Руководство пользователя

QSW-6510

Оглавление

1 КОНФИГУРАЦИЯ ИНТЕРФЕЙСОВ

1.1 Обзор

Интерфейсы играют важную роль при коммутации данных на сетевых устройствах. Устройства QTECH поддерживают два типа интерфейсов: физические интерфейсы и логические интерфейсы. Физический интерфейс — это аппаратный порт на устройстве, например, интерфейс 100Мбит/с Ethernet и гигабитный интерфейс Ethernet. Логический интерфейс не является аппаратным портом устройства. Логический интерфейс, такой как интерфейс loopback и интерфейс туннеля, может быть связан с физическим портом или не зависеть от любого физического порта. Для сетевых протоколов физические порты и логические интерфейсы выполняют одну и ту же функцию.

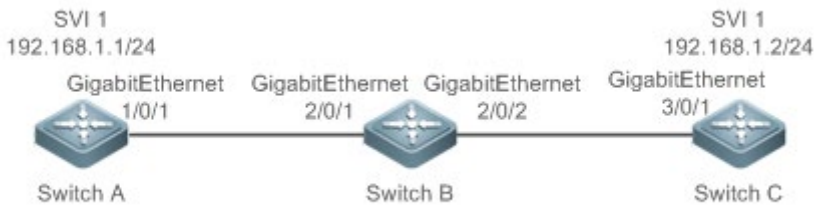
1.2 Применение

Применение	Описание
Коммутация данных L2 через физический интерфейс Ethernet	Реализация передачи данных на уровне 2 (L2) сетевых устройств через физический интерфейс L2 Ethernet.
Маршрутизация L3 через физический интерфейс Ethernet	Реализация передачи данных на уровне 3 (L3) для сетевых устройств через физический интерфейс L3 Ethernet.

1.2.1 Коммутация данных L2 через физический интерфейс Ethernet

Сценарий

Изображение 1-1



Как показано на Изображении 1-1, коммутатор A, коммутатор B и коммутатор C образуют простую сеть коммутации данных L2.

Описание

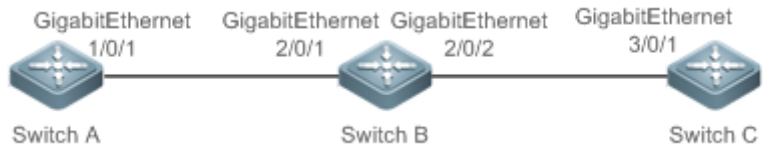
- Подключите коммутатор A к коммутатору B через физические порты GigabitEthernet 1/0/1 и GigabitEthernet 2/0/1.
- Подключите коммутатор B к коммутатору C через физические порты GigabitEthernet 2/0/2 и GigabitEthernet 3/0/1.

- Настройте порты 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 коммутаторах A и C соответственно и настройте IP-адреса из сегмента сети 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.
- Выполните команду **ping 192.168.1.2** на коммутаторе A и команду **ping 192.168.1.1** на коммутаторе C для применения коммутации данных с помощью коммутатора B.

1.2.2 Маршрутизация L3 через физический интерфейс Ethernet

Сценарий

Изображение 1-2



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

Описание

- 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.
- Сконфигурируйте порты GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, GigabitEthernet 2/0/2 и GigabitEthernet 3/0/1 в качестве портов с маршрутизацией L3.
- Настройка IP-адресов 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.
- Настройка IP-адресов 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 таким образом, чтобы коммутатор C мог получить прямой доступ к сегменту сети 192.168.1.0/24.
- Выполните команду **ping 192.168.2.2** на коммутаторе A и команду **ping 192.168.1.1** на коммутаторе C для применения L3 с помощью коммутатора B.

1.3 Функции

Базовые концепции

Классификация интерфейса

Интерфейсы устройств QTECH делятся на три категории:

- Интерфейс L2
- Интерфейс L3 (поддерживается устройствами L3)
- Интерфейс Fibre Channel (FC) (поддерживается некоторыми коммутаторами для центров обработки данных)

1. Интерфейсы L2 делятся на следующие типы:
- Порт коммутации
- Агрегированный порт L2 (LAG)

2. Интерфейсы L3 делятся на следующие типы:
- Порт маршрутизации
- Порт L3 LAG
- SVI
- Интерфейс loopback
- Туннельный интерфейс

3. Интерфейсы FC делятся на следующие типы:
- FC интерфейс
- Порт FC LAG

Порт коммутатора

Порт коммутатора является отдельным физическим портом устройства и реализует только функцию коммутации L2. Порт коммутатора используется для управления физическими портами и протоколами L2, связанными с физическими портами.

L2 LAG Порт

Агрегированный порт формируется путем объединения нескольких физических портов. Несколько физических каналов могут быть связаны друг с другом, образуя простую логическую связь. Этот логический канал называется агрегированным портом.

Для коммутации L2 порт LAG эквивалентен порту коммутатора, который объединяет пропускную способность нескольких портов, увеличивая тем самым пропускную способность канала. Кадры, отправляемые через агрегированный порт L2, сбалансированы между портами-участниками агрегированного порта L2. При сбое одного канала участника агрегированный порт L2 автоматически перенаправляет трафик с неисправного канала на другие каналы, повышая надежность соединений.

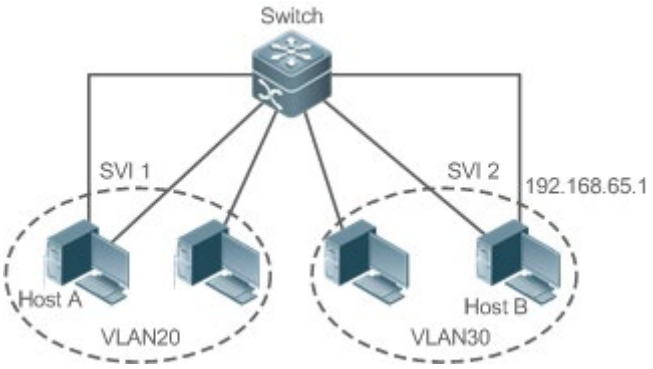
SVI

SVI может использоваться в качестве интерфейса управления локального устройства, с помощью которого администратор может управлять устройством. Кроме того, можно создать интерфейс SVI в качестве интерфейса шлюза, который привязан к виртуальному интерфейсу каждой VLAN для реализации маршрутизации между сетями VLAN и между устройствами L3. Можно выполнить команду **interface vlan** для создания интерфейса SVI и назначать IP-адрес этому интерфейсу для настройки маршрута между сетями VLAN.

Как показано на Изображении 1-3, хосты в сети VLAN 20 могут напрямую взаимодействовать 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.

Изображение 1-3



Порт маршрутизации

Физический порт на устройстве L3 можно настроить как порт маршрутизации, который функционирует как интерфейс шлюза для коммутации L3. Порт маршрутизации (Routed Port)не связан с определенной VLAN. Наоборот, это просто порт доступа. Порт маршрутизации (Routed Port)не может быть использован для коммутации L2. Можно выполнить команду **no switchport**, чтобы изменить порт коммутатора на Порт маршрутизации (Routed Port)и назначить IP-адрес этому порту для настройки маршрута. Обратите внимание, что перед выполнением команды **no switchport** необходимо удалить все функции L2 порта коммутатора.

Если порт является портом участником агрегированного порта L2 или портом DOT1X, не прошедшим проверку подлинности, нельзя запустить команду **switchport** или команду **no switchport** для настройки порта коммутатора или порта маршрутизации.

Порт L3 LAG

Как и порт L2 LAG, порт L3 LAG является логическим портом, который объединяет несколько физических портов-участников. Агрегированные порты должны быть портами L3 того же типа. Порт LAG функционирует как интерфейс шлюза для коммутации L3. Несколько физических каналов объединены в один логический канал, что расширяет полосу пропускания канала. Кадры, отправляемые через агрегированный порт L3, сбалансированы между портами-участниками агрегированного порта L3. При сбое одного канала участника агрегированный порт L3 автоматически перенаправляет трафик с неисправного канала на другие каналы, повышая надежность соединений.

Порт L3 LAG не может использоваться для коммутации L2. Можно выполнить команду **no switchport**, чтобы изменить порт L2 LAG, не содержащий ни одного порта-участника, на порт L3 LAG, добавить несколько портов маршрутизации к этому порту L3 LAG, а затем назначить IP-адрес на данный порт L3 LAG, чтобы настроить маршрут.

Интерфейс loopback

Интерфейс loopback представляет собой локальный логический интерфейс L3, постоянно используемый программой QROS. Пакеты, отправленные на интерфейс loopback, обрабатываются устройством локально, включая информацию о маршруте. IP-адрес интерфейса loopback можно использовать в качестве идентификатора устройства протокола маршрутизации кратчайшего пути (OSPF) или в качестве адреса источника, используемого протоколом пограничного шлюза (BGP) для настройки TCP-соединения. Процедура настройки интерфейса loopback аналогична процедуре настройки интерфейса Ethernet, и интерфейс loopback можно рассматривать как виртуальный интерфейс Ethernet.

Туннельный интерфейс

Интерфейс туннеля реализует функцию туннеля. Через туннельный интерфейс протоколы передачи (например, IP) могут использоваться для пересылки пакетов любого протокола. Как и другие логические интерфейсы, туннельный интерфейс также является виртуальным интерфейсом системы. Вместо указания любого протокола передачи или протокола нагрузки туннельный интерфейс обеспечивает стандартный режим передачи "точка-точка" (P2P). Таким образом, интерфейс туннеля должен быть настроен для каждого отдельного канала.

Интерфейс FC

Интерфейс FC — это физический порт, используемый для поддержки связи между оптическими сетями хранения данных (SAN). Можно настроить различные рабочие режимы (E, F или NP) для интерфейса FC, чтобы установить соединения с существующей или только что созданной FC SAN, таким образом организуя работу в сети.

Порт FC LAG

Порт FC LAG аналогичен порту L2 или L3 LAG. Порт FC LAG — это виртуальный логический порт, который связывает несколько физических портов FC, работающих в режиме E. Теоретически пропускная способность порта FC LAG равна сумме пропускной способности всех портов-участников. Таким образом, функция агрегирования FC может соответствовать требованиям к более высокой пропускной способности.

Обзор

Функция	Описание
Команды конфигурации интерфейса (Interface Configuration Commands)	Настройки, связанные с интерфейсом, можно настроить в режиме конфигурации интерфейса. При переходе в режим конфигурации несуществующего логического интерфейса будет создан новый интерфейс.
Описание интерфейса и административный статус (Interface	Можно настроить имя интерфейса для идентификации интерфейса и указания его отличительных функций. Также можно настроить состояние администрирования интерфейса.

Description and Administrative Status)	
MTU	Можно настроить максимальный размер передаваемого пакета (MTU) для порта, чтобы ограничить длину кадра, который может быть получен или отправлен через этот порт.
Полоса пропускания (Bandwidth)	Можно настроить полосу пропускания интерфейса.
Интервал нагрузки (Load Interval)	Можно указать интервал для расчета нагрузки на интерфейс.
Задержка при Административном отключении/ включении (Carrier Delay)	Можно настроить Задержку при Административном отключении/ включении (Carrier Delay) для интерфейса, чтобы настроить интервал, после которого состояние канала интерфейса изменяется с "опущен" на "поднят" и наоборот.
Политика канальных прерываний (Link Trap Policy)	На интерфейсе можно включить или отключить функцию канальных прерываний.
Сохранение индекса интерфейса (Interface Index Persistence) (Interface Index Persistence)	Можно включить функцию сохранения индекса интерфейса, чтобы индекс интерфейса оставался неизменным после перезапуска устройства.
Порт маршрутизации (Routed Port)	Физический порт на устройстве L3 можно настроить в качестве порта маршрутизации, который функционирует как интерфейс шлюза для коммутации L3.
Порт L3 LAG	Агрегированный порт на устройстве L3 можно настроить как порт L3 LAG, который функционирует как интерфейс шлюза для коммутации уровня L3.
Скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования(Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation	Можно настроить скорость, дуплексный режим, режим управления потоком и режим автоматического согласования интерфейса.

Mode)	
Автоматическое определение модуля (Automatic Module Detection)	Если скорость интерфейса установлена на auto, она может быть автоматически отрегулирована в зависимости от типа вставленного модуля.
Защищенный порт (Protected Port)	Некоторые порты можно настроить в качестве защищенных портов для отключения связи между этими портами. Можно также отключить маршрутизацию между защищенными портами.
Порт восстановления Errdisable (Port Errdisable Recovery) (Port Errdisable Recovery)	После завершения работы порта из-за нарушения безопасности можно запустить команду **errdisable recovery** в режиме глобальной конфигурации, чтобы восстановить все порты в состоянии errdisable, и затем включить эти порты.

1.3.1 Команды конфигурации интерфейса (Interface Configuration Commands)

Выполните команду **interface** в режиме глобальной конфигурации, чтобы войти в режим конфигурации интерфейса. Настройки, связанные с интерфейсом, можно настроить в режиме конфигурации интерфейса.

Принцип работы

Выполните команду **interface** в режиме глобальной конфигурации, чтобы войти в режим конфигурации интерфейса. При переходе в режим конфигурации несуществующего логического интерфейса будет создан новый интерфейс. Также можно выполнить команду **interface range** или **interface range macro** в режиме глобальной конфигурации для настройки диапазона (ID) интерфейсов. Интерфейсы, определенные в одном и том же диапазоне, должны быть одного типа и иметь одинаковые функции.

Для удаления указанного логического интерфейса можно выполнить команду **no interface** в режиме глобальной конфигурации.

Правила нумерации интерфейсов

В автономном режиме идентификатор физического порта состоит из двух частей: идентификатор слота и идентификатор порта в слоте. Например, если идентификатор слота порта 2, а идентификатор порта в слоте — 3, идентификатор интерфейса — 2/3. В режиме VSU или стека идентификатор физического порта состоит из трех частей: идентификатор устройства, идентификатор слота и идентификатор порта в слоте. Например, если идентификатор устройства — 1, идентификатор порта — 2, а идентификатор порта — 3, идентификатор интерфейса — 1/2/3.

Идентификатор устройства варьируется от 1 до максимального количества поддерживаемых устройств-участников.

Правила номеров слотов: Идентификатор статического слота — 0, а идентификатор динамического слота (подключаемого модуля или линейной карты) — от 1 до общего количества слотов. Предположим, что вы находитесь лицом к панели устройства. Динамические слоты пронумерованы от 1 последовательно слева направо и сверху вниз.

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

Идентификатор порта LAG варьируется от 1 до количества портов LAG, поддерживаемых устройством.

Идентификатор SVI — это VID определенной VLAN, соответствующий этому SVI.

Настройка интерфейсов в пределах диапазона

Вы можете запустить команду **interface range** в режиме глобальной конфигурации для одновременной настройки нескольких интерфейсов. Настройки, настроенные в режиме конфигурации интерфейса, применяются ко всем интерфейсам диапазона.

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

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

Диапазоны можно разделять запятыми (,).

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

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

Допустимы следующие форматы диапазона интерфейса:

- **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 агрегированного порта в диапазоне от 1 до максимального количества портов LAG, поддерживаемых устройством).
- **vlan** vlan-ID-vlan-ID (VLAN ID в диапазоне от 1 до 4094)
- **Loopback** loopback-ID (идентификатор loopback варьируется от 1 до 2147483647).
- **Tunnel** tunnel-ID (идентификатор туннеля варьируется от 0 до максимального количества интерфейсов туннеля, поддерживаемых устройством минус 1).

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

Настройка макросов диапазонов интерфейса

Можно определить макросы для замены диапазонов интерфейса. Прежде чем использовать параметр **macro** в команде **interface range**, необходимо сначала выполнить команду **define interface-range** в режиме глобальной конфигурации, чтобы определить эти макросы.

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

1.3.2 Описание интерфейса и административный статус (Interface Description and Administrative Status)

Можно настроить имя интерфейса для идентификации интерфейса и указания его отличительных функций.

Для включения или отключения интерфейса можно войти в режим конфигурации интерфейса.

Принцип работы

Описание интерфейса

Имя интерфейса можно настроить в соответствии с назначением интерфейса. Например, если вы хотите назначить GigabitEthernet 1/1 для исключительного управления пользователем A, вы можете описать интерфейс как "Порт для пользователя A".

Административный статус интерфейса

Можно настроить состояние администрирования интерфейса, чтобы отключить его при необходимости. Если интерфейс отключен, этот интерфейс не будет получать или отправлять кадры, и интерфейс потеряет все свои функции. Отключенный интерфейс можно включить, настроив состояние администрирования интерфейса. Определены два типа административного состояния канала интерфейса: Опущен и Поднят. Административный статус канала интерфейса - опущен, когда интерфейс отключен, и поднят, когда интерфейс включен.

1.3.3 MTU

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

Принцип работы

При обмене большим количеством данных через порт могут существовать кадры, превышающие стандартный кадр Ethernet. Этот тип кадра называется jumbo frame. MTU — это длина допустимого сегмента данных в кадре. Он не включает издержки инкапсуляции Ethernet.

Если порт получает или отправляет кадр с длиной больше MTU, этот кадр будет удален.

Размер MTU варьируется от 64 байт до 9216 байт с шагом в четыре байта. MTU по умолчанию составляет 1500 байт.

Команда **mtu** действует только на физический порт или порт LAG.

1.3.4 Полоса пропускания (Bandwidth)

Принцип работы

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

Команда **bandwidth** является параметром маршрутизации и не влияет на пропускную способность физического канала.

1.3.5 Интервал нагрузки

Принцип работы

Можно выполнить команду **load-interval**, чтобы указать интервал для расчета нагрузки интерфейса. Обычно интервал составляет 10 секунд.

1.3.6 Задержка при Административном отключении/ включении (Carrier Delay)

Принцип работы

Задержка при Административном отключении/ включении (Carrier Delay) относится к интервалу, после которого оператор связи определяет изменение состояния канала (DCD) из положения опущен в положение поднят. Если состояние DCD изменяется во время задержки, система проигнорирует это изменение, чтобы избежать согласования по пути восходящего потока канала данных. Если этот параметр имеет большое значение, почти каждое изменение DCD не обнаруживается. Напротив, если параметр установлен на 0, будет обнаружено каждое изменение сигнала DCD, что приведет к нестабильной работе.

Если оператор DCD прерывается на длительное время, для ускорения конвергенции топологии или маршрута необходимо задать меньшую Задержку при Административном отключении/ включении (Carrier Delay). Напротив, если время прерывания оператора DCD меньше времени конвергенции топологии или маршрута, то для Задержки при Административном отключении/ включении (Load Interval) необходимо задать большее значение, чтобы избежать перекрытия топологии или маршрута.

1.3.7 Политика канальных прерываний (Link Trap Policy)

На интерфейсе можно включить или отключить функцию канальных прерываний.

Принцип работы

Когда функция прерывания канала на интерфейсе включена, протокол SNMP отправляет оповещения о состоянии канала при изменении состояния канала в интерфейсе.

1.3.8 Сохранение индекса интерфейса (Interface Index Persistence)

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

Принцип работы

После включения сохранения индекса интерфейса, он остается неизменным после перезапуска устройства.

1.3.9 Порт маршрутизации

Принцип работы

Физический порт на устройстве L3 можно настроить как порт маршрутизации, который функционирует как интерфейс шлюза для коммутации L3. Порт маршрутизации (Routed Port) не может быть использован для коммутации L2. Можно выполнить команду **no switchport**, чтобы изменить порт коммутатора на Порт маршрутизации (Routed Port) и назначить IP-адрес этому порту для настройки маршрута. Обратите внимание, что перед выполнением команды **no switchport** необходимо удалить все функции L2 порта коммутатора.

1.3.10 Порт L3 LAG

Принцип работы

Как и с портом маршрутизации L3, можно выполнить команду **no switchport**, чтобы изменить порт L2 LAG на порт L3 LAG на устройстве L3, а затем назначить IP-адрес этому порту LAG для настройки маршрута. Обратите внимание, что перед выполнением команды **no switchport** необходимо удалить все функции L2 порта LAG.

Порт L2 LAG с одним или несколькими портами-участниками не может быть настроен как порт L3 LAG. Аналогично, порт L3 LAG с одним или несколькими портами-участниками не может быть изменен на порт L2 LAG.

1.3.11 Скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования (Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode)

Можно настроить Скорость интерфейса, дуплексный режим, режим управления потоком и режим автоматического согласования (Interface Speed, Duplex Mode, Flow Control Mode, and Auto Negotiation Mode) физического порта Ethernet или порта LAG.

Принцип работы

Скорость работы

Как правило, скорость физического порта Ethernet определяется путем согласования с одноранговым устройством. Согласованная скорость может быть любой скоростью в пределах возможностей интерфейса. Можно также настроить

любую скорость в пределах возможностей интерфейса для физического порта Ethernet.

При настройке скорости агрегированного порта конфигурация влияет на все порты, входящие в группу. (Все эти порты являются физическими портами Ethernet).

Дуплексный режим

- Дуплексный режим физического порта Ethernet или порта LAG можно настроить следующим образом:
- Установите дуплексный режим интерфейса на полнодуплексный, чтобы интерфейс мог принимать пакеты во время отправки других пакетов.
- Установите дуплексный режим интерфейса на полудуплексный, чтобы интерфейс мог принимать или отправлять пакеты в единицу времени.
- Установите дуплексный режим интерфейса на автоматическое согласование, чтобы дуплексный режим интерфейса определялся посредством автоматического согласования между локальным интерфейсом и одноранговым интерфейсом.
- При настройке дуплексного режима порта LAG конфигурация влияет на все порты, входящие в группу. (Все эти порты-участники являются физическими портами Ethernet).

Контроль потока данных

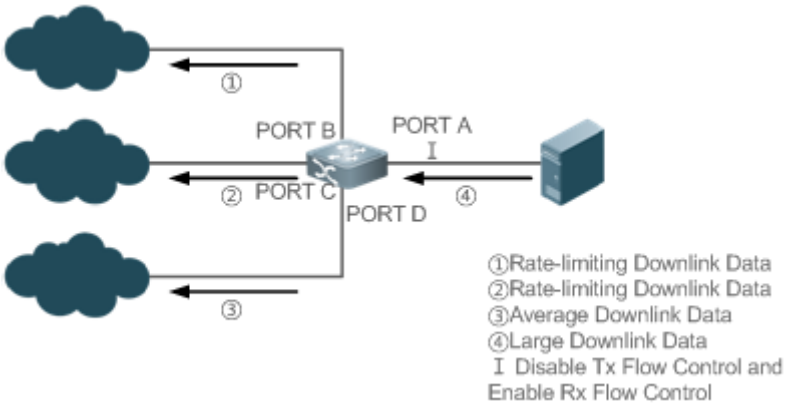
Для интерфейса определены два режима управления потоком:

- Режим симметричного управления потоком: Как правило, после включения управления потоком интерфейс обрабатывает полученные кадры управления потоком и отправляет кадры управления потоком при возникновении перегрузки на интерфейсе. Полученные и отправленные кадры управления потоком обрабатываются таким же образом. Это называется симметричным режимом управления потоком.
- Режим асимметричного управления потоком: в некоторых случаях интерфейс устройства должен обрабатывать полученные кадры управления потоком, чтобы гарантировать отсутствие отбрасываемых пакетов из-за перегрузки, а не отправлять кадры управления потоком во избежание 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.
- При настройке режима управления потоком порта LAG конфигурация влияет на все порты-участники. (Все эти порты-участники являются физическими портами Ethernet).

Как показано на Изображении 1-4, порт A устройства является портом восходящего канала, а порты B, C и D — портами нисходящего канала. Предположим, что порт A включен с функциями отправки и получения кадров управления потоком. Порты B и C подключены к разным медленным сетям. Если большое количество данных отправляется на порты B и C, порт B и порт C будут перегружены, и, следовательно, перегрузка происходит во входном направлении порта A, поэтому порт A отправляет кадры управления потоком. Когда устройство

выше по потоку реагирует на кадры управления потоком, оно уменьшает поток данных, отправляемых в порт A. Это косвенно снижает скорость сети на порту D. В это время можно отключить функцию отправки кадров управления потоком на порт A, чтобы обеспечить использование полосы пропускания всей сети.

Изображение 1-4



Режим автоматического согласования

- Режим автоматического согласования интерфейса может быть включен или выключен. Состояние автоматического согласования интерфейса не полностью эквивалентно режиму автоматического согласования. Состояние автоматического согласования интерфейса совместно определяется скоростью интерфейса, дуплексным режимом, режимом управления потоком и режимом автоматического согласования.
- При настройке режима автоматического согласования порта LAG конфигурация действует на все порты-участники. (Все эти порты-участники являются физическими портами Ethernet).

Как правило, если одно из следующих условий: скорость интерфейса, дуплексный режим и режим управления потоком установлены в автоматический режим или включен режим автоматического согласования интерфейса, то функция автоматического согласования интерфейса включена. Если ни одно из условий: скорость интерфейса, дуплексный режим и режим управления потоком не настроены на автоматический режим, а режим автоматического согласования интерфейса выключен, то функция автоматического согласования интерфейса отключена.

Для оптоволоконного порта 100Мбит/с функция автоматического согласования всегда отключена. Для гигабитного медного порта функция автоматического согласования всегда включена.

1.3.12 Автоматическое определение модуля

Если скорость интерфейса установлена на auto, она может быть автоматически отрегулирована в зависимости от типа вставленного модуля.

Принцип работы

В настоящее время функция автоматического обнаружения модулей может использоваться только для обнаружения модулей SFP и SFP+. SFP представляет собой гигабитный модуль, а SFP+ — 10-гигабитный модуль. Если установлен

модуль SFP, интерфейс работает в гигабитном режиме. Если установлен модуль SFP+, интерфейс работает в 10-гигабитном режиме.

Функция автоматического определения модуля действует только в том случае, если скорость интерфейса установлена на автоматический режим.

1.3.13 Защищенный порт (Protected Port)

В некоторых программных средах необходимо отключить связь между определенными портами. Для этого можно настроить данные порты в качестве защищенных. Можно также отключить маршрутизацию между защищенными портами.

Принцип работы

Защищенный порт (Protected Port)

После настройки портов в качестве защищенных, они не могут взаимодействовать друг с другом, но могут взаимодействовать с незащищенными портами.

Защищенные порты работают в любом из двух режимов. В первом режиме переключение на 2-й уровень блокируется, но маршрутизация между защищенными портами разрешена. Во втором режиме блокируется и переключение на 2-й уровень и маршрутизация на 2-м уровне между защищенными портами. Если Защищенный порт (Protected Port) поддерживает оба режима, первый режим используется по умолчанию.

Если два защищенных порта настроены как пара портов зеркалирования, кадры, отправленные или полученные исходным портом, могут быть зеркалированы на конечный порт.

В настоящее время в качестве защищенного порта можно настроить только физический порт Ethernet или агрегированный порт. Если агрегированный порт настроен как Защищенный порт (Protected Port), все его порты-участники настроены как защищенные порты.

Блокировка маршрутизации L3 между защищенными портами

По умолчанию маршрутизация L3 между защищенными портами не заблокирована. В этом случае можно запустить команду **protected-ports route-deny** для блокировки маршрутизации между защищенными портами.

1.3.14 Порт восстановления Errdisable (Port Errdisable Recovery) (Port Errdisable Recovery)

Некоторые протоколы поддерживают функцию восстановления errdisable для обеспечения безопасности и стабильности сети. Например, в протоколе безопасности порта при включении защиты порта и настройке максимального количества адресов безопасности на порту генерируется событие нарушения порта, если количество адресов, полученных на этом порте, превышает максимальное количество адресов безопасности. Другие протоколы, такие как протокол STP, DOT1X и REUP, поддерживают аналогичные функции, и при

нарушении безопасности порта, они автоматически отключаются для обеспечения безопасности.

Принцип работы

После завершения работы порта из-за нарушения безопасности можно запустить команду **errdisable recovery** в режиме глобальной конфигурации, чтобы восстановить все порты в состоянии errdisable, и затем включить эти порты. Можно вручную восстановить порт или автоматически восстановить порт в запланированное время.

1.3.15 Разделение и комбинация порта 40Гбит/с

Принцип работы

Порт Ethernet 40Гбит/с — это порт с высокой пропускной способностью. В основном он используется на устройствах на уровне конвергенции или на уровне ядра для увеличения пропускной способности порта. Разделение порта 40Гбит/с означает, что он разделяется на четыре порта 10Гбит/с. В это время порт 40Гбит/с становится недоступным, а четыре порта 10Гбит/с начинают пересылать данные независимо друг от друга. Комбинация порта 40Гбит/с означает, что четыре порта 10Гбит/с объединяются в порт 40Гбит/с. В это время четыре порта 10Гбит/с становятся недоступными, и только порт 40Гбит/с пересылает данные. Вы можете гибко регулировать пропускную способность, комбинируя или разделяя порты.

1.4 Конфигурация

Конфигурация	Описание и команда	
Выполнение базовых настроек	(Дополнительно) Используется для управления конфигурациями интерфейса, например, для создания/удаления интерфейса или настройки описания интерфейса.	
	Interface	Создает интерфейс и переходит в режим конфигурации созданного интерфейса или указанного интерфейса.
	interface range	Вводит диапазон интерфейса, создает эти интерфейсы (если они не созданы) и переходит в режим конфигурации интерфейса.
	define interface-range	Создает макрос для указания диапазона интерфейса.
	snmp-server if-index persist	Включает функцию сохранения индекса интерфейса, чтобы индекс интерфейса оставался неизменным после

		перезапуска устройства.
	description	Настраивает описание интерфейса длиной до 80 символов в режиме конфигурации интерфейса.
	snmp Trap link-status	Настраивает отправку сообщений-ловушек в канале интерфейса.
	Shutdown	Выключает интерфейс в режиме конфигурации интерфейса.
	split interface	Разделяет порт 40Гбит/с в режиме глобальной конфигурации.
Настройка **параметров** интерфейса	(Дополнительно) Используется для настройки **параметров** интерфейса.	
	Bandwidth	Настраивает полосу пропускания интерфейса в режиме конфигурации интерфейса.
	carrier-delay	Настраивает Задержку при Административном отключении/ включении (Carrier Delay) интерфейса в режиме конфигурации интерфейса.
	load-interval	Настраивает интервал для расчета нагрузки на интерфейс.
	duplex	Настраивает дуплексный режим интерфейса.
	flowcontrol	Включает или выключает управление потоком интерфейса.
	mtu	Настраивает MTU интерфейса.
	negotiation mode	Настраивает автоматический режим согласования интерфейса.
	speed	Настраивает скорость работы интерфейса.
	switchport	Настраивает интерфейс в качестве интерфейса L2 в режиме конфигурации интерфейса. (Выполните команду **no switchport**, чтобы настроить интерфейс в

		качестве интерфейса L3).
	switchport protected	Настраивает порт в качестве защищенного порта.
	protected-ports route-deny	Блокирует маршрутизацию L3 между защищенными портами в режиме глобальной конфигурации.
	errdisable recovery	Восстанавливает порт из состояния errdisable в режиме глобальной конфигурации.

1.4.1 Выполнение базовых настроек

Сценарий

- 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 перезапуска устройства.
- Настройте описание интерфейса таким образом, чтобы пользователи могли напрямую узнать информацию об интерфейсе.
- Включите или отключите функцию канальных прерываний на интерфейсе.
- Включите или отключите интерфейс.
- Разделите порт 40Гбит/с или объедините четыре порта 10Гбит/с в порт 40Гбит/с.

Примечания

- Для удаления указанного логического интерфейса или логических интерфейсов в указанном диапазоне можно использовать форму команды с **no**, но ее нельзя использовать для удаления физического порта или физических портов в указанном диапазоне.
- Форма команды **default** может использоваться в режиме конфигурации интерфейса для восстановления настроек по умолчанию указанного физического или логического интерфейса или интерфейсов в указанном диапазоне.

Этапы конфигурации

Настройка указанных интерфейсов

- Опционально.
- Выполните эту команду, чтобы создать логический интерфейс или войти в режим конфигурации физического порта или существующего логического интерфейса.

Команда	**interface** *interface-type interface-number*
Описание параметра	*interface-type interface-number*: Указывает тип и номер интерфейса. Интерфейс может быть физическим портом Ethernet, портом LAG, интерфейсом SVI или интерфейсом loopback.
Установки по умолчанию	Не доступны
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	❖ Если логический интерфейс еще не создан, выполните эту команду, чтобы создать данный интерфейс и войти в режим конфигурации этого интерфейса. ❖ Для физического порта или существующего логического интерфейса выполните эту команду, чтобы войти в режим конфигурации данного интерфейса. ❖ Используйте форму **no** команды для удаления указанного логического интерфейса. ❖ Используйте форму **default** команды для восстановления настроек интерфейса по умолчанию в режиме конфигурации интерфейса.

Настройка интерфейсов в пределах диапазона

❖ Опционально.
❖ Выполните 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 параметра	*port-range*: Указывает тип и диапазон идентификаторов интерфейсов. Такими интерфейсами могут быть физические порты Ethernet, порты LAG, SVI или интерфейсы loopback. *macro_name*: Указывает имя макроса диапазона интерфейсов.
Установки по умолчанию	Не доступны
Режим команды	Режим глобальной конфигурации

Встроенная подсказка	❖ Если логические интерфейсы еще не созданы, выполните эту команду, чтобы создать данные интерфейсы и войти в режим конфигурации интерфейса. ❖ Для нескольких физических портов или существующих логических интерфейсов выполните эту команду, чтобы войти в режим конфигурации интерфейса. ❖ Используйте форму **default** команды для восстановления настроек этих интерфейсов по умолчанию в режиме конфигурации интерфейса. ❖ Перед использованием макроса выполните 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.
❖ Выполните эту команду, если индексы интерфейса должны оставаться неизменными после перезапуска устройства.

Команда	**snmp-server if-index persist**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию Сохранение индекса интерфейса (Interface Index Persistence) отключено.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	После выполнения этой команды текущие индексы всех интерфейсов будут сохранены, а индексы останутся неизменными после перезапуска устройства. Для отключения функции сохранения индекса интерфейса можно использовать команду **no** или форму команды с **default**.

Настройка описания интерфейса

❖ Опционально.
❖ Выполните эту команду, чтобы настроить описание интерфейса.

Команда	**description** *string*
Описание	*string:* Указывает строку длиной до 80 символов.

параметра	
Установки по умолчанию	По умолчанию описание не настроено.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Выполните эту команду, чтобы настроить описание интерфейса. Для удаления описания интерфейса можно использовать команду **no** или форму команды с **default**.

Настройка функции Link Trap интерфейса

- ❖ Опционально.
- ❖ Выполните эту команду, чтобы получать канальные прерывания через SNMP.

Команда	**snmp Trap link-status**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию функция прерывания канала включена.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Эта команда используется для настройки функции прерывания канала в интерфейсе. Если эта функция включена, SNMP отправляет канальные прерывания, когда состояние канала изменяется в интерфейсе. Для отключения функции канальных прерываний можно использовать команду **no** или форму команды с **default**.

Настройка административного состояния интерфейса

- ❖ Опционально.
- ❖ Выполните эту команду, чтобы включить или отключить интерфейс.
- ❖ Интерфейс не может отправлять или принимать пакеты после отключения.

Команда	**Shutdown**
Описание	Недоступно

параметра	
Установки по умолчанию	По умолчанию канал интерфейса находится в состоянии «поднят».
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Можно запустить команду **shutdown**, чтобы отключить интерфейс, или команду **no shutdown**, чтобы включить интерфейс. В некоторых случаях, например, когда интерфейс находится в состоянии errdisable, невозможно выполнить команду **no shutdown** в интерфейсе. Для включения интерфейса можно использовать форму команды **no** или **default**.

Разделение порта 40Гбит/с или объединение четырех портов 10Гбит/с в порт 40Гбит/с.

- Опционально.
- Выполните эту команду, чтобы разделить порт 40Гбит/с или объединить четыре порта 10Гбит/с в порт 40Гбит/с.

Команда	**[no] split interface** *interface-type interface-number*
Описание параметра	*interface-type interface-number*: Указывает тип и номер интерфейса. Порт должен быть 40Гбит/с.
Установки по умолчанию	По умолчанию порты объединены.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Можно выполнить команду **split** для разделения порта 40Гбит/с или команду **no split** для объединения разделенного порта 40Гбит/с. После настройки этой команды вам, как правило, необходимо перезапустить линейную плату или все устройство, чтобы конфигурация могла быть запущена.

Проверка конфигурации

Настройка указанных интерфейсов

- Выполните команду **interface**. Если вы можете войти в режим конфигурации интерфейса, конфигурация выполнена успешно.
- Для логического интерфейса после выполнения команды **no interface** выполните команду **show running** или **show interfaces**, чтобы проверить, остался ли логический интерфейс.
- После выполнения команды **default interface** выполните команду **show running**, чтобы проверить, восстановились ли настройки по умолчанию для соответствующего интерфейса. Если да, операция выполнена успешно.

Настройка интерфейсов в пределах диапазона

- Выполните команду **interface range**. Если вы можете войти в режим конфигурации интерфейса, конфигурация выполнена успешно.
- После выполнения команды **default interface range** выполните команду **show running**, чтобы проверить, восстановились ли настройки по умолчанию для соответствующего интерфейса. Если да, операция выполнена успешно.

Настройка сохранения индекса интерфейса

- После запуска команды **snmp-server if-index persist** выполните команду записи для сохранения конфигурации, перезапустите устройство и выполните команду **show interface** для проверки индекса интерфейса. Если индекс интерфейса остается неизменным после перезапуска, активируется функция сохранения индекса интерфейса.

Настройка функции Link Trap интерфейса

- Извлеките и вставьте сетевой кабель в физический порт и включите сервер SNMP. Если сервер SNMP получает оповещения о соединении, функция оповещения о соединении включена.
- Запустите форму **no** команды **snmp Trap link-status**. Извлеките и вставьте сетевой кабель в физический порт. Если сервер SNMP не получает канальных прерываний, функция link Trap отключена.

Настройка административного состояния интерфейса

- Подключите сетевой кабель к физическому порту, включите порт и запустите команду **shutdown** на этом порту. Если на консоли отображается системный журнал, указывающий на то, что канал порта находится в состоянии «опущен», а индикатор порта выключен, то порт отключен. Запустите команду **show interfaces** и убедитесь, что состояние интерфейса изменилось на Administratively Down. Затем выполните команду **no shutdown**, чтобы включить порт. Если на консоли отображается системный журнал, указывающий на то, что канал порта находится в состоянии «поднят», а индикатор порта включен, то порт включен.

Разделение порта 40Гбит/с или объедините четырех портов 10Гбит/с в порт 40Гбит/с.

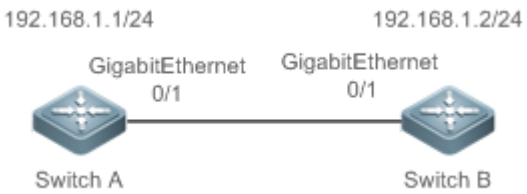
- Выполните команду **split** для порта 40Гбит/с в режиме глобальной конфигурации. Убедитесь, что соответствующий системный журнал отображается в консоли. Выполните команду **write**, чтобы сохранить конфигурацию, и перезапустите устройство или линейную карту в соответствии с методом, описанным в системном журнале. Запустите команду

show run и убедитесь, что сообщение "!merged to interface" больше не отображается в информации, относящейся к четырем портам 10Гбит/с, на которые разделен порт 40Гбит/с. Кроме того, четыре порта 10Гбит/с могут быть настроены как порты L2 или L3, но разделенный порт 40Гбит/с не может быть настроен как порт L2 или L3. Запустите команду **show run** и убедитесь, что сообщение "!splited into interface" отображается в информации, относящейся к порту 40Гбит/с.

- Выполните команду **no split** на разделенном порте 40Гбит/с. Убедитесь, что соответствующий системный журнал отображается в консоли. Выполните команду **write**, чтобы сохранить конфигурацию, и перезапустите устройство или линейную карту в соответствии с методом, описанным в системном журнале. Запустите команду **show run** и убедитесь, что сообщение "!merged to interface" отображается в информации, относящейся к четырем портам 10Гбит/с, объединенным в порт 40Гбит/с. Кроме того, четыре порта 10Гбит/с не могут быть настроены как порты L2 или L3, но комбинированный порт 40Гбит/с может быть настроен как порт L2 или L3.

Пример конфигурации

Настройка основных **параметров** интерфейсов

Сценарий Изображение 1-5	
Этапы конфигурации	❖ Подключите два устройства через порты коммутатора. ❖ Настройте SVI на двух устройствах и назначьте IP-адреса сегмента сети двум SVI. ❖ Включите Сохранение индекса интерфейса (Interface Index Persistence) на двух устройствах. ❖ Включите функцию канального прерывания 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 конфигурации	Выполните проверку коммутаторов A и B следующим образом: ❖ Запустите команду **shutdown** на порту GigabitEthern 0/1 и проверьте, не находится ли канал порта GigabitEthern 0/1 и SVI 1 в состоянии «опущен». ❖ Запустите команду **shutdown** на порту GigabitEthern 0/1 и проверьте, не отправлено ли прерывание, указывающее на то, что канал этого интерфейса «опущен». ❖ Перезапустите устройство и проверьте, совпадает ли индекс GigabitEthern 0/1 с индексом, который был установлен перед перезапуском.
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 00d0.f865.de9b (bia 00d0.f865.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 00d0.f822.33af (bia 00d0.f822.33af)
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 00d0.f865.de9b (bia 00d0.f865.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 00d0.f822.33af (bia 00d0.f822.33af)
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
```

1.4.2 Настройка атрибутов интерфейса

Сценарий

- Активируйте устройство для подключения и обмена данными с другими устройствами через порт коммутатора или порт маршрутизации.
- Настройте различные Настройки интерфейса на устройстве.

Этапы конфигурации

Настройка порта маршрутизации

- Опционально.
- Выполните эту команду, чтобы настроить порт в качестве порта маршрутизации L3.
- После настройки порта в качестве порта маршрутизации L3 протоколы L2, работающие на порту, не вступят в силу.
- Эта команда применима к порту коммутатора L2.

Команда	**no switchport**

Описание параметра	Недоступно
Установки по умолчанию	По умолчанию физический порт Ethernet является портом коммутатора L2.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	На устройстве L3 можно выполнить эту команду, чтобы настроить порт коммутатора L2 в качестве порта маршрутизации L3. Можно выполнить команду **switchport**, чтобы изменить Порт маршрутизации (Routed Port)L3 на порт коммутатора L2.

Конфигурирование порта L3 LAG

- Опционально.
- Выполните команду **no switchport** в режиме конфигурации интерфейса, чтобы настроить порт L2 LAG в качестве порта L3 LAG. Выполните команду **switchport**, чтобы настроить порт L3 LAG в качестве порта L2 LAG.
- После настройки порта в качестве порта маршрутизации L3 протоколы L2, работающие на порту, не будут работать.
- Эта команда применима к порту L2 LAG.

Команда	**no switchport**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию агрегированный порт является портом L2 LAG.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	После входа в режим конфигурации порта L2 LAG на устройстве L3 можно выполнить эту команду, чтобы настроить порт L2 LAG в качестве порта L3 LAG. После входа в режим конфигурации порта L3 LAG можно выполнить команду **switchport**, чтобы изменить порт L3 LAG на порт L2 LAG.

Настройка скорости интерфейса

- Опционально.

- При изменении настроенной скорости порта может произойти перекрывание портов.
- Эта команда применима к физическому порту Ethernet или порту LAG.

Команда	**speed** [**10** | **100** | **1000** | **10G** | **40G** | **auto**]
Описание параметра	**10**: Указывает, что скорость интерфейса составляет 10Мбит/с. **100**: Указывает, что скорость интерфейса составляет 100Мбит/с. **1000**: Указывает, что скорость интерфейса составляет 1000Мбит/с. **10G**: Указывает, что скорость интерфейса составляет 10Гбит/с. **auto**: Указывает, что скорость интерфейса автоматически адаптируется к фактическому состоянию.
Установки по умолчанию	По умолчанию выбор скорости интерфейса установлен на авто.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если интерфейс является портом-участником LAG, скорость этого интерфейса определяется скоростью агрегированного порта. Когда интерфейс выходит из порта LAG, он использует собственную настройку скорости. Можно запустить **show interfaces** для отображения конфигураций скорости. Параметры скорости, доступные для интерфейса, зависят от типа интерфейса. Например, нельзя установить скорость интерфейса SFP на 10Мбит/с. Скорость физического порта 40Гбит/с может быть установлена только на автоматический режим.

Настройка дуплексного режима интерфейса

- Опционально.
- При изменении настроенного дуплексного режима порта может произойти перекрывание портов.
- Эта команда применима к физическому порту Ethernet или порту LAG.

Команда	**duplex** { **auto** | **full** | **half** }
Описание параметра	**auto**: Указывает на автоматическое переключение между полнодуплексным и полудуплексным режимами. **full**: Обозначает полнодуплексный режим. **half**: Обозначает полудуплексный режим.

Установки по умолчанию	По умолчанию дуплексный режим интерфейса выбран как auto.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Дуплексный режим интерфейса связан с типом интерфейса. Можно запустить **show interfaces** для отображения конфигураций дуплексного режима.

Настройка режима управления потоком интерфейса

- Опционально.
- Обычно режим управления потоком интерфейса отключен по умолчанию. Для некоторых коммутаторов режим управления потоком включен по умолчанию.
- После включения управления потоком на интерфейсе кадры управления потоком будут отправлены или получены для регулировки объема данных при перегрузке интерфейса.
- При изменении настроенного режима управления потоком порта может произойти перекрывание портов.
- Эта команда применима к физическому порту Ethernet или порту LAG.

Команда	**flowcontrol** { **auto** | **off** | **on** | **receive** { **auto** | **off** | **on** } | **send** { **auto** | **off** | **on** } }
Описание параметра	**auto**: Указывает на автоматическое управление потоком. **off**: Указывает на то, что управление потоком отключено. **on**: Указывает на то, что управление потоком включено. **receive**: Указывает направление приема для управления асимметричным потоком. **send**: Указывает направление отправки для управления асимметричным потоком.
Установки по умолчанию	По умолчанию управление потоком отключено в интерфейсе.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Некоторые коммутаторы не могут управлять асимметричным потоком, поэтому не поддерживают ключевые слова **send** и **receive**. Можно запустить команду **show interfaces**, чтобы проверить, вступит ли

	конфигурация в силу.

Настройка режима автоматического согласования интерфейса

- Опционально.
- При изменении настроенного режима автоматического согласования порта может произойти перекрывание портов.
- Эта команда применима к физическому порту Ethernet или порту LAG.

Команда	**negotiation mode** { **on** | **off** }
Описание параметра	**on**: Указывает на то, что включен режим автоматического согласования. **off**: Указывает на то, что режим автоматического согласования выключен.
Установки по умолчанию	По умолчанию режим автоматического согласования выключен.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка MTU интерфейса

- Опционально.
- Можно 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 параметра	*num*: 64-9216
Установки по умолчанию	По умолчанию MTU интерфейса составляет 1500 байт.
Режим команды	Режим конфигурации интерфейса
Встроенная	Эта команда используется для настройки MTU интерфейса, то есть

подсказка	максимальной длины фрейма данных на уровне канала. В настоящее время MTU можно настроить только для физического порта или порта LAG, который содержит один или несколько портов-участников.

Настройка полосы пропускания интерфейса

- Опционально.
- Как правило, Полоса пропускания (Bandwidth) интерфейса совпадает со скоростью интерфейса.

Команда	**bandwidth** *kilobits*
Описание параметра	*kilobits*: Значение варьируется от 1 до максимальной скорости, которую могут поддерживать устройства QTECH. Единица измерения - килобиты.
Установки по умолчанию	Как правило, Полоса пропускания (Bandwidth) интерфейса соответствует типу интерфейса. Например, пропускная способность гигабитного физического порта Ethernet по умолчанию составляет 1000000, а физического порта 10Гбит/с Ethernet — 10000000.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка Задержки при Административном отключении/ включении (Load Interval) интерфейса

- Опционально.
- Если настроенная Задержка при Административном отключении/ включении (Carrier Delay) имеет большое значение, изменение состояния протокола занимает много времени при изменении физического состояния интерфейса. Если Задержка при Административном отключении/ включении (Carrier Delay) установлена на 0, состояние протокола изменяется сразу после изменения физического состояния интерфейса.

Команда	**carrier-delay {[milliseconds]** *num* **| up [milliseconds]** *num* **down [milliseconds]** *num***}**
Описание параметра	*num*: Диапазон значений от 0 до 60. Единица измерения - секунды. ***milliseconds***: Указывает Задержку при Административном отключении/ включении (Carrier Delay). Диапазон значений от 0 до 60 000. Единица измерения — миллисекунда. ***Up***: Указывает задержку, после которой состояние DCD изменяется с

	"опущен" на "поднят". ***Down***: Указывает задержку, после которой состояние DCD меняется с "поднят" на "опущен".
Установки по умолчанию	По умолчанию Задержка при Административном отключении/ включении (Carrier Delay) интерфейса составляет 2 сек.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если в качестве единицы используется миллисекунда, то настроенная Задержка при Административном отключении/ включении (Carrier Delay) должна быть целым числом, кратным 100 миллисекундам.

Настройка интервала нагрузки интерфейса

- Опционально.
- Настроенный интервал нагрузки влияет на вычисление средней скорости передачи пакетов в интерфейсе. Если настроенный интервал нагрузки короткий, средняя скорость передачи пакетов может точно отражать изменения трафика в реальном времени.

Команда	**load-interval** *seconds*
Описание параметра	*seconds*: Диапазон значений от 5 до 600. Единица измерения - секунды.
Установки по умолчанию	По умолчанию интервал нагрузки интерфейса составляет 10 сек.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка защищенного порта

- Опционально.
- Пакеты L2 не могут быть переданы между защищенными портами.
- Эта команда применима к физическому порту Ethernet или порту LAG.

Команда	**switchport protected**

Описание параметра	Недоступно
Установки по умолчанию	По умолчанию Защищенный порт (Protected Port) не настроен.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Блокировка маршрутизации L3 между защищенными портами

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

Команда	**protected-ports route-deny**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию функция блокировки маршрутизации L3 между защищенными портами отключена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	По умолчанию маршрутизация L3 между защищенными портами не заблокирована. В этом случае можно выполнить данную команду, чтобы заблокировать маршрутизацию между защищенными портами.

Настройка восстановления порта после Errdisable

- Опционально.
- По умолчанию порт будет отключен и не будет восстановлен после нарушения безопасности. После настройки восстановления состояния errdisable порта, он будет восстановлен и включен.

Команда	**errdisable recovery [interval** *time***]**
Описание	*time*: Указывает время автоматического восстановления. Диапазон

параметра	значений от 30 до 86400. Единица измерения - секунды.
Установки по умолчанию	По умолчанию восстановление при состоянии errdisable порта отключено.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	По умолчанию порт в состоянии errdisable не восстанавливается. Можно восстановить порт вручную или выполнить эту команду для автоматического восстановления порта.

Включение статистики пакетов в SVI

- Опционально.
- По умолчанию статистика пакетов отключена в SVI. Вы можете запустить эту команду, чтобы включить статистику, когда она была отключена. Сброс счетчика пакетов на ноль также поддерживается в SVI.

Команда	**route-statistics enable**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию статистика пакетов в SVI отключена.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Списки ACL используются, когда эта функция включена. Если ACL-списки полностью доступны, статистику пакетов можно выполнить на 512 SVI. Если нет, то максимальное число SVI, где можно применить статистику пакетов, уменьшается.

Проверка конфигурации

- Запустите команду **show interfaces** для отображения конфигураций **параметров** интерфейсов.

Команда	**show interfaces** [*interface-type interface-number*] [**description | switchport | trunk**]

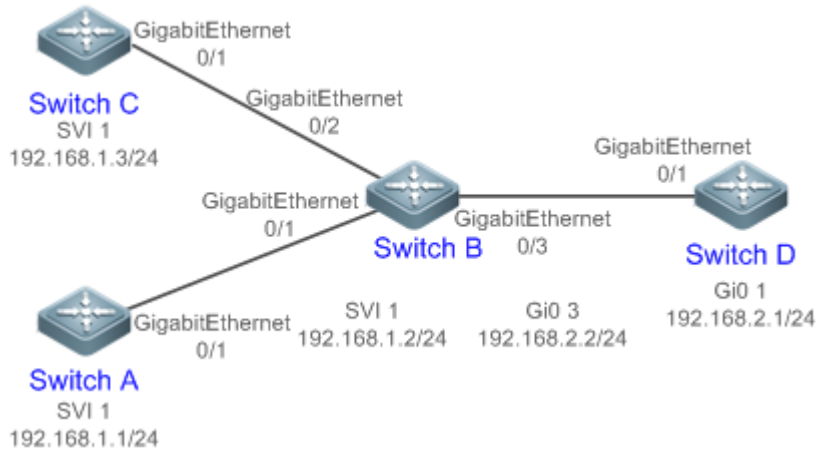
Описание параметра	*interface-type interface-number*: Указывает тип и номер интерфейса. description: Указывает описание интерфейса, включая состояние соединения. switchport: Отображает информацию интерфейса L2. Этот параметр применяется только для интерфейса L2. trunk: Указывает информацию о магистральном порте. Этот параметр эффективен для физического порта или порта LAG.
Режим команды	Привилегированный EXEC режим
Встроенная подсказка	Используйте эту команду без какого-либо параметра 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 00d0.f865.de9b (bia 00d0.f865.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 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)
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  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
SwitchA#show interface vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP  , line protocol is UP
  Hardware is VLAN, address is 5869.6c9d.b309 (bia 5869.6c9d.b309)
  Interface address is: no ip address
  ARP type: ARPA, ARP Timeout: 3600 seconds
  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
  Rxload is 1/255, Txload is 1/255
  VLAN attributes:
    Last link state change time: 14.10.2019 9:46:01
    Time duration since last link state change: 0 days, 21 hours,
36 minutes,  6 seconds
   10 seconds input rate 65 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
   Input l3 packets              0                        Input l3
bytes              0
   Input l3 multicasts packets   0                        Input l3
multicasts bytes   0
   Input broadcasts packets      0                          Input
```

	broadcasts bytes 0 Output l3 packets 0 Output l3 bytes 0 Output l3 multicasts packets 0 Output l3 multicasts bytes 0

Пример конфигурации

Настройка **параметров** интерфейса

Сценарий Изображение 1-1	
Этапы конфигурации	❖ На коммутаторе A настройте GigabitEthernet 0/1 с режимом доступа, и VLAN ID по умолчанию — 1. Настройте SVI 1, назначьте IP-адрес на SVI 1 и настройте маршрут к коммутатору D. ❖ На коммутаторе B настройте порты GigabitEthernet 0/1 и GigabitEthernet 0/2 в качестве магистральных портов, и VLAN ID по умолчанию — 1. Настройте SVI 1 и назначьте IP-адрес SVI 1. Настройте GigabitEthernet 0/3 как маршрутизируемые порты и назначьте IP-адрес из другого сегмента сети этому порту. ❖ На коммутаторе C настройте GigabitEthernet 0/1 в качестве порта доступа и VLAN ID по умолчанию — 1. Настройте SVI 1 и назначьте IP-адрес SVI 1. ❖ На коммутаторе D настройте GigabitEthernet 0/1 в качестве маршрутизируемого порта, назначьте IP-адрес этому порту 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 конфигурации	Выполните проверку коммутаторов A, B, C и D следующим образом: ❖ На коммутаторе A отправьте эхо-запрос на IP-адреса интерфейсов трех других коммутаторов. Убедитесь, что вы можете получить доступ к трем другим коммутаторам на коммутаторе A. ❖ Убедитесь, что коммутаторы B и D могут обмениваться эхо-запросами. ❖ Убедитесь, что состояние интерфейса правильное.
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 00d0.f865.de90 (bia 00d0.f865.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: 22.12.2012 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 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 00d0.f865.de91 (bia 00d0.f865.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: 22.12.2012 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 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 00d0.f865.de92 (bia 00d0.f865.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: 22.12.2012 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 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 00d0.f865.de93 (bia 00d0.f865.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: 22.12.2012 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50
minutes, 50 seconds
    Priority is 0

    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
```

1.5 Мониторинг

Очистка

⚠ Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	Команда
Очищает счетчики указанного интерфейса.	**clear counters** [*interface-type interface-number*]
Сбрасывает аппаратную платформу интерфейса.	**clear interface** *interface-type interface-number*

Отображение

Отображение конфигураций и состояния интерфейса

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 состояние errdisable интерфейса.	**show interfaces** [*interface-type interface-number*] **status err-disable**
Отображает время изменения состояния канала и счетчик указанного порта.	**show interfaces** [*interface-type interface-number*] **link-state-change statistics**
Отображает административные и рабочие состояния портов коммутатора (немаршрутизируемые порты).	**show interfaces** [*interface-type interface-number*] **switchport**
Отображает описание и состояние указанного интерфейса.	**show interfaces** [*interface-type interface-number*] **description**
Показывает счетчики указанного порта, среди которых скорость отображения может иметь погрешность ±0,5%.	**show interfaces** [*interface-type interface-number*] **counters**
Отображает прирост пакетов за интервал нагрузки.	**show interfaces** [*interface-type interface-number*] **counters increment**
Отображает статистику по пакетам ошибок.	**show interfaces** [*interface-type interface-number*] **counters error**
Отображает скорость передачи/приема пакетов интерфейса.	**show interfaces** [*interface-type interface-number*] **counters rate**
Отображает сводную информацию об интерфейсе.	**show interfaces** [*interface-type interface-number*] **counters summary**
Отображает использование полосы пропускания интерфейса.	**show interfaces** [*interface-type interface-number*] **usage**

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 неисправности оптического модуля на определенном интерфейсе. Если неисправность не обнаружена, отображается сообщение "None" (Нет).	**show interfaces** [*interface-type interface-number*] **transceiver alarm**
Отображает диагностические значения оптического модуля для указанного интерфейса.	**show interfaces** [*interface-type interface-number*] **transceiver diagnosis**

2 КОНФИГУРИРОВАНИЕ MAC-АДРЕСА

2.1 Обзор

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

Когда устройство пересылает пакет, оно находит выходной порт из таблицы MAC в соответствии с MAC-адресом назначения и идентификатором VLAN пакета.

После этого пакет является одноадресным, многоадресным или широковещательным.

В этом документе рассматриваются динамические MAC-адреса, статические MAC-адреса и отфильтрованные MAC-адреса. Для управления MAC-адресами многоадресной рассылки см. раздел *Настройка конфигурации отслеживания IGMP*.

Протоколы и стандарты

- IEEE 802.3: Множественный доступ с поддержкой распознавания несущей (CSMA/CD) с использованием метода обнаружения столкновений и характеристики физического уровня
- IEEE 802.1Q: Виртуальные коммутируемые локальные сети

2.2 Применение

Применение	Описание
Изучение MAC-адресов	Пересылка одноадресных пакетов через Изучение MAC-адресов.
Уведомление об изменении MAC-адреса	Отслеживайте смену устройств, подключенных к коммутатору, с помощью уведомления об изменении MAC-адреса.

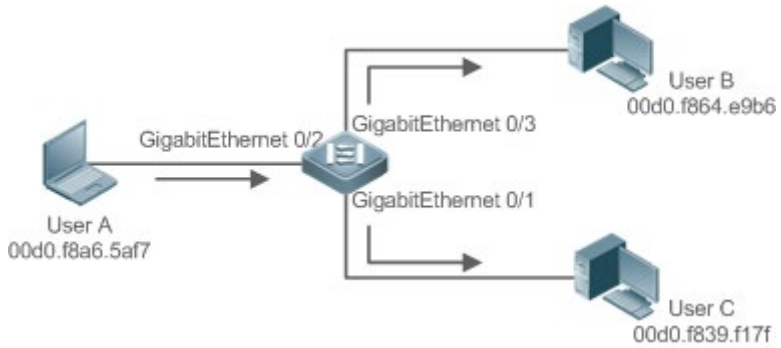
2.2.1 Изучение MAC-адресов

Сценарий

Обычно устройство поддерживает таблицу MAC, динамически обучаясь MAC-адресам. Принцип работы описан ниже:

Как показано на следующем Изображении, таблица MAC-адресов коммутатора не заполнена. Когда пользователь A обменивается данными с пользователем B, он отправляет пакет на порт GigabitEthernet 0/2 коммутатора, который обучается MAC-адресу пользователя A, и затем сохраняет его в таблице. Поскольку в таблице не содержится MAC-адрес пользователя B, коммутатор передает пакет на порты всех подключенных устройств, кроме пользователя A, включая пользователя B и пользователя C.

Изображение 2-1 Этап 1 обучения MAC-адресу

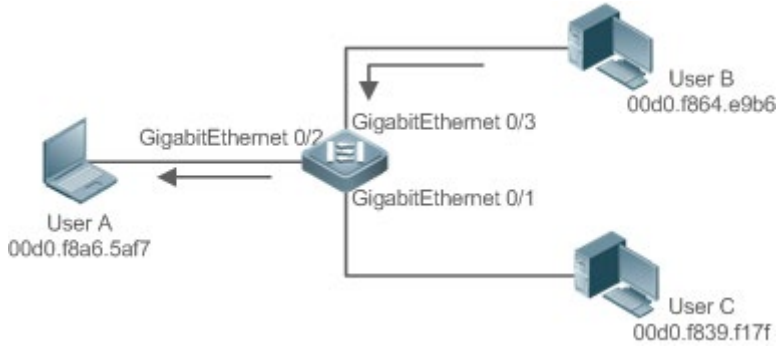


Изображение 2-2 Таблица 1 MAC-адресов

Статус	VLAN	MAC-адрес	Интерфейс
Динамический	1	00d0.f8a6.5af7	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 указан в таблице MAC-адресов, коммутатор отправляет одноадресный пакет ответа на порт GigabitEthernet 0/2 и обучается MAC-адресу пользователя B. Пользователь C не получает ответный пакет от пользователя B к пользователю A.

Изображение 2-3 Этап 2 обучения MAC-адресу



Изображение 2-4 Таблица 2 MAC-адреса

Статус	VLAN	MAC-адрес	Интерфейс
Динамический	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Динамический	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

При взаимодействии между пользователем A и пользователем B коммутатор обучается MAC-адресам пользователя A и пользователя B. После этого пакеты между пользователем A и пользователем B будут обмениваться через одноадресную рассылку без получения пользователем C.

Описание

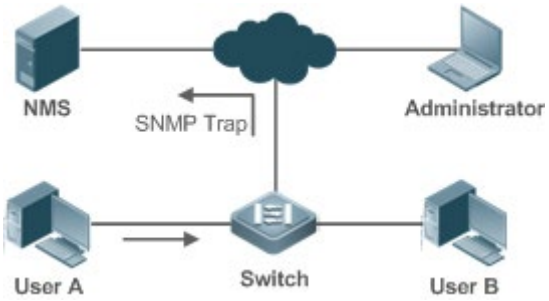
- При обучении MAC-адресам коммутатор 2-го уровня пересылает пакеты через одноадресную рассылку, уменьшая количество широковещательных пакетов и нагрузку на сеть.

2.2.2 Уведомление об изменении MAC-адреса

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

Сценарий

Изображение 2-5 Уведомление об изменении MAC-адреса



После того, как на устройстве включено уведомление об изменении MAC-адреса, оно генерирует уведомление, когда обучается новому MAC-адресу или ставит статус «устаревший» уже обученному MAC-адресу, и отправляет сообщение-ловушку SNMP указанной NMS.

Уведомление о добавлении MAC-адреса означает, что новый пользователь получает доступ к сети, а уведомление об удалении MAC-адреса означает, что пользователь не отправил пакеты в течение срока устаревания, и обычно после этого пользователь выходит из сети.

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

При создании данное уведомление сохраняется в хронологической таблице уведомлений об изменении MAC-адреса. Администратор может узнать последние изменения MAC-адресов, проверив таблицу истории уведомлений даже без NMS.

Уведомление об изменении MAC-адреса создается только для динамического MAC-адреса.

Описание

- Включите уведомление об изменении MAC-адреса на коммутаторе 2-го уровня для отслеживания изменений устройств, подключенных к сетевому устройству.

2.3 Функции

Базовые концепции

Динамический MAC-адрес

Динамический MAC-адрес — это запись MAC-адреса, созданная в процессе обучения устройства MAC-адресу.

Устаревание адреса

Устройство запоминает только ограниченное количество MAC-адресов, а неактивные записи удаляются путем устаревания.

Устройство начинает процесс устаревания MAC-адреса при его получении. Если устройство не получает пакет, содержащий MAC-адрес источника, то по истечении этого времени MAC-адрес будет удален из таблицы MAC.

Пересылка через Unicast

- Если устройство находит в своей таблице MAC запись, содержащую MAC-адрес и идентификатор VLAN пакета, и выходной порт является уникальным, оно отправит пакет напрямую через порт.

Передача посредством широковещательной рассылки

- Если устройство получает пакет с адресом назначения ffff.ffff.ffff или неидентифицированным адресом назначения, оно отправит пакет через все порты в VLAN, откуда поступает пакет, за исключением входного порта.

Обзор

Функция	Описание
Ограничение динамических адресов для VLAN	Ограничение количества динамических MAC-адресов в сети VLAN.
Ограничение динамических адресов для интерфейса	Ограничение количества динамических MAC-адресов интерфейса.

2.3.1 Ограничение динамических адресов для VLAN

Принцип работы

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

VLAN может обучиться ограниченному количеству динамических MAC-адресов только после настройки определенного предела. Пакеты, превышающие этот лимит, передаются через широковещательную рассылку.

Если количество MAC-адресов, обученных в интерфейсе, превышает предельное значение, устройство прекратит Изучение MAC-адресов из VLAN и не начнет обучение снова до тех пор, пока число не опустится ниже предельного значения после устаревания других адресов.

На MAC-адреса, скопированные в определенную VLAN, ограничение не распространяется.

2.3.2 Ограничение динамических адресов для интерфейса

Принцип работы

Интерфейс может обучиться ограниченному количеству динамических MAC-адресов только после настройки определенного предела. Пакеты, превышающие этот лимит, передаются через широковещательную рассылку

Если количество MAC-адресов, обученных в интерфейсе, превышает предельное значение, устройство прекратит Изучение MAC-адресов в интерфейсе и не начнет обучение снова до тех пор, пока число не опустится ниже предельного значения после устаревания других адресов.

2.4 Конфигурация

Конфигурация	Описание и команда	
Настройка динамического MAC-адреса	(Дополнительно) Данная команда используется для включения функции обучения MAC-адресам.	
	mac-address-learning	Настраивает Изучение MAC-адресов глобально или через интерфейс.
	mac-address-table aging-time	Настраивает время старения для динамического MAC-адреса.
Настройка статического MAC-адреса	(Дополнительно) Используется для привязки MAC-адреса устройства к порту коммутатора.	
	mac-address-table static	Настраивает статический MAC-адрес.
Настройка MAC-адреса для фильтрации пакетов	(Дополнительно) Используется для фильтрации пакетов.	
	mac-address-table filtering	Настраивает MAC-адрес для фильтрации пакетов.
Настройка	(Дополнительно) Используется для мониторинга смены устройств,	

уведомления об изменении MAC-адреса	подключенных к сетевому устройству.	
	mac-address-table notification	Глобально настраивает уведомление об изменении MAC-адреса.
	snmp Trap mac-notification	Настраивает уведомление об изменении MAC-адреса на интерфейсе.
Настройка управляющей VLAN для порта LAG	⚠ (Дополнительно) Используется для настройки управляющей VLAN для порта LAG.	
	aggregateport-admin vlan	Настраивает управляющую VLAN для агрегированного порта.

2.4.1 Настройка динамического MAC-адреса

Сценарий

Динамическое Изучение MAC-адресов и передача пакетов через одноадресную рассылку.

Этапы конфигурации

Настройка глобальному обучению MAC-адресам

- Опционально.
- Эту конфигурацию можно выполнить, чтобы отключить глобальное Изучение MAC-адресов.
- Конфигурация:

Команда	**mac-address-learning** { **enable** | **disable** }
Описание параметра	**enable**: Включает глобальное Изучение MAC-адресов. **disable**: Отключает глобальное Изучение MAC-адресов.
Установки по умолчанию	Глобальное Изучение MAC-адресов включено по умолчанию.
Режим команды	Режим глобальной конфигурации
Встроенная	Недоступно

подсказка	

По умолчанию включено глобальное Изучение MAC-адресов. Если включено глобальное Изучение MAC-адресов, то на интерфейсе будет действовать конфигурация обучения MAC-адресам; если функция отключена, MAC-адресам невозможно обучиться глобально.

Настройка обучения MAC-адресам в интерфейсе

- Опционально.
- Эту конфигурацию можно выполнить, чтобы отключить Изучение MAC-адресов в интерфейсе.
- Конфигурация:

Команда	**mac-address-learning**
Описание параметра	Недоступно
Установки по умолчанию	Изучение MAC-адресов включено по умолчанию.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Выполните эту настройку на интерфейсе уровня 2, например, на порту коммутатора или на агрегированном порте.

По умолчанию Изучение MAC-адресов включено. Если на порту настроена функция DOT1X, IP SOURCE GUARD или функция безопасности порта, Изучение MAC-адресов не может быть включено. Управление доступом не может быть включено на порту с отключенным обучением MAC-адресам.

Настройка времени старения для динамического MAC-адреса

- Опционально.
- Настраивает время старения для динамического MAC-адреса.
- Конфигурация:

Команда	**mac-address-table aging-time** *value*
Описание параметра	*value*: Указывает время старения. Значение равно 0 или находится в диапазоне от 10 до 1000000.
Установки по	Значение по умолчанию — 300 сек.

умолчанию	
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если установлено значение 0, то устаревание MAC-адресов отключается, и полученные MAC-адреса никогда не устареют.

Фактическое время старения может отличаться от настроенного значения, но не более, чем в два раза от настроенного значения.

Проверка конфигурации

- 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 старения динамических MAC-адресов.

Команда	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Описание параметра	**address** *mac-address*: Отображает информацию о конкретном динамическом MAC-адресе. **interface** *interface-id*: Указывает физический интерфейс или порт LAG. **vlan** *vlan-id*: Отображает динамические MAC-адреса в определенной VLAN.
Режим команды	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
	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 Address	Указывает MAC-адрес.
Type	Указывает тип MAC-адреса.
Интерфейс	Указывает интерфейс, в котором находится MAC-адрес.

Команда	**show mac-address-table aging-time**
Описание параметра	Недоступно
Режим команды	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
	`QTECH# show mac-address-table aging-time` `Aging time : 300`

Пример конфигурации

Настройка динамического MAC-адреса

Сценарий Изображение 2-6	
Этапы конфигурации	❖ Включите Изучение MAC-адресов в интерфейсе. ❖ Настройте время устаревания динамических MAC-адресов на 180 сек. ❖ 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 конфигурации	❖ Проверьте обучение MAC-адресу в интерфейсе. ❖ Отображает время старения динамических MAC-адресов. ❖ Отображает 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 00d0.f800.1001 STATIC GigabitEthernet 1/1**

Типичные ошибки

Настройте Изучение MAC-адресов в интерфейсе перед настройкой интерфейса в качестве интерфейса уровня 2, например, порта коммутатора или порта LAG.

2.4.2 Настройка статического MAC-адреса

Сценарий

❖ Привяжите MAC-адрес сетевого устройства к порту коммутатора.

Этапы конфигурации

Настройка статического MAC-адреса

❖ Опционально.
❖ Привяжите MAC-адрес сетевого устройства к порту коммутатора.
❖ Конфигурация:

Команда	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*
Описание параметра	**address** *mac-address*: Указывает MAC-адрес. **vlan** *vlan-id*: Указывает VLAN, в которой находится MAC-адрес.

	interface *interface-id*: Указывает физический интерфейс или порт LAG.
Установки по умолчанию	По умолчанию статический MAC-адрес не настроен.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Когда коммутатор получает пакет, содержащий указанный MAC-адрес в указанной VLAN, пакет пересылается на привязанный интерфейс.

Проверка конфигурации

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

Команда	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Описание параметра	**address** *mac-address*: Указывает MAC-адрес. **interface** *interface-id*: Указывает физический интерфейс или порт LAG. **vlan** *vlan-id*: Указывает VLAN, в которой находится MAC-адрес.
Режим команды	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
	QTECH# show mac-address-table static Vlan MAC Address Type Interface ----- ----------- -------- ------------------ 1 00d0.f800.1001 STATIC GigabitEthernet 1/1 1 00d0.f800.1002 STATIC GigabitEthernet 1/1 1 00d0.f800.1003 STATIC GigabitEthernet 1/1

Пример конфигурации

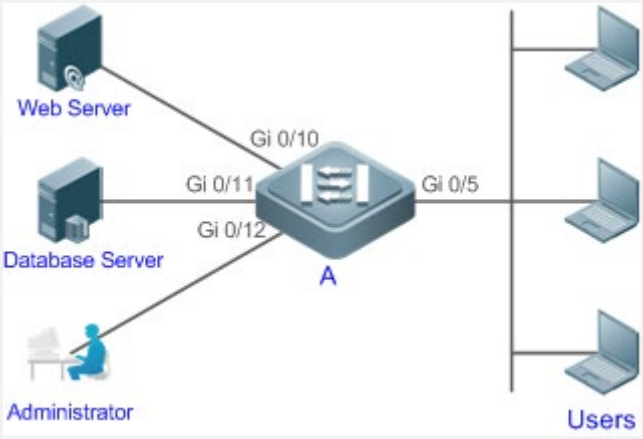
Настройка статического MAC-адреса

В приведенном выше примере соотношение MAC-адресов, VLAN и интерфейсов показано в следующей таблице.

Роль	Mac-адрес	Идентификатор VLAN	Идентификатор интерфейса
Веб-сервер	00d0.3232.0001	VLAN2	Gi0/10
Сервер базы данных	00d0.3232.0002	VLAN2	Gi0/11
Администратор	00d0.3232.1000	VLAN2	Gi0/12

Сценарий

Изображение 2-7



Этапы конфигурации

- Укажите MAC-адреса назначения (*mac-address*).
- Укажите VLAN (*vlan-id*), в которой находятся MAC-адреса.
- Укажите идентификаторы интерфейса (*interface-id*).

A

```
A# configure terminal
A(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2
interface gigabitEthernet 0/10
A(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2
interface gigabitEthernet 0/11
A(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2
interface gigabitEthernet 0/12
```

Проверка конфигурации

Отображение конфигурации статического MAC-адреса на коммутаторе.

A

```
A# show mac-address-table static
Vlan        MAC Address          Type     Interface
----------  -------------------- -------- --------------------
```

	2 00d0.f800.3232.0001 STATIC GigabitEthernet 0/10 2 00d0.f800.3232.0002 STATIC GigabitEthernet 0/11 2 00d0.f800.3232.1000 STATIC GigabitEthernet 0/12

Типичные ошибки

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

2.4.3 Настройка MAC-адреса для фильтрации пакетов

Сценарий

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

Этапы конфигурации

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 параметра	**address** *mac-address*: Указывает MAC-адрес. **vlan** *vlan-id*: Указывает VLAN, в которой находится MAC-адрес.
Установки по умолчанию	По умолчанию фильтрация MAC-адресов не настроена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если устройство получает пакеты, содержащие MAC-адрес источника или MAC-адрес назначения, указанный в качестве отфильтрованного MAC-адреса, пакеты отбрасываются.

Проверка конфигурации

- Запустите команду **show mac-address-table filter** для отображения отфильтрованного MAC-адреса.

Команда	**show mac-address-table filter** [**address** *mac-address*] [**vlan** *vlan-id*]
Описание	**address** *mac-address*: Указывает MAC-адрес.

параметра	**vlan** *vlan-id*: Указывает VLAN, в которой находится MAC-адрес.
Режим команды	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
	QTECH# show mac-address-table filtering Vlan MAC Address Type Interface ------ ------------------ -------- ----------- **1 0000.2222.2222 FILTER**

Пример конфигурации

Настройка MAC-адреса для фильтрации пакетов

Этапы конфигурации	❖ Укажите MAC-адрес назначения (*mac-address*) для фильтрации. ❖ Укажите VLAN, в которой находятся MAC-адреса.
	QTECH# configure terminal QTECH(config)# mac-address-table static 00d0.f800.3232.0001 vlan 1
Проверка конфигурации	Отобразите конфигурацию фильтрации MAC-адресов.
	QTECH# show mac-address-table filter Vlan MAC Address Type Interface ---------- ------------------ -------- ------------------ **1 00d0.f800.3232.0001 FILTER**

2.4.4 Настройка уведомления об изменении MAC-адреса

Сценарий

❖ Мониторинг смены устройств, подключенных к сетевому устройству.

Этапы конфигурации

Конфигурирование NMS

❖ Опционально.
❖ Выполните эту настройку, чтобы система NMS получала уведомления об изменении MAC-адреса.
❖ Конфигурация:

Команда	**snmp-server host** *host-addr* **Traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*
Описание параметра	**host** *host-addr*: Указывает IP-адрес получателя. **version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: Указывает версию сообщений SNMP TRAP. Можно также указать проверку подлинности и уровень безопасности для пакетов версии 3. *community-string*: Указывает имя для аутентификации.
Установки по умолчанию	По умолчанию функция отключена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Включение SNMP Trap

- Опционально.
- Выполните эту настройку, чтобы отправлять SNMP Trap сообщения.
- Конфигурация:

Команда	**snmp-server enable Traps**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию функция отключена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Настройка уведомления об изменении MAC-адреса глобально

- Опционально.
- Если уведомление об изменении MAC-адреса отключено глобально, оно отключается во всех интерфейсах.

❖ Конфигурация:

Команда	**mac-address-table notification**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию уведомление об изменении MAC-адреса отключено глобально.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Настройка уведомления об изменении MAC-адреса в интерфейсе

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

Команда	**snmp Trap mac-notification** { **added** | **removed** }
Описание параметра	**added**: Создает уведомление при добавлении MAC-адреса. **removed**: Создает уведомление при удалении MAC-адреса.
Установки по умолчанию	По умолчанию уведомление об изменении MAC-адреса отключено в интерфейсе.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка интервала для создания уведомлений об изменении MAC-адреса и объема истории уведомлений

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

Команда	**mac-address-table notification** { **interval** *value* | **history-size** *value* }
Описание параметра	**interval** *value*: (Дополнительно) Указывает интервал создания уведомлений об изменении MAC-адреса. Диапазон значений от 1 до 3600 секунд. **history-size** *value*: Указывает максимальное количество записей в таблице журнала уведомлений. Диапазон значений от 1 до 200.
Установки по умолчанию	Интервал по умолчанию составляет 1 секунду. Максимальное количество уведомлений по умолчанию — 50.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Проверка конфигурации

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

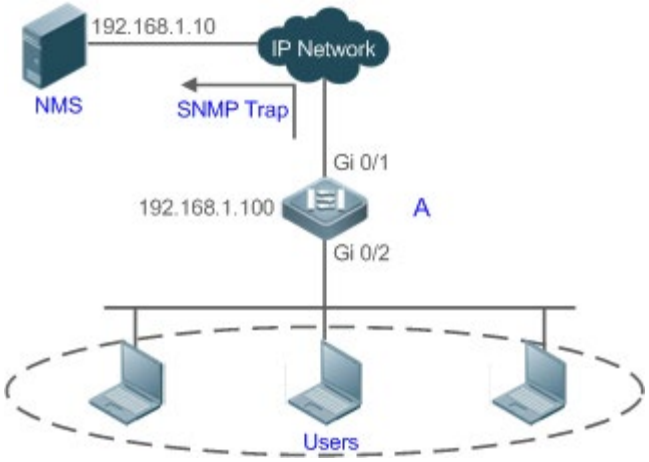
Команда	**show mac-address-table notification** [**interface** [*interface-id*] | **history**]
Описание параметра	**Interface**: отображает конфигурацию уведомления об изменении MAC-адреса во всех интерфейсах. *interface-id*: Отображает конфигурацию уведомления об изменении MAC-адреса в указанном интерфейсе. **history**: Отображает историю уведомлений об изменении MAC-адреса.
Режим команды	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Встроенная подсказка	Отображение конфигурации уведомления об изменении MAC-адреса глобально.
	`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 создания уведомлений об изменении MAC-адреса.
Maximum History Size	Указывает максимальное количество записей в таблице журнала уведомлений.
Current History Size	Указывает текущее количество записей уведомления.

Пример конфигурации

Сценарий Изображение 2-8	 На Изображении показана интрасеть предприятия. Пользователи подключаются к A через порт Gi0/2. Выполните настройку для получения следующих результатов: ❖ Когда порт Gi0/2 запоминает новый MAC-адрес или завершает устаревание обученного MAC-адреса, генерируется уведомление об изменении MAC-адреса. ❖ В то же время A отправляет уведомление об изменении MAC-адреса в сообщении SNMP Trap в указанную NMS. ❖ В случае, если устройство A подключено к нескольким пользователям, конфигурация может предотвратить прирост количества сообщений уведомления об изменении MAC-адреса, чтобы уменьшить сетевой поток.
Этапы	❖ Включите уведомление об изменении MAC-адреса глобально на A и

конфигурации	настройте уведомление об изменении MAC-адреса на порту Gi0/2. ❖ Настройте IP-адрес хоста NMS и включите A на отправку SNMP Trap. A обменивается данными с NMS посредством маршрутизации. ❖ 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 конфигурации	❖ Проверьте, включено ли уведомление об изменении MAC-адреса глобально. ❖ Проверьте, включено ли в интерфейсе уведомление об изменении MAC-адреса. ❖ Отобразите MAC-адреса интерфейсов и выполните команду **clear mac-address-table dynamic** для симуляции устаревания динамических MAC-адресов. ❖ Проверьте, включено ли уведомление об изменении MAC-адреса глобально. ❖ 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`
	`---------- -------------------- -------- -------------------`
	`1 00d0.3232.0001 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: 00d0.3232.0003 GigabitEthernet 0/2
```

2.4.5 Настройка управляющей VLAN для порта LAG

Сценарий

- Включите агрегированный порт для обработки пакетов из управляющей VLAN как пакетов управления, а пакетов из неуправляющей VLAN как пакетов данных.

