равна сумме пропускных способностей каналов-участников.
- Когда канал-участник порта AP отключен, нагрузка, переносимая каналом, автоматически распределяется между другими функциональными каналами-участниками.
- LACP требуется 90 секунд для обнаружения сбоя соединения в режиме длительного ожидания и 3 секунды в режиме короткого времени ожидания.

4.5.2.2. Примечания

- После того, как порт выйдет из порта LACP AP, настройки порта по умолчанию могут быть восстановлены. Различные функции по-разному обрабатывают настройки портов-участников по умолчанию. Рекомендуется проверять и подтверждать настройки порта после того, как порт-участник выходит из порта LACP AP.
- Изменение системного приоритета LACP может привести к тому, что порты-участники LACP будут дезагрегированы и снова объединены.
- Изменение приоритета порта-участника LACP может привести к дезагрегации и повторному объединению других портов-участников.

4.5.2.3. Шаги настройки

Настройка портов-участников LACP

- Обязательный.
- Выполните эту настройку на устройствах с поддержкой LACP.

Команда	**port-group** *key-number* **mode** { **active** | **passive** }
Описание параметров	*key-number*: указывает ключ управления порта AP. Другими словами, это номер порта LACP AP. Максимальное значение зависит от количества портов AP, поддерживаемых устройством. **active**: указывает, что порты активно добавляются к порту динамического AP. **passive**: указывает, что порты пассивно добавляются к порту динамического AP

По умолчанию	По умолчанию к любому порту LACP AP не добавляются физические порты
Командный режим	Режим конфигурации интерфейса указанного физического порта
Руководство по использованию	Используйте эту команду в режиме конфигурации интерфейса, чтобы добавить порты-участники к порту LACP AP

ПРИМЕЧАНИЕ: конфигурация порта-участника LACP на обоих концах канала должна быть согласованной.

Настройка идентификатора системы LACP

- Опционально.
- Настройте идентификатор системы LACP, когда LACP-порты нескольких (максимум четыре) независимых устройств должны согласоваться с LACP-портом определенного устройства. Настройте идентификатор системы LACP вместе с идентификатором устройства LACP.

Команда	**lacp system-id** *system-id*
Описание параметров	*system-id*: указывает системный идентификатор группы агрегации. Это должен быть действительный MAC-адрес unicast-рассылки
По умолчанию	Идентификатор системы LACP — это MAC-адрес изустройства по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду в режиме конфигурации интерфейса для настройки идентификатора системы LACP

Настройка идентификатора устройства LACP

- Опционально.
- Настройте идентификатор устройства LACP, когда LACP-порты нескольких (максимум четыре) независимых устройств должны согласоваться с LACP-портом определенного устройства. Настройте идентификатор устройства LACP вместе с идентификатором системы LACP.

Команда	**lacp device** *number*
Описание параметров	*number*: указывает идентификатор устройства группы агрегации. Значение варьируется от 0 до 3
По умолчанию	Идентификатор устройства LACP по умолчанию равен 0

Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду в режиме конфигурации интерфейса для настройки идентификатора устройства LACP

Настройка приоритета системы LACP

- Опционально.
- Выполните эту настройку, когда вам нужно настроить приоритет идентификатора системы. Меньшее значение указывает на более высокий приоритет идентификатора системы. Устройство с более высоким приоритетом идентификатора системы выбирает порт AP.
- Выполните эту настройку на устройствах с поддержкой LACP.

Команда	**lacp system-priority** *system-priority*
Описание параметров	*system-priority*: указывает системный приоритет LACP. Диапазон значений от 0 до 65 535
По умолчанию	По умолчанию системный приоритет LACP равен 32768
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте эту команду в режиме глобальной конфигурации для настройки системного приоритета LACP. Все динамические каналы-участники имеют общий системный приоритет LACP. Изменение системного приоритета LACP повлияет на все каналы-участники. Чтобы восстановить настройки по умолчанию, запустите **no lacp system-priority** в режиме конфигурации интерфейса

Настройка приоритета порта-участника LACP

- Опционально.
- Выполните эту настройку, если вам нужно указать приоритет идентификатора порта. Меньшее значение указывает на более высокий приоритет идентификатора порта. Порт с наивысшим приоритетом идентификатора порта будет выбран в качестве master-порта.
- Выполните эту настройку на устройствах с поддержкой LACP.

Команда	**lacp port-priority** *port-priority*
Описание параметров	*port-priority*: указывает приоритет порта-участника LACP. Диапазон значений от 0 до 65 535
По умолчанию	По умолчанию приоритет порта-участника LACP равен 32 768

Командный режим	Режим конфигурации интерфейса указанного физического порта
Руководство по использованию	Используйте эту команду в режиме глобальной конфигурации, чтобы настроить приоритет порта-участника LACP. Для восстановления настроек запустите **no lacp port-priority** в режиме конфигурации интерфейса

Настройка режима тайм-аута портов-участников LACP

- Необязательный.
- Если вам нужно реализовать обнаружение сбоя канала в реальном времени, настройте режим короткого тайм-аута. LACP требуется 90 секунд для обнаружения сбоя соединения в режиме длительного тайм-аута и 3 секунды в режиме короткого тайм-аута. (Время тайм-аута по умолчанию в режиме короткого тайм-аута LACP составляет 3 секунды. Это значение можно изменить.)
- Выполните эту настройку на устройствах с поддержкой LACP, таких как коммутаторы.

Команда	**lacp short-timeout**
По умолчанию	По умолчанию режим тайм-аута портов-участников LACP — длительный тайм-аут
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Режим тайм-аута поддерживается только физическими портами. Чтобы восстановить настройки по умолчанию, запустите **no lacp short-timeout** в режиме конфигурации интерфейса

Настройка времени тайм-аута системы LACP в режиме короткого тайм-аута

- Опционально.
- Настройте эту функцию, когда необходимо настроить тайм-аут устройства в режиме короткого тайм-аута LACP.
- Настройте эту функцию на устройствах, поддерживающих функцию LACP.

Команда	**lacp short-timeout period** *value*
Описание параметров	*value*: указывает время тайм-аута в режиме короткого тайм-аута. Значение варьируется от 3 секунд до 90 секунд
По умолчанию	Тайм-аут по умолчанию в режиме короткого тайм-аута LACP составляет 3 секунды
Командный режим	Режим глобальной конфигурации

Руководство по использованию	В режиме глобальной конфигурации запустите команду, чтобы настроить тайм-аут в режиме короткого тайм-аута LACP. Все группы динамических каналов, настроенные на устройстве, имеют одинаковый тайм-аут в режиме короткого тайм-аута LACP. Изменение значения повлияет на все агрегатные группы на коммутаторе. В режиме конфигурации интерфейса запустите команду **no lacp short-timeout period**, чтобы восстановить тайм-аут в режиме короткого тайм-аута LACP до значения по умолчанию

4.5.2.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show lacp summary**, чтобы отобразить состояние канала LACP.

Команда	**show lacp summary** [*key-number*]
Описание параметров	*key-number*: указывает номер порта LACP AP
Командный режим	Любой режим
Руководство по использованию	Информация обо всех портах LACP AP отображается, если вы не укажете *key-name*. Идентификатор системы и идентификатор устройства отображается, если настроены
	QTECH#show lacp summary System Id:32768, 0000.1236.54aa Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 2: System Id: 0000.1236.54aa Device num : 1 Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Te1/0/1 SA down 32768 0x2 0x4001 0x45 Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State ---

	Te1/0/1	SP	0	0000.0000.0000	0x0	0x0	0x0

4.5.2.5. Пример конфигурации

Настройка LACP

Сценарий:

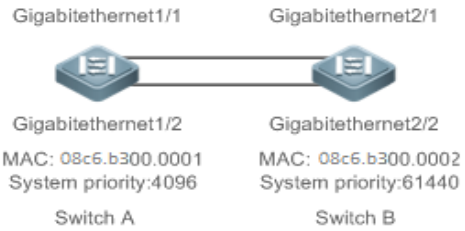


Рисунок 4-4.

Шаги настройки	• На коммутаторе A установите для системного приоритета LACP значение 4096. • Включите динамическую агрегацию каналов на портах GigabitEthernet1/1 и GigabitEthernet1/2 на коммутаторе A и добавьте порты в порт 3 AP LACP. • На коммутаторе B установите для системного приоритета LACP значение 61 440. • Включите динамическую агрегацию каналов на портах GigabitEthernet2/1 и GigabitEthernet2/2 на коммутаторе B и добавьте порты в порт 3 AP LACP
Коммутатор A	SwitchA# configure terminal SwitchA(config)# lacp system-priority 4096 SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# end
Коммутатор B	SwitchB# configure terminal SwitchB(config)# lacp system-priority 61440 SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# end
Проверка	Запустите команду **show lacp summary 3**, чтобы проверить, содержит ли порт 3 AP LACP порты-участники GigabitEthernet2/1 и GigabitEthernet2/2
Коммутатор A	SwitchA# show LACP summary 3

	System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d
Комму-татор Б	SwitchB# show LACP summary 3 System Id:32768, 08c6.b3.0002 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi2/1 SA bndl 32768 0x3 0x1 0x3d Gi2/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi2/1 SA 32768 08c6.b3.0001 0x3 0x1 0x3d Gi2/2 SA 32768 08c6.b3.0001 0x3 0x2 0x3d

4.5.3. Включение LinkTrap

4.5.3.1. Эффект конфигурации

Включите систему с LinkTrap для отправки сообщений LinkTrap при изменении каналов агрегации.

4.5.3.2. Шаги настройки

Включение LinkTrap для порта AP

- Необязательный.
- Включите LinkTrap в режиме настройки интерфейса. По умолчанию LinkTrap включен. Сообщения LinkTrap отправляются при изменении состояния канала или протокола порта AP.
- Выполните эту настройку на устройствах с поддержкой AP.

Команда	**snmp trap link-status**
По умолчанию	По умолчанию LinkTrap включен
Командный режим	Режим настройки интерфейса указанного порта AP
Руководство по использованию	Используйте эту команду в режиме конфигурации интерфейса, чтобы включить LinkTrap для указанного порта AP. После включения LinkTrap сообщения LinkTrap отправляются при изменении состояния канала порта AP. В противном случае сообщения LinkTrap не отправляются. По умолчанию LinkTrap включен. Чтобы отключить LinkTrap для порта AP, запустите **no snmp trap link-status** в режиме конфигурации интерфейса. LinkTrap нельзя включить для определенного порта-участника AP. Чтобы включить LinkTrap для всех портов-участников AP, запустите **aggregateport member linktrap** в режиме глобальной конфигурации

Включение LinkTrap для портов-участников AP

- Опционально.
- По умолчанию LinkTrap отключен для портов-участников AP.
- Выполните эту настройку на устройствах с поддержкой AP.

Команда	**aggregateport member linktrap**
По умолчанию	По умолчанию LinkTrap отключен для портов-участников AP
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Используйте эту команду в режиме глобальной конфигурации, чтобы включить LinkTrap для всех портов-участников AP. По умолчанию сообщения LinkTrap не отправляются при изменении состояния соединения портов-участников AP. Чтобы отключить LinkTrap для всех портов-участников AP, запустите **no aggregateport member linktrap** в режиме глобальной конфигурации

4.5.3.3. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- После включения LinkTrap вы можете отслеживать эту функцию на портах AP или их портах-участниках с помощью программного обеспечения MIB.

4.5.3.4. Пример конфигурации

Включение LinkTrap для портов-участников AP

Сценарий:

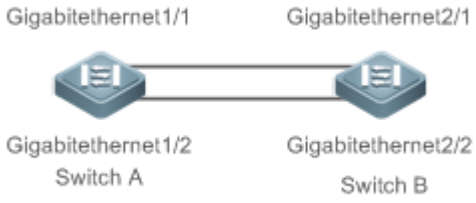


Рисунок 4-5.

Шаги настройки	• Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A к порту 3 статического AP. • Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B к порту 3 статического AP. • На коммутаторе A отключите LinkTrap для порта AP 3 и включите LinkTrap для его портов-участников. • На коммутаторе B отключите LinkTrap для порта 3 AP и включите LinkTrap для его портов-участников AP
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport member linktrap SwitchA(config)# interface Aggregateport 3 SwitchA(config-if-AggregatePort 3)# no snmp trap link-status
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2

	SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport member linktrap SwitchB(config)# interface Aggregateport 3 SwitchB(config-if-AggregatePort 3)# no snmp trap link-status
Проверка	Запустите **show running**, чтобы проверить, включен ли LinkTrap для порта AP 3 и его портов-участников
Коммута-тор A	SwitchA# show run | include AggregatePort 3 Building configuration… Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchA# show run | include AggregatePort aggregateport member linktrap
Коммута-тор B	SwitchB# show run | include AggregatePort 3 Building configuration… Current configuration: 54 bytes interface AggregatePort 3 no snmp trap link-status SwitchB# show run | include AggregatePort aggregateport member linktrap

4.5.4. Настройка режима балансировки нагрузки

4.5.4.1. Эффект конфигурации

- Система распределяет входящие пакеты по каналам-участникам, используя указанный алгоритм балансировки нагрузки. Поток пакетов с согласованной функцией передается по одному каналу-участнику, тогда как разные потоки пакетов равномерно распределяются по разным каналам. Устройство с расширенной балансировкой нагрузки сначала определяет тип передаваемых пакетов и выполняет балансировку нагрузки на основе указанных полей в пакетах. Например, порт AP выполняет балансировку нагрузки на основе исходного IP-адреса для пакетов, содержащих постоянно меняющийся исходный IPv4-адрес.
- В расширенном режиме балансировки нагрузки настройте коэффициент хеш-неполадок, чтобы гарантировать, что одни и те же пакеты от двух устройств одного типа будут распределяться по разным каналам.
- В расширенном режиме балансировки нагрузки включите хеш-синхронизацию, чтобы гарантировать, что пакеты uplink- и downlink-каналов одного типа будут передаваться по одному и тому же каналу. Например, при балансировке нагрузки на основе исходного и целевого IP-адресов включите хеш-синхронизацию для

пакетов IPv4, чтобы гарантировать, что пакеты IPv4 uplink- и downlink-каналов будут передаваться по одному и тому же пути.

4.5.4.2. Примечания

- Различные факторы неполадок могут привести к одному и тому же эффекту неполадок.
- Включите или отключите хеш-синхронизацию для IPv4, IPv6, FCoE и On по мере необходимости.

4.5.4.3. Шаги настройки

- Настройка алгоритма глобальной балансировки нагрузки порта AP.
- (Опционально) Выполните эту настройку, если вам нужно оптимизировать балансировку нагрузки.
- Выполните эту настройку на устройствах с поддержкой AP.

Команда	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **enhanced profile** *profile-name* }
Описание параметров	**dst-mac**: указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов. **src-mac**: указывает, что нагрузка распределяется на основе исходных MAC-адресов входящих пакетов. **src-dst-ip**: указывает, что нагрузка распределяется на основе исходного и конечного IP-адресов входящих пакетов. **dst-ip**: указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов. **src-ip**: указывает, что нагрузка распределяется на основе исходных IP-адресов входящих пакетов. **src-dst-mac**: указывает, что нагрузка распределяется на основе MAC-адресов источника и получателя входящих пакетов. **src-dst-ip-l4port**: указывает, что нагрузка распределяется на основе исходного IP-адреса и IP-адреса назначения, а также номеров исходного и целевого портов уровня 4. **enhanced profile** *profile-name*: указывает имя расширенного профиля балансировки нагрузки
По умолчанию	Балансировка нагрузки может основываться на MAC-адресах источника и получателя (применимо к коммутаторам), IP-адресах источника и получателя (применимо к шлюзам) или профиле расширенной балансировки нагрузки (применимо к коммутаторам с линейными картами CB)
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no aggregateport load-balance** в режиме глобальной конфигурации. Можно запустить **aggregateport load-balance** в режиме конфигурации интерфейса порта AP на устройствах, которые поддерживают настройку балансировки нагрузки на конкретном порту AP. Конфигурация в режиме конфигурации интерфейса превалирует. Чтобы отключить алгоритм балансировки нагрузки, запустите **no aggregateport load-balance** в режиме конфигурации интерфейса порта AP. После этого вступает в силу алгоритм балансировки нагрузки, настроенный в режиме глобальной конфигурации. Можно запустить **aggregateport load-balance** в режиме конфигурации интерфейса порта AP на устройствах, которые поддерживают настройку балансировки нагрузки на конкретном порту AP

Переименование профиля улучшенной балансировки нагрузки

- По умолчанию, если устройство поддерживает расширенную балансировку нагрузки, система создает профиль с именем по умолчанию для улучшенной балансировки нагрузки. Выполните эту настройку, когда вам нужно переименовать профиль или восстановить настройки по умолчанию. В остальных случаях конфигурация необязательна.
- Выполните эту настройку на устройствах, поддерживающих расширенную балансировку нагрузки, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**load-balance-profile** *profile-name*
Описание параметров	*profile-name*: указывает имя профиля, которое может содержать до 31 символа
По умолчанию	Имя профиля по умолчанию — **default**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Чтобы войти в режим профиля по умолчанию, запустите **load-balance-profile default**. Чтобы переименовать расширенный профиль балансировки нагрузки, запустите **load-balance-profile** *profile-name*. Чтобы восстановить имя профиля по умолчанию, запустите **default load-balance-profile** в режиме глобальной конфигурации. Чтобы восстановить настройки балансировки нагрузки по умолчанию, запустите **default load-balance-profile** *profile-name* в режиме глобальной конфигурации. Глобально поддерживается только один профиль. Пожалуйста, не удаляйте профиль. Чтобы отобразить расширенный профиль балансировки нагрузки, запустите **show load-balance-profile**

Настройка режима балансировки нагрузки пакетов уровня 2

- (Опционально) Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов уровня 2.

- Выполните эту настройку на устройствах, поддерживающих расширенную балансировку нагрузки, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**l2 field** { [**src-mac**] [**dst-mac**] [**l2-protocol**] [**src-port**] [**dst-port**] }
Описание параметров	**src-mac**: указывает, что нагрузка распределяется на основе MAC-адресов источника входящих пакетов уровня 2. **dst-mac**: указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов уровня 2. **l2-protocol**: указывает, что нагрузка распределяется на основе типов протоколов уровня 2 для входящих пакетов уровня 2. **src-port**: указывает, что нагрузка распределяется на основе порта панели для входящих пакетов уровня 2
По умолчанию	По умолчанию режим балансировки нагрузки пакетов уровня 2 — **src-mac** и **dst-mac**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no l2 field** в режиме конфигурации профиля

Настройка режима балансировки нагрузки пакетов IPv4

- Опционально.
- Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов IPv4.
- Выполните эту настройку на устройствах, поддерживающих расширенную балансировку нагрузки, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**ipv4 field** {[**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**][**l4-dst-port**] [**src-port**] }
Описание параметров	**src-ip**: указывает, что нагрузка распределяется на основе исходных IP-адресов входящих пакетов IPv4. **dst-ip**: указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов IPv4. **protocol**: указывает, что нагрузка распределяется на основе типов протоколов входящих пакетов IPv4. **l4-src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов уровня 4 входящих пакетов IPv4. **l4-dst-port**: указывает, что нагрузка распределяется на основе номеров портов назначения уровня 4 для входящих пакетов IPv4. **src-port**: указывает, что нагрузка распределяется на основе порта панели для входящих пакетов IPv4

По умолчанию	По умолчанию режим балансировки нагрузки пакетов IPv4 — **src-ip** и **dst-ip**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no ipv4 field** в режиме настройки профиля

Настройка режима балансировки нагрузки пакетов IPv6

- Опционально.
- Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов IPv6.
- Выполните эту настройку на устройствах, поддерживающих балансировку нагрузки пакетов IPv6, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**ipv6 field** { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**][**l4-dst-port**] [**src-port**]}
Описание параметров	**src-ip**: указывает, что нагрузка распределяется на основе исходных IP-адресов входящих пакетов IPv6. **dst-ip**: указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов IPv6. **protocol**: указывает, что нагрузка распределяется на основе типов протоколов входящих пакетов IPv6. **l4-src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов уровня 4 входящих пакетов IPv6. **l4-dst-port**: указывает, что нагрузка распределяется на основе номеров портов назначения уровня 4 для входящих пакетов IPv6. **src-port**: указывает, что нагрузка распределяется в соответствии с номерами исходных портов входящих пакетов IPv6
По умолчанию	По умолчанию режим балансировки нагрузки пакетов IPv6 — **src-ip** и **dst-ip**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no ipv6 field** в режиме настройки профиля

Настройка режима балансировки пакетной нагрузки MPLS

- Опционально.
- Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов MPLS.

- Выполните эту настройку на устройствах, поддерживающих балансировку нагрузки пакетов MPLS, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**mpls field** { [**top-label**] [**2nd-label**] [**3rd-label**] [**src-ip**] [**dst-ip**] [**vlan**] [**src-port**] [**dst-port**] [**src-mac**] [**dst-mac**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**l2-etype**] }
Описание параметров	**src-ip**: указывает, что нагрузка распределяется на основе исходных IP-адресов входящих пакетов MPLS. **dst-ip**: указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов MPLS. **top-label**: указывает, что нагрузка распределяется на основе top label входящих пакетов MPLS. **2nd-label**: указывает, что нагрузка распределяется на основе вторых меток входящих пакетов MPLS. **3rd-label**: указывает, что нагрузка распределяется на основе третьих меток входящих пакетов MPLS. **vlan**: указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов MPLS. **src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов входящих пакетов MPLS. **dst-port**: указывает, что нагрузка распределяется на основе порта для исходящих пакетов MPLS. **src-mac**: указывает, что нагрузка распределяется на основе MAC-адресов источника входящих пакетов MPLS. **dst-mac**: указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов MPLS. **protocol**: указывает, что нагрузка распределяется на основе типов протоколов входящих пакетов MPLS. **l4-src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов уровня 4 входящих пакетов MPLS. **l4-dst-port**: указывает, что нагрузка распределяется на основе номеров портов назначения уровня 4 входящих пакетов MPLS. **l2-etype**: указывает, что нагрузка распределяется на основе типов Ethernet пакетов MPLS
По умолчанию	По умолчанию режим балансировки нагрузки для пакетов MPLS — **top-label** и **2nd-label**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no mpls field** в режиме конфигурации профиля

ПРИМЕЧАНИЕ: алгоритм балансировки нагрузки MPLS действует только для пакетов MPLS Layer-3 VPN.

Настройка режима балансировки нагрузки пакетов TRILL

- Опционально.
- Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов TRILL.
- Выполните эту настройку на устройствах, поддерживающих балансировку нагрузки пакетов TRILL, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**trill field** { [**vlan**] [**src-ip**] [**dst-ip**] [**src-port**] [**dst-port**] [**src-mac**] [**dst-mac**] [**l4-src-port**] [**l4-dst-port**] [**l2-etype**] [**protocol**] [**ing-nick**] [**egr-nick**] }
Описание параметров	**vlan**: указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов TRILL. **src-ip**: указывает, что нагрузка распределяется на основе исходных IP-адресов входящих пакетов TRILL. **dst-ip**: указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов TRILL. **src-port**: трафик распределяется в соответствии с номерами портов источника входящих пакетов TRILL. **src-mac**: указывает, что нагрузка распределяется на основе MAC-адресов источника входящих пакетов TRILL. **dst-ip**: указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов TRILL. **l4-src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов уровня 4 входящих пакетов TRILL. **l4-dst-port**: указывает, что нагрузка распределяется на основе номеров портов назначения уровня 4 для входящих пакетов TRILL. **l2-etype**: указывает, что нагрузка распределяется на основе типов Ethernet пакетов TRILL. **protocol**: указывает, что нагрузка распределяется на основе типов протоколов входящих пакетов TRILL. **ing-nick**: указывает, что нагрузка распределяется на основе псевдонимов Ingress Rbridge для входящих пакетов TRILL. **egr-nick**: указывает, что нагрузка распределяется на основе псевдонимов Egress Rbridge входящих пакетов TRILL
По умолчанию	По умолчанию режим балансировки нагрузки для пакетов TRILL — **src-mac, dst-mac** и **vlan**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no trill field** в режиме настройки профиля.

	ПРИМЕЧАНИЕ: потоки пакетов TRILL Transit RBridge сбалансированы на основе следующих полей: **ing-nick**, **egr-nick**, **src-mac**, **dst-mac**, **vlan** и **l2-etype**. **ПРИМЕЧАНИЕ:** потоки пакетов TRILL Egress RBridge сбалансированы на основе следующих полей: • Пакеты уровня 2: **src-mac**, **dst-mac**, **vlan** и **l2-protocol**. • Пакеты уровня 3: **src-ip**, **dst-ip**, **l4-src-port**, **l4-dst-port**, **protocol** и **vlan**. **ПРИМЕЧАНИЕ:** поля **src-port** и **dst-port** могут использоваться для балансировки всех потоков пакетов TRILL Transit RBridge и TRILL Egress RBridge

Настройка режима балансировки нагрузки пакетов FCoE

- Опционально.
- Выполните эту настройку, чтобы указать режим балансировки нагрузки пакетов FCoE.
- Выполните эту настройку на устройствах, поддерживающих балансировку нагрузки пакетов FCoE, таких как коммутаторы агрегации и коммутаторы ядра.

Команда	**fcoe field** {[**vlan**] [**src-port**] [**dst-port**] [**src-id**] [**dst-id**] [**rx-id**] [**ox-id**] [**fabric-id**]}
Описание параметров	**vlan**: указывает, что нагрузка распределяется на основе идентификаторов VLAN для входящих пакетов FCoE. **src-port**: указывает, что нагрузка распределяется на основе номеров исходных портов входящих пакетов FCoE. **src-id**: указывает, что нагрузка распределяется на основе идентификаторов источников пакетов FCoE. **dst-id**: указывает, что нагрузка распределяется на основе идентификаторов назначения пакетов FCoE. **rx-id**: указывает, что нагрузка распределяется на основе идентификаторов Responder Exchange пакетов FCoE. **ox-id**: указывает, что нагрузка распределяется на основе идентификаторов Originator Exchange пакетов FCoE. **fabric-id**: указывает, что нагрузка распределяется на основе идентификаторов сетевой структуры FC пакетов FCoE
По умолчанию	По умолчанию режим балансировки нагрузки пакетов FCoE — **src-id, dst-id** и **ox-id**
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no fcoe field** в режиме настройки профиля

Настройка фактора неполадок хеша

- Опционально
- Выполните эту операцию, чтобы сбалансировать пакеты одного типа через порт AP для устройств одного типа.

Команда	**hash-disturb** *string*
Описание параметров	*string*: указывает строку символов, используемую для расчета коэффициента неполадок хеша
По умолчанию	По умолчанию коэффициент неполадок хеша не установлен
Командный режим	Режим конфигурации профиля
Руководство по использованию	Чтобы восстановить настройки по умолчанию, запустите **no hash-disturb** в режиме настройки профиля

Включение или отключение хеш-синхронизации

- Опционально
- Выполните эту операцию, чтобы убедиться, что uplink- и downlink-потоки пакетов одного и того же типа передаются по одному и тому же пути.

Команда	**hash-disturb** {**ipv4** | **ipv6** | **fcoe**| **on** }
Описание параметров	**ipv4**: указывает, что хеш-синхронизация включена для пакетов IPv4. **ipv6**: указывает, что хеш-синхронизация включена для пакетов IPv6. **fcoe**: указывает, что для пакетов FCoE включена хеш-синхронизация. **on**: указывает, что хеш-синхронизация включена для пакетов в модуле. Различные модули поддерживают разные типы пакетов
По умолчанию	Установите его по мере необходимости
Командный режим	Режим конфигурации профиля
Руководство по использованию	Когда хеш-синхронизация включена для пакетов IPv4, IPv6 и FCoE по мере необходимости, если uplink- и downlink-потоки одного и того же типа пакетов не должны передаваться по одному и тому же пути, запустите форму **no** этой команды в режиме конфигурации профиля

Настройка режима алгоритма глобального баланса трафика на AP

- Опционально.
- Выполняйте эту операцию при изменении трафика, чтобы сохранить баланс трафика.

Команда	**aggregateport algorithm mode** *number*
Описание параметров	*number*: указывает режим алгоритма
По умолчанию	Режим по умолчанию зависит от продукта. Выполнить команду **show aggregateport load-balance**, чтобы проверить настройки по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите команду **no aggregate port algorithm mode** в режиме глобальной конфигурации, чтобы восстановить настройки по умолчанию. Запустите команду **show running** и **show aggregateport load-balance**, чтобы проверить, вступает ли она в силу

Настройка режима получения коэффициента балансировки для туннельных пакетов

- Опционально. При выполнении балансировки нагрузки используйте эту команду, чтобы указать режим получения коэффициента балансировки для конкретных туннельных пакетов, чтобы оптимизировать балансировку трафика.

Команда	**aggregateport hash-header** {**inner** | **outer** | **inner-outer**}
Описание параметров	**inner**: указывает внутренний уровень в заголовке туннельных пакетов в качестве источника для получения коэффициента балансировки. **outer**: указывает внешний уровень в заголовке туннельных пакетов в качестве источника для получения коэффициента балансировки. **inner-outer**: указывает как внутренний, так и внешний уровни в заголовке туннельных пакетов в качестве источника для получения коэффициента балансировки
По умолчанию	Конфигурация по умолчанию зависит от продукта
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Используйте форму **default** этой команды, чтобы восстановить режим сбора данных по умолчанию. После настройки, если команда **show running** не отображает конфигурацию, сконфигурированный режим совпадает со значением по умолчанию. **ПРИМЕЧАНИЕ:** поддерживаемые параметры конфигурации и типы туннельных пакетов зависят от продукта

4.5.4.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show aggregateport load-balance**, чтобы отобразить конфигурацию балансировки нагрузки. Если устройство поддерживает конфигурацию балансировки нагрузки на определенном порту AP, запустите **show aggregateport summary**, чтобы отобразить конфигурацию.
- Запустите **show load-balance-profile**, чтобы отобразить расширенный профиль балансировки нагрузки.

Команда	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Описание параметров	*aggregate-port-number*: указывает номер порта AP. **load-balance**: отображает алгоритм балансировки нагрузки. **summary**: отображает сводку по каждому каналу
Командный режим	Любой режим
Руководство по использованию	Информация о всех портах AP отображается, если вы не укажете номер порта AP
	QTECH# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---- Ag1 8 Enabled ACCESS dst-mac Gi0/2

Команда	**show load-balance-profile** [*profile-name*]
Описание параметров	*profile-name*: указывает имя профиля
Командный режим	Любой режим

Руководство по использованию	Отображаются все расширенные профили, если не указать номер профиля
	QTECH# show load-balance-profile module0 Load-balance-profile: module0 Packet Hash Field: IPv4: src-ip dst-ip IPv6: src-ip dst-ip L2 : src-mac dst-mac vlan MPLS: top-labe l2nd-label

4.5.4.5. Пример конфигурации

Настройка режима балансировки нагрузки

Сценарий:

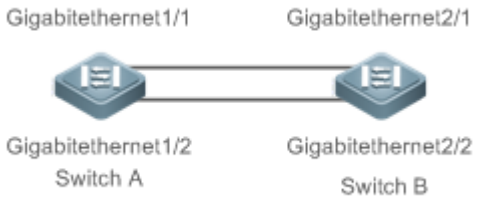


Рисунок 4-6.

Шаги настройки	• Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A к порту 3 статического AP. • Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B к порту 3 статического AP. • На коммутаторе A настройте балансировку нагрузки на основе MAC-адреса источника для порта 3 AP в режиме глобальной конфигурации. • На коммутаторе B настройте балансировку нагрузки на основе MAC-адреса назначения для порта 3 AP в режиме глобальной конфигурации
Коммута-тор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac
Коммута-тор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2

	SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Проверка	Запустите **show aggregateport load-balance**, чтобы проверить конфигурацию алгоритма балансировки нагрузки
Коммута-тор A	SwitchA# show aggregatePort load-balance Load-balance : Source MAC
Коммута-тор A	witchB# show aggregatePort load-balance Load-balance : Destination MAC

Настройка управления балансировкой хеш-нагрузки

Сценарий:

Рисунок 4-7.

Шаги настройки	• Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A к порту 3 статического AP. • Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B к порту 3 статического AP. • На коммутаторе A отключите хеш-синхронизацию для пакетов FCoE. • На коммутаторе B отключите хеш-синхронизацию для пакетов FCoE. • На коммутаторе A настройте коэффициент хеш-неполадок A. • На коммутаторе B настройте коэффициент хеш-неполадок B. • На коммутаторе A включите гибкий хеш. • На коммутаторе B включите гибкий хеш
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)#load-balance-profile

	SwitchA(config-load-balance-profile)#no hash-symmetrical fcoe SwitchA(config-load-balance-profile)#hash-disturb A SwitchA(config-load-balance-profile)#exit SwitchA(config)#aggregateport hash-elasticity enable
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)#load-balance-profile SwitchB(config-load-balance-profile)# no hash-symmetrical fcoe SwitchA(config-load-balance-profile)#hash-disturb B SwitchB(config-load-balance-profile)#exit SwitchB(config)#aggregateport hash-elasticity enable
Проверка	Запустите **show running**, чтобы проверить правильность конфигурации

4.5.4.6. Распространенные ошибки

Пользователь включает хеш-синхронизацию для пакетов IPv4, IPv6, FCoE и On. Однако конфигурация не отображается, когда пользователь запускает **show running**. Это связано с тем, что хеш-синхронизация для пакетов IPv4, IPv6 и FCoE включена по умолчанию. После того, как пользователь отключит функцию, отобразится конфигурация.

4.5.5. Настройка режима емкости AP

4.5.5.1. Эффект конфигурации

Измените максимальное количество настраиваемых портов AP и максимальное количество портов-участников в каждом порту AP.

4.5.5.2. Примечания

- В системе установлен режим емкости AP по умолчанию. Вы можете запустить команду **show aggregateport capacity**, чтобы отобразить текущий режим емкости.
- Если текущая конфигурация (максимальное количество портов AP или количество портов-участников в каждом порту AP) превышает емкость, которую необходимо настроить, конфигурация режима емкости завершится ошибкой.

4.5.5.3. Шаги настройки

Настройка режима емкости AP

- (Опционально) Выполните эту настройку, чтобы изменить емкость AP.
- Выполните эту настройку на устройствах, поддерживающих изменение пропускной способности AP, таких как коммутаторы ядра.

Команда	**aggregateport capacity mode** *capacity-mode*
Описание параметров	*capacity-mode*: указывает режим емкости
По умолчанию	По умолчанию режимы пропускной способности AP зависят от устройства. Например, 256×16 указывает, что устройство имеет максимум 256 портов AP и 16 портов-участников в каждом порту AP
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В системе предусмотрено несколько режимов емкости для устройств, поддерживающих настройку режима емкости. Чтобы восстановить настройки по умолчанию, запустите **no aggregateport capacity mode** в режиме глобальной конфигурации

4.5.5.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите команду **show aggregateport capacity**, чтобы отобразить текущий режим емкости AP и использование емкости AP.

Команда	**show aggregateport capacity**
Командный режим	Любой режим
	QTECH# show aggregateport capacity AggregatePort Capacity Information: Configuration Capacity Mode: 128*16. Effective Capacity Mode : 256*8. Available Capacity : 128*8. Total Number: 128, Used: 1, Available: 127

4.5.5.5. Пример конфигурации

Настройка режима емкости AP

Сценарий:

Рисунок 4-8.

Шаги настройки	• Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A к порту 3 статической AP. • Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B к порту 3 статической AP. • На коммутаторе A настройте режим пропускной способности AP 128x128. • На коммутаторе B настройте режим пропускной способности AP 256x64
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport capacity mode 128*128
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport capacity mode 256*64
Проверка	Запустите команду **show aggregateport capacity**, чтобы проверить конфигурацию режима емкости AP
Коммутатор A	SwitchA# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 128*128. Effective Capacity Mode : 128*128. Available Capacity Mode : 128*128.

	Total Number : 128, Used: 1, Available: 127
Коммута-тор B	SwitchB# show aggregatePort capacity AggregatePort Capacity Information: Configuration Capacity Mode: 256*64. Effective Capacity Mode : 256*64. Available Capacity Mode : 256*64. Total Number : 256, Used: 1, Available: 255

4.5.6. Включение BFD для портов-участников AP

4.5.6.1. Эффект конфигурации

- Включите BFD для всех портов-участников указанного порта AP.
- После включения BFD для порта AP каждый порт-участник выполняет BFD, чтобы определить, следует ли распределять пакеты на порт-участник для реализации балансировки нагрузки. Когда BFD обнаруживает, что порт-участник отключен, пакеты не распределяются на порт. Когда BFD обнаруживает, что порт-участник восстановлен в состоянии Up, пакеты снова распределяются на порт.

4.5.6.2. Примечания

- После включения BFD для порта AP настраиваются сеансы BFD. Чтобы сеансы вступили в силу, вам необходимо настроить параметры BFD. Дополнительные сведения см. в разделе Reliability Configuration Настройка BFD.
- Включение или отключение BFD для одного порта-участника AP не поддерживается. Вы должны включить или отключить BFD для всей группы AP.
- Только порты-участники в состоянии пересылки включены с BFD. Если порт-участник не находится в состоянии пересылки из-за того, что канал или LACP не работает, сеанс BFD на порту-участнику автоматически удаляется.
- Если доступен только один порт-участник (в состоянии пересылки), все пакеты распределяются на этот порт. В этом случае BFD не работает. Когда имеется более одного доступного порта-участника, BFD снова вступает в силу.

4.5.6.3. Шаги настройки

Включение BFD для портов-участников AP

- (Опционально) Включите BFD, если вам нужно определить сбой пути на портах-участниках в миллисекундах. Трафик по неисправному каналу будет переключен на каналы других участников в случае сбоя связи.
- Выполните эту настройку на устройствах, которые поддерживают корреляцию AP-BFD.

Команда	**aggregate bfd-detect** {**ipv4** | **ipv6**} *src_ip dst_ip*
Описание параметров	**ipv4**: включает IPv4 BFD, если порт AP настроен с адресом IPv4. **ipv6**: включает IPv6 BFD, если порт AP настроен с адресом IPv6

Описание параметров	*src_ip*: указывает исходный IP-адрес, т. е. IP-адрес, настроенный для порта AP. *dst_ip*: указывает IP-адрес назначения, т. е. IP-адрес, настроенный на порту peer AP
По умолчанию	По умолчанию BFD отключен
Командный режим	Режим конфигурации интерфейса указанного порта AP
Руководство по использованию	1. Чтобы сеансы BFD вступили в силу, необходимо настроить параметры BFD. Дополнительные сведения см. в разделе Reliability Configuration Настройка BFD. 2. Различные продукты могут поддерживать разные IPv4/IPv6 BFD. 3. Для порта AP можно включить как IPv4 BFD, так и IPv6 BFD, если они оба поддерживаются. 4. После включения BFD для порта AP сеансы BFD автоматически настраиваются на его портах-участниках в состоянии пересылки

4.5.6.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show interface aggregateport**, чтобы отобразить состояние BFD портов-участников AP.

Команда	**show interface aggregateport** *ap-num*
Описание параметров	*ap-num*: указывает номер порта AP
Командный режим	Любой режим
	QTECH# show interface aggregateport 11 … Aggregate Port Informations: Aggregate Number: 11 Name: "AggregatePort 11" Members: (count=2) GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl BFD Status: UP GigabitEthernet 0/2 Link Status: Up Lacp Status: susp BFD Status: Invalid

4.5.6.5. Пример конфигурации

Включение IPv4 BFD для портов-участников AP

Сценарий:

Рисунок 4-9.

Шаги настройки	• Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A и добавьте порты в порт 3 AP LACP. • Включите LACP для портов GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B и добавьте порты в порт 3 AP LACP. • Настройте IP-адрес 1.0.0.1 для порта AP 3 на коммутаторе A и включите IPv4 BFD. • Настройте IP-адрес 1.0.0.2 для порта AP 3 на коммутаторе B и включите IPv4 BFD
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# no switchport SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# ip address 1.0.0.1 SwitchA(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2 SwitchA(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 1/1-2 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# ip address 1.0.0.2 SwitchB(config-if-Aggregateport 3)# aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1 SwitchB(config-if-Aggregateport 3)# bfd interval 50 min_rx 50 multiplier 3

Проверка	Запустите **show run**, чтобы проверить, вступила ли конфигурация в силу. Запустите **show interface aggregateport**, чтобы отобразить состояние BFD портов-участников AP
Коммутатор A	SwitchA# show run | include AggregatePort 3 Building configuration… Current configuration: 54 bytes interface AggregatePort 3 no switchport ip address 1.0.0.1 aggregate bfd-detect ipv4 1.0.0.1 1.0.0.2 bfd interval 50 min_rx 50 multiplier 3 SwitchA# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl BFD Status: UP GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl BFD Status: UP …
Коммутатор B	SwitchB# show run | include AggregatePort 3 Building configuration… Current configuration: 54 bytes interface AggregatePort 3 no switchport ip address 1.0.0.2 aggregate bfd-detect ipv4 1.0.0.2 1.0.0.1 bfd interval 50 min_rx 50 multiplier 3 SwitchB# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl BFD Status: UP

	GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl BFD Status: UP ...

4.5.6.6. Распространенные ошибки

1. Если BFD включен для порта AP без параметров BFD, BFD не вступает в силу.
2. После того, как BFD включен для порта AP, сосед BFD должен быть напрямую подключенным портом AP, включенным с BFD.

4.5.7. Настройка предпочтительного порта-участника AP

4.5.7.1. Эффект конфигурации

- Настройте порт-участник в качестве предпочтительного порта-участника AP.
- После настройки предпочтительного порта-участника пакеты VLAN управления на порте AP перенаправляются этим портом.

4.5.7.2. Примечания

- Дополнительные сведения о настройке VLAN для управления см. в разделе Настройка MAC.
- Для одного порта AP можно настроить только один предпочтительный порт-участник.
- После того, как порт-участник AP LACP настроен в качестве предпочтительного порта-участника AP, если согласование LACP на всех портах-участниках AP не удается, предпочтительный порт автоматически понижается до статического порта-участника AP.

4.5.7.3. Шаги настройки

Настройка предпочтительного порта-участника AP

- (Опционально) Выполните эту настройку, чтобы указать порт-участник AP, предназначенный для пересылки пакетов управления VLAN.
- Конфигурация применима к двухсистемным серверам. Настройте порт, подключенный к управлению NIC сервера, в качестве предпочтительного порта-участника AP.

Команда	**aggregateport primary-port**
По умолчанию	По умолчанию, ни один порт-участник AP не является предпочтительным портом
Командный режим	Режим настройки интерфейса порта-участника AP

4.5.7.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show interface aggregateport**, чтобы отобразить предпочтительный порт-участник AP.

Команда	**show interface aggregateport** *ap-num*
Описание параметров	*ap-num*: указывает номер порта AP
Командный режим	Любой режим
	QTECH# show interface aggregateport 11 … Aggregate Port Informations: Aggregate Number: 11 Name: "AggregatePort 11" Members: (count=2) Primary Port: GigabitEthernet 0/1 GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl GigabitEthernet 0/2 Link Status: Up Lacp Status: bndl …

4.5.7.5. Пример конфигурации

Настройка предпочтительного порта-участника AP

Сценарий:

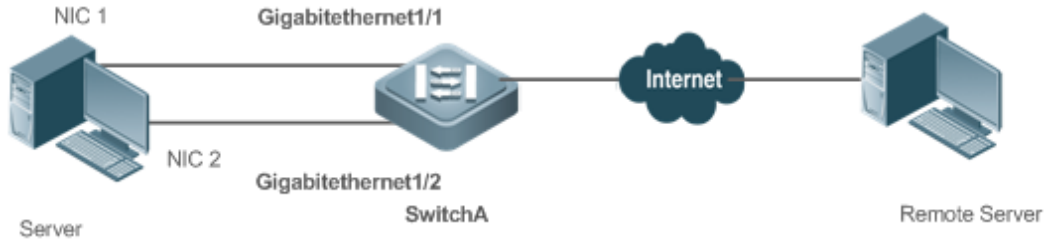


Рисунок 4-10.

Шаги настройки	• Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A и добавьте порты в порт 3 AP LACP. • Настройте порт GigabitEthernet 1/1 на коммутаторе A в качестве предпочтительного порта. • Настройте VLAN 10 на коммутаторе A в качестве управляющей VLAN
Коммута-тор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active

	SwitchA(config-if-range)# exit SwitchA(config)# interface gigabitEthernet 1/1 SwitchA(config-if-GigabitEthernet 1/1) aggregateport primary-port SwitchA(config-if-GigabitEthernet 1/1)# exit SwitchA(config)# aggregateport-admin vlan 10 SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# switchport mode trunk SwitchA(config-if-Aggregateport 3)#
Проверка	Запустите **show run**, чтобы проверить, вступила ли конфигурация в силу. Запустите **show interface aggregateport**, чтобы отобразить предпочтительный порт-участник AP
Коммута-тор A	SwitchA# show run | include GigabitEthernet 1/1 Building configuration... Current configuration: 54 bytes interface GigabitEthernet 1/1 aggregateport primary-port portgroup 3 mode active SwitchA# show interface aggregateport 3 ... Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) Primary Port: GigabitEthernet 1/1 GigabitEthernet 1/1 Link Status: Up Lacp Status: bndl GigabitEthernet 1/2 Link Status: Up Lacp Status: bndl ...

4.5.8. Настройка минимального количества портов-участников LACP AP

4.5.8.1. Эффект конфигурации

После настройки минимального количества портов-участников AP группа агрегации вступает в силу только тогда, когда количество портов-участников больше минимального числа.

4.5.8.2. Примечания

- Если количество портов-участников AP LACP для группы агрегации LACP меньше, чем минимальное настроенное количество портов-участников AP, все порты-участники AP находятся в состоянии отмены привязки.
- После настройки минимального количества портов-участников статических AP, если количество портов-участников статических AP в состоянии Up меньше минимального числа, порты-участники статических AP в состоянии Up не могут пересылать данные, а соответствующая AP не работает. Однако на состояние peer'а это не влияет. Следовательно, соответствующие функции должны быть настроены на peer'е.

4.5.8.3. Шаги настройки

Настройка минимального количества портов-участников AP

- (Опционально) Выполните эту настройку, чтобы указать минимальное количество портов-участников AP.

Команда	**aggregateport member minimum** *number*
Описание параметров	*number*: указывает минимальное количество портов-участников
По умолчанию	По умолчанию минимальное количество портов-участников равно 1
Командный режим	Режим конфигурации интерфейса указанного порта AP

Настройка минимального количества портов-участников AP (действие)

- (Опционально) Выполните эту настройку, когда количество портов-участников AP в состоянии Up меньше минимального количества портов-участников AP.

Команда	**aggregateport member minimum action** [*shutdown*]
Описание параметров	*shutdown*: отключает объединенный порт, когда количество портов-участников AP в состоянии Up меньше минимального количества портов-участников AP
По умолчанию	По умолчанию никакое действие не запускается
Командный режим	Режим конфигурации интерфейса указанного порта AP

4.5.8.4. Проверка

- Запустите **show running**, чтобы отобразить конфигурацию.
- Запустите **show interface aggregateport**, чтобы отобразить состояние портов-участников AP.

Команда	**show interface aggregateport** *ap-num*
Описание параметров	*ap-num*: указывает номер порта AP
Командный режим	Любой режим
	QTECH# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 0/1 Link Status: Up Lacp Status: bndl GigabitEthernet 0/2 Link Status: Up Lacp Status: bndl …

4.5.8.5. Пример конфигурации

Настройка минимального количества портов-участников LACP AP с количеством портов-участников LACP AP меньше минимального количества портов-участников LACP AP

Сценарий:

Рисунок 4-11.

Шаги настройки	• Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A и добавьте порты в порт 3 AP LACP. • Включите LACP для портов GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B и добавьте порты в порт 3 AP LACP. • На коммутаторе A установите минимальное количество портов-участников порта AP с 3 на 3
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2

	SwitchA(config-if-range)# no switchport SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# aggregateport minimum member 3
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# aggregateport minimum member 3
Проверка	• Запустите **show run**, чтобы проверить, вступила ли конфигурация в силу. • Запустите **show lacp summery**, чтобы отобразить состояние агрегирования каждого порта-участника AP
Коммутатор A	SwitchA# show LACP summary 3 System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d

Настройка минимального количества портов-участников LACP AP с количеством портов-участников LACP AP не меньше минимального количества портов-участников LACP AP

Рисунок 4-12.

Шаги настройки	• Включите LACP для портов GigabitEthernet 1/1, GigabitEthernet 1/2 и GigabitEthernet 1/3 на коммутаторе A и добавьте порты в порт 3 AP LACP. • Включите LACP для портов GigabitEthernet 2/1, GigabitEthernet2/2 и GigabitEthernet 2/3 на коммутаторе B и добавьте порты в порт 3 AP LACP. • Установите минимальное количество портов-участников порта LACP AP с 3 на 2
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-3 SwitchA(config-if-range)# no switchport SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)# aggregateport member minimum 2
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-3 SwitchB(config-if-range)# no switchport SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# exit SwitchB(config)# interface aggregateport 3 SwitchB(config-if-Aggregateport 3)# aggregateport member minimum 2
Проверка	Запустите **show run**, чтобы проверить правильность конфигурации. Запустите **show lacp summery**, чтобы запросить статус каждого порта-участника порта AP

Коммутатор A	SwitchA# show LACP summary 3 System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State ----------
	Gi1/1 SA bndl 32768 0x3 0x1 0x3d Gi1/2 SA bndl 32768 0x3 0x2 0x3d Gi1/3 SA bndl 32768 0x3 0x3 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State ----------
	Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d Gi1/3 SA 32768 08c6.b3.0002 0x3 0x3 0x3d

4.5.8.6. Распространенные ошибки

Количество портов-участников AP LACP в группе агрегации LACP меньше, чем минимальное настроенное количество портов-участников AP, группа агрегации LACP не находится в состоянии привязки.

4.5.9. Включение функции независимого порта LACP

4.5.9.1. Эффект конфигурации

- После включения функции независимого порта LACP порт-участник LACP автоматически меняется на общий физический порт, если порт-участник LACP не получает пакеты LACP в течение установленного периода времени ожидания. Состояние порта-участника LACP изменяется на **individual**, и порт-участник LACP может правильно пересылать пакеты.
- После того, как порт-участник LACP получает пакеты LACP, он снова переключается на независимый порт LACP для выполнения согласования пакетов LACP.
- Период тайм-аута независимого порта можно настроить в конфигурации.

4.5.9.2. Примечания

- После включения функции независимого порта LACP порт-участник LACP не сразу изменится на общий физический порт. Порт-участник LACP меняется на независимый порт (общий физический порт) только в том случае, если он не получает пакеты LACP в течение установленного тайм-аута.
- Конфигурация периода тайм-аута для независимого порта LACP влияет только на те порты-участники LACP, которые не превратились в независимые порты. После настройки периода тайм-аута расчет периода возобновится.
- В режиме длительного тайм-аута пакет LACP отправляется каждые 30 секунд. Период тайм-аута должен быть больше 30 секунд, чтобы не влиять на нормальное согласование LACP. Рекомендуется настроить период тайм-аута как минимум в два раза больше периода отправки пакета LACP. В течение короткого периода тайм-аута ограничений нет.

4.5.9.3. Шаги настройки

Включение функции независимого порта LACP

- Опционально.
- Выполните эту операцию, чтобы порт-участник агрегированной группы LACP мог нормально пересылать пакеты, когда порт-участник LACP не может выполнять согласование LACP.

Команда	**lacp individual-port enable**
По умолчанию	По умолчанию функция независимого порта LACP отключена
Командный режим	Режим конфигурации интерфейса

Настройка периода тайм-аута для независимого порта LACP

- Опционально.
- Выполните эту операцию, когда независимому порту LACP необходимо настроить период тайм-аута.

Команда	**lacp individual-timeout period** *time*
Описание параметров	*time*: период тайм-аута. Диапазон 10–90, единица измерения секунды
По умолчанию	Период тайм-аута независимого порта LACP по умолчанию составляет 90 секунд
Командный режим	Режим глобальной конфигурации

4.5.9.4. Проверка

- Запустите **show running**, чтобы запросить соответствующую конфигурацию.

- Запустите **show interface aggregateport**, чтобы запросить состояние порта-участника AP.

Команда	**show interface aggregateport** *ap-num*
Описание параметров	*ap-num*: указывает номер AP
Командный режим	Все режимы
Представление команды	QTECH# show interface aggregateport 3 … Aggregate Port Informations: Aggregate Number: 3 Name: "AggregatePort 3" Members: (count=2) GigabitEthernet 0/1 Link Status: Up Lacp Status: individual GigabitEthernet 0/2 Link Status: Up Lacp Status: individual …

4.5.9.5. Пример конфигурации

Включение функции независимого порта LACP

Сценарий:

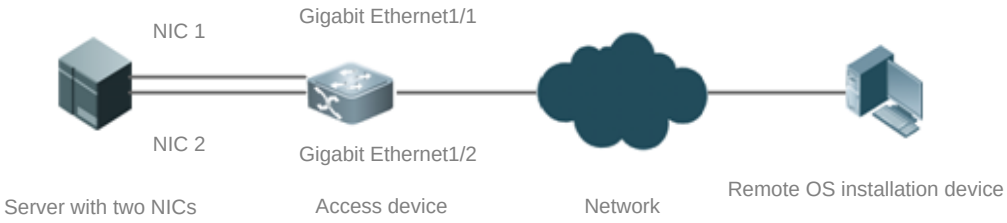


Рисунок 4-13.

Описание	Как показано на Рисунке 4-13, сервер использует NIC 1 и NIC 2 в качестве коммуникационных портов для доступа к портам Gigabitethernet1/1 и Gigabitethernet1/2 устройства доступа. В группу агрегации LACP добавляются порты Gigabitethernet1/1 и Gigabitethernet1/2, например, порт AP 3. Выделяется конкретная VLAN, например, VLAN 10. Функция независимого порта LACP включена для портов Gigabitethernet1/1 и Gigabitethernet1/2. Если ОС не установлена на сервере, согласование LACP между сервером и устройством доступа не выполняется. В этом случае порты Gigabitethernet1/1 и Gigabitethernet1/2 устройства доступа меняются на общие физические порты и автоматически выделяются для

	VLAN 10. Сервер использует сетевую карту 1 или сетевую карту 2 для связи с удаленным устройством установки ОС. После установки ОС сервер подключается к устройству доступа в режиме LACP
Шаги настройки	• Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на устройстве доступа и добавьте порты в порт 3 AP LACP. • Включите функцию независимого порта LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на устройстве доступа. • Выделите порт AP 3 на устройстве доступа для VLAN 10
Коммутатор A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 1/1-2 SwitchA(config-if-range)# port-group 3 mode active SwitchA(config-if-range)# lacp individual-port enable SwitchA(config-if-range)# exit SwitchA(config)# interface aggregateport 3 SwitchA(config-if-Aggregateport 3)#switch access vlan 10 SwitchA(config-if-Aggregateport 3)#
Проверка	Запустите **show run**, чтобы проверить правильность конфигурации. Запустите **show lacp summery**, чтобы запросить статус каждого порта-участника порта AP
Коммутатор A	SwitchA# show LACP summary 3 System Id:32768, 08c6.b3.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregate port 3: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi1/1 SA individual 32768 0x3 0x1 0x3d Gi1/2 SA individual 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State ---

	Gi1/1 SA 32768 08c6.b3.0002 0x3 0x1 0x3d Gi1/2 SA 32768 08c6.b3.0002 0x3 0x2 0x3d

4.6. Мониторинг

4.6.1. Очистка

Описание	Команда
Очищает статистику пакетов LACP на порту-участнике LACP	**clear lacp counters** [*key-number* | *interface-type interface-number*]

4.6.2. Отображение

Описание	Команда
Отображает конфигурацию расширенного профиля балансировки нагрузки	**show load-balance-profile** [*profile-name*]
Отображает состояние агрегации LACP. Вы можете отобразить информацию об указанном порту LACP AP, указав номер ключа	**show lacp summary** [*key-number*]
Отображает статистику пакетов LACP на портах-участниках LACP. Вы можете отобразить информацию об указанном порту LACP AP, указав номер ключа	**show lacp counters** [*key-number*]
Отображает сводку или алгоритм балансировки нагрузки порта AP	**show aggregateport** [*ap-number*] { **load-balance** | *summary* }
Отображает режим емкости и использование порта AP	**show aggregateport capacity**

4.6.3. Отладка

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

Описание	Команда
Отладка порта AP	**debug lsm ap**

Описание	Команда
Отладка LACP	**debug lacp** { **packet** | **event** | **database** | **ha** | **realtime** | **stm** | **timer** | **all**}

5. НАСТРОЙКА VLAN

5.1. Обзор

Виртуальная локальная сеть (VLAN) — это логическая сеть, созданная на основе физической сети. VLAN можно разделить на сети уровня 2 модели OSI.

VLAN имеет те же свойства, что и обычная LAN, за исключением ограничения физического местоположения. Unicast-, broadcast- и multicast-кадры уровня 2 пересылаются и передаются внутри VLAN, сохраняя разделение трафика.

Мы можем определить порт как участник VLAN, и все терминалы, подключенные к этому порту, являются частью виртуальной сети, которая поддерживает несколько VLAN. Вам не нужно физически настраивать сеть при добавлении, удалении и изменении пользователей. Связь между VLAN осуществляется через Устройства уровня 3, как показано на следующем Рисунке.

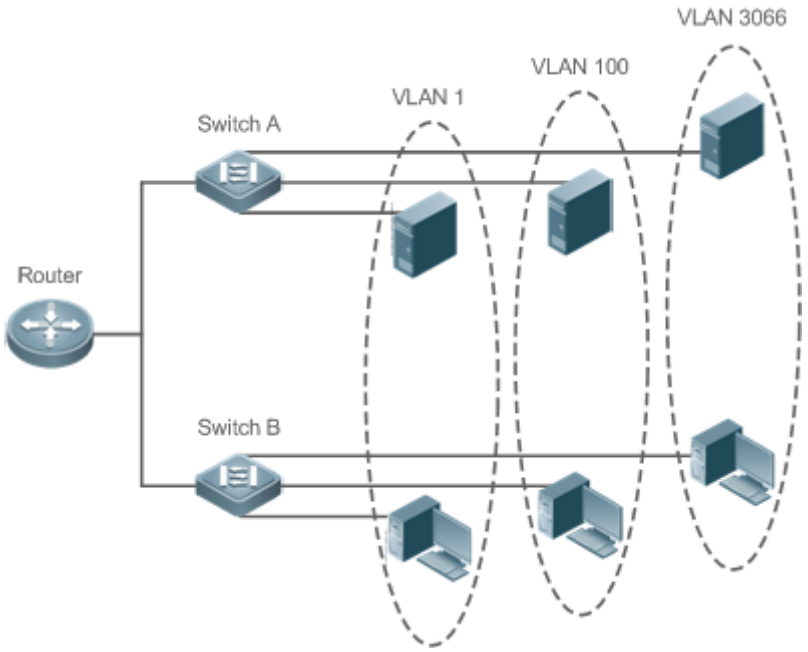


Рисунок 5-1.

5.1.1. Протоколы и стандарты

IEEE 802.1Q

5.2. Приложения

Приложение	Описание
Изоляция VLAN на уровне 2 и соединение VLAN на уровне 3	Интранет разделен на несколько VLAN, реализующих изоляцию уровня 2 и взаимосвязь уровня 3 друг с другом посредством IP-переадресации с помощью коммутаторов ядра

5.2.1. Изоляция VLAN на уровне 2 и соединение VLAN на уровне 3

5.2.1.1. Сценарий

Интранет делится на VLAN 10, VLAN 20 и VLAN 30, реализуя изоляцию уровня 2 друг от друга. Три VLAN соответствуют IP-подсетям 192.168.10.0/24, 192.168.20.0/24 и 192.168.30.0/24, реализуя взаимосвязь друг с другом посредством IP-переадресации с помощью коммутаторов ядра уровня 3.

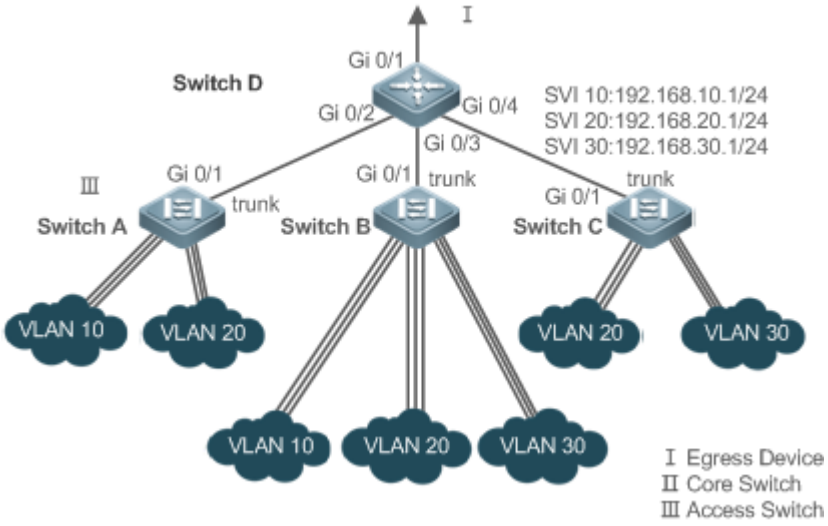


Рисунок 5-2.

Коммутатор A, коммутатор B и коммутатор C являются коммутаторами доступа.

Настройте три VLAN на основном коммутаторе и порт, подключенный к коммутаторам доступа, в качестве магистрального порта и укажите список разрешенных VLAN для реализации изоляции уровня 2.

Настройте три SVI на основном коммутаторе, которые являются интерфейсами шлюза IP-подсетей, соответствующих трем VLAN, и настройте IP-адреса для этих интерфейсов.

Создайте VLAN соответственно на трех коммутаторах доступа, назначьте порты доступа для VLAN и укажите магистральные порты коммутатора ядра.

5.2.1.2. Развертывание

- Разделите интрасеть на несколько VLAN, чтобы реализовать изоляцию уровня 2 между ними.
- Настройте SVI на коммутаторе 3-го уровня для реализации связи 3-го уровня между сетями VLAN.

5.3. Функции

5.3.1. Базовые определения

VLAN

VLAN — это логическая сеть, созданная на основе физической сети. VLAN имеет те же свойства, что и обычная LAN, за исключением ограничения физического местоположения. Unicast-, broadcast- и multicast-кадры уровня 2 пересылаются и передаются внутри VLAN, сохраняя разделение трафика.

ПРИМЕЧАНИЕ: сети VLAN, поддерживаемые продуктами QTECH, соответствуют стандарту IEEE802.1Q. Поддерживается не более 4094 VLAN (VLAN ID 1-4094), среди которых VLAN 1 нельзя удалить.

ПРИМЕЧАНИЕ: настраиваемые идентификаторы VLAN находятся в диапазоне от 1 до 4094.

ПРИМЕЧАНИЕ: в случае нехватки аппаратных ресурсов система возвращает информацию о сбое создания VLAN.

Режим порта

Вы можете определить кадры, которым разрешено проходить через порт, и сети VLAN, к которым принадлежит порт, настроив режим порта.

Режим порта	Описание
Порт доступа (Access port)	Порт доступа принадлежит только одной VLAN, которая указывается вручную
Магистральный порт (Trunk port) (802.1Q)	Магистральный порт по умолчанию принадлежит всем VLAN коммутатора доступа и может пересылать кадры всех VLAN или кадры разрешенных VLAN
Uplink-порт	Порт Uplink по умолчанию принадлежит всем VLAN коммутатора доступа и может пересылать кадры всех VLAN и помечать тегом исходящий трафик Native VLAN
Гибридный порт (Hybrid port)	Гибридный порт по умолчанию принадлежит всем сетям VLAN коммутатора доступа и может пересылать кадры всех сетей VLAN и отправлять кадры сетей VLAN без тегов. Он также может передавать кадры разрешенных VLAN
Сервисный порт (Servicechain Port)	Сервисный порт не изучает MAC-адреса и по умолчанию может пересылать пакеты из любой VLAN. Кроме того, никакая другая конфигурация не допускается

5.3.2. Обзор

Особенность	Описание
VLAN	VLAN помогает реализовать изоляцию уровня 2

5.3.3. VLAN

Каждая VLAN имеет независимый broadcast-домен, а разные VLAN изолированы на уровне 2.

5.3.3.1. Принцип работы

Каждая VLAN имеет независимый broadcast-домен, а разные VLAN изолированы на уровне 2.

Изоляция уровня 2: если SVI не настроены для VLAN, VLAN изолированы на уровне 2. Это означает, что пользователи в этих VLAN не могут взаимодействовать друг с другом.

Межсоединение уровня 3: если SVI настроены на коммутаторе уровня 3 для VLAN, эти VLAN могут взаимодействовать друг с другом на уровне 3.

5.4. Конфигурация

Конфигурация	Описание и команда	
Настройка базовой VLAN	(Обязательный) Он используется для создания VLAN	
	vlan	Вводит идентификатор VLAN
	(Опционально) Он используется для настройки порта доступа для передачи потоков из одной VLAN	
	switchport mode access	Определяет порт как порт доступа уровня 2
	switchport access vlan	Назначает порт для VLAN
	add interface	Добавляет один порт доступа или группу таких портов в текущую VLAN
	(Опционально) Он используется для переименования VLAN	
	name	Называет VLAN
Настройка магистрального порта	(Обязательный) Он используется для настройки порта в качестве магистрального порта	
	switchport mode trunk	Определяет порт как магистральный порт уровня 2
	(Опционально) Он используется для настройки магистральных портов для передачи потоков из нескольких VLAN	
	switchport trunk allowed vlan	Настраивает разрешенные VLAN для магистрального порта
	switchport trunk native vlan	Указывает Native VLAN для магистрального порта

Конфигурация	Описание и команда	
Настройка uplink-порта	(Обязательный) Он используется для настройки порта в качестве порта Uplink	
	switchport mode uplink	Настраивает порт как uplink-порт
	(Опционально) Используется для восстановления режима порта	
	no switchport mode	Восстанавливает режим порта
Настройка гибридного порта	(Обязательный) Он используется для настройки порта как гибридного порта	
	switchport mode hybrid	Настраивает порт как гибридный порт
	(Опционально) Он используется для передачи кадров нескольких сетей VLAN без тегов	
	no switchport mode	Восстанавливает режим порта
	switchport hybrid allowed vlan	Настраивает разрешенные VLAN для гибридного порта
	switchport hybrid native vlan	Настраивает VLAN по умолчанию для гибридного порта
Настройка сервисного порта	(Обязательно) Используется для настройки порта в качестве сервисного порта	
	switchport mode servicechain	Настраивает порт как сервисный порт

5.4.1. Настройка базовой VLAN

5.4.1.1. Эффект конфигурации

VLAN идентифицируется идентификатором VLAN. Вы можете добавлять, удалять, изменять VLAN с 2 по 4094, но VLAN 1 создается автоматически и не может быть удалена. Вы можете настроить режим порта и добавить или удалить VLAN.

