Руководство по настройке гигабитного управляемого Ethernet коммутатора с помощью команд

www.polyvision.ru

версия 1.0 (2023)

www.polyvision.ru

Оглавление

Введение в командную строку CLI 6
1.1 CLI коммутатора доступа 6
1.2 Введение в режим CLI 9
1.3 Введение в синтаксис команд 11
1.4 Ярлыки командной строки 13
1.5 История команд 15

Конфигурация управления системой 16
2.1 Конфигурация безопасности системы 16
2.2 Обслуживание и отладка системы 23
2.3 Управление файлом конфигурации 28
2.4 Обновление версии программного обеспечения 32

Конфигурация портов 34
3.1 Общая конфигурация портов 34
3.2 Конфигурация зеркалирования 35
3.3 Настройка управления штормом 36
3.5 Настройка управления потоком 40
3.6 Настройка пропускной способности портов 40
3.7 Настройка агрегированных портов 41
3.8 Настройка сверхбольшого кадра 44
3.9 Настройка резервных портов 44
3.10 Конфигурирование LLDP 46

Безопасность MAC на основе портов 48
4.1 Краткое введение 48
4.2 Конфигурация привязки MAC 49
4.3 Конфигурация фильтрации MAC 50
4.4 Конфигурация ограничения изучения портов 51

Привязка портов IP и MAC 52
5.1 Краткое введение 52
5.2 Конфигурации привязки IP и MAC 53
5.3 Пример конфигурации 53
5.4 Неправильная конфигурация 54

Конфигурация VLAN 55
6.1 Введение в виртуальные локальные сети 55
6.2 Конфигурация VLAN 60
6.3 Пример конфигурации VLAN 63
6.4 VLAN на основе MAC, IP-подсети, протокола 66
6.5 Голосовая VLAN 67
6.6 Сопоставление VLAN 69

6.7 QinQ 69

Конфигурация QoS 72
7.1 Введение в QoS 72
7.2 Конфигурация QoS 74
7.3 Пример базовой конфигурации QoS 78
7.4 Пример конфигурации политики QoS 79

Конфигурация MSTP 80
8.1 Введение в MSTP 80
8.2 Конфигурация MSTP 86
8.3 Пример конфигурации MSTP 94

Конфигурация EAPS 95
9.1 Краткое введение EAPS 95
9.2 Основные понятия EAPS 95
9.3 Введение в протокол EAPS 95
9.4 Конфигурация EAPS 97
9.5 Ограничительные условия 97
9.6 Краткое введение в команду EAPS 98
9.7 Пример конфигурации с одним контуром 99
9.8 Пример конфигурации пересылки данных через кольцо 104

Конфигурация ERPS 107
10.1 Обзор ERPS 107
10.2 Внедрение в технологию ERPS 107
10.3 Принцип работы ERPS 109
10.4 Технические характеристики ERPS 111
10.5 Команды протокола ERPS 112
10.6 Типичное использование ERPS 114
11.1 Введение в 802.1x 129
11.2 Введение в RADIUS 135
11.3 Настройка 802.1x 138
11.4 Конфигурация RADIUS 144
11.5 Пример конфигурации 146

Конфигурация GMRP 147
12.1 Введение в GMRP 147
12.2 Конфигурация GMRP 147
12.3 Примеры типичных конфигураций GMRP 149

Конфигурация SNOOPING 150
13.1 Введение в IGMP SNOOPING 150
13.2 Конфигурация IGMP SNOOPING 154
13.3 Пример конфигурации IGMP SNOOPING 155

Конфигурация MVR 157
14.1 Профиль MVR 157
14.2 Конфигурация MVR 157
14.3 Пример конфигурации MVR 158

Конфигурация DHCP SNOOPING 160
15.1 Введение в DHCP SNOOPING 160
15.2 Конфигурация DHCP SNOOPING 162
15.3 Пример конфигурации DHCP SNOOPING 164
15.4 Ошибки в конфигурации DHCP SNOOPING 165

Конфигурация MLD SNOOPING 166
16.1 Введение в MLD SNOOPING 166
16.2 Конфигурация MLD SNOOPING 170
16.3 Пример конфигурации MLD SNOOPING 172

Конфигурация ACL 173
17.1 Введение библиотеки ресурсов ACL 173
17.2 Введение в фильтрацию ACL 175
17.3 Конфигурация репозитория ACL 176
17.4 ACL на основе временного интервала 178
17.5 Конфигурация фильтра ACL 180
17.6 Пример конфигурации ACL 181
17.7 Отладка конфигурации ACL 182

Базовая конфигурация TCP/IP 183
18.1 Настройка интерфейса VLAN 183
18.2 Настройка ARP 185
18.3 Настройка статической маршрутизации 187
18.4 Пример базовой конфигурации TCP/IP 190

Конфигурация SNMP 192
19.1 Введение в SNMP 192
19.2 Конфигурация SNMP 193
19.3 Пример конфигурации SNMP 195

Конфигурация RMON 196
20.1 Введение в RMON 196
20.2 Конфигурация RMON 197
20.3 Пример конфигурации RMON 198

Конфигурация кластера 200
21.1 Введение управления кластером 200
21.2 Краткое введение в конфигурацию кластера 206
21.3 Оборудование для управления конфигурацией 207
21.4 Устройство-участника конфигурации 211

21.5 Настройка участника кластера доступа 212
21.6 Отображение и обслуживание управления кластером 212
21.7 Пример типовой конфигурации управления кластером 213

Конфигурация системного журнала 215
22.1 Введение в системный журнал 215
22.2 Конфигурация системного журнала 218

Петля порта 223
23.1 Профиль 223
23.2 Принцип протокола 223
23.3 Введение в конфигурацию 224

Конфигурация SNTP 226
24.1 Внедрение SNTP 226
24.2 Конфигурация SNTP 226
24.3 Отображение информации SNTP 228

Конфигурация OAM 229
25.1 Внедрение в OAM 229
25.2 Конфигурация OAM 230
25.3 Типовые примеры конфигурации OAM 232

Конфигурация CFM 233
26.1 Профиль CFM 233
26.2 Краткое введение в задачу настройки CFM 237
26.3 Базовая конфигурация CFM 238
26.4 Настройка различных функций CFM 240
26.5 CFM дисплей и обслуживание 242
26.6 Типовые примеры конфигурации 243

Базовая конфигурация IPv6 247
27.1 Профиль IPv6 247
27.2 Профиль задачи базовой конфигурации IPv6 255
27.3 Настройка базовой функциональности IPv6 255
27.4 Настройка протокола обнаружения соседей IPv6 256
27.5 Конфигурация статической маршрутизации IPv6 259
27.6 Отображение и обслуживание IPv6 259

Первая глава

Введение в командную строку CLI

В этой главе представлено подробное описание интерфейса командной строки CLI, Содержание выглядит следующим образом:

- Cli коммутатора доступа
- Введение в режим CLI
- Введение в синтаксис команд
- Сочетания клавиш для командной строки
- Команда "История"

1.1 CLI коммутатора доступа

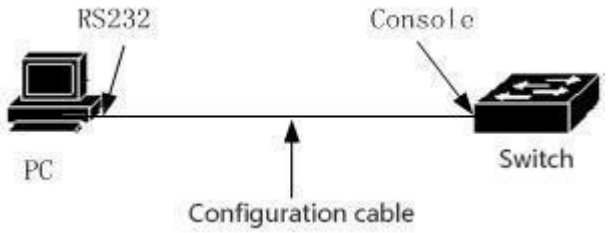
Интерфейс командной строки (CLI) коммутатора предоставляет пользователю интерфейс для управления коммутатором. Пользователь может получить доступ к интерфейсу командной строки (CLI) коммутатора через Console порт и два терминала Telnet, Следующее представлено отдельно.

Содержание включает:
Пользовательский доступ к CLI через Console порт
Пользовательский доступ к CLI через TELNET

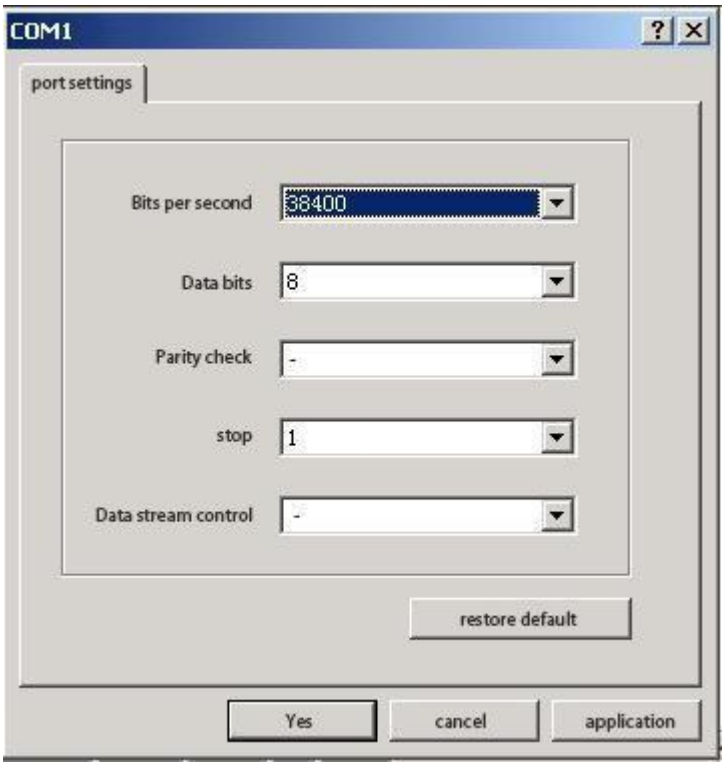
1.1.1 Пользовательский доступ к CLI через консольный порт

Порядок работы следующий:

Первый шаг - соедините последовательный порт ПК с консольным портом коммутатора с помощью кабеля, по следующей схеме:



Второй шаг: Запуск программы эмуляции терминала на компьютере (например, HyperTerminal, Putty в Windows), настройка параметров связи в программе.
Коммуникационные параметры терминала настраиваются следующим образом:
Скорость передачи данных: 38400
Биты данных: 8
Проверка четности: ничего
Стоп-бит: 1
Управление потоком данных: ничего
Конфигурация параметров связи показана ниже:

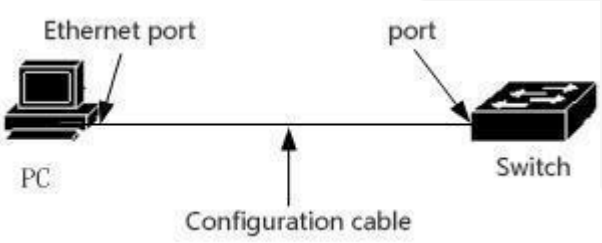


Третий шаг: Запуск коммутатора. После запуска коммутатора на терминале появится приглашение (по умолчанию Switch >). Пользователь может вводить команды в этом поле. Это позволит пользователю получить доступ к CLI коммутатора.

1.1.2 Пользовательский доступ к CLI через TELNET

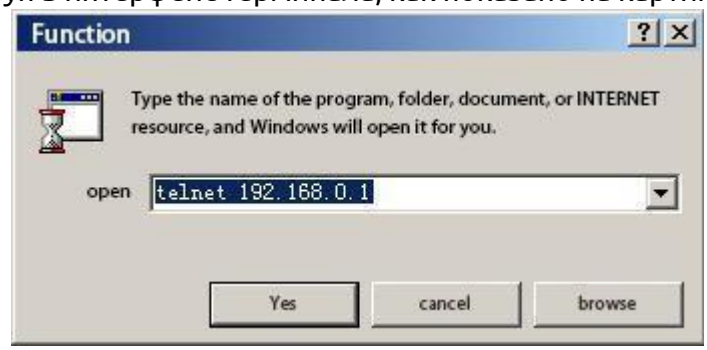
Пользователь может получить доступ к коммутатору через порт коммутатора.
IP адрес порта коммутатора по умолчанию 192.168.0.1
Для доступа на коммутатор необходимо проделать следующие шаги:

Шаг первый: Соединить Ethernet порт коммутатора и компьютера Ethernet кабелем, по следующей схеме:



Шаг второй : Задать IP адрес Ethernet порта вашего ПК, IP адрес должен быть в следующего образца 192.168.0.0/24 (наример 192.168.0.100). Убедитесь в том что связь между ПК и коммутатором имеется путем испоьзования утилиты Ping 192.168.0.1

Шаг третий : Если связь между коммутатором и ПК имеется связь, значит 192.168.0.1 по Telnet можно получить доступ в интерфейс терминала, как показано на картинке:



Шаг четвертый: Если система не имеет пароля, интерфейс Telnet переходит непосредственно к CLI, и появляется приглашение CLI (по умолчанию Switch >) Если в системе установлен пароль, необходимо ввести пароль в интерфейсе Telnet, чтобы войти в CLI.

Следует обратить особое внимание на два момента:

- IP адрес порта коммутатора основан на интерфейсе третьего уровня VLAN. Перед доступом к коммутатору необходимо установить IP адрес интерфейса VLAN. По умолчанию IP адрес VLAN1 192.168.0 его можно использовать напрямую. IP адрес интерфейса VLAN может быть настроен через консольный порт.
- Получение доступа к коммутатору через порт: вы можете соединить ПК и коммутатор напрямую кабелем Ethernet, либо через сеть, вам необходимо чтобы коммуникация ПК и коммутатора была в одном из VLAN коммутатора.

1.2 Введение в режим CLI

Содержание включает:

- Роль модели CLI
- Идентификация режима CLI
- Классификация шаблонов CLI

1.2.1 Роль модели CLI

Существует две основные функции модели CLI:

- Удобная классификация пользователей

Предотвращение незаконного использования CLI неавторизованными пользователями.
Пользователи могут быть разделены на два уровня: Обычные пользователи и привилегированные пользователи.
Обычные пользователи могут просматривать рабочее состояние коммутатора и использовать только команды отображения.
Привилегированные пользователи могут не только просматривать рабочее состояние коммутатора, но и поддерживать и настраивать коммутатор для изменения режимов работы коммутатора.

- Удобная настройка коммутатора

Коммутаторы имеют много конфигураций, и если вы поместите всю конфигурацию в один режим, это очень удобно для пользователя.
Для этой цели необходимо установить несколько режимов в CLI, схожие команды, размещенные в определенном режиме удобны в понимании и использовании.

