QTECH
МИР ДОСТУПНЕЕ

КОНФИГУРАЦИЯ VLAN

Коммутатор агрегации

СЕРИЯ QSW-8400

Оглавление

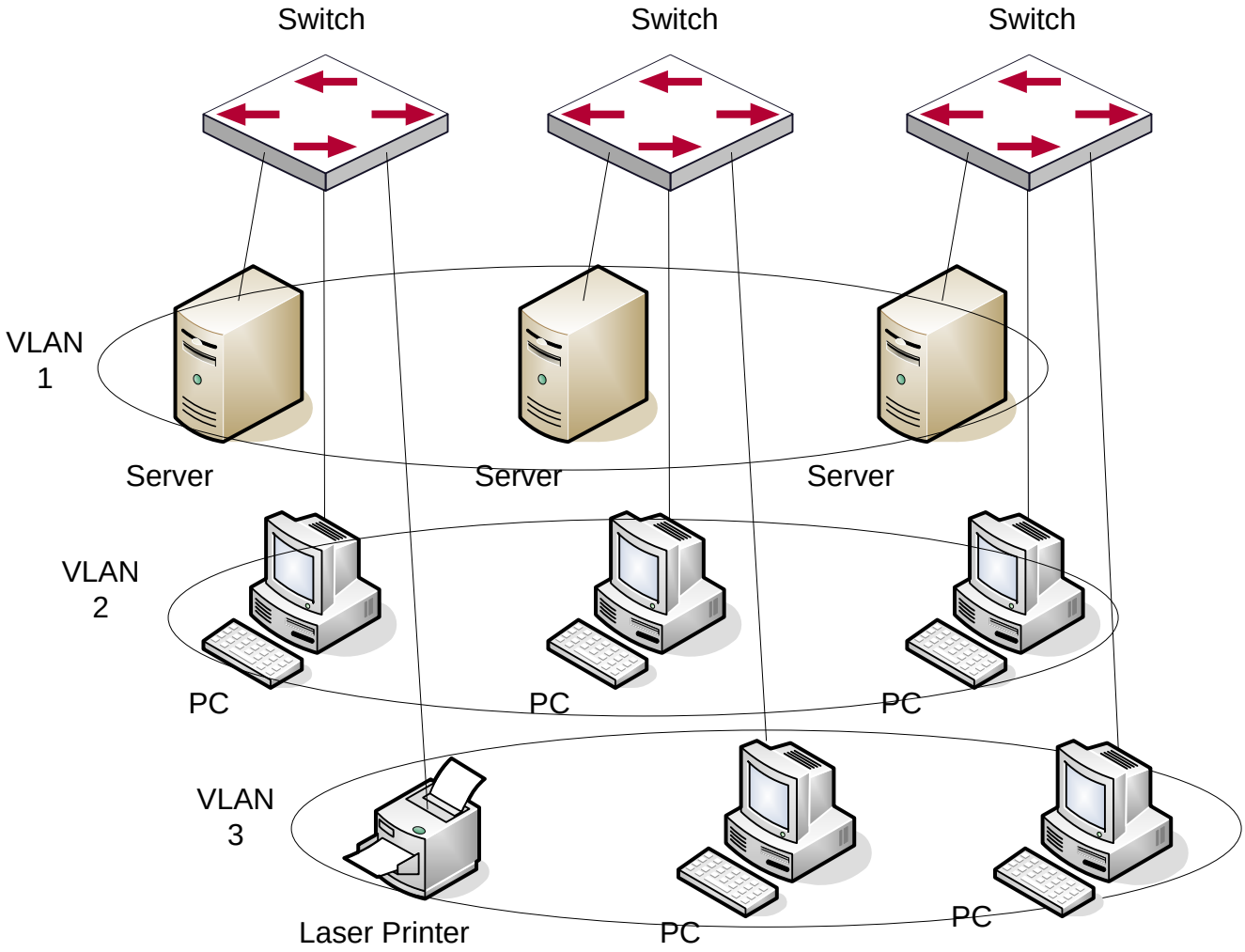
1 КОНФИГУРИРОВАНИЕ VLAN

1.1 Конфигурирование VLAN

1.1.1 Начальные сведения о VLAN

VLAN (Virtual Local Area Network – виртуальная локальная сеть) – технология, разделяющая логические адреса устройств в сети для отделения сегментов сети в зависимости от функций, выполняемых устройствами, приложений или требований управления. Таким образом, виртуальные локальные группы могут формироваться независимо от физического расположения устройств. IEEE опубликовал протокол IEEE 802.1Q для стандартизации применения VLAN. VLAN на коммутаторе работает в соответствии с этим протоколом.

Основная идея технологии VLAN в том, чтобы разделить динамически большую локальную сеть на несколько независимых широковещательных доменов в соответствии с требованиями, предъявляемыми к сети.



Каждый широковещательный домен на рисунке является VLAN. Сети VLAN имеют те же

свойства, что и физические сети, за исключением того, что VLAN – логическое объединение, а не физическое. Поэтому объединение сетей VLAN может создаваться вне зависимости от физического расположения устройств и широковещательный, многопользовательский и однопользовательский трафик внутри VLAN отделен от других сетей VLAN.

Благодаря вышеперечисленным особенностям, технология VLAN обеспечивает

следующие преимущества:

- Улучшается производительность сети;
- Экономятся сетевые ресурсы;
- Упрощается управление сетью;
- Снижается стоимость сети;
- Улучшается безопасность сети;

Ethernet порты коммутатора могут работать в трех различных режимах: Access, Hybrid и Trunk. Каждый режим имеет свой способ пересылки пакетов, с меткой или без.

Порты типа Access принадлежат только одному VLAN. Обычно они используются для подключения к компьютеру.

Порты типа Trunk позволяют пересылать пакеты нескольких VLAN. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств.

Порты типа Hybrid также позволяют пересылать пакеты нескольких VLAN. Они могут использоваться для соединения между коммутаторами или подключения пользовательских устройств.

Порты типов Hybrid и Trunk принимают данные по одному алгоритму, но методы отправки данных отличаются: порты типа Hybrid могут отправлять пакеты в различные VLAN без метки VLAN, тогда как порты типа Trunk отправляют пакеты различных VLAN только с меткой VLAN, за исключением VLAN, прописанного на порту как native.

Применение VLAN и GVRP (GARP VLAN Registration Protocol – протокол регистрации GARP VLAN) на коммутаторе описывается в стандарте 802.1Q. Данная глава детально объясняет использование и конфигурацию VLAN и GVRP.

1.1.2 Конфигурирование VLAN

1. Создание или удаление VLAN.

Команда	Описание
Режим глобального конфигурирования	
vlan WORD **no vlan WORD**	Создание/удаление VLAN или вход в режим VLAN

2. Установка или удаление имени VLAN.

Команда	Описание
VLAN Mode	
name <vlan-name> **no name**	Установка или удаление имени VLAN

3. Присоединение порта коммутатора к VLAN.

Команда	Описание
VLAN Mode	
switchport interface <*interface-list*> **no switchport interface <*interface-list*>**	Назначение порта коммутатора VLAN

4. Установка типа порта коммутатора.

Команда	Описание
Режим конфигурирования порта	
switchport mode {trunk | access | hybrid}	Установка текущего порта как транкового, порта доступа или гибридного.