5.4.1.2. Шаги настройки

Создание и изменение VLAN

- Обязательный.
- В случае нехватки аппаратных ресурсов система возвращает информацию о сбое создания VLAN.

- Используйте команду **vlan** *vlan-id*, чтобы создать VLAN или войти в режим VLAN.
- Конфигурация:

Команда	**vlan** *vlan-id*
Описание параметров	*vlan-id*: указывает идентификатор VLAN в диапазоне от 1 до 4094
По умолчанию	VLAN 1 создается автоматически и не может быть удалена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если вы введете новый идентификатор VLAN, будет создана соответствующая VLAN. Если вы введете существующий идентификатор VLAN, соответствующая VLAN будет изменена. Вы можете использовать команду **no vlan** *vlan-id* для удаления VLAN. К неудаляемым VLAN относятся VLAN1, VLAN, настроенные с помощью SVI, и SubVLAN

Переименование VLAN

- Опционально.
- Вы не можете назвать VLAN так же, как названа по умолчанию другая VLAN.
- Конфигурация:

Команда	**name** *vlan-name*
Описание параметров	*vlan-name*: указывает имя VLAN
По умолчанию	По умолчанию именем VLAN является ее идентификатор VLAN. Например, имя по умолчанию для VLAN 4 — VLAN 0004
Командный режим	Режим конфигурации VLAN
Руководство по использованию	Чтобы восстановить имя VLAN по умолчанию, используйте команду **no name**

Назначение текущего порта доступа указанной VLAN

- Опционально.
- Используйте команду **switchport mode access**, чтобы указать порты уровня 2 (порты коммутатора) в качестве портов доступа.
- Используйте команду **switchport access vlan** *vlan-id*, чтобы добавить порт доступа к определенной VLAN, чтобы потоки из VLAN могли передаваться через порт.

Команда	**switchport mode access**
По умолчанию	Порт коммутации по умолчанию является портом доступа
Командный режим	Режим конфигурации интерфейса

Команда	**switchport access vlan** *vlan-id*
Описание параметров	*vlan-id*: указывает идентификатор VLAN
По умолчанию	Порт доступа добавляется к VLAN 1 по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если порт назначен несуществующей VLAN, VLAN будет создана автоматически

Добавление порта доступа к текущей VLAN

- Опционально.
- Эта команда действует только на порт доступа. После добавления порта доступа к VLAN потоки VLAN могут передаваться через порт.
- Конфигурация:

Команда	**add interface** { *interface-id* | **range** *interface-range* }
Описание параметров	*interface-id*: указывает один порт. *interface-range*: указывает несколько портов
По умолчанию	По умолчанию все порты Ethernet уровня 2 принадлежат VLAN 1
Командный режим	Режим конфигурации VLAN
Руководство по использованию	В режиме конфигурации VLAN добавьте определенный порт доступа к VLAN. Эта команда имеет тот же эффект, что и команда **switchport access vlan** *vlan-id*

ПРИМЕЧАНИЕ: для двух команд добавления порта в VLAN команда, настроенная позже, перезапишет другую.

5.4.1.3. Проверка

- Отправляйте непомеченные тегом пакеты на порт доступа, и они транслируются в сети VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, вступила ли конфигурация в силу.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметров	*vlan-id*: указывает идентификатор VLAN
Командный режим	Любой режим
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ---------- 20 VLAN0020 STATIC Gi0/1

5.4.1.4. Пример конфигурации

Настройка базовой VLAN и порта доступа

Шаги настройки	• Создайте VLAN и переименуйте ее. • Добавьте порт доступа к VLAN. Есть два подхода. Один:
	QTECH# configure terminal QTECH(config)# vlan 888 QTECH(config-vlan)# name test888 QTECH# (config-vlan)# exit QTECH(config)# interface GigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)# switchport mode access QTECH(config-if-GigabitEthernet 0/3)# switchport access vlan 20 Другой подход добавления порта доступа (GigabitEthernet 0/3) к VLAN20: QTECH# configure terminal SwitchA(config)#vlan 20 SwitchA(config-vlan)#add interface GigabitEthernet 0/3
Проверка	Проверьте правильность конфигурации
	QTECH(config-vlan)#show vlan VLAN Name Status Ports

```
---- ------------------------------ --------- ------------------------
1 VLAN0001       STATIC
20 VLAN0020      STATIC      Gi0/3
888 test888      STATIC
QTECH(config-vlan)#
QTECH# show interface GigabitEthernet 0/3 switchport
Interface               Switchport Mode  Access   Native  Protected  VLAN
lists
------------------------------ ---------- --------- ------ ------
GigabitEthernet 0/3 enabled             ACCESS  20       1          Disabled
ALL
QTECH# show run
!
```

5.4.2. Настройка магистрального порта

5.4.2.1. Эффект конфигурации

Транк или магистральный порт — это канал точка-точка, соединяющий один или несколько интерфейсов Ethernet с другими сетевыми устройствами (например, маршрутизатором или коммутатором), и он может передавать потоки из нескольких VLAN.

Магистральные устройства QTECH используют стандарт инкапсуляции 802.1Q. На следующем Рисунке показана сеть, использующая магистральное соединение.

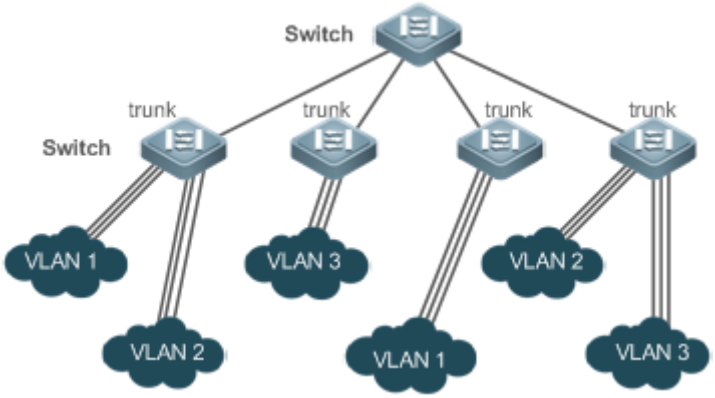


Рисунок 5-3.

Вы можете настроить порт Ethernet или агрегированный порт (подробности см. в разделе Настройка агрегированного порта) в качестве магистрального порта.

Вы должны указать Native VLAN для магистрального порта. Пакеты без тегов, полученные и отправленные из магистрального порта, считаются принадлежащими Native VLAN. Идентификатор VLAN по умолчанию (PVID в IEEE 802.1Q) этого магистрального порта является собственным идентификатором VLAN. При этом кадры Native VLAN, отправляемые через магистральный порт, не помечены. Native VLAN по умолчанию для магистрального порта — это VLAN 1.

При настройке магистрального канала убедитесь, что магистральные порты на двух концах канала используют одну и ту же Native VLAN.

5.4.2.2. Шаги настройки

Настройка магистрального порта

- Обязательный.
- Настройте магистральный порт для передачи потоков из нескольких VLAN.
- Конфигурация:

Команда	**switchport mode trunk**
По умолчанию	Режим по умолчанию — Access (доступ), который может быть изменен на Trunk (транк)
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить значения по умолчанию для всех свойств магистрального порта, используйте команду **no switchport mode**

Определение разрешенных VLAN для магистрального порта

- Опционально.
- По умолчанию магистральный порт передает потоки из всех VLAN (от 1 до 4094). Вы можете настроить список разрешенных VLAN, чтобы запретить прохождение потоков некоторых VLAN через магистральный порт.
- Конфигурация:

Команда	**switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Описание параметров	Параметр *vlan-list* может быть VLAN или несколькими VLAN, а идентификаторы VLAN соединяются по порядку через "-". Например: 10–20. **all** указывает разрешенные VLAN включают все VLAN; **add** указывает на добавление конкретной VLAN в список разрешенных VLAN; **remove** указывает удаление конкретной VLAN из списка разрешенных VLAN; **except** указывает на добавление всех VLAN, кроме перечисленных VLAN, в список разрешенных VLAN. **only** указывает на добавление перечисленных VLAN в список разрешенных VLAN, и удаление других VLAN из списка
По умолчанию	Магистральный порт и порт uplink принадлежат всем VLAN
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Чтобы восстановить конфигурацию магистрального порта по умолчанию (**all**), используйте команду **no switchport trunk allowed vlan**

Настройка Native VLAN

- Опционально.
- Магистральный порт получает и отправляет тегированные или нетегированные кадры 802.1Q. Кадры без тегов передают потоки из Native VLAN. Native VLAN по умолчанию — VLAN 1.
- Если кадр содержит идентификатор VLAN Native VLAN, его тег будет автоматически удален при прохождении магистрального порта.
- Конфигурация:

Команда	**switchport trunk native vlan** *vlan-id*
Описание параметров	*vlan-id*: указывает идентификатор VLAN
По умолчанию	VLAN по умолчанию для магистрального и порта uplink — это VLAN 1
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить Native VLAN магистрального порта до значений по умолчанию, используйте команду **no switchport trunk native vlan**

ПРИМЕЧАНИЕ: когда вы устанавливаете Native VLAN порта как несуществующую VLAN, эта VLAN не будет создана автоматически. Кроме того, Native VLAN может быть вне списка разрешенных VLAN для этого порта. В этом случае потоки из Native VLAN не могут проходить через порт.

5.4.2.3. Проверка

- Отправляйте пакеты с тегами на магистральный порт, и они транслируются в пределах указанных VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, вступила ли конфигурация в силу.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметров	*vlan-id*: указывает идентификатор VLAN
Командный режим	Любой режим

Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- -------------------- 20 VLAN0020 STATIC Gi0/1

5.4.2.4. Пример конфигурации

Настройка базовой VLAN для реализации изоляции уровня 2 и взаимодействия уровня 3

Сценарий:

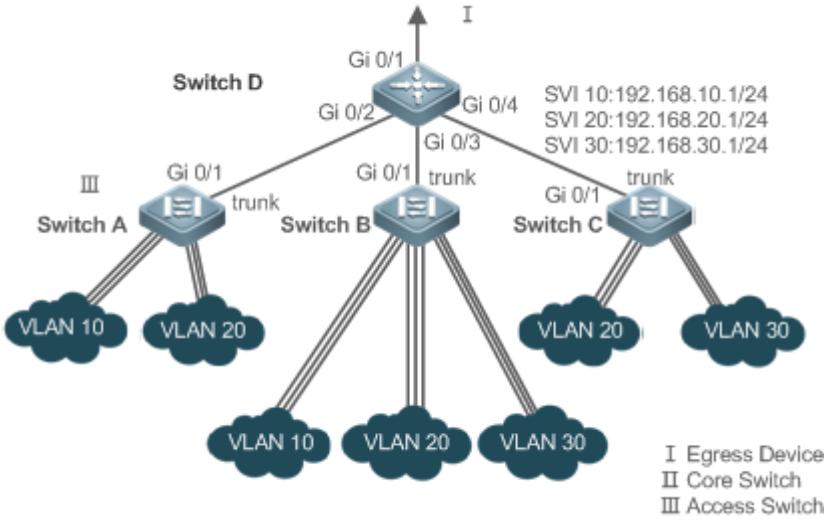


Рисунок 5-4.

Шаги настройки	Требования к сети: Как показано на Рисунке выше, интрасеть делится на VLAN 10, VLAN 20 и VLAN 30, реализуя изоляцию уровня 2 друг от друга. Три VLAN соответствуют IP-подсетям 192.168.10.0/24, 192.168.20.0/24 и 192.168.30.0/24, реализуя взаимосвязь друг с другом посредством IP-переадресации с помощью коммутаторов ядра уровня 3. Ключевые моменты: В следующем примере описаны этапы настройки коммутатора ядра и коммутатора доступа. • Настройте три VLAN на коммутаторе ядра и порт, подключенный к коммутаторам доступа, в качестве магистрального порта и укажите список разрешенных VLAN для реализации изоляции уровня 2. • Настройте три SVI на коммутаторе ядра, которые являются интерфейсами шлюза IP-подсетей, соответствующих трем VLAN, и настройте IP-адреса для этих интерфейсов. • Создайте VLAN соответственно на трех коммутаторах доступа, назначьте порты доступа для VLAN и укажите магистральные порты коммутатора ядра. В следующем примере описаны этапы настройки коммутатора A

D	D#configure terminal D(config)#vlan 10 D(config-vlan)#vlan 20 D(config-vlan)#vlan 30 D(config-vlan)#exit D(config)#interface range GigabitEthernet 0/2-4 D(config-if-range)#switchport mode trunk D(config-if-range)#exit D(config)#interface GigabitEthernet 0/2 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20 D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan add 10,20,30 D(config-if-GigabitEthernet 0/3)#interface GigabitEthernet 0/4 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan add 20,30 D#configure terminal D(config)#interface vlan 10 D(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0 D(config-if-VLAN 10)#interface vlan 20 D(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0 D(config-if-VLAN 20)#interface vlan 30 D(config-if-VLAN 30)#ip address 192.168.30.1 255.255.255.0 D(config-if-VLAN 30)#exit
A	A#configure terminal A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#interface range GigabitEthernet 0/2-12 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 10 A(config-if-range)#interface range GigabitEthernet 0/13-24 A(config-if-range)#switchport mode access A(config-if-range)#switchport access vlan 20

	A(config-if-range)#exit A(config)#interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport mode trunk
Проверка	• Отобразите конфигурацию VLAN на коммутаторе ядра. • Отображение информации о VLAN, включая идентификаторы VLAN, имена VLAN, статус и задействованные порты. • Отображение состояния портов Gi 0/2, Gi 0/3 и Gi 0/4
D	D#show vlan VLAN Name Status Ports ---- -------- -------- ------------------------------ 1 VLAN0001 STATIC Gi0/1, Gi0/5, Gi0/6, Gi0/7 Gi0/8, Gi0/9, Gi0/10, Gi0/11 Gi0/12, Gi0/13, Gi0/14, Gi0/15 Gi0/16, Gi0/17, Gi0/18, Gi0/19 Gi0/20, Gi0/21, Gi0/22, Gi0/23 Gi0/24 10 VLAN0010 STATIC Gi0/2, Gi0/3 20 VLAN0020 STATIC Gi0/2, Gi0/3, Gi0/4 30 VLAN0030 STATIC Gi0/3, Gi0/4 D#show interface GigabitEthernet 0/2 switchport Interface Switchport Mode AccessNative Protected VLAN lists ---------- ---------- --------- ------ ------ GigabitEthernet 0/2 enabled TRUNK1 1 Disabled 10,20 D#show interface GigabitEthernet 0/3 switchport Interface Switchport Mode AccessNative Protected VLAN lists ---------- ---------- --------- ------ ------ GigabitEthernet 0/3 enabled TRUNK1 1 Disabled 10,20,30 D#show interface GigabitEthernet 0/4 switchport Interface Switchport Mode AccessNative Protected VLAN lists ---------- ---------- --------- ------ ------ GigabitEthernet 0/4 enabled TRUNK1 1 Disabled 20,30

5.4.3. Настройка uplink-порта

5.4.3.1. Эффект конфигурации

Uplink-порт обычно используется в среде QinQ (стандарт IEEE 802.1ad) и подобен магистральному порту. Их отличие состоит в том, что порт uplink передает только тегированные кадры, а магистральный порт отправляет нетегированные кадры Native VLAN.

5.4.3.2. Шаги настройки

Настройка uplink-порта

- Обязательный.
- Настройте uplink-порт для передачи потоков из нескольких VLAN, но можно передавать только тегированные кадры.
- Конфигурация:

Команда	**switchport mode uplink**
По умолчанию	Режим по умолчанию — Access (доступ), который можно изменить на Uplink
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить значения по умолчанию для всех свойств uplink-порта, используйте команду **no switchport mode**

Определение разрешенных VLAN для магистрального порта

- Опционально.
- Вы можете настроить список разрешенных VLAN, чтобы запретить прохождение потоков некоторых VLAN через порт uplink.
- Конфигурация:

Команда	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Описание параметров	Параметр *vlan-list* может быть VLAN или несколькими VLAN, а идентификаторы VLAN соединяются по порядку через "-". Например: 10–20. **all** указывает, что разрешенные VLAN включают все VLAN; **add** указывает добавление конкретной VLAN в список разрешенных VLAN; **remove** указывает удаление конкретной VLAN из списка разрешенных VLAN; **except** указывает добавление всех VLAN, кроме перечисленных VLAN, в список разрешенных VLAN;

	only указывает добавление перечисленных VLAN в список разрешенных VLAN и удаление других VLAN из списка
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить значения по умолчанию для разрешенных VLAN (**all**), используйте команду **no switchport trunk allowed vlan**

Настройка Native VLAN

- Опционально.
- Если кадр содержит идентификатор VLAN Native VLAN, его тег не будет удален при прохождении через порт uplink. Это противоречит транковому порту.
- Конфигурация:

Команда	**switchport trunk native vlan** *vlan-id*
Описание параметров	*vlan-id*: указывает идентификатор VLAN
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить настройки по умолчанию для Native VLAN uplink-канала, используйте команду **no switchport trunk native vlan**

5.4.3.3. Проверка

- Отправляйте пакеты с тегами на uplink-порт, и они транслируются в пределах указанных VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, вступила ли конфигурация в силу.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметров	*vlan-id*: указывает идентификатор VLAN
Командный режим	Любой режим
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- -------------------- 20 VLAN0020 STATIC Gi0/1

5.4.3.4. Пример конфигурации

Настройка uplink-порта

Шаги настройки	Ниже приведен пример настройки Gi0/1 как uplink-порта
	QTECH# configure terminal QTECH(config)# interface gi 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode uplink QTECH(config-if-GigabitEthernet 0/1)# end
Проверка	Проверьте правильность конфигурации
	QTECH# show interfaces GigabitEthernet 0/1 switchport Interface Switchport Mode AccessNative Protected VLAN lists ---------- ---------- ---------- ------ ------ GigabitEthernet 0/1 enabled UPLINK 1 1 disabled ALL

5.4.4. Настройка гибридного порта

5.4.4.1. Эффект конфигурации

Гибридный порт обычно используется в среде SHARE VLAN. По умолчанию гибридный порт совпадает с магистральным портом. Их отличие состоит в том, что гибридный порт может отправлять кадры из VLAN, кроме VLAN по умолчанию, в нетегированном формате.

5.4.4.2. Шаги настройки

Настройка гибридного порта

- Обязательный.
- Настройте гибридный порт для передачи потоков из нескольких VLAN.
- Конфигурация:

Команда	**switchport mode hybrid**
По умолчанию	Режим по умолчанию — Access (доступ), который можно изменить на Hybrid (гибридный)
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить значения по умолчанию для всех свойств гибридного порта, используйте команду **no switchport mode**

Определение разрешенных VLAN для гибридного порта

- Опционально.

- По умолчанию гибридный порт передает потоки из всех VLAN (от 1 до 4094). Вы можете настроить список разрешенных VLAN, чтобы запретить прохождение потоков некоторых VLAN через гибридный порт.
- Конфигурация:

Команда	**switchport hybrid allowed vlan** [[**add** | **only**] **tagged** | [**add**] **untaged** | **remove**] *vlan_list*
Описание параметров	*vlan-id*: указывает идентификатор VLAN
По умолчанию	По умолчанию гибридный порт принадлежит всем VLAN. Порт добавляется в VLAN по умолчанию в нетегированном виде и в другие VLAN в тегированном виде
Командный режим	Режим конфигурации интерфейса

Настройка Native VLAN

- Опционально.
- Если кадр содержит идентификатор VLAN Native VLAN, его тег будет автоматически удален при прохождении через гибридный порт.
- Конфигурация:

Команда	**switchport hybrid native vlan** *vlan_id*
Описание параметров	*vlan-id*: указывает идентификатор VLAN
По умолчанию	По умолчанию Native VLAN — это VLAN 1
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы восстановить исходную VLAN гибридного порта до значений по умолчанию, используйте команду **no switchport hybrid native vlan**

5.4.4.3. Проверка

- Отправляйте помеченные тегами пакеты на гибридный порт, и они транслируются в пределах указанных VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, вступила ли конфигурация в силу.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметров	*vlan-id*: указывает идентификатор VLAN

Командный режим	Любой режим
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- ---------- --------- ---------- 20 VLAN0020 STATIC Gi0/1

5.4.4.4. Пример конфигурации

Настройка гибридного порта

Шаги настройки	Ниже приведен пример настройки Gi0/1 в качестве гибридного порта
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode hybrid QTECH(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3 QTECH(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30 QTECH(config-if-GigabitEthernet 0/1)# end
Проверка	Проверьте правильность конфигурации
	QTECH(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration... Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode hybrid switchport hybrid native vlan 3 switchport hybrid allowed vlan add untagged 20-30

5.4.5. Настройка сервисного порта

5.4.5.1. Эффект конфигурации

В обычных случаях сервисный порт используется в среде перенаправления уровня 2. По умолчанию сервисный порт не изучает MAC-адреса и может пересылать пакеты из любой

VLAN. Кроме того, он развертывается в прозрачном режиме для перенаправления пакетов уровня 2 и уровня 3.

5.4.5.2. Шаги настройки

Настройка сервисного порта

- Обязательный.
- Выполните эту операцию, чтобы настроить порт в качестве сервисного порта.
- Выполните эту операцию на коммутаторе.

Команда	**switchport mode servicechain**
По умолчанию	Режим по умолчанию — Access (доступ)
Командный режим	Модель конфигурации интерфейса
Руководство по использованию	Перед изменением порта с порта доступа, магистрального, гибридного, uplink или туннельного порта 802.1Q на сервисный порт очистите другие конфигурации порта и сначала измените порт на порт доступа. Чтобы восстановить настройки по умолчанию, запустите **no switchport mode** в режиме конфигурации интерфейса

5.4.5.3. Проверка

Сервисный порт не изучает MAC-адрес, когда пакеты с тегами отправляются через сервисный порт. Кроме того, пакеты передаются независимо от переносимого тега и от того, создана ли VLAN.

5.4.5.4. Пример конфигурации

Настройка сервисного порта

ПРИМЕЧАНИЕ: описывается только конфигурация, относящаяся к сервисному порту.

Шаги настройки	Настройте порт Gi0/1 в качестве сервисного порта
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# switchport mode servicechain QTECH(config-if-GigabitEthernet 0/1)# end
Проверка	Запустите **show run**, чтобы проверить правильность конфигурации
	QTECH(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1 Building configuration…

	Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport switchport mode servicechain

5.4.6. Настройка унаследованной VLAN для независимого порта

5.4.6.1. Эффект конфигурации

Эту конфигурацию поддерживают только магистарльные, uplink и гибридные порты. После указания расширенного списка VLAN магистрального или uplink-порта, когда этот порт является AP, а порт-участник AP изменен на независимый порт, порт-участник использует расширенный список VLAN, настроенный на AP, в качестве списка разрешенных VLAN. Аналогичным образом, после указания расширенного списка VLAN гибридного порта этот расширенный список VLAN используется в качестве списка разрешенных VLAN гибридного порта-участника, а гибридный порт-участник, измененный на независимый порт, также наследует список тегов VLAN от AP.

5.4.6.2. Шаги настройки

Настройка унаследованной VLAN для независимого порта

- Обязательный.
- Выполните эту операцию на коммутаторе. В сценариях установки ОС PXE выполните эту операцию на AP.

Команда	**switchport individual-port extend-vlan** *vlan-list*
По умолчанию	Унаследованная VLAN не настроена по умолчанию
Командный режим	Режим конфигурации интерфейса порта коммутатора
Руководство по использованию	Чтобы отключить эту функцию, используйте команду **no switchport individual-port extend-vlan** или команду **default switchport individual-port extend-vlan**. Эту конфигурацию поддерживают только магистральные, uplink и гибридные порты

5.4.6.3. Проверка

Запустите команду **show run**, чтобы проверить, существует ли на интерфейсе команда **switchport individual-port extend-vlan**.

5.4.6.4. Пример конфигурации

Настройка унаследованной VLAN для независимого порта

ПРИМЕЧАНИЕ: описывается только конфигурация, относящаяся к унаследованным VLAN независимых портов.

Шаги настройки	Ниже приведен пример этой команды:
	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1) switchport mode trunk QTECH(config-if-GigabitEthernet 0/1) switchport individual-port extend-vlan 10
Проверка	Запустите команду **show run**, чтобы проверить правильность конфигурации
	QTECH(config-if-GigabitEthernet 0/1)#show run Building configuration… Current configuration : 166 bytes interface GigabitEthernet 0/1 switchport individual-port extend-vlan 10

5.5. Мониторинг

5.5.1. Отображение

Описание	Команда
Отображает конфигурацию VLAN	**show vlan**
Отображает конфигурацию портов коммутатора	**show interface switchport**

5.5.2. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Выключите отладки сразу после использования.

Описание	Команда
Отладка VLAN	**debug bridge vlan**

6. НАСТРОЙКА MAC VLAN

6.1. Обзор

Функция MAC VLAN относится к назначению VLAN на основе MAC-адресов, что является новым методом назначения VLAN. Эта функция часто используется с динамическим назначением VLAN 802.1X для реализации безопасного и гибкого доступа к терминалам 802.1X. После прохождения аутентификации пользователем 802.1X коммутатор доступа автоматически создает запись MAC VLAN на основе VLAN и MAC-адреса пользователя, переданных сервером аутентификации. Сетевой администратор также может заранее настроить связь между MAC-адресом и VLAN на коммутаторе.

6.1.1. Протоколы

IEEE 802.1Q: виртуальные мостовые локальные сети и стандарты

6.2. Приложения

Приложение	Описание
Настройка MAC VLAN	Настраивает функцию MAC VLAN для назначения сетей VLAN на основе MAC-адресов пользователей. При изменении физического местоположения пользователя, т. е. при переключении с одного коммутатора на другой, нет необходимости перенастраивать VLAN порта, используемого пользователем

6.2.1. Настройка MAC VLAN

6.2.1.1. Сценарий

С популяризацией мобильного офиса терминальные устройства обычно не используют фиксированные порты для доступа к сети. Терминальное устройство может использовать порт A для доступа к сети в этот раз, но использовать порт B для доступа к сети в следующий раз. Если конфигурации VLAN портов A и B отличаются, терминальное устройство будет назначено другой VLAN при втором доступе и не сможет использовать ресурсы предыдущей VLAN. Если конфигурации VLAN портов A и B одинаковы, могут возникнуть проблемы с безопасностью, когда порт B назначается другим оконечным устройствам. Как разрешить хостам разных VLAN доступ к сети через один и тот же порт? Настоящим представлена функция MAC VLAN.

Самое большое преимущество MAC VLAN заключается в том, что при изменении физического местоположения пользователя, т. е. при переключении с одного коммутатора на другой, нет необходимости перенастраивать VLAN порта, используемого пользователем. Таким образом, назначение VLAN на основе MAC-адресов можно рассматривать как пользовательское.

6.2.1.2. Развертывание

Настройте или отправьте записи MAC VLAN на коммутатор уровня 2 или беспроводное устройство, чтобы назначить VLAN на основе MAC-адресов пользователей.

6.3. Обзор

6.3.1. Особенность

Особенность	Описание
Настройка MAC VLAN	Настраивает функцию MAC VLAN для назначения сетей VLAN на основе MAC-адресов пользователей

6.3.2. Настройка MAC VLAN

6.3.2.1. Принцип работы

Когда коммутатор получает пакет, он сравнивает исходный MAC-адрес пакета с MAC-адресом, указанным в записи MAC VLAN. Если они совпадают, коммутатор пересылает пакет в сеть VLAN, указанную в записи MAC VLAN. Если они не совпадают, VLAN, к которой принадлежит поток данных, по-прежнему определяется правилом назначения VLAN порта.

Чтобы убедиться, что ПК назначен в указанную VLAN независимо от того, к какому коммутатору он подключен, вы можете выполнить настройку, используя следующие подходы:

- Статическая конфигурация с помощью команд. Вы можете настроить связь между MAC-адресом и VLAN на локальном коммутаторе с помощью команд.
- Автоматическая настройка с использованием сервера аутентификации (динамическое назначение VLAN 802.1X). После того, как пользователь проходит аутентификацию, коммутатор динамически создает связь между MAC-адресом и VLAN на основе информации, предоставленной сервером аутентификации. Когда пользователь выходит из сети, коммутатор автоматически удаляет связь. Этот подход требует, чтобы ассоциация MAC-VLAN была настроена на сервере аутентификации. Подробнее о назначении динамической VLAN 802.1X см. в разделе Настройка 802.1X.

Записи MAC VLAN поддерживают оба подхода, то есть записи можно настроить как на локальном коммутаторе, так и на сервере аутентификации. Конфигурации могут вступить в силу только в том случае, если они согласованы. Если конфигурации отличаются, вступает в силу конфигурация, выполненная ранее.

ПРИМЕЧАНИЕ: функцию MAC VLAN можно настроить только на гибридных портах.

ПРИМЕЧАНИЕ: записи MAC VLAN эффективны только для нетегированных пакетов, но не для тегированных пакетов.

ПРИМЕЧАНИЕ: для записей MAC VLAN, настроенных статически или динамически созданных, указанные VLAN должны существовать.

ПРИМЕЧАНИЕ: VLAN, указанные в записях MAC VLAN, не могут быть Super VLAN (но могут быть SubVLAN), удаленными VLAN или первичными VLAN (но могут быть вторичными VLAN).

ПРИМЕЧАНИЕ: MAC-адреса, указанные в записях MAC VLAN, должны быть unicast.

ПРИМЕЧАНИЕ: MAC VLAN эффективны для всех гибридных портов, для которых включена функция MAC VLAN.

6.4. Конфигурация

Конфигурация	Описание и команда	
Включение MAC VLAN на порту	(Обязательно) Используется для включения функции MAC VLAN на порту	
	mac-vlan enable	Включает MAC VLAN на порту
Глобальное добавление статической записи MAC VLAN	(Опционально) Используется для привязки MAC-адресов к VLAN	
	mac-vlan mac-address	Настраивает статическую запись MAC VLAN

6.4.1. Включение MAC VLAN на порту

6.4.1.1. Эффект конфигурации

Включите функцию MAC VLAN на порту, чтобы записи MAC VLAN могли действовать на порту.

6.4.1.2. Шаги настройки

Включение MAC VLAN на порту

- Обязательный.
- По умолчанию функция MAC VLAN отключена на портах, и все записи MAC VLAN не действуют на портах.
- Включите MAC VLAN на коммутаторе.

Команда	**mac-vlan enable**
По умолчанию	Функция MAC VLAN отключена на порту
Командный режим	Режим конфигурации интерфейса

6.4.1.3. Проверка

Запустите команду **show mac-vlan interface**, чтобы отобразить информацию о портах, включенных с помощью функции MAC VLAN.

Команда	**show mac-vlan interface**
Командный режим	Привилегированный режим конфигурации/Глобальный режим конфигурации/Режим конфигурации интерфейса

Отображение команд	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: --- FastEthernet 0/1

6.4.1.4. Пример конфигурации

Включение MAC VLAN на порту

Шаги настройки	Включите функцию MAC VLAN на порту Fast Ethernet 0/10
	QTECH# configure terminal QTECH(config)# interface FastEthernet0/10 QTECH(config-if-FastEthernet 0/10)# mac-vlan enable
Проверка	Проверьте информацию о порте, включенном с помощью функции MAC VLAN
	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: --- FastEthernet 0/10

6.4.1.5. Распространенные ошибки

Когда функция MAC VLAN включена для порта, порт не настраивается заранее как порт уровня 2 (например, порт коммутации или порт AP).

6.4.2. Глобальное добавление статической записи MAC VLAN

6.4.2.1. Эффект конфигурации

Настройте статическую запись MAC VLAN для привязки MAC-адресов к VLAN. Можно настроить приоритет 802.1p, который по умолчанию равен 0.

6.4.2.2. Шаги настройки

Добавление статической записи MAC VLAN

- Опционально.
- Чтобы связать MAC-адреса с VLAN, вы должны выполнить эту настройку. Можно настроить приоритет 802.1p, который по умолчанию равен 0.
- Добавьте статическую запись MAC VLAN на коммутаторе.

Команда	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]
Описание параметров	**mac-address** *mac-address*: указывает MAC-адрес. **mask** *mac-mask*: обозначает маску. **vlan** *vlan-id*: указывает связанную сеть VLAN. **priority** *pri_val*: указывает приоритет
По умолчанию	По умолчанию запись статического MAC-адреса VLAN не настроена
Командный режим	Режим глобальной конфигурации

ПРИМЕЧАНИЕ: если нетегированный пакет сопоставляется с записью MAC VLAN, пакет изменяется на VLAN, указанную записью MAC VLAN, после прибытия на коммутатор, поскольку запись MAC VLAN имеет наивысший приоритет. Последующие функции и протоколы реализуются на основе измененной VLAN. Возможные воздействия следующие:

ПРИМЕЧАНИЕ: если пользователь 802.1X не проходит аутентификацию, гибридный порт переходит к сети VLAN 100, указанной функцией FAIL VLAN; однако статически настроенная запись MAC VLAN перенаправляет все пакеты этого пользователя в VLAN 200. Следовательно, пользователь не может реализовать нормальную связь в FAIL VLAN 100.

ПРИМЕЧАНИЕ: после того, как нетегированный пакет сопоставляется с записью MAC VLAN, VLAN, которая инициирует изучение MAC-адреса, становится VLAN перенаправленной на основе записи MAC VLAN.

ПРИМЕЧАНИЕ: для порта, для которого включена функция MAC VLAN, если полученные пакеты совпадают как с записями MAC VLAN с полными F-масками, так и с записями без полных F-масок, пакеты обрабатываются на основе записей MAC VLAN без полных F-масок.

ПРИМЕЧАНИЕ: если нетегированный пакет соответствует как записи MAC VLAN, так и записи VOICE VLAN, приоритет пакета изменяется одновременно. Приоритет записи VOICE VLAN используется как приоритет пакета.

ПРИМЕЧАНИЕ: если нетегированный пакет совпадает как с записью MAC VLAN, так и с записью PROTOCOL VLAN, VLAN, передаваемая в пакете, должна быть MAC VLAN.

ПРИМЕЧАНИЕ: функция MAC VLAN применяется только к нетегированным пакетам, но не применяется к пакетам PRIORITY (пакетам с тегом VLAN равным 0 и содержащим информацию COS PRIORITY), а действия по обработке неопределенны.

ПРИМЕЧАНИЕ: модель доверия пакетов QoS на коммутаторе по умолчанию отключена, что изменит PRIORITY всех пакетов на 0 и перезапишет изменение приоритетов пакетов функцией MAC VLAN. Запустите команду **mls qos trust cos** в режиме конфигурации интерфейса, чтобы включить модель доверия QoS и доверительные приоритеты пакетов.

Удаление всех статических записей MAC VLAN

- Опционально.
- Чтобы удалить все статические записи MAC VLAN, вы должны выполнить эту настройку.

- Выполните эту настройку на коммутаторе.

Команда	**no mac-vlan all**
Командный режим	Режим глобальной конфигурации

Удаление записи статической MAC VLAN для указанного MAC-адреса

- Опционально.
- Чтобы удалить запись MAC VLAN для указанного MAC-адреса, вы должны выполнить эту настройку.
- Выполните эту настройку на коммутаторе.

Команда	**no mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]
Описание параметров	**mac-address** *mac-address*: указывает MAC-адрес. **mask** *mac-mask*: обозначает маску
Командный режим	Режим глобальной конфигурации

Удаление статической записи MAC VLAN для указанной VLAN

- Необязательный.
- Чтобы удалить запись MAC VLAN указанной VLAN, вы должны выполнить эту настройку.
- Выполните эту настройку на коммутаторе.

Команда	**no mac-vlan vlan** *vlan-id*
Описание параметров	**vlan** *vlan-id*: указывает VLAN
Командный режим	Режим глобальной конфигурации

6.4.2.3. Проверка

- Запустите команду **show mac-vlan static**, чтобы проверить правильность всех статических записей MAC VLAN.
- Запустите команду **show mac-vlan vlan** *vlan-id*, чтобы проверить правильность записи MAC VLAN указанной VLAN.
- Запустите команду **show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*], чтобы отобразить запись MAC VLAN для указанного MAC-адреса.

Команда	**show mac-vlan static** **show mac-vlan vlan** *vlan-id* **show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]
Описание параметров	**vlan** *vlan-id*: указывает указанную сеть VLAN. **mac-address** *mac-address*: указывает указанный MAC-адрес. **mask** *mac-mask*: указывает указанную маску
Командный режим	Привилегированный режим конфигурации/Глобальный режим конфигурации/Режим конфигурации интерфейса
Отображение команд	QTECH# show mac-vlan all The following MAC VLAN address exist: S: Static D: Dynamic MAC ADDR MASK VLAN ID PRIO STATE ---------- 0000.0000.0001 ffff.ffff.ffff 2 0 D 0000.0000.0002 ffff.ffff.ffff 3 3 S 0000.0000.0003 ffff.ffff.ffff 3 3 S&D Total MAC VLAN address count: 3

6.4.2.4. Пример конфигурации

Глобальное добавление статической записи MAC VLAN

Как показано на Рисунке 6-1, ПК-A1 и ПК-A2 принадлежат отделу A и назначены сети VLAN 100. ПК-B1 и ПК-B2 принадлежат отделу B и назначены сети VLAN 200. Из-за мобильности сотрудников Компания предоставляет временный офис в комнате для совещаний, но требует, чтобы сотрудники, к которым осуществляется доступ, были назначены на виртуальные локальные сети их собственных отделов. Например, ПК-A1 должен быть назначен для VLAN 100, а ПК-B1 должен быть назначен для VLAN 200 после доступа.

Поскольку порты доступа для ПК в конференц-зале не являются фиксированными, функция MAC VLAN может использоваться для связывания MAC-адресов ПК с VLAN их отделов. Независимо от того, какие порты сотрудники используют для доступа, функция MAC VLAN автоматически назначает виртуальные локальные сети их отделов.

Сценарий:

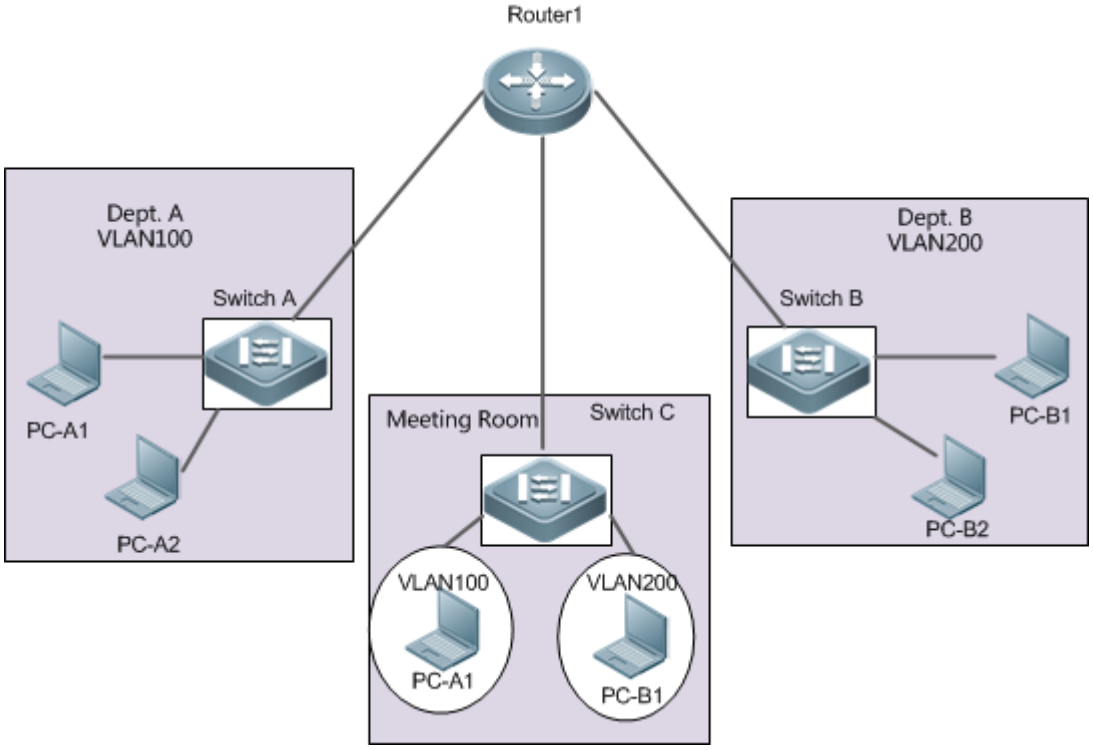


Рисунок 6-1.

Шаги настройки	• Настройте порт, соединяющий коммутатор C и маршрутизатор 1, в качестве магистрального порта. • Настройте все порты, соединяющие ПК на коммутаторе C, как гибридные порты, включите функцию MAC VLAN и измените список нетегированных VLAN по умолчанию. • Настройте записи MAC VLAN на коммутаторе C
A	A# configure terminal A(config)# interface interface_name A(config-if)# switchport mode trunk A(config-if)# exit A(config)# interface interface_name A(config-if)# switchport mode hybrid A(config-if)# switchport hybrid allowed vlan add untagged 100,200 A(config-if)# mac-vlan enable A(config-if)# exit A(config)# mac-vlan mac-address PC-A1-mac vlan 100 A(config)# mac-vlan mac-address PC-B1-mac vlan 200
Проверка	Проверьте настроенные статические записи MAC VLAN на коммутаторе C

A	A# QTECH# show mac-vlan static The following MAC VLAN address exist: S: Static D: Dynamic MAC ADDR MASK VLAN ID PRIO STATE --- PC-A1-macffff.ffff.ffff 100 0 S PC-B1-macffff.ffff.ffff 200 3 S Total MAC VLAN address count: 2

6.4.3. Мониторинг

6.4.4. Отображение

Описание	Команда
Отображает все записи MAC VLAN, включая статические и динамические	**show mac-vlan all**
Отображает динамические записи MAC VLAN	**show mac-vlan dynamic**
Отображает статические записи MAC VLAN	**show mac-vlan static**
Отображает записи MAC VLAN указанной VLAN	**show mac-vlan vlan** *vlan-id*
Отображает записи MAC VLAN для указанного MAC-адреса	**show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]

6.4.5. Отладка

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

Описание	Команда
Отладка функцию MAC VLAN	**debug bridge mvlan**

7. НАСТРОЙКА SUPER VLAN

7.1. Обзор

Супер виртуальная локальная сеть (Super VLAN) — это подход к разделению VLAN. Super VLAN также называется агрегацией VLAN и представляет собой технологию управления, предназначенную для оптимизации IP-адресов.

Использование Super VLAN может значительно сэкономить IP-адреса. Для Super VLAN, состоящей из нескольких SubVLAN, необходимо назначить только один IP-адрес, что значительно экономит IP-адреса и упрощает управление сетью.

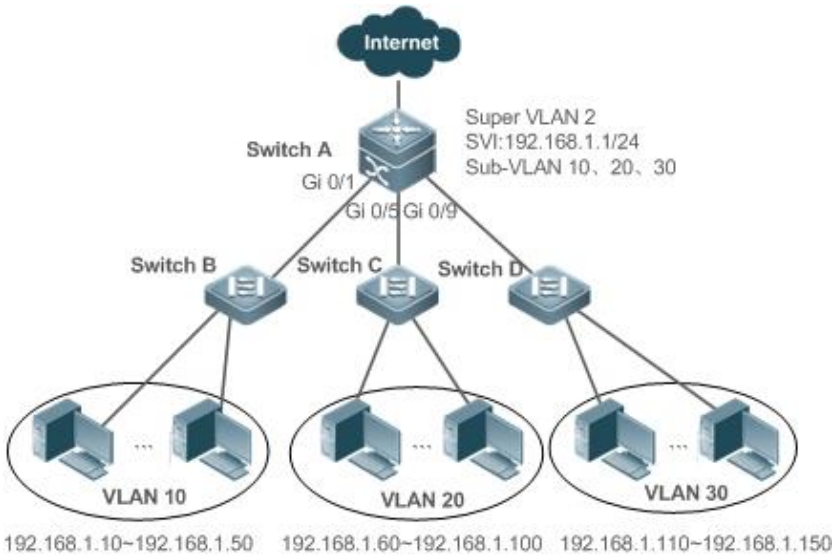
7.2. Приложение

Приложение	Описание
Совместное использование одного IP-шлюза несколькими VLAN	Сети VLAN разделены для реализации изоляции пользователей доступа уровня 2 (L2). Все пользователи VLAN совместно используют один IP-шлюз для реализации связи уровня 3 (L3) и связи с внешними сетями

7.2.1. Совместное использование одного IP-шлюза несколькими VLAN

7.2.1.1. Сценарий

Несколько VLAN изолированы на L2 на устройстве L3, но пользователи этих VLAN могут осуществлять связь L3 друг с другом в одном и том же сегменте сети.



Коммутатор A является шлюзом или коммутатором ядра.

Коммутатор B, коммутатор C и коммутатор D являются коммутаторами доступа.

На коммутаторе A настроены Super VLAN и несколько SubVLAN, а интерфейс L3 и IP-адрес интерфейса L3 настроены для Super VLAN.

VLAN 10 настроен на коммутаторе B, VLAN 20 настроен на коммутаторе C, а VLAN 30 настроен на коммутаторе D. Различные отделы компании находятся в разных VLAN.

7.2.1.2. Развертывание

В интрасети используйте Super VLAN, чтобы несколько SubVLAN могли совместно использовать один IP-шлюз, а в то же время VLAN были взаимно изолированы на уровне L2.

Пользователи в SubVLAN могут осуществлять связь L3 через шлюз Super VLAN.

7.3. Функции

7.3.1. Базовые определения

Super VLAN

Super VLAN также называется агрегацией VLAN и представляет собой технологию управления, предназначенную для оптимизации IP-адресов. Он объединяет несколько VLAN в один сегмент IP-сети. В Super VLAN нельзя добавить физический порт. Виртуальный интерфейс коммутатора (SVI) используется для управления обменом данными между VLAN между SubVLAN. Super VLAN нельзя использовать как обычную VLAN 802.1Q, но ее можно рассматривать как первичную VLAN для SubVLAN.

SubVLAN

SubVLAN — это независимый broadcast-домен. SubVLAN'ы взаимно изолированы на уровне L2. Пользователи SubVLAN одной или разных Super VLAN взаимодействуют друг с другом через L3 SVI своих собственных Super VLAN.

ARP-прокси

SVI L3 можно создать только для Super VLAN. Пользователи в SubVLAN взаимодействуют с пользователями в других подсетях той же самой Super VLAN или пользователями в других сегментах сети через прокси-сервер ARP и L3 SVI Super VLAN. Когда пользователь SubVLAN отправляет запрос ARP пользователю другой SubVLAN, шлюз Super VLAN использует свой собственный MAC-адрес для отправки или ответа на запросы ARP. Этот процесс называется ARP-прокси.

Диапазон IP-адресов SubVLAN

В зависимости от IP-адреса шлюза, настроенного для Super VLAN, можно настроить диапазон IP-адресов для каждой SubVLAN.

7.3.2. Обзор

Особенность	Описание
Super VLAN	Создайте интерфейс L3 в качестве SVI, чтобы позволить всем SubVLAN совместно использовать один и тот же сегмент IP-сети через ARP-прокси

7.3.3. Super VLAN

Пользователям всех SubVLAN Super VLAN могут быть назначены IP-адреса в одном диапазоне IP-адресов, и они могут использовать один и тот же IP-шлюз. Через этот шлюз пользователи могут осуществлять обмен данными между VLAN. Нет необходимости выделять шлюз для каждой VLAN, что сохраняет IP-адреса.

7.3.3.1. Принцип работы

IP-адреса в сетевом сегменте выделяются разным SubVLAN, принадлежащим одной и той же Super VLAN. Каждая SubVLAN имеет независимый broadcast-домен VLAN, а разные SubVLAN изолированы друг от друга на уровне L2. Когда пользователям в SubVLAN необходимо выполнить связь L3, IP-адрес SVI Super VLAN используется в качестве адреса шлюза. Таким образом, несколько VLAN используют один и тот же IP-шлюз, и нет необходимости настраивать шлюз для каждой VLAN. Кроме того, для реализации связи L3 между подсетями VLAN и между SubVLAN и другими сегментами сети используется функция ARP-прокси для пересылки и обработки запросов и ответов ARP.

Связь уровня 2 SubVLAN: если SVI не настроен для Super VLAN, SubVLAN Super VLAN взаимно изолированы на уровне L2, то есть пользователи в разных SubVLAN не могут общаться друг с другом. Если SVI настроен для Super VLAN, а шлюз Super VLAN может функционировать как ARP-прокси, пользователи в разных SubVLAN одной и той же Super VLAN могут взаимодействовать друг с другом. Это связано с тем, что IP-адреса пользователей в разных SubVLAN относятся к одному и тому же сегменту сети, и связь между этими пользователями по-прежнему рассматривается как связь L2.

Коммуникация L3 SubVLAN: если пользователям в SubVLAN Super VLAN необходимо выполнить связь L3 между сегментами сети, шлюз этой Super VLAN функционирует как ARP-прокси для ответа на запросы ARP вместо SubVLAN.

7.4. Конфигурация

Элемент конфигурации	Описание и команда	
Настройка основных функций Super VLAN	Обязательный	
	supervlan	Настраивает Super VLAN
	subvlan *vlan-id-list*	Настраивает SubVLAN
	proxy-arp	Включает функцию ARP-прокси
	interface vlan *vlan-id*	Создает виртуальный интерфейс для Super VLAN
	ip address *ip mask*	Настраивает IP-адрес виртуального интерфейса Super VLAN
	Опционально	
	subvlan-address-range *start-ip end-ip*	указывает диапазон IP-адресов в SubVLAN

7.4.1. Настройка основных функций Super VLAN

7.4.1.1. Эффект конфигурации

Включите функцию super VLAN и настройте SVI для super VLAN, чтобы реализовать связь L2/L3 между SubVLAN через VLAN.

Пользователи во всех SubVLAN Super VLAN используют один и тот же IP-шлюз. Нет необходимости указывать сегмент сети для каждой VLAN, в которой сохраняются IP-адреса.

7.4.1.2. Примечания

Super VLAN не принадлежит какому-либо физическому порту. Таким образом, устройство, настроенное для работы с Super VLAN, не может обрабатывать пакеты, содержащие тег super VLAN.

Должны быть включены как функция Super VLAN, так и функция ARP-прокси каждой SubVLAN.

SVI и IP-адрес должны быть настроены для Super VLAN. SVI — это виртуальный интерфейс, используемый для связи пользователей во всех SubVLAN.

7.4.1.3. Шаги настройки

Настройка Super VLAN

- Обязательный.
- В Super VLAN нет физического порта.
- Функция ARP-прокси должна быть включена. Эта функция включена по умолчанию.
- Вы можете запустить команду **supervlan**, чтобы изменить обычную VLAN на Super VLAN.
- После того как обычная VLAN станет Super VLAN, порты, добавленные в эту VLAN, будут удалены из этой VLAN, поскольку в Super VLAN не существует физического порта.

ПРИМЕЧАНИЕ: Super VLAN действительна только после настройки дополнительных VLAN для этой Super VLAN.

ПРИМЕЧАНИЕ: VLAN 1 нельзя настроить как Super VLAN.

ПРИМЕЧАНИЕ: Super VLAN не может быть настроена как SubVLAN другой Super VLAN. SubVLAN Super VLAN нельзя настроить как Super VLAN.

Команда	**supervlan**
По умолчанию	По умолчанию VLAN является общей VLAN
Командный режим	Режим конфигурации VLAN

Руководство по использованию	По умолчанию функция Super VLAN отключена. В Super VLAN нельзя добавить физический порт. Как только VLAN не является Super VLAN, все ее SubVLAN становятся обычными статическими VLAN

Настройка виртуального интерфейса для Super VLAN

- Обязательный.
- В Super VLAN нельзя добавить физический порт. Вы можете настроить SVI L3 для VLAN.

ПРИМЕЧАНИЕ: когда Super VLAN конфигурируется с помощью SVI, он выделяет интерфейс L3 для каждой SubVLAN. Если для SubVLAN не выделен интерфейс L3 из-за нехватки ресурсов, SubVLAN снова становится общей VLAN.

Команда	**interface vlan** *vlan-id*
Описание параметров	*vlan-id*: указывает идентификатор Super VLAN
По умолчанию	По умолчанию ни один Super VLAN не настроен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Интерфейс L3 должен быть настроен как виртуальный интерфейс Super VLAN

Настройка шлюза Super VLAN

- Обязательный.
- Шлюз IP на SVI L3 настроен как прокси-сервер для всех пользователей в SubVLAN для ответа на запросы ARP.

Команда	**ip address** *ip mask*
Описание параметров	*ip*: указывает IP-адрес шлюза на виртуальный интерфейс Super VLAN. *mask*: обозначает маску
По умолчанию	По умолчанию шлюз не настроен для Super VLAN
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы настроить шлюз для Super VLAN. Пользователи всех SubVLAN Super VLAN совместно используют этот шлюз

Настройка SubVLAN

- Обязательный.
- Физические порты могут быть добавлены в SubVLAN. SubVLAN Super VLAN совместно используют адрес шлюза Super VLAN и находятся в одном сегменте сети.
- Функция ARP-прокси должна быть включена. Эта функция включена по умолчанию.
- Вы можете запустить команду **subvlan** *vlan-id-list*, чтобы изменить обычную VLAN на SubVLAN Super VLAN. Физические порты могут быть добавлены в SubVLAN.
- Коммуникация пользователей в SubVLAN управляется Super VLAN.

ПРИМЕЧАНИЕ: вы должны изменить SubVLAN на общую VLAN, прежде чем сможете удалить эту SubVLAN, выполнив команду **no vlan**.

ПРИМЕЧАНИЕ: одна SubVLAN принадлежит только одной Super VLAN.

Команда	**subvlan** *vlan-id-list*
Описание параметров	*vlan-id-list*: указывает несколько VLAN в качестве SubVLAN Super VLAN
По умолчанию	По умолчанию VLAN является обычной VLAN
Командный режим	Режим конфигурации VLAN
Руководство по использованию	Интерфейсы подключения могут быть добавлены в SubVLAN. Вы должны изменить SubVLAN на общую VLAN, прежде чем сможете удалить эту SubVLAN, выполнив команду **no vlan** [*id*]. Вы не можете настроить SVI уровня 3 VLAN для SubVLAN. **ПРИМЕЧАНИЕ:** если вы настроили SVI уровня 3 для Super VLAN, попытка добавления дополнительных SubVLAN может завершиться неудачей из-за нехватки ресурсов. **ПРИМЕЧАНИЕ:** если вы настроите SubVLAN на Super VLAN, а затем настроите SVI уровня 3 VLAN для Super VLAN, некоторые SubVLAN могут снова стать общими VLAN из-за нехватки ресурсов

Настройка ARP-прокси

- (Обязательно) Функция ARP-прокси включена по умолчанию.
- Пользователи в SubVLAN могут реализовать связь L2/L3 между виртуальными локальными сетями через прокси-сервер шлюза только после того, как функция ARP-прокси включена как в Super VLAN, так и в SubVLAN.
- Пользователи в SubVLAN могут общаться с пользователями других VLAN только после того, как функция ARP-прокси включена как в Super VLAN, так и в SubVLAN.

ПРИМЕЧАНИЕ: функция ARP-прокси должна быть включена как в Super VLAN, так и в SubVLAN. В противном случае эта функция не действует.

Команда	**proxy-arp**
По умолчанию	По умолчанию функция ARP-прокси включена
Командный режим	Режим конфигурации VLAN
Руководство по использованию	По умолчанию функция ARP-прокси включена. Запустите эту команду, чтобы включить функцию ARP-прокси как в Super VLAN, так и в SubVLAN. Пользователи в SubVLAN могут реализовать связь L2/L3 между виртуальными локальными сетями только после того, как функция ARP-прокси будет включена как в Super VLAN, так и в SubVLAN

Настройка диапазона IP-адресов SubVLAN

- Вы можете выделить диапазон IP-адресов для каждой SubVLAN. Пользователи в SubVLAN могут общаться с пользователями других VLAN, только если их IP-адреса находятся в указанном диапазоне.
- Если не указано иное, вам не нужно настраивать диапазон IP-адресов.

ПРИМЕЧАНИЕ: IP-адреса, динамически выделяемые пользователям через DHCP, могут не входить в диапазон выделенных IP-адресов. Если IP-адреса, выделенные через DCHP, не входят в указанный диапазон, пользователи в SubVLAN не могут общаться с пользователями других VLAN. Поэтому будьте осторожны при использовании команды **subvlan-address-range** *start-ip end-ip*.

ПРИМЕЧАНИЕ: диапазон IP-адресов SubVLAN должен находиться в пределах диапазона IP-адресов Super VLAN, к которой принадлежит SubVLAN. В противном случае пользователи SubVLAN не могут взаимодействовать друг с другом.

ПРИМЕЧАНИЕ: IP-адреса пользователей в SubVLAN должны находиться в пределах диапазона IP-адресов SubVLAN. В противном случае пользователи в SubVLAN не смогут взаимодействовать друг с другом.

Команда	**subvlan-address-range** *start-ip end-ip*
Описание параметров	*start-ip*: указывает начальный IP-адрес SubVLAN. *end-ip*: указывает конечный IP-адрес SubVLAN
По умолчанию	По умолчанию диапазон IP-адресов не настроен
Командный режим	Режим конфигурации VLAN

Руководство по использованию	Опционально. Запустите эту команду, чтобы настроить диапазон IP-адресов пользователей в SubVLAN. Диапазоны IP-адресов разных SubVLAN Super VLAN не могут перекрываться друг с другом. **ПРИМЕЧАНИЕ:** диапазон IP-адресов SubVLAN должен находиться в пределах диапазона IP-адресов SubVLAN, к которой принадлежит SubVLAN. В противном случае пользователи в SubVLAN не смогут взаимодействовать друг с другом. **ПРИМЕЧАНИЕ:** пользователи в SubVLAN могут общаться с пользователями других VLAN только в том случае, если их IP-адреса (динамически выделяемые через DHCP или статически настроенные) находятся в настроенном диапазоне IP-адресов. **ПРИМЕЧАНИЕ:** IP-адреса, назначенные через DHCP, могут не входить в настроенный диапазон IP-адресов. В этом случае пользователи SubVLAN не могут общаться с пользователями других VLAN. Поэтому будьте осторожны при использовании этой команды

7.4.1.4. Проверка

После того, как каждая SubVLAN сопоставлена со шлюзом Super VLAN, пользователи SubVLAN могут отправлять эхо-запросы друг другу.

7.4.1.5. Пример конфигурации

Настройка Super VLAN в сети, чтобы пользователи в ее SubVLAN использовали один и тот же сегмент сети и совместно использовали один и тот же IP-шлюз для сохранения IP-адресов

Сценарий:

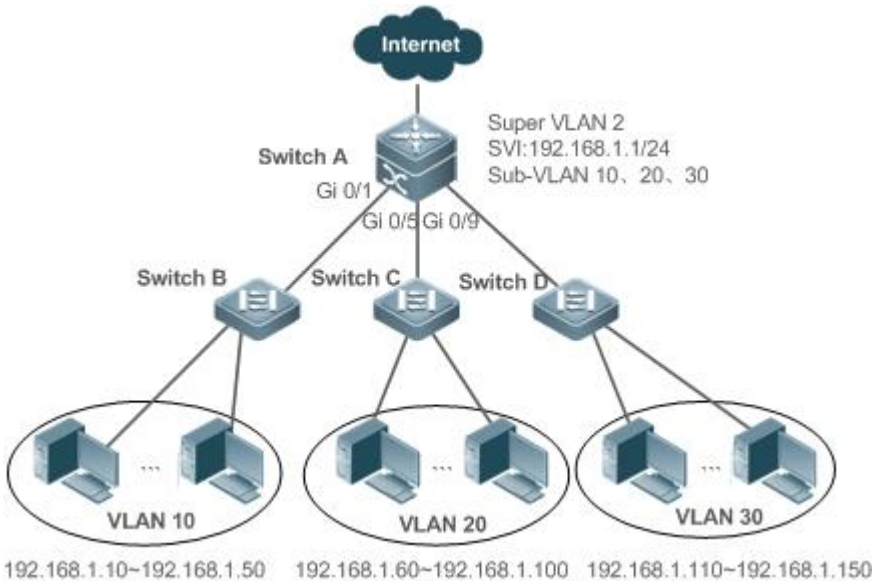


Рисунок 7-1.

Шаги настройки	Выполните соответствующую настройку Super VLAN на коммутаторе ядра. На коммутаторах доступа настройте общие сети VLAN, соответствующие SubVLAN на коммутаторе ядра
A	SwitchA#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. SwitchA(config)#vlan 2 SwitchA(config-vlan)#exit SwitchA(config)#vlan 10 SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#exit SwitchA(config)#vlan 2 SwitchA(config-vlan)#supervlan SwitchA(config-vlan)#subvlan 10,20,30 SwitchA(config-vlan)#exit SwitchA(config)#interface vlan 2 SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0 SwitchA(config)#vlan 10 SwitchA(config-vlan)#subvlan-address-range 192.168.1.10 192.168.1.50 SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#subvlan-address-range 192.168.1.60 192.168.1.100 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#subvlan-address-range 192.168.1.110 192.168.1.150 SwitchA(config)#interface range gigabitEthernet 0/1,0/5,0/9 SwitchA(config-if-range)#switchport mode trunk
Проверка	Убедитесь, что исходный хост (192.168.1.10) и конечный хост (192.168.1.60) могут проверить связь друг с другом

A	SwitchA(config-if-range)#show supervlan supervlan id supervlan arp-proxy subvlan id subvlan arp-proxy subvlan ip range ---------- ---------- ---------- ---------- --------- 2 ON 10 ON 192.168.1.10 - 192.168.1.50 20 ON 192.168.1.60 - 192.168.1.100 30 ON 192.168.1.110 - 192.168.1.150

7.4.1.6. Распространенные ошибки

Шлюз SVI и IP не настроен для Super VLAN. Следовательно, происходит сбой связи между SubVLAN и между SubVLAN и другими виртуальными локальными сетями.

Функция ARP-прокси отключена в Super VLAN или SubVLAN. Следовательно, пользователи в SubVLAN не могут общаться с пользователями других VLAN.

Диапазон IP-адресов SubVLAN настроен, но IP-адреса, выделенные пользователям, не входят в этот диапазон.

7.5. Мониторинг

7.5.1. Отображение

Описание	Команда
Отображает конфигурацию Super VLAN	**show supervlan**

7.5.2. Отладка

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

Описание	Команда
Отладка Super VLAN	**debug bridge svlan**

8. НАСТРОЙКА PROTOCOL VLAN

8.1. Обзор

Технология Protocol VLAN — это технология распределения VLAN, основанная на типе пакетного протокола. Он может распределять пакеты определенного типа протокола с нулевым идентификатором VLAN в ту же VLAN. То есть коммутатор на основе типа протокола и формата инкапсуляции пакетов, полученных портами, сопоставляет полученные нетегированные пакеты с профилями протоколов. Если сопоставление прошло успешно, коммутатор автоматически распределяет пакеты по соответствующей VLAN для передачи. Существует два типа Protocol VLAN: Protocol VLAN на основе IP-адресов и Protocol VLAN на основе типа пакета и типа Ethernet на портах. Protocol VLAN, основанная на типе пакета и типе Ethernet на портах, для краткости называется Protocol VLAN, а Protocol VLAN на основе IP-адреса для краткости называется VLAN подсети.

ПРИМЕЧАНИЕ: Protocol VLAN применима только к транковым портам и гибридным портам.

8.1.1. Протоколы и стандарты

Стандарт IEEE 802.1Q

8.2. Приложения

Приложение	Описание
Конфигурация и применение Protocol VLAN	Реализует коммуникационную изоляцию 2-го уровня для пользовательских хостов, которые используют пакеты разных протоколов для связи, чтобы уменьшить сетевой трафик
Конфигурация и применение VLAN подсети	Указывает диапазон VLAN на основе сегмента IP-сети, к которому принадлежат пользовательские пакеты

8.2.1. Конфигурация и применение Protocol VLAN

8.2.1.1. Сценарий

Как показано на следующем Рисунке, сетевая архитектура состоит из взаимосвязанных сервера Windows NT и сервера Novell Netware, а офисная зона подключена к коммутатору A устройства уровня 3 через хаб. В офисе есть разные компьютеры. Некоторые ПК используют операционную систему (ОС) Windows NT и поддерживают протокол IP, а некоторые ПК используют ОС Novell Netware и поддерживают протокол IPX. ПК в офисе обмениваются данными с внешней сетью и серверами через uplink-порт Gi 0/3.

Основные требования следующие:

- Связь уровня 2 ПК, использующих ОС Windows NT, изолирована от связи ПК, использующих ОС Novell Netware, чтобы уменьшить сетевой трафик.