1.2.2 Идентификация режима CLI

Приглашение CLI - это идентификатор режима CLI, когда пользователь использует CLI, глядя на приглашение вы можете определить в каком пользовательском режиме находитесь в настоящее время.
Приглашение CLI состоит из двух частей, одна часть идентифицирует хост, другая шаблоны. Хост-часть приглашения CLI использует имя хоста системы, его можно настроить, по умолчанию Switch, обычно используют имя хоста по умолчанию.
Раздел схемы в приглашении CLI не настраивается, каждый шаблон имеет свою собственную соответствующую строку, некоторые строки шаблона неизменяемы, некоторые строки шаблона могут изменится. Если шаблон конфигурации VLAN фиксирован, строка шаблона конфигурации интерфейса является переменной.
Например:
Командная строка (CLI) Switch# идентифицирует привилегированный режим, Switch идентифицирует хост, а # модель идентификации.
Подсказка CLI (config-ge1/1)# определяет режим конфигурации интерфейса и настраивается с портом ge1/1, Switch идентифицирует хост, а (config-ge1/1) # модель идентификации.
Командная строка Switch(config-vlan2)# определяет режим конфигурации интерфейса , И настройка интерфейса vlan2 , Коммутатор идентифицирует хост, а (config-vlan2) # модель идентификации.

1.2.3 Классификация шаблонов CLI

Модель CLI разделена на четыре категории: общий режим, привилегированный режим, глобальный режим конфигурации и подшаблон конфигурации, в то время как подмодель конфигурации состоит из множества режимов CLI.

Обычные пользователи могут получить доступ только к общим шаблонам, а привилегированные пользователи могут получить доступ ко всем шаблонам CLI.

Консольные и Telnet-терминалы сначала переходят в общий режим, после ввода команды enable в обычном режиме и успешной проверке пароля переходит в привилегированный режим. Через терминал Telnet обычные пользователи могут оставаться только в обычном режиме и не могут войти в привилегированный режим. Войдите в конфигурационный терминал в привилегированном режиме, чтобы режим CLI перешел в глобальный режим конфигурации. В режиме глобальной конфигурации вы можете ввести соответствующие команды и войти в каждый подрежим конфигурации.

В следующей таблице перечислены основные режимы CLI коммутаторов:

Режим	Описание	Подсказка CLI	Команды входа в режим	Команды выхода из режима
Общий режим	Предоставляет команду отображения для просмотра	Switch>	Режим первого входа в терминал	В общем режиме на консольном терминале отсутствует команда выхода, а команда exit или quit используется для выхода из терминала Telnet
Привилегированный режим	Помимо предоставления команд для просмотра информации о состоянии коммутатора, он также предоставляет такие команды, как отладка, обновление версии и обслуживание конфигурации.	Switch#	Введите команду enable в обычном режиме	Вернутся в нормальный режим можно с помощью команды disable. На консольном терминале используется команда exit или quit, чтобы перейти в обычный режим.
Режим глобального конфигурирования	Предоставляет универсальные команды, которые не могут быть реализованы в подшаблонах конфигурации, такие как настройка статических команд маршрутизации.	Switch(config)#	Введите команду configure terminal в привилегированном режиме.	Используйте команды exit, quit или end для выхода в привилегированный режим
Режим конфигурирования интерфейса	Предоставляет команды для конфигурирования портов и интерфейсов VLAN	port: Switch(config-ge1/1)# VLANInterface: Switch(config-vlan1)#	Вход в режим глобального конфигурирования <if-name>	Используйте команду exit или quit для выхода в режим глобальной конфигурации, команда end производит выход в привилегированный режим

Режим конфигурирования VLAN	Предоставляет команды для настройки VLAN. Например, команды для создания и удаления VLAN.	Switch(config-vlan)#	В режиме глобальной конфигурации введите команду VLAN database.	Используйте команду exit или quit для выхода в режим глобальной конфигурации и выхода в привилегированный режим с помощью команды end
Режим конфигурирования MSTP	Предоставляет команды для настройки MSTP. Например, команды для создания и удаления экземпляров MSTP.	Switch(config-mst)#	В режиме глобальной конфигурации введите команду конфигурации spanning-tree MST.	Используйте команду exit или quit, чтобы выйти в режим глобальной конфигурации и с помощью команды end выйти в привилегированный режим.
Режим конфигурирования терминала	Предоставляет команды для настройки терминалов консоли и Telnet, такие как настройка времени ожидания для терминала.	Switch(config-line)#	В режиме глобального конфигурирования введите команду line vty.	Используйте команду exit или quit, чтобы выйти в режим глобальной конфигурации и выйти с помощью команды end в привилегированный режим.

1.3 Введение в синтаксис команд

Команда CLI состоит из двух частей: ключевого слова и параметра. Первое слово должно быть ключевым словом, а второе слово может быть ключевым словом или параметром, а ключевые слова и параметры могут появляться поочередно. Команда должна иметь ключевое слово, но она не может иметь параметров. Например, команда write — это только одно ключевое слово без параметра; версия команды show имеет два ключевых слова без параметра; команда VLAN <vlan-id> имеет <instance-id> <vlan-id> ключ и параметры команды VLAN экземпляра; два ключевых слова и два параметра.

1.3.2 Тип параметра

Параметры порядка CLI делятся на два типа: обязательные и необязательные. Команда ввода должна включать требуемые параметры, а необязательные параметры можно не вводить. Параметр команды VLAN in <vlan-id> является обязательным параметром, он должен быть введен; а интерфейс [if-name] в параметре команды является необязательным полем, этот параметр можно не вводить.

1.3.3 Правила синтаксиса команд

При описании команд текстом должны соблюдаться следующие правила:

1) Ключевые слова непосредственно представлены словами. Например, команда show version.
2) Параметр должен быть заключен в < > , например, команда VLAN <vlan-id>
3) Если это необязательный параметр, параметры должны быть заключены в [...]

Например, команда show VLAN [<vlan-id>], для этой ситуации параметр <> может быть опущен и изменен: команда show vlan [vlan-id] то есть параметр vlan-id можно и не вводить. Если это обязательный параметр, параметры не могут иметь [].

4) Если у вас есть несколько ключевых слов или параметров, вы должны выбрать одно из них. Можно объединить несколько ключевых слов и параметров с помощью {}, между ключевыми словами или параметрами должна быть разделяющая линия « | » , до и после

черты « | » должны быть пробелы. Если требуется несколько ключевых слов: spanning-tree mst link-type {точка-точка | общий} между точка-точка и общий, нужно выбрать что-то одно. Ряд параметров, необходимых команде: no arp {<ip-address> | <ip-prefix>}, ключевые слова и параметры, смешанные с необходимыми командами: show spanning-tree mst {none|instance <0-15>}ng

5) Если выбрано несколько ключевых слов или параметров, заключите ряд ключевых слов или параметров в [...], между несколькими ключевыми словами или параметрами с | разделительной полосой | требуется пробелы до и после полосы. В следующей команде: debug ip tcp [recv | send], ключевые слова recv и send, вы можете выбрать одно из них. Вы не можете выбрать оба. show ip route [<ip-address> | <ip-prefix>] show interface [<if-name> | switchport]
6) Если у вас есть ключевое слово или параметр, или набор ключевых слов или параметров, вы можете повторить ввод и добавить символ «*» после ключевого слова или параметра. Например команда ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]* -j <count> <ip-address>* --- Несколько IP-адресов могут быть введены многократно -k <count> <ip-address>*
7) Параметры представлены дескрипторами из одного или нескольких слов. Если в параметре более одного слова, каждое слово отделяется знаком « - », каждое слово пишется со строчной буквы. Правильное представление параметров: <vlan-id>, <if-name>, <router-id>, <count> и т.д. Неправильное представление параметров: <1-255>, <A.B.C.D>, <WORD>, <IFNAME> и т.д.

1.3.4 Аббревиатура команд

Когда пользователь вводит команду в интерфейсе CLI, ключевое слово команды может быть сокращено. CLI поддерживает функцию сопоставления префикса команды. Пока входное слово соответствует префиксу ключевого слова, CLI анализирует входное слово на соответствие ключевому слову. Таким образом, пользователям очень удобно использовать CLI, и пользователь может ввести команду с очень небольшим количеством символов, например команда show version, которая может быть сокращена до sh ver.

1.3.5 Справка по грамматике

Интерфейс командной строки CLI настроен с помощью синтаксиса для поддержки команд и параметров каждого уровня:

1) Прямой ввод в режиме CLI знака « ? » : На терминале будет выведено первое ключевое слово и его описание для всех команд в этом режиме.

например, Switch(config)#?

2) Введите предшествующую часть команды, затем введите пробел и клавишу Enter, на терминале будут перечислены все ключевые слова или параметры следующего уровня и даны их описания.

Например, Switch#show ?

3) Введите неполное ключевое слово и введите знака « ? », все ключевые слова и их описания, соответствующие входному префиксу, перечислены на терминале. Например, Switch#show ver?
4) Введите предшествующую часть команды, затем введите пробел, а затем нажмите клавишу Tab, терминал отобразит все ключевые слова на следующем уровне. Следующий уровень, если это параметр, не будет указан.

5) Если ввод не является полным ключевым словом, непосредственно нажмите клавишу Tab, если есть только одно ключевое слово и входной префикс совпадает, заполняется напрямую, если есть несколько ключевых слов, совпадающих с входным префиксом, все списки совпадающих ключевых слов в терминале.

1.3.6 Сообщение об ошибке командной строки

Если команда, введенная пользователем, не прошла проверку синтаксиса, на терминал выводится сообщение об ошибке. Информация об общих ошибках представлена в следующей таблиц:

Сообщение об ошибке	Причина ошибки
Invalid input or Unrecognized command	Подходящие ключевые слова не найдены Неверный ввод параметра Введено слишком много ключевых слов или параметров
Incomplete command	Ввод команды неполный, и ключевое слово или параметр не введен
Ambiguous command	Ввод ключевого слова является неполным, и несколько ключевых слов соответствуют входному префиксу

1.4 Ярлыки командной строки

Содержание включает:

- Клавиша быстрого редактирования строки
- Клавиша быстрого доступа к командам дисплея

1.4.1 Клавиша быстрого редактирования строки

Интерфейс командной строки CLI поддерживает функцию ярлыка редактирования строки, а ярлык редактирования строки может облегчить ввод и редактирование команды CLI. Когда вы вводите или редактируете команды, вы можете использовать ярлык редактирования строки для ускорения ввода команды. В следующей таблице перечислены все ярлыки редактирования строки и функции для их реализации:

Клавиша быстрого доступа	Функция
Ctrl+p Или стрелка вверх	Последняя команда
Ctrl+n Или стрелка вниз	Следующая команда
Ctrl+u	Удаление целой строки
Ctrl+a	Вернуть курсор к
Ctrl+f Или правая клавиша	Сдвинуть курсор вправо
Ctrl+b Или левая клавиша	Сдвинуть курсор влево
Ctrl+d	Удалите символ при наведении курсора
Ctrl+h	Удалить символ слева от курсора
Ctrl+k	Удалить все символы слева от курсора и курсор
Ctrl+w	Удалить все символы слева от курсора
Ctrl+e	Переместить курсор в конец строки
Ctrl+c	Прерывание - остановить выполнение команды. Если CLI находится в режиме глобального конфигурирования или подрежим конфигурирования, интерфейс командной строки переходит в привилегированный режим
Ctrl+z	Такая же функция как и ctrl+c
Tab	Нажмите эту кнопку при вводе неполного ключевого слова и если есть ключевое слово, соответствующее введенному префиксу, ключевое слово будет дополнено; если введенному префиксу соответствует более одного ключевого слова, перечисляются все совпадающие ключевые слова; Если нет соответствия ключевому слову, эта кнопка не будет работать

Будьте осторожны: на некоторые консолях в терминале ↑, ↓,→, ← кнопки недоступны

1.4.2 Клавиша быстрого доступа к командам дисплея

Команды, начинающиеся с ключевого слова show - это все команды отображения. Некоторые команды отображения не могут быть отображены на одном экране из-за отображения большого количества содержимого, и терминал обеспечивает функцию отображения экрана. После отображения экрана, терминал ожидает ввода пользователя для определения последующей обработки. В следующей таблице перечислены клавиши быстрого доступа для отображения команд и их функции.

Клавиша быстрого доступа	Функции
Space	Отображение следующего экрана
Enter	Показать следующую строку
Ctrl+c	Прервать выполнение команды и выйти в режим CLI
Остальные клавиши	Та же функция, что и Ctrl+c

1.5 История команд

Интерфейс командной строки CLI поддерживает функцию истории команд. Он может запомнить 20 команд, которые пользователь недавно использовал, и сохранить. Вы можете использовать функцию показать историю использования команд, которые были введены, также можете использовать Ctrl+p, Ctrl+n или клавиши ↑ , ↓ для выбора команд в истории.

Вторая глава

Конфигурация управления системой

Прежде чем приступить к настройке соответствующих функций коммутатора, необходимо освоить базовую конфигурацию управления системой и обслуживания коммутатора. В этой главе описывается базовая конфигурация управления и обслуживания этих систем, включая следующее:

- Конфигурация безопасности системы
- Обслуживания и отладка системы
- Управление файлами конфигурации
- Обновление версии программного обеспечения

2.1 Конфигурация безопасности системы

Для того чтобы предотвратить незаконное вторжение пользователей в коммутаторы, система обеспечивает несколько мер для управления безопасностью , в основном, включая:

- Многопользовательский контроль управления
- TACACS+ авторизация и аутентификация
- Контроль паролей анонимных пользователей
- Включение контроля паролей
- Служба управления TELNET
- Служба управления SNMP
- Служба управления HTTP
- Управление SSH-сервисом

2.1.1 Контроль многопользовательского управления

Многопользовательское управление не только обеспечивает безопасность системы коммутаторов, но и предоставляет возможность нескольким пользователям управлять и обслуживать коммутатор одновременно. Многопользовательское управление через предоставление каждому пользователю имени пользователя, пароля и полномочий для обеспечения безопасности системы: пользователю сначала необходимо аутентифицировать имя пользователя и пароль в коммутаторе доступа, если имя пользователя и пароль являются правильными и совпадают с установленными в системе, пользователь может получить доступ к коммутатору, но уровень полномочий пользователя ограничивают область доступа к коммутатору. Многопользовательское управление делит права пользователей на два уровня: обычные пользователи и привилегированные пользователи. Обычные пользователи могут оставаться только в обычном режиме интерфейса командной строки CLI и могут использовать только команду display для запроса информации о коммутаторе.

Привилегированные пользователи могут получить доступ ко всем режимам интерфейса командной строки CLI, и все командам, могут использовать команды для запроса информации о коммутаторах, а также для обслуживания и управления коммутаторами. Функция многопользовательского управления применяется только к терминалу Telnet, а консольный терминал не контролируется. Когда вы используете консольный терминал для доступа к коммутатору, вам не нужно проверять имя пользователя и пароль, и пользователь может получить доступ к CLI напрямую. А через терминал Telnet для доступа к коммутатору проверяются имя пользователя и пароль, прежде чем пользователь сможет получить доступ к CLI. В коммутаторе нет пользователя по умолчанию, то есть функция управления пользователями не включена по умолчанию. В таком случае терминалу Telnet не нужно подтверждать имя пользователя и пароль. При добавлении имени пользователя в работу включается многопользовательская функция управления и тогда терминал Telnet должен подтвердить имя пользователя и пароль. Когда используются команда для удаления всех пользователей, функция многопользовательского управления закрывается, и система возвращается в состояние по умолчанию.