5. Настройка транкового порта.

Команда	Описание
Режим конфигурирования порта	
switchport trunk allowed vlan {WORD | all | add WORD | except WORD | remove WORD}	Установка/удаление VLAN, приписанных к этому транку. Команда “no” восстанавливает значение по

no switchport trunk allowed vlan	умолчанию.
switchport trunk native vlan <*vlan-id*> **no switchport trunk native vlan**	Установка/удаление PVID для транкового порта.

6. Настройка порта доступа

Команда	Описание
Режим конфигурирования порта	
switchport access vlan <*vlan-id*> **no switchport access vlan**	Добавляет текущий порт к указанному VLAN. Команда NO восстанавливает значение по умолчанию.

7. Настройка гибридного порта.

Команда	Описание
Режим конфигурирования порта	
switchport hybrid allowed vlan {WORD | all | add WORD | except WORD | remove WORD} {tag | untag} **no switchport hybrid allowed vlan**	Установка/удаление VLAN, приписанного к гибридному порту с режимом метки или без нее.
switchport hybrid native vlan <*vlan-id*> **no switchport hybrid native vlan**	Установка/удаление PVID на порту.

8. Включение/выключение правил обработки входных пакетов VLAN на портах.

Команда	Описание
Режим конфигурирования порта	
vlan ingress enable **no vlan ingress enable**	Включение/выключение входящих правил на VLAN.

9. Конфигурация приватного VLAN.

Команда	Описание
VLAN mode	
private-vlan {primary | isolated | community} **no private-vlan**	Конфигурация текущего VLAN как приватного. Команда NO удаляет приватный VLAN.

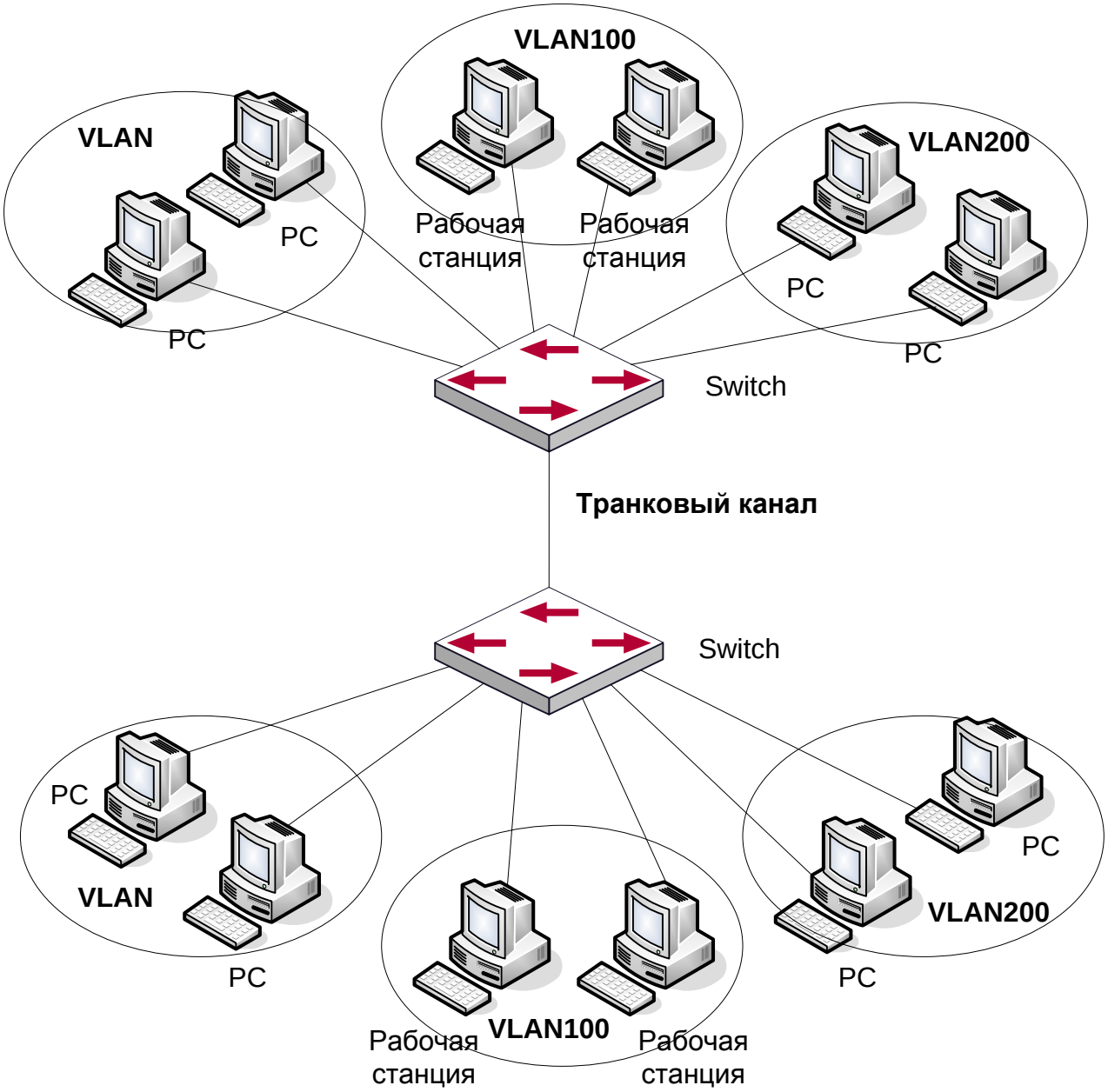
10. Настройка связей приватного VLAN.

Команда	Описание
VLAN mode	
private-vlan association <secondary-vlan-list> **no private-vlan association**	Установка/удаление связей приватного VLAN.

11. Определение внутреннего идентификатора VLAN.

Команда	Описание
Режим глобального конфигурирования	
vlan <2-4094> internal	Определяет идентификатор внутреннего VLANa.

1.1.3 Типичное применение VLAN



В соответствии с требованиями приложений и безопасности существующую локальную сеть необходимо разделить на три VLAN. Три VLAN имеют идентификаторы VLAN2, VLAN100 и VLAN200. Эти три VLAN охватывают два различных физических места размещения: площадки A и B.

На каждой площадке имеется коммутатор, требования к связи между площадками удовлетворяются, если коммутаторы могут выполнять обмен трафиком VLAN.

Объект конфигурации	Описание конфигурации
VLAN2	Site A and site B switch port 2 -4.

VLAN100	Site A and site B switch port 5 -7.
VLAN200	Site A and site B switch port 8 -10.
Trunk port	Site A and site B switch port 11.

Транковые порты с обеих сторон подключены к транковому каналу для передачи между узлами трафика VLAN. Остальные устройства подключены к другим портам VLAN.

В данном примере порты 1 и 12 свободны и могут быть использованы для управляющих портов или других целей.