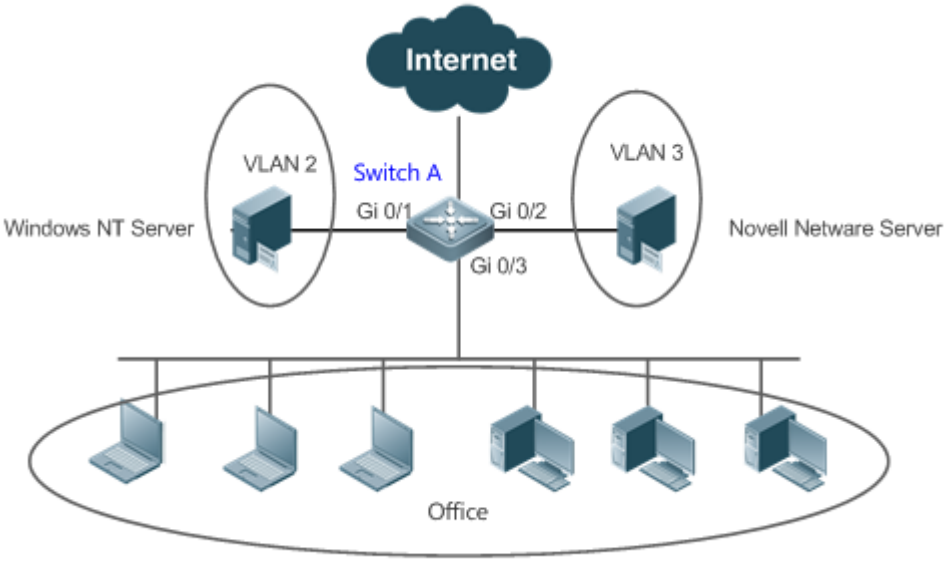


Рисунок 8-1.

Коммутатор A — это коммутатор, а порт Gi 0/3 — гибридный порт. Порт Gi 0/1 является портом доступа и принадлежит сети VLAN 2. Порт Gi 0/2 также является портом доступа и принадлежит сети VLAN 3.

8.2.1.2. Развертывание

- Настройте профили типа пакета и типа Ethernet (в этом примере настройте профиль 1 для пакетов протокола IP и настройте профиль 2 для пакетов протокола IPX).
- Примените профили к uplink-порту (в этом примере порт Gi 0/3) и свяжите их с виртуальными локальными сетями (в этом примере свяжите профиль 1 с VLAN 2 и свяжите профиль 2 с VLAN 3).

ПРИМЕЧАНИЕ: настроенные Protocol VLAN действуют только на магистральных (транковых) и гибридных портах.

8.2.2. Конфигурация и применение VLAN подсети

8.2.2.1. Сценарий

Как показано на следующем Рисунке, ПК в офисе A и офисе B подключены к коммутатору A устройства уровня 3 через хабы. В офисе A ПК принадлежат фиксированному сетевому сегменту и распределены по портам в одну и ту же VLAN. В офисе B ПК принадлежат к двум сетевым сегментам, но их нельзя распределить по VLAN через фиксированный порт.

Основные требования следующие:

Для ПК в офисе B коммутатор A может определить диапазон VLAN для ПК на основе сегмента IP-сети, к которому принадлежат их пакеты.

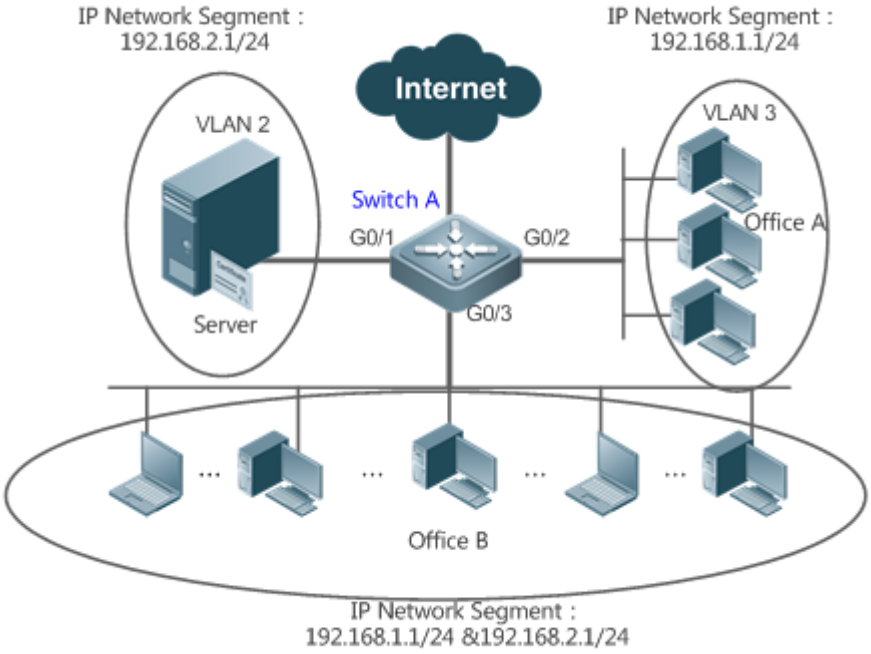


Рисунок 8-2.

Коммутатор A — это коммутатор. Порт G0/1 является портом доступа и принадлежит сети VLAN 2. Порт G0/2 также является портом доступа и принадлежит сети VLAN 3. Порт G0/3 является гибридным портом.

8.2.2.2. Развертывание

Глобально настройте VLAN подсети (в этом примере выделите сегмент IP-сети 192.168.1.1/24 для VLAN 3 и сегмент IP-сети 192.168.2.1/24 для VLAN 2) и включите функцию VLAN подсети на порте uplink (порт Gi 0). /3 в этом примере).

ПРИМЕЧАНИЕ: настроенные VLAN подсети действуют только на магистральных и гибридных портах.

8.3. Функции

8.3.1. Базовые определения

Protocol VLAN

Технология Protocol VLAN — это технология распределения VLAN, основанная на типе пакетного протокола. Он может распределять пакеты определенного типа протокола с нулевым идентификатором VLAN в ту же VLAN.

VLAN необходимо указывать для пакетов, получаемых портами устройств, чтобы пакет принадлежал уникальной VLAN. Возможны три случая:

- Если пакет содержит нулевой идентификатор VLAN (нетегированный или приоритетный пакет), а устройство поддерживает только распределение VLAN на основе портов, идентификатор VLAN в теге, добавленном к пакету, представляет собой PVID входного порта.
- Если пакет содержит нулевой идентификатор VLAN (нетегированный или приоритетный пакет), а устройство поддерживает распределение VLAN на основе типа протокола пакета, идентификатор VLAN в теге, добавленном к пакету,

выбирается из идентификаторов VLAN, сопоставленных с конфигурацией набора протоколов входного порта. Если тип протокола пакета не соответствует конфигурации всех наборов протоколов входного порта, идентификатор VLAN назначается в соответствии с распределением VLAN на основе портов.

- Если пакет помечен тегом, VLAN, к которой принадлежит пакет, определяется идентификатором VLAN в теге.

VLAN подсети можно настроить только глобально, то есть на портах можно включить или отключить только функцию Protocol VLAN. Конфигурация сопоставления выполняется глобально для Protocol VLAN, конфигурация сопоставления выбирается для портов, а идентификаторы VLAN указываются для пакетов, которые успешно сопоставлены.

- Если входной пакет содержит нулевой идентификатор VLAN и IP-адрес входного пакета совпадает с IP-адресом, пакет распространяется в VLAN подсети.
- Если входной пакет содержит нулевой идентификатор VLAN, а тип пакета и тип Ethernet входного пакета совпадают с типом пакета и типом Ethernet входного порта, пакет назначается протоколу VLAN.

Приоритет Protocol VLAN

Приоритет VLAN подсети выше, чем у Protocol VLAN. То есть, если VLAN подсети и Protocol VLAN настроены одновременно, а входной пакет соответствует как VLAN подсети, так и Protocol VLAN, превалирует VLAN подсети.

8.3.1.1. Обзор

Особенность	Описание
Автоматическое распределение VLAN на основе типа пакета	Типы услуг, поддерживаемые в сети, связаны с виртуальными локальными сетями, или пакеты из указанного сегмента IP-сети передаются в указанной виртуальной локальной сети для облегчения управления и обслуживания

8.3.2. Автоматическое распределение VLAN на основе типа пакета

8.3.2.1. Принцип работы

Установите правила для оборудования и включите правила для портов. Правила вступают в силу только после их включения на портах. Правила включают тип пакета и IP-адрес пакетов. Когда порт получает нетегированные пакеты данных, соответствующие правилам, порт автоматически распределяет их по VLAN, указанным в правилах для передачи. Когда правила для портов отключены, непомеченные пакеты данных распределяются по Native VLAN в соответствии с конфигурацией порта.

8.4. Конфигурация

Конфигурация	Описание и команда	
Настройка функции Protocol VLAN	(Обязательно) Используется для включения функции распределения VLAN на основе типа пакета и типа Ethernet Protocol VLAN	
	protocol-vlan profile *num* **frame-type** [*type*] **ether-type** [*type*]	Настраивает профиль типа пакета и типа Ethernet
	protocol-vlan profile *num* **ether-type** [*type*]	Настраивает профиль типа Ethernet (некоторые модели не поддерживают идентификацию фрейма)
	protocol-vlan profile *num* **vlan** *vid*	(Режим конфигурации интерфейса) Применяет Protocol VLAN к порту
Настройка функции VLAN подсети	(Обязательный) Используется для включения функции распределения VLAN на основе IP-адреса Protocol VLAN	
	protocol-vlan ipv4 *address* **mask** *address* **vlan** *vid*	Настраивает IP-адрес, маску подсети и распределение VLAN
	protocol-vlan ipv4	(Режим конфигурации интерфейса) Включает SubVLAN на порту

8.4.1. Настройка функции Protocol VLAN

8.4.1.1. Эффект конфигурации

Свяжите поддерживаемые в сети типы сервисов с виртуальными локальными сетями для облегчения управления и обслуживания.

8.4.1.2. Примечания

- Рекомендуется, чтобы Protocol VLAN настраивался после VLAN, а также настраивались атрибуты Trunk, Hybrid, Access и AP портов.
- Если Protocol VLAN настроен на магистральном порту или гибридном порту, все виртуальные локальные сети, относящиеся к Protocol VLAN, должны содержаться в списке разрешенных VLAN магистрального порта или гибридного порта.

8.4.1.3. Шаги настройки

Глобальная настройка Protocol VLAN

- Обязательный.
- Protocol VLAN можно применять на интерфейсе только в режиме глобальной конфигурации.

Команда	**protocol-vlan profile** *num* **frame-type** [*type*] **ether-type** [*type*]
Описание параметров	*num*: указывает индекс профиля. *type*: указывает тип пакета и тип Ethernet
По умолчанию	Protocol VLAN отключен по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Protocol VLAN можно настроить на интерфейсе, только если Protocol VLAN настроен глобально. При удалении глобальной конфигурации профиля Protocol VLAN конфигурация Protocol VLAN удаляется со всех интерфейсов, соответствующих профилю Protocol VLAN

Переключение режима порта на магистральный/гибридный режим

Обязательный. Функция Protocol VLAN действует только на порты, которые находятся в магистральном/гибридном режиме (Trunk/Hybrid).

Включение Protocol VLAN на порту

- Обязательный. Protocol VLAN отключен по умолчанию.
- Protocol VLAN действительно включен только тогда, когда он применяется к интерфейсам.

Команда	**protocol-vlan profile** *num* **vlan** *vid*
Описание параметров	*num*: указывает индекс профиля. *vid*: указывает идентификатор VLAN. Значение 1 указывает максимальный идентификатор VLAN, поддерживаемый продуктом
По умолчанию	Protocol VLAN отключен по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Интерфейс должен работать в режиме Trunk/Hybrid

8.4.1.4. Проверка

Запустите команду **show protocol-vlan profile**, чтобы проверить конфигурацию.

8.4.1.5. Пример конфигурации

Включение функции Protocol VLAN в топологической среде

Сценарий:

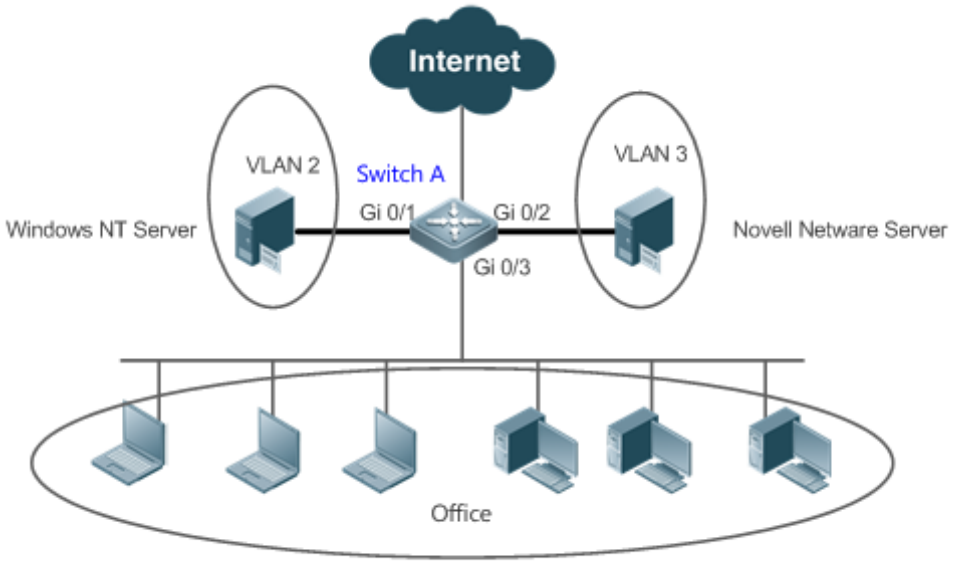


Рисунок 8-3.

Шаги настройки	• Настройте VLAN 2 и VLAN 3 для связи пользователей на коммутаторе A. • Настройте Protocol VLAN глобально на коммутаторе A (в этом примере настройте профиль 1 для пакетов протокола IP и настройте профиль 2 для пакетов протокола IPX), включите функцию Protocol VLAN на порте uplink (в данном примере порт Gi 0/3), и завершите соединение Protocol VLAN (в этом примере свяжите профиль 1 с VLAN 2 и свяжите профиль 2 с VLAN 3). • Порт Gi 0/1 является портом доступа и принадлежит сети VLAN 2. Порт Gi 0/2 также является портом доступа и принадлежит сети VLAN 3. Порт Gi 0/3 является гибридным портом. Убедитесь, что VLAN для связи с пользователем содержатся в списке разрешенных нетегированных VLAN гибридного порта

A	1. Создайте VLAN 2 и VLAN 3 для связи пользователей по сети.
	
	`# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`A(config)# vlan range 2-3`
	
	2. Настройте режим порта.
	`A(config)#interface gigabitEthernet 0/1`

	A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3 3. Настройте Protocol VLAN глобально. Настройте профиль 1 для пакетов протокола IP и профиль 2 для пакетов протокола IPX (в этом примере предполагается, что пакеты инкапсулированы с использованием Ethernet II, а типы пакетов протокола IP и пакетов протокола IPX Ethernet — 0X0800 и 0X8137 соответственно). A(config)#protocol-vlan profile 1 frame-type ETHERII ether-type 0x0800 A(config)#protocol-vlan profile 2 frame-type ETHERIIether-type 0x8137 4. Примените профиль 1 и профиль 2 к портам Gi 0/3 и назначьте профиль 1 — для сети VLAN 2, а профиль 2 — для сети VLAN 3. A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 1 vlan 2 A(config-if-GigabitEthernet 0/3) #protocol-vlan profile 2 vlan 3
Проверка	Проверьте правильность конфигурации Protocol VLAN на устройстве
A	A(config)#show protocol-vlan profile Profile frame-type ether-type/DSAP+SSAP interface vlan ------- ---------- ---------- ---------- ---- 1 ETHERII 0x0800 Gi0/3 2 2 ETHERII 0x8137 Gi0/3 3

8.4.1.6. Распространенные ошибки

- Порт, подключенный к устройству, не находится в режиме Trunk/Hybrid.
- Список разрешенных VLAN для порта, подключенного к устройству, не содержит VLAN для связи с пользователем.

- Функция Protocol VLAN отключена на порту.

8.4.2. Настройка функции VLAN подсети

8.4.2.1. Эффект конфигурации

Распределять пакеты из указанного сегмента сети или IP-адреса в указанную сеть VLAN для передачи.

8.4.2.2. Примечания

- Рекомендуется, чтобы Protocol VLAN настраивался после VLAN, а также настраивались атрибуты Trunk, Hybrid, Access и AP портов.
- Если Protocol VLAN настроен на магистральном порту или гибридном порту, все виртуальные локальные сети, относящиеся к Protocol VLAN, должны содержаться в списке разрешенных VLAN магистрального порта или гибридного порта.

8.4.2.3. Шаги настройки

Глобальная настройка VLAN подсети

- Обязательный.
- VLAN подсети можно применить к интерфейсу только в режиме глобальной конфигурации.

Команда	**protocol-vlan ipv4** *address* **mask** *address* **vlan** *vid*
Описание параметров	*address*: указывает IP-адрес. *vid*: указывает идентификатор VLAN. Значение 1 указывает максимальный идентификатор VLAN, поддерживаемый продуктом
По умолчанию	По умолчанию VLAN подсети отключен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	VLAN подсети можно включить на интерфейсе, даже если Protocol VLAN не включен глобально. Тем не менее, VLAN подсети действует только тогда, когда Protocol VLAN настроен глобально

Переключение режима порта на магистральный/гибридный режим

- Обязательный. Функция VLAN подсети действует только на порты, которые находятся в режиме Trunk/Hybrid.

Включение VLAN подсети на порту

- Обязательный. По умолчанию VLAN подсети отключен.
- VLAN подсети действительно включен только тогда, когда он применяется к интерфейсам.

Команда	**protocol-vlan ipv4**
По умолчанию	По умолчанию VLAN подсети отключен

Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Интерфейс должен работать в режиме Trunk/Hybrid

8.4.2.4. Проверка

Запустите команду **show protocol-vlan ipv4**, чтобы проверить конфигурацию.

8.4.2.5. Пример конфигурации

Включение функции VLAN подсети в топологической среде

Сценарий:

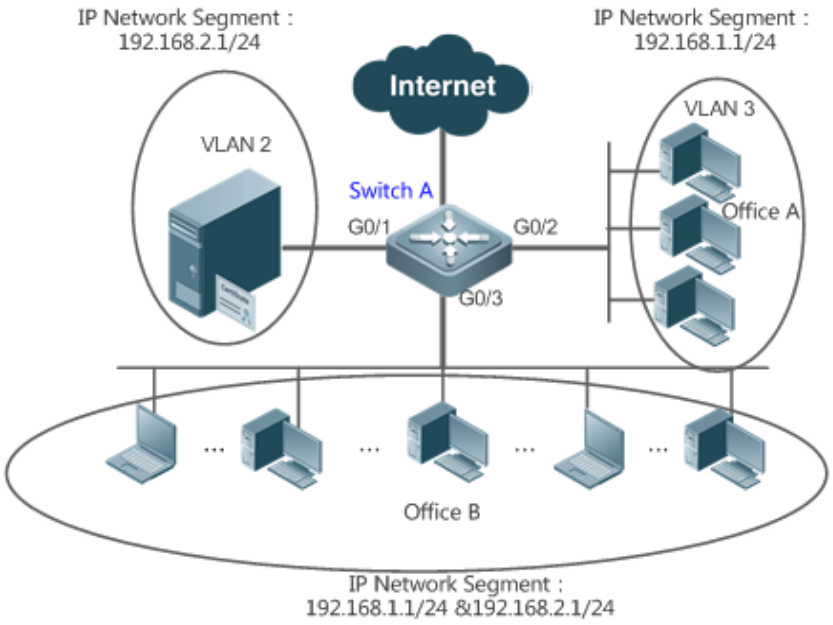


Рисунок 8-4.

Шаги настройки	• Настройте VLAN 2 и VLAN 3 для связи пользователей на коммутаторе A. • Глобально настройте VLAN подсети на коммутаторе A (в этом примере выделите сегмент IP-сети 192.168.1.1/24 для VLAN 3 и сегмент IP-сети 192.168.2.1/24 для VLAN 2) и включите функцию VLAN подсети на порте uplink (Порт Gi 0/3 в этом примере). • Порт Gi 0/1 является портом доступа и принадлежит сети VLAN 2. Порт Gi 0/2 также является портом доступа и принадлежит сети VLAN 3. Порт Gi 0/3 является гибридным портом. Убедитесь, что VLAN для связи с пользователем содержатся в списке разрешенных нетегированных VLAN гибридного порта

A	1. Создайте VLAN 2 и VLAN 3 для связи пользователей по сети. A# configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. A(config)# vlan range 2-3 2. Настройте режим порта. A(config)#interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)#switchport A(config-if-GigabitEthernet 0/1)#switchport access vlan 2 A(config-if-GigabitEthernet 0/1)#exit A(config)#interface gigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#switchport A(config-if-GigabitEthernet 0/2)#switchport access vlan 3 A(config-if-GigabitEthernet 0/2)#exit A(config)# interface gigabitEthernet 0/3 A(config-if-GigabitEthernet 0/3)#switchport A(config-if-GigabitEthernet 0/3)# switchport mode hybrid A(config-if-GigabitEthernet 0/3)# switchport hybrid allowed vlan untagged 2-3 3. Настройте VLAN подсети глобально. A(config)# protocol-vlan ipv4 192.168.1.0 mask 255.255.255.0 vlan 3 A(config)# protocol-vlan ipv4 192.168.2.0 mask 255.255.255.0 vlan 2 4. Включите VLAN подсети на интерфейсах. По умолчанию VLAN подсети отключен. (config-if-GigabitEthernet 0/3)# protocol-vlan ipv4
Проверка	Проверьте правильность конфигурации VLAN подсети на устройстве
A	A# show protocol-vlan ipv4 ip mask vlan --- --- ---- ---- 192.168.1.0 255.255.255.0 3 192.168.2.0 255.255.255.0 2 interface ipv4 status --- ---

	Gi0/3	enable

8.4.2.6. Распространенные ошибки

- Порт, подключенный к устройству, не находится в режиме Trunk/Hybrid.
- Список разрешенных VLAN для порта, подключенного к устройству, не содержит VLAN для связи с пользователем.
- VLAN подсети отключен на порту.

8.5. Мониторинг

8.5.1. Отображение

Описание	Команда
Отображает содержимое Protocol VLAN	**show protocol-vlan**

8.5.2. Отладка

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

Описание	Команда
Отладка Protocol VLAN	**debug bridge protvlan**

9. НАСТРОЙКА PRIVATE VLAN

9.1. Обзор

Private VLAN делит broadcast-домен уровня 2 VLAN на несколько поддоменов. Каждый поддомен состоит из одной пары Private VLAN: первичной VLAN и вторичной VLAN.

Один домен Private VLAN может состоять из нескольких пар Private VLAN, и каждая пара Private VLAN представляет один субдомен. В домене Private VLAN все пары Private VLAN используют одну и ту же первичную VLAN. Вторичные идентификаторы VLAN для поддоменов отличаются.

Если поставщик услуг выделяет одну сеть VLAN каждому пользователю, количество пользователей, которое может поддерживаться поставщиком услуг, ограничивается, поскольку одно устройство поддерживает не более 4096 сетей VLAN. На устройстве уровня 3 каждой VLAN выделяется один адрес подсети или серия адресов, что приводит к потере IP-адресов. Технология Private VLAN правильно решает две предыдущие проблемы. Private VLAN в дальнейшем для краткости называется PVLAN.

9.2. Приложения

Приложение	Описание
Применение PVLAN между устройствами уровня 2	Пользователи предприятия могут общаться друг с другом, но взаимодействие пользователей между предприятиями изолировано
Применение PVLAN на одном устройстве уровня 3	Все корпоративные пользователи используют один и тот же адрес шлюза и могут взаимодействовать с внешней сетью

9.2.1. Применение PVLAN между устройствами уровня 2

9.2.1.1. Сценарий

Как показано на следующем Рисунке, в операционной сети службы хостинга хосты корпоративных пользователей подключены к сети через коммутатор A или коммутатор B. Основные требования следующие:

- Пользователи предприятия могут общаться друг с другом, но взаимодействие пользователей между предприятиями изолировано.
- Все корпоративные пользователи используют один и тот же адрес шлюза и могут взаимодействовать с внешней сетью.

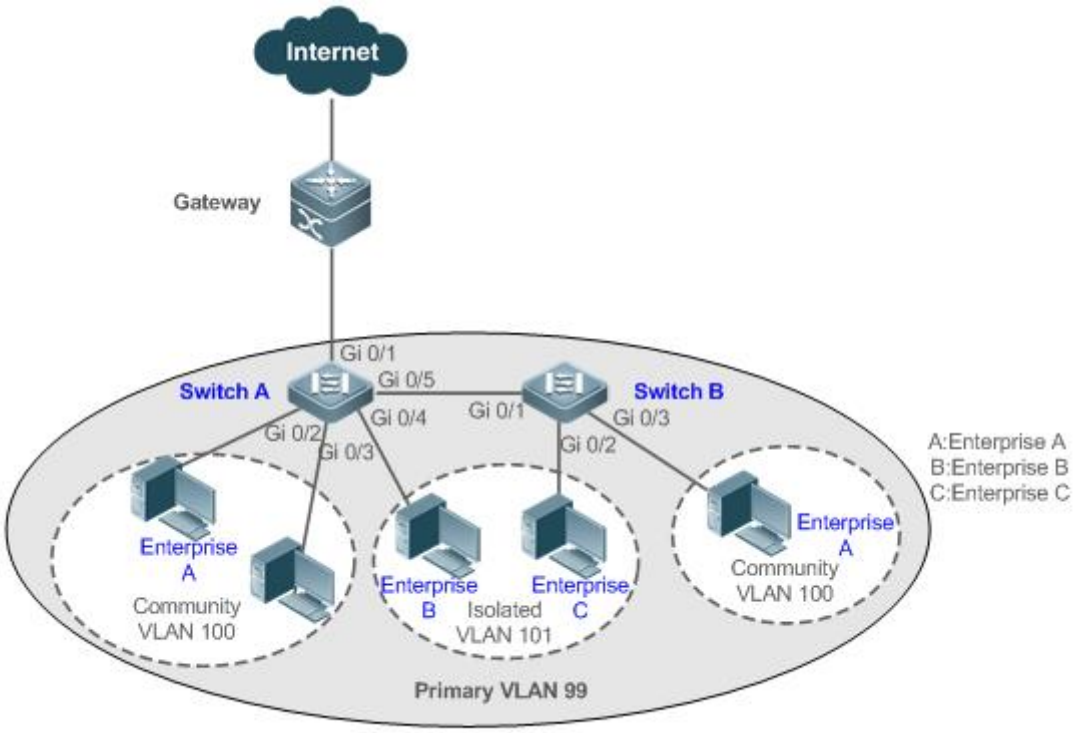


Рисунок 9-1.

Коммутатор A и коммутатор B являются коммутаторами доступа.

PVLAN работает на устройствах. Порты для подключения устройств должны быть настроены как магистральные порты, то есть порт Gi 0/5 коммутатора A и порт Gi 0/1 коммутатора B настроены как магистральные порты.

Порт Gi 0/1 для подключения коммутатора A к шлюзу необходимо настроить как неразборчивый порт (promiscuous-порт).

Порт Gi 0/1 шлюза можно настроить как магистральный или гибридный порт, а Native VLAN является основной VLAN для PVLAN.

9.2.1.2. Развертывание

- Настройте все предприятия так, чтобы они находились в одной и той же PVLAN (основная VLAN 99 в этом примере). Все корпоративные пользователи используют один и тот же интерфейс уровня 3 через эту VLAN для связи с внешней сетью.
- Если на предприятии имеется несколько пользовательских хостов, распределите пользовательские хосты разных предприятий по разным VLAN сообщества. То есть настройте порты, подключенные к хостам пользователей предприятия, в качестве портов хостов VLAN сообщества, чтобы реализовать взаимодействие пользователей внутри предприятия, но изолировать взаимодействие пользователей между предприятиями.
- Если на предприятии имеется только один пользовательский хост, настройте порты, подключенные к пользовательским хостам таких предприятий, как порты хостов изолированной VLAN, чтобы реализовать изоляцию взаимодействия пользователей между предприятиями.

9.2.2. Применение PVLAN на одном устройстве уровня 3

Как показано на следующем Рисунке, в операционной сети службы хостинга хосты корпоративных пользователей подключаются к сети через коммутатор A устройства уровня 3. Основные требования следующие:

- Пользователи предприятия могут общаться друг с другом, но взаимодействие пользователей между предприятиями изолировано.
- Все корпоративные пользователи могут получить доступ к серверу.
- Все корпоративные пользователи используют один и тот же адрес шлюза и могут взаимодействовать с внешней сетью.

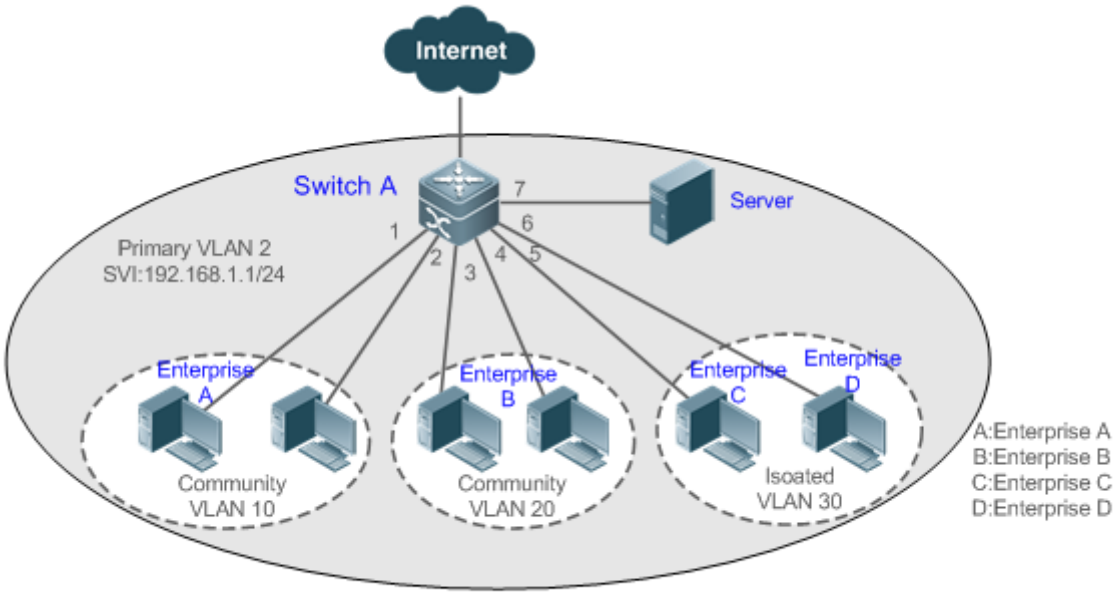


Рисунок 9-2.

Коммутатор A является коммутатором шлюза.

Когда пользовательские хосты подключены к одному устройству, порт Gi 0/7 для подключения к серверу настраивается как случайный порт, чтобы корпоративные пользователи могли взаимодействовать с сервером.

Сопоставление уровня 3 должно быть выполнено в первичной VLAN и вторичных VLAN, чтобы пользователи могли взаимодействовать с внешней сетью.

9.2.2.1. Развертывание

- Настройте порт, который напрямую подключен к серверу, как неразборчивый порт. После этого все корпоративные пользователи смогут взаимодействовать с сервером через неразборчивый порт.
- Настройте адрес шлюза PVLAN на устройстве уровня 3 (коммутатор A в этом примере) (в этом примере установите адрес SVI VLAN 2 на 192.168.1.1/24) и настройте сопоставление между первичной VLAN и вторичными VLAN на интерфейс уровня 3. После этого все корпоративные пользователи смогут взаимодействовать с внешней сетью через адрес шлюза.

9.3. Функции

9.3.1. Базовые определения

PVLAN

PVLAN поддерживает три типа VLAN: первичные VLAN, изолированные VLAN и VLAN сообщества.

Домен PVLAN имеет только одну основную VLAN. Вторичные VLAN реализуют изоляцию уровня 2 в том же домене PVLAN. Существует два типа вторичных VLAN.

Изолированная VLAN

Порты в одной и той же изолированной VLAN не могут взаимно устанавливать связь уровня 2. Домен PVLAN имеет только одну изолированную VLAN.

VLAN сообщества

Порты в одной VLAN сообщества могут устанавливать связь уровня 2 друг с другом, но не могут осуществлять связь уровня 2 с портами в других VLAN сообщества. Домен PVLAN может иметь несколько VLAN сообщества.

Ассоциация уровня 2 PVLAN

Пары PVLAN существуют только после того, как будет выполнена ассоциация уровня 2 между тремя типами VLAN PVLAN. Затем первичная VLAN имеет указанную вторичную VLAN, а вторичная VLAN имеет указанную первичную VLAN. Первичная VLAN и вторичные VLAN находятся в отношениях «один ко многим» (one-to-many).

Ассоциация уровня 3 PVLAN

В PVLAN интерфейсы уровня 3, то есть коммутируемые виртуальные интерфейсы (SVI), могут быть созданы только в первичной VLAN. Пользователи во вторичной VLAN могут установить связь уровня 3 только после того, как будет выполнена ассоциация уровня 3 между вторичной VLAN и первичной VLAN. В противном случае пользователи могут осуществлять связь только на уровне 2.

Порт сообщества

Порты сообщества — это порты в сети VLAN сообщества. Порты сообщества в одной VLAN сообщества могут взаимодействовать друг с другом и могут взаимодействовать с неразборчивыми портами. Они не могут обмениваться данными с портами сообщества в других VLAN сообщества или изолированными портами в изолированной сети VLAN.

Неразборчивый порт (promiscuous-порт)

Неразборчивые порты — это порты в первичной VLAN. Они могут взаимодействовать с любыми портами, включая изолированные порты и порты сообщества во вторичных VLAN того же домена PVLAN.

ПРИМЕЧАНИЕ: в PVLAN SVI можно создавать только в первичной VLAN, а SVI нельзя создавать во вторичных VLAN.

ПРИМЕЧАНИЕ: порты в PVLAN можно использовать в качестве портов источника зеркалирования, но нельзя использовать в качестве портов назначения зеркалирования.

9.3.1.1. Обзор

Особенность	Описание
Изоляция уровня 2 PVLAN и сохранение IP-адреса	Порты различных типов PVLAN можно настроить для реализации взаимодействия и изоляции промежуточных пользовательских хостов VLAN
	После выполнения сопоставления уровня 2 между первичной VLAN и вторичными VLAN поддерживается только связь уровня 2. Если требуется связь уровня 3, пользователям вторичной VLAN необходимо использовать SVI первичной VLAN для осуществления связи уровня 3

9.3.2. Изоляция уровня 2 PVLAN и сохранение IP-адреса

Добавьте пользователей в поддомены PVLAN, чтобы изолировать связь между предприятиями и между корпоративными пользователями.

9.3.2.1. Принцип работы

Настройте PVLAN, настройте ассоциацию уровня 2 и ассоциацию уровня 3 между основной VLAN и SubVLAN PVLAN, а также настройте порты, подключенные к пользовательским хостам, внешним сетевым устройствам и серверам, как различные типы портов PVLAN. Таким образом может быть реализовано разделение поддоменов и связь пользователей в поддоменах с внешней сетью и серверами.

Отношения пересылки пакетов между портами разных типов

Выходной порт Входной порт	Неразборчивый порт	Изолированный порт	Порт сообщества
Неразборчивый порт	Поддерживается	Поддерживается	Поддерживается
Изолированный порт	Поддерживается	Не поддерживается	Не поддерживается
Порт сообщества	Поддерживается	Не поддерживается	Поддерживается
Изолированный магистральный порт (в той же VLAN)	Поддерживается	Не поддерживается	Поддерживается
Неразборчивый магистральный порт (в той же VLAN)	Поддерживается	Поддерживается	Поддерживается
Магистральный порт (в той же VLAN)	Поддерживается	Поддерживается	Поддерживается

Изменения тега VLAN после пересылки пакетов между портами разных типов

Выходной порт **Входной порт**	**Неразборчивый порт**	**Изолированный порт**	**Порт сообщества**	**ЦП коммутатора**
Неразборчивый порт	Без изменений	Без изменений	Без изменений	Снять тег
Изолированный порт	Без изменений	нет данных	нет данных	Снять тег
Порт сообщества	Без изменений	нет данных	Без изменений	Снять тег
Изолированный магистральный порт (в той же VLAN)	Добавляется вторичный идентификатор VLAN	нет данных	Добавляется тег идентификатора VLAN сообщества	Добавляется вторичный тег идентификатора VLAN
Неразборчивый магистральный порт (в той же VLAN)	Добавляется первичный тег идентификатора VLAN, а тег VLAN остается неизменным в сети, отличной от PVLAN	Добавляется первичный тег идентификатора VLAN, а тег VLAN остается неизменным в сети, отличной от PVLAN	Добавляется первичный тег идентификатора VLAN, а тег VLAN остается неизменным в сети, отличной от PVLAN	Добавляется первичный тег идентификатора VLAN, а тег VLAN остается неизменным в сети, отличной от PVLAN
Магистральный порт (в той же VLAN)	Добавляется первичный тег идентификатора VLAN	Добавлен изолированный тег идентификатора VLAN	Добавлен тег идентификатора VLAN сообщества	Добавляется первичный тег идентификатора VLAN

9.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций PVLAN	(Обязательно) Используется для настройки первичной VLAN и вторичных VLAN	
	private-vlan {**community** | **isolated** | **primary**}	Настраивает тип PVLAN
	(Обязательный) Он используется для настройки ассоциации уровня 2 между первичной VLAN и вторичными VLAN PVLAN для формирования пар PVLAN	
	private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	Настраивает ассоциацию уровня 2 между первичной VLAN и вторичными VLAN для формирования пар PVLAN
	(Опционально) Он используется для распределения пользователей по изолированной VLAN или VLAN сообщества	
	switchport mode private-vlan host	Настраивает хост-порт PVLAN
	switchport private-vlan host-association *p_vid s_vid*	Связывает порты уровня 2 с PVLAN и выделяет порты поддоменам
	(Опционально) Используется для настройки порта как неразборчивого порта	
	switchport mode private-vlan promiscuous	Настраивает неразборчивый порт PVLAN
	switchport private-vlan mapping *p_vid* { *svlist* | **add** *svlist* | **remove** *svlist* }	Настраивает первичную VLAN, к которой принадлежит неразборчивый порт PVLAN, и список вторичных сетей VLAN. Пакеты PVLAN могут передаваться или приниматься через этот порт только после выполнения настройки

Конфигурация	Описание и команда	
Настройка основных функций PVLAN	(Опционально) Он используется для настройки связи уровня 3 для пользователей во вторичной VLAN	
	private-vlan mapping { *svlist* | **add** *svlist* | **remove** *svlist* }	Настраивает SVI первичной VLAN и настраивает ассоциацию уровня 3 между первичной VLAN и вторичными VLAN после создания PVLAN и выполнения ассоциации уровня 2. Пользователи в SubVLAN могут устанавливать связь уровня 3 через SVI первичной VLAN

9.4.1. Настройка основных функций PVLAN

9.4.1.1. Эффект конфигурации

- Включите формирование поддоменов PVLAN для реализации изоляции между предприятиями и между корпоративными пользователями.
- Реализуйте сопоставление уровня 3 между несколькими вторичными VLAN и первичной VLAN, чтобы несколько VLAN использовали один и тот же IP-шлюз, тем самым помогая сохранить IP-адреса.

9.4.1.2. Примечания

- После настройки первичной VLAN и вторичной VLAN поддомен PVLAN существует только после того, как между ними будет выполнена ассоциация уровня 2.
- Порт, подключенный к хосту использования, должен быть настроен как определенный порт PVLAN, чтобы хост пользователя присоединялся к поддомену для реализации реальной изоляции пользователя.
- Порт, подключенный к внешней сети, и порт, подключенный к серверу, должны быть настроены как неразборчивые порты, чтобы upstream- и downstream-пакеты пересылались нормально.
- Пользователи во вторичной VLAN могут установить связь уровня 3 через SVI первичной VLAN только после того, как будет выполнено сопоставление уровня 3 между вторичной VLAN и первичной VLAN.

9.4.1.3. Шаги настройки

Настройка PVLAN

- Обязательный.
- Необходимо настроить первичную VLAN и вторичную VLAN. Два типа VLAN не могут существовать независимо друг от друга.
- Запустите **private-vlan** { **community** | **isolated** | **primary** } для настройки VLAN в качестве первичной VLAN для PVLAN и других VLAN в качестве вторичных VLAN.

Команда	**private-vlan** { **community** | **isolated** | **primary** }
Описание параметров	**community**: указывает, что тип VLAN — это VLAN сообщества. **isolated**: указывает, что тип VLAN — изолированная VLAN. **primary**: указывает, что тип VLAN является основной VLAN пары PVLAN
По умолчанию	Сети VLAN являются обычными сетями VLAN и не имеют атрибутов PVLAN
Командный режим	Режим VLAN
Руководство по использованию	Эта команда используется для указания первичной VLAN и вторичных VLAN PVLAN

Настройка ассоциации уровня 2 PVLAN

- Обязательный.
- Поддомены PVLAN формируются, а изолированные порты, общие порты и ассоциация уровня 3 могут быть настроены только после того, как ассоциация уровня 2 будет выполнена между первичной VLAN и вторичными VLAN PVLAN.
- По умолчанию после настройки различных PVLAN первичные VLAN и вторичные VLAN не зависят друг от друга. Первичная VLAN имеет вторичную VLAN, а вторичная VLAN имеет первичную VLAN только после выполнения ассоциации уровня 2.
- Запустите **private-vlan association** { *svlist* | **add** *svlist* | **remove** *svlist* } для настройки или отмены ассоциации уровня 2 между первичной VLAN и вторичными VLAN PVLAN. Поддомен PVLAN формируется только после настройки ассоциации уровня 2. Поддомен PVLAN не существует после отмены ассоциации уровня 2. Если ассоциация уровня 2 не выполняется, когда для настройки связанных пар PVLAN используются изолированные порты и неразборчивые порты, конфигурация завершится ошибкой или ассоциация между портами и сетями VLAN будет отменена.

Команда	**private-vlan association** { *svlist* | **add** *svlist* | **remove** *svlist* }
Описание параметров	*svlist*: указывает список вторичных сетей VLAN, которые необходимо связать или разъединить. **add** *svlist*: добавляет вторичные VLAN для связывания. **remove** *svlist*: отменяет связь между *svlist* и первичной VLAN
По умолчанию	По умолчанию первичная VLAN и вторичная VLAN не связаны
Командный режим	Основной режим VLAN PVLAN

Руководство по использованию	Эта команда используется для настройки ассоциации уровня 2 между первичной VLAN и вторичными VLAN для формирования пар PVLAN. Каждая первичная VLAN может быть связана только с одной изолированной сетью VLAN, но может быть связана с несколькими сетями VLAN сообщества

Настройка ассоциации уровня 3 PVLAN

- Если пользователям в домене вторичной VLAN необходимо установить связь уровня 3, настройте SVI интерфейса уровня 3 для первичной VLAN, а затем настройте ассоциацию уровня 3 между первичной VLAN и вторичными VLAN на SVI.
- По умолчанию SVI можно настроить только в первичной VLAN. Вторичные VLAN не поддерживают связь уровня 3.
- Если пользователям во вторичной сети VLAN PVLAN необходимо установить связь уровня 3, SVI первичной сети VLAN необходимо использовать для передачи и приема пакетов.
- Запустите **private-vlan mapping** { *svlist* | **add** *svlist* | **remove** *svlist* } для настройки или отмены ассоциации уровня 3 между первичной VLAN и вторичными VLAN PVLAN. Пользователи во вторичной VLAN могут устанавливать связь уровня 3 с внешней сетью только после настройки ассоциации уровня 3. После отмены ассоциации уровня 3 пользователи вторичной VLAN не могут осуществлять связь уровня 3.

Команда	**private-vlan mapping** { *svlist* | **add** *svlist* | **remove** *svlist* }
Описание параметров	*svlist*: указывает список вторичных сетей VLAN, для которых необходимо настроить сопоставление уровня 3. **add** *svlist*: добавляет вторичные сети VLAN, которые будут связаны с интерфейсом уровня 3. ***remove*** *svlist*: отменяет вторичные сети VLAN, связанные с интерфейсом уровня 3
По умолчанию	По умолчанию первичная VLAN и вторичная VLAN не связаны
Командный режим	Режим конфигурации интерфейса первичной VLAN
Руководство по использованию	Сначала необходимо настроить SVI уровня 3 для основной VLAN. Интерфейсы уровня 3 можно настроить только в первичной VLAN. Ассоциация уровня 2 должна выполняться между связанными вторичными VLAN и первичной VLAN

Настройка изолированных портов и портов сообщества

- После того, как первичная VLAN и вторичные VLAN PVLAN, а также ассоциация уровня 2 настроены, выделите порты устройств, подключенных к пользовательским хостам, чтобы указать поддомены, к которым принадлежат пользовательские хосты.

- Если на предприятии имеется только один пользовательский хост, установите порт, подключенный к пользовательскому хосту, как изолированный порт.
- Если на предприятии имеется несколько пользовательских хостов, установите порты, подключенные к пользовательским хостам, в качестве портов сообщества.

Команда	**switchport mode private-vlan host** **switchport private-vlan host-association** *p_vid s_vid*
Описание параметров	*p_vid*: указывает основной идентификатор VLAN в паре PVLAN. *s_vid*: указывает вторичный идентификатор VLAN в паре PVLAN. Порт является связанным портом, если VLAN является изолированной VLAN, и портом сообщества, если VLAN является VLAN сообщества
По умолчанию	По умолчанию интерфейс работает в режиме доступа (Access); никакие приватные пары VLAN не связаны
Командный режим	Обе команды выполняются в режиме настройки интерфейса
Руководство по использованию	Обе предыдущие команды необходимо настроить. Прежде чем порт будет настроен как изолированный порт или неразборчивый порт, режим порта должен быть настроен как режим хост-порта. От параметра *s_vid* зависит, настроен ли порт как изолированный порт или порт сообщества. *p_vid* и *s_vid* должны быть соответственно идентификаторами первичной VLAN и вторичной VLAN в паре PVLAN, на которой выполняется ассоциация уровня 2. Один хост-порт может быть связан только с одной парой PVLAN

Настройка неразборчивого порта

- Тип PVLAN с одним портом не может обеспечить симметричную пересылку upstream- и downstream-пакетов. Порты для подключения к внешней сети или серверу необходимо настроить как неразборчивые порты, чтобы пользователи могли успешно получить доступ к внешней сети или серверу.

Команда	**switchport mode private-vlan promiscuous** **switchport private-vlan mapping** *p_vid*{ *svlist* | **add** *svlist* | **remove** *svlist* }
Описание параметров	*p_vid*: указывает основной идентификатор VLAN в паре PVLAN. *svlist*: указывает вторичную сеть VLAN, связанную с неразборчивым портом. Между ним и *p_vid* должна быть выполнена ассоциация уровня 2. **add** *svlist*: добавляет вторичную сеть VLAN, которая будет связана с портом. **remove** *svlist*: отменяет вторичную VLAN, связанную с портом

По умолчанию	По умолчанию интерфейс работает в режиме доступа (Access); неразборчивый порт не связан со вторичной VLAN
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Режим порта должен быть настроен как неразборчивый режим. Если порт настроен как неразборчивый порт, он должен быть связан с парами PVLAN. В противном случае порт не может нести или пересылать сервисы. Один неразборчивый порт может быть связан с несколькими парами PVLAN в пределах одной первичной сети VLAN, но не может быть связан с несколькими первичными сетями VLAN

9.4.1.4. Проверка

Заставьте пользовательские хосты, подключенные к портам PVLAN, передавать и получать пакеты в соответствии с правилами переадресации портов PVLAN для реализации изоляции. Настройте ассоциацию уровня 3, чтобы пользователи в первичной VLAN и вторичных VLAN одной и той же PVLAN использовали один и тот же IP-адрес шлюза и осуществляли связь уровня 3.

9.4.1.5. Пример конфигурации

Применение Layer-2 PVLAN между устройствами

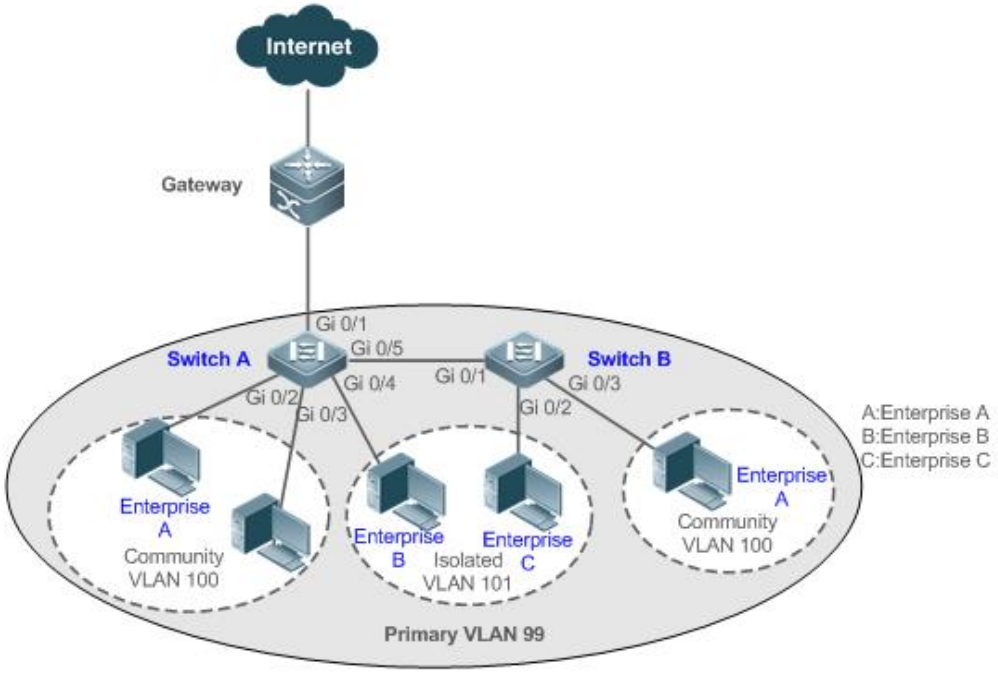


Рисунок 9-3.

Шаги настройки	• Настройте все предприятия так, чтобы они находились в одной и той же PVLAN (первичная VLAN 99 в этом примере). Все корпоративные пользователи используют один и тот же интерфейс уровня 3 через эту VLAN для связи с внешней сетью. • Если на предприятии имеется несколько пользовательских хостов, выделите каждое предприятие для отдельной сети VLAN сообщества (в этом примере для предприятия A выделите сеть VLAN сообщества 100), чтобы реализовать взаимодействие пользователей внутри предприятия и изолировать взаимодействие пользователей между предприятиями. • Если на предприятии есть только один пользовательский хост, выделите такие предприятия в одну и ту же изолированную VLAN (в этом примере назначьте предприятия B и C для изолированной VLAN 101), чтобы изолировать взаимодействие пользователей между предприятиями
A	SwitchA#configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchA(config)#vlan 99 SwitchA(config-vlan)#private-vlan primary SwitchA(config-vlan)#exit SwitchA(config)#vlan 100 SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 101 SwitchA(config-vlan)#private-vlan isolated SwitchA(config-vlan)#exit SwitchA(config)#vlan 99 SwitchA(config-vlan)#private-vlan association 100-101 SwitchA(config-vlan)#exit SwitchA(config)#interface range gigabitEthernet 0/2-3 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 99 100 SwitchA(config-if-range)#exit SwitchA(config)#interface gigabitEthernet 0/4 SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan host-association 99 101
B	SwitchB#configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	SwitchB(config)#vlan 99 SwitchB(config-vlan)#private-vlan primary SwitchB(config-vlan)#exit SwitchB(config)#vlan 100 SwitchB(config-vlan)#private-vlan community SwitchB(config-vlan)#exit SwitchB(config)#vlan 101 SwitchB(config-vlan)#private-vlan isolated SwitchB(config-vlan)#exit SwitchB(config)#vlan 99 SwitchB(config-vlan)#private-vlan association 100-101 SwitchB(config-vlan)#exit SwitchB(config)#interface gigabitEthernet 0/2 SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan host-association 99 101 SwitchB(config-if-GigabitEthernet 0/2)#exit SwitchB(config)#interface gigabitEthernet 0/3 SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan host-association 99 100 SwitchB(config-if-GigabitEthernet 0/3)#exit
Проверка	Проверьте правильность настройки VLAN и портов, а также проверьте правильность переадресации пакетов в соответствии с правилами переадресации пакетов
A	SwitchA#show running-config ! vlan 99 private-vlan primary private-vlan association add 100-101 ! vlan 100 private-vlan community ! vlan 101 private-vlan isolated

	! interface GigabitEthernet 0/1 switchport mode private-vlan promiscuous switchport private-vlan mapping 99 add 100-101 ! interface GigabitEthernet 0/2 switchport mode private-vlan host switchport private-vlan host-association 99 100 ! interface GigabitEthernet 0/3 switchport mode private-vlan host switchport private-vlan host-association 99 100 ! interface GigabitEthernet 0/4 switchport mode private-vlan host switchport private-vlan host-association 99 101 !
B	SwitchB#show running-config ! vlan 99 private-vlan primary private-vlan association add 100-101 ! vlan 100 private-vlan community ! vlan 101 private-vlan isolated !

9.4.1.6. Распространенные ошибки

- Ассоциация уровня 2 не выполняется между первичной VLAN и вторичными VLAN PVLAN, а список портов VLAN не может быть добавлен при настройке изолированных портов, неразборчивых портов и общих портов.
- Один хост-порт не может быть связан с несколькими парами PVLAN.

9.4.1.7. Пример конфигурации

Применение уровня 3 PVLAN на одном устройстве

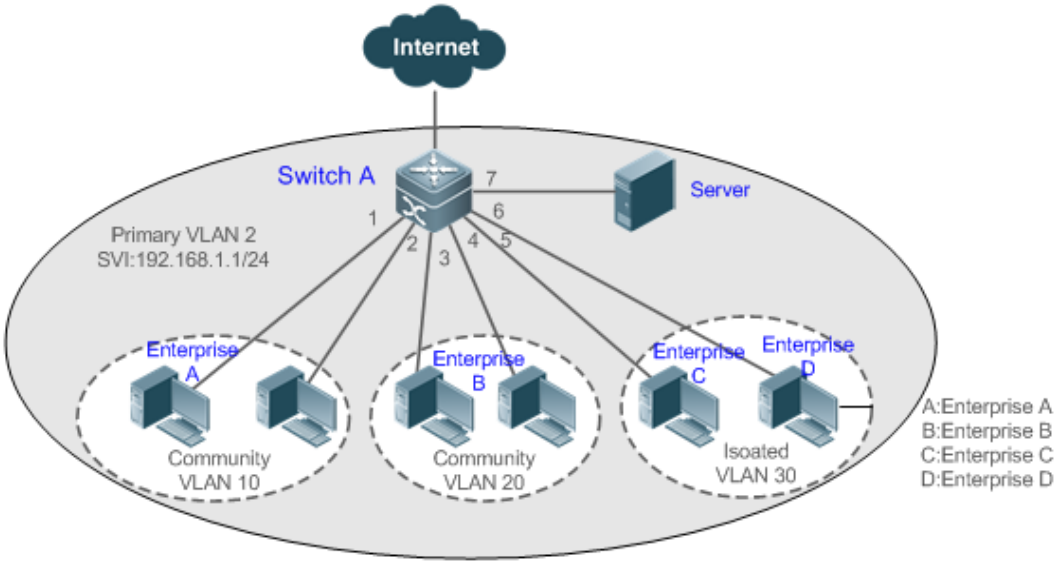


Рисунок 9-4.

Шаги настройки	• Настройте функцию PVLAN на устройстве (коммутатор A в этом примере). Дополнительные сведения о настройке см. в советах по настройке в разделе Пример конфигурации «Применение Layer-2 PVLAN между устройствами». • Установите порт, который напрямую подключен к серверу (порт Gi 0/7 в этом примере), как неразборчивый порт. После этого все корпоративные пользователи смогут взаимодействовать с сервером через неразборчивый порт. • Настройте адрес шлюза PVLAN на устройстве уровня 3 (коммутатор A в этом примере) (в этом примере установите адрес SVI сети VLAN 2 на 192.168.1.1/24) и настройте отображение интерфейса уровня 3 между основной сетью VLAN. (VLAN 2 в этом примере) и вторичные VLAN (VLAN 10, VLAN 20 и VLAN 30 в этом примере). После этого все корпоративные пользователи смогут взаимодействовать с внешней сетью через адрес шлюза
A	SwitchA#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. SwitchA(config)#vlan 2 SwitchA(config-vlan)#private-vlan primary SwitchA(config-vlan)#exit SwitchA(config)#vlan 10 SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 20

	SwitchA(config-vlan)#private-vlan community SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#private-vlan isolated SwitchA(config-vlan)#exit SwitchA(config)#vlan 2 SwitchA(config-vlan)#private-vlan association 10,20,30 SwitchA(config-vlan)#exit SwitchA(config)#interface range gigabitEthernet 0/1-2 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 10 SwitchA(config-if-range)#exit SwitchA(config)#interface range gigabitEthernet 0/3-4 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 20 SwitchA(config-if-range)#exit SwitchA(config)#interface range gigabitEthernet 0/5-6 SwitchA(config-if-range)#switchport mode private-vlan host SwitchA(config-if-range)#switchport private-vlan host-association 2 30 SwitchA(config-if-range)#exit SwitchA(config)#interface gigabitEthernet 0/7 SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan promiscuous SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan maping 2 10,20,30 SwitchA(config-if-GigabitEthernet 0/7)#exit SwitchA(config)#interface vlan 2 SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0 SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30 SwitchA(config-if-VLAN 2)#exit
Проверка	Пропингуйте адрес шлюза 192.168.1.1 с хостов пользователей в разных поддоменах. Операция **ping** прошла успешно
A	SwitchA#show running-config ! vlan 2 private-vlan primary

```
private-vlan association add 10,20,30
!
vlan 10
private-vlan community
!
vlan 20
private-vlan community
!
vlan 30
private-vlan isolated
!
interface GigabitEthernet 0/1
switchport mode private-vlan host
switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
switchport mode private-vlan host
switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
switchport mode private-vlan host
switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
switchport mode private-vlan host
switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
switchport mode private-vlan host
switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
switchport mode private-vlan host
switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
```

```
switchport mode private-vlan promiscuous
switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
no ip proxy-arp
ip address 192.168.1.1 255.255.255.0
private-vlan mapping add 10,20,30
!
SwitchA#show vlan private-vlan
VLAN  Type       Status  Routed   Ports          Associated VLANs
----------------------------      ---------------
2     primary    active  Enabled  Gi0/7          10,20,30
10    community  active  Enabled  Gi0/1, Gi0/2   2
20    community  active  Enabled  Gi0/3, Gi0/4   2
30    isolated   active  Enabled  Gi0/5, Gi0/6   2
```

Распространенные ошибки

- Ассоциация уровня 2 не выполняется в первичной VLAN и вторичных VLAN PVLAN, а связь уровня 3 не может быть настроена.
- Устройство подключается к внешней сети до настройки ассоциации уровня 3. В результате устройство не может обмениваться данными с внешней сетью.
- Интерфейсы для подключения к серверу и внешней сети не настроены как неразборчивые интерфейсы, что приводит к асимметричной пересылке upstream- и downstream-пакетов.

9.5. Мониторинг

9.5.1. Отображение

Описание	Команда
Отображает конфигурацию PVLAN	**show vlan private-vlan**

9.5.2. Отладка

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

Описание	Команда
Отладка PVLAN	**debug bridge pvlan**

10. НАСТРОЙКА MSTP

10.1. Обзор

Spanning Tree Protocol (STP) — это протокол управления уровня 2. Он может не только выборочно блокировать избыточные каналы для устранения петель уровня 2, но также может создавать резервные копии каналов.

Подобно многим протоколам, STP постоянно обновляется с протокола Rapid Spanning Tree Protocol (RSTP) до протокола Multiple Spanning Tree Protocol (MSTP) по мере развития сети.

Для Ethernet уровня 2 между двумя локальными сетями (LAN) может существовать только одно активное соединение. В противном случае произойдет широковещательный шторм. Для повышения надежности локальной сети необходимо установить резервный канал и сохранить некоторые пути в резервном состоянии. Если сеть неисправна и канал не работает, вы должны переключить резервный канал в активное состояние. STP может автоматически активировать резервный канал без каких-либо ручных операций. STP позволяет устройствам в локальной сети:

- обнаруживать и запускать лучшую топологию дерева в локальной сети;
- устранять неполадки и автоматически обновлять топологии сети, чтобы всегда выбиралась наилучшая возможная топология «дерева».

Топология локальной сети рассчитывается автоматически на основе набора параметров моста, настроенного администратором. Наилучшее «дерево» топологии можно получить, правильно настроив эти параметры.

RSTP полностью совместим с 802.1D STP. Подобно традиционному STP, RSTP предоставляет сервисы без петель и с резервированием. Характеризуется быстрой скоростью. Если все мосты в локальной сети поддерживают протокол RSTP и правильно настроены администратором, для повторного создания «дерева» топологии после изменения топологии сети требуется менее 1 секунды (около 50 секунд при использовании традиционного протокола STP).

STP и RSTP имеют следующие дефекты:

- Миграция STP происходит медленно. Даже на каналах точка-точка или граничных портах для переключения портов в состояние пересылки по-прежнему требуется удвоенная задержка пересылки.
- RSTP может быстро конвергировать, но имеет тот же недостаток, что и STP: поскольку все VLAN в локальной сети используют одно и то же spanning tree, пакеты всех VLAN пересылаются по этому spanning tree. Следовательно, избыточные каналы нельзя заблокировать в соответствии с конкретными VLAN, а трафик данных нельзя сбалансировать между VLAN.

MSTP, определенный IEEE в 802.1s, устраняет дефекты STP и RSTP. Он не только быстро конвергирует, но и позволяет пересылать трафик разных VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для избыточных каналов.

Как правило, STP/RSTP работает на основе портов, а MSTP — на основе экземпляров. Экземпляр — это набор из нескольких VLAN. Связывание нескольких VLAN с одним экземпляром может снизить коммуникационные издержки и использование ресурсов.

Устройства QTECH поддерживают STP, RSTP и MSTP и соответствуют стандартам IEEE 802.1D, IEEE 802.1w и IEEE 802.1s.

10.1.1.1. Протоколы и стандарты

- IEEE 802.1D: мосты управления доступом к медиа (MAC)
- IEEE 802.1w: часть 3: мосты управления доступом к медиа (MAC) — Поправка 2: Быстрая реконфигурация
- IEEE 802.1s: виртуальные локальные сети с мостами — Поправка 3: Multiple Spanning Trees

10.2. Приложения

Приложение	Описание
Топология Dual-Core MSTP+VRRP	В модели иерархической сетевой архитектуры режим MSTP+VRRP используется для реализации избыточности и балансировки нагрузки для повышения доступности системы в сети
Туннель BPDU	В сетевой среде QinQ туннель блока данных протокола моста (BPDU) используется для реализации прозрачной передачи пакетов STP на основе туннеля

10.2.1. Топология Dual-Core MSTP+VRRP

10.2.1.1. Сценарий

Типичным применением MSTP является Dual-Core решение MSTP+VRRP. Это решение является отличным решением для повышения доступности системы в сети. Используя модель иерархической сетевой архитектуры, она обычно делится на три уровня (уровень ядра, уровень конвергенции и уровень доступа) или два уровня (уровень ядра и уровень доступа). Они образуют базовую сетевую систему для предоставления услуги обмена данными.

Основным преимуществом этой архитектуры является ее иерархическая структура. В иерархической сетевой архитектуре все показатели пропускной способности, характеристики и функции сетевых устройств на каждом уровне оптимизируются в зависимости от их расположения в сети и ролей, что повышает их стабильность и доступность.

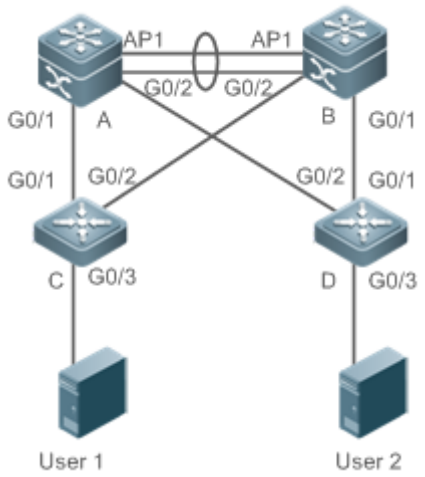


Рисунок 10-1. Dual-Core топология MSTP+VRRP

Топология разделена на два уровня: уровень ядра (устройства A и B) и уровень доступа (устройства C и D).

10.2.1.2. Развертывание

- Уровень ядра: несколько экземпляров MSTP настроены для реализации балансировки нагрузки. Например, создаются два экземпляра: экземпляр 1 и экземпляр 2. Экземпляр 1 сопоставляет VLAN 10, а экземпляр 2 сопоставляет VLAN 20. Устройство A является root bridge экземпляров 0 и 1 (экземпляр 0 — это CIST, который существует по умолчанию). Устройство B является root bridge экземпляра 2.
- Уровень ядра: устройства A и B являются активными устройствами VRRP соответственно в сетях VLAN 10 и VLAN 20.
- Уровень доступа: настройте порт, напрямую подключенный к терминалу (ПК или серверу), в качестве порта PortFast и включите защиту BPDU, чтобы предотвратить доступ неавторизованных пользователей с нелегальных устройств.

10.2.2. Туннель BPDU

10.2.2.1. Сценарий

Сеть QinQ обычно делится на две части: сеть клиента и сеть поставщика сервисов (SP). Вы можете включить BPDU Tunnel для расчета пакетов STP сети клиента независимо от сети поставщика сервисов, тем самым предотвратив влияние пакетов STP между сетью клиента на сеть поставщика сервисов.