С многопользовательским управлением связаны следующие команды:

Команда	Описания	Режим CLI
username <user-name> password <key> {normal | privilege}	Добавление пользователя. Если указанный пользователь уже существует, измените пароль и разрешения пользователя. Первый параметр — это имя пользователя, второй параметр — пароль, параметр предоставляет полномочия, normal — обычного пользователя, privilege — привилегированного пользователя.	Режим глобального конфигурирования
no username [user-name]	Удалить одного или всех пользователей. Если вы не ввели параметр, это означает удаление всех пользователей, если входной параметр представляет собой имя пользователя, то удаляет указанного пользователя.	Режим глобального конфигурирования
show running-config	Просматривая текущую конфигурацию системы, можно увидеть конфигурацию многопользовательского управления.	Привилегированный режим

2.1.2. TACACS+ авторизация и аутентификация

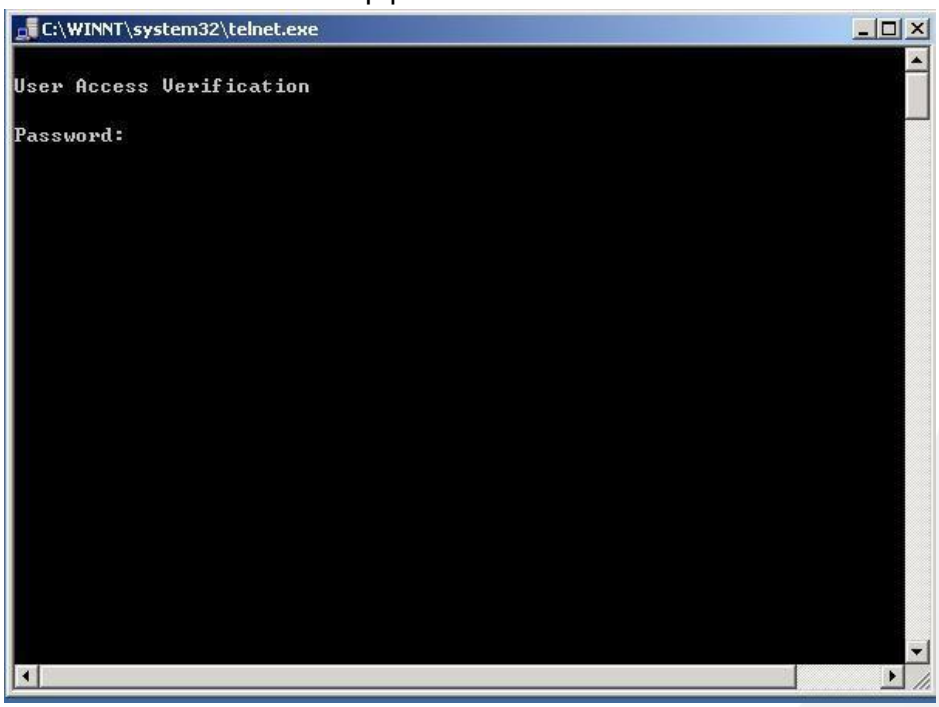
Аутентификация и авторизация TACACS+ обеспечивают более строгое управление правами пользователей не только для проверки допустимости пользователей, но и для авторизации команды. После открытия аутентификации TACACS+ пользователю сначала необходимо проверить имя пользователя и пароль через сервер TACACS+ при доступе к коммутатору. Только когда имя пользователя и пароль верны и согласованы, они могут пройти проверку. Пользователь может получить доступ к коммутатору после проверки. TACACS+ также делит разрешения пользователя на два уровня: обычные пользователи и привилегированные пользователи. Обычные пользователи могут оставаться только в обычном режиме интерфейса командной строки CLI, а привилегированные пользователи могут получить доступ ко всем шаблонам интерфейса командной строки CLI. На основе уровня разрешений он также устанавливает полномочия выполнения команд, пользователь вводит команду (кроме enable, end и exit), которая должна быть проверена на сервере TACACS+, сбой верификации не будет происходить. Функция аутентификации и авторизации TACACS+ применяется только к терминалам Telnet и SSH и не управляет консольным терминалом. Имя пользователя и пароль необходимо проверить при доступе к коммутатору через терминал Telnet или SSH. Аутентификация TACACS+ также применяется для входа в систему WEB но только для проверки прав доступа пароля, нет авторизации команд. По умолчанию TACACS+ не включен, Telnet, SSH или WEB работает с использованием многопользовательской функции управления, откройте функцию TACACS+, функция управления пользователем может продолжать настраиваться, но не фактическое использование.

Ниже перечислены команды, связанные с авторизацией и аутентификацией TACACS+:

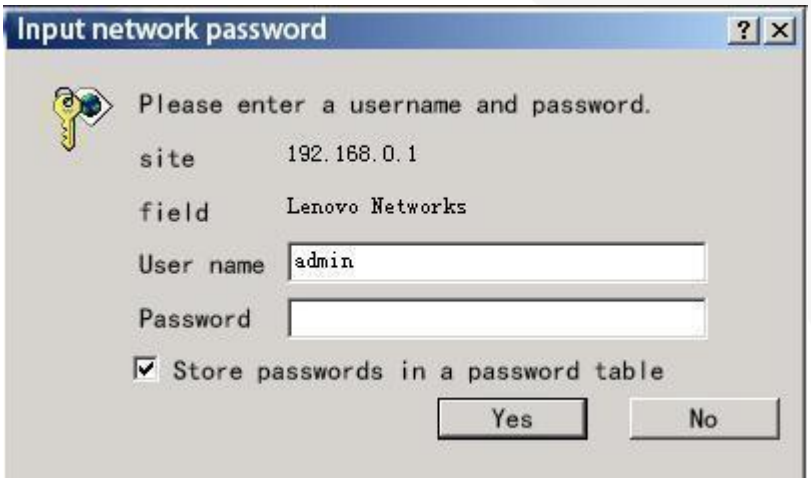
Команда	Описание	Режим CLI
tacacsplus enable	Открывает функцию TACACS+	Режим глобального конфигурирования
tacacsplus disable	Закрывает функцию TACACS+	Режим глобального конфигурирования
tacacsplus host A.B.C.D	Настройка адреса главного сервера, рекомендуется использовать ACS Cisco	Режим глобального конфигурирования
tacacsplus key WORD	Настройте общий ключ, который шифрует данные и должен соответствовать конфигурации на устройстве.	Режим глобального конфигурирования
tacacsplus auth-type (PAP|CHAP)	Выберите методы аутентификации, включая PAP и CHAP. Среди них PAP является режимом по умолчанию, поле заключает в себе пароль, а CHAP заключает в себе проверочный код MD5 пароля.	Режим глобального конфигурирования
show tacacsplus	Просмотр информация о конфигурации TACACS+	Режим глобального конфигурирования
no tacacsplus host	Очистить адрес главного сервера	Режим глобального конфигурирования
no tacacsplus key	Очистка общих ключей	Режим глобального конфигурирования

2.1.3 Контроль паролей анонимных пользователей

Когда многопользовательское управление не включено, терминалу Telnet не нужно проверять имя пользователя и пароль, вы можете напрямую получить доступ к Telnet CLI. Для повышения безопасности системы, коммутатор добавляет анонимный пароль пользователя (admin) для управления Telnet и Web. Если на коммутаторе установлен анонимный пароль пользователя и управление пользователями не включено, чтобы проверить вход с анонимным пароле, произведите ввод пароля чтобы иметь возможность получить доступ к CLI и веб-страницы. Если система использует многопользовательское управление, анонимный пароль пользователя не будет эффективным, доступ пользователя к терминалу Telnet и Web не будет проверять анонимный пароль, коммутатор будет проверять имя пользователя и пароль для входа.
Если на коммутаторе нет пароля анонимного пользователя. В этом случае пользователю вводить пароль анонимного пользователя при доступе к терминалу Telnet и Web.
На рисунке ниже показан интерфейс терминала Telnet для входа пользователя, введите анонимный пароль пользователя в этом интерфейсе.



На приведенной ниже схеме показано диалоговое окно, в котором пользователь может войти в Интернет. В этом диалоговом окне вводятся пользователь (админ) и пароль.



Ниже перечислены связанные команды для паролей анонимных пользователей:

Команды	Описание	Режим CLI
password <key>	Установка пароля анонимного пользователя	Режим глобального конфигурирования
no password	Очистить анонимный пароль	Режим глобального конфигурирования
show running-config	Просматривая текущую конфигурацию системы, можно увидеть конфигурацию пароля анонимного пользователя.	Привилегированный режим

Будьте осторожны: Для безопасности системы администратору необходимо устанавливать анонимный пароль пользователя системы.

2.1.4 Включение контроля паролей

Пароль Enable используется для управления переключением из обычного режима в привилегированный режим. Пока пароль Enable не подтвержден, пользователь может только просматривать информацию о коммутаторе, после проверки пароля Enable пользователь может настраивать и поддерживать коммутатор.

Пароль Enable не зависит от пароля пользователя, пользователь входит в терминал Telnet используя пользовательский пароль. Чтобы войти в привилегированный режим необходимо ввести пароль Enable, если аутентификация не прошла, вы можете пользоваться функциями только обычного режима.

В обычном режиме введите команду Enable, терминал предложит пользователю ввести пароль, затем пользователь может ввести пароль Enable, если проверка пароля прошла успешно, терминал переходит в привилегированный режим, в противном случае останется в обычном режиме, обычные пользователи даже с правильным паролем не могут войти в привилегированный режим.

Пароль Enable по умолчанию пустой, в этом случае, в обычном режиме, введите команду Enable, терминал не запросит пароль, войдите в привилегированный режим напрямую. Ниже перечислены соответствующие команды пароля Enable:

Команда	Описание	Режим CLI
enable password <key>	Установите пароль Enable	Режим глобального конфигурирования
no enable password	Очистить пароль Enable	Режим глобального конфигурирования
show running-config	Просмотр текущей конфигурации системы, вы можете увидеть конфигурацию пароля Enable	Привилегированный режим
enable	Интерактивная команда проверяет пароль Enable. После успешной проверки терминал переходит в привилегированный режим	Привилегированный режим

Примечание: Для обеспечения безопасности системы администратору необходимо устанавливать пароль Enable

2.1.5 Служба управления TELNET

В некоторых случаях, администратору не нужно удаленное управление коммутатора, а только через Консольный терминал в местном управлении. Чтобы повысить безопасность системы, чтобы предотвратить незаконный вход в терминал Telnet удаленно, тогда администратор может закрыть службу Telnet.
Ниже перечислены соответствующие команды управления службой Telnet:

Команда	Описание	Режим CLI
security-manage telnet enable	Включить Telnet	Режим глобального конфигурирования
security-manage telnet disable	Отключить Telnet	Режим глобального конфигурирования
security-manage telnet number <1-100>	Числовой параметр колеблется от 1 до 100 и по умолчанию равен 5	Режим глобального конфигурирования
security-manage telnet access-group <1-99>	Укажите группу ACL и откройте исходный элемент управления IP-адресами. Если указанная группа ACL не существует или не является стандартной группой ACL, то исходный IP-адрес не контролируется	Режим глобального конфигурирования
no security-manage telnet access-group	Закрытый исходный контроль IP-адресов	Режим глобального конфигурирования
show security-manage	Вы можете увидеть конфигурацию элементов управления сервиса	Привилегированный режим

2.1.6 Служба управления SNMP

Служба управления SNMP может включать/выключать службу SNMP, а также управлять IP-адресом коммутатора доступа по ACL.Ниже приведены связанные команды управления службами SNMP.

Команда	Описание	Режим CLI
security-manage snmp enable	Включить службу SNMP	Режим глобального конфигурирования
security-manage snmp disable	Выключить службу SNMP	Режим глобального конфигурирования
Security-manage snmp access-group <1-99>	Укажите группу ACL и откройте исходный элемент управления IP-адресами. Если указанная группа ACL не существует или не является стандартной группой ACL, то исходный IP-адрес не контролируется.	Режим глобального конфигурирования
no security-manage snmp access-group	Закрытый исходный контроль IP-адресов	Режим глобального конфигурирования
show security-manage	Вы можете увидеть конфигурацию управления службой	Привилегированный режим

2.1.7 Служба управления HTTP

Служба управления HTTP может включать/выключать службу HTTP, а также управлять IP-адресом коммутатора доступа по ACL

Ниже приведены связанные команды управления службой HTTP.

Команда	Описание	Режим CLI
security-manage http enable	Включить службу HTTP	Режим глобального конфигурирования
security-manage httpdisable	Отключить службу HTTP	Режим глобального конфигурирования
security-manage http access-group <1-99>	Укажите группу ACL и откройте управления исходным IP-адресом. Если указанная группа ACL не существует или не является стандартной группой ACL, то исходный IP-адрес не контролируется.	Режим глобального конфигурирования
no security-manage http access-group	Закрытый исходный контроль IP-адресов	Режим глобального конфигурирования
show security-manage	Вы можете увидеть конфигурацию службы управления	Привилегированный режим

2.1.8 Служба управления SSH

Традиционные сетевые службы, такие как: ftp, pop и telnet не являются безопасными по своей природе, потому что они используют пароли в открытом виде и передачу данных по сети, любой у кого есть скрытый мотив может очень легко перехватить эти пароли и данные. Более того, проверка безопасности этих сервисных программ также уязвима, то есть очень легко произвести атаку «человек посередине» (man-in-the-middle). Так называемая атака «посредника» — вы отправляете данные на сервер «посредник», который выдает себя за реальный сервер для получения данных, а затем притворяется, что данные были переданы на реальный сервер. С помощью SSH можно зашифровать все передаваемые данные, так что «Посредник» не сможет добится результата такой атакой, к тому же это предотвратит DNS-спуфинг и IP-спуфинг. При использовании SSH есть дополнительное преимущество в том, что передача данных сжимается, поэтому можно ускорить скорость передачи. SSH имеет много функций, он может заменить Telnet, но также может использоваться для FTP, PoP и даже для PPP чтобы предоставлять безопасный канал.