Шаги конфигурации описаны ниже:

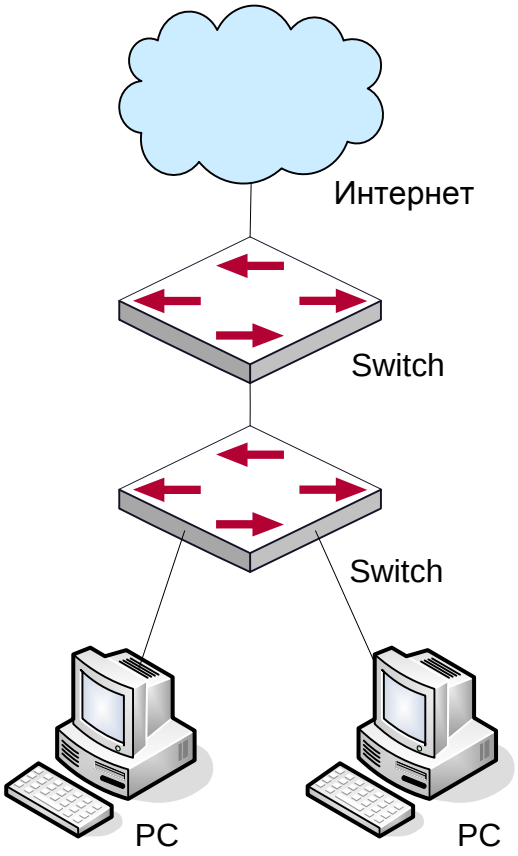
Коммутатор A:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/0/2-4
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/5-7
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/0/8-10
Switch(Config-Vlan200)#exit
Switch(config)#interface ethernet 1/0/11
Switch(Config-If-Ethernet1/0/11)#switchport mode trunk
Switch(Config-If-Ethernet1/0/11)#exit
Switch(config)#
```

Коммутатор B:

```
Switch(config)#vlan 2
Switch(Config-Vlan2)#switchport interface ethernet 1/0/2-4
Switch(Config-Vlan2)#exit
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/5-7
Switch(Config-Vlan100)#exit
Switch(config)#vlan 200
Switch(Config-Vlan200)#switchport interface ethernet 1/0/8-10
Switch(Config-Vlan200)#exit
Switch(config)#interface ethernet 1/0/11
Switch(Config-If-Ethernet1/0/11)#switchport mode trunk
Switch(Config-If-Ethernet1/0/11)#exit
```

1.1.4 Типичное применение гибридных портов



PC1 подключен к интерфейсу Ethernet 1/0/7 коммутатора B, PC2 подключен к интерфейсу Ethernet 1/0/9 коммутатора B. Порт Ethernet 1/0/10 коммутатора A к порту Ethernet 1/0/10 коммутатора B.

Требуется, чтобы PC1 и PC2 не видели друг друга по соображениям секретности. Но PC1 и PC2 должны иметь доступ к другим сетевым ресурсам через шлюз коммутатора A. Мы можем реализовать эту схему через гибридный порт.

Конфигурация объектов как описано ниже:

Порт	Тип	PVID	Пропускаемые VLAN
Port 1/0/10 of Switch A	Access	10	Пропускает пакеты VLAN 10 без меток.
Port 1/0/10 of Switch B	Hybrid	10	Пропускает пакеты VLAN 7,9, 10 без меток.
Port 1/0/7 of Switch B	Hybrid	7	Пропускает пакеты VLAN 7, 10 без меток
Port 1/0/9 of Switch B	Hybrid	9	Пропускает пакеты VLAN 9, 10 без

			меток.

Шаги конфигурации описаны ниже:

Коммутатор A:

```
Switch(config)#vlan 10
Switch(Config-Vlan10)#switchport interface ethernet 1/0/10
```

Коммутатор B:

```
Switch(config)#vlan 7;9;10
Switch(config)#interface ethernet 1/0/7
Switch(Config-If-Ethernet1/0/7)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/7)#switchport hybrid native vlan 7
Switch(Config-If-Ethernet1/0/7)#switchport hybrid allowed vlan 7;10 untag
Switch(Config-If-Ethernet1/0/7)#exit
Switch(Config)#interface Ethernet 1/0/9
Switch(Config-If-Ethernet1/0/9)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/9)#switchport hybrid native vlan 9
Switch(Config-If-Ethernet1/0/9)#switchport hybrid allowed vlan 9;10 untag
Switch(Config-If-Ethernet1/0/9)#exit
Switch(Config)#interface Ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode hybrid
Switch(Config-If-Ethernet1/0/10)#switchport hybrid native vlan 10
Switch(Config-If-Ethernet1/0/10)#switchport hybrid allowed vlan 7;9;10 untag
Switch(Config-If-Ethernet1/0/10)#exit
```

1.2 Конфигурирование GVRP

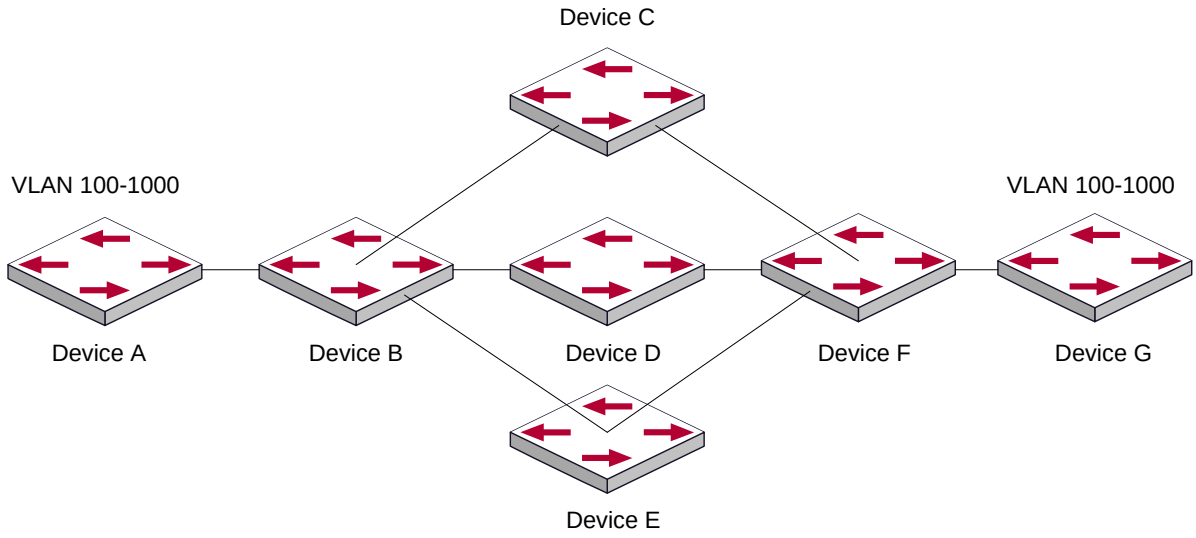
1.2.1 Общая информация о GVRP

Протокол GARP (Generic Attribute Registration Protocol), используется для динамического распределения, распространения и регистрации атрибутов информации между коммутаторами-членами в сети коммутации.

Атрибутом может быть информация VLAN, групповой MAC-адрес и так далее. Очевидно, что протокол GARP может транспортировать множество атрибутов на коммутатор, на который их необходимо передать (populate). На основе GARP определены различные приложения (называемые приложениями-объектами GARP), одним из них является GVRP.

Протокол GVRP (GARP VLAN Registration Protocol) — это приложение, использующее для работы механизм GARP. Оно отвечает за обслуживание информации динамической регистрации VLAN и передачу регистрационной информации на другие коммутаторы. Коммутаторы, поддерживающие GVRP могут принимать информацию динамической регистрации VLAN от других коммутаторов и обновлять локальную информацию регистрации VLAN в соответствии с принятой.

Коммутатор, на котором включен протокол GVRP, может передавать свою собственную информацию регистрации VLAN на другие коммутаторы. Принятая информация содержит локальную статическую информацию, заданную вручную и динамическую информацию, полученную обучением от других коммутаторов. Поэтому, за счет передачи информации регистрации VLAN, состоятельная информация VLAN может быть распространена на все коммутаторы с включенным GVRP.



Коммутаторы A и G не соединены между собой на сети второго уровня; B,C,D,E,F промежуточные коммутаторы, подключенные к A и G. На коммутаторах A и G сконфигурировали VLAN100-1000 вручную, тогда как на B,C,D,E,F их нет. Когда GVRP выключен, A и G не могут ни с кем соединиться, поскольку промежуточные узлы не имеют соответствующих VLAN. Однако после включения GVRP на всех узлах, его механизм передачи атрибутов VLAN позволяет промежуточным узлам регистрировать VLAN динамически, и VLAN в VLAN100-1000 узлов A и G могут соединяться с любым другим. Все VLAN, динамически зарегистрированные на промежуточных узлах, будут разрегистрированы, когда на узлах A и G вручную удалятся VLAN100-1000. Таким образом, одинаковые VLAN двух не соседних узлов могут соединяться посредством протокола GVRP вместо ручной конфигурации всех промежуточных узлов для получения простой конфигурации VLAN.

1.2.2 Настройка GVRP

1. Конфигурация таймера GARP.

Команда	Описание
Режим глобального конфигурирования	
garp timer join <200-500>	Конфигурирование таймеров

garp timer leave <500-1200> **garp timer leaveall <5000-60000>** **no garp timer (join | leave | leaveAll)**	удержания, слияния и выхода для GARP.

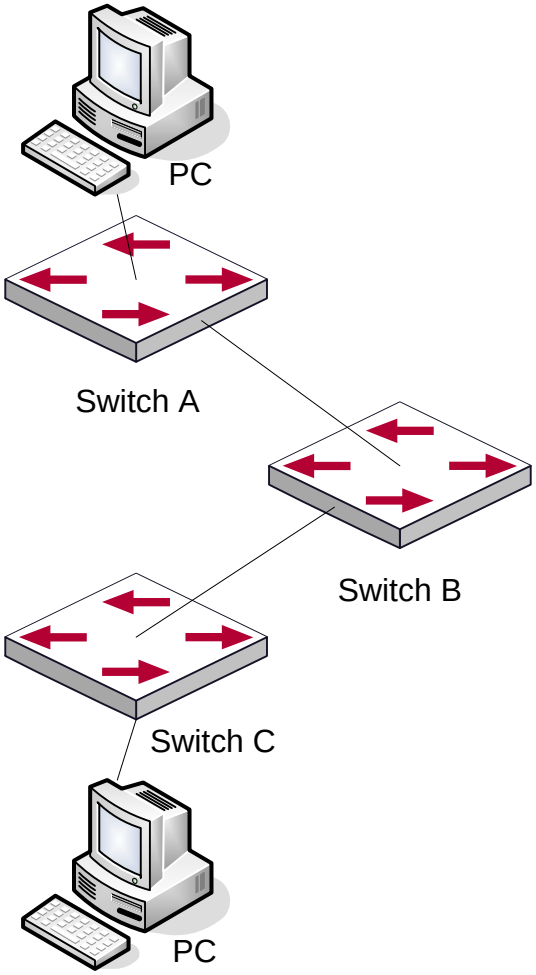
2. Включение/выключение функции GVRP на порту.

Команда	Описание
Режим конфигурирования порта	
gvrp **no gvrp**	Включение/выключение функции GVRP на порту.

3. Включение функции GVRP в коммутаторе.

Команда	Описание
Режим глобального конфигурирования	
gvrp **no gvrp**	Включение/выключение функции GVRP в коммутаторе.

1.2.3 Примеры применения GVRP



Для получения информации динамической регистрации VLAN и ее обновления на коммутаторах должен быть сконфигурирован протокол GVRP.

Сконфигурированный на коммутаторах A, B и C протокол GVRP, позволяет динамически сконфигурировать VLAN 100 на коммутаторе B и двум рабочим станциям, подключенным к VLAN 100 на коммутаторах A и C связаться между собой без статического конфигурирования VLAN 100 на коммутаторе B.

Объект настройки	Описание объекта настройки
VLAN100	Порты 2-6 на коммутаторах A и C.
Trunk port	Порты 11 на коммутаторах A и C, порты 10, 11 на коммутаторе B.
GVRP в режиме глобального	Коммутаторы A, B, C.

конфигурирования	
GVRP в режиме конфигурирования портов	Порты 11 коммутаторов A и C, порты 10, 11 коммутатора B.

Подключим две рабочие станции к портам VLAN 100 на коммутаторах A и C, подключим порт 11 на коммутаторе A к порту 10 на коммутаторе B и порт 11 на коммутаторе B к порту 11 на коммутаторе C.

Шаги конфигурации описаны ниже:

Коммутатор A:

```
Switch(config)# gvrp
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/2-6
Switch(Config-Vlan100)#exit
Switch(config)#interface ethernet 1/0/11
Switch(Config-If-Ethernet1/0/11)#switchport mode trunk
Switch(Config-If-Ethernet1/0/11)# gvrp
Switch(Config-If-Ethernet1/0/11)#exit
```

Коммутатор B:

```
Switch(config)#gvrp
Switch(config)#interface ethernet 1/0/10
Switch(Config-If-Ethernet1/0/10)#switchport mode trunk
Switch(Config-If-Ethernet1/0/10)# gvrp
Switch(Config-If-Ethernet1/0/10)#exit
Switch(config)#interface ethernet 1/0/11
Switch(Config-If-Ethernet1/0/11)#switchport mode trunk
Switch(Config-If-Ethernet1/0/11)# gvrp
Switch(Config-If-Ethernet1/0/11)#exit
```

Коммутатор C:

```
Switch(config)# gvrp
Switch(config)#vlan 100
Switch(Config-Vlan100)#switchport interface ethernet 1/0/2-6
Switch(Config-Vlan100)#exit
Switch(config)#interface ethernet 1/0/11
Switch(Config-If-Ethernet1/0/11)#switchport mode trunk
Switch(Config-If-Ethernet1/0/11)# gvrp
Switch(Config-If-Ethernet1/0/11)#exit
```

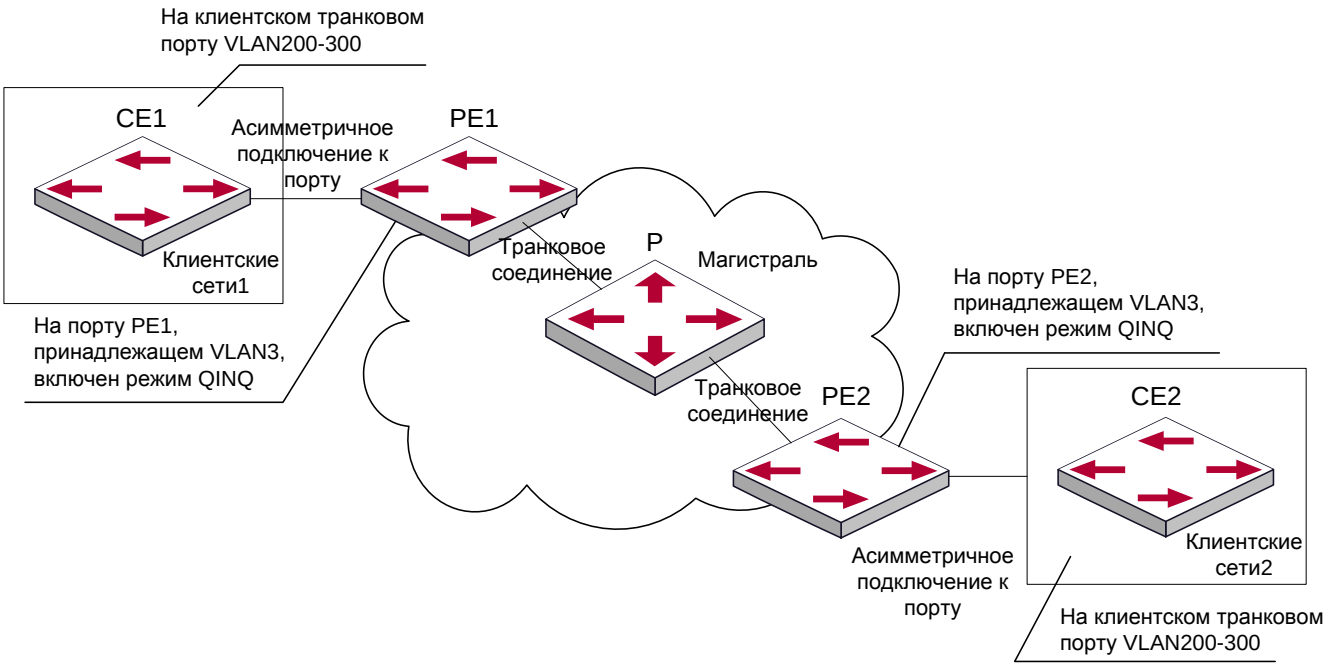
1.2.4 Устранение неисправностей GVRP

Счетчик GARP, установленный на транковых портах на обоих концах магистральной линии должен быть одинаковым, в противном случае GVRP не сможет работать нормально. Рекомендуется избегать одновременной работы протоколов GVRP и RSTP на узле. Если требуется включить протокол GVRP, необходимо сначала выключить функцию RSTP на портах.

1.3 Конфигурирование туннеля Dot1Q

1.3.1 Общие сведения о туннелях Dot1q

Туннель Dot1q, также называемый QinQ (802.1q-in-802.1q), является расширением протокола 802.1q. Основная идея заключается в упаковке метки клиентского VLAN (CVLAN tag) в метку VLAN сервис-провайдера (SPVLAN tag). Пакет с двумя метками VLAN передается через магистральную сеть интернет-провайдера, таким образом, обеспечивая простой туннель второго уровня для пользователя. Это просто и легко для управления, применимо только на статических конфигурациях и специально адаптировано для небольших офисных или метро-сетей, использующих коммутаторы третьего уровня как магистральное оборудование.



Как показано выше, после включения на клиентском порту, туннель Dot1q присваивает каждому пользователю идентификатор SPVLAN (SPVID). Здесь идентификатор пользователя – 3. Такой же SPVID может быть присвоен таким же пользователям на других PE. Когда пакет приходит с CE1 на PE1, он несет метки VLAN 200-300 внутренней сети пользователя. Когда туннель Dot1q включен, клиентский порт на PE1 добавляет в пакет дополнительные метки VLAN, у которых идентификатором является назначенный пользователю SPVID. Потом пакет будет направлен только в VLAN3, который уходит в сеть интернет-провайдера, и будет нести две метки VLAN (внутренняя метка добавлена, когда

пакет пришел на PE1, и другая является SPVID), в то время как информация о клиентских VLAN открыта для провайдера сети. Когда пакет достигнет PE2 и перед отправкой на CE2 с клиентского порта на PE2, внешняя метка VLAN удаляется и пакет, пришедший на CE2, становится полностью идентичен пакету, отправленному с CE1. Для пользователя роль оператора сети между PE1 и PE2 заключается в обеспечении канала второго уровня.

Технология туннеля Dot1q позволяет интернет-сервис-провайдеру поддерживать множество клиентских VLAN с помощью одного своего VLAN. Провайдер и клиент могут конфигурировать свои VLAN независимо друг от друга.

Технология туннеля Dot1q имеет следующие характеристики:

- Применима через простую статическую конфигурацию, не нужны сложная конфигурация и манипуляции;
- Оператор присваивает один SPVID каждому пользователю, что увеличивает количество одновременно поддерживаемых пользователей; в то же время пользователи имеют полную свободу при выборе и управлении идентификаторов VLAN (пользователь выбирает из диапазона от 1 до 4096);
- Клиентская сеть полностью независима. Когда интернет-сервис-провайдер модернизирует свою сеть, клиентские сети не требуют изменения конфигурации.

1.3.2 Конфигурирование туннеля Dot1q

1. Конфигурирование функции туннеля Dot1q на порту.

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel enable **no dot1q-tunnel enable**	Вход/выход из режима туннеля dot1q-на порту

2. Конфигурирование типа протокола (TPID) на порту.

Команда	Описание
Режим конфигурирования порта	
dot1q-tunnel tpid {0x8100|0x9100|0x9200|<1-65535>}	Конфигурирование типа протокола на магистральном порту.

1.3.3 Типичное применение туннеля Dot1q

Пограничные узлы PE1 и PE2 интернет-провайдера пересылают данные VLAN 200-300. Между CE1 и CE2 клиентской сети через VLAN3. Порт PE1 подключен к CE1, порт 10

подключен к публичной сети, TPID подключенного оборудования – 9100; Порт 1 PE2 подключен к CE2, порт 10 подключен к публичной сети.

Объект конфигурации	Описание конфигурации
VLAN3	Порт1 узлов PE1 и PE2.
dot1q-tunnel	Порт1 узлов PE1 и PE2.
tpid	9100

Процедура конфигурации описана ниже:

PE1:

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/0/1)# exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)#switchport mode trunk
Switch(Config-Ethernet1/0/1)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/0/1)#exit
Switch(Config)#
```

PE2:

```
Switch(config)#vlan 3
Switch(Config-Vlan3)#switchport interface ethernet 1/0/1
Switch(Config-Vlan3)#exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)# dot1q-tunnel enable
Switch(Config-Ethernet1/0/1)# exit
Switch(Config)#interface ethernet 1/0/1
Switch(Config-Ethernet1/0/1)#switchport mode trunk
Switch(Config-Ethernet1/0/1)#dot1q-tunnel tpid 0x9100
Switch(Config-Ethernet1/0/1)#exit
Switch(Config)#
```

1.3.4 Устранение неисправностей туннеля Dot1q

Включение туннеля Dot1q на транковом порту делает метку пакета данных непредсказуемой, что не подходит приложениям. Поэтому не рекомендуется использовать туннель Dot1q на транковом порту.