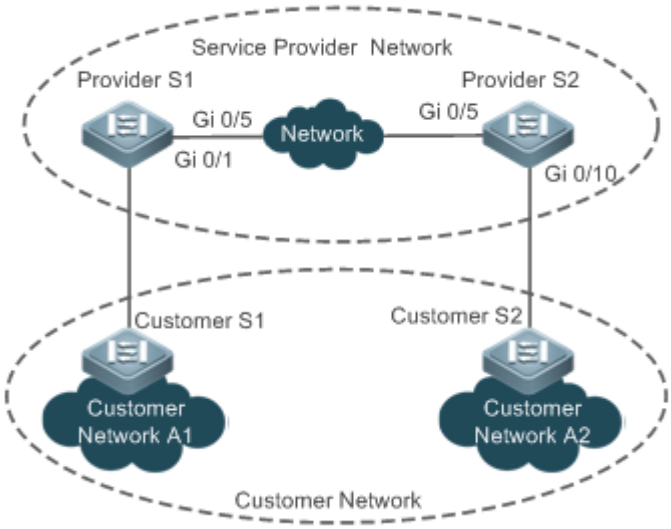


Рисунок 10-2. Топология туннеля BPDU

Как показано на Рисунке выше, верхняя часть — это сеть поставщика сервисов, а нижняя — сеть клиента. Сеть SP состоит из двух границ провайдера (PE): Provider S1 и Provider S2. Клиентская сеть A1 и Клиентская сеть A2 — это два сайта пользователя в разных регионах. Заказчик S1 и Заказчик S2, устройства доступа из сети заказчика в сеть SP, получают доступ к сети SP соответственно через Provider S1 и Provider S2.

Используя BPDU Tunnel, Клиентская сеть A1 и Клиентская сеть A2 в разных регионах, можно выполнять унифицированный расчет spanning tree в сети SP, не влияя на расчет spanning tree в сети SP.

10.2.2.2. Развертывание

- Включите базовый QinQ на PE (в этом примере Provider S1/Provider S2), чтобы пакеты данных сети клиента передавались в пределах указанной VLAN в сети SP.
- Включите прозрачную передачу STP на PE (провайдер S1/Provider S2 в этом примере), чтобы сеть SP могла передавать пакеты STP сети клиента через туннель BPDU.

10.2.3. Функции

10.2.3.1. Базовые определения

BPDU

Для создания стабильной сети с древовидной топологией должны быть выполнены следующие условия:

- Каждый мост имеет уникальный идентификатор, состоящий из приоритета моста и MAC-адреса.
- Накладные расходы пути от моста к root bridge называются стоимостью пути root.
- Идентификатор порта состоит из приоритета порта и номера порта.

Мосты обмениваются пакетами BPDU для получения информации, необходимой для установления наилучшей топологии «дерева». Эти пакеты используют групповой адрес 01-80-C2-00-00-00 (шестнадцатеричный) в качестве адреса получателя.

BPDU состоит из следующих элементов:

- Идентификатор root bridge, предполагаемый локальным мостом.
- Стоимость пути root локального моста.
- Bridge ID (идентификатор локального моста).
- Возраст сообщения (возраст пакета).
- Идентификатор порта (идентификатор порта, отправляющего этот пакет).
- **Forward-Delay Time, Hello Time, Max-Age Time** — параметры времени, указанные в MSTP.
- Другие флаги, такие как флаги, указывающие на изменения топологии сети и статус локального порта.

Если мост получает BPDU с более высоким приоритетом (меньший идентификатор моста и более низкая стоимость пути root) на порт, он сохраняет информацию BPDU на этом порту и передает информацию на все остальные порты. Если мост получает BPDU с более низким приоритетом, он отбрасывает информацию.

Такой механизм позволяет передавать информацию с более высоким приоритетом по всей сети. Результаты обмена BPDU следующие:

- В качестве root bridge выбирается мост.
- За исключением root bridge, каждый мост имеет корневой порт (root-порт), то есть порт, обеспечивающий кратчайший путь к root bridge.
- Каждый мост вычисляет кратчайший путь к root bridge.
- Каждая локальная сеть имеет назначенный мост, расположенный на кратчайшем пути между локальной сетью и root bridge. Порт, предназначенный для соединения моста и локальной сети, называется назначенным портом.
- Корневой порт и назначенный порт переходят в статус пересылки.

Идентификатор моста

Согласно IEEE 802.1W каждый мост имеет уникальный идентификатор. Алгоритм spanning tree выбирает root bridge на основе идентификатора моста. Идентификатор моста состоит из восьми байтов, из которых последние шесть байтов являются MAC-адресом моста. В его первых двух байтах (как указано в следующей таблице) первые четыре бита указывают приоритет; последние восемь битов указывают идентификатор системы для использования в расширенном протоколе. В RSTP идентификатор системы равен 0. Следовательно, приоритет моста должен быть целым числом, кратным 4096.

	Бит	Значение
Значение приоритета	16	32 768
	15	16 384
	14	8192
	13	4096

	Бит	Значение
Идентификатор системы	12	2048
	11	1024
	10	512
	9	256
	8	128
	7	64
	6	32
	5	16
	4	8
	3	4
	2	2
	1	1

Таймеры spanning tree

Следующие три таймера влияют на производительность всего spanning tree:

- Hello timer (Таймер приветствия): интервал периодической отправки пакета BPDU.
- Forward-Delay timer (Таймер задержки пересылки): интервал изменения состояния порта, то есть интервал перехода порта из состояния прослушивания в состояние изучения или из состояния изучения в состояние пересылки, когда RSTP работает в режиме, совместимом с STP.
- Max-Age timer (Таймер максимального возраста): максимальное время жизни (TTL) пакета BPDU. По истечении этого времени пакет отбрасывается.

Роли портов и состояния портов

Каждый порт играет роль в сети, отражая различные функции в топологии сети.

- Корневой порт: порт, обеспечивающий кратчайший путь к root bridge.
- Назначенный порт: порт, используемый каждой локальной сетью для подключения к root bridge.
- Альтернативный порт: альтернативный порт корневого порта. Как только корневой порт теряет силу, альтернативный порт немедленно меняется на корневой порт.
- Резервный порт: резервный порт назначенного порта. Когда мост имеет два порта, подключенных к локальной сети, порт с более высоким приоритетом является

назначенным портом, а порт с более низким приоритетом является резервным портом.

- Отключенный порт: неактивный порт. Эту роль играют все порты с выключенным рабочим состоянием.

На следующих рисунках показаны роли различных портов:

R = корневой порт D = назначенный порт A = альтернативный порт B = резервный порт

Если не указано иное, приоритеты портов уменьшаются слева направо.

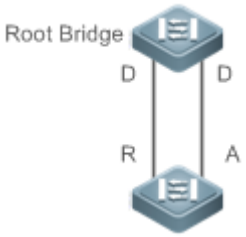


Рисунок 10-3.

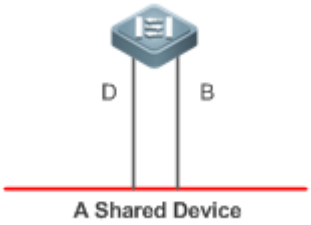


Рисунок 10-4.

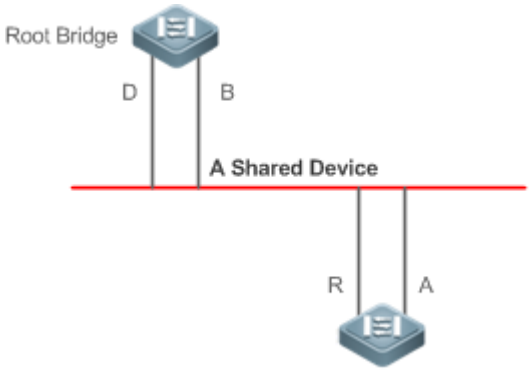


Рисунок 10-5.

Каждый порт имеет три состояния, указывающие, следует ли пересылать пакеты данных, чтобы контролировать всю топологию spanning tree.

- Отбрасывание: не пересылает полученные пакеты и не узнает исходный MAC-адрес.
- Изучение: не пересылает полученные пакеты, но изучает MAC-адрес источника, что является переходным состоянием.
- Пересылка: пересылает полученные пакеты и узнает исходный MAC-адрес.

Для стабильной топологии сети только корневой порт и назначенный порт могут войти в состояние пересылки, в то время как другие порты всегда находятся в состоянии отбрасывания.

Счетчик Hop-ов (Hop Count)

Внутренние spanning tree (IST) и множественные экземпляры spanning tree (MSTI) вычисляют, истекает ли время пакета BPDU, на основе механизма Hop Count, похожего на IP TTL, вместо Message Age и Max Age.

Рекомендуется запустить команду **spanning-tree max-hops** в режиме глобальной конфигурации, чтобы настроить количество hop'ов. В регионе каждый раз, когда пакет BPDU проходит через устройство от root bridge, Hop Count уменьшается на 1. Когда Hop Count становится равным 0, время пакета BPDU истекает, и устройство отбрасывает пакет.

Чтобы быть совместимым с STP и RSTP за пределами региона, MSTP также сохраняет механизмы Message Age и Max Age.

10.2.3.2. Обзор

Особенность	Описание
STP	STP, определенный IEEE в 802.1D, используется для устранения физических петель на канальном уровне в локальной сети
RSTP	RSTP, определенный IEEE в 802.1w, оптимизирован на основе STP для быстрой конвергенции топологии сети
MSTP	MSTP, определенный IEEE в 802.1s, устраняет дефекты STP, RSTP и spanning tree для каждой VLAN (PVST). Он может не только быстро сходиться, но и перенаправлять трафик различных VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для избыточных каналов
Дополнительные функции MSTP	MSTP включает следующие функции: PortFast, BPDU guard, BPDU filter, TC protection, TC guard, TC filter, BPDU check на основе исходного MAC-адреса, BPDU filter на основе недопустимой длины, Auto Edge, root guard и loop guard

10.2.4. STP

STP используется для предотвращения широковещательных штормов, вызванных петлями, и обеспечения избыточности каналов.

10.2.4.1. Принцип работы

Для Ethernet уровня 2 между двумя локальными сетями может существовать только один активный канал. В противном случае произойдет широковещательный шторм. Для повышения надежности локальной сети необходимо установить резервный канал и сохранить некоторые пути в резервном состоянии. Если сеть неисправна и канал не работает, вы должны переключить резервный канал в активное состояние. STP может автоматически активировать резервный канал без каких-либо ручных операций. STP позволяет устройствам в локальной сети:

- Обнаружить и запустить лучшую топологию «дерева» в локальной сети.
- Устранить неполадки и автоматически обновить топологию сети, чтобы всегда выбиралась наилучшая возможная топология «дерева».

Топология локальной сети рассчитывается автоматически на основе набора параметров моста, настроенных администратором. Наилучшее «дерево» топологии можно получить, правильно настроив эти параметры.

10.2.4.2. Связанная конфигурация

Включение spanning tree

- По умолчанию функция spanning tree отключена.
- Запустите **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] для включения STP и настройки основных атрибутов.
- Время пересылки (forward-time) колеблется от 4 до 30. Время приветствия (hello-time) колеблется от 1 до 10. Максимальное время (max-age) колеблется от 6 до 40.

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб. Диапазоны значений forward-time, hello-time и max-age связаны. Если изменить один из них, это повлияет на два других диапазона. Эти три значения должны соответствовать следующему условию: 2×(hello-time + 1 секунда) ≤ max-age ≤ 2×(Forward-Delay Time — 1 секунда). В противном случае конфигурация не будет выполнена.

10.2.5. RSTP

RSTP полностью совместим с 802.1D STP. Подобно традиционному STP, RSTP предоставляет сервисы без петель и с резервированием. Характеризуется быстрой скоростью. Если все мосты в локальной сети поддерживают протокол RSTP и правильно настроены администратором, для повторного создания «дерева» топологии после изменения топологии сети требуется менее 1 секунды (около 50 секунд при использовании традиционного протокола STP).

10.2.5.1. Принцип работы

Быстрая конвергенция RSTP

RSTP имеет специальную функцию, то есть быстро переводить порты в состояние переадресации.

STP позволяет порту войти в состояние пересылки через 30 секунд (в два раза больше Forward-Delay Time; Forward-Delay Time можно настроить со значением по умолчанию 15 секунд) после выбора роли порта. Каждый раз, когда топология изменяется, корневой порт и назначенный порт, повторно выбранные каждым мостом, переходят в состояние пересылки через 30 секунд. Поэтому требуется около 50 секунд, чтобы вся топология сети стала древовидной.

RSTP сильно отличается от STP в процессе пересылки. Как показано на Рисунке 10-6, коммутатор A отправляет пакет RSTP Proposal на коммутатор B. Если коммутатор B обнаруживает, что приоритет коммутатора A выше, он выбирает коммутатор A в качестве root bridge, а порт, получающий пакет, в качестве корневого порта, переходит в состояние пересылки и затем отправляет Пакет подтверждения (Agree packet) от корневого порта к коммутатору A. Если назначенный порт коммутации A согласован, порт переходит в состояние пересылки. Назначенный порт коммутации B повторно отправляет пакет Proposal для расширения spanning tree по порядку. Теоретически RSTP может восстановить сетевую топологию «дерева» для быстрой сходимости после изменения топологии сети.

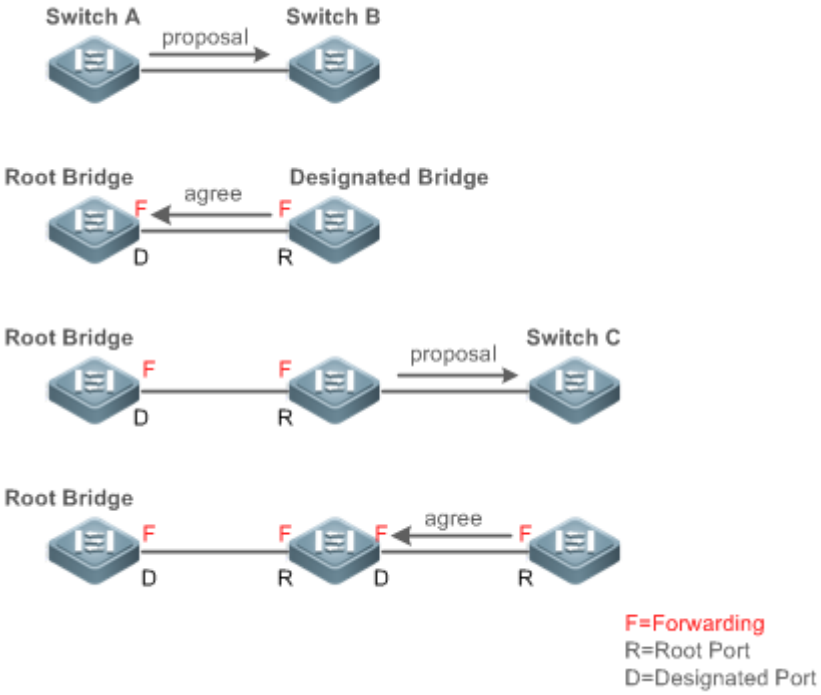


Рисунок 10-6.

ПРИМЕЧАНИЕ: описанный выше процесс «рукопожатия» реализуется только тогда, когда соединение между портами находится в режиме «точка-точка». Чтобы дать устройствам полную свободу действий, рекомендуется не включать соединение «точка-точка» между устройствами.

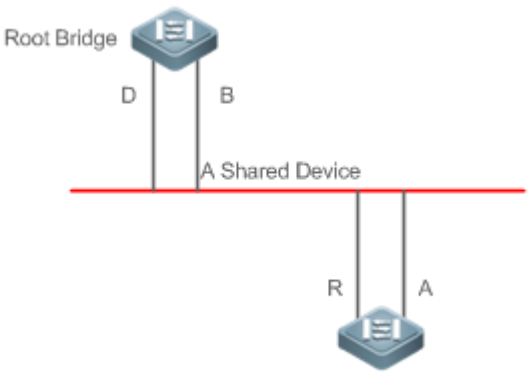


Рисунок 10-7. Пример соединения не «точка-точка»

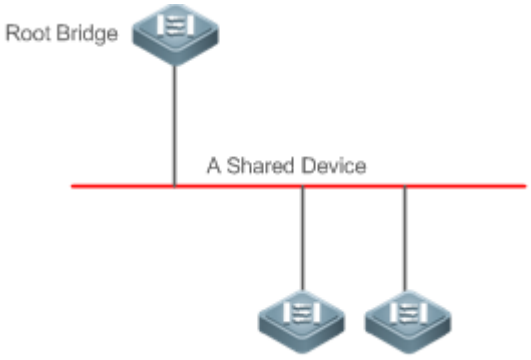


Рисунок 10-8. Пример соединения не «точка-точка»

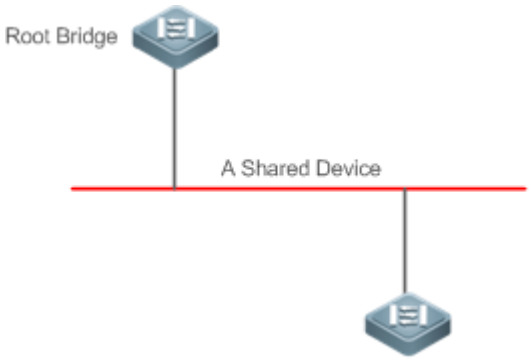


Рисунок 10-9. Пример соединения «точка-точка»

Совместимость между RSTP и STP

RSTP полностью совместим с STP. RSTP автоматически проверяет, поддерживает ли подключенный мост STP или RSTP, на основе полученного номера версии BPDU. Если порт подключается к мосту STP, порт переходит в состояние пересылки через 30 секунд, что не позволяет полноценно использовать RSTP.

Другая проблема может возникнуть при совместном использовании протоколов RSTP и STP. Как показано на следующих Рисунках, коммутатор A (RSTP) подключается к коммутатору B (STP). Если коммутатор A обнаруживает, что подключен к мосту STP, он отправляет пакет STP BPDU. Однако, если коммутатор B заменен коммутатором C (RSTP), но коммутатор A по-прежнему отправляет пакеты STP BPDU, коммутатор C будет считать себя подключенным к мосту STP. В результате два устройства RSTP работают под STP, что сильно снижает эффективность.

RSTP предоставляет функцию миграции протокола для принудительной отправки пакетов RSTP BPDU (peer-мост должен поддерживать RSTP). В этом случае коммутатор A принудительно отправляет RSTP BPDU, а затем коммутатор C обнаруживает, что он подключен к мосту RSTP. В результате два RSTP-устройства работают под RSTP, как показано на Рисунке 10-11.

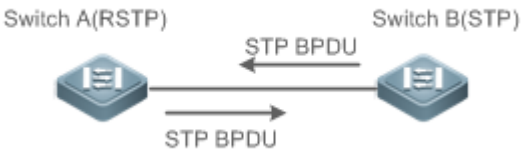


Рисунок 10-10.

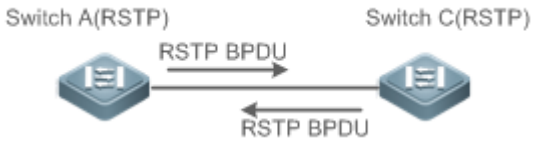


Рисунок 10-11.

10.2.5.2. Связанная конфигурация

- Настройка миграции протокола
- Запустите команду **clear spanning-tree detected-protocols** [**interface** *interface-id*], чтобы принудительно проверить версию на порту. Дополнительные сведения см. в разделе «Совместимость между RSTP и STP» выше.

10.2.6. MSTP

MSTP устраняет дефекты STP и RSTP. Он может не только быстро сходиться, но и перенаправлять трафик различных VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для избыточных каналов.

10.2.6.1. Принцип работы

Устройства QTECH поддерживают MSTP. MSTP — это новый протокол spanning tree, разработанный на основе традиционных STP и RSTP и включающий механизм быстрой пересылки RSTP.

Поскольку традиционные протоколы spanning tree не имеют отношения к VLAN, проблемы могут возникнуть в определенных сетевых топологиях:

Как показано на Рисунке 10-12, устройства A и B находятся в сети VLAN 1, а устройства C и D — в сети VLAN 2, образуя петлю.

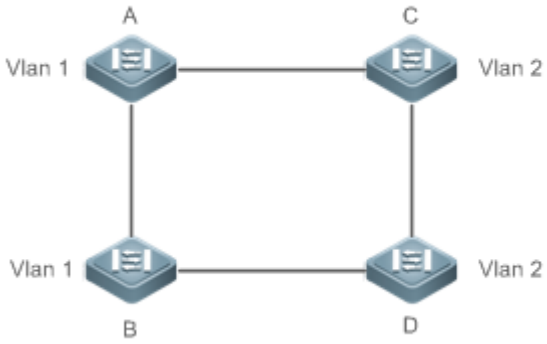


Рисунок 10-12.

Если канал от устройства A к устройству B через устройства C и D стоит меньше, чем канал от устройства A напрямую к устройству B, связь между устройством A и устройством B переходит в состояние отбрасывания (как показано на Рисунке 10-13). Поскольку устройства C и D не включают VLAN 1 и не могут пересылать пакеты данных VLAN 1, VLAN 1 устройства A не может обмениваться данными с VLAN 1 устройства B.

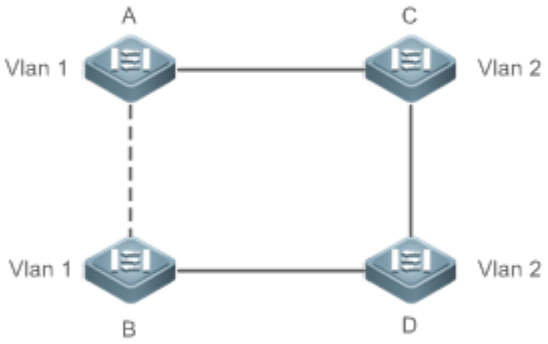


Рисунок 10-13.

MSTP разработан для решения этой проблемы. Он делит одну или несколько VLAN устройства на экземпляр. Устройства, настроенные с одним и тем же экземпляром, образуют регион MST для запуска независимого spanning tree (называемого IST). Эта область MST, подобно большому устройству, реализует алгоритм spanning tree с другими областями MST для создания полного spanning tree, называемого общим spanning tree (CST).

На основе этого алгоритма приведенная выше сеть может сформировать топологию, показанную на Рисунке 10-14 по алгоритму MSTP: устройства A и B находятся в регионе MSTP 1, в котором не возникает петель, и, следовательно, ни один канал не переходит в состояние отбрасывания. Это также относится к региону 2 MSTP. Регион 1 и регион 2, подобно двум большим устройствам с петлями, выбирают канал для перехода в состояние отбрасывания на основе связанной конфигурации.

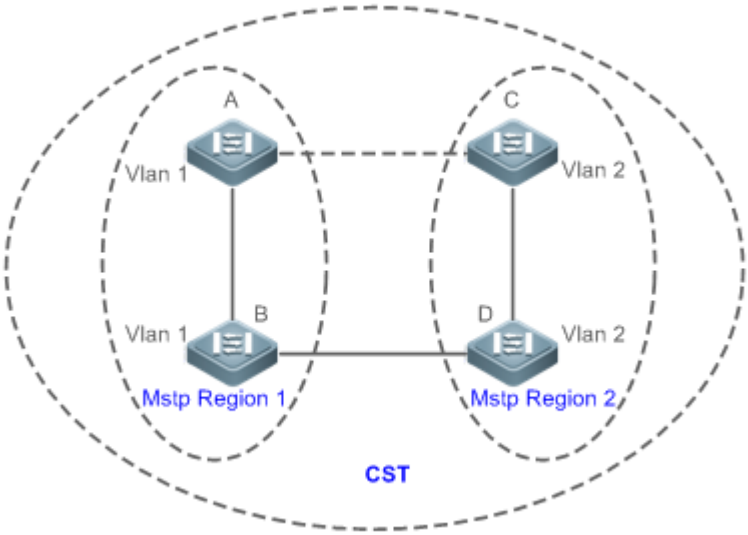


Рисунок 10-14.

Это предотвращает образование петель и обеспечивает правильную связь между устройствами в одной VLAN.

Региональное отделение MSTP

Чтобы MSTP работал должным образом, правильно разделите регионы MSTP и сконфигурируйте одинаковую информацию о конфигурации MST для устройств в одном регионе MSTP.

Информация о конфигурации MST включает:

- Имя конфигурации MST: состоит не более чем из 32 байтов для идентификации региона MSTP.
- Номер версии MST: состоит из 16 бит для идентификации региона MSTP.
- Таблица сопоставления экземпляров MST и VLAN: для каждого устройства создается не более 64 экземпляров (с их идентификаторами в диапазоне от 1 до 64), а экземпляр 0 существует в обязательном порядке. Таким образом, система поддерживает максимальное количество экземпляров 65. Пользователи могут назначать от 1 до 4994 VLAN, принадлежащих разным экземплярам (от 0 до 64) по мере необходимости. Неназначенные VLAN принадлежат экземпляру 0 по умолчанию. В этом случае каждый MSTI представляет собой группу VLAN и реализует алгоритм spanning tree MSTI, указанный в пакете BPDU, на который не влияют CIST и другие MSTI.

Запустите команду **spanning-tree mst configuration** в режиме глобальной конфигурации, чтобы войти в режим конфигурации MST для настройки указанной выше информации.

BPDU MSTP несут указанную выше информацию. Если BPDU, полученный устройством, содержит ту же информацию о конфигурации MST, что и информация об устройстве, считается, что подключенное устройство принадлежит к тому же региону MST, что и оно. В противном случае это относится к подключенному устройству из другого региона MST.

ПРИМЕЧАНИЕ: таблицу сопоставления экземпляр-VLAN рекомендуется настраивать после отключения MSTP. После настройки снова включите MSTP, чтобы обеспечить стабильность и конвергенцию топологии сети.

IST (spanning tree в регионе MSTP)

После того, как регионы MSTP разделены, каждый регион выбирает независимый root bridge для каждого экземпляра на основе соответствующих параметров, таких как приоритет моста и приоритет порта, назначает роли каждому порту на каждом устройстве и указывает, находится ли порт в состоянии пересылки или отбрасывания в экземпляре на основе роли порта.

Через обмен MSTP BPDU создается IST, и каждый экземпляр имеет свои собственные spanning tree (MSTI), в которых spanning tree, соответствующее экземпляру 0 и CST, единообразно называется spanning tree общего экземпляра (CIST). То есть каждый экземпляр предоставляет единую сетевую топологию без петель для своих групп VLAN.

Как показано на Рисунке 10-15, Устройства A, B и C образуют петлю в регионе 1. Устройство A имеет наивысший приоритет в CIST (Экземпляр 0) и поэтому выбрано в качестве root региона. Затем MSTP позволяет каналу между A и C перейти в состояние отбрасывания на основе других параметров. Следовательно, для группы VLAN экземпляра 0 доступны только каналы от A до B и от B до C, что разрывает петлю этой группы VLAN.

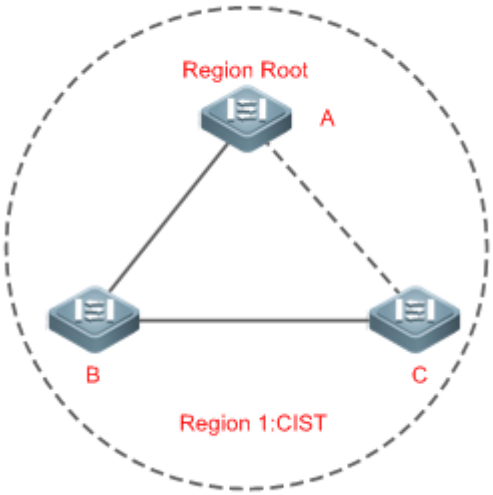


Рисунок 10-15.

Как показано на Рисунке 10-16, устройство B имеет наивысший приоритет в MSTI 1 (экземпляр 1) и поэтому выбирается в качестве root региона. Затем MSTP позволяет каналу между B и C перейти в состояние отбрасывания на основе других параметров. Поэтому для группы VLAN Экземпляра 1 доступны только каналы от A до B и от A до C, разрывая петлю этой группы VLAN.

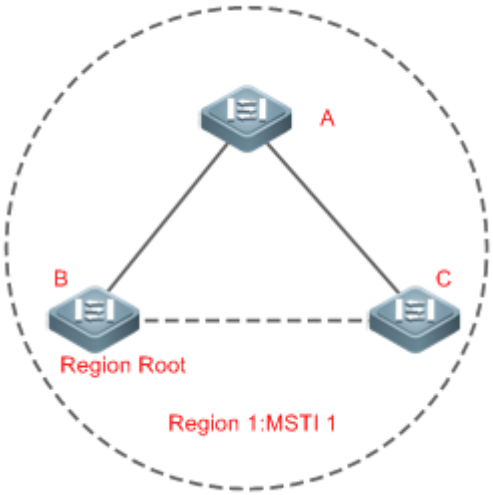


Рисунок 10-16.

Как показано на Рисунке 10-17, устройство C имеет наивысший приоритет в MSTI 2 (экземпляр 2) и поэтому выбирается в качестве root региона. Затем MSTP позволяет каналу между B и C перейти в состояние отбрасывания на основе других параметров. Поэтому для группы VLAN Экземпляра 2 доступны только каналы от B к C и от A к C, разрывая петлю этой группы VLAN.

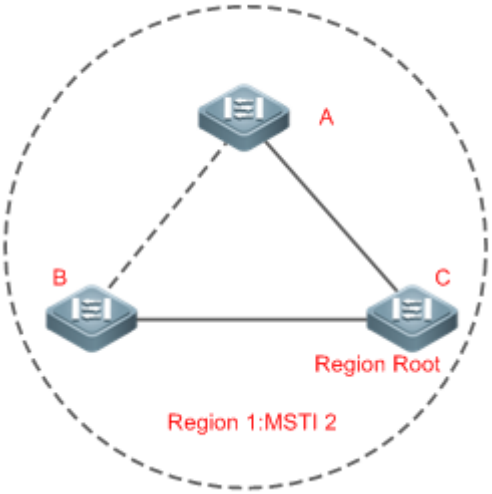


Рисунок 10-17.

Обратите внимание, что MSTP не имеет значения, к какой VLAN принадлежит порт. Таким образом, пользователи должны настроить стоимость пути и приоритет соответствующего порта на основе фактической конфигурации VLAN, чтобы MSTP не прерывал неправильные петли.

CST (spanning tree между регионами MSTP)

Каждый регион MSTP подобен большому устройству для CST. Различные регионы MSTP образуют «дерево» топологии bit-сети, называемое CST. Как показано на Рисунке 10-18, Устройство A, у которого идентификатор моста наименьший, выбирается в качестве root во всем CST и регионального root CIST в этом регионе. В регионе 2, поскольку стоимость пути root от устройства B до root CST является самой низкой, устройство B выбирается в качестве регионального root CIST в этом регионе. По той же причине устройство C выбрано в качестве регионального root CIST.

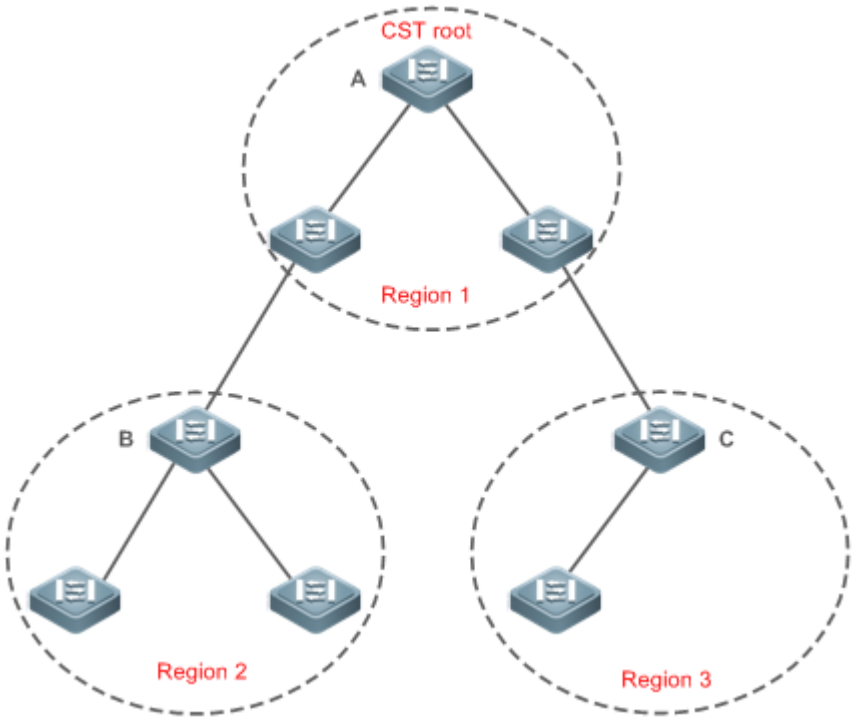


Рисунок 10-18.

Региональный root CIST может быть не устройством, у которого идентификатор моста является наименьшим в регионе, но указывает устройство, для которого стоимость пути root от этого региона до root CST является наименьшей.

Для MSTI корневой порт регионального root CIST имеет новую роль «master-порт». Master-порт действует как исходящий порт для всех экземпляров и находится в состоянии пересылки для всех экземпляров. Чтобы сделать топологию более стабильной, мы предлагаем, чтобы master-порт каждого региона к root CST находился на том же устройстве региона, если это возможно.

Совместимость между MSTP, RSTP и STP

Подобно RSTP, MSTP отправляет STP BPDU для обеспечения совместимости с STP. Дополнительные сведения см. в разделе Принцип работы «Совместимость между RSTP и STP».

Поскольку RSTP обрабатывает BPDU MSTP CIST, MSTP не нужно отправлять BPDU RSTP для обеспечения совместимости с ним.

Каждое устройство STP или RSTP представляет собой отдельный регион и не образует один и тот же регион ни с какими устройствами.

10.2.6.2. Связанная конфигурация

Настройка STP

- По умолчанию режим STP — это режим MSTP.
- Запустите **spanning-tree mode** [**stp** | **rstp** | **mstp**], чтобы изменить режим STP.

10.2.7. Дополнительные функции MSTP

Дополнительные функции MSTP в основном включают порт PortFast, PDU guard, BPDU filter, TC guard и guard. Дополнительные функции в основном используются для развертывания конфигураций MSTP на основе топологии сети и характеристик приложений в сети MSTP. Это повышает стабильность, надежность и возможности защиты от атак MSTP, отвечая требованиям приложений MSTP в различных сценариях клиентов.

10.2.7.1. Принцип работы

PortFast

Если порт устройства напрямую подключается к сетевому терминалу, этот порт настраивается как порт PortFast для прямого перехода в состояние пересылки. Если порт PortFast не настроен, порту необходимо подождать 30 секунд, чтобы войти в состояние пересылки. Рисунок 10-19 показывает, какие порты устройства можно настроить как порты PortFast.

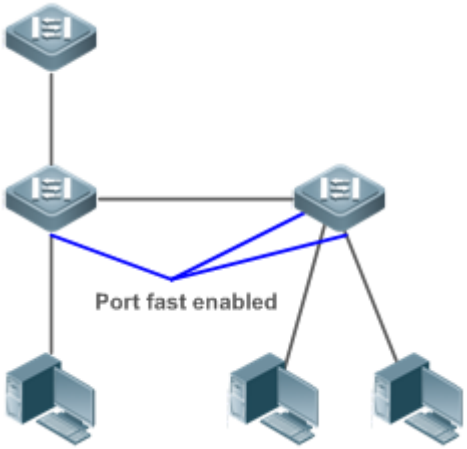


Рисунок 10-19.

Если порт PortFast по-прежнему получает BPDU, его рабочее состояние PortFast (Port Fast Operational State) будет отключено, и порт перейдет в состояние пересылки в соответствии с обычным алгоритмом STP.

BPDU Guard

BPDU Guard может быть включена глобально или на интерфейсе.

Рекомендуется запустить команду **spanning-tree portfast bpduguard default** в режиме глобальной конфигурации, чтобы включить глобальную BPDU Guard. Если PortFast включен для порта или этот порт автоматически идентифицируется как пограничный порт, этот порт переходит в состояние отключения из-за ошибки, чтобы указать на ошибку конфигурации сразу после получения BPDU. В то же время порт отключен, что указывает на то, что сетевое устройство может быть добавлено неавторизованным пользователем для изменения топологии сети.

Также рекомендуется запустить команду **spanning-tree bpduguard enable** в режиме конфигурации интерфейса, чтобы включить BPDU Guard на порту (независимо от того, включен PortFast или нет на порту). В этом случае порт переходит в состояние отключения из-за ошибки сразу после получения BPDU.

BPDU Filter

BPDU Filter можно включить глобально или включить на интерфейсе.

Рекомендуется запустить команду **spanning-tree portfast bpdufilter default** в режиме глобальной конфигурации, чтобы включить глобальный BPDU Filter. В этом случае порт PortFast не получает и не отправляет BPDU, поэтому хост, подключающийся напрямую к порту PortFast, не получает BPDU. Если порт меняет свое рабочее состояние PortFast на Disabled после получения BPDU, фильтр BPDU автоматически перестает действовать.

Также рекомендуется запустить команду **spanning-tree bpdufilter enable** в режиме конфигурации интерфейса, чтобы включить фильтр BPDU на порту (независимо от того, включен или нет PortFast на порту). В этом случае порт не получает и не отправляет BPDU, а напрямую переходит в состояние пересылки.

TC Protection

TC BPDU — это пакеты BPDU, несущие TC. Если коммутатор получает такие пакеты, это указывает на изменение топологии сети, и коммутатор удалит таблицу MAC-адресов. Для коммутаторов уровня 3 в этом случае модуль переадресации снова включается, а состояние порта в записи ARP изменяется. Когда коммутатор подвергается атаке с помощью поддельных TC BPDU, он часто выполняет вышеуказанные операции, вызывая

большую нагрузку и влияя на стабильность сети. Чтобы предотвратить эту проблему, вы можете включить TC Protection.

TC Protection может быть включена или отключена только глобально. Эта функция отключена по умолчанию.

Когда TC Protection включена, коммутатор удаляет TC BPDU в течение заданного периода (обычно 4 секунды) после их получения и отслеживает получение каких-либо пакетов TC BPDU в течение этого периода. Если устройство получает пакеты TC BPDU в течение этого периода, оно удаляет их по истечении этого периода. Это может предотвратить частое удаление устройством записей MAC-адресов и записей ARP.

TC Guard

TC Protection обеспечивает удаление менее динамичных MAC-адресов и записей ARP, когда в сети генерируется большое количество пакетов TC. Однако устройство, получающее пакеты атак TC, по-прежнему выполняет множество операций по удалению, и пакеты TC могут распространяться, затрагивая всю сеть. Пользователи могут включить TC Guard, чтобы предотвратить распространение пакетов TC глобально или по порту. Если TC Guard включена глобально или для порта, порт, получающий пакеты TC, фильтрует эти пакеты TC или пакеты TC, созданные им самим, чтобы пакеты TC не распространялись на другие порты. Это может эффективно контролировать возможные атаки TC в сети для обеспечения стабильности сети. В частности, на устройствах уровня 3 эта функция может эффективно предотвращать flapping устройства уровня доступа и прерывание основного маршрута.

ПРИМЕЧАНИЕ: при неправильном использовании TC guard связь между сетями прерывается.

ПРИМЕЧАНИЕ: рекомендуется включать эту функцию только при получении в сети нелегальных пакетов атак TC.

ПРИМЕЧАНИЕ: если TC Guard включена глобально, ни один порт не передает пакеты TC другим. Эта функция может быть включена только на портативных устройствах доступа.

ПРИМЕЧАНИЕ: если на порту включена TC Guard, происходят изменения топологии, и пакеты TC, полученные портом, не будут распространяться на другие порты. Эту функцию можно включить только на uplink-портах, особенно на портах ядра конвергенции.

TC Filter

Если TC Guard включена для порта, порт не пересылает пакеты TC, полученные и сгенерированные портом, на другие порты, выполняющие вычисление spanning tree на устройстве. Когда состояние порта изменяется (например, с блокировки на пересылку), порт генерирует пакеты TC, указывая, что топология могла измениться.

В этом случае, поскольку TC Guard предотвращает распространение пакетов TC, устройство может не очистить MAC-адреса порта при изменении топологии сети, что приведет к ошибке пересылки данных.

Чтобы решить эту проблему, вводится TC Filter. TC Filter не обрабатывает пакеты TC, полученные портами, а обрабатывает пакеты TC при нормальных изменениях топологии. Если включен TC Filter, можно избежать проблемы удаления адреса, и основной маршрут не будет прерываться, когда порты, не включенные с помощью PortFast, часто выходят из строя, а записи основного маршрута могут своевременно обновляться при изменении топологии.

ПРИМЕЧАНИЕ: по умолчанию TC Filter отключен.

Проверка исходного MAC-адреса BPDU

Проверка исходного MAC-адреса BPDU предотвращает злонамеренную атаку коммутаторов пакетами BPDU и ненормальную работу MSTP. Когда коммутатор,

подключенный к порту на канале «точка-точка», определен, вы можете включить проверку исходного MAC-адреса BPDU, чтобы получать пакеты BPDU, отправленные только peer-коммутатором, и отбрасывать все остальные пакеты BPDU, тем самым предотвращая вредоносные атаки. Вы можете включить проверку исходного MAC-адреса BPDU в режиме конфигурации интерфейса для определенного порта. Один порт может фильтровать только один MAC-адрес. Если вы запустите команду **no bpdu src-mac-check**, чтобы отключить проверку исходного MAC-адреса BPDU на порту, порт будет получать все пакеты BPDU.

BPDU Filter

Если длина Ethernet BPDU превышает 1500, этот BPDU будет отброшен, что предотвратит получение недопустимых пакетов BPDU.

Auto Edge

Если назначенный порт устройства не получает BPDU от downlink-порта в течение определенного периода (3 секунды), устройство рассматривает сетевое устройство, подключенное к назначенному порту, настраивает порт как пограничный порт и переключает порт напрямую. в состояние пересылки. Пограничный порт будет автоматически идентифицирован как не пограничный порт после получения BPDU.

Вы можете запустить команду **spanning-tree autoedge disabled**, чтобы отключить Auto Edge.

Эта функция включена по умолчанию.

ПРИМЕЧАНИЕ: если Auto Edge конфликтует с настроенным вручную PortFast, приоритет имеет ручная настройка.

ПРИМЕЧАНИЕ: поскольку эта функция используется для быстрого согласования и переадресации между назначенным портом и портом downlink, STP не поддерживает эту функцию. Если назначенный порт находится в состоянии пересылки, конфигурация Auto Edge не действует на этот порт. Требуется только при повторном выполнении быстрого согласования, например, при удалении и подключении сетевого кабеля.

ПРИМЕЧАНИЕ: если для порта включен фильтр BPDU, порт напрямую переходит в состояние пересылки и не идентифицируется автоматически как пограничный порт.

ПРИМЕЧАНИЕ: эта функция применяется только к назначенному порту.

Root Guard

В структуре сети root bridge и резервный root bridge обычно разделены на один и тот же регион. Из-за неправильной настройки обслуживающего персонала или злонамеренных атак в сети root bridge может получить информацию о конфигурации с более высоким приоритетом и тем самым переключиться на резервный root bridge, что приведет к некорректным изменениям топологии сети. Root Guard должен решить эту проблему.

Если для порта включена Root Guard, его роли во всех экземплярах применяются как назначенный порт. Как только порт получит информацию о конфигурации с более высоким приоритетом, он входит в несовместимое с root (блокирующее) состояние. Если порт не получает информацию о конфигурации с более высоким приоритетом в течение периода, он возвращается в исходное состояние.

Если порт переходит в состояние блокировки из-за Root Guard, вы можете вручную восстановить порт в нормальное состояние, отключив Root Guard на этом порту или отключив защиту spanning tree (запустив **spanning-tree guard none** в режиме настройки интерфейса).

ПРИМЕЧАНИЕ: если Root Guard используется неправильно, сетевое соединение будет прервано.

ПРИМЕЧАНИЕ: если защита root включена для неназначенного порта, этот порт будет применен как назначенный порт и перейдет в состояние BKN. Это указывает на то, что порт переходит в состояние блокировки из-за root-несогласованности.

ПРИМЕЧАНИЕ: если порт переходит в состояние BKN из-за получения информации о конфигурации с более высоким приоритетом в MST0, этот порт будет переведен в состояние BKN во всех остальных случаях.

ПРИМЕЧАНИЕ: Root Guard и Loop Guard не могут действовать на порт одновременно.

Loop Guard

Из-за сбоя однонаправленного канала root-порт или резервный порт становится назначенным портом и переходит в состояние пересылки, если он не получает BPDU, вызывая сетевую петлю. Loop Guard должен предотвратить эту проблему.

Если порт с Loop Guardне получает BPDU, порт переключает свою роль, но остается в состоянии отбрасывания до тех пор, пока не получит BPDU и не пересчитает spanning tree.

ПРИМЕЧАНИЕ: можно включить Loop Guard глобально или для порта.

ПРИМЕЧАНИЕ: Root Guard и Loop Guard не могут действовать на порт одновременно.

ПРИМЕЧАНИЕ: перед перезапуском MSTP на порту порт переходит в состояние блокировки в Loop Guard. Если порт по-прежнему не получает BPDU после перезапуска MSTP, он становится назначенным портом и переходит в состояние пересылки. Поэтому рекомендуется определить причину, по которой порт переходит в состояние блокировки в Loop Guard, и устранить ошибку как можно скорее перед перезапуском MSTP. В противном случае после перезапуска MSTP топология spanning tree все равно станет ненормальной.

Прозрачная передача BPDU

В IEEE 802.1Q MAC-адрес получателя 01-80-C2-00-00-00 BPDU используется в качестве зарезервированного адреса. То есть устройства, совместимые с IEEE 802.1Q, не пересылают полученные пакеты BPDU. Однако устройствам может потребоваться прозрачная передача пакетов BPDU при фактическом развертывании сети. Например, если STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы spanning tree между устройствами было правильно рассчитано.

ПРИМЕЧАНИЕ: прозрачная передача BPDU отключена по умолчанию.

ПРИМЕЧАНИЕ: прозрачная передача BPDU вступает в силу только тогда, когда STP отключен. Если на устройстве включен протокол STP, оно не передает прозрачно пакеты BPDU.

Туннель BPDU

Сеть QinQ обычно делится на две части: сеть клиента и сеть SP. Прежде чем пользовательский пакет войдет в сеть SP, он инкапсулируется тегом VLAN сети SP, а также сохраняет исходный тег VLAN в качестве данных. В результате пакет содержит две метки VLAN для прохождения через сеть SP. В сети SP пакеты передаются только на основе тега VLAN внешнего уровня. Когда пакеты покидают сеть SP, тег VLAN внешнего уровня удаляется.

Функция прозрачной передачи пакетов STP, а именно туннель BPDU, может использоваться для реализации передачи пакетов STP между клиентской сетью без какого-либо влияния на сеть SP. Если пакет STP, отправленный из клиентской сети, входит в PE, PE меняет MAC-адрес назначения пакета на приватный адрес до того, как пакет будет перенаправлен сетью SP. Когда пакет достигает PE на peer end, PE изменяет MAC-адрес назначения на общедоступный (public) адрес и возвращает пакет в клиентскую сеть на peer end, реализуя прозрачную передачу по сети SP. В этом случае STP в сети клиента рассчитывается независимо от STP в сети поставщика сервисов.

10.2.7.2. Связанная конфигурация

Настройка PortFast

- По умолчанию PortFast отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast default**, чтобы включить PortFast на всех портах, и команду **no spanning-tree portfast default**, чтобы отключить PortFast на всех портах.
- В режиме конфигурации интерфейса запустите команду **spanning-tree portfast**, чтобы включить PortFast на порту, и команду **spanning-tree portfast disabled**, чтобы отключить PortFast на порту.

Настройка BPDU Guard

- BPDU Guard отключена по умолчанию.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast bpduguard default**, чтобы включить BPDU Guard на всех портах, и команду **no spanning-tree portfast bpduguard default**, чтобы отключить BPDU Guard на всех портах.
- В режиме конфигурации интерфейса запустите команду **spanning-tree bpduguard enabled**, чтобы включить BPDU Guard на порту, и команду **spanning-tree bpduguard disabled**, чтобы отключить BPDU Guard на порту.

Настройка BPDU Filter

- По умолчанию BPDU Filter отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast bpdufilter default**, чтобы включить BPDU Filter на всех портах, и команду **no spanning-tree portfast bpdufilter default**, чтобы отключить BPDU Filter на всех портах.
- В режиме конфигурации интерфейса запустите команду **spanning-tree bpdufilter enabled**, чтобы включить BPDU Filter на порту, и команду **spanning-tree bpdufilter disabled**, чтобы отключить BPDU Filter на порту.

Настройка TC Protection

- TC Protection по умолчанию отключена.
- В режиме глобальной конфигурации запустите команду **spanning-tree tc-protection**, чтобы включить TC Protection на всех портах, и команду **no spanning-tree tc-protection**, чтобы отключить TC Protection на всех портах.
- TC Protection может быть включена или отключена только глобально.

Включение TC Guard

- TC Guard по умолчанию отключена.
- В режиме глобальной конфигурации запустите команду **spanning-tree tc-protection tc-guard**, чтобы включить TC Guard на всех портах, и команду **no spanning-tree tc-protection tc-guard**, чтобы отключить TC Guard на всех портах.
- В режиме конфигурации интерфейса запустите команду **spanning-tree tc-guard**, чтобы включить TC Guard на порту, и команду **no spanning-tree tc-guard**, чтобы отключить TC Guard на порту.

Настройка TC Filter

- По умолчанию TC Filter отключен.
- В режиме конфигурации интерфейса запустите команду **spanning-tree ignore tc**, чтобы включить TC Filter на порту, и команду **no spanning-tree ignore tc**, чтобы отключить его на порту.

Включение проверки исходного MAC-адреса BPDU

- Проверка исходного MAC-адреса BPDU отключена по умолчанию.
- В режиме конфигурации интерфейса запустите команду **bpdu src-mac-check** *H.H.H*, чтобы включить проверку исходного MAC-адреса BPDU на порту, и команду **no bpdu src-mac-check**, чтобы отключить ее на порту.

Настройка Auto Edge

- Auto Edge отключен по умолчанию.
- В режиме конфигурации интерфейса запустите команду **spanning-tree autoedge**, чтобы включить Auto Edge на порту, и команду **spanning-tree autoedge disabled**, чтобы отключить его на порту.

Настройка Root Guard

- По умолчанию Root Guard отключен.
- В режиме конфигурирования интерфейса выполните команду **spanning-tree guard root**, чтобы включить Root Guard на порту, и команду **no spanning-tree guard root**, чтобы отключить ее на порту.

Настройка Loop Guard

- Loop Guard по умолчанию отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree loopguard default**, чтобы включить Loop Guard на всех портах, и команду **no spanning-tree loopguard default**, чтобы отключить ее на всех портах.
- В режиме конфигурации интерфейса запустите команду **spanning-tree guard loop**, чтобы включить Loop Guard на порту, и команду **no spanning-tree guard loop**, чтобы отключить ее на порту.

Настройка прозрачной передачи BPDU

- Прозрачная передача BPDU отключена по умолчанию.
- В режиме глобальной конфигурации запустите команду **bridge-frame forwarding protocol bpdu**, чтобы включить прозрачную передачу BPDU, и команду **no bridge-frame forwarding protocol bpdu**, чтобы отключить ее.
- Прозрачная передача BPDU вступает в силу только тогда, когда STP отключен. Если на устройстве включен протокол STP, оно не передает прозрачно пакеты BPDU.

Настройка BPDU-туннеля

- Туннель BPDU по умолчанию отключен.
- В режиме глобальной конфигурации запустите команду **l2protocol-tunnel stp**, чтобы глобально включить BPDU-туннель, и команду **no l2protocol-tunnel stp**, чтобы глобально отключить его.
- В режиме конфигурации интерфейса запустите команду **l2protocol-tunnel stp enable**, чтобы включить BPDU-туннель на порту, и команду **no l2protocol-tunnel stp enable**, чтобы отключить его на порту.
- Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса.

10.3. Конфигурация

Конфигурация	Описание и команда	
Включение STP	(Обязательно) Используется для включения STP	
	spanning-tree	Включает STP и настраивает основные атрибуты
	spanning-tree mode	Настраивает режим STP
Настройка совместимости STP	(Опционально) Используется для совместимости с устройствами конкурентов	
	spanning-tree compatible enable	Включает режим совместимости порта
	clear spanning-tree detected-protocols	Выполняет обязательную проверку версии для BPDU
Настройка региона MSTP	(Опционально) Используется для настройки региона MSTP	
	spanning-tree mst configuration	Вход в режим конфигурации MST
Включение быстрой конвергенции RSTP	(Опционально) Он используется для настройки того, является ли тип соединения порта соединением «точка-точка»	
	spanning-tree link-type	Настраивает тип канала
Настройка приоритетов	(Опционально) Используется для настройки приоритета коммутатора или приоритета порта	
	spanning-tree priority	Настраивает приоритет коммутатора
	spanning-tree port-priority	Настраивает приоритет порта
Настройка стоимости пути к порту	(Опционально) Используется для настройки стоимости пути порта или метода расчета стоимости пути по умолчанию	
	spanning-tree cost	Настраивает стоимость пути порта
	spanning-tree pathcost method	Настраивает метод расчета стоимости пути по умолчанию

Конфигурация	Описание и команда	
Настройка максимального числа hop-ов для пакета BPDU	(Опционально) Он используется для настройки максимального числа hop'ов пакета BPDU	
	spanning-tree max-hops	Настраивает максимальное количество hop'ов пакета BPDU
Включение функций, связанных с PortFast	(Опционально) Используется для включения функций, связанных с PortFast	
	spanning-tree portfast	Включает PortFast
	spanning-tree portfast bpduguard default	Включает BPDU Guard на всех портах
	spanning-tree bpduguard enabled	Включает BPDU Guard на порту
	spanning-tree portfast bpdufilter default	Включает BPDU Filter на всех портах
	spanning-tree bpdufilter enabled	Включает BPDU Filter на порту
Включение функций, связанных с TC	(Опционально) Используется для включения функций, связанных с TC	
	spanning-tree tc-protection	Включает TC Guard
	spanning-tree tc-protection tc-guard	Включает TC Guard на всех портах
	spanning-tree tc-guard	Включает TC Guard на порту
	spanning-tree ignore tc	Включает TC Filter на порту
Включение проверки исходного MAC-адреса BPDU	(Опционально) Используется для включения проверки исходного MAC-адреса BPDU	
	bpdu src-mac-check	Включает проверку исходного MAC-адреса BPDU на порту

Конфигурация	Описание и команда	
Настройка Auto Edge	(Опционально) Используется для настройки Auto Edge	
	spanning-tree autoedge	Включает Auto Edge на порту. Эта функция включена по умолчанию
Включение функций, связанных с Guard	(Опционально) Используется для включения функций Guard портов	
	spanning-tree guard root	Включает Root Guard на порту
	spanning-tree loopguard default	Включает Loop Guard на всех портах
	spanning-tree guard loop	Включает Loop Guard на порту
	spanning-tree guard none	Отключает функцию Guard порта
Включение прозрачной передачи BPDU	(Опционально) Используется для включения прозрачной передачи BPDU	
	bridge-frame forwarding protocol bpdu	Включает прозрачную передачу BPDU
Включение BPDU-туннеля	(Опционально) Используется для включения туннеля BPDU	
	l2protocol-tunnel stp	Включает туннель BPDU глобально
	l2protocol-tunnel stp enable	Включает BPDU-туннель на порту
	l2protocol-tunnel stp tunnel-dmac	Настраивает прозрачный адрес передачи туннеля BPDU

10.3.1. Включение STP

10.3.1.1. Эффект конфигурации

- Включите STP глобально и настройте основные атрибуты.
- Настройте режим STP.

10.3.1.2. Примечания

- STP по умолчанию отключен. После включения STP устройство начинает работать с STP. Устройство использует MSTP по умолчанию.
- Режим STP по умолчанию — режим MSTP.
- STP и прозрачное соединение множества каналов (TRILL) центра обработки данных не могут быть включены одновременно.
- Параметры таймера STP вступают в силу только тогда, когда устройство выбрано в качестве root bridge spanning tree. То есть параметры таймера не root bridge должны использовать значения таймера root bridge.

10.3.1.3. Шаги настройки

Включение STP

- Обязательный.
- Если не указано иное, включите STP на каждом устройстве.
- Запустите **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*] для включения STP и настройки основных атрибутов.

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы сервисов. Диапазоны значений forward-time, hello-time и max-age связаны. Если изменить один из них, это повлияет на два других диапазона.Эти три значения должны соответствовать следующему условию: 2×(Hello Time + 1 секунда) ≤ Max-Age Time ≤ 2×(Forward-Delay Time – 1 секунда). В противном случае топология может стать нестабильной.

Команда	**spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **tx-hold-count** *numbers*]
Описание параметров	**forward-time** *seconds*: указывает интервал изменения состояния порта. Значение варьируется от 4 до 30 секунд. Значение по умолчанию — 15 секунд. **hello-time** *seconds*: указывает интервал, через который устройство отправляет пакет BPDU. Диапазон значений от 1 до 10 секунд. Значение по умолчанию — 2 секунды. **max-age** *seconds*: указывает самое длинное время жизни пакета BPDU. Значение варьируется от 6 до 40 секунд. Значение по умолчанию — 20 секунд. **tx-hold-count** *numbers*: указывает максимальное количество BPDU, отправляемых в секунду. Диапазон значений от 1 до 10. Значение по умолчанию — 3
По умолчанию	STP по умолчанию отключен
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Диапазоны значений forward-time, hello-time и max-age связаны. Если изменить один из них, это повлияет на два других диапазона.Эти три значения должны соответствовать следующему условию: 2×(Hello Time + 1 секунда) ≤ Max-Age Time ≤ 2×(Forward-Delay Time — 1 секунда). В противном случае топология может стать нестабильной

Настройка режима STP

- Опционально.
- Согласно родственным стандартам протокола 802.1, STP, RSTP и MSTP взаимно совместимы и не требуют настройки администратором. Однако устройства некоторых поставщиков не работают в соответствии со стандартами протокола 802.1, что может привести к несовместимости. Поэтому QTECH предоставляет администратору команду переключить режим STP на более низкую версию, если устройства других производителей несовместимы с устройствами QTECH.
- Запустите **spanning-tree mode** [**stp** | **rstp** | **mstp**] для изменения режима STP.

Команда	**spanning-tree mode** [**stp** | **rstp** | **mstp**]
Описание параметров	**stp**: протокол spanning tree (IEEE 802.1d) **rstp**: протокол быстрого spanning tree (IEEE 802.1w) **mstp**: протокол множественного spanning tree (IEEE 802.1s)
По умолчанию	Значение по умолчанию — mstp
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Однако устройства некоторых поставщиков не работают в соответствии со стандартами протокола 802.1, что может привести к несовместимости. Если устройства других производителей несовместимы с устройствами QTECH, запустите эту команду, чтобы переключить режим STP на более низкую версию

10.3.1.4. Проверка

Отобразите конфигурацию.

10.3.1.5. Связанные команды

Настройка STP

Команда	**spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **tx-hold-count** *numbers*]
Описание параметров	**forward-time** *seconds*: указывает интервал изменения состояния порта. Значение варьируется от 4 до 30 секунд. Значение по умолчанию — 15 секунд

Описание параметров	**hello-time** *seconds*: указывает интервал, через который устройство отправляет пакет BPDU. Диапазон значений от 1 до 10 секунд. Значение по умолчанию — 2 секунды. **max-age** *seconds*: указывает самый длинный TTL пакета BPDU. Это значение колеблется от 6 до 40 секунд. Значение по умолчанию — 20 секунд. **tx-hold-count** *numbers*: указывает максимальное количество BPDU, отправляемых в секунду. Диапазон значений от 1 до 10. Значение по умолчанию — 3
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Диапазоны значений forward-time, hello-time, and max-age связаны. Если изменить один из них, это повлияет на два других диапазона. Эти три значения должны соответствовать следующему условию: 2×(Hello Time + 1 секунда) ≤ Max-Age Time ≤ 2×(Forward-Delay Time – 1 секунда) В противном случае топология может стать нестабильной, и конфигурация не будет работать

Настройка режима STP

Команда	**spanning-tree mode** [**stp** | **rstp** | **mstp**]
Описание параметров	**stp**: протокол spanning tree (IEEE 802.1d) **rstp**: протокол быстрого spanning tree (IEEE 802.1w) **mstp**: протокол множественного spanning tree (IEEE 802.1s)
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Однако устройства некоторых поставщиков не работают в соответствии со стандартами протокола 802.1, что может привести к несовместимости. Если устройства других производителей несовместимы с устройствами QTECH, запустите эту команду, чтобы переключить режим STP на более низкую версию

10.3.1.6. Пример конфигурации

Включение STP и настройка параметров таймера

Сценарий:

Рисунок 10-20.

Шаги настройки	• Включите STP и установите режим STP на STP на устройствах. • Настройте параметры таймера root bridge DEV A следующим образом: Hello Time = 4 c, Max Age = 25 c, Forward Delay = 18 c
DEV A	Шаг 1. Включите STP и установите режим STP на STP. QTECH#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mode stp Шаг 2. Настройте параметры таймера root bridge DEV A. QTECH(config)#spanning-tree hello-time 4 QTECH(config)#spanning-tree max-age 25 QTECH(config)#spanning-tree forward-time 18
DEV B	Включите STP и установите режим STP на STP. QTECH#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mode stp
Проверка	Запустите команду **show spanning-tree summary**, чтобы отобразить топологию spanning tree и параметры конфигурации протокола
DEV A	QTECH#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0

	Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 0 Address 08c6.b3.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Bound(STP) Gi0/1 Root FWD 20000 128 False P2p Bound(STP)

10.3.2. Настройка совместимости STP

10.3.2.1. Эффект конфигурации

- Включите режим совместимости порта, чтобы реализовать взаимосвязь между устройствами QTECH и устройствами других поставщиков услуг.
- Включите миграцию протокола, чтобы выполнить принудительную проверку версии, чтобы повлиять на совместимость между RSTP и STP.

10.3.2.2. Примечания

- Если для порта включен режим совместимости, этот порт будет добавлять различную информацию MSTI в подлежащий отправке BPDU на основе текущего порта, чтобы реализовать взаимосвязь между устройствами QTECH и устройствами других поставщиков услуг.
- При включении совместимости на порту убедитесь, что для порта указана правильная информация об обрезке (trimming information) VLAN. Рекомендуется настроить согласованные списки VLAN для портов на обоих концах канала.

10.3.2.3. Шаги настройки

Включение режима совместимости на порту

Опционально.

Настройка миграции протокола

- Опционально.
- Если peer-устройство поддерживает RSTP, вы можете включить проверку версии на локальном устройстве, чтобы два устройства запускали RSTP.

10.3.2.4. Проверка

Отобразите конфигурацию.

10.3.2.5. Связанные команды

Включение режима совместимости на порту

Команда	**spanning-tree compatible enable**
По умолчанию	Режим совместимости отключен для порта по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если для порта включен режим совместимости, этот порт будет добавлять различную информацию MSTI в подлежащий отправке BPDU на основе текущего порта, чтобы реализовать взаимосвязь между устройствами QTECH и устройствами других поставщиков услуг

Включение миграции протокола

Команда	**clear spanning-tree detected-protocols** [**interface** *interface-id*]
Описание параметров	**interface** *interface-id*: указывает порт
Командный режим	Привилегированный режим EXEC
Руководство по использованию	Эта команда используется для того, чтобы заставить порт отправлять пакеты RSTP BPDU и выполнять их принудительную проверку

10.3.2.6. Пример конфигурации

Включение совместимости с STP

Сценарий:

Рисунок 10-21.

Шаги настройки	• Настройте экземпляры 1 и 2 на устройствах A и B и сопоставьте экземпляр 1 с VLAN 10, а экземпляр 2 с VLAN 20. • Настройте Gi0/1 и Gi0/2, чтобы они принадлежали соответственно VLAN 10 и VLAN 20, и включите совместимость с STP
DEV A	Шаг 1. Настройте экземпляры 1 и 2 и сопоставьте экземпляры 1 и 2 соответственно с VLAN 10 и 20. QTECH#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. QTECH(config)#spanning-tree mst configuration QTECH(config-mst)#instance 1 vlan 10 QTECH(config-mst)#instance 2 vlan 20 Шаг 2. Настройте VLAN, к которой принадлежит порт, и включите STP-совместимость на порту. QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport access vlan 10 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable QTECH(config-if-GigabitEthernet 0/1)#int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)#switchport access vlan 20 QTECH(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable
DEV B	Выполните те же действия, что и для DEV A
Проверка	Запустите команду **show spanning-tree summary**, чтобы проверить правильность расчета топологии spanning tree

DEV A

```
QTECH#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
Root ID Priority 32768
        Address 08c6.b3.78cc
        this bridge is root
        Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Bridge ID Priority 32768
        Address 08c6.b3.78cc
        Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

Interface      Role Sts Cost         Prio    OperEdge     Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2          Desg FWD 20000      128     False        P2p
Gi0/1          Desg FWD 20000      128     False        P2p

MST 1 vlans map : 10
Region Root Priority 32768
        Address 08c6.b3.78cc
        this bridge is region root

Bridge ID Priority 32768
        Address 08c6.b3.78cc

Interface      Role Sts Cost         Prio     OperEdge     Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1          Desg FWD 20000      128      False        P2p

MST 2 vlans map : 20
Region Root Priority 32768
        Address 08c6.b3.78cc
        this bridge is region root

Bridge ID Priority 32768
```

	Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 08c6.b3.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 08c6.b3.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Gi0/1 Root FWD 20000 128 False P2p MST 1 vlans map : 10 Region Root Priority 32768 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 32768 Address 08c6.b3.3344 Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/1 Root FWD 20000 128 False P2p MST 2 vlans map : 20

```
Region Root Priority 32768
        Address 08c6.b3.78cc
        this bridge is region root

Bridge ID Priority 32768
        Address 08c6.b3.3344

Interface       Role Sts Cost       Prio      OperEdge    Type
--------------- ---- --- ---------- -------- -------- ----------------
Gi0/2           Root FWD 20000      128       False       P2p
```

10.3.3. Настройка региона MSTP

10.3.3.1. Эффект конфигурации

Настройте регион MSTP, чтобы определить, какие устройства принадлежат к одному и тому же региону MSTP и тем самым повлиять на топологию сети.