2.2 Обслуживание и отладка системы

Основные функции обслуживания и отладки системы включают следующее содержание:

- Настройка имени узла системы
- Настройка системных часов
- Настройка атрибутов времени ожидания терминала
- Перезагрузка системы
- Просмотр информации о системе
- Отладка сетевых подключений
- Определение расстояния между линиями
- Отладка трассировки маршрута
- Клиент Telnet
- Конфигурация UDLD

2.2.1 Настройка имени хоста системы

Имя хоста системы используется для идентификации коммутатора, что облегчает пользователю различать коммутаторы, также имя хоста системы является частью командной строки терминала.
Имя хоста системы по умолчанию — Switch.
Команды имени хоста системы следующие:

Команда	Описание	Режим CLI
hostname <name>	Задать имя хоста системы	Режим глобального конфигурирования
no hostname	Очистите имя узла системы, то есть имя хоста возвращает значение по умолчанию Switch.	Режим глобального конфигурирования
show running-config	Просмотр текущей конфигурации системы, проверка конфигурации имени хоста системы.	Привилегированный режим

2.2.2 Настройка системных часов

Коммутатор обеспечивает функцию часов в реальном времени, текущие часы можно установить с помощью команды, часы также могут быть просмотрены. Системные часы питаются от внутренних, так что часы реального времени могут работать непрерывно, когда система выключена, и системе не нужно сбрасывать часы после запуска.
Коммутатор был настроен на заводское время, пользователю не нужно устанавливать снова, если пользователь обнаружил, что время не разрешено, пользователь может сбросить часы.
Ниже приведены связанные команды системных часов:

Команда	Описание	Режим CLI
set date-time <year> <month> <day> <hour> <minute> <second>	Установите текущего времени системы, нужно ввести параметры года, месяца, дня, часа, минуты и секунды.	Привилегированный режим
show date-time	Показать текущее время системы	Обычный режим, Привилегированный режим

2.2.3 Настройка атрибутов времени ожидания терминала

Для безопасности терминала, когда команды не вводятся более определенного времени, терминал производит выход. Обработка выхода консольного терминала и терминала Telnet не одинакова, для консольного терминала, когда время ожидания терминала заканчивается, режим CLI возвращается в Обычный режим, для терминала Telnet, когда время ожидания терминала заканчивается, соединение Telnet прерывается, происходит выход из терминала Telnet. Время ожидания терминала по умолчанию составляет 10 минут, и пользователь также может настроить терминал без тайм-аута.
Ниже перечислены связанные команды для тайм-аута терминала:

Команда	Описание	Режим CLI
exec-timeout <minutes> [seconds]	Установить время тайм-аута терминала, если параметры равны 0, это означает, что терминал никогда не будет иметь тайм-аута.	Режим конфигурирования терминала
no exec-timeout	Установить время тайм-аута терминала обратно на значение по умолчанию, то есть 10 минут.	Режим конфигурирования терминала
show running-config	Просмотр текущей конфигурации системы, вы можете просматривать конфигурацию тайм-аута терминала.	Привилегированный режим

2.2.4 Сброс системы

Система обеспечивает метод сброса:

- Сброс коммутатора

Ниже перечислены соответствующие команды сброса системы:

Команда	Описание	Режим CLI
reset	Сброс коммутатора	Привилегированный режим

2.2.5 Просмотр информации о системе

Система предоставляет множество команд отображения для просмотра состояния работы системы и системной информации, здесь перечислены только некоторые часто используемые команды отображения обслуживания системы, в следующей таблице:

Команда	Описание	Режим CLI
show version	Отображает номер версии системы и время компиляции исполняемого файла подключения.	Обычный режим, Привилегированный режим
show snmp system information	Отображение основной информации о системе, включая время запуска системы.	Обычный режим, Привилегированный режим
show history	Отображает список недавно введенных команд в командной строке CLI.	Обычный режим, Привилегированный режим

2.2.6 Отладка сетевого подключения

Чтобы наладить соединение коммутатора с другим устройством в сети, необходимо выполнить ping коммутатора на коммутаторе и ping IP-адреса одноранговое устройства. Если коммутатор получает ответ ping от другой стороны, это означает, что два устройства соединены. Коммутатор не только реализует команду ping, но и поддерживает множество опций в команде команда ping. Пользователь может использовать эти опции для более точной и сложной отладки. Команда ping описана в соответствующей таблице:

Команда	Описание	Режим CLI
ping <ip-address> [-n <count> | -l <size> | -r <count> | -s <count> | -j <count> <ip-address>* | -k <count> <ip-address>* | -w <timeout>]*	Команду можно использовать без каких-либо опций или с одной или несколькими опциями. Если у вас нет никаких вариантов, это самая простая команда ping. Когда команда выполняется, вы можете завершить выполнение командой прерывания Ctrl+c.	Привилегированный режим

2.2.7 Диагностика кабеля

Команда	Описание	Режим CLI
show cable-diag interface IFNAME	Определение расстояния до электрического кабеля	Привилегированный режим

2.2.8 Отладка Traceroute

Для отладки промежуточных устройств, через которые коммутатор связывается с другим устройством в сети, необходимо реализовать команду traceroute на коммутаторе. При использовании команды traceroute на коммутаторе, укажите IP-адрес другой стороны. Когда команда будет выполнена, будет показан путь через все узлы которые проходит команда. Коммутатор не только реализует команду traceroute, но и поддерживает множество опций команды traceroute, что позволяет пользователям производить более точную и сложную отладку с помощью этих опций.
Команда traceroute описана в соответствующей таблице:

Команда	Описание	Режим CLI
traceroute <ip-address> [-h <maximum-hops> | -j <count> <ip-address>* | -w <timeout>]*	Вы можете использовать одну или несколько опций. Если у вас нет никаких опций, это самая простая команда traceroute. Когда команда выполняется, вы можете завершить выполнение командой прерывания Ctrl+c.	Привилегированный режим

2.2.9 Клиент Telnet

Коммутаторы серии предоставляют клиентские функции Telnet, и пользователи могут удаленно получать доступ с других устройствам через клиент Telnet.

Команда	Описание	Режим CLI
telnet <ip-address>	Параметр является IP-адресом оконечного устройства	Привилегированный режим

2.2.10 Конфигурация UDLD

UDLD (UniDirectional Link Detection): это протокол второго уровня, который отслеживает физическую конфигурацию канала Ethernet с использованием соединений оптоволокна или витой пары. Когда однонаправленная ссылка (передается только в одном направлении, например, я могу отправить вам данные или получить, но вы отправляете мне данные, которые я не могу получить), UDLD может обнаружить эту ситуацию, закрыть соответствующий интерфейс и отправить предупреждающее сообщение. Однонаправленные ссылки могут вызвать много проблем, особенно связующие деревья, которые могут вызвать циклы. Примечание: UDLD требует, чтобы оба конца канала поддерживались для нормальной работы.
UDLD поддерживает два режима работы: обычный режим (по умолчанию) и радикальный (агрессивный) режим. Общий (нормальный) режим: В этом режиме UDLD может обнаруживать однонаправленные соединения и помечать порты как неопределенные состояния для создания системных журналов. Другими словами, нормальный режим отключает порт, только если он может однозначно определить, что соответствующее соединение неисправно в течение длительного периода времени. Агрессивный режим: В этом режиме UDLD может быть обнаружен однонаправленным соединением. И будет пытаться восстановить связь, непрерывная передача 8 секунд UDLD сообщение, если нет UDLD эхо ответ, этот порт будет помещен в состояние errdisable.

Команда	Описание	Режим CLI
udld enable	Глобальное включение функции UDLD	Режим глобального конфигурирования
udld message time <time>	Интервал передачи сообщений UDLD	Режим глобального конфигурирования
udld port	Включение UDLD на порту	Режим глобального конфигурирования
udld aggressive	Включить радикальный режим порта, по умолчанию нормальный режим	Режим конфигурирования интерфейса
show udld <ifname>	Просмотр информации о UDLD порта	Привилегированный режим

2.3 Управление файлом конфигурации

Конфигурация делится на текущую конфигурацию и начальную конфигурацию. Текущая конфигурация относится к конфигурации системной среды выполнения, наличию системной памяти, а начальная конфигурация используется для запуска конфигурации системы, системный FLASH, то есть файл конфигурации. Когда пользователь выполняет соответствующую команду для изменения текущей конфигурации системы, только реализация команды сохранения перед текущей конфигурацией записывает в начальную конфигурацию для запуска следующей системы. Когда система запущена, система не имеет никакой конфигурации. Текущая информация о конфигурации системы такая же, как и начальная информация о конфигурации.
Текущая конфигурация и начальная конфигурация, использующая один и тот же формат, являются текстовым форматом командной строки, очень интуитивно понятным, легким для чтения пользователями. Формат конфигурационного файла имеет следующие особенности:

- Файл конфигурации представляет собой текстовый файл.
- Все команды сохраняются.
- Сохраняйте только конфигурации, отличные от конфигураций по умолчанию, и не сохраняйте конфигурацию по умолчанию.
- Команды организованы в режиме CLI, а команды в одном режиме CLI организованы вместе, чтобы сформировать сегмент, разделенный "!". Для команд в режиме глобальной конфигурации организуйте команды с одной и той же функцией или функцией, которые должны быть разделены "!".
- Для команды, которая настраивает подшаблон, перед командой ставится пробел, а для команд в режиме глобальной конфигурации не требуется никаких пробелов.
- "end" как конец конфигурации.

Управление файлами конфигурации в основном включает следующее:

- Просмотр информации о конфигурации
- Сохранение конфигурацию
- Удаление файла конфигурации
- Загрузка файла конфигурации

2.3.1 Просмотр информации о конфигурации

Просмотр информации о конфигурации, включая просмотр текущей конфигурации и начальной конфигурации системы. Начальная конфигурация фактически находится в файле конфигурации FLASH, когда FLASH не существует в конфигурационном файле, система начинает использовать конфигурацию по умолчанию, если вы просматриваете начальную конфигурацию системы, система сообщит что файл конфигурации не существует. Команды для просмотра сведений о конфигурации приведены в следующей таблице:

Команда	Описание	Режим CLI
show running-config	Просмотреть текущую конфигурацию системы.	Привилегированный режим
show startup-config	Ознакомится с начальной конфигурацией системы.	Привилегированный режим

2.3.2 Сохранение конфигурации

Когда пользователь изменяет текущую конфигурацию системы, эти изменения необходимо сохранить в файл конфигурации, чтобы такая конфигурация после перезагрузки коммутатора все еще существовала, в противном случае после перезапуска эта информация теряется. Сохранить файл текущей конфигурации в файл начальной конфигурации.
Сохраните команды настроек следующим образом:

Команда	Описание	Режим CLI
write	Сохранить текущую конфигурацию	Привилегированный режим

Примечание: Вам нужно использовать эту команду, чтобы сохранить конфигурацию после настройки коммутатора.
В противном случае конфигурация будет потеряна после перезагрузки системы.

2.3.3 Удаление конфигурационного файла

Когда пользователь хочет вернуться к исходной конфигурации системы, конфигурация по умолчанию может быть удалена, когда вы вернетесь к исходной конфигурации системы для применения настроек нужно перезагрузить коммутатор. Пользователи должны быть осторожны при удалении конфигурационных файлов, иначе конфигурация будет потеряна.
Команды для удаления конфигурационных файлов выглядят следующим образом:

command	describe	CLI mode
delete startup-config	Удалить конфигурационный файл из системы.	Привилегированный режим

2.3.4 Загрузка конфигурационных файлов

Чтобы настроить безопасность файла, пользователь может использовать команду для загрузки файла конфигурации на ПК для выполнения резервного копирования, когда конфигурация системы отсутствует или изменена для возврата к исходной конфигурации, вы можете загрузить исходный файл конфигурации с ПК На коммутатор, загрузить файл конфигурации после того, как текущая конфигурация системы не будет иметь никакого эффекта. Необходимо перезапустить коммутатор после того, как конфигурация вступит в силу.
WEB также может быть настроен на загрузку и скачивание файлов, конкретные операции могут относиться к Web руководству.

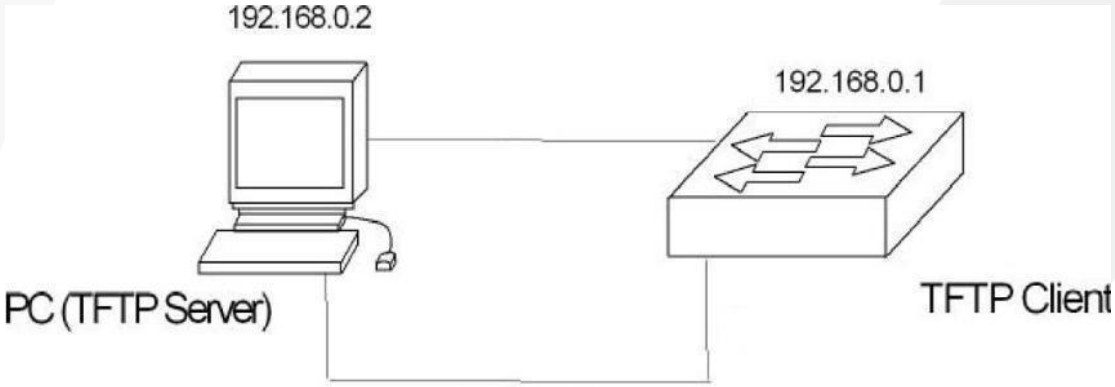
Из файла конфигурации загружаются следующие команды:

Команда	Описание	Режим CLI
upload configure <ip-address> <file-name>	Загрузить конфигурационный файл с ПК, первый параметр — IP-адрес ПК, а вторым параметром является имя конфигурационного файла, хранящегося на ПК.	Привилегированный режим
download configure <ip-address> <file-name>	Конфигурационный файл сохраняется на ПК, первый параметр - IP-адрес ПК, второй параметр - файл конфигурации, хранящийся на имени файла ПК.	Привилегированный режим

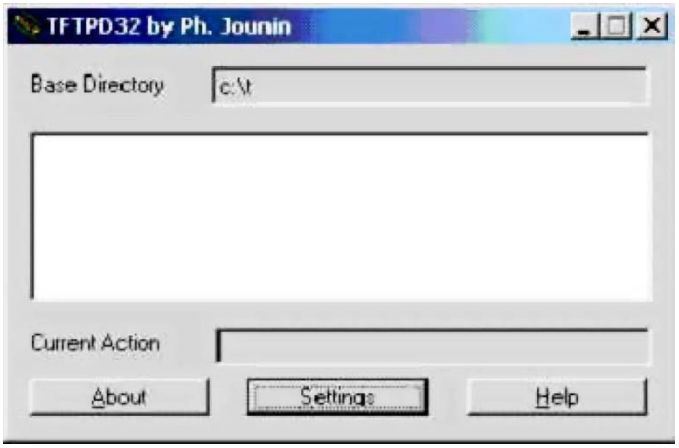
Конфигурационный файл загружается и используется в протоколе TFTP. Клиентское программное обеспечение TFTP запускается на коммутаторе, а программное обеспечение TFTP-сервера — на сервере ПК. Операционные шаги, загруженные из файла конфигурации, следующие:
Первый шаг: Построение сетевой среды.
Второй шаг: Запустите программное обеспечение TFTP-сервера на ПК и установите каталог, хранящийся в конфигурационном файле.
Третий шаг: Сохраните конфигурацию на коммутаторе.
Четвертый шаг: Команда загрузки файла конфигурации выполняется на коммутаторе, а файлы конфигурации резервируются на ПК.
Пятый шаг: Когда коммутатору требуется файл конфигурации с ПК, на коммутаторе выполняется команда загрузки файла конфигурации, а файл конфигурации на ПК загружается на коммутатор.
Шестой шаг: Чтобы конфигурация была эффективной, коммутатор должен быть перезапущен.