Этапы конфигурации

Настройка управляющей VLAN для порта LAG

- Опционально.
- Выполните эту настройку, чтобы включить порт LAG для различения пакетов управления от пакетов данных.
- Конфигурация:

Команда	**aggregateport-admin vlan** *vlan-list*
Описание параметра	*vlan-list*: Указывает VLAN или диапазон VLAN, разделенный знаком "-".
Установки по умолчанию	По умолчанию для порта LAG не настроена управляющая VLAN.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Порт LAG обрабатывает пакеты, полученные в управляющей VLAN, как пакеты управления.

Проверка конфигурации

- Порт LAG обрабатывает пакеты из управляющей VLAN как пакеты управления, а пакеты из неуправляющей VLAN — как пакеты данных.

Пример конфигурации

Настройка управляющей VLAN для порта LAG

Этапы конфигурации	❖ Укажите управляющую VLAN для порта LAG.
	`QTECH# configure terminal` `QTECH(config)# aggregateport-admin vlan 1-20`
Проверка конфигурации	Выполните команду **show running** для отображения конфигурации.

2.5 Мониторинг

Очистка

⚠ Выполнение команд очистки может привести к потере важной информации и прерыванию служб.

Описание	Команда
Очистка динамических MAC-адресов.	**clear mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

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 динамических MAC-адресов.	**show mac-address-table aging-time**
Отображает максимальное количество динамических MAC-адресов.	**show mac-address-table max-dynamic-mac-count**
Отображает	**show mac-address-table notification** [**interface** [*interface-id*

конфигурацию и историю уведомлений об изменении MAC-адреса.	] **| history**]

Отладка

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

Описание	**Команда**
Отладка работы с MAC-адресами.	**debug bridge mac**

3 КОНФИГУРИРОВАНИЕ АГРЕГИРОВАННОГО ПОРТА

3.1 Обзор

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

Порт LAG поддерживает балансировку нагрузки, а именно равномерное распределение нагрузки между каналами-участниками. Кроме того, порт LAG выполняет резервирование канала. При отсоединении канала-участника нагрузка на канал, автоматически распределяется на другие функционирующие каналы-участники. Канал-участник не пересылает широковещательные или многоадресные пакеты другим каналам-участникам.

Например, канал связи между двумя устройствами поддерживает максимальную пропускную способность 1000 Мбит/с. Если трафик, передаваемый по каналу, превышает 1000 Мбит/с, превышающий трафик, будет отклонен. Для решения этой проблемы можно использовать агрегирование портов. Например, можно подключить два устройства с помощью сетевых кабелей и объединить несколько каналов для создания логического канала, поддерживающего многократное превышение скорости передачи данных в 1000 Мбит/с.

Например, имеется два устройства, подключенные с помощью сетевого кабеля. При отключении соединения между двумя портами устройств службы, выполняемые по каналу, будут прерваны. После объединения подключенных портов службы не будут затронуты до тех пор, пока один канал остается подключенным.

Протоколы и стандарты

- IEEE 802.3ad

3.2 Применение

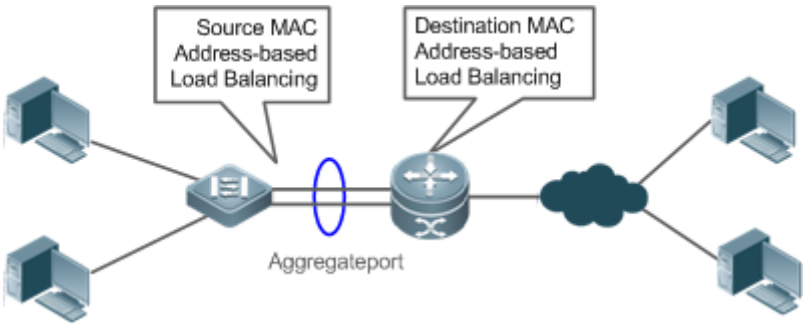
Применение	Описание
Агрегация каналов LAG и балансировка нагрузки	Между устройством агрегации и устройством уровня ядра передается большое количество пакетов, что требует большей пропускной способности. Для выполнения этого требования можно объединить физические каналы между устройствами в один логический канал, чтобы увеличить пропускную способность канала, и настроить правильный алгоритм балансировки нагрузки для равномерного распределения рабочей нагрузки по каждому физическому каналу, тем самым повышая коэффициент использования полосы пропускания.

3.2.1 Агрегация каналов LAG и балансировка нагрузки

Сценарий

На Изображении 3-1 коммутатор обменивается данными с маршрутизатором через порт LAG. Все устройства в интрасети (например, два ПК слева) используют маршрутизатор в качестве шлюза. Все устройства в экстрасети (например, два компьютера справа) отправляют пакеты на интернет-устройства через маршрутизатор с MAC-адресом шлюза в качестве MAC-адреса источника. Чтобы распределить нагрузку между маршрутизатором и другими хостами по другим каналам, настройте балансировку нагрузки на основе MAC-адреса назначения. На коммутаторе настройте балансировку нагрузки на основе MAC-адреса источника.

Рис. 3.1 Агрегирование каналов связи и балансировка нагрузки LAG



Описание

- Настройте порты, напрямую подключенные между коммутатором и маршрутизатором, как статический порт LAG или порт LAG протокола LACP (Link Aggregation Control Protocol).
- На коммутаторе настройте алгоритм балансировки нагрузки на основе MAC-адреса источника.
- На маршрутизаторе настройте алгоритм балансировки нагрузки на основе MAC-адреса назначения.
- Функции

Базовые концепции

Статический LAG

Статический режим агрегированного порта — это режим агрегации, в котором физические порты напрямую добавляются в группу агрегирования LAG посредством ручной настройки, чтобы физические порты могли пересылать пакеты, когда порты находятся в состоянии соединения и работы по протоколу.

Порт LAG в статическом режиме называется статическим LAG, а его порты-участники называются статическими портами-участниками LAG.

LACP

LACP — это протокол динамического агрегирования каналов связи. Он обменивается информацией с подключенным устройством через блоки данных LACP (LACPDU).

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

Режим порта участника LAG

Существует три режима агрегирования, а именно: активный, пассивный и статический.

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

Режим порта	Режим одноранговой порта
Активный режим	Активный или пассивный режим
Пассивный режим	Активный режим
Статический режим	Статический режим

Статус порта-участника LAG

Существует два типа состояния порта-участника LAG:

- Когда канал участника находится в положении «опущен», порт не может пересылать пакеты. Состояние канала «опущен» отображается.
- Когда порт-участник находится в состоянии «поднят» и протокол соединения готов, порт может пересылать пакеты. Состояние канала «поднят» отображается.
- Существует три типа состояния порта-участника LACP:
- Когда канал участника находится в положении «опущен», порт не может пересылать пакеты. Состояние канала «опущен» отображается.
- Когда канал порта находится в состоянии «поднят» и порт добавляется в группу агрегации, отображается состояние bndl.
- Если канал порта находится в состоянии «поднят», но передача данных на порту приостановлена, так как одноранговый порт не настроен с LACP, или Настройки портов не соответствуют атрибутам главного порта, отображается состояние susp. (Порт в состоянии susp не пересылает пакеты.)

Агрегирование LACP возможно только через полнодуплексные порты.

Агрегация LACP может быть реализована только в том случае, если скорости, подходы к управлению потоком, типы сред и Настройки уровня 2/3 для портов-участников согласованы.

При изменении названных **параметров** порта-участника в группе агрегирование LACP будет невозможно.

Порты, запрещенные к присоединению или выходу из порта LAG, не могут быть добавлены или удалены из статического порта LAG или порта LACP LAG.

Режим емкости LAG

Максимальное количество портов-участников фиксировано, что равно максимальному количеству портов LAG, умноженному на максимальное количество портов-участников, поддерживаемых одним портом LAG. Если требуется увеличить максимальное количество портов LAG, максимальное количество портов-участников, поддерживаемых одним портом LAG, должно быть уменьшено, и наоборот. Это относится к концепции режима емкости LAG. Некоторые устройства поддерживают настройку режима емкости LAG. Например, если система поддерживает 16384 порта-участника, можно выбрать режимы 1024 x 16, 512 x 32 и другие режимы емкости LAG (максимальное количество портов LAG, умноженное на максимальное количество портов-участников, поддерживаемых одним портом LAG).

Идентификатор системы LACP

Одно устройство может быть настроено только с одной системой агрегирования LACP. Система идентифицируется по ID системы, и каждая система имеет приоритет, который можно настроить. 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 совпадают, меньший MAC-адрес устройства указывает на более высокий приоритет идентификатора системы. Состояние порта определяется системой с идентификатором с более высоким приоритетом. Состояние порта системы с идентификатором более низкого приоритета соответствует состоянию с более высоким приоритетом.

Идентификатор порта LACP

Каждый порт имеет независимый приоритет порта LACP, который можно настроить. 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.

Мастер порт LACP

Когда каналы динамических портов-участников находятся в состоянии «поднят», LACP выбирает один из этих портов в качестве главного порта на основе скорости и дуплексного режима, приоритетов идентификаторов портов в группе агрегации и объединения каналов портов-участников в состоянии «поднят». Только порты, имеющие те же Настройки, что и главный порт, находятся в состоянии Bundle и участвуют в пересылке данных. При изменении **параметров** портов LACP выбирает главный порт заново. Когда новый главный порт не находится в состоянии Bundle, LACP разделяет порты-участники и выполняет агрегирование снова.

Предпочтительный порт участника LAG

Функция предпочтительного порта участника LAG используется, когда порт LAG подключен к серверу с двумя системами. Порт участника LAG выбирается в качестве предпочтительного порта, который пересылает указанные пакеты (пакеты VLAN управления) на сервер. Эти пакеты не будут распределяться на

другие порты-участники путем балансировки нагрузки. Это обеспечивает связь с сервером.

⚠ Настройте порт, подключенный к сетевой интерфейсной плате (NIC) сервера, в качестве предпочтительного порта-участника LAG.

Некоторые серверы Linux имеют две системы. Например, сервер HP имеет главную систему и систему удаленного управления. Главная система - это система Linux. Система удаленного управления с функцией Integrated Lights-Out (iLO) обеспечивает удаленное управление на аппаратном уровне. iLO может управлять сервером удаленно, даже при перезапуске главной системы. Основная система имеет две сетевые карты, объединенные в порт LAG для обработки сервисов. Система управления использует одну из двух сетевых карт для удаленного управления. Поскольку службы разделены разными сетями VLAN, VLAN, используемая системой управления, называется VLAN управления. Порт устройства, подключенного к серверу с двумя сетевыми картами, является портом LAG. Пакеты VLAN управления должны быть отправлены портом-участником, подключенным к сетевым интерфейсным платам сервера, чтобы обеспечить связь с системой удаленного управления. Можно настроить предпочтительный порт участника LAG для отправки пакетов VLAN управления.

⚠ Если на сервере с двумя сетевыми картами, объединенными через LACP, не работает LACP при перезапуске главной системы, происходит сбой согласования LACP и порт LAG не работает. В это время предпочитаемый порт участника LAG понизится до статического порта участника, и будет привязан к порту LAG для связи с системой удаленного управления сервера. После перезапуска системы Linux и нормальной работы LACP порт предпочтительного участника LAG будет снова включен с LACP для согласования.

Минимальное количество портов-участников LAG

В системе агрегирования LACP можно настроить минимальное количество портов-участников LAG. Когда порт-участник выходит из группы агрегирования LACP, это приводит к тому, что количество портов-участников становится меньше минимального количества, другие порты-участники группы разделяются. Когда порт-участник снова присоединяется к группе, в результате чего количество портов-участников превышает минимальное число, порты-участники автоматически объединяются в группу.

Обзор

Обзор	Описание
Агрегирование каналов связи	Объединение физических каналов статически или динамически для реализации расширения полосы пропускания и резервирования каналов.
Балансировка нагрузки	Гибко балансирует нагрузку в группе агрегации с помощью различных методов балансировки нагрузки.

3.2.2 Агрегирование каналов связи

Принцип работы

Существует два типа агрегирования каналов связи LAG. Один из них — статический LAG, а другой — динамическая агрегация через LACP.

- Статический LAG
- Статическая конфигурация LAG проста. Выполните команду, чтобы добавить указанный физический порт к порту LAG. После присоединения к группе агрегации порт-участник может принимать и передавать данные и участвовать в балансировке нагрузки внутри группы.
- Динамический LAG (LACP)
- Порт с поддержкой LACP отправляет LACPDU для объявления системного приоритета, системного MAC-адреса, приоритета порта, номера порта и ключа операции. При получении LACPDU от одноранговой узла устройство сравнивает системные приоритеты обоих концов на основе системного идентификатора в пакете. На узле с более высоким приоритетом идентификатора системы порты в группе агрегации устанавливаются в состояние Bundle на основе приоритетов идентификатора порта в нисходящем порядке и отправляются обновленные LACPDU. При получении LACPDU одноранговый узел устанавливает соответствующие порты в состояние Bundle, чтобы оба конца сохранили согласованность при выходе порта из группы агрегации или присоединении к ней. Физический канал может пересылать пакеты только после того, как порты на обоих концах будут объединены динамически.
- После агрегирования каналов связи порты-участники LACP периодически обмениваются LACPDU. Если порт не получает LACPDU в указанное время, происходит тайм-аут и каналы разъединяются. В этом случае порты-участники не могут пересылать пакеты. Существует два режима тайм-аута: длительное время ожидания и короткое время ожидания. В режиме длительного времени порт отправляет пакет каждые 30 секунд. Если пакет не поступает от одноранговой узла за 90 сек., возникает тайм-аут. В режиме короткого тайм-аута порт отправляет пакет каждую секунду. Если пакет не поступает от одноранговой узла за 3 сек., происходит тайм-аут.

3.2.3 Балансировка нагрузки

Принцип работы

Порты LAG разделяют потоки пакетов, используя алгоритмы балансировки нагрузки на основе содержимого пакета, такого как MAC-адрес источника и назначения, IP-адреса источника и назначения, а также номера портов источника и назначения уровня 4. Поток пакетов с согласованной функцией передается одним каналом-участником, и различные потоки пакетов равномерно распределяются по каналам-участникам. Например, при балансировке нагрузки на основе MAC-адреса источника пакеты распределяются по каналам-участникам на основе MAC-адресов источника пакетов. Пакеты с разными MAC-адресами источника равномерно распределяются по каналам-участникам. Пакеты с идентичным MAC-адресом источника пересылаются одним каналом-участником.

В настоящее время существует несколько режимов балансировки нагрузки LAG:

- 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 порта источника 4-го уровня или номер порта назначения 4-го уровня
- Номер порта источника 4-го уровня + номер порта назначения 4-го уровня
- IP-адрес источника + номер порта источника 4-го уровня
- IP-адрес источника + номер порта назначения 4-го уровня
- IP-адрес назначения + номер порта источника 4-го уровня
- IP-адрес назначения + номер порта назначения 4-го уровня
- IP-адрес источника + номер порта источника 4-го уровня + номер порта назначения 4-го уровня
- IP-адрес назначения + номер порта источника 4-го уровня + номер порта назначения 4-го уровня
- IP-адрес источника + IP-адрес назначения + номер порта источника 4-го уровня
- IP-адрес источника + IP-адрес назначения + номер порта назначения 4-го уровня
- IP-адрес источника + IP-адрес назначения + номер порта источника 4-го уровня + номер порта назначения 4-го уровня
- Панельный порт для входящих пакетов
- Теги пакетов многопротокольной коммутации меток (MPLS)
- Опрос портов-участников агрегации
- Расширенный режим

Балансировка нагрузки на основе IP-адресов или номеров портов применима только к пакетам 3-го уровня. Когда устройство, включенное методом балансировки нагрузки, получает пакеты 2-го уровня, оно автоматически переключается на метод балансировки нагрузки по умолчанию.

Все методы балансировки нагрузки используют алгоритм нагрузки (хеш-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-адрес назначения, IP-адрес источника + IP-адрес назначения + номер порта 4-го уровня и т. д. Алгоритм обеспечивает равномерное распределение пакетов с различными входными параметрами по каналам-участникам. Это не означает, что эти пакеты всегда распределяются по различным каналам-участникам. Например, при балансировке нагрузки на основе IP-адреса два пакета с разными IP-адресами источника и назначения могут быть распределены по одному и тому же каналу-участнику путем расчета.

Различные коммутаторы могут поддерживать различные алгоритмы балансировки нагрузки.

Улучшенная балансировка нагрузки

Улучшенная балансировка нагрузки позволяет комбинировать несколько полей в пакетах разных типов. Эти поля включают **src-mac**, **dst-mac**, **l2-protocol**, **vlan**, **src-port** и **dst-port** в пакетах 2-го уровня, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-**

dst-port, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac** и **dst-mac** в пакетах IPv4, **src-ip**, **dst-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **vlan**, **src-port**, **dst-port**, **l2-etype**, **src-mac** и **dst-mac** в пакетах IPv6; **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** и **l2-etype** в пакетах MPLS; **vlan**, **src-port**, **src-mac**, **src-ip**, **protocol**, **l4-src-port**, **l4-dst-port**, **l2-etype**, **ing-nick**, **egr-nick**, **dst-port**, **dst-mac** и **dst-ip** в пакетах TRILL и **vlan**, **src-port**, **src-id**, **rx-id**, **ox-id**, **fabric-id**, **dst-port**, а также **dst-id** в пакетах FCoE.

Устройство, включенное с улучшенной балансировкой нагрузки, сначала определяет тип передаваемых пакетов и выполняет балансировку нагрузки на основе указанных полей в пакетах. Например, порт LAG выполняет балансировку нагрузки на основе IP-адреса источника для пакетов, содержащих постоянно изменяющийся IPv4-адрес источника.

- Все методы балансировки нагрузки применимы к портам LAG 2-го и 3-го уровня. Чтобы полностью использовать полосу пропускания сети, необходимо настроить правильные методы распределения нагрузки на основе различных сетевых сред.
- Выполните расширенную балансировку нагрузки на основе полей src-mac, dst-mac и vlan в пакетах 2-го уровня и поля src-ip в пакетах IPv4. Если входящий пакет представляет собой пакет IPv4 с постоянно меняющимся MAC-адресом источника, алгоритм расширенной балансировки не действует, так как устройство будет выполнять балансировку нагрузки только на основе поля src-ip в пакете IPv4 после того, как будет установлено, что это пакет IPv4.
- При улучшенной балансировке нагрузки алгоритм балансировки MPLS действует только для пакетов VPN MPLS 3-го уровня, но не применяется для пакетов VPN MPLS 2-го уровня.

3.3 Конфигурация

Конфигурация	Описание и команда	
Настройка статических агрегированных портов	(Обязательно) Используется для настройки агрегирования каналов связи вручную.	
	interface aggregateport	Создает агрегированный порт Ethernet.
	interface san-port-channel	Создает агрегированный порт FC.
	port-group	Настраивает статические порты-участники агрегированного порта.
Настройка агрегированных портов LACP	(Обязательно) Используется для настройки агрегирования каналов связи динамически.	
	port-group mode	Настраивает порты-участники LACP.
	lacp port-priority	Настраивает приоритет порта.

	lacp short-timeout	Настраивает режим короткого времени ожидания на порту.
Включение LinkTrap	(Дополнительно) Используется для включения LinkTrap.	
	snmp Trap link-status	Включает объявление LinkTrap для порта LAG.
	aggregateport member linkTrap	Включает функцию LinkTrap для портов-участников LAG
Настройка режима балансировки нагрузки	(Дополнительно) Используется для настройки режима балансировки нагрузки для агрегированного канала.	
	aggregateport load-balance	Настраивает алгоритм балансировки нагрузки для порта LAG или портов-участников LAG.
	(Дополнительно) Используется для настройки профиля улучшенной балансировки нагрузки.	
	load-balance-profile	Создает профиль улучшенной балансировки нагрузки.
	l2 field	Настраивает режим балансировки нагрузки для пакетов 2-го уровня.
	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.
Настройка режима емкости LAG	(Дополнительно) Используется для настройки режима емкости агрегированного порта.	
	aggregateport cLAGacity mode	Настраивает режим емкости агрегированного порта в режиме глобальной конфигурации.

Настройка предпочтительного порта участника LAG	(Дополнительно) Используется для настройки порта участника агрегированного порта в качестве предпочтительного порта.	
	aggregateport primary-port	Настраивает порт-участник агрегированного порта в качестве предпочтительного порта.
Настройка минимального количества портов-членов LACP LAG	**aggregateport minimum member**	Настраивает минимальное количество портов-участников LACP LAG.

3.3.1 Настройка статических портов LAG

Сценарий

- Настройте несколько физических портов в качестве портов-участников LAG для агрегирования каналов связи.
- Полоса пропускания (Bandwidth) канала агрегации равна сумме пропускной способности каналов-участников.
- При отсоединении канала-участника нагрузка на канал, автоматически распределяется на другие функционирующие каналы-участники.

Примечания

- В агрегированный порт можно добавить только физические порты.
- Порты различных типов сред или режимов не могут быть добавлены в один и тот же порт LAG.
- Порты 2-го уровня можно добавлять только в порт LAG 2-го уровня, а порты 3-го уровня — только в порт LAG 3-го уровня. Настройки 2-го и 3-го уровня порта LAG, содержащего порты-участники, изменить нельзя.
- После добавления порта в порт LAG Настройки порта заменяются атрибутами порта LAG.
- После удаления порта из порта LAG Настройки порта восстанавливаются.

После добавления порта в порт LAG Настройки порта согласуются с атрибутами порта LAG. Поэтому не следует выполнять настройку портов-участников LAG или применять конфигурацию к определенному порту-участнику LAG. Однако некоторые конфигурации (команды **shutdown** и **no shutdown**) можно настроить на портах-участниках LAG. При использовании портов-участников LAG проверьте, может ли функция, которую необходимо настроить, повлиять на конкретный порт-участник LAG и выполните эту настройку правильно.

Этапы конфигурации

Создайте агрегированный порт Ethernet

- Обязательно.
- Выполните эту настройку на устройстве с поддержкой агрегированного порта.

Команда	**interface aggregateport** *LAG-number*

Описание параметра	*LAG-number*: Указывает номер агрегированного порта.
Установки по умолчанию	По умолчанию агрегированный порт не создан.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Чтобы создать агрегированный порт Ethernet, запустите команду **interfaces aggregateport** в режиме глобальной конфигурации. Чтобы удалить указанный агрегированный порт Ethernet, выполните команду **no interfaces aggregateport** *LAG-number* в режиме глобальной конфигурации.

- Запустите команду **port-group**, чтобы добавить физический порт в статический агрегированный порт в режиме конфигурации интерфейса. Если агрегированный порт не существует, он будет создан автоматически.
- Запустите команду **port-group mode**, чтобы добавить физический порт в LACP агрегированный порт в режиме конфигурации интерфейса. Если агрегированный порт не существует, он будет создан автоматически.
- Функция LAG должна быть настроена на устройствах на обоих концах канала, и режим LAG должен быть одинаковым (статический LAG или LACP LAG).

Настройка статических портов-участников LAG

- Обязательно.
- Выполните эту настройку на устройстве с поддержкой агрегированного порта.

Команда	**port-group** *LAG-number*
Описание параметра	**port-group** *LAG-number*: Указывает номер агрегированного порта.
Установки по умолчанию	По умолчанию порты не добавлены в любой статический агрегированный порт.
Режим команды	Режим конфигурации интерфейса указанного порта Ethernet
Встроенная подсказка	Чтобы добавить порты-участники в агрегированный порт, запустите команду **port-group** в режиме конфигурации интерфейса. Чтобы удалить порты-участники из агрегированного порта, запустите команду

	no port-group в режиме конфигурации интерфейса.

- Статические порты-участники LAG, настроенные на устройствах на обоих концах канала, должны быть согласованными.
- После выхода порта-участника из агрегированного порта настройки порта-участника восстанавливаются по умолчанию. Различные функции согласуются с настройками по умолчанию портов-участников по-разному. Рекомендуется проверять и подтверждать настройки порта после выхода порта участника из агрегированного порта.
- После выхода порта участника из LAG порт отключается с помощью команды **shutdown**, чтобы избежать петель. После подтверждения правильности топологии запустите команду **no shutdown** в режиме конфигурации интерфейса, чтобы снова включить порт.

Преобразование LAG 2-го уровня в LAG 3-го уровня

- Опционально.
- Если требуется включить маршрутизацию 3-го уровня на порту LAG, например, для настройки IP-адресов или записей статических маршрутов, преобразуйте порт LAG 2-го уровня в порт LAG 3-го уровня и включите маршрутизацию на порту LAG 3-го уровня.
- Выполните эту настройку на устройствах с LAG, которые поддерживают функции 2-го и 3-го уровня, такие как коммутаторы 3-го уровня или контроллеры беспроводного доступа (AC).

Команда	**no switchport**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию порты LAG являются портами LAG 2-го уровня.
Режим команды	Режим конфигурации интерфейса указанного порта LAG
Встроенная подсказка	Функция LAG 3-го уровня поддерживается только устройствами 3-го уровня.

- Порт LAG, созданный на устройстве 3-го уровня, не поддерживающем функцию 2-го уровня, является портом LAG 3-го уровня. В противном случае порт LAG является портом LAG 2-го уровня.

Создание субинтерфейса агрегированного порта Ethernet

- Опционально.

- На устройстве, поддерживающем конфигурацию субинтерфейса, запустите команду **interface aggregateport** *sub-LAG-number*, чтобы создать субинтерфейс.
- Выполните эту настройку на устройствах с LAG, которые поддерживают функции 2-го и 3-го уровня, такие как коммутаторы 3-го уровня.

Команда	**interface aggregateport** *sub-LAG-number*
Описание параметра	*sub-LAG-number*: Указывает номер субинтерфейса LAG.
Установки по умолчанию	По умолчанию субинтерфейсы не создаются.
Режим команды	Режим конфигурации интерфейса указанного порта LAG
Встроенная подсказка	Перед созданием субинтерфейса необходимо преобразовать мастер порт LAG в порт 3-го уровня.

Проверка конфигурации

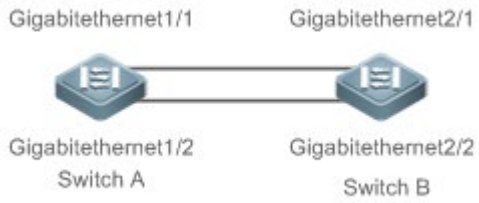
- Запустите **show run** для отображения конфигурации.
- Запустите команду **show aggregateport summary**, чтобы отобразить конфигурацию LAG.

Команда	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Описание параметра	*aggregate-port-number*: Указывает номер агрегированного порта. **load-balance**: Отображает алгоритм балансировки нагрузки. **summary**: Отображает сводку по каждому каналу.
Режим команды	Любой режим
Встроенная подсказка	Информация обо всех портах LAG отображается, если не указан номер порта LAG.
	QTECH# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Load balance Ports ---------- ---------- ---------- ------ ---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac**

	Gi0/2

Пример конфигурации

Настройка статических агрегированных портов Ethernet

Сценарий **Изображение 3-2**	
Этапы конфигурации	❖ Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A в статический порт LAG 3. ❖ Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B в статический порт LAG 3.
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 конфигурации	❖ Запустите команду **show aggregateport summary**, чтобы проверить, содержит ли порт LAG 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**

3.3.2 Настройка агрегированных портов LACP

Сценарий

- Подключенные устройства выполняют автоматическое согласование через LACP для реализации динамического агрегирования каналов связи.
- Полоса пропускания (Bandwidth) канала агрегации равна сумме пропускной способности каналов-участников.
- При отсоединении канала-участника нагрузка на канал, автоматически распределяется на другие функционирующие каналы-участники.
- LACP требуется 90 сек. для обнаружения сбоя канала в режиме с большим временем ожидания и 3 сек. в режиме с коротким временем ожидания.

Примечания

- После выхода порта из LACP LAG можно восстановить настройки порта по умолчанию. Различные функции согласуются с настройками по умолчанию портов-участников по-разному. Рекомендуется проверять и подтверждать настройки порта после выхода порта-участника из LACP LAG.
- Изменение приоритета порта-участника LACP может привести к тому, что другие порты-участники будут дезагрегированы и агрегированы снова.

Этапы конфигурации

Настройка портов-участников LACP.

- Обязательно.
- Выполните эту настройку на устройстве с поддержкой LACP.

Команда	**port-group** *key-number* **mode** { **active** | **passive** }
Описание параметра	*Key-number*: Указывает ключ управления агрегированного порта. Другими словами, это номер порта LACP LAG. Максимальное значение зависит от количества портов LAG, поддерживаемых устройством. **active**: Указывает, что порты активно добавляются в динамический порт LAG. **passive**: Указывает, что порты добавляются в динамический порт LAG пассивно.
Установки по умолчанию	По умолчанию физические порты не добавляются в любой порт LACP LAG.
Режим команды	Режим конфигурации интерфейса указанного физического порта

Встроенная подсказка	Эта команда используется в режиме конфигурации интерфейса для добавления портов-участников в порт LACP LAG.

Порты-участники LACP, настроенные на обоих концах канала, должны быть согласованными.

Настройка режима ожидания для портов-участников LACP

- Опционально.
- Если требуется выполнить обнаружение сбоя канала в реальном времени, настройте режим короткого времени ожидания. LACP требуется 90 сек. для обнаружения сбоя канала в режиме с большим временем ожидания и 3 сек. в режиме с коротким временем ожидания.
- Выполните эту настройку на устройствах с поддержкой LACP, таких как коммутаторы.

Команда	**lacp short-timeout**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию режим ожидания для портов-участников LACP имеет значение с большим временем задержки.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Режим ожидания поддерживается только физическими портами. Чтобы восстановить настройки по умолчанию, запустите команду **no lacp short-timeout** в режиме конфигурации интерфейса.

Проверка конфигурации

- Запустите **show run** для отображения конфигурации.
- Запустите команду **show lacp summary**, чтобы отобразить состояние канала LACP.

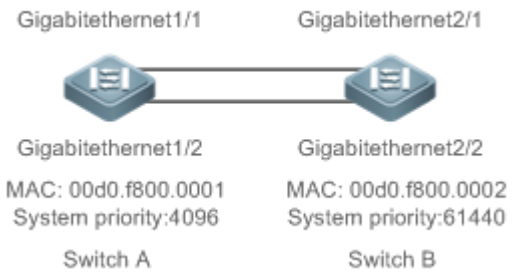
Команда	**show lacp summary** [*key-number*]
Описание параметра	*key-name*: Указывает номер порта LACP LAG.
Режим команды	Любой режим

Встроенная подсказка	Информация обо всех портах LACP LAG отображается, если не указан параметр *key-name*.

```
QTECH(config)# show lacp summary 3
System Id:32768, 00d0.f8fb.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.
Aggregate port 3:
Local information:
LACP port        Oper     Port      Port
Port      Flags      State      Priority        Key      Number   State
---------------------------------------------------------------------
Gi0/1      SA         bndl         4096          0x3      0x1       0x3d
Gi0/2      SA         bndl         4096          0x3      0x2       0x3d
Gi0/3      SA         bndl         4096          0x3      0x3       0x3d
Partner information:
                    LACP port                    Oper     Port      Port
Port       Flags       Priority        Dev ID          Key       Number
State
---------------------------------------------------------------------
-
Gi0/1      SA         61440      00d0.f800.0001    0x3      0x1       0x3d
Gi0/2      SA         61440      00d0.f800.0001    0x3      0x2       0x3d
Gi0/3      SA         61440      00d0.f800.0001    0x3      0x3       0x3d
```

Пример конфигурации

Конфигурирование LACP

Сценарий **Изображение 3-3**	
Этапы конфигурации	❖ На коммутаторе A установите приоритет системы LACP на 4096. ❖ Включите динамическое агрегирование каналов связи на портах GigabitEthernet1/1 и GigabitEthernet1/2 коммутатора A и добавьте

	порты в LACP LAG 3. ❖ На коммутаторе B установите приоритет системы LACP на 61440. ❖ Включите динамическое агрегирование каналов связи на портах GigabitEthernet2/1 и GigabitEthernet2/2 коммутатора B и добавьте порты в LACP LAG 3.
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)# end
Коммутатор B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 2/1-2 SwitchB(config-if-range)# port-group 3 mode active SwitchB(config-if-range)# end
Проверка конфигурации	❖ Запустите команду **show lacp summary 3**, чтобы проверить, содержит ли порт LACP LAG 3 порты-участники GigabitEthernet2/1 и GigabitEthernet2/2.
Коммутатор A	SwitchA# show LACP summary 3 System Id:32768, 00d0.f8fb.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 ---------- Gi2/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d

	Gi2/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d
Коммутатор B	SwitchB# show LACP summary 3 System Id:32768, 00d0.f8fb.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. Aggregate 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 ---------- Gi1/1 SA 32768 00d0.f800.0001 0x3 0x1 0x3d Gi1/2 SA 32768 00d0.f800.0001 0x3 0x2 0x3d

3.3.3 Включение LinkTrap

Сценарий

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

Этапы конфигурации

Включение LinkTrap для порта LAG

- ❖ Опционально.
- ❖ Включите LinkTrap в режиме конфигурации интерфейса. По умолчанию LinkTrap включен. Сообщения LinkTrap отправляются при изменении состояния канала или при изменении состояния протокола агрегированного порта.
- ❖ Выполните эту настройку на устройстве с поддержкой LAG.

Команда	**snmp Trap link-status**

Описание параметра	Недоступно
Установки по умолчанию	По умолчанию LinkTrap включен.
Режим команды	Режим конфигурации интерфейса указанного порта LAG
Встроенная подсказка	Используйте эту команду в режиме конфигурации интерфейса, чтобы включить LinkTrap для указанного порта LAG. После включения LinkTrap сообщения LinkTrap отправляются при изменении состояния соединения порта LAG. В противном случае сообщения LinkTrap не отправляются. По умолчанию LinkTrap включен. Чтобы отключить LinkTrap для порта LAG, выполните команду **no snmp Trap link-status** в режиме конфигурации интерфейса. LinkTrap не может быть включен для определенного порта-участника LAG. Чтобы включить LinkTrap для всех портов-участников LAG, запустите **aggregateport member linkTrap** в режиме глобальной конфигурации.

Включение LinkTrap для портов-участников LAG

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

Команда	**aggregateport member linkTrap**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию LinkTrap отключен для портов-участников LAG.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Используйте эту команду в режиме глобальной конфигурации, чтобы включить LinkTrap для всех портов участников LAG. По умолчанию сообщения LinkTrap не отправляются при изменении состояния каналов портов-участников LAG. Чтобы отключить LinkTrap для всех портов-участников LAG, запустите команду **no aggregateport member linkTrap**

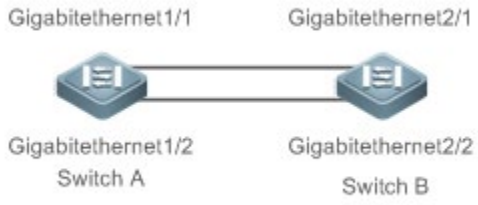
	в режиме глобальной конфигурации.

Проверка конфигурации

- ❖ Запустите **show run** для отображения конфигурации.
- ❖ После включения LinkTrap эту функцию можно отслеживать на портах LAG или их портах-участниках с помощью программного обеспечения для чтения MIB.

Пример конфигурации

Включение LinkTrap для портов-участников LAG

Сценарий **Изображение 3-4**	
Этапы конфигурации	❖ Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A в статический порт LAG 3. ❖ Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B в статический порт LAG 3. ❖ На коммутаторе A отключите LinkTrap для порта LAG 3 и включите LinkTrap для его входящих портов. ❖ На коммутаторе B отключите LinkTrap для порта LAG 3 и включите LinkTrap для портов-участников LAG.

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 команду **show run**, чтобы проверить, включена ли

конфигурации	функция LinkTrap для порта LAG 3 и его портов-участников.
Коммутатор 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
Коммутатор 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

3.3.4 Настройка режима балансировки нагрузки

Сценарий

Система распределяет входящие пакеты между каналами-участниками с помощью указанного алгоритма балансировки нагрузки. Поток пакетов с согласованной функцией передается одним каналом-участником, а различные потоки пакетов равномерно распределяются по каналам-участникам. Устройство, включенное с улучшенной балансировкой нагрузки, сначала определяет тип передаваемых пакетов и выполняет балансировку нагрузки на основе указанных полей в пакетах. Например, порт LAG выполняет балансировку нагрузки на основе IP-адреса источника для пакетов, содержащих постоянно изменяющийся IPv4-адрес источника.

Этапы конфигурации

Настройка глобального алгоритма балансировки нагрузки порта LAG

- (Дополнительно) Выполните эту настройку, если необходимо оптимизировать балансировку нагрузки.
- Выполните эту настройку на устройстве с поддержкой LAG.

Команда	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **enhanced profile** *profile-name* }
Описание параметра	**dst-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов.

	src-mac: Указывает, что нагрузка распределяется на основе MAC-адресов источника входящих пакетов. **src-dst-ip**: Указывает, что нагрузка распределяется на основе IP-адресов источника и назначения входящих пакетов. **dst-ip**: Указывает, что нагрузка распределяется на основе IP-адресов назначения входящих пакетов. **src-ip**: Указывает, что нагрузка распределяется на основе IP-адресов источника входящих пакетов. **src-dst-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов источника и назначения входящих пакетов. **enhanced profile** *profile-name*: Указывает имя профиля расширенной балансировки нагрузки.
Установки по умолчанию	Балансировка нагрузки может быть основана на MAC-адресах источника и назначения (применимо к коммутаторам) или IP-адресах источника и назначения (применимо к шлюзам).
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите **no aggregateport load-balance** в режиме глобальной конфигурации. В режиме конфигурации интерфейса порта LAG на устройствах, которые поддерживают балансировку нагрузки на определенном порте LAG, можно выполнить команду **aggregateport load-balance**. Приоритет имеет настройка в режиме конфигурации интерфейса. Чтобы отключить алгоритм балансировки нагрузки, выполните команду **no aggregateport load-balance** в режиме конфигурации интерфейса порта LAG. После этого вступает в силу алгоритм балансировки нагрузки, настроенный в режиме глобальной конфигурации. В режиме конфигурации интерфейса порта LAG на устройствах, которые поддерживают балансировку нагрузки на определенном порте LAG, можно выполнить команду **aggregateport load-balance**.

Создание профиля расширенной балансировки нагрузки

- Если выбран режим расширенной балансировки нагрузки, необходимо настроить профиль расширенной балансировки нагрузки. В противном случае не удастся установить балансировку нагрузки LAG на расширенную. В других случаях конфигурация является дополнительной.

❖ Эта конфигурация выполняется на устройствах, поддерживающих улучшенную балансировку нагрузки, например, на коммутаторах агрегации и коммутаторах ядра.

Команда	**load-balance-profile** *profile-name*
Описание параметра	*profile-name*: Указывает имя профиля, которое может содержать до 31 символа.
Установки по умолчанию	Профиль расширенной балансировки нагрузки не существует.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Чтобы удалить профиль балансировки нагрузки по умолчанию, запустите команду **default load-balance-profile** *profile-name* в режиме глобальной конфигурации. Чтобы создать имя профиля, запустите **load-balance-profile** *profile-name* в режиме глобальной конфигурации. При успешном создании сохраняются настройки профиля по умолчанию. Глобально поддерживается только один профиль. Для отображения профиля расширенной балансировки нагрузки выполните команду **show load-balance-profile**.

Настройка режима балансировки пакетной нагрузки 2-го уровня

❖ (Дополнительно) выполните эту настройку, чтобы задать режим балансировки пакетной нагрузки 2-го уровня.

❖ Эта конфигурация выполняется на устройствах, поддерживающих улучшенную балансировку нагрузки, например, на коммутаторах агрегации и коммутаторах ядра.

Команда	**l2 field** { [**src-mac**] [**dst-mac**] [**l2-protocol**] [**vlan**] [**src-port**] }
Описание параметра	**src-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов источника входящих пакетов 2-го уровня. **dst-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов назначения входящих пакетов 2-го уровня. **l2-protocol**: Указывает, что нагрузка распределяется на основе типов протоколов 2-го уровня входящих пакетов 2-го уровня. **vlan**: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов 2-го уровня.

	src-port: Указывает, что нагрузка распределяется на основе панельного порта для входящих пакетов 2-го уровня.
Установки по умолчанию	По умолчанию для пакетов 2-го уровня используется режим балансировки нагрузки **src-mac**, **dst-mac** и **vlan**.
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите **no l2 field** в режиме конфигурации профиля.

Настройка режима балансировки пакетной нагрузки IPv4

- Опционально.
- Выполните эту настройку, чтобы задать режим балансировки пакетной нагрузки IPv4.
- Эта конфигурация выполняется на устройствах, поддерживающих расширенную балансировку нагрузки, например, на коммутаторах агрегации и коммутаторах ядра.

Команда	**ipv4 field** { [**src-ip**] [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**vlan**] [**src-port**] }
Описание параметра	**src-ip**: Указывает, что нагрузка распределяется на основе IP-адресов источников входящих пакетов IPv4. **dst-ip**: Указывает, что нагрузка распределяется на основе IP-адресов назначений 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 портов источников 4-го уровня входящих пакетов IPv4. **l4-dst-port**: Указывает, что нагрузка распределяется на основе номеров портов назначений 4-го уровня входящих пакетов IPv4. **vlan**: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов IPv4. **src-port**: Указывает, что нагрузка распределяется на основе порта панели для входящих пакетов IPv4.
Установки	По умолчанию для пакетов IPv4 используется режим балансировки

по умолчанию	нагрузки **src-ip** и **dst-ip**.
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите **no ipv4 field** в режиме конфигурации профиля.

Настройка режима балансировки пакетной нагрузки IPv6

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

Команда	**ipv6 field** { [**dst-ip**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**vlan**] [**src-port**] }
Описание параметра	**dst-ip**: Указывает, что нагрузка распределяется на основе IP-адресов назначений 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 портов источников 4-го уровня входящих пакетов IPv6. **l4-dst-port**: Указывает, что нагрузка распределяется на основе номеров портов назначений 4-го уровня входящих пакетов IPv6. **vlan**: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов IPv6. **src-port**: Указывает, что загрузка распределяется в соответствии с номерами портов источников входящих пакетов IPv6.
Установки по умолчанию	По умолчанию для пакетов IPv6 используется режим балансировки нагрузки **src-ip** и **dst-ip**.
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите **no ipv6 field** в режиме конфигурации профиля.

Настройка режима балансировки пакетной нагрузки MPLS

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

Команда	**mpls field** { [**top-label**] [**2nd-label**] [**3rd-label**] [**src-ip**] [**dst-ip**] [**vlan**] [**src-port**] [**src-mac**] [**dst-mac**] [**protocol**] [**l4-src-port**] [**l4-dst-port**] [**l2-etype**] }
Описание параметра	**src-ip**: Указывает, что нагрузка распределяется на основе IP-адресов источников входящих пакетов MPLS. **dst-ip**: Указывает, что нагрузка распределяется на основе IP-адресов назначений входящих пакетов MPLS. **top-label**: Указывает, что нагрузка распределяется на основе верхних меток входящих пакетов MPLS. **2nd-label**: Указывает, что нагрузка распределяется на основе второй метки входящих пакетов MPLS. **3rd-label**: Указывает, что нагрузка распределяется на основе третьей метки входящих пакетов MPLS. **vlan**: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов MPLS. **src-port**: Указывает, что нагрузка распределяется на основе номеров портов источников входящих пакетов MPLS. **src-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов источников входящих пакетов MPLS. **dst-mac**: Указывает, что нагрузка распределяется на основе MAC-адресов назначений 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 портов источников 4-го уровня входящих пакетов MPLS. **l4-dst-port**: Указывает, что нагрузка распределяется на основе номеров портов назначений 4-го уровня входящих пакетов MPLS. **l2-etype**: Указывает, что нагрузка распределяется на основе типов Ethernet пакетов MPLS.
Установки по	По умолчанию для пакетов MPLS используется режим балансировки нагрузки **top-label** и **2nd-label**.

умолчанию	
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите команду **no mpls field** в режиме конфигурации профиля.

Алгоритм балансировки нагрузки MPLS действует только для пакетов VPN 3-го уровня MPLS.

Настройка режима балансировки пакетной нагрузки TRILL

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

Команда	**trill field** { [**vlan**] [**src-ip**] [**dst-ip**] [**src-port**] [**src-mac**] [**dst-mac**] [**l4-src-port**] [**l4-dst-port**] [**l2-etype**] [**protocol**] [**ing-nick**] [**egr-nick**] }
Описание параметра	vlan: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов TRILL. src-ip: Указывает, что нагрузка распределяется на основе IP-адресов источников входящих пакетов TRILL. dst-ip: Указывает, что нагрузка распределяется на основе IP-адресов назначений входящих пакетов TRILL. src-port: Трафик распределяется в соответствии с номерами портов-источников входящих пакетов TRILL. src-mac: Указывает, что нагрузка распределяется на основе MAC-адресов источников входящих пакетов TRILL. dst-mac: Указывает, что нагрузка распределяется на основе MAC-адресов назначений входящих пакетов TRILL. l4-src-port: Указывает, что нагрузка распределяется на основе номеров портов источников 4-го уровня входящих пакетов TRILL. l4-dst-port: Указывает, что нагрузка распределяется на основе номеров портов назначений 4-го уровня 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 входящих названий Rbridge пакетов TRILL. egr-nick: Указывает, что нагрузка распределяется на основе номеров портов источников входящих пакетов TRILL.
Установки по умолчанию	По умолчанию для пакетов TRILL используется режим балансировки нагрузки **src-mac**, **dst-mac** и **vlan**.
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите команду **no trill field** в режиме конфигурации профиля. Потоки транзитных пакетов TRILL RBridge сбалансированы по следующим полям: **ing-nick**, **egr-nick**, **src-mac**, **dst-mac**, **vlan** и **l2-etype**. Потоки исходящих пакетов TRILL RBridge сбалансированы на основе следующих полей: Пакеты 2-го уровня: **src-mac**, **dst-mac**, **vlan** и **l2-protocol**. Пакеты 3-го уровня: **src-ip**, **dst-ip**, **l4-src-port**, **l4-dst-port**, **protocol** и **vlan**. Поля **src-port** и **dst-port** можно использовать для балансировки всех потоков транзитных и исходящих пакетов TRILL Transit RBridge и TRILL Egress RBridge.

Настройка режима балансировки пакетной нагрузки FCoE

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

Команда	**fcoe field** {[**vlan**] [**src-port**] [**src-id**] [**dst-id**] [**rx-id**] [**ox-id**] [**fabric-id**]}
Описание параметра	**vlan**: Указывает, что нагрузка распределяется на основе идентификаторов VLAN входящих пакетов FCoE. **src-port**: Указывает, что нагрузка распределяется на основе номеров портов источников входящих пакетов FCoE. **src-id**: Указывает, что нагрузка распределяется на основе идентификаторов источников пакетов FCoE. **dst-id**: Указывает, что нагрузка распределяется на основе идентификаторов назначений 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 для пакетов FCoE. **fabric-id**: Указывает, что нагрузка распределяется на основе идентификаторов сети Fibre Channel для пакетов FCoE.
Установки по умолчанию	По умолчанию для пакетов FCoE используется режим балансировки нагрузки **src-id**, **dst-id** и **ox-id**.
Режим команды	Режим конфигурации профиля
Встроенная подсказка	Чтобы восстановить настройки по умолчанию, запустите команду **no fcoe field** в режиме конфигурации профиля.

Проверка конфигурации

- Запустите **show run** для отображения конфигурации.
- Запустите **show aggregateport load-balance**, чтобы отобразить конфигурацию балансировки нагрузки. Если устройство поддерживает конфигурацию балансировки нагрузки на определенном порте LAG, запустите команду **show aggregateport summary**, чтобы отобразить конфигурацию.
- Запустите **show load-balance-profile** для отображения профиля расширенной балансировки нагрузки.

Команда	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Описание параметра	*aggregate-port-number*: Указывает номер агрегированного порта. **load-balance**: Отображает алгоритм балансировки нагрузки. **summary**: Отображает сводку по каждому каналу.
Режим команды	Любой режим
Встроенная подсказка	Информация обо всех портах LAG отображается, если не указан номер порта LAG.

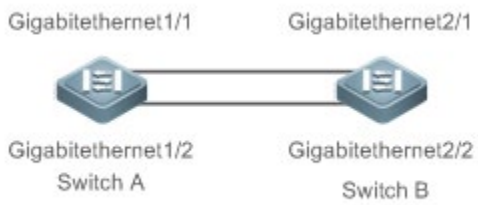
	`QTECH# show aggregateport 1 summary`
	`AggregatePort MaxPorts SwitchPort Mode Load balance Ports`
	`------------ -------------- ---------- ------ -----------------`

	---------- ---------- **Ag1** 8 Enabled ACCESS **dst-mac** **Gi0/2**

Команда	**show load-balance-profile** [*profile-name*]
Описание параметра	*profile-name*: Указывает имя профиля.
Режим команды	Любой режим
Встроенная подсказка	Отображаются все расширенные профили, если номер профиля не указан.
	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

Пример конфигурации

Настройка режима балансировки нагрузки

Сценарий **Изображение 3-5**	
Этапы конфигурации	❖ Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A в статический порт LAG 3. ❖ Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B в статический порт LAG 3. ❖ На коммутаторе A настройте балансировку нагрузки на основе MAC-адреса источника для порта LAG 3 в режиме глобальной

	конфигурации. ❖ На коммутаторе B настройте балансировку нагрузки на основе MAC-адреса назначения для порта LAG 3 в режиме глобальной конфигурации.
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 load-balance src-mac
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 load-balance dst-mac
Проверка конфигурации	❖ Запустите **show aggregateport load-balance**, чтобы отобразить конфигурацию алгоритма балансировки нагрузки.
Коммутатор A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Коммутатор B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

3.3.5 Настройка режима емкости LAG

Сценарий

❖ Измените максимальное количество настраиваемых агрегированных портов (LAG) и максимальное количество портов-участников в каждом порте LAG.

Примечания

❖ Система имеет режим емкости порта LAG по умолчанию. Можно запустить **show aggregateport cLAGacity**, чтобы отобразить текущий режим емкости.

❖ Если текущая конфигурация (максимальное количество портов LAG или количество портов-участников в каждом порте LAG) превышает емкость, которую необходимо настроить, конфигурация режима емкости будет неудачной.

Этапы конфигурации

Настройка режима емкости порта LAG

- (Дополнительно) Чтобы изменить емкость порта LAG, выполните данную настройку.
- Выполните данную настройку на устройствах, поддерживающих изменение емкости порта LAG, например, на коммутаторах уровня ядра.

Команда	**aggregateport cLAGacity mode** *cLAGacity-mode*
Описание параметра	*cLAGacity-mode*: Указывает режим емкости.
Установки по умолчанию	По умолчанию режимы емкости порта LAG различаются в зависимости от устройства. Например, 256 x 16 означает, что устройство имеет максимум 256 портов LAG и 16 портов-участников в каждом порте LAG.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Система предоставляет несколько режимов емкости для устройств, поддерживающих режим емкости. Чтобы восстановить настройки по умолчанию, выполните команду **no aggregateport cLAGacity mode** в режиме глобальной конфигурации.

Проверка конфигурации

- Запустите команду **show run** для отображения конфигурации.
- Запустите команду **show aggregateport cLAGacity**, чтобы отобразить текущий режим и использование емкости LAG.

Команда	**show aggregateport cLAGacity**
Описание параметра	Недоступно
Режим команды	Любой режим
Встроенная подсказка	Недоступно

	`QTECH# show aggregateport cLAGacity`
	`AggregatePort CLAGacity Information:`
	`Configuration CLAGacity Mode: 128*16.`

	Effective CLAGacity Mode : 256*8. Available CLAGacity : 128*8. Total Number: 128, Used: 1, Available: 127.

Пример конфигурации

Настройка режима емкости порта LAG

Сценарий **Изображение 3-6**	
Этапы конфигурации	❖ Добавьте порты GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A в статический порт LAG 3. ❖ Добавьте порты GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B в статический порт LAG 3. ❖ На коммутаторе A настройте режим емкости порта LAG 128x128. ❖ На коммутаторе B настройте режим емкости порта LAG 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 cLAGacity 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 cLAGacity mode 256*64
Проверка конфигурации	❖ Запустите **show aggregateport cLAGacity**, чтобы проверить конфигурацию режима емкости порта LAG.

Коммутатор A	SwitchA# show aggregatePort cLAGacity AggregatePort CLAGacity Information: Configuration CLAGacity Mode: 128*128. Effective CLAGacity Mode : 128*128. Available CLAGacity Mode : 128*128. Total Number : 128, Used: 1, Available: 127.
Коммутатор B	SwitchB# show aggregatePort cLAGacity AggregatePort CLAGacity Information: Configuration CLAGacity Mode: 256*64. Effective CLAGacity Mode : 256*64. Available CLAGacity Mode : 256*64. Total Number : 256, Used: 1, Available: 255.

3.3.6 Настройка предпочтительного порта-участника LAG

Сценарий

- Настройте порт участника в качестве предпочтительного порта-участника LAG.
- После настройки предпочтительного порта-участника пакеты управляющей VLAN на порту LAG пересылаются данным портом.

Примечания

- Подробнее о настройке управляющей VLAN см. в разделе *Настройка MAC*.
- Для одного порта LAG можно настроить только один предпочтительный порт-участник.
- Если после настройки порта-участника LACP LAG в качестве предпочтительного порта-участника LAG происходит сбой согласования LACP на всех портах-участках LAG, предпочтительный порт автоматически понижается до статического порта-участника LAG.

Этапы конфигурации

Настройка предпочтительного порта-участника LAG

- (Дополнительно) Выполните эту настройку, чтобы указать порт участника LAG, выделенный для пересылки пакетов VLAN управления.
- Конфигурация применима к двухсистемным серверам. Настройте порт, подключенный к сетевой интерфейсной плате управления сервера, в качестве предпочтительного порта-участника LAG.

Команда	**aggregateport primary-port**
Описание параметра	Недоступно

Установки по умолчанию	По умолчанию порт-участник LAG не является предпочтительным.
Режим команды	Режим конфигурации интерфейса порта-участника LAG
Встроенная подсказка	Недоступно

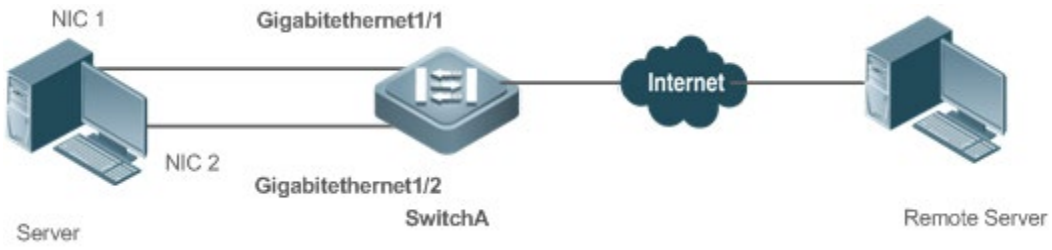
Проверка конфигурации

- Запустите команду **show run** для отображения конфигурации.
- Запустите **show interface aggregateport** для отображения предпочтительного порта-участника LAG.

Команда	**show interface aggregateport** *LAG-num*
Описание параметра	*LAG-num:* Указывает номер агрегированного порта.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
	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 …

Пример конфигурации

Настройка предпочтительного порта-участника LAG

Сценарий **Изображение 3-7**	
Этапы конфигурации	❖ Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A и добавьте порты в LACP LAG 3. ❖ Настройте порт GigabitEthernet 1/1 на коммутаторе A в качестве предпочтительного порта. ❖ Настройте VLAN 10 на коммутаторе A в качестве VLAN управления.

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)# 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 конфигурации	❖ Запустите команду **show run**, чтобы проверить, действует ли конфигурация. ❖ Запустите команду **show interface aggregateport** для отображения предпочтительного порта-участника LAG.

Коммутатор 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
  …
```

3.3.7 Настройка минимального количества портов-участников LACP LAG

Сценарий

- После настройки минимального количества портов LACP LAG группа агрегации действует только в том случае, если количество портов-участников превышает минимальное число.

Примечания

Недоступно

Этапы конфигурации

Настройка минимального количества портов-участников LACP LAG

- (Дополнительно) Выполните эту настройку, чтобы указать минимальное количество портов LACP LAG.

Команда	**aggregateport minimum member** *number*
Описание параметра	*number*: Указывает минимальное количество портов-участников.
Установки по умолчанию	По умолчанию минимальное количество портов-участников равно 0.
Режим команды	Режим конфигурации интерфейса указанного порта LAG
Встроенная подсказка	Недоступно

Проверка конфигурации

- Запустите команду **show run** для отображения конфигурации.
- Запустите команду **show interface aggregateport**, чтобы отобразить состояние портов-участников LAG.

Команда	**show interface aggregateport** *LAG-num*
Описание параметра	*LAG-num:* Указывает номер агрегированного порта.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
	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 …

Пример конфигурации

Настройка минимального количества портов-участников LACP LAG

Сценарий **Изображение 3-8**	
Этапы конфигурации	❖ Включите LACP для портов GigabitEthernet 1/1 и GigabitEthernet 1/2 на коммутаторе A и добавьте порты в LACP LAG 3. ❖ Включите LACP для портов GigabitEthernet 2/1 и GigabitEthernet 2/2 на коммутаторе B и добавьте порты в LACP LAG 3. ❖ На коммутаторе A установите минимальное количество портов-участников LAG 3 на 3.
Коммутатор	SwitchA# configure terminal

A	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 2
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)# aggregateport minimum member 2
Проверка конфигурации	❖ Запустите команду **show run**, чтобы проверить, действует ли конфигурация. ❖ Запустите команду **show lacp summary**, чтобы отобразить состояние агрегирования каждого порта-участника LAG.
Коммутатор A	SwitchA# show LACP summary 3 System Id:32768, 00d0.f8fb.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 ----------

	- Gi2/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d Gi2/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d

3.4 Мониторинг

Отображение

Описание	Команда
Отображает конфигурацию профиля расширенной балансировки нагрузки.	**show load-balance-profile** [*profile-name*]
Отображает состояние агрегирования LACP. Можно отобразить информацию об указанном порте LACP LAG, указав *key-number*.	**show lacp summary** [*key-numebr*]
Отображает алгоритм сводки или балансировки нагрузки порта LAG.	**show aggregateport** [*LAG-number*] { **load-balance** | **summary** }
Отображает режим емкости и использование порта LAG.	**show aggregateport cLAGacity**

Отладка

⚠ При выводе отладочной информации используются ресурсы системы. Поэтому, отключите отладку сразу после использования.

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

4 НАСТРОЙКА КЛАСТЕРА ECMP

4.1 Обзор

Кластер ECMP (множественный путь с равной стоимостью) — это технология для балансировки нагрузки при изменении пути следующего перехода протокола ECMP.

Кластер балансировки нагрузки в центре обработки данных обычно связывается с устройством TOR (верхнее устройство в стойке) через ECMP, а устройство TOR распределяет трафик данных сбалансированным образом между участниками кластера балансировки нагрузки через ECMP.

Если маршрут ECMP создается между устройством TOR и кластером балансировки нагрузки посредством протокола динамической маршрутизации, протокол динамической маршрутизации позволяет повторно выполнять конвергенцию маршрута при сбое канала маршрута ECMP. Трафик от устройства TOR к кластеру балансировки нагрузки перераспределяется, что нарушает исходное состояние сеанса участников кластера. В результате всему кластеру необходимо восстановить сеансы, что приведет к прерыванию некоторых сеансов.

Кластер ECMP позволяет преодолеть перебалансировку трафика, вызванную изменениями в количестве путей ECMP. После настройки кластера ECMP, если количество путей ECMP уменьшаются, только трафик, на неисправных каналах, балансируется на активные каналы, а исходный трафик, передаваемый по активным каналам, остается неизменным. Если количество путей ECMP увеличивается, некоторый трафик, передаваемый по активным каналам, распределяется по новым каналам.

Если следующий переход ECMP чувствителен к сеансу, то есть, если выходное устройство следующего переходом трафика является терминалом (например, сервер), рекомендуется кластер ECMP. Если выход следующего перехода является промежуточным сетевым узлом, кластер ECMP не приносит выгоды.

4.2 Применение

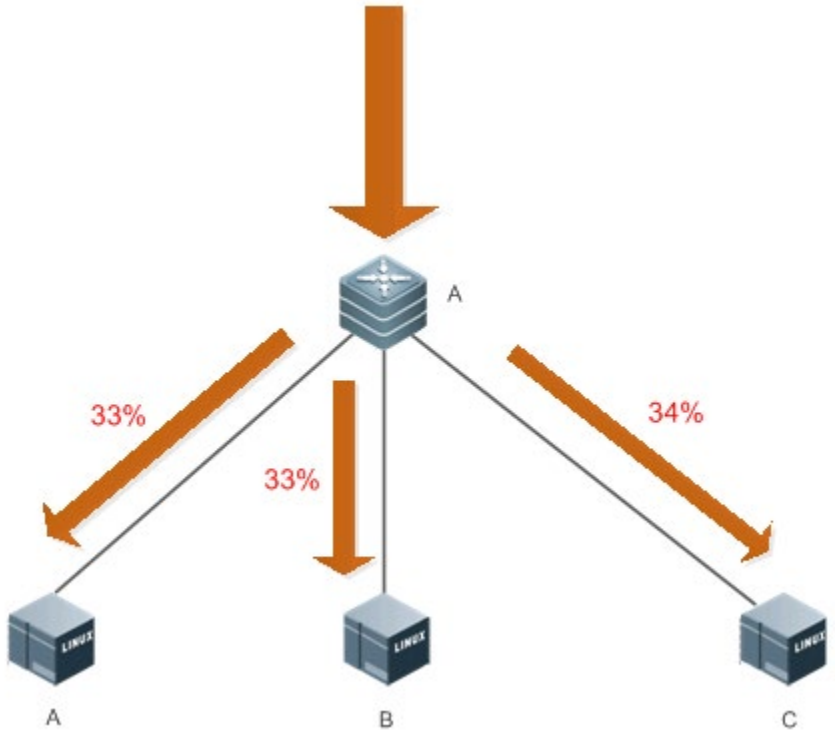
Применение	Описание
Подключение кластера балансировки нагрузки LVS к устройству TOR через ECMP	Устройство TOR подключено к серверу с учетом сеанса через ECMP.

4.2.1 Подключение кластера балансировки нагрузки LVS к устройству TOR через ECMP

Сценарий

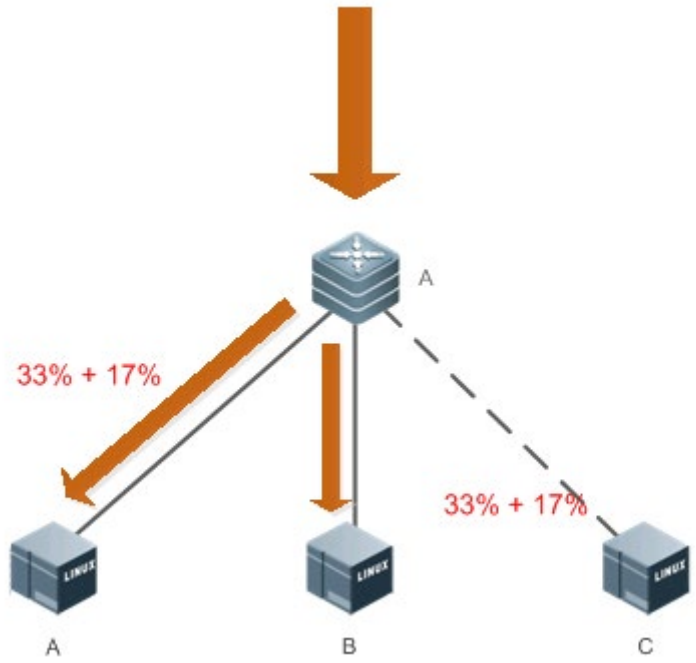
Как показано на Изображении 4-1, устройство TOR подключено к кластеру балансировки нагрузки виртуального сервера Linux (LVS) через ECMP.

Изображение 4-1 Взаимосвязь между устройством TOR и кластером балансировки нагрузки LVS через ECMP



При сбое соединения между устройством A и устройством C трафик пересылается, как показано на Изображении 4-2.

Изображение 4-2 Пересылка трафика



Примечание: A — это коммутатор TOR, а B, C и D — участники кластера балансировки нагрузки.

Описание

- Запустите протокол Open Shortest Path First (OSPF) между устройством TOR и участниками кластера балансировки нагрузки, чтобы реализовать маршрутизацию с множественными путями.
- Включите кластер ECMP на устройстве TOR.

4.3 Функции

Базовые концепции

Маршрутизация ECMP

Существует несколько маршрутов к следующему переходу, направленному на сеть назначения, например, IP-адрес сети назначения — 192.168.0.0/24, и IP-адреса маршрутизаторов к следующему переходу — 1.1.1.1, 2.2.2.2 и 3.3.3.3.

Обзор

Функция	Описание
Кластер ECMP	При изменении следующего перехода маршрута ECMP необходимо поддерживать балансировку нагрузки и равномерно распределять трафик, передаваемый по неисправным каналам, на другие активные каналы, сохраняя при этом исходный трафик, передаваемый активными каналами, неизменным.

Принцип работы

Сохраняет модуль хеш-функции, используемой при расчете маршрута, во время маршрутизации пакетов ECMP, неизменным. Убедитесь, что общее число следующих переходов остается неизменным во время аппаратной маршрутизации ECMP, а при сбое следующего перехода маршрута ECMP для замены отказавшего канала используется активный канал.

4.4 Конфигурация

Конфигурация	Описание и команда	
Настройка кластера ECMP	⚠ (Обязательно) Используется для включения кластера ECMP.	
	ecmp cluster enable	Включает кластер ECMP.

4.4.1 Настройка кластера ECMP

Сценарий

- Увеличение или уменьшение числа последующих переходов ECMP для минимизации влияния исходного пересылаемого трафика после включения кластера ECMP.

Примечания

- Кластер ECMP применяется для ECMP. Поэтому в сети необходимо настроить ECMP.

Этапы конфигурации

Включение кластера ECMP

- Обязательно.

Команда	**ecmp cluster enable**
Описание параметра	**Недоступно**
Установки по умолчанию	По умолчанию кластер ECMP отключен.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Выполните форму данной команды с no, чтобы отключить кластер ECMP: **no ecmp cluster enable**.

Проверка конфигурации

- После включения кластера ECMP проверьте, сбалансирован ли трафик, пересылаемый по множественным путям.
- После сбоя канала проверьте, распределен ли трафик, передаваемый по неисправному каналу, на другие активные каналы, и не изменился ли исходный трафик, передаваемый активными каналами.

Примеры конфигурации

- Включите кластер ECMP на коммутаторе и проверьте, включена ли функция ECMP.