10.3.3.2. Примечания

- Чтобы несколько устройств принадлежали к одному и тому же региону MSTP, настройте для них одно и то же имя, номер версии и таблицу сопоставления экземпляров и VLAN.
- Вы можете настроить виртуальные локальные сети для экземпляров с 0 по 64, а затем оставшиеся виртуальные локальные сети будут автоматически выделены для экземпляра 0. Одна виртуальная локальная сеть принадлежит только одному экземпляру.
- Таблицу сопоставления экземпляр-VLAN рекомендуется настраивать после отключения STP. После настройки снова включите MSTP, чтобы обеспечить стабильность и конвергенцию топологии сети.

10.3.3.3. Шаги настройки

Настройка региона MSTP

- Опционально.
- Настройте регион MSTP, если несколько устройств должны принадлежать одному региону MSTP.

10.3.3.4. Проверка

Отобразите конфигурацию.

10.3.3.5. Связанные команды

Вход в режим настройки региона MSTP

- Опционально.
- Настройте регион MSTP, если несколько устройств должны принадлежать одному региону MSTP.

- Запустите команду **spanning-tree mst configuration**, чтобы войти в режим конфигурации MST.
- Запустите команду **instance** *instance-id* **vlan** *vlan-range*, чтобы настроить сопоставление MSTI-VLAN.
- Запустите команду **name** *name*, чтобы настроить имя MST.
- Запустите команду **revision** *version*, чтобы настроить номер версии MST.

Команда	**spanning-tree mst configuration**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы войти в режим конфигурации MST

Настройка сопоставления экземпляра и VLAN

Команда	**instance** *instance-id* **vlan** *vlan-range*
Описание параметров	*instance-id*: указывает идентификатор MSTI в диапазоне от 0 до 64. *vlan-range*: указывает идентификатор VLAN в диапазоне от 1 до 4094
По умолчанию	Сопоставление экземпляр-VLAN по умолчанию таково, что все VLAN находятся в экземпляре 0
Командный режим	Режим конфигурации MST
Руководство по использованию	Чтобы добавить группу VLAN в MSTI, выполните эту команду. Например, instance 1 vlan 2-200: добавляет VLAN 2–200 к экземпляру 1. instance 1 vlan 2,20,200: добавляет VLAN 2, 20 и 200 к экземпляру 1. Вы можете использовать форму **no** этой команды для удаления VLAN из экземпляра. Удаленные VLAN автоматически перенаправляются в экземпляр 0

Настройка имени версии MST

Команда	**name** *name*
Описание параметров	*name*: указывает имя MST. Он состоит максимум из 32 байтов
По умолчанию	Имя по умолчанию представляет собой пустую строку символов

Командный режим	Режим конфигурации MST

Настройка номера версии MST

Команда	**revision** *version*
Описание параметров	*version*: указывает номер версии MST в диапазоне от 0 до 65 535
По умолчанию	Номер версии по умолчанию — 0
Командный режим	Режим конфигурации MST

10.3.3.6. Проверка

- Отобразите конфигурацию.
- Запустите команду **show spanning-tree mst configuration**, чтобы отобразить конфигурацию региона MSTP.

10.3.3.7. Пример конфигурации

Включение MSTP для достижения балансировки нагрузки VLAN в топологии MSTP+VRRP

Сценарий:

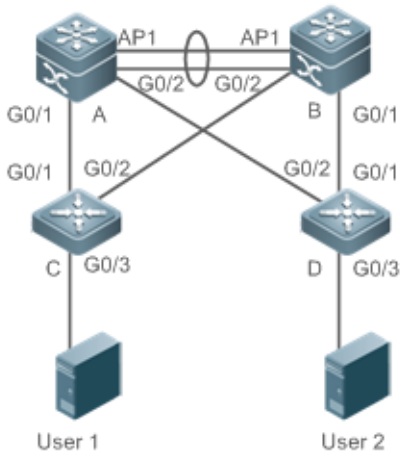


Рисунок 10-22.

Шаги настройки	• Включите MSTP и создайте экземпляры 1 и 2 на коммутаторах A, B, C и D. • Настройте коммутатор A в качестве root bridge для экземпляров 0 и 1, а коммутатор B — в качестве root bridge для экземпляра 2

Шаги настройки	• Настройте коммутатор A в качестве master-устройства VRRP для сетей VLAN 1 и 10, а коммутатор B — в качестве master-устройства VRRP для сети VLAN 20
A	Шаг 1. Настройте VLAN 10 и 20 и настройте порты как магистральные порты. A(config)#vlan 10 A(config-vlan)#vlan 20 A(config-vlan)#exit A(config)#int range gi 0/1-2 A(config-if-range)#switchport mode trunk A(config-if-range)#int ag 1 A(config-if-AggregatePort 1)# switchport mode trunk Шаг 2. Включите MSTP и создайте экземпляры 1 и 2. A(config)#spanning-tree A(config)# spanning-tree mst configuration A(config-mst)#instance 1 vlan 10 A(config-mst)#instance 2 vlan 20 A(config-mst)#exit Шаг 3. Настройте коммутатор A в качестве root bridge экземпляров 0 и 1. A(config)#spanning-tree mst 0 priority 4096 A(config)#spanning-tree mst 1 priority 4096 A(config)#spanning-tree mst 2 priority 8192 Шаг 4. Настройте приоритеты VRRP, чтобы коммутатор A мог действовать как master-устройство VRRP в сети VLAN 10, и настройте IP-адрес виртуального шлюза VRRP. A(config)#interface vlan 10 A(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0 A(config-if-VLAN 10) vrrp 1 priority 120 A(config-if-VLAN 10) vrrp 1 ip 192.168.10.1 Шаг 5. Установите для приоритета VRRP значение по умолчанию 100, чтобы коммутатор A мог действовать как резервное устройство VRRP для VLAN 20. A(config)#interface vlan 20 A(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0 A(config-if-VLAN 20) vrrp 1 ip 192.168.20.1

B	Шаг 1. Настройте VLAN 10 и 20 и настройте порты как магистральные порты. B(config)#vlan 10 B(config-vlan)#vlan 20 B(config-vlan)#exit B(config)#int range gi 0/1-2 B(config-if-range)#switchport mode trunk B(config-if-range)#int ag 1 B(config-if-AggregatePort 1)# switchport mode trunk Шаг 2. Включите MSTP и создайте экземпляры 1 и 2. B(config)#spanning-tree B(config)# spanning-tree mst configuration B(config-mst)#instance 1 vlan 10 B(config-mst)#instance 2 vlan 20 B(config-mst)#exit Шаг 3. Настройте коммутатор A в качестве root bridge экземпляра 2. B(config)#spanning-tree mst 0 priority 8192 B(config)#spanning-tree mst 1 priority 8192 B(config)#spanning-tree mst 2 priority 4096 Шаг 4. Настройте IP-адрес виртуального шлюза VRRP. B(config)#interface vlan 10 B(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0 B(config-if-VLAN 10) vrrp 1 ip 192.168.10.1 Шаг 5. Установите для приоритета VRRP значение 120, чтобы коммутатор B мог действовать как резервное устройство VRRP для VLAN 20. B(config)#interface vlan 20 B(config-if-VLAN 20)vrrp 1 priority 120 B(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0 B(config-if-VLAN 20) vrrp 1 ip 192.168.20.1
C	Шаг 1. Настройте VLAN 10 и 20 и настройте порты как магистральные порты. C(config)#vlan 10 C(config-vlan)#vlan 20 C(config-vlan)#exit

	C(config)#int range gi 0/1-2 C(config-if-range)#switchport mode trunk Шаг 2. Включите MSTP и создайте экземпляры 1 и 2. C(config)#spanning-tree C(config)# spanning-tree mst configuration C(config-mst)#instance 1 vlan 10 C(config-mst)#instance 2 vlan 20 C(config-mst)#exit Шаг 3. Настройте порт, соединяющий устройство C напрямую с пользователями, как порт PortFast и включите защиту BPDU. C(config)#int gi 0/3 C(config-if-GigabitEthernet 0/3)#spanning-tree portfast C(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
D	Выполните те же действия, что и для устройства C
Проверка	• Запустите команду **show spanning-tree summary**, чтобы проверить правильность расчета топологии spanning tree. • Запустите команду **show vrrp brief**, чтобы проверить, успешно ли созданы основные/резервные устройства VRRP
A	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 4096 Address 08c6.b3.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p

	Gi0/2 Desg FWD 200000 128 False P2p MST 1 vlans map : 10 Region Root Priority 4096 Address 08c6.b3.3344 this bridge is region root Bridge ID Priority 4096 Address 08c6.b3.3344 Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 2 vlans map : 20 Region Root Priority 4096 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 8192 Address 08c6.b3.3344 Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Root FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p
B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 8192 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec

	Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Root FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 1 vlans map : 10 Region Root Priority 4096 Address 08c6.b3.3344 this bridge is region root Bridge ID Priority 8192 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Root FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p MST 2 vlans map : 20 Region Root Priority 4096 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 4096 Address 08c6.b3.78cc Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Ag1 Desg FWD 19000 128 False P2p Gi0/1 Desg FWD 200000 128 False P2p Gi0/2 Desg FWD 200000 128 False P2p
C	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 08c6.b3.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

	Bridge ID Priority 32768 Address 08c6.b3.00ea Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 1 vlans map : 10 Region Root Priority 4096 Address 08c6.b3.3344 this bridge is region root Bridge ID Priority 32768 Address 08c6.b3.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 2 vlans map : 20 Region Root Priority 4096 Address 08c6.b3.78cc this bridge is region root Bridge ID Priority 32768 Address 08c6.b3.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Root FWD 200000 128 P2p False Fa0/1 Altn BLK 200000 128 P2p False
D	Опущено

10.3.3.8. Распространенные ошибки

- Конфигурации региона MST несовместимы с топологией MSTP.

- VLAN не создаются до того, как вы настроите сопоставление между экземпляром и VLAN.
- Устройство запускает STP или RSTP в топологии MSTP+VRRP, но вычисляет spanning tree в соответствии с алгоритмами разных регионов MST.

10.3.4. Включение быстрой конвергенции RSTP

10.3.4.1. Эффект конфигурации

Настройте тип канала, чтобы обеспечить быструю сходимость RSTP.

10.3.4.2. Примечания

- Если тип соединения порта — соединение «точка-точка», RSTP может быстро сходиться. Дополнительные сведения см. в разделе Принцип работы «Быстрая конвергенция RSTP». Если тип соединения не настроен, устройство автоматически устанавливает тип соединения в зависимости от дуплексного режима порта. Если порт находится в полнодуплексном режиме, устройство устанавливает тип соединения «точка-точка». Если порт находится в полудуплексном режиме, устройство устанавливает тип соединения как shared (общий). Вы также можете принудительно настроить тип соединения, чтобы определить, является ли соединение порта соединением «точка-точка».
- Тип соединения порта связан со скоростью и дуплексным режимом. Если порт находится в полудуплексном режиме, тип соединения является shared.

10.3.4.3. Шаги настройки

Настройка типа канала

Опционально.

10.3.4.4. Проверка

Отобразите конфигурацию

Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*, чтобы отобразить конфигурацию spanning tree порта.

10.3.4.5. Связанные команды

Настройка типа канала

Команда	**spanning-tree link-type** [**point-to-point** | **shared**]
Описание параметров	**point-to-point**: принудительно настраивает тип связи порта как «точка-точка». **shared**: принудительно настраивает тип ссылки порта как shared
По умолчанию	Если порт находится в полнодуплексном режиме, тип соединения порта — «точка-точка». Если порт находится в полудуплексном режиме, тип соединения порта является shared
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Если тип соединения порта — соединение «точка-точка», RSTP может быстро сходиться. Если тип соединения не настроен, устройство автоматически устанавливает тип соединения в зависимости от дуплексного режима порта

10.3.4.6. Пример конфигурации

Включение быстрой конвергенции RSTP

Шаги настройки	Установите для порта тип связи «точка-точка»
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point
Проверка	Запустите команду **show spanning-tree summary**, чтобы отобразить тип связи порта
	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 32768 Address 08c6.b3.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 08c6.b3.3344 Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- --------- -------- -------- ---------- Gi0/1 Root FWD 20000 128 False P2p

10.3.5. Настройка приоритетов

10.3.5.1. Эффект конфигурации

- Настройте приоритет коммутатора, чтобы определить устройство как root всей сети и определить топологию всей сети.
- Настройте приоритет порта, чтобы определить, какой порт переходит в состояние пересылки.

10.3.5.2. Примечания

- Рекомендуется установить приоритет основного устройства выше (на меньшее значение) для обеспечения стабильности всей сети. Разным экземплярам можно назначить разные приоритеты коммутатора, чтобы каждый экземпляр запускал независимый STP на основе назначенных приоритетов. Устройства в разных регионах используют приоритет только CIST (экземпляр 0). Как описано в идентификаторе моста, приоритет коммутатора имеет 16 дополнительных значений: 0, 4096, 8192, 12 288, 16 384, 20 480, 24 576, 28 672, 32 768, 36 864, 40 960, 45 056, 49 152, 53 248, 57 344, 61 440. Они являются целыми числами кратными 4096. Значение по умолчанию — 32 768.
- Если два порта подключены к общему устройству, устройство выбирает порт с более высоким приоритетом (меньшее значение) для перехода в состояние пересылки и порт с более низким приоритетом (большее значение) для перехода в состояние отбрасывания. Если два порта имеют одинаковый приоритет, устройство выбирает порт с меньшим идентификатором порта для перехода в состояние переадресации. Вы можете назначить разные приоритеты портов для разных экземпляров на порту, чтобы каждый экземпляр запускал независимый STP на основе назначенных приоритетов.
- Подобно приоритету коммутатора, приоритет порта также имеет 16 дополнительных значений: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. Они являются целыми числами кратными 16. Значение по умолчанию — 128.
- Измененный приоритет порта действует только на указанный порт.

10.3.5.3. Шаги настройки

Настройка приоритета коммутатора

- Опционально.
- Чтобы изменить root или топологию сети, настройте приоритет коммутатора.

Настройка приоритета порта

- Опционально.
- Чтобы изменить предпочтительный порт, входящий в состояние переадресации, настройте приоритет порта.

10.3.5.4. Проверка

Отобразите конфигурацию

Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*, чтобы отобразить конфигурацию spanning tree порта.

10.3.5.5. Связанные команды

Настройка приоритета коммутатора

Команда	**spanning-tree** [**mst** *instance-id*] **priority** *priority*
Описание параметров	**mst** *instance-id*: указывает идентификатор экземпляра в диапазоне от 0 до 64. **priority** *priority*: указывает приоритет коммутатора. Есть 16 необязательных значений: 0, 4096, 8192, 12 288, 16 384, 20 480, 24 576,

	28 672, 32 768, 36 864, 40 960, 45 056, 49 152, 53 248, 57 344, 61 440. Они являются целыми числами кратными 4096
По умолчанию	Значение по умолчанию для *instance-id* равно 0, а для *priority* — 32 768
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте приоритет коммутатора, чтобы определить устройство как root всей сети и определить топологию всей сети

Настройка приоритета порта

Команда	**spanning-tree** [**mst** *instance-id*] **port-priority** *priority*
Описание параметров	**mst** *instance-id*: указывает идентификатор экземпляра в диапазоне от 0 до 64. **port-priority** *priority*: указывает приоритет порта. Есть 16 необязательных значений: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. Они кратны 4096
По умолчанию	Значение *instance-id* по умолчанию равно 0. Значение *priority* по умолчанию равно 128
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если в регионе возникает петля, предпочтительнее использовать порт с более высоким приоритетом для перехода в состояние пересылки. Если два порта имеют одинаковый приоритет, выбирается порт с меньшим идентификатором порта, чтобы войти в состояние пересылки. Запустите эту команду, чтобы определить, какой порт в петле региона переходит в состояние пересылки

10.3.5.6. Пример настройки

Настройка приоритета порта

Сценарий:

Рисунок 10-23.

Шаги настройки	• Настройте приоритет моста так, чтобы DEV A стал root bridge spanning tree. • Настройте приоритет Gi0/2 на DEV A равным 16, чтобы Gi0/2 на DEV B можно было выбрать в качестве корневого порта
DEV A	Шаг 1. Включите STP и настройте приоритет моста. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mst 0 priority 0 Шаг 2. Настройте приоритет Gi 0/2. QTECH(config)# int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16
DEV B	QTECH(config)#spanning-tree
Проверка	Запустите команду **show spanning-tree summary**, чтобы отобразить результат вычисления топологии spanning tree
DEV A	QTECH# QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 0 Address 08c6.b3.3344 Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type

	---------- ---- --- --------- -------- -------- ---------- Gi0/2 Desg FWD 20000 16 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- --------- -------- -------- ---------- Gi0/2 Root FWD 20000 128 False P2p Gi0/1 Altn BLK 20000 128 False P2p

10.3.6. Настройка стоимости пути к порту

10.3.6.1. Эффект конфигурации

- Настройте стоимость пути порта, чтобы определить состояние пересылки порта и топологию всей сети.
- Если стоимость пути порта использует значение по умолчанию, настройте метод расчета стоимости пути, чтобы повлиять на результат расчета.

10.3.6.2. Примечания

- Устройство выбирает порт в качестве корневого порта, если стоимость пути от этого порта до root bridge наименьшая. Следовательно, стоимость пути к порту определяет корневой порт локального устройства. Стоимость пути к порту по умолчанию рассчитывается автоматически на основе скорости порта (Media Speed). Порт с более высокой скоростью будет иметь низкую стоимость пути. Поскольку этот метод может рассчитать наиболее научную стоимость пути, не изменяйте стоимость пути без необходимости. Вы можете назначить разные стоимости пути для разных экземпляров на порту, чтобы каждый экземпляр запускал независимый STP на основе назначенной стоимости пути.
- Если стоимость пути порта использует значение по умолчанию, устройство автоматически вычисляет стоимость пути порта на основе скорости порта. Однако IEEE 802.1d-1998 и IEEE 802.1t определяют разную стоимость пути для одной и той же скорости канала. Значение представляет собой короткое целое число в диапазоне от 1 до 65 535 в 802.1d-1998 и длинное целое число в диапазоне от 1 до 200 000 000 в IEEE 802.1t. Стоимость пути агрегированного порта (AP) имеет

два решения: 1. Решение QTECH: стоимость пути порта × 95 %; 2. Решение, рекомендованное в стандартах: 20 000 000 000/фактическая пропускная способность канала AP, где фактическая пропускная способность канала AP = пропускная способность порта-участника × количество активных портов-участников. Администратор должен унифицировать метод расчета стоимости пути во всей сети. Стандартом по умолчанию является приватный стандарт длинных целых чисел.

- В следующей таблице указана стоимость пути, автоматически настроенная для разной скорости канала в двух решениях.

Скорость порта	Порт	IEEE 802.1d (короткий)	IEEE 802.1t (длинный)	IEEE 802.1t (длинный стандарт)
10M	Общий порт	100	2 000 000	2 000 000
	AP	95	1 900 000	2 000 000÷linkupcnt
100M	Общий порт	19	200 000	200 000
	AP	18	190 000	200 000÷linkupcnt
1000M	Общий порт	4	20 000	20 000
	AP	3	19 000	20 000÷linkupcnt
10 000M	Общий порт	2	2000	2000
	AP	1	1900	20 000÷linkupcnt

- Стандарт длинных целых чисел QTECH используется по умолчанию. После изменения решения на решение стоимости пути, рекомендованное стандартами, стоимость пути AP изменяется в зависимости от количества портов-участников в состоянии UP. Если стоимость пути порта изменится, топология сети также изменится.
- Если AP является статической, linkupcnt в таблице — это количество активных портов-участников. Если AP является AP LACP, то linkupcnt в таблице — это количество портов-участников, пересылающих данные AP. Если ни один из портов-участников в AP не поднимается, linkupcnt равен 1. Подробную информацию о AP и LACP см. в Настройка AP.
- Измененная стоимость пути порта действует только на порт Rx.

10.3.6.3. Шаги настройки

Настройка стоимости пути порта

- Опционально.
- Чтобы определить, через какой порт или по какому пути лучше проходить пакетам данных, настройте стоимость пути порта.

Настройка метода расчета стоимости пути по умолчанию

- Опционально.
- Чтобы изменить метод расчета стоимости пути, настройте метод расчета стоимости пути по умолчанию.

10.3.6.4. Проверка

Отобразите конфигурацию.

Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*, чтобы отобразить конфигурацию spanning tree порта.

10.3.6.5. Связанные команды

Настройка стоимости пути к порту

Команда	**spanning-tree** [**mst** *instance-id*] **cost** *cost*
Описание параметров	**mst** *instance-id*: указывает идентификатор экземпляра в диапазоне от 0 до 64. **cost** *cost*: указывает стоимость пути в диапазоне от 1 до 200 000 000
По умолчанию	Значение по умолчанию *instance-id* равно 0. Значение по умолчанию рассчитывается автоматически на основе скорости порта. 1000 Мбит/с — 20 000 100 Мбит/с — 200 000 10 Мбит/с — 2 000 000
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Большее значение *cost* указывает на более высокую стоимость пути

Настройка метода расчета стоимости пути по умолчанию

Команда	**spanning-tree pathcost method** { *long* [*standard*] | *short* }
Описание параметров	*long*: использует стоимость пути, указанную в 802.1t. *standard*: использует стоимость, рассчитанную в соответствии со стандартом. *short*: использует стоимость пути, указанную в 802.1d
По умолчанию	Стоимость пути, указанная в 802.1t, используется по умолчанию
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Если стоимость пути порта использует значение по умолчанию, устройство автоматически вычисляет стоимость пути порта на основе скорости порта

10.3.6.6. Пример конфигурации

Настройка стоимости пути порта

Сценарий:

Рисунок 10-24.

Шаги настройки	• Настройте приоритет моста так, чтобы DEV A стал root bridge spanning tree. • Настройте стоимость пути Gi 0/2 на DEV B равной 1, чтобы Gi 0/2 можно было выбрать в качестве корневого порта
DEV A	QTECH(config)#spanning-tree QTECH(config)#spanning-tree mst 0 priority 0
DEV B	QTECH(config)#spanning-tree QTECH(config)# int gi 0/2 QTECH(config-if-GigabitEthernet 0/2)# spanning-tree cost 1
Проверка	Запустите команду **show spanning-tree summary**, чтобы отобразить результат вычисления топологии spanning tree
DEV A	QTECH# QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 0

	Address 08c6.b3.3344 Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- --------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
DEV B	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : ALL Root ID Priority 0 Address 08c6.b3.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 08c6.b3.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- Gi0/2 Root FWD 1 128 False P2p Gi0/1 Altn BLK 20000 128 False P2p

10.3.7. Настройка максимального числа hop-ов для пакета BPDU

10.3.7.1. Эффект конфигурации

Настройте максимальное число hop-ов пакета BPDU, чтобы изменить TTL BPDU и, таким образом, повлиять на топологию сети.

10.3.7.2. Примечания

Максимальное число hop'ов для пакета BPDU по умолчанию равно 20. Как правило, не рекомендуется изменять значение по умолчанию.

10.3.7.3. Шаги настройки

Настройка максимального количества hop-ов

(Опционально) Если топология сети настолько велика, что пакет BPDU превышает установленные по умолчанию 20 hop'ов, рекомендуется изменить максимальное количество hop'ов.

10.3.7.4. Проверка

Отобразите конфигурацию.

10.3.7.5. Связанные команды

Настройка максимального количества hop-ов

Команда	**spanning-tree max-hops** *hop-count*
Описание параметров	*hop-count*: указывает количество устройств, через которые проходит BPDU, прежде чем он будет отброшен. Он варьируется от 1 до 40
По умолчанию	Значение по умолчанию для счетчика hop'ов равно 20
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В регионе BPDU, отправляемый root bridge, включает количество hop'ов. Каждый раз, когда BPDU проходит через устройство от root bridge, счетчик hop'ов уменьшается на 1. Когда счетчик hop'ов становится равным 0, время ожидания BPDU истекает, и устройство отбрасывает пакет. Эта команда указывает количество устройств, через которые BPDU проходит в регионе, прежде чем будет отброшен. Изменение максимального количества hop'ов повлияет на все экземпляры

10.3.7.6. Пример конфигурации

Настройка максимального числа hop'ов для пакета BPDU

Шаги настройки	Установите максимальное количество hop'ов для пакета BPDU на 25
	QTECH(config)# spanning-tree max-hops 25
Проверка	Запустите команду **show spanning-tree**, чтобы отобразить конфигурацию
	QTECH# show spanning-tree StpVersion : MSTP SysStpStatus : ENABLED MaxAge : 20 HelloTime : 2 ForwardDelay : 15 BridgeMaxAge : 20 BridgeHelloTime : 2 BridgeForwardDelay : 15 MaxHops: 25 TxHoldCount : 3

	PathCostMethod : Long BPDUGuard : Disabled BPDUFilter : Disabled LoopGuardDef : Disabled ###### mst 0 vlans map : ALL BridgeAddr : 08c6.b3.3344 Priority: 0 TimeSinceTopologyChange : 2d:0h:46m:4s TopologyChanges : 25 DesignatedRoot : 0.08c6.b3.78cc RootCost : 0 RootPort : GigabitEthernet 0/1 CistRegionRoot : 0.08c6.b3.78cc CistPathCost : 20000

10.3.8. Включение функций, связанных с PortFast

10.3.8.1. Эффект конфигурации

- После того, как PortFast включен для порта, порт напрямую переходит в состояние пересылки. Однако, поскольку рабочее состояние PortFast отключается из-за получения BPDU, порт может правильно запустить алгоритм STP и войти в состояние пересылки.
- Если защита BPDU включена для порта, порт переходит в состояние отключения из-за ошибки после получения BPDU.
- Если для порта включен фильтр BPDU, порт не отправляет и не получает BPDU.

10.3.8.2. Примечания

- Глобальная BPDU Guard вступает в силу только в том случае, если PortFast включен на порту.
- Если BPDU Filter включен глобально, порт с поддержкой PortFast не отправляет и не получает BPDU. В этом случае хост, подключающийся напрямую к порту с поддержкой PortFast, не получает никаких BPDU. Если порт меняет свое рабочее состояние PortFast на Disabled после получения BPDU, фильтр BPDU автоматически выходит из строя.
- Глобальный BPDU Filter действует только тогда, когда PortFast включен на порту.

10.3.8.3. Шаги настройки

Включение PortFast

- Опционально.
- Если порт подключается напрямую к сетевому терминалу, настройте этот порт как порт PortFast.

Включение BPDU Guard

- Опционально.
- Если порты устройств подключаются напрямую к сетевым терминалам, вы можете включить BPDU Guard на этих портах, чтобы предотвратить атаки BPDU, вызывающие аномалии в топологии spanning tree. Порт, включенный с BPDU Guard, переходит в состояние отключения из-за ошибки после получения BPDU.
- Если порты устройств подключаются напрямую к сетевым терминалам, вы можете включить BPDU Guard, чтобы предотвратить образование петель на портах. Предпосылкой является то, что устройство downlink (например, хаб) может пересылать пакеты BPDU.

Включение BPDU Filter

- Опционально.
- Чтобы предотвратить влияние аномальных пакетов BPDU на топологию spanning tree, можно включить BPDU Filter на порту для фильтрации аномальных пакетов BPDU.

10.3.8.4. Проверка

Отобразите конфигурацию.

Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*, чтобы отобразить конфигурацию spanning tree порта.

10.3.8.5. Связанные команды

Настройка PortFast

Команда	**spanning-tree portfast**
По умолчанию	PortFast отключен для порта по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	После того, как PortFast включен для порта, порт напрямую переходит в состояние пересылки. Однако, поскольку рабочее состояние PortFast отключается из-за получения BPDU, порт может правильно запустить алгоритм STP и войти в состояние пересылки

Настройка BPDU Guard для всех портов

Команда	**spanning-tree portfast bpduguard default**
По умолчанию	BPDU Guard глобально отключена по умолчанию
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Если BPDU Guard включена для порта, порт переходит в состояние отключения из-за ошибки после получения BPDU. Запустите команду **show spanning-tree**, чтобы отобразить конфигурацию

Настройка BPDU Guard для порта

Команда	**spanning-tree bpduguard enabled**
По умолчанию	BPDU Guard отключена на порту по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если BPDU Guard включена для порта, порт переходит в состояние отключения из-за ошибки после получения BPDU

Настройка BPDU Filter для всех портов

Команда	**spanning-tree portfast bpdufilter default**
По умолчанию	По умолчанию BPDU Filter глобально отключен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Если включен BPDU Filter, соответствующие порты не отправляют и не получают BPDU

Настройка BPDU Filter для порта

Команда	**spanning-tree bpdufilter enabled**
По умолчанию	По умолчанию BPDU Filter для порта отключен
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если для порта включен BPDU Filter, порт не отправляет и не получает BPDU

10.3.8.6. Пример конфигурации

Включение PortFast на порту

Сценарий:

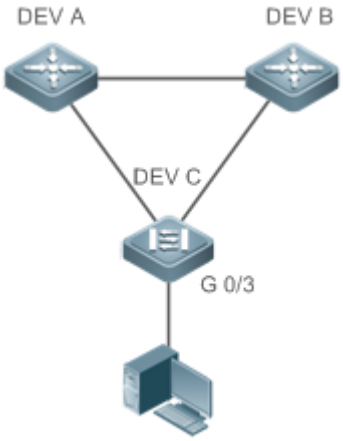


Рисунок 10-25.

Шаги настройки	Настройте Gi 0/3 DEV C в качестве порта PortFast и включите BPDU Guard
DEV C	QTECH(config)# int gi 0/3 QTECH(config-if-GigabitEthernet 0/3)# spanning-tree portfast %Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, switches, bridges to this interface when portfast is enabled,can cause temporary loops. QTECH(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable
Проверка	Запустите команду **show spanning-tree interface**, чтобы отобразить конфигурацию порта
DEV C	QTECH#show spanning-tree int gi 0/3 PortAdminPortFast : Enabled PortOperPortFast : Enabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Enabled PortAdminLinkType : auto PortOperLinkType : point-to-point PortBPDUGuard : Enabled PortBPDUFilter : Disabled PortGuardmode : None

```
###### MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.08c6.b3.3344
PortDesignatedCost : 0
PortDesignatedBridge :0.08c6.b3.3344
PortDesignatedPortPriority : 128
PortDesignatedPort : 4
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
```

10.3.9. Включение функций, связанных с TC

10.3.9.1. Эффект конфигурации

- Если для порта включена BPDU Filter, порт удаляет пакеты TC BPDU в течение заданного времени (обычно 4 секунды) после их получения, предотвращая удаление записей MAC и ARP.
- Если TC protection включена, порт, получающий пакеты TC, фильтрует пакеты TC, полученные или сгенерированные им самим, чтобы пакеты TC не распространялись на другие порты. Таким образом, возможные атаки TC эффективно предотвращаются, чтобы поддерживать стабильность сети.
- TC Filter не обрабатывает пакеты TC, полученные портами, а обрабатывает пакеты TC при нормальных изменениях топологии.

10.3.9.2. Примечания

Рекомендуется включать TC Guard только при получении в сети недопустимых пакетов атаки TC.

10.3.9.3. Шаги настройки

Включение TC Protection

- Опционально.
- TC Protection по умолчанию отключена.

Включение TC Guard

- Опционально.
- TC Guard по умолчанию отключена.
- Чтобы фильтровать пакеты TC, полученные или сгенерированные из-за изменений топологии, вы можете включить TC Guard.

Включение TC Filter

- Опционально.
- По умолчанию TC Filter отключен.
- Чтобы отфильтровать пакеты TC, полученные портом, вы можете включить TC Filter на порту.

10.3.9.4. Проверка

Отобразите конфигурацию.

10.3.9.5. Связанные команды

Включение TC Protection

Команда	**spanning-tree tc-protection**
По умолчанию	TC Protection по умолчанию отключена
Командный режим	Режим глобальной конфигурации

Настройка TC Guard для всех портов

Команда	**spanning-tree tc-protection tc-guard**
По умолчанию	TC Guard глобально отключена по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Включите TC Guard, чтобы предотвратить распространение пакетов TC

Настройка TC Guard для порта

Команда	**spanning-tree tc-guard**
По умолчанию	TC Guard отключена на порту по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Включите TC Guard, чтобы предотвратить распространение пакетов TC

Настройка TC Filter для порта

Команда	**spanning-tree ignore tc**
По умолчанию	По умолчанию TC Filter отключен
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если для порта включен TC Filter, порт не обрабатывает полученные пакеты TC

10.3.9.6. Пример настройки

Включение TC Guard на порту

Шаги настройки	Включите TC Guard на порту
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard
Проверка	Запустите команду **show run interface**, чтобы отобразить конфигурацию TC Guard порта
	QTECH#show run int gi 0/1 Building configuration... Current configuration : 134 bytes interface GigabitEthernet 0/1 switchport mode trunk spanning-tree tc-guard

10.3.9.7. Распространенные ошибки

Если TC Guard или TC Filter настроены неправильно, может возникнуть ошибка при пересылке пакетов сетевого устройства. Например, при изменении топологии устройство не может своевременно очистить MAC-адрес, что приводит к ошибкам пересылки пакетов.

10.3.10. Включение проверки исходного MAC-адреса BPDU

10.3.10.1. Эффект конфигурации

Включить проверку исходного MAC-адреса BPDU. После этого устройство получает только пакеты BPDU с исходным MAC-адресом, являющимся указанным MAC-адресом, и отбрасывает другие пакеты BPDU.

10.3.10.2. Примечания

Когда коммутатор, подключенный к порту канала «точка-точка», определен, вы можете включить проверку исходного MAC-адреса BPDU, чтобы коммутатор получал пакеты BPDU, отправленные только peer-коммутатором.

10.3.10.3. Шаги настройки

Включение проверки исходного MAC-адреса BPDU

- Опционально.
- По умолчанию проверка исходного MAC-адреса BPDU отключена.
- Чтобы предотвратить злонамеренные атаки BPDU, вы можете включить проверку исходного MAC-адреса BPDU.

10.3.10.4. Проверка

Отобразите конфигурацию.

10.3.10.5. Связанные команды

Включение проверки исходного MAC-адреса BPDU

Команда	**bpdu src-mac-check** *H.H.H*
Описание параметров	*H.H.H*: указывает MAC-адрес. Устройство получает только пакеты BPDU с этим адресом, являющимся исходным MAC-адресом
По умолчанию	По умолчанию проверка исходного MAC-адреса BPDU отключена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Проверка исходного MAC-адреса BPDU предотвращает злонамеренную атаку коммутаторов пакетами BPDU и ненормальную работу MSTP. Когда коммутатор, подключенный к порту на канале «точка-точка», определен, вы можете включить проверку исходного MAC-адреса BPDU, чтобы получать пакеты BPDU, отправленные только peer-коммутатором, и отбрасывать все остальные пакеты BPDU, тем самым предотвращая вредоносные атаки. Вы можете включить проверку исходного MAC-адреса BPDU в режиме конфигурации интерфейса для определенного порта. Один порт может фильтровать только один MAC-адрес

10.3.10.6. Пример конфигурации

Включение проверки исходного MAC-адреса BPDU на порту

Шаги настройки	Включить проверку исходного MAC-адреса BPDU на порту
	QTECH(config)#int gi 0/1

	QTECH(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 08c6.b3.1234
Проверка	Запустите команду **show run interface**, чтобы отобразить конфигурацию spanning tree порта
	QTECH#show run int gi 0/1 Building configuration... Current configuration : 170 bytes interface GigabitEthernet 0/1 switchport mode trunk bpdu src-mac-check 08c6.b3.1234 spanning-tree link-type point-to-point

10.3.10.7. Распространенные ошибки

Если для порта включена проверка исходного MAC-адреса BPDU, порт получает только пакеты BPDU с настроенным MAC-адресом, являющимся исходным MAC-адресом, и отбрасывает все остальные пакеты BPDU.

10.3.11. Настройка Auto Edge

10.3.11.1. Эффект конфигурации

Включите Auto Edge. Если назначенный порт не получает никаких BPDU в течение заданного времени (3 секунды), он автоматически идентифицируется как пограничный порт. Однако, если порт получает BPDU, его рабочее состояние Port Fast становится отключенным.

10.3.11.2. Примечания

- Если не указано иное, не отключайте Auto Edge.
- По умолчанию порт автоматически идентифицируется как пограничный порт и переходит в состояние пересылки, если назначенный порт не получает никаких BPDU в течение 3 секунд. Если в сети происходит потеря пакетов или задержка пакетов Tx/Rx, рекомендуется отключить Auto Edge.

10.3.11.3. Шаги настройки

Настройка Auto Edge

- Опционально.
- Auto Edge включен по умолчанию.

10.3.11.4. Проверка

Отобразите конфигурацию.

10.3.11.5. Связанные команды

Настройка Auto Edge

Команда	**spanning-tree autoedge**
По умолчанию	Auto Edge включен по умолчанию
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если назначенный порт устройства не получает BPDU от downlink-порта в течение определенного периода (3 секунды), устройство рассматривает сетевое устройство, подключенное к назначенному порту, настраивает порт как пограничный порт и переключает порт напрямую в состояние пересылки. Пограничный порт будет автоматически идентифицирован как не пограничный порт после получения BPDU. Вы можете запустить команду **spanning-tree autoedge disabled**, чтобы отключить Auto Edge

10.3.11.6. Пример конфигурации

Отключение Auto Edge на порту

	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled
Проверка	Запустите команду **show spanning-tree interface**, чтобы отобразить конфигурацию spanning tree порта
	QTECH#show spanning-tree interface gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Disabled PortOperAutoEdge : Disabled PortAdminLinkType : point-to-point PortOperLinkType : point-to-point PortBPDUGuard : Disabled PortBPDUFilter : Disabled PortGuardmode : None ###### MST 0 vlans mapped :ALL

	PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.08c6.b3.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.08c6.b3.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 2 PortForwardTransitions : 6 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

10.3.12. Включение функций, связанных с Guard

10.3.12.1. Эффект конфигурации

- Если для порта включена Root Guard, его роли во всех экземплярах применяются как назначенный порт. Как только порт получает информацию о конфигурации с более высоким приоритетом, он переходит в несовместимое с root (блокирующее) состояние. Если порт не получает информацию о конфигурации с более высоким приоритетом в течение периода, он возвращается в исходное состояние.
- Из-за сбоя однонаправленного канала корневой или резервный порт становится назначенным портом и переходит в состояние пересылки, если он не получает BPDU, вызывая сетевую петлю. Loop Guard должен предотвратить эту проблему.

10.3.12.2. Примечания

Root Guard и Loop Guard не могут действовать на порт одновременно.

10.3.12.3. Шаги настройки

Включение Root Guard

- Опционально.
- Root bridge может получить конфигурацию с более высоким приоритетом из-за неправильной настройки обслуживающим персоналом или вредоносных атак в сети. В результате текущий root bridge может потерять свою роль, что приведет к некорректным изменениям топологии. Чтобы предотвратить эту проблему, вы можете включить Root Guard на указанном порту устройства.

Включение Loop Guard

- Опционально.
- Вы можете включить Loop Guard для порта (корневого порта, master-порта или AP), чтобы предотвратить сбой в получении BPDU, отправленных назначенным мостом, что повышает стабильность устройства. В противном случае изменится топология сети, что может привести к возникновению петли.

Отключение Guard

- Опционально.
- Guard отключена по умолчанию.

10.3.12.4. Проверка

Отобразите конфигурацию.

10.3.12.5. Связанные команды

Включение Root Guard

Команда	**spanning-tree guard root**
По умолчанию	По умолчанию Root Guard отключена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если Root Guard включена, текущий root bridge не изменится из-за неправильной конфигурации или незаконных пакетных атак

Включение Loop Guard для всех портов

Команда	**spanning-tree loopguard default**
По умолчанию	Loop Guard по умолчанию отключена
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Включение Loop Guard на корневом или резервном порту предотвратит возможные петли, вызванные сбоем получения BPDU

Включение Loop Guard порта

Команда	**spanning-tree guard loop**
По умолчанию	Loop Guard по умолчанию отключена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Включение Loop Guard на корневом или резервном порту предотвратит возможные петли, вызванные сбоем получения BPDU

Отключение Guard

Команда	**spanning-tree guard none**
По умолчанию	Guard отключена по умолчанию
Командный режим	Режим конфигурации интерфейса

10.3.12.6. Пример конфигурации

Включение Loop Guard на порту

Сценарий:

Рисунок 10-26.

Шаги настройки	• Настройте DEV A в качестве root bridge, а DEV B — в качестве не root bridge spanning tree. • Включите Loop Guard на портах Gi 0/1 и Gi 0/2 устройства DEV B
DEV A	QTECH(config)#spanning-tree QTECH(config)#spanning-tree mst 0 priority 0
DEV B	QTECH(config)#spanning-tree QTECH(config)# int range gi 0/1-2 QTECH(config-if-range)#spanning-tree guard loop
Проверка	Запустите команду **show spanning-tree interface**, чтобы отобразить конфигурацию spanning tree порта
DEV B	QTECH#show spanning-tree int gi 0/1 PortAdminPortFast : Disabled PortOperPortFast : Disabled PortAdminAutoEdge : Enabled PortOperAutoEdge : Disabled PortAdminLinkType : auto

PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : Guard loop
MST 0 vlans mapped :ALL
PortState : forwarding
PortPriority : 128
PortDesignatedRoot : 0.08c6.b3.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.08c6.b3.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 17
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : rootPort
QTECH#show spanning-tree int gi 0/2
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode : Guard loop
MST 0 vlans mapped :ALL
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 0.08c6.b3.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.08c6.b3.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 18
PortForwardTransitions : 1

	PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : alternatePort

10.3.12.7. Распространенные ошибки

Если Root Guard включена на корневом порту, master-порту или AP, порт может быть заблокирован неправильно.

10.3.13. Включение прозрачной передачи BPDU

10.3.13.1. Эффект конфигурации

Если STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы spanning tree между устройствами было правильно рассчитано.

10.3.13.2. Примечания

Прозрачная передача BPDU вступает в силу только тогда, когда STP отключен. Если на устройстве включен протокол STP, оно не передает прозрачно пакеты BPDU.

10.3.13.3. Шаги настройки

Включение прозрачной передачи BPDU

- Опционально.
- Если STP отключен на устройстве, которому необходимо прозрачно передавать пакеты BPDU, включите прозрачную передачу BPDU.

10.3.13.4. Проверка

Отобразите конфигурацию.

10.3.13.5. Связанные команды

Включение прозрачной передачи BPDU

Команда	**bridge-frame forwarding protocol bpdu**
По умолчанию	Прозрачная передача BPDU отключена по умолчанию
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В IEEE 802.1Q MAC-адрес получателя 01-80-C2-00-00-00 BPDU используется в качестве зарезервированного адреса. То есть устройства, совместимые с IEEE 802.1Q, не пересылают полученные пакеты BPDU. Однако устройствам может потребоваться прозрачная передача пакетов BPDU при фактическом развертывании сети. Например, если STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы spanning tree между устройствами было правильно рассчитано.

	Прозрачная передача BPDU вступает в силу только тогда, когда STP отключен. Если на устройстве включен протокол STP, оно не передает прозрачно пакеты BPDU

10.3.13.6. Пример конфигурации

Включение прозрачной передачи BPDU

Сценарий:

Рисунок 10-27.

	STP включен на DEV A и DEV C, но отключен на DEV B
Шаги настройки	Включите прозрачную передачу BPDU на DEV B, чтобы можно было правильно рассчитать STP между DEV A и DEV C
DEV B	QTECH(config)#bridge-frame forwarding protocol bpdu
Проверка	Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача BPDU
DEV B	QTECH#show run Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol bpdu

10.3.14. Включение BPDU-туннеля

10.3.14.1. Эффект конфигурации

Включите туннель BPDU, чтобы пакеты STP из сети клиента могли прозрачно передаваться по сети поставщика услуг. Передача пакетов STP между сетью клиента не влияет на сеть SP, поэтому STP в сети клиента рассчитывается независимо от STP в сети SP.

10.3.14.2. Примечания

Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса.

10.3.14.3. Шаги настройки

Включение BPDU-туннеля

(Опционально) В сети QinQ можно включить туннель BPDU, если STP необходимо рассчитывать отдельно между сетями клиентов и сетями SP.

10.3.14.4. Проверка

Запустите команду **show l2protocol-tunnel stp**, чтобы отобразить конфигурацию туннеля BPDU.

10.3.14.5. Связанные команды

Настройка туннеля BPDU в режиме глобальной конфигурации

Команда	**l2protocol-tunnel stp**
По умолчанию	Туннель BPDU по умолчанию отключен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса

Настройка туннеля BPDU в режиме настройки интерфейса

Команда	**l2protocol-tunnel stp enable**
По умолчанию	Туннель BPDU по умолчанию отключен
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса

Настройка адреса прозрачной передачи туннеля BPDU

Команда	**l2protocol-tunnel stp tunnel-dmac** *mac-address*
Описание параметров	*mac-address*: указывает адрес STP для прозрачной передачи
По умолчанию	MAC-адрес по умолчанию — 01d0.f800.0005
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Если пакет STP, отправленный из клиентской сети, поступает в PE, PE меняет MAC-адрес назначения пакета на приватный адрес до того, как пакет будет перенаправлен сетью SP. Когда пакет достигает PE на peer end, PE изменяет MAC-адрес назначения на общедоступный (public) адрес и возвращает пакет в клиентскую сеть на peer end, реализуя прозрачную передачу по сети SP. Этот приватный адрес является адресом прозрачной передачи туннеля BPDU. Дополнительные адреса прозрачной передачи пакетов STP включают 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1 и 0100.0ccd.cdd2. Если адрес прозрачной передачи не настроен, BPDU Tunnel использует адрес по умолчанию 01d0.f800.0005

10.3.14.6. Пример настройки

Включение BPDU-туннеля

Сценарий:

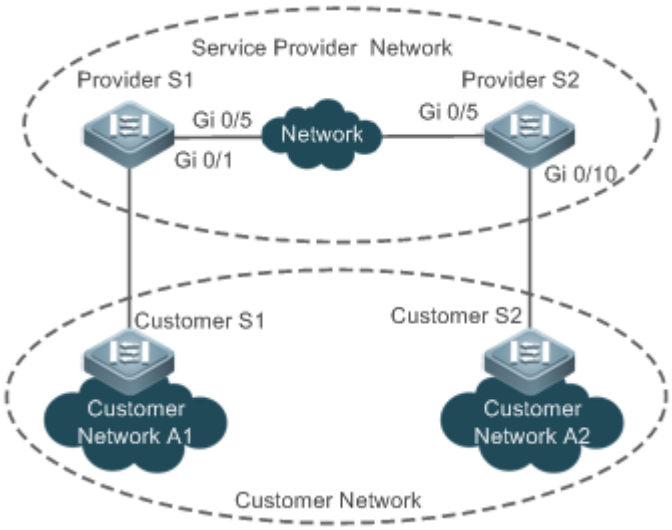


Рисунок 10-28.

Шаги настройки	• Включите базовый QinQ на PE (в данном примере Провайдер S1/ Провайдер S2), чтобы пакеты данных сети клиента передавались в VLAN 200 в сети SP. • Включите прозрачную передачу STP на PE (Провайдер S1/ Провайдер S2 в этом примере), чтобы сеть SP могла передавать пакеты STP сети клиента через туннель BPDU

Провайдер S1	Шаг 1. Создайте VLAN 200 в сети SP.
	`QTECH#configure terminal`
	Введите команды конфигурации, по одной в строке. Конец с CNTL/Z.
	`QTECH(config)#vlan 200`
	`QTECH(config-vlan)#exit`

	Шаг 2. Включите базовый QinQ на порту, подключенном к сети клиента, и используйте VLAN 20 для туннелирования. QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200 Шаг 3. Включите прозрачную передачу STP на порту, подключенном к сети клиента. QTECH(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable QTECH(config-if-GigabitEthernet 0/1)#exit Шаг 4. Включите прозрачную передачу STP в режиме глобальной конфигурации. QTECH(config)#l2protocol-tunnel stp Шаг 5. Настройте Uplink-порт. QTECH(config)# interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink
Провайдер S2	Настройте Провайдер S2, выполнив те же действия
Проверка	Проверьте правильность конфигурации туннеля BPDU. Проверьте конфигурацию туннельного порта, проверив: 1. Тип порта — dot1q-tunnel; 2. VLAN с внешним тегом согласуется с Native VLAN и добавляется в список VLAN туннельного порта; 3. Порт, который обращается к сети SP, настроен как порт Uplink
Провайдер S1	Шаг 1. Проверьте правильность конфигурации туннеля BPDU. QTECH#show l2protocol-tunnel stp L2protocol-tunnel: stp Enable L2protocol-tunnel destination mac address: 01d0.f800.0005 GigabitEthernet 0/1 l2protocol-tunnel stp enable Шаг 2. Проверьте правильность конфигурации QinQ. QTECH#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200 switchport dot1q-tunnel native vlan 200 l2protocol-tunnel stp enable

	spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink
Провайдер S2	Проверьте конфигурацию Провайдера S2, выполнив те же действия

10.3.14.7. Распространенные ошибки

В сети SP пакеты BPDU могут корректно прозрачно передаваться только в том случае, если адреса прозрачной передачи туннеля BPDU согласованы.

10.4. Мониторинг

10.4.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает статистику пакетов, отправленных и полученных через порт	**clear spanning-tree counters** [**interface** *interface-id*]
Очищает информацию об изменении топологии STP	**clear spanning-tree mst** *instance-id* **topochange record**

10.4.2. Отображение

Описание	Команда
Отображает параметры MSTP и информацию о топологии spanning tree	**show spanning-tree**
Отображает количество отправленных и полученных пакетов MSTP	**show spanning-tree counters** [**interface** *interface-id*]
Отображает экземпляры MSTP и соответствующий статус переадресации портов	**show spanning-tree summary**
Отображает порты, которые заблокированы с помощью Root Guard или Loop Guard	**show spanning-tree inconsistentports**

Описание	Команда
Отображает конфигурацию региона MST	**show spanning-tree mst configuration**
Отображает информацию MSTP об экземпляре	**show spanning-tree mst** *instance-id*
Отображает информацию MSTP об экземпляре, соответствующем порту	**show spanning-tree mst** *instance-id* **interface** *interface-id*
Отображает изменения топологии порта в экземпляре	**show spanning-tree mst** *instance-id* **topochange record**
Отображает информацию MSTP обо всех экземплярах, соответствующих порту	**show spanning-tree interface** *interface-id*
Отображает время переадресации	**show spanning-tree forward-time**
Отображает время Hello	**show spanning-tree hello time**
Отображает максимальное количество hop'ов	**show spanning-tree max-hops**
Отображает максимальное количество пакетов BPDU, отправляемых в секунду	**show spanning-tree tx-hold-count**
Отображает метод расчета стоимости пути	**show spanning-tree pathcost method**
Отображает информацию о туннеле BPDU	**show l2protocol-tunnel stp**

10.4.3. Отладка

ПРИМЕЧАНИЕ: системные ресурсы заняты при выводе отладочной информации. Поэтому отключайте переключатель отладки сразу после использования.

Описание	Команда
Отладка всех STP	**debug mstp all**
Отладка MSTP Graceful Restart (GR)	**debug mstp gr**
Отладка получения пакетов BPDU	**debug mstp rx**

Описание	Команда
Отладка отправки пакетов BPDU	**debug mstp tx**
Отладка события MSTP	**debug mstp event**
Отладка Loop Guard	**debug mstp loopguard**
Отладка Root Guard	**debug mstp rootguard**
Отладка state machine обнаружения моста	**debug mstp bridgedetect**
Отладка state machine информации о порте	**debug mstp bridgedetect**
Отладка state machine миграции протокола порта	**debug mstp protomigrat**
Отладка изменения топологии MSTP	**debug mstp topochange**
Отладка принимающей state machine MSTP	**debug mstp receive**
Отладка state machine перехода роли порта	**debug mstp roletran**
Отладка state machine перехода состояния порта	**debug mstp statetran**
Отладка state machine отправки MSTP	**debug mstp transmit**

11. НАСТРОЙКА GVRP

11.1. Обзор

Протокол регистрации VLAN GARP (GVRP) — это приложение протокола Generic Attribute Registration Protocol (GARP), используемое для динамической настройки и распространения членства в VLAN.

GVRP упрощает настройку и управление VLAN. Это снижает нагрузку на ручную настройку VLAN и добавление портов в VLAN, а также снижает вероятность отключения сети из-за несогласованной конфигурации. С помощью GVRP вы можете динамически поддерживать VLAN и добавлять/удалять порты в/из VLAN, чтобы обеспечить подключение VLAN в топологии.

11.1.1. Протоколы и стандарты

Стандарт IEEE 802.1D

Стандарт IEEE 802.1Q

11.2. Приложения

Приложение	Описание
Конфигурация GVRP в локальной сети	Соедините два коммутатора в локальную сеть (LAN) и осуществите синхронизацию VLAN
Туннельное приложение GVRP PDU	Используйте функцию туннеля блоков данных протокола GVRP (PDU) для прозрачной передачи пакетов GVRP через туннель в сетевой среде QinQ

11.2.1. Конфигурация GVRP в локальной сети

11.2.1.1. Сценарий

Включите GVRP и установите для режима регистрации GVRP значение «Normal», чтобы зарегистрировать и отменить регистрацию всех динамических и статических сетей VLAN между устройством A и устройством F.

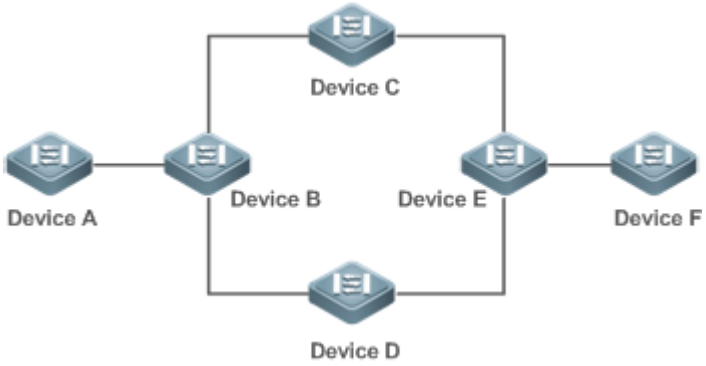


Рисунок 11-1.

Устройство A, Устройство B, Устройство C, Устройство D, Устройство E и Устройство F являются коммутаторами. Порты, подключенные между двумя устройствами, являются транковыми портами.

На Устройстве A и Устройстве F настройте статические VLAN, используемые для связи.

Включите GVRP на всех коммутаторах.

11.2.1.2. Развертывание

- На каждом устройстве включите функции создания GVRP и динамической VLAN, а также убедитесь, что динамические VLAN можно создавать на промежуточных устройствах.
- На Устройстве A и Устройстве F настройте статические VLAN, используемые для связи. Устройство B, Устройство C, Устройство D и Устройство E будут динамически изучать VLAN через GVRP.

ПРИМЕЧАНИЕ: рекомендуется включить протокол spanning tree (STP), чтобы избежать петель в топологии сети клиента.

11.2.2. Туннельное приложение GVRP PDU

11.2.2.1. Сценарий

Сетевая среда QinQ обычно делится на сеть клиента и сеть поставщика услуг (SP). Функция туннеля GVRP PDU позволяет передавать пакеты GVRP между сетями клиентов без влияния на сети SP. Расчет GVRP в клиентских сетях отделен от расчетов в сетях SP без помех.

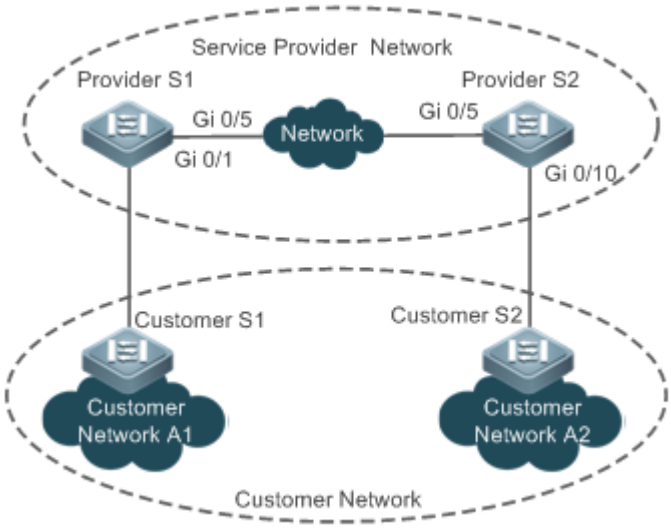


Рисунок 11-2. Топология туннельных приложений GVRP PDU

Рисунок выше показывает сеть SP и сеть клиента. Сеть SP содержит Provider Edge (PE) устройства Провайдер S1 и Провайдер S2. Клиентская сеть A1 и Клиентская сеть A2 — это два канала одного и того же клиента в разных местах. Абонент S1 и Абонент S2 — это устройства доступа в клиентской сети, которые подключены к сети SP через Провайдера S1 и Провайдера S2 соответственно.

Функция туннеля PDU GVRP позволяет клиентской сети A1 и клиентской сети A2 выполнять унифицированный расчет GVRP в сети поставщика услуг, не влияя на расчет GVRP в сети поставщика услуг.

11.2.2.2. Развертывание

- Включите базовый QinQ на PE (Провайдер S1 и Провайдер S2) в сети SP для передачи пакетов данных из сети клиента через указанную VLAN в сети SP.
- Включите прозрачную передачу GVRP на устройствах PE (Провайдер S1 и Провайдер S2) в сети SP, чтобы позволить сети SP туннелировать пакеты GVRP из сети клиента с помощью функции туннелирования PDU GVRP.

11.3. Функции

11.3.1. Базовые определения

GVRP

GVRP — это приложение GARP, используемое для регистрации и отмены регистрации атрибутов VLAN в следующих режимах:

- Когда порт получает объявление атрибута VLAN, порт регистрирует атрибуты VLAN, содержащиеся в объявлении (то есть порт присоединится к VLAN).
- Когда порт получает объявление отзыва атрибута VLAN, порт отменяет регистрацию атрибутов VLAN, содержащихся в объявлении (то есть порт выходит из VLAN).

Рисунок 11-3.

Динамическая VLAN

VLAN, которую можно динамически создавать и удалять без необходимости ручной настройки, называется динамической VLAN.

Вы можете вручную преобразовать динамическую VLAN в статическую VLAN, но не наоборот.

State machine протокола управляет присоединением портов к динамическим сетям VLAN, созданным с помощью GVRP. Только магистральные порты, которые получают объявление атрибута GVRP VLAN, могут присоединяться к этим VLAN. Вы не можете вручную добавлять порты в динамические VLAN.

Типы сообщений

(1) Сообщение Join

Когда объект приложения GARP надеется, что другие объекты GARP зарегистрируют его атрибуты, он отправит сообщение Join. Когда объект GARP получает сообщение Join от другого объекта или требует, чтобы другие объекты зарегистрировали его статические атрибуты, он отправляет сообщение Join. Существует два типа сообщений о присоединении: JoinEmpty и JoinIn.

- Сообщение JoinEmpty: используется для объявления незарегистрированного атрибута.
- Сообщение JoinIn: используется для объявления зарегистрированного атрибута.

(2) Сообщение Leave

Когда объект приложения GARP надеется, что другие объекты GARP отменят регистрацию его атрибутов, он отправит сообщение Leave. Когда объект GARP получает сообщение Leave от другого объекта или требует, чтобы другие объекты отменили регистрацию его статически отмененных атрибутов, он отправит сообщение Leave. Существует два типа сообщения о выходе: LeaveEmpty и LeaveIn.

- Сообщение LeaveEmpty: используется для отмены регистрации незарегистрированного атрибута.
- Сообщение LeaveIn: используется для отмены регистрации зарегистрированного атрибута.

(3) Сообщение LeaveAll

Каждый объект приложения GARP запускает свой таймер LeaveAll во время запуска. Когда таймер истекает, объект отправляет сообщение LeaveAll для отмены регистрации всех атрибутов, чтобы позволить другим объектам GARP перерегистрировать атрибуты. Когда объект приложения GARP получает сообщение LeaveAll от другого объекта, он также отправляет сообщение LeaveAll. Таймер LeaveAll перезапускается при повторной отправке сообщения LeaveAll, чтобы инициировать новый цикл.

Типы таймеров

GARP определяет четыре таймера, используемых для управления отправкой сообщений GARP.

(1) Таймер Hold

Таймер Hold управляет отправкой сообщений GARP (включая сообщения Join и Leave). Когда объект приложения GARP изменяет свои атрибуты или получает сообщение GARP от другого объекта, он запускает таймер Hold. В течение периода тайм-аута объект приложения GARP инкапсулирует все сообщения GARP, которые должны быть отправлены, в пакеты, возможное малое количество пакетов, и отправляет пакеты, когда таймер истекает. Это уменьшает количество отправляемых пакетов и экономит ресурсы пропускной способности.

(2) Таймер Join

Таймер Join управляет отправкой сообщений Join. После того как объект приложения GARP отправляет сообщение Join, он ожидает один интервал тайм-аута таймера Join, чтобы убедиться, что сообщение о присоединении надежно передано другому объекту. Если объект приложения GARP получает сообщение JoinIn от другого объекта до истечения времени таймера, он не будет повторно отправлять сообщение Join; в противном случае он повторно отправит сообщение Join. Не каждый атрибут имеет собственный таймер Join, но каждый объект приложения GARP имеет один таймер Join.

(3) Таймер Leave

Таймер Leave управляет отменой регистрации атрибута. Когда объект приложения GARP надеется, что другие объекты отменят регистрацию одного из его атрибутов, он отправляет сообщение Leave. Другие объекты, получившие сообщение Leave, запускают таймер Leave. Регистрация атрибута будет отменена только в том случае, если эти объекты не получат сообщения Join, сопоставленного с атрибутом, в течение тайм-аута.

(4) Таймер LeaveAll

Каждый объект приложения GARP запускает свой собственный таймер LeaveAll при запуске. Когда таймер истекает, объект отправляет сообщение LeaveAll, чтобы позволить другим объектам перерегистрировать атрибуты. Затем таймер LeaveAll перезапускается, чтобы инициировать новый цикл.

Режимы объявления GVRP

GVRP позволяет коммутатору информировать другие подключенные устройства о своих VLAN и инструктировать peer-устройство о создании конкретных VLAN и добавлении портов, передающих пакеты GVRP, в соответствующие VLAN.

Доступны два режима объявления GVRP:

- Режим Normal: устройство извне объявляет информацию о своей VLAN, включая динамические и статические VLAN.
- Режим Non-applicant: устройство не объявляет извне информацию о своей VLAN.

Режимы регистрации GVRP

Режим регистрации GVRP указывает, обрабатывает ли коммутатор, который получает пакет GVRP, информацию о VLAN в пакете, например, динамически создает новую VLAN и добавляет порт, который получает пакет, в VLAN.

Доступны два режима регистрации GVRP:

- Режим Normal: обработка информации VLAN в полученном пакете GVRP.
- Режим Disabled: нет обработки информации VLAN в полученном пакете GVRP.

11.3.1.1. Обзор

Особенность	Описание
Синхронизация информации VLAN внутри топологии	Динамически создает VLAN и добавляет/удаляет порты в/из VLAN, что снижает нагрузку на ручную настройку и вероятность отключения VLAN из-за отсутствия конфигурации

11.3.2. Синхронизация информации VLAN внутри топологии

11.3.2.1. Принцип работы

GVRP — это приложение GARP, основанное на рабочем механизме GARP. GVRP поддерживает динамическую регистрационную информацию VLAN на устройстве и распространяет эту информацию на другие устройства. Устройство с поддержкой GVRP получает регистрационную информацию VLAN от других устройств и динамически обновляет регистрационную информацию локальной VLAN. Устройство также распространяет информацию о регистрации локальной VLAN на другие устройства, чтобы все устройства в сети поддерживали согласованную информацию о сети VLAN. Регистрационная информация VLAN, распространяемая GVRP, включает настроенную вручную статическую регистрационную информацию на локальном устройстве и динамическую регистрационную информацию от других устройств.

Информационное объявление внешней VLAN

Магистральный порт на устройстве с поддержкой GVRP периодически собирает информацию о VLAN внутри порта, включая VLAN, к которым магистральный порт присоединяется или отсоединяется. Собранная информация о VLAN инкапсулируется в пакет GVRP для отправки на peer-устройство. После того, как магистральный порт на peer-устройстве получает пакет, он принимает информацию о VLAN. Затем будут динамически созданы соответствующие VLAN, а магистральный порт присоединится к созданным VLAN или выйдет из других VLAN. Дополнительные сведения об информации о VLAN см. в приведенном выше описании типов сообщений GVRP.

11.3.2.2. Связанные конфигурации

GVRP отключен по умолчанию.

- Запустите [**no**] **gvrp enable**, чтобы включить или отключить GVRP.

После включения GVRP на устройстве устройство отправляет пакеты GVRP, содержащие информацию о VLAN. Если протокол GVRP отключен на устройстве, устройство не отправляет пакеты GVRP, содержащие информацию о VLAN, и не обрабатывает полученные пакеты GVRP.

Регистрация и отмена регистрации VLAN

При получении пакета GVRP коммутатор определяет, следует ли обрабатывать информацию VLAN в пакете в соответствии с режимом регистрации соответствующего порта. Дополнительные сведения см. в приведенном выше описании режимов регистрации GVRP.

11.3.2.3. Связанные конфигурации

- Если GVRP включен, порт в режиме Trunk по умолчанию активируется с динамической регистрацией VLAN.
- Чтобы включить динамическую регистрацию VLAN на порту, выполните команду **gvrp registration mode normal**. Чтобы отключить динамическую регистрацию VLAN на порту, выполните команду **gvrp register mode disable**.
- Если динамическая регистрация VLAN включена, динамические VLAN будут созданы на локальном устройстве, когда порт получит пакет GVRP, содержащий информацию о VLAN, от peer end.
- Если динамическая регистрация VLAN отключена, динамическая VLAN не будет создана на локальном устройстве, когда порт получит пакет GVRP от peer end.