Использование туннеля совместно с STP/MSTP не поддерживается.

Использование туннеля совместно с PVLAN не поддерживается.

1.4 Настройка трансляции VLAN

1.4.1 Общие сведения о трансляции VLAN

Трансляция VLAN, как следует из названия, транслирует оригинальный идентификатор VLAN в новый в соответствии с требованиями пользователя или для обмена данными между различными VLAN. Трансляция может применяться как для входящей, так и исходящей информации. Данное оборудование поддерживает изменение идентификатора VLAN только на входе.

Применение и конфигурирование трансляции VLAN подробно объясняется далее.

1.4.2 Конфигурирование трансляции VLAN

1. Конфигурирование функции трансляции VLAN на порту.

Команда	Описание
Режим конфигурирования порта	
vlan-translation enable **no vlan-translation enable**	Включает или выключает режим трансляции VLAN

2. Конфигурирование соответствий трансляции VLAN на порту.

Команда	Описание
Режим конфигурирования порта	
vlan-translation <*old-vlan-id*> to <*new-vlan-id*> in **no vlan-translation old-vlan-id in**	Добавление/удаление соответствий трансляции VLAN

3. Конфигурирование условий сброса пакета, если проверка трансляции VLAN прошла неуспешно.

Команда	Описание
Режим конфигурирования порта	

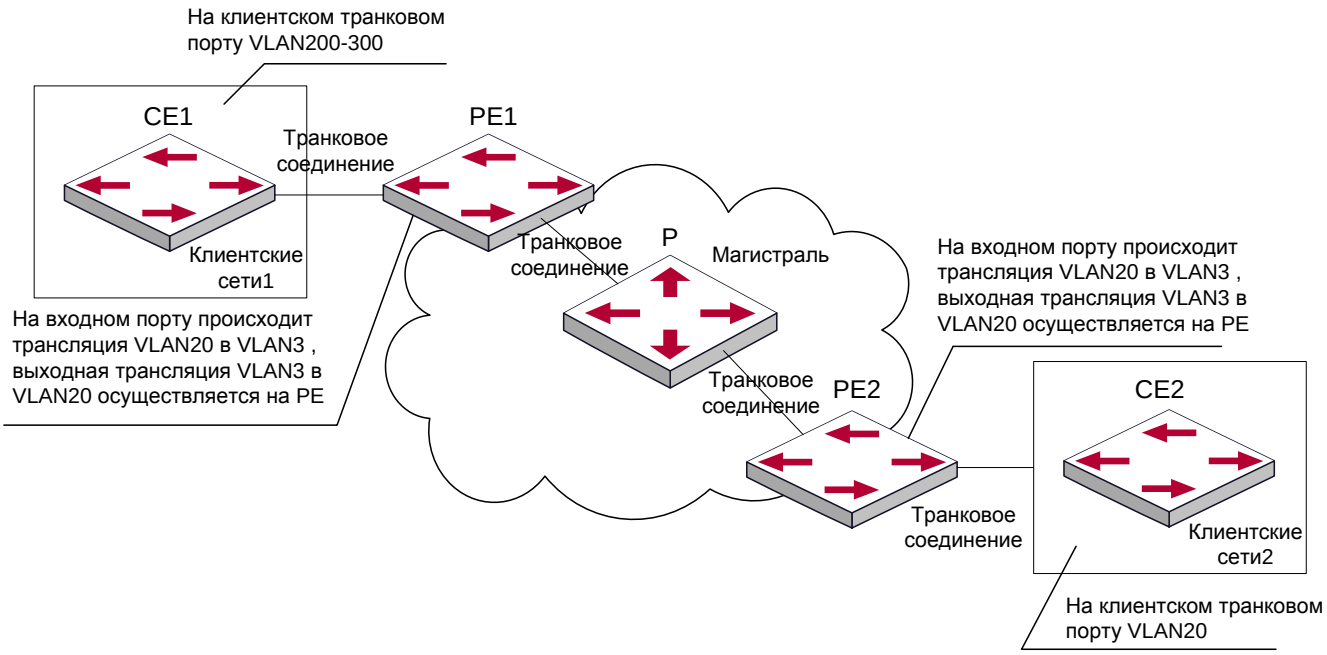
vlan-translation miss drop in **no vlan-translation miss drop in**	Конфигурирование сброса пакетов при возникновении ошибок трансляции VLAN

4. Просмотр конфигурации соответствий трансляции VLAN.

Команда	Описание
Режим администратора	
show vlan-translation	Просмотр сконфигурированных соответствий трансляции VLAN

1.4.3 Типовое применение трансляции VLAN

Пограничные узлы PE1 и PE2 интернет-провайдера поддерживают VLAN данных 20 между CE1 и CE2 из клиентской сети через VLAN 3. Порт 1 PE1 Подключен к CE1, порт 10 подключен к публичной сети, порт 1 PE2 подключен к CE2, порт 10 подключен к публичной сети.



Объект конфигурации	Описание конфигурации
VLAN-translation	Порт 1 узлов PE1 и PE2.

Trunk port	Порты 1 и 10 узлов PE1 и PE2.

Процедура конфигурирования указана ниже:

PE1, PE2:

```
switch(Config)#interface ethernet 1/0/1
switch(Config-Ethernet1/0/1)#switchport mode trunk
switch(Config-Ethernet1/0/1)# vlan-translation enable
switch(Config-Ethernet1/0/1)# vlan-translation 20 to 3 in
switch(Config-Ethernet1/0/1)# vlan-translation 3 to 20 out
switch(Config-Ethernet1/0/1)# exit
switch(Config)#interface ethernet 1/0/1
switch(Config-Ethernet1/0/1)#switchport mode trunk
switch(Config-Ethernet1/0/1)#exit
switch(Config)#
```

1.4.4 Устранение неисправностей трансляции VLAN

Обычно трансляция VLAN применяется на транковых портах.

Приоритеты между трансляцией VLAN и входящей фильтрацией VLAN распределяются так: Трансляция VLAN выше входящей фильтрации VLAN.

1.5 Конфигурирование динамических VLAN

1.5.1 Общие сведения

Динамическим VLAN называется так в противовес статическому VLAN (называемому портом, приписанным к VLAN). Динамический VLAN, поддерживаемый коммутатором, включает в себя VLAN на MAC-адресах, VLAN подсетей и протокольный VLAN. Подробное описание далее:

VLAN, базирующийся на MAC адресах представляет собой технологию, когда каждый хост с определенным MAC адресом соответствует определенному VLAN. Это позволяет пользователю сети сохранить свое членство в VLAN при перемещении из одного места в другое. Как мы видим, главное преимущество этого метода в том, что нет необходимости переконфигурировать VLAN, когда пользователь меняет свое месторасположение, а именно переключается с одного коммутатора на другой. Это следствие того, что VLAN базируется на MAC адресе пользователя, а не на порту коммутатора.

VLAN, базирующийся на IP подсетях представляет собой технологию, где метка VLAN назначается в соответствии с IP адресом источника и его маской подсети. Преимущество этого метода то же, что и у предыдущего, пользователю не требуется изменять конфигурацию при изменении местонахождения.