```
QTECH(config)#ecmp cluster enable
QTECH(config)#QTECH(config)#show run | in ecmp
ecmp cluster enable
QTECH(config)#
```

4.5 Мониторинг

Отображение

Описание	Команда
Показывает, включен ли кластер ECMP.	**show run**

5 КОНФИГУРИРОВАНИЕ VLAN

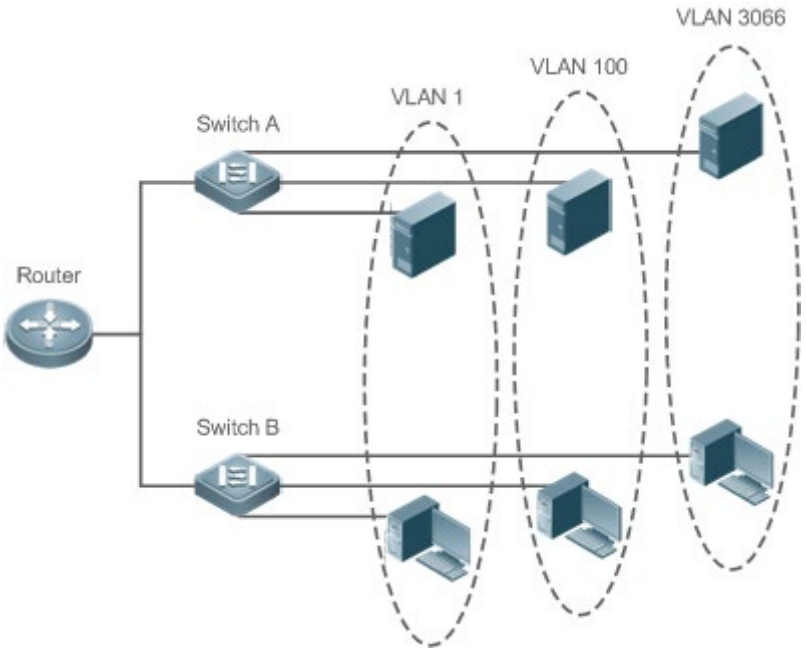
5.1 Обзор

Виртуальная локальная сеть (VLAN) — это логическая сеть, созданная на основе физической сети. Сеть VLAN может быть классифицирована как сеть 2-го уровня модели OSI.

VLAN имеет те же свойства, что и обычная локальная сеть, за исключением ограничений по физическому местоположению. Одноадресные, широковещательные и многоадресные кадры 2-го уровня пересылаются и передаются в пределах VLAN, сохраняя трафик изолированным.

Мы можем определить порт как участник VLAN, и все терминалы, подключенные к этому порту, являются частями виртуальной сети, поддерживающей несколько VLAN. При добавлении, удалении и изменении пользователей нет необходимости физически настраивать сеть. Обмен данными между сетями VLAN осуществляется с помощью устройств 3-го уровня, как показано на следующем Изображении.

Изображение 5-1



Протоколы и стандарты

- IEEE 802.1Q

5.2 Применение

Применение	Описание
Изоляция сетей VLAN на	Интрасеть разделена на несколько сетей VLAN, что

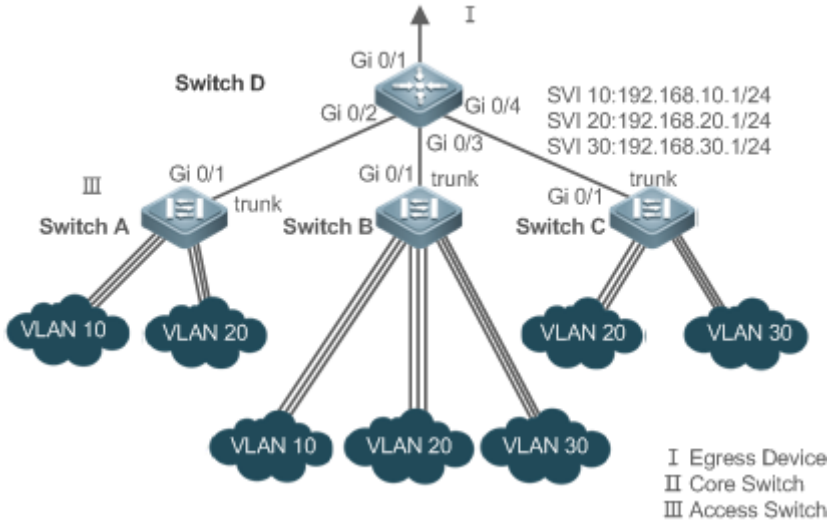
2-м уровне и взаимосвязь сетей VLAN на 3-м уровне	позволяет реализовать изоляцию на 2-м уровне и взаимосвязать сети VLAN на 3-м уровне посредством пересылки по IP с помощью коммутаторов уровня ядра.

5.2.1 Изоляция сетей VLAN на 2-м уровне и взаимосвязь сетей VLAN на 3-м уровне

Сценарий

Интрасеть разделена на VLAN 10, VLAN 20 и VLAN 30, реализуя изоляцию между собой на 2-м уровне. Три сети 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 пересылки по IP с помощью коммутаторов ядра 3-го уровня.

Изображение 5-2



Примечания:	Коммутаторы A, B и C работают на уровне доступа. Настройте три сети VLAN на коммутаторе уровня ядра и порт, подключенный к коммутаторам доступа как магистральный порт, и укажите список разрешенных сетей VLAN для реализации изоляции на 2-м уровне; Настройте три интерфейса SVI на коммутаторе уровня ядра, которые являются интерфейсами шлюза подсетей IP, соответствующих трем VLAN, и настройте IP-адреса для этих интерфейсов. Создайте VLAN на трех коммутаторах доступа, назначьте порты доступа для VLAN и укажите магистральные порты коммутатора уровня ядра.

Описание

- Разделите интрасеть на несколько VLAN, чтобы обеспечить изоляцию на 2-м уровне.
- Настройте SVI на коммутаторе уровня 3 для реализации связи на 3-м уровне между сетями VLAN.

5.3 Функции

Базовые концепции

VLAN

VLAN — это логическая сеть, созданная на основе физической сети. VLAN имеет те же свойства, что и обычная локальная сеть, за исключением ограничений по физическому местоположению. Одноадресные, широковещательные и многоадресные кадры 2-го уровня пересылаются и передаются в пределах VLAN, сохраняя трафик изолированным.

- Сети VLAN, поддерживаемые коммутаторами QTECH, соответствуют стандарту IEEE802.1Q. Поддерживается не более 4094 VLAN (идентификатор VLAN 1-4094), VLAN 1 не может быть удалена.
- Настраиваемые идентификаторы VLAN могут быть от 1 до 4094.
- В случае нехватки аппаратных ресурсов система возвращает информацию о сбое создания VLAN.

Режим порта

Можно определить кадры, которым разрешено проходить порт, и сети VLAN, к которым принадлежит порт, настроив режим порта. Подробнее см. в следующей таблице.

Режим порта	Описание
Порт доступа	Порт доступа принадлежит только одной VLAN, которая задается вручную.
Магистральный порт (802.1Q)	По умолчанию магистральный порт принадлежит всем VLAN коммутатора доступа, и он может пересылать кадры всех VLAN или кадры разрешенных VLAN.
Порт восходящего канала	Порт восходящего канала по умолчанию принадлежит всем VLAN коммутатора доступа, и он может пересылать кадры всех VLAN и тегировать выходной трафик DSP-сети VLAN.
Гибридный порт	По умолчанию гибридный порт принадлежит всем сетям VLAN коммутатора доступа, и он может пересылать кадры всех сетей VLAN и отправлять кадры нетегированных сетей VLAN. Он также может передавать кадры разрешенных сетей VLAN.

Обзор

Функция	Описание
VLAN	VLAN помогает реализовать изоляцию на 2-м уровне.

5.3.1 VLAN

Каждая VLAN имеет независимый широковещательный домен, а различные VLAN изолированы на 2-м уровне.

Принцип работы

Каждая VLAN имеет независимый широковещательный домен, а различные VLAN изолированы на 2-м уровне.

Изоляция на 2-м уровне: Если для сетей VLAN не настроены SVI, сети VLAN изолируются на 2-м уровне. Это означает, что пользователи этих сетей VLAN не могут обмениваться данными друг с другом.

Взаимосвязь на 3-м уровне: Если SVI настроены на коммутаторе 3-го уровня для сетей VLAN, эти сети VLAN могут обмениваться данными друг с другом на 3-м уровне.

5.4 Конфигурация

Конфигурация	Описание и команда	
Настройка базовой VLAN	⚠ (Обязательно) Используется для создания VLAN.	
	vlan	Вводит идентификатор VLAN.
	⚠ (Дополнительно) Используется для настройки порта доступа для передачи потоков из отдельностоящей VLAN.	
	switchport mode access	Определяет порт как порт доступа 2-го уровня.
	switchport access vlan	Назначает порт сети VLAN.
	add interface	Добавляет один порт доступа или группу таких портов в текущую VLAN.
	⚠ (Дополнительно) Используется для переименования VLAN.	
	name	Назначает имя VLAN.
Настройка порта магистральной линии	⚠ (Обязательно) Используется для настройки порта как магистрального порта.	
	switchport mode trunk	Определяет порт как магистральный порт 2-го уровня.
	⚠ (Дополнительно) Используется для настройки магистральных	

	портов для передачи потоков из нескольких VLAN.	
	switchport trunk allowed vlan	Настраивает разрешенные сети VLAN для магистрального порта.
	switchport trunk native vlan	Указывает DSP-сеть VLAN для магистрального порта.
Настройка порта восходящего потока	⚠ (Обязательно) Используется для настройки порта как порта восходящего потока.	
	switchport mode uplink	Настраивает порт в качестве порта восходящего потока (Uplink).
	⚠ (Дополнительно) Используется для восстановления режима порта.	
	no switchport mode	Восстанавливает режим порта.
Настройка гибридного порта	⚠ (Обязательно) Используется для настройки порта в качестве гибридного порта.	
	switchport mode hybrid	Настраивает порт в качестве гибридного порта.
	⚠ (Дополнительно) Используется для передачи кадров нескольких нетегированных сетей VLAN.	
	no switchport mode	Восстанавливает режим порта.
	switchport hybrid allowed vlan	Настраивает разрешенные сети VLAN для гибридного порта.
	switchport hybrid native vlan	Настраивает VLAN по умолчанию для гибридного порта.

5.4.1 Настройка базовой VLAN

Сценарий

❖ Сеть VLAN идентифицируется ее VLAN ID. Можно добавлять, удалять, изменять VLAN от 2 до 4094, но VLAN 1 создается автоматически и не может быть удалена. Можно настроить режим порта и добавить или удалить VLAN.

Примечания

❖ Недоступно

Этапы конфигурации

Создание и изменение VLAN

- Обязательно.
- В случае нехватки аппаратных ресурсов система возвращает информацию о сбое создания VLAN.
- Используйте команду **vlan** *vlan-id* для создания VLAN или входа в режим VLAN.
- Конфигурация:

Команда	**vlan** *vlan-id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN в диапазоне от 1 до 4094.
Установки по умолчанию	VLAN 1 создается автоматически и не может быть удалена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	При вводе нового идентификатора VLAN будет создана соответствующая VLAN. При вводе существующего идентификатора VLAN соответствующая VLAN будет изменена. Для удаления VLAN можно использовать команду **no vlan** *vlan-id*. К неизменным VLAN относятся VLAN1, а также VLAN, настроенные с SVI, и SubVLAN.

Переименование VLAN

- Опционально.
- Невозможно переименовать VLAN так же, как и имя по умолчанию другой VLAN.
- Конфигурация:

Команда	**name** *vlan-name*
Описание параметра	*vlan-name*: указывает имя VLAN.
Установки по умолчанию	По умолчанию имя VLAN является его идентификатором VLAN. Например, имя VLAN 4 по умолчанию — VLAN 0004.
Режим команды	Режим конфигурирования VLAN

Встроенная подсказка	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 2-го уровня (порты коммутатора) в качестве портов доступа.
- Используйте команду **switchport access vlan** *vlan-id* для добавления порта доступа к определенной VLAN, чтобы потоки из VLAN могли передаваться через порт.
- Конфигурация:

Команда	**switchport mode access**
Описание параметра	Недоступно
Установки по умолчанию	Порт коммутатора по умолчанию является портом доступа.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Команда	**switchport access vlan** *vlan-id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN.
Установки по умолчанию	Порт доступа по умолчанию добавляется в VLAN 1.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если порт назначен несуществующей VLAN, VLAN создается автоматически.

Добавление порта доступа к текущей VLAN

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

Команда	**add interface** { *interface-id* | **range** *interface-range* }
Описание параметра	*interface-id*: указывает на один порт. *interface-range:* указывает несколько портов.
Установки по умолчанию	По умолчанию все порты Ethernet 2-го уровня принадлежат VLAN 1.
Режим команды	Режим конфигурирования VLAN
Встроенная подсказка	В режиме настройки VLAN добавьте определенный порт доступа в VLAN. Эта команда действует так же, как команда **switchport access vlan** *vlan-id*.

Для двух команд добавления порта в VLAN, команда, настроенная позже, перезаписывает другую.

Проверка конфигурации

- Отправьте нетегированные пакеты на порт доступа для широковещательной рассылки в VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, действует ли конфигурация.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметра	*vlan-id* **:** Указывает идентификатор VLAN.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
Отображение команд	`QTECH(config-vlan)#show vlan id 20` `VLAN Name Status Ports`

```
---- -------------------------------- --------- ------------------
---------------
 20 VLAN0020                         STATIC    Gi0/1
```

Пример конфигурации

Настройка базовой VLAN и порта доступа

Этапы конфигурации	❖ Создайте и переименуйте VLAN. ❖ Добавьте порт доступа в VLAN. Существует два подхода. Один из них:

	`QTECH# configure terminal`
	`QTECH(config)# vlan 888`
	`QTECH(config-vlan)# name test888`
	`QTECH# configure terminal`
	`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 заключается в добавлении порта доступа (GigabitEthernet 0/3) к VLAN20:
	`QTECH# configure terminal`
	`SwitchA(config)#vlan 20`
	`SwitchA(config-vlan)#add interface GigabitEthernet 0/3`

Проверка конфигурации	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

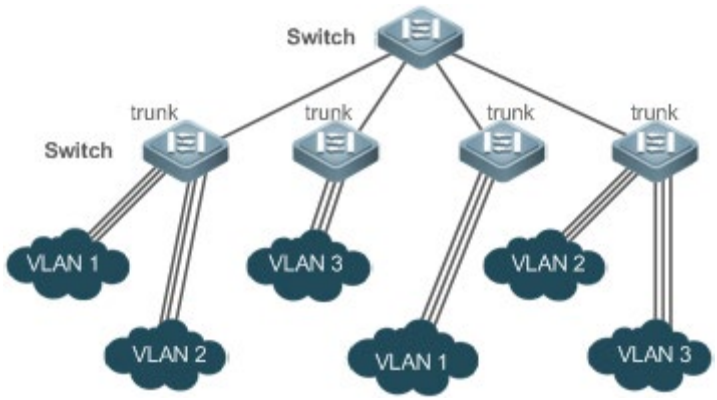
5.4.2 Конфигурирование магистрального порта

Сценарий

Магистральный канал — это канал "точка-точка", соединяющий один интерфейс Ethernet или несколько интерфейсов с другими сетевыми устройствами (например, маршрутизатором или коммутатором) и который может передавать потоки из нескольких VLAN.

Магистральный канал устройств QTECH использует стандарт инкапсуляции 802.1Q. На следующем Изображении показана сеть, которая принимает магистральные соединения.

Изображение 5-3



Можно настроить порт Ethernet или агрегированный порт (подробнее см. в разделе *Настройка агрегированного порта*) как магистральный порт.

Необходимо указать DSP-сеть (нативную) VLAN для магистрального порта. Нетегированные пакеты, полученные и отправленные из магистрального порта, считаются принадлежащими нативной VLAN. Идентификатор VLAN по умолчанию (PVID в IEEE 802.1Q) этого магистрального порта — это собственный идентификатор VLAN. Между тем, кадры нативной VLAN, отправляемые по магистральному каналу, нетегированные. По умолчанию нативная VLAN магистрального порта — VLAN 1.

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

Этапы конфигурации

Конфигурирование магистрального порта

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

Команда	**switchport mode trunk**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию используется режим доступа, который можно изменить на магистральный.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить все свойства магистрального порта по умолчанию, используйте команду **no switchport mode**.

Определение разрешенных сетей VLAN для магистрального порта

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

Команда	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Описание параметра	В качестве параметра vlan-list может использоваться VLAN или несколько VLAN, а идентификаторы VLAN соединяются по порядку символом "-". Например: 10-20. **all** указывает на то, что разрешенные VLAN включают все VLAN; **add** указывает на добавление определенной VLAN в список разрешенных VLAN; **remove** указывает на удаление определенной VLAN из списка разрешенных VLAN; **except** указывает на добавление всех VLAN, кроме тех, что указаны в списке VLAN, в список разрешенных VLAN. **only** указывает только на добавление перечисленных VLAN в список разрешенных VLAN и удаление других VLAN из списка.
Установки по умолчанию	Магистральный порт и порт Uplink относятся ко всем сетям VLAN.

Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить конфигурацию магистрального порта по умолчанию (**all**), используйте команду **no switchport trunk allowed vlan**.

Конфигурирование нативных VLAN

- Опционально.
- Магистральный порт получает и отправляет помеченные или нетегированные кадры 802.1Q. Нетегированные кадры передают потоки из нативной VLAN. По умолчанию, нативная VLAN - это VLAN 1.
- Если кадр содержит идентификатор VLAN нативной VLAN, то при прохождении через магистральный порт его тег будет автоматически убран.
- Конфигурация:

Команда	**switchport trunk native vlan** *vlan-id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN.
Установки по умолчанию	Значение по умолчанию для магистрального порта/порта восходящего канала (Trunk/Uplink) — VLAN 1.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить нативную VLAN для магистрального порта на значение по умолчанию, используйте команду **no switchport trunk native vlan**.

При установке нативной VLAN порта на несуществующую VLAN эта VLAN не будет создана автоматически. Кроме того, нативная VLAN может находиться вне списка разрешенных VLAN для этого порта. В этом случае потоки из нативной VLAN не могут пройти через порт.

Проверка конфигурации

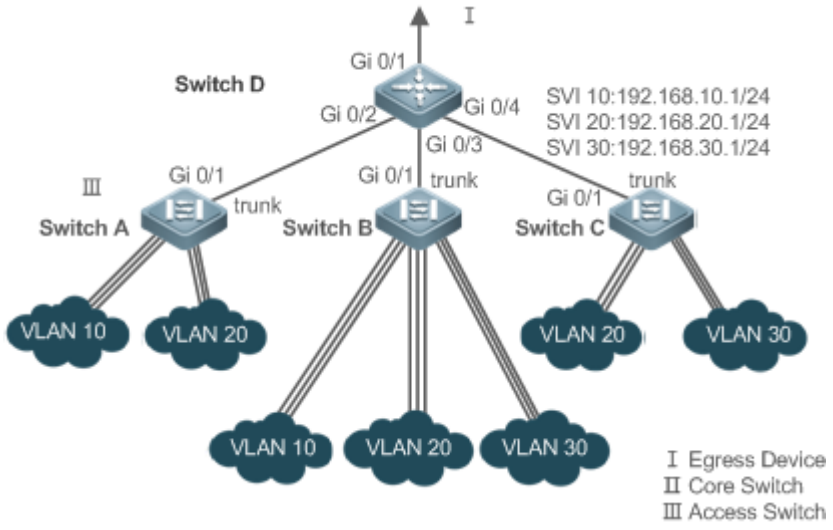
- Отправьте тегированные пакеты на магистральный порт, и они будут разосланы широковещательно в указанные VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, действует ли конфигурация.

Команда	**show vlan** [**id** *vlan-id*]

Описание параметра	*vlan-id* **:** Указывает идентификатор VLAN.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ------------------- 20 VLAN0020 STATIC Gi0/1

Пример конфигурации

Настройка базовой VLAN для реализации изоляции на 2-м уровне и взаимосвязи на 3-м уровне

Сценарий Изображение 5-4	
Этапы конфигурации	Требования к сети: Как показано на Изображении выше, интрасеть разделена на VLAN 10, VLAN 20 и VLAN 30, реализуя изоляцию между собой на 2-м уровне. Три сети 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 пересылки по IP с помощью коммутаторов ядра 3-го уровня. Ключевые моменты: В следующем примере описаны этапы настройки на коммутаторе

	уровня ядра и коммутаторе доступа. ❖ Настройте три сети VLAN на коммутаторе уровня ядра и порт, подключенный к коммутаторам доступа как магистральный порт, и укажите список разрешенных сетей VLAN для реализации изоляции на 2-м уровне; ❖ Настройте три интерфейса SVI на коммутаторе уровня ядра, которые являются интерфейсами шлюза подсетей IP, соответствующих трем VLAN, и настройте IP-адреса для этих интерфейсов. ❖ Создайте VLAN на трех коммутаторах доступа, назначьте порты доступа для VLAN и укажите магистральные порты коммутатора уровня 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 0/2)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20,30 D(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/4 D(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094 D(config-if-GigabitEthernet 0/2)#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 конфигурации	Отображение конфигурации VLAN на коммутаторе уровня ядра. ❖ Отобразите информацию о VLAN, включая идентификаторы VLAN, имена VLAN, состояние и задействованные порты. ❖ Отобразите состояние 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      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/2                 enabled     TRUNK      1      1
```

```
Disabled  10,20
D#show interface GigabitEthernet 0/3 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/3                 enabled     TRUNK      1      1
Disabled  10,20,30
D#show interface GigabitEthernet 0/4 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/4                 enabled     TRUNK      1      1
Disabled  20,30
```

Типичные ошибки

- Недоступно

5.4.3 Настройка порта восходящего потока

Сценарий

- Порт восходящего потока (Uplink) обычно используется в среде QinQ (стандарт IEEE 802.1ad) и аналогичен магистральному порту (Trunk). Их отличие заключается в том, что порт Uplink передает только тегированные кадры, а порт Trunk отправляет нетегированные кадры нативной VLAN.

Этапы конфигурации

Настройка порта восходящего потока

- Обязательно.
- Настройте порт Uplink для передачи потоков из нескольких сетей VLAN, но передаются только тегированные кадры.
- Конфигурация:

Команда	**switchport mode uplink**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию используется режим доступа, который можно изменить на Uplink.
Режим команды	Режим конфигурации интерфейса

Встроенная подсказка	Чтобы восстановить все свойства порта Uplink по умолчанию, используйте команду **no switchport mode**.

Определение разрешенных сетей VLAN для магистрального порта

- Опционально.
- Можно настроить список разрешенных сетей VLAN, чтобы запретить прохождение потоков некоторых сетей VLAN через порт Uplink.
- Конфигурация:

Команда	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Описание параметра	В качестве параметра *vlan-list* может использоваться VLAN или несколько VLAN, а идентификаторы VLAN соединяются по порядку символом "-". Например: 10-20. **all** указывает на то, что разрешенные VLAN включают все VLAN; **add** указывает на добавление определенной VLAN в список разрешенных VLAN; **remove** указывает на удаление определенной VLAN из списка разрешенных VLAN; **except** указывает на добавление всех VLAN, кроме тех, что указаны в списке VLAN, в список разрешенных VLAN; **only** указывает только на добавление перечисленных VLAN в список разрешенных VLAN и удаление других VLAN из списка.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить для разрешенных VLAN значение по умолчанию (**all**), используйте команду **no switchport trunk allowed vlan**.

Конфигурирование нативных VLAN

- Опционально.
- Если кадр содержит идентификатор VLAN нативной сети VLAN, то при прохождении через порт Uplink тег не будет убран. Это противоречит магистральному порту.
- Конфигурация:

Команда	**switchport trunk native vlan** *vlan-id*
Описание	*vlan-id*: указывает идентификатор VLAN.

параметра	
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить нативную VLAN канала Uplink в значения по умолчанию, используйте команду **no switchport trunk native vlan**.

Проверка конфигурации

- ❖ Отправка тегированных пакетов на порт Uplink, и передача их через указанные VLAN.
- ❖ Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, действует ли конфигурация.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметра	*vlan-id*: указывает идентификатор VLAN.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- -------------------- --------------- 20 VLAN0020 STATIC Gi0/1

Пример конфигурации

Настройка порта восходящего потока

Этапы конфигурации	Ниже приведен пример настройки Gi0/1 в качестве порта Uplink.
	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 конфигурации	Проверьте правильность конфигурации.
	QTECH# show interfaces GigabitEthernet 0/1 switchport Interface Switchport Mode Access Native Protected VLAN lists -------------------------------- ---------- --------- ------ ------ --------- ----------------- GigabitEthernet 0/1 enabled **UPLINK** 1 1 disabled ALL

5.4.4 Настройка гибридного порта

Сценарий

- Гибридный порт обычно используется в общей среде VLAN. По умолчанию гибридный порт совпадает с магистральным портом. Их отличие заключается в том, что гибридный порт может отправлять кадры из VLAN в нетегированном формате, за исключением VLAN по умолчанию.

Этапы конфигурации

Настройка гибридного порта

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

Команда	**switchport mode hybrid**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию используется режим доступа, который можно изменить на гибридный.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить все свойства гибридного порта по умолчанию, используйте команду **no switchport mode**.

Определение разрешенных сетей VLAN для гибридного порта

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

Команда	**switchport hybrid allowed vlan** [[**add** | **only**] **tagged** | **untaged** | **remove**] *vlan_list*
Описание параметра	*vlan-id*: указывает идентификатор VLAN.
Установки по умолчанию	По умолчанию гибридный порт принадлежит всем сетям VLAN. Порт добавляется в сеть VLAN по умолчанию в нетегированном виде и в другие сети VLAN в тегированном виде.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Конфигурирование нативных VLAN

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

Команда	**switchport hybrid native vlan** *vlan_id*
Описание параметра	*vlan-id*: указывает идентификатор VLAN.
Установки по умолчанию	По умолчанию, нативная VLAN - это VLAN 1.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы восстановить исходные настройки VLAN для гибридного порта по умолчанию, используйте команду **no switchport hybrid native vlan**.

Проверка конфигурации

- Отправьте тегированные пакеты на гибридный порт, и они будут разосланы широковещательно в указанные VLAN.
- Используйте команды **show vlan** и **show interface switchport**, чтобы проверить, действует ли конфигурация.

Команда	**show vlan** [**id** *vlan-id*]
Описание параметра	*vlan-id* **:** Указывает идентификатор VLAN.
Режим команды	Любой режим
Встроенная подсказка	Недоступно
Отображение команд	QTECH(config-vlan)#show vlan id 20 VLAN Name Status Ports ---- -------------------------------- --------- ------------------- ---------- 20 VLAN0020 STATIC Gi0/1

Пример конфигурации

Настройка гибридного порта

Этапы конфигурации	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 конфигурации	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
```

5.5 Мониторинг

Отображение

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

Отладка

⚠ При выводе отладочной информации используются ресурсы системы. Поэтому, отключите отладку сразу после использования.

Описание	Команда
Отладка VLAN	**debug bridge vlan**

6 КОНФИГУРИРОВАНИЕ 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 при динамическом назначении VLAN 802.1X для обеспечения безопасного и гибкого доступа к терминалам 802.1X. После того, как пользователь 802.1X проходит аутентификацию коммутатор доступа автоматически создает запись MAC VLAN на основе VLAN и MAC-адреса пользователя, передаваемого сервером аутентификации. Сетевой администратор также может заранее настроить связь между MAC-адресом и VLAN на коммутаторе.

Протокол

- ❖ IEEE 802.1Q: Виртуальные локальные сети и стандарты с параллельным подключением

6.2 Применение

Применение	Описание
Настройка MAC VLAN	Настройка функции MAC VLAN для назначения VLAN на основе MAC-адресов пользователей. При изменении физического местоположения пользователя, т.е. при переключении с одного коммутатора на другой, нет необходимости повторно настраивать VLAN порта, используемого пользователем.

6.2.1 Конфигурирование MAC VLAN

Сценарий

С популяризацией мобильных офисов терминальные устройства обычно не используют фиксированные порты для доступа к сети. Терминальное устройство может использовать для доступа к сети, как порт A, так и порт B. Если конфигурации VLAN портов A и B отличаются, терминальное устройство будет назначено другой VLAN во время второго доступа и не сможет использовать ресурсы предыдущей VLAN. Если конфигурация VLAN портов A и B одинакова, то при назначении порта B другим терминальным устройствам могут возникнуть проблемы с безопасностью. Как разрешить хостам разных сетей VLAN получать доступ к сети на одном порту? Таким образом, обеспечивается 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 повторно настраивать VLAN порта, используемого пользователем. Таким образом, назначение VLAN на основе MAC-адресов может рассматриваться как назначение на основе пользователей.

Описание

- Настройка или передача записей MAC VLAN на коммутаторе 2-го уровня или беспроводном устройстве для назначения VLAN на основе MAC-адресов пользователей.

6.3 Обзор

Функция

Функция	Описание
Настройка MAC VLAN	Настройка функции MAC VLAN для назначения VLAN на основе MAC-адресов пользователей.

6.3.1 Конфигурирование MAC VLAN

Принцип работы

Когда коммутатор получает пакет, он сравнивает MAC-адрес источника пакета с MAC-адресом, указанным в записи MAC VLAN. Если они совпадают, коммутатор пересылает пакет в 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 определенной VLAN независимо от того, к какому коммутатору он подключен, можно выполнить настройку, используя следующие подходы:

- Статическая конфигурация с помощью команд. Можно 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 переходит в автономный режим, коммутатор автоматически удаляет связь. Этот подход требует настройки связи MAC-VLAN на сервере аутентификации. Подробнее о динамическом назначении VLAN 802.1X см. в разделе Настройка 802.1X.

Записи MAC VLAN поддерживают оба подхода, то есть записи могут быть настроены как на локальном коммутаторе, так и на сервере аутентификации. Эти конфигурации могут быть доступны только в том случае, если они согласованы. Если конфигурации отличаются, то будет действовать конфигурация, выполненная ранее.

- Функцию MAC VLAN можно настроить только на гибридных портах.
- Записи MAC VLAN эффективны только для нетегированных пакетов, но не эффективны для тегированных пакетов.
- Для записей MAC VLAN, которые статически настроены или динамически генерируются, должны существовать указанные VLAN.

- VLAN, указанные в записях MAC VLAN, не могут быть Super VLAN (но могут быть Sub VLAN), Remote VLAN или Primary VLAN (но могут быть и Secondary VLAN).
- MAC-адреса, указанные в записях MAC VLAN, должны быть одноадресными.
- Сети MAC VLAN эффективны для всех гибридных портов, которые включены с функцией MAC VLAN.

6.4 Конфигурация

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

6.4.1 Включение MAC VLAN на порту

Сценарий

Включите функцию MAC VLAN на порту, чтобы записи MAC VLAN могли повлиять на порт.

Примечания

Недоступно

Этапы конфигурации

Включает MAC VLAN на порту

- Обязательно.
- По умолчанию функция MAC VLAN отключена на портах, и все записи MAC VLAN на портах неактивны.
- Включает MAC VLAN на коммутаторе.

Команда	**mac-vlan enable**
Описание параметра	Недоступно
Установки по	Функция MAC VLAN отключена на порту.

умолчанию	
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

❖ Запустите команду **show mac-vlan interface** для отображения информации о портах, включенных с помощью функции MAC VLAN.

Команда	**show mac-vlan interface**
Описание параметра	Недоступно
Режим команды	Режим привилегированной конфигурации/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
Отображение команд	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: --------------------------------------- **FastEthernet 0/1**

Пример конфигурации

Включает MAC VLAN на порту

Этапы конфигурации	❖ 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

конфигурации	MAC VLAN.
	QTECH# show mac-vlan interface MAC VLAN is enabled on following interface: --------------------------------------- **FastEthernet 0/10**

Типичные ошибки

Если функция MAC VLAN включена на порту, порт заранее не настроен как порт 2-го уровня (например, порт коммутатора или порт точки доступа).

6.4.2 Глобальное добавление статической записи MAC VLAN

Сценарий

- Настройте статический ввод MAC VLAN для привязки MAC-адресов к VLAN. Можно настроить приоритет 802.1p, который по умолчанию составляет 0.

Примечания

Недоступно

Этапы конфигурации

Добавление статической записи MAC VLAN

- Опционально.
- Чтобы связать MAC-адреса с VLAN, необходимо выполнить эту настройку. Можно настроить приоритет 802.1p, который по умолчанию составляет 0.
- Добавление статической записи MAC VLAN на коммутаторе.

Команда	**mac-vlan mac-address** *mac-address* [**mask** *mac-mask*] **vlan** *vlan-id* [**priority** *pri_val*]
Описание параметра	**mac-address** *mac-address*: Указывает MAC-адрес. **mask** *mac-mask*: Указывает на маску. **vlan** *vlan-id*: Указывает связанную VLAN. **priority** *pri_val*: Указывает на приоритет.
Установки по умолчанию	По умолчанию статическая запись MAC VLAN не настроена.
Режим команды	Режим глобальной конфигурации

Встроенная подсказка	Недоступно

- Когда пакет поступает на коммутатор, он изменяется на VLAN; если нетегированный пакет сопоставлен с записью MAC VLAN, указанной в результирующей VLAN, то запись MAC VLAN имеет наивысший приоритет. Последующие функции и протоколы реализуются на основе измененной VLAN. Возможные воздействия:
- Если пользователь 802.1X не проходит проверку подлинности, гибридный порт переходит в VLAN 100, указанную функцией FAIL VLAN; однако при статически настроенной записи MAC VLAN все пакеты этого пользователя перенаправляются в VLAN 200. Следовательно, пользователь не может установить нормальное соединение в FAIL VLAN 100.
- После сопоставления нетегированных пакетов с записью MAC VLAN, VLAN, которая запускает Изучение MAC-адресов, перенаправляется на основе записи MAC VLAN.
- Для порта, который включен с функцией MAC VLAN, если полученные пакеты совпадают с записями MAC VLAN с маской ffff.ffff.ffff и с другими масками, пакеты обрабатываются на основе записей MAC VLAN без маски ffff.ffff.ffff.
- Если нетегированный пакет совпадает с записью MAC VLAN и с записью VOICE VLAN, приоритет пакетов изменяется одновременно. Приоритет записи VOICE VLAN используется как приоритет пакета.
- Если нетегированный пакет совпадает с записью MAC VLAN и с записью PROTOCOL VLAN, то в пакете должна быть MAC VLAN.
- Функция MAC VLAN применяется только к нетегированным пакетам, но не применяется к пакетам PRIORITY (пакетам с меткой VLAN 0 и несущей информацией COS PRIORITY), и действия по обработке не ясны.
- По умолчанию режим доверительного доступа к пакетам QoS на коммутаторе отключен, что изменит поле 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 приоритеты доверенных пакетов.

Удаление всех статических записей MAC VLAN

- Опционально.
- Чтобы удалить все статические записи MAC VLAN, необходимо выполнить эту настройку.
- Выполните эту настройку на коммутаторе.

Команда	**no mac-vlan all**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации

Встроенная подсказка	Недоступно

Удаление статической записи MAC VLAN для указанного MAC-адреса

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

Команда	**no mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]
Описание параметра	**mac-address** *mac-address*: Указывает MAC-адрес. **mask** *mac-mask*: Указывает на маску.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Удаление статической записи MAC VLAN для указанной VLAN

- Опционально.
- Чтобы удалить запись MAC VLAN указанной VLAN, необходимо выполнить эту настройку.
- Выполните эту настройку на коммутаторе.

Команда	**no mac-vlan vlan** *vlan-id*
Описание параметра	**vlan** *vlan-id*: Указывает VLAN.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Проверка конфигурации

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

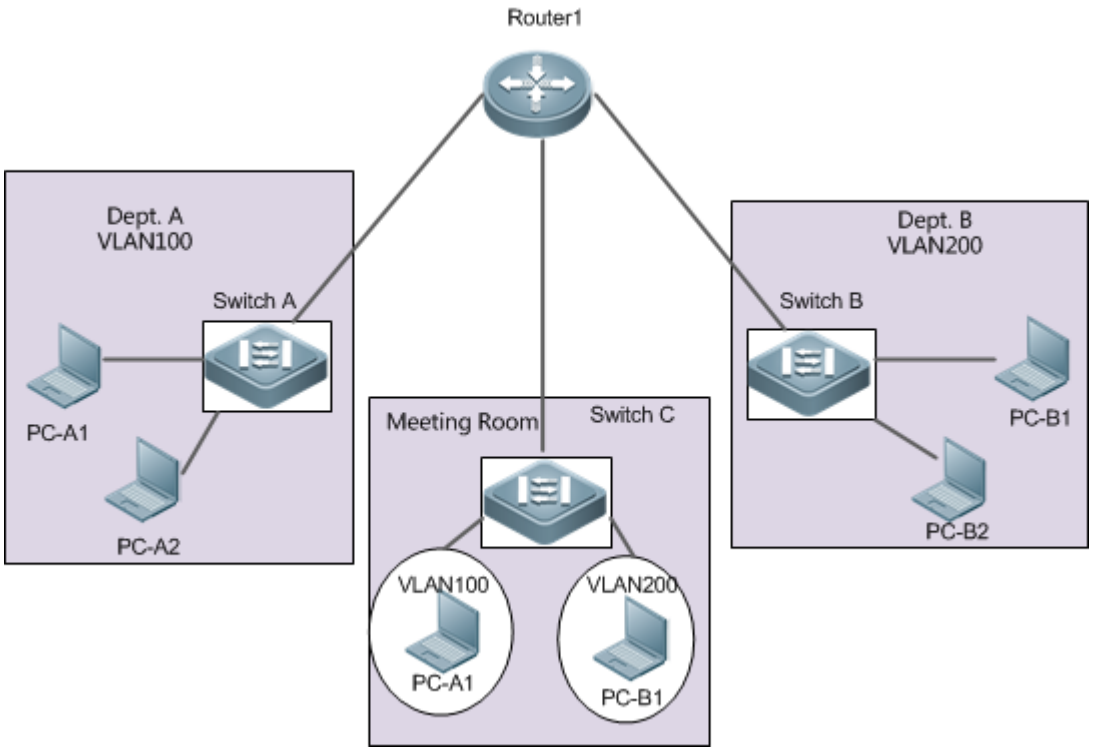
Команда	**show mac-vlan static** show mac-vlan vlan *vlan-id* show mac-vlan mac-address *mac-address* [mask *mac-mask*]
Описание параметра	**vlan** *vlan-id*: Указывает идентификатор VLAN. **mac-address** *mac-address*: Указывает MAC-адрес. **mask** *mac-mask*: Указывает маску.
Режим команды	Режим привилегированной конфигурации/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно
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

Пример конфигурации

Глобальное добавление статической записи MAC VLAN

Как показано на Изображении 6-1, PC-A1 и PC-A2 относятся к отделу A и назначаются VLAN 100. PC-B1 и PC-B2 относятся к отделу B и назначаются VLAN 200. Из-за мобильности сотрудников компания предоставляет временный офис в конференц-зале, но требует, чтобы сотрудники, которые имеют доступ, были назначены в сети VLAN своих отделов. Например, PC-A1 должен быть назначен VLAN 100, а PC-B1 должен быть назначен VLAN 200 после доступа.

Поскольку порты доступа для ПК в конференц-зале не фиксированы, функцию MAC VLAN можно использовать для связывания MAC-адресов ПК с сетями VLAN их отделов. Независимо от портов, используемых сотрудниками для доступа, функция MAC VLAN автоматически назначает VLAN своих подразделений.

Сценарий Изображение 6-1	
Этапы конфигурации	❖ Настройте порт, соединяющий Switch C и Router 1 как магистральный порт. ❖ Настройте порты, соединяющие все ПК на Switch C, как гибридные порты, включите функцию MAC VLAN и измените список нетегированных VLAN по умолчанию. ❖ Настройте записи MAC VLAN на Switch 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 конфигурации	Проверьте настроенные статические записи MAC VLAN на Switch 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**

6.5 Мониторинг

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 указанного MAC-адреса.	**show mac-vlan mac-address** *mac-address* [**mask** *mac-mask*]

Отладка

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

Описание	Команда
Отладка функции MAC VLAN.	**debug bridge mvlan**

7 НАСТРОЙКА SUPER VLAN

7.1 Обзор

Виртуальная локальная суперсеть (VLAN) — это подход к разделению сетей VLAN. Super VLAN также называется агрегированием VLAN и представляет собой технологию управления, специально разработрованную для оптимизации IP-адресов.

Использование Super VLAN может значительно сохранить IP-адреса. Super VLAN, которая состоит из нескольких подсетей VLAN, должна быть назначена только одному IP-адресу, что значительно экономит IP-адреса и облегчает управление сетью.

7.2 Применение

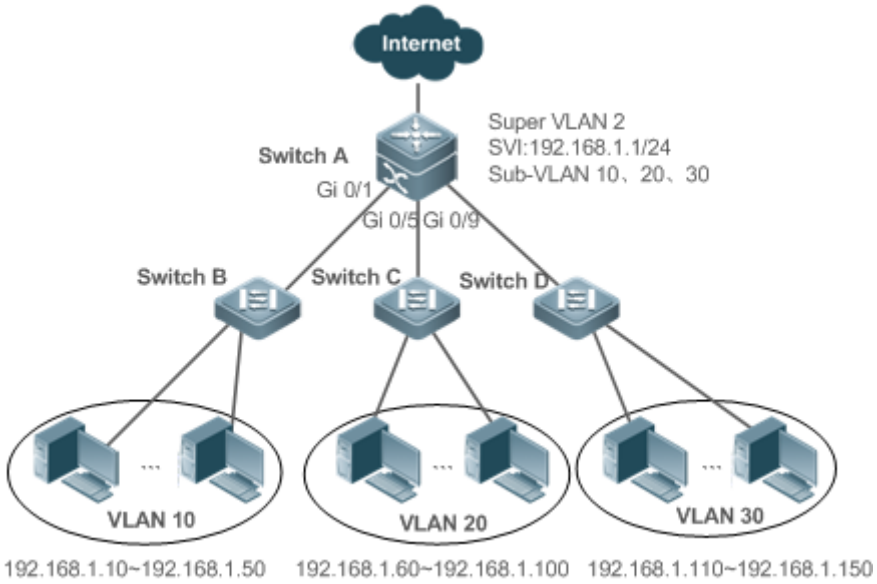
Применение	Описание
Совместное использование одного IP-шлюза между несколькими сетями VLAN	Сети VLAN разделены для реализации изоляции пользователей доступа на 2-м уровне (L2). Все пользователи VLAN совместно используют один IP-шлюз для реализации связи 3-го уровня (L3) и обмена данными с внешними сетями.

7.2.1 Совместное использование одного IP-шлюза между несколькими сетями VLAN

Сценарий

Несколько VLAN изолированы на уровне L2 на устройстве L3, но пользователи этих VLAN могут осуществлять обмен данными уровня L3 между собой в одном и том же сегменте сети.

Изображение 7-1



Заметки	Switch A является шлюзом или коммутатором уровня ядра. Коммутаторы Switch B, C и D являются коммутаторами доступа. На коммутаторе Switch A конфигурируются Super VLAN и несколько Sub VLAN, а интерфейс L3 и IP-адрес интерфейса L3 настроены для Super VLAN. VLAN 10 настраивается на Switch B, VLAN 20 настраивается на Switch C, а VLAN 30 настраивается на Switch D. Различные подразделения компании находятся в разных сетях VLAN.

Описание

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

Пользователи Sub VLAN могут осуществлять обмен данными L3 через шлюз Super VLAN.

7.3 Функции

Базовые концепции

Super VLAN

Super VLAN также называется агрегированием VLAN и представляет собой технологию управления, специально разработрованную для оптимизации IP-адресов. Она объединяет несколько VLAN в один сегмент IP-сети. В Super VLAN не может быть добавлен физический порт. Виртуальный интерфейс коммутации (SVI) используется для управления связи между VLAN и их подсетями. Super VLAN не может использоваться в качестве общей VLAN 802.1Q, но может рассматриваться как основная VLAN подсетей VLAN.

Sub VLAN

Sub VLAN является независимым широковещательным доменом. Подсети VLAN взаимно изолированы на уровне L2. Пользователи подсетей VLAN одной или нескольких суперсетей VLAN обмениваются данными между собой через свои собственные виртуальные локальные сети 3-го уровня.

ARP-прокси

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

Диапазон IP-адресов Sub VLAN

На основе IP-адреса шлюза, настроенного для Super VLAN, можно настроить диапазон IP-адресов для каждой подсети VLAN.

Обзор

Функция	Описание
Super VLAN	Создает интерфейс L3 в качестве SVI, чтобы разрешить всем подсетям VLAN совместно использовать один и тот же сегмент IP-сети через прокси-сервер ARP.

7.3.1 Super VLAN

Пользователям всех подсетей VLAN суперсети могут быть назначены IP-адреса в одном и том же диапазоне IP-адресов, и они могут совместно использовать один и тот же IP-шлюз. Пользователи могут осуществлять обмен данными между сетями VLAN через этот шлюз. Нет необходимости выделять шлюз для каждой VLAN, которая сохраняет IP-адреса.

Принцип работы

IP-адреса в сегменте сети выделяются разным подсетям VLAN, которые принадлежат одной Super VLAN. Каждая подсеть VLAN имеет независимый широковещательный домен VLAN, и различные подсети VLAN изолированы друг от друга на уровне L2. Когда пользователям подсетей VLAN необходимо выполнить обмен данными L3, в качестве адреса шлюза используется IP-адрес SVI суперсети VLAN. 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 подсетями VLAN и другими сегментами сети функция прокси-сервера ARP используется для пересылки и обработки запросов и ответов ARP.

Обмен данными на уровне 2 между подсетями VLAN: Если протокол SVI не настроен для суперсети VLAN, подсети VLAN суперсети VLAN взаимно изолированы на уровне L2, то есть пользователи в разных подсетях VLAN не

могут взаимодействовать между собой. Если SVI настроен для суперсети VLAN, а шлюз суперсети VLAN может функционировать как прокси-сервер ARP, пользователи в разных подсетях VLAN одной и той же суперсети VLAN могут обмениваться данными между собой. Это связано с тем, что IP-адреса пользователей в разных подсетях VLAN принадлежат одному и тому же сегменту сети, а связь между ними по-прежнему рассматривается как связь на уровне L2.

Обмен данными на уровне 3 между подсетями VLAN: Если пользователям в подсетях VLAN суперсети VLAN необходимо выполнить обмен данными L3 между сегментами сети, шлюз этой суперсети VLAN выполняет роль прокси-сервера ARP для ответа на запросы ARP вместо подсетей VLAN.

7.4 Конфигурация

Конфигурационный элемент	Описание и команда	
Настройка основных функций Super VLAN	⚠ Обязательно.	
	supervlan	Настраивает Super VLAN.
	subvlan *vlan-id-list*	Настраивает подсеть VLAN.
	proxy-arp	Включает функцию прокси-сервера ARP.
	interface vlan *vlan-id*	Создает виртуальный интерфейс для Super VLAN.
	ip address *ip mask*	Настраивает IP-адрес виртуального интерфейса Super VLAN.
	ℹ Опционально.	
	subvlan-address-range *start-ip end-ip*	Указывает диапазон IP-адресов в подсети VLAN.

7.4.1 Настройка основных функций Super VLAN

Сценарий

Включите функцию Super VLAN и настройте SVI для Super VLAN, реализуя связь L2/L3 между подсетями VLAN в одной VLAN.

Пользователи во всех подсетях VLAN суперсети VLAN используют один и тот же IP-шлюз. Нет необходимости указывать сетевой сегмент для каждой VLAN, которая сохраняет IP-адреса.

Примечания

⚠ Суперсеть VLAN не принадлежит ни одному физическому порту. Таким образом, устройство, настроенное на использование суперсети VLAN, не может обрабатывать пакеты, содержащие тег суперсети VLAN.

⚠ Необходимо включить как функцию Super VLAN, так и функцию ARP proxy для каждой подсети VLAN.

⚠ Протокол SVI и IP-адрес должны быть настроены для суперсети VLAN. SVI — это виртуальный интерфейс, используемый для связи пользователей во всех подсетях VLAN.

Этапы конфигурации

Настройка Super VLAN

- Обязательно.
- В суперсети VLAN нет физических портов.
- Должна быть включена функция ARP proxy. Данная функция включена по умолчанию.
- Можно выполнить команду **supervlan**, чтобы изменить обычную VLAN на суперсеть VLAN.
- После того как обычная VLAN станет суперсетью VLAN, порты, добавленные в эту VLAN, будут удалены из данной VLAN, так как в суперсети VLAN нет физических портов.

ℹ Super VLAN действительна только после настройки подсетей VLAN для этой суперсети VLAN.

⚠ VLAN 1 не может быть настроена как Super VLAN.

⚠ Суперсеть VLAN не может быть настроена в качестве подсети VLAN другой Super VLAN. Подсеть VLAN суперсети VLAN не может быть настроена в качестве Super VLAN.

Команда	**supervlan**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию сеть VLAN является обычной сетью VLAN.
Режим команды	Режим конфигурирования VLAN
Встроенная подсказка	По умолчанию функция Super VLAN отключена. В Super VLAN не может быть добавлен физический порт. Когда у VLAN отменяется статус суперсети, все ее подсети

	становятся обычными статическими VLAN.

Настройка виртуального интерфейса для Super VLAN

- Обязательно.
- В Super VLAN не может быть добавлен физический порт. Можно настроить SVI уровня L3 для VLAN. IP-шлюз в SVI уровня L3 настроен как прокси-сервер для всех пользователей в подсетях VLAN в ответ на запросы ARP.

⚠ Когда суперсеть VLAN настраивается с помощью SVI, она выделяет интерфейс L3 для каждой подсети VLAN. Если подсети VLAN не назначен интерфейс L3 из-за нехватки ресурсов, подсеть VLAN снова становится обычной VLAN.

Команда	**interface vlan** *vlan-id*
Описание параметра	*vlan-id*: Указывает идентификатор Super VLAN.
Установки по умолчанию	По умолчанию Super VLAN не настроена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Интерфейс L3 должен быть настроен как виртуальный интерфейс суперсети VLAN.

Настройка шлюза суперсети VLAN

- Обязательно.
- IP-шлюз в SVI уровня L3 настроен как прокси-сервер для всех пользователей в подсетях VLAN в ответ на запросы ARP.

Команда	**ip address** *ip mask*
Описание параметра	*ip*: Указывает IP-адрес шлюза в виртуальном интерфейсе суперсети VLAN. *mask*: Указывает маску.
Установки по умолчанию	По умолчанию шлюз не настроен для суперсети VLAN.
Режим команды	Режим конфигурации интерфейса

Встроенная подсказка	Выполните эту команду, чтобы настроить шлюз для суперсети VLAN. Пользователи всех подсетей VLAN суперсети совместно используют этот шлюз.

Настройка подсети VLAN

- Обязательно.
- Физические порты могут быть добавлены в подсети VLAN. Подсети VLAN суперсети совместно используют адрес шлюза суперсети и находятся в одном и том же сегменте сети.
- Должна быть включена функция ARP proxy. Данная функция включена по умолчанию.
- Можно выполнить команду **subvlan** *vlan-id-list*, чтобы изменить обычную VLAN на подсеть суперсети. Физические порты могут быть добавлены в подсети VLAN.
- Связь пользователей в подсети VLAN управляется суперсетью.

⚠ Чтобы удалить данную подсеть VLAN, необходимо изменить подсеть VLAN на обычную VLAN, выполнив команду **no vlan**.

⚠ Одна подсеть VLAN принадлежит только одной суперсети VLAN.

Команда	**subvlan** *vlan-id-list*
Описание параметра	*vlan-id-list* : Указывает несколько VLAN в качестве подсетей суперсети.
Установки по умолчанию	По умолчанию VLAN является обычной сетью VLAN.
Режим команды	Режим конфигурирования VLAN
Встроенная подсказка	Интерфейсы подключения могут быть добавлены в подсеть VLAN. Чтобы удалить данную подсеть VLAN, необходимо изменить ее на обычную VLAN, выполнив команду **no vlan** [*id*]. Нельзя настроить SVI уровня L3 сети VLAN для подсети VLAN. ℹ Если вы настроили SVI уровня L3 для суперсети VLAN, попытка добавления дополнительных подсетей VLAN может быть неудачной из-за нехватки ресурсов. ⚠ Если вы настроите дополнительные VLAN на суперсети, а затем настроите SVI уровня L3 сети VLAN для суперсети, некоторые подсети VLAN могут снова стать обычными VLAN из-за нехватки ресурсов.

Настройка прокси-сервера ARP

- (Обязательно) Функция ARP proxy включена по умолчанию.
- Пользователи в подсетях VLAN могут осуществлять обмен данными L2/L3 между сетями VLAN через прокси-сервер шлюза только после включения функции прокси-сервера ARP как в суперсети, так и в подсетях VLAN.
- Пользователи подсетей VLAN могут взаимодействовать с пользователями других сетей VLAN только после включения функции прокси-сервера ARP в суперсетях и подсетях.

⚠ Функция ARP proxy должна быть включена как в суперсети VLAN, так и в подсети. В противном случае эта функция не будет действовать.

Команда	**proxy-arp**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию функция ARP proxy включена.
Режим команды	Режим конфигурирования VLAN
Встроенная подсказка	По умолчанию функция ARP proxy включена. Выполните данную команду, чтобы включить функцию прокси-сервера ARP как в суперсети, так и в подсети. Пользователи в подсетях VLAN могут осуществлять обмен данными L2/L3 между сетями VLAN только после включения функции прокси-сервера ARP в суперсети и подсетях.

Настройка диапазона IP-адресов подсети VLAN

- Можно назначить диапазон IP-адресов для каждой подсети VLAN. Пользователи подсети VLAN могут взаимодействовать с пользователями других VLAN только в том случае, если их IP-адреса находятся в указанном диапазоне.
- Если не указано иное, не требуется настраивать диапазон IP-адресов.

⚠ IP-адреса, динамически выделяемые пользователям через DHCP, могут не находиться в выделенном диапазоне IP-адресов. Если IP-адреса, выделенные через DCHP, находятся вне указанного диапазона, пользователи подсети VLAN не могут связаться с пользователями других VLAN. Поэтому будьте осторожны при использовании команды **subvlan-address-range** *start-ip end-ip*.

⚠ Диапазон IP-адресов подсети VLAN должен находиться в пределах диапазона IP-адресов суперсети VLAN, к которой принадлежит подсеть VLAN. В противном случае пользователи подсети VLAN не могут обмениваться данными между собой.

⚠ IP-адреса пользователей в подсети VLAN должны находиться в пределах диапазона IP-адресов подсети VLAN. В противном случае пользователи подсети VLAN не могут обмениваться данными между собой.

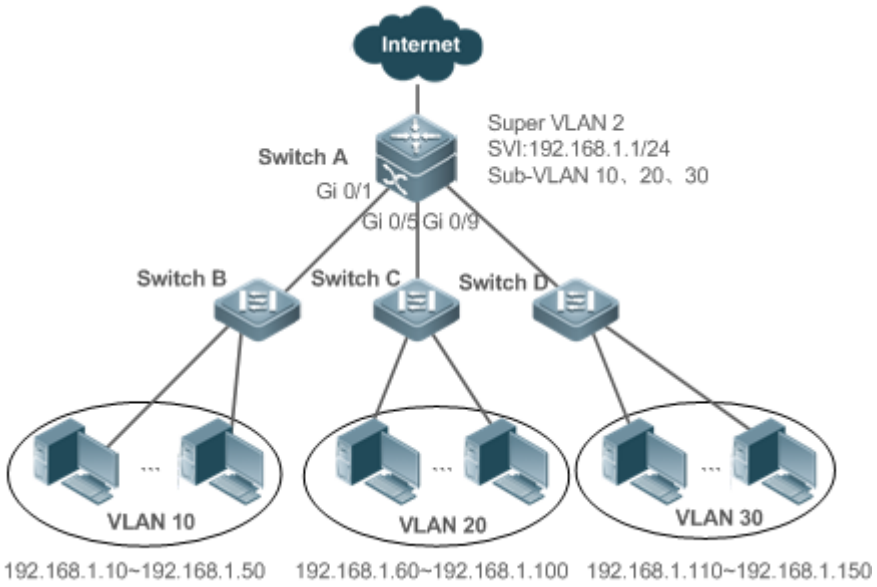
Команда	**subvlan-address-range** *start-ip end-ip*
Описание параметра	*start-ip*: Указывает начальный IP-адрес подсети VLAN. *end-ip*: Указывает конечный IP-адрес подсети VLAN.
Установки по умолчанию	По умолчанию диапазон IP-адресов не настроен.
Режим команды	Режим конфигурирования VLAN
Встроенная подсказка	Опционально. Выполните эту команду, чтобы настроить диапазон IP-адресов пользователей в подсети VLAN. Диапазоны IP-адресов различных подсетей суперсети не могут перекрываться друг другом. ⚠ Диапазон IP-адресов подсети VLAN должен находиться в пределах диапазона IP-адресов суперсети VLAN, к которой принадлежит подсеть. В противном случае пользователи подсетей VLAN не могут обмениваться данными между собой. ⚠ Пользователи подсети VLAN могут взаимодействовать 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. ⚠ IP-адреса, выделенные через DHCP, могут не находиться в настроенном диапазоне IP-адресов. В этом случае пользователи подсети VLAN не могут взаимодействовать с пользователями других VLAN. Поэтому будьте осторожны при использовании этой команды.

Проверка конфигурации

После того, как каждая подсеть VLAN соотносится со шлюзом суперсети, пользователи подсетей VLAN могут отправлять эхо-запросы друг другу.

Пример конфигурации

Настройте Super VLAN в сети таким образом, чтобы пользователи в своих подсетях VLAN использовали один и тот же сегмент сети и имели один и тот же IP-шлюз для экономии IP-адресов

Сценарий Изображение 7-2	
Этапы конфигурации	Выполните соответствующую конфигурацию суперсети VLAN на коммутаторе уровня ядра. На коммутаторах доступа настройте обычные сети VLAN, соответствующие подсетям VLAN на коммутаторе уровня ядра.
A	SwitchA#configure terminal Enter configuration commands, one per line. End with 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 конфигурации	Убедитесь, что хост источника (192.168.1.10) и целевой хост (192.168.1.60) могут отправлять эхо-запросы друг другу.
A	SwitchA(config-if-range)#show supervlan supervlan id supervlan arp-proxy subvlan id subvlan arp-proxy subvlan ip range ---------- ---------- ---------- ---------- 2 ON 10 ON192.168.1.10 - 192.168.1.50 20 ON 192.168.1.60 - 192.168.1.100 30 ON 192.168.1.110 - 192.168.1.150

Типичные ошибки

SVI и IP-шлюз не настроен для суперсети VLAN. Следовательно, происходит сбой связи между подсетями VLAN и между подсетями VLAN и другими сетями VLAN.

Функция ARP proxy отключена в суперсети VLAN или подсетях VLAN. Следовательно, пользователи подсетей VLAN не могут взаимодействовать с пользователями других сетей VLAN.

Диапазон IP-адресов подсети VLAN настроен, но IP-адреса, выделенные пользователям, находятся вне этого диапазона.

7.5 Мониторинг

Отображение

Описание	Команда
Отображает конфигурацию Super	**show supervlan**

VLAN.	

Отладка

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

Описание	Команда
Отладка суперсети VLAN.	**debug bridge svlan**

8 НАСТРОЙКА VLAN ПРОТОКОЛА

8.1 Обзор

Технология VLAN протокола — это технология распределения VLAN на основе типа пакетного протокола. Она может распределять пакеты определенного типа протокола с нулевым идентификатором VLAN в одну и ту же VLAN. То есть, коммутатор, основываясь на типе протокола и формате инкапсуляции пакетов, полученных портами, ищет соответствие полученным нетегированным пакетам с профилями протокола. Если сопоставление выполнено успешно, коммутатор автоматически распределяет пакеты по соответствующей VLAN для передачи. Существует два типа сетей VLAN с протоколом: VLAN с протоколом на основе IP-адреса и VLAN с протоколом на основе типа пакета и типа Ethernet на портах. VLAN с протоколом, основывающаяся на типе пакета и типе Ethernet на портах, называется кратко VLAN протокола, а VLAN протокола на основе IP-адреса кратко называется VLAN подсети.

VLAN протокола применима только к магистральным портам и гибридным портам.

Протоколы и стандарты

Стандарт IEEE 802.1Q

8.2 Применение

Применение	Описание
Настройка и применение VLAN протокола	Реализует изоляцию связи на 2-м уровне для хостов пользователей, использующих различные пакеты протоколов для снижения сетевого трафика и обмена данными.
Настройка и применение VLAN подсети	Указывает диапазон VLAN на основе сегмента IP-сети, к которому принадлежат пользовательские пакеты.

8.2.1 Настройка и применение VLAN протокола

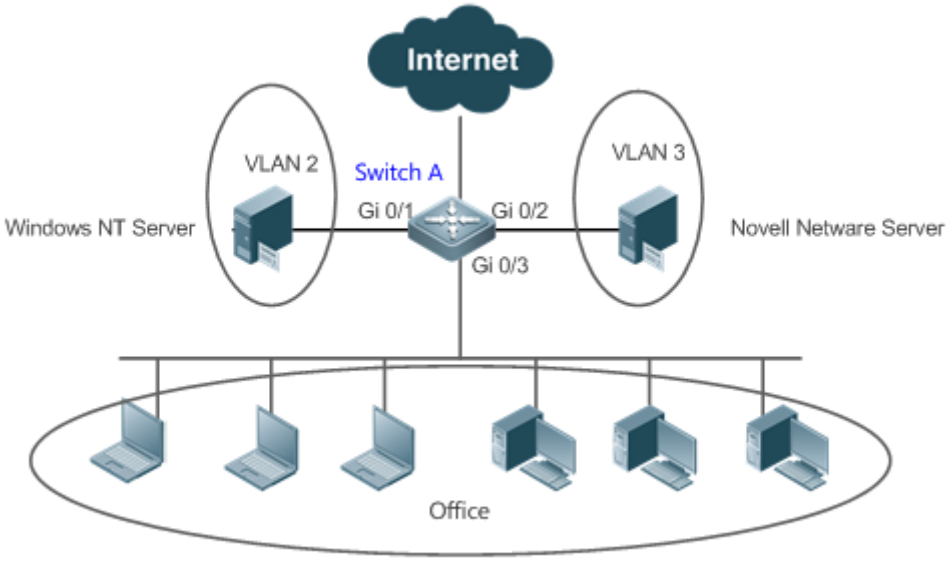
Сценарий

Как показано на следующем Изображении, сетевая архитектура состоит из подключенного сервера Windows NT и сервера Novell Netware, а офис подключен к коммутатору Switch A 3-го уровня через концентратор. В офисном помещении имеются разные ПК. Некоторые компьютеры используют операционную систему Windows NT (ОС) и поддерживают протокол IP, а некоторые ПК используют ОС Novell Netware и поддерживают протокол IPX. ПК в офисном помещении обмениваются данными с внешней сетью и серверами через порт восходящего канала Gi 0/3.

Основные требования:

- Обмен данными 2-го уровня между ПК, использующим ОС Windows NT, изолирован от обмена данными между ПК, использующим ОС Novell Netware, чтобы уменьшить сетевой трафик.

Изображение 8-1



Заметки	Switch A является коммутатором, а порт Gi 0/3 — гибридным портом. Порт Gi 0/1 является портом доступа и принадлежит сети VLAN 2. Порт Gi 0/2 также является портом доступа и принадлежит VLAN 3.

Описание

- Настройте профили пакетного типа и Ethernet-типа (в данном примере настройте профиль 1 для пакетов протокола IP и настройте профиль 2 для пакетов протокола IPX).
- Примените профили к порту восходящего канала (в данном примере порт Gi 0/3) и свяжите их с VLAN (в данном примере свяжите профиль 1 с VLAN 2 и свяжите профиль 2 с VLAN 3).

⚠ Настроенные VLAN протокола действуют только на магистральные и гибридные порты.

8.2.2 Настройка и применение VLAN подсети

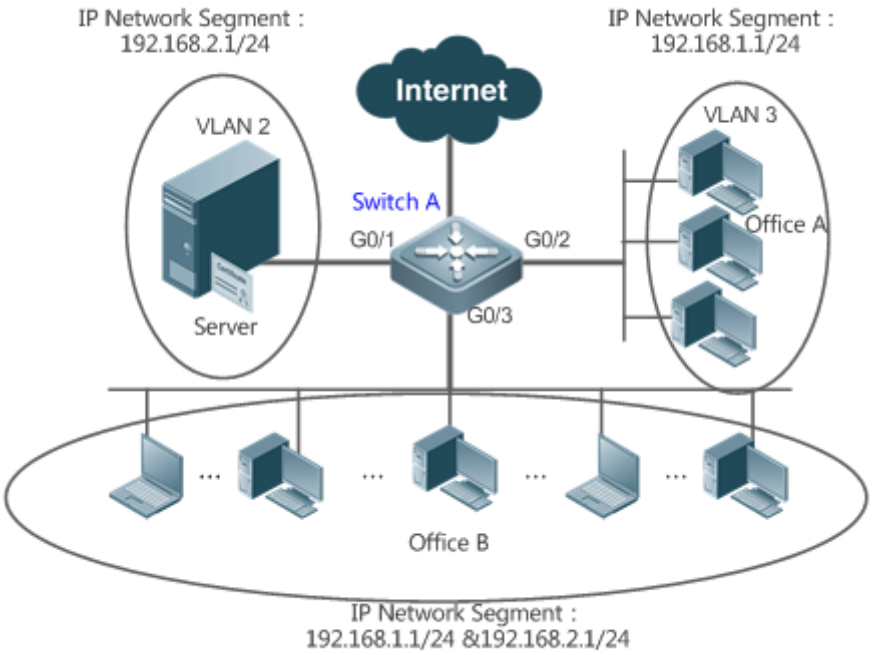
Сценарий

Как показано на Изображении ниже, ПК в Office A и Office B подключены к коммутатору 3-го уровня Switch A через концентраторы. В Office A ПК принадлежат к фиксированному сегменту сети и распределяются на одну и ту же VLAN через порты. В Office B ПК относятся к двум сегментам сети, но они не могут быть распределены в сети VLAN через фиксированные порты.

Основные требования:

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

Изображение 8-2



Заметки	Switch A - 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.

Описание

- ❖ Глобально настройте VLAN подсети (в данном примере назначьте сегмент IP-сети 192.168.1.1/24 сети VLAN 3, а сегмент IP-сети 192.168.2.1/24 — VLAN 2) и включите функцию VLAN подсети на порту восходящего канала (в данном примере порт Gi 0/3).

⚠ Настроенные VLAN подсети действуют только на магистральные порты и гибридные порты.

8.3 Функции

Базовые концепции

VLAN протокола

Технология VLAN протокола — это технология распределения VLAN на основе типа пакетного протокола. Он может распределять пакеты определенного типа протокола с нулевым идентификатором VLAN в одну и ту же VLAN.

Для пакетов, полученных портами устройств, необходимо указать VLAN, чтобы пакет принадлежал к уникальной VLAN. Возможны три варианта:

- Если пакет содержит нулевой идентификатор VLAN (нетегированный или приоритетный пакет) и устройство поддерживает только распределение VLAN на основе портов, идентификатор VLAN в теге, добавленном к пакету, является PVID входного порта.
- Если пакет содержит нулевой идентификатор VLAN (нетегированный или приоритетный пакет) и устройство поддерживает распределение VLAN на основе типа протокола пакетов, идентификатор VLAN в теге, добавленном к пакету, выбирается из идентификаторов VLAN, сопоставленных с конфигу/рацией набора протоколов входного порта. Если тип протокола пакета не соответствует конфигурации набора протоколов входного порта, идентификатор VLAN назначается в соответствии с распределением VLAN на основе портов.
- Если пакет представляет собой помеченный пакет, VLAN, к которому принадлежит пакет, определяется идентификатором VLAN в теге.

VLAN подсети могут быть настроены только глобально, то есть на портах можно включить или отключить только функцию VLAN протокола. Соответствующая конфигурация выполняется глобально для VLAN протокола, на портах выбирается соответствующая конфигурация, а идентификаторы VLAN указаны для успешно сопоставленных пакетов.

- Если входной пакет содержит нулевой идентификатор VLAN, а IP-адрес входного пакета совпадает с IP-адресом, пакет передается в VLAN подсети.
- Если входной пакет содержит нулевой идентификатор VLAN, а тип пакета и тип Ethernet входного пакета соответствуют типу пакета и типу Ethernet входного порта, пакет назначается VLAN протокола.

Приоритет VLAN протокола

Приоритет VLAN подсети выше, чем у VLAN протокола. То есть, если VLAN подсети и VLAN протокола настроены одновременно, а входной пакет соответствует VLAN подсети и VLAN протокола, то приоритет имеет VLAN подсети.

Обзор

Функция	Описание
Автоматическое распределение VLAN на основе типа пакета (protocol based vlan)	Типы служб, поддерживаемые в сети, связаны с сетями VLAN или пакетами из указанного сегмента IP-сети, передаются в указанной сети VLAN для упрощения управления и обслуживания.

8.3.1 Автоматическое распределение VLAN на основе типа пакета

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, он автоматически распределяет их по VLAN, указанной в правилах передачи. Когда правила отключены на портах, нетегированные пакеты данных распределяются в нативную VLAN в соответствии с конфигурацией порта.

Связанная конфигурация

8.4 Конфигурация

Конфигурация	Описание и команда	
Настройка функции VLAN протокола	⚠ (Обязательно) Используется для включения функции распределения VLAN на основе типа пакета и типа Ethernet протокола 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 кадров).
	protocol-vlan profile *num* **vlan** *vid*	(Режим конфигурации интерфейса) Применяет протокол VLAN к порту.
Настройка функции VLAN подсети	⚠ (Обязательно) Используется для включения функции распределения VLAN на основе IP-адреса протокола.	
	protocol-vlan ipv4 *address* **mask** *address* **vlan** *vid*	Настраивает IP-адрес, маску подсети и распределение VLAN.
	protocol-vlan ipv4	(Режим конфигурации интерфейса) Включает VLAN подсети на порту.

8.4.1 Настройка функции VLAN протокола

Сценарий

Связывание типов служб, поддерживаемых в сети, с сетями VLAN для упрощения управления и обслуживания.

Примечания

- Рекомендуется настроить VLAN протокола после обычных VLAN, а также настроить Настройки портов Trunk, Hybrid, Access и LAG.
- Если VLAN протокола настроена на магистральном или гибридном порте, все VLAN, относящиеся к VLAN протокола, должны содержаться в списке разрешенных VLAN магистрального или гибридного портов.

Этапы конфигурации

Глобальная настройка VLAN протокола

- Обязательно.
- VLAN протокола может быть применена к интерфейсу только в режиме глобальной конфигурации.

Команда	**protocol-vlan profile** *num* **frame-type** [*type*] **ether-type** [*type*]
Описание параметра	*num:* Указывает индекс профиля. *type*: Указывает тип пакета и тип Ethernet.
Установки по умолчанию	VLAN протокола по умолчанию отключена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	VLAN протокола можно настроить в интерфейсе только в том случае, если она настроена глобально. При удалении глобальной конфигурации профиля VLAN протокола конфигурация VLAN протокола удаляется со всех интерфейсов, соответствующих профилю VLAN протокола.

Переключение режима порта в режим Trunk/Hybrid

- Обязательно. Функция VLAN протокола действует только на порты, которые находятся в режиме Trunk/Hybrid.

Включение VLAN протокола на порту

- Обязательно. VLAN протокола по умолчанию отключена.
- VLAN протокола включается, только если она применяется в интерфейсах.

Команда	**protocol-vlan profile** *num* **vlan** *vid*
Описание параметра	*num:* Указывает индекс профиля. *vid*: Указывает идентификатор VLAN. Значение **1** указывает максимальный идентификатор VLAN, поддерживаемый устройством.

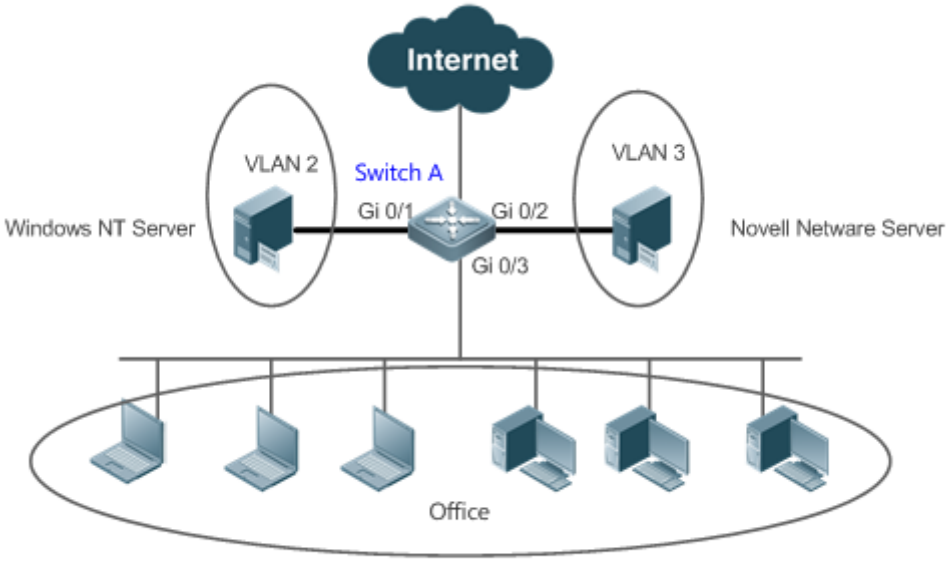
Установки по умолчанию	VLAN протокола по умолчанию отключена.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Интерфейс должен работать в режиме Trunk/Hybrid.

Проверка конфигурации

Выполните команду **show protocol-vlan profile**, чтобы проверить конфигурацию.

Пример конфигурации

Включение функции VLAN протокола в топологической среде

Сценарий **Изображение 8-3**	
Этапы конфигурации	❖ Настройте VLAN 2 и VLAN 3 для обмена данными с пользователем на коммутаторе Switch A. ❖ Глобально настройте VLAN протокола на Switch A (в данном примере настройте профиль 1 для пакетов IP-протокола и настройте профиль 2 для пакетов протокола IPX), включите функцию VLAN протокола на порту восходящего канала (порт Gi 0/3 в данном примере), и завершите привязку VLAN протокола (в данном 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 VLAN 3. Порт Gi 0/3 является гибридным портом. Убедитесь, что сети VLAN для связи пользователей содержатся в списке разрешенных нетегированных сетей VLAN гибридного порта.

A	1. Создайте сети VLAN 2 и VLAN 3 для обмена данными между пользователями.
	
	`# 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 VLAN протокола глобально.
	Настройте профиль 1 для пакетов IP-протокола и профиль 2 для пакетов протокола IPX (в данном примере предполагается, что пакеты инкапсулируются с помощью Ethernet II, а типы Ethernet пакетов IP-протокола и пакеты протокола IPX — соответственно 0X0800 и 0X8137).
	
	`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 профили 1 и 2 к порту Gi 0/3 и назначьте профиль 1 для

	VLAN 2 и профиль 2 для 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 конфигурации	❖ Проверьте правильность конфигурации VLAN протокола на устройстве.

A	`A(config)#show protocol-vlan profile`
	
	`profile frame-type ether-type/DSLAG+SSLAG interface vlan`
	`------- --------------- ---------- -------------- ----`
	`1 ETHERII 0x0800 Gi0/3 2`
	
	`2 ETHERII 0x8137 Gi0/3 3`

Типичные ошибки

- ❖ Порт, подключенный к устройству, не находится в режиме Trunk/Hybrid.
- ❖ Список разрешенных VLAN порта, подключенных к устройству, не содержит VLAN для связи с пользователем.
- ❖ Функция VLAN протокола отключена на порту.

8.4.2 Настройка функции VLAN подсети

Сценарий

Распределите пакеты из указанного сетевого сегмента или IP-адреса в указанную VLAN для передачи.

Примечания

- ❖ Рекомендуется настроить VLAN протокола после обычных VLAN, а также настроить Настройки портов Trunk, Hybrid, Access и LAG.
- ❖ Если VLAN протокола настроена на магистральном или гибридном порте, все VLAN, относящиеся к VLAN протокола, должны содержаться в списке разрешенных VLAN магистрального или гибридного портов.

Этапы конфигурации

Глобальная настройка VLAN подсети

- ❖ Обязательно.
- ❖ VLAN подсети может быть применена в интерфейсе только в режиме глобальной конфигурации.

Команда	**protocol-vlan ipv4** *address* **mask** *address* **vlan** *vid*
Описание параметра	*address*: Указывает IP-адрес. *vid*: Указывает идентификатор VLAN. Значение **1** указывает максимальный идентификатор VLAN, поддерживаемый устройством.
Установки по умолчанию	VLAN подсети по умолчанию отключена.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	VLAN подсети может быть включена в интерфейсе, даже если протокол VLAN не включен глобально. Тем не менее, VLAN подсети действует только в том случае, если VLAN протокола настроена глобально.

Переключение режима порта в режим Trunk/Hybrid

- ❖ Обязательно. Функция VLAN подсети действует только на порты, которые находятся в режиме Trunk/Hybrid.

Включение VLAN подсети на порту

- ❖ Обязательно. VLAN подсети по умолчанию отключена.
- ❖ VLAN подсети включается, только если она применяется в интерфейсах.

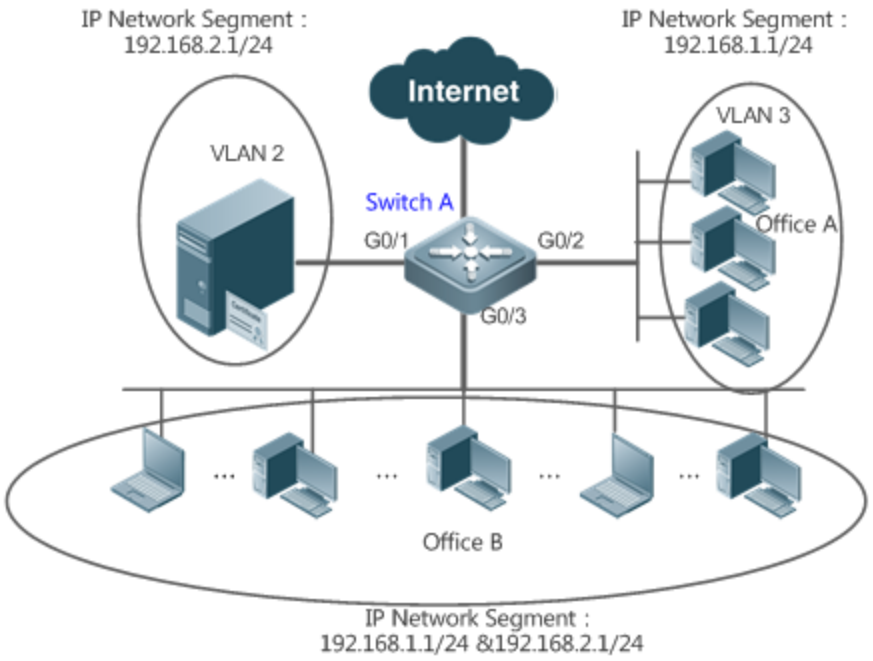
Команда	**protocol-vlan ipv4**
Описание параметра	Недоступно
Установки по умолчанию	VLAN подсети по умолчанию отключена.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Интерфейс должен работать в режиме Trunk/Hybrid.

Проверка конфигурации

Выполните команду **show protocol-vlan ipv4**, чтобы проверить конфигурацию.

Пример конфигурации

Включение функции VLAN подсети в топологической среде

Сценарий Изображение 8-4	
Этапы конфигурации	❖ Настройте VLAN 2 и VLAN 3 для обмена данными с пользователем на коммутаторе Switch A. ❖ Глобально настройте VLAN подсети (в данном примере назначьте сегмент IP-сети 192.168.1.1/24 сети VLAN 3, а сегмент IP-сети 192.168.2.1/24 — VLAN 2) и включите функцию VLAN подсети на порту восходящего канала (в данном примере порт Gi 0/3). ❖ Порт Gi 0/1 является портом доступа и принадлежит сети VLAN 2. Порт Gi 0/2 также является портом доступа и принадлежит VLAN 3. Порт Gi 0/3 является гибридным портом. Убедитесь, что сети VLAN для связи пользователей содержатся в списке разрешенных нетегированных сетей VLAN гибридного порта.

A	1. Создайте сети VLAN 2 и VLAN 3 для обмена данными между пользователями.
	`A# 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 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 в интерфейсах. VLAN подсети по умолчанию отключена. (config-if-GigabitEthernet 0/1)# protocol-vlan ipv4
Проверка конфигурации	❖ 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

Типичные ошибки

- ❖ Порт, подключенный к устройству, не находится в режиме Trunk/Hybrid.
- ❖ Список разрешенных VLAN порта, подключенных к устройству, не содержит VLAN для связи с пользователем.
- ❖ VLAN подсети отключена на порту.

8.5 Мониторинг

Отображение

Описание	Команда
Отображение содержимого протокола VLAN.	**show protocol-vlan**

Отладка

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

Описание	Команда
Отладка VLAN протокола.	**debug bridge protvlan**

9 НАСТРОЙКА ЧАСТНОЙ VLAN(PRIVATE VLAN)

9.1 Обзор

Частная VLAN делит широковещательный домен VLAN уровня 2 на несколько поддоменов. Каждый поддомен состоит из одной частной пары VLAN: первичной и вторичной VLAN.

Один частный домен VLAN может состоять из нескольких частных пар VLAN, а каждая частная пара VLAN представляет один поддомен. В частном домене VLAN все частные пары VLAN совместно используют одну и ту же первичную VLAN. Идентификаторы вторичной VLAN субдоменов различаются.

Если поставщик услуг выделяет каждому пользователю по одной сети VLAN, количество пользователей, которое может поддерживаться поставщиком услуг, ограничено, поскольку одно устройство поддерживает до 4096 сетей VLAN. На устройстве 3-го уровня каждой VLAN назначается один адрес подсети или ряд адресов, что приводит к перерасходу IP-адресов. Технология частной сети VLAN должным образом решает две предыдущие проблемы. Частная VLAN коротко называется PVLAN.

9.2 Применение

Применение	Описание
Применение PVLAN между устройствами 2-го уровня	Пользователи предприятия могут взаимодействовать друг с другом, но взаимодействие пользователей между предприятиями изолировано.
Применение PVLAN на одном устройстве 3-го уровня	Все корпоративные пользователи используют один и тот же адрес шлюза и могут обмениваться данными с внешней сетью.

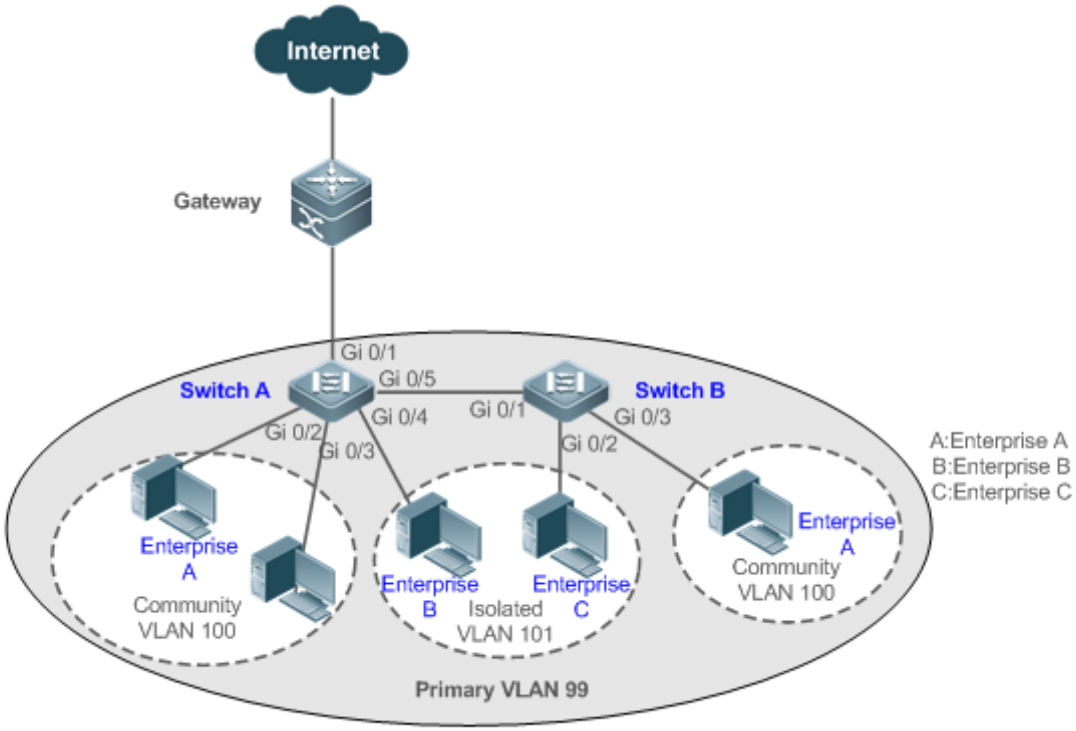
9.2.1 Применение PVLAN между устройствами 2-го уровня

Сценарий

Как показано на Изображении ниже, в сети управления хостингом хосты корпоративных пользователей подключаются к сети через коммутаторы Switch A или Switch B. Основные требования:

- Пользователи предприятия могут взаимодействовать друг с другом, но взаимодействие пользователей между предприятиями изолировано.
- Все корпоративные пользователи используют один и тот же адрес шлюза и могут обмениваться данными с внешней сетью.

Изображение 9-1



Заметки	Коммутаторы Switch A и B являются коммутаторами доступа. PVLAN работает на разных устройствах. Порты для подключения устройств должны быть настроены как магистральные порты, то есть порты Gi 0/5 коммутатора A и Gi 0/1 коммутатора B настроены как магистральные порты. Порт Gi 0/1 для подключения коммутатора A к шлюзу необходимо настроить как смешанный (promiscuous) порт. Порт Gi 0/1 шлюза можно настроить как магистральный или гибридный порт, а нативная VLAN является основной VLAN для PVLAN.

Описание

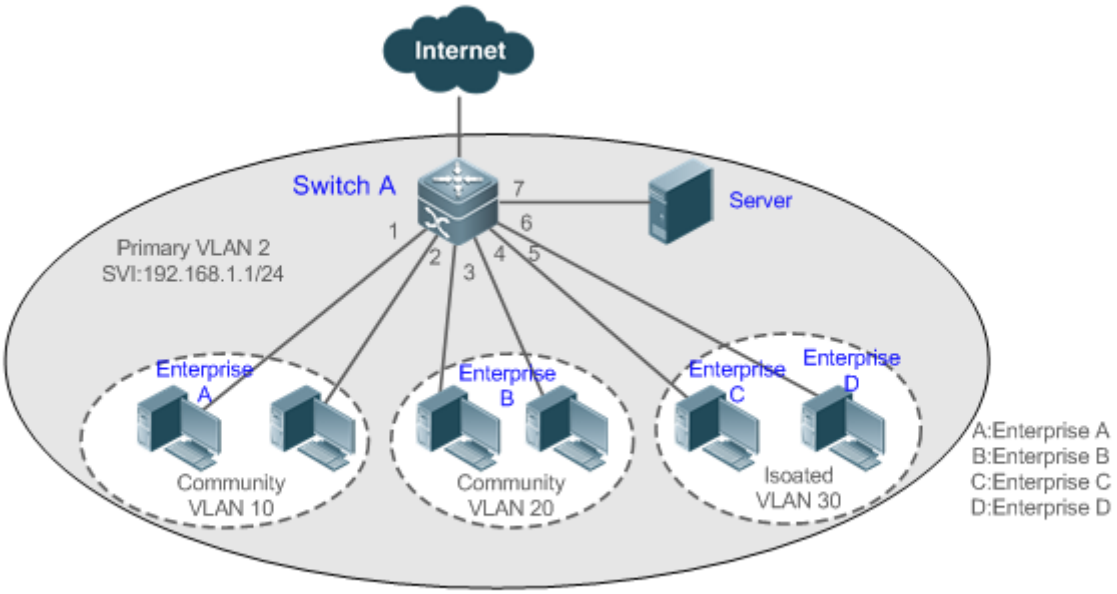
- Настройте все предприятия на одну и ту же PVLAN (в данном примере основная VLAN 99). Все корпоративные пользователи используют один и тот же интерфейс 3-го уровня через эту VLAN для связи с внешней сетью.
- Если на предприятии имеется несколько хостов пользователей, назначьте хосты пользователей разных предприятий различным сообществам VLAN. То есть, настройте порты, подключенные к хостам корпоративных пользователей, в качестве портов хоста сообщества VLAN, чтобы обеспечить взаимодействие пользователей внутри предприятия, но изолировать взаимодействие пользователей между предприятиями.
- Если на предприятии имеется только один хост пользователя, настройте порты, подключенные к хостам пользователей таких предприятий, как порты хоста изолированной VLAN, чтобы обеспечить изоляцию связи пользователей между предприятиями.

9.2.2 Применение PVLAN на одном устройстве 3-го уровня

Как показано на Изображении ниже, в сети обслуживания дата-центра хосты корпоративных пользователей подключаются к сети через коммутатор 3-го уровня Switch A. Основные требования:

- Пользователи предприятия могут взаимодействовать 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 обмениваться данными с внешней сетью.

Изображение 9-2



Заметки	Switch A является шлюзом. Когда хосты пользователей подключены к одному устройству, порт Gi 0/7 для подключения к серверу настраивается как смешанный (promiscuous) порт, чтобы корпоративные пользователи могли обмениваться данными с сервером. Сопоставление на 3-м уровне необходимо выполнять в основной и вторичной VLAN, чтобы пользователи могли обмениваться данными с внешней сетью.

Описание

- Настройте порт, напрямую подключенный к серверу, как смешанный (promiscuous) порт. Затем все корпоративные пользователи могут взаимодействовать с сервером через смешанный (promiscuous) порт.
- Настройте адрес шлюза PVLAN на устройстве 3-го уровня (в данном примере Switch A) (в данном примере задайте для адреса SVI VLAN 2 значение 192.168.1.1/24) и настройте сопоставление между первичной и вторичной

VLAN на интерфейсе 3-го уровня. Затем все корпоративные пользователи могут обмениваться данными с внешней сетью через адрес шлюза.

9.3 Функции

Базовые концепции

PVLAN

PVLAN поддерживает три типа VLAN: первичные VLAN, изолированные VLAN и VLAN сообществ.

Домен PVLAN имеет только одну основную VLAN. Вторичные VLAN реализуют изоляцию 2-го уровня в одном домене PVLAN. Существует два типа вторичных сетей VLAN.

Изолированная VLAN

- Порты в одной и той же изолированной VLAN не могут взаимно обеспечить связь на 2-м уровне. Домен PVLAN имеет только одну изолированную VLAN.

VLAN сообщества

- Порты в одной и той же сети VLAN сообщества могут обеспечить связь на 2-м уровне друг с другом, но не могут обеспечить связь на 2-м уровне с портами в других сетях VLAN сообщества. Домен PVLAN может иметь несколько сетей VLAN сообщества.

Привязка PVLAN на 2-м уровне

Пары PVLAN существуют только после установления связи на 2-м уровне между тремя типами VLAN частной PVLAN. Затем первичная VLAN имеет указанную вторичную VLAN, а вторичная VLAN — указанную первичную VLAN. Первичная и вторичная VLAN находятся в взаимосвязи «один ко многим».

Привязка PVLAN на 3-м уровне

В PVLAN интерфейсы 3-го уровня, то есть коммутируемые виртуальные интерфейсы (SVI) могут быть созданы только в первичной VLAN. Пользователи вторичной VLAN могут осуществлять связь на 3-м уровне только после установления связи на 3-м уровне между вторичной и первичной VLAN. В противном случае пользователи могут осуществлять только связь на 2-м уровне.

Изолированный порт

Порт в изолированной VLAN может взаимодействовать только с неразборчивым портом. Изолированный порт может пересылать полученные пакеты на магистральный порт, но магистральный порт не может пересылать пакеты с VID изолированной VLAN на изолированный порт.

Порт сообщества

Порты сообщества — это порты в сети VLAN сообщества. Порты сообщества в одной и той же сети VLAN сообщества могут обмениваться данными друг с другом и обмениваться данными с неразборчивыми портами. Они не могут обмениваться данными с портами сообщества в других локальных сетях или изолированных портах в изолированной VLAN.

Неразбочивый порт

Смешанные (promiscuous) порты — это порты в первичной VLAN. Они могут обмениваться данными с любыми портами, включая изолированные порты и порты сообщества во вторичных VLAN одного домена PVLAN.

Смешанный (promiscuous) магистральный порт

Смешанный (promiscuous) магистральный порт — это порт-участник, который одновременно принадлежит нескольким обычным сетям VLAN и нескольким сетям PVLAN. Он может обмениваться данными с любыми портами в одной сети VLAN.

- В обычной VLAN пересылка пакетов соответствует стандарту 802.1Q.
- Если в PVLAN для пересылки пакетов с тегами ипользуется смешанный (promiscuous) магистральный порт, и VID пакетов является идентификатором вторичной VLAN, VID преобразуется в соответствующий идентификатор первичной VLAN перед пересылкой пакетов.

Изолированный магистральный порт

Изолированный магистральный порт — это порт-участник, который принадлежит нескольким обычным VLAN и нескольким PVLAN одновременно.

- В изолированной VLAN изолированный магистральный порт может взаимодействовать только с неразборчивым портом.
- В сети VLAN сообщества изолированный магистральный порт может взаимодействовать с портами сообщества в одной сети VLAN сообщества и неразборчивыми портами.
- В обычной VLAN пересылка пакетов соответствует стандарту 802.1Q.
- Изолированный магистральный порт может пересылать полученные пакеты с идентификатором изолированной VLAN на магистральный порт, но магистральный порт не может пересылать пакеты с VID изолированной VLAN на изолированный порт.
- Если для пересылки пакетов с тегами используется изолированный магистральный порт, и VID пакетов является идентификатором первичной VLAN, VID преобразуется в идентификатор вторичной VLAN перед пересылкой пакетов.

⚠ В PVLAN порты SVI можно создавать только в первичной VLAN, и нельзя создавать во вторичных VLAN.

⚠ Порты в PVLAN могут использоваться в качестве портов источников зеркалирования, но не могут использоваться в качестве портов назначения зеркалирования.

Обзор

Функция	Описание
Изоляция PVLAN на 2-м уровне и	Порты разных типов PVLAN могут быть настроены для реализации взаимодействия и изоляции промежуточных пользовательских хостов VLAN.

сохранение IP-адресов	После выполнения сопоставления на 2-м уровне между первичной и вторичной VLAN поддерживается связь только на 2-м уровне. Если требуется связь на 3-м уровне, пользователям вторичной VLAN необходимо использовать SVI первичной VLAN для обеспечения связи на 3-м уровне.

9.3.1 Изоляция PVLAN на 2-м уровне и сохранение IP-адресов

Добавление пользователей в поддомены PVLAN для изоляции связи между предприятиями и между корпоративными пользователями.

Принцип работы

Настройте PVLAN, настройте привязку на 2-м уровне и привязку на 3-м уровне между первичной VLAN и SubVLAN частной PVLAN, а также настройте порты, подключенные к хостам пользователей, внешним сетевым устройствам и серверам, как различные типы портов PVLAN. Таким образом, можно реализовать разделение субдоменов и связь пользователей в поддоменах с внешней сетью и серверами.

Взаимодействие пересылки пакетов между портами разных типов

Выходной порт Входной порт	**Смешанный (promiscuous) порт**	**Изолированный порт**	**Порт сообщества**	**Изолированный магистральный порт (в той же VLAN)**	**Смешанный (promiscuous) магистральный порт (в той же VLAN)**	**Магистральный порт (в той же VLAN)**
Неразбочивый порт	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Изолированный порт	Поддерживается	Не поддерживается	Не поддерживается	Не поддерживается	Поддерживается	Поддерживается
Порт сообщества	Поддерживается	Не поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Изолированный магистральн	Поддерживается	Не поддерж	Поддерживается	Не поддерживается (не	Поддерживается	Поддерживается

ый порт (в той же VLAN)		ивается		поддерживается в изолированной сети VLAN, но поддерживается в неизолированной сети VLAN)		я
Смешанный (promiscuous) магистральный порт (в той же VLAN)	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается	Поддерживается
Магистральный порт (в той же VLAN)	Поддерживается	Не поддерживается	Поддерживается	Не поддерживается (не поддерживается в изолированной сети VLAN, но поддерживается в неизолированной сети VLAN)	Поддерживается	Поддерживается

Тег VLAN изменяется после пересылки пакетов между портами разных типов

Выходной порт Входной порт	**Неразборчивый порт**	**Изолированный порт**	**Порт сообщества**	**Изолированный магистральный порт** (в той же сети VLAN)	**Смешанный (promiscuous) магистральный порт** (в той же сети VLAN)	**Магистральный порт** (в той же сети VLAN)
Неразборчивый порт	Неизменный	Неизменный	Неизменный	Добавляется дополнительный идентификатор VLAN.	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других	Добавляется тег идентификатора первичн

					VLAN.	ой VLAN.
Изолированный порт	Неизменный	Не доступен	Не доступен	Не доступен	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других VLAN.	Добавляется тег идентификатора изолированной VLAN.
Порт сообщества	Неизменный	Не доступен	Неизменный	Добавляется тег идентификатора VLAN сообщества.	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других VLAN.	Добавляется тег идентификатора VLAN сообщества.
Изолированный магистральный порт (в той же VLAN)	Тег VLAN удаляется.	Не доступен	Тег VLAN удаляется.	Тег VLAN остается неизменным в неизолированной VLAN.	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других VLAN.	Неизменный
Смешанный (promiscuous) магистральный порт (в той же сети VLAN)	Тег VLAN удаляется.	Неизменный	Неизменный	Добавляется дополнительный идентификатор VLAN.	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других VLAN.	Неизменный
Магистральный порт	Тег VLAN удаляетс	Не доступе	Тег VLAN	Тег VLAN преобразуется	Добавляется основной тег	Неизменный

(в той же VLAN)	я.	н	удаляется.	в идентификатор вторичной VLAN в первичной VLAN, и остается неизменным в других неизолированных VLAN.	VLAN ID, и тег VLAN остается неизменным в других VLAN.	
ЦП коммутатора	Нетегированный	Нетегированный	Нетегированный	Добавляется тег идентификатора вторичной VLAN.	Добавляется основной тег VLAN ID, и тег VLAN остается неизменным в других VLAN.	Добавляется тег идентификатора первичной VLAN.

9.4 Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций PVLAN	⚠ (Обязательно) Используется для настройки основной и вторичной VLAN.	
	private-vlan {**community** | **isolated** | **primary**}	Настройка типа PVLAN.
	⚠ (Обязательно) Используется для настройки связи на 2-м уровне между первичной и вторичной VLAN частной PVLAN для формирования пар PVLAN.	
	private-vlan association {*svlist* | **add** *svlist* | **remove** *svlist*}	Настраивает связь 2-го уровня между первичной и вторичной VLAN для формирования пар PVLAN.
	⚠ (Дополнительно) Используется для выделения пользователей в изолированную VLAN или локальную сеть сообщества.	

switchport mode private-vlan host	Настраивает порт хоста PVLAN.
switchport private-vlan host-association *p_vid s_vid*	Связывает порты 2-го уровня с PVLAN и выделяет порты для поддоменов.
⚠ (Дополнительно) Используется для настройки порта в качестве смешанного (promiscuous) порта.	
Switchport mode private-vlan promiscuous	Настраивает смешанный (promiscuous) порт PVLAN.
switchport private-vlan mapping *p_vid* { *svlist* | **add** *svlist* | **remove** *svlist* }	Настраивает первичную VLAN, к которой принадлежит смешанный (promiscuous) порт PVLAN, и список вторичных VLAN. Пакеты PVLAN могут быть переданы или получены через этот порт только после выполнения конфигурации.
⚠ (Дополнительно) Используется для выделения пользователей изолированным магистральным портам и для привязки нескольких PVLAN.	
switchport private-vlan association trunk *p_vid s_vid*	Настраивает порт, подключенный к хосту пользователя, в качестве изолированного магистрального порта после создания PVLAN и выполнения привязки на 2-м уровне. Порты этого типа поддерживают привязку к нескольким парам PVLAN. Параметры *p_vid* и *s_vid* указывают первичную и изолированную VLAN соответственно.
⚠ (Дополнительно) Используется для выделения пользователей неразборчивым магистральным портам и для привязки нескольких PVLAN.	
switchport private-vlan	Настраивает порт,

	promiscuous trunk *p_vid s_list*	подключенный к хосту пользователя, в качестве смешанного (promiscuous) магистрального порта после создания PVLAN и выполнения привязки на 2-м уровне. Порты этого типа поддерживают привязку к нескольким парам PVLAN. Параметры *p_vid* и *s_list* указывают списки идентификаторов первичной и вторичной VLAN соответственно.
	⚠ (Дополнительно) Используется для настройки связи на 3-м уровне для пользователей во вторичной VLAN.	
	private-vlan mapping { *svlist* | **add** *svlist* | **remove** *svlist* }	Настраивает SVI первичной VLAN и настраивает привязку на 3-м уровне между первичной и вторичной VLAN после создания PVLAN и выполнения привязки на 2-м уровне. Пользователи в SubVLAN могут осуществлять связь на 3-м уровне через SVI первичной VLAN.

9.4.1 Настройка основных функций PVLAN

Сценарий

- Включите поддомены PVLAN для создания изоляции между предприятиями и между корпоративными пользователями.
- Внедрение сопоставления на 3-м уровне между несколькими вторичными сетями VLAN и первичной сетью VLAN, чтобы несколько сетей VLAN использовали один и тот же IP-шлюз, что позволяет экономить IP-адреса.

Примечания

- После настройки первичной и вторичной VLAN поддомен PVLAN существует только после привязки между ними на 2-м уровне.
- Порт, подключенный к хосту пользователя, должен быть настроен как определенный порт PVLAN, чтобы хост пользователя присоединился к поддомену для реализации настоящей изоляции пользователей.
- Порт, подключенный к внешней сети, и порт, подключенный к серверу, должны быть настроены как смешанные (promiscuous) порты, чтобы пересылать пакеты по восходящему и нисходящему каналам в обычном режиме.

- Пользователи вторичной VLAN могут осуществлять связь на 3-м уровне через SVI первичной VLAN только после того, как выполняется сопоставление на 3-м уровне между вторичной и первичной VLAN.

Этапы конфигурации

Конфигурирование PVLAN

- Обязательно.
- Необходимо настроить первичную и вторичную VLAN. Два типа VLAN не могут существовать независимо друг от друга.
- Запустите команду **private-vlan** { **community** | **isolated** | **primary** }, чтобы настроить VLAN в качестве первичной VLAN частной PVLAN и других VLAN в качестве вторичных VLAN.

Команда	**private-vlan** { **community** | **isolated** | **primary** }
Описание параметра	**community**: Указывает, что тип VLAN — это сеть VLAN сообщества. **isolated**: Указывает, что тип VLAN является изолированной VLAN. **primary**: Указывает, что тип VLAN является первичной VLAN пары PVLAN.
Установки по умолчанию	VLAN являются обычными и не имеют **параметров** PVLAN.
Режим команды	VLAN mode
Встроенная подсказка	Эта команда используется для указания первичной и вторичной VLAN частной PVLAN.

Настройка привязки PVLAN на 2-м уровне

- Обязательно.
- Поддомены PVLAN, изолированные порты, порты сообщества и привязку на 3-м уровне можно настроить только после привязки на 2-м уровне между первичной и вторичной VLAN частной PVLAN.
- По умолчанию после настройки различных PVLAN первичные и вторичные VLAN независимы друг от друга. Первичная VLAN имеет привязанную вторичную VLAN, а вторичная VLAN может иметь привязанную первичную VLAN только после выполнения привязки на 2-м уровне.
- Выполните команду **private-vlan association** { *svlist* | **add** *svlist* | **remove** *svlist* }, чтобы настроить или отменить привязку на 2-м уровне между основной VLAN и вторичной VLAN частной PVLAN. Поддоменны PVLAN можно сформировать только после настройки привязки на 2-м уровне. Поддомен PVLAN расформировывается после отмены привязки на 2-м уровне. Если привязка на 2-м уровне не выполнена, когда изолированные порты и смешанные

(promiscuous) порты используются для настройки связанных пар PVLAN, конфигурация не будет выполнена, или связь между портами и VLAN будет отменена.

Команда	**private-vlan association** { *svlist* | **add** *svlist* | **remove** *svlist* }
Описание параметра	*svlist*: Указывает список вторичных VLAN, которые должны быть связаны или разъединены. **add** svlist: Добавляет дополнительные сети VLAN для привязки. **remove** *svlist*: Отменяет привязку между *svlist* и первичной VLAN.
Установки по умолчанию	По умолчанию первичная и вторичная VLAN не связаны.
Режим команды	Режим первичной VLAN для PVLAN
Встроенная подсказка	Эта команда используется для настройки связи на 2-м уровне между первичной и вторичной сетями VLAN для формирования пар PVLAN. Каждая первичная VLAN может быть связана только с одной изолированной VLAN, но может быть связана с несколькими сетями VLAN сообщества.

Настройка привязки PVLAN на 3-м уровне

- Если пользователям во вторичном домене VLAN необходимо установить связь на 3-м уровне, настройте интерфейс SVI 3-го уровня для первичной VLAN, а затем настройте привязку на 3-м уровне между первичной и вторичной VLAN в SVI.
- По умолчанию SVI можно настроить только в первичной VLAN. Вторичные VLAN не поддерживают связь на 3-м уровне.
- Если пользователям вторичной VLAN частной PVLAN необходимо установить связь на 3-м уровне, то для передачи и получения пакетов необходимо использовать SVI первичной VLAN.
- Выполните команду **private-vlan mapping** { *svlist* \| **add** *svlist* \| **remove** *svlist* }, чтобы настроить или отменить привязку на 3-м уровне между первичной и вторичной VLAN частной PVLAN. Пользователи вторичной VLAN могут установить связь на 3-м уровне с внешней сетью только после настройки привязки на 3-м уровне. После отмены привязки на 3-м уровне пользователи вторичной VLAN не могут установить связь на 3-м уровне.

Команда	**private-vlan mapping** { *svlist* | **add** *svlist* | **remove** *svlist* }
Описание	*svlist*: Указывает список вторичных сетей VLAN, для которых

параметра	необходимо настроить сопоставление на 3-м уровне. add *svlist*: Добавляет вторичные сети VLAN, которые будут привязаны к интерфейсу 3-го уровня. remove *svlist:* Отменяет привязку вторичных сетей VLAN к интерфейсу 3-го уровня.
Установки по умолчанию	По умолчанию первичная и вторичная VLAN не связаны.
Режим команды	Режим конфигурации интерфейса первичной VLAN
Встроенная подсказка	Сначала необходимо настроить SVI 3-го уровня для первичной VLAN. Интерфейсы 3-го уровня могут быть настроены только в первичной VLAN. Привязка на 2-м уровне должна выполняться между связанными вторичными сетями VLAN и первичной сетью VLAN.

Настройка изолированных портов и портов сообщества

- После настройки первичной и вторичной VLAN частной PVLAN, а также привязки на 2-м уровне выделите порты устройств, подключенные к хостам пользователей, чтобы указать поддомены, к которым принадлежат хосты пользователей.
- Если на предприятии имеется только один хост пользователя, установите порт, подключенный к хосту пользователя, в качестве изолированного порта.
- Если на предприятии имеется несколько пользовательских хостов, настройте порты, подключенные к хостам пользователей, как порты сообщества.

Команда	**switchport mode private-vlan host** switchport private-vlan host-association *p_vid s_vid*
Описание параметра	*p_vid*: Указывает идентификатор первичной VLAN в паре PVLAN. s_vid: Указывает идентификатор вторичной VLAN в паре PVLAN. Порт является привязанным, если VLAN является изолированной; также порт является портом сообщества, если VLAN является VLAN сообщества.
Установки по умолчанию	По умолчанию интерфейс работает в режиме доступа; нет привязанных пар частных VLAN.
Режим	Обе команды выполняются в режиме конфигурации интерфейса.

команды	
Встроенная подсказка	Необходимо настроить обе предшествующие команды. Перед настройкой порта в качестве изолированного или смешанного (promiscuous) порта необходимо настроить режим порта как режим порта хоста. Настройка порта как изолированного порта или порта сообщества зависит от параметра *s_vid*. *p_vid* и *s_vid* должны быть соответственно идентификаторами первичной и вторичной VLAN в паре PVLAN, в которой выполняется привязка на 2-м уровне. Один порт хоста может быть связан только с одной парой PVLAN.

Настройка смешанного (promiscuous) порта

- Согласно таблице, приведенной в разделе "функции", правила передачи и получения пакетов портов, один тип порта PVLAN не может обеспечить симметричную пересылку пакетов на входе и выходе. Порты для подключения к внешней сети или серверу необходимо настроить в качестве неразборчивых портов, 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 параметра	*p_vid*: Указывает идентификатор первичной VLAN в паре PVLAN. svlist: Указывает вторичную VLAN, связанную с неразборчивым портом. Между данным параметром и p_vid должна быть выполнена привязка на 2-м уровне. **add** svlist: Добавляет привязку вторичной VLAN к порту. **remove** svlist: Отменяет привязку вторичной VLAN к порту.
Установки по умолчанию	По умолчанию интерфейс работает в режиме доступа; смешанный (promiscuous) порт не привязан к вторичной VLAN.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Порт должен быть настроен в смешанном (promiscuous) режиме. Если порт настроен как смешанный (promiscuous), он должен быть привязан к парам PVLAN. В противном случае порт не может

	предоставлять или пересылать услуги. Один смешанный (promiscuous) порт может быть связан с несколькими парами PVLAN в одной первичной VLAN, но не может быть связан с несколькими первичными VLAN.

Настройка изолированного магистрального порта и привязка порта к паре PVLAN интерфейса 2-го уровня

- Когда следующее устройство нисходящего канала не поддерживает PVLAN, и если порт должен изолировать пакеты некоторых VLAN, порт должен быть настроен как изолированный магистральный порт, также должна быть настроена привязка между портом и парой PVLAN интерфейса 2-го уровня.
- После того как порт настроен как изолированный магистральный порт, он служит восходящим портом PVLAN. Когда порт получает пакеты с тегом VLAN частной PVLAN, порт является изолированным портом PVLAN. Когда порт получает другие пакеты, он является обычным магистральным портом.

Команда	**switchport mode trunk** switchport private-vlan association trunk *p_vid s_vid*
Описание параметра	*p_vid*: Указывает идентификатор первичной VLAN в паре PVLAN. s_vid: Указывает привязанную изолированную VLAN. Между данным параметром и p_vid должна быть выполнена привязка на 2-м уровне.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Привязанная PVLAN должна быть парой VLAN, в которой привязка выполняется на 2-м уровне. Интерфейс должен работать в режиме магистрального порта. Один магистральный порт может быть связан с несколькими парами PVLAN.

Настройка смешанного (promiscuous) магистрального порта и привязка порта к паре PVLAN интерфейса 2-го уровня

- Если управляющая VLAN и первичная VLAN устройства не совпадают, а также если порт должен одновременно разрешать пакеты управляющей VLAN и первичной VLAN, то он должен быть настроен как смешанный (promiscuous) магистральный порт, и необходимо настроить привязку между данным портом и парой PVLAN интерфейса 2-го уровня.
- После того как порт настроен как смешанный (promiscuous) магистральный порт, он служит восходящим портом PVLAN. Когда порт получает пакеты с тегом VLAN частной PVLAN, порт является неразборчивым портом PVLAN.

Когда порт получает другие пакеты, он является обычным магистральным портом.

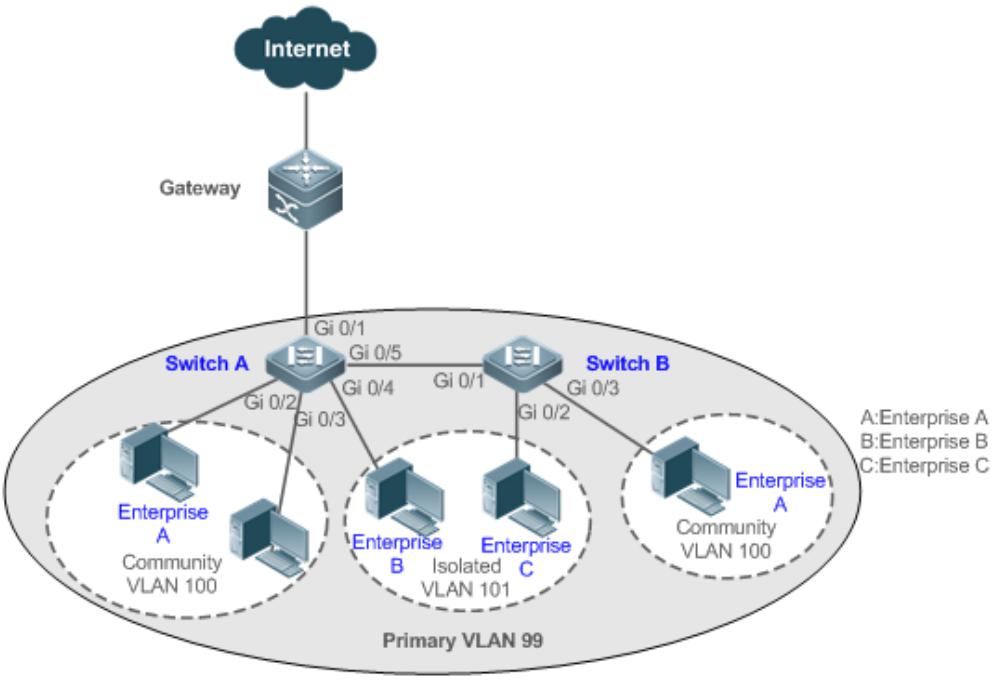
Команда	**switchport mode trunk** switchport private-vlan promiscuous trunk *p_vid s_list*
Описание параметра	*p_vid*: Указывает идентификатор первичной VLAN в паре PVLAN. svlist: Указывает вторичную VLAN, связанную с неразборчивым портом. Между данным параметром и p_vid должна быть выполнена привязка на 2-м уровне.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Интерфейс должен работать в режиме магистрального порта. Привязка на 2-м уровне должна выполняться на уже привязанной первичной и вторичной VLAN.

Проверка конфигурации

Подключите хосты пользователей к портам PVLAN для передачи и получения пакетов в соответствии с правилами пересылки портов PVLAN для реализации изоляции. Настройте привязку на 3-м уровне, чтобы пользователи в первичной и вторичной VLAN одной и той же PVLAN могли совместно использовать один и тот же IP-адрес шлюза и установить связь на 3-м уровне.

Пример конфигурации

Применение PVLAN между устройствами 2-го уровня

Изображение 9-3	
Этапы конфигурации	❖ Настройте все предприятия на одну и ту же PVLAN (в данном примере основная VLAN 99). Все корпоративные пользователи используют один и тот же интерфейс 3-го уровня через эту VLAN для связи с внешней сетью. ❖ Если на предприятии имеется несколько хостов пользователей, назначьте каждое предприятие на разные сети VLAN сообщества (в данном примере назначьте Enterprise A на сеть сообщества VLAN 100), чтобы осуществить взаимодействие пользователей внутри предприятия и изолировать взаимодействие пользователей между предприятиями. ❖ Если на предприятии имеется только один хост пользователя, выделите такие предприятия в одну изолированную сеть VLAN (в данном примере назначьте Enterprise B и Enterprise C на изолированную сеть VLAN 101), чтобы изолировать связь 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 SwitchA(config)#interface gigabitEthernet 0/5 SwitchA(config-if-GigabitEthernet 0/5)#switchport mode trunk SwitchA(config-if-GigabitEthernet 0/5)#exit
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 SwitchB(config)#interface gigabitEthernet 0/1 SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk SwitchB(config-if-GigabitEthernet 0/1)#exit
Проверка конфигурации	Проверьте, правильно ли настроены VLAN и порты, и проверьте правильность пересылки пакетов в соответствии с правилами пересылки пакетов в разделе "функции".
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 !

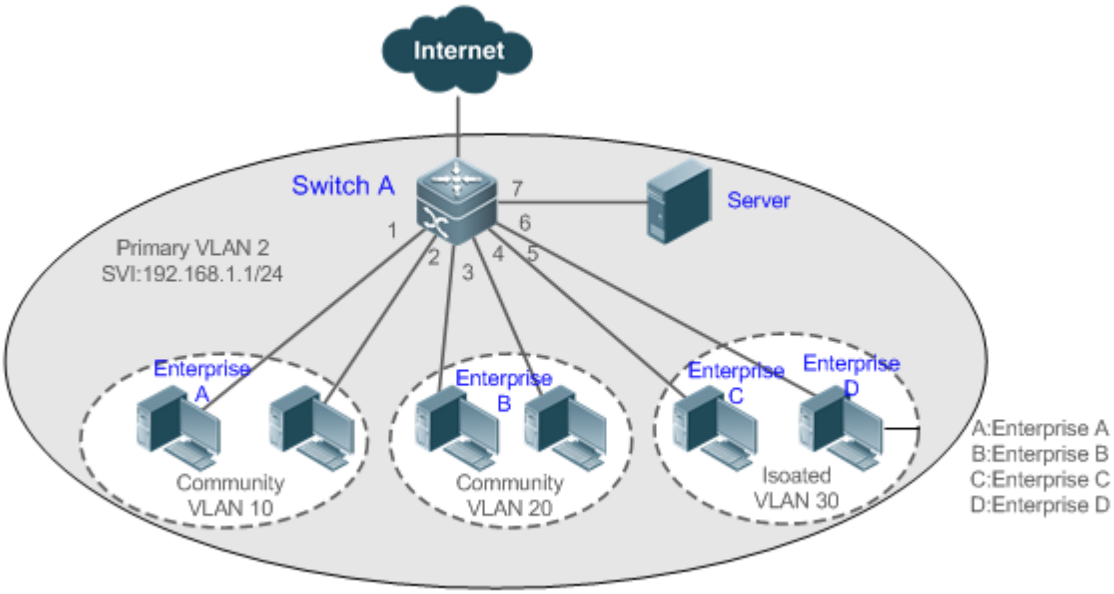
	interface GigabitEthernet 0/5 switchport mode trunk ! SwitchA# show vlan private-vlan VLAN Type Status Routed Ports Associated VLANs ------------------------------ ------------------ 99 primary active Disabled Gi0/1, Gi0/5 100-101 100 community active Disabled Gi0/2, Gi0/3, Gi0/5 99 101 isolated active Disabled Gi0/4, Gi0/5 99 ...
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 ! interface GigabitEthernet 0/1 switchport mode trunk ! interface GigabitEthernet 0/2 switchport mode private-vlan host switchport private-vlan host-association 99 101 ! interface GigabitEthernet 0/3 switchport mode private-vlan host switchport private-vlan host-association 99 100

Типичные ошибки

- Привязка на 2-м уровне не выполнена между первичной и вторичной VLAN частной PVLAN, и список VLAN порта не удается добавить при настройке изолированных портов, неразборчивых портов и портов сообщества.
- Один порт хоста не может быть привязан к нескольким парам PVLAN.

Пример конфигурации

Применение PVLAN на одном устройстве 3-го уровня

Изображение 9-4	
Этапы конфигурации	❖ Настройте функцию PVLAN на устройстве (в данном примере на устройстве Switch A). Дополнительные сведения о конфигурации см. в разделе «Применение PVLAN между устройствами 2-го уровня». ❖ Установите порт, напрямую подключенный к серверу (в данном примере порт Gi 0/7), в качестве смешанного (promiscuous) порта. Затем все корпоративные пользователи могут взаимодействовать с сервером через смешанный (promiscuous) порт. ❖ Настройте адрес шлюза PVLAN на устройстве 3-го уровня (в данном примере Switch A) (в данном примере установите адрес SVI VLAN 2 на 192.168.1.1/24) и настройте сопоставление интерфейса 3-го уровня между первичной VLAN (в данном примере VLAN 2) и вторичными VLAN (в данном примере VLAN 10, VLAN 20 и VLAN 30). Затем все корпоративные пользователи могут обмениваться данными с внешней сетью через адрес шлюза. ⚠ Запустите PVLAN и настройте порты для подключения к устройствам как магистральные порты.

A	`SwitchA#configure terminal`
	`Enter configuration commands, one per line.  End with 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 mLAGing 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 конфигурации	Отправьте эхо-запрос на адрес шлюза 192.168.1.1 с хостов пользователей в различных поддоменах. Эхо-запрос выполнен 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
```