Конфигурация	Описание и команда	
Настройка основных функций GVRP и синхронизации информации VLAN	(Обязательный) Он используется для включения GVRP и динамического создания VLAN	
	gvrp enable	Включает GVRP
	gvrp dynamic-vlan-creation enable	Включает динамическое создание VLAN
	switchport mode trunk	Переключение в режим магистрального порта. GVRP действует только в режиме Trunk
	switchport trunk allowed vlan all	Позволяет трафику из всех VLAN проходить

Конфигурация	Описание и команда	
Настройка основных функций GVRP и синхронизации информации VLAN	**gvrp applicant state**	Настраивает режим объявления порта. Режим Normal указывает на объявление информации о VLAN извне путем отправки пакета GVRP. Режим Non-applicant указывает, что не следует объявлять информацию о VLAN извне
	gvrp registration mode	Настраивает режим регистрации порта. Режим Normal указывает на обработку информации о VLAN в полученном пакете GVRP, например, динамическое создание VLAN и добавление портов в VLAN. Режим Disabled указывает, что не следует обрабатывать информацию VLAN в полученном пакете GVRP
	(Опционально) Используется для настройки таймеров и режима регистрации и режима объявления порта	
	gvrp timer	Настраивает таймеры
Настройка прозрачной передачи GVRP PDU	(Опционально) Он используется для настройки прозрачной передачи GVRP PDU	
	bridge-frame forwarding protocol gvrp	Включает прозрачную передачу GVRP PDU
Настройка функции туннеля GVRP PDU	(Опционально) Он используется для настройки функции туннеля PDU GVRP	
	l2protocol-tunnel gvrp	Включает функцию туннеля PDU GVRP в режиме глобальной конфигурации
	l2protocol-tunnel gvrp enable	Включает функцию туннеля PDU GVRP в режиме конфигурации интерфейса
	l2protocol-tunnel gvrp tunnel-dmac	Настраивает адрес прозрачной передачи, используемый функцией туннеля GVRP PDU

11.4. Конфигурация

11.4.1. Настройка основных функций GVRP и синхронизации информации VLAN

11.4.1.1. Эффект конфигурации

- Динамически создавать/удалять VLAN и добавлять/удалять порты в/из VLAN.
- Синхронизирует информацию VLAN между устройствами, чтобы обеспечить нормальную связь внутри топологии.
- Сокращает нагрузку на ручную настройку и упрощает управление VLAN.

11.4.1.2. Примечания

- GVRP должен быть включен на обоих подключенных устройствах. Информация GVRP передается только по магистральным каналам. Передаваемая информация содержит информацию обо всех сетях VLAN на текущем устройстве, включая динамически изученные сети VLAN и сети VLAN, настроенные вручную.
- Если STP включен, только порты в состоянии Forwarding участвуют в GVRP (например, получают и отправляют PDU GVRP) и получают информацию о своей VLAN, распространяемую GVRP.
- Все порты VLAN, добавленные GVRP, являются помеченными тегами портами.
- Система не сохраняет информацию о VLAN, которая динамически изучается GVRP. Информация будет потеряна при перезагрузке устройства и не может быть сохранена вручную.
- Все устройства, которым необходимо обмениваться информацией GVRP, должны поддерживать согласованные таймеры GVRP (таймер Join, таймер Leave и таймер Leaveall).
- Если STP не включен, все доступные порты могут участвовать в GVRP. Если включено одно spanning tree (SST), только порты в состоянии пересылки (Forwarding) в контексте SST участвуют в GVRP. Если включено несколько spanning tree (MST), GVRP может работать в контексте spanning tree, которому принадлежит VLAN1. Вы не можете указать другой контекст spanning tree для GVRP.

11.4.1.3. Шаги настройки

Включение GVRP

- Обязательный.
- Только устройства с поддержкой GVRP могут обрабатывать пакеты GVRP.

Включение динамического создания VLAN

- Обязательный.
- После включения динамического создания VLAN на устройстве устройство будет динамически создавать VLAN при получении сообщений GVRP Join.

Настройка таймеров

- Опционально.
- Существует три таймера GVRP: таймер Join, таймер Leave и таймер Leaveall, которые используются для управления интервалами отправки сообщений.

- Взаимоотношения интервалов таймера следующие: интервал таймера Leave должен быть в три или более раз больше, чем интервал таймера Join; интервал таймера Leaveall должен быть больше, чем интервал таймера Leave.
- Три таймера управляются state machine GVRP и могут запускаться друг другом.

Настройка режима объявления порта

- Опционально.
- Доступны два режима объявления GVRP: Normal (по умолчанию) и Non-applicant.
- Режим Normal: указывает, что устройство извне объявляет информацию о своей VLAN.
- Режим Non-applicant: указывает, что устройство не объявляет извне информацию о своей VLAN.

Настройка режима регистрации порта

- Опционально.
- Доступны два режима регистрации GVRP: Normal и Disabled.

Переключение в режим магистрального порта

- Обязательный.
- GVRP действует только на порты в режиме Trunk.

11.4.1.4. Проверка

- Запустите команду **show gvrp configuration**, чтобы проверить конфигурацию.
- Проверьте, настроена ли динамическая VLAN, и соответствующий порт присоединяется к VLAN.

11.4.1.5. Связанные команды

Включение GVRP

Команда	**gvrp enable**
По умолчанию	По умолчанию GVRP выключен
Командный режим	Режим глобальной конфигурации
Руководство по использованию	GVRP можно включить только в режиме глобальной конфигурации. Если GVRP не включен глобально, вы все равно можете установить другие параметры GVRP, но настройки параметров вступят в силу только после запуска GVRP

Включение динамического создания VLAN

Команда	**gvrp dynamic-vlan-creation enable**
По умолчанию	По умолчанию динамическое создание VLAN выключено
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Когда порт получает сообщение JoinIn или JoinEmpty, указывающее на несуществующую VLAN на локальном устройстве, GVRP может создать эту VLAN в зависимости от конфигурации этой команды

ПРИМЕЧАНИЕ: параметры динамической VLAN, созданной через GVRP, нельзя изменить вручную.

Настройка таймеров

Команда	**gvrp timer** { **join** *timer-value* | **leave** *timer-value* | **leaveall** *timer-value* }
Описание параметров	*timer-value*: 1–2 147 483 647 мс
По умолчанию	Таймер Join: 200 мс, таймер Leave: 600 мс, таймер Leaveall: 10 000 мс
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Интервал таймера Leave должен быть в три раза больше, чем интервал таймера Join. Интервал таймера Leaveall должен быть больше, чем интервал таймера Leave. Единицей времени являются миллисекунды. В реальной сети рекомендуются следующие интервалы таймера: Таймер Join: 6000 мс (6 с) Таймер Leave: 30 000 мс (30 с) Таймер Leaveall: 120 000 мс (2 минуты) Убедитесь, что настройки таймера GVRP на всех взаимосвязанных устройствах GVRP согласованы; в противном случае GVRP может работать неправильно

Настройка режима объявления порта

Команда	**gvrp applicant state** { **normal** | **non-applicant** }
Описание параметров	**normal**: указывает, что порт внешне объявляет информацию о VLAN. **non-applicant**: указывает порт не объявляет извне информацию о VLAN
По умолчанию	По умолчанию портам разрешено отправлять уведомление GVRP
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Эта команда используется для настройки режима объявления GVRP порта

Настройка режима регистрации порта

Команда	**gvrp registration mode** { **normal** | **disabled** }
Описание параметров	**normal**: указывает, что порту разрешено присоединяться к динамической VLAN. **disabled**: указывает, что порту не разрешено присоединяться к динамической VLAN
По умолчанию	Если GVRP включен, порт в режиме Trunk по умолчанию активируется с динамической регистрацией VLAN
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Эта команда используется для настройки режима регистрации GVRP порта

11.4.1.6. Пример конфигурации

Включение GVRP в топологии и динамическое обслуживание VLAN и взаимоотношение VLAN-порт

Сценарий:

Рисунок 11-4.

Шаги настройки	• На коммутаторе A и коммутаторе C настройте VLAN, используемые для связи в сети клиента. • Включите функции создания GVRP и динамической VLAN на коммутаторе A, коммутаторе B и коммутаторе C. • Настройте порты, подключенные между коммутаторами, как магистральные порты и убедитесь, что списки VLAN магистральных портов включают коммуникационные VLAN. По умолчанию магистральный порт пропускает трафик из всех сетей VLAN. • Рекомендуется включить STP, чтобы избежать петель

A	1. Создайте VLAN 1–200, используемую для связи в сети клиента.
	`A# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`A(config)# vlan range 1-200`

	2. Включите функции создания GVRP и динамической VLAN. A(config)# gvrp enable A(config)# gvrp dynamic-vlan-creation enable 3. Настройте порт, подключенный к коммутатору B, как магистральный порт. По умолчанию магистральный порт пропускает трафик из всех сетей VLAN. A(config)# interface gigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# switchport mode trunk 4. Настройте режим объявления и режим регистрации магистрального порта. Режим Normal используется по умолчанию, и его не нужно настраивать вручную. A(config-if-GigabitEthernet 0/1)# gvrp applicant state normal A(config-if-GigabitEthernet 0/1)# gvrp registration mode normal A(config-if-GigabitEthernet 0/1)# end
C	Конфигурация на коммутаторе C такая же, как и на коммутаторе A
B	1. Включите функции создания GVRP и динамической VLAN. B# configure terminal B(config)# gvrp enable B(config)# gvrp dynamic-vlan-creation enable 2. Настройте порты, подключенные к коммутатору A и коммутатору C, как магистральные порты. B(config)# interface range GigabitEthernet 0/2-3 B(config-if-GigabitEthernet 0/2)# switchport mode trunk
Проверка	Проверьте правильность конфигурации GVRP на каждом устройстве. Проверьте, что VLAN 2–100 динамически создаются на коммутаторе B и присоединяются ли порт G 0/2 и порт G 0/3 на коммутаторе B к динамическим VLAN
A	A# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------- ---------- ----------

	GigabitEthernet 0/1 normal normal
B	B# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------- ---------- ---------- GigabitEthernet 0/2 normal normal GigabitEthernet 0/3 normal normal
C	C# show gvrp configuration Global GVRP Configuration: GVRP Feature:enabled GVRP dynamic VLAN creation:enabled Join Timers(ms):200 Leave Timers(ms):600 Leaveall Timers(ms):1000 Port based GVRP Configuration: PORT Applicant Status Registration Mode ---------- ---------- ---------- GigabitEthernet 0/1 normal normal

11.4.1.7. Распространенные ошибки

- Порты, подключенные между устройствами, не находятся в режиме Trunk.
- Списки VLAN портов, подключенных между устройствами, не включают VLAN, используемые для связи в сети клиента.
- Режимы объявления GVRP и режимы регистрации магистральных портов не установлены на Normal.

11.4.2. Настройка прозрачной передачи GVRP PDU

11.4.2.1. Эффект конфигурации

Разрешает устройствам прозрачно передавать кадры PDU GVRP, чтобы реализовать нормальный расчет GVRP между устройствами, когда GVRP не включен.

11.4.2.2. Примечания

Прозрачная передача GVRP PDU вступает в силу только тогда, когда GVRP отключен. После включения GVRP устройства не будут прозрачно передавать кадры GVRP PDU.

11.4.2.3. Шаги настройки

Настройка прозрачной передачи GVRP PDU

- Опционально.
- Выполните эту настройку, если вам нужно разрешить устройствам прозрачно передавать кадры PDU GVRP, когда GVRP отключен.

11.4.2.4. Проверка

Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача GVRP PDU.

11.4.2.5. Связанные команды

Настройка прозрачной передачи GVRP PDU

Команда	**bridge-frame forwarding protocol gvrp**
Командный режим	Режим глобальной конфигурации
По умолчанию	По умолчанию функция отключена
Руководство по использованию	В стандарте IEEE 802.1Q MAC-адрес назначения 01-80-C2-00-00-06 зарезервирован для PDU GVRP. Устройства, совместимые с IEEE 802.1Q, не пересылают полученные кадры GVRP PDU. Однако при фактическом развертывании сети устройствам может потребоваться прозрачная передача кадров GVRP PDU для реализации нормального расчета GVRP между устройствами, когда GVRP не включен. Прозрачная передача GVRP PDU вступает в силу только тогда, когда GVRP отключен. После включения GVRP устройства не будут прозрачно передавать кадры GVRP PDU

11.4.2.6. Пример конфигурации

Настройка прозрачной передачи GVRP PDU

Сценарий:

Рисунок 11-5.

	Включите GVRP на DEV A и DEV C. (DEV B не включается с GVRP)
Шаги настройки	Настройте прозрачную передачу GVRP PDU на DEV B для реализации нормального Расчета GVRP между DEV A и DEV C
DEV B	QTECH(config)#bridge-frame forwarding protocol gvrp
Проверка	Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача GVRP PDU
DEV B	QTECH#show run Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol gvrp

11.4.3. Настройка функции туннеля GVRP PDU

11.4.3.1. Эффект конфигурации

Прозрачно передавайте пакеты GVRP между сетями клиентов через туннели в сетях SP, не влияя на сети SP, и тем самым отделяйте расчеты GVRP в сетях клиентов от расчетов в сетях SP.

11.4.3.2. Примечания

Функция туннеля PDU GVRP вступает в силу после ее включения в режиме глобальной конфигурации и режиме конфигурации интерфейса.

11.4.3.3. Шаги настройки

Настройка функции туннеля GVRP PDU

(Опционально) Выполните эту настройку, если вам нужно разделить расчет GVRP между сетями клиентов и сетями поставщика услуг в среде QinQ.

11.4.3.4. Проверка

Запустите команду **show l2protocol-tunnel gvrp**, чтобы проверить конфигурацию туннеля GVRP PDU.

11.4.3.5. Связанные команды

Настройка функции туннелирования PDU GVRP в режиме глобальной конфигурации

Команда	**l2protocol-tunnel gvrp**
По умолчанию	По умолчанию функция отключена

Командный режим	Режим глобальной конфигурации
Руководство по использованию	Функция туннелирования GVRP PDU вступает в силу после ее включения в режиме глобальной конфигурации и режиме настройки интерфейса

Настройка функции туннелирования GVRP PDU в режиме конфигурации интерфейса

Команда	**l2protocol-tunnel gvrp enable**
По умолчанию	По умолчанию функция отключена
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Функция туннелирования GVRP PDU вступает в силу после ее включения в режиме глобальной конфигурации и режиме настройки интерфейса

Настройка адреса прозрачной передачи туннеля PDU GVRP

Команда	**l2protocol-tunnel gvrp tunnel-dmac** *mac-address*
Описание параметров	*mac-address*: указывает адрес GVRP, используемый прозрачной передачей
По умолчанию	По умолчанию адрес 01d0.f800.0006
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В приложении туннеля GVRP PDU, когда пакет GVRP из клиентской сети входит в PE в сети SP, MAC-адрес назначения пакета изменяется на приватный адрес до того, как пакет перенаправляется в сеть SP. Когда пакет достигает peer PE, MAC-адрес назначения изменяется на общедоступный адрес, прежде чем пакет будет отправлен в клиентскую сеть на другом конце. Таким образом, пакет GVRP может быть прозрачно передан по сети SP. Приватный адрес — это адрес прозрачной передачи, используемый функцией туннеля GVRP PDU. **ПРИМЕЧАНИЕ:** диапазон адресов для прозрачной передачи пакетов GVRP: 01d0.f800.0006, 011a.a900.0006 **ПРИМЕЧАНИЕ:** если адрес прозрачной передачи не настроен, используется адрес по умолчанию 01d0.f800.0006

11.4.3.6. Пример конфигурации

Настройка функции туннеля GVRP PDU

Сценарий:

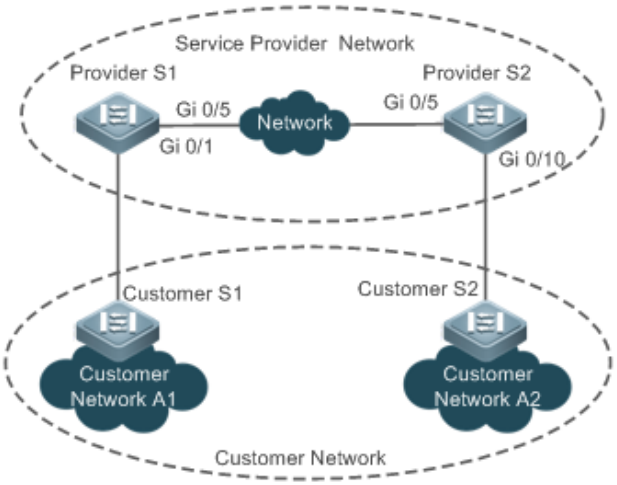


Рисунок 11-6.

Шаги настройки	• Включите базовый QinQ на PE (Провайдер S1 и Провайдер S2) в сети SP для передачи пакетов данных из сети клиента через VLAN 200 в сети SP. • Включите прозрачную передачу GVRP на устройствах PE (Провайдер S1 и Провайдер S2) в сети SP, чтобы позволить сети SP туннелировать пакеты GVRP из сети клиента с помощью функции туннелирования PDU GVRP
Провайдер S1	Шаг 1. Создайте VLAN 200 в сети SP. QTECH#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. QTECH(config)#vlan 200 QTECH(config-vlan)#exit Шаг 2. Включите базовый QinQ на порту, подключенном к сети клиента, для туннелирования данных из сети клиента через VLAN 200. QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200 QTECH(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 200 Шаг 3. Включите прозрачную передачу GVRP на порту, подключенном к сети клиента. QTECH(config-if-GigabitEthernet 0/1)#l2protocol-tunnel gvrp enable QTECH(config-if-GigabitEthernet 0/1)#exit Шаг 4. Глобально включите прозрачную передачу GVRP.

	QTECH(config)#l2protocol-tunnel gvrp Шаг 5: Настройте uplink-порт. QTECH(config)# interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink
Провайдер S2	Конфигурация Провайдера S2 аналогична конфигурации Провайдера S1
Проверка	• Проверьте правильность конфигурации туннеля GVRP PDU. • Проверьте, правильно ли настроен туннельный порт. Обратите внимание на следующее: 1. Тип порта — dot1q-tunnel. 2. VLAN с внешним тегом является Native VLAN и добавляется в список VLAN туннельного порта. 3. Порты на PE в направлении uplink настроены как порты uplink
Провайдер S1	1. Проверьте правильность конфигурации туннеля GVRP PDU. QTECH#show l2protocol-tunnel gvrp L2protocol-tunnel: Gvrp Enable L2protocol-tunnel destination mac address: 01d0.f800.0006 GigabitEthernet 0/1 l2protocol-tunnel gvrp enable 2. Проверьте правильность конфигурации QinQ. QTECH#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200 switchport dot1q-tunnel native vlan 200 l2protocol-tunnel gvrp enable ! interface GigabitEthernet 0/5 switchport mode uplink
Провайдер S2	Проверка у Провайдера S2 такая же, как и у Провайдера S1

11.4.3.7. Распространенные ошибки

В сети SP прозрачные адреса передачи не настроены последовательно, что влияет на передачу кадров GVRP PDU.

11.5. Мониторинг

11.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает счетчики портов	**clear gvrp statistics** { *interface-id* | **all** }

11.5.2. Отображение

Описание	Команда
Отображает счетчики портов	**show gvrp statistics {** *interface-id* **| all }**
Отображает текущий статус GVRP	**show gvrp status**
Отображает текущую конфигурацию GVRP	**show gvrp configuration**
Отображает информацию о функции туннеля GVRP PDU	**show l2protocol-tunnel gvrp**

11.5.3. Отладка

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

Описание	Команда
Включает отладку события GVRP	**debug gvrp event**
Включает отладку таймера GVRP	**debug gvrp timer**

12. НАСТРОЙКА LLDP

12.1. Обзор

Протокол обнаружения канального уровня (LLDP), определенный в стандарте IEEE 802.1AB, используется для обнаружения топологии и выявления топологических изменений. LLDP инкапсулирует локальную информацию об устройстве в блоки данных LLDP (LLDPDU) в формате тип/длина/значение (TLV), а затем отправляет LLDPDU соседям. Он также хранит LLDPDU от соседей в базе управляющей информации (MIB), чтобы к ним могла обращаться система управления сетью (NMS).

С помощью LLDP NMS может узнать о топологии, например, какие порты устройства подключены к другим устройствам и являются ли скорости и дуплексные режимы на обоих концах канала последовательными. Администраторы могут быстро обнаружить и устранить неисправность на основе информации.

QTECH LLDP-совместимое устройство способно обнаружить соседей, когда peer является одним из следующих:

- Устройство, совместимое с QTECH LLDP.
- Устройство Endpoint, которое соответствует стандарту Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED).

12.1.1. Протоколы и стандарты

- IEEE 802.1AB 2005: обнаружение возможности подключения управления доступом к станциям и средам
- ANSI/TIA-1057: протокол обнаружения канального уровня для оконечных медиа-устройств

12.2. Приложения

Приложение	Описание
Отображение топологии	Несколько коммутаторов, устройство MED и NMS развернуты в топологии сети
Проведение обнаружения ошибок	Два коммутатора подключены напрямую, и будет отображаться неправильная конфигурация

12.2.1. Отображение топологии

12.2.1.1. Сценарий

Несколько коммутаторов, устройство MED и NMS развернуты в топологии сети.

Как показано на следующем Рисунке, функция LLDP включена по умолчанию, и дополнительная настройка не требуется.

- Коммутатор A и коммутатор B обнаруживают, что они являются соседями.
- Коммутатор A обнаруживает соседнее MED-устройство, то есть IP-телефон, через порт GigabitEthernet 0/1.
- NMS обращается к MIB коммутатора A.

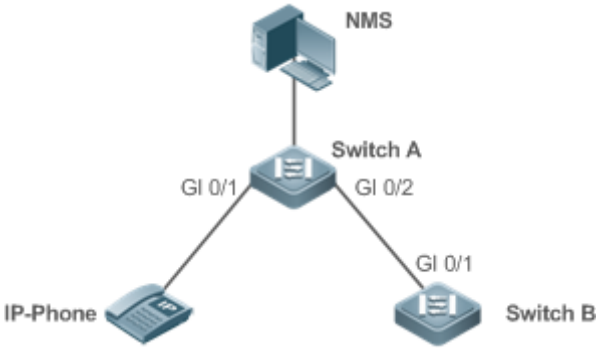


Рисунок 12-1.

Коммутатор A, Коммутатор B и IP-телефон поддерживают LLDP и LLDP-MED.

LLDP на портах коммутатора работает в режиме TxRx.

Интервал передачи по протоколу LLDP составляет 30 секунд, а задержка передачи по умолчанию составляет 2 секунды.

12.2.1.2. Развертывание

- Запустите LLDP на коммутаторе, чтобы реализовать обнаружение соседей.
- Запустите простой протокол управления сетью (SNMP) на коммутаторе, чтобы NMS получала и устанавливала информацию, относящуюся к LLDP, на коммутаторе.

12.2.2. Проведение обнаружения ошибок

12.2.2.1. Сценарий

Два коммутатора подключены напрямую, и будет отображаться неправильная конфигурация.

Как показано на следующем Рисунке, функция LLDP и функция обнаружения ошибок LLDP включены по умолчанию, и дополнительная настройка не требуется.

После того как вы настроите виртуальную локальную сеть (VLAN), скорость порта и режим дуплекса, агрегацию каналов и максимальную единицу передачи (MTU) порта на коммутаторе A, будет выдано сообщение об ошибке, если конфигурация не соответствует конфигурации на коммутаторе B, и наоборот.

Рисунок 12-2.

Коммутатор A и Коммутатор B поддерживают LLDP.

LLDP на портах коммутатора работает в режиме TxRx.

Интервал передачи по протоколу LLDP составляет 30 секунд, а задержка передачи по умолчанию составляет 2 секунды.

12.2.2.2. Развертывание

Запустите LLDP на коммутаторе, чтобы реализовать обнаружение соседей и обнаружить неисправность канала.

12.3. Функции

12.3.1. Базовые определения

LLDPDU

LLDPDU — это блок данных протокола, инкапсулированный в пакет LLDP. Каждый LLDPDU представляет собой последовательность структур TLV. Коллекция TLV состоит из трех обязательных TLV, ряда необязательных TLV и одного End Of TLV. На следующем Рисунке показан формат LLDPDU.

Рисунок 12-3. Формат LLDPDU

На предыдущем Рисунке:

- M указывает обязательный TLV.
- В LLDPDU TLV идентификатора шасси (Chassis ID), TLV идентификатора порта (Port ID), TLV времени жизни (Time To Live) и End Of LLDPDU TLV являются обязательными, а TLV других TLV являются необязательными.

Формат инкапсуляции LLDP

Пакеты LLDP могут быть инкапсулированы в двух форматах: Ethernet II и протоколы доступа к подсети (SNAP).

На следующем Рисунке показан формат пакетов LLDP, инкапсулированных в формате Ethernet II.

Рисунок 12-4. Формат Ethernet II

На предыдущем Рисунке:

- Адрес назначения (Destination Address): указывает MAC-адрес назначения, который является multicast-адресом LLDP 01-80-C2-00-00-0E.
- Исходный адрес (Source Address): указывает исходный MAC-адрес, который является MAC-адресом порта.
- Ethertype: указывает тип Ethernet, который равен 0x88CC.
- LLDPDU: указывает блок данных протокола LLDP.
- FCS: указывает последовательность проверки кадра.

На Рисунке ниже показан формат пакетов LLDP, инкапсулированных в формате SNAP.

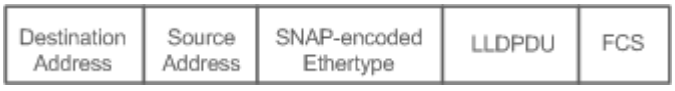


Рисунок 12-5. Формат SNAP

На предыдущем Рисунке:

- Адрес назначения (Destination Address): указывает MAC-адрес назначения, который является multicast-адресом LLDP 01-80-C2-00-00-0E.
- Исходный адрес (Source Address): указывает исходный MAC-адрес, который является MAC-адресом порта.

- SNAP-encoded Ethertype: указывает тип Ethernet инкапсуляции SNMP, то есть AA-AA-03-00-00-00-88-CC.
- LLDPDU: указывает блок данных протокола LLDP.
- FCS: указывает последовательность проверки кадра.

TLV

TLV, инкапсулированные в LLDPDU, можно разделить на два типа:

- Базовые TLV управления
- Специфичные TLV организаций

Базовые TLV управления представляют собой набор базовых TLV, используемых для управления сетью. Специфичные TLV организаций определяются стандартными организациями и другими учреждениями, например, организация IEEE 802.1 и организация IEEE 802.3 определяют свои собственные коллекции TLV.

Базовые TLV управления

Базовая коллекция TLV для управления состоит из двух типов TLV: обязательных TLV и необязательных TLV. Обязательный TLV должен содержаться в LLDPDU для объявления, а необязательный TLV содержится выборочно.

В следующей таблице описаны базовые TLV управления.

Тип TLV	Описание	Обязательный/ необязательный
End Of LLDPDU TLV	Указывает окончание LLDPDU, содержит два байта	Обязательный
TLV идентификатора шасси (Chassis ID TLV)	Идентифицирует устройство с MAC-адресом	Обязательный
TLV идентификатора порта (Port ID TLV)	Идентифицирует порт, отправляющий LLDPDU	Опциональный
TLV времени жизни (Time To Live)	Указывает время жизни (TTL) локальной информации о соседе. Когда устройство получает TLV, содержащий TTL 0, оно удаляет информацию о соседях	Обязательный
TLV описания порта (Port Description)	Указывает дескриптор порта, отправляющего LLDPDU	Необязательный
TLV имени системы (System Name)	Описывает имя устройства	Необязательный
TLV описания системы (System Description)	Указывает описание устройства, включая версию оборудования, версию программного обеспечения и информацию об операционной системе	Необязательный

Тип TLV	Описание	Обязательный/ необязательный
TLV возможностей системы (System Capabilities)	Описывает основные функции устройства, такие как функции моста, маршрутизации и relay	Необязательный
TLV адреса управления (Management Address)	Указывает адрес управления, который содержит идентификатор интерфейса и идентификатор объекта (OID)	Необязательный

ПРИМЕЧАНИЕ: коммутаторы QTECH, совместимые с LLDP, поддерживают объявление базового TLV управления.

Специфичные TLV организаций

Различные организации, такие как IEEE 802.1, IEEE 802.3, IETF и поставщики устройств, определяют определенные TLV для объявления конкретной информации об устройствах. Поле организационного уникального идентификатора (OUI) в TLV используется для различения различных организаций.

- Специфичные TLV организаций являются необязательными и выборочно объявляются в LLDPDU. В настоящее время существует три типа общепринятых TLV для конкретных организаций: TLV для конкретных организаций IEEE 802.1, TLV для конкретных организаций IEEE 802.3 и TLV для LLDP-MED.

В следующей таблице описываются TLV для конкретных организаций IEEE 802.1.

Тип TLV	Описание
TLV идентификатора VLAN порта	Указывает идентификатор VLAN порта
TLV порта и идентификатора Protocol VLAN	Указывает идентификатор Protocol VLAN порта
TLV имени VLAN	Указывает имя VLAN порта
TLV идентификации протокола	Указывает тип протокола, поддерживаемый портом

ПРИМЕЧАНИЕ: коммутаторы QTECH, совместимые с LLDP, не отправляют TLV идентификации протокола, но получают этот TLV.

IEEE 802.3 Специфичные TLV организаций

В следующей таблице описываются TLV для конкретных организаций IEEE 802.3.

Тип TLV	Описание
Конфигурация MAC/PHY//Статус TLV	Указывает скорость и дуплексный режим порта, а также необходимость поддержки и включения автосогласования

Тип TLV	Описание
TLV питания через MDI	Указывает мощность источника питания порта
TLV агрегации каналов	Указывает емкость агрегации каналов порта и текущее состояние агрегации
TLV максимального размера кадра	Указывает максимальный размер кадра, передаваемого портом

ПРИМЕЧАНИЕ: устройства, совместимые с QTECH LLDP, поддерживают объявление TLV, специфичных для организации IEEE 802.3.

LLDP-MED TLV

LLDP-MED — это расширение LLDP на основе IEEE 802.1AB LLDP. Это позволяет пользователям удобно развертывать сеть Voice Over IP (VoIP) и обнаруживать неисправности. Он предоставляет приложения, включая политики конфигурации сети, обнаружение устройств, управление PoE и управление ресурсами, отвечающие требованиям низкой стоимости, эффективного управления и простоты развертывания.

В следующей таблице описаны TLV LLDP-MED.

Тип TLV	Описание
TLV возможностей LLDP-MED	Указывает тип TLV LLDP-MED, инкапсулированный в LLDPDU, и тип устройства (устройство сетевого подключения или оконечное устройство), а также необходимость поддержки LLDP-MED
TLV сетевой политики	Объявляет конфигурацию портов VLAN, поддерживающую тип приложения (например, услуги передачи голоса или видео) и информацию о приоритете уровня 2
TLV идентификации местоположения	Находит и идентифицирует оконечное устройство
Расширенный TLV питания через MDI	Обеспечивает более продвинутое управление питанием
Оборудование — TLV аппаратной версии	Указывает аппаратную версию устройства MED
Оборудование — TLV версии прошивки	Указывает версию прошивки устройства MED
Оборудование — TLV версии программного обеспечения	Указывает версию программного обеспечения устройства MED

Тип TLV	Описание
Оборудование — TLV серийного номера	Указывает серийный номер устройства MED
Оборудование – TLV названия производителя	Указывает название производителя устройства MED
Оборудование — TLV названия модели	Указывает имя модуля устройства MED
Оборудование — TLV идентификатор объекта	Указывает идентификатор объекта устройства MED, используемый для управления ресурсами и отслеживания объектов

ПРИМЕЧАНИЕ: LLDP-совместимые устройства QTECH поддерживают объявление TLV LLDP-MED.

12.3.2. Обзор

Особенность	Описание
Режим работы LLDP	Настраивает режим передачи и приема пакетов LLDP
Механизм передачи LLDP	Позволяет напрямую подключенным устройствам, совместимым с LLDP, отправлять пакеты LLDP peer'у
Механизм приема LLDP	Позволяет напрямую подключенным устройствам, совместимым с LLDP, получать пакеты LLDP от peer'а

12.3.3. Режим работы LLDP

Настройте рабочий режим LLDP, чтобы указать режим передачи и приема пакетов LLDP.

12.3.3.1. Принцип работы

LLDP обеспечивает три режима работы:

- TxRx: передает и принимает LLDPDU.
- Rx Only: принимает только LLDPDU.
- Tx Only: передаются только LLDPDU.

При изменении режима работы LLDP порт инициализирует протокол state machine. Вы можете установить задержку инициализации порта, чтобы предотвратить повторную инициализацию порта из-за частых изменений режима работы LLDP.

12.3.3.2. Связанная конфигурация

Настройка режима работы LLDP

Режим работы LLDP по умолчанию — TxRx.

Вы можете запустить команду **lldp mode**, чтобы настроить режим работы LLDP.

Если установлен режим работы TxRx, устройство может как передавать, так и принимать пакеты LLDP. Если для режима работы установлено значение Rx Only, устройство может принимать только пакеты LLDP. Если установлен режим работы Tx Only, устройство может передавать только пакеты LLDP. Если рабочий режим отключен, устройство не может передавать или принимать LLDP-пакеты.

12.3.4. Механизм передачи LLDP

Пакеты LLDP информируют peer'ы об их соседях. Когда режим передачи LLDP отменен или отключен, пакеты LLDP не могут быть переданы соседям.

12.3.4.1. Принцип работы

LLDP периодически передает пакеты LLDP при работе в режиме TxRx или Tx Only. При изменении информации о локальном устройстве LLDP немедленно передает LLDP-пакеты. Вы можете настроить время задержки, чтобы избежать частой передачи пакетов LLDP, вызванных частыми изменениями локальной информации.

LLDP предоставляет два типа пакетов:

- Стандартный пакет LLDP, который содержит информацию об управлении и конфигурации локального устройства.
- Shutdown-пакет: когда режим работы LLDP отключен или порт выключен, будут передаваться пакеты Shutdown LLDP. Пакет Shutdown состоит из Chassis ID TLV, Port ID TLV, Time To Live TLV и End OF LLDP TLV. TTL в Time to Live TLV равен 0. Когда устройство получает пакет LLDP Shutdown, оно считает информацию о соседе недействительной и немедленно удаляет ее.

Когда рабочий режим LLDP изменяется с disabled или Rx на TxRx или Tx, или, когда LLDP обнаруживает нового соседа (т. е. устройство получает новый пакет LLDP, а информация о соседе не сохраняется локально), запускается механизм быстрой передачи, чтобы сосед быстро узнал информацию об устройстве. Механизм быстрой передачи позволяет устройству передавать несколько пакетов LLDP с интервалом в 1 секунду.

12.3.4.2. Связанная конфигурация

Настройка режима работы LLDP

Режим работы по умолчанию — TxRx.

Запустите команду **lldp mode txrx** или **lldp mode tx**, чтобы включить функцию передачи пакетов LLDP. Запустите команду **lldp mode rx** или **no lldp mode**, чтобы отключить функцию передачи пакетов LLDP.

Чтобы включить прием пакетов LLDP, установите режим работы TxRx или Rx Only. Если для режима работы установлено значение Rx Only, устройство может принимать только пакеты LLDP.

Настройка задержки передачи LLDP

Задержка передачи LLDP по умолчанию составляет 2 секунды.

Запустите команду **lldp timer tx-delay**, чтобы изменить задержку передачи LLDP.

Если для задержки установлено очень маленькое значение, частая смена локальной информации вызовет частую передачу пакетов LLDP. Если для задержки установлено очень большое значение, пакет LLDP не может быть передан, даже если локальная информация изменена.

Настройка интервала передачи LLDP

Интервал передачи LLDP по умолчанию составляет 30 секунд.

Запустите команду **lldp timer tx-interval**, чтобы изменить интервал передачи LLDP.

Если интервал установлен на очень маленькое значение, пакеты LLDP могут передаваться часто. Если для интервала задано очень большое значение, peer может не обнаружить локальное устройство вовремя.

Настройка TLV для объявления

По умолчанию интерфейсу разрешено объявлять TLV всех типов, кроме Location Identification TLV.

Запустите команду **lldp tlv-enable**, чтобы изменить объявляемые TLV.

Настройка счетчика быстрой передачи LLDP

По умолчанию быстро передаются три пакета LLDP.

Запустите команду **lldp fast-count**, чтобы изменить количество быстро передаваемых пакетов LLDP.

12.3.5. Механизм приема LLDP

Устройство может обнаружить соседа и определить, следует ли состарить информацию о соседе в соответствии с полученными пакетами LLDP.

12.3.5.1. Принцип работы

Устройство может получать пакеты LLDP при работе в режиме TxRx или Rx Only. После получения пакета LLDP устройство выполняет проверку достоверности. После того, как пакет проходит проверку, устройство проверяет, содержит ли пакет информацию о новом соседе или о существующем соседе, и сохраняет информацию о соседе локально. Устройство устанавливает TTL информации о соседях в соответствии со значением TTL TLV в пакете. Если значение TTL TLV равно 0, информация о соседях немедленно устаревает.

12.3.5.2. Связанная конфигурация

Настройка режима работы LLDP

Режим работы LLDP по умолчанию — TxRx.

Запустите команду **lldp mode txrx** или **lldp mode rx**, чтобы включить функцию приема пакетов LLDP. Запустите команду **lldp mode tx** или **no lldp mode**, чтобы отключить функцию приема пакетов LLDP.

Чтобы включить прием пакетов LLDP, установите режим работы TxRx или Rx Only. Если установлен режим работы Tx Only, устройство может передавать только пакеты LLDP.

12.4. Конфигурация

Конфигурация	Описание и команда	
Настройка функции LLDP	(Опционально) Используется для включения или отключения функции LLDP в режиме глобальной конфигурации или конфигурации интерфейса	
	lldp enable	Включает функцию LLDP

Конфигурация	Описание и команда	
Настройка функции LLDP	**no lldp enable**	Отключает функцию LLDP
Настройка режима работы LLDP	(Опционально) Используется для настройки режима работы LLDP	
	lldp mode {rx | tx | txrx }	Настраивает режим работы LLDP
	no lldp mode	Выключает рабочий режим LLDP
Настройка TLV для объявления	(Опционально) Он используется для настройки объявляемых TLV	
	lldp tlv-enable	Настраивает TLV для объявления
	no lldp tlv-enable	Отменяет TLV
Настраивает адрес управления для объявления	(Опционально) Используется для настройки адреса управления, который будет объявляться в пакетах LLDP	
	lldp management-address-tlv [*ip-address*]	Настраивает адрес управления для объявления в пакетах LLDP
	no lldp management-address-tlv	Отменяет адрес управления
Настройка	(Опционально) Используется для настройки количества быстро передаваемых пакетов LLDP	
	lldp fast-count value	Настраивает счетчик быстрых передач LLDP
	no lldp fast-count	Восстанавливает значение по умолчанию счетчика быстрых передач LLDP
Настройка множителя TTL и интервала передачи	(Опционально) Используется для настройки множителя TTL и интервала передачи	
	lldp hold-multiplier *value*	Настраивает множитель TTL
	no lldp hold-multiplier	Восстанавливает множитель TTL по умолчанию

Конфигурация	Описание и команда	
Настройка множителя TTL и интервала передачи	**lldp timer tx-interval** *seconds*	Настраивает интервал передачи
	no lldp timer tx-interval	Восстанавливает интервал передачи по умолчанию
Настройка	(Опционально) Используется для настройки времени задержки для передачи пакетов LLDP	
	lldp timer reinit-delay *seconds*	Настраивает задержку передачи
	no lldp timer reinit-delay	Восстанавливает задержку передачи по умолчанию
	(Опционально) Используется для настройки времени задержки для инициализации LLDP на любом интерфейсе	
	lldp timer reinit-delay *seconds*	Настраивает задержку инициализации
	no lldp timer reinit-delay	Восстанавливает задержку инициализации по умолчанию
Настройка функции Trap LLDP	(Опционально) Используется для настройки функции LLDP Trap	
	lldp notification remote-change enable	Включает функцию LLDP Trap
	no lldp notification remote-change enable	Отключает функцию LLDP Trap
	lldp timer notification-interval	Настраивает интервал передачи LLDP Trap
	no lldp timer notification-interval	Восстанавливает интервал передачи LLDP Trap по умолчанию
Настройка функции обнаружения ошибок LLDP	(Опционально) Используется для настройки функции обнаружения ошибок LLDP	
	lldp error-detect	Включает функцию обнаружения ошибок LLDP

Конфигурация	Описание и команда	
Настройка функции обнаружения ошибок LLDP	**no lldp error-detect**	Отключает функцию обнаружения ошибок LLDP
Настройка формата инкапсуляции LLDP	(Опционально) Используется для настройки формата инкапсуляции LLDP	
	lldp encapsulation snap	Устанавливает формат инкапсуляции LLDP на SNAP
	no lldp encapsulation snap	Устанавливает формат инкапсуляции LLDP на Ethernet II
Настройка сетевой политики LLDP	(Опционально) Используется для настройки сетевой политики LLDP	
	lldp network-policy profile profile-num	Настраивает сетевую политику LLDP
	no lldp network-policy profile *profile-num*	Удаляет сетевую политику LLDP
Настройка адреса Civic	(Опционально) Используется для настройки адрес Civic устройства	
	{ country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-locationinformation | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code } *ca-word*	Настраивает адрес Civic устройства

Конфигурация	Описание и команда	
Настройка адреса Civic	**no { country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code }** *ca-word*	Удаляет адрес Civic устройства
Настройка номера телефона экстренной службы	(Опционально) Используется для настройки номера экстренной службы устройства	
	lldp location elin identifier *id* **elin-location** *tel-number*	Настраивает экстренный номер телефона устройства
	no lldp location elin identifier *id*	Удаляет экстренный номер телефона устройства
Настройка функции игнорирования обнаружения PVID	(Опционально) Используется для игнорирования обнаружения PVID	
	lldp ignore pvid-error-detect	Включает функцию игнорирования обнаружения PVID
	no lldp ignore pvid-error-detect	Отключает функцию игнорирования обнаружения PVID

12.4.1. Настройка функции LLDP

12.4.1.1. Эффект конфигурации

Включите или отключите функцию LLDP.

12.4.1.2. Примечания

Чтобы функция LLDP действовала на интерфейсе, необходимо включить функцию LLDP глобально и на интерфейсе.

12.4.1.3. Шаги настройки

- Опционально.
- Настройте функцию LLDP в глобальном режиме или в режиме конфигурации интерфейса.

12.4.1.4. Проверка

Показать статус LLDP

- Проверьте, включена ли функция LLDP в режиме глобальной конфигурации.
- Проверьте, включена ли функция LLDP в режиме конфигурации интерфейса.

12.4.1.5. Связанные команды

Включение функции LLDP

Команда	**lldp enable**
Командный режим	Режим глобальной конфигурации/режим конфигурации интерфейса
Руководство по использованию	Функция LLDP вступает в силу на интерфейсе только после ее включения в режиме глобальной конфигурации и режиме конфигурации интерфейса

Отключение функции LLDP

Команда	**no lldp enable**
Командный режим	Режим глобальной конфигурации/режим конфигурации интерфейса

12.4.1.6. Пример конфигурации

Отключение функции LLDP

Шаги настройки	Отключите функцию LLDP в режиме глобальной конфигурации
	QTECH(config)#no lldp enable
Проверка	Отображает глобальный статус LLDP
	QTECH(config)#show lldp status Global status of LLDP: Disable

12.4.1.7. Распространенные ошибки

- Если функция LLDP включена на интерфейсе, но отключена в режиме глобальной конфигурации, функция LLDP не действует на интерфейсе.
- Порт может узнать максимум пять соседей.
- Если сосед не поддерживает LLDP, но подключен к устройству с поддержкой LLDP, порт может получить информацию об устройстве, которое не подключено к порту напрямую, поскольку сосед может пересылать пакеты LLDP.

12.4.2. Настройка режима работы LLDP

12.4.2.1. Эффект конфигурации

- Если вы установите режим работы LLDP на TxRx, интерфейс может передавать и получать пакеты.
- Если вы установите режим работы LLDP на Tx, интерфейс может только передавать пакеты, но не может принимать пакеты.
- Если вы установите режим работы LLDP на Rx, интерфейс может только получать пакеты, но не может передавать пакеты.
- Если отключить режим работы LLDP, интерфейс не может ни принимать, ни передавать пакеты.

12.4.2.2. Примечания

LLDP работает на физических портах (портах-участниках AP для портов AP). Стекированные порты и порты VSL не поддерживают LLDP.

12.4.2.3. Шаги настройки

- Опционально.
- Установите рабочий режим LLDP на Tx или Rx по мере необходимости.

12.4.2.4. Проверка

Отображение информации о статусе LLDP на интерфейсе.

- Проверьте, вступила ли конфигурация в силу.

12.4.2.5. Связанные команды

Настройка режима работы LLDP

Команда	**lldp mode { rx | tx | txrx }**
Описание параметров	**rx**: принимает только LLDPDU. **tx**: передает только LLDPDU. **txrx**: передает и принимает LLDPDU
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Чтобы LLDP вступил в силу для интерфейса, обязательно включите LLDP глобально и установите режим работы LLDP на интерфейсе на Tx, Rx или TxRx

Отключение режима работы LLDP

Команда	**no lldp mode**
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	После отключения режима работы LLDP на интерфейсе интерфейс не передает и не принимает пакеты LLDP

12.4.2.6. Пример конфигурации

Настройка режима работы LLDP

Шаги настройки	Установите рабочий режим LLDP на Tx в режиме конфигурации интерфейса
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp mode tx
Проверка	Отобразите информации о статусе LLDP на интерфейсе
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : TxOnly Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

12.4.3. Настройка TLV для объявления

12.4.3.1. Эффект конфигурации

Настройте тип объявляемых TLV, чтобы указать LLDPDU в пакетах LLDP.

12.4.3.2. Примечания

- Если вы настраиваете параметр **all** для TLV основного управления, специфичных TLV организации IEEE 802.1 и специфичных TLV организации IEEE 802.3, объявляются все необязательные TLV этих типов.
- Если вы настраиваете параметр **all** для TLV LLDP-MED, объявляются все TLV LLDP-MED, кроме Location Identification TLV.
- Если вы хотите настроить LLDP-MED Capability TLV, сначала настройте LLDP 802.3 MAC/PHY TLV; Если вы хотите отменить LLDP 802.3 MAC/PHY TLV, сначала отмените LLDP-MED Capability TLV.
- Если вы хотите настроить TLV LLDP-MED, настройте LLDP-MED Capability TLV перед настройкой других типов TLV LLDP-MED. Если вы хотите отменить TLV LLDP-MED, отмените TLV Capability LLDP-MED перед отменой TLV других типов

LLDP-MED. Если устройство подключено к IP-телефону, который поддерживает LLDP-MED, вы можете настроить Network Policy TLV для отправки конфигурации политики на IP-телефон.

- Если устройство поддерживает функцию DCBX по умолчанию, портам устройства по умолчанию не разрешено объявлять специфичные TLV организаций IEEE 802.3 и TLV LLDP-MED.

12.4.3.3. Шаги настройки

- Опционально.
- Настройте тип TLV для объявления на интерфейсе.

12.4.3.4. Проверка

Отобразите конфигурации TLV, которые будут объявлены на интерфейсе

- Проверьте, вступила ли конфигурация в силу.

12.4.3.5. Связанные команды

Настройка TLV для объявления

Команда	**lldp tlv-enable { basic-tlv { all | port-description | system-capability | system-description | system-name } |dot1-tlv { all | port-vlan-id | protocol-vlan-id [** *vlan-id* **] | vlan-name [** *vlan-id* **] } |dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier** *id* **| network-policy profile [** *profile-num* **] | power-over-ethernet } }**
Описание параметров	**basic-tlv**: указывает TLV основного управления. **port-description**: указывает TLV описания порта. **system-capability**: указывает TLV системных возможностей. **system-description**: указывает TLV описания системы. **system-name**: указывает TLV имени системы. **dot1-tlv**: указывает специфичные TLV организации IEEE 802.1. **port-vlan-id**: указывает TLV идентификатора порта VLAN. **protocol-vlan-id**: указывает TLV идентификатора VLAN порта и протокола. *vlan-id*: указывает TLV идентификатора VLAN порта и протокола в диапазоне от 1 до 4094. **vlan-name**: указывает TLV имени VLAN. *vlan-id*: указывает имя VLAN в диапазоне от 1 до 4094. **dot3-tlv**: указывает специфичные TLV организации IEEE 802.3. **link-aggregation**: указывает TLV агрегации каналов. **mac-physic**: указывает TLV конфигурации/состояния MAC/PHY. **max-frame-size**: указывает TLV максимального размера кадра. **power**: указывает TLV питания через MDI.

	med-tlv: указывает LLDP MED TLV. **capability**: указывает TLV возможностей LLDP-MED. **inventory**: указывает TLV управлениях ресурсами, который содержит версию аппаратного обеспечения, версию встроенного ПО, версию программного обеспечения, SN, название производителя, название модуля и идентификатор объекта. **location**: указывает TLV идентификации местоположения. **civic-location**: указывает информацию об адресе civic и почтовую информацию. **elin**: указывает номер телефона экстренной службы. *id*: указывает идентификатор политики в диапазоне от 1 до 1024. **network-policy**: указывает TLV сетевой политики. *profile-num*: указывает TLV сетевой политики в диапазоне от 1 до 1024. **power-over-ethernet**: указывает расширенный TLV питания через MDI
Командный режим	Режим конфигурации интерфейса

Отмена TLV

Команда	**no lldp tlv-enable {basic-tlv { all | port-description | system-capability | system-description | system-name } | dot1-tlv { all | port-vlan-id | protocol-vlan-id | vlan-name } | dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power } | med-tlv { all | capability | inventory | location { civic-location | elin } identifier** *id* **| network-policy profile [** *profile-num* **] | power-over-ethernet } }**
Описание параметров	**basic-tlv**: указывает TLV основного управления. **port-description**: указывает TLV описания порта. **system-capability**: указывает TLV системных возможностей. **system-description**: указывает TLV описания системы. **system-name**: указывает TLV имени системы. **dot1-tlv**: указывает специфичные TLV организации IEEE 802.1. **port-vlan-id**: указывает TLV идентификатора порта VLAN. **protocol-vlan-id**: указывает TLV идентификатора VLAN порта и протокола. **vlan-name**: указывает TLV имени VLAN. **dot3-tlv**: указывает специфичные TLV организации IEEE 802.3. **link-aggregation**: указывает TLV агрегации каналов. **mac-physic**: указывает TLV конфигурации/состояния MAC/PHY. **max-frame-size**: указывает TLV максимального размера кадра. **power**: указывает TLV питания через MDI.

	med-tlv: указывает LLDP MED TLV. **capability**: указывает TLV возможностей LLDP-MED. **inventory**: указывает TLV управления ресурсами, который содержит версию аппаратного обеспечения, версию встроенного ПО, версию программного обеспечения, SN, название производителя, название модуля и идентификатор объекта. **location**: указывает TLV идентификации местоположения. **civic-location**: указывает информацию об адресе civic и почтовую информацию. **elin**: указывает номер телефона экстренной службы. *id*: указывает идентификатор политики в диапазоне от 1 до 1024. **network-policy**: указывает TLV сетевой политики. *profile-num*: указывает TLV сетевой политики в диапазоне от 1 до 1024. **power-over-ethernet**: указывает расширенный TLV питания через MDI
Командный режим	Режим конфигурации интерфейса

12.4.3.6. Пример конфигурации

Настройка TLV для объявления

Шаги настройки	Отмените специфичные TLV организации IEEE 802.1 идентификатора VLAN порта и протокола
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Проверка	Отображение конфигурации LLDP TLV в режиме конфигурации интерфейса
	QTECH(config-if-GigabitEthernet 0/1)#show lldp tlv-config interface gigabitethernet 0/1 LLDP tlv-config of port [GigabitEthernet 0/1] NAME STATUS DEFAULT ---------- ------ ------- Basic optional TLV: Port Description TLV YES YES System Name TLV YES YES System Description TLV YES YES System Capabilities TLV YES YES

	Management Address TLV	YES	YES
	IEEE 802.1 extend TLV:		
	Port VLAN ID TLV	YES	YES
	Port And Protocol VLAN ID TLV	NO	YES
	VLAN Name TLV	YES	YES
	IEEE 802.3 extend TLV:		
	MAC-Physic TLV	YES	YES
	Power via MDI TLV	YES	YES
	Link Aggregation TLV	YES	YES
	Maximum Frame Size TLV	YES	YES
	LLDP-MED extend TLV:		
	Capabilities TLV	YES	YES
	Network Policy TLV	YES	YES
	Location Identification TLV	NO	NO
	Extended Power via MDI TLV	YES	YES
	Inventory TLV	YES	YES

12.4.4. Настраивает адрес управления для объявления

12.4.4.1. Эффект конфигурации

- Настройте адрес управления для объявления в пакетах LLDP в режиме настройки интерфейса.
- После того, как адрес управления, который должен быть объявлен, отменен, адрес управления в пакетах LLDP зависит от настроек по умолчанию.

12.4.4.2. Примечания

LLDP работает на физических портах (порты-участники AP для портов AP). Стекированные порты и порты VSL не поддерживают LLDP.

12.4.4.3. Шаги настройки

- Опционально.
- Настройте адрес управления для объявления в пакетах LLDP в режиме настройки интерфейса.

12.4.4.4. Проверка

Отображение информации LLDP на локальном интерфейсе

Проверьте, вступила ли конфигурация в силу.

12.4.4.5. Связанные команды

Настройка адреса управления для объявления

Команда	**lldp management-address-tlv** [*ip-address*]
Описание параметров	*ip-address*: указывает адрес управления, который будет объявлен в пакете LLDP
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Адрес управления по умолчанию объявляется через пакеты LLDP. Адрес управления — это IPv4-адрес минимальной сети VLAN, поддерживаемой портом. Если для VLAN не настроен адрес IPv4, LLDP продолжает поиск соответствующего IP-адреса. Если адрес IPv4 не найден, LLDP ищет IPv6-адрес минимальной VLAN, который поддерживается портом. Если адрес IPv6 не найден, loopback-адрес 127.0.0.1 используется в качестве адреса управления

Отмена адреса управления

Команда	**no lldp management-address-tlv**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Адрес управления по умолчанию объявляется через пакеты LLDP. Адрес управления — это IPv4-адрес минимальной сети VLAN, поддерживаемой портом. Если для VLAN не настроен адрес IPv4, LLDP продолжает поиск соответствующего IP-адреса. Если адрес IPv4 не найден, LLDP ищет IPv6-адрес минимальной VLAN, который поддерживается портом. Если адрес IPv6 не найден, loopback-адрес 127.0.0.1 используется в качестве адреса управления

12.4.4.6. Пример конфигурации

Настройка адреса управления для объявления

Шаги настройки	Установите адрес управления 192.168.1.1 на интерфейсе
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1

	Отобразите конфигурацию на интерфейсе
	QTECH(config-if-GigabitEthernet 0/1)#show lldp local-information interface GigabitEthernet 0/1 Lldp local-information of port [GigabitEthernet 0/1] Port ID type : Interface name Port id : GigabitEthernet 0/1 Port description : GigabitEthernet 0/1 Management address subtype : ipv4 Management address : 192.168.1.1 Interface numbering subtype : ifIndex Interface number : 1 Object identifier : 802.1 organizationally information Port VLAN ID : 1 Port and protocol VLAN ID(PPVID) : 1 PPVID Supported : YES PPVID Enabled : NO VLAN name of VLAN 1 : VLAN0001 Protocol Identity : 802.3 organizationally information Auto-negotiation supported : YES Auto-negotiation enabled : YES PMD auto-negotiation advertised : 1000BASE-T full duplex mode, 100BASE-TX full duplex mode, 100BASE-TX half duplex mode, 10BASE-T full duplex mode, 10BASE-T half duplex mode Operational MAU type : speed(100)/duplex(Full) PoE support : NO Link aggregation supported : YES Link aggregation enabled : NO Aggregation port ID : 0 Maximum frame Size : 1500 LLDP-MED organizationally information

	Power-via-MDI device type : PD Power-via-MDI power source : Local Power-via-MDI power priority : Power-via-MDI power value : Model name : Model name

12.4.5. Настройка счетчика быстрой передачи LLDP

12.4.5.1. Эффект конфигурации

Настройте количество быстро передаваемых пакетов LLDP.

12.4.5.2. Шаги настройки

- Опционально.
- Настройте количество пакетов LLDP, которые быстро передаются, в режиме глобальной конфигурации.

12.4.5.3. Проверка

Отображение глобальной информации о статусе LLDP.

- Проверьте, вступила ли конфигурация в силу.

12.4.5.4. Связанные команды

Настройка счетчика быстрой передачи LLDP

Команда	**lldp fast-count** *value*
Описание параметров	*value*: указывает количество пакетов LLDP, которые быстро передаются. Диапазон значений от 1 до 10. Значение по умолчанию 3
Командный режим	Режим глобальной конфигурации

Восстановление счетчика быстрой передачи LLDP по умолчанию

Команда	**no lldp fast-count**
Командный режим	Режим глобальной конфигурации

12.4.5.5. Пример конфигурации

Настройка счетчика быстрой передачи LLDP

Шаги настройки	Установите счетчик быстрой передачи LLDP на 5 в режиме глобальной конфигурации
	QTECH(config)#lldp fast-count 5
Проверка	Отображение глобальной информации о статусе LLDP
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5

12.4.6. Настройка множителя TTL и интервала передачи

12.4.6.1. Эффект конфигурации

- Настройте множитель TTL.
- Настройте интервал передачи пакетов LLDP.

12.4.6.2. Шаги настройки

- Опционально.
- Выполнять настройку в режиме глобальной конфигурации.

12.4.6.3. Проверка

Отображение информации о статусе LLDP на интерфейсе.

- Проверьте, вступила ли конфигурация в силу.

12.4.6.4. Связанные команды

Настройка множителя TTL

Команда	**lldp hold-multiplier** *value*
Описание параметров	*value*: указывает множитель TTL. Значение варьируется от 2 до 10. Значение по умолчанию — 4

Командный режим	Режим глобальной конфигурации
Руководство по использованию	В пакете LLDP значение TLV Time To Live рассчитывается по следующей формуле: TLV Time to Live = множитель TTL x интервал передачи пакета + 1. Следовательно, вы можете изменить TLV Time to Live в пакетах LLDP, настроив множитель TTL

Восстановление множителя TTL по умолчанию

Команда	**no lldp hold-multiplier**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	В пакете LLDP значение TLV Time To Live рассчитывается по следующей формуле: TLV Time To Live = множитель TTL x интервал передачи пакета + 1. Следовательно, вы можете изменить TLV Time To Live в пакетах LLDP, настроив множитель TTL

Настройка интервала передачи

Команда	**lldp timer tx-interval** *seconds*
Описание параметров	*seconds*: указывает интервал передачи пакета LLDP. Диапазон значенийот 5 до 32 768
Командный режим	Режим глобальной конфигурации

Восстановление интервала передачи по умолчанию

Команда	**no lldp timer tx-interval**
Командный режим	Режим глобальной конфигурации

12.4.6.5. Пример конфигурации

Настройка множителя TTL и интервала передачи

Шаги настройки	Установите множитель TTL на 3 и интревал передачи на 20 секунд. TTL информации локального устройства о соседях составляет 61 секунду
	QTECH(config)#lldp hold-multiplier 3 QTECH(config)#lldp timer tx-interval 20
Проверка	Отображение глобальной информации о статусе LLDP

	QTECH(config)#lldp hold-multiplier 3 QTECH(config)#lldp timer tx-interval 20 QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 20s Hold multiplier : 3 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 3

12.4.7. Настройка задержки передачи

12.4.7.1. Эффект конфигурации

Настройте время задержки для передачи пакетов LLDP.

12.4.7.2. Шаги настройки

- Опционально.
- Выполните настройку в режиме глобальной конфигурации.

12.4.7.3. Проверка

Отображение глобальной информации о статусе LLDP.

- Проверьте, вступила ли конфигурация в силу.

12.4.7.4. Связанные команды

Настройка задержки передачи

Команда	**lldp timer tx-delay** *seconds*
Описание параметров	*seconds*: указывает задержку передачи. Значение варьируется 1 до 8192
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Когда локальная информация об устройстве изменяется, устройство немедленно передает пакеты LLDP своим соседям. Настройте задержку передачи, чтобы предотвратить частую передачу пакетов LLDP, вызванную частыми изменениями локальной информации

Восстановление задержки передачи по умолчанию

Команда	**no lldp timer tx-delay**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Когда локальная информация об устройстве изменяется, устройство немедленно передает пакеты LLDP своим соседям. Настройте задержку передачи, чтобы предотвратить частую передачу пакетов LLDP, вызванную частыми изменениями локальной информации

12.4.7.5. Пример конфигурации

Настройка задержки передачи

Шаги настройки	Установите задержку передачи на 3 секунды
	QTECH(config)#lldp timer tx-delay 3
Проверка	Отображение глобальной информации о статусе LLDP
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s Transmit delay : 3s Notification interval : 5s Fast start counts : 3

12.4.8. Настройка задержки инициализации

12.4.8.1. Эффект конфигурации

Настройте время задержки для инициализации LLDP на любом интерфейсе.

12.4.8.2. Шаги настройки

- Опционально.
- Настройте время задержки для инициализации LLDP на любом интерфейсе.

12.4.8.3. Проверка

Отображение глобальной информации о статусе LLDP.

- Проверьте, вступила ли конфигурация в силу.

12.4.8.4. Связанные команды

Настройка задержки инициализации

Команда	**lldp timer reinit-delay** *seconds*
Описание параметров	*seconds*: указывает задержку инициализации. Диапазон значений от 1 до 10 секунд
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте задержку инициализации для предотвращения частой инициализации state machine, вызванной частыми изменениями режима работы порта

Восстановление задержки инициализации по умолчанию

Команда	**no lldp timer reinit-delay**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте задержку инициализации для предотвращения частой инициализации state machine, вызванной частыми изменениями режима работы порта

12.4.8.5. Пример конфигурации

Настройка задержки инициализации

Шаги настройки	Установите задержку инициализации на 3 секунды
	QTECH(config)#lldp timer reinit-delay 3
Проверка	Отображение глобальной информации о статусе LLDP
	QTECH(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 3s Transmit delay : 2s Notification interval : 5s

	Fast start counts : 3

12.4.9. Настройка функции Trap LLDP

12.4.9.1. Эффект конфигурации

Настройте интервал для передачи Trap-сообщений LLDP.

12.4.9.2. Шаги настройки

Включение функции Trap LLDP

- Опционально.
- Выполните настройку в режиме настройки интерфейса.

Настройка интервала передачи Trap-сообщений LLDP

- Опционально.
- Выполните настройку в режиме глобальной конфигурации.

12.4.9.3. Проверка

Отображение информации о статусе LLDP

- Проверьте, включена ли функция Trap LLDP.
- Проверьте, действует ли настройка интервала.

12.4.9.4. Связанные команды

Включение функции Trap LLDP

Команда	**lldp notification remote-change enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Trap-сообщения LLDP позволяет устройству отправлять локальную информацию LLDP (например, обнаружение соседа и неисправность канала связи) на сервер NMS, чтобы администраторы могли узнать о производительности сети

Отключение функции Trap LLDP

Команда	**no lldp notification remote-change enable**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Trap-сообщения LLDP позволяет устройству отправлять локальную информацию LLDP (например, обнаружение соседа и неисправность канала связи) на сервер NMS, чтобы администраторы могли узнать о производительности сети

Настройка интервала передачи Trap LLDP

Команда	**lldp timer notification-interval** *seconds*
Описание параметров	*seconds*: указывает интервал для передачи Trap-сообщений LLDP. Значение варьируется от 5 до 3600 секунд. Значение по умолчанию 5 секунд
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте интервал передачи Trap LLDP, чтобы предотвратить частую передачу сообщений Trap LLDP. Изменения LLDP, обнаруженные в течение этого интервала, будут переданы на сервер NMS

Восстановление интервала передачи Trap LLDP

Команда	**no lldp timer notification-interval**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Настройте интервал передачи Trap LLDP, чтобы предотвратить частую передачу сообщений Trap LLDP. Изменения LLDP, обнаруженные в течение этого интервала, будут переданы на сервер NMS

12.4.9.5. Пример конфигурации

Включение функции Trap LLDP и настройка интервала передачи Trap LLDP

Шаги настройки	Включите функцию Trap LLDP и установите интервал передачи Trap LLDP равным 10 секундам
	QTECH(config)#lldp timer notification-interval 10 QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp notification remote-change enable
Проверка	Отображение информации о состоянии LLDP
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s Hold multiplier : 4 Reinit delay : 2s

	Transmit delay : 2s Notification interval : 10s Fast start counts : 3 ---------- Port [GigabitEthernet 0/1] ---------- Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : YES Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

12.4.10. Настройка функции обнаружения ошибок LLDP

12.4.10.1. Эффект конфигурации

- Включите функцию обнаружения ошибок LLDP. Когда LLDP обнаруживает ошибку, она регистрируется.
- Настройте функцию обнаружения ошибок LLDP для определения конфигурации VLAN на обоих концах канала, состояния порта, общей конфигурации порта, конфигурации MTU и петель.

12.4.10.2. Шаги настройки

- Опционально.
- Включите или отключите функцию обнаружения ошибок LLDP в режиме конфигурации интерфейса.

12.4.10.3. Проверка

Отображение информации о статусе LLDP на интерфейсе

- Проверьте, вступила ли конфигурация в силу.