Метод VLAN на базе протоколов сетевого уровня назначает различным протоколам различные номера VLAN. Это очень удобно для тех сетевых администраторов, которые хотят упорядочивать пользователей по приложениям и сервисам. Более того,

пользователи могут свободно перемещаться по сети, зарегистрировавшись в ней один раз. Преимуществом данного метода является то, что он позволяет пользователям менять свое местоположение без изменения конфигурации VLAN, а то, что VLAN различаются по типу протоколов – очень важно для сетевого администратора. К тому же, данный метод не требует добавления метки фрейма для идентификации VLAN, что снижает общий трафик в сети.

Замечание: Порты, которые необходимо приписать к динамическим VLAN должны быть сконфигурированы как гибридные.

1.5.2 Конфигурирование динамических VLAN

Конфигурирование соответствия между протоколами и VLAN.

Команда	Описание
Режим глобального конфигурирования	
protocol-vlan mode {ethernetii etype *<etype-id>*|llc {dsap *<dsap-id>* ssap *<ssap-id>*}|snap etype *<etype-id>*} vlan *<vlan-id>* priority *<priority-id>* **no protocol-vlan {mode {ethernetii etype *<etype-id>*|llc {dsap *<dsap-id>* ssap *<ssap-id>*}|snap etype *<etype-id>*}|all}**	Добавление/удаление соответствий между протоколами и VLANами, а именно – вхождение/исключение определенного протокола в/из определенного VLANa.

1.5.3 Устранение неисправностей динамического VLANa

При необходимости каждый IP-протокол VLAN должен включать протокол ARP во избежание проблем соединения, вызванных протоколом ARP.

2 НАСТРОЙКА ТАБЛИЦЫ MAC АДРЕСОВ

2.1 Общие сведения о таблице MAC адресов

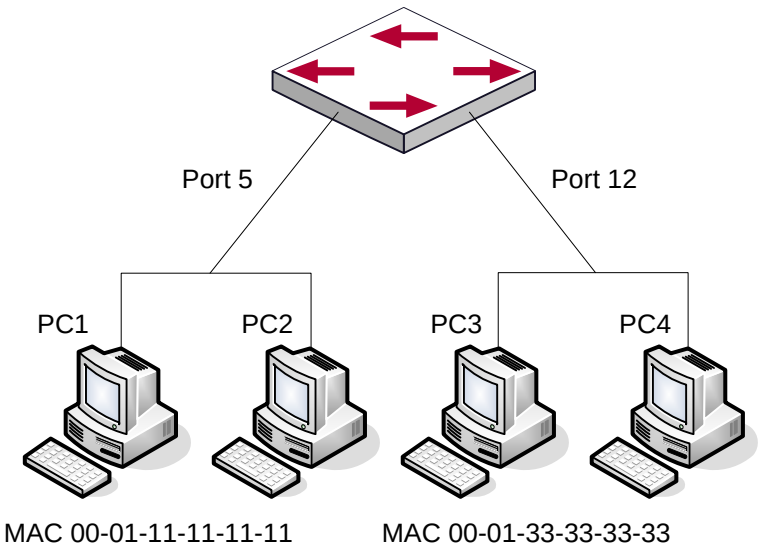
Таблица MAC-адресов — это таблица соответствий MAC-адресов устройств назначения портам коммутатора. MAC адреса делятся на статические и динамические. Статические MAC адреса вручную сконфигурированы пользователем, имеют наивысший приоритет и действуют постоянно (они не могут быть замещены динамическим MAC адресами). Динамические адреса запоминаются коммутатором при передаче пакетов данных, и они действуют ограниченное время. Когда коммутатор получает фрейм данных для пересылки, он сохраняет MAC адрес источника фрейма и соответствующий ему порт назначения. Когда таблица MAC адресов опрашивается на предмет MAC адреса приемника, при нахождении нужного адреса, пакет данных отправляется на соответствующий порт, в противном случае коммутатор пересылает пакет на свой широковещательный домен. Если динамический MAC адрес не встречается в пакетах для пересылки длительное время, запись о нем удаляется из таблицы MAC адресов коммутатора.

Для таблицы MAC адресов определены две операции:

- Получение MAC адреса.
- Отправка или фильтрация пакета данных в соответствии с таблицей MAC адресов.

2.1.1 Получение таблицы MAC адресов

Таблица MAC адресов может быть построена статически или динамически. Статическим конфигурированием настраивается соответствие между MAC адресами и портами. Динамическое обучение – это процесс, когда коммутатор изучает связи между MAC адресами и портами и регулярно обновляет таблицу MAC адресов. В этой секции мы остановимся на процессе динамического построения таблицы MAC адресов.



Топология на рисунке выше: 4 компьютера подключены к коммутатору, где PC1 и PC2 принадлежат одному физическому сегменту (домену коллизий), физический сегмент подключен к порту 1/0/5 коммутатора, PC3 и PC4 принадлежат к другому физическому сегменту, подключенному к порту 1/0/12 коммутатора.

Начальная таблица MAC адресов не содержит никаких значений. Возьмем для примера процесс связи между PC1 и PC3. Процесс обучения MAC адресам следующий:

1. Когда PC1 посылает сообщение к PC3, MAC адрес источника 00-01-11-11-11-11 и порт 1/0/5 из этого сообщения заносятся в таблицу MAC адресов коммутатора.
2. В то же время коммутатору надо понять, как доставить сообщение на адрес 00-01-33-33-33-33. Так как таблица содержит запись только для адреса 00-01-11-11-11-11 и порта 1/0/5, а для адреса 00-01-33-33-33-33 никаких записей нет, коммутатор рассылает данное сообщение на все свои порты (предполагаем, что все порты принадлежат по умолчанию VLAN1).
3. PC3 и PC4 получают сообщение, посланное PC1, но PC4 не отвечает на это сообщение, так как адрес приемника 00-01-33-33-33-33, и отвечать на него будет только PC3. Когда порт 1/0/12 получает сообщение, отправленное PC3, в таблицу MAC адресов добавляется запись о MAC адресе 00-01-33-33-33-33 и соответствующем ему порте 1/0/12.
4. Теперь таблица MAC адресов имеет две динамические записи: MAC адрес 00-01-11-11-11-11 – порт 1/0/5 и 00-01-33-33-33-33 – порт 1/0/12.
5. После обмена пакетами между PC1 и PC3, коммутатор больше не получает пакетов, отправленных PC1 и PC3. И записи в таблице MAC адресов, соответствующие этим устройствам удаляются через 300 или 2*300 секунд (т.е. простое или двойное время жизни). 300 секунд здесь это время жизни по умолчанию для записей в таблице MAC адресов. Время жизни может быть изменено на коммутаторе.

2.1.2 Пересылка или фильтрация кадров

Коммутатор посылает или отфильтровывает принимаемые пакеты данных в соответствии с таблицей MAC адресов. Рассматривая для примера рисунок выше, предполагаем, что коммутатор изучил адреса PC1 и PC3, и пользователь вручную настроил соответствие портов для PC2 и PC4. Таблица MAC адресов коммутатора будет следующей:

MAC адрес	Номер порта	Кем добавлена запись
00-01-11-11-11-11	1/0/5	Динамическое обучение
00-01-22-22-22-22	1/0/5	Статическая конфигурация
00-01-33-33-33-33	1/0/12	Динамическое обучение
00-01-44-44-44-44	1/0/12	Статическая конфигурация

1. Отправка пакетов в соответствии с таблицей MAC адресов.