Типичные ошибки

- На первичной и вторичной VLAN частной PVLAN не выполнена привязка на 2-м уровне, и не удается настроить привязку на 3-м уровне.
- Устройство подключено к внешней сети до настройки привязки на 3-м уровне. В результате устройство не может установить связь с внешней сетью.
- Интерфейсы для подключения к серверу и внешней сети не настроены как смешанные (promiscuous) интерфейсы, что приводит к асимметричной пересылке пакетов восходящих и нисходящих потоков.

9.5 Мониторинг

Отображение

Описание	Команда
Отображает конфигурацию PVLAN.	**show vlan private-vlan**

Отладка

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

Описание	Команда
Отладка PVLAN.	**debug bridge pvlan**

10 КОНФИГУРИРОВАНИЕ MSTP

10.1 Обзор

Протокол STP (Spanning Tree Protocol) — это протокол управления уровня 2. Он может не только выборочно блокировать избыточные каналы для устранения петель уровня 2, но и может выполнять резервирование каналов.

Согласно требованиям современных сетей, на базе STP созданы протоколы RSTP (RLAGid Spanning Tree Protocol) и протокол MSTP (Multiple Spanning Tree Protocol).

Для Ethernet уровня 2 между двумя локальными сетями (LAN) может существовать только один активный канал. В противном случае произойдет широковещательный шторм. Для повышения надежности локальной сети необходимо создать резервный канал и сохранить некоторые пути в состоянии резервирования. Если сеть неисправна и канал неисправен, необходимо переключить резервный канал в активное состояние. STP может автоматически активировать резервный канал без выполнения каких-либо операций вручную. Протокол STP позволяет устройствам в локальной сети:

- Находить и начинать лучшую топологию дерева в локальной сети.
- Устранять неисправность и автоматически обновлять топологию сети, чтобы всегда выбирать наилучшую топологию дерева.

Топология LAN автоматически рассчитывается набором параметров моста, заданных администратором. Лучшую топологию дерева можно получить, правильно настроив данные параметры.

Протокол RSTP полностью совместим с протоколом 802.1D STP. Подобно традиционному протоколу STP, протокол RSTP предоставляет сервисы обхода петель и резервирования. Он характеризуется высокой скоростью. Если все мосты в локальной сети поддерживают протокол RSTP и настроены администратором надлежащим образом, то после изменения топологии сети потребуется менее 1 секунды (около 50 секунд, если используется традиционный протокол STP) для повторного создания топологии дерева.

STP и RSTP имеют следующие дефекты:

- Медленная миграция STP. Даже при использовании каналов «точка-точка» или пограничных портов для переключения портов в состояние пересылки требуется в два раза больше времени.
- Протокол RSTP может быстро сходиться, но имеет тот же дефект, что и STP: Так как все VLAN в локальной сети используют одно и то же связующее дерево, пакеты всех VLAN пересылаются по этому связующем дереву. Поэтому резервные каналы не могут быть заблокированы в соответствии с определенными сетями VLAN, и трафик данных не может быть сбалансирован между сетями VLAN.

Протокол MSTP, определенный IEEE в 802.1s, устраняет дефекты STP и RSTP. Он не только может быстро выполнить конвергенцию, но и может обеспечить

передачу трафика различных сетей VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для резервных каналов.

В целом, STP/RSTP работает на основе портов, а MSTP работает на основе объектов. Объект представляет собой набор из нескольких сетей VLAN. Привязка нескольких сетей VLAN к одному объекту может снизить издержки связи и коэффициент использования ресурсов.

Устройства QTECH поддерживают протоколы STP, RSTP, MSTP, а также соответствуют стандартам IEEE 802.1D, IEEE 802.1w и IEEE 802.1s.

Протоколы и стандарты

- IEEE 802.1D: Мосты управления доступом к среде (MAC)
- IEEE 802.1w: Часть 3: Мосты управления доступом к среде (MAC) — поправка 2: Быстрая перенастройка
- IEEE 802.1s: Виртуальные локальные сети с параллельным подключением — поправка 3: Множественные связующие деревья

10.2 Применение

Применение	Описание
Отказоустойчивая топология MSTP+VRRP	В иерархической модели 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 передачи данных протокола моста (Bridge Protocol Data Unit - BPDU) используется для реализации прозрачной передачи пакетов STP на основе туннеля.

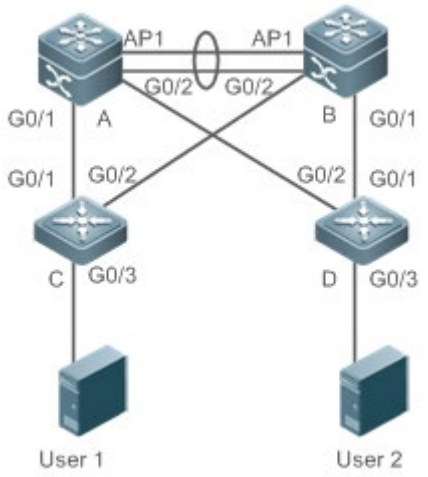
10.2.1 Отказоустойчивая топология MSTP+VRRP

Сценарий

Типичным применением MSTP является отказоустойчивая система MSTP+VRRP. Это решение является отличным решением для повышения доступности системы в сети. Используя иерархическую модель 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 основную сетевую систему для предоставления услуг обмена данными.

Главное преимущество этой архитектуры — ее иерархическая структура. В иерархической сетевой архитектуре все показатели емкости, характеристики и функции сетевых устройств на каждом уровне оптимизированы на основе их местоположения и ролей, что повышает их стабильность и доступность.

Изображение 10-1 Топология двухъядерной MSTP+VRRP



Заметки	Топология разделена на два уровня: Базовый уровень (устройства A и B) и уровень доступа (устройства C и D).

Описание

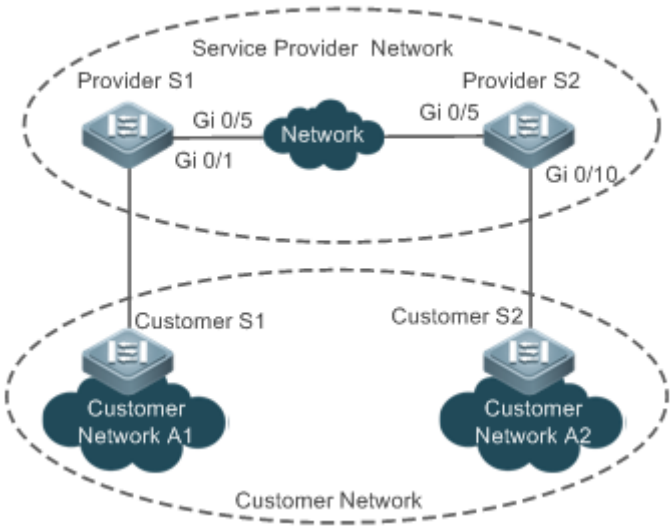
- Уровень ядра: Несколько объектов MSTP настроены для обеспечения балансировки нагрузки. Например, создаются два объекта: Объект 1 и объект 2. Объект 1 сопоставляется с VLAN 10, а объект 2 сопоставляется с VLAN 20. Устройство A является корневым мостом объектов 0 и 1 (объект 0 — CIST, существует по умолчанию). Устройство B является корневым мостом объекта 2.
- Уровень ядра: Устройства A и B являются активными устройствами VRRP в сетях VLAN 10 и VLAN 20 соответственно.
- Уровень доступа: Настройте порт, напрямую подключенный к терминалу (ПК или серверу), как порт PortFast и включите защиту BPDU, чтобы предотвратить несанкционированный доступ пользователей к неназначенным устройствам.

10.2.2 Туннель BPDU

Сценарий

Сеть QinQ обычно разделена на две части: сеть заказчика и сеть поставщика услуг (SP). Можно включить туннель BPDU для вычисления пакетов STP клиентской сети независимо от сети SP, тем самым предотвращая влияние пакетов STP клиентской сети на сеть SP.

Изображение 10-2 Топология туннеля BPDU



Заметки	Как показано на Изображении выше, верхняя часть — это сеть SP, а нижняя часть — сеть заказчика. Сеть SP состоит из двух пограничных устройств поставщика (PE): Provider S1 и Provider S2. Customer Network A1 и Customer Network A2 являются двумя объектами пользователя в разных регионах. Customer S1 и Customer S2 имеют доступ к устройствам из сети заказчика к сети SP, осуществляя доступ к сети SP соответственно через Provider S1 и Provider S2. С помощью туннеля BPDU сети Customer Network A1 и Customer Network A2 в разных регионах могут выполнять унифицированный расчет связующего дерева во всей сети SP, не влияя на расчет связующего дерева самой сети SP.

Описание

- Включите Basic QinQ на PE (в данном примере Provider S1/Provider S2), чтобы пакеты данных клиентской сети передавались в пределах указанной VLAN в сети SP.
- Включите прозрачную передачу STP на PE (в данном примере Provider S1/Provider S2), чтобы сеть SP могла передавать пакеты STP сети клиента через туннель BPDU.

10.3 Функции

Базовые концепции

BPDU

Для создания стабильной сети с топологией дерева необходимо выполнить следующие условия:

- Каждый мост имеет уникальный идентификатор, состоящий из приоритета моста и MAC-адреса.
- Издержка на путь от моста до корневого моста называется затратой на корневой путь.

- Каждый port ID состоит из приоритета порта и номера порта.

Мосты обмениваются пакетами BPDU для получения информации, необходимой для создания лучшей топологии дерева. Эти пакеты используют адрес многоадресной рассылки 01-80-C2-00-00-00 (шестнадцатеричный) в качестве адреса назначения.

BPDU состоит из следующих элементов:

- Идентификатора корневого моста принимаемого локальным мостом
- Стоимости корневого пути локального моста
- Идентификатора моста (идентификатор локального моста)
- Возраста сообщения (возраст пакета)
- Идентификатора порта (идентификатора порта, передающего этот пакет)
- **Forward-Delay Time**, **Hello Time**, **Max-Age Time** — это параметры времени, указанные в MSTP.
- Другие флаги, такие как флаги, указывающие на изменение топологии сети и состояния локального порта.

Если мост получает BPDU с более высоким приоритетом (меньший идентификатор моста и более низкая стоимость корневого пути) на порту, он сохраняет информацию BPDU на этом порте 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 высокими приоритетами по всей сети. Результаты обмена BPDU следующие:

- Мост выбирается в качестве корневого моста.
- За исключением корневого моста, каждый мост имеет корневой порт, то есть порт, обеспечивающий кратчайший путь к корневому мосту.
- Каждый мост рассчитывает кратчайший путь к корневому мосту.
- Каждая локальная сеть имеет назначенный мост, который находится в самом коротком пути между этой локальной сетью и корневым мостом. Порт, предназначенный для подключения моста к локальной сети, называется назначенным портом.
- Корневой порт и назначенный порт входят в состояние пересылки.

Идентификатор моста

Согласно IEEE 802.1W, каждый мост имеет уникальный идентификатор. Алгоритм связующего дерева выбирает корневой мост на основе идентификатора моста. Идентификатор моста состоит из восьми байт, из которых последние шесть байт являются MAC-адресом моста. В первых двух байтах идентификатора моста (как указано в следующей таблице) четыре бита указывают на приоритет, а последние восемь битов указывают идентификатор системы для использования в расширенном протоколе. В RSTP идентификатор системы — 0. Таким образом, приоритет моста должен быть интегральным кратным 4096.

	Бит	Значение
Значение приоритета	16	32768
	15	16384
	14	8192
	13	4096
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 связующего дерева

На производительность всего связующего дерева влияют следующие три таймера:

- Таймер Hello: Интервал периодической отправки пакета BPDU.
- Таймер Forward-Delay: Интервал для изменения состояния порта, то есть интервал для перехода порта из состояния прослушивания в состояние обучения или из состояния обучения в состояние пересылки, когда RSTP работает в режиме, совместимом с STP.

- Таймер Max-Age: Самый длительный срок жизни (TTL) пакета BPDU. По истечении этого времени пакет отбрасывается.

Роли портов и состояния портов

Каждый порт играет роль в сети, чтобы отразить различные функции в топологии сети.

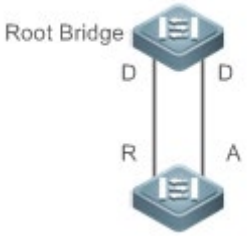
- Корневой порт: Порт, обеспечивающий кратчайший путь к корневому мосту.
- Назначенный порт: Порт, используемый каждой локальной сетью для подключения корневого моста.
- Альтернативный порт: Альтернативный порт для корневого порта. После того как корневой порт утратит способность воздействовать на локальную сеть, альтернативный порт немедленно переключается на него.
- Резервный порт: Резервный порт назначенного порта. Если мост имеет два порта, подключенных к локальной сети, порт с более высоким приоритетом является назначенным портом, а порт с более низким приоритетом — резервным портом.
- Отключенный порт: Неактивный порт. Эту роль исполняют все порты, чей канал опущен на консоли мультиплексирования.

На следующих рисунках показаны роли различных портов:

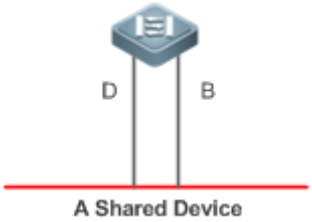
R = корневой порт, D = назначенный порт, A = Альтернативный порт, B = резервный порт

Если не указано иное, приоритеты портов уменьшаются слева направо.

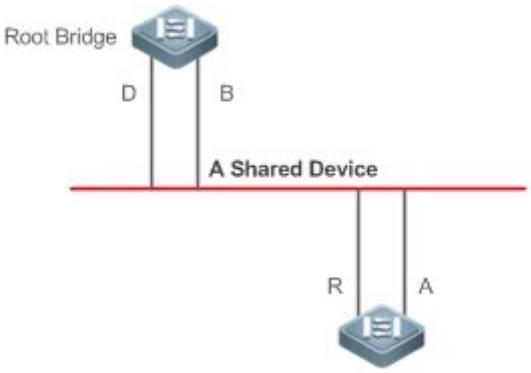
Изображение 10-3



Изображение 10-4



Изображение 10-5



Каждый порт имеет три состояния, указывающие, следует ли пересылать пакеты данных для управления всей топологией связующего дерева.

- Отклоняет: Не пересылает полученные пакеты и не запоминает MAC-адрес источника.
- Обучается: Не пересылает полученные пакеты, но запоминает MAC-адрес источника, который находится в транзитном состоянии.
- Пересылает: Пересылает полученные пакеты и запоминает MAC-адрес источника.

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 отмены.

Число переходов

Внутренние связующие деревья (IST) и несколько объектов связующего дерева (MSTI) вычисляют, истекает ли время пакета BPDU на основе IP TTL-механизма подсчета переходов, а не на основе Message Age и Max Age.

Для настройки количества переходов рекомендуется запустить команду **spanning-tree max-hops** в режиме глобальной конфигурации. В зоне каждый раз, когда пакет BPDU проходит через устройство от корневого моста, счетчик переходов уменьшается на 1. Когда счетчик переходов равен 0, время пакетов 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.

Обзор

Функция	Описание
STP	Протокол STP, определенный IEEE в 802.1D, используется для устранения физических петель на уровне канала передачи данных в локальной сети.
RSTP	Протокол RSTP, определенный IEEE в 802.1w, оптимизирован на основе протокола STP для быстрой конвергенции топологии сети.

MSTP	Протокол MSTP, определенный IEEE в 802.1s, устраняет дефекты STP, RSTP и протокола Per-VLAN Spanning Tree (PVST). Он не только может быстро выполнить конвергенцию, но и может пересылать трафик различных сетей VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для резервных каналов.
Расширенные функции MSTP	MSTP включает следующие функции: PortFast, BPDU Guard, BPDU Filter, TC Protection, TC Guard, фильтрацию TC, проверку BPDU на основе MAC-адреса источника, фильтрацию BPDU на основе недопустимой длины, Auto Edge, root guard и loop guard.

10.3.1 STP

Протокол STP используется для предотвращения широковещательных штормов, вызванных петлями, и обеспечения резервирования каналов.

Принцип работы

Для Ethernet уровня 2 между двумя LAN может существовать только один активный канал. В противном случае произойдет широковещательный шторм. Для повышения надежности локальной сети необходимо создать резервный канал и сохранить некоторые пути в состоянии резервирования. Если сеть неисправна и канал неисправен, необходимо переключить резервный канал в активное состояние. STP может автоматически активировать резервный канал без выполнения каких-либо операций вручную. Протокол STP позволяет устройствам в локальной сети:

- Находить и начинать лучшую топологию дерева в локальной сети.
- Устранять неисправность и автоматически обновлять топологию сети, чтобы всегда выбирать наилучшую топологию дерева.

Топология LAN автоматически рассчитывается набором параметров моста, заданных администратором. Лучшую топологию дерева можно получить, правильно настроив данные параметры.

Связанная конфигурация

Включение связующего дерева

- По умолчанию функция связующего дерева отключена.
- Запустите команду **spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds*], чтобы включить STP и настроить основные Настройки.
- Диапазон forward-time от 4 до 30. Диапазон hello-time от 1 до 10. Диапазон max-age от 6 до 40.

⚠ Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб. Диапазоны значений времени персылки (forward-time), времени приветствия (hello-time) и времени устаревания (max-age) связаны. При изменении одного из них изменяются два других диапазона. Три значения должны соответствовать следующим условиям: 2 x (Hello Time + 1 секунда)

<= Max-Age Time <= 2 x (Forward-Delay Time –1 секунда). В противном случае конфигурация не будет выполнена.

10.3.2 RSTP

Протокол RSTP полностью совместим с протоколом 802.1D STP. Подобно традиционному протоколу STP, протокол RSTP предоставляет сервисы обхода петель и резервирования. Он характеризуется высокой скоростью. Если все мосты в локальной сети поддерживают протокол RSTP и настроены администратором надлежащим образом, то после изменения топологии сети потребуется менее 1 секунды (около 50 секунд, если используется традиционный протокол STP) для повторного создания топологии дерева.

Принцип работы

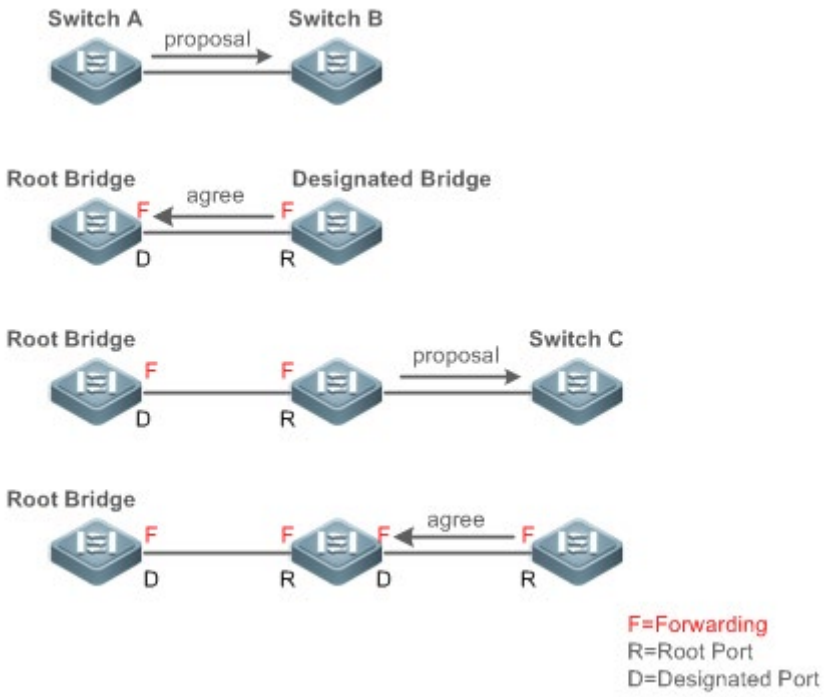
Быстрая конвергенция RSTP

RSTP имеет специальную функцию, быстрого перестроения портов в состояние пересылки.

STP позволяет порту войти в состояние пересылки через 30 секунд (удвоенное время Forward-Delay Time; его можно настроить в значение по умолчанию 15 секунд) после выбора роли порта. Каждый раз при изменении топологии корневой порт и назначенный порт, переизбранные каждым мостом, вступают в состояние пересылки на 30 секунд позднее. Поэтому для того, чтобы вся топология сети стала деревом, требуется около 50 секунд.

Протокол RSTP сильно отличается от STP в процессе пересылки. Как показано на Изображении 10-6, коммутатор Switch A отправляет пакет предложения RSTP Proposal коммутатору Switch B. Если коммутатор B обнаруживает, что приоритет коммутатора A выше, он выбирает коммутатор A в качестве корневого моста, а порт, получающий пакет в качестве корневого порта, переходит в состояние пересылки, и затем отправляет пакет согласования Agree из корневого порта коммутатору A. Если назначенный порт коммутатора A согласован, порт переходит в состояние пересылки. Назначенный коммутатор B пересылает пакет Proposal для последовательного расширения связующего дерева. Теоретически RSTP может восстановить топологию дерева сети для быстрой конвергенции после изменения топологии сети.

Изображение 10-6

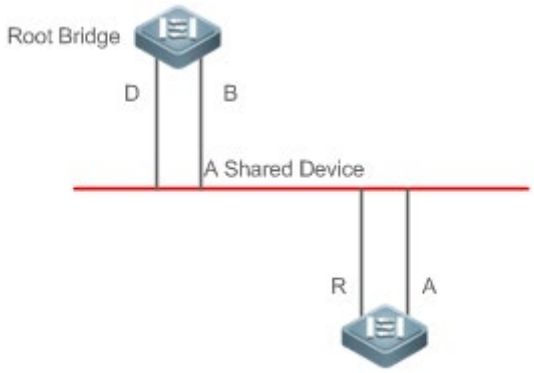


Описанный выше процесс установления соединения выполняется только в том случае, если соединение между портами находится в режиме «точка-точка». Для обеспечения полного воспроизведения устройств рекомендуется не включать двухточечное соединение между устройствами.

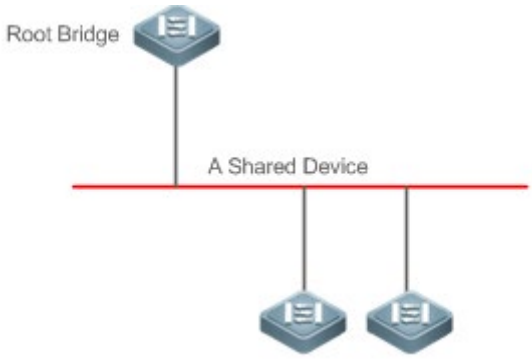
Изображение 10-7 и Изображение 10-8 изображают примеры соединений, отличных от «точка-точка».

Пример соединения, отличного от «точка-точка»:

Изображение 10-7

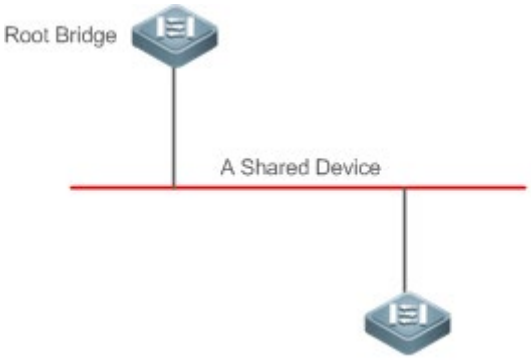


Изображение 10-8



На Изображении 10-9 показан пример соединения «точка-точка».

Изображение 10-9



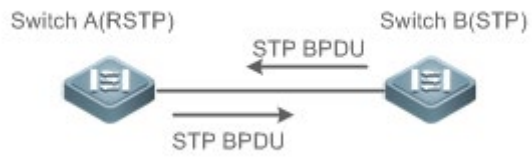
Совместимость между RSTP и STP

Протокол RSTP полностью совместим с протоколом STP. Протокол RSTP автоматически проверяет, поддерживает ли подключенный мост протокол STP или RSTP на основании номера версии полученного BPDU. Если порт подключается к мосту STP, порт переходит в состояние пересылки через 30 секунд, что не позволяет RSTP полностью воспроизвести его.

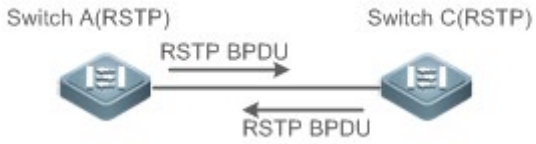
Другая проблема может возникнуть при совместном использовании RSTP и STP. Как показано на следующих рисунках, коммутатор Switch A (RSTP) подключается к коммутатору Switch B (STP). Если коммутатор A обнаруживает, что подключен к мосту STP, он отправляет пакет BPDU STP. Однако если коммутатор B заменяется коммутатором C (RSTP), но коммутатор A все еще отправляет пакеты BPDU STP, коммутатор C будет считать себя подключенным к мосту STP. В результате два устройства RSTP работают под STP, что значительно снижает эффективность.

Протокол RSTP предоставляет функцию миграции протокола для принудительной отправки пакетов RSTP BPDU (одноранговый мост должен поддерживать RSTP). В этом случае коммутатор A принудительно отправляет RSTP BPDU, а коммутатор C затем обнаруживает, что он подключен к мосту RSTP. В результате под RSTP работают два устройства RSTP, как показано на Изображении 10-11.

Изображение 10-10



Изображение 10-11



Связанная конфигурация

Настройка переноса протоколов

- Запустите команду **clear spanning-tree detected-protocols** [**interface** *interface-id*], чтобы принудительно проверить версию на порту. Подробнее см. в разделе «Совместимость между RSTP и STP».

10.3.3 MSTP

MSTP устраняет дефекты STP и RSTP. Он не только может быстро выполнить конвергенцию, но и может пересылать трафик различных сетей VLAN по соответствующим путям, тем самым обеспечивая лучший механизм балансировки нагрузки для резервных каналов.

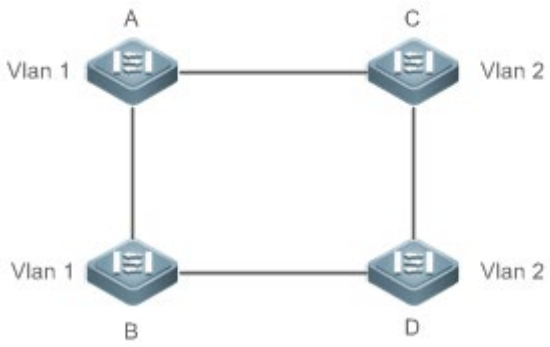
Принцип работы

Устройства QTECH поддерживают MSTP. MSTP — это новый протокол связующего дерева, разработанный на основе традиционных протоколов STP и RSTP и включающий механизм быстрой пересылки RSTP.

Поскольку традиционные протоколы связующего дерева не имеют отношения к сетям VLAN, в некоторых топологиях сети могут возникнуть проблемы:

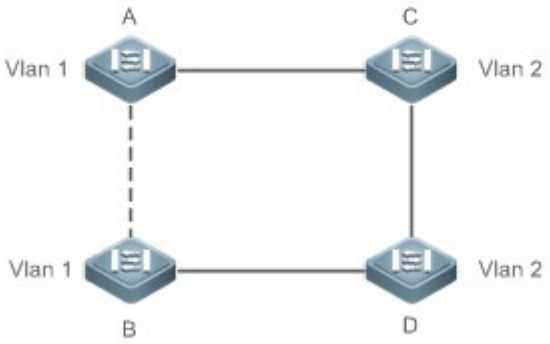
Как показано на Изображении 10-12, устройства A и B находятся в сети VLAN 1, а устройства C и D находятся в сети VLAN 2, образуя петлю.

Изображение 10-12



Если связь между устройством A и устройством B через устройства C и D стоит меньше, чем связь между устройством A напрямую и устройством B, связь между устройством A и устройством B переходит в состояние отмены (как показано на Изображении 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 установить связь с VLAN 1 устройства B.

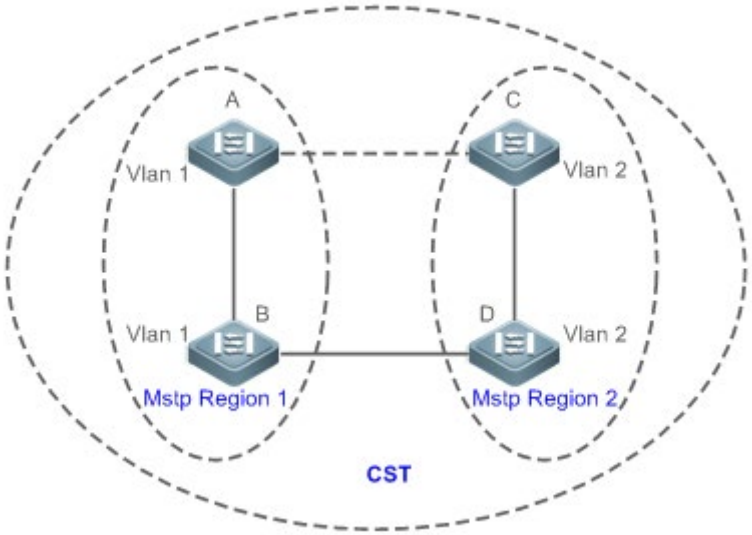
Изображение 10-13



Для решения этой проблемы разработан MSTP. Он делит одну или несколько VLAN устройства на объекты. Устройства, настроенные с одним и тем же объектом, образуют область MST для запуска независимого связующего дерева (называемого IST). В данной зоне MST, как и в масштабированном в большую сторону устройстве, используется алгоритм связующего дерева с другими областями MST для создания полного связующего дерева, называемого общим связующим деревом (CST).

На основе этого алгоритма вышеуказанная сеть может сформировать топологию, показанную на Изображении 10-14 в алгоритме MSTP: Устройства A и B находятся в зоне MSTP 1, в которой не происходит петель, и поэтому ни один канал не переходит в состояние отмены. Это также относится к зоне MSTP 2. Зона 1 и зона 2, как и два масштабированных устройства с объектами в состоянии петли, выбирают канал, чтобы войти в состояние отмены на основе соответствующей конфигурации.

Изображение 10-14



Это предотвращает возникновение петель для обеспечения надлежащего обмена данными между устройствами в одной и той же сети VLAN.

Разделение зон MSTP

Для обеспечения надлежащего воспроизведения MSTP правильно разделите зоны MSTP и настройте ту же информацию о конфигурации MST для устройств в одной и той же зоне MSTP.

Информация о конфигурации MST включает:

- Имя конфигурации MST: Содержит не более 32 байт для идентификации зоны MSTP.
- Номер ревизии MST: Состоит из 16 бит для идентификации области MSTP.
- Таблица сопоставления объекта MST-к-VLAN: Для каждого устройства создается не более 64 объектов (с их идентификаторами от 1 до 64), а объект 0 обязателен к существованию. Таким образом, система поддерживает не более 65 объектов. При необходимости пользователи могут назначить от 1 до 4994 VLAN, принадлежащих разным объектам (от 0 до 64). По умолчанию неназначенные VLAN принадлежат объекту 0. В этом случае каждая MSTI является группой VLAN и реализует алгоритм связующего дерева MSTI, указанный в пакете BPDU, не подверженного влиянию CIST и других MSTI.

Запустите команду **spanning-tree mst configuration** в режиме глобальной конфигурации, чтобы войти в режим конфигурации MST, чтобы настроить указанную выше информацию.

Блоки BPDU MSTP имеют указанную выше информацию. Если BPDU, полученный устройством, содержит ту же информацию о конфигурации MST, что и информация об устройстве, оно считает, что подключенное устройство принадлежит к той же области MST. В противном случае устройство будет подключено из другого региона MST.

После отключения MSTP рекомендуется настроить таблицу привязки объекта-к-VLAN. После настройки снова включите MSTP, чтобы обеспечить стабильность и конвергенцию топологии сети.

IST (связующее дерево в регионе MSTP)

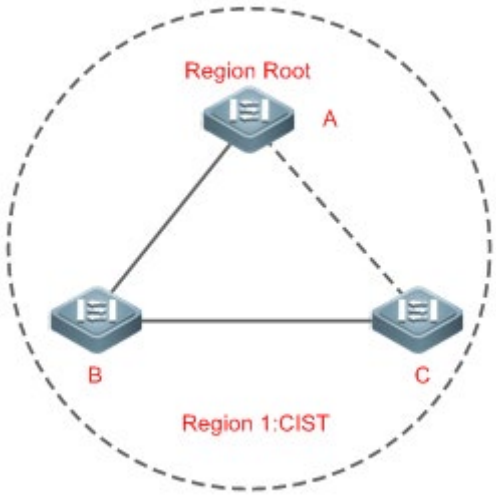
После деления областей MSTP каждая область выбирает независимый корневой мост для каждого объекта на основе соответствующих параметров, таких как приоритет моста и приоритет порта, назначает роли каждому порту на каждом устройстве, и указывает, находится ли порт в состоянии пересылки или отмены в объекте на основе роли порта.

При обмене BPDU MSTP генерируется IST, и каждый объект имеет свои собственные связующие деревья (MSTI), в которых связующее дерево, соответствующее объекту 0 и CST, равномерно называется общим связующим деревом объекта (CIST). То есть, каждый объект предоставляет единую топологию сети без петель для собственных групп VLAN.

Как показано на Изображении 10-15, устройства A, B и C образуют петлю в зоне 1.

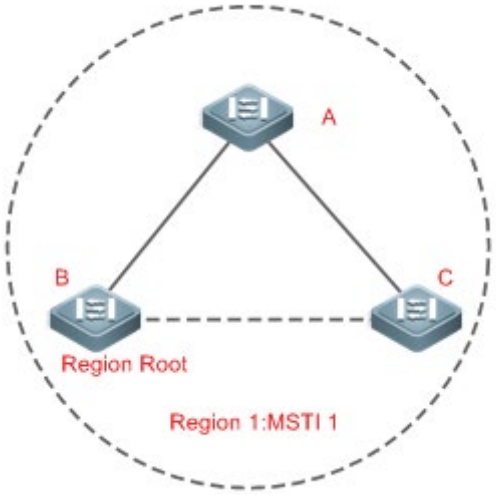
Как показано на Изображении 10-15, устройство A имеет самый высокий приоритет в CIST (объект 0) и, таким образом, выбрано в качестве корневого каталога региона. Затем MSTP позволяет каналу A и C войти в состояние отмены на основе других параметров. Таким образом, для группы VLAN объекта 0 доступны только каналы от A до B и от B до C, прерывая цикл этой группы VLAN.

Изображение 10-15



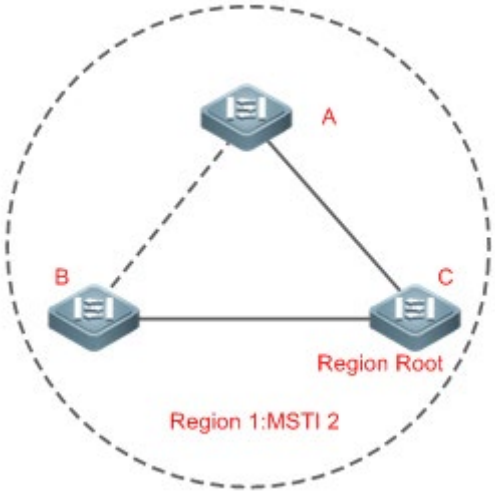
Как показано на Изображении 10-16, устройство B имеет самый высокий приоритет в MSTI 1(объект 1) и, таким образом, выбрано в качестве корневого каталога зоны. Затем MSTP позволяет каналу между B и C войти в состояние отмены на основе других параметров. Таким образом, для группы VLAN объекта 1 доступны только каналы от A до B и от B до C, прерывая цикл этой группы VLAN.

Изображение 10-16



Как показано на Изображении 10-17, устройство C имеет самый высокий приоритет в MSTI 2 (объект 2) и, таким образом, выбрано в качестве корневого каталога зоны. Затем MSTP позволяет каналу между B и C войти в состояние отмены на основе других параметров. Таким образом, для группы VLAN объекта 2 доступны только каналы от B до C и от A до C, прерывая цикл этой группы VLAN.

Изображение 10-17



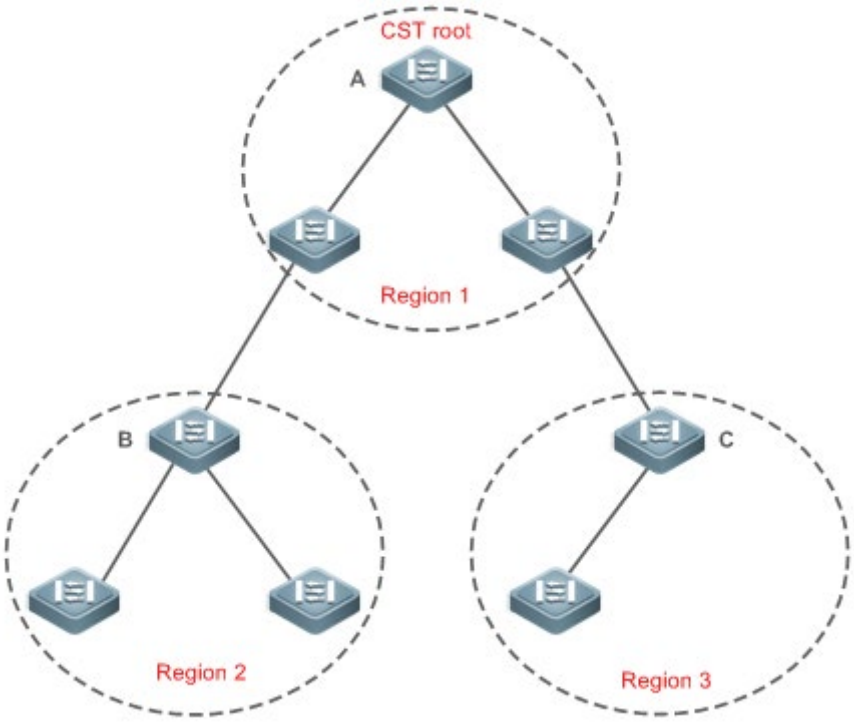
Обратите внимание, что MSTP не заботится о том, к какой VLAN принадлежит порт. Поэтому пользователи должны настроить стоимость и приоритет пути для соответствующего порта на основе фактической конфигурации VLAN, чтобы предотвратить прерывание протоколом MSTP неправильных петель.

CST (связующее дерево между зонами MSTP)

Каждая зона MSTP похожа на масштабированное устройство (мейнфрейм) для CST. Различные области MSTP образуют дерево топологии сети с битом под

названием CST. Как показано на Изображении 10-18, устройство A, идентификатор моста которого является наименьшим, выбирается в качестве корневого объекта во всем CST и корневым каталогом зоны CIST в этой зоне. В регионе 2, поскольку стоимость корневого пути от устройства B к корневому каталогу CST является самой низкой, устройство B выбирается в качестве корневого каталога зоны CIST в этой зоне. По этой же причине устройство C выбирается в качестве корневого каталога зоны CIST.

Изображение 10-18



Корень каталога зоны CIST может не быть устройством, идентификатор моста которого является наименьшим в зоне, но указывает устройство, стоимость корневого пути из данной зоны которого до корневого каталога зоны CST является наименьшей.

Для MSTI корневой порт каталога зоны CIST имеет новую роль «мастер-порт». Мастер-порт выступает в качестве исходящего порта всех объектов и находится в состоянии пересылки для всех объектов. Чтобы топология была более стабильной, рекомендуется, чтобы главный порт каждой зоны, ведущий к корневому каталогу CST, был, по возможности, на одном устройстве зоны.

Совместимость между MSTP, RSTP и STP

Подобно RSTP, MSTP отправляет BPDU STP для совместимости с STP. Подробнее см. в разделе «Совместимость между RSTP и STP».

Поскольку RSTP обрабатывает BPDU MSTP зоны CIST, MSTP не нужно отправлять BPDU RSTP, чтобы они были совместимы с ним.

Каждое устройство STP или RSTP является одной зоной и не образует одну и ту же зону с любыми устройствами.

Связанная конфигурация

Конфигурирование STP

- По умолчанию STP работает в режиме MSTP.
- Запустите **spanning-tree mode** [**stp | rstp | mstp**], чтобы изменить режим STP.

10.3.4 Дополнительные функции MSTP

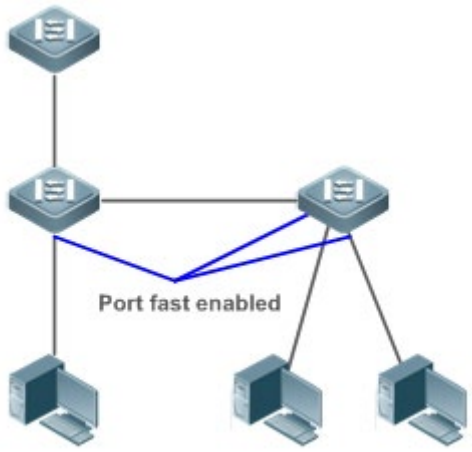
Дополнительные функции MSTP, в основном, включают порт PortFast, защиту BPDU, фильтр BPDU, защиту TC и обыкновенную защиту. Дополнительные функции в основном используются для развертывания конфигураций MSTP на основе топологии сети и характеристик применения в сети MSTP. Это повышает стабильность, надежность и способность MSTP к отражению атак, удовлетворяя требованиям к применению MSTP в различных сценариях использования.

Принцип работы

PortFast

Если порт устройства подключается непосредственно к сетевому терминалу, этот порт настраивается как порт PortFast для прямого входа в состояние пересылки. Если порт PortFast не настроен, порт должен подождать 30 секунд, чтобы войти в состояние пересылки. Изображение 10-19 показывает, какие порты устройства можно настроить как порты PortFast.

Изображение 10-19



Если порт PortFast по-прежнему получает блоки BPDU, его состояние работы быстрого порта отключается, и порт переходит в состояние пересылки в соответствии с обычным алгоритмом STP.

BPDU Guard

Защита BPDU может быть включена глобально или включена на интерфейсе.

Для включения глобальной защиты BPDU рекомендуется запустить команду **spanning-tree portfast bpduguard default** в режиме глобальной конфигурации. Если PortFast включен на порту или этот порт автоматически определяется как граничный порт, этот порт переходит в состояние отключенного из-за ошибки, что указывает на ошибку конфигурации сразу после получения BPDU. В то же время

порт отключен, указывая, что неавторизованный пользователь может добавить сетевое устройство для изменения топологии сети.

Также рекомендуется запустить команду **spanning-tree bpduguard enable** в режиме конфигурации интерфейса, чтобы включить защиту BPDU на порту (независимо от того, включен или нет порт PortFast). В этом случае порт переходит в состояние отключения из-за ошибки сразу после получения BPDU.

Фильтр BPDU

Фильтр BPDU можно включить глобально или на интерфейсе.

Для включения глобального фильтра BPDU рекомендуется выполнить команду **spanning-tree portfast bpdufilter default** по умолчанию в режиме глобальной конфигурации. В этом случае порт PortFast не получает и не отправляет блоки BPDU, поэтому хост, подключаясь напрямую к порту PortFast, не получает блоков BPDU. Если после получения BPDU порт изменяет свое состояние работы быстрого порта на Disabled (Отключено), фильтр BPDU автоматически пропускается.

Также рекомендуется запустить команду **spanning-tree bpdufilter enable** в режиме конфигурации интерфейса, чтобы включить фильтр BPDU на порту (независимо от того, включен или нет порт PortFast). В этом случае порт не получает и не отправляет BPDU, а напрямую входит в состояние пересылки.

Защита TC

Блоки BPDU TC представляют собой пакеты BPDU, которые передают TC. Если коммутатор получает такие пакеты, он указывает на изменение топологии сети и удаляет таблицу MAC-адресов коммутатора. В этом случае для коммутаторов уровня 3 модуль пересылки снова включен, и состояние порта в записи ARP изменяется. При атаке на коммутатор с помощью вилочных блоков BPDU TC, он часто выполняет указанные выше операции, вызывая высокую нагрузку и влияя на стабильность сети. Чтобы предотвратить эту проблему, можно включить защиту TC.

Защиту TC можно включить или отключить только в глобальном масштабе. Данная функция выключена по умолчанию.

Когда защита TC включена, коммутатор удаляет блоки BPDU TC в течение заданного периода времени (обычно 4 секунд) после их получения и отслеживает, получен ли в течение этого периода какой-либо пакет BPDU TC. Если устройство получает пакеты TC BPDU в течение этого периода, оно удаляет их по истечении этого времени. Это может предотвратить частое удаление устройством записей MAC-адресов и записей ARP.

TC Guard

Защита TC обеспечивает уменьшение динамических MAC-адресов и записей ARP, которые удаляются при генерации большого количества пакетов TC в сети. Тем не менее, устройство, получающее пакеты атаки TC, по-прежнему выполняет множество операций удаления, и пакеты TC могут быть распределены, что влияет на всю сеть. Пользователи могут включить защиту TC, чтобы предотвратить распространение пакетов TC глобально или через порт. Если

защита TC включена глобально или на порту, порт, принимающий пакеты TC, фильтрует эти пакеты TC или пакеты TC, генерируемые самим портом, чтобы пакеты TC не распространялись на другие порты. Это позволяет эффективно контролировать возможные атаки TC в сети для обеспечения стабильности сети. В частности, на устройствах уровня 3 эта функция может эффективно предотвратить мерцания устройства уровня доступа и прерывание маршрута уровня ядра.

⚠ Если защита TC используется неправильно, связь между сетями прерывается.

⚠ Эту функцию рекомендуется включать только в том случае, если в сети получены нелегальные пакеты атак TC.

⚠ Если защита TC включена глобально, ни один порт не распределяет пакеты TC между другими. Эту функцию можно включить только на устройствах доступа, таких как ноутбуках.

⚠ Если на порту включена защита TC, топология изменится, и пакеты TC, полученные на порту, не будут распространяться на другие порты. Эту функцию можно включить только на портах восходящего канала, особенно на портах мультиплексора уровня ядра.

Фильтр TC

Если на порту включена защита TC, он не пересылает полученные и сгенерированные пакеты TC другим портам, выполняющим расчет связующего дерева на устройстве. Когда состояние порта изменяется (например, с блокировки на пересылку), он генерирует пакеты TC, что указывает на изменение топологии.

В этом случае, поскольку защита TC предотвращает распространение пакетов TC, устройство может не очистить MAC-адреса порта при изменении топологии сети, что приведет к ошибке пересылки данных.

Для решения этой проблемы внедрен фильтр TC. Фильтр TC не обрабатывает пакеты TC, полученные портами, но обрабатывает пакеты TC в случае нормальных изменений топологии. Если фильтр TC включен, проблема с удалением адреса будет устранена, и маршрут уровня ядра не будет прерван, если каналы портов, не включенные с функцией PortFast, будут подниматься или опускаться на консоли мультиплексора, а записи маршрутизации уровня ядра могут быть обновлены своевременно при изменении топологии.

⚠ По умолчанию фильтр TC отключен.

Проверка MAC-адреса источника BPDU

Проверка MAC-адреса источника BPDU предотвращает злоумышленные атаки пакетов BPDU и приводит к отклонениям MSTP. После определения коммутатора, подключенного к порту на канале «точка-точка», можно включить проверку MAC-адреса источника BPDU для получения пакетов BPDU, отправленных только одноранговым коммутатором, и отбросить все остальные пакеты BPDU, тем самым предотвращая атаки злоумышленников. Можно включить проверку MAC-адреса источника BPDU в режиме конфигурации интерфейса для определенного порта. Один порт может фильтровать только один MAC-адрес. Если вы

запускаете команду **no bpdu src-mac-check** для отключения проверки MAC-адреса источника BPDU на порту, порт начинает получать все пакеты BPDU.