12.4.10.4. Связанные команды

Включение функции обнаружения ошибок LLDP

Команда	**lldp error-detect**
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Функция обнаружения ошибок LLDP зависит от определенных TLV в пакетах LLDP, которыми обмениваются устройства на обоих концах канала. Следовательно, устройство должно объявить правильные TLV, чтобы обеспечить функцию обнаружения ошибок LLDP

Отключение функции обнаружения ошибок LLDP

Команда	**no lldp error-detect**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Функция обнаружения ошибок LLDP зависит от определенных TLV в пакетах LLDP, которыми обмениваются устройства на обоих концах канала. Следовательно, устройство должно объявить правильные TLV, чтобы обеспечить функцию обнаружения ошибок LLDP

12.4.10.5. Пример конфигурации

Включение функции обнаружения ошибок LLDP

Шаги настройки	Включите функцию обнаружения ошибок LLDP на интерфейсе GigabitEthernet 0/1
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp error-detect
Проверка	Отображение информации о статусе LLDP на интерфейсе
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable Port state : UP Port encapsulation : Ethernet II Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

12.4.11. Настройка формата инкапсуляции LLDP

12.4.11.1. Эффект конфигурации

Настройте формат инкапсуляции LLDP.

12.4.11.2. Шаги настройки

- Опционально.
- Настройте формат инкапсуляции LLDP на интерфейсе.

12.4.11.3. Проверка

Отображение информации о статусе LLDP интерфейса.

- Проверьте, вступила ли конфигурация в силу.

12.4.11.4. Связанные команды

Установка формата инкапсуляции LLDP на SNAP

Команда	**lldp encapsulation snap**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	**ПРИМЕЧАНИЕ:** конфигурация формата инкапсуляции LLDP на устройстве и его соседях должна быть согласованной

Восстановление формата инкапсуляции LLDP по умолчанию (Ethernet II)

Команда	**no lldp encapsulation snap**
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	**ПРИМЕЧАНИЕ:** конфигурация формата инкапсуляции LLDP на устройстве и его соседях должна быть согласованной

12.4.11.5. Пример конфигурации

Установка формата инкапсуляции LLDP на SNAP

Шаги настройки	Установите формат инкапсуляции LLDP на SNAP
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#lldp encapsulation snap
Проверка	Отображение информации о статусе LLDP на интерфейсе
	QTECH(config-if-GigabitEthernet 0/1)#show lldp status interface gigabitethernet 0/1 Port [GigabitEthernet 0/1] Port status of LLDP : Enable

	Port state : UP Port encapsulation : Snap Operational mode : RxAndTx Notification enable : NO Error detect enable : YES Number of neighbors : 0 Number of MED neighbors : 0

12.4.12. Настройка сетевой политики LLDP

12.4.12.1. Эффект конфигурации

- Настройте сетевую политику LLDP.
- Если устройство подключено к IP-телефону, который поддерживает LLDP-MED, вы можете настроить TLV сетевой политики для передачи конфигурации политики на IP-телефон, что позволит IP-телефону изменить тег и QoS голосовых потоков. В дополнение к сетевой политике LLDP выполните на устройстве следующие шаги: 1. Включите функцию Voice VLAN и добавьте порт, подключенный к IP-телефону, в Voice VLAN. 2. Настройте порт, подключенный к IP-телефону, как доверенный порт QoS (рекомендуется доверенный режим DSCP). 3. Если для порта также включена аутентификация 802.1X, настройте безопасный канал для пакетов из Voice VLAN. Если IP-телефон не поддерживает LLDP-MED, включите функцию Voice VLAN и вручную добавьте MAC-адрес IP-телефона в список OUI Voice VLAN.
- Для настройки режима доверия QoS см. ACL&QoS Configuration/Настройка IP QoS; для настройки безопасного канала см. ACL&QoS Configuration/Настройка ACL.

12.4.12.2. Шаги настройки

- Опционально.
- Настройте сетевую политику LLDP.

12.4.12.3. Проверка

Отображение конфигурации сетевой политики LLDP.

- Проверьте, вступила ли конфигурация в силу.

12.4.12.4. Связанные команды

Настройка сетевой политики LLDP

Команда	**lldp network-policy profile** *profile-num*
Описание параметров	*profile-num*: указывает идентификатор сетевой политики LLDP. Значение варьируется от 1 до 1024
Командный режим	Режим глобальной конфигурации

Руководство по использованию	Запустите эту команду, чтобы перейти в режим сетевой политики LLDP после указания идентификатора политики. После входа в режим сетевой политики LLDP запустите команду **{ voice | voice-signaling } vlan** для настройки определенной сетевой политики

Удаление сетевой политики LLDP

Команда	**no lldp network-policy profile** *profile-num*
Описание параметров	*profile-num*: указывает идентификатор сетевой политики LLDP. Значение варьируется от 1 до 1024
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Запустите эту команду, чтобы перейти в режим сетевой политики LLDP после указания идентификатора политики. После входа в режим сетевой политики LLDP запустите команду **{ voice | voice-signaling } vlan** для настройки определенной сетевой политики

12.4.12.5. Пример конфигурации

Настройка сетевой политики LLDP

Шаги настройки	Установите TLV сетевой политики равным 1, чтобы пакеты LLDP объявлялись портом GigabitEthernet 0/1 и установите идентификатор VLAN для голосового приложения на 3, COS на 4 и DSCP на 6
	QTECH#config QTECH(config)#lldp network-policy profile 1 QTECH(config-lldp-network-policy)# voice vlan 3 cos 4 QTECH(config-lldp-network-policy)# voice vlan 3 dscp 6 QTECH(config-lldp-network-policy)#exit QTECH(config)# interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# lldp tlv-enable med-tlv network-policy profile 1
Проверка	Показать конфигурацию сетевой политики LLDP на локальном устройстве
	network-policy information: ------------------------- network policy profile :1 voice vlan 3 cos 4 voice vlan 3 dscp 6

12.4.13. Настройка адреса Civic

12.4.13.1. Эффект конфигурации

Настройте адрес Civic устройства.

12.4.13.2. Шаги настройки

- Опционально.
- Выполните эту настройку в режиме конфигурации LLDP Civic Address.

12.4.13.3. Проверка

Показать адрес civic LLDP локального устройства

Проверьте, вступила ли конфигурация в силу.

12.4.13.4. Связанные команды

Настройка адреса civic устройства

Команда	Настройка адрес civic LLDP. Используйте опцию **no**, чтобы удалить адрес. **{ country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code }** *ca-word*
Описание параметров	**country**: указывает код страны, состоящий из двух символов. CH означает Китай. **state**: указывает, что тип CA равен 1. **county**: указывает, что тип CA равен 2. **city**: указывает, что тип CA — 3. **division**: указывает, что тип CA равен 4. **neighborhood**: указывает, что тип CA равен 5. **street-group**: указывает, что тип CA равен 6. **leading-street-dir**: указывает, что тип CA равен 16. **trailing-street-suffix**: указывает, что тип CA — 17. **street-suffix**: указывает, что тип CA — 18. **number**: указывает, что тип CA — 19. **street-number-suffix**: указывает, что тип CA равен 20. **landmark**: указывает, что тип CA — 21. **additional-location-information**: указывает, что тип CA — 22. **name**: указывает, что тип CA — 23. **postal-code**: указывает, что тип CA — 24. **building**: указывает, что тип CA — 25. **unit**: указывает, что тип CA — 26.

	floor: указывает, что тип CA — 27. **room**: указывает, что тип CA — 28. **type-of-place**: указывает, что тип CA — 29. **postal-community-name**: указывает, что тип CA равен 30. **post-office-box**: указывает, что тип CA — 31. **additional-code**: указывает, что тип CA — 32. *ca-word*: указывает адрес
Командный режим	Режим конфигурации LLDP Civic Address
Руководство по использованию	После входа в режим конфигурации LLDP Civic Address настройте адрес civic LLDP

Удаление адреса civic устройства

Команда	**no { country | state | county | city | division | neighborhood | street-group | leading-street-dir | trailing-street-suffix | street-suffix | number | street-number-suffix | landmark | additional-location-information | name | postal-code | building | unit | floor | room | type-of-place | postal-community-name | post-office-box | additional-code }**
Командный режим	Режим конфигурации LLDP Civic Address
Руководство по использованию	После входа в режим конфигурации LLDP Civic Address настройте адрес civic LLDP

Настройка типа устройства

Команда	**device-type** *device-type*
Описание параметров	*device-type*: указывает тип устройства. Значение варьируется от 0 до 2. Значение по умолчанию 1. 0 указывает, что тип устройства — сервер DHCP. 1 указывает, что тип устройства — коммутатор. 2 указывает, что тип устройства — LLDP MED
Командный режим	Режим конфигурации адреса civic LLDP
Руководство по использованию	После входа в режим конфигурации LLDP Civic Address настройте тип устройства

Восстановление типа устройства

Команда	**no device-type**
Командный режим	Режим конфигурации LLDP Civic Address
Руководство по использованию	После входа в режим конфигурации LLDP Civic Address восстановите настройки по умолчанию

12.4.13.5. Пример конфигурации

Настройка адреса civic устройства

Шаги настройки	Установить адрес порта GigabitEthernet 0/1 следующим образом: укажите страну RU, город Moscow и почтовый индекс 121471
	QTECH#config QTECH(config)#lldp location civic-location identifier 1 QTECH(config-lldp-civic)# country RU QTECH(config-lldp-civic)# city Moscow QTECH(config-lldp-civic)# postal-code 121471
Проверка	Отобразите адрес civic LLDP порта GigabitEthernet 0/11
	civic location information: --------------------------- Identifier :1 country :RU device type :1 city :Moscow postal-code :121471

12.4.14. Настройка номера телефона экстренной службы

12.4.14.1. Эффект конфигурации

Настройте номер телефона экстренной службы устройства.

12.4.14.2. Шаги настройки

- Опционально.
- Выполните эту настройку в режиме глобальной конфигурации.

12.4.14.3. Проверка

Отображение номера телефона экстренной службы локального устройства

Проверьте, вступила ли конфигурация в силу.

12.4.14.4. Связанные команды

Настройка номера телефона экстренной службы устройства

Команда	**lldp location elin identifier** *id* **elin-location** *tel-number*
Описание параметров	*id*: указывает идентификатор номера телефона экстренной службы. Диапазон значений от 1 до 1024. *tel-number*: указывает номер телефона экстренной службы, содержащий от 10 до 25 символов
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы настроить номер телефона экстренной службы

Удаление номера телефона экстренной службы устройства

Команда	**no lldp location elin identifier** *id*
Описание параметров	*id*: указывает идентификатор номера телефона экстренной службы. Диапазон значенийот 1 до 1024
Командный режим	Режим глобальной конфигурации

12.4.14.5. Пример конфигурации

Настройка номера телефона экстренной службы устройства

Шаги настройки	Установите номер телефона экстренной службы порта GigabitEthernet 0/1 на 84954718118
	QTECH#config QTECH(config)#lldp location elin identifier 1 elin-location 84954718118
Проверка	Отображение номера телефона экстренной службы порта GigabitEthernet 0/1
	elin location information: ------------------------

	Identifier :1 elin number : 84954718118

12.4.15. Настройка функции игнорирования обнаружения PVID

12.4.15.1. Эффект конфигурации

Игнорирует обнаружение PVID.

12.4.15.2. Шаги настройки

- Опционально.
- В соответствии с текущим состоянием выберите, следует ли включить функцию.

12.4.15.3. Проверка

Отображение информации LLDP.

- Проверьте, совпадает ли состояние обнаружения PVID в глобальном LLDP с вашей конфигурацией.

12.4.15.4. Связанные команды

Игнорирование обнаружения PVID

Команда	**lldp ignore pvid-error-detect**
Командный режим	Режим глобальной конфигурации
Руководство по использованию	Используйте команду, чтобы игнорировать обнаружение PVID

12.4.15.5. Пример конфигурации

Настройка функции игнорирования обнаружения PVID

Шаги настройки	Игнорирует обнаружение PVID в режиме глобальной конфигурации
	QTECH#config QTECH(config)#lldp ignore pvid-error-detect
Проверка	Показать глобальную информация LLDP
	uijie(config)#show lldp status Global status of LLDP : Enable Neighbor information last changed time : Transmit interval : 30s

	Hold multiplier : 4 Reinit delay : 2s Transmit delay : 2s Notification interval : 5s Fast start counts : 5 Igore PVID error detect : YES

12.5. Мониторинг

12.5.1. Очистка

ПРИМЕЧАНИЕ: выполнение команд **clear** может привести к потере жизненно важной информации и, таким образом, к прерыванию работы служб.

Описание	Команда
Очищает статистику LLDP	**clear lldp statistics** [**interface** *interface-name*]
Очищает информацию о соседях LLDP	**clear lldp table** [**interface** *interface-name*]

12.5.2. Отображение

Описание	Команда
Отображает информацию LLDP на локальном устройстве, которая будет организована как TLV и отправлена соседям	**show lldp local-information** [**global** | **interface** *interface-name*]
Отображает адрес civic LLDP или номер телефона экстренной службы локального устройства	**show lldp location** { **civic-location** | **elin-location** } { **identifier** *id* | **interface** *interface-name* | **static** }
Отображает информацию LLDP о соседе	**show lldp neighbors** [**interface** *interface-name*] [**detail**]
Отображает конфигурацию сетевой политики LLDP локального устройства	**show lldp network-policy** { **profile** [*profile-num*] | **interface** *interface-name* }
Отображает статистику LLDP	**show lldp statistics** [**global** | **interface** *interface-name*]
Отображает информацию о состоянии LLDP	**show lldp status** [**interface** *interface-name*]

Описание	Команда
Отображает конфигурацию TLV, которые должны быть объявлены портом	**show lldp tlv-config** [**interface** *interface-name*]

12.5.3. Отладка

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

Описание	Команда
Отладка обработки ошибок LLDP	**debug lldp error**
Отладка обработки событий LLDP	**debug lldp event**
Отладка обработки «горячего» резервного копирования LLDP	**debug lldp ha**
Отладка приема пакетов LLDP	**debug lldp packet**
Отладка state machine LLDP	**debug lldp stm**

13. НАСТРОЙКА QINQ

13.1. Обзор

QinQ используется для вставки тега общедоступной виртуальной локальной сети (VLAN) в пакет с тегом приватной VLAN, чтобы разрешить передачу пакета с двойным тегом по сети поставщика услуг (SP).

Пользователи в городской сети (MAN) должны быть разделены с помощью VLAN. IEEE 802.1Q поддерживает только 4094 VLAN, что не достаточно. Благодаря инкапсуляции с двойным тегом, предоставляемой QinQ, пакет передается по сети SP на основе уникального внешнего тега VLAN, назначенного общедоступной сетью. Таким образом, можно повторно использовать приватные VLAN, что увеличивает количество доступных тегов VLAN и обеспечивает простую функцию виртуальной приватной сети уровня 2 (VPN).

Рисунок 13-1 ниже показывает процесс внедрения двойного тега. Вход в сеть SP называется портом dot1q-tunnel или сокращенно туннельным портом. Все кадры, поступающие на границы провайдера (PE), считаются непомеченными тегами. Все теги, будь то кадры без тегов или кадры с тегами клиентской VLAN, инкапсулируются с тегами сети SP. Идентификатор VLAN сети SP — это идентификатор VLAN по умолчанию для туннельного порта.

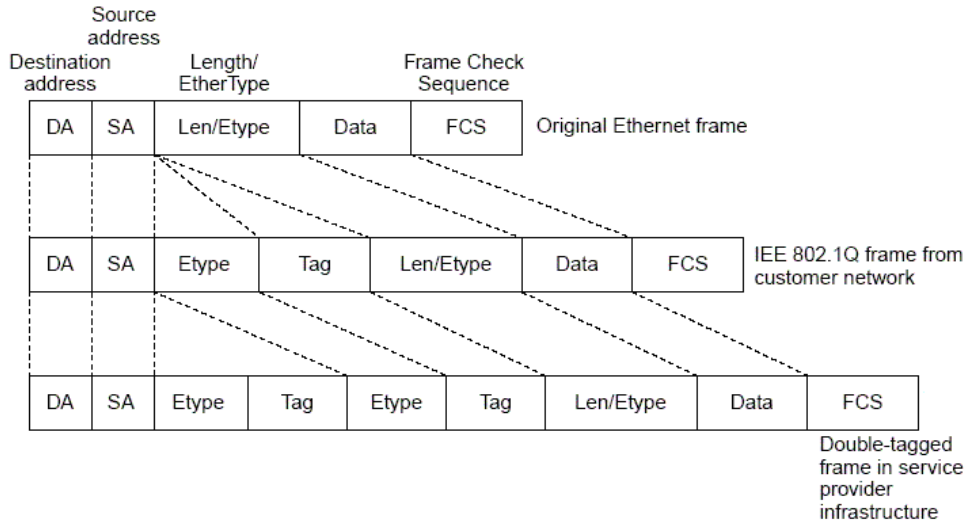


Рисунок 13-1. Инкапсуляция внешнего тега

13.1.1. Протоколы и стандарты

IEEE 802.1ad

13.2. Приложения

Приложение	Описание
Внедрение VPN уровня 2 с помощью базового QinQ на основе портов	Данные передаются от клиента A и клиента B к peer end'y без конфликтов в сети SP, даже если данные поступают из одной и той же VLAN

Приложение	Описание
Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью выборочного QinQ (Selective QinQ) на основе C-TAG	Внешние теги гибко вставляются в кадры в зависимости от различных клиентских VLAN для достижения VPN уровня 2, разделения потоков трафика сервисов (например, широкополосного доступа в Интернет и IPTV) и реализации различных политик QoS. QinQ на основе тега клиента (C-TAG) более гибок, чем QinQ на основе порта
Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью выборочного QinQ (Selective QinQ) на основе ACL	Различные потоки трафика сервисов, такие как широкополосный доступ в Интернет и IPTV, разделяются на основе списков управления доступом (ACL). Различные политики QoS применяются к потокам трафика сервисов через Selective QinQ
Внедрение агрегации VLAN для различных сервисов посредством сопоставления VLAN	Различные потоки трафика сервисов (PC, IPTV и VoIP) передаются через разные VLAN. Сети VLAN объединяются в кампусной сети, поэтому только одна VLAN используется для передачи одних и тех же потоков трафика сервисов, что позволяет экономить ресурсы VLAN
Реализация прозрачной передачи уровня 2 на основе QinQ	Клиентская сеть A и клиентская сеть B в разных областях могут выполнять расчет единого протокола множественного spanning tree (MSTP) или развертывание VLAN в сети SP, не затрагивая сеть SP

13.2.1. Внедрение VPN уровня 2 с помощью базового QinQ на основе портов

13.2.1.1. Сценарий

SP предоставляет услугу VPN клиенту A и клиенту B.

- Клиент A и клиент B принадлежат к разным VLAN в сети SP и обеспечивают связь через соответствующие VLAN SP.
- Сети VLAN Клиента A и Клиента B прозрачны для сети SP. Сети VLAN можно использовать повторно без конфликтов.
- Туннельный порт инкапсулирует собственный тег VLAN в каждый пакет. Пакеты передаются через Native VLAN по сети SP, не затрагивая VLAN Клиента A и Клиента B, таким образом реализуя простую VPN уровня 2.

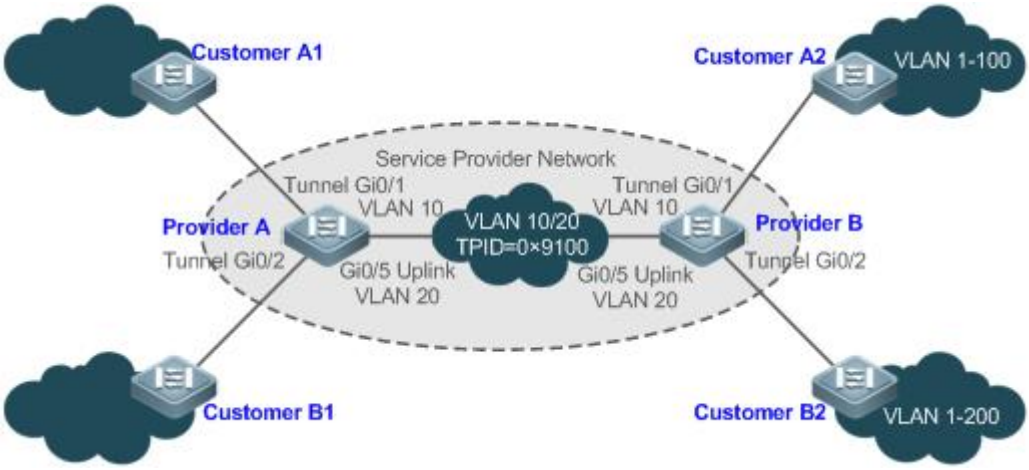


Рисунок 13-2.

Клиент A1 и Клиент A2 являются конечными клиентами (CE) для сети Клиента A. Клиент B1 и Клиент B2 являются CE для сети Клиента B.

Провайдер A и Провайдер B являются PE в сети SP. Клиент A и Клиент B получают доступ к сети SP через Провайдера A и Провайдера B.

Диапазон VLAN Клиента A от 1 до 100.

Диапазон VLAN Клиента B от 1 до 200.

13.2.1.2. Развертывание

- Включите базовый QinQ на PE для реализации VPN уровня 2.
- Идентификаторы протокола тегов (TPID), используемые многими коммутаторами (включая коммутаторы QTECH), установлены на 0x8100, но коммутаторы некоторых поставщиков не используют 0x8100. В последнем случае вам необходимо изменить значение TPID на портах Uplink PE на значения TPID, используемые сторонними коммутаторами.
- Настройте репликацию приоритетов и сопоставление приоритетов для класса обслуживания (CoS) на туннельных портах PE, а также настройте разные политики QoS для разных потоков трафика сервисов (подробности см. в разделе ACL&QoS Configuration/Настройка QoS).

13.2.2. Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью выборочного QinQ (Selective QinQ) на основе C-TAG

13.2.2.1. Сценарий

Базовый QinQ инкапсулирует внешний тег Native VLAN в пакет. То есть инкапсуляция внешних тегов зависит от Native VLAN на туннельных портах. Selective QinQ инкапсулирует внешний тег в пакет на основе его внутреннего тега для реализации прозрачной передачи VPN и гибкого применения политик QoS.

- Широкополосный доступ в Интернет и IPTV являются важными услугами, предоставляемыми MAN. SP управляют различными потоками трафика сервисов через разные VLAN и предоставляют политики QoS для VLAN или CoS. Вы можете включить QinQ на основе C-TAG на PE для инкапсуляции внешних тегов VLAN в потоки трафика сервисов для достижения прозрачной передачи на основе политик QoS сети SP.

- Важные сервисы и обычные сервисы разделены в разных диапазонах VLAN. Клиент может прозрачно передавать потоки трафика сервисов по сети SP через Selective QinQ на основе C-TAG и обеспечивать предпочтительную передачу важных потоков трафика сервисов с помощью политик QoS сети SP.

На Рисунке ниже объединяются коммутаторы по этажам внутри жилых домов. Широкополосный доступ в Интернет и услуги IPTV разделены виртуальными локальными сетями с различными политиками QoS.

- Потоки трафика сервисов широкополосного доступа в Интернет и IPTV передаются прозрачно различными VLAN по сети SP.
- Сеть SP предоставляет политики QoS на основе VLAN или CoS. На PE вы можете инкапсулировать внешний тег в поток трафика сервисов на основе его внутреннего тега VLAN или установить CoS для обеспечения предпочтительной передачи потоков трафика сервисов по сети SP.
- Значения CoS сервисных пакетов могут быть изменены с помощью сопоставления приоритетов или репликации, чтобы гибко применять политики QoS сети SP.

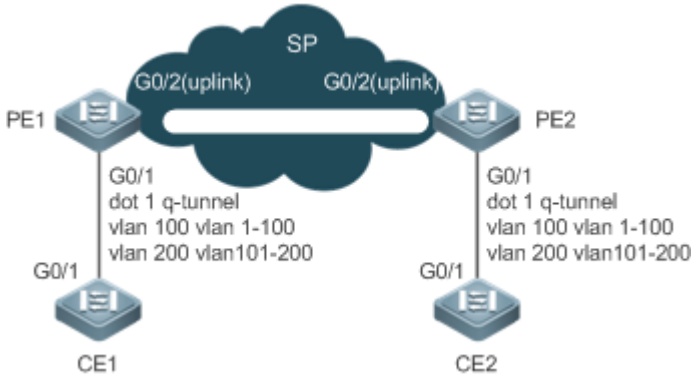


Рисунок 13-3.

CE 1 и CE 2 имеют доступ к сети SP через PE1 и PE2.

На CE 1 and CE 2, потоки широкополосного доступа в Интернет передаются через VLAN 1–100, а потоки IPTV передаются через VLAN 101–200.

PE 1 и PE 2 настроены с Туннельными портами и сопоставлением VLAN для разделения потоки трафика сервисов.

13.2.2.2. Развертывание

- Настройте Selective QinQ на основе C-TAG на портах (G0/1) PE 1 и PE 2, подключенных к CE 1 и CE 2 соответственно, чтобы реализовать разделение и прозрачную передачу потоков трафика сервисов.
- Если сеть SP предоставляет политики QoS на основе VLAN или CoS, вы можете инкапсулировать внешний тег в потоке обслуживания на основе его внутреннего тега или установить CoS посредством репликации приоритета или сопоставления на PE 1 и PE 2, чтобы обеспечить предпочтительную передачу потоков трафика сервисов по сети SP.

13.2.3. Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью выборочного QinQ (Selective QinQ) на основе ACL

13.2.3.1. Сценарий

Потоки трафика сервисов из клиентской сети могут быть классифицированы по MAC-адресу, IP-адресу или типу протокола, а не по VLAN. В клиентской сети может быть много низкоуровневых устройств доступа, которые не могут разделять потоки трафика сервисов по идентификаторам VLAN. В предыдущих двух ситуациях пакеты из клиентской сети не могут быть инкапсулированы внешними тегами на основе их внутренних тегов для реализации прозрачной передачи и реализации политик QoS. Потоки трафика сервисов можно классифицировать по MAC-адресу, IP-адресу или типу протокола с помощью ACL. Selective QinQ использует ACL для разделения потоков трафика сервисов и добавления или изменения внешних тегов для реализации политик VPN уровня 2 и QoS на основе различных потоков трафика сервисов.

На Рисунке ниже разные VLAN настроены на PE 1 и PE 2 для передачи различных потоков трафика сервисов, классифицированных с помощью ACL. Если сеть SP предоставляет политики QoS, основанные на различных сервисах, некоторые сервисы могут передаваться с предпочтением.

- Внешние теги VLAN инкапсулируются на основе различных потоков трафика сервисов. Потоки трафика сервисов клиентской сети могут передаваться прозрачно, а ее филиалы могут получать доступ друг к другу.
- Сеть SP предоставляет политики QoS на основе тегов VLAN или значений CoS для обеспечения предпочтительной передачи определенных потоков трафика сервисов.

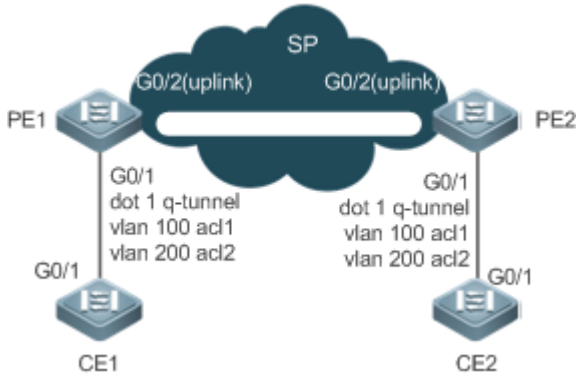


Рисунок 13-4.

CE 1 и CE 2 имеют доступ к сети SP через PE1 и PE2.

PE 1 и PE 2 классифицируют потоки на основе списков ACL: ACL 1 соответствует потокам протокола «точка-точка» через Ethernet (PPPoE), а ACL 2 соответствует потокам IPTV.

PE 1 и PE 2 настроены с туннельными портами, а также политиками инкапсуляции внешних тегов, применимыми к потокам трафика сервисов, распознаваемым различными ACL.

13.2.3.2. Развертывание

- Настройте ACL на PE 1 и PE 2, чтобы разделить потоки трафика сервисов.
- Настройте Selective QinQ на основе ACL на портах (G0/1) PE 1 и PE 2, подключенных к CE 1 и CE 2 соответственно, чтобы реализовать разделение и прозрачную передачу потоков трафика сервисов.

- Если сеть SP предоставляет политики QoS на основе VLAN или CoS, вы можете инкапсулировать внешний тег в потоке трафика сервисов на основе его внутреннего тега или установить CoS посредством репликации приоритета или сопоставления на PE 1 и PE 2, чтобы обеспечить предпочтительную передачу потоков трафика сервисов по сети SP.

13.2.4. Внедрение агрегации VLAN для различных сервисов посредством сопоставления VLAN

13.2.4.1. Сценарий

Различные потоки трафика сервисов разных пользователей разделены в сети кампуса.

- Различные потоки трафика сервисов передаются через разные сети VLAN на домашнем шлюзе.
- Одни и те же потоки трафика сервисов от разных пользователей разделяются на коммутаторе на этаже.
- Одни и те же потоки трафика сервисов от разных пользователей отправляются коммутатором кампуса через одну единственную VLAN.

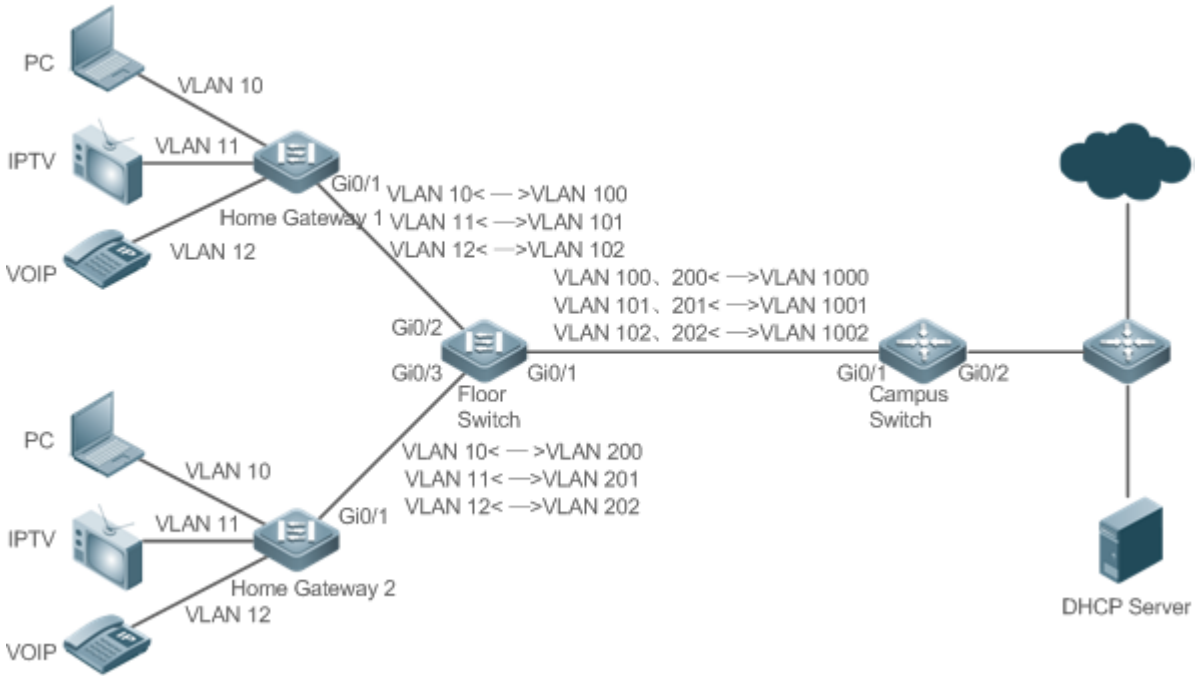


Рисунок 13-5.

PC, IPTV и VoIP — это разные пользовательские сервисы.

Коммутатор A и Коммутатор B являются шлюзовыми устройствами разных пользователей.

Коммутатор C — коммутатор на этаже.

Коммутатор D — это кампусный коммутатор.

13.2.4.2. Развертывание

- На домашних шлюзах настройте виртуальные локальные сети для разных сервисов, чтобы разделить потоки трафика сервисов. Например, настройте VLAN 10 для службы PC, VLAN 11 для IPTV и VLAN 12 для VoIP.

- На портах коммутатора на этаже (коммутатор D), подключенного к устройствам домашнего шлюза, настройте сопоставление VLAN для разделения потоков трафика сервисов разных пользователей.
- На кампусном коммутаторе настройте сопоставление VLAN для разделения потоков трафика сервисов.
- В предыдущем развертывании различные потоки трафика сервисов для разных пользователей были разделены.

13.2.5. Реализация прозрачной передачи уровня 2 на основе QinQ

13.2.5.1. Сценарий

Прозрачная передача уровня 2 между клиентскими сетями не влияет на сеть SP.

- Пакеты уровня 2 в сетях клиентов прозрачны для сетей SP и могут передаваться между сетями клиентов без воздействия на сети SP.

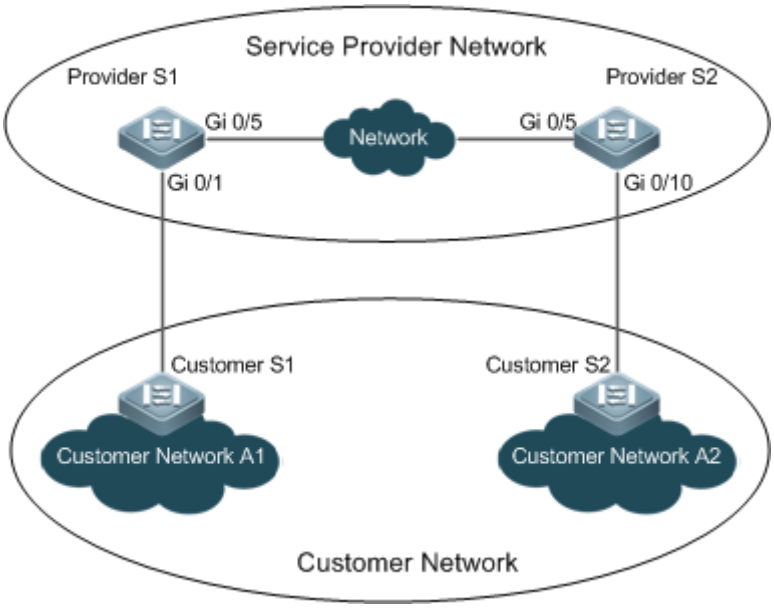


Рисунок 13-6.

Клиент S1 и Клиент S2 имеют доступ к сети SP через Провайдера S1 и Провайдера S2.

Провайдер S1 и Провайдер S2 включены с прозрачной передачей уровня 2 глобально, а порты Gi 0/1 и Gi 0/10 поддерживают прозрачную передачу уровня 2.

13.2.5.2. Развертывание

- На портах PE (Провайдер S1 и Провайдер S2), подключенных к Клиенту S1 и Клиенту S2 соответственно, настройте прозрачную передачу уровня 2 между клиентской сетью A1 и клиентской сетью A2 без влияния на сеть SP.
- Настройте прозрачную передачу STP на основе требований пользователя, чтобы реализовать прозрачную передачу пакетов блока данных протокола моста (BPDU) между сетью клиента A1 и сетью клиента A2 и выполнить вычисления унифицированных MSTP в сети SP.
- Настройте прозрачную передачу протокола регистрации VLAN GARP (GVRP) на основе требований пользователя для реализации прозрачной передачи пакетов GVRP между сетями клиентов A1 и сетями клиентов A2 и динамической конфигурации VLAN в сетях клиентов через сеть SP.

13.3. Функции

13.3.1. Базовые определения

Basic QinQ (Базовый QinQ)

Настройте базовый QinQ на туннельном порту и настройте Native VLAN для порта. Пакеты, входящие в порт, инкапсулируются внешними тегами, содержащими идентификатор Native VLAN. Базовый QinQ не разделяет потоки трафика сервисов и не может гибко инкапсулировать пакеты на основе VLAN.

Selective QinQ

Selective QinQ подразделяется на два типа: Selective QinQ на основе C-TAG и Selective QinQ на основе ACL.

В Selective QinQ на основе C-TAG внешние теги инкапсулируются в пакеты на основе внутренних тегов для разделения потоков трафика сервисов и реализации прозрачной передачи.

В Selective QinQ на основе ACL внешние теги инкапсулируются в пакеты на основе ACL для разделения потоков трафика сервисов.

TPID

Тег кадра Ethernet состоит из четырех полей: TPID, приоритет пользователя, индикатор канонического формата (CFI) и идентификатор VLAN.

По умолчанию TPID равен 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых производителей для TPID установлено значение 0x9100 или другие значения. Конфигурация TPID направлена на то, чтобы TPID пересылаемых пакетов были совместимы с TPID, поддерживаемыми сторонними коммутаторами.

Отображение приоритетов и репликация приоритета

Значение по умолчанию User Priority в тегах кадров Ethernet равно 0, что указывает на регулярные потоки. Вы можете установить это поле, чтобы обеспечить приоритетную передачу определенных пакетов. Вы можете указать приоритет пользователя, задав значение CoS в политике QoS.

Репликация приоритета: если сеть SP предоставляет политику QoS, соответствующую указанной CoS во внутреннем теге, вы можете реплицировать CoS внутреннего тега во внешний тег, чтобы включить прозрачную передачу на основе политики QoS, предоставляемой сетью SP.

Сопоставление приоритетов: если сеть SP предоставляет различные политики QoS, соответствующие указанным значениям CoS для различных потоков трафика сервисов, вы можете сопоставить значение CoS внутреннего тега со значением CoS внешнего тега, чтобы обеспечить предпочтительную передачу потоков трафика сервисов на основе политик QoS, предоставляемых сетью SP.

Прозрачная передача уровня 2

Пакеты STP и GVRP могут влиять на топологию сети SP. Если вы хотите унифицировать топологию двух клиентских сетей, разделенных сетью SP, не влияя на топологию сети SP, прозрачно передавайте пакеты STP и GVRP из сетей клиентов по сети SP.

13.3.2. Обзор

Особенность	Описание
Базовый QinQ	Настраивает туннельный порт и указывает, помечаются ли пакеты тегами, отправляемые с порта
Selective QinQ	Инкапсулирует различные внешние теги в потоки данных на основе списков ACL
Сопоставление VLAN	Заменяет внутренние теги пакетов внешними тегами, а затем восстанавливает внешние теги во внутренние теги на основе тех же правил
Конфигурация TPID	По умолчанию TPID равен 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых производителей TPID внешних тегов имеют значение 0x9100 или другие значения. Конфигурация TPID направлена на то, чтобы TPID пересылаемых пакетов были совместимы с TPID, поддерживаемыми сторонними коммутаторами
Репликация MAC-адресов	В Selective QinQ на основе ACL идентификаторы VLAN для MAC-адресов, которые изучают коммутаторы, принадлежат Native VLAN. Если преобразование VLAN реализовано на основе ACL, после получения пакетов от peer end'a локальный конец может не запросить MAC-адреса, что приведет к флуду. Чтобы решить эту проблему, предоставляется репликация MAC-адресов для репликации MAC-адресов Native VLAN в VLAN, где находится внешний тег
Прозрачная передача уровня 2	Передает пакеты 2-го уровня между сетями клиентов без влияния на сети SP
Репликация	Если сеть SP предоставляет политику QoS, соответствующую указанному значению CoS во внутреннем теге, вы можете реплицировать CoS внутреннего тега во внешний тег, чтобы включить прозрачную передачу на основе политики QoS, предоставленной сетью SP
Сопоставление	Если сеть SP предоставляет различные политики QoS, соответствующие заданным значениям CoS для различных потоков трафика сервисов, можно сопоставить значение CoS внутреннего тега со значением CoS внешнего тега, чтобы обеспечить предпочтительную передачу потоков трафика сервисов на основе политик QoS, предоставляемых сеть SP

13.3.3. Базовый QinQ

Базовый QinQ можно использовать для реализации простой VPN уровня 2, но ему не хватает гибкости при инкапсуляции внешних тегов.

13.3.3.1. Принцип работы

После того, как туннельный порт получает пакет, коммутатор добавляет к пакету внешний тег, содержащий идентификатор VLAN по умолчанию. Если полученный пакет уже содержит тег VLAN, он инкапсулируется как пакет с двойным тегом. Если у него нет тега VLAN, он добавляется с тегом VLAN, содержащим идентификатор VLAN по умолчанию.

13.3.4. Selective QinQ

Selective QinQ гибко добавляет различные внешние теги к потокам данных.

13.3.4.1. Принцип работы

Selective QinQ можно использовать для инкапсуляции различных внешних тегов на основе внутренних тегов, MAC-адресов, номеров протоколов, исходных адресов, целевых адресов, приоритетов или номеров портов приложений. Таким образом, пакеты разных пользователей, сервисов и приоритетов инкапсулируются с помощью разных внешних тегов VLAN.

Вы можете настроить следующие политики Selective QinQ:

- Добавить внешний тег VLAN на основе внутреннего тега VLAN.
- Изменить тег внешней VLAN на основе тега внешней VLAN.
- Изменить тег внешней VLAN на основе тега внутренней VLAN.
- Изменить тег внешней VLAN на основе тегов внутренней и внешней VLAN.
- Добавить внешний тег VLAN на основе ACL.
- Изменить тег внешней VLAN на основе ACL.
- Изменить внутренний тег VLAN на основе ACL.

13.3.5. Сопоставление VLAN

13.3.5.1. Принцип работы

Внутренний тег пакета заменяется внешним тегом, что позволяет передавать пакет на основе топологии общедоступной сети. Когда пакет передается в клиентскую сеть, внешний тег восстанавливается до исходного внутреннего тега на основе того же правила. Сопоставление VLAN поддерживает следующее правило сопоставления:

- Сопоставление VLAN 1:1: изменяет идентификатор VLAN на указанный идентификатор VLAN.
- Сопоставления VLAN 1:1 Режим 1

Сопоставление VLAN 1:1 в основном применяется на коммутаторах на этажах для использования разных VLAN для передачи одних и тех же сервисов от разных пользователей, как показано на Рисунке ниже.

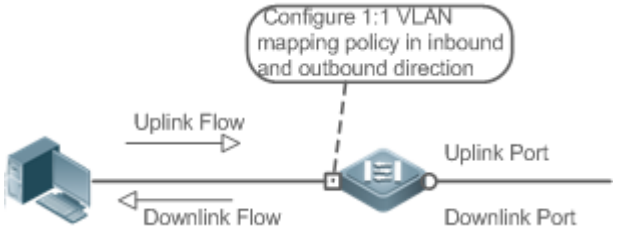


Рисунок 13-7.

- Настройте downlink-порт с политикой сопоставления VLAN во входящем направлении, чтобы сопоставить внутренний тег uplink-потока с внешним тегом.

- Настройте порт uplink с политикой сопоставления VLAN в исходящем направлении, чтобы сопоставить внешний тег downlink-потока с исходным внутренним тегом.
- Сопоставления VLAN 1:1 Режим 2

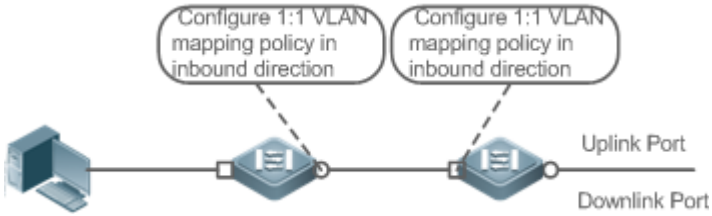


Рисунок 13-8.

- Настройте downlink-порт с политикой сопоставления VLAN во входящем направлении, чтобы сопоставить внутренний тег uplink-потока с внешним тегом.
- Для downstream-потоков данных настройте порт uplink с политикой сопоставления VLAN во входящем направлении к внешнему тегу downlink-потока с исходным внутренним тегом.

13.3.6. Конфигурация TPID

13.3.6.1. Принцип работы

Тег кадра Ethernet состоит из четырех полей, а именно: TPID, User Priority, CFI и VLAN ID. По умолчанию TPID равен 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых производителей TPID внешних тегов имеют значение 0x9100 или другие значения. Функция конфигурации TPID позволяет настроить TPID на портах, которые заменят TPID внешних тегов VLAN в пакетах настроенными TPID для реализации совместимости TPID.

13.3.7. Репликация MAC-адресов

13.3.7.1. Принцип работы

В Selective QinQ на основе ACL MAC-адрес, полученный коммутатором, принадлежит Native VLAN. Туннельный порт помечает пакет указанным внешним идентификатором VLAN на основе политики Selective QinQ. При получении ответного пакета, содержащего тот же тег внешней VLAN, туннельному порту не удается найти MAC-адрес во внешней VLAN, поскольку он находится в Native VLAN, что вызывает флуд.

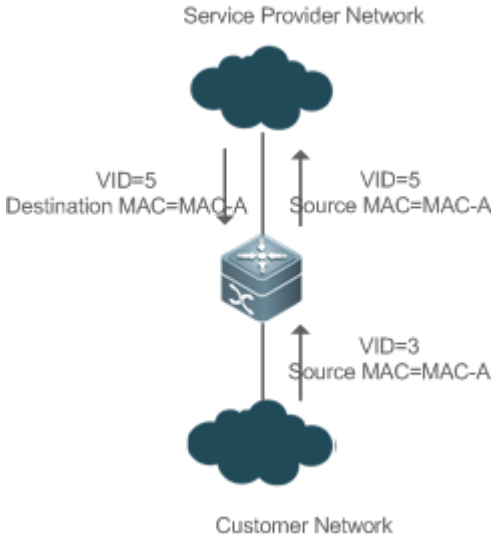


Рисунок 13-9.

На Рисунке выше клиентская сеть подключена к туннельному порту коммутатора. Настроенный с Native VLAN 4, туннельный порт помечает пакет с исходным MAC-адресом как A внешней VLAN 5. При получении пакета с внутренним тегом VLAN 3 и исходным MAC-адресом A коммутатор помечает пакет внешней VLAN 5. Поскольку порт настроен с Native VLAN 4, MAC-адрес A известен VLAN 4. После получения ответного пакета коммутатор ищет MAC-адрес A в VLAN 5, поскольку внешний тег пакета содержит VLAN ID 5. Однако MAC-адрес A не изучен VLAN 5, вызывая флуд.

Вы можете настроить туннельный порт для репликации MAC-адреса Native VLAN во внешнюю VLAN, чтобы избежать непрерывного потока пакетов из сети SP. Вы также можете настроить туннельный порт для репликации MAC-адреса внешней VLAN для внешнего тега в Native VLAN, чтобы избежать непрерывного флудинга пакетов из клиентской сети.

13.3.8. Прозрачная передача уровня 2

13.3.8.1. Принцип работы

Функция прозрачной передачи уровня 2 предназначена для реализации передачи пакетов уровня 2 между клиентскими сетями без влияния на сети SP. Когда пакет уровня 2 из клиентской сети поступает в PE, PE изменяет MAC-адрес назначения пакета на приватный адрес перед пересылкой пакета. Peer PE изменяет MAC-адрес назначения на общедоступный адрес, чтобы отправить пакет в клиентскую сеть на другом конце, реализуя прозрачную передачу в сети SP.

13.3.9. Репликация приоритета

13.3.9.1. Принцип работы

Если сеть SP предоставляет политику QoS, соответствующую указанному приоритету пользователя (CoS) во внутреннем теге, вы можете реплицировать CoS внутреннего тега во внешний тег, чтобы обеспечить прозрачную передачу на основе политики QoS, предоставленной сетью SP.

13.3.10. Сопоставление приоритета

13.3.10.1. Принцип работы

Если сеть SP предоставляет различные политики QoS, соответствующие заданным значениям CoS для различных потоков трафика сервисов, можно сопоставить значение CoS внутреннего тега со значением CoS внешнего тега, чтобы обеспечить предпочтительную передачу потоков трафика сервисов на основе политик QoS, предоставляемых сетью SP.

13.4. Ограничение

Продукты серии QSW-6900 поддерживают четыре глобальных значения идентификатора протокола тегов (TPID). Одно из значений TPID должно быть 0x8100, а остальные три являются случайными.

13.5. Конфигурация

Конфигурация	Описание и команда	
Настройка QinQ	Обязательный	
	switchport mode dot1q-tunnel	Настраивает Туннельный порт
	switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }	Добавляет VLAN к туннельному порту в тегированном или нетегированном режиме
	switchport dot1q-tunnel native vlan *VID*	Настраивает VLAN по умолчанию для туннельного порта
Настройка Selective QinQ на основе C-TAG	(Обязательно) Используется для настройки Selective QinQ на основе C-TAG на основе базового QinQ. Selective QinQ преобладает над базовым QinQ	
	dot1q outer-vid *VID* **register inner-vid** *v_list*	Настраивает политику для добавления идентификаторов VLAN внешних тегов на основе внутренних тегов
Настройка Selective QinQ на основе ACL	(Обязательно) Используется для настройки Selective QinQ на основе ACL на основе базового QinQ. Selective QinQ преобладает над базовым QinQ	
	traffic-redirect access-group *acl* **nested-vlan** *VID* **in**	Настраивает политику для добавления идентификаторов VLAN внешних тегов на основе списков ACL

Конфигурация	Описание и команда	
Настройка сопоставления VLAN	(Обязательно) Используется для включения сопоставления VLAN	
	vlan-mapping-in vlan *cvlan* **remark** *svlan*	Настраивает сопоставление VLAN 1:1 во входящем направлении. Эта функция изменяет внутренний идентификатор VLAN для пакета, входящего в порт, на указанный внешний идентификатор VLAN
	vlan-mapping-out vlan *svlan* **remark** *cvlan*	Настраивает сопоставление VLAN 1:1 в исходящем направлении. Эта функция изменяет внешний идентификатор VLAN для пакета, входящего в порт, на указанный внутренний идентификатор VLAN
	vlan-mapping-in vlan *cvlan-list* **remark** *svlan*	Настраивает сопоставление VLAN N:1 во входящем направлении. Эта функция изменяет внутренний идентификатор VLAN для пакета, входящего в порт, на указанный внешний идентификатор VLAN
Настройка TPID	(Опционально) Используется для реализации совместимости с TPID	
	frame-tag tpid *tpid*	Настраивает TPID тега кадра. Если вы хотите установить его на 0x9100, настройте команду **frame-tag tpid 9100**. По умолчанию TPID имеет шестнадцатеричный формат. Вам необходимо настроить эту функцию на выходном порту
Настройка репликации MAC-адресов	(Необязательно) Используется для настройки репликации MAC-адресов для предотвращения флуда	
	mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*	Реплицирует динамический MAC-адрес исходной VLAN в целевую VLAN

Конфигурация	Описание и команда	
Настройка внутренней/внешней политики модификации тегов VLAN	(Опционально) Он используется для настройки внешних и внутренних тегов VLAN пакетов, передаваемых по сетям SP, в зависимости от топологии сети	
	dot1q relay-vid *VID* **translate local-vid** *v_list*	Настраивает политику для изменения идентификаторов VLAN внешних тегов на основе внешних тегов
	dot1q relay-vid *VID* **translate inner-vid** *v_list*	Настраивает политику для изменения идентификаторов VLAN внешних тегов на основе внутренних тегов
	dot1q new-outer-vlan *VID* **translate old-outer-vlan vid inner-vlan** *v_list*	Настраивает политику для изменения идентификаторов VLAN внешних тегов на основе внешних и внутренних тегов
	traffic-redirect access-group *acl* **outer-vlan** *VID* **in**	Настраивает политику для изменения идентификаторов VLAN внешних тегов на основе ACL
	traffic-redirect access-group *acl* **inner-vlan** *VID* **out**	Настраивает политику для изменения идентификаторов VLAN внутренних тегов на основе ACL
Настройка сопоставления приоритетов и репликации приоритетов	(Опционально) Используется для применения политики QoS, обеспечиваемой сетью SP, посредством репликации с приоритетом	
	inner-priority-trust enable	Реплицирут значение поля User Priority во внутреннем теге (C-TAG) в поле User Priority внешнего тега (S-TAG)
	(Опционально) Используется для применения политики QoS, обеспечиваемой сетью SP, путем сопоставления приоритетов	
	dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*	Задает значение поля User Priority во внешнем теге (S-TAG) на основе поля User Priority во внутреннем теге (C-TAG)

Конфигурация	Описание и команда	
Настройка прозрачной передачи уровня 2	(Опционально) Используется для прозрачной передачи пакетов MSTP и GVRP на основе топологии сети клиента, не влияя на топологию сети SP	
	l2protocol-tunnel stp	Включает прозрачную передачу STP в режиме глобальной конфигурации
	l2protocol-tunnel stp enable	Включает прозрачную передачу STP в режиме конфигурации интерфейса
	l2protocol-tunnel gvrp	Включает прозрачную передачу GVRP в режиме глобальной конфигурации
	l2protocol-tunnel gvrp enable	Включает прозрачную передачу GVRP в режиме конфигурации интерфейса
	l2protocol-tunnel { **STP** | **GVRP** } **tunneld-mac** *mac-address*	Настраивает прозрачный адрес передачи

ПРИМЕЧАНИЯ: обратите внимание на следующие ограничения при настройке QinQ:

- Не настраивайте маршрутизируемый порт в качестве туннельного порта.
- Не включайте 802.1X на туннельном порту.
- Когда туннельный порт настроен как исходный порт анализатора удаленных коммутируемых портов (RSPAN), отслеживаются пакеты, внешние теги которых содержат идентификаторы VLAN, соответствующие идентификаторам RSPAN VLAN.
- Если вы хотите сопоставить ACL, примененный к туннельному порту, с идентификаторами VLAN внутренних тегов, используйте ключевое слово **inner**.
- Настройте выходной порт клиентской сети, подключенной к сети SP, как порт uplink. Если вы настраиваете TPID внешнего тега на порту с поддержкой QinQ, установите такое же значение для TPID внешнего тега на порту Uplink.
- По умолчанию максимальная единица передачи (MTU) для порта составляет 1500 байт. После добавления внешнего тега VLAN пакет становится на четыре байта длиннее. Рекомендуется увеличить MTU порта в сетях SP как минимум до 1504 байтов.
- После включения порта коммутатора с помощью QinQ необходимо включить совместное использование SVGL перед включением IGMP snooping. В противном случае IGMP snooping не будет работать на порту с поддержкой QinQ.
- Если пакет соответствует двум или более политикам Selective QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

13.5.1. Настройка QinQ

13.5.1.1. Эффект конфигурации

Внедрите VPN уровня 2 на основе политики QinQ на основе портов.

13.5.1.2. Примечания

Не рекомендуется настраивать Native VLAN магистрального порта на PE в качестве VLAN по умолчанию, поскольку магистральный порт удаляет теги, содержащие идентификаторы Native VLAN, при отправке пакетов.

13.5.1.3. Шаги настройки

Настройка туннельного порта

- (Обязательно) Настройте туннельный порт в режиме конфигурации интерфейса.
- Запустите команду **switchport mode dot1q-tunnel** в режиме конфигурации интерфейса, чтобы настроить туннельный порт.

Команда	**switchport mode dot1q-tunnel**
По умолчанию	По умолчанию туннельный порт не настроен
Командный режим	Режим конфигурации интерфейса

Настройка Native VLAN

- Обязательный.
- Настройте Native VLAN для туннельного порта.
- После настройки Native VLAN добавьте ее в список VLAN туннельного порта в нетегированном режиме.
- Запустите команду **switchport dot1q-tunnel native vlan** *VID* в режиме конфигурации интерфейса, чтобы настроить VLAN по умолчанию для туннельного порта.
- Если Native VLAN добавляется в список VLAN в нетегированном режиме, исходящие пакеты через туннельный порт не помечаются тегами. Если Native VLAN добавляется в список VLAN в тегированном режиме, исходящие пакеты через туннельный порт помечаются идентификатором Native VLAN. Чтобы обеспечить передачу по uplink- и downlink-каналам, добавьте Native VLAN в список VLAN в нетегированном режиме.

Команда	**switchport dot1q-tunnel native vlan** *VID*
Описание параметров	*VID*: указывает идентификатор Native VLAN. Значение варьируется от 1 до 4,094. Значение по умолчанию — 1
По умолчанию	По умолчанию Native VLAN — это VLAN 1
Командный режим	Режим конфигурации интерфейса

Руководство по использованию	Используйте эту команду для настройки VLAN сети SP

Добавление VLAN на туннельный порт

- Обязательный.
- После настройки Native VLAN добавьте ее в список VLAN туннельного порта в нетегированном режиме.
- Если QinQ на основе портов включен, вам не нужно добавлять VLAN сети клиента в список VLAN туннельного порта.
- Если включен Selective QinQ, добавьте VLAN клиентской сети в список VLAN туннельного порта в тегированном или нетегированном режиме в зависимости от требований.
- Запустите команду **switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* } в режиме конфигурации интерфейса для добавления VLAN в список VLAN туннельного порта. При получении пакетов из соответствующих сетей VLAN туннельный порт добавляет или удаляет теги в зависимости от настроек.

Команда	**switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist*	[**add**] **untagged** *vlist*	**remove** *vlist* }
Описание параметров	*vlist*: указывает список VLAN на туннельном порту
По умолчанию	По умолчанию VLAN 1 добавляется в список VLAN туннельного порта в нетегированном режиме. Другие VLAN не добавляются
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду, чтобы добавить или удалить VLAN на Туннельный порт и укажите, будут ли исходящие пакеты тегированы или нет. Если базовый QinQ включен, добавьте Native VLAN в список VLAN туннельного порта в нетегированном режиме

13.5.1.4. Проверка

Проверьте конфигурацию туннельного порта.

Проверьте, правильно ли настроен туннельный порт на коммутаторе.

13.5.1.5. Пример конфигурации

Настройка базового QinQ для реализации VPN уровня 2

Сценарий:

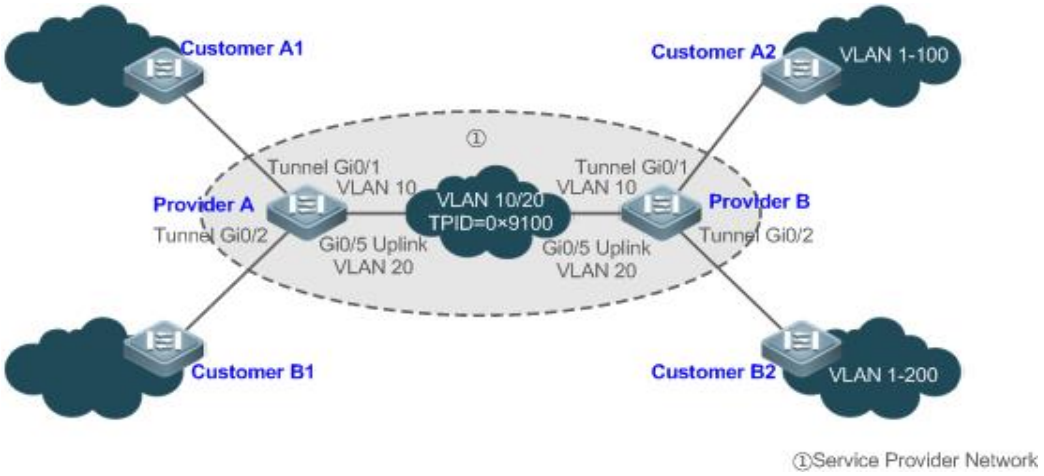


Рисунок 13-10.

Шаги настройки	• Настройте туннельные порты на PE и подключите CE к туннельным портам. • Настройте сети Native VLAN для туннельных портов и добавьте Native VLAN в списки VLAN туннельных портов соответственно в нетегированном режиме. • Настройте VLAN в сетях клиентов в соответствии с требованиями. **ПРИМЕЧАНИЕ:** коммутаторы с поддержкой QinQ инкапсулируют внешние теги в пакеты для передачи по сети SP. Поэтому вам не нужно настраивать клиентские VLAN на PE. **ПРИМЕЧАНИЕ:** TPID по умолчанию равен 0x8100 в соответствии с IEEE802.1Q. На некоторых сторонних коммутаторах для TPID установлено другое значение. Если такие коммутаторы развернуты, установите TPID на портах, подключенных к сторонним коммутаторам, чтобы реализовать совместимость TPID. **ПРИМЕЧАНИЕ:** если PE подключены через магистральные порты или гибридные порты, не настраивайте сети Native VLAN для магистральных или гибридных портов в качестве сетей VLAN по умолчанию для туннельных портов. Магистральные порты или гибридные порты удаляют теги VLAN, содержащие идентификаторы Native VLAN, при отправке пакетов

Провайдер A	Шаг 1. Создайте VLAN 10 и VLAN 20 в сети SP, чтобы разделить данные клиента A и клиента B.
	`ProviderA#configure terminal`
	Введите команды конфигурации, по одной в строке. Конец с CNTL/Z.
	`ProviderA(config)#vlan 10`
	`ProviderA(config-vlan)#exit`

	ProviderA(config)#vlan 20 ProviderA(config-vlan)#exit Шаг 2. Включите базовый QinQ на порту, подключенном к сети клиента A, чтобы использовать VLAN 10 для туннелирования. ProviderA(config)#interface gigabitEthernet 0/1 ProviderA(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 10 ProviderA(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed vlan add untagged 10 Шаг 3. Включите базовый QinQ на порту, подключенном к сети клиента B, чтобы использовать VLAN 20 для туннелирования. ProviderA(config)#interface gigabitEthernet 0/2 ProviderA(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan 20 ProviderA(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed vlan add untagged 20 Шаг 4. Настройте Uplink-порт. ProviderA(config)# interface gigabitEthernet 0/5 ProviderA(config-if-GigabitEthernet 0/5)#switchport mode uplink Шаг 5. Измените TPID исходящих пакетов на порту Uplink на значение (например, 0x9100), распознаваемое сторонними коммутаторами. ProviderA(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100 Шаг 6. Настройте провайдер B, выполнив те же действия
Проверка	Клиент A1 отправляет пакет, содержащий идентификатор VLAN 100, предназначенный для клиента A2. Пакет через Провайдера A помечен внешним тегом, указанным туннельным портом. Пакет, который достигает Клиента A2, содержит исходный идентификатор VLAN 100. Проверьте, правильно ли настроен туннельный порт. Проверьте, правильно ли настроен TPID
Провайдер A	ProviderA#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 10 switchport dot1q-tunnel native vlan 10 spanning-tree bpdufilter enable !

	interface GigabitEthernet 0/2 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 20 switchport dot1q-tunnel native vlan 20 spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink frame-tag tpid 0x9100 ProviderA#show interfaces dot1q-tunnel ========Interface Gi0/1======== Native vlan: 10 Allowed vlan list:1,10, Tagged vlan list: ========Interface Gi0/2======== Native vlan: 20 Allowed vlan list:1,20, Tagged vlan list: ProviderA#show frame-tag tpid Ports Tpid ------- ------------- Gi0/5 0x9100
Провайдер B	Проверьте Провайдер B, выполнив те же действия

13.5.1.6. Распространенные ошибки

- Native VLAN не добавляется в список VLAN туннельного порта в нетегированном режиме.
- Для порта, подключенного к стороннему коммутатору, TPID которого не равен 0x8100, не настроен TPID. В результате пакеты не могут быть распознаны сторонним коммутатором.

13.5.2. Настройка Selective QinQ на основе C-TAG

13.5.2.1. Эффект конфигурации

Инкапсулируйте внешние теги VLAN (S-TAG) в пакеты на основе внутренних тегов, чтобы обеспечить приоритетную передачу, управление VPN уровня 2 и потоки трафика сервисов.

13.5.2.2. Примечания

- Selective QinQ на основе C-TAG должен быть настроен на основе базового QinQ.

- Некоторые политики Selective QinQ не поддерживаются некоторыми продуктами из-за ограничений чипов.
- Если вам нужно продолжать использовать приоритет тега VLAN, указанный в сети клиента, вы можете настроить репликацию приоритета, чтобы настроить внешний тег так же, как и внутренний тег.
- Если в сети SP требуется передача пакетов на основе приоритета внешнего тега, необходимо настроить репликацию приоритета, чтобы установить для CoS внешнего тега указанное значение.

13.5.2.3. Шаги настройки

- Настройка политики для добавления идентификаторов VLAN внешних тегов на основе внутренних тегов
- Обязательный.
- При получении пакета туннельный порт добавляет идентификатор VLAN внешнего тега на основе идентификатора VLAN внутреннего тега. Эта функция позволяет туннельному порту добавить идентификатор VLAN внутреннего тега к внешнему тегу и добавить порт в сеть VLAN в нетегированном режиме. Таким образом, исходящие пакеты содержат исходные внутренние теги.

ПРИМЕЧАНИЕ: политика QinQ, основанная на ACL-списке, преобладает над политикой QinQ на основе порта и C-TAG.

ПРИМЕЧАНИЕ: когда порт-участник добавляется или удаляется из агрегированного порта (AP), политика QinQ, настроенная на порте AP, будет удалена. Вам нужно настроить политику заново. Рекомендуется настроить политику Selective QinQ для порта AP после настройки его портов-участников.

ПРИМЕЧАНИЕ: вы должны настроить туннельный порт и порт, подключенный к общедоступной сети, чтобы разрешить прохождение пакетов с указанными идентификаторами VLAN (включая собственный идентификатор VLAN) во внешнем теге.

Команда	**dot1q outer-vid** *VID* **register inner-vid** *v_list*
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

13.5.2.4. Проверка

- Проверьте, могут ли пользователи внутри VLAN общаться друг с другом.
- Проверьте, реализована ли VPN уровня 2.
- Проверьте, передается ли другой сервисный трафик на основе политики Selective QinQ, такой как вставка внешнего тега, репликация приоритета и сопоставление приоритета.