Пример: Коммутатор, настроенный с VLAN и адресами интерфейса, который необходимо загрузить в конфигурационный файл.

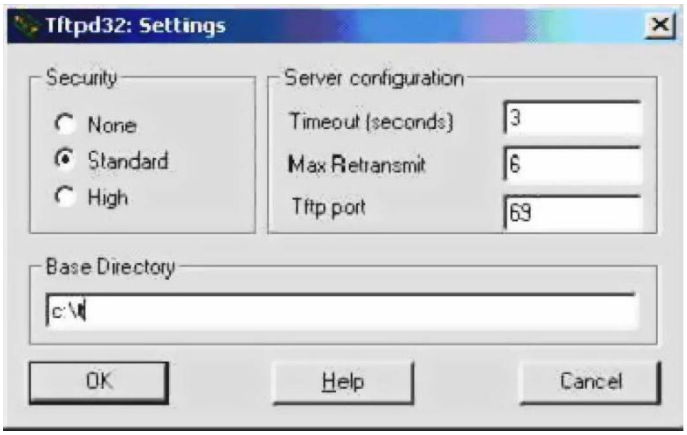
Первый шаг: Создайте следующую сетевую среду.



Конфигурационный порт коммутатора подключается через кабель к ПК. Установите TFTP сервер на ПК, настройте IP-адрес порта Ethernet ПК, предположим, что IP-адрес ПК равен 192. 168.0.2. Затем настройте IP-адрес коммутатора, где предполагается, что IP-адрес коммутатора равен 192.168. 0.1 для обеспечения связи между ПК и коммутатором.
Второй шаг: Запустите TFTP-сервер, настройте параметры TFTP-сервера.
Запустите TFTP Server, интерфейс окна, как показано ниже:



Затем задайте каталог файла конфигурации резервной копии. Конкретная операция заключается в том, чтобы щелкнуть кнопку [Настройки], установите интерфейс, так, как на следующей диаграмме:



Введите путь к файлу в "Base Directory". Нажмите кнопку [OK] для подтверждения.

Третий шаг: Выполните команду write на коммутаторе и сохраните текущую конфигурацию в конфигурационном файле.

Четвертый шаг: Чтобы создать резервную копию файла на ПК, запустите конфигурацию загрузки Switch # 192.168.0.2 beifen.cfg.

Пятый шаг: При необходимости загрузите файл резервной копии на коммутатор и выполните команду Switch#download configuration 192.168.0.2 beifen.cfg.

Шестой шаг: Если вы хотите загрузить файл конфигурации, чтобы он вступил в силу, необходимо перезапустить коммутатор, выполнить команду Switch#reset.

2.4 Обновление версии программного обеспечения

Коммутаторы поддерживают онлайн-обновление версий программного обеспечения. Обновление выполняется с помощью инструмента TFTP.
Основное содержание заключается в следующем:

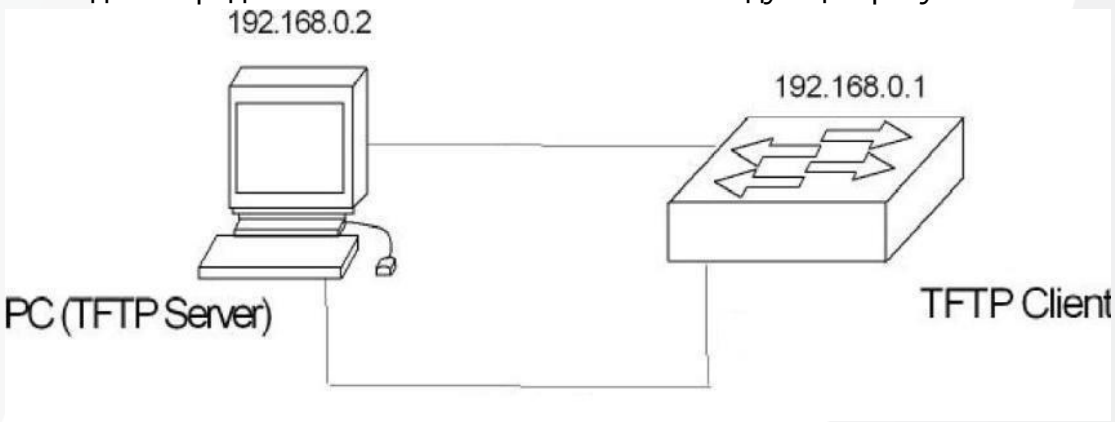
- Команды обновления версии программного обеспечения
- Процесс обновления программного обеспечения

2.4.1 Команды обновления версии программного обеспечения

Обновите файл образа коммутатора в режиме глобальной конфигурации. Команды следующие: download image <ip-address> <file-name>
Где <ip-address> — IP-адрес ПК, на котором запущен TFTP-сервер, и <file-name> имя файла образа, сохраненного на TFTP-сервере.
В процессе обновления нельзя отключать питание, или файл образа коммутатор может быть поврежден и из-за чего сам коммутатор не сможет запуститься. После завершения загрузки необходимо перезапустить коммутатор, чтобы запустить недавно загруженную программу файлов образов. Весь процесс обновления занимает несколько минут.

2.4.2 Процесс обновления программного обеспечения

Обновите файл образа следующим образом:
Первый шаг: Создание среды обновления. Как показано на следующем рисунке.

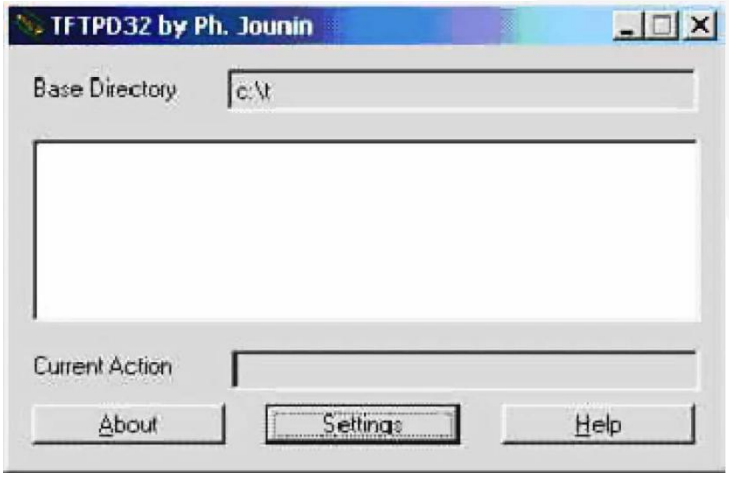


Процесс строительства выглядит следующим образом:

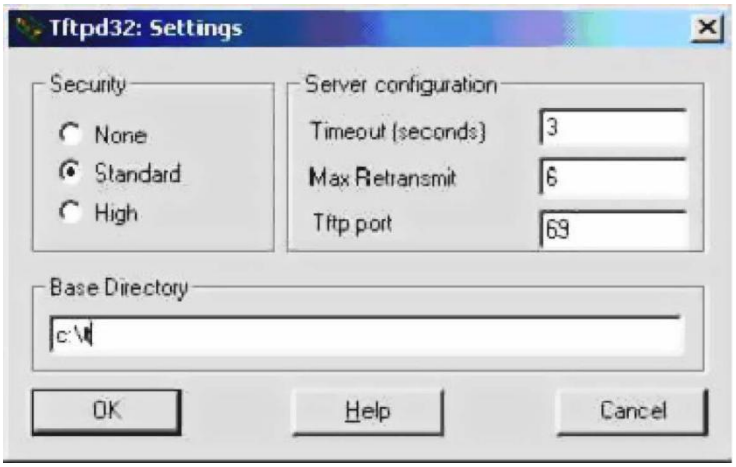
- Подключите консольный порт коммутатора к ПК.
- Установите сервер TFTP на ПК.
- Скопируйте новый файл образа в путь на ПК, где путь предполагается как c:\t;
- Настройте IP-адрес порта Ethernet ПК, где IP-адрес ПК предполагается как 192.168.0.2
- Настройте IP-адрес коммутатора, где IP-адрес коммутатора принимается равным 192.168.0.1

Второй шаг:Запустите сервер TFTP и настройте сервер TFTP.

Запустите сервер TFTP. Интерфейс окна TFTPD32, как показано ниже:



Затем установите каталог файлов TFTP сервера. После запуска TFTP сервера, сбросьте каталог файлов TFTP сервера и скопируйте файлы образа в этот каталог. Конкретная операция, нажмите кнопку [Настройки], там TFTPD32 интерфейс настройки, как показано ниже.



Введите путь к файлу в "Base Directory". Нажмите кнопку [OK] для подтверждения.

Третий шаг:

Файл обновления.

Подключите порт коммутатора к компьютеру программы TFTP Server через

Сеть Ethernet. Команда ping используется для проверки соединения между хостом и коммутатором.

Затем введите команду в подсказке hyperterminal Switch#:

Switch# download image 192.168.0.2 switch.img, Enter and wait for the upgrade file to finish.

Программное обеспечение обновляется. Пожалуйста, подождите и не выключайте питание!

.....

Обновление завершено. Хотите ли вы сбросить настройки?

После завершения передачи файла система укажет, нужно ли перезагрузить коммутатор;В общем, мы рекомендуем выбрать "Y" для перезапуска коммутатора, потому что обновление системы может вступить в силу только после перезапуска;Если ваш файл конфигурации не сохранен, вы можете выбрать "N". сначала не перезапускайте; завершите установку диска и другие операции, затем перезапустите коммутатор. Коммутатор# примечание:

Коммутатор нельзя отключать во время процесса обновления.

Четвертый шаг: Перезагрузка.

Switch# reset

Третья глава

Конфигурация портов

В этой главе представлена конфигурация, связанная с портами, в основном включающая следующее содержимое:

- Общая конфигурация портов
- Конфигурация зеркалирования
- Настройка контроль шторма
- Настройка сдерживания штормов
- Настройка управления потоком
- Настройка пропускной способности портов
- Настройка агрегированных портов
- Настройка сверхкрупного кадра
- Настройка избыточных портов
- Настройка LLDP

3.1 Общая конфигурация портов

Администратор может отключить порт, настраивать порт управления, как, порт доступа коммутатора. Если пользователю не разрешен доступ к сети через порт, администратор может отключить порт. В этом разделе описывается общая конфигурация порта, в том числе:

- Открытие и закрытие портов
- Конфигурация скорости порта
- Отображение информации о порте

3.1.1 Конфигурация скорости порта

Конфигурация скорости по умолчанию для всех портов является адаптивной (автосогласование). Следующая команда настраивает скорость портов в режиме конфигурации интерфейса:
speed {autonegotiate |full-1000 |full-100 |full-10 |half-100 |half-10 } autonegotiate--- self-adaption full-1000------- Full duplex Gigabit full-100-------- Full duplex fast
full-10 -------- Full duplex ten trillion half-100-------- Half duplex Gigabit
half-10--------- Half duplex ten trillion
Например, скорость порта 1/1 настраивается полнодуплексным 100M: Switch(config-ge1/1)# speed full-100

3.2 Конфигурация зеркалирования

Зеркалирование портов является очень полезной функцией для мониторинга потока пакетов, принимаемых и отправляемых одним или несколькими портами. Могут быть использованы зеркальные порты для мониторинга пакетов, полученных и отправленных с одного или нескольких портов. Коммутаторы поддерживают возможности зеркалирования портов, зеркалирование это способность порта отслеживать входящие данные с других портов и данные, которые выходят из строя. Зеркальный порт может контролировать несколько портов одновременно. В этом разделе основное внимание уделяется настройке MIRROR, включая следующее:

- Конфигурация зеркалирования прослушивает порт
- Отображение конфигурации зеркалирования

3.2.1 Конфигурация зеркалирования прослушивания одного порта другим

Когда администратор настраивает порт мониторинга, необходимо войти в режим конфигурации интерфейса, чтобы настроить отслеживаемый порт. Например, установить на порт ge1/1 мониторинг порта ge1/2, нужно ввести порт ge1/1 и ввести команду:

Switch(config-ge1/1)# mirror interface ge1/2 direction both

На этом этапе порт ge1/1 устанавливается на прослушивающий порт, а ge1/2 — на прослушивающий порт.

Команда для настройки отслеживаемого порта выглядит следующим образом:

Switch(config-ge1/1)#mirror interface <if-name> direction {both | receive | transmit}

В это время порт ge1/1 настроен на мониторинг порта, <if-name> настроен на прослушивающий порт, в то время как за {both receive transmit} | | указано направление мониторинга: Receive представляет принятые пакеты; передача отслеживает отправленные пакеты; оба отслеживают все отправленные и полученные пакеты. например:

Switch(config-ge1/1)#mirror interface ge1/2 direction both

Представляет отправляющие и принимающие пакеты порта ge1/1 порта мониторинга ge1/2.

Если вы хотите установить несколько контролируемых портов, вам нужно выполнить несколько команд. В режиме конфигурации интерфейса администратор может отменить отслеживаемый порт, а команда выглядит следующим образом:

Switch(config-ge1/1)#no mirror interface <if-name> direction { receive | transmit}

Когда <if-name> порт прослушивания больше не прослушивается, {прием | передача} указывает, что направление не прослушивается:Прием указывает, что пакет не отслеживается; передача указывает, что пакет не отслеживается, как:

Switch(config-ge1/1)# no mirror interface ge1/2 receive

Указывает, что порт ge1/1 больше не прослушивает пакеты, полученные портом ge1/2.

Когда все контролируемые порты будут отменены, прослушивающий порт также будет очищен.

3.2.2 Отображение конфигурации зеркалирования

Администратор может просмотреть настроенную конфигурацию зеркалирования с помощью следующей команды в обычном или привилегированном режиме:

Switch# show mirror

Необходимо обратить внимание на следующие моменты:

- Порт не может быть одновременно установлен, как прослушивающий порт и прослушиваемый порт.
- Есть только один порт для мониторинга, но есть несколько портов подлежащий мониторингу.

3.3 Настройка управления штормом

В реальной жизни сетевая карта с высокой скоростью одноадресных, многоадресных, широковещательных пакетов может привести к сбою сети, в этом случае включение функции подавления особенно важно, оно может предотвратить перегрузку пакета в сеть, все порты коммутатора поддерживают подавление широковещательных пакетов, многоадресных пакетов и пакетов DLF.