Фильтр BPDU

Если длина BPDU протокола Ethernet превышает 1500, этот BPDU будет отброшен, предотвращая получение нелегальных пакетов BPDU.

Auto Edge

Если назначенный порт устройства не получает BPDU от порта нисходящего канала в течение определенного периода (3 секунд), устройство рассматривает сетевой хост, подключенный к назначенному порту, настраивает порт как граничный порт и переключает порт непосредственно в состояние пересылки. После получения BPDU граничный порт будет автоматически идентифицирован как неграничный порт.

Чтобы отключить функцию Auto Edge, можно запустить команду **spanning-tree autoedge disabled**.

Данная функция включена по умолчанию.

⚠ Если функция Auto Edge конфликтует с настроенным вручную PortFast, приоритет имеет ручная настройка.

⚠ Поскольку эта функция используется для быстрого согласования и пересылки между назначенным портом и портом нисходящего канала, STP не поддерживает эту функцию. Если назначенный порт находится в состоянии пересылки, конфигурация Auto Edge не будет влиять на этот порт. Это требуется только при повторном выполнении быстрого согласования, например, при извлечении и подключении сетевого кабеля.

⚠ Если фильтр BPDU включен на порту, порт напрямую переходит в состояние пересылки и не определяется автоматически как граничный порт.

⚠ Эта функция применяется только к назначенному порту.

Root Guard

При проектировании сети корневой мост и резервный корневой мост всегда разделяются в одном регионе. Если обслуживающий персонал выполнил неправильную конфигурацию или совершается вредоносная атака на сеть корневой мост может получать информацию о конфигурации с более высоким приоритетом и, таким образом, переключается на резервный корневой мост, что приводит к неправильным изменениям в топологии сети. Для решения этой проблемы используется Root guard (Защита от корневого доступа).

Если на порту включена защита от корневого доступа, роли этого порта на всех объектах будут принудительно заданы в качестве назначенного порта. После того как порт получает информацию о конфигурации с более высоким приоритетом, он переходит в состояние, не согласованное с корнем (блокирующее). Если порт не получает информацию о конфигурации с более высоким приоритетом в течение определенного периода времени, он возвращается в исходное состояние.

Если порт переходит в блокирующее состояние из-за защиты корневого каталога, можно вручную восстановить порт в нормальное состояние, отключив защиту корневого каталога на этом порту или отключив защиту связующего дерева

(выполнив в режиме конфигурации интерфейса команду **spanning-tree guard none**).

- При неправильном использовании защиты от корневого доступа сетевое соединение будет разорвано.
- Если на неназначенном порту включена защита от корневого доступа, этот порт будет принудительно использоваться в качестве назначенного порта и войдет в состояние BKN. Это указывает на то, что порт переходит в состояние блокировки из-за несоответствия корневого каталога.
- Если порт переходит в состояние BKN из-за получения информации о конфигурации с более высоким приоритетом в MST0, этот порт будет принудительно использоваться в состоянии BKN во всех остальных случаях.
- Защита от корневого доступа и защита от петель не может быть применена на порту в одно и то же время.

Loop Guard

Из-за однонаправленного сбоя канала корневой порт или резервный порт становятся назначенным портом и переходят в состояние пересылки, если они не получают BPDU, что приводит к возникновению сетевой петли. Loop guard (защита от петли) предотвращает эту проблему.

Если порт, включенный с функцией Loop Guard, не получает BPDU, он переключает свою роль, но остается в состоянии блокирования до получения BPDU и перерасчета связующего дерева.

- Можно включить функцию защиты от петель глобально или на порту.
- Защита от корневого доступа и защита от петель не может быть применена на порту в одно и то же время.
- Перед перезапуском MSTP порт переходит в состояние блокировки в системе защиты от петель. Если после перезапуска MSTP порт по-прежнему не получает BPDU, порт становится назначенным портом и переходит в состояние пересылки. Поэтому рекомендуется определить причину, по которой порт переходит в состояние блокировки в системе защиты от петель, и устранить неисправность как можно скорее перед перезапуском MSTP. В противном случае после перезапуска MSTP топология связующего дерева будет по-прежнему несогласованной.

Прозрачная передача BPDU

В IEEE 802.1Q в качестве зарезервированного адреса используется MAC-адрес назначения BPDU 01-80-C2-00-00-00. То есть устройства, совместимые с IEEE 802.1Q, не пересылают полученные пакеты BPDU. Однако при фактическом развертывании сети устройствам может потребоваться прозрачная передача пакетов BPDU. Например, если протокол STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы связующее дерево было правильно рассчитано.

- Прозрачная передача BPDU отключена по умолчанию.
- Прозрачная передача BPDU вступает в силу, только если протокол STP отключен. Если протокол STP включен на устройстве, устройство не передает пакеты BPDU прозрачно.

Туннель BPDU

Сеть QinQ обычно разделена на две части: сеть заказчика и сеть поставщика услуг. Перед тем как пакет пользователя войдет в сеть поставщика услуг, он инкапсулируется с меткой VLAN в данной сети, а также сохраняет исходный тег VLAN в качестве передаваемых данных. В результате пакет передает два тега VLAN для прохождения через сеть поставщика услуг. В сети поставщика услуг пакеты передаются только на основе внешней метки VLAN. Когда пакеты покидают сеть поставщика услуг, метка VLAN внешнего уровня удаляется.

Функция прозрачной передачи пакетов STP, а именно туннель BPDU, может использоваться для реализации передачи пакетов STP между сетями заказчика без какого-либо влияния на сеть поставщика услуг. Если пакет STP, отправленный из сети заказчика, входит в PE, PE изменяет MAC-адрес назначения пакета на частный адрес до того, как пакет будет передан сетью поставщика услуг. Когда пакет достигает PE на стороне однорангового узла, PE изменяет MAC-адрес назначения на публичный адрес и возвращает пакет в сеть заказчика на стороне однорангового узла, реализуя прозрачную передачу по сети поставщика услуг. В этом случае протокол STP в сети заказчика рассчитывается независимо от протокола в сети поставщика услуг.

Связанная конфигурация

Настройка PortFast

- По умолчанию PortFast выключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast default** для включения PortFast на всех портах и команду **no spanning-tree portfast default** для отключения PortFast на всех портах.
- В режиме настройки интерфейса запустите команду **spanning-tree portfast** для включения PortFast на порту и команду **spanning-tree portfast disabled** для отключения PortFast на всех портах.

Настройка BPDU Guard

- По умолчанию BPDU guard отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast default** для включения PortFast на всех портах и команду **no spanning-tree portfast default** для отключения PortFast на всех портах.
- В режиме настройки интерфейса запустите команду **spanning-tree bpduguard enabled** для включения BPDU guard на порту и команду **spanning-tree bpduguard disabled** для отключения BPDU guard на порту.

Настройка фильтра BPDU

- По умолчанию фильтр BPDU отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree portfast bpdufilter default** для включения BPDU filter на всех портах и команду **no spanning-tree portfast bpdufilter default** для отключения BPDU filter на всех портах.
- В режиме настройки интерфейса запустите команду **spanning-tree bpdufilter enabled** для включения BPDU filter на порту и команду **spanning-tree bpdufilter disabled** для отключения BPDU filter на порту.

Настройка защиты TC (Topology Change - Изменение топологии)

- По умолчанию защита TC отключена.
- В режиме глобальной конфигурации запустите команду **spanning-tree tc-protection** для включения защиты TC на всех портах и команду **no spanning-tree tc-protection** для отключения защиты TC на всех портах.
- Защиту TC можно включить или отключить только глобально.

Включение функции TC Guard

- По умолчанию TC guard отключен.
- В режиме глобальной конфигурации запустите команду **spanning-tree tc-protection tc-guard** для включения защиты TC на всех портах и команду **no spanning-tree tc-protection tc-guard** для отключения защиты TC на всех портах.
- В режиме настройки интерфейса запустите команду **spanning-tree tc-guard** для включения TC guard на порту и команду **no spanning-tree tc-guard** для отключения TC guard на порту.

Настройка фильтра TC

- По умолчанию фильтр TC отключен.
- В режиме настройки интерфейса запустите команду **spanning-tree ignore tc** для включения TC filter на порту и команду **no spanning-tree ignore tc** для отключения TC filter на порту.

Включение проверки MAC-адреса источника BPDU

- Проверка MAC-адреса источника BPDU отключена по умолчанию.
- В режиме конфигурации интерфейса запустите команду **bpdu src-mac-check** *H.H.H* для включения проверки MAC-адреса источника BPDU на порту и команду **no bpdu src-mac-check** для выключения ее на порту.

Настройка Auto Edge

- По умолчанию функция Auto Edge отключена.
- В режиме настройки интерфейса запустите команду **spanning-tree autoedge** для включения Auto Edge на порту и команду **spanning-tree autoedge disabled** для отключения ее на порту.

Настройка защиты от корневого доступа (Root Guard)

- По умолчанию Root guard отключен.
- В режиме настройки интерфейса запустите команду **spanning-tree guard root** для включения Root Guard на порту и команду **no spanning-tree guard root** для отключения Root Guard на порту.

Настройка функции Loop Guard

- По умолчанию функция Loop Guard отключена.
- В режиме глобальной конфигурации запустите команду **spanning-tree loopguard default** для включения Loop Guard на всех портах и команду **no spanning-tree loopguard default** для отключения Loop Guard на всех портах.
- В режиме настройки интерфейса запустите команду **spanning-tree guard loop** для включения Loop Guard на порту и команду **no spanning-tree guard loop** для отключения Loop Guard на порту.

Настройка прозрачной передачи BPDU

- Прозрачная передача BPDU отключена по умолчанию.
- В режиме глобальной конфигурации запустите команду **bridge-frame forwarding protocol bpdu** для включения прозрачной передачи BPDU и команду **no bridge-frame forwarding protocol bpdu** для выключения данной функции.
- Прозрачная передача BPDU вступает в силу, только если протокол STP отключен. Если протокол STP включен на устройстве, устройство не передает пакеты BPDU прозрачно.

Настройка туннеля BPDU

- По умолчанию туннель BPDU отключен.
- В режиме глобальной конфигурации выполните команду **l2protocol-tunnel stp**, чтобы глобально включить туннель BPDU и команду **no l2protocol-tunnel stp**, чтобы глобально отключить данную функцию.
- В режиме настройки интерфейса запустите команду **l2protocol-tunnel stp enable** для включения туннеля BPDU на порту и команду **no l2protocol-tunnel stp enable** для отключения данной функции на порту.
- Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса.

10.4 Настройка

Конфигурация	Описание и команда	
Включение STP	⚠ (Обязательно) Используется для включения STP.	
	spanning-tree	Включает протокол STP и настраивает основные Настройки.
	spanning-tree mode	Настраивает режим STP.
Настройка совместимости STP	⚠ (Дополнительно) Используется для совместимости с устройствами конкурентов.	
	spanning-tree compatible enable	Включает режим совместимости порта.
	clear spanning-tree detected-protocols	Выполняет обязательную проверку версий BPDU.
Настройка региона	⚠ (Дополнительно) Используется для настройки региона MSTP.	

MSTP	**spanning-tree mst configuration**	Входит в режим конфигурации MST.
Включение быстрой конвергенции RSTP	⚠ (Дополнительно) Используется для настройки типа соединения порта "точка-точка".	
	spanning-tree link-type	Настраивает тип соединения.
Настройка приоритетов	⚠ (Дополнительно) 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	⚠ (Дополнительно) Используется для настройки стоимости пути для порта или метода расчета стоимости пути по умолчанию.	
	spanning-tree cost	Настраивает стоимость пути к порту.
	spanning-tree pathcost method	Настраивает метод расчета стоимости пути по умолчанию.
Настройка максимального количества переходов пакета BPDU	⚠ (Дополнительно) Используется для настройки максимального количества переходов пакета BPDU.	
	spanning-tree max-hops	Настраивает максимальное количество переходов для пакета BPDU.
Включение функций, связанных с PortFast	⚠ (Дополнительно) Используется для включения функций, связанных с PortFast.	
	spanning-tree portfast	Включает PortFast.
	spanning-tree portfast bpduguard default	Включает защиту BPDU на всех портах.
	spanning-tree bpduguard enabled	Включает защиту BPDU на порту.

	spanning-tree portfast bpdufilter default	Включает фильтр BPDU на всех портах.
	spanning-tree bpdufilter enabled	Включает фильтр BPDU на порту.
Включение функций, связанных с TC	⚠ (Дополнительно) Используется для включения функций, связанных с TC.	
	spanning-tree tc-protection	Включает защиту TC.
	spanning-tree tc-protection tc-guard	Включает защиту TC на всех портах.
	spanning-tree tc-guard	Включает защиту TC на порту.
	spanning-tree ignore tc	Включает фильтр TC на порту.
Включение проверки MAC-адреса источника BPDU	⚠ (Дополнительно) Используется для включения проверки MAC-адреса источника BPDU.	
	bpdu src-mac-check	Включает проверку MAC-адреса источника BPDU на порту.
Настройка функции Auto Edge	⚠ (Дополнительно) Используется для настройки Auto Edge	
	spanning-tree autoedge	Включает функцию Auto Edge на порту. Данная функция включена по умолчанию.
Включение функций, связанных с защитой	⚠ (Дополнительно) Используется для включения функций защиты портов.	
	spanning-tree guard root	Включает защиту корневого каталога на порту.
	spanning-tree loopguard default	Включает защиту от петель на всех портах.
	spanning-tree guard loop	Включает защиту от петель на порту.

	spanning-tree guard none	Отключает функцию защиты на порту.
Включение прозрачной передачи BPDU	⚠ (Дополнительно) Используется для обеспечения прозрачной передачи BPDU	
	bridge-frame forwarding protocol bpdu	Включает прозрачную передачу BPDU.
Включение туннеля BPDU	⚠ (Дополнительно) Используется для включения туннеля BPDU.	
	l2protocol-tunnel stp	Включает туннель BPDU глобально.
	l2protocol-tunnel stp enable	Включает туннель BPDU на порту.
	l2protocol-tunnel stp tunnel-dmac	Настройка прозрачной передачи адреса в туннеле BPDU.

10.4.1 Включение STP

Сценарий

- Включите протокол STP глобально и настройте основные Настройки.
- Настройте режим STP.

Примечания

- STP выключен по умолчанию. После включения STP устройство начинает исполнять протокол STP. Устройство по умолчанию запускает MSTP.
- 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 в том случае, если устройство выбрано в качестве корневого моста связующего дерева. То есть, параметры таймера обычного моста должны использовать значения таймера корневого моста.

Этапы конфигурации

Включение STP

- Обязательно.
- Если не указано иное, включите протокол STP на каждом устройстве.

Настройка режима STP

- Опционально.

- Согласно соответствующим стандартам протокола 802.1, STP, RSTP и MSTP совместимы друг с другом, без какой-либо настройки со стороны администратора. Однако устройства некоторых поставщиков не работают в соответствии со стандартами протокола 802.1, что может привести к несовместимости. Поэтому QTECH предоставляет администратору команду переключения режима STP на более низкую версию, если устройства других производителей несовместимы с устройствами QTECH.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Конфигурирование STP

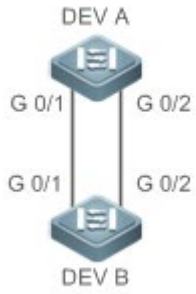
Команда	**spanning-tree** [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **tx-hold-count** *numbers*]
Описание параметра	forward-time *seconds*: Указывает интервал изменения состояния порта. Значение варьируется от 4 до 30 секунд. Значение по умолчанию: 15 секунд. hello-time *seconds:* Указывает интервал, в течение которого устройство отправляет пакет BPDU. Значение варьируется от 1 до 10 секунд. Значение по умолчанию: 2 секунды. max-age *seconds:* Обозначает самый длинный TTL пакета BPDU. Значение варьируется от 6 до 40 секунд. Значение по умолчанию: 20 секунд. tx-hold-count *numbers:* Указывает максимальное количество пакетов BPDU, отправленных в секунду. Диапазон значений от 1 до 10. Значение по умолчанию: 3.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Диапазоны значений времени персылки (forward-time), времени приветствия (hello-time) и времени устаревания (max-age) связаны. При изменении одного из них изменяются два других диапазона. Три значения должны соответствовать следующим условиям: 2 x (Hello Time + 1 секунда) <= Max-Age Time <= 2 x (Forward-Delay Time – 1 секунда) В противном случае топология может стать нестабильной, и конфигурация не будет настроена.

Настройка режима STP

Команда	**spanning-tree mode** [**stp** | **rstp** | **mstp**]
Описание параметра	**stp**: Протокол связующего дерева (IEEE 802.1d) **rstp**: Быстрый протокол связующего дерева (IEEE 802.1w) **mstp**: Множественный протокол связующего дерева (IEEE 802.1s)
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	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, выполните эту команду, чтобы переключить режим STP на более низкую версию.

Пример конфигурации

Включение STP и настройка параметров таймера

Сценарий Изображение 10-20	
Этапы конфигурации	❖ Включите STP и установите режим STP на устройствах. ❖ Настройте параметры таймера корневого моста DEV A следующим образом: Hello Time = 4 сек., Max Age = 25 сек., Forward Delay = 18 сек.

DEV A	Шаг 1: Включите STP и установите режим STP.
	`QTECH#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`QTECH(config)#spanning-tree`
	`QTECH(config)#spanning-tree mode stp`
	Шаг 2: Настройте параметры таймера корневого моста 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. QTECH#configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)#spanning-tree QTECH(config)#spanning-tree mode stp
Проверка конфигурации	❖ Выполните команду **show spanning-tree summary**, чтобы отобразить топологию связующего дерева и параметры конфигурации протокола.
DEV A	QTECH#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 0 Address 00d0.f822.3344 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 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec

```
  Bridge ID  Priority    32768
             Address     001a.a917.78cc
             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)
```

Типичные ошибки

Недоступно

10.4.2 Настройка совместимости STP

Сценарий

- Включите режим совместимости порта, чтобы реализовать связь между устройствами QTECH и устройствами других поставщиков услуг.
- Включите миграцию протоколов для выполнения принудительной проверки версий, чтобы повлиять на совместимость между RSTP и STP.

Примечания

- Если режим совместимости включен на порту, этот порт добавит в BPDU для пересылки другую информацию MSTI на основе текущего порта, чтобы реализовать связь между устройствами QTECH и устройствами других поставщиков услуг.
- При включении совместимости на порту убедитесь в правильности информации об отсеке VLAN для порта. Рекомендуется настроить согласованные списки VLAN для портов на обоих концах канала.

Этапы конфигурации

Включение режима совместимости порта

- Опционально.

Настройка переноса протоколов

- Опционально.
- Если одноранговое устройство поддерживает протокол RSTP, можно принудительно проверить версию на локальном устройстве, чтобы обязать два устройства запустить протокол RSTP.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Включение режима совместимости порта

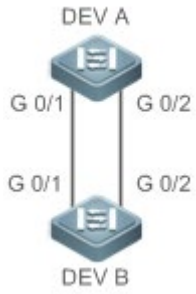
Команда	**spanning-tree compatible enable**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если режим совместимости включен на порту, этот порт добавит в BPDU для пересылки другую информацию MSTI на основе текущего порта, чтобы реализовать связь между устройствами QTECH и устройствами других поставщиков услуг.

Включение миграции протоколов

Команда	**clear spanning-tree detected-protocols** [**interface** *interface-id*]
Описание параметра	**interface** *interface-id*: Указывает порт.
Режим команды	Привилегированный EXEC режим
Встроенная подсказка	Эта команда используется для принудительного выполнения порта для отправки пакетов RSTP BPDU и выполнения принудительной проверки.

Пример конфигурации

Включение совместимости STP

Сценарий Изображение 10-21	
Этапы конфигур	❖ Настройте объекты 1 и 2 на устройствах A и B и сопоставьте объект 1 с VLAN 10 и объект 2 с VLAN 20.

ации	❖ Настройте Gi0/1 и Gi0/2 соответственно для VLAN 10 и VLAN 20 и включите совместимость STP.

DEV A	Шаг 1: Настройте объекты 1 и 2 и сопоставьте объекты 1 и 2 с сетями VLAN 10 и 20 соответственно.
	`QTECH#configure terminal`
	`Enter configuration commands, one per line.  End with 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 совместимость с STP 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 DEV A.
Проверка конфигурации	❖ Запустите команду **show spanning-tree summary**, чтобы проверить правильность расчета топологии связующего дерева.

DEV A	`QTECH#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans mLAG : 1-9, 11-19, 21-4094`
	`  Root ID    Priority    32768`
	`              Address     001a.a917.78cc`
	`              this bridge is root`
	`              Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    32768`
	`              Address     001a.a917.78cc`
	`              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 mLAG : 10 Region Root Priority 32768 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 001a.a917.78cc Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- - Gi0/1 Desg FWD 20000 128 False P2p MST 2 vlans mLAG : 20 Region Root Priority 32768 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 001a.a917.78cc 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 mLAG : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 001a.a917.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768

```
             Address     00d0.f822.3344
             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 mLAG : 10
  Region Root Priority   32768
             Address     001a.a917.78cc
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
-
Gi0/1            Root FWD 20000      128      False    P2p

MST 2 vlans mLAG : 20
  Region Root Priority   32768
             Address     001a.a917.78cc
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
-
Gi0/2            Root FWD 20000      128      False    P2p
```

Типичные ошибки

Недоступно

10.4.3 Настройка региона MSTP

Сценарий

- Настройте регион MSTP, чтобы настроить устройства, принадлежащие одному региону MSTP, и таким образом повлиять на топологию сети.

Примечания

- Чтобы несколько устройств принадлежали к одному региону MSTP, настройте для них одно и то же имя, номер редакции и таблицу привязки VLAN-объекта.
- Можно настроить VLAN для объектов 0 - 64, а остальные VLAN выделятся автоматически на объект 0. Одна VLAN назначается только на один объект.
- После отключения STP рекомендуется настроить таблицу привязки VLAN-объекта. После настройки снова включите MSTP, чтобы обеспечить стабильность и конвергенцию топологии сети.

Этапы конфигурации

Настройка региона MSTP

- Опционально.
- Настройте регион MSTP, если несколько устройств должны принадлежать одному региону MSTP.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Вход в режим конфигурации региона MSTP

Команда	**spanning-tree mst configuration**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы войти в режим конфигурации MST.

Настройка привязки VLAN-объекта

Команда	**instance** *instance-id* **vlan** *vlan-range*
Описание параметра	*instance-id*: Указывает идентификатор MSTI ID в диапазоне от 0 до 64. *vlan-range*: Указывает идентификатор VLAN ID в диапазоне от 1 до 4 094.

Режим команды	Режим конфигурирования MST
Встроенная подсказка	Чтобы добавить группу VLAN в MSTI, выполните эту команду. Например, instance 1 vlan 2-200: Добавляет VLAN 2 - 200 на объект 1. instance 1 vlan 2, 20, 200: Добавляет VLAN 2, 20 и 200 на объект 1. Используйте форму команды с **no** для удаления VLAN из объекта. Удаленные виртуальные локальные сети автоматически пересылаются в объект 0.

Настройка имени версии MST

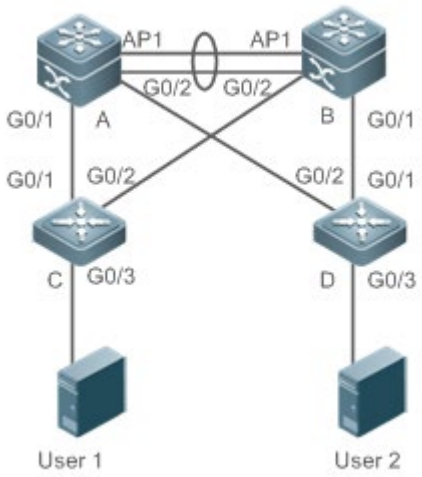
Команда	**name** *name*
Описание параметра	*name*: Указывает имя MST. Имя состоит максимум из 32 байт.
Режим команды	Режим конфигурирования MST
Встроенная подсказка	Недоступно

Настройка номера версии MST

Команда	**revision** *version*
Описание параметра	*version*: Указывает идентификатор ревизии MST в диапазоне от 0 до 65535.
Режим команды	Режим конфигурирования MST
Встроенная подсказка	Недоступно

Пример конфигурации

Включение MSTP для обеспечения балансировки нагрузки VLAN в топологии MSTP+VRRP

Сценарий Изображение 10-22	
Этапы конфигурации	❖ Включите MSTP и создайте объекты 1 и 2 на коммутаторах A, B, C и D. ❖ Настройте коммутатор A в качестве корневого моста объектов 0 и 1, а коммутатор B в качестве корневого моста объекта 2. ❖ Настройте коммутатор A в качестве основного устройства VRRP сетей VLAN 1 и 10 и коммутатор B в качестве мастер устройства VRRP сети VLAN 20.

A	Шаг 1: Настройте VLAN 10 и 20 и настройте порты как магистральные.
	`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 объекты 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 корневого моста объектов 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 действовал в качестве мастер устройства VRRP 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 приоритет VRRP на значение по умолчанию 100, чтобы коммутатор A действовал в качестве резервного устройства VRRP в сети 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. 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 объекты 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 корневого моста объекта 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 приоритет VRRP на значение по умолчанию 120, чтобы коммутатор B действовал в качестве резервного устройства VRRP в сети 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, 20 и настройте порты как магистральные.
	`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 объекты 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 непосредственно 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 конфигурации	❖ Запустите команду **show spanning-tree summary**, чтобы проверить правильность расчета топологии связующего дерева. ❖ 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 mLAG : 1-9, 11-19, 21-4094
  Root ID     Priority    4096
              Address     00d0.f822.3344
              this bridge is root
              Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID   Priority    4096
              Address     00d0.f822.3344
              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 mLAG : 10
  Region Root Priority   4096
              Address     00d0.f822.3344
              this bridge is region root

  Bridge ID   Priority    4096
              Address     00d0.f822.3344

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 mLAG : 20
  Region Root Priority   4096
              Address     001a.a917.78cc
              this bridge is region root
```

	Bridge ID Priority 8192 Address 00d0.f822.3344 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 mLAG : 1-9, 11-19, 21-4094 Root ID Priority 4096 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 8192 Address 001a.a917.78cc 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 mLAG : 10 Region Root Priority 4096 Address 00d0.f822.3344 this bridge is region root Bridge ID Priority 8192 Address 001a.a917.78cc 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 mLAG : 20
  Region Root Priority   4096
              Address     001a.a917.78cc
              this bridge is region root

  Bridge ID  Priority    4096
              Address     001a.a917.78cc

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 mLAG : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
              Address     00d0.f822.3344
              this bridge is root
              Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    32768
              Address     001a.a979.00ea
              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 mLAG : 10
```

	Region Root Priority 4096 Address 00d0.f822.3344 this bridge is region root Bridge ID Priority 32768 Address 001a.a979.00ea 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 mLAG : 20 Region Root Priority 4096 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 001a.a979.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Root FWD 200000 128 P2p False Fa0/1 Altn BLK 200000 128 P2p False
D	Пропущено.

Типичные ошибки

- Конфигурации региона MST не однородны в топологии MSTP.
- Сети VLAN не создаются до настройки сопоставления между объектом и VLAN.
- Устройство исполняет протокол STP или RSTP в топологии MSTP+VRRP, но рассчитывает связующее дерево согласно алгоритмам различных областей MST.

10.4.4 Включение быстрой конвергенции RSTP

Сценарий

- Настройте тип канала, чтобы обеспечить быструю конвергенцию RSTP.

Примечания

- Если тип канала порта является соединением "точка-точка", RSTP может быстро выполнить конвергенцию. Подробнее см. в разделе «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 как "точка-точка". Если порт находится в полудуплексном режиме, устройство устанавливает тип соединения как общедоступный. Можно также принудительно настроить тип канала, чтобы определить, является ли соединение на порту топологией "точка-точка".
- Тип канала порта связан со скоростью и дуплексным режимом. Если порт находится в полудуплексном режиме, тип канала является общедоступным.

Этапы конфигурации

Настройка типа канала.

- Опционально.

Проверка конфигурации

- Отобразите конфигурацию.
- Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* для отображения конфигурации связующего дерева порта.

Связанные команды

Настройка типа канала.

Команда	**spanning-tree link-type** [**point-to-point** | **shared**]
Описание параметра	**point-to-point**: Принудительно настраивает тип канала порта как "точка-точка". **shared**: Принудительно настраивает тип канала порта как общедоступный.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если тип канала порта является соединением "точка-точка", RSTP может быстро выполнить конвергенцию. Если тип соединения не настроен, устройство автоматически устанавливает тип соединения в зависимости от дуплексного режима порта.

Пример конфигурации

Включение быстрой конвергенции RSTP

Этапы конфигураци	❖ Установите тип канала порта как "точка-точка".

и	
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point
Проверка конфигурации	❖ Запустите команду **show spanning-tree summary**, чтобы отобразить тип канала порта.
	QTECH#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans mLAG : ALL Root ID Priority 32768 Address 001a.a917.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 00d0.f822.3344 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

Типичные ошибки

❖ Недоступно

10.4.5 Настройка приоритетов

Сценарий

❖ Настройте приоритет коммутатора, чтобы определить устройство как корневое для всей сети и определить топологию всей сети.
❖ Настройте приоритет порта, чтобы определить, какой порт переходит в состояние пересылки первым.

Примечания

❖ Для обеспечения стабильности всей сети рекомендуется установить более высокий приоритет для устройства уровня ядра (с меньшим значением).

Можно назначить разные приоритеты коммутации для разных объектов, чтобы каждый объект исполнял независимый протокол STP на основе назначенных приоритетов. Устройства в разных регионах используют только приоритет CIST (объект 0). Как описывается в идентификаторе моста, приоритет коммутатора имеет 16 дополнительных значений: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. Они являются алгебраической прогрессией с коэффициентом a=4096. Значение по умолчанию: 32768.

- Если к общедоступному устройству подключены два порта, устройство выбирает порт с более высоким приоритетом (меньшее значение) для входа в состояние пересылки, и порт с более низким приоритетом (большее значение) для входа в состояние отбрасывания пакетов. Если два порта имеют одинаковый приоритет, устройство выбирает порт с меньшим идентификатором порта для входа в состояние пересылки. Можно назначить разные приоритеты портов различным объектам порта, чтобы каждый объект запускал независимый протокол STP на основе назначенных приоритетов.
- Аналогично 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 алгебраической прогрессией с коэффициентом a=16. Значение по умолчанию: 128. Измененный приоритет порта действует только на указанный порт.

Этапы конфигурации

Настройка приоритета коммутатора

- Опционально.
- Чтобы изменить корневое устройство или топологию сети сконфигурируйте приоритет коммутатора.

Настройка приоритета порта

- Опционально.
- Чтобы изменить предпочитаемый порт, входящий в состояние пересылки, настройте приоритет порта.

Проверка конфигурации

- Отобразите конфигурацию.
- Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* для отображения конфигурации связующего дерева порта.

Связанные команды

Настройка приоритета коммутатора

Команда	**spanning-tree** [**mst** *instance-id*] **priority** *priority*
Описание параметра	**mst** *instance-id*: Указывает идентификатор объекта в диапазоне от 0 до 64. **priority** *priority*: Указывает приоритет коммутатора. Существует 16

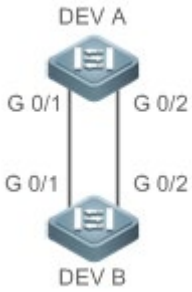
	дополнительных значений: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. Они являются алгебраической прогрессией с коэффициентом a=4096.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Настройте приоритет коммутатора, чтобы определить устройство как корневое для всей сети и определить топологию всей сети.

Настройка приоритета порта

Команда	spanning-tree [**mst** *instance-id*] **port-priority** *priority*
Описание параметра	**mst** *instance-id*: Указывает идентификатор объекта в диапазоне от 0 до 64. **port-priority** *priority*: Указывает приоритет порта. Существует 16 дополнительных значений: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. Они являются алгебраической прогрессией с коэффициентом a=4096.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если в области происходит петля, порт с более высоким приоритетом входит в состояние пересылки. Если два порта имеют одинаковый приоритет, то для входа в состояние пересылки выбирается порт с меньшим идентификатором порта. Выполните эту команду, чтобы определить, какой порт в петле региона переходит в состояние пересылки.

Пример конфигурации

Настройка приоритета порта

Сценарий Изображение 10-23	
Этапы конфигурации	❖ Настройте приоритет моста таким образом, чтобы DEV A стал корневым мостом связующего дерева. ❖ 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 протокол 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 конфигурации	❖ Запустите команду **show spanning-tree summary**, чтобы отобразить результат расчета топологии связующего дерева.

DEV A	`QTECH# QTECH#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans mLAG : ALL`
	`Root ID Priority 0`
	`Address 00d0.f822.3344`
	`this bridge is root`
	`Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec`
	
	`Bridge ID Priority 0`
	`Address 00d0.f822.3344`
	`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 mLAG : ALL Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 001a.a917.78cc 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

Типичные ошибки

Недоступно

10.4.6 Настройка стоимости пути к порту

Сценарий

- Настройте стоимость пути для порта, чтобы определить находится ли порт в состоянии пересылки и топологию всей сети.
- Если стоимость пути порта использует значение по умолчанию, настройте метод расчета стоимости пути, чтобы повлиять на результат расчета.

Примечания

- Устройство выбирает порт в качестве корневого порта, если стоимость пути от этого порта до корневого моста является самой низкой. Поэтому стоимость

пути к порту определяет корневой порт локального устройства. Стоимость пути к порту по умолчанию рассчитывается автоматически на основе скорости порта (скорости передачи данных). Порт с более высокой скоростью будет иметь низкую стоимость пути. Так как этот метод является наиболее научным для расчета стоимости пути, не изменяйте стоимость пути, если это не требуется. Можно назначить разные стоимости путей объектам порта, чтобы каждый объект исполнял независимый протокол STP на основе назначенных затрат на пути.

- Если стоимость пути порта использует значение по умолчанию, устройство автоматически рассчитывает стоимость пути порта на основе скорости порта. Тем не менее, IEEE 802.1d-1998 и IEEE 802.1t определяют разные стоимости пути для одной и той же скорости соединения. Значение представляет собой целое число формата short от 1 до 65535 в 802.1d-1998, и целое число формата long от 1 до 200000000 в IEEE 802.1t. Стоимость пути для агрегированного порта (LAG) состоит из двух решений: 1. Решение QTECH: Стоимость пути порта x 95%;
  2. Решение, рекомендованное в стандартах: 20000000000/фактическую пропускную способность канала агрегированного порта, при которой фактическая пропускная способность канала агрегированного порта = Полоса пропускания (Bandwidth) порта участника x количество активных портов участников. Администратор должен унифицировать метод расчета стоимости пути во всей сети. Стандарт по умолчанию является целое число формата private long.
- В следующей таблице перечислены стоимости путей, автоматически настроенные для разных скоростей каналов связи в двух решениях.

Скорость порта	Порт	IEEE 802.1d (short)	IEEE 802.1t (long)	IEEE 802.1t (стандартный long)
10 Мбит/с	Обычный порт	100	2000000	2000000
	Агрегированный порт	95	1900000	2000000÷linkupcnt
100 Мбит/с	Обычный порт	19	200000	200000
	Агрегированный порт	18	190000	200000÷linkupcnt
1000 Мбит/с	Обычный порт	4	20000	20000
	Агрегированный порт	3	19000	20000÷linkupcnt
10000	Обычный порт	2	2000	2000

Мбит/с	Агрегированный порт	1	1900	20000÷linkupcnt

- По умолчанию используется целое число формата long стандарта QTECH. После изменения решения на стоимость пути, рекомендованную стандартами, стоимость пути агрегированного порта изменяется с номером порта участника в состоянии восходящего канала. При изменении стоимости пути к порту также изменится топология сети.
- Если агрегированный порт - статический, параметр linkupcnt в таблице является количеством действующих портов участников. Если агрегированный порт является портом LACP, параметр linkupcnt в таблице является количеством портов участников, пересылающих данные агрегированного порта. Если в агрегированном порту нет портов участников, и значение поднимается на 1, linkupcnt тоже становится 1. Подробнее об агрегированном порте и LACP см. раздел *Конфигурирование агрегированного порта*. Измененная стоимость пути порта влияет только на порт Rx.

Этапы конфигурации

Настройка стоимости пути порта

- Опционально.
- Чтобы определить, какой порт или пакеты данных пути лучше пропускать, 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.

Проверка конфигурации

- Отобразите конфигурацию.
- Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* для отображения конфигурации связующего дерева порта.

Связанные команды

Настройка стоимости пути порта

Команда	**spanning-tree** [**mst** *instance-id*] **cost** *cost*
Описание параметра	**mst** *instance-id*: Указывает идентификатор объекта в диапазоне от 0 до 64. **cost** *cost*: Указывает весовой коэффициент в диапазоне от 1 до 200000000.
Режим команды	Режим конфигурации интерфейса

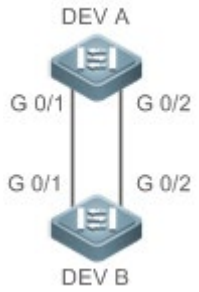
Встроенная подсказка	Более высокое значение параметра *cost* указывает на более высокую стоимость пути.

Настройка метода расчета стоимости пути по умолчанию

Команда	**spanning-tree pathcost method** { *long* [*standard*] | *short* }
Описание параметра	*long*: Использует стоимость пути, указанную в 802.1t. *standard*: Использует стоимость пути, рассчитанную в соответствии со стандартом. *short*: Использует стоимость пути, указанную в 802.1d.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если стоимость пути порта использует значение по умолчанию, устройство автоматически рассчитывает стоимость пути порта на основе скорости порта.

Пример конфигурации

Настройка стоимости пути порта

Сценарий Изображение 10-24	
Этапы конфигурации	❖ Настройте приоритет моста таким образом, чтобы DEV A стал корневым мостом связующего дерева. ❖ Настройте стоимость пути Gi 0/2 на DEV B на 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 конфигурации	❖ Запустите команду **show spanning-tree summary**, чтобы отобразить результат расчета топологии связующего дерева.

DEV A	QTECH# QTECH#show spanning-tree summary
	
	Spanning tree enabled protocol mstp
	MST 0 vlans mLAG : ALL
	  Root ID Priority 0
	  Address 00d0.f822.3344
	  this bridge is root
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	  Bridge ID Priority 0
	  Address 00d0.f822.3344
	  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 mLAG : ALL
	  Root ID Priority 0
	  Address 00d0.f822.3344
	  this bridge is root
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	  Bridge ID Priority 32768
	  Address 001a.a917.78cc
	  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

Типичные ошибки

❖ Недоступно

10.4.7 Настройка максимального количества переходов пакета BPDU

Сценарий

❖ Настройте максимальное количество переходов пакета BPDU, чтобы изменить TTL BPDU и, таким образом, повлиять на топологию сети.

Примечания

❖ По умолчанию максимальное число переходов пакета BPDU составляет 20. Как правило, не рекомендуется изменять значение по умолчанию.

Этапы конфигурации

Настройка максимального количества переходов

❖ (Дополнительно) Если топология сети настолько велика, что пакет BPDU превышает 20 переходов, установленных по умолчанию, рекомендуется изменить максимальное количество переходов.

Проверка конфигурации

❖ Отобразите конфигурацию.

Связанные команды

Настройка максимального количества переходов

Команда	**spanning-tree max-hops** *hop-count*
Описание параметра	*hop-count*: Указывает количество устройств, через которые проходит BPDU, перед тем как данный пакет будет отклонен. Диапазон составляет от 1 до 40.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	В регионе, BPDU, отправленный корневым мостом, включает определенное количество переходов. Каждый раз, когда BPDU проходит через устройство от корневого моста, счетчик переходов уменьшается на 1. Когда счетчик переходов равен 0, время пакета BPDU истекает, и устройство отбрасывает пакет. Эта команда определяет количество устройств, через которые BPDU проходит в регионе, перед тем как их отбрасывать. Изменение

	максимального количества переходов повлияет на все объекты.

Пример конфигурации

Настройка максимального количества переходов пакета BPDU

Этапы конфигурации	❖ Настройте максимальное количество переходов для пакета BPDU на 25.
	`QTECH(config)# spanning-tree max-hops 25`
Проверка конфигурации	❖ Выполните команду **show spanning-tree** для отображения конфигурации.

	`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 mLAG : ALL`
	`BridgeAddr : 00d0.f822.3344`
	`Priority: 0`
	`TimeSinceTopologyChange : 2d:0h:46m:4s`
	`TopologyChanges : 25`
	`DesignatedRoot : 0.001a.a917.78cc`
	`RootCost : 0`
	`RootPort : GigabitEthernet 0/1`
	`CistRegionRoot : 0.001a.a917.78cc`
	`CistPathCost : 20000`

10.4.8 Включение функций, связанных с PortFast

Сценарий

- После включения фунции PortFast, порт напрямую переходит в состояние пересылки. Однако, поскольку рабочее состояние Port Fast становится выключенным из-за получения BPDU, порт может правильно исполнять алгоритм STP и войти в состояние пересылки.
- Если защита BPDU включена, порт переходит в состояние «отключен из-за ошибки» после получения BPDU.
- Если фильтр BPDU включен, порт не отправляет и не получает пакеты BPDU.

Примечания

- Глобальная защита BPDU действует только при включении PortFast на порту.
- Если фильтр BPDU включен глобально, порт с включенным PortFast не отправляет и не получает пакеты BPDU. В этом случае хост, подключаясь непосредственно к порту PortFast, не получает BPDU. Если после получения BPDU порт изменяет свое состояние работы быстрого порта на Disabled (Отключено), фильтр BPDU автоматически становится неисправным.
- Глобальный фильтр BPDU действует только при включении PortFast на порту.

Этапы конфигурации

Включение PortFast

- Опционально.
- Если порт подключается непосредственно к сетевому терминалу, настройте этот порт как PortFast.

Включение функции BPDU Guard

- Опционально.
- Если порты устройств подключаются напрямую к сетевым терминалам, можно включить защиту BPDU на этих портах, чтобы предотвратить атаки BPDU из-за вызванных нарушений в топологии связующего дерева. Порт, включенный с защитой BPDU, переходит в состояние «отключен из-за ошибки» после получения BPDU.
- Если порты устройств подключаются напрямую к сетевым терминалам, можно включить защиту BPDU, чтобы предотвратить образование петель на портах. Обязательным условием является возможность пересылки пакетов BPDU устройством нисходящего канала (например, концентратором).

Включение фильтра BPDU

- Опционально.
- Чтобы предотвратить влияние нестандартных пакетов BPDU на топологию связующего дерева, можно включить фильтр BPDU на порту для фильтрации нестандартных пакетов BPDU.

Проверка конфигурации

- Отобразите конфигурацию.
- Запустите команду **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* для отображения конфигурации связующего дерева порта.

Связанные команды

Настройка PortFast

Команда	**spanning-tree portfast**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	После включения фунции PortFast, порт напрямую переходит в состояние пересылки. Однако, поскольку рабочее состояние Port Fast становится выключенным из-за получения BPDU, порт может правильно исполнять алгоритм STP и войти в состояние пересылки.

Настройка BPDU Guard для всех портов

Команда	**spanning-tree portfast bpduguard default**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если защита BPDU включена, порт переходит в состояние «отключен из-за ошибки» после получения BPDU. Выполните команду **show spanning-tree** для отображения конфигурации.

Настройка BPDU Guard для порта

Команда	**spanning-tree bpduguard enabled**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если защита BPDU включена, порт переходит в состояние «отключен из-за ошибки» после получения BPDU.

Настройка BPDU Filter для всех портов

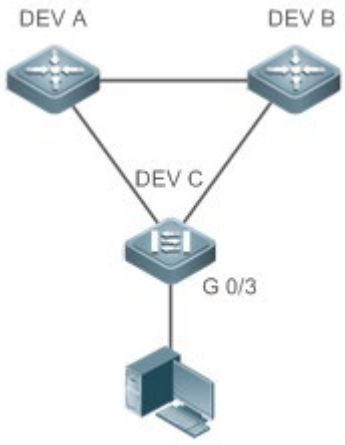
Команда	**spanning-tree portfast bpdufilter default**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если фильтр BPDU включен, порт не отправляет и не получает пакеты BPDU.

Настройка BPDU Filter для порта

Команда	**spanning-tree bpdufilter enabled**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если фильтр BPDU включен, порт не отправляет и не получает пакеты BPDU.

Пример конфигурации

Включение PortFast на порту

Сценарий Изображение 10-25	
Этапы конфигурации	❖ Настройте Gi 0/3 устройства DEV C в качестве порта PortFast и включите защиту BPDU.

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 конфигурации	❖ Выполните команду **show spanning-tree interface** для отображения конфигурации 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 mLAGped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.00d0.f822.3344 PortDesignatedCost : 0 PortDesignatedBridge :0.00d0.f822.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 4 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

10.4.9 Включение функций, связанных с TC

Сценарий

- Если на порту включена защита TC, порт удаляет пакеты TC BPDU в течение заданного времени (обычно 4 секунды) после их получения, предотвращая удаление записей MAC и ARP.
- Если защита TC включена, порт, принимающий пакеты TC, фильтрует пакеты TC или пакеты TC, генерируемые самим портом, чтобы пакеты TC не распространялись на другие порты. Таким образом, для поддержания стабильности сети эффективно предотвращаются возможные атаки TC.
- Фильтр TC не обрабатывает пакеты TC, полученные портами, но обрабатывает пакеты TC в случае нормальных изменений топологии.

Примечания

- TC Guard рекомендуется включать только в том случае, если в сеть поступают нелегальные пакеты TC.

Этапы конфигурации

Включение защиты TC

- Опционально.
- По умолчанию защита TC отключена.

Включение функции TC Guard

- Опционально.
- По умолчанию TC guard отключен.
- Для фильтрации пакетов TC, полученных или созданных в результате изменений топологии, можно включить защиту TC.

Включение фильтра TC

- Опционально.
- По умолчанию фильтр TC отключен.
- Для фильтрации пакетов TC, полученных через порт, можно включить фильтр TC на порту.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Включение защиты TC

Команда	**spanning-tree tc-protection**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации

Встроенная подсказка	Недоступно

Настройка TC Guard для всех портов

Команда	**spanning-tree tc-protection tc-guard**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Включите защиту TC, чтобы предотвратить распространение пакетов TC.

Настройка TC Guard для порта

Команда	**spanning-tree tc-guard**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Включите защиту TC, чтобы предотвратить распространение пакетов TC.

Настройка TC Filter для порта

Команда	**spanning-tree ignore tc**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если фильтр TC включен, порт не обрабатывает полученные пакеты TC.

Пример конфигурации

Включение защиты TC на порту

Этапы конфигурации	❖ Включите защиту TC на порту.
	QTECH(config)#int gi 0/1 QTECH(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard
Проверка конфигурации	❖ Запустите команду **show run interface** для отображения конфигурации защиты TC для 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

Типичные ошибки

❖ Если защита TC или фильтр TC настроены неправильно, во время пересылки пакетов сетевого устройства может произойти ошибка. Например, при изменении топологии устройство не сможет своевременно очистить MAC-адрес, что приведет к ошибкам пересылки пакетов.

10.4.10 Включение проверки MAC-адреса источника BPDU

Сценарий

❖ Включение проверки MAC-адреса источника BPDU. После этого устройство получает только пакеты BPDU с MAC-адресом источника, будучи указанным MAC-адресом, и отбрасывает другие пакеты BPDU.

Примечания

❖ После определения коммутатора, подключенного к порту на канале «точка-точка», можно включить проверку MAC-адреса источника BPDU, чтобы коммутатор получил пакеты BPDU, отправленные только одноранговым коммутатором.

Этапы конфигурации

Включение проверки MAC-адреса источника BPDU

❖ Опционально.
❖ Проверка MAC-адреса источника BPDU отключена по умолчанию.
❖ Чтобы предотвратить атаки BPDU злоумышленниками, можно включить проверку MAC-адреса источника BPDU.

Проверка конфигурации

❖ Отобразите конфигурацию.

Связанные команды

Включение проверки MAC-адреса источника BPDU

Команда	**bpdu src-mac-check** *H.H.H*
Описание параметра	*H.H.H*: Указывает MAC-адрес. Устройство получает только пакеты BPDU с этим адресом в качестве MAC-адреса источника.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Проверка MAC-адреса источника BPDU предотвращает злоумышленные атаки пакетов BPDU и приводит к отклонениям MSTP. После определения коммутатора, подключенного к порту на канале «точка-точка», можно включить проверку MAC-адреса источника BPDU для получения пакетов BPDU, отправленных только одноранговым коммутатором, и отбросить все остальные пакеты BPDU, тем самым предотвращая атаки злоумышленников. Можно включить проверку MAC-адреса источника BPDU в режиме конфигурации интерфейса для определенного порта. Один порт может фильтровать только один MAC-адрес.

Пример конфигурации

Включение проверки MAC-адреса источника BPDU на порту

Этапы конфигурации	❖ Включите проверку MAC-адреса источника BPDU на порту.
	`QTECH(config)#int gi 0/1` `QTECH(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234`
Проверка конфигурации	❖ Запустите команду **show run interface** для отображения конфигурации связующего дерева 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 00d0.f800.1234 spanning-tree link-type point-to-point

Типичные ошибки

- Если проверка MAC-адреса источника BPDU включена на порту, порт принимает только пакеты BPDU с настроенным MAC-адресом источника и отбрасывает все остальные пакеты BPDU.

10.4.11 Настройка Auto Edge

Сценарий

- Включите функцию Auto Edge. Если назначенный порт не получает BPDU в течение указанного времени (3 секунд), он автоматически определяется как граничный порт. Однако, если порт получит пакеты BPDU, его рабочее состояние Port Fast перейдет на «отключен».

Примечания

- Если не указано иное, не отключайте функцию Auto Edge. По умолчанию порт автоматически определяется как граничный порт и переходит в состояние пересылки, если назначенный порт не получает BPDU в течение 3 секунд. Если в сети происходит потеря пакетов или задержка Tx/Rx пакетов, рекомендуется отключить Auto Edge.

Этапы конфигурации

Настройка Auto Edge

- Опционально.
- По умолчанию функция Auto Edge включена.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Настройка Auto Edge

Команда	**spanning-tree autoedge**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная	Если назначенный порт устройства не получает BPDU от порта

подсказка	нисходящего канала в течение определенного периода (3 секунд), устройство рассматривает сетевой хост, подключенный к назначенному порту, настраивает порт как граничный порт и переключает порт непосредственно в состояние пересылки. После получения BPDU граничный порт будет автоматически идентифицирован как неграничный порт. Чтобы отключить функцию Auto Edge, можно запустить команду **spanning-tree autoedge disabled**.

Пример конфигурации

Выключение функции Auto Edge на порту

Этапы конфигурации	❖ Выключите функцию Auto Edge на порту.
	`QTECH(config)#int gi 0/1` `QTECH(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled`
Проверка конфигурации	❖ Запустите команду **show spanning-tree interface** для отображения конфигурации связующего дерева 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 mLAGped :ALL`
	`PortState : forwarding`
	`PortPriority : 128`
	`PortDesignatedRoot : 0.00d0.f822.3344`
	`PortDesignatedCost : 0`

```
PortDesignatedBridge :0.00d0.f822.3344
PortDesignatedPortPriority : 128
PortDesignatedPort : 2
PortForwardTransitions : 6
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : designatedPort
```

Типичные ошибки

Недоступно

10.4.12 Включение функций, связанных с защитой

Сценарий

- Если на порту включена защита от корневого доступа, роли этого порта на всех объектах будут принудительно заданы в качестве назначенного порта. После того как порт получает информацию о конфигурации с более высоким приоритетом, он переходит в состояние, не согласованное с корнем (блокирующее). Если порт не получает информацию о конфигурации с более высоким приоритетом в течение определенного периода времени, он возвращается в исходное состояние.
- Из-за однонаправленного сбоя канала корневой порт или резервный порт становятся назначенным портом и переходят в состояние пересылки, если они не получают BPDU, что приводит к возникновению сетевой петли. Loop guard (защита от петли) предотвращает эту проблему.

Примечания

- Защита от корневого доступа и защита от петель не может быть применена на порту в одно и то же время.

Этапы конфигурации

Включение Root Guard

- Опционально.
- Корневой мост может получить конфигурацию с более высоким приоритетом из-за неправильной настройки обслуживающим персоналом или вредоносных атак в сети. В результате, текущий корневой мост может потерять свою роль, что приведет к неправильным изменениям в топологии сети. Чтобы предотвратить эту проблему, можно включить root guard (защиту от корневого доступа) на указанном порту устройства.

Включение Loop Guard

- Опционально.
- Можно включить функцию защиты от петель на порту (корневом порте, главном порте или агрегированном порте), чтобы предотвратить сбой при получении пакетов BPDU, отправленных назначенным мостом, что повышает

стабильность устройства. В противном случае топология сети изменится, что может привести к образованию петли.

Отключение защиты

- Опционально.
- По умолчанию функция Guard отключена.

Проверка конфигурации

- Отобразите конфигурацию.

Связанные команды

Включение Root Guard

Команда	**spanning-tree guard root**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Если включена защита от корневого доступа, текущий корневой мост не изменится из-за неправильной конфигурации или незаконных атак пакетами.

Включение защиты от петель на всех портах

Команда	**spanning-tree loopguard default**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Включение функции защиты от петель на корневом порте или резервном порте предотвратит возникновение петель, вызванных сбоем при получении BPDU.

Включение защиты от петель на всех портах

Команда	**spanning-tree guard loop**
Описание параметра	Недоступно

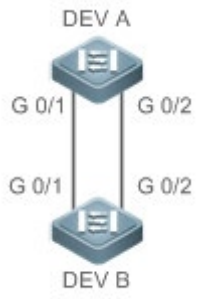
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Включение функции защиты от петель на корневом порте или резервном порте предотвратит возникновение петель, вызванных сбоем при получении BPDU.

Отключение защиты

Команда	**spanning-tree guard none**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Пример конфигурации