13.5.2.5. Пример конфигурации

Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью Selective QinQ на основе C-TAG

Сценарий:

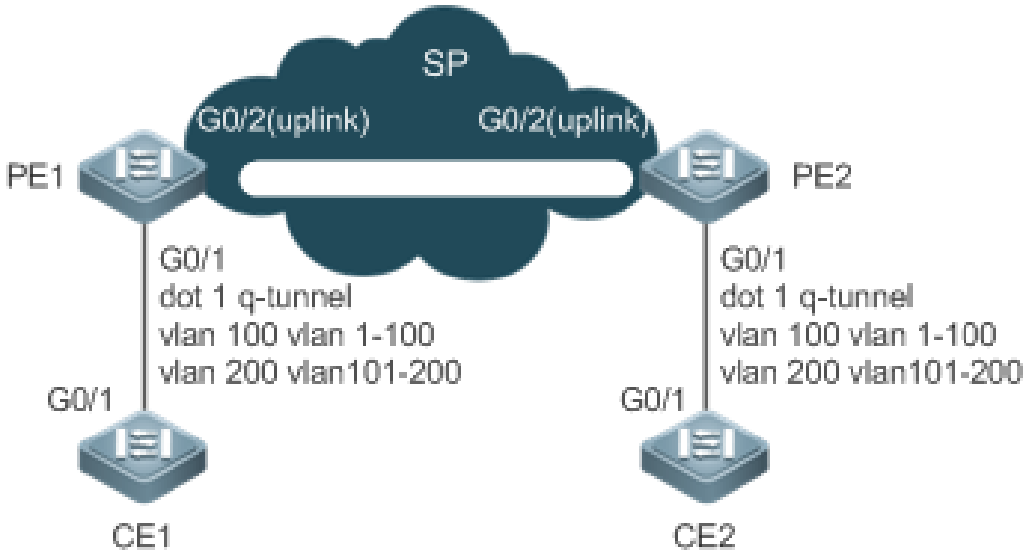


Рисунок 13-11.

Шаги настройки	Настройте порты на PE 1 и PE 2, подключенные к CE 1 и CE 2, как туннельные порты. Настройте политику Selective QinQ для добавления внешнего тега к пакету на основе его внутреннего тега. Если сеть SP предоставляет политику QoS на основе VLAN, политика позволяет порту добавлять внешние теги с соответствующим идентификатором VLAN к указанным пакетам потока трафика сервисов. Если сеть SP предоставляет политику QoS на основе CoS, а значение CoS такое же, как и у внутреннего тега, можно настроить сопоставление приоритетов для репликации значения CoS внутреннего тега во внешний тег VLAN, чтобы пакет передавался на основе политики приоритета для внутреннего тега. Если в сети SP предусмотрена политика QoS на основе CoS, можно настроить сопоставление приоритетов, чтобы установить для значения CoS тега внешней VLAN заданное значение, чтобы пакет передавался на основе политики приоритета
PE1	Шаг 1. Настройте VLAN для прозрачной передачи. **PE1#configure terminal** Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. **PE1(config)#vlan 100** **PE1(config-vlan)#exit** **PE1(config)#vlan 200** **PE1(config-vlan)#exit** Шаг 2. На Downlink-порту коммутатора доступа настройте политику Selective QinQ для добавления внешних тегов на основе внутренних тегов.

	Настройте порт Gi 0/1 как туннельный порт. **PE1(config)#interface gigabitEthernet 0/1** **PE1(config-if)# switchport mode dot1q-tunnel** Добавьте VLAN 101 и VLAN 201 SP в список VLAN туннельного порта и настройте туннельный порт для удаления внешнего тега из входящих пакетов. **PE1(config-if)# switchport dot1q-tunnel allowed vlan add untagged 100,200** Настройте туннельный порт для добавления VLAN 100 с внешним тегом во входящие кадры данных, содержащие VLAN с внутренним тегом 1–100. **PE1(config-if)# switchport dot1q-tunnel allowed vlan add untagged 100,200** Настройте туннельный порт, чтобы добавить внешний тег VLAN 200 к входящим кадрам данных, содержащим внутренний тег VLAN 101–200. **PE1(config-if)# dot1q outer-vid 200 register inner-vid 101-200** Шаг 3. Настройте порт, который обращается к сети SP, как порт Uplink. **PE1(config)# interface gigabitEthernet 0/2** **PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink**
PE2	Выполните ту же настройку на PE 2
Проверка	Проверьте конфигурацию, проверив: • Downlink-порт настроен как туннельный порт. • VLAN, указанная внешним тегом, добавляется в список VLAN туннельного порта. • Политика Selective QinQ на туннельном порту верна. • Порт Uplink настроен правильно
PE1	Шаг 1. Проверьте правильность политики сопоставления VLAN. **PE1#show running-config interface gigabitEthernet 0/1** **interface GigabitEthernet 0/1** **switchport mode dot1q-tunnel** **switchport dot1q-tunnel allowed vlan add untagged 100,200** **dot1q outer-vid 100 register inner-vid 1-200** **dot1q outer-vid 200 register inner-vid 101-200** **spanning-tree bpdufilter enable** **!** Шаг 2. Проверьте политику Selective QinQ на основе C-TAG. Проверьте правильность отношения сопоставления между внутренними и внешними тегами VLAN. **PE1#show registration-table**

```
Ports    Type         Outer-VID      Inner-VID-list
------ ---------- ---------- --------------
Gi0/1    Add-outer    100            1-200
Gi0/1    Add-outer    200            101-200
```

13.5.3. Настройка Selective QinQ на основе ACL

13.5.3.1. Эффект конфигурации

Инкапсулируйте внешние теги VLAN (S-TAG) в пакеты на основе классификации потоков на основе ACL, чтобы позволить сети SP управлять различными сервисами.

13.5.3.2. Примечания

- Selective QinQ на основе ACL должен быть настроен на основе базового QinQ.
- Некоторые политики Selective QinQ не поддерживаются некоторыми продуктами из-за ограничений чипов.
- Если вам нужно продолжать использовать приоритет тега VLAN, указанный в сети клиента, вы можете настроить репликацию приоритета, чтобы настроить внешний тег так же, как и внутренний тег.
- Если в сети SP требуется передача пакетов на основе приоритета внешнего тега, необходимо настроить репликацию приоритета, чтобы установить для CoS внешнего тега указанное значение.

ПРИМЕЧАНИЕ: политика QinQ на основе ACL превалирует над политикой QinQ на основе портов и C-TAG.

ПРИМЕЧАНИЕ: при удалении ACL соответствующая политика будет автоматически удалена.

ПРИМЕЧАНИЕ: при получении пакета с двумя или более тегами туннельный порт не может добавить внешний тег к пакету на основе политики Selective QinQ на основе ACL-списков.

ПРИМЕЧАНИЕ: если пакет соответствует двум или более политикам Selective QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

ПРИМЕЧАНИЕ: вы должны настроить туннельный порт и порт, подключенный к общедоступной сети, чтобы разрешить прохождение пакетов с указанными идентификаторами VLAN (включая собственный идентификатор VLAN) во внешнем теге.

13.5.3.3. Шаги настройки

Настройка политики для добавления идентификаторов VLAN внешних тегов на основе списков ACL

- Обязательный.
- Туннельный порт добавляет внешние теги с разными идентификаторами VLAN к входящим пакетам на основе содержимого пакета.

Команда	**traffic-redirect access-group** *acl* **nested-vlan** *VID* **in**
По умолчанию	По умолчанию политика не добавляется

Командный режим	Режим конфигурации интерфейса

13.5.3.4. Проверка

- Проверьте, могут ли пользователи одного и того же сервиса в разных филиалах общаться друг с другом и передаются ли указанные данные сервиса предпочтительно через конфигурацию сегмента виртуальной приватной локальной сети (VPLS).
- Проверьте, реализована ли VPN уровня 2.
- Проверьте, передается ли другой сервисный трафик на основе политики Selective QinQ, такой как вставка внешнего тега, репликация приоритета и сопоставление приоритета.

13.5.3.5. Пример конфигурации

Внедрение VPN уровня 2 и управления потоком трафика сервисов с помощью Selective QinQ на основе ACL

Сценарий:

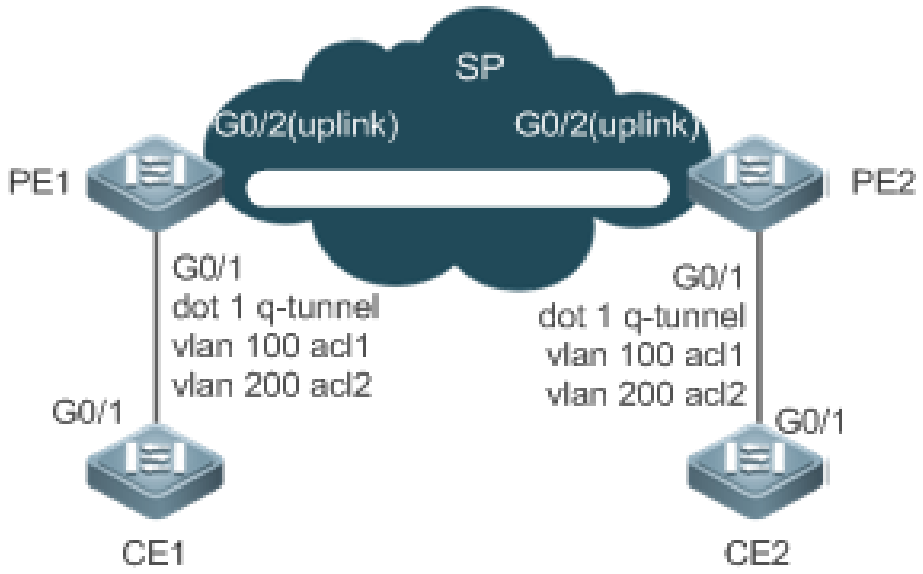


Рисунок 13-12.

Шаги настройки	• Настройте порты на PE 1 и PE 2, подключенные к CE 1 и CE 2, как туннельные порты. • Настройте политики ACL на PE 1 и PE 2, чтобы отделить потоки трафика сервисов от клиентской сети. • На туннельных портах настройте политику Selective QinQ, чтобы добавить внешний тег к пакету на основе политик ACL. • Если сеть SP предоставляет политику QoS на основе VLAN, политика позволяет порту добавлять соответствующий идентификатор VLAN к внешним тегам указанного потока трафика сервисов.

	• Если в сети SP предусмотрена политика QoS на основе CoS, можно настроить сопоставление приоритетов, чтобы установить для значения CoS тега внешней VLAN заданное значение, чтобы пакет передавался на основе политики приоритета
PE 1	Шаг 1. Создайте ACL, чтобы разрешить прохождение потоков типа PPPoE (0x8863/0x8864) и типа IPoE (0x0800). **PE1#configure terminal** Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. **PE1(config)# expert access-list extended acl1** **PE1(config-exp-nacl)# permit 0x8863 any any** **PE1(config-exp-nacl)# permit 0x8864 any any** **PE1(config-exp-nacl)#exit** **PE1(config)# expert access-list extended acl2** **PE1(config-exp-nacl)#permit 0x0800 any any** Шаг 2. Настройте VLAN 100 и VLAN 200 в сети SP для разделения данных. **PE#configure terminal** Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. **PE1(config)#vlan 100** **PE1(config-vlan)#exit** **PE1(config)#vlan 200** **PE1(config-vlan)#exit** Шаг 3. На Downlink-порту коммутатора доступа настройте политику Selective QinQ для добавления внешних тегов VLAN на основе списков ACL. Настройте порт Gi 0/1 как туннельный порт. **PE1(config)#interface gigabitEthernet 0/1** **PE1(config-if)# switchport mode dot1q-tunnel** Добавьте VLAN 100 и VLAN 200 SP в список VLAN туннельного порта и настройте туннельный порт для удаления внешнего тега из входящих пакетов. **PE1(config-if)#switchport dot1q-tunnel allowed vlan add untagged 100,200** Настройте туннельный порт для добавления внешнего тега VLAN 100 к входящим кадрам данных, которые соответствуют ACL 1. **PE1(config-if)# traffic-redirect access-group acl1 nested-vlan 100 in** Настройте туннельный порт, чтобы добавить внешний тег VLAN 200 к входящим кадрам данных, которые соответствуют ACL 2. **PE1(config-if)# traffic-redirect access-group acl1 nested-vlan 200 in** Шаг 4. Настройте порт, подключенный к сети SP, как порт Uplink. **PE1(config)# interface gigabitEthernet 0/2**

	PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink
Проверка	• Проверьте, могут ли пользователи одного и того же сервиса в разных филиалах общаться друг с другом и передаются ли указанные данные сервиса предпочтительно. • Проверьте, реализована ли VPN уровня 2. • Проверьте правильность ACL. • Проверьте правильность приоритета сервиса. • Проверьте, настроен ли Downlink-порт как туннельный порт, добавлена ли VLAN с внешним тегом в список VLAN туннельного порта и правильно ли настроена политика сопоставления туннельного порта
PE1	Шаг 1. Проверьте, правильно ли настроен туннельный порт. QTECH#show running-config interface gigabitEthernet 0/1 interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 100,200 traffic-redirect access-group acl1 nested-vlan 100 in traffic-redirect access-group acl2 nested-vlan 200 in spanning-tree bpdufilter enable ! Шаг 2. Проверьте политику Selective QinQ на основе ACL. Проверьте правильность отношения сопоставления между внутренними и внешними тегами VLAN. PE1#show traffic-redirect Ports Type VID Match-filter ------- ---------- ----- ------------ Gi0/1 Nested-vid 101 acl1 Gi0/1 Nested-vid 201 acl2

13.5.3.6. Распространенные ошибки

- Политика ACL не настроена.
- Политики ACL используются для разделения потоков на основе MAC-адресов. Произойдет флудинг пакетов, если репликация MAC-адресов не настроена.

13.5.4. Настройка сопоставления VLAN

13.5.4.1. Эффект конфигурации

Замените внутренние теги пакетов внешними тегами, чтобы разрешить передачу пакетов на основе планирования VLAN в сети SP.

13.5.4.2. Примечания

Сопоставление VLAN можно настроить только для портов Access (доступа), Trunk (магистральных), Hybrid (гибридных) или Uplink.

ПРИМЕЧАНИЕ: после настройки сопоставления VLAN идентификаторы VLAN в пакетах, отправляемых на ЦП, заменяются на указанный идентификатор VLAN.

ПРИМЕЧАНИЕ: не рекомендуется настраивать сопоставление VLAN и Selective QinQ на одном порту.

13.5.4.3. Шаги настройки

- Настройка сопоставления VLAN 1:1.
- Обязательно, если используется режим 1:1. Настройте правило сопоставления VLAN 1:1.
- Запустите команду **vlan-mapping-in vlan** *CVID* **remark** *SVID* или команду **vlan-mapping-out vlan** *SVID* **remark CVID** на магистральном или Uplink-порту, чтобы включить сопоставление VLAN 1:1.

Команда	**vlan-mapping-in vlan** *src-vlan-list* **remark** *dest-vlan*
Описание параметров	*src-vlan-list*: указывает клиента VLAN. *dest-vlan*: указывает сервисную VLAN, то есть VLAN, в которой расположена сеть SP
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду для настройки сопоставления VLAN 1:1 во входящем направлении

Команда	**vlan-mapping-out vlan** *src-vlan* **remark** *dest-vlan*
Описание параметров	*src-vlan*: указывает сервисную VLAN, т. е. VLAN, в которой расположена сеть SP. *dest-vlan*: указывает клиентскую VLAN
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Используйте эту команду для настройки сопоставления VLAN 1:1 в исходящем направлении

13.5.4.4. Проверка

- Проверьте, что сопоставление VLAN настроено правильно.
- Запустите команду **show interfaces**[*intf-id*] **vlan-mapping**, чтобы отобразить сопоставление VLAN.

13.5.4.5. Пример конфигурации

Внедрение агрегации VLAN для различных сервисов посредством сопоставления VLAN

Сценарий:

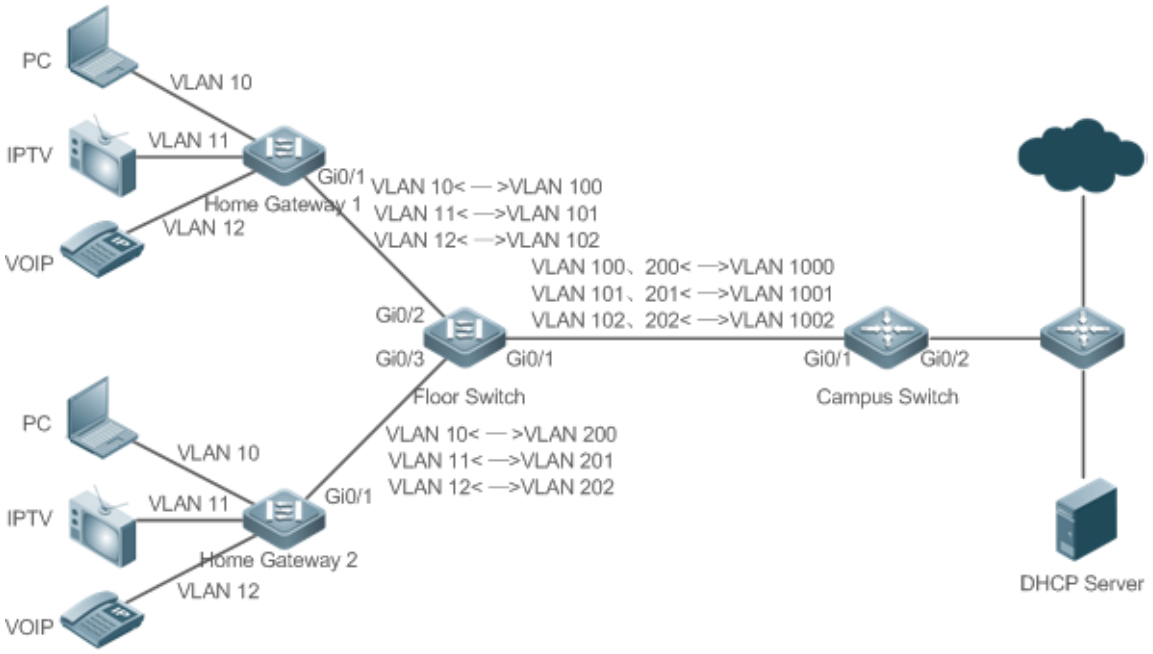


Рисунок 13-13.

Шаги настройки	Настройте домашний шлюз 1 и домашний шлюз 2. Шаг 1. На домашних шлюзах настройте исходные сети VLAN для различных сервисов. QTECH#configure terminal Введите команды конфигурации, по одной в строке. Конец с CNTL/Z. QTECH(config)#vlan range 10-12 QTECH(config-vlan-range)#exit Шаг 2. Настройте атрибуты портов, подключенных к ПК, IPTV и VoIP. Предположим, что подключены порты Gi 0/2, Gi 0/3 и Gi 0/4 соответственно. QTECH(config)#interface gigabitEthernet 0/2 QTECH(config-if-GigabitEthernet 0/2)#switchport access vlan 10 QTECH(config-if-GigabitEthernet 0/2)#exit QTECH(config)#interface gigabitEthernet 0/3 QTECH(config-if-GigabitEthernet 0/3)#switchport access vlan 11 QTECH(config-if-GigabitEthernet 0/3)#exit QTECH(config)#interface gigabitEthernet 0/4 QTECH(config-if-GigabitEthernet 0/4)#switchport access vlan 12 QTECH(config-if-GigabitEthernet 0/4)#exit

Шаг 3. Настройте Uplink-порт.

```
QTECH(config)# interface gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink
```

- Настройте коммутатор на этаже с политиками сопоставления VLAN 1:1.

Шаг 1. На домашних шлюзах настройте исходные сети VLAN и сопоставленные сети VLAN для различных сервисов.

```
QTECH#configure terminal
```

Введите команды конфигурации, по одной в строке. Конец с CNTL/Z.

```
QTECH(config)#vlan range 10-12
QTECH(config-vlan-range)#exit
QTECH(config)#vlan range 100-102
QTECH(config-vlan-range)#exit
QTECH(config)#vlan range 200-202
QTECH(config-vlan-range)#exit
```

Шаг 2. На Downlink-порту домашнего шлюза 1 настройте политики сопоставления VLAN 1:1 для входящего и исходящего направлений.

```
QTECH(config)#interface gigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)#switchport mode uplink
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 10 remark 100
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 11 remark 101
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-in vlan 12 remark 102
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 100 remark 10
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 101 remark 11
QTECH(config-if-GigabitEthernet 0/2)#vlan-mapping-out vlan 102 remark 12
```

Шаг 3. На Downlink-порту домашнего шлюза 2 настройте политики сопоставления VLAN 1:1 для входящего и исходящего направлений.

```
QTECH(config)#interface gigabitEthernet 0/3
QTECH(config-if-GigabitEthernet 0/3)#switchport mode uplink
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 10 remark 200
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 11 remark 201
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-in vlan 12 remark 202
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 200 remark 10
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 201 remark 11
QTECH(config-if-GigabitEthernet 0/3)#vlan-mapping-out vlan 202 remark 12
```

Шаг 4. Настройте Uplink-порт.

```
QTECH(config)# interface gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink
```

Проверка	Отобразите политики сопоставления VLAN 1:1, настроенные на коммутаторе этажа.

```
QTECH#show interfaces vlan-mapping
Ports     type   Status     Service-Vlan   Customer-Vlan-list
----------  -----  ---------  ----------- ----------------
Gi0/2     in     active     100           10
Gi0/2     in     active     101           11
Gi0/2     in     active     102           12
Gi0/2     out    active     100           10
Gi0/2     out    active     101           11
Gi0/2     out    active     102           12
Gi0/3     in     active     200           10
Gi0/3     in     active     201           11
Gi0/3     in     active     202           12
Gi0/3     out    active     200           10
Gi0/3     out    active     201           11
Gi0/3     out    active     202           12
```

13.5.5. Настройка TPID

13.5.5.1. Эффект конфигурации

Настройте TPID'ы в тегах на сетевых устройствах SP, чтобы реализовать совместимость с TPID.

13.5.5.2. Примечания

Если PE подключен к стороннему коммутатору, на котором TPID не равен 0x8100, вам необходимо настроить TPID на порту PE, подключенного к стороннему коммутатору.

ПРИМЕЧАНИЕ: не устанавливайте для TPID любое из следующих значений: 0x0806 (ARP), 0x0200 (PUP), 0x8035 (RARP), 0x0800 (IP), 0x86DD (IPv6), 0x8863/0x8864 (PPPoE), 0x8847/0x8848 (MPLS). , 0x8137 (IPX/SPX), 0x8000 (IS-IS), 0x8809 (LACP), 0x888E (802.1X), 0x88A7 (кластеры) и 0x0789 (зарезервировано QTECH Networks).

13.5.5.3. Шаги настройки

- Если PE подключен к стороннему коммутатору, на котором TPID не равен 0x8100, вам необходимо настроить TPID на порту PE, подключенного к стороннему коммутатору.
- TPID можно настроить в режиме конфигурации интерфейса и в режиме глобальной конфигурации. В следующем примере используется режим конфигурации интерфейса.

Настройте команду **frame-tag tpid** *0x9100* в режиме конфигурации интерфейса, чтобы изменить TPID на 0x9100.

Команда	**frame-tag tpid** *tpid*
Описание параметров	*tpid*: указывает новое значение TPID
По умолчанию	Значение TPID по умолчанию — 0x8100
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	Если PE подключен к стороннему коммутатору, на котором TPID не 0x8100, используйте эту команду для настройки TPID на порту, подключенном к стороннему коммутатору

13.5.5.4. Проверка

Проверьте, настроен ли TPID.

13.5.5.5. Пример конфигурации

Настройка TPID на порту

Шаги настройки	Настройте TPID на порту. QTECH(config)# interface gigabitethernet 0/1 QTECH(config-if)# frame-tag tpid 9100
Проверка	Отображение TPID на порту. QTECH# show frame-tag tpid interfaces gigabitethernet 0/1 Port tpid ------- ------------- Gi0/1 0x9100

13.5.6. Настройка репликации MAC-адресов

13.5.6.1. Эффект конфигурации

- Реплицируйте динамический адрес, полученный на порту, из одной VLAN в другую.
- Избегайте лавинной рассылки пакетов (флуда), когда потоки трафика сервисов разделены с помощью списков ACL на основе MAC-адресов.

13.5.6.2. Примечания

ПРИМЕЧАНИЕ: после отключения репликации MAC-адресов система удалит все изученные записи MAC-адресов из VLAN назначения.

ПРИМЕЧАНИЕ: репликация MAC-адреса может быть настроена для порта только один раз. Если вам нужно изменить конфигурацию, удалите текущую конфигурацию и настройте ее заново.

ПРИМЕЧАНИЕ: репликацию MAC-адресов VLAN нельзя использовать вместе с совместным использованием VLAN, а MAC-адреса нельзя реплицировать в динамические VLAN.

ПРИМЕЧАНИЕ: на каждом порту можно настроить до восьми целевых VLAN. Репликация MAC-адреса вступает в силу, даже если порт не принадлежит указанной целевой VLAN.

ПРИМЕЧАНИЕ: репликация MAC-адресов не может быть настроена на портах хоста и неразборчивых портах, портах мониторинга и портах с включенной безопасностью портов/802.1X.

ПРИМЕЧАНИЕ: реплицировать можно только динамические адреса. Репликация адресов отключается, когда таблица адресов заполнена. Если исходные адреса уже существуют до включения репликации, соответствующие MAC-адреса не будут реплицированы.

ПРИМЕЧАНИЕ: реплицированные адреса имеют более высокий приоритет, чем динамические адреса, но имеют более низкий приоритет, чем другие типы адресов.

ПРИМЕЧАНИЕ: когда MAC-адрес устаревает, реплицированный MAC-адрес также устаревает. При удалении MAC-адреса реплицированный адрес будет удален автоматически.

ПРИМЕЧАНИЕ: горячее резервное копирование не поддерживается. После основного/вторичного переключения рекомендуется отключить репликацию MAC-адресов, а затем снова включить ее.

ПРИМЕЧАНИЕ: записи MAC-адресов, полученные посредством репликации MAC-адресов, нельзя удалить вручную. Если вам нужно удалить эти записи, отключите репликацию MAC-адресов.

13.5.6.3. Шаги настройки

- Настройка репликацию MAC-адресов.
- Выполните эту настройку, чтобы реплицировать MAC-адреса из одной VLAN в другую, чтобы избежать флудинга.
- Запустите команду **mac-address-mapping** <1-8> **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id* на магистральном порту, чтобы включить репликацию MAC-адреса. *src-vlan-list* и *dst-vlan-id* указывают диапазон VLAN.

Команда	**mac-address-mapping** *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
Описание параметров	*x*: указывает номер индекса для репликации MAC-адреса. Значение колеблется от 1 до 8. *src-vlan-list*: указывает список исходных VLAN. *dst-vlan-id*: указывает список целевых VLAN
По умолчанию	По умолчанию репликация MAC-адресов отключена
Командный режим	Режим конфигурации интерфейса

13.5.6.4. Проверка

Проверьте, реплицирован ли MAC-адрес указанной VLAN в другую VLAN.

13.5.6.5. Пример настройки

Настройка репликации MAC-адресов

Шаги настройки	Настройте репликацию MAC-адресов. QTECH(config)# interface gigabitethernet 0/1 QTECH(config-if)# switchport mode trunk QTECH(config-if)#mac-address-mapping 1 source-vlan 1-3 destination-vlan 5
Проверка	• Проверьте, влияет ли конфигурация на порт. • Отправьте пакет из исходной VLAN и проверьте, реплицирован ли исходный MAC-адрес пакета в целевую VLAN. QTECH# show interfaces mac-address-mapping Ports destination-VID Source-VID-list --- Gi0/1 5 1-3

13.5.6.6. Распространенные ошибки

См. «Примечания».

13.5.7. Настройка внутренней/внешней политики модификации тегов VLAN

13.5.7.1. Эффект конфигурации

Измените внешние или внутренние теги в соответствии с фактическими требованиями к сети.

13.5.7.2. Примечания

ПРИМЕЧАНИЕ: политика QinQ на основе ACL-списка преобладает над политикой QinQ на основе порта и C-TAG.

ПРИМЕЧАНИЕ: при удалении ACL соответствующая политика будет автоматически удалена.

ПРИМЕЧАНИЕ: политики модификации тегов действуют только на порты доступа, магистральные порты, гибридные порты и Uplink-порты.

ПРИМЕЧАНИЕ: политики модификации тегов в основном используются для изменения внутренних и внешних тегов в сети SP.

ПРИМЕЧАНИЕ: если пакет соответствует двум или более политикам Selective QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

13.5.7.3. Шаги настройки

Настройка политики для изменения идентификаторов VLAN внешних тегов на основе внутренних тегов

- Опционально.

- Выполните эту настройку, чтобы изменить идентификаторы VLAN внешних тегов на основе идентификаторов VLAN внутренних тегов.
- Вы можете изменить идентификаторы VLAN внешних тегов в пакетах, которые входят в порты доступа, магистральные порты, гибридные порты и Uplink-порты, на основе идентификаторов VLAN внутренних тегов в этих пакетах.

Команда	**dot1q relay-vid** *VID* **translate inner-vid** *v_list*
Описание параметров	*VID*: указывает измененный идентификатор VLAN внешнего тега. *v_list*: указывает идентификатор VLAN внутреннего тега
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

Настройка политики для изменения идентификаторов VLAN внешних тегов на основе идентификаторов VLAN внешних и внутренних тегов

- Опционально.
- Выполните эту настройку, чтобы изменить идентификаторы VLAN внешних тегов на основе идентификаторов VLAN внутренних и внешних тегов.
- Вы можете изменить идентификаторы VLAN внешних тегов в пакетах, которые входят в порты доступа, магистральные порты, гибридные порты и Uplink-порты, на основе идентификаторов VLAN внутренних и внешних тегов в этих пакетах.

Команда	**dot1q new-outer-vlan** *new-vid* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*
Описание параметров	*new-vid*: указывает измененный идентификатор VLAN внешнего тега. *vid*: указывает исходный идентификатор VLAN внешнего тега. *v_list*: указывает идентификатор VLAN внутреннего тега
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

Настройка политики для изменения идентификаторов VLAN внешних тегов на основе внешних тегов

- Опционально.
- Выполните эту настройку, чтобы изменить идентификаторы VLAN внешних тегов на основе этих идентификаторов VLAN.
- Вы можете изменить идентификаторы VLAN внешних тегов в пакетах, которые входят в порты доступа, магистральные порты, гибридные порты и Uplink-порты на основе этих идентификаторов VLAN.

Команда	**dot1q relay-vid** *VID* **translate local-vid** *v_list*
Описание параметров	*VID*: указывает измененный идентификатор VLAN внешнего тега. *v_list*: указывает исходный идентификатор VLAN внешнего тега
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

Настройка политики для изменения идентификаторов VLAN внутренних тегов на основе списков ACL

- Опционально.
- Вы можете изменить идентификаторы VLAN внутренних тегов в пакетах, которые выходят из портов доступа, магистральных портов, гибридных портов и Uplink-портов, на основе содержимого пакета.
- Прежде чем настраивать такую политику, настройте ACL.

Команда	**traffic-redirect access-group** *acl* **inner-vlan** *vid* **out**
Описание параметров	*acl*: указывает ACL. *vid*: указывает измененный идентификатор VLAN внутреннего тега
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

Настройка политики для изменения идентификаторов VLAN внешних тегов на основе списков ACL

- Опционально.
- Вы можете изменить идентификаторы VLAN внешних тегов в пакетах, которые выходят из портов доступа, магистральных портов, гибридных портов и Uplink-портов, на основе содержимого пакета.
- Прежде чем настраивать такую политику, настройте ACL.

Команда	**traffic-redirect access-group** *acl* **outer-vlan** *vid* **in**
Описание параметров	*acl*: указывает ACL. *vid*: указывает измененный идентификатор VLAN внешнего тега
По умолчанию	По умолчанию политика не настроена
Командный режим	Режим конфигурации интерфейса

13.5.7.4. Проверка

Проверьте, действует ли конфигурация и изменяет ли порт теги в полученных пакетах на основе политики.

13.5.7.5. Пример конфигурации

Настройка политики для изменения идентификаторов VLAN внешних тегов на основе внешних тегов

Шаги настройки	• Настройте политики модификации внутренних/внешних тегов для порта в соответствии с фактическими требованиями к сети. • В следующем примере показано, как изменить идентификаторы VLAN внешних тегов на основе внешних тегов и ACL соответственно. Дополнительные сведения о других политиках см. в описании выше. • Настройте политику для изменения тегов внешней VLAN на основе тегов внешней VLAN. QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if)# switchport mode trunk QTECH(config-if)# dot1q relay-vid 100 translate local-vid 10-20 • Настройте политику для изменения внешних тегов VLAN на основе списков ACL. QTECH# configure terminal QTECH(config)# ip access-list standard 2 QTECH(config-acl-std)# permit host 1.1.1.1 QTECH(config-acl-std)# exit QTECH(config)# interface gigabitEthernet 0/2 QTECH(config-if)# switchport mode trunk QTECH(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
Проверка	• Проверьте, влияет ли конфигурация на порт. • Проверьте, изменяет ли порт идентификаторы VLAN внешних тегов в полученных пакетах на основе настроенной политики

13.5.8. Настройка сопоставления приоритетов и репликации приоритетов

13.5.8.1. Эффект конфигурации

- Если сеть SP предоставляет политику QoS на основе поля User Priority внутреннего тега, настройте репликацию приоритетов, чтобы применить политику QoS к внешнему тегу.
- Если сеть SP предоставляет политику QoS, основанную на поле User Priority внутреннего тега, настройте сопоставление приоритетов, чтобы применить поле User Priority, предоставленное сетью SP, к внешнему тегу.

13.5.8.2. Примечания

ПРИМЕЧАНИЕ: только туннельный порт можно настроить с репликацией приоритетов, который имеет более высокий приоритет, чем доверенный QoS, но более низкий, чем QoS на основе ACL.

ПРИМЕЧАНИЕ: репликация приоритетов и сопоставление приоритетов не могут быть одновременно включены на одном порту.

ПРИМЕЧАНИЕ: только для туннельного порта можно настроить сопоставление приоритетов, которое преобладает над QoS.

ПРИМЕЧАНИЕ: конфигурация сопоставления приоритетов не вступает в силу, если режим доверия не настроен (никому не доверяет) или режим доверия не соответствует сопоставлению приоритетов.

13.5.8.3. Шаги настройки

- Только для туннельного порта можно настроить сопоставление приоритетов или репликацию приоритетов.
- Настройте репликацию приоритетов для применения внутренней политики QoS на основе тегов, предоставляемой сетью SP.
- Настройте сопоставление приоритетов, чтобы настроить поле User Priority внешнего тега VLAN на основе внутреннего тега и гибко применить политику QoS.
- Чтобы включить репликацию приоритетов, запустите команду **inner-priority-trust enable** на туннельном порту.
- Чтобы включить сопоставление приоритетов, запустите команду **dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value* на туннельном порту.

inner-cos-value и *outer-cos-value* находятся в диапазоне от 0 до 7.

ПРИМЕЧАНИЕ: если сопоставление приоритетов не настроено, используется следующее сопоставление приоритетов:

inner pri	0	1	2	3	4	5	6	7
outer pri	0	1	2	3	4	5	6	7

Рисунок 13-14.

Команда	**inner-priority-trust enable**
По умолчанию	По умолчанию репликация приоритетов отключена
Командный режим	Режим конфигурации интерфейса

Команда	**dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value*
Описание параметров	*inner-cos-value*: указывает значение CoS внутреннего тега. *outer-cos-value*: указывает значение CoS внешнего тега

По умолчанию	По умолчанию сопоставление приоритетов отключено
Командный режим	Режим конфигурации интерфейса

13.5.8.4. Проверка

Запустите команду **show inner-priority-trust interfaces** *type intf-id* и команду **show interfaces** *type intf-id* **remark**, чтобы проверить, действует ли сопоставление приоритетов или репликация приоритетов.

13.5.8.5. Пример конфигурации

Настройка сопоставления приоритетов и репликации приоритетов

Шаги настройки	• Чтобы сохранить приоритет пакета, вам необходимо реплицировать приоритет внутреннего тега в пакете на внешний тег на туннельном порту. • Чтобы гибко управлять приоритетом пакетов на туннельном порту, вы можете добавлять к пакетам внешние теги с разными приоритетами на основе приоритетов внутренних тегов в пакетах. Настройте репликацию приоритетов. QTECH(config)# interface gigabitethernet 0/1 QTECH(config-if)#mls qos trust cos QTECH(config-if)# inner-priority-trust enable QTECH(config)# end Настройте сопоставление приоритетов. QTECH(config)# interface gigabitethernet 0/2 QTECH(config-if)#dot1q-Tunnel cos 3 remark-cos 5
Проверка	Отображение конфигурации приоритета порта. Проверьте, включена ли репликация приоритетов на туннельном порту. QTECH# show inner-priority-trust interfaces gigabitethernet 0/1 Port inner-priority-trust ------ ------------------ Gi0/1 enable Отображение сопоставления приоритетов, настроенного для туннельного порта. QTECH# show interfaces gigabitethernet 0/1 remark Ports Type From value To value ----------- ---------- ---------- -------- Gi0/1 Cos-To-Cos 3 5

13.5.8.6. Распространенные ошибки

См. «Примечания».

13.5.9. Настройка прозрачной передачи уровня 2

13.5.9.1. Эффект конфигурации

Передавайте пакеты 2-го уровня прозрачно, не влияя на сеть SP и сеть клиента.

13.5.9.2. Примечания

ПРИМЕЧАНИЕ: если протокол STP не включен, необходимо выполнить команду **bridge-frame forwarding protocol bpdu**, чтобы включить прозрачную передачу STP.

ПРИМЕЧАНИЕ: прозрачная передача, включенная для порта, вступает в силу только после того, как она будет включена глобально. Когда на порте действует прозрачная передача, порт не участвует в вычислении соответствующего протокола. Если порт получает пакет, MAC-адрес назначения которого является специальным broadcast-адресом, он определяет, что произошла сетевая ошибка, и отбрасывает пакет.

13.5.9.3. Шаги настройки

Настройка прозрачной передачи STP

- Обязательно, если вам нужно прозрачно передавать пакеты BPDU через STP.
- Включите прозрачную передачу STP в режиме глобальной конфигурации и режиме конфигурации интерфейса.
- Запустите команду **l2protocol-tunnel stp** в режиме глобальной конфигурации, чтобы включить прозрачную передачу STP.
- Запустите команду **l2protocol-tunnel stp enable** в режиме конфигурации интерфейса, чтобы включить прозрачную передачу STP.

Команда	**l2protocol-tunnel stp**
По умолчанию	По умолчанию прозрачная передача STP отключена
Командный режим	Режим глобальной конфигурации
Команда	**l2protocol-tunnel stp enable**
По умолчанию	По умолчанию прозрачная передача STP отключена
Командный режим	Режим конфигурации интерфейса

Настройка прозрачной передачи GVRP

- Обязательно, если вам нужно прозрачно передавать пакеты GVRP.
- Включите прозрачную передачу GVRP в режиме глобальной конфигурации и режиме конфигурации интерфейса.
- Запустите команду **l2protocol-tunnel gvrp** в режиме глобальной конфигурации, чтобы включить прозрачную передачу GVRP.

- Запустите команду **l2protocol-tunnel gvrp enable** в режиме настройки интерфейса, чтобы включить прозрачную передачу GVRP.

Команда	**l2protocol-tunnel gvrp**
По умолчанию	По умолчанию прозрачная передача GVRP отключена
Командный режим	Режим глобальной конфигурации

Команда	**l2protocol-tunnel gvrp enable**
По умолчанию	По умолчанию прозрачная передача GVRP отключена
Командный режим	Режим конфигурации интерфейса

Настройка прозрачного адреса передачи

- Опционально.
- Настройте прозрачный адрес передачи.

Команда	**l2protocol-tunnel** { **stp** | **gvrp** } **tunnel-dmac** *mac-address*
Описание параметров	*mac-address*: указывает адрес, используемый для прозрачной передачи пакетов
По умолчанию	По умолчанию первые три байта прозрачного адреса передачи — 01d0f8, а последние три байта — 000005 и 000006 для STP и GVTP соответственно
Командный режим	Режим конфигурации интерфейса
Руководство по использованию	**ПРИМЕЧАНИЕ:** для STP доступны следующие адреса: 01d0.f800.0005, 011a.a900.0005, 010f.e200.0003, 0100.0ccd.cdd0, 0100.0ccd.cdd1 и 0100.0ccd.cdd2. Для GVRP доступны следующие адреса: 01d0.f800.0006 и 011a.a900.0006. **ПРИМЕЧАНИЕ:** если адрес прозрачной передачи не настроен, используются настройки по умолчанию

13.5.9.4. Проверка

Запустите команду **show l2protocol-tunnel stp** и команду **show l2protocol-tunnel gvrp**, чтобы проверить, правильно ли настроен адрес прозрачной передачи.

13.5.9.5. Пример конфигурации

В следующем примере показано, как настроить прозрачную передачу STP.

Настройка прозрачной передачи STP

Сценарий:

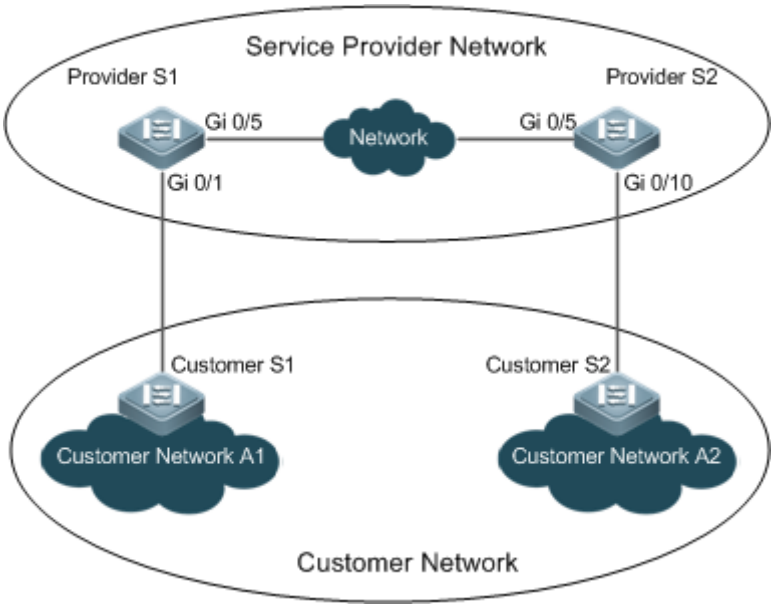


Рисунок 13-15.

Шаги настройки	• На PE (Провайдер S1 и Провайдер S2) включите прозрачную передачу STP в режиме глобальной конфигурации и режиме конфигурации интерфейса. • Прежде чем включить прозрачную передачу STP, включите STP в режиме глобальной конфигурации, чтобы коммутаторы могли пересылать пакеты STP
Провайдер S1	Шаг 1. Включите STP. **bridge-frame forwarding protocol bpdu** Шаг 2. Настройте VLAN для прозрачной передачи. **ProviderS1#configure terminal** **Enter configuration commands, one per line. End with CNTL/Z.** **ProviderS1(config)#vlan 200** **ProviderS1(config-vlan)#exit** Шаг 3. Включите базовый QinQ на порту, подключенном к сети клиента, и используйте VLAN 200 для туннелирования. **ProviderS1(config)#interface gigabitEthernet 0/1** **ProviderS1(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel** **ProviderS1(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan 200** Шаг 4. Включите прозрачную передачу STP на порту, подключенном к сети клиента. **ProviderS1(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable**

	ProviderS1(config-if-GigabitEthernet 0/1)#exit Шаг 5. Включите прозрачную передачу STP в режиме глобальной конфигурации. ProviderS1(config)#l2protocol-tunnel stp Шаг 6. Настройте Uplink-порт. ProviderS1(config)# interface gigabitEthernet 0/5 ProviderS1(config-if-GigabitEthernet 0/5)#switchport mode uplink
Провайдер S2	Настройте Провайдер S2, выполнив те же действия
Проверка	Шаг 1. Проверьте, включена ли прозрачная передача STP в режиме глобальной конфигурации и режиме конфигурации интерфейса. ProviderS1#show l2protocol-tunnel stp L2protocol-tunnel: Stp Enable GigabitEthernet 0/1 l2protocol-tunnel stp enable Шаг 2. Проверьте конфигурацию, проверив: • Тип порта — dot1q-tunnel. • VLAN с внешним тегом согласуется с Native VLAN и добавляется в список VLAN туннельного порта. • Порт, который обращается к сети SP, настроен как порт Uplink. ProviderS1#show running-config interface GigabitEthernet 0/1 switchport mode dot1q-tunnel switchport dot1q-tunnel allowed vlan add untagged 200 switchport dot1q-tunnel native vlan 200 l2protocol-tunnel stp enable spanning-tree bpdufilter enable ! interface GigabitEthernet 0/5 switchport mode uplink

13.5.9.6. Распространенные ошибки

- STP не включен в режиме глобальной конфигурации.
- Прозрачная передача не включена в режиме глобальной конфигурации и режиме конфигурации интерфейса.

13.6. Мониторинг

13.6.1. Отображение

Описание	Команда
Отображает, является ли указанный порт туннельным портом	**show dot1q-tunnel** [**interfaces** *intf-id*]
Отображает конфигурацию туннельного порта	**show interfaces dot1q-tunnel**
Отображает политики Selective QinQ на основе C-TAG для туннельного порта	**show registration-table** [**interfaces** *intf-id*]
Отображает политики Selective QinQ на основе C-TAG для порта доступа, транкового порта или гибридного порта	**show translation-table** [**interfaces** *intf-id*]
Отображает сопоставление VLAN на портах	**show interfaces** [*intf-id*] **vlan-mapping**
Отображает политики Selective QinQ на основе ACL	**show traffic-redirect** [**interfaces** *intf-id*]
Отображает конфигурацию TPID на портах	**show frame-tag tpid interfaces** [*intf-id*]
Отображает конфигурацию репликации приоритетов	**show inner-priority-trust**
Отображает конфигурацию сопоставления приоритетов	**show interface intf-name remark**
Отображает конфигурацию репликации MAC-адресов	**show mac-address-mapping**
Отображает конфигурацию прозрачной передачи уровня 2	**show l2protocol-tunnel** { **gvrp** | **stp** }

13.6.2. Отладка

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

Описание	Команда
Отладка QinQ	**debug bridge qinq**

14. НАСТРОЙКА HASH-СИМУЛЯТОРА

14.1. Обзор

HASH-симулятор — это программа, которая имитирует HASH-алгоритм коммутатора. Симулятор HASH поддерживает режимы балансировки нагрузки агрегированного порта (AP).

Симулятор AP HASH имитирует алгоритм HASH для расчета порта-участника AP для пересылки пакетов на основе поля пакета, режима балансировки нагрузки и указанной информации AP. Результат расчета соответствует реальному порту переадресации.

ПРИМЕЧАНИЕ: если вы настраиваете AP на коммутаторе, используйте симулятор AP, чтобы вычислить порт-участник AP для пересылки пакетов, указав поле пакета.

Симулятор HASH можно использовать для отслеживания и мониторинга пути пересылки указанных пакетов, облегчая управление пользователями и устранение неполадок.

14.1.1. Протоколы и стандарты

IEEE 802.3ad

14.2. Приложения

Приложение	Описание
Симулятор AP HASH	Объединение нескольких физических каналов в один логический — эффективный способ увеличить пропускную способность порта и повысить надежность коммутатора L3. Пакеты пересылаются по физическому каналу в соответствии с алгоритмом балансировки нагрузки. Расчет симулятора AP позволяет пользователям проверять ссылку на участника, которая служит ориентиром для устранения неполадок и развертывания топологии

14.2.1. Симулятор AP HASH

14.2.1.1. Сценарий

С помощью симулятора HASH вы можете рассчитать порт пересылки AP с балансировкой нагрузки.

- Балансировка нагрузки AP: сервер с двумя сетевыми картами (dual-NIC) объединен в один логический канал для совместного использования потока трафика сервисных данных.
- Вы должны знать, какая сетевая карта на сервере получает пакеты с IP-адресами назначения 2.2.2.1/24, 4.4.4.1/24 и 9.9.9.1/24, отправленными с uplink-порта сервера.

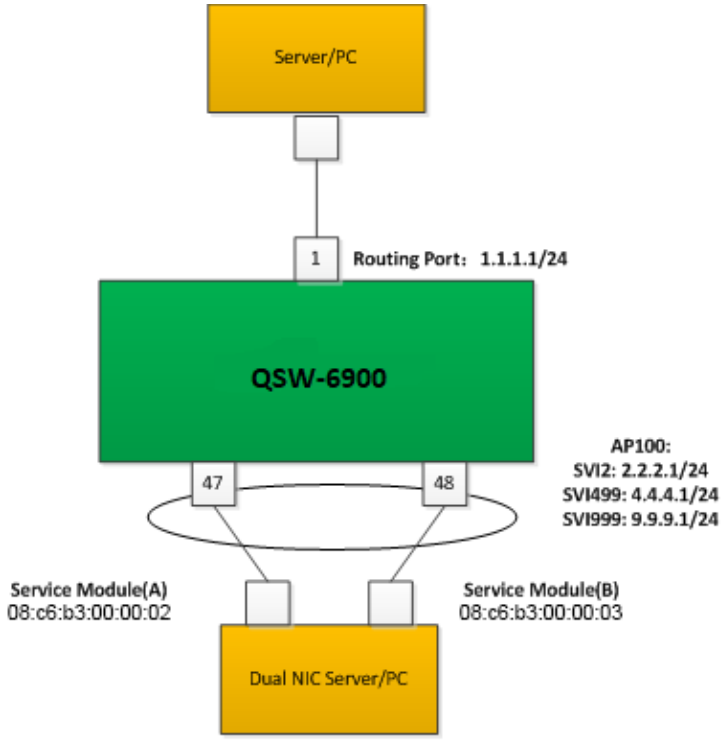


Рисунок 14-1.

14.2.1.2. Развертывание

- Порты, соединяющие сервер с двумя сетевыми картами и QSW-6900, объединяются в AP для совместного использования потока трафика сервисных данных.
- Используйте VLAN 2, VLAN 499 и VLAN 999 для разделения сети и предоставления различных типов сервисов.
- Вы можете определить порт пересылки с балансировкой нагрузки AP на QSW-6900 в соответствии с характеристиками пакета.

ПРИМЕЧАНИЕ: функция пакета может быть IP-адресом источника (Source IP), IP-адресом назначения (Destination IP), исходным портом L4 (Source L4 port) или портом назначения L4 (Destination L4 port).

14.3. Функции

14.3.1. Базовые определения

AP

AP — это логический порт, состоящий из нескольких физических портов. AP можно разделить на статические и динамические (LACP AP) в зависимости от протокола или на AP L2 и L3 в зависимости от характеристик порта.

L2 AP

L2 AP — это логический порт, состоящий из нескольких портов L2 с одинаковыми функциями L2.

L3 AP

L3 AP — это логический порт, состоящий из нескольких портов L3 с одинаковыми функциями L3.

Режим балансировки нагрузки

Пакеты пересылаются портом-участником AP на основе его режима балансировки нагрузки. Доступны следующие режимы балансировки нагрузки AP:

- MAC-адрес источника/MAC-адрес получателя (Src-mac/Dst-mac)
- MAC-адрес источника + MAC-адрес назначения (Src-dst-mac)
- IP-адрес источника/IP-адрес назначения (Src-ip/Dst-ip)
- IP-адрес источника + IP-адрес назначения (Src-dst-ip)
- IP-адрес источника + IP-адрес назначения + исходный порт L4 + порт назначения L4 (Src-dst-ip-l4port)
- Порт панели входящих пакетов
- Расширенный режим (расширенный)
- HASH-симулятор

HASH-симулятор — это программа, которая имитирует HASH-алгоритм коммутатора.

Quintuple

Quintuple относится к исходному IP-адресу, IP-адресу назначения, протоколу, исходному порту L4 и порту получателя L4.

Обзор

Обзор	Описание
Симулятор AP HASH	Вычисляет порт-участник AP для пересылки пакетов в соответствии с полем пакета, режимом балансировки нагрузки AP и указанной информацией о AP

14.3.2. Симулятор AP HASH

Симулятор AP HASH используется для расчета порта-участника AP для пересылки пакетов путем указания поля пакета.

14.3.2.1. Принцип работы

Симулятор HASH имитирует алгоритм HASH на коммутаторе. Процесс расчета балансировки нагрузки AP на коммутаторе состоит из следующих шагов:

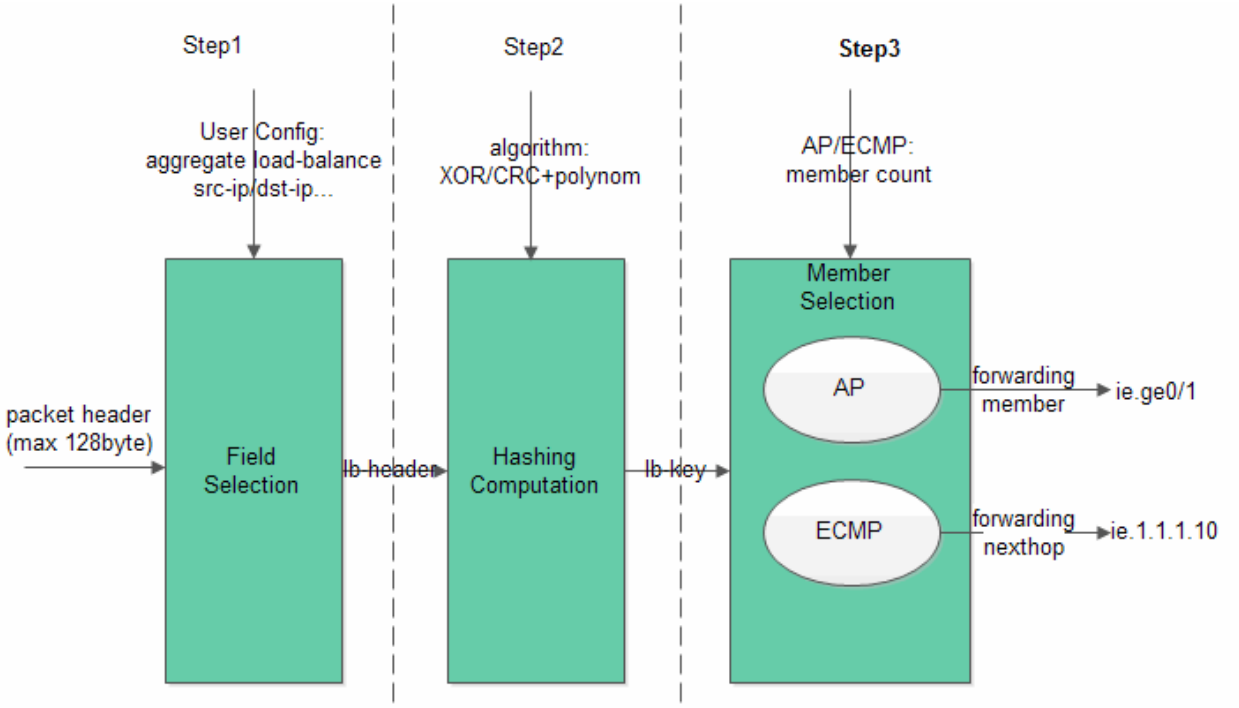


Рисунок 14-2.

Шаг 1. Выбор поля. Поля извлекаются в соответствии с настроенным режимом балансировки нагрузки.

- В качестве HASH-факторов выбираются разные поля в зависимости от настроенного режима балансировки нагрузки:

Режим балансировки нагрузки	**HASH-фактор**
Src-mac	MAC-адрес источника
Dst-mac	MAC-адрес назначения
Src-dst-mac	MAC-адрес источника и MAC-адрес назначения
Src-ip	IP-адрес источника
Dst-ip	IP-адрес назначения
Src-dst-ip	IP-адрес источника и IP-адрес назначения
Src-dst-ip-l4port	IP-адрес источника и IP-адрес назначения, исходный порт L4 и порт назначения L4

Режим балансировки нагрузки	HASH-фактор
Enhanced	Поля извлекаются в соответствии с профилем балансировки нагрузки. Используйте команду **show load-balance profile** *profile-name* для отображения всех полей пакетов, соответствующих поддерживаемым типам пакетов

ПРИМЕЧАНИЕ: симулятор AP HASH поддерживает режимы балансировки нагрузки src-mac, dst-mac, src-dst-mac, src-ip, dst-ip, src-dst-ip, src-dst-ip-l4port и Enhanced.

ПРИМЕЧАНИЕ: выбранные коэффициенты HASH для балансировки нагрузки AP могут различаться в зависимости от продукта.

Шаг 2. Вычисление HASH.

- Алгоритм HASH используется для вычисления ключа HASH lb (ключ балансировки нагрузки) на основе коэффициента HASH, выбранного на шаге 1. Алгоритмы HASH различаются в зависимости от различных коммутаторов, таких как XOR, CRC и CRC+scramble.
- Симулятор HASH имитирует алгоритм HASH на коммутаторе.

Шаг 3. Выбор участника.

- Разделите номер участника AP на HASH lb-ключ, а остаток представляет собой индекс порта пересылки. Индекс уникален для коммутаторов серии QTECH BCM (включая коммутатор ядра и коммутатор доступа). Следовательно, его можно использовать для идентификации порта пересылки.

14.3.2.2. Связанная конфигурация

Отображение результата расчета симулятора AP

Пользователи могут проверить порт переадресации IPv4 AP с балансировкой нагрузки, указав функцию Quintuple пакетов IPv4.

Пользователи могут проверить порт переадресации IPv6 AP с балансировкой нагрузки, указав функцию Quintuple пакетов IPv6.

ПРИМЕЧАНИЕ: симулятор AP HASH поддерживает симуляционный расчет только для пересылки unicast-пакетов.

14.4. Конфигурация

Конфигурация	Описание и команда	
Отображение порта переадресации AP с балансировкой нагрузки	Опционально	
	show aggregate load-balance to interface aggregateport *ap-id* **ip** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	Отображает IPv4 AP порт переадресации с балансировкой нагрузки

Конфигурация	Описание и команда	
Отображение порта переадресации AP с балансировкой нагрузки	**show aggregate load-balance to interface aggregateport** *ap-id* **ipv6** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	Отображает IPv6 AP порт переадресации с балансировкой нагрузки
	show aggregate load-balance interface *interface-type interface number* **to interface aggregateport** *ap-id* **forward** [L2 | L3] **mac** [**src-mac** *source-mac*] [**dst-mac** *dest-mac*] [**vlan** *vlan-id*] [**etype** *value*]	Отображает порт переадресации AP уровня 2 с балансировкой нагрузки

14.4.1. Отображение порта переадресации AP с балансировкой нагрузки

14.4.1.1. Эффект конфигурации

Отображение порта-участника AP для пересылки пакетов.

14.4.1.2. Примечания

- Симулятор хеширования AP работает на основе режима балансировки нагрузки AP. Поэтому сначала используйте команду агрегированной баланстровки нагрузки, чтобы настроить режим балансировки нагрузки AP.
- Создайте AP и добавьте порты-участники.

ПРИМЕЧАНИЕ: см. раздел Настройка агрегированного порта.

14.4.1.3. Шаги настройки

Отображение порта переадресации AP уровня 2 с балансировкой нагрузки

- Мониторинг пути пересылки и устранение неполадок.
- Введите команду, чтобы отобразить порты переадресации AP на коммутаторе.

Отображение порта переадресации IPv4 AP с балансировкой нагрузки

То же, что и выше.

Отображение порта переадресации IPv6 AP с балансировкой нагрузки

То же, что и выше.

14.4.1.4. Проверка

- Проверьте конфигурацию, пропустив реальный трафик. Отметьте и запишите порт пересылки.
- Проверьте, соответствует ли реальный порт переадресации отображаемому порту.

14.4.1.5. Связанные команды

Отображение порта переадресации AP уровня 2 с балансировкой нагрузки

Команда	**show aggregate load-balance interface** *interface-type interface-number* **to interface aggregateport** *ap-id* **forward** [*L2* | *L3*] **mac** [**src-mac** *source-mac*] [**dst-mac** *dest-mac*] [**vlan** *vlan-id*] [**etype** *value*]
Параметр	**interface** *interface-type interface-number*: входящий трафик. **aggregateport** *ap-id*: идентификатор AP назначения. **forward** [*L2* | *L3*]: режим пересылки уровня 2 или уровня 3. **src-mac** *source-mac*: MAC-адрес источника. **dst-mac** *dest-mac*: MAC-адрес назначения. **vlan** *vlan-id*: идентификатор тега. **etype** *value*: тип пакета Ethernet
Командный режим	Привилегированный режим EXEC/режим глобальной конфигурации/ режим конфигурации интерфейса

Отображение порта переадресации IPv4 AP с балансировкой нагрузки

Команда	**show aggregate load-balance interface** *interface-type interface-number* **to interface aggregateport** *ap-id* **forward** [*L2* | *L3*] **ip** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]
Параметр	**interface** *interface-type interface-number*: входящий трафик. **aggregateport** *ap-id*: идентификатор AP назначения. **forward** [*L2* | *L3*]: режим пересылки уровня 2 или уровня 3. **source** *source-ip*: IPv4-адрес источника. **destination** *dest-ip*: IPv4-адрес назначения. **ip-protocol** *protocol-id*: идентификатор IP-протокола. Например, идентификаторы протоколов TCP и UDP равны 6 и 17 соответственно. **l4-source-port** *src-port*: идентификатор исходного порта L4. **l4-dest-port** *dest-port*: идентификатор порта назначения L4
Командный режим	Привилегированный режим EXEC/режим глобальной конфигурации/ режим конфигурации интерфейса

Отображение порта переадресации IPv6 AP с балансировкой нагрузки

Команда	**show aggregate load-balance interface** *interface-type interface-number* **to interface aggregateport** *ap-id* **forward** [*L2* | *L3*] **ipv6** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]
Параметр	**interface** *interface-type interface-number*: входящий трафик. **aggregateport** *ap-id*: идентификатор AP назначения. **forward** [*L2* | *L3*]: режим пересылки уровня 2 или уровня 3. **source** *source-ip*: IPv6-адрес источника. **destination** *dest-ip*: IPv6-адрес назначения. **ip-protocol** *protocol-id*: идентификатор IP-протокола. Например, идентификаторы протоколов TCP и UDP равны 6 и 17 соответственно. **l4-source-port** *src-port*: идентификатор исходного порта L4. **l4-dest-port** *dest-port*: идентификатор порта назначения L4
Командный режим	Привилегированный режим EXEC/режим глобальной конфигурации/ режим конфигурации интерфейса

14.4.1.6. Распространенные ошибки

- Симулятор AP HASH не поддерживает настроенный режим балансировки нагрузки.
- Текущий коммутатор не поддерживает симулятор AP HASH.
- AP не создана или не имеет портов-участников.

14.4.1.7. Пример конфигурации

Отображение порта переадресации AP уровня 2 с балансировкой нагрузки

Шаги настройки	Настраивает режим балансировки нагрузки. QTECH# configure terminal QTECH(config)# aggregateport load-balance dst-mac QTECH(config)# show agg load-balance Load-balance : Destination MAC QTECH# end
Проверка	Запустите команду **show aggregate load-balance to**, чтобы отобразить порт переадресации AP в соответствии с пакетом dmac. • Отображает порт переадресации с балансировкой нагрузки AP для пакетов, предназначенных для MAC-адреса 08c6.b300.0002. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002

	aggregateport load-balance mode : Destination MAC balance to port : GigabitEthernet 0/47 • Отображает порт переадресации с балансировкой нагрузки AP для пакетов, предназначенных для MAC-адреса 08c6.b300.0003. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002 aggregateport load-balance mode : Destination MAC balance to port : GigabitEthernet 0/48 • Если указанный AP не имеет портов-участников, порт переадресации отображается как NULL. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L2 mac dst-mac 08c6.b300.0002 aggregateport load-balance mode : Destination MAC balance to port :

Отображение порта переадресации IPv4 AP с балансировкой нагрузки

Сетевое окружение:

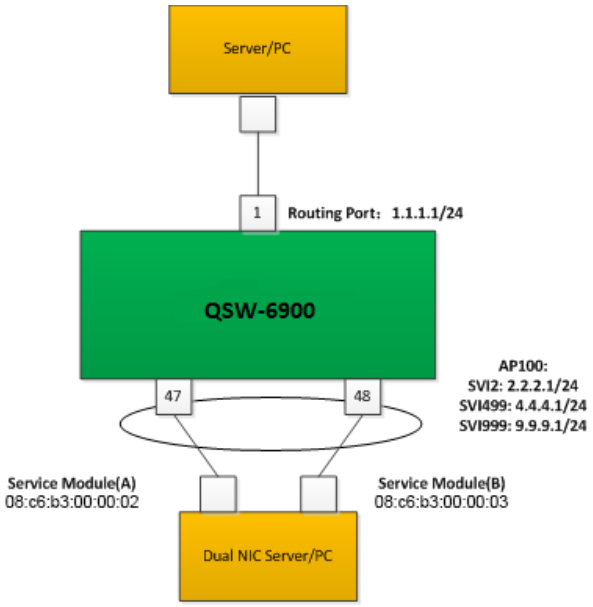


Рисунок 14-3.

Шаги настройки	Настройте режим балансировки нагрузки. QTECH# configure terminal QTECH(config)# aggregate load-balance dst-ip QTECH(config)# show agg load-balance Load-balance : Destination IP QTECH# end

Проверка	Используйте команду **show aggregate load-balance to** для отображения порта переадресации AP. • Отображение порта пересылки AP с балансировкой нагрузки для пакетов, предназначенных для IP-адреса 2.2.2.2. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip destination 2.2.2.2 aggregateport load-balance mode : Destination IP balance to port : GigabitEthernet 0/47 • Отображение порта пересылки AP с балансировкой нагрузки для пакетов, предназначенных для IP-адреса 4.4.4.4. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip destination 4.4.4.4 aggregateport load-balance mode : Destination IP balance to port : GigabitEthernet 0/48 • Если указанный AP не имеет портов-участников, порт переадресации отображается как NULL. QTECH# show aggregate load-balance interface gigabitethernet 0/1 to interface aggregateport 1 forward L3 ip source 1.1.1.1 aggregateport load-balance mode : Destination IP balance to port :

15. ОБЩАЯ ИНФОРМАЦИЯ

15.1. 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.

15.2. 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

15.3. Электронная версия документа

Дата публикации 31.01.2025

https://files.qtech.ru/upload/switchers/QSW-6900/QSW-6900_ethernet_switching_config_guide.pdf