В этом разделе приведено подробное описание конфигурации управление штормом, включая следующие:

- Конфигурация по умолчанию
- Конфигурация подавления широковещательной рассылки
- Конфигурация подавления многоадресной рассылки
- Конфигурация подавления DLF
- Конфигурация скорости подавления
- Отображение конфигурации управление штормом

3.3.1 Конфигурация по умолчанию

Коммутатор поддерживает настройку широковещательных, многоадресных, DLF пакетов для каждого порта отдельно, и три настройки имеют отдельное ограничение скорости. Широковещательное отклонение пакета порта, по умолчанию открыт со скоростью отклонения 64 КБ. Цель состоит в том, чтобы предотвратить формирование в сети широковещательного шторма. Пакеты DLF и пакеты многоадресной рассылки не подавляются по умолчанию.

3.3.2 Конфигурация подавления широковещательной рассылки

Следующая команда настраивает широковещательное подавление выбранного порта в режиме конфигурации интерфейса: storm-control broadcast
Следующая команда отменяет конфигурацию подавления широковещательной передачи для выбранного порта в режиме конфигурации интерфейса: no storm-control broadcast

3.3.3 Конфигурация подавления многоадресной рассылки

Следующая команда настраивает подавление многоадресной рассылки для выбранного порта в режиме конфигурации интерфейса: storm-control multicast
Следующая команда отменяет настройку подавления многоадресной рассылки для выбранного порта в режиме конфигурации интерфейса: no storm-control multicast

3.3.4 Конфигурация подавления DLF

Следующая команда настраивает подавление DLF для выбранного порта в режиме конфигурации интерфейса: storm-control dlf

Следующая команда отменяет настройку подавления DLF для выбранного порта в режиме конфигурации интерфейса: no storm-control dlf

3.3.5 Конфигурация скорости подавления

Следующая команда настраивает скорость блокировки этого порта в режиме конфигурации интерфейса:
storm-control ratelimit { broadcast | dlf | multicast } <1- 1048575 >.

3.3.6 Отображение конфигурации управление штормом

Следующая команда отображает конфигурацию управления штормом в нормальном или привилегированном режиме: show storm-control

3.4 Настройка сдерживания штормов

Контроль порога трафика портов используется для управления штормом сообщений в Ethernet. Порты, которые включают эту функцию, обнаруживают одноадресный трафик, многоадресный трафик и широковещательный трафик сообщений на порту назначения через регулярные интервалы времени. Если класс трафика сообщений превышает заданное пороговое значение верхнего предела, пользователь может настроить его так, чтобы определить, следует ли заблокировать порт или закрыть порт, а также отправить ли информацию о ловушках и журналах.
Когда определенный тип трафика сообщений превышает верхний предел, указанный в сообщении, система предоставляет два метода обработки:

(1) Блокировка: если порт одноадресной, многоадресной, широковещательной рассылки в потоке сообщений больше верхнего порога, порт приостановит пересылку пакетов (другие типы пересылки пакетов, как обычно) порт в блокированном состоянии, но порт по-

прежнему собирает статистику типа потока сообщений. Когда этот тип трафика сообщений станет меньше нижнего порога, порт возобновит пересылку такого рода сообщений.

(2) Режим завершения работы: если класс одноадресной, многоадресной, широковещательной рассылки на порту больше верхнего предела, порт будет закрыт, и система прекратит пересылку всех пакетов. Состояние порта может быть восстановлено путем выполнения команды undo shutdown, а также может быть восстановлено путем отмены конфигурации порога трафика порта.

Примечание: для определенного типа трафика сообщений он может быть подавлен определенной функцией или функцией подавления шторма порта Ethernet, но две функции не могут быть настроены одновременно, в противном случае эффект подавления неясен. Например, функция управления порогом одноадресного трафика и функция подавления одноадресного трафика не могут быть настроены одновременно.

Ниже приведены команды настройки интерфейса командной строки:

Команда	Описание	Режим CLI
storm-constrain (broadcast|multicast|unicast) min-rate <1-1488100> max-rate <1-1488100>	Управление штормом для широковещательных, многоадресных или неизвестных одноадресных сообщений в интерфейсе	Режим конфигурации интерфейса
no storm-constrain (broadcast|multicast|unicast|all)	Отмена управления штормом	Режим конфигурации интерфейса
storm-constrain action (block|shutdown)	Настройка действий управления штормом и, без использования по умолчанию, управления штормом для сообщений	Режим конфигурации интерфейса
no storm-constrain action	Отмена настроенного действия управления штормом	Режим конфигурации интерфейса
storm-constrain enable (log|trap)	Переключение на запись или сообщение тревоги при открытии системы управления штормом	Режим конфигурации интерфейса
no storm-constrain enable (log|trap|all)	Переключатель для регистрации или сообщения о тревоге при закрытии штормового регулятора	Режим конфигурации интерфейса
storm-constrain interval <6-180>	Настройте интервал обнаружения контроля шторма, по умолчанию интервал времени обнаружения контроля шторма составляет 5 секунд	Режим конфигурации интерфейса
no storm-constrain interval	Интервал обнаружения штормового контроля восстанавливается до значения по умолчанию	Режим конфигурации интерфейса
no storm-constrain	Удалить функцию управления штормом интерфейса	Режим конфигурации интерфейса
show storm-constrain	Просмотр информации о штормовом контроле для всех интерфейсов	Привилегированный режим
show storm-constrain interface IFNAME	Просмотр информации об управлении штормом интерфейса	Привилегированный режим

Спецификация конфигурации:

Проект	Описание
interface	Имя интерфейса
type	Тип сообщений (1) broadcast- широковещательное сообщение; (2) multicast-многоадресное сообщение; (3) unicast- одноадресное сообщение
rate	Min- низкий порог; max-высокий порог
action	К действиям по управлению штормом относятся: (1) block-блокировка сообщений; (2) shutdown-закрытие интерфейса
punish-status	Сообщения состояния текущего интерфейса включает в себя (1) block- если скорость больше max-rate и действие управления штормом - блокирующее сообщение, состояние - блокирующее сообщение; (2) Normal - обычная переадресация; (3) shutdown-Если скорость превышает max-rate и действие штормового контроля заключается в закрытии интерфейса, состояние - закрытый интерфейс.
trap	Состояние сигнализации коммутатора, on/off
log	Статус журнала коммутатора, on/off
interval	Интервал обнаружения штормового контроля в секундах, значение по умолчанию — 5 секунд.
last-punish-time	Наконец, время последствие за нарушение штормового контроля

(1) Просмотр таблицы описания информации об управлении штормом для интерфейса.

(2) Выполняя команду storm-constrain action для настройки действия управления штормом и выполняя команду storm-constrain для настройки высокого-низкого порога управления штормом, штормовое сообщение можно контролировать, чтобы предотвратить переполнение. В интервале обнаружения штормового управления, когда средняя скорость широковещательных, многоадресных или одноадресных пакетов на интерфейсе превышает указанное пороговое значение, управление штормом блокирует пакеты в соответствии с настроенными действиями или выключает интерфейс. Когда действие storm control заблокировано, если трафик ниже минимального порога, интерфейс возобновляется в нормальное состояние пересылки. Когда действие управления штормом закрыто, интерфейс не может быть восстановлен автоматически. Для восстановления интерфейса необходимо вручную выполнить команду no shutdown. Конфигурация действия по завершению работы по управлению штормом портов для восстановления.

(3) Трафик порта превышает верхний порог или падает с верхнего предела на нижний порог. Информация о выходном журнале / ловушке.

3.5 Настройка управления потоком

Управление потоком (flow control) используется для предотвращения потери пакетов в случае блокировки портов. В полудуплексном режиме управление потоком осуществляется методом обратного давления (Backpressure), что снижает скорость отправки источника информации. В полнодуплексном режиме управление потоком соответствует стандарту IEEE802.3x. Блокирующий порт отправляет пакет "Pause" источнику информации для приостановки передачи.

В данном разделе приведено подробное описание конфигурации управления потоком (flow control), в том числе следующие:

- Конфигурация по умолчанию
- Настройка управления боковым потоком приема и отправки портов
- Управление потоком в закрытом порту
- Отображение информации об управлении потоком

3.5.1 Конфигурация по умолчанию

Коммутатор поддерживает управление потоком портов отправки и приема для каждого порта. Порт по умолчанию не открывает функцию управления потоком.

3.5.2 Настройка управления боковым потоком приема и отправки портов

Следующая команда настраивает управление боковым потоком приема и отправки портов в режиме конфигурации интерфейса: flowcontrol

3.5.3 Управление потоком в закрытом порту

Следующая команда закрывает управление боковым потоком порта отправки и получения в режиме конфигурации интерфейса: no flowcontrol

3.5.4 Отображение информации об управлении потоком

Следующая команда отображает сведения об управлении потоком для всех портов в обычном или привилегированном режиме: show flowcontrol

Следующая команда отображает информацию об управлении потоком порта в общем или привилегированном режиме: show flowcontrol interface <if-name>

где <if-name> имя порта для запроса информации об управлении потоком.

3.6 Настройка пропускной способности портов

Управление пропускной способностью портов используется для управления скоростью отправки и получения портов.

В этом разделе приводится подробное описание конфигурации пропускной способности портов, включая следующие:

- Конфигурация по умолчанию
- Настройка управления пропускной способностью портов передачи или приема
- Отмена управления пропускной способностью портов передачи или приема
- Управление пропускной способностью конфигурации порта дисплея

3.6.1 Конфигурация по умолчанию

Коммутатор поддерживает пропускную способность отправки и приема на каждый порт соответственно. Порт по умолчанию не выполняет управление пропускной способностью.

3.6.2 Настройка управления пропускной способностью портов передачи или приема

Следующая команда задает порт для отправки или получения управления пропускной способностью в режиме конфигурации интерфейса: portrate {egress | ingress} <rate>
Egress представляет собой контроль пропускной способности над отправленными пакетами.
Ingress представляет собой управление пропускной способностью принимаемых пакетов.
<rate> Говорят, что для установки диапазона значений пропускной способности 11024000, единица измерения равна kbits.

3.6.3 Отмена управления пропускной способностью передачи или приема портов

Следующая команда отменяет управление пропускной способностью порта в режиме конфигурации интерфейса: no portrate {egress | ingress}
Egress представляет собой управление пропускной способностью для отмены отправки пакетов.
Ingress представляет собой управление пропускной способностью отмененного пакета.

3.6.4 Управление пропускной способностью конфигурации порта дисплея

Следующая команда просматривает контроль полосы пропускания конфигурации порта в общем режиме или привилегированном режиме: show portrate interface <if-name>
<if-name> - это имя порта для запроса информации об управлении полосой пропускания.

3.7 Настройка агрегированных портов

Агрегация - это объединение нескольких портов в один логический порт, который может использоваться для увеличения пропускной способности, обеспечения резервных соединений, а также может использоваться для балансировки нагрузки. Когда агрегированная группа используется в качестве выходного логического порта, коммутатор будет отправлять пакет из группы портов, выбирая порт в соответствии с политикой агрегирования, установленной пользователем. Конфигурация порта и стратегии агрегации в агрегированной группе завершается программно, но пересылка потока данных осуществляется аппаратно.
Все порты в агрегированной группе должны быть настроены на одну скорость и в полнодуплексном режиме. Коммутаторы могут поддерживать до 8 агрегированных групп, в каждой агрегированной группе до 8 участников. Особое внимание следует обратить на то, что каждый порт может принадлежать только к одной агрегированной группе.
Протокол LACP является протоколом, основанным на стандарте IEEE802.3a. Протокол LACP взаимодействует с клиентом через LACPDU (Link Aggregation Control Protocol Data Unit).
Интерфейс в группе агрегации включает протокол LACP. Интерфейс сообщает приоритет протокола LACP, MAC-адрес системы, приоритет LACP порта, номер порта и ключ работы аналогу через

LACPDU. После получения LACPDU одноранговый узел сравнивает информацию с информацией, полученной другими интерфейсами, чтобы выбрать интерфейс, который может находиться в выбранном состоянии, чтобы обе стороны могли договориться.

Ключ операции представляет собой конфигурационную комбинацию, которая автоматически генерируется в соответствии с некоторыми конфигурациями портов-участников во время агрегирования каналов. Он включает в себя скорость порта, дуплексный режим, состояние вверх / вниз, VLAN, разрешенные на порту, идентификатор VLAN по умолчанию, тип канала порта (то есть магистральный, гибридный, тип доступа) и так далее. В группе агрегирования порты-участники в выбранном состоянии имеют одну и ту же операцию Key.

В этом разделе приведено подробное описание конфигурации агрегации, включая следующие:

- Конфигурация протокола LACP
- Конфигурация агрегированные группы
- Конфигурация порта-участника агрегированной группы
- Конфигурация политики балансировки нагрузки агрегации
- Отображение агрегации

3.7.1 Конфигурация протокола LACP

Команда	Описание	Режим CLI
lacp system-priority <1-65535>	Установление приоритета системы LACP	Режим глобального конфигурирования
no lacp system-priority	Восстановление системного приоритета по умолчанию 32768	Режим глобального конфигурирования
lacp max-active-link-number <1-8>	Установка LACP для активации верхней границы порта	Режим глобального конфигурирования
no lacp max-active-link-number	Восстановите LACP, чтобы активировать совокупный лимит портов по умолчанию 8	Режим глобального конфигурирования
lacp port-priority <1-65535>	Установить приоритет порта LACP	Режим конфигурирования интерфейса
no lacp port-priority	Восстановить приоритет портов по умолчанию 32768	Режим конфигурирования интерфейса
lacp timeout (short|long)	Установить тайм-аут порта LACP, тайм-аут отсутствующего регулятора	Режим конфигурирования интерфейса
show lacp summary	Показывает все простые вещи о LACP	Привилегированный режим
show lacp detail	Показать все сценарии LACP	Привилегированный режим
show lacp <1-8>	Подробности порта LACP	Привилегированный режим
show lacp port IFNAME	Показать сведения порта LACP	Привилегированный режим
show lacp system-id	Отображение системы LACP	Привилегированный режим
show lacp counter <1-8>	Показать статистику порта LACP	Привилегированный режим
show lacp counter	Show the statistics of all LACP ports	Привилегированный режим

clear lacp <1-8> counters	Очистить статистику LACP порта	Привилегированный режим
clear lacp counters	Очистить статистику всех портов LACP	Привилегированный режим

3.7.2 Конфигурация агрегированной группы

Следующая команда создает агрегированную группу вручную в режиме глобальной конфигурации:

trunk <trunk-id>

Создает агрегированную группу, <trunk-id> диапазон значений 1-8, идентификационный номер агрегированной группы для создания. После успешного создания имя интерфейса агрегированной группы является trunk+id, например если ID группы 1 имя интерфейса агрегированной группы является trunk1.

Вы можете выбрать интерфейс группы агрегации:

interface trunk+id

А затем работать с агрегированной группой, например, использование команды:

interface mode trunk

Следующая команда создает статическую группу LACP TRUNK в режиме глобальной конфигурации:

trunk <1-8> dynamic

Следующая команда удаляет агрегированную группу в режиме глобальной конфигурации:

no trunk <trunk-id>

Когда вы удаляете агрегированную группу, вы должны убедиться, что агрегированная группа не имеет портов участников.