Включение защиты от петель на порту

Сценарий Изображение 10-26	
Этапы конфигурации	❖ Настройте DEV A в качестве корневого моста и DEV B в качестве обычного моста на связующем дереве. ❖ Включите защиту от петель 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 конфигурации	❖ Запустите команду **show spanning-tree interface** для отображения конфигурации связующего дерева порта.
DEV A	Пропущено.
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 mLAGped :ALL PortState : forwarding PortPriority : 128 PortDesignatedRoot : 0.001a.a917.78cc PortDesignatedCost : 0 PortDesignatedBridge :0.001a.a917.78cc 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 mLAGped :ALL
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 18
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : alternatePort
```

Типичные ошибки

- Если на корневом порте, главном порте или агрегированном порте включена защита от корневого доступа, возможно, порт заблокирован по ошибке.

10.4.13 Включение прозрачной передачи BPDU

Сценарий

- Если протокол STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы связующее дерево между устройствами было правильно рассчитано.

Примечания

- Прозрачная передача BPDU вступает в силу, только если протокол STP отключен. Если протокол STP включен на устройстве, устройство не передает пакеты BPDU прозрачно.

Этапы конфигурации

Включение прозрачной передачи BPDU

- Опционально.
- Если протокол STP отключен на устройстве, которое должно прозрачно передавать пакеты BPDU, включите прозрачную передачу BPDU.

Проверка конфигурации

❖ Отобразите конфигурацию.

Связанные команды

Включение прозрачной передачи BPDU

Команда	**bridge-frame forwarding protocol bpdu**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	В IEEE 802.1Q в качестве зарезервированного адреса используется MAC-адрес назначения BPDU 01-80-C2-00-00-00. То есть устройства, совместимые с IEEE 802.1Q, не пересылают полученные пакеты BPDU. Однако при фактическом развертывании сети устройствам может потребоваться прозрачная передача пакетов BPDU. Например, если протокол STP отключен на устройстве, устройство должно прозрачно передавать пакеты BPDU, чтобы связующее дерево было правильно рассчитано. Прозрачная передача BPDU вступает в силу, только если протокол STP отключен. Если протокол STP включен на устройстве, устройство не передает пакеты BPDU прозрачно.

Пример конфигурации

Включение прозрачной передачи BPDU

Сценарий Изображение 10-27	
	❖ STP включен на DEV A и DEV C, и отключен на DEV B.
Этапы конфигурации	❖ 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 конфигур	❖ Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача BPDU.

ации	
DEV B	QTECH#show run Building configuration... Current configuration : 694 bytes bridge-frame forwarding protocol bpdu

10.4.14 Включение туннеля BPDU

Сценарий

- Включите туннель BPDU, чтобы пакеты STP из сети заказчика могли быть прозрачно переданы по сети поставщика услуг. Передача пакетов STP между сетью заказчика не влияет на сеть поставщика услуг, в результате чего протокол STP в сети заказчика рассчитывается независимо от сети поставщика услуг.

Примечания

- Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса.

Этапы конфигурации

Включение туннеля BPDU

- (Дополнительно) В сети QinQ можно включить туннель BPDU, если необходимо отдельно рассчитать STP между сетью заказчика и сетью поставщика услуг.

Проверка конфигурации

- Запустите команду **show l2protocol-tunnel stp**, чтобы отобразить конфигурацию туннеля BPDU.

Связанные команды

Настройка туннеля BPDU в режиме глобальной конфигурации

Команда	**l2protocol-tunnel stp**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	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 интерфейса конфигурации

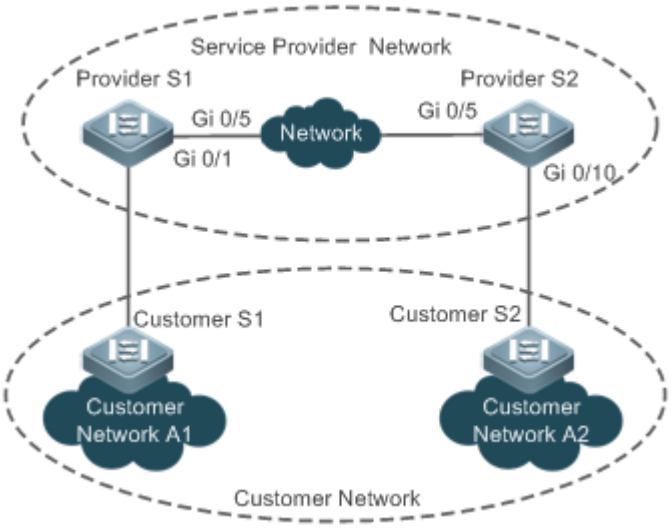
Команда	**l2protocol-tunnel stp enable**
Описание параметра	Недоступно
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Туннель BPDU действует только в том случае, если он включен как в режиме глобальной конфигурации, так и в режиме конфигурации интерфейса.

Настройка адреса прозрачной передачи для туннеля BPDU

Команда	**l2protocol-tunnel stp tunnel-dmac** *mac-address*
Описание параметра	*mac-address*: Указывает адрес STP для прозрачной передачи.
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Если пакет STP, отправленный из сети заказчика, входит в PE, PE изменяет MAC-адрес назначения пакета на частный адрес до того, как пакет будет передан сетью поставщика услуг. Когда пакет достигает PE на стороне однорангового узла, PE изменяет MAC-адрес назначения на публичный адрес и возвращает пакет в сеть заказчика на стороне однорангового узла, реализуя прозрачную передачу по сети поставщика услуг. Этот частный 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, туннель BPDU использует адрес по умолчанию 01d0.f800.0005.

Пример конфигурации

Включение туннеля BPDU

Сценарий Изображение 10-28	
Этапы конфигурации	❖ Включите Basic QinQ на PE (в данном примере Provider S1/Provider S2), чтобы пакеты данных сети заказчика передавались в пределах указанной VLAN в сети поставщика услуг. ❖ Включите прозрачную передачу STP на PE (в данном примере Provider S1/Provider S2), чтобы сеть поставщика услуг могла передавать пакеты STP сети заказчика через туннель BPDU.

Поставщик S1	Шаг 1: Создайте VLAN 200 в сети поставщика услуг.
	`QTECH#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`QTECH(config)#vlan 200`
	`QTECH(config-vlan)#exit`
	Шаг 2: Включите Basic QinQ на порту, подключенном к сети заказчика, 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 заказчика.
	`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: Настройка порта восходящего потока. QTECH(config)# interface gigabitEthernet 0/5 QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink
Поставщик S2	Настройте поставщика S2, выполнив те же действия.
Проверка конфигурации	❖ Проверьте правильность конфигурации туннеля BPDU. ❖ Подтвердите конфигурацию туннельного порта, проверив: 1. Тип порта: dot1q-tunnel; 2. Внешняя VLAN-метка соответствует VLAN, описанной на языке C++ (нативной VLAN) и добавляется в список VLAN туннельного порта; 3. Порт, через который осуществляется доступ к сети поставщика услуг, настраивается как порт восходящего канала.
Поставщик 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
Поставщик S2	Проверьте конфигурацию поставщика S2, выполнив те же действия.

Типичные ошибки

❖ В сети поставщика услуг пакеты BPDU могут быть корректно прозрачно переданы только в том случае, если адреса прозрачной передачи туннеля BPDU согласованы.

10.5 Мониторинг

Очистка

⚠ Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	Команда
Удаляет статистику отправленных и полученных пакетов на порту.	**clear spanning-tree counters** [**interface** *interface-id*]
Очищает информацию об изменении топологии STP.	**clear spanning-tree mst** *instance-id* **topochange record**

Отображение

Описание	Команда
Отображает параметры MSTP и информацию о топологии связующего дерева.	**show spanning-tree**
Отображает количество отправленных и полученных пакетов MSTP.	**show spanning-tree counters** [**interface** *interface-id*]
Отображает объекты MSTP и соответствующее состояние пересылки на порту.	**show spanning-tree summary**
Отображает порты, заблокированные root guard (защитой от корневого доступа) или loop guard (защитой от петель).	**show spanning-tree inconsistentports**
Отображает конфигурацию региона MST.	**show spanning-tree mst configuration**
Отображает информацию объекта MSTP.	**show spanning-tree mst** *instance-id*
Отображает информацию объекта MSTP, соответствующую порту.	**show spanning-tree mst** *instance-id* **interface** *interface-id*
Отображает изменения топологии порта в объекте.	**show spanning-tree mst** *instance-id* **topochange record**

Отображает информацию MSTP всех объектов, соответствующую порту.	**show spanning-tree interface** *interface-id*
Отображает время пересылки.	**show spanning-tree forward-time**
Отображает время приветствия.	**show spanning-tree hello time**
Отображает максимальное количество переходов.	**show spanning-tree max-hops**
Отображает максимальное количество пакетов BPDU, отправленных в секунду.	**show spanning-tree tx-hold-count**
Отображает метод расчета стоимости пути.	**show spanning-tree pathcost method**
Отображает информацию туннеля BPDU.	**show l2protocol-tunnel stp**

Отладка

⚠ Системные ресурсы заняты при выводе отладочной информации. Поэтому, отключите отладочный коммутатор сразу после использования.

Описание	**Команда**
Отладка всех STP.	**debug mstp all**
Отладка порогового сброса MSTP (GR).	**debug mstp gr**
Отладка приема пакетов BPDU.	**debug mstp rx**
Отладка отправки пакетов BPDU.	**debug mstp tx**
Отладка событий MSTP.	**debug mstp event**
Отладка защиты от петель.	**debug mstp loopguard**
Отладка защиты от корневого доступа.	**debug mstp rootguard**
Отладка машины состояния обнаружения моста.	**debug mstp bridgedetect**

Отладка машины состояния информации порта.	**debug mstp portinfo**
Отладка машины состояния миграции протокола порта.	**debug mstp protomigrat**
Отладка изменений топологии MSTP.	**debug mstp topochange**
Отладка машины состояния приема MSTP.	**debug mstp receive**
Отладка машины состояния перехода роли порта.	**debug mstp roletran**
Отладка машины перехода состояния порта.	**debug mstp statetran**
Отладка машины состояния передачи MSTP.	**debug mstp transmit**

11 КОНФИГУРИРОВАНИЕ GVRP

11.1 Обзор

Протокол GARP VLAN Registration Protocol (GVRP) — это приложение общего протокола регистрации **параметров** (GARP), используемое для динамической настройки и распространения членства в VLAN.

Протокол GVRP упрощает настройку и управление VLAN. Это позволяет снизить рабочую нагрузку при ручной настройке сетей VLAN и добавлении портов в сети VLAN, а также снижает вероятность отключения сети из-за несогласованных настроек. С помощью протокола GVRP можно динамически обслуживать сети VLAN и добавлять/удалять порты в сети VLAN и из нее, чтобы обеспечить подключение VLAN в топологии сети.

Протоколы и стандарты

Стандарт IEEE 802.1D

Стандарт IEEE 802.1Q

11.2 Применение

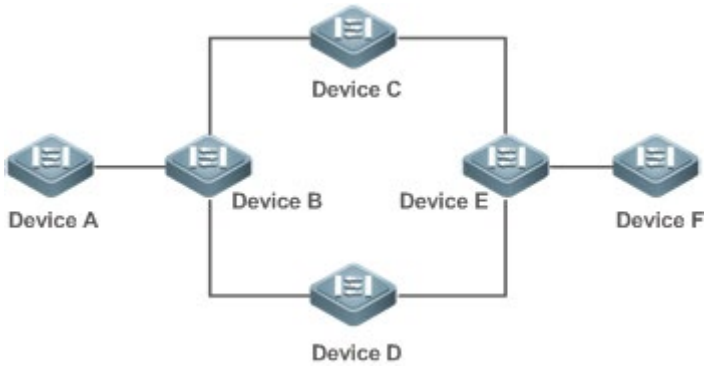
Применение	Описание
Конфигурация GVRP в локальной сети	Подключите два коммутатора в локальной сети (LAN) и выполните синхронизацию VLAN.
Туннельное приложение GVRP PDU	Используйте функцию туннеля GVRP Protocol Data Units (PDU) для прозрачной передачи пакетов GVRP через туннель в сетевой среде QinQ.

11.2.1 Конфигурация GVRP в локальной сети

Сценарий

Включите GVRP и установите режим регистрации GVRP на значение Normal (Нормальный), чтобы зарегистрировать и отменить регистрацию всех динамических и статических VLAN между устройством A и устройством F.

Изображение 11-1



Заметки	Устройство A, устройство B, устройство C, устройство D, устройство E и устройство F являются коммутаторами. Порты, подключенные между двумя устройствами, являются магистральными портами. На устройстве A и устройстве F настройте статические сети VLAN, используемые для связи. Включите GVRP на всех коммутаторах.

Описание

- ❖ На каждом устройстве включите GVRP и функции динамического создания VLAN, а также убедитесь, что динамические VLAN могут быть созданы на промежуточных устройствах.
- ❖ На устройстве A и устройстве F настройте статические сети VLAN, используемые для связи. Устройство B, устройство C, устройство D и устройство E будут динамически изучать сети VLAN с помощью протокола GVRP.

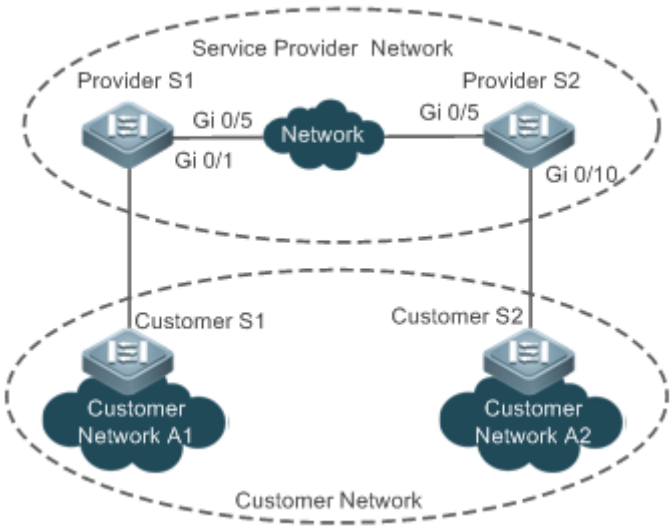
⚠ Рекомендуется включить протокол связующего дерева (STP), чтобы избежать образования петель в топологии сети заказчика.

11.2.2 Туннельное приложение GVRP PDU

Сценарий

Сетевая среда QinQ обычно разделена на сеть заказчика и сеть поставщика услуг (SP). Функция GVRP PDU Tunnel позволяет передавать пакеты GVRP между сетями клиентов без воздействия на сети SP. Расчет GVRP в сетях клиентов отделен от расчета в сетях SP без помех.

Изображение 11-2 Топология применения функции GVRP PDU Tunnel



Заметки	Изображение 11-2 Показывает сеть поставщика услуг и сеть заказчика. В сети поставщика услуг содержатся периферийные устройства поставщика (PE), провайдер S1 и провайдер S2. Сеть заказчика A1 и сеть заказчика A2

	являются двумя объектами пользователя в разных регионах. Клиент S1 и клиент S2 — это устройства доступа в сети заказчика, которые подключены к сети поставщика услуг через провайдера S1 и провайдер S2 соответственно. Функция GVRP PDU Tunnel позволяет сети заказчика A1 и сети заказчика A2 выполнять унифицированный расчет GVRP по сети поставщика услуг, не влияя на расчет GVRP сети поставщика услуг.

Описание

- Включите Basic QinQ на PE (провайдер S1 и провайдер S2) в сети SP для передачи пакетов данных из сети заказчика через указанную VLAN в сети SP.
- Включите прозрачную передачу GVRP на PE (провайдер S1 и провайдер S2) в сети SP, чтобы позволить сети SP туннелировать пакеты GVRP от сети заказчика через туннель GVRP PDU.

11.3 Функции

Базовые концепции

GVRP

GVRP — это приложение GARP, используемое для регистрации и отмены регистрации **параметров** VLAN в следующих режимах:

- Когда порт получает объявление атрибута VLAN, порт регистрирует Настройки VLAN, содержащиеся в объявлении (то есть порт присоединится к VLAN).
- Когда порт получает объявление об аннулировании **параметров** VLAN, порт отменяет регистрацию **параметров** VLAN, содержащихся в объявлении (то есть порт выходит из VLAN).
- Изображение 11-3

Динамическая VLAN

VLAN, которая может быть динамически создана и удалена без необходимости ручной настройки, называется динамической VLAN.

Можно вручную преобразовать динамическую VLAN в статическую, однако обратное преобразование невозможно.

Процесс состояния протокола управляет соединением портов с динамическими сетями VLAN, созданными с помощью протокола GVRP. К этим VLAN могут присоединиться только магистральные порты, которые получают объявление атрибута GVRP VLAN. Невозможно вручную добавить порты в динамические VLAN.

Типы сообщений

(1) Сообщения Join

Когда объект приложения GARP рассчитывает, что другие объекты GARP зарегистрировали свои Настройки, он отправит сообщение Join (Присоединиться). Когда объект GARP получает сообщение о подключении от другого объекта или требует, чтобы другие объекты зарегистрировали его статические Настройки, он отправит сообщение Join. Существует два типа сообщения Join: JoinEmpty и JoinIn.

- Сообщение JoinEmpty: Используется для объявления незарегистрированного атрибута
- Сообщение JoinIn: Используется для объявления зарегистрированного атрибута

(2) Сообщение Leave

Когда объект приложения GARP рассчитывает, что другие объекты GARP отменили регистрацию своих **параметров**, он отправит сообщение Leave (Отсоединиться). Когда объект GARP получает сообщение об отсоединении от другого объекта или требует, чтобы другие объекты зарегистрировали его статические Настройки, он отправит сообщение Leave. Существует два типа сообщения Leave: 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 начинает отсчет таймера LeaveAll во время запуска. По истечении времени таймера объект отправляет сообщение LeaveAll для отмены регистрации всех **параметров**, чтобы другие объекты GARP могли повторно зарегистрировать Настройки. Когда объект приложения GARP получает сообщение LeaveAll от другого объекта, он также отправляет сообщение LeaveAll. Таймер LeaveAll перезапускается при повторной отправке сообщения LeaveAll для запуска нового цикла.

Типы таймеров

GARP определяет четыре таймера, используемых для управления отправкой сообщения GARP.

(1) Таймер Hold

Таймер Hold (Удерживание) управляет отправкой сообщений GARP (включая сообщения Join и Leave). Если Настройки объекта приложения GARP изменены или получают сообщение GARP от другого объекта, запускается таймер удерживания. В течение периода тайм-аута объект приложения GARP инкапсулирует все сообщения GARP, которые должны быть отправлены с минимальным количеством пакетов, и отправляет пакеты по истечении времени таймера. Это сокращает количество отправленных пакетов и экономит ресурсы полосы пропускания.

(2) Таймер Join

Таймер Join управляет отправкой сообщений Join. После того, как объект приложения GARP отправит сообщение Join, он ожидает окончания одного интервала времени ожидания таймера Join, чтобы сообщение Join было надежно передано другому объекту. Если объект приложения GARP получает сообщение JoinIn от другого объекта до истечения времени таймера, то 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 контролирует отмену регистрации атрибута. Когда объект приложения GARP вычисляет, что другие объекты отменяют регистрацию одного из их параметров, он отправляет сообщение Leave. Другие объекты, которые получают сообщение Leave, запускают свой таймер Leave. Регистрация атрибута будет отменена только в том случае, если эти объекты не получат сообщение Join, сопоставленное с атрибутом в течение периода тайм-аута.

(4) Таймер LeaveAll

Каждый объект приложения GARP начинает отсчет собственного таймера LeaveAll при запуске. По истечении времени таймера объект отправляет сообщение LeaveAll, чтобы другие объекты могли повторно зарегистрировать Настройки. Затем таймер LeaveAll перезапускается, чтобы начать отсчет нового цикла.

Режимы объявлений GVRP

Протокол GVRP позволяет коммутатору сообщать другим взаимосвязанным устройствам о своих сетях VLAN, а одноранговому устройству — создавать определенные сети VLAN и добавлять порты, которые передают пакеты GVRP в соответствующие сети VLAN.

Доступны два режима объявлений GVRP:

- Нормальный режим: Внешнее устройство объявляет информацию о своей VLAN, включая динамические и статические VLAN.
- Режим «без заявки»: Устройство не сообщает информацию во внешнюю среду о своей VLAN.

Режимы регистрации GVRP

Режим регистрации GVRP определяет, обрабатывает ли коммутатор, получающий пакет GVRP, информацию VLAN в пакете, например, динамически создает новую VLAN и добавляет порт, который получает пакет в VLAN.

Доступны два режима регистрации GVRP:

- Нормальный режим: Обработка информации VLAN в полученном пакете GVRP.
- Режим «отключен»: Говорит о том, что информация VLAN, в полученном пакете GVRP не обрабатывается.

Обзор

Функция	Описание
Синхронизация информации VLAN внутри топологии	Динамически создает VLAN и добавляет/удаляет порты в/из VLAN, что снижает рабочую нагрузку во время ручной настройки и вероятность отключения VLAN из-за отсутствия конфигурации.

11.3.1 Синхронизация информации VLAN внутри топологии

Принцип работы

- GVRP – это приложение GARP, основанное на рабочем механизме GARP. GVRP поддерживает информацию динамической регистрации сетей VLAN на устройстве и распространяет информацию на другие устройства. Устройство с поддержкой протокола GVRP получает информацию о регистрации VLAN от других устройств и динамически обновляет информацию о регистрации локальной сети VLAN. Устройство также передает информацию о регистрации локальной сети VLAN другим устройствам, чтобы все устройства в локальной сети сохранили согласованную информацию о своей сети VLAN. Информация о регистрации VLAN, распространяемая GVRP, включает в себя настроенную вручную информацию о статической регистрации на локальном устройстве и информацию о динамической регистрации с других устройств.

Объявление внешней информации VLAN

Магистральный порт на устройстве с поддержкой GVRP периодически собирает информацию о VLAN в пределах порта, включая VLAN, к которым подключается или выходит магистральный порт. Собранная информация VLAN инкапсулируется в пакет GVRP, который будет отправлен на одноранговое устройство. После того как порт внешней линии на одноранговом устройстве получает пакет, он разрешает информацию VLAN. Затем будут динамически созданы соответствующие VLAN, и магистральный порт присоединится к созданным VLAN или выйдет из других VLAN. Подробнее о VLAN см. в описании типов сообщений GVRP выше.

Связанные конфигурации

- GVRP выключен по умолчанию.
- Запустите [no] gvrp enable, чтобы включить или отключить GVRP.
- После включения протокола GVRP на устройстве коммутатор отправляет пакеты GVRP с информацией о VLAN. Если протокол GVRP отключен на устройстве, коммутатор не отправляет пакеты GVRP с информацией о VLAN или 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. Подробнее см. в описании режимов регистрации GVRP выше.

Связанные конфигурации

- Если протокол GVRP включен, порт в режиме магистрального канала по умолчанию включен 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 включена динамическая регистрация VLAN, то на локальном устройстве будут созданы динамические VLAN, когда порт получит пакет GVRP, передающий информацию VLAN от одноранговой узла.
- Если динамическая регистрация VLAN отключена, то при получении портом пакета GVRP от одноранговой узла динамическая VLAN на локальном устройстве не создается.

Конфигурация	Описание и команда	
Настройка основных функций GVRP и синхронизации информации VLAN	(Обязательно) Используется для включения GVRP и динамического создания VLAN.	
	gvrp enable	Включает GVRP.
	gvrp dynamic-vlan-creation enable	Включает создание динамических VLAN.
	switchport mode trunk	Переключает в режим магистрального порта. GVRP вступает в силу только в магистральном режиме.
	switchport trunk allowed vlan all	Позволяет пропускать трафик из всех сетей VLAN.
	gvrp LAGplicant state	Настраивает режим объявления порта. Нормальный режим указывает на то, что информация VLAN объявляется во внешнюю среду, отправив пакет GVRP. Режим «без заявки» указывает на то, что не следует объявлять информацию о VLAN во внешнюю среду.
	gvrp registration mode	Настраивает режим регистрации порта. Нормальный режим указывает на обработку информации VLAN в полученном пакете GVRP, например, динамическое создание сетей

		VLAN и добавление портов в сети VLAN. Режим Disabled («отключен») указывает, что не нужно обрабатывать информацию VLAN в полученном пакете GVRP.
	(Дополнительно) он используется для настройки таймеров, режима регистрации и режима объявлений порта.	
	gvrp timer	Настраивает таймеры.
Настройка прозрачной передачи данных PDU GVRP	(Дополнительно) Используется для настройки прозрачной передачи данных GVRP PDU.	
	bridge-frame forwarding protocol gvrp	Обеспечивает прозрачную передачу данных PDU GVRP.
Настройка функции туннеля GVRP PDU	(Дополнительно) Используется для настройки функции туннеля GVRP PDU.	
	l2protocol-tunnel gvrp	Включает функцию туннеля GVRP PDU в режиме глобальной конфигурации.
	l2protocol-tunnel gvrp enable	Включает функцию туннеля GVRP PDU в режиме конфигурации интерфейса.
	l2protocol-tunnel gvrp tunnel-dmac	Настраивает адрес для прозрачной передачи, используемый функцией туннеля GVRP PDU.

11.3.2 Настройка основных функций GVRP и синхронизации информации VLAN

Сценарий

- Динамически создает/удаляет сети VLAN и добавляет/удаляет порты в/из сетей VLAN.
- Синхронизирует данные VLAN между устройствами, чтобы обеспечить нормальную связь между топологий.
- Уменьшает рабочую нагрузку во время ручной настройки и упрощает управление сетями VLAN.

Примечания

- Протокол 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 изучаемую сеть VLAN и настроенные вручную сети VLAN.

- Если протокол STP включен, в GVRP (например, при получении и отправке PDU GVRP) участвуют только порты в состоянии пересылки, а информация о VLAN передается в GVRP.
- Все порты VLAN, добавленные GVRP, являются тегированными портами.
- Система не сохраняет информацию VLAN, которая динамически определяется GVRP. Информация будет утеряна при сбросе устройства и не может быть сохранена вручную.
- Все устройства, которым требуется обмен информацией о GVRP, должны поддерживать согласованные таймеры GVRP (таймер Join, таймер Leave и таймер Leaveall).
- Если протокол STP не включен, все доступные порты могут участвовать в GVRP. Если включено единое связующее дерево (SST), в GVRP участвуют только порты в состоянии пересылки в контексте SST. Если включено множественное связующее дерево (MST), GVRP может запускаться в контексте связующего дерева, к которому принадлежит VLAN1. Нельзя указать другой контекст связующего дерева для GVRP.

Этапы конфигурации

Включение GVRP

- Обязательно.
- Только устройства с поддержкой GVRP могут обрабатывать пакеты GVRP.

Включение динамического создания VLAN

- Обязательно.
- После включения динамического создания VLAN на устройстве коммутатор будет динамически создавать VLAN при получении сообщений Join в GVRP.

Настройка таймеров

- Опционально.
- Существует три таймера GVRP: Таймер Join, таймер Leave и таймер Leaveall, которые используются для управления интервалами отправки сообщений.
- Существуют следующие взаимосвязи интервалов таймера: Интервал таймера Leave должен быть в три или более раза больше, чем таймера Join; интервал таймера Leaveall должен быть больше, чем таймера Leave.
- Управление тремя таймерами осуществляется машиной состояния GVRP и может быть взаимно запущено.

Настройка режима объявления порта

- Опционально.
- Доступны два режима объявлений GVRP: Нормальный (по умолчанию) и «без заявки».
- Нормальный режим: Указывает, что устройство объявляет информацию во внешнюю среду о своей VLAN.
- Режим «без заявки»: Указывает, что устройство не объявляет информацию во внешнюю среду о своей VLAN.

Настройка режима регистрации порта

- Опционально.
- Доступны два режима регистрации GVRP: Нормальный и «отключен».

Переключение в режим магистрального порта

- Обязательно.
- Протокол GVRP действует только на порты в магистральном режиме.

Проверка конфигурации

- Выполните команду **show gvrp configuration**, чтобы проверить конфигурацию.
- Проверьте, настроена ли динамическая VLAN, и соответствующий порт, который присоединяется к VLAN.

Связанные команды

Включение GVRP

Команда	**gvrp enable**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Протокол GVRP может быть включен только в режиме глобальной конфигурации. Если протокол GVRP не включен глобально, можно задать другие параметры GVRP, но настройки параметров вступят в силу только при запуске протокола GVRP.

Включение динамического создания VLAN

Команда	**gvrp dynamic-vlan-creation enable**
Описание параметра	Недоступно
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Когда порт получает сообщение JoinIn или JoinEmpty, которое указывает на несуществующую VLAN на локальном устройстве, GVRP может создать эту VLAN в зависимости от конфигурации этой команды.

Параметры динамической VLAN, созданной с помощью GVRP, невозможно изменить вручную.

Настройка таймеров

Команда	**gvrp timer** { **join** *timer-value* | **leave** *timer-value* | **leaveall** *timer-value* }
Описание параметра	*timer-value* : 1–2147483647 мс
Режим команды	Режим глобальной конфигурации
Встроенная подсказка	Интервал таймера Leave должен быть в три или более раза больше интервала таймера Join. Интервал таймера Leaveall должен быть больше, чем таймера Leave. Единица измерения времени является миллисекунды. В реальной сетевой ситуации рекомендуются следующие интервалы таймера: Таймер Join: 6000 мс (6 сек.) Таймер Leave: 30000 мс (30 сек.) Таймер Leaveall: 120000 мс (2 мин.) Убедитесь, что настройки таймера GVRP на всех подключенных устройствах GVRP согласованы; в противном случае GVRP может работать неправильно.

Настройка режима объявления порта

Команда	**gvrp LAGplicant state** { **normal** | **non-LAGplicant** }
Описание параметра	**normal:** Указывает, что устройство объявляет информацию во внешнюю среду о VLAN. **non-LAGplicant:** Указывает, что устройство не объявляет информацию во внешнюю среду о VLAN.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Эта команда используется для настройки режима объявлений порта GVRP.

Настройка режима регистрации порта

Команда	**gvrp registration mode** { **normal** | **disabled** }

Описание параметра	**normal:** Указывает, что порт может присоединиться к динамической VLAN. **disabled:** Указывает на то, что порту запрещено присоединяться к динамической VLAN.
Режим команды	Режим конфигурации интерфейса
Встроенная подсказка	Эта команда используется для настройки режима регистрации порта GVRP.

Пример конфигурации

Включение протокола GVRP в топологии и динамическое обслуживание сетей VLAN и взаимосвязь портов VLAN.

Сценарий Изображение 11-4	
Этапы конфигурации	❖ На коммутаторах A и C настройте сети VLAN, используемые для связи в сети заказчика. ❖ Включите функции GVRP и динамическое создание VLAN на коммутаторах A, B и C. ❖ Настройте порты, подключенные между коммутаторами, как магистральные порты, и убедитесь, что списки VLAN магистральных портов включают в себя сети связи VLAN. По умолчанию магистральный порт позволяет пропускать трафик из всех сетей VLAN. ❖ Рекомендуется включить протокол STP, чтобы избежать петель.

A	1. Создайте VLAN 1–200, используемую для связи в сети заказчика.
	`A# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`A(config)# vlan range 1-200`
	2. Включите функции GVRP и динамическое создание 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 позволяет пропускать 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 порта магистральной линии. Стандартный режим используется по умолчанию и не требует настройки вручную. A(config-if-GigabitEthernet 0/1)# gvrp LAGplicant state normal A(config-if-GigabitEthernet 0/1)# gvrp registration mode normal A(config-if-GigabitEthernet 0/1)# end
C	❖ Конфигурация коммутатора C аналогична конфигурации коммутатора A.
B	1. Включите функции GVRP и динамическое создание VLAN. B# configure terminal B(config)# gvrp enable B(config)# gvrp dynamic-vlan-creation enable 2. Настройте порты, подключенные к коммутаторам A и C, как магистральные порты. B(config)# interface range GigabitEthernet 0/2-3 B(config-if-GigabitEthernet 0/2)# switchport mode trunk
Проверка конфигурации	❖ Проверьте правильность конфигурации GVRP на каждом устройстве. Проверьте, динамически ли создаются VLAN 2–100 на коммутаторе B и присоединяются ли порты G 0/2 и G 0/3 на коммутаторе B.
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 LAGplicant 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 LAGplicant 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 LAGplicant Status Registration Mode ---------- ---------- ---------- GigabitEthernet 0/1 normal normal

Типичные ошибки

- Порты, подключенные между устройствами, не находятся в режиме магистральных линий.
- Списки VLAN портов, подключенных между устройствами, не включают VLAN, используемые для связи в сети заказчика.
- Режимы объявления и регистрации магистральных портов GVRP не установлены в режим «нормально».

11.3.3 Включение прозрачной передачи данных PDU GVRP

Сценарий

Разрешает устройствам прозрачно передавать кадры PDU GVRP для выполнения обычного расчета GVRP между устройствами, когда протокол GVRP не включен.

Примечания

Прозрачная передача GVRP PDU действует только при отключенной GVRP. После включения протокола GVRP устройства не будут прозрачно передавать кадры PDU GVRP.

Этапы конфигурации

Настройка прозрачной передачи данных PDU GVRP

- Опционально.
- Выполните эту настройку, если необходимо разрешить устройствам прозрачно передавать кадры PDU GVRP при отключенной GVRP.

Проверка конфигурации

Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача GVRP.

Связанные команды

Настройка прозрачной передачи данных PDU GVRP

Команда	**bridge-frame forwarding protocol gvrp**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	В стандарте IEEE 802.1Q зарезервирован MAC-адрес назначения 01-80-C2-00-00-06 для PDU GVRP. Устройства, совместимые с IEEE 802.1Q, не пересылают полученные кадры PDU GVRP. Однако при фактическом развертывании сети устройствам может потребоваться прозрачная передача кадров PDU GVRP для выполнения обычного расчета GVRP между устройствами, когда протокол GVRP не включен. Прозрачная передача GVRP PDU действует только при отключенной GVRP. После включения протокола GVRP устройства не будут прозрачно передавать кадры PDU GVRP.

Пример конфигурации

Настройка прозрачной передачи данных PDU GVRP

Сценарий Изображение 11-5	

	Включите GVRP на DEV A и DEV C (DEV B не включается с GVRP).
Этапы конфигурации	Настройте прозрачную передачу GVRP PDU на DEV B для выполнения нормального расчета GVRP между DEV A и DEV C.
DEV B	`QTECH(config)#bridge-frame forwarding protocol gvrp`
Проверка конфигурации	Запустите команду **show run**, чтобы проверить, включена ли прозрачная передача GVRP.

DEV B	`QTECH#show run`
	
	`Building configuration...`
	`Current configuration : 694 bytes`
	`bridge-frame forwarding protocol gvrp`

11.3.4 Настройка функции туннеля GVRP PDU

Сценарий

Прозрачная передача пакетов GVRP между сетями клиентов через туннели в сетях SP возможна без воздействия на сети SP и, таким образом, отделяет расчет GVRP в сетях заказчиков от расчета в сетях SP.

Примечания

Функция туннелирования GVRP PDU действует после включения в режиме глобальной конфигурации и режиме конфигурации интерфейса.

Этапы конфигурации

Настройка функции туннеля GVRP PDU

- (Дополнительно) Выполните эту настройку, если необходимо разделить расчет GVRP между сетями заказчика и сетями поставщика услуг в среде QinQ.

Проверка конфигурации

Запустите команду **show l2protocol-tunnel gvrp**, чтобы проверить конфигурацию туннеля GVRP PDU.

Связанные команды

Включение функции туннеля GVRP PDU в режиме глобальной конфигурации

Команда	**l2protocol-tunnel gvrp**

Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Функция туннелирования GVRP PDU действует после включения в режиме глобальной конфигурации и режиме конфигурации интерфейса.

Включение функции туннеля GVRP PDU в режиме конфигурации интерфейса

Команда	**l2protocol-tunnel gvrp enable**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Функция туннелирования GVRP PDU действует после включения в режиме глобальной конфигурации и режиме конфигурации интерфейса.

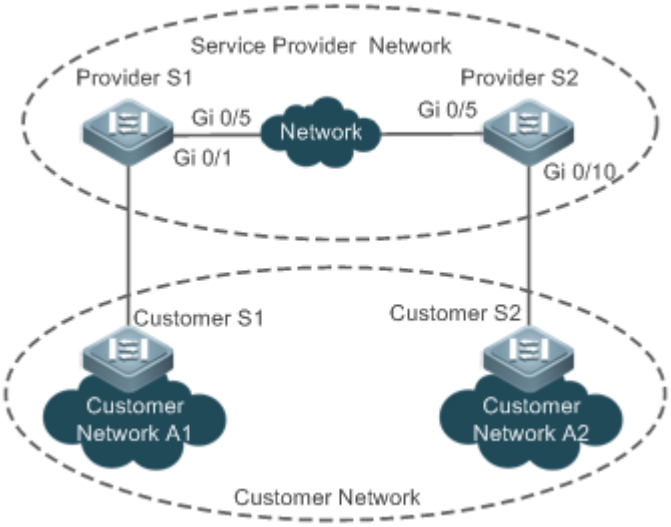
Настройка адреса прозрачной передачи данных туннеля GVRP PDU

Команда	**l2protocol-tunnel gvrp tunnel-dmac** *mac-address*
Описание параметра	*mac-address*: Указывает адрес GVRP, используемый при прозрачной передаче.
Установки по умолчанию	Адрес по умолчанию: 01d0.f800.0006.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	В приложении туннелирования GVRP PDU, когда пакет GVRP из сети заказчика поступает на PE в сети поставщика услуг, MAC-адрес назначения пакета изменяется на частный адрес до того, как пакет пересылается в сеть поставщика услуг. Когда пакет достигает одноранговогo PE, MAC-адрес назначения изменяется на публичный адрес до отправки пакета в сеть заказчика на другом концевом узле. Таким образом, пакет GVRP может быть прозрачно передан по сети поставщика услуг. Частный адрес — это адрес прозрачной передачи,

	используемый функцией туннелирования GVRP PDU. ⚠ Диапазон адресов для прозрачной передачи пакетов GVRP: 01d0.f800.0006 - 011a.a900.0006 ⚠ Если адрес прозрачной передачи не настроен, используется адрес по умолчанию 01d0.f800.0006.

Пример конфигурации

Настройка функции туннеля GVRP PDU

Сценарий Изображение 11-6	
Этапы конфигурации	❖ Включите Basic QinQ на PE (провайдер S1 и провайдер S2) в сети SP для передачи пакетов данных из сети заказчика через указанную VLAN в сети SP. ❖ Включите прозрачную передачу GVRP на PE (провайдер S1 и провайдер S2) в сети SP, чтобы позволить сети SP туннелировать пакеты GVRP от сети заказчика через туннель GVRP PDU.

Поставщик S1	Шаг 1: Создайте VLAN 200 в сети поставщика услуг.
	`QTECH#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`QTECH(config)#vlan 200`
	`QTECH(config-vlan)#exit`
	Шаг 2: Включите базовый QinQ на порту, подключенном к сети заказчика, для передачи данных из сети заказчика по сети 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 заказчика.
	`QTECH(config-if-GigabitEthernet 0/1)#l2protocol-tunnel gvrp enable`
	`QTECH(config-if-GigabitEthernet 0/1)#exit`
	Шаг 4: Включите прозрачную передачу GVRP глобально.
	`QTECH(config)#l2protocol-tunnel gvrp`
	Шаг 5: Настройка порта восходящего потока.
	`QTECH(config)# interface gigabitEthernet 0/5`
	`QTECH(config-if-GigabitEthernet 0/5)#switchport mode uplink`

Поставщик S2	Конфигурация на провайдере S2 аналогична конфигурации на провайдере S1.
Проверка конфигурации	❖ Проверьте правильность конфигурации туннеля GVRP. ❖ Убедитесь, что туннельный порт настроен правильно. Обратите внимание на следующее: ❖ Тип порта должен быть: dot1q-tunnel. ❖ Внешняя VLAN-метка является собственной VLAN и добавляется в список VLAN туннельного порта. ❖ Порты на PE в направлении восходящего канала настроены как порты восходящего канала.

Поставщик S1	1. Проверьте правильность конфигурации туннеля GVRP.
	`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`

Поставщик	Проверка поставщика S2 аналогична проверке поставщика S1.

S2	

Типичные ошибки

В сети поставщика услуг адреса прозрачной передачи не согласованы, что влияет на передачу кадров GVRP PDU.

11.4 Мониторинг

Очистка

⚠ Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	Команда
Очищает счетчики портов.	**clear gvrp statistics** { *interface-id* | **all** }

Отображение

Описание	Команда
Отображает счетчики портов.	**show gvrp statistics** { *interface-id* | **all** }
Отображает текущее состояние GVRP.	**show gvrp status**
Отображает конфигурацию текущего GVRP.	**show gvrp configuration**
Отображает информацию о функции туннеля GVRP PDU.	**show l2protocol-tunnel gvrp**

Отладка

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

Описание	Команда
Включает отладку событий GVRP.	**debug gvrp event**
Включает отладку таймера GVRP.	**debug gvrp timer**

12 КОНФИГУРИРОВАНИЕ LLDP

12.1 Обзор

Протокол LLDP (Link Layer Discovery Protocol), определенный в стандарте IEEE 802.1AB, используется для обнаружения топологии и определения топологических изменений. LLDP инкапсулирует локальную информацию устройства в блоки данных LLDP (LLDPDU) в формате типа/длины/значения (TLV), а затем отправляет LLDPDU соседним устройствам. Кроме того, в нем хранятся LLDPDU от соседних устройств в базе управляющей информации (MIB), доступ к которой осуществляется системой управления сетью (NMS).

С помощью LLDP NMS может узнать о топологии, например, какие порты устройства подключены к другим устройствам, а также о том, согласованы ли скорости и дуплексный режим на обоих концах канала. Администраторы могут быстро найти и устранить неисправность на основе данной информации.

Устройство, совместимое с QTECH LLDP, может обнаруживать соседние устройства, если одноранговый узел является одним из следующих:

- Устройство, совместимое с QTECH LLDP
- Оконечное устройство, которое соответствует протоколу обнаружения канального уровня
  Обнаружение оконечных медиа-устройств по протоколу (LLDP-MED)

Протоколы и стандарты

- IEEE 802.1AB 2005: Обнаружение соединения управления станцией и доступом к среде передачи данных
- ANSI/TIA-1057: Протокол обнаружения уровня канала для конечных устройств в данной среде

12.2 Применение

Применение	Описание
Отображение топологии	В топологии сети развернуты несколько коммутаторов, устройство MED и NMS.
Обнаружение ошибок при проведении	Два коммутатора подключены напрямую, и отображается неправильная конфигурация.

12.2.1 Отображение топологии

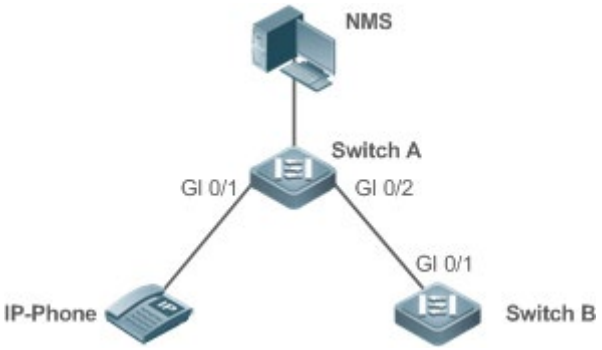
Сценарий

В топологии сети развернуты несколько коммутаторов, устройство MED и NMS.

Как показано на следующем Изображении, функция LLDP включена по умолчанию, и дополнительная настройка не требуется.

- Коммутаторы A и B обнаруживают, что они соседи.
- Коммутатор A обнаруживает соседнее устройство MED, то есть IP-телефон, через порт GigabitEthernet 0/1.
- NMS получает доступ к MIB коммутатора A.

Изображение 12-1



Заметки	QTECH коммутатор A, коммутатор B и IP-телефон поддерживают LLDP и LLDP-MED. LLDP на портах коммутатора работает в режиме TxRx. Интервал передачи LLDP составляет 30 секунд, а задержка передачи по умолчанию составляет 2 секунды.

Описание

- Запустите LLDP на коммутаторе, чтобы внедрить обнаружение соседних устройств.
- Запустите протокол SNMP на коммутаторе, чтобы NMS получала и задавала информацию, относительно LLDP на коммутаторе.

12.2.2 Вычисление при обнаружении ошибок

Сценарий

Два коммутатора подключены напрямую, и отображается неправильная конфигурация.

Как показано на следующем Изображении, функция LLDP и функция обнаружения ошибок LLDP включены по умолчанию, поэтому дополнительная настройка не требуется.

- После настройки виртуальной локальной сети (VLAN), скорости портов и дуплексного режима, агрегирования каналов связи и максимального блока передачи (MTU) порта коммутатора A появится сообщение об ошибке, если конфигурация не соответствует конфигурации коммутатора B и наоборот.

Изображение 12-2

Заметки	Коммутаторы QTECH A и B поддерживают LLDP.

	LLDP на портах коммутатора работает в режиме TxRx. Интервал передачи LLDP составляет 30 секунд, а задержка передачи по умолчанию составляет 2 секунды.

Описание

- Запустите LLDP на коммутаторе, чтобы внедрить обнаружение соседних узлов и обнаружить сбой канала.

12.3 Функции

Базовые концепции

LLDPDU

LLDPDU — это блок данных протокола, инкапсулированный в пакет LLDP. Каждый LLDPDU представляет собой последовательность структур TLV. Коллекция TLV состоит из трех обязательных TLV, серии дополнительных TLV и одного концевого TLV. На следующем Изображении показан формат LLDPDU.

Изображение 12-3 Формат LLDPDU

На предыдущем Изображении:

- M обозначает обязательный TLV.
- В LLDPDU, Chassis ID TLV, Port ID TLV, Time to Live TLV и End Of LLDPDU TLV являются обязательными TLV, в то время как другие TLV являются дополнительными.

Формат инкапсуляции LLDP

Пакеты LLDP могут быть инкапсулированы в двух форматах: Ethernet II и протоколы доступа к подсети (SNAP).

На следующем Изображении показан формат LLDP-пакетов, инкапсулированных в формате Ethernet II.

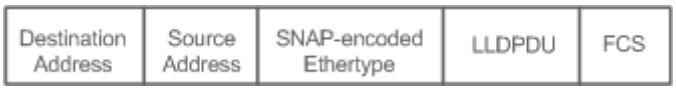
Изображение 12-4 Формат Ethernet II

На предыдущем Изображении:

- Адрес назначения: Указывает MAC-адрес назначения, который является многоадресным адресом LLDP 01-80-C2-00-00-0E.
- Адрес источника: Указывает MAC-адрес источника, который является MAC-адресом порта.
- Тип Ethertype: Указывает тип Ethernet, который 0x88CC.
- LLDPDU: Указывает блок данных протокола LLDP.
- FCS: Показывает последовательность проверки кадров.

На рис. 12-5 показан формат LLDP-пакетов, инкапсулированных в формате SNAP.

Изображение 12-5 Формат SNAP



На предыдущем Изображении:

- Адрес назначения: Указывает MAC-адрес назначения, который является многоадресным адресом LLDP 01-80-C2-00-00-0E.
- Адрес источника: Указывает MAC-адрес источника, который является MAC-адресом порта.
- Ethertype с кодированным SNAP: Указывает тип инкапсуляции SNMP Ethernet, который представляет собой AA-AA-03-00-00-00-88-CC.
- LLDPDU: Указывает блок данных протокола LLDP.
- FCS: Показывает последовательность проверки кадров.

TLV

TLV, инкапсулированные в LLDPDU, можно разделить на два типа:

- Основные управляющие TLV
- TLV, специфичные для организации

Основные управляющие TLV — это группа базовых TLV для управления сетью. Специфичные для организации TLV определяются организациями стандартизации и другими организациями, например, организацией IEEE 802.1 и IEEE 802.3, которые определяют свои собственные списки TLV.

1. Основные управляющие TLV

Базовый набор TLV управления состоит из двух типов TLV: Обязательных TLV и дополнительных TLV. Обязательный TLV должен содержаться в LLDPDU для объявления, а дополнительный TLV включается выборочно.

В следующей таблице описаны базовые TLV для управления.

Тип TLV	**Описание**	**Обязательно/дополнительно**
End Of LLDPDU TLV	Указывает конец LLDPDU, занимающий два байта.	Обязательно
Chassis ID TLV	Идентифицирует устройство с MAC-адресом.	Обязательно
Port ID TLV	Определяет порт, передающий LLDPDU.	Фиксированный
Time To Live TLV	Указывает время жизни (TTL) локальной информации о соседе.	Обязательно

	Когда устройство получает TLV, содержащее TTL 0, оно удаляет информацию о соседнем устройстве.	
Port Description TLV	Указывает дескриптор порта, передающего LLDPDU.	Дополнительно
System Name TLV	Описывает имя устройства.	Дополнительно
System Description TLV	Описывает устройства, включая версию аппаратного обеспечения, версию программного обеспечения и информацию об операционной системе.	Дополнительно
System CLAGabilities TLV	Описывает основные функции устройства, такие как мост, маршрутизация и функции реле.	Дополнительно
Management Address TLV	Указывает адрес управления, содержащий идентификатор интерфейса и идентификатор объекта (OID).	Дополнительно

Коммутаторы, совместимые с QTECH LDP, поддерживают объявления базовых TLV управления.

2. TLV, специфичные для организации

Различные организации, такие как IEEE 802.1, IEEE 802.3, IETF и поставщики устройств, определяют конкретные TLV для объявлений определенной информации об устройствах. Поле уникального идентификатора организации (OUI) в TLV используется для дифференциации различных организаций.

- Специфичные для организации TLV являются дополнительными и объявляются в LLDPDU выборочно. В настоящее время существует три типа общих организационных TLV: TLV, специфичные для организации IEEE 802.1, TLV, специфичные для организации IEEE 802.3, и LLDP-MED TLV.

В следующей таблице описаны TLV, специфичные для организации IEEE 802.1.

Тип TLV	**Описание**
VLAN ID TLV порта	Указывает идентификатор VLAN порта.
VLAN ID TLV порта и протокола	Указывает идентификатор VLAN протокола порта.

VLAN Name TLV	Указывает имя VLAN порта.
Protocol Identity TLV	Указывает тип протокола, поддерживаемый портом.

Коммутаторы, совместимые с QTECH LDP, не посылают TLV идентификатора протокола, но получают этот TLV.

❖ TLV, специфичные для организации IEEE 802.3

В следующей таблице описаны TLV, специфичные для организации IEEE 802.1.

Тип TLV	Описание
MAC/Конфигурирование PHY/TLV статуса	Указывает скорость и дуплексный режим порта, а также необходимость поддержки и включения автоматического согласования.
Power Via MDI TLV	Указывает мощность источника питания порта.
Link Aggregation TLV	Указывает агрегирование каналов связи для порта и текущее состояние агрегирования.
Maximum Frame Size TLV	Указывает максимальный размер кадра, переданного портом.

Устройства, совместимые с QTECH LDP, поддерживают объявление TLV, специфичное для организации IEEE 802.3.

❖ LLDP-MED TLV

LLDP-MED является расширением LLDP на основе IEEE 802.1AB LLDP. Данный TLV позволяет пользователям удобно развертывать сеть VoIP и обнаруживать неисправности. Данный TLV предоставляет приложения, включая политики конфигурации сети, обнаружение устройств, управление PoE и управление инвентаризацией, соответствуя требованиям к низкой стоимости, эффективному управлению и простому развертыванию.

В следующей таблице описаны LLDP-MED TLV.

Тип TLV	Описание
LLDP-MED CLAGabilities TLV	Указывает тип LLDP-MED TLV, инкапсулированного в LLDPDU и тип устройства (устройство сетевого подключения или оконечное устройство), а также на

	необходимость поддержки LLDP-MED.
Network Policy TLV	Объявляет конфигурацию VLAN порта, поддерживаемые типы приложений (например, голосовые или видеосервисы) и информацию о приоритете уровня 2.
Location Identification TLV	Поиск и идентификация конечного устройства.
Extended Power-via-MDI TLV	Обеспечивает более совершенную систему управления питанием.
Inventory – Hardware Revision TLV	Обозначает версию аппаратного обеспечения устройства MED.
Inventory – Firmware Revision TLV	Указывает версию микропрограммы устройства MED.
Inventory – Software Revision TLV	Указывает версию программного обеспечения устройства MED.
Inventory – Serial Number TLV	Указывает серийный номер устройства MED.
Inventory – Manufacturer Name TLV	Указывает имя производителя устройства MED.
Inventory – Model Name TLV	Указывает название модуля устройства MED.
Inventory – Asset ID TLV	Указывает идентификатор ресурса устройства MED, используемого для управления запасами и отслеживания активов.

Устройства, совместимые с QTECH LLDP, поддерживают объявление LLDP-MED TLV.

Обзор

Функция	Описание
Режим работы LLDP	Настройка режима передачи и приема LLDP-пакетов.

Механизм передачи LLDP	Позволяет напрямую подключенным устройствам, совместимым с LLDP, отправлять пакеты LLDP на одноранговый узел.
Механизм приема LLDP	Позволяет напрямую подключенным устройствам, совместимым с LLDP, получать пакеты LLDP от однорангового узла.

12.3.1 Режим работы LLDP

Настраивает рабочий режим LLDP, чтобы задать режим передачи и приема пакетов LLDP.

Принцип работы

LLDP поддерживает три режима работы:

- TxRx Передает и принимает LLDPDU.
- Rx Only: Только получает LLDPDU.
- Tx Only: Только передает LLDPDU.

При изменении рабочего режима LLDP порт инициализирует машину состояния протокола. Можно установить задержку инициализации порта, чтобы предотвратить повторяющееся выполнение инициализации порта из-за частого изменения рабочего режима LLDP.

Связанная конфигурация

Настройка рабочего режима LLDP

По умолчанию LLDP работает в режиме TxRx.

Для настройки режима работы LLDP можно выполнить команду **lldp mode**.

Если режим работы установлен на TxRx, устройство может передавать и принимать пакеты LLDP. Если режим работы установлен на Rx Only, устройство может только принимать пакеты LLDP. Если режим работы установлен на Tx Only, устройство может только передавать пакеты LLDP. Если режим работы «отключено», устройство не может передавать или принимать пакеты LLDP.

12.3.2 Механизм передачи LLDP

Пакеты LLDP информируют одноранговые узлы о своих соседях. Если режим передачи LLDP отмененяется или в состоянии «отключен», пакеты LLDP не могут быть переданы соседям.

Принцип работы

LLDP периодически передает пакеты LLDP при работе в режиме TxRx или Tx Only. При изменении информации о локальном устройстве, LLDP немедленно передает пакеты LLDP. Можно настроить время задержки, чтобы избежать частой передачи пакетов LLDP, вызванной частыми изменениями локальной информации.

LLDP предоставляет два типа пакетов:

- Стандартный пакет LLDP, содержащий информацию об управлении и конфигурации локального устройства.
- Пакет Shutdown: Если режим работы LLDP «отключен» или порт отключен, пакеты LLDP Shutdown будут переданы. 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 - 0. Когда устройство получает пакет отключения LLDP, оно считает, что информация о соседнем устройстве недействительна и немедленно удаляет ее.

Если рабочий режим LLDP изменен с Disabled («отключен») или Rx на TxRx или Tx, или когда LLDP обнаруживает нового соседа (то есть, устройство получает новый пакет LLDP, а информация о соседнем устройстве не хранится 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.

Связанная конфигурация

Настройка режима работы LLDP

По умолчанию используется режим работы 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 LLDP-пакетов, установите для режима работы значение TxRx или Rx Only. Если для режима работы установлено значение Rx Only, устройство может только принимать 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 задержка установлена на очень малое значение, частое изменение локальной информации приведет к частой передаче пакетов LLDP. Если задержка установлена на очень большое значение, пакет LLDP не может быть передан даже при изменении локальной информации.

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 малое значение, пакеты LLDP могут передаваться часто. Если интервал установлен на очень большое значение, одноранговый узел может не обнаружить локальное устройство вовремя.

Настройка объявленных TLV

По умолчанию интерфейс может объявлять TLV всех типов, кроме TLV идентификации местоположения.

Запустите команду **lldp tlv-enable**, чтобы изменить TLV, которые будут объявлены.

Настройка счетчика быстрой передачи LLDP

По умолчанию передаются три LLDP-пакета.

Запустите команду **lldp fast-count**, чтобы изменить количество быстро передаваемых пакетов LLDP.

12.3.3 Механизм приема LLDP

Устройство может обнаружить соседа и определить, нужно ли возрастить информацию о соседе в соответствии с полученными пакетами LLDP.

Принцип работы

Устройство может принимать пакеты LLDP при работе в режиме TxRx или Rx Only. После получения пакета LLDP устройство проводит 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 соседе в соответствии со значением TTL TLV в пакете. Если значение TTL TLV равно 0, информация о соседе немедленно устаревает.

Связанная конфигурация

Настройка режима работы LLDP

По умолчанию LLDP работает в режиме TxRx.

Запустите команду **lldp mode txrx** или **lldp mode rx**, чтобы включить функцию приема пакетов LLDP. Для отключения функции приема пакетов LLDP запустите режим **lldp mode tx** или **no lldp mode**.

Чтобы включить прием LLDP-пакетов, установите для режима работы значение TxRx или Rx Only. Если режим работы установлен на Tx Only, устройство может только передавать пакеты LLDP.

12.4 Конфигурация

Конфигурация	Описание и команда	
Настройка функции LLDP	⚠ (Дополнительно) Используется для включения или отключения функции LLDP в режиме глобальной конфигурации или конфигурации интерфейса.	
	lldp enable	Включает функцию LLDP.
	no lldp enable	Выключает функцию LLDP.
Настройка рабочего	⚠ (Дополнительно) Используется для настройки рабочего режима	

режима LLDP	LLDP.	
	lldp mode {rx | tx | txrx }	Настройка рабочего режима LLDP.
	no lldp mode	Выключение рабочего режима LLDP.
Настройка объявленных TLV	⚠ (Дополнительно) Используется для настройки TLV, которые будут объявлены.	
	lldp tlv-enable	Настраивает TLV для объявления.
	no lldp tlv-enable	Отменяет TLV.
Настройка адреса управления для объявления	⚠ (Дополнительно) Используется для настройки адреса управления для объявления в LLDP-пакеты.	
	lldp management-address-tlv [*ip-address*]	Настраивает адрес управления, который будет объявляться в LLDP-пакетах.
	no lldp management-address-tlv	Отменяет адрес управления.
Настройка счетчика быстрой передачи LLDP	⚠ (Дополнительно) Используется для настройки количества быстро передаваемых пакетов LLDP.	
	lldp fast-count *value*	Настраивает счетчик Быстрой передачи LLDP.
	no lldp fast-count	Восстанавливает значение по умолчанию для Быстрой передачи LLDP.
Настройка множителя TTL и интервала передачи	⚠ (Дополнительно) Используется для настройки множителя TTL и интервала передачи.	
	lldp hold-multiplier *value*	Настраивает множитель TTL.

	no lldp hold-multiplier	Восстанавливает множитель TTL по умолчанию.
	lldp timer tx-interval *seconds*	Настраивает интервал передачи.
	no lldp timer tx-interval	Восстанавливает интервал передачи по умолчанию.
Настройка задержки передачи	⚠ (Дополнительно) Используется для настройки времени задержки передачи пакетов LLDP.	
	lldp timer tx-delay *seconds*	Настраивает задержку передачи.
	no lldp timer tx-delay	Восстанавливает задержку передачи по умолчанию.
Настройка задержки инициализации	⚠ (Дополнительно) 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 LLDP Trap	⚠ (Дополнительно) 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 запросов LLDP.
	no lldp timer notification-interval	Восстанавливает интервал передачи запросов LLDP по умолчанию.

Настройка функции обнаружения ошибок LLDP	⚠ (Дополнительно) Используется для настройки функции обнаружения ошибок LLDP.	
	lldp error-detect	Включает функцию обнаружения ошибок LLDP.
	no lldp error-detect	Отключает функцию обнаружения ошибок LLDP.
Настройка формата инкапсуляции LLDP	⚠ (Дополнительно) 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	⚠ (Необязательно) 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 почтового адреса	⚠ (Дополнительно) Используется для настройки почтового адреса устройства.	
	{ **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*	Настраивает почтовый адрес устройства.

	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 почтовый адрес устройства.
Настройка номера телефона экстренной связи	⚠ (Дополнительно) Используется для настройки номера экстренной связи для устройства.	
	lldp location elin identifier *id* **elin-location** *tel-number*	Настраивает номер телефона экстренной связи для устройства.
	no lldp location elin identifier *id*	Удаляет номер телефона экстренной связи для устройства.

12.4.1 Конфигурирование функции LLDP

Сценарий

- Включение или отключение функции LLDP.

Примечание

- Чтобы функция LLDP была включена в интерфейсе, необходимо включить функцию LLDP глобально и на интерфейсе.

Этапы конфигурации

- Опционально.
- Настройте функцию LLDP в режиме глобальной конфигурации или конфигурации интерфейса.

Проверка конфигурации

Отображение состояния LLDP

- Проверьте, включена ли функция LLDP в режиме глобальной конфигурации.
- Проверьте, включена ли функция LLDP в режиме конфигурации интерфейса.

Связанные команды

Включение функции LLDP

Команда	**lldp enable**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Функция LLDP действует в интерфейсе только после его включения в режиме глобальной конфигурации и режиме конфигурации интерфейса.

Отключение функции LLDP

Команда	**no lldp enable**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Пример конфигурации

Отключение функции LLDP

Этапы конфигурации	❖ Отключите функцию LLDP в режиме глобальной конфигурации.
	`QTECH(config)#no lldp enable`
Проверка конфигурации	❖ Отображение глобального состояния LLDP.
	`QTECH(config)#show lldp status` `Global status of LLDP: Disable`

Типичные ошибки

❖ Если функция LLDP включена в интерфейсе, но отключена в режиме глобальной конфигурации, функция LLDP не действует в интерфейсе.

- Порт может обучиться не более пяти соседям.
- Если соседний узел не поддерживает LLDP, но подключен к устройству, поддерживающему LLDP, порт может получить информацию об устройстве, которое не подключено напрямую к порту, так как соседний узел может пересылать пакеты LLDP.

12.4.2 Настройка режима работы LLDP

Сценарий

- Если для рабочего режима LLDP установлено значение TxRx, интерфейс может передавать и принимать пакеты.
- Если для рабочего режима LLDP установлено значение Tx, интерфейс может только передавать пакеты, но не может принимать пакеты.
- Если для рабочего режима LLDP установлено значение Rx, интерфейс может только принимать пакеты, но не может передавать пакеты.
- Если отключить режим работы LLDP, интерфейс не сможет принимать и передавать пакеты.

Примечание

- LLDP работает на физических портах (или на портах-участниках для агрегированного порта). Стекируемые порты и порты VSL не поддерживают LLDP.

Этапы конфигурации

- Опционально.
- При необходимости установите рабочий режим LLDP в положение Tx (Передача) или Rx (Прием).

Проверка конфигурации

Отобразите информацию о состоянии LLDP в интерфейсе

- Проверьте, действует ли конфигурация.

Связанные команды

Настройка режима работы LLDP

Команда	**lldp mode** { **rx** | **tx** | **txrx** }
Описание параметра	**rx**: Только получает LLDPDU. **tx**: Только передает LLDPDU. **txrx**: Передает и принимает LLDPDU.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Чтобы LLDP вступил в силу для интерфейса, убедитесь, что LLDP включен глобально, и установите режим работы LLDP в интерфейсе на

	Tx, Rx или TxRx.

Отключение рабочего режима LLDP

Команда	**no lldp mode**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	После отключения режима работы LLDP интерфейс не передает и не принимает пакеты LLDP.

Пример конфигурации

Настройка режима работы LLDP

Этапы конфигурации	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 конфигурации	Отобразите информацию о состоянии LLDP в 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 объявленных TLV

Сценарий

- Настройте тип TLV для объявления, чтобы указать LLDPDU в пакетах LLDP.

Примечания

- При настройке параметра **all** для TLV базового управления, TLV, специфичных для организации IEEE 802.1, и TLV, специфичных для организации IEEE 802.3, будут объявлены все дополнительные TLV этих типов.
- При настройке параметра **all** для LLDP-MED TLV будут объявлены все LLDP-MED TLV, кроме TLV идентификации местоположения.
- Если необходимо настроить TLV совместимости LLDP-MED, сначала настройте LLDP 802.3 MAC/PHY TLV; если вы хотите отменить TLV LLDP 802.3 MAC/PHY, сначала отмените TLV совместимости LLDP-MED.
- Если необходимо настроить LLDP-MED TLV, настройте TLV совместимости LLDP-MED перед настройкой других типов LLDP-MED TLV. Если вы хотите отменить LLDP-MED TLV, отмените TLV совместимости LLDP-MED перед отменой других типов LLDP-MED TLV; если устройство подключено к IP-телефону, поддерживающему LLDP-MED, можно настроить TLV сетевой политики для передачи конфигурации политики на IP-телефон.
- Если устройство по умолчанию поддерживает функцию DCBX, порты устройства не могут объявлять TLV, специфичные для организации IEEE 802.3, и TLV LLDP-MED.

Этапы конфигурации

- Опционально.
- Настройте тип TLV, который будет объявляться в интерфейсе.

Проверка конфигурации

Отобразите конфигурацию TLV для объявления в интерфейсе

- Проверьте, действует ли конфигурация.

Связанные команды

Настройка объявляемых TLV

Команда	**lldp tlv-enable** { **basic-tlv** { **all** | **port-description** | **system-cLAGability** | **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** | **cLAGability** | **inventory** | **location** { **civic-location** | **elin** } **identifier** *id* | **network-policy profile** [*profile-num*] | **power-over-ethernet** } }
Описание параметра	**basic-tlv**: Указывает TLV базового управления. port-description: Указывает TLV описания порта. system-cLAGability: Указывает TLV системных возможностей.

	system-description: Указывает TLV описания системы. system-name: Указывает TLV имени системы. dot1-tlv: Указывает на специфичные для организации TLV IEEE 802.1. port-vlan-id: Указывает TLV идентификатора VLAN порта. protocol-vlan-id: Указывает TLV идентификатора VLAN порта и протокола. *vlan-id*: Указывает идентификатор VLAN протокола порта 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 на специфичные для организации TLV IEEE 802.3. link-aggregation: Указывает TLV агрегирования каналов связи. 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 TLV LLDP MED. cLAGability: Указывает TLV возможностей LLDP-MED. Inventory: Указывает TLV управления активами, в котором содержится версия аппаратного обеспечения, версия микропрограммы, версия программного обеспечения, серийный номер, название производителя, имя модуля и идентификатор актива. location: Указывает TLV идентификации местоположения. civic-location: Указывает информацию о гражданском адресе и почтовый адрес. elin: Указывает номер телефона экстренной связи. *id*: Указывает идентификатор политики в диапазоне от 1 до 1024. network-policy: Указывает TLV сетевой политики. *profile-num*: Указывает идентификатор сетевой политики в диапазоне от 1 до 1024. power-over-ethernet: Указывает расширенный TLV питания через MDI.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Отмена TLV

Команда	**no lldp tlv-enable {basic-tlv** { **all | port-description | system-cLAGability | 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 | cLAGability | inventory | location** { **civic-location | elin** } **identifier** *id* **| network-policy profile** [*profile-num*] **| power-over-ethernet** } }
Описание параметра	**basic-tlv**: Указывает TLV базового управления. port-description: Указывает TLV описания порта. system-cLAGability: Указывает TLV системных возможностей. system-description: Указывает TLV описания системы. system-name: Указывает TLV имени системы. dot1-tlv: Указывает на специфичные для организации TLV IEEE 802.1. port-vlan-id: Указывает TLV идентификатора VLAN порта. protocol-vlan-id: Указывает TLV идентификатора VLAN порта и протокола. vlan-name: Указывает TLV имени VLAN. dot3-tlv: Указывает на специфичные для организации TLV IEEE 802.3. link-aggregation: Указывает TLV агрегирования каналов связи. 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 TLV LLDP MED. cLAGability: Указывает TLV возможностей LLDP-MED. Inventory: Указывает TLV управления активами, в котором содержится версия аппаратного обеспечения, версия микропрограммы, версия программного обеспечения, серийный номер, название производителя, имя модуля и идентификатор актива. location: Указывает TLV идентификации местоположения. civic-location: Указывает информацию о гражданском адресе и почтовый адрес. 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 идентификатор сетевой политики в диапазоне от 1 до 1024. power-over-ethernet: Указывает расширенный TLV питания через MDI.

Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Пример конфигурации

Настройка объявляемых TLV

Этапы конфигурации	Отмените объявление TLV для определенного порта и идентификатора VLAN протокола IEEE 802.1.
	QTECH(config)#interface gigabitethernet 0/1 QTECH(config-if-GigabitEthernet 0/1)#no lldp tlv-enable dot1-tlv protocol-vlan-id
Проверка конфигурации	Отобразите конфигурацию 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 CLAGabilities 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: CLAGabilities 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 Настройка адреса управления для передачи соседним устройствам

Сценарий

- Настройте адрес управления, который будет объявляться в пакетах LLDP в режиме конфигурации интерфейса.
- После отмены объявленного адреса управления адрес управления в пакетах LLDP зависит от настроек по умолчанию.

Примечания

- LLDP работает на физических портах (или на портах-участниках для агрегированного порта). Стекируемые порты и порты VSL не поддерживают LLDP.

Этапы конфигурации

- Опционально.
- Настройте адрес управления, который будет объявляться в пакетах LLDP в режиме конфигурации интерфейса.

Проверка конфигурации

Отобразите информацию LLDP на локальном интерфейсе

- Проверьте, действует ли конфигурация.

Связанные команды

Настройка адреса управления для объявления

Команда	**lldp management-address-tlv** [*ip-address*]
Описание параметра	*ip-address*: Настраивает адрес управления, который будет объявляться в пакетах LLDP.
Режим команд	Режим конфигурации интерфейса
Встроенная	По умолчанию адрес управления объявляется через пакеты LLDP.

подсказка	Адрес управления — это IPv4-адрес минимальной VLAN, поддерживаемой портом. Если для VLAN не настроен IPv4-адрес, LLDP продолжает поиск свободного IP-адреса. Если IPv4-адрес не найден, LLDP ищет IPv6-адрес минимальной VLAN, поддерживаемой портом. Если IPv6-адрес не найден, в качестве адреса управления используется адрес loopback 127.0.0.1.

Отмена адреса управления

Команда	**no lldp management-address-tlv**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	По умолчанию адрес управления объявляется через пакеты LLDP. Адрес управления — это IPv4-адрес минимальной VLAN, поддерживаемой портом. Если для VLAN не настроен IPv4-адрес, LLDP продолжает поиск свободного IP-адреса. Если IPv4-адрес не найден, LLDP ищет IPv6-адрес минимальной VLAN, поддерживаемой портом. Если IPv6-адрес не найден, в качестве адреса управления используется адрес loopback 127.0.0.1.

Пример конфигурации

Настройка адреса управления для объявления

Этапы конфигурации	Установите адрес управления на 192.168.1.1 в интерфейсе.
	`QTECH(config)#interface gigabitethernet 0/1` `QTECH(config-if-GigabitEthernet 0/1)#lldp management-address-tlv 192.168.1.1`
Проверка конфигурации	Отобразите конфигурацию в 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

Сценарий

- ❖ Настройка количества быстро передаваемых пакетов LLDP.

Этапы конфигурации

- ❖ Опционально.
- ❖ Настройка количества пакетов LLDP, которые быстро передаются в режиме глобальной конфигурации.

Проверка конфигурации

Отображение глобальной информации о состоянии LLDP

- ❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка счетчика быстрой передачи LLDP

Команда	**lldp fast-count** *value*
Описание параметра	*value*: Указывает количество быстро передаваемых пакетов LLDP. Диапазон значений от 1 до 10. Значение по умолчанию: 3.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Восстанавливает значение по умолчанию для Быстрой передачи LLDP

Команда	**no lldp fast-count**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Пример конфигурации

Настройка счетчика быстрой передачи LLDP

Этапы конфигурации	Установите значение счетчика быстрой передачи LLDP на 5 в режиме глобальной конфигурации.
	`QTECH(config)#lldp fast-count 5`
Проверка конфигурации	Отобразите глобальную информацию о состоянии 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

Сценарий

- ❖ Настройте множитель TTL.
- ❖ Настройте интервал передачи пакетов LLDP.

Этапы конфигурации

- ❖ Опционально.
- ❖ Выполните настройку в режиме глобальной конфигурации.

Проверка конфигурации

Отобразите информацию о состоянии LLDP в интерфейсе

- ❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка множителя TTL

Команда	**lldp hold-multiplier** *value*
Описание параметра	*value*: Указывает множитель TLL. Диапазон значений от 2 до 10. Значение по умолчанию: 4.
Режим	Режим глобальной конфигурации

команд	
Встроенная подсказка	В пакете LLDP значение Time To Live TLV рассчитывается по следующей формуле: Time to Live TLV = множитель TTL x интервал передачи пакетов + 1. Таким образом, можно изменить Time to Live TLV в LLDP-пакетах, настроив множитель TTL.

Восстановление множителя TTL по умолчанию

Команда	**no lldp hold-multiplier**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	В пакете LLDP значение Time To Live TLV рассчитывается по следующей формуле: Time to Live TLV = множитель TTL x интервал передачи пакетов + 1. Таким образом, можно изменить Time to Live TLV в LLDP-пакетах, настроив множитель TTL.

Настройка интервала передачи

Команда	**lldp timer tx-interval** *seconds*
Описание параметра	*seconds*: Указывает интервал передачи пакетов LLDP. Диапазон значений от 5 до 32768.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Восстановление интервала передачи по умолчанию

Команда	**no lldp timer tx-interval**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации

Встроенная подсказка	Недоступно

Пример конфигурации

Настройка множителя TTL и интервала передачи

Этапы конфигурации	Установите множитель TTL на 3, а интервал передачи - на 20 секунд. TTL локальной информации об устройствах на соседних устройствах составляет 61 секунду.
	QTECH(config)#lldp hold-multiplier 3 QTECH(config)#lldp timer tx-interval 20
Проверка конфигурации	Отобразите глобальную информацию о состоянии 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

Сценарий

❖ Настройка времени задержки для передачи пакетов LLDP.

Этапы конфигурации

❖ Опционально.
❖ Выполните настройку в режиме глобальной конфигурации.

Проверка конфигурации

Отображение глобальной информации о состоянии LLDP

❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка задержки передачи

Команда	**lldp timer tx-delay** *seconds*
Описание параметра	*seconds*: Указывает задержку передачи. Диапазон значений от 1 до 8192.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	При изменении локальной информации об устройстве коммутатор немедленно передает пакеты LLDP соседним устройствам. 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**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	При изменении локальной информации об устройстве коммутатор немедленно передает пакеты LLDP соседним устройствам. Настройте задержку передачи, чтобы предотвратить частую передачу пакетов LLDP, вызванную частыми изменениями локальной информации.

Пример конфигурации

Настройка задержки передачи

Этапы конфигурации	Установите задержку передачи на 3 секунды.
	`QTECH(config)#lldp timer tx-delay 3`
Проверка конфигурации	Отобразите глобальную информацию о состоянии 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

Сценарий

❖ Настройте время задержки для инициализации LLDP в любом интерфейсе.

Этапы конфигурации

❖ Опционально.
❖ Настройте время задержки для инициализации LLDP в любом интерфейсе.

Проверка конфигурации

Отобразите глобальную информацию о состоянии LLDP

❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка задержки инициализации

Команда	**lldp timer reinit-delay** *seconds*
Описание параметра	*seconds*: Указывает задержку инициализации. Значение варьируется от 1 до 10 секунд.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Настройте задержку инициализации для предотвращения частой инициализации машины состояния, вызванной частыми изменениями режима работы порта.

Восстановление задержки инициализации по умолчанию

Команда	**no lldp timer reinit-delay**
Описание	Недоступно

параметра	
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Настройте задержку инициализации для предотвращения частой инициализации машины состояния, вызванной частыми изменениями режима работы порта.

Пример конфигурации

Настройка задержки инициализации

Этапы конфигурации	Установите задержку инициализации на 3 секунды.
	`QTECH(config)#lldp timer reinit-delay 3`
Проверка конфигурации	Отобразите глобальную информацию о состоянии 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 LLDP Trap

Сценарий

- Настройка интервала для передачи сообщений LLDP Trap.

Этапы конфигурации

Включение функции LLDP Trap

- Опционально.
- Выполните настройку в режиме конфигурации интерфейса.

Настройка интервала передачи LLDP Trap

- Опционально.
- Выполните настройку в режиме глобальной конфигурации.

Проверка конфигурации

Отображение информации о состоянии LLDP

- Проверьте, включена ли функция LLDP Trap.
- Проверьте, вступила ли в силу конфигурация интервала.

Связанные команды

Включение функции LLDP Trap

Команда	**lldp notification remote-change enable**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Функция LLDP Trap позволяет устройству отправлять локальные данные LLDP (например, обнаружение соседей и сбой канала связи) на сервер NMS, чтобы администраторы могли узнать о производительности сети.

Отключение функции LLDP Trap

Команда	**no lldp notification remote-change enable**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Функция LLDP Trap позволяет устройству отправлять локальные данные LLDP (например, обнаружение соседей и сбой канала связи) на сервер NMS, чтобы администраторы могли узнать о производительности сети.

Настройка интервала передачи LLDP Trap

Команда	**lldp timer notification-interval** *seconds*
Описание	*seconds*: Указывает интервал передачи сообщений LLDP Trap. Значение варьируется от 5 до 3600 секунд. Значение по умолчанию: 5

параметра	секунд.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Настройте интервал передачи запросов LLDP, чтобы предотвратить частую передачу сообщений LLDP Trap. Изменения LLDP, обнаруженные в течение этого интервала, будут переданы на сервер NMS.

Восстановление интервала передачи LLDP Trap

Команда	**no lldp timer notification-interval**
Описание параметра	Недоступно
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Настройте интервал передачи запросов LLDP, чтобы предотвратить частую передачу сообщений LLDP Trap. Изменения LLDP, обнаруженные в течение этого интервала, будут переданы на сервер NMS.

Пример конфигурации

Включение функции LLDP Trap и настройка интервала передачи LLDP Trap.

Этапы конфигурации	Включите функцию LLDP Trap и установите интервал передачи запросов LLDP на 10 секунд.

	`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 конфигурации	Отобразите информацию 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

Сценарий

- Включает функцию обнаружения ошибок LLDP. Когда LLDP обнаруживает ошибку, она регистрируется в журнале.
- Настройте функцию обнаружения ошибок LLDP для обнаружения конфигурации VLAN на обоих концах канала, состояния порта, конфигурации агрегированного порта, конфигурации MTU и петель.

Примечания

- Недоступно

Этапы конфигурации

- Опционально.
- Включение или отключение функции обнаружения ошибок LLDP в режиме конфигурации интерфейса.

Проверка конфигурации

Отобразите информацию о состоянии LLDP в интерфейсе

- Проверьте, действует ли конфигурация.

Связанные команды

Включение функции обнаружения ошибок LLDP

Команда	**lldp error-detect**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Функция обнаружения ошибок LLDP основана на определенных TLV в LLDP-пакетах, которые обмениваются между устройствами на обоих концах канала. Поэтому для обеспечения функции обнаружения ошибок LLDP устройство должно объявить правильные TLV.

Отключение функции обнаружения ошибок LLDP

Команда	**no lldp error-detect**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Функция обнаружения ошибок LLDP основана на определенных TLV в LLDP-пакетах, которые обмениваются между устройствами на обоих концах канала. Поэтому для обеспечения функции обнаружения ошибок LLDP устройство должно объявить правильные TLV.

Пример конфигурации

Включение функции обнаружения ошибок LLDP

Этапы конфигурации	Включите функцию обнаружения ошибок LLDP в интерфейсе GigabitEthernet 0/1.
	`QTECH(config)#interface gigabitethernet 0/1` `QTECH(config-if-GigabitEthernet 0/1)#lldp error-detect`
Проверка конфигурации	Отобразите информацию о состоянии LLDP в 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

Сценарий

❖ Настройка формата инкапсуляции LLDP.

Этапы конфигурации

❖ Опционально.
❖ Настройте формат инкапсуляции LLDP в интерфейсе.

Проверка конфигурации

Отобразите информацию о состоянии LLDP в интерфейсе

❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка формата инкапсуляции LLDP на SNAP

Команда	**lldp encapsulation snap**
Описание параметра	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	⚠ Конфигурация формата инкапсуляции LLDP на устройстве и соседних устройствах должна быть согласованной.

Восстановление формата инкапсуляции LLDP по умолчанию (Ethernet II)

Команда	**no lldp encapsulation snap**
Описание	Недоступно

параметра	
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	⚠ Конфигурация формата инкапсуляции LLDP на устройстве и соседних устройствах должна быть согласованной.

Пример конфигурации

Настройка формата инкапсуляции LLDP на SNAP

Этапы конфигурации	Установите формат инкапсуляции LLDP на SNAP.
	`QTECH(config)#interface gigabitethernet 0/1` `QTECH(config-if-GigabitEthernet 0/1)#lldp encapsulation snap`
Проверка конфигурации	Отобразите информацию о состоянии LLDP в 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

Сценарий

- Настройка сетевой политики LLDP.
- Если устройство подключено к IP-телефону, поддерживающему LLDP-MED, можно настроить TLV сетевой политики для передачи конфигурации политики на IP-телефон, что позволяет IP-телефону изменять тег и QoS голосовых потоков. В дополнение к сетевой политике LLDP выполните следующие действия на устройстве: 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 режим доверенного DSCP). 3. Если на порту также включена аутентификация 802.1X, настройте безопасный канал для пакетов из голосовой VLAN. Если IP-телефон не поддерживает LLDP-MED, включите функцию голосовой VLAN и добавьте MAC-адрес IP-телефона в список Voice VLAN OUI вручную.

- Информацию о настройке доверенного режима QoS см. в разделе *Настройка IP QoS*; о настройке голосовой VLAN см. в разделе *Настройка голосовой VLAN*; о настройке безопасного канала см. в разделе *Настройка ACL*.

Этапы конфигурации

- Опционально.
- Настройка сетевой политики LLDP.

Проверка конфигурации

Отобразите конфигурацию сетевой политики LLDP.

- Проверьте, действует ли конфигурация.

Связанные команды

Настройка сетевой политики LLDP

Команда	**lldp network-policy profile** *profile-num*
Описание параметра	*profile-num*: Указывает идентификатор сетевой политики LLDP. Диапазон значений от 1 до 1024.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы войти в режим сетевой политики LLDP после указания идентификатора политики. После входа в режим сетевой политики LLDP выполните команду **{ voice | voice-signaling } vlan** для настройки определенной сетевой политики.

Настройка сетевой политики LLDP

Команда	**no lldp network-policy profile** *profile-num*
Описание параметра	*profile-num*: Указывает идентификатор сетевой политики LLDP. Диапазон значений от 1 до 1024.
Режим команд	Режим конфигурации интерфейса

Встроенная подсказка	Выполните эту команду, чтобы войти в режим сетевой политики LLDP после указания идентификатора политики. После входа в режим сетевой политики LLDP выполните команду **{ voice | voice-signaling } vlan** для настройки определенной сетевой политики.

Пример конфигурации

Настройка сетевой политики LLDP

Этапы конфигурации	Установите для параметра Network Policy TLV значение 1, чтобы пакеты LLDP были объявлены портом GigabitEthernet 0/1, и установите для идентификатора VLAN приложения Voice значение 3, COS — 4, DSCP — 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 конфигурации	Отображение конфигурации 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 почтового адреса

Сценарий

- Настраивает почтовый адрес устройства.

Этапы конфигурации

- Опционально.
- Выполните эту настройку в режиме настройки почтового адреса LLDP.

Проверка конфигурации

Отобразите почтовый адрес LLDP локального устройства.

❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка почтового адреса устройства

Команда	Настройте почтовый адрес LLDP. Для удаления адреса используйте опцию **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*
Описание параметра	**country**: Код страны, состоящий из двух символов. RU обозначает Россию. **state**: Указывает CA тип 1. **county**: Указывает CA тип 2. **city**: Указывает CA тип 3. **division**: Указывает CA тип 4. **neighborhood**: Указывает CA тип 5. **street-group**: Указывает CA тип 6. **leading-street-dir**: Указывает CA тип 16. **trailing-street-suffix**: Указывает CA тип 17. **street-suffix**: Указывает CA тип 18. **number**: Указывает CA тип 19. **street-number-suffix**: Указывает CA тип 20. **landmark**: Указывает CA тип 21. **additional-location-information**: Указывает CA тип 22. **name**: Указывает CA тип 23. **postal-code**: Указывает CA тип 24. **building**: Указывает CA тип 25. **unit**: Указывает CA тип 26. **floor**: Указывает CA тип 27. **room**: Указывает CA тип 28. **type-of-place**: Указывает CA тип 29.

	postal-community-name: Указывает CA тип 30. **post-office-box**: Указывает CA тип 31. **additional-code**: Указывает CA тип 32. *ca-word*: Указывает адрес.
Режим команд	Режим настройки почтового адреса LLDP
Встроенная подсказка	После входа в режим настройки почтового адреса LLDP настройте почтовый адрес LLDP.

Удаление почтового адреса 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** }
Описание параметра	Недоступно
Режим команд	Режим настройки почтового адреса LLDP
Встроенная подсказка	После входа в режим настройки почтового адреса LLDP настройте почтовый адрес LLDP.

Настройка типа устройства

Команда	**device-type** *device-type*
Описание параметра	*device-type*: Указывает тип устройства. Диапазон значений от 0 до 2. Значение по умолчанию: 1. 0 указывает, что тип устройства — DHCP-сервер. 1 указывает, что тип устройства — коммутатор. 2 означает, что тип устройства — LLDP MED.
Режим команд	Режим настройки почтового адреса LLDP
Встроенная	После входа в режим настройки почтового адреса LLDP настройте тип

подсказка	устройства.

Восстановление типа устройства

Команда	**no device-type**
Описание параметра	Недоступно
Режим команд	Режим настройки почтового адреса LLDP
Встроенная подсказка	После входа в режим настройки почтового адреса LLDP восстановите настройки по умолчанию.

Пример конфигурации

Настройка почтового адреса устройства

Этапы конфигурации	Задайте адрес порта GigabitEthernet 0/1 следующим образом: Установите значение страны RU, города – Moscow, а почтового индекса – 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 конфигурации	Отобразите почтовый адрес LLDP порта GigabitEthernet 0/1 1.
	civic location information: --------------------------- Identifier :1 country :RU device type :1 city :Moscow postal-code :121471

12.4.14 Настройка номера телефона экстренной связи

Сценарий

❖ Настройте номер телефона экстренной связи устройства.

Этапы конфигурации

❖ Опционально.
❖ Выполните эту настройку в режиме глобальной конфигурации.

Проверка конфигурации

Отображение номера телефона экстренной связи на локальном устройстве

❖ Проверьте, действует ли конфигурация.

Связанные команды

Настройка номера телефона экстренной связи устройства

Команда	**lldp location elin identifier** *id* **elin-location** *tel-number*
Описание параметра	*id*: Указывает идентификатор номера телефона экстренной связи. Диапазон значений от 1 до 1024. *tel-number*: Указывает номер телефона экстренной связи, содержащий 10-25 символов.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Выполните эту команду, чтобы настроить номер телефона экстренной связи.

Удаление номера телефона экстренной связи устройства

Команда	**no lldp location elin identifier** *id*
Описание параметра	*id*: Указывает идентификатор номера телефона экстренной связи. Диапазон значений от 1 до 1024.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Пример конфигурации

Настройка номера телефона экстренной связи устройства

Этапы конфигурации	Установите номер телефона экстренной связи порта GigabitEthernet 0/1 на 085285555556.
	`QTECH#config` `QTECH(config)#lldp location elin identifier 1 elin-location 085283671111`
Проверка конфигурации	Отобразите номер телефона экстренной связи порта GigabitEthernet 0/1.

	`elin location information:`
	`-------------------------`
	`Identifier :1`
	`elin number :085283671111`

12.5 Мониторинг

Очистка

⚠ Выполнение команд **clear** может привести к потере важной информации и, следовательно, прерыванию работы служб.

Описание	Команда
Очищает статистику LLDP.	**clear lldp statistics** [**interface** *interface-name*]
Очищает информацию о соседе LLDP.	**clear lldp table** [**interface** *interface-name*]

Отображение

Описание	Команда
Отображает информацию LLDP на локальном устройстве, которая будет организована как набор TLV и отправлена соседним устройствам.	**show lldp local-information** [**global** | **interface** interface-name]
Отображает почтовый адрес LLDP или номер телефона для экстренной	**show lldp location** { **civic-location** | **elin-location** } { **identifier** *id* | **interface** *interface-name* | **static** }

связи на локальном устройстве.	
Отображает информацию LLDP о соседнем устройстве.	**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*]
Отображает конфигурацию TLV, объявленную портом.	**show lldp tlv-config** [**interface** *interface-name*]

Отладка

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

Описание	Команда
Отладка обработки ошибок LLDP.	**debug lldp error**
Отладка обработки событий LLDP.	**debug lldp event**
Отладка обработки горячего резервирования LLDP.	**debug lldp ha**
Отладка приема пакетов LLDP.	**debug lldp packet**
Отладка машины состояния LLDP.	**debug lldp stm**

13 НАСТРОЙКА QINQ

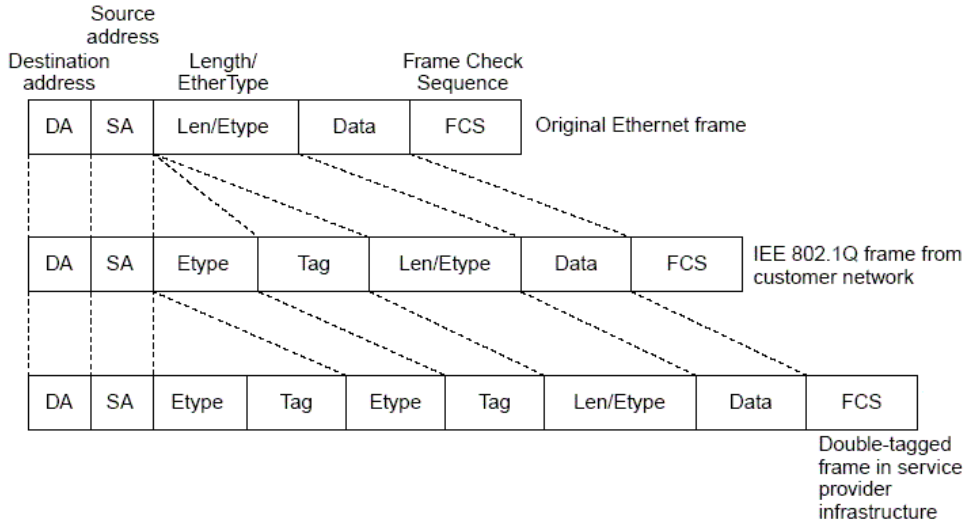
13.1 Обзор

QinQ используется для вставки тега общедоступной виртуальной локальной сети (VLAN) в пакет с частной меткой VLAN, чтобы разрешить передачу пакета с двойными метками по сети поставщика услуг (SP).

Пользователи в сети городских агломераций должны быть разделены сетями VLAN. IEEE 802.1Q поддерживает только 4094 виртуальных локальных сети (VLAN), что недостаточно. Благодаря инкапсуляции с двумя метками, предоставленной QinQ, пакет передается по сети поставщика услуг на основе уникального внешнего тега VLAN, назначенного общедоступной сетью. Таким образом, частные сети VLAN можно использовать повторно, что увеличивает количество доступных меток VLAN и предоставляет простую функцию виртуальной частной сети уровня 2 (VPN).

Изображение 13-1 показывает процесс инкапсуляции двойных меток. Вход в сеть поставщика услуг называется туннельным портом dot1q или просто туннельным портом. Все кадры, входящие в пограничные порты поставщика услуг (PE), считаются немаркированными. Все кадры с метками, будь то немаркированные кадры или кадры с пользовательскими метками VLAN, инкапсулируются с метками сети поставщика услуг. Идентификатор VLAN сети SP — это идентификатор VLAN по умолчанию для туннельного порта.

Изображение 13-1 Инкапсуляция внешней метки



Протоколы и стандарты

- IEEE 802.1ad

13.2 Применение

Применение	Описание

Внедрение VPN уровня 2 через Basic QinQ на основе портов	Данные передаются от клиента A и клиента B в одноранговый узел без конфликтов в сети поставщика услуг, даже если данные поступают из той же VLAN.
Внедрение VPN уровня 2 и управления потоком сервисов через Selective QinQ на основе C-TAG	Внешние метки инкапсулируются в фреймы гибко на основе различных виртуальных локальных сетей клиентов для обеспечения VPN уровня 2, разделения потоков услуг (например, широкополосного доступа в Интернет и IPTV) и реализации различных политик QoS. Технология QinQ на основе меток клиентов (C-TAG) более гибкая, чем QinQ на основе портов.
Внедрение VPN уровня 2 и управления потоком сервисов через Selective QinQ на основе ACL	Различные потоки услуг, такие как широкополосный доступ в Интернет и IPTV, разделяются на основе списков контроля доступа (ACL). Различные политики QoS применяются к сервисным потокам через Selective QinQ.
Внедрение агрегирования VLAN для различных служб через картирование VLAN	Различные потоки услуг (ПК, IPTV и VoIP) передаются по разным сетям VLAN. Сети VLAN объединяются в кампусную сеть, поэтому для передачи одних и тех же потоков обслуживания используется только одна VLAN, что позволяет экономить ресурсы.
Функция передачи данных VLAN-Translate по сетям VLAN	При настройке функции VLAN-Translate трафик может передаваться по двум сетям VLAN.
Реализация прозрачной передачи на уровне 2 на основе QinQ	Сеть заказчика A и сеть заказчика B в различных областях могут выполнять унифицированный расчет протокола MSTP или развертывание VLAN по сети поставщика услуг без влияния на сеть поставщика услуг.

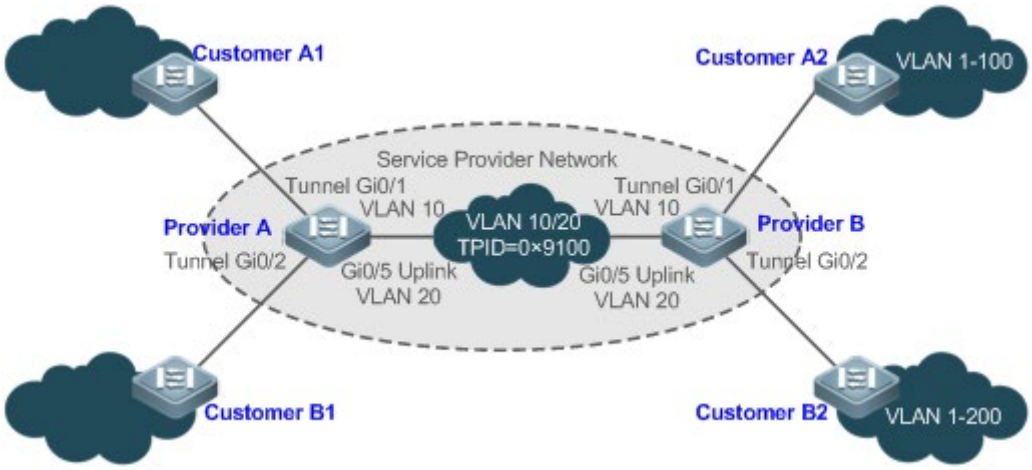
13.2.1 Внедрение VPN уровня 2 через Basic QinQ на основе порта

Сценарий

Поставщик услуг предоставляет сервис VPN заказчику A и заказчику B.

- Заказчики A и B принадлежат к разным сетям VLAN в сети поставщика услуг и обеспечивают связь через соответствующие сети VLAN поставщика услуг.
- Сети VLAN заказчика A и заказчика B прозрачны для сети поставщика услуг. Сети VLAN можно использовать повторно без конфликтов.
- Туннельный порт инкапсулирует метку DSP-процесса VLAN в каждый пакет. Пакеты передаются по DSP-сети VLAN через сеть поставщика услуг без воздействия на VLAN заказчика A и заказчика B, таким образом, внедряя простую VPN уровня 2.

Изображение 13-2



Заметки	Заказчик A1 и заказчик A2 — это границы клиентской сети (CE) для сети заказчика A. Заказчик B1 и заказчик B2 — это CE для сети заказчика B. Поставщики A и B являются PE в сети SP. Заказчик A и заказчик B получают доступ к сети поставщика услуг через поставщиков A и B. Сети VLAN заказчика A находятся в диапазоне от 1 до 100. Сети VLAN заказчика B находятся в диапазоне от 1 до 200.

Описание

- Включите Basic QinQ на PE для реализации VPN уровня 2.
- Идентификаторы протокола тегов (TPID), используемые многими коммутаторами (включая коммутаторы QTECH), установлены на 0x8100, но коммутаторы некоторых производителей не используют 0x8100. В последнем случае необходимо изменить значение TPID на портах восходящих каналов PE на значения TPID, используемые коммутаторами сторонних производителей.
- Настройте репликацию приоритетов и сопоставление по приоритетам для класса обслуживания (CoS) на туннельных портах PE и настройте различные политики QoS для различных потоков обслуживания (подробнее см. в разделе *Настройка QoS*).

13.2.2 Внедрение VPN уровня 2 и управления потоком сервисов через Selective QinQ на основе C-TAG

Сценарий

Basic QinQ инкапсулирует внешнюю метку DSP-сети VLAN в пакет. То есть, инкапсуляция внешних тегов зависит от DSP-сети VLAN на туннельных портах. Selective QinQ инкапсулирует внешнюю метку в пакет на основе внутренней метки, чтобы реализовать прозрачную передачу VPN и гибко применять политики QoS.

- Широкополосный доступ в Интернет и IPTV являются важными услугами, которые предоставляет городская агломерация. Поставщики услуг управляют различными сервисными потоками через различные сети VLAN и

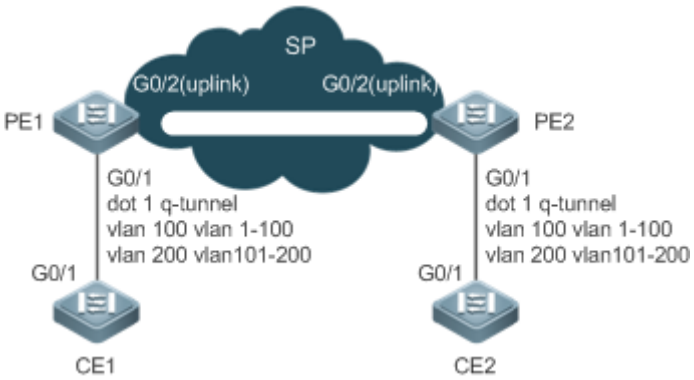
предоставляют политики QoS для сетей VLAN или CoS. Можно включить QinQ на основе C-TAG на PE для инкапсуляции внешних меток VLAN в сервисные потоки, чтобы обеспечить прозрачную передачу на основе политик QoS в сети SP.

- ❖ Важные службы и обычные службы разделены в пределах разных диапазонов VLAN. Клиент может прозрачно передавать потоки услуг по сети SP через Selective QinQ на основе C-TAG и обеспечивать предпочтительную передачу важных потоков услуг с помощью политик QoS в сети SP.

На Изображении 13-3 CE агрегируются коммутаторами на этажах внутри жилых зданий. Широкополосный доступ в Интернет и услуги IPTV разделяются сетями VLAN с различными политиками QoS.

- ❖ Потоки услуг широкополосного доступа в Интернет и IPTV прозрачно передаются различными сетями VLAN по сети SP.
- ❖ Сеть SP предоставляет политики QoS на основе сетей VLAN или CoS. На PE можно инкапсулировать внешнюю метку в потоке услуг на основе внутренней метки VLAN или задать CoS для обеспечения предпочтительной передачи сервисных потоков по сети SP.
- ❖ Значения CoS для пакетов услуг можно изменить с помощью сопоставления приоритетов или репликации, чтобы политики QoS в сети SP применялись гибко.

Изображение 13-3



Заметки	CE 1 и CE 2 получают доступ к сети SP через PE1 и PE2. На CE 1 и CE 2 потоки широкополосного доступа в Интернет передаются по VLAN 1–100, а потоки IPTV передаются по VLAN 101–200. PE 1 и PE 2 настроены с туннельными портами и привязками VLAN для разделения потоков услуг.

Описание

- ❖ Настройте Selective QinQ на основе C-TAG на портах (G0/1) PE 1 и PE 2, подключенных к CE 1 и CE 2, соответственно, для реализации разделения и прозрачной передачи потоков обслуживания.
- ❖ Если сеть SP предоставляет политики QoS на основе сетей VLAN или CoS, внешнюю метку можно инкапсулировать в сервисный поток на основе внутренней метки или задать CoS посредством репликации приоритетов или

привязки на PE 1 и PE 2, чтобы обеспечить предпочтительную передачу потоков услуг по сети SP.

13.2.3 Внедрение VPN уровня 2 и управления потоком сервисов через Selective QinQ на основе ACL

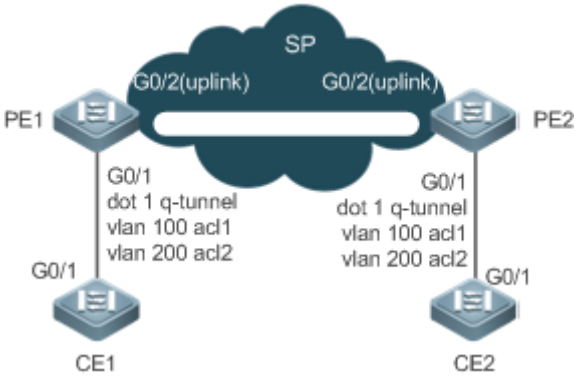
Сценарий

Потоки услуг из сети заказчика могут быть классифицированы по MAC-адресу, IP-адресу или типу протокола, а не по VLAN. Сеть заказчика может содержать множество низкокачественных устройств доступа, которые не могут разделять потоки услуг по идентификаторам VLAN. В двух предыдущих случаях пакеты из сети заказчика не могут быть инкапсулированы внешними метками на основе внутренних меток для обеспечения прозрачной передачи и реализации политик QoS. Потоки услуг могут быть классифицированы по MAC-адресу, IP-адресу или типу протокола через ACL. Selective QinQ использует ACL для разделения потоков услуг и добавления или изменения внешних меток для внедрения политик VPN и QoS уровня 2 на основе различных потоков услуг.

На Изображении 13-4 различные сети VLAN настраиваются на PE 1 и PE 2 для передачи различных потоков услуг, классифицированных через ACL. Если в сети поставщика услуг предусмотрены политики QoS, основанные на различных сервисах, некоторые сервисы имеют преимущественную передачу.

- Внешние метки VLAN инкапсулируются на основе различных потоков обслуживания. Сервисные потоки сети заказчика могут передаваться прозрачно с доступом филиалов друг к другу.
- Сеть SP предоставляет политики QoS на основе меток VLAN или значений CoS для обеспечения предпочтительной передачи определенных сервисных потоков.

Изображение 13-4



Заметки	CE 1 и CE 2 получают доступ к сети SP через PE1 и PE2. PE 1 и PE 2 классифицируют потоки на основе ACL: ACL-список 1 соответствует потокам протокола PPPoE (Point-to-Point Protocol over Ethernet), а ACL-список 2 соответствует потокам IPTV. PE 1 и PE 2 настроены с туннельными портами, а также политиками инкапсуляции внешних меток, применимыми к потокам услуг,

	распознаваемым различными ACL-списками.

Описание

- ❖ Настройте ACL-списки на PE 1 и PE 2 для разделения потоков обслуживания.
- ❖ Настройте Selective QinQ на основе ACL на портах (G0/1) PE 1 и PE 2, подключенных к CE 1 и CE 2, соответственно, для реализации разделения и прозрачной передачи потоков обслуживания.
- ❖ Если сеть SP предоставляет политики QoS на основе сетей VLAN или CoS, внешнюю метку можно инкапсулировать в сервисный поток на основе внутренней метки или задать CoS посредством репликации приоритетов или привязки на PE 1 и PE 2, чтобы обеспечить предпочтительную передачу потоков услуг по сети SP.

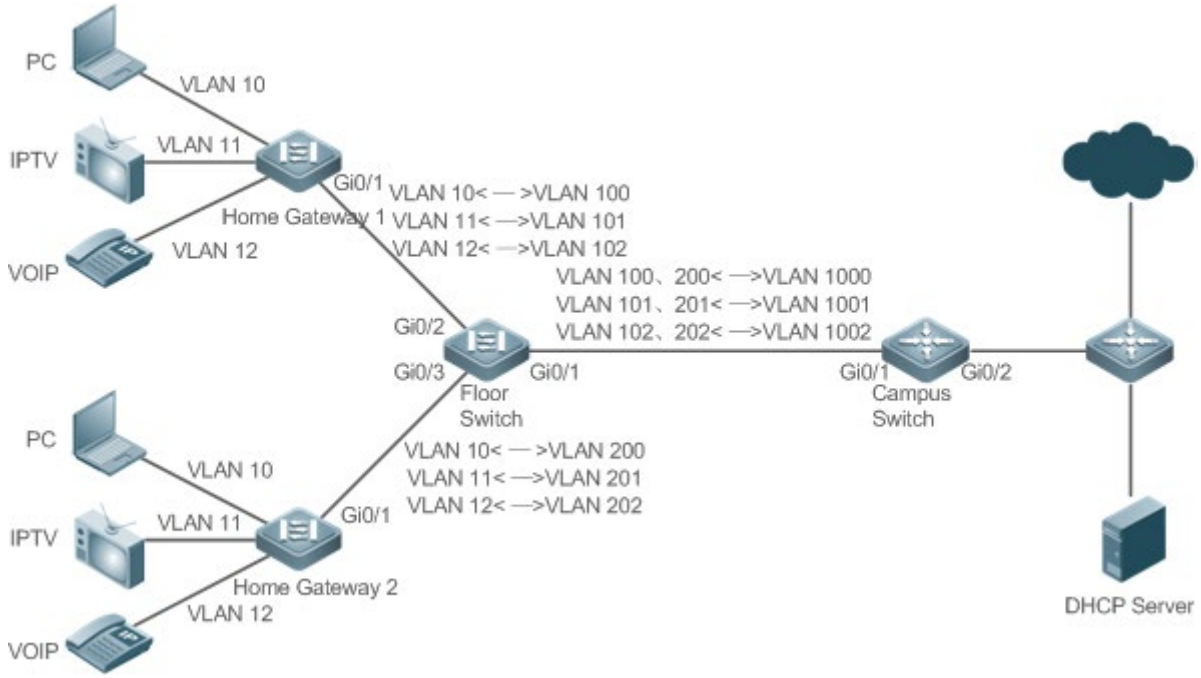
13.2.4 Внедрение агрегирования VLAN для различных служб через картирование VLAN

Сценарий

Различные сервисные потоки разных пользователей разделяются в кампусной сети.

- ❖ Различные сервисные потоки передаются через различные VLAN на домашнем шлюзе.
- ❖ Одни и те же сервисные потоки от разных пользователей разделяются на коммутаторе этажа.
- ❖ Одни и те же сервисные потоки от разных пользователей передаются коммутатором кампуса через одну VLAN.

Изображение 13-5



Заметки	ПК, IPTV и VoIP — это разные пользовательские сервисы.

	Коммутаторы A и B являются шлюзовыми устройствами разных пользователей. Коммутатор C - коммутатор этажа. Коммутатор D - коммутатор кампуса.

Описание

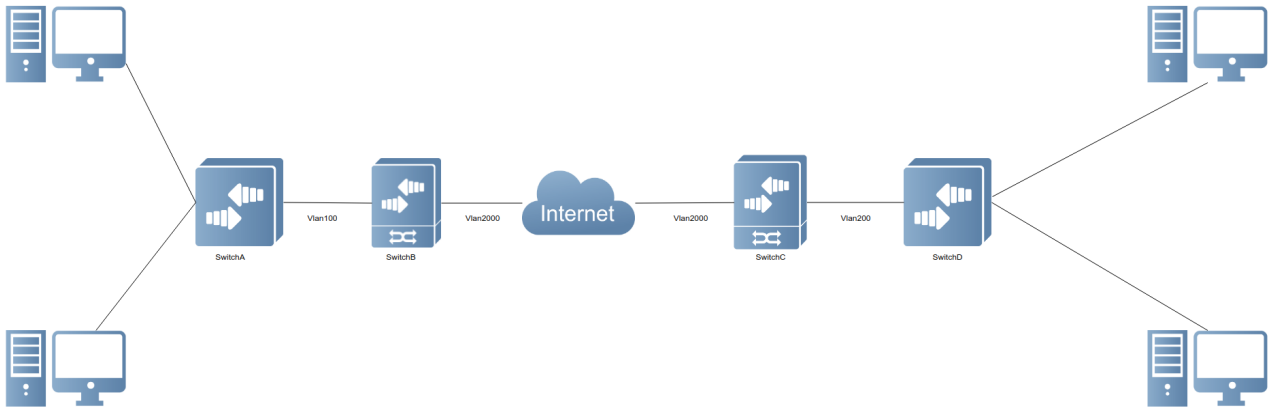
- На устройствах домашнего шлюза настройте сети VLAN для различных служб, чтобы разделить сервисные потоки. Например, настройте VLAN 10 для службы ПК, VLAN 11 для IPTV и VLAN 12 для VoIP.
- На портах коммутатора этажа (Switch C), подключенного к домашним шлюзам, настройте привязку VLAN для разделения сервисных потоков разных пользователей.
- На коммутаторе кампуса настройте привязку VLAN для разделения сервисных потоков.
- При предыдущем развертывании различные сервисные потоки разных пользователей разделяются.

13.2.5 Реализация передачи данных между VLAN

Сценарий

Трафик может проходить между двумя сетями VLAN путем настройки функции VLAN-Translate на коммутаторах поставщика услуг.

Изображение 13-6



Заметки	Коммутаторы A и B являются коммутаторами доступа. Коммутаторы B и C являются коммутаторами поставщика услуг.

Описание

- Существует две VLAN, где VLAN 100 работает в зоне A и VLAN 200 в зоне D.
- Выполните функцию VLAN-Translate на физических портах. Таким образом, при получении пакетов из VLAN 100 по сети SP в зоне D информация о VLAN меняется на VLAN 200 и наоборот.

❖ Такое развертывание делает возможным передачу данных между VLAN.

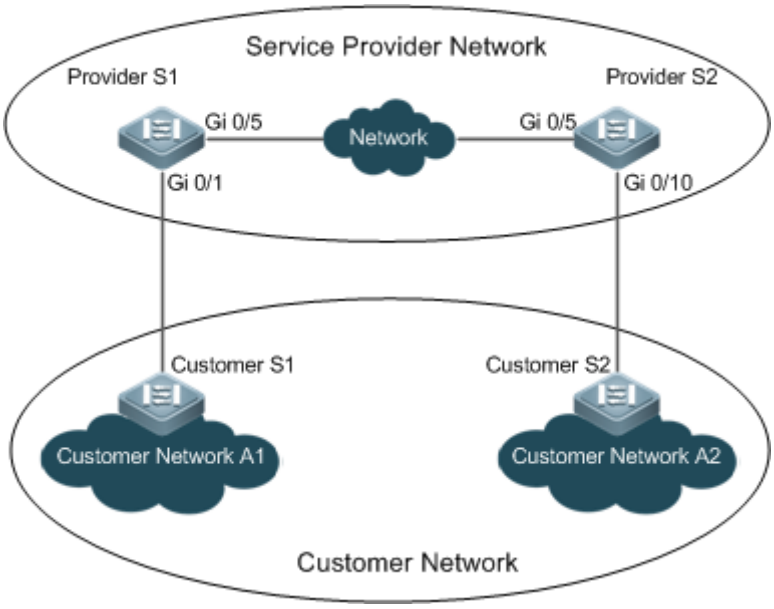
13.2.6 Реализация прозрачной передачи на уровне 2 на основе QinQ

Сценарий

Прозрачная передача данных уровня 2 между сетями заказчика не оказывает влияния на сеть поставщика услуг.

❖ Пакеты уровня 2 в сетях заказчика прозрачны для сетей SP и могут передаваться между сетями заказчика без воздействия на сети SP.

Изображение 13-7



Заметки	Заказчик S1 и заказчик S2 получают доступ к сети поставщика услуг через провайдера S1 и провайдера S2. Провайдер S1 и провайдер S2 предоставляют доступ с прозрачной передачей уровня 2 глобально, а порты Gi 0/1 и Gi 0/10 оперируют с прозрачной передачей уровня 2.

Описание

❖ На портах PE (провайдера S1 и провайдера S2), подключенных к заказчику S1 и заказчику S2 соответственно, настройте прозрачную передачу уровня 2 между сетью заказчика A1 и сетью заказчика A2 без воздействия на сеть поставщика услуг.

❖ Настройте прозрачную передачу STP на основе требований пользователя для обеспечения прозрачной передачи пакетов BPDU между сетью заказчика A1 и сетью заказчика A2 и выполнения унифицированного расчета MSTP по сети поставщика услуг.

❖ Настройте прозрачную передачу протокола GARP VLAN Registration Protocol (GVRP) в соответствии с требованиями пользователя, чтобы обеспечить прозрачную передачу пакетов GVRP между сетью заказчика A1 и сетью

заказчика A2 и динамическую конфигурацию VLAN в сетях заказчика во всей сети поставщика услуг.

13.3 Функции

Базовые концепции

Basic QinQ

Настройте Basic QinQ на туннельном порте и настройте DSP-сеть VLAN для порта. Пакеты, входящие в порт, инкапсулируются внешними метками, содержащими собственный идентификатор VLAN. Basic QinQ не разделяет сервисные потоки и не может гибко инкапсулировать пакеты на основе VLAN.

Selective QinQ

Selective QinQ классифицируется по двум типам: Selective QinQ на основе C-TAG и Selective QinQ на основе ACL.

В выборочной QinQ на основе C-TAG внешние метки инкапсулируются в пакеты на основе внутренних меток для разделения сервисных потоков и обеспечения прозрачной передачи.

В выборочной QinQ на основе ACL внешние метки инкапсулируются в пакеты, основанные на ACL-списках для разделения сервисных потоков.

TPID

Метка кадра Ethernet состоит из четырех полей: TPID, User Priority, Canonical Format Indicator (CFI) и VLAN ID.

По умолчанию TPID составляет 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых поставщиков значение TPID равно 0x9100 или другому значению. Конфигурация TPID предназначена для обеспечения совместимости TPID пакетов, которые будут пересылаться, с TPID, поддерживаемыми коммутаторами сторонних производителей.

Сопоставление приоритетов и репликация приоритетов

Значение приоритета пользователя в метках кадров Ethernet по умолчанию равно 0, что указывает на обычные потоки. Это поле можно установить для обеспечения предпочтительной передачи определенных пакетов. Можно указать приоритет пользователя, установив значение CoS в политике QoS.

Репликация приоритетов: Если в сети поставщика услуг предусмотрена политика QoS, соответствующая указанному CoS во внутренней метке, можно реплицировать CoS внутренней метки во внешнюю метку, чтобы обеспечить прозрачную передачу на основе политики QoS, предоставляемой сетью поставщика услуг.

Сопоставление приоритетов: Если в сети поставщика услуг предусмотрены различные политики QoS, соответствующие указанным значениям CoS для различных сервисных потоков, можно сопоставить значение CoS внутренней метки со значением CoS внешней метки, чтобы обеспечить преференциальную передачу сервисных потоков на основе политик QoS, предоставляемых сетью поставщика услуг.

Прозрачная передача уровня 2

Пакеты STP и GVRP могут повлиять на топологию сети поставщика услуг. Если требуется объединить топологию двух сетей заказчика, разделенных сетью поставщика услуг, не влияя на топологию сети поставщика услуг, передавайте пакеты STP и GVRP из сетей заказчика по сети поставщика услуг прозрачно.

Обзор

Функция	Описание
Basic QinQ	Настраивает туннельный порт и определяет, помечены ли пакеты, отправленные с порта.
Selective QinQ	Инкапсулирует различные внешние метки в потоки данных на основе ACL-списков.
VLAN mapping	Заменяет внутренние метки пакетов внешними метками, а затем восстанавливает внешние метки во внутренние, основываясь на тех же правилах.
VLAN-Translate	Передает пакеты между двумя VLAN.
Настройка TPID	По умолчанию TPID составляет 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых производителей идентификаторы TPID внешних меток устанавливаются на 0x9100 или другие значения. Конфигурация TPID предназначена для обеспечения совместимости TPID пакетов, которые будут пересылаться, с TPID, поддерживаемыми коммутаторами сторонних производителей.
Репликация MAC-адресов	В выборочной QinQ на основе ACL идентификаторы MAC VLAN-адресов, которым обучаются коммутаторы, принадлежат DSP-сети VLAN. Если преобразование VLAN осуществляется на основе ACL-списков, то при получении пакетов от одноранговой узла на конце линии связи локальный конец может не запросить MAC-адреса, что приведет к флуду. Для решения этой проблемы предоставляется репликация MAC-адресов для репликации MAC-адресов DSP-сети VLAN в VLAN, где расположена внешняя метка.
Прозрачная передача уровня 2	Передает пакеты уровня 2 между сетями заказчика без влияния на сети поставщика услуг.
Репликация приоритетов	Если в сети поставщика услуг предусмотрена политика QoS, соответствующая указанному CoS во внутренней метке, можно реплицировать CoS внутренней метки во внешнюю метку, чтобы обеспечить прозрачную передачу на основе политики QoS,

	предоставляемой сетью поставщика услуг.
Сопоставление приоритетов	Если в сети поставщика услуг предусмотрены различные политики QoS, соответствующие указанным значениям CoS для различных сервисных потоков, можно сопоставить значение CoS внутренней метки со значением CoS внешней метки, чтобы обеспечить преференциальную передачу сервисных потоков на основе политик QoS, предоставляемых сетью поставщика услуг.

13.3.1 Basic QinQ

Basic QinQ может использоваться для реализации простой VPN уровня 2, но ей не хватает гибкости при инкапсуляции внешних меток.

Принцип работы

После получения пакета через туннельный порт коммутатор добавляет в пакет внешнюю метку, содержащую идентификатор VLAN по умолчанию. Если полученный пакет уже содержит метку VLAN, он инкапсулируется как пакет с двойными метками. Если метка VLAN отсутствует, пакет добавляется вместе с меткой VLAN, содержащей идентификатор VLAN по умолчанию.

13.3.2 Selective QinQ

Функция выборочной QinQ позволяет гибко добавлять различные внешние метки к потокам данных.

Принцип работы

Selective QinQ может использоваться для инкапсуляции различных внешних меток на основе внутренних меток, MAC-адресов, номеров протоколов, адресов источника, адресов назначения, приоритетов или номеров портов приложений. Таким образом, пакеты различных пользователей, служб и приоритетов инкапсулируются с различными внешними метками VLAN.

Можно настроить следующие выборочные политики QinQ:

- Добавление внешней метки VLAN на основе внутренней метки VLAN.
- Изменение внешней метки VLAN на основе внешней метки VLAN.
- Изменение внешней метки VLAN на основе внутренней метки VLAN.
- Изменение внешней метки VLAN на основе внутренних и внешних меток VLAN.
- Добавление внешней метки VLAN на основе ACL-списка.
- Изменение внешней метки VLAN на основе ACL-списка.
- Изменение внутренней метки VLAN на основе ACL-списка.

13.3.3 VLAN mapping

Принцип работы

Внутренняя метка пакета заменяется внешней меткой, что позволяет передавать пакет на основе топологии общедоступной сети. Когда пакет передается в сеть клиента, внешняя метка восстанавливается в исходную внутреннюю метку на

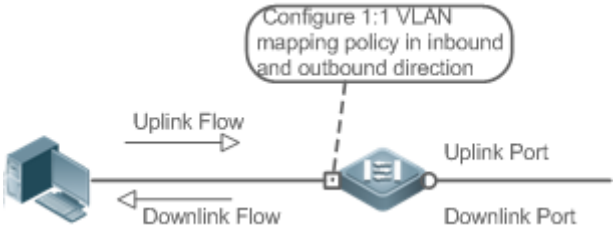
основе того же правила. VLAN mapping поддерживает следующие два правила сопоставления:

- VLAN mapping 1:1: Изменяет идентификатор VLAN на указанный идентификатор VLAN.
- VLAN mapping N:1: Изменяет несколько идентификаторов VLAN на указанный идентификатор VLAN.

Режим 1 сопоставления VLAN 1:1

VLAN mapping 1:1 в основном применяется к коммутаторам на этаже, чтобы использовать разные VLAN для передачи одних и тех же сервисов от разных пользователей, как показано на Изображении 13-8.

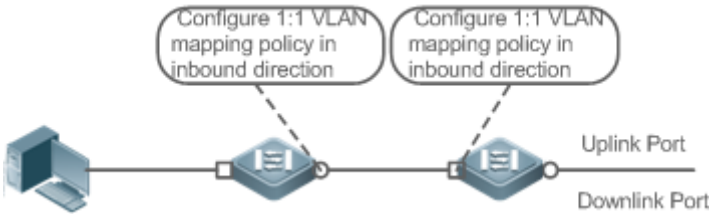
Изображение 13-8



- Настраивает порт нисходящего канала с помощью политики сопоставления VLAN во входящем направлении, чтобы связать внутреннюю метку восходящего потока с внешней меткой.
- Настраивает порт восходящего канала с помощью политики сопоставления VLAN в направлении исходящего трафика, чтобы сопоставить внешнюю метку нисходящего потока с исходной внутренней меткой.

Режим 2 сопоставления VLAN 1:1

Изображение 13-9

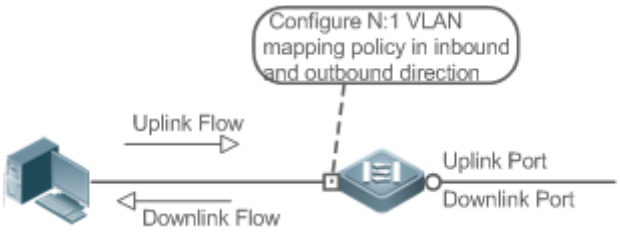


- Настраивает порт нисходящего канала с помощью политики сопоставления VLAN во входящем направлении, чтобы связать внутреннюю метку восходящего потока с внешней меткой.
- Для нисходящих потоков данных настраивает порт восходящего канала с помощью политики сопоставления VLAN в направлении входящего трафика, чтобы сопоставить внешнюю метку нисходящего потока с исходной внутренней меткой.

Режим сопоставления VLAN N:1

Режим сопоставления VLAN N:1 в основном применяется на кампусном коммутаторе для использования одной VLAN при передаче одной и той же службы из разных сетей VLAN, которые принадлежат разным пользователям, как показано на Изображении 13-10.

Изображение 13-10



- Настраивает порт восходящего канала с помощью политики сопоставления VLAN во входящем направлении, чтобы связать внутреннюю метку восходящего потока с внешней меткой.
- В настоящее время сопоставление нисходящих потоков VLAN не поддерживается.

13.3.4 VLAN-Translate

Принцип работы

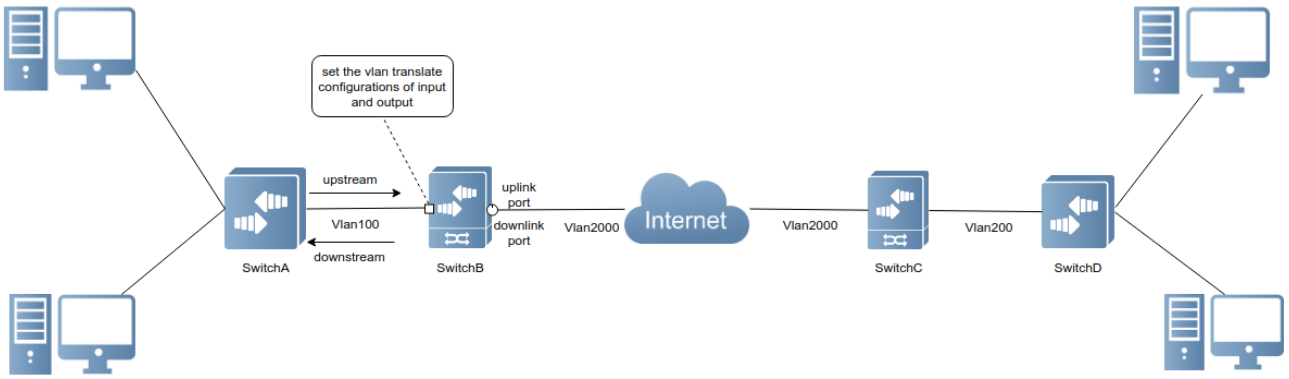
CVID и SVID пакетов заменяются или удаляются для облегчения обмена между VLAN. Поддерживаются следующие две модификации на основе меток:

- VLAN-Translate на входном порте: Заменяет исходный CVID указанным, затем добавляет SVID.
- VLAN-Translate на выходном порте: Заменяет исходный CVID указанным, а затем удаляет SVID.

VLAN-Translate на портах входа/выхода

VLAN-Translate развертывается на коммутаторах L2 для замены и удаления CVID и SVID пакетов, чтобы обеспечить возможность передачи между VLAN, как показано на Изображении 13-11.

Изображение 13-11



- Для восходящих данных политика VLAN-Translate развертывается на входном порту. Таким образом, CVID меток пакетов изменяется на указанный CVID, и добавляется назначенный SVID.
- Для нисходящего потока данных политика VLAN-Translate развертывается на выходном порту. Таким образом, CVID меток пакетов изменяется на указанный CVID, и SVID очищается.

13.3.5 Конфигурация TPID

Принцип работы

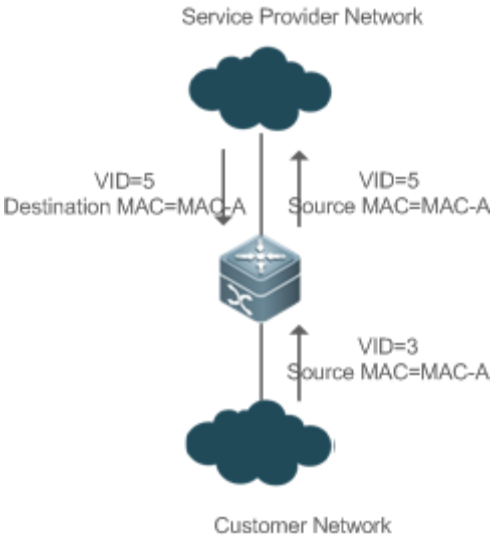
Метка кадра Ethernet состоит из четырех полей: TPID, User Priority, CFI и VLAN ID. По умолчанию TPID составляет 0x8100 в соответствии с IEEE802.1Q. На коммутаторах некоторых производителей идентификаторы TPID внешних меток устанавливаются на 0x9100 или другие значения. Функция конфигурации TPID позволяет настроить идентификаторы TPID на портах, которые заменят идентификаторы TPID внешних меток VLAN в пакеты с настроенными идентификаторами TPID для обеспечения совместимости с TPID.

13.3.6 Репликация MAC-адресов

Принцип работы

В выборочной QinQ на основе ACL MAC-адрес, полученный коммутатором, принадлежит DSP-сети VLAN. Туннельный порт помечает пакет указанным внешним идентификатором VLAN на основе выборочной политики QinQ. При получении ответного пакета, содержащего ту же внешнюю метку VLAN, туннельный порт не находит MAC-адрес во внешней VLAN, как это принято в DSP-сети VLAN, что вызывает флуд.

Изображение 13-12



Как и на Изображении 13-14, сеть заказчика подключена к туннельному порту коммутатора. В конфигурации с DSP-сетью VLAN 4 туннельный порт помечает пакет, чей MAC-адрес источника — A с внешней сетью VLAN 5. При получении пакета с внутренней меткой VLAN 3 и MAC-адресом источника A коммутатор помечает пакет внешней сетью VLAN 5. Поскольку порт настроен на DSP-сеть VLAN 4, VLAN 4 обучается MAC-адресу A. При получении ответного пакета коммутатор ищет MAC-адрес A в сети VLAN 5, так как внешняя метка пакета содержит идентификатор VLAN 5. Однако VLAN 5 не может обучаться MAC-адресу A, что приводит к флуду.

Можно настроить туннельный порт для репликации MAC-адреса DSP-сети VLAN во внешнюю VLAN, чтобы избежать непрерывного флуда пакетов из сети поставщика услуг. Кроме того, можно настроить туннельный порт для репликации MAC-адреса внешней VLAN для внешней метки в DSP-сеть VLAN, чтобы избежать непрерывного переполнения пакетов из клиентской сети.

13.3.7 Прозрачная передача уровня 2

Принцип работы

Функция прозрачной передачи уровня 2 предназначена для реализации передачи пакетов уровня 2 между сетями клиентов без воздействия на сети поставщика услуг. Когда пакет уровня 2 из клиентской сети поступает в PE, PE изменяет MAC-адрес назначения пакета на частный адрес перед пересылкой пакета. Одноранговый PE изменяет MAC-адрес назначения на общедоступный адрес, чтобы отправить пакет в сеть заказчика на другом конце, осуществляя прозрачную передачу в сети поставщика услуг.

13.3.8 Репликация приоритетов

Принцип работы

Если в сети поставщика услуг предусмотрена политика QoS, соответствующая указанному CoS во внутренней метке, можно реплицировать CoS внутренней метки во внешнюю метку, чтобы обеспечить прозрачную передачу на основе политики QoS, предоставляемой сетью поставщика услуг.

13.3.9 Сопоставление приоритетов

Принцип работы

Если в сети поставщика услуг предусмотрены различные политики QoS, соответствующие указанным значениям CoS для различных сервисных потоков, можно сопоставить значение CoS внутренней метки со значением CoS внешней метки, чтобы обеспечить преференциальную передачу сервисных потоков на основе политик QoS, предоставляемых сетью поставщика услуг.

13.4 Конфигурация

Конфигурация	Описание и команда	
Настройка QinQ	⚠ Обязательно.	
	switchport mode dot1q-tunnel	Настройка туннельного порта.
	switchport dot1q-tunnel allowed vlan { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }	Добавление сетей VLAN к туннельному порту в режиме с метками или без меток.
	switchport dot1q-tunnel native	Настраивает VLAN по умолчанию для туннельного

	vlan *VID*	порта.
Настройка Selective QinQ на основе C-TAG	⚠ (Обязательно) Используется для настройки Selective QinQ на основе C-TAG и базовой QinQ. Selective QinQ преобладает над базовой QinQ.	
	dot1q outer-vid *VID* **register inner-vid** *v_list*	Настраивает политику для добавления идентификаторов VLAN внешних меток на основе внутренних меток.
Настройка Selective QinQ на основе ACL	⚠ (Обязательно) Используется для настройки Selective QinQ на основе ACL и базовой QinQ. Selective QinQ преобладает над базовой QinQ.	
	traffic-redirect access-group *acl* **nested-vlan** *VID* **in**	Настраивает политику для добавления идентификаторов VLAN внешних меток на основе списков ACL.
Настройка сопоставления VLAN	⚠ (Обязательно) Используется для включения сопоставления VLAN.	
	vlan-mapping-in vlan *cvlan* **remark** *svlan*	Настраивает VLAN mapping 1:1 в направлении входящего трафика. Эта функция изменяет внутренний идентификатор VLAN пакета, вводя порт, на указанный внешний идентификатор VLAN.
	vlan-mapping-out vlan *svlan* **remark** *cvlan*	Настраивает VLAN mapping 1:1 в направлении исходящего трафика. Эта функция изменяет внешний идентификатор VLAN пакета, выходящего из порта, на указанный внутренний идентификатор VLAN.
	vlan-mapping-in vlan *cvlan-list* **remark** *svlan*	Настраивает VLAN mapping N:1 в направлении входящего трафика. Эта функция изменяет внутренний идентификатор VLAN пакета, вводя порт, на указанный внешний идентификатор

		VLAN.
Настройка TPID	⚠ (Дополнительно) Используется для реализации совместимости с TPID.	
	frame-tag tpid *tpid*	Настраивает TPID метки кадра. Если вы хотите установить значение 0x9100, настройте команду **frame-tag tpid 9100**. По умолчанию TPID имеет шестнадцатеричный формат. Эту функцию необходимо настроить на порту выхода.
Настройка репликации MAC-адресов	⚠ (Дополнительно) 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.
Настройка политики изменения меток внутренней/внешней VLAN	⚠ (Дополнительно) Используется для настройки внешних и внутренних меток VLAN пакетов, передаваемых по сетям поставщика услуг на основе топологий сети.	
	dot1q relay-vid *VID* **translate local-vid** *v_list*	Настраивает политику для изменения идентификаторов VLAN внешних меток на основе внешних меток.
	dot1q relay-vid *VID* **translate inner-vid** *v_list*	Настраивает политику для добавления идентификаторов VLAN внешних меток на основе внутренних меток.
	dot1q new-outer-vlan *VID* **translate old-outer-vlan vid inner-vlan** *v_list*	Настраивает политику для изменения идентификаторов VLAN внешних меток на основе внешних и внутренних меток.
	traffic-redirect access-group *acl* **outer-vlan** *VID* **in**	Настраивает политику для изменения идентификаторов VLAN внешних меток на

		основе ACL-списка.
	traffic-redirect access-group *acl* **inner-vlan** *VID* **out**	Настраивает политику для изменения идентификаторов VLAN внутренних меток на основе ACL-списка.
Настройка сопоставления приоритетов и репликации приоритетов	⚠ (Дополнительно) Используется для применения политики QoS, предоставляемой сетью поставщика услуг посредством репликации приоритетов.	
	inner-priority-trust enable	Копирует значение поля User Priority (Приоритет пользователя) во внутренней метке (C-TAG) в поле User Priority внешней метки (S-TAG).
	⚠ (Дополнительно) Используется для применения политики QoS, предоставляемой сетью поставщика услуг посредством сопоставления приоритетов.	
	dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*	Задает значение поля User Priority во внешней метке (S-TAG) на основе поля User Priority внутренней метки (C-TAG).
Настройка прозрачной передачи уровня 2	⚠ (Дополнительно) Используется для прозрачной передачи пакетов MSTP и GVRP на основе топологии сети заказчика без влияния на топологию сети поставщика услуг.	
	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}tunnel-dmac *mac-address*	Настраивает адрес прозрачной передачи.

- При настройке QinQ обратите внимание на следующие ограничения:
- Не настраивайте маршрутизируемые порты как туннельный порт.
- Не включайте 802.1X на туннельном порте.
- Не включайте функцию безопасности порта на туннельном порте.
- Если туннельный порт настроен в качестве исходного порта анализатора удаленного коммутируемого порта (RSPAN), отслеживаются пакеты, внешние метки которых содержат идентификаторы VLAN, соответствующие идентификаторам VLAN RSPAN.
- Если требуется сопоставить ACL-список, примененный к туннельному порту, с идентификаторами VLAN внутренних меток, используйте ключевое слово **inner**.
- Настройте выходной порт сети заказчика, подключенной к сети поставщика услуг, в качестве порта восходящего канала. При настройке TPID внешней метки на порту QinQ установите значение TPID внешней метки порта восходящего канала на то же значение.
- По умолчанию максимальный размер передаваемого пакета (MTU) для порта составляет 1500 байт. Пакет увеличивается на четыре байта после добавления с внешней меткой VLAN. Рекомендуется увеличить MTU порта в сетях поставщика услуг не менее чем до 1504 байт.
- После включения порта коммутатора с QinQ необходимо включить общий доступ SVGL перед включением отслеживания IGMP. В противном случае отслеживание IGMP не будет работать на порту с поддержкой QinQ.
- Если пакет соответствует двум или более избирательным политикам QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

13.4.1 Настройка QinQ

Сценарий

- Внедрение VPN уровня 2 на основе политики QinQ, применяемой к портам.

Примечание

- Не рекомендуется настраивать собственную VLAN порта внешней линии на PE в качестве VLAN по умолчанию, так как порт внешней линии отбрасывает метки, содержащие идентификаторы DSP-сети VLAN при отправке пакетов.

Этапы конфигурации

Настройка туннельного порта

- (Обязательно) Туннельный порт настраивается в режиме конфигурации интерфейса.
- Выполните команду **switchport mode dot1q-tunnel** в режиме конфигурации интерфейса для настройки туннельного порта.

Команда	**switchport mode dot1q-tunnel**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию туннельный порт не настроен.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Конфигурирование DSP-сети VLAN

- Обязательно.
- Настройте DSP-сеть VLAN для туннельного порта.
- После настройки DSP-сети VLAN добавьте ее в список VLAN туннельного порта в режиме без меток.
- Запустите команду **switchport dot1q-tunnel native vlan** *VID* в режиме конфигурации интерфейса, чтобы настроить VLAN по умолчанию для туннельного порта.
- Если DSP-сеть VLAN добавляется в список VLAN в режиме без меток, исходящие пакеты на туннельном порте не помечаются. Если собственная VLAN добавляется в список VLAN в режиме с метками, исходящие пакеты на туннельном порте помечаются собственным идентификатором VLAN. Чтобы обеспечить передачу восходящего и нисходящего каналов, добавьте DSP-сеть VLAN в список VLAN в режиме без меток.

Команда	**switchport dot1q-tunnel native vlan** *VID*
Описание параметра	*VID*: Указывает идентификатор DSP-сети VLAN. Диапазон значений от 1 до 4094. Значение по умолчанию: 1.
Установки по умолчанию	По умолчанию, DSP-сеть (нативная) VLAN - это VLAN 1.
Режим команд	Режим конфигурации интерфейса
Встроенная	Используйте эту команду для настройки VLAN сети поставщика услуг.

подсказка	

Добавление сетей VLAN в туннельный порт

- Обязательно.
- После настройки DSP-сети VLAN добавьте ее в список VLAN туннельного порта в режиме без меток.
- Если QinQ на основе портов включен, нет необходимости добавлять VLAN сети заказчика в список VLAN туннельного порта.
- Если включен режим выборочной QinQ, добавьте VLAN сети заказчика в список VLAN туннельного порта в режиме с метками или без меток в соответствии с требованиями.
- Запустите команду **switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* } в режиме конфигурации интерфейса, чтобы добавить VLAN в список VLAN туннельного порта. При получении пакетов из соответствующих сетей VLAN туннельный порт добавляет или удаляет метки в соответствии с настройками.

Команда	**switchport dot1q-tunnel allowed vlan** { [**add**] **tagged** *vlist* | [**add**] **untagged** *vlist* | **remove** *vlist* }
Описание параметра	*v_list*: Указывает список сетей VLAN на туннельном порте.
Установки по умолчанию	По умолчанию сеть VLAN 1 добавляется в список VLAN туннельного порта в режиме без меток. Другие VLAN не добавляются.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Используйте эту команду для добавления или удаления сетей VLAN на туннельном порте и укажите, помечены ли исходящие пакеты. Если включена Basic QinQ, добавьте DSP-сеть VLAN в список VLAN туннельного порта в режиме без метки.

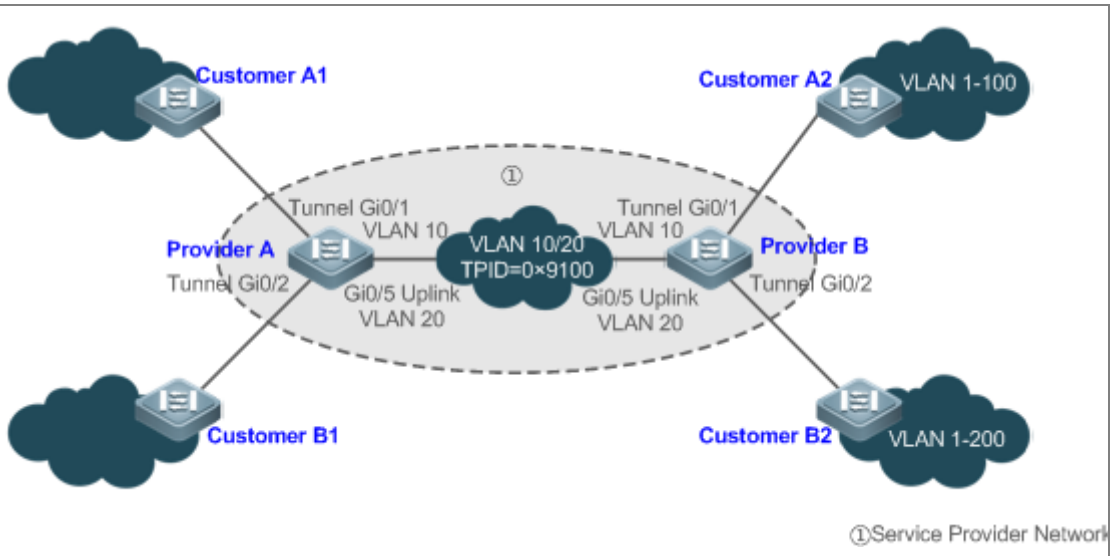
Проверка конфигурации

Проверьте конфигурацию туннельного порта.

- Проверьте, правильно ли настроен туннельный порт на коммутаторе.

Пример конфигурации

Настройка базовой QinQ для реализации VPN уровня 2

Сценарий Изображение 13-13	
Этапы конфигурации	❖ Настройте туннельный порт на PE и подключите CE к туннельным портам. ❖ Настройте нативные VLAN для туннельных портов и добавьте нативные VLAN в списки VLAN туннельных портов в режиме без метки. ❖ Настройте сети VLAN в сетях заказчика на основе требований. ℹ Коммутаторы с поддержкой QinQ инкапсулируют внешние метки в пакеты для передачи по сети поставщика услуг. Поэтому не нужно настраивать клиентские сети VLAN на PE. ℹ По умолчанию для IEEE802.1Q используется TPID 0x8100. На некоторых коммутаторах сторонних производителей для TPID установлено другое значение. Если такие коммутаторы используются в сети, настройте идентификаторы TPID на портах, подключенных к коммутаторам сторонних производителей, чтобы обеспечить совместимость с TPID. ⚠ Если PE подключены через магистральные или гибридные порты, не настраивайте DSP-сети VLAN для магистральных или гибридных портов в качестве VLAN по умолчанию для туннельных портов. Магистральные или гибридные порты при отправке пакетов отбрасывают метки VLAN, содержащие идентификаторы DSP-сети VLAN.

Поставщик A	❖ Шаг 1: Создайте VLAN 10 и VLAN 20 в сети поставщика услуг для разделения данных заказчика A и заказчика B.
	`ProviderA#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`ProviderA(config)#vlan 10`
	`ProviderA(config-vlan)#exit`
	`ProviderA(config)#vlan 20`
	`ProviderA(config-vlan)#exit`
	❖ Шаг 2: Включите Basic QinQ на порту, подключенном к сети

	заказчика 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 Basic QinQ на порту, подключенном к сети заказчика 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 порт восходящего потока.
	`ProviderA(config)# interface gigabitEthernet 0/5`
	`ProviderA(config-if-GigabitEthernet 0/5)#switchport mode uplink`
	Шаг 5: Измените TPID исходящих пакетов на порту восходящего потока на значение (например, 0x9100), распознаваемое коммутаторами сторонних производителей.
	`ProviderA(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100`
	Шаг 6: Настройте поставщика B, выполнив те же действия.

Проверка конфигурации	❖ Заказчик A1 отправляет пакет с идентификатором VLAN 100, предназначенным для заказчика A2. Пакет, проходящий через поставщика A, помечен внешней меткой, назначенной туннельным портом. Пакет, который достигает заказчика A2, содержит исходный идентификатор VLAN 100. ❖ Убедитесь, что туннельный порт настроен правильно. ❖ Проверьте правильность настройки TPID.

Поставщик 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
Поставщик B	❖ Настройте поставщика B, выполнив те же действия.

Типичные ошибки

- ❖ DSP-сеть VLAN не добавляется в список VLAN туннельного порта в режиме без меток.
- ❖ TPID не настроен на порту, подключенном к коммутатору стороннего производителя, где TPID отличен от 0x8100. В результате пакеты не могут быть распознаны коммутатором стороннего производителя.

13.4.2 Настройка Selective QinQна основе C-TAG

Сценарий

- ❖ Инкапсулирует внешние метки VLAN (S-TAG) в пакеты на основе внутренних меток, чтобы обеспечить предпочтительную передачу, управление VPN уровня 2 и сервисные потоки.

Примечания

- Selective QinQ на основе C-TAG должна быть настроена на основе базовой QinQ.
- Выборочные политики QinQ не поддерживаются некоторыми коммутаторами из-за ограничений чипов.
- Если необходимо продолжить использование приоритета меток VLAN, указанных сетью заказчика, можно настроить репликацию приоритетов для настройки внешней метки, такой же, как и для внутренней метки.
- Если для сети поставщика услуг требуется передача пакетов на основе приоритета внешней метки, необходимо настроить репликацию приоритетов, чтобы установить CoS внешней метки на указанное значение.

Этапы конфигурации

Настройка политики для добавления идентификаторов VLAN внешних меток на основе внутренних меток.

- Обязательно.
- При получении пакета туннельный порт добавляет идентификатор VLAN внешней метки на основе идентификатора VLAN внутренней метки. Эта функция позволяет туннельному порту добавлять идентификатор VLAN внутренней метки во внешнюю метку и добавляет порт в VLAN в режиме без меток. Таким образом, исходящие пакеты имеют исходные внутренние метки.

Политика QinQ, основанная на ACL, имеет приоритет над политикой QinQ, основанной на портах и C-TAG.

При добавлении или удалении порта участника из агрегированного порта (LAG) политика QinQ, настроенная на агрегированном порте, будет удалена. Необходимо снова настроить политику. Рекомендуется настроить выборочную политику QinQ на агрегированном порте после настройки его портов-участников.

Необходимо настроить туннельный порт и порт, подключенный к публичной сети, чтобы разрешить прохождение пакетов с указанными идентификаторами VLAN (включая собственный идентификатор VLAN) во внешней метке.

Команда	**dot1q outer-vid** *VID* **register inner-vid** *v_list*
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса
Встроенная	Недоступно

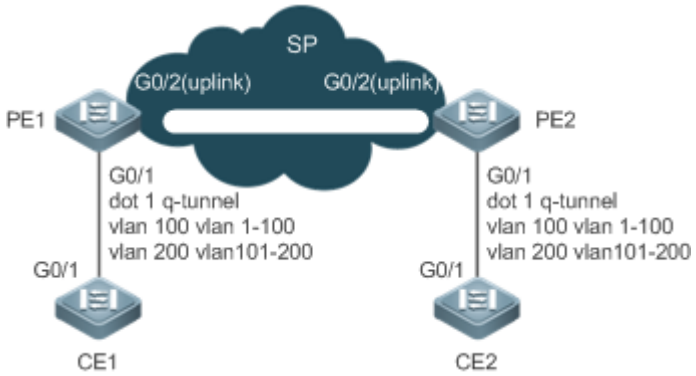
подсказка	

Проверка конфигурации

- ❖ Проверьте, могут ли пользователи в сетях VLAN обмениваться данными друг с другом.
- ❖ Проверьте, реализована ли сеть VPN уровня 2.
- ❖ Проверьте, передается ли различный сервисный трафик на основе выборочной политики QinQ, например, вставка внешних тегов, репликация приоритетов и сопоставление приоритетов.

Пример конфигурации

Внедрение VPN уровня 2 и управления потоком сервисов через выборочный QinQ на основе C-TAG

Сценарий Изображение 13-14	
Этапы конфигурации	❖ Настройте порты PE 1 и PE 2, подключенные к CE 1 и CE 2, как туннельные порты. ❖ Настройте выборочную политику QinQ, чтобы добавить внешнюю метку в пакет на основе внутренней метки. ❖ Если в сети поставщика услуг предусмотрена политика QoS на основе VLAN, политика позволяет порту добавлять внешние метки с соответствующим идентификатором VLAN к указанным пакетам сервисных потоков. ❖ Если в сети поставщика услуг предусмотрена политика QoS на основе CoS, а значение CoS совпадает со значением внутренней метки, можно настроить сопоставление приоритетов для репликации значения CoS внутренней метки во внешнюю метку VLAN так, чтобы пакет передался на основе политики приоритета внутренней метки. ❖ Если в сети поставщика услуг предусмотрена политика QoS на основе CoS, можно настроить сопоставление приоритетов, чтобы установить значение CoS внешней метки VLAN на заданное значение, чтобы пакет передался на основе приоритета политики.
PE1	❖ Шаг 1: Настройте VLAN для прозрачной передачи. `PE1#configure terminal`

	Enter configuration commands, one per line. End with CNTL/Z. PE1(config)#vlan 100 PE1(config-vlan)#exit PE1(config)#vlan 200 PE1(config-vlan)#exit ❖ Шаг 2: На порту нисходящего канала коммутатора доступа настройте избирательную политику QinQ для добавления внешних меток на основе внутренних меток. ❖ 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 поставщика услуг в список VLAN туннельного порта и настройте туннельный порт на фильтрацию внешней метки от входящих пакетов. PE1(config-if)# switchport dot1q-tunnel allowed vlan add untagged 100,200 ❖ Настройте туннельный порт для добавления внешней метки VLAN 100 к входящим кадрам данных, содержащим внутреннюю метку VLAN 1–100. PE1(config-if)# dot1q outer-vid 100 register inner-vid 1-100 ❖ Настройте туннельный порт для добавления внешней метки VLAN 200 к входящим кадрам данных, содержащим внутреннюю метку VLAN 101–200. PE1(config-if)# dot1q outer-vid 200 register inner-vid 101-200 ❖ Шаг 3: Настройте порт, через который осуществляется доступ к сети поставщика услуг, как порт восходящего канала. PE1(config)# interface gigabitEthernet 0/2 PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink
PE2	❖ Выполните аналогичную настройку на PE 2.
Проверка конфигурации	❖ Подтвердите конфигурацию, проверив: ❖ Порт нисходящего канала настроен как туннельный порт. ❖ VLAN, указанная внешней меткой, добавляется в список VLAN туннельного порта. ❖ В туннельном порту используется правильная политика выборочной QinQ. ❖ Порт восходящего канала настроен правильно. ❖ Шаг 1: Проверьте правильность политики сопоставления VLAN.
PE1	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 выборочную политику QinQ на основе C-TAG. Проверьте правильность связи между внутренней и внешней меткой 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
```