Если PC1 посылает пакет к PC3, коммутатор отправляет данные, полученные с порта 1/0/5 на порт 1/0/12.

2. Фильтрация данных в соответствии с таблицей MAC адресов.

Если PC1 посылает сообщение PC2, коммутатор, проверив таблицу MAC адресов, находит PC2 и PC1 в одном физическом сегменте и отфильтровывает это сообщение (то есть сбрасывает это сообщение).

Коммутатором могут пересылаться три типа фреймов:

- Широковещательные фреймы;
- Многопользовательские фреймы;
- Однопользовательские фреймы.

Далее описывается, как коммутатор работает со всеми тремя типами пакетов:

1. Широковещательный фрейм: Коммутатор может определять коллизии в домене, но только не для широковещательных доменов. Если VLAN не установлены, все устройства, подключенные к коммутатору, считаются находящимися в одном широковещательном домене. Когда коммутатор получает широковещательный фрейм, он пересылает его во все порты. Если VLAN сконфигурированы, таблица MAC адресов адаптируется в соответствии с дополнительной информацией о VLAN. В этом случае коммутатор отправляет фрейм только на порты, находящиеся в том же VLAN.
2. Многопользовательский фрейм: Если многопользовательский домен неизвестен, коммутатор рассылает фрейм в том же VLAN, но если включена функция IGMP snooping или сконфигурирована статическая многопользовательская группа, коммутатор будет посылать этот фрейм в порты многопользовательской группы.
3. Однопользовательский фрейм: если VLANы не сконфигурированы, то, если MAC адрес приемника есть в таблице MAC адресов коммутатора, коммутатор напрямую пересылает пакет в соответствующий порт. Если же адрес приемника в таблице не найден, коммутатор делает широковещательную рассылку этого фрейма. Если VLAN сконфигурированы, коммутатор рассылает однопользовательский фрейм только внутри одного VLAN. Если MAC адрес найден в таблице, но принадлежит другому VLAN, коммутатор делает широковещательную рассылку фрейма в том VLAN, к которому принадлежит фрейм.

2.2 Конфигурирование таблицы MAC адресов

1. Конфигурирование времени жизни MAC адресов.

Команда	Описание
Режим глобального конфигурирования	
mac-address-table aging-time <*0*|*aging-time*>	Конфигурирование времени жизни MAC

no mac-address-table aging-time	адресов

Конфигурирование статической фильтрации или пересылки.

Команда	Описание
Общий режим	
mac-address-table {static | static-multicast | blackhole} address *<mac-addr>* **vlan** *<vlan-id>* **[interface [ethernet | portchannel]** *<interface-name>***] | [source|destination|both]** **no mac-address-table {static | static-multicast | blackhole | dynamic} [address** *<mac-addr>***] [vlan** *<vlan-id>***] [interface [ethernet | portchannel]** *<interface-name>***]**	Конфигурирование статических записей для MAC адресов, статических многопользовательских записей, записей фильтрации пакетов.

Очистка динамической таблицы MAC адресов.

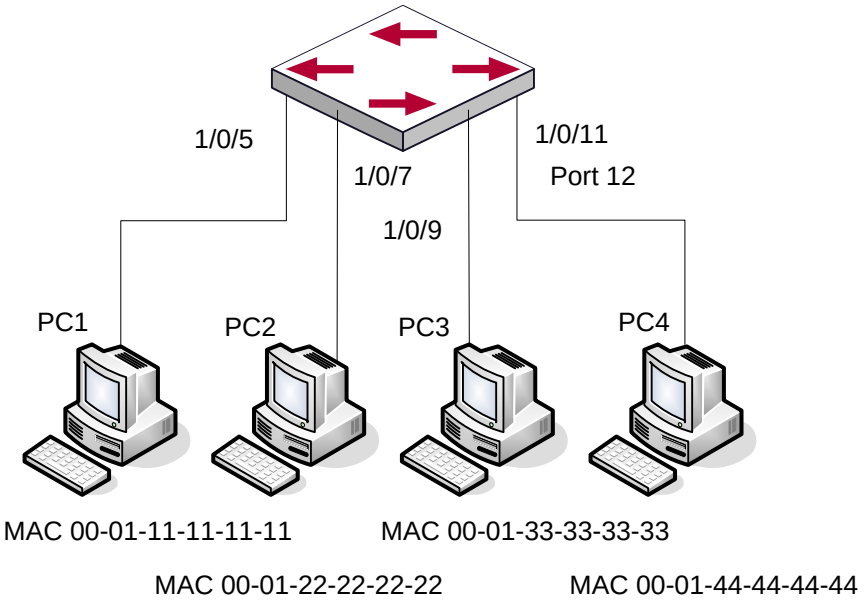
Команда	Описание
Режим администратора	
clear mac-address-table dynamic [address *<mac-addr>***] [vlan** *<vlan-id>***] [interface [ethernet | portchannel]** *<interface-name>***]**	Очистка динамической таблицы MAC адресов

Распознавание MAC адреса через CPU.

Команда	Описание
Общий режим	
mac-address-learning cpu-control **no mac-address-learning cpu-control**	Включает функцию распознавания MAC адреса через управление CPU; команда “no mac-address-learning cpu-control” восстанавливает автоматическое определение MAC адреса

showCollisionMacTable	Отображение хэш конфликтов в таблице MAC адресов
Режим администратора	
clearCollisionMacTable	Очищает таблицу хэш конфликтов MAC адресов

2.3 Примеры типичной конфигурации



Четыре компьютера, как показано на рисунке, подключены к портам 1/0/5, 1/0/7,1/0/9, 1/0/11 коммутатора. Все 4 компьютера принадлежат по умолчанию VLAN1. В соответствии с требованиями к сети, включено обучение динамическим адресам. PC1 содержит важные данные, и недоступен для других компьютеров из других физических сегментов; PC2 и PC3 статически приписаны к портам 7 и 9, соответственно.

Этапы конфигурации показаны ниже:

1. Установка MAC адреса 00-01-11-11-11-11 PC1 как фильтруемого.

```
Switch(config)#mac-address-table static 00-01-11-11-11-11 discard vlan 1.
```

2. Установка статической связи для PC2 и PC3 с портами 7 и 9 соответственно.

```
Switch(config)#mac-address-table static address 00-01-22-22-22-22 vlan 1
interface ethernet 1/0/7
Switch(config)#mac-address-table static address 00-01-33-33-33-33 vlan 1
interface ethernet 1/0/9
```

2.4 Устранение неисправностей с таблицей MAC адресов

Если при использовании команды show mac-address-table, было выяснено, что на порту произошел сбой распознавания MAC адресов устройств, подключенных к нему. Возможные причины:

- Подключенный кабель поврежден;
- На порту включен Spanning Tree в статусе «discarding» или порт только что подключился и Spanning Tree пока в статусе вычисления дерева. Дождитесь, пока вычисление структуры закончится и порт обучится MAC адресу;
- Если проблемы, описанные выше, не обнаружены, проверьте порт коммутатора и свяжитесь с технической поддержкой для решения проблемы.