3.7.3 Конфигурация порта участника агрегированной группы

Следующая команда в режиме конфигурации интерфейса новых участников агрегированного порта: trunk interface IFNAME (passive|)

<if-name> - это имя порта, который необходимо добавить в агрегированную группу, и он должен быть двухуровневым интерфейсом. Каждая агрегированная группа может добавить максимум 8 двухуровневых интерфейсов. Если агрегированная группа является статической группой LACP TRUNK, интерфейс добавления по умолчанию находится в активном состоянии и может быть настроен как пассивный.

Следующая команда удаляет все порты-участники агрегированные группы в режиме конфигурации интерфейса: no trunk interface

Следующая команда удаляет указанный порт-участник агрегированные группы в режиме конфигурации интерфейса: no trunk interface <if-name>.

Вы можете использовать эту команду несколько раз для удаления нескольких портов-участников агрегированные группы.

3.7.4 Конфигурация политики балансировки нагрузки агрегации

Следующая команда устанавливает политику балансировки нагрузки агрегации в режиме конфигурации интерфейса: trunk load-balance {dst-mac | dst-ip | src-dst-mac | src-dst-ip | src-mac | src-ip} dst-mac-------- Равновесная стратегия на основе объективного MAC dst-ip----------Равновесная стратегия на основе объективного IP src-dst-mac--- Равновесная стратегия на основе MAC источника и MAC назначения src-dst-ip------ Равновесная стратегия на основе IP источника и IP назначения src-mac-------- Равновесная стратегия на основе MAC источника src-ip---------- Равновесная стратегия на основе IP источника.

Следующая команда устанавливает политику балансировки нагрузки агрегации по умолчанию в режиме конфигурации интерфейса: no trunk load-balance
Политика балансировки нагрузки на порт по умолчанию - src-dst-mac (сбалансированная стратегия на основе MAC источника и MAC назначения).

3.7.5 Отображение агрегации

Следующая команда используется для просмотра всех конфигураций агрегированные группы в общем режиме или привилегированном режиме: show trunk
Следующая команда используется для просмотра конфигурации указанной агрегированные группы в общем режиме или привилегированном режиме: show trunk <trunk-id>.
<trunk-id> - это идентификационный номер проверяемой агрегированные группы.

3.8 Настройка сверхбольшого кадра

3.8.1 Введение сверхбольшого размера

Для того, чтобы порт мог получать сверхбольшой кадр, вы можете настроить порт для поддержки определенной длины суперкадра.

3.8.2 Конфигурация сверхбольших размеров

Конфигурация порта поддерживает суперкадровую длину, в режиме конфигурации, в режиме конфигурации порта, такой как интерфейс ge1/1, выполните следующую команду: Switch(config-ge1/1)# jumbo frame 2000
Сверхбольшая длина кадра, поддерживаемая портом дисплея:
Switch#show jumbo frame ge1/1
Jumbo кадр на порту (байты) ge1/1 2000

3.9 Настройка резервных портов

В некоторых особых случаях, таких как необходимость сосредоточиться на защите определенных серверов, связанных со стабильностью сети, резервный порт коммутатора может обеспечить два порта, связанных с сервером, и гарантировать, что за один раз сервер только один порт связывает сеть, а когда происходит порт LINK DOWN, система немедленно включает другой порт.

Когда порт находится в избыточной группе портов в состоянии LINK UP, мы вызываем активное состояние; с другой стороны, если избыточная группа портов в состоянии LINK DOWN, мы вызываем состояние Disable.

В этом разделе основное внимание уделяется настройке избыточных портов, включая следующие:

- Конфигурация резервных портов
- Отображение избыточных портов

3.9.1 Настройка резервных портов

Можно настроить 8 наборов избыточных портов, группа избыточных портов может настроить только 2 порта; Один порт может быть настроен только для избыточной группы портов.

Избыточная группа портов может настраивать основной и вторичный порты. При настройке избыточных групп портов:

1. Если два порта находятся в состоянии LINK UP одновременно, основной порт устанавливается в состояние Active, а вторичный порт — в состояние Disable;
2. Если только один порт находится в состоянии LINK UP, текущий порт LINK UP устанавливается в состояние Active, а другой порт находится в состоянии Disable;
3. В противном случае два порта выходят из состояния Disable.

Если событие LINK DOWN происходит на порту активного состояния, другой порт попытается стать в активным. Существует также параметр конфигурации - force-switch, который находится во вторичном порту в активном, первичном порту в состоянии Disable, если событие первичного порта LINK UP возникает, когда решение о повторном переключении на первичный порт Для Active, вторичный порт находится в состоянии Disable. Если force-switch настроен как enable, то он принудительно переключается, в противном случае состояние порта исходной избыточной группы портов будет сохранено.

Команда	Описание	Режим CLI
redundant-port <1-8> primary-port IFNAME secondary-port IFNAME [force-switch]	Настройка группы избыточных портов, <1-8> представляет собой группу первичных портов IFNAME — имя главного порта интерфейса. Вторичный порт IFNAME является альтернативным именем интерфейса порта. Необходимо ли использование force-switch	Режим глобального конфигурирования
redundant-port <1-8> force-switch	Принудительное переключение с резервных портов.	Режим глобального конфигурирования
no redundant-port <1-8>	Удалите лишние группы портов.	Режим глобального конфигурирования
no redundant-port <1-8> force-switch	Принудительное переключение для закрытия резервных портов.	Режим глобального конфигурирования

3.9.2 Отображение резервных портов

Команды для отображения резервных портов

Команды	Описание	Режим CLI
show redundant-port	Показать конфигурацию всех резервных групп портов в системе отображения	Привилегированный режим

3.10 Конфигурирование LLDP

В настоящее время типы сетевых устройств становятся все более многочисленными, а их конфигурация - сложной. Для того чтобы устройства разных производителей могли обнаруживать и взаимодействовать друг с другом в сети, им необходима стандартизированная платформа обмена информацией.

LLDP (Link Layer Discovery Protocol) генерируется в этом контексте, он обеспечивает стандартное обнаружение канального уровня, локальное оборудование может быть основной способностью, адресом управления, идентификацией устройства, идентификацией интерфейса и другой информационной организацией (Type / Length / Value), и инкапсулированной в LLDPDU (Link Layer Discovery Protocol Data Unit), выданной соседней директории, непосредственно связанным со своими соседями, получать эту информацию после стандартного MIB (Management Information) Base) в виде сохранения для системы управления сетью для запроса и определения состояния связи связи.

В этом разделе основное внимание уделяется настройке LLDP, включая следующие:

- LLDP конфигурация
- LLDP отображение

3.10.1 Конфигурация LLDP

Существует 4 типа режимов работы порта LLDP:

TxRx: отправка и получение сообщения LLDP.

Tx: отправить только не получить сообщение LLDP.

Rx: только получать, а не отправлять LLDP сообщение.

Disable: не отправляет и не получает сообщения LLDP.

При изменении режима работы LLDP порта порт инициализирует протокол состояния устройства .

Чтобы избежать частой смены режима работы порта и непрерывного выполнения портом операции инициализации, настраивается время задержки инициализации порта, а операция инициализации задерживается при изменении режима работы порта.

Команда	Описание	Режим CLI
lldp global enable	Команда глобального включения LLDP	Режим глобального конфигурирования
lldp hold-multiplier <num>	Мультипликаторы Lldp TTL	Режим глобального конфигурирования
lldp timer [<reinit-delay><time>][< tx-delay><time>][< tx-interval ><time>]	Настройка различных таймеров LLDP	Режим глобального конфигурирования
lldp enable	Включить интерфейс LLDP	Режим конфигурирования интерфейса

lldp admin-status{ disable| rx|tx|rxtx}	Настройка режима работы порта LLDP	Режим конфигурирования интерфейса
lldp check-change-interval <time>	Настройка интервала обновления информационного интерфейса	Режим конфигурирования интерфейса
lldp management-address <A.B.C.D>	Настройка интерфейса LLDP для управления адресами	Режим конфигурирования интерфейса
lldp tlv-enable{ dot1-tlv| dot3-tlv|med-tlv }	Настройка интерфейса LLDP расширенные возможности набора коммутатора	Режим конфигурирования интерфейса

3.10.2 Отображение LLDP

Команды LLDP:

Команды	Описание	Режим CLI
show lldp configuration [ifname]	Отображение сведений о конфигурации lldp	Привилегированный режим
show lldp local-information [ifname]	Отображение локальной информации lldp	Привилегированный режим
show lldp neighbor-information [ifname]	Отображение информации о соседе lldp	Привилегированный режим
show lldp statistics [ifname]	Отображение статистики сообщений lldp	Привилегированный режим
show lldp status [ifname]	Отображение информации о состоянии lldp	Привилегированный режим

Четвертая глава

Безопасность MAC на основе портов

В этой главе представлена конфигурация безопасности MAC на основе портов, включая следующее содержимое:

- Краткое введение
- Конфигурация привязки MAC
- Конфигурация фильтрации MAC
- Конфигурация ограничений обучения портам

4.1 Краткое введение

Безопасность MAC на основе порта может обеспечить три функции: привязка MAC, фильтрации MAC и управления обучением порта для улучшения производительности безопасности двухуровневой пересылки коммутатора.

MAC привязка может быть на основе MAC и порта вместе, ограничения определенного MAC адреса может быть только в определенном порту для доступа к сети; в то же время порт может разрешить доступ к сети только связанным MAC-адресам; порт может одновременно связывать несколько MAC-адресов. Привязка MAC может быть применена к назначенному порту одновременно с 802.1x. Эта функция очень полезна для некоторых устройств, которые не имеют функциональности 802.1x или неудобны для использования устройств 802.1x, таких как принтеры, файловые серверы и т.д.

Фильтрация MAC-адресов позволяет некоторым назначенным MAC-адресам не получить доступ к сети. Основной целью является предотвращение от доступа к сети некоторых незаконных устройств. Когда MAC адрес настроен как MAC фильтр, MAC адрес не может быть доступен на любом порту коммутатора в сети, также не может получить назначение MAC - указанные пакеты данных MAC-адреса и привязку MAC, порт также может настроить фильтрацию нескольких MAC-адресов. В приложении, если какое-либо вирусное программное обеспечение атакует сеть через поддельный MAC-адрес, помимо ACL, атака контроля этих поддельных пакетов может быть доступна с помощью фильтрации MAC.

Управление изучением порта, может управлять портом для динамического определения количества MAC-адресов. Если порт указывает, что он может динамически узнавать количество MAC-адресов, когда количество MAC-адресов, полученных этим портом, равно номеру конфигурации порта, новый MAC-адрес больше не будет изучен. Для этих новых MAC-адресов пакет будет отброшен.
Важно отметить, что MAC-адрес здесь на самом деле MAC + VID. Кроме того, функция привязки MAC и 802.1x могут быть настроены на одном порту одновременно.

Фильтрация MAC-адресов и ограничение изучения портов могут быть настроены на одном порту одновременно. Функция привязки MAC, фильтрация 802.1x и MAC, ограничение обучения портов между двумя группами не может быть одновременно отнесено к одному и тому же порту.

4.2 Конфигурация привязки MAC

Конфигурация привязки MAC поддерживает ручную привязку MAC-адресов и автоматическую привязку MAC-адресов. Ручная привязка MAC-адреса пользователя через команду один за другим входной MAC-адрес и привязка порта. Автоматическая привязка MAC-адреса заключается в чтении существующих записей порта в двухуровневой таблице аппаратной пересылки и непосредственной привязке MAC-адреса. Команда для чтения двухслойной аппаратной таблицы — Show bridge FDB.

Команды конфигурации

Команда	Описание	Режим CLI
switchport-security mac-bind HHHH.HHHH.HHHH vlan <1-4094>	Ручная привязка MAC-адреса к интерфейсу	Режим конфигурирования интерфейса
switchport-security mac-bind auto-conversion number <1-16383>	Автоматическое преобразование заданного количества MAC-адресов в конфигурацию привязки MAC-адресов	Режим конфигурирования интерфейса
switchport-security mac-bind auto-conversion vlan <1-4094>	Автоматическое преобразование заданного количества MAC-адресов в конфигурацию привязки MAC-адресов	Режим конфигурирования интерфейса
show port-security mac-bind [IFNAME]	Конфигурация привязки MAC-адресов дисплея	Привилегированный режим

заметка:
Причина недействительной или неудачной привязки MAC-адреса может быть следующей:
Порт настроен на 802.1x
Порт настроен с фильтрацией MAC-адресов или настроенными ограничениями на обучение порта;
MAC-адрес был привязан к другим портам или настроен с фильтрацией MAC;
Таблица L2 коммутатора заполнена.

4.3 Конфигурация фильтрации MAC

Конфигурация фильтрации MAC поддерживает ручную привязку MAC-адресов и автоматическую привязку MAC-адресов. Ручная настройка фильтрации MAC осуществляется пользователем через ввод команд для фильтрации MAC и привязки порта. Автоматическая настройка фильтрации MAC заключается в считывании существующих записей порта в двухуровневой таблице аппаратной пересылки и непосредственной настройке фильтрации MAC. Команда для чтения двухслойной таблицы оборудования — Show bridge FDB.

Команды конфигурации

Команда	Описание	Режим CLI
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Ручная настройка интерфейса для фильтрации MAC-адресов	Режим конфигурирования интерфейса
switch port-security mac- filter auto-conversion number <1-16383>	Автоматическое преобразование заданного количества MAC-адресов в конфигурацию фильтрации MAC	Режим конфигурирования интерфейса
switch port-security mac-filter HHHH.HHHH.HHHH vlan <1-4094>	Автоматически преобразует MAC-адрес указанной VLAN интерфейса в конфигурацию фильтрации MAC	Режим конфигурирования интерфейса
show port-security mac-filter [IFNAME]	Отображение конфигурации привязки MAC	Привилегированный режим

заметка:

Причина неправильной или неудачной настройки фильтра MAC может быть следующей:

Порт был настроен с привязками MAC или включена функция протокола 802.1x;

MAC-адрес был привязан к другим портам или настроен с привязками MAC;

Таблица L2 коммутатора заполнена.

4.4 Конфигурация ограничения изучения портов

Коммутаторы могут настраивать максимальное количество динамически изученных адресов на порт. Если на порту настроено количество динамически изученных MAC-адресов, то порт может изучить только соответствующее количество MAC-адресов, когда число изученных MAC-адресов более установленного лимита, эти MAC-адреса не изучаются и перенаправление на этот порт отсутствует.

Без ограничений порт может изучать не более 16383 MAC-адресов.

Команды конфигурации

Команда	Описание	Режим CLI
switchport port-security learn-limit <0-16383>	Настройка количества MAC-адресов, которые может изучать интерфейс	Режим конфигурирования интерфейса
no switchport port-security learn-limit	Удаляет лимит количества MAC-адресов, которые может узнать интерфейс.	Режим конфигурирования интерфейса
show port-security learn-limit [IFNAME]	Отобразить конфигурацию изучение портов	Привилегированный режим

Пример конфигурации

Настройка порта ge1/5 позволяет изучить только 7 MAC-адресов

Switch#configure terminal

Switch(config)interface ge1/5

Switch(config-ge1/5)switchport port-security learn-limit 7

примечание:

Причины недействительного или неудачного изучения портом могут быть следующими:

Порт был настроен с привязкой MAC или включена функция протокола 802.1x

Четвертая глава

Привязка портов IP и MAC

В этой главе представлена конфигурация привязки портов IP и MAC, включая следующее содержимое:

- Краткое введение
- Конфигурации привязки IP и MAC
- Пример конфигурации
- Неправильная конфигурация

5.1 Краткое введение

Настройка привязки IP и MAC на портах коммутатора уровня 2 является статической защитой от атак ARP. Злоумышленники атакуют MAC пользователей, отправляя сообщения ARP с ложными MAC-адресами, что приводит к тому, что локальная таблица кэша ARP покрывается адресом злоумышленника, так что обычные потоки данных перенаправляются к злоумышленнику. В конфигурации порта коммутатора команда статической привязки IP-адреса пользователя и MAC-адреса может эффективно фильтровать атакующие ARP пакеты.

В дополнение к функции защиты от спуфинга ARP, функция привязки IP MAC может защитить IP и MAC по сопоставлению, то есть IP может соответствовать только MAC, MAC может соответствовать только IP, если Входящее устройство изменяет это сопоставление, оно не сможет обмениваться данными в этой сети. Функция защиты от спуфинга 802.1x ARP и протокол DHCP SNOOPING являются динамической реализацией этой функции.

Четыре функции: привязка IP MAC, ACL, защита от спуфинга 802.1x ARP и DHCP.

SNOOPING использует один и тот же системный ресурс CFP, и обратите внимание на то, исчерпаны ли ресурсы CFP при настройке. Мы разработали описание схожести в дизайне между ними в следующей таблице:

	Привязка IP MAC	ACL	802.1x	DHCP SNOOPING
Привязка IP MAC	совместимо	несовместимо	совместимо	совместимо
ACL	несовместимо	совместимо	несовместимо	несовместимо
802.1x	совместимо	несовместимо	совместимо	несовместимо
DHCP SNOOPING	совместимо	несовместимо	несовместимо	совместимо

CFP является ограниченным аппаратным ресурсом, в среднем для каждого порта можно настроить только 16 записей привязки IP MAC, поэтому при сетевом доступе к хосту, если необходимо контролировать только несколько портов или небольшое количество IP и MAC-адресов, вы можно использовать статическую функцию привязки IP MAC. Избегание исчерпания функции CFP приводит к сбою пересылки данных.

Кроме того, что касается использования протокола 802.1x или DHCP SNOOPING, в зависимости от текущей ситуации, если вы используете конфигурацию статического IP-адреса и используете

протокол 802.1x для доступа к сети, использование спуфинга 801.1x против ARP будет эффективным. Если используется динамический доступ к IP-адресу, используйте протокол DHCP SNOOPING.

5.2 Конфигурации привязки IP и MAC

IP привязывается к MAC в режиме конфигурирования интерфейса
Настройка привязки портов IP и MAC:
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind A.B.C.D MAC

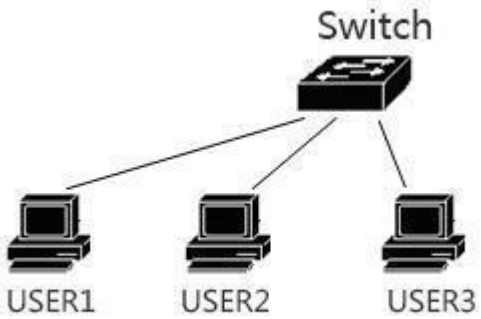
Удалить привязку портов IP и MAC:
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#no ip mac-bind A.B.C.D MAC

Отображение конфигурации
Отображает связанные записи всех портов
show ip mac-bind

Отображает запись в таблице привязок интерфейсов
show ip mac-bind IFNAME

5.3 Пример конфигурации

В сети есть пользователь 1, пользователь 2 и пользователь 3, а IP-адрес и MAC-адрес пользователя привязаны к порту, который может защитить от атаки ARP.



Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#ip mac-bind 192.168.1.100 0011.5b34.42ad
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#ip mac-bind 192.168.1.101 0011.6452.135d
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#ip mac-bind 192.168.1.102 0011.804d.a246
Switch(config-ge1/3)#end

```
Switch#show ip mac-bind

[ge1/1] sum: 1
        MAC                     IP
                0011.5b34.42ad      192.168.1.100
[ge1/2] sum: 1
        MAC                     IP
                0011.6452.135d      192.168.1.101
[ge1/3] sum: 1
        MAC                     IP
                0011.804d.a246      192.168.1.102
Switch#show ip mac-bind ge1/1 [ge1/1] sum: 1
        MAC                     IP
                0011.5b34.42ad      192.168.1.100
Switch#show running-config
!
spanning-tree mst configuration
!
Interface vlan1 ip address 192.168.0.1/24
!
interface ge1/1 ip mac-bind 192.168.1.100 0011.5b34.42ad
!
interface ge1/2 ip mac-bind 192.168.1.101 0011.6452.135d
!
interface ge1/3 ip mac-bind 192.168.1.102 0011.804d.a246
!
line vty
!
end
```

5.4 Неправильная конфигурация

Если конфигурация привязки IP MAC не удалась, это может быть вызвано следующими причинами:

1. Исчерпание ресурсов системы CFP.
2. Текущий интерфейс настроен с функцией фильтрации ACL.
3. Настроенный интерфейс представляет собой трехуровневый интерфейс или интерфейс агрегации.

Шестая глава

Конфигурация VLAN

VLAN является важной концепцией коммутатора и очень часто используется на практике в приложениях. Это основа внутреннего разделения нескольких сетей. VLAN — это сокращение от виртуальной локальной сети (LAN). Это сеть, которая логически соединяет несколько устройств, независимо от их физического местоположения. Каждая VLAN представляет собой логическую сеть, обладающую всеми функциями и атрибутами традиционной физической сети. Каждая VLAN является широковещательным доменом, широковещательные пакеты могут пересылаться только внутри VLAN, не могут передаваться в других VLAN, передача данных VLAN должна передаваться через три уровня.

Основное содержание этой главы следующее:

- введение в VLAN
- конфигурация VLAN
- пример конфигурации VLAN
- MAC, IP подсеть, протокол VLAN
- VOICE VLAN
- сопоставление сетей VLAN
- QINQ

6.1 Введение в виртуальные локальные сети

В этом разделе представлено подробное введение в VLAN, включая следующее содержание:

- Преимущества VLAN
- Идентификатор VLAN
- Тип участника порта VLAN
- VLAN порта по умолчанию
- Режим VLAN порта
- Ретрансляция VLAN
- Перенаправление потока данных в VLAN

6.1.1 Преимущества VLAN

VLAN значительно расширяет масштаб физических сетей. VLAN значительно расширяет масштаб физических сетей. Традиционная физическая сеть может иметь только очень маленький масштаб, который может вместить тысячи устройств, а физическая сеть с использованием VLAN может вместить десятки тысяч или даже сотни тысяч устройств. VLAN имеет ту же функции и атрибуты, как традиционная физическая сеть.

Использование VLAN имеет следующие преимущества:

- VLAN может эффективно контролировать трафик в сети.

В традиционных сетях, независимо от необходимости, все широковещательные пакеты передаются всем устройствам, увеличивая нагрузку на сеть и оборудование. И VLAN может организовать устройства в логической сети в соответствии с необходимостью, VLAN является широковещательным доменом, широковещательные пакеты передаются только в пределах VLAN. Путем разделения VLAN, трафик в сети эффективно контролируется.

- VLAN может улучшить безопасность сети.

Оборудование с VLAN будет работать с другим устройством, на котором VLAN отличен, только посредствам уровня 3. Если переадресация уровня 3 между VLAN не включена, то связи между VLAN не будет. Благодаря этома сети могут быть изолированны между собой, что обеспечивает безопасность данных каждой VLAN. Например, отдел исследований и разработок компании не хочет делиться данными с отделом маркетинга, отдел исследований и разработок может создать свою VLAN. Тогда связь между сетями не будет установлена, если переадресация уровня 3 не включена.

- VLAN позволяет легко перемещать устройство.

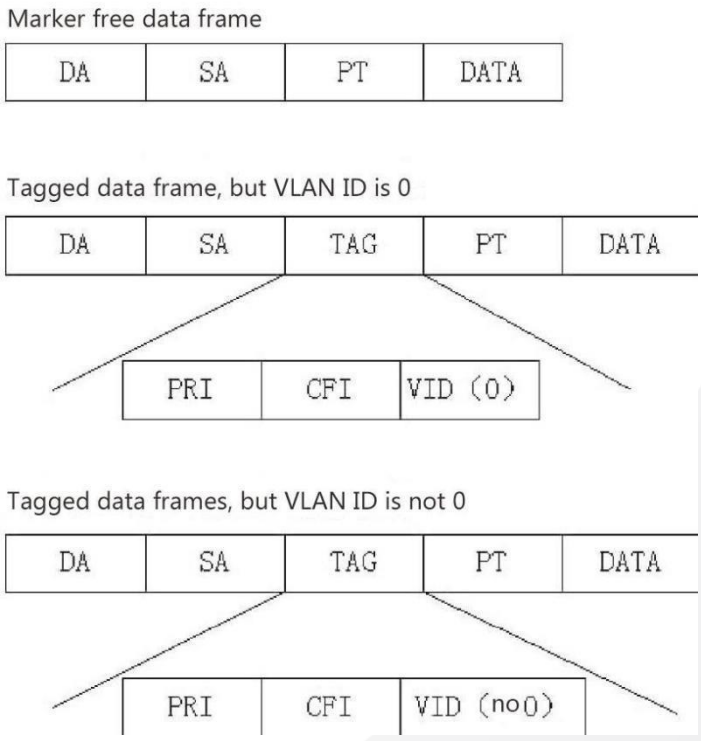
В традиционной сети, если устройство перемещается из одного места в другое, и принадлежит к разным сетям, необходимо изменить сетевую конфигурацию перемещаемого устройства, что очень неудобно для пользователя. VLAN является логической сетью, может быть помещена схожее физическое местоположение, обозначенного в той же сети. Перемещаемое устройство также можно сделать принадлежащим к тому же VLAN, поэтому перемещаемому устройству не нужно изменять какую-либо конфигурацию.

6.1.2 Идентификатор VLAN

Каждая VLAN имеет идентификационный номер, называемый VLAN ID. Диапазон идентификаторов VLAN колеблется от 0 до 4095, из которых 0 и 4095 не используются, а фактическая эффективность составляет всего от 1 до 4094.

Идентификатор VLAN однозначно идентифицирует VLAN.

Коммутатор поддерживает 4094 VLAN, и при создании VLAN вы выбираете идентификатор VLAN в диапазоне от 2 до 4094. Идентификатор VLAN по умолчанию на коммутаторах используется VLAN1, и VLAN1 не может быть удален.



Все кадры данных внутри коммутатора помечены. Если в коммутатор вводится кадр данных без маркера, коммутатор добавляет тег к кадру данных и выбирает значение идентификатора VLAN для

заполнения помеченного VID. Если в коммутатор введен кадр данных с VID 0, коммутатор выбирает значение идентификатора VLAN для заполнения помеченного VID. Если в коммутатор вводится кадр данных с тегом VID non 0, кадр остается неизменным.

6.1.3 Тип порта участника VLAN

Коммутаторы поддерживают VLAN на основе портов и VLAN на основе 802.1Q. VLAN состоит из двух типов элементов порта: нетегированные участники и тегированные участники. VLAN может включать в себя и тегированных и нетегированных участников.
VLAN может не иметь участников, а также может иметь один или несколько участников. Когда порт участник принадлежит к определенному VLAN, он может быть тегированным или нетегированным.Порт может принадлежать одному или нескольким VLAN с тегами или без тегов. Если порт принадлежит двум или более тегированным VLAN, этот порт также называется портом ретрансляции VLAN. Порт может принадлежать одному или нескольким нетегированным VLAN и помеченным, принадлежащим к другой или нескольким VLAN.

6.1.4 VLAN порта по умолчанию

Порт имеет только один VLAN по умолчанию, и VLAN по умолчанию используется для определения VLAN, которая не помечена или не помечена входом VID 0 от порта. VLAN по умолчанию также называется портом VID или PVID. По умолчанию VLAN порта по умолчанию равна 1.

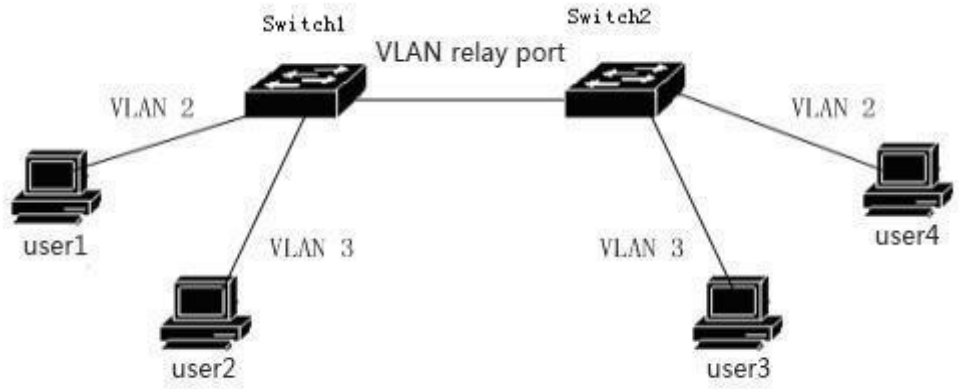
6.1.5 Режим VLAN порта

На порту существует три режима работы VLAN: access, trunk, hybrid. Прежде чем настраивать VLAN нужно настроить режим работы порта.
Режим порта ACCESS представляет собой порт доступа, который непосредственно ориентирован на пользователя. Порт может принадлежать только участнику нетегированного VLAN, а VLAN по умолчанию — это указанный пользователем VLAN. Если порт принадлежит только участнику нетегированного VLAN, режим VLAN порта может быть указан как режим ACCESS. Порт TRUNK является магистральным портом, для прямого подключения коммутаторов, порт может быть участникам одного или нескольких тегированных VLAN, но ни одному нетегированному VLAN принадлежать не может, порт VLAN по умолчанию равен 1, и не может быть изменен. Режим порта HYBRID представляет собой порт ретрансляции, для прямого подключения коммутаторов. Порт может принадлежать одному или нескольким тегированным VLAN и/