13.4.3 Настройка Selective QinQна основе ACL

Сценарий

❖ Инкапсулирует внешние метки VLAN (S-TAG) в пакеты на основе классификации потоков посредством ACL, чтобы позволить сети поставщика услуг управлять различными службами.

Примечания

❖ Selective QinQ на основе ACL должна быть настроена на основе базовой QinQ.
❖ Выборочные политики QinQ не поддерживаются некоторыми коммутаторами из-за ограничений чипов.
❖ Если необходимо продолжить использование приоритета меток VLAN, указанных сетью заказчика, можно настроить репликацию приоритетов для настройки внешней метки, такой же, как и для внутренней метки.
❖ Если для сети поставщика услуг требуется передача пакетов на основе приоритета внешней метки, необходимо настроить репликацию приоритетов, чтобы установить CoS внешней метки на указанное значение.

Политика QinQ, основанная на ACL, имеет приоритет над политикой QinQ, основанной на портах и C-TAG.

При удалении ACL-списка соответствующая политика будет автоматически удалена.

При получении пакета с двумя или более метками туннельный порт не может добавить внешнюю метку в пакет на основе политики QinQ, основанной на ACL.

Если пакет соответствует двум или более избирательным политикам QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

Необходимо настроить туннельный порт и порт, подключенный к публичной сети, чтобы разрешить прохождение пакетов с указанными идентификаторами VLAN (включая собственный идентификатор VLAN) во внешней метке.

Этапы конфигурации

Настройка политики для добавления идентификаторов VLAN внешних меток на основе ACL-списков

- Обязательно.
- Туннельный порт добавляет внешние метки с разными идентификаторами VLAN к входящим пакетам на основе содержимого пакета.

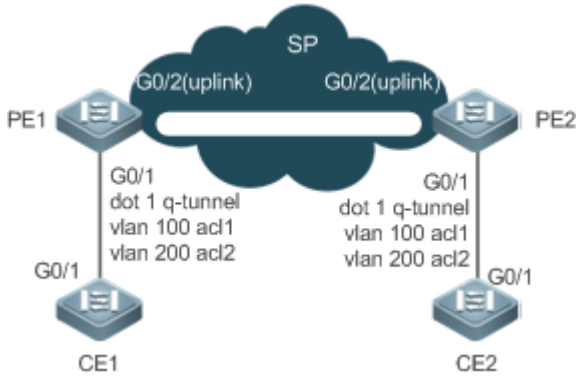
Команда	**traffic-redirect access-group** *acl* **nested-vlan** *VID* **in**
Описание параметра	Недоступно
Установки по умолчанию	По умолчанию политика не добавляется.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

- Проверьте, могут ли пользователи одной и той же службы в разных филиалах взаимодействовать друг с другом, и передаются ли указанные сервисные данные преимущественно через конфигурацию сегмента виртуальной частной локальной сети (VPLS).
- Проверьте, реализована ли сеть VPN уровня 2.
- Проверьте, передается ли различный сервисный трафик на основе выборочной политики QinQ, например, вставка внешних тегов, репликация приоритетов и сопоставление приоритетов.

Пример конфигурации

Внедрение VPN уровня 2 и управления потоком сервисов через выборочный QinQ на основе ACL

Сценарий Изображение 13-15	
Этапы конфигурации	❖ Настройте порты 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 услуг от сети заказчика. ❖ На туннельных портах настройте выборочную политику QinQ, чтобы добавить внешнюю метку в пакет на основе политик ACL. ❖ Если в сети поставщика услуг предусмотрена политика QoS на основе VLAN, эта политика позволяет порту добавлять соответствующий идентификатор VLAN во внешние метки указанного сервисного потока. ❖ Если в сети поставщика услуг предусмотрена политика QoS на основе CoS, можно настроить сопоставление приоритетов, чтобы установить значение CoS внешней метки VLAN на заданное значение, чтобы пакет передался на основе приоритета политики.

PE 1	Шаг 1: Создайте ACL-список, чтобы разрешить пропуск потоков PPPoE типа 0x8863/0x8864 и IPoE типа 0x0800.
	`PE1#configure terminal`
	`Enter configuration commands, one per line.  End with 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 поставщика услуг для разделения данных.
	`PE#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`PE1(config)#vlan 100`
	`PE1(config-vlan)#exit`

	PE1(config)#vlan 200 PE1(config-vlan)#exit Шаг 3: На порту нисходящего канала коммутатора доступа настройте политику Selective QinQдля добавления внешних меток VLAN на основе 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 поставщика услуг в список VLAN туннельного порта и настройте туннельный порт на фильтрацию внешней метки от входящих пакетов. PE1(config-if)#switchport dot1q-tunnel allowed vlan add untagged 100,200 Настройте туннельный порт для добавления внешней метки 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 для добавления внешней метки 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 поставщика услуг, в качестве порта восходящего канала. PE1(config)# interface gigabitEthernet 0/2 PE1(config-if-GigabitEthernet 0/2)#switchport mode uplink
Проверка конфигурации	Проверьте, могут ли пользователи одной и той же службы в разных филиалах взаимодействовать друг с другом и передаются ли указанные сервисные данные в преимущественном порядке. ❖ Проверьте, реализована ли сеть VPN уровня 2. ❖ Проверьте правильность ACL. ❖ Проверьте правильность приоритета сервисного потока. ❖ Проверьте, настроен ли порт нисходящего канала как туннельный порт, добавлена ли внешняя метка VLAN в список VLAN туннельного порта, и правильно ли задана политика сопоставления на туннельном порте.
PE1	Шаг 1: Убедитесь, что туннельный порт настроен правильно. 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 QinQна основе ACL. Проверьте правильность связи между внутренней и внешней меткой VLAN.

```
PE1#show traffic-redirect
Ports        Type            VID     Match-filter
-------    ----------     -----    ------------
Gi0/1        Nested-vid    101         acl1
Gi0/1        Nested-vid    201         acl2
```

Типичные ошибки

- Политика ACL не настроена.
- Политики ACL используются для разделения потоков на основе MAC-адресов. Если репликация MAC-адресов не настроена, произойдет переполнение пакетов.

13.4.4 Настройка сопоставления VLAN

Сценарий

- Замените внутренние метки пакетов внешними метками, чтобы разрешить передачу пакетов на основе планирования VLAN в сети поставщика услуг.

Примечания

- VLAN mapping может быть настроено только на портах доступа, магистральных портах, гибридных портах или портах восходящего канала.

⚠ После настройки сопоставления VLAN идентификаторы VLAN пакетов, отправленных на ЦП, изменяются на указанный идентификатор VLAN.

⚠ Не рекомендуется настраивать VLAN mapping и Selective QinQ на одном порту.

Этапы конфигурации

Настройте VLAN mapping 1:1

- Обязательно, если используется режим 1:1. Настройте правило сопоставления VLAN 1:1.
- Выполните команду **vlan-mapping-in vlan** *CVID* **remark** *SVID* или команду **vlan-mapping-out vlan** *SVID* **remark CVID** на магистральном порте или порте восходящего канала, чтобы включить VLAN mapping 1:1.

Команда	**vlan-mapping-in vlan** *src-vlan-list* **remark** *dest-vlan*

Описание параметра	*src-vlan-list*: Указывает VLAN заказчика *dest-vlan:* Указывает сервисную VLAN, которая является виртуальной локальной сетью, в которой находится сеть поставщика услуг.
Установки по умолчанию	
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Эта команда используется для настройки сопоставления VLAN 1:1 во входящем направлении.

Команда	**vlan-mapping-out vlan** *src-vlan* **remark** *dest-vlan*
Описание параметра	*src-vlan*: Указывает сервисную VLAN, которая является виртуальной локальной сетью, в которой находится сеть поставщика услуг. *dest-vlan*: Указывает VLAN заказчика
Установки по умолчанию	
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Используйте эту команду для настройки сопоставления VLAN 1:1 в исходящем направлении.

Настройка сопоставления VLAN 1:1

- Обязательно, если используется режим N:1. Настройте правило сопоставления VLAN N:1.
- Запустите команду **vlan-mapping-in vlan** *CVID-LIST* **remark** *SVID* на магистральном порте или порте восходящего канала, чтобы включить VLAN mapping N:1.
- Значения *CVID*, *CVID-LIST* и *SVID* находятся в указанном диапазоне VLAN.

Команда	**vlan-mapping-in vlan** *src-vlan-list* **remark** *dest-vlan*
Описание	*src-vlan-list*: Указывает список VLAN, содержащий несколько клиентских

параметра	VLAN. *dest-vlan:* Указывает сервисную VLAN, которая является виртуальной локальной сетью, в которой находится сеть поставщика услуг.
Установки по умолчанию	
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

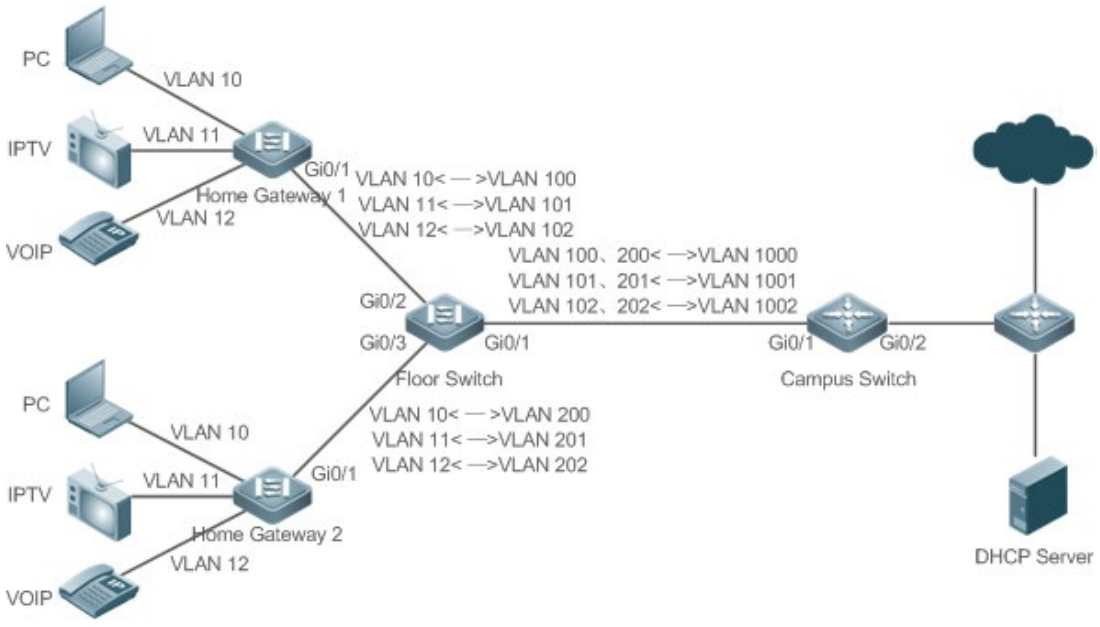
Проверка конфигурации

Проверьте правильность настройки сопоставления VLAN.

- Запустите команду **show interfaces**[*intf-id*] **vlan-mapping** для отображения сопоставления VLAN.

Пример конфигурации

Внедрение агрегирования VLAN для различных служб через картирование VLAN

Сценарий Изображение 13-16	
Этапы конфигурации	❖ Настройте шлюз Home Gateway 1 и шлюз Home Gateway 2. Шаг 1: На домашних шлюзах настройте исходные сети VLAN для различных служб. `QTECH#configure terminal`

```
Enter configuration commands, one per line.  End with CNTL/Z.
QTECH(config)#vlan range 10-12
QTECH(config-vlan-range)#exit
```

Шаг 2: Настройте Настройки 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 порт восходящего потока.

```
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 служб.

```
QTECH#configure terminal
Enter configuration commands, one per line.  End with 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 порту нисходящего канала домашнего шлюза 1 настройте политики сопоставления VLAN 1:1 в направлении входящего и исходящего трафика.

```
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 порту нисходящего канала домашнего шлюза 2 настройте политики сопоставления VLAN 1:1 в направлении входящего и исходящего трафика.

```
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 порт восходящего потока.

```
QTECH(config)# interface gigabitEthernet 0/1
QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink
```

❖ Настройте кампусный коммутатор с политиками сопоставления VLAN N:1.

Шаг 1: Настройте все используемые VLAN, включая исходные VLAN и сопоставленные VLAN.

```
QTECH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
QTECH(config)#vlan range 100-102
QTECH(config-vlan-range)#exit
QTECH(config)#vlan range 200-202
QTECH(config-vlan-range)#exit
QTECH(config)#vlan range 1000-1002
QTECH(config-vlan-range)#exit
```

Шаг 2: На порту нисходящего канала сопоставьте VLAN для различных служб с VLAN.

```
QTECH(config)#interface gigabitEthernet 0/1
```

```
QTECH(config-if-GigabitEthernet 0/1)#switchport mode uplink
QTECH(config-if-GigabitEthernet 0/1)#vlan-mapping-in vlan 100 200 remark 1000
QTECH(config-if-GigabitEthernet 0/1)#vlan-mapping-in vlan 101 201 remark 1001
QTECH(config-if-GigabitEthernet 0/1)#vlan-mapping-in vlan 102 202 remark 1002
```

Шаг 3: Настройте порт восходящего потока.

```
QTECH(config)# interface gigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)#switchport mode uplink
```

(Дополнительно) Шаг 4: Включите отслеживание DHCP.

```
QTECH(config)# ip dhcp snooping
```

(Дополнительно) Шаг 5: Настройте порт, подключенный к серверу поставщика услуг, как доверенный порт.

```
QTECH(config)# interface gigabitEthernet 0/2
QTECH(config-if-GigabitEthernet 0/2)#ip dhcp snooping trust
```

Проверка конфигурации

❖ Отобразите политики сопоставления VLAN 1:1, настроенные на этажном коммутаторе.

```
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
```

❖ Отобразите политики сопоставления VLAN N:1, настроенные на коммутаторе комплекса зданий.

```
QTECH#show interfaces vlan-mapping
Ports        type   Status     Service-Vlan   Customer-Vlan-list
-----------  -----  ---------  -----------    ----------------
Gi0/1        in     active     1000           100,200
```

	Gi0/1	in	active	1001	101,201
	Gi0/1	in	active	1002	102,202

13.4.5 Настройка VLAN-Translate

Сценарий

- Включите функцию VLAN-Translate на коммутаторах поставщика услуг, чтобы облегчить передачу данных между двумя сетями VLAN.

Примечания

- Политика VLAN-Translate должна быть развернута на портах L3 с назначенными VLAN.

Этапы конфигурации

Настройка VLAN-Translate

- Обязательно.
- Конфигурация должна работать в режиме настройки интерфейса.
- Функция VLAN-Translate должна быть включена на портах, где была исполнена команда **switchport mode dot1q-tunnel**.

Связанные команды

Настройка VLAN-Translate на входящем порту

Команда	**vlan-translate-in old-cvid** *old-cvid* **remark new-cvid** *new-cvid* **svid** *svid*
Описание параметра	*old-cvid*: Указывает старый CVID. *new-cvid*: Указывает новый CVID. *svid*: Указывает новый SVID.
Установки по умолчанию	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка VLAN-Translate на исходящем порту

Команда	**vlan-translate-out old-svid** *old-svid* **old-cvid** *old-cvid* **remark new-vid** *vid*
Описание	*old-cvid*: Указывает старый SVID.

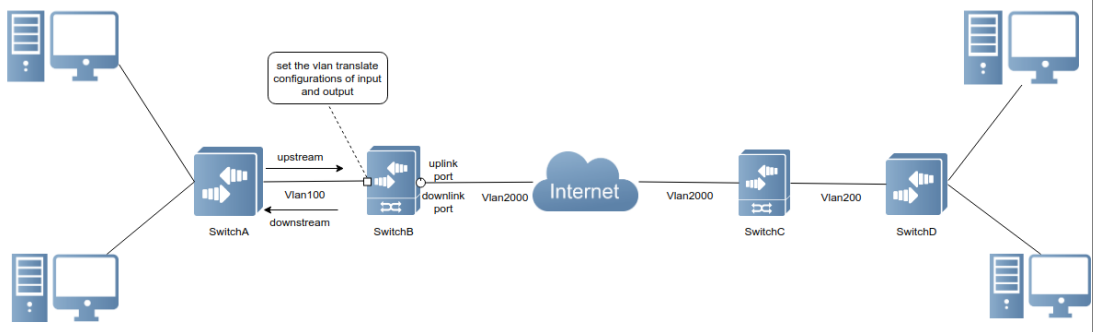
параметра	*new-cvid*: Указывает старый CVID. *vid*: Указывает новый VID.
Установки по умолчанию	Недоступно
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

Проверьте, правильно ли настроена функция VLAN-Translate.

Пример конфигурации

Настройка VLAN-Translate

Сценарий Изображение 13-17	

Этапы конфигурации	❖ Настройте VLAN-Translate на входном порте коммутатора B. Таким образом, после передачи пакетов через коммутатор B их CVID изменяется с 100 на 200, что позволяет им передавать на коммутатор D через VLAN 200.
	❖ Настройте VLAN-Translate на выходном порте коммутатора B. Таким образом, после передачи пакетов через коммутатор B их CVID изменяется с 200 на 100, что позволяет ему передавать на коммутатор A через VLAN 100.
	Настройте VLAN-Translate на входящем порту.
	`SwitchB#configure`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`SwitchB(config)#interface tenGigabitEthernet 0/13`

	SwitchB(config-if-TenGigabitEthernet 0/13)#vlan-translate-in old-cvid 100 remark new-cvid 200 svid 2000 Настройте VLAN-Translate на исходящем порту. SwitchB#configure Enter configuration commands, one per line. End with CNTL/Z. SwitchB(config)#interface tenGigabitEthernet 0/13 SwitchB(config-if-TenGigabitEthernet 0/13)# vlan-translate-out old-svid 2000 old-cvid 200 remark new-vid 100
Проверка конфигурации	❖ Отобразите VLAN-Translate на входном порту. SwitchB(config-if-TenGigabitEthernet 0/13)#show this Building configuration... ! switchport mode dot1q-tunnel vlan-translate-in old-cvid 100 remark new-cvid 200 svid 2000 spanning-tree bpdufilter enable ! end SwitchB(config-if-TenGigabitEthernet 0/13)# ❖ Отобразите VLAN-Translate на выходном порте. SwitchB(config-if-TenGigabitEthernet 0/13)#show this Building configuration... ! switchport mode dot1q-tunnel vlan-translate-out old-svid 2000 old-cvid 200 remark new-vid 100 spanning-tree bpdufilter enable ! end SwitchB(config-if-TenGigabitEthernet 0/13)#

13.4.6 Настройка TPID

Сценарий

❖ Настройте идентификаторы TPID в метках на сетевых устройствах поставщика услуг, чтобы обеспечить совместимость с TPID.

Примечания

❖ Если PE подключен к коммутатору стороннего производителя, на котором TPID не 0x8100, необходимо настроить TPID на порту PE, подключенном к коммутатору стороннего производителя.

⚠ Не задавайте значения TPID ни на одно 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).

Этапы конфигурации

- Если PE подключен к коммутатору стороннего производителя, на котором TPID не 0x8100, необходимо настроить TPID на порту PE, подключенном к коммутатору стороннего производителя.
- 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. Подробнее о значении TPID см. в разделе 1.4.5.

Команда	**frame-tag tpid** *tpid*
Описание параметра	*tpid:* Указывает новое значение TPID.
Установки по умолчанию	Значение TPID по умолчанию — 0x8100.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Если PE подключен к коммутатору стороннего производителя, на котором TPID не 0x8100, используйте эту команду для настройки TPID на порту, подключенном к коммутатору стороннего производителя.

Проверка конфигурации

Проверьте, настроен ли TPID.

Пример конфигурации

Настройка TPID на порту

Этапы конфигурации	❖ Настройте TPID на порту.
	`QTECH(config)# interface gigabitethernet 0/1`
	`QTECH(config-if)# frame-tag tpid 9100`

Проверка конфигураци	❖ Отобразите TPID на порту. `QTECH# show frame-tag tpid interfaces gigabitethernet 0/1`

и	Port tpid ------- ------------- Gi0/1 0x9100

13.4.7 Настройка репликации MAC-адресов

Сценарий

- ❖ Реплицируйте динамический адрес, полученный на порту из одной VLAN в другую.
- ❖ Избегайте флуда пакетов при разделении сервисных потоков через списки ACL на основе MAC-адресов.

Примечания

- После отключения репликации MAC-адресов система удалит все введенные MAC-адреса из целевой VLAN.
- Репликация MAC-адресов может быть настроена на порту только один раз. Если необходимо изменить конфигурацию, удалите текущую конфигурацию и настройте ее снова.
- Репликация MAC-адресов VLAN не может использоваться совместно с общим доступом к VLAN, а MAC-адреса не могут быть реплицированы в динамические VLAN.
- На каждом порте можно настроить до восьми целевых VLAN. Репликация MAC-адресов вступает в силу, даже если порт не принадлежит указанной целевой VLAN.
- Репликация MAC-адресов не может быть настроена на хост-портах и разнородных портах, портах мониторинга и портах с поддержкой защиты портов/802.1X.
- Можно реплицировать только динамические адреса. Репликация адресов отключается, когда таблица адресов заполнена. Если исходные адреса уже существуют до включения репликации, соответствующие MAC-адреса не будут реплицироваться.
- Реплицированные адреса имеют более высокий приоритет, чем динамические адреса, но имеют более низкий приоритет, чем другие типы адресов.
- Когда MAC-адрес устареет, его реплицированная копия также устареет. При удалении MAC-адреса реплицированный адрес будет удален автоматически.
- Горячее резервирование не поддерживается. После переключения между первичным и вторичным интерфейсами рекомендуется отключить репликацию MAC-адресов и снова включить ее.
- Записи MAC-адресов, полученные при репликации MAC-адресов, невозможно удалить вручную. Если необходимо удалить эти записи, отключите репликацию MAC-адресов.

Этапы конфигурации

Настройка репликации MAC-адресов

- ❖ Выполните эту настройку, чтобы реплицировать MAC-адреса из одной VLAN в другую во избежание пакетного переполнения буфера.

❖ Запустите команду **mac-address-mapping** <1-8> **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id* на магистральном порту, чтобы включить репликацию MAC-адресов. *src-vlan-list* и *dst-vlan-id* определяют диапазон VLAN.

Команда	**mac-address-mapping** *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*
Описание параметров	*x:* Указывает порядковый номер для репликации MAC-адресов. Диапазон значений от 1 до 8. src-vlan-list: Указывает список исходных сетей VLAN. dst-vlan-id: Указывает список целевых сетей VLAN.
Установки по умолчанию	По умолчанию репликация MAC-адресов отключена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

❖ Проверьте, реплицирован ли MAC-адрес указанной VLAN в другую VLAN.

Пример конфигурации

Настройка репликации MAC-адресов

Этапы конфигурации	❖ 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 конфигурации	❖ Проверьте, влияет ли конфигурация на порт.
	❖ Отправьте пакет из исходной VLAN и проверьте, реплицируется 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`

Типичные ошибки

❖ См. "Примечания".

13.4.8 Настройка политики изменения меток внутренней/внешней VLAN

Сценарий

❖ Изменяет внешние или внутренние метки в соответствии с фактическими требованиями к сети.

Примечания

- Политика QinQ, основанная на ACL, имеет приоритет над политикой QinQ, основанной на портах и C-TAG.
- При удалении ACL-списка соответствующая политика будет автоматически удалена.
- Политики изменения меток действуют только на порты доступа, магистральные порты, гибридные порты и порты восходящего канала.
- Политики изменения меток в основном используются для изменения внутренних и внешних меток в сети поставщика услуг.
- Если пакет соответствует двум или более политикам Selective QinQ на основе ACL без приоритета, выполняется только одна политика. Рекомендуется указать приоритет.

Этапы конфигурации

Настройка политики для изменения идентификаторов VLAN внешних меток на основе внутренних меток.

❖ Опционально.
❖ Выполните эту настройку, чтобы изменить идентификаторы VLAN внешних меток на основе идентификаторов VLAN внутренних меток.
❖ Идентификаторы VLAN внешних меток можно изменить в пакетах, которые входят в порты доступа, магистральные порты, гибридные порты и порты восходящего канала, на основе идентификаторов VLAN внутренних меток в этих пакетах.

Команда	**dot1q relay-vid** *VID* **translate inner-vid** *v_list*
Описание параметров	*VID*: Указывает измененный идентификатор VLAN внешней метки. *v_list:* Указывает идентификатор VLAN внутренней метки.
Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса

Встроенная подсказка	Недоступно

Настраивает политику для изменения идентификаторов VLAN внешних меток на основе идентификаторов VLAN внешних и внутренних меток

- Опционально.
- Выполните эту настройку, чтобы изменить идентификаторы VLAN внешних меток на основе идентификаторов VLAN внутренних и внешних меток.
- Идентификаторы VLAN внешних меток можно изменить в пакетах, которые поступают в порты доступа, магистральные порты, гибридные порты и порты восходящего канала, на основе идентификаторов VLAN внутренних и внешних меток 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 внешней метки. vid: Указывает исходный идентификатор VLAN внешней метки. *v_list:* Указывает идентификатор VLAN внутренней метки.
Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настраивает политики для изменения идентификаторов VLAN внешних меток на основе внешних меток

- Опционально.
- Выполните данную настройку, чтобы изменить идентификаторы VLAN внешних меток на основе этих идентификаторов VLAN.
- Идентификаторы VLAN внешних меток можно изменить в пакетах, которые входят в порты доступа, магистральные порты, гибридные порты и порты восходящего канала на основе этих идентификаторов VLAN.

Команда	**dot1q relay-vid** *VID* **translate local-vid** *v_list*
Описание параметров	*VID*: Указывает измененный идентификатор VLAN внешней метки. *v_list:* Указывает исходный идентификатор VLAN внешней метки.

Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настраивает политики для изменения идентификаторов VLAN внутренних меток на основе списков ACL

- Опционально.
- Идентификаторы VLAN внутренних меток можно изменить в пакетах, которые выходят из портов доступа, магистральных портов, гибридных портов и портов восходящего канала на основе содержимого пакета.
- Перед настройкой такой политики настройте ACL-список.

Команда	**traffic-redirect access-group** *acl* **inner-vlan** *vid* **out**
Описание параметров	*acl*: Указывает ACL-список. *vid:* Указывает измененный идентификатор VLAN внутренней метки.
Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настраивает политики для изменения идентификаторов VLAN внешних меток на основе списков ACL

- Опционально.
- Идентификаторы VLAN внешних меток можно изменить в пакетах, которые выходят из портов доступа, магистральных портов, гибридных портов и портов восходящего канала на основе содержимого пакета.
- Перед настройкой такой политики настройте ACL-список.

Команда	**traffic-redirect access-group** *acl* **outer-vlan** *vid* **in**

Описание параметров	*acl*: Указывает ACL-список. *vid:* Указывает измененный идентификатор VLAN внешней метки.
Установки по умолчанию	По умолчанию политика не настроена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

Проверьте, действует ли конфигурация и изменяет ли порт метки в полученных пакетах на основе политики.

Пример конфигурации

Настраивает политики для изменения идентификаторов VLAN внешних меток на основе внешних меток

Этапы конфигурации	❖ Настройте политики изменения внутренних и внешних меток на порту в соответствии с фактическими требованиями к сети.
	❖ В следующем примере показано, как изменить идентификаторы VLAN внешних меток на основе внешних меток и списков ACL соответственно. Дополнительные сведения о других политиках см. в описании выше.
	Настройте политику для изменения внешних меток VLAN на основе внешних меток 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 меток 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 конфигурации	❖ Проверьте, вступила ли в силу конфигурация на порту. ❖ Проверьте, изменяет ли порт идентификаторы VLAN внешних меток в полученных пакетах на основе настроенной политики.

13.4.9 Настройка сопоставления приоритетов и репликации приоритетов

Сценарий

- ❖ Если сеть поставщика услуг предоставляет политику QoS на основе поля User Priority внутренней метки, настройте репликацию приоритетов, чтобы применить политику QoS к внешней метке.
- ❖ Если в сети поставщика услуг политика QoS основана на поле User Priority внутренней метки, настройте сопоставление приоритетов, чтобы применить поле User Priority, предоставляемое сетью поставщика услуг, к внешней метке.

Примечания

⚠ Только туннельный порт может быть настроен с репликацией приоритетов, которая имеет более высокий приоритет, чем доверенное QoS, но ниже, чем QoS на основе ACL.

⚠ На одном порту нельзя одновременно включить репликацию приоритетов и сопоставление приоритетов.

⚠ Только туннельный порт может быть настроен с привязкой приоритетов, которая преобладает над QoS.

⚠ Конфигурация сопоставления приоритетов не вступит в силу, если не настроен режим доверия или режим доверия не совпадает с сопоставлением приоритетов.

Этапы конфигурации

- ❖ Только туннельный порт может быть настроен с сопоставлением приоритетов и репликацией приоритетов.
- ❖ Настройте репликацию приоритетов, чтобы применить внутреннюю политику QoS на основе меток, предоставляемую сетью поставщика услуг.
- ❖ Настройте сопоставление приоритетов, чтобы настроить поле User Priority внешней метки VLAN на основе внутренней метки и гибкого применения политик QoS.
- ❖ Чтобы включить репликацию с приоритетом, выполните команду **inner-priority-trust enable** на туннельном порте.
- ❖ Чтобы включить сопоставление приоритетов, запустите команду **dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value* на туннельном порте.
- ❖ Диапазон *inner-cos-value* и *outer-cos-value* от 0 до 7.

ℹ При отсутствии настроенного сопоставления приоритетов используется следующее сопоставление приоритетов:

```
inner pri    0   1   2   3   4   5   6   7
-------------------------------------------------------------------
outer pri    0   1   2   3   4   5   6   7
```

Команда	**inner-priority-trust enable**

Описание параметров	Недоступно
Установки по умолчанию	По умолчанию репликация приоритетов отключена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Команда	**dot1q-Tunnel cos** *inner-cos-value* **remark-cos** *outer-cos-value*
Описание параметров	*inner-cos-value*: Указывает значение CoS внутренней метки. *outer-cos-value*: Указывает значение CoS внешней метки.
Установки по умолчанию	По умолчанию сопоставление приоритетов отключено.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Проверка конфигурации

- Запустите команду **show inner-priority-trust interfaces** *type intf-id* и команду **show interfes** *type intf-id* **remark**, чтобы проверить, действует ли сопоставление приоритетов или репликация приоритетов.

Пример конфигурации

Настройка сопоставления приоритетов и репликации приоритетов

Этапы конфигурации	- Для поддержания приоритета пакетов необходимо реплицировать приоритет внутренней метки в пакете во внешнюю метку туннельного порта. - Для гибкого управления приоритетом пакетов на туннельном порте можно добавлять внешние метки различных приоритетов к пакетам

	на основе приоритетов внутренних меток 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 конфигурации	❖ Отобразите конфигурацию приоритетов на порту.
	Проверьте, включена ли репликация приоритетов на туннельном порте.
	`QTECH# show inner-priority-trust interfaces gigabitethernet 0/1`
	`Port inner-priority-trust`
	`------ ------------------`
	`Gi0/1 enable`
	
	Отобразите сопоставление приоритетов, настроенное на туннельном порте.
	`QTECH# show interfaces gigabitethernet 0/1 remark`
	`Ports Type From value To value`
	`---------- ---------- ---------- --------`
	`Gi0/1 Cos-To-Cos 3 5`

Типичные ошибки

❖ См. "Примечания".

13.4.10 Настройка прозрачной передачи уровня 2

Сценарий

❖ Прозрачная передача пакетов уровня 2 без влияния на сеть поставщика услуг и сеть заказчика.

Примечания

⚠ Если протокол STP не включен, необходимо выполнить команду **bridge-frame forwarding protocol bpdu**, чтобы включить прозрачную передачу STP.

⚠ Прозрачная передача, включенная на порту, вступает в силу только после глобального включения. Когда на порту вступает в силу прозрачная передача, порт не участвует в вычислении соответствующего протокола. Если порт получает пакет, MAC-адрес назначения которого является специальным широковещательным адресом, он определяет, что происходит сетевая ошибка и отбрасывает пакет.

Этапы конфигурации

Настройка прозрачной передачи STP

- Обязательно, если требуется прозрачная передача пакетов BPDU через STP.
- Включает 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**
Описание параметров	Недоступно
Установки по умолчанию	По умолчанию прозрачная передача STP отключена.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Команда	**l2protocol-tunnel stp enable**
Описание параметров	Недоступно
Установки по умолчанию	По умолчанию прозрачная передача STP отключена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка прозрачной передачи GVRP

- Обязательно, если требуется прозрачная передача пакетов GVRP.

- Включает 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 конфигурации интерфейса, чтобы включить прозрачную передачу GVRP.

Команда	**l2protocol-tunnel gvrp**
Описание параметров	Недоступно
Установки по умолчанию	По умолчанию прозрачная передача GVRP отключена.
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	Недоступно

Команда	**l2protocol-tunnel gvrp enable**
Описание параметров	Недоступно
Установки по умолчанию	По умолчанию прозрачная передача GVRP отключена.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Настройка адреса прозрачной передачи

- Опционально.
- Настраивает адрес прозрачной передачи.

Команда	**l2protocol-tunnel** { **stp** | **gvrp** } **tunnel-dmac** *mac-address*

Описание параметров	*mac-address*: Указывает адрес, используемый для прозрачной передачи пакетов.
Установки по умолчанию	По умолчанию первые три байта адреса прозрачной передачи — 01d0f8, а последние три байта — 000005 и 000006 для STP и GVTP соответственно.
Режим команд	Режим конфигурации интерфейса
Встроенная подсказка	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. Если адрес прозрачной передачи не настроен, используются настройки по умолчанию.

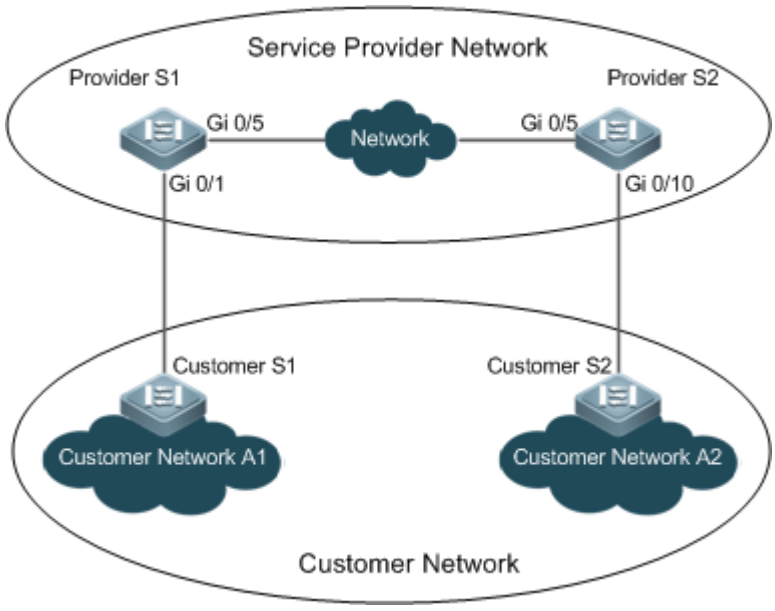
Проверка конфигурации

Запустите команду **show l2protocol-tunnel stp** и команду **show l2protocol-tunnel gvrp**, чтобы проверить правильность настройки адреса прозрачной передачи.

Пример конфигурации

В следующем примере показано, как настроить прозрачную передачу STP.

Настройка прозрачной передачи STP

Сценарий Изображение 13-18	
Этапы конфигураци	❖ На PE (Provider S1 и Provider S2) включите прозрачную передачу STP в режиме глобальной конфигурации и режиме конфигурации интерфейса.

и	❖ Прежде чем включить прозрачную передачу STP, включите STP в режиме глобальной конфигурации, чтобы позволить коммутаторам пересылать пакеты STP.

Поставщик 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 Basic QinQ на порту, подключенном к сети заказчика, 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 заказчика.
	`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 4: Настройте порт восходящего потока.
	`ProviderS1(config)# interface gigabitEthernet 0/5`
	`ProviderS1(config-if-GigabitEthernet 0/5)#switchport mode uplink`

Поставщик S2	❖ Настройте поставщика S2, выполнив те же действия.

Проверка конфигурации	❖ 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: Подтвердите конфигурацию, проверив:
	❖ Тип порта должен быть: dot1q-tunnel.

	❖ Внешняя VLAN-метка соответствует DSP-сети VLAN и добавляется в список VLAN туннельного порта.
	❖ Порт, через который осуществляется доступ к сети поставщика услуг, настраивается как порт восходящего канала.
	`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`

Типичные ошибки

❖ Протокол STP не включен в режиме глобальной конфигурации.
❖ Прозрачная передача не включена в режиме глобальной конфигурации и режиме конфигурации интерфейса.

13.5 Мониторинг

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 на туннельном порте.	**show registration-table** [**interfaces** *intf-id*]
Отображает политики Selective QinQ на основе C-TAG для порта доступа, магистрального порта или гибридного порта.	**show translation-table** [**interfaces** *intf-id*]
Отображает VLAN mapping на портах.	**show interfaces** [*intf-id*] **vlan-mapping**

Отображает выборочные политики 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** }

Отладка

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

Описание	Команда
Отлаживает QinQ.	**debug bridge qinq**

14 КОНФИГУРИРОВАНИЕ MGMT

14.1 Обзор

- Из-за пределов внутренней модификации Ethernet-интерфейс на передней панели отделен от схем передачи внутри устройства и не имеет влияния на плоскость пересылки и плоскость управления. Соответственно, связь через такой Ethernet-интерфейс также отделена от сервисов связи, выполняемых на устройстве, и называется "внеполосной связью". Ethernet-интерфейс можно использовать для управления устройством аналогичным образом, когда устройство подключено через консольный интерфейс. Ethernet-интерфейс управления, обычно называемый MGMT, используется только для управления устройством, но не поддерживает пересылку по линии связи.

Интерфейс MGMT можно использовать для отделения сети управления от сети обслуживания, чтобы избежать помех от трафика и состояния связи в сети обслуживания, а также повысить надежность управления. В частности, при возникновении неисправности в сети обслуживания можно использовать сеть управления для управления устройством. По сравнению с внутриполосным методом управления сервисной сетью такое преимущество не сравнимо.

Кроме того, по сравнению с консольным интерфейсом, интерфейс MGMT имеет большую полосу пропускания (например, 100 Мб по сравнению с 115200 бит/с). В сети управления с сервером журналирования интерфейс MGMT может использоваться для отправки журналов на сервер журналов, так что отправка и хранение журналов также не зависит от состояния связи в сервисной сети.

Из-за различных аппаратных компонентов интерфейс MGMT может быть интерфейсом FastEthernet (FE) или GigabitEthernet (GE).

В следующем разделе описывается конфигурация Ethernet-интерфейса для управления.

14.2 Применение

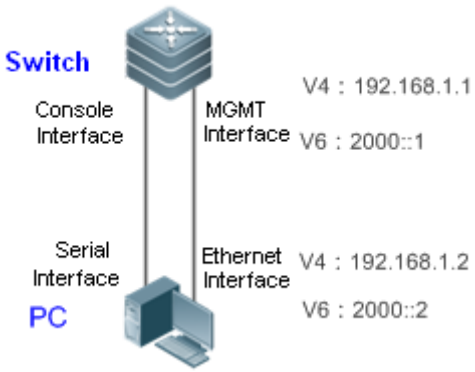
Применение	Описание
Инструмент управления сетью	Интерфейс MGMT используется для управления и отладки сетевого соединения.
Управление файлами	Интерфейс MGMT используется для копирования файлов между сетью управления и устройством.
Управление сетевым подключением	Интерфейс MGMT используется для удаленного входа на другое устройство или хост с локального устройства.
Управление MIB	Интерфейс MGMT используется для отправки сообщения ловушки SNMP на сервер NMS.

Управление журналом	Интерфейс MGMT используется для отправки сообщения журнала на сервер Syslog.

14.2.1 Способ управления сетью

Сценарий

Рис. 14-1 Инструмент управления сетью



Как показано на Изображении 14-1, последовательный интерфейс ПК подключен к интерфейсу консоли коммутатора, чтобы настроить атрибут интерфейса уровня 3 и атрибут интерфейса уровня 2 для интерфейса MGMT, определить доступные хосты интерфейса MGMT и отследить маршруты этих доступных хостов.

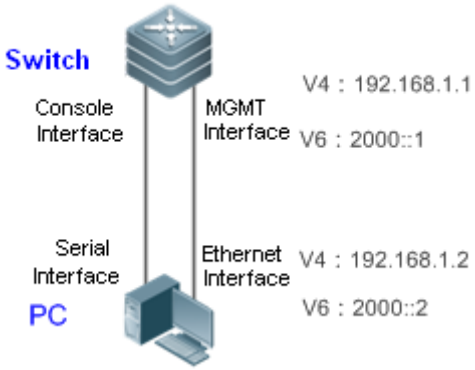
Описание

- Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора.
- Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора.
- Используйте последовательный интерфейс ПК для настройки интерфейса MGMT коммутатора.
- Используйте последовательный интерфейс ПК для отправки команды обнаружения доступных узлов интерфейса MGMT.
- Используйте последовательный интерфейс ПК для отправки команды трассировки маршрутов доступных хостов интерфейса MGMT.

14.2.2 Управление файлами

Сценарий

Рис. 14-2 Управление файлами



Как показано на Изображении 14-2, последовательный интерфейс ПК подключен к интерфейсу консоли коммутатора, чтобы настроить атрибут интерфейса уровня 3 и атрибут интерфейса уровня 2 для интерфейса MGMT. Коммутатор использует интерфейс MGMT для копирования файла с файлового сервера.

Заметки	-

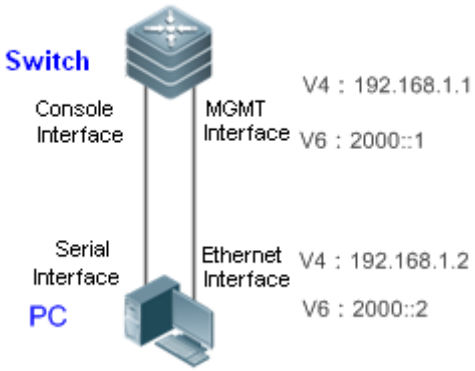
Описание

- Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора.
- Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора.
- Используйте последовательный интерфейс ПК для настройки интерфейса MGMT коммутатора.
- Включите файловый сервер на ПК.
- Используйте последовательный порт ПК для отправки команды, которую коммутатор использует для интерфейса MGMT при копировании файла с файлового сервера.

14.2.3 Управление сетевым подключением

Сценарий

Рис. 14-3 Управление сетевым подключением



Как показано на Изображении 14-3, последовательный интерфейс ПК подключен к интерфейсу консоли коммутатора, чтобы настроить атрибут интерфейса уровня

3 и атрибут интерфейса уровня 2 для интерфейса MGMT. Коммутатор использует интерфейс MGMT для входа на сервер Telnet данного ПК.

Заметки	-

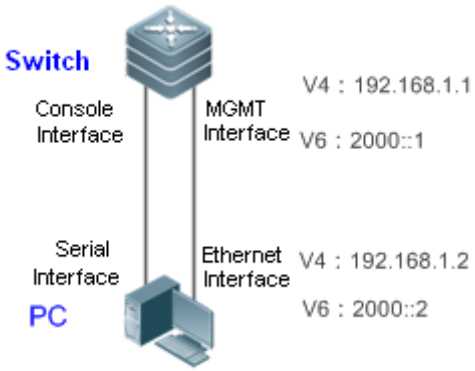
Описание

- ❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора.
- ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора.
- ❖ Используйте последовательный интерфейс ПК для настройки интерфейса MGMT коммутатора.
- ❖ Включите сервер Telnet на ПК.
- ❖ Используйте последовательный порт ПК для отправки команды, которая используется коммутатором для входа на сервер Telnet данного ПК посредством интерфейс MGMT.

14.2.4 Управление MIB

Сценарий

Рис. 14-4 Управление MIB



Как показано на Изображении 14-4, последовательный интерфейс ПК подключен к интерфейсу консоли коммутатора, чтобы настроить атрибут интерфейса уровня 3 и атрибут интерфейса уровня 2 для интерфейса MGMT. Коммутатор использует интерфейс MGMT для отправки сообщения ловушки SNMP на сервер NMS ПК.

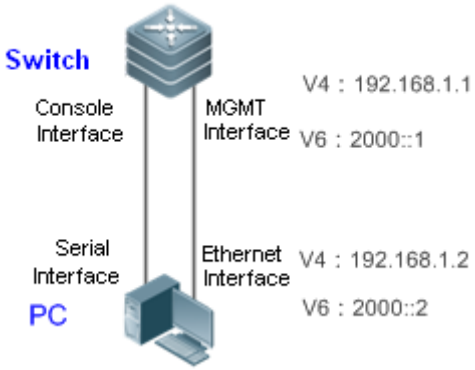
Описание

- ❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора.
- ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора.
- ❖ Используйте последовательный интерфейс ПК для настройки интерфейса MGMT коммутатора.
- ❖ Включите сервер NMS на ПК.
- ❖ Используйте последовательный порт ПК для отправки команды, которую коммутатор использует для отправки сообщения SNMP-ловушки на сервер NMS ПК посредством интерфейса MGMT.

14.2.5 Управление журналом

Сценарий

Рис. 14-5 Управление журналом



Как показано на Изображении 14-5, последовательный интерфейс ПК подключен к интерфейсу консоли коммутатора, чтобы настроить атрибут интерфейса уровня 3 и атрибут интерфейса уровня 2 для интерфейса MGMT. Коммутатор использует интерфейс MGMT для отправки сообщения журнала на сервер журналирования в ПК.

Заметки	-

Описание

- ❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора.
- ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора.
- ❖ Используйте последовательный интерфейс ПК для настройки интерфейса MGMT коммутатора.
- ❖ Включите сервер журналирования на ПК.
- ❖ Используйте последовательный порт ПК для отправки команды, которая используется коммутатором для отправки сообщения журнала на сервер журналирования ПК посредством интерфейса MGMT.

14.3 Функции

Обзор

Функция	Описание
Управление атрибутами интерфейса	С точки зрения сетевого взаимодействия, интерфейс MGMT не сильно отличается от других интерфейсов LAN. Единственное отличие заключается в том, что интерфейс MGMT не поддерживает пересылку по линии связи, и поэтому настраиваемых элементов меньше, чем у других интерфейсов LAN. В некоторых командах должно быть указано, что интерфейс MGMT используется для внеполосной связи.

Инструмент управления сетью	Для удобного управления и отладки коммуникаций в сети система предоставляет несколько командных инструментов, которые используют интерфейс MGMT для управления сетью.
Управление файлами	Система позволяет пользователю использовать интерфейс MGMT для копирования файлов между сетью управления и устройством.
Управление сетевым подключением	Система позволяет пользователю использовать интерфейс MGMT локального устройства для удаленного входа на другие устройства или хосты.
Управление MIB	Для удобного управления MIB система предоставляет пользователю возможность использовать интерфейс MGMT для отправки сообщения SNMP-ловушки на сервер NMS.
Управление журналом	Для удобного управления журналами система позволяет пользователю использовать интерфейс MGMT для отправки сообщения журнала на сервер журналирования.

14.3.1 Управление атрибутами интерфейса

Принцип работы

С точки зрения сетевого взаимодействия, интерфейс MGMT не сильно отличается от других интерфейсов LAN. Таким образом, можно настроить Настройки интерфейса MGMT, чтобы включить интерфейс MGMT с функциями канала связи, аналогичными обычному интерфейсу LAN. Следует отметить, что интерфейс MGMT не поддерживает пересылку по линии связи.

Связанная конфигурация

Настройка IPv4-адреса интерфейса MGMT

По умолчанию интерфейс MGMT не имеет IPv4-адреса. В режиме интерфейса MGMT можно выполнить следующую команду для настройки IPv4-адреса интерфейса MGMT.

- **ip address** *address mask*
- Где параметр *address* указывает **IPv4 адрес**, а *mask* указывает **маску IPv4 адреса**.

Настройка шлюза IPv4 интерфейса MGMT

По умолчанию интерфейс MGMT не имеет шлюза IPv4. В режиме интерфейса MGMT можно выполнить следующую команду для настройки шлюза IPv4 интерфейса MGMT.

- **gateway** *A.B.C.D*
- В которой A.B.C.D указывает **адрес шлюза IPv4**.

Настройка IPv6-адреса интерфейса MGMT

По умолчанию интерфейс MGMT не имеет IPv6-адреса и маски подсети. В режиме интерфейса MGMT можно выполнить следующую команду для настройки IPv6-адреса интерфейса MGMT.

- **ipv6 address** *ipv6-address*/*prefix-length*

Где *ipv6-address* указывает **IPv6 адрес**, а *prefix-length* указывает длину префикса маски IPv6 адреса.

Настройка шлюза IPv6 интерфейса MGMT

По умолчанию интерфейс MGMT не имеет шлюза IPv6. В режиме интерфейса MGMT можно выполнить следующую команду для настройки шлюза IPv6 интерфейса MGMT.

- **ipv6 gateway** *ipv6-address*
- В которой параметр *ipv6-address* указывает **адрес шлюза IPv6**.

Настройка MTU интерфейса MGMT

По умолчанию значение MTU интерфейса MGMT равно 1500. Для настройки MTU интерфейса MGMT можно выполнить следующую команду.

MTU *mtu-value*

Где *mtu-value* указывает **на значение MTU**. **Значение варьируется от 64 до максимального значения MTU, поддерживаемого устройством.**

Настройка режима скорости интерфейса MGMT

По умолчанию режим скорости интерфейса MGMT работает в автоматическом режиме. Для настройки режима скорости интерфейса MGMT можно выполнить следующую команду.

- **speed** {**10** | **100** | **1000** | **auto**}

Настройка дуплексного режима интерфейса MGMT

По умолчанию дуплексный режим интерфейса MGMT работает автоматически. Для настройки дуплексного режима интерфейса MGMT можно выполнить следующую команду.

- **duplex** {**full** | **half** | **auto**}

Настройка дескриптора интерфейса MGMT

По умолчанию интерфейс MGMT не имеет дескриптора интерфейса. Для настройки дескриптора интерфейса MGMT можно выполнить следующую команду.

description *text*

Где параметр *text* указывает дескриптор интерфейса.

Отключение интерфейса MGMT

По умолчанию интерфейс MGMT включен. Для отключения интерфейса MGMT можно выполнить следующую команду.

shutdown

14.3.2 Инструмент управления сетью

Для удобного управления и отладки коммуникаций в сети система предоставляет несколько командных инструментов, которые используют интерфейс MGMT для управления сетью.

Принцип работы

- Система использует интерфейс MGMT для отправки эхо-пакета и определения доступности адресов IPv4/IPv6 узла/хоста в сети управления.
- Система использует интерфейс MGMT для отправки пакета трассировки для обнаружения маршрутов IPv4/IPv6 узла/хоста в сети управления.

Связанная конфигурация

Определение доступности адреса IPv4

В привилегированном режиме команда ниже используется для определения доступности IPv4-адреса узла/хоста через интерфейс MGMT.

ping oob *address* ***via*** *mgmt-name*

В этом случае *address* указывает IPv4-адрес обнаруженного узла/хоста, а *mgmt-name* указывает выходной интерфейс управления пакетов в режиме oob.

Трассировка маршрута IPv4

В привилегированном режиме команда ниже используется для отслеживания IPv4-маршрута узла/хоста через интерфейс MGMT.

traceroute *oob* *address* ***via*** *mgmt-name*

В которой *address* указывает IPv4-адрес трассированного узла/хоста.

Определение доступности адреса IPv6

В привилегированном режиме команда ниже используется для определения доступности IPv6-адреса узла/хоста через интерфейс MGMT.

ping oob ipv6 *ipv6-address* ***via*** *mgmt-name*

Где *ipv6-address* указывает IPv6-адрес детектированного узла/хоста.

Трассировка маршрута IPv6

В привилегированном режиме команда ниже используется для отслеживания IPv6-маршрута узла/хоста через интерфейс MGMT.

traceroute *oob* ipv6 *ipv6-address* ***via*** *mgmt-name*

Где *ipv6-address* указывает IPv6-адрес трассированного узла/хоста, а *mgmt-name* указывает выходной интерфейс управления пакетов в режиме oob.

14.3.3 Управление файлами

Система позволяет пользователю использовать интерфейс MGMT для копирования файлов между сетью управления и устройством.

Принцип работы

- Скопируйте указанный файл с исходного URL-адреса на целевой URL-адрес через интерфейс MGMT.

Связанная конфигурация

Копирование файлов

В привилегированном режиме команда ниже используется для копирования указанного файла с URL-адреса источника на URL-адрес назначения через интерфейс MGMT.

copy oob_tftp://***source-url destination-url***

Где *source-url* — указывает на URL-адрес источника файла, а *destination-url* — указывает на URL-адрес назначения файла.

14.3.4 Управление сетевым входом

Система позволяет пользователю использовать интерфейс MGMT локального устройства для удаленного входа на другие устройства или хосты.

Принцип работы

Войдите в указанный узел/хост устройства через интерфейс MGMT для удаленного управления устройства узла.

Связанная конфигурация

Управление сетевым входом

В привилегированном режиме команда ниже используется для входа в узел/хост через интерфейс MGMT.

telnet oob *ip-address* | *ipv6-address*

Где *ip-address* указывает IPv4-адрес узла/хоста устройства, а *ipv6-address* — IPv6-адрес узла/хоста устройства.

14.3.5 Управление MIB

Для удобного управления MIB система позволяет пользователю использовать интерфейс MGMT для отправки сообщения SNMP-ловушки на сервер NMS.

Принцип работы

Отправка сообщения ловушки SNMP на сервер NMS через интерфейс MGMT и адрес IPv4/IPv6 сервера NMS.

Связанная конфигурация

Отправка сообщения ловушки на адрес IPv4 сервера NMS

В глобальном режиме команда ниже используется для отправки сообщения ловушки на IPv4-адрес сервера NMS через интерфейс MGMT. Данная функция выключена по умолчанию.

- **snmp-server host oob** *ip-address*

Где *ip-address* указывает IPv4-адрес сервера NMS.

Отправка сообщения ловушки на IPv6-адрес сервера NMS

В привилегированном режиме команда ниже используется для отправки сообщения ловушки на IPv6-адрес сервера NMS через интерфейс MGMT. Данная функция выключена по умолчанию.

- **snmp-server host oob ipv6** *ipv6-address*

Где *ipv6-address* указывает IPv6-адрес сервера NMS.

14.3.6 Управление журналом

Для удобного управления журналами система позволяет пользователю использовать интерфейс MGMT для отправки сообщения журнала на сервер журналирования.

Принцип работы

Отправка сообщения ловушки SNMP на сервер журналирования через интерфейс MGMT и адрес IPv4/IPv6 сервера журналирования.

Связанная конфигурация

Отправка сообщения журнала через интерфейс MGMT и IPv4-адрес сервера журналирования.

В глобальном режиме команда ниже используется для отправки сообщения журнала на сервер журналирования через интерфейс MGMT и IPv4-адрес сервера журналирования. Данная функция выключена по умолчанию.

- **logging server oob** *ip-address*

Где ip-address указывает IPv4-адрес сервера журналирования.

Отправка сообщения журнала через интерфейс MGMT и IPv6-адрес сервера журналирования.

В привилегированном режиме команда ниже используется для отправки сообщения журнала на сервер журналирования через интерфейс MGMT и IPv6-адрес сервера журналирования. Данная функция выключена по умолчанию.

- **logging server oob ipv6** *ipv6-address*

Где ipv6-address указывает IPv6-адрес сервера журналирования.

14.4 Конфигурация

Конфигурация	Описание и команда	
Управление атрибутами интерфейса	Необходимо настроить адреса IPv4 и IPv6 интерфейса MGMT. Адреса IPv4/IPv6 можно настроить для управления устройством через интерфейс MGMT.	
	ip address *address mask*	Используется для настройки IPv4-адреса и маски подсети интерфейса MGMT.

	ipv6 address *ipv6-address/prefix-length*	Используется для настройки IPv6-адреса и маски подсети интерфейса MGMT.
	gateway *A.B.C.D*	Используется для настройки шлюза IPv4 сети управления.
	ipv6 gateway *ipv6-address*	Используется для настройки шлюза IPv6 сети управления.
	(Дополнительно) Используется для обеспечения наилучшего состояния интерфейса MGMT в соответствии с потребностями развертывания сети.	
	mtu *mtu-value*	Настраивает значение MTU интерфейса MGMT.
	speed { **10** | **100** | **1000** | **auto** }	Настраивает режим скорости интерфейса MGMT. Значение по умолчанию — auto.
	duplex { **full** | **half** | **auto** }	Настраивает дуплексный режим интерфейса MGMT. Значение по умолчанию — auto.
	shutdown	Отключает интерфейс MGMT
	description *text*	Настраивает дескриптор.
Инструмент управления сетью	(Дополнительно) Используется для управления сетью через интерфейс MGMT, например, для выполнения операции эхо-запроса или отслеживания сетевого маршрута, чтобы определить доступность и маршрутную информацию сетевого узла.	
	ping oob *address*	Эхо-запрос ICMP для определения доступности хостов в сети управления.
	ping oob ipv6 *ipv6-address*	Эхо-запрос ICMPv6 для определения доступности хостов в сети управления.
	traceroute oob *address*	Используется для обнаружения маршрутов к хостам в сети управления.

	traceroute *oob* ipv6 *ipv6-address*	Используется для обнаружения маршрутов к хостам IPv6 в сети управления.
Управление файлами	(Дополнительно) Используется для копирования файлов между сетью управления и устройством через интерфейс MGMT.	
	copy oob_tftp://*source-url* destination-url	Используется для копирования файла из источника, указанного в параметре source-url, в назначение, указанное в destination-url.
Управление сетевым подключением	(Дополнительно) Используется для удаленного входа на другие устройства или хосты через интерфейс MGMT.	
	telnet oob *ip-address*| *ipv6-address*	Эта команда используется для выполнения команды telnet на устройстве и обмена данными через интерфейс MGMT. Во время настройки не требуется указывать такие параметры, как **ip** и **ipv6**, чтобы определить протокол (IPv4/IPv6), поскольку система автоматически определяет, что вводимый адрес является допустимым адресом IPv4 или IPv6.
Управление MIB	(Дополнительно) Используется для отправки сообщения ловушки SNMP на сервер NMS через интерфейс MGMT.	
	snmp-server host oob *ip-address*	Настраивает агента SNMP для указания отправки сообщения ловушки на IPv4-адрес сервера NMS через интерфейс MGMT.
	snmp-server host oob ipv6 *ipv6-address*	Настраивает агента SNMP для указания отправки сообщения ловушки на IPv6-адрес сервера NMS через интерфейс MGMT.
Управление	(Дополнительно) Используется для отправки сообщения журнала	

журналом	на сервер журналирования через интерфейс MGMT.	
	logging server oob *ip-address*	Настраивает адрес журналирования для отправки сообщений через интерфейс MGMT на IPv4-адрес сервера.
	logging server oob ipv6 *ipv6-address*	Настраивает адрес журналирования для отправки сообщений через интерфейс MGMT на IPv6-адрес сервера.

14.4.1 Управление атрибутами интерфейса

Сценарий

- Настройка адреса уровня 3 интерфейса MGMT.
- Настройка адреса шлюза сети управления.
- Настройка физических **параметров** интерфейса MGMT.
- После настройки интерфейс MGMT можно использовать для управления устройствами.

Примечание

- Интерфейс MGMT не поддерживает пересылку по каналу связи.

Этапы конфигурации

Настройте адрес уровня 3 интерфейса MGMT.

- Войдите в режим конфигурации интерфейса MGMT.
- Настройте адрес уровня 3 интерфейса MGMT.

Настройте адрес шлюза сети управления.

- Войдите в режим конфигурации интерфейса MGMT.
- Настройка адреса шлюза сети управления.

Проверка конфигурации

- Запустите команду **show run** для отображения конфигурации.

Связанные команды

Настройка IPv4-адреса интерфейса MGMT

Команда	**ip address** *address mask*
Описание параметров	*address:* **Указывает адрес IPv4.** *Mask:* **Указывает маску адреса IPv4.**
Режим команд	Режим интерфейса MGMT.

Встроенная подсказка	-

Настройка шлюза IPv4 в сети управления

Команда	**gateway** *A.B.C.D*
Описание параметров	*A.B.C.D*: Указывает адрес шлюза IPv4.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка IPv6-адреса интерфейса MGMT

Команда	**ipv6 address** *ipv6-address/prefix-length*
Описание параметров	*ip-address:* **Указывает адрес IPv6.** *prefix-length:* **Указывает длину префикса маски IPv4-адреса.**
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка шлюза IPv6 в сети управления

Команда	**ipv6 gateway** *ipv6-address*
Описание параметров	ip-address: Указывает адрес шлюза IPv6.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка MTU интерфейса MGMT

Команда	
Описание параметров	*mtu-value:* Настраивает значение MTU интерфейса MGMT.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка режима скорости интерфейса MGMT

Команда	**speed** {**10** | **100** | **1000** | **auto**}
Описание параметров	Значение по умолчанию — auto.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка дуплексного режима интерфейса MGMT

Команда	**duplex** {**full** | **half** | **auto**}
Описание параметров	Значение по умолчанию — auto.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Настройка дескриптора интерфейса MGMT

Команда	**description** *text*
Описание параметров	*text*: Указывает дескриптор интерфейса. Значение по умолчанию недоступно.

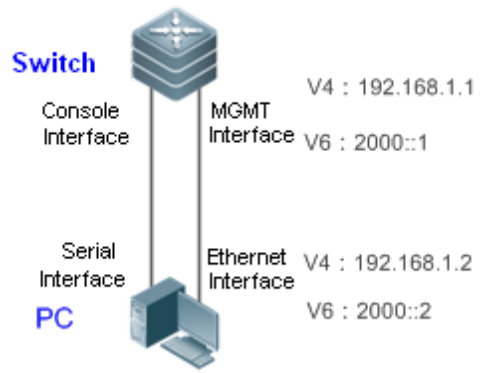
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Отключение интерфейса MGMT

Команда	**shutdown**
Описание параметров	Значение по умолчанию — *no shutdown*.
Режим команд	Режим интерфейса MGMT.
Встроенная подсказка	-

Пример конфигурации

Настройка интерфейса MGMT

Сценарий Изображение 14-6	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес 3-го уровня интерфейса MGMT коммутатора на 192.168.1.1. ❖ Настройте адрес шлюза IPv4 в сети управления на 192.168.1.2. ❖ Настройте IPv6-адрес 3-го уровня интерфейса MGMT коммутатора на 2000::1. ❖ Настройте адрес шлюза IPv6 в сети управления на 2000::2. ❖ Настройте скорость интерфейса MGMT на коммутаторе на 1000 Мбит/с.

	❖ Отключите интерфейс MGMT на коммутаторе.
Коммутатор	QTECH# configure QTECH(config)# interface mgmt 0 QTECH(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0 QTECH(config-if-Mgmt 0)# gateway 192.168.1.1 QTECH(config-if-Mgmt 0)# ipv6 address 2000::1/64 QTECH(config-if-Mgmt 0)# gateway 2000::2 QTECH(config-if-Mgmt 0)# speed 1000 QTECH(config-if-Mgmt 0)# shutdown
Проверка конфигурации	❖ Выполните команду **show running** для проверки указанных выше конфигураций на коммутаторе.
Коммутатор	QTECH# show run int mgmt 0 Building configuration... Current configuration : 168 bytes ! interface MGMT 0 no switchport speed 1000 no ip proxy-arp ip address 192.168.1.1 255.255.255.0 ipv6 address 2000::1/64 ipv6 enable gateway 192.168.1.1 ipv6 gateway 2000::2 shutdown

14.4.2 Инструмент управления сетью

Сценарий

- ❖ Определение доступности IPv4-адреса узла/хоста устройства через интерфейс MGMT.
- ❖ Трассировка маршрута IPv4 узла/хоста устройства через интерфейс MGMT.
- ❖ Определение доступности IPv6-адреса узла/хоста устройства через интерфейс MGMT.
- ❖ Трассировка маршрута IPv6 узла/хоста устройства через интерфейс MGMT.

Этапы конфигурации

Определите доступность адреса IPv4

- Войдите в привилегированный режим.
- Определение доступность IPv4-адреса узла/хоста устройства через интерфейс MGMT.

Трассировка маршрута IPv4

- Войдите в привилегированный режим.
- Трассируйте маршрут IPv4 узла/хоста устройства через интерфейс MGMT.

Определите доступность адреса IPv6

- Войдите в привилегированный режим.
- Определите доступность IPv6-адреса узла/хоста устройства через интерфейс MGMT.

Трассировка маршрута IPv6

- Войдите в привилегированный режим.
- Трассируйте маршрут IPv6 узла/хоста устройства через интерфейс MGMT.

Проверка конфигурации

- Просмотр процесса в реальном времени.

Связанные команды

Определите доступность адреса IPv4

Команда	**ping oob** *address* ***via*** *mgmt-name*
Описание параметров	*address:* **Указывает адрес IPv4.** *mgmt-name:* Указывает выходной интерфейс управления пакетов в режиме oob.
Режим команд	Привилегированный режим
Встроенная подсказка	-

Трассировка маршрута IPv4

Команда	**traceroute oob** *address* ***via*** *mgmt-name*
Описание параметров	address: Указывает адрес IPv4. *mgmt-name:* Указывает выходной интерфейс управления пакетов в режиме oob.
Режим команд	Привилегированный режим

Встроенная подсказка	-

Определите доступность адреса IPv6

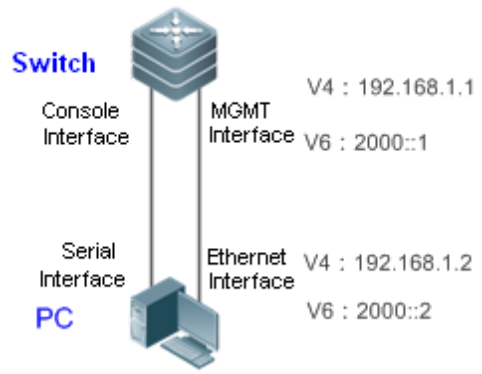
Команда	**ping oob ipv6** *ipv6-address* ***via*** *mgmt-name*
Описание параметров	*ip-address:* **Указывает адрес IPv6.** *mgmt-name:* Указывает выходной интерфейс управления пакетов в режиме oob.
Режим команд	Привилегированный режим
Встроенная подсказка	-

Трассировка маршрута IPv6

Команда	**traceroute *oob* ipv6** *ipv6-address* ***via*** *mgmt-name*
Описание параметров	ip-address: Указывает адрес IPv6. *mgmt-name:* Указывает выходной интерфейс управления пакетов в режиме oob.
Режим команд	Привилегированный режим
Встроенная подсказка	-

Пример конфигурации

Инструмент управления сетью

Сценарий Изображение 14-7	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес интерфейса MGMT коммутатора 3-го уровня на 192.168.1.1. ❖ Настройте IPv6-адрес интерфейса MGMT коммутатора 3-го уровня на 2000::1. ❖ Настройте адрес шлюза IPv6 в сети управления на 2000::2. ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора. ❖ Настройте адреса IPv4 и IPv6 интерфейса Ethernet ПК на 192.168.1.2 и 2000::2 соответственно. ❖ Определите доступность адресов IPv4 и IPv6 ПК через интерфейс MGMT. ❖ Отследите маршруты IPv4 и IPv6 через интерфейс MGMT.

Коммутатор	`QTECH# configure`
	`QTECH(config)# int mgmt 0`
	`QTECH(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0`
	`QTECH(config-if-Mgmt 0)# ipv6 address 2000::1/64`
	`QTECH# ping oob 192.168.1.2`
	`QTECH# traceroute oob 192.168.1.2`
	`QTECH# ping oob ipv6 2000::2`
	`QTECH# traceroute oob ipv6 2000::2`

Проверка конфигурации	❖ Просмотрите процесс в реальном времени. Хосты в сети управления могут быть определены, посредством эхо-запросов, а команда traceroute может использоваться для отслеживания маршрутов к хостам в сети управления.
Коммутатор	`QTECH# ping oob 192.168.1.2` `Sending 5, 100-byte ICMP Echoes to 192.168.1.2, timeout is 2 seconds:`

	!!!!! Success rate is 100 percent, round-trip min/avg/max = 4/4/4 ms QTECH# traceroute oob 192.168.1.2 Tracing route to 192.168.1.2 over a maximum of 10 hops 1 <10 ms <10 ms <10 ms 192.168.1.2 QTECH# ping oob ipv6 2000::2 Sending 5, 100-byte ICMP Echoes to 2000::2, timeout is 2 seconds: < press Ctrl+C to break > !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms. QTECH# traceroute oob ipv6 2000::2 Tracing route to 2000::2 over a maximum of 10 hops 1 <10 ms <10 ms <10 ms 2000::2

14.4.3 Управление файлами

Сценарий

- Скопируйте файл из источника, указанного в *source-url*, в назначение, указанное в *destination-url*, через интерфейс MGMT.

Этапы конфигурации

Управление файлами

- Войдите в привилегированный режим.
- Скопируйте файл из источника, указанного в source-url, в назначение, указанное в destination-url.

Проверка конфигурации

- Просмотр процесса в реальном времени.

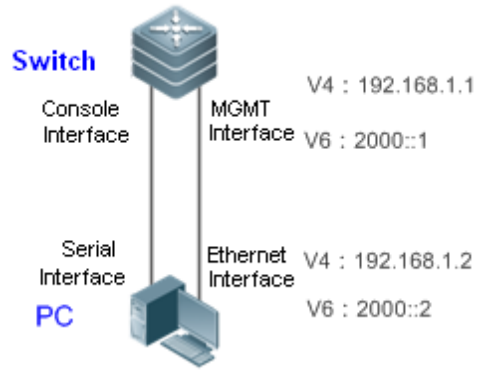
Связанные команды

Управление файлами

Команда	**copy oob_tftp:**//*source-url destination-url*
Описание параметров	*source-url:* Указывает URL-адрес источника файла. *destination-url:* Указывает URL-адрес назначения файла.
Режим команд	Привилегированный режим
Встроенная подсказка	-

Пример конфигурации

Управление файлами

Сценарий Изображение 14-8	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес интерфейса MGMT коммутатора 3-го уровня на 192.168.1.1. ❖ Настройте IPv6-адрес интерфейса MGMT коммутатора 3-го уровня на 2000::1. ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора. ❖ Настройте адреса IPv4 и IPv6 интерфейса Ethernet ПК на 192.168.1.2 и 2000::2 соответственно. ❖ Включите сервер TFTP для ПК на базе IPv4. ❖ Включите сервер TFTP для ПК на базе IPv6. ❖ Загрузите файл с хоста IPv4 в сети управления на файловую систему флэш-накопителя. ❖ Загрузите файл с хоста IPv6 в сети управления на файловую систему флэш-накопителя.

Коммутатор	`QTECH# configure`
	`QTECH(config)# int mgmt 0`
	`QTECH(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0`
	`QTECH(config-if-Mgmt 0)# ipv6 address 2000::1/64`
	`QTECH# copy oob_tftp://192.168.1.2/ngsa-compress.bin`
	`QTECH# copy oob_tftp://[2000::2]/ngsa-compress.bin`

Проверка конфигурации	❖ Просмотр процесса в реальном времени. Файл загружается с хоста IPv4/IPv6 в сети управления в файловую систему флэш-накопителя.
Коммутатор	`QTECH# copy oob_tftp://192.168.1.2/ngsa-compress.bin`

	flash:file.bin Accessing tftp://192.168.1.2/ngsa-compress.bin... !! Success : Transmission success, file length 1183856 bytes QTECH# copy oob_tftp://[2000::2]/ngsa-compress.bin flash:file.bin Accessing tftp://192.168.1.2/ngsa-compress.bin... !! Success : Transmission success, file length 1183856 bytes

14.4.4 Управление сетевым входом

Сценарий

❖ Войдите в систему на других устройствах или хостах через интерфейс MGMT.

Этапы конфигурации

Управление сетевым входом

❖ Войдите в привилегированный режим.
❖ Войдите в систему на других устройствах или хостах через интерфейс MGMT.

Проверка конфигурации

❖ Просмотр процесса в реальном времени.

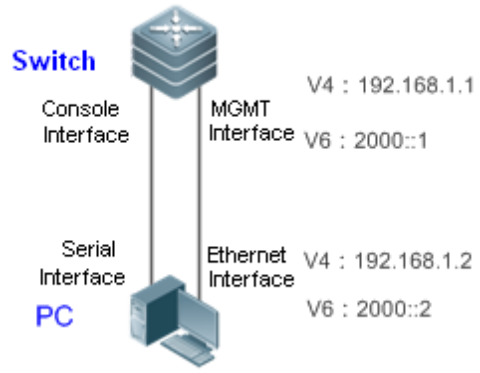
Связанные команды

Управление сетевым входом

Команда	**telnet oob** *ip-address* | *ipv6-address*
Описание параметров	*ip-address:* **Указывает адрес IPv4.** *ipv6-address:* **Указывает адрес IPv6.**
Режим команд	Привилегированный режим
Встроенная подсказка	Эта команда используется для выполнения команды telnet на устройстве и обмена данными через интерфейс MGMT. Во время настройки не требуется указывать такие параметры, как **ip** и **ipv6**, чтобы определить протокол (IPv4/IPv6), поскольку система автоматически определяет, что вводимый адрес является допустимым адресом IPv4 или IPv6.

Пример конфигурации

Управление сетевым входом

Сценарий Изображение 14-9	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес интерфейса MGMT коммутатора 3-го уровня на 192.168.1.1. ❖ Настройте IPv6-адрес интерфейса MGMT коммутатора 3-го уровня на 2000::1. ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора. ❖ Настройте адреса IPv4 и IPv6 интерфейса Ethernet ПК на 192.168.1.2 и 2000::2 соответственно. ❖ Включите сервер telnet для ПК на основе IPv4. ❖ Включите сервер telnet для ПК на основе IPv6. ❖ Коммутатор A входит на ПК посредством интерфейса MGMT.

Коммутатор	`QTECH A# configure`
	`QTECH A(config)# int mgmt 0`
	`QTECH A(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0`
	`QTECH A(config-if-Mgmt 0)# ipv6 address 2000::1/64`
	`QTECH A# telnet oob 192.168.1.2`
	`QTECH A# telnet oob 2000::2`

Проверка конфигурации	❖ Просмотр процесса в реальном времени. Коммутатор может войти на ПК.

Коммутатор A	`QTECH A# telnet oob 192.168.1.2`
	`User Access Verification`
	`Password:`
	`QTECH A# telnet oob 2000::2`

	User Access Verification Password:

14.4.5 Управление MIB

Сценарий

- ❖ Определите отправление сообщения-ловушки на сервер NMS через интерфейс MGMT и IPv4-адрес сервера NMS.
- ❖ Определите отправление сообщения-ловушки на сервер NMS через интерфейс MGMT и IPv6-адрес сервера NMS.

Этапы конфигурации

Управление MIB

- ❖ Войдите в глобальный режим.
- ❖ Определите отправление сообщения-ловушки на сервер NMS через интерфейс MGMT и IPv4-адрес сервера NMS.
- ❖ Определите отправление сообщения-ловушки на сервер NMS через интерфейс MGMT и IPv6-адрес сервера NMS.

Проверка конфигурации

- ❖ Выполните команду **show running** для проверки конфигураций.

Связанные команды

Определите отправление сообщения-ловушки через интерфейс MGMT и IPv4-адрес сервера NMS.

Команда	**snmp-server host oob** *ip-address*
Описание параметров	*ip-address:* **Указывает адрес IPv4.**
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	-

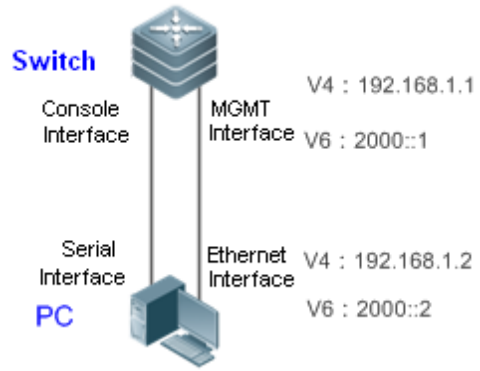
Определите отправление сообщения-ловушки через интерфейс MGMT и IPv6-адрес сервера NMS.

Команда	**snmp-server host oob ipv6** *ipv6-address*
Описание параметров	*Ipv6-address:* **Указывает адрес IPv6.**

Режим команд	Режим глобальной конфигурации
Встроенная подсказка	-

Пример конфигурации

Настройка управления MIB интерфейса MGMT

Сценарий Изображение 14-10	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес интерфейса MGMT коммутатора 3-го уровня на 192.168.1.1. ❖ Настройте IPv6-адрес интерфейса MGMT коммутатора 3-го уровня на 2000::1. ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора. ❖ Настройте адреса IPv4 и IPv6 интерфейса Ethernet ПК на 192.168.1.2 и 2000::2 соответственно. ❖ Включите сервер NMS для ПК на базе IPv4. ❖ Включите сервер NMS для ПК на базе IPv6. ❖ Определите отправление сообщения-ловушки через интерфейс MGMT и IPv4-адрес сервера NMS. ❖ Определите отправление сообщения-ловушки через интерфейс MGMT и IPv4-адрес сервера NMS.

Коммутатор	`QTECH# configure`
	`QTECH(config)# int mgmt 0`
	`QTECH(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0`
	`QTECH(config-if-Mgmt 0)# ipv6 address 2000::1/64`
	`QTECH(config)# snmp-server host oob 192.168.1.2`
	`QTECH(config)# snmp-server host oob ipv6 2000::2`

Проверка конфигурации	❖ Выполните команду **show running** для проверки указанных выше конфигураций на коммутаторе.
Коммутатор	`QTECH# show running	include snmp-server` `snmp-server host oob 192.168.1.2` `snmp-server host oob ipv6 2000::2`

14.4.6 Управление журналом

Сценарий

❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv4-адрес сервера журналирования.
❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv6-адрес сервера журналирования.

Примечания

❖ Недоступно

Этапы конфигурации

Управление журналом

❖ Войдите в глобальный режим.
❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv4-адрес сервера журналирования.
❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv6-адрес сервера журналирования.

Проверка конфигурации

❖ Выполните команду **show running** для проверки конфигураций.

Связанные команды

Определите отправление сообщения журнала через интерфейс MGMT и IPv4-адрес сервера журналирования.

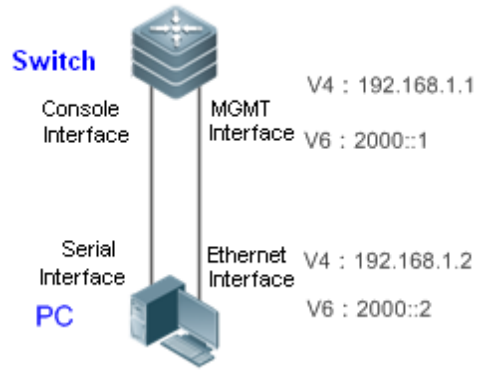
Команда	**logging server oob** *ip-address*
Описание параметров	*ip-address:* **Указывает адрес IPv4.**
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	-

Определите отправление сообщения журнала через интерфейс MGMT и IPv6-адрес сервера журналирования.

Команда	**logging server oob ipv6** *ipv6-address*
Описание параметров	*Ipv6-address:* **Указывает адрес IPv6.**
Режим команд	Режим глобальной конфигурации
Встроенная подсказка	-

Пример конфигурации

Настройка управления MIB интерфейса MGMT

Сценарий Изображение 14-11	
Этапы конфигурации	❖ Подключите последовательный интерфейс ПК к интерфейсу консоли коммутатора. ❖ Настройте IPv4-адрес интерфейса MGMT коммутатора 3-го уровня на 192.168.1.1. ❖ Настройте IPv6-адрес интерфейса MGMT коммутатора 3-го уровня на 2000::1. ❖ Подключите интерфейс Ethernet ПК к интерфейсу MGMT коммутатора. ❖ Настройте адреса IPv4 и IPv6 интерфейса Ethernet ПК на 192.168.1.2 и 2000::2 соответственно. ❖ Включите сервер Syslog для ПК на основе IPv4. ❖ Включите сервер Syslog для ПК на основе IPv6. ❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv4-адрес сервера журналирования. ❖ Определите отправление сообщения журнала через интерфейс MGMT и IPv6-адрес сервера журналирования.

Коммутатор	QTECH# configure QTECH(config)# int mgmt 0 QTECH(config-if-Mgmt 0)# ip address 192.168.1.1 255.255.255.0 QTECH(config-if-Mgmt 0)# ipv6 address 2000::1/64 QTECH(config)# logging server oob *192.168.1.2* QTECH(config)# logging server oob ipv6 *2000::2*
Проверка конфигурации	❖ Выполните команду **show running** для проверки конфигураций.
Коммутатор	QTECH# show running | include logging logging server oob *192.168.1.2* logging server oob ipv6 *2000::2*

14.5 Мониторинг

Отображение

Описание	Команда
Отображает состояние участника и статистическую информацию виртуального интерфейса MGMT.	**show mgmt virtual**

15 НАСТРОЙКА БАЛАНСИРОВЩИКА НАГРУЗКИ

15.1 Обзор

Балансировщик нагрузки — это программа, которая имитирует алгоритм хеширования коммутатора. Балансировщик нагрузки поддерживает режимы балансировки нагрузки агрегированного порта (LAG) и равнозатратной маршрутизации по нескольким путям (ECMP).

- Балансировщик нагрузки агрегированного порта имитирует алгоритм хеширования для расчета пересылки пакетов портом участником на основе поля пакета, режима балансировки нагрузки и указанной информации агрегированного порта. Результат расчета соответствует реальному порту пересылки.

При настройке агрегированного порта на коммутаторе используйте симулятор LAG для расчета пересылки пакетов портом участником, указав поле пакета.

- Балансировщик нагрузки ECMP имитирует алгоритм хеширования для расчета следующего перехода для пересылки пакетов на основе поля пакета и режима балансировки нагрузки. Результат расчета соответствует реальной пересылке по следующему переходу.

Если вы настроили ECMP на коммутаторе и хотите узнать следующий переход для указанных пакетов без выполнения тестов, используйте симулятор ECMP для расчета следующего перехода.

Балансировщик нагрузки может использоваться для отслеживания и мониторинга маршрута пересылки указанных пакетов, что облегчает управление пользователями, а также поиск и устранение неисправностей.

Протоколы и стандарты

- IEEE 802.3ad

15.2 Применение

Применение	Описание
Балансировщик нагрузки агрегированного порта	Объединение нескольких физических каналов в один логический канал является эффективным способом увеличения пропускной способности портов и повышения надежности коммутатора L3. Пакеты пересылаются по физическому каналу в соответствии с алгоритмом балансировки нагрузки. Расчет симулятора LAG позволяет пользователям проверить канал участника, который служит сверочным для поиска и устранения неисправностей и развертывания топологии.
Балансировщик нагрузки ECMP	На коммутаторе L3, настроенном с ECMP, пакеты пересылаются через следующий переход с балансировкой

	нагрузки ECMP. Расчет симулятора ECMP позволяет пользователям проверить канал участника, который служит сверочным для поиска и устранения неисправностей и развертывания топологии.

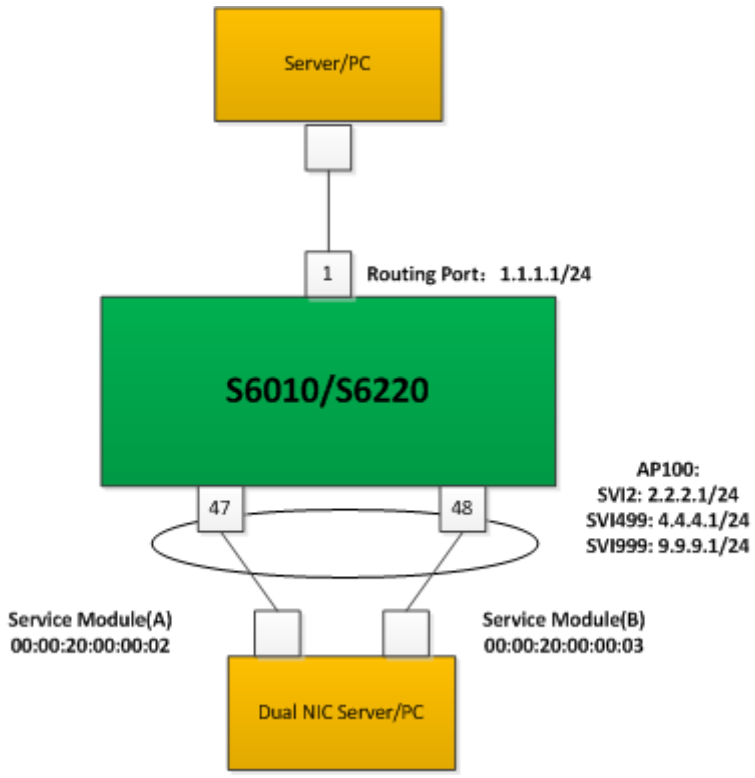
15.2.1 Балансировщик нагрузки LAG

Сценарий

С помощью Балансировщика нагрузкиможно рассчитать пересылку с балансировкой нагрузки на агрегированном порте.

- ❖ Распределение нагрузки LAG: Сервер с двумя сетевыми картами объединен в один логический канал для обмена служебными данными.
- ❖ 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, отправленные вышестоящим сервером.

Изображение 15-1



Описание

- ❖ Порты, соединяющие сервер с двумя сетевыми картами и коммутаторами, объединяются в точку доступа для совместного использования потока данных службы.
- ❖ Используйте VLAN 2, VLAN 499 и VLAN 999 для разделения сети и предоставления различных видов услуг.
- ❖ В соответствии с функционалом пакетов можно определить агрегированный порт пересылки с балансировкой нагрузки.

Функционалом пакетов могут быть IP-адрес источника, IP-адрес назначения, порт источника L4 или порт назначения L4.

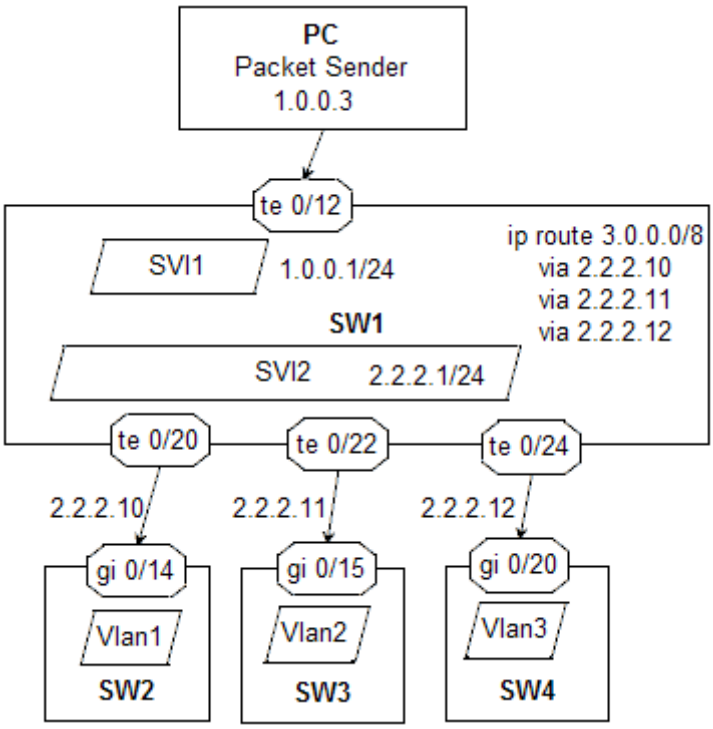
15.2.2 Балансировщик нагрузки ECMP

Сценарий

С помощью Балансировщика нагрузкиможно рассчитать следующий переход с балансировкой нагрузки ECMP.

- SW1 подключен к сегменту сети по восходящему каналу 1.0.0.0/24 и подключен к сегменту сети 2.2.2.0/24 по нисходящему каналу. ПК восходящего канала может обмениваться данными с клиентами нисходящего канала через SW1.
- Вы должны знать, какой порт нисходящего канала может принимать или пересылать пакеты, содержащие разные IP-адреса, отправленные с ПК восходящего канала.

Изображение 15-2



Описание

- Настройте маршрут ECMP на 3.0.0.0/8 на SW1 и соедините несколько последующих переходов ECMP с нисходящим каналом.
- В соответствии с функционалом пакетов можно определить следующий переход на SW1 с балансировкой нагрузки ECMP.

Функционалом пакетов могут быть IP-адрес источника, IP-адрес назначения, порт источника L4 или порт назначения L4.

15.3 Функции

Базовые концепции

Агрегированный порт

Агрегированный порт — это логический порт, который состоит из нескольких физических портов. Агрегированный порт может быть разделен на статический LAG и динамический LAG (LACP LAG) на основе протокола или на агрегированные порты уровня L2 и L3 на основе функции порта.

L2 LAG

Агрегированный порт L2 — это логический порт, который состоит из нескольких портов L2 с одинаковыми функциями L2.

L3 LAG

Агрегированный порт L3 — это логический порт, который состоит из нескольких портов L3 с одинаковыми функциями L3.

Режим балансировки нагрузки

Пакеты пересылаются портом участником LAG в зависимости от режима балансировки нагрузки. Доступны следующие режимы балансировки нагрузки LAG:

- Mac-адрес источника/MAC-адрес назначения (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 + порт источника L4 + порт назначения L4 (Src-dst-ip-l4port)
- Панельный порт для входящих пакетов
- Расширенный режим

ECMP

ECMP — это стратегия маршрутизации, в которой пересылка пакетов следующего перехода на одно назначение может осуществляться по нескольким «лучшим путям», которые становятся приоритетными при расчетах метрик маршрутизации. Когда следующий переход становится недоступным, трафик переключается на другой следующий переход.

Следующий переход ECMP также выбирается в зависимости от режима балансировки нагрузки.

Балансировщик нагрузки

Балансировщик нагрузки — это программа, которая имитирует алгоритм хеширования коммутатора.

Quintuple

Quintuple означает IP-адрес источника, IP-адрес назначения, протокол, порт источника L4 и порт назначения L4.

Обзор

Обзор	Описание
Балансировщик нагрузки LAG	Вычисляет порт участника LAG для пересылки пакетов в соответствии с полем пакета, режимом балансировки нагрузки LAG и указанной информацией об LAG.
Балансировщик нагрузки ECMP	Вычисляет следующий переход для пересылки пакетов в соответствии с полем пакета, режимом балансировки нагрузки и IP-адресом назначения.

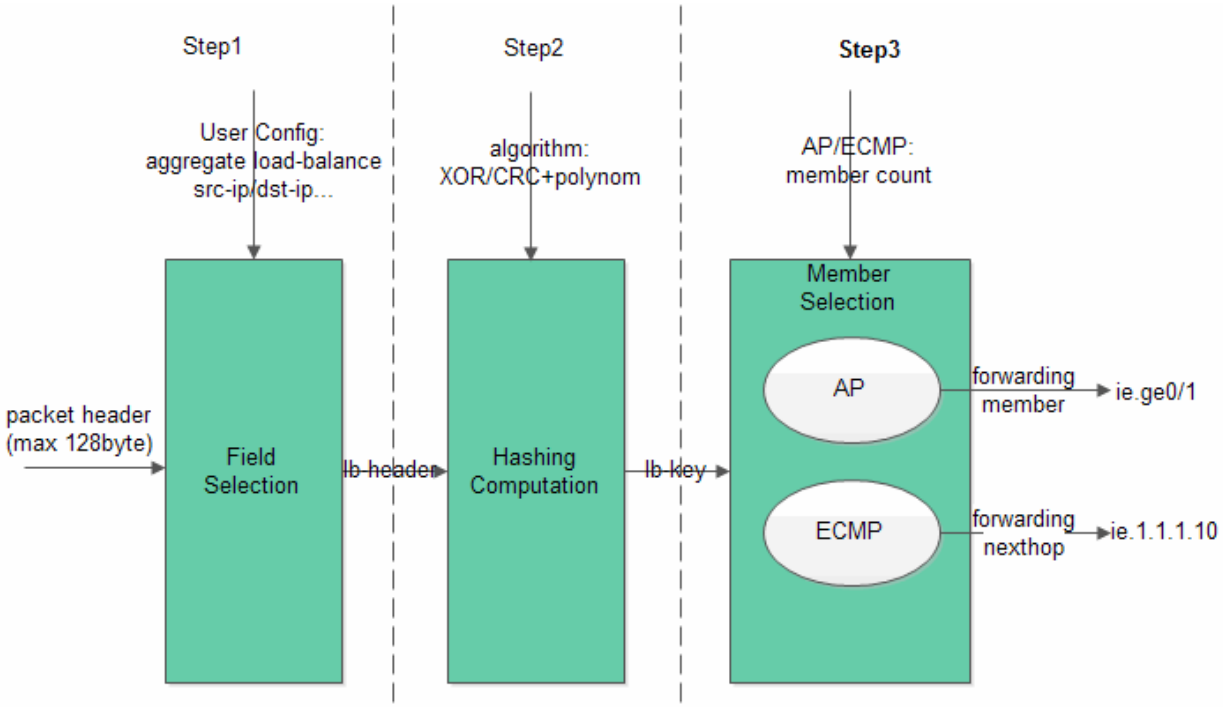
15.3.1 Балансировщик нагрузки LAG

Балансировщик нагрузки LAG используется для расчета порта-участника LAG для пересылки пакетов путем указания поля пакета.

Принцип работы

Балансировщик нагрузки имитирует алгоритм хеширования на коммутаторе. Процесс расчета балансировки нагрузки LAG на коммутаторе выполняется следующим образом:

Изображение 15-3



❖ Шаг 1: Выбор поля. Поля извлекаются в соответствии с настроенным режимом балансировки нагрузки.

В зависимости от настроенного режима балансировки нагрузки в качестве ХЕШ-факторов выбираются различные поля:

Режим балансировки нагрузки	ХЕШ-фактор
Src-mac	Mac-адреса источника
Dst-mac	Mac-адрес назначения
Src-dst-mac	Mac-адреса источника и назначения
Src-ip	IP-адрес источника
Dst-ip	IP-адрес назначения
Src-dst-ip	IP-адреса источника и назначения
Src-dst-ip-l4port	IP-адреса источника и назначения, L4 порт источника и L4 порт назначения
Расширенные настройки	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.

Балансировщик нагрузки LAG поддерживает режимы src-ip, dst-ip, src-dst-ip, src-dst-ip-l4port и режим улучшенной балансировки нагрузки.

Выбранные режимы ХЕШ-симуляции для балансировки нагрузки LAG могут отличаться в зависимости от различных коммутаторов.

❖ Шаг 2: Вычисление хеша

ХЕШ-алгоритм используется для вычисления ХЕШ-ключа lb-key (ключ балансировки нагрузки) на основе ХЕШ-фактора, выбранного в шаге 1. ХЕШ-алгоритмы различаются в зависимости от разных моделей коммутаторов, поддерживаются такие алгоритмы как XOR, CRC и CRC+ скрэмблирование.

Балансировщик нагрузки имитирует алгоритм хеширования на коммутаторе.

❖ Шаг 3: Выбор участника

Разделите номер участника LAG на ключ хеширования lb-key, остатком будет порядковый номер порта передачи. Порядковый номер уникален для коммутаторов QTECH (включая коммутаторы уровня ядра и уровня доступа). Поэтому его можно использовать для идентификации порта передачи.

Связанная конфигурация

Отображение результатов расчета симулятора LAG.

Пользователи могут проверить порт пересылки IPv4 LAG с балансировкой нагрузки, указав quintuple функций пакета IPv4.

Пользователи могут проверить порт пересылки IPv6 LAG с балансировкой нагрузки, указав quintuple функций пакета IPv6.

Балансировщик нагрузки LAG поддерживает одновременный расчет только пересылки одноадресных пакетов.

15.3.2 Балансировщик нагрузки ECMP

Балансировщик нагрузки ECMP используется для расчета пересылки пакетов по следующему переходу путем указания поля пакета.

Принцип работы

Балансировщик нагрузки ECMP имитирует алгоритм хеширования, аналогичный Балансировщик нагрузкиу LAG.

- Шаг 1: Выбор поля. Поля извлекаются в соответствии с настроенным режимом балансировки нагрузки.

Режимы балансировки нагрузки ECMP совместно используют конфигурацию с режимами балансировки нагрузки LAG. Режимы балансировки нагрузки соответствуют ХЕШ-факторам:

Режим балансировки нагрузки	ХЕШ-фактор
Src-mac	IP-адрес источника
Dst-mac	IP-адрес источника
Src-dst-mac	IP-адрес источника
Src-ip	IP-адрес источника
Dst-ip	IP-адреса источника и назначения
Src-dst-ip	IP-адреса источника и назначения
Src-dst-ip-l4port	IP-адреса источника и назначения, L4 порт источника и L4 порт назначения
Расширенные настройки	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.

Балансировщик нагрузки ECMP поддерживает режимы src-ip, dst-ip, src-dst-ip, src-dst-ip-l4port и режим улучшенной балансировки нагрузки.

Выбранные режимы ХЕШ-симуляции для балансировки нагрузки ECMP отличаются в зависимости от различных коммутаторов.

⚠ Для некоторых коммутаторов, режимы балансировки нагрузки соответствуют ХЭШ-факторам. Например, режим src-mac соответствует ХЭШ-фактору MAC-адреса источника; режим dst-mac соответствует ХЭШ-фактору MAC-адреса назначения.

❖ Шаг 2: Вычисление хеша

ХЕШ-алгоритм используется для вычисления ХЕШ-ключа lb-key (ключ балансировки нагрузки) на основе ХЕШ-фактора, выбранного в шаге 1. Балансировка нагрузки ECMP поддерживает алгоритмы хеширования CRC и CRC+ со скрэмблированием.

❖ Шаг 3: Выбор участника

Разделите число следующего перехода ECMP на ХЭШ-ключ lb-key, а остаток будет номером следующего перехода. Уникальный индекс может использоваться для идентификации следующего перехода.

Связанная конфигурация

Отображение результатов расчета симулятора ECMP.

Пользователи могут проверить следующий переход IPv4 при балансировке нагрузки ECMP, указав quintuple функций пакета IPv4.

Пользователи могут проверить следующий переход IPv6 при балансировке нагрузки ECMP, указав quintuple функций пакета IPv6.

ℹ Если следующий переход ECMP является LAG, порт передачи выбирается в зависимости от режима балансировки нагрузки LAG. Пользователи могут ввести команду для отображения порта передачи пакетов.

15.4 Конфигурация

Конфигурация	Описание и команда	
Отображение порта передачи LAG с балансировкой нагрузки	Дополнительно	
	show aggregate load-balance to interface aggregateport *LAG-id* **ip** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	Отображает порт пересылки IPv4 LAG с балансировкой нагрузки
	show aggregate load-balance to interface aggregateport *LAG-id* **ipv6** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]	Отображает порт пересылки IPv6 LAG с балансировкой нагрузки
Отображение порта передачи ECMP с	**show ip ecmp-nexthop address destination** *dest-ip* [**source**	Отображает следующий переход IPv4 ECMP

балансировкой нагрузки	*source-ip*] [**protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dst-port*]] [**vrf** *vrf-name*]	
	show ipv6 ecmp-nexthop address destination *dest-ip* [**source** *source-ip*] [**next-header** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dst-port*]] [**vrf** *vrf-name*]	Отображает следующий переход IPv6 ECMP

15.4.1 Отображение порта передачи LAG с балансировкой нагрузки

Сценарий

- Отображение порта участника LAG для пересылки пакетов.

Примечания

- Балансировщик нагрузки LAG работает в режиме балансировки нагрузки LAG. Поэтому, сначала используйте команду aggregate load-balance для настройки режима балансировки LAG.
- Создайте агрегированный порт и добавьте порты-участники.

См. раздел Настройка агрегированного порта в Руководстве по настройке коммутатора Ethernet.

Этапы конфигурации

Отображение порта передачи IPv4 LAG с балансировкой нагрузки

- Отследите маршрут пересылки и устраните неполадки.
- Введите команду для отображения портов передачи LAG на коммутаторе.

Отображение порта передачи IPv6 LAG с балансировкой нагрузки

- То же самое, что и выше.

Проверка конфигурации

- Проверьте конфигурацию, подкачивая реальный трафик. Проверьте и запишите порт передачи.
- Проверьте, соответствует ли реальный порт передачи отображаемому порту.

Связанные команды

Отображение порта передачи IPv4 LAG с балансировкой нагрузки

Команда	**show aggregate load-balance to interface aggregateport** *LAG-id* **ip** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]
Параметр	**aggregateport** *LAG-id*: Идентификатор LAG назначения. **source** *source-ip*: Адрес IPv4 источника

	destination *dest-ip*: Адрес IPv4 назначения **ip-protocol** *protocol-id*: Идентификатор IP-протокола. Например, идентификаторы протокола TCP и UDP - 6 и 17 соответственно. **l4-source-port** *src-port*: Идентификатор порта L4-источника **l4-dest-port** *dst-port*: Идентификатор порта L4-назначения
Режим команд	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Отображает порт пересылки IPv6 LAG с балансировкой нагрузки

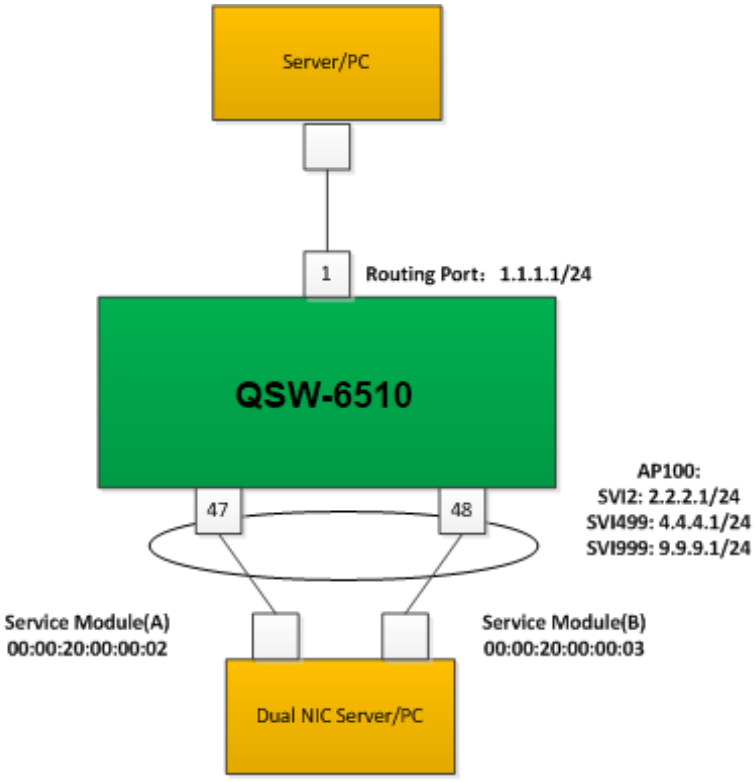
Команда	**show aggregate load-balance to interface aggregateport** *LAG-id* **ipv6** [**source** *source-ip*] [**destination** *dest-ip*] [**ip-protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dest-port*]
Параметр	**aggregateport** *LAG-id*: Идентификатор LAG назначения **source** *source-ip*: Адрес IPv6 источника **destination** *dest-ip*: Адрес IPv6 назначения **ip-protocol** *protocol-id*: Идентификатор IP-протокола. Например, идентификаторы протокола TCP и UDP - 6 и 17 соответственно. **l4-source-port** *src-port*: Идентификатор порта L4-источника **l4-dest-port** *dst-port*: Идентификатор порта L4-назначения
Режим команд	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Типичные ошибки

- Балансировщик нагрузки LAG не поддерживает настроенный режим балансировки нагрузки.
- Текущий коммутатор не поддерживает Балансировщик нагрузки LAG.
- Агрегированный порт не создан или не имеет портов-участников.

Пример конфигурации

Отображает порт пересылки IPv4 LAG с балансировкой нагрузки

Сетевая среда Изображение 15-4	

Этапы конфигурации	❖ 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 конфигурации	❖ Используйте команду **show aggregate load-balance** для отображения порта передачи LAG.
	❖ Отобразите порт передачи LAG с балансировкой нагрузки для пакетов, предназначенных для IP-адреса 2.2.2.2.
	`QTECH# show aggregate load-balance to interface aggregateport 1 ip destination 2.2.2.2`
	`aggregateport load-balance mode : Destination IP`
	`balance to port : GigabitEthernet 0/47`
	❖ Отобразите порт передачи LAG с балансировкой нагрузки для пакетов, предназначенных для IP-адреса 4.4.4.4.
	`QTECH# show aggregate load-balance to interface aggregateport 1 ip destination 4.4.4.4`
	`aggregateport load-balance mode : Destination IP`
	`balance to port : GigabitEthernet 0/48`

	❖ Если у указанного LAG нет портов-участников, порт передачи отображается как NULL.
	`QTECH# show aggregate load-balance to interface aggregateport 1 ip source 1.1.1.1`
	`aggregateport load-balance mode : Destination IP`
	`balance to port :`

15.4.2 Отображение порта передачи ECMP с балансировкой нагрузки

Сценарий

❖ Отображение следующего перехода ECMP для пересылки пакетов.

Примечание

❖ Только следующие зоны доступа идут с балансировкой нагрузки.

Этапы конфигурации

Отображает следующий переход IPv4 ECMP

❖ Отслеживание маршрута пересылки и устранение неполадок.
❖ Введите команду для отображения портов передачи LAG на коммутаторе.

Отображает следующий переход IPv6 ECMP

❖ То же самое, что и выше

Проверка конфигурации

❖ Проверьте конфигурацию, подкачивая реальный трафик. Наблюдайте и запишите следующий переход для пересылки трафика.
❖ Проверьте, соответствует ли реальный следующий переход отображаемому следующему переходу.

Связанные команды

Отображает следующий переход IPv4 ECMP

Команда	**show ip ecmp-nexthop address destination** *dest-ip* [**source** *source-ip*] [**protocol** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dst-port*] [**vrf** *vrf-name*]
Параметр	**source** *source-ip*: Адрес IPv4 источника **destination** *dest-ip*: Адрес IPv4 назначения **protocol** *protocol-id*: Идентификатор IP-протокола. Например, идентификаторы протокола TCP, UDP и ICMP - 6, 17 и 1 соответственно. **l4-source-port** *src-port*: Идентификатор порта L4-источника **l4-dest-port** *dst-port*: Идентификатор порта L4-назначения **vrf** *vrf-name*: Имя VRF

Режим команд	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

Отображает следующий переход IPv6 ECMP

Команда	**show ipv6 ecmp-nexthop address destination** *dest-ip* [**source** *source-ip*] [**next-header** *protocol-id*] [**l4-source-port** *src-port*] [**l4-dest-port** *dst-port*] [**vrf** *vrf-name*]
Параметр	**source** *source-ip*: Адрес IPv6 источника **destination** *dest-ip*: Адрес IPv6 назначения **next-header** *protocol-id*: Идентификатор IP-протокола. Например, идентификаторы протокола TCP, UDP и ICMP - 6, 17 и 1 соответственно. **l4-source-port** *src-port*: Идентификатор порта L4-источника **l4-dest-port** *dst-port*: Идентификатор порта L4-назначения **vrf** *vrf-name*: Имя VRF
Режим команд	Привилегированный режим EXEC/режим глобальной конфигурации/режим конфигурации интерфейса
Встроенная подсказка	Недоступно

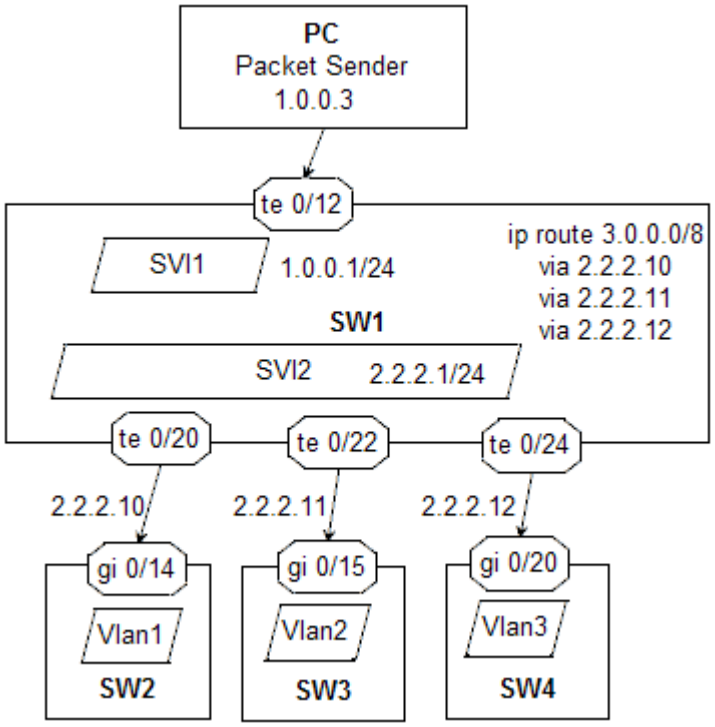
Типичные ошибки

- Балансировщик нагрузки ECMP не поддерживает настроенный режим балансировки нагрузки.
- Текущий коммутатор не поддерживает Балансировщик нагрузки ECMP.
- ECMP не настроен или недоступен следующий переход.

Пример конфигурации

Отображает следующий переход IPv4 ECMP

Сетевая среда Изображение 15-5	



Этапы конфигурации

- 1. Настройте ECMP.
- 2. Настройте режим балансировки нагрузки.

```
QTECH# configure terminal
QTECH(config)# aggregate load-balance src-dst-ip
QTECH(config)# show agg load-balance
Load-balance    : Source IP and Destination IP
QTECH(config)# end
```

Проверка конфигурации

Используйте команду **show ip ecmp-nexthop** для отображения маршрута в vrf 0. Следующий переход канала-прострела отмечен «*». Параметр DIP является обязательным для расчета ХЕША. Балансировщик нагрузки ECMP можно использовать для расчета одного следующего перехода для одноадресного маршрута.

- Отобразите следующий переход с балансировкой нагрузки ECMP для пакетов от 1.0.0.1 до 3.0.0.1. Измените IP-адрес назначения на 3.0.0.2 и снова отобразите следующий переход.

```
QTECH#show ip ecmp-nexthop address destination 3.0.0.1 source 1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
```

```
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1 *
  via 2.2.2.12 weight 1
QTECH#show ip ecmp-nexthop address destination 3.0.0.2 source
1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1
  via 2.2.2.12 weight 1 *
```

❖ Если DIP в введенной команде CLI не попал в таблицу маршрутизации, отображается ошибка.

```
QTECH#show ip ecmp-nexthop address destination 5.0.0.1 source
1.0.0.7
%ecmp HASH failed, for look up time out or no route hitted
```

❖ Отобразите следующий переход с балансировкой нагрузки ECMP для пакетов от 1.0.0.1 до 3.0.0.1. Измените IP-адрес источника на 1.0.0.3 и снова отобразите следующий переход.

```
QTECH#show ip ecmp-nexthop address destination 3.0.0.1 source
1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1 *
  via 2.2.2.12 weight 1
QTECH#show ip ecmp-nexthop address destination 3.0.0.1 source
1.0.0.3
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1 *
  via 2.2.2.11 weight 1
  via 2.2.2.12 weight 1
```

❖ Канал следующего перехода ECMP погашен. Снова отобразите симулированный следующий переход.

```
QTECH#show arp
Protocol   Address              Age(min)   Hardware            Type
Interface
Internet  2.2.2.11         <static>  0000.0000.0011  arpa   VLAN 2
Internet  2.2.2.12         <static>  0000.0000.0012  arpa   VLAN 2
Internet  1.0.0.1          --        00d0.f822.33b2  arpa   VLAN 1
Internet  2.2.2.1          --        00d0.f822.33b2  arpa   VLAN 2
Internet  2.2.2.10         <--->     <Incomplete>    arpa   VLAN 2
```

❖ Снова отобразите следующий переход с балансировкой нагрузки ECMP для пакетов от 1.0.0.1 до 3.0.0.1, до 3.0.0.2 и до 3.0.0.6 соответственно.

```
QTECH#show ip ec ad de 3.0.0.1 so 1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1 *
  via 2.2.2.12 weight 1
QTECH#show ip ec ad de 3.0.0.2 so 1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1
  via 2.2.2.12 weight 1 *
QTECH#show ip ec ad de 3.0.0.6 so 1.0.0.1
balance mode:   Source IP and Destination IP
route table:    vrf 0
hit ip route, actual nexthop marked by "*":
3.0.0.0/8
  via 2.2.2.10 weight 1
  via 2.2.2.11 weight 1 *
  via 2.2.2.12 weight 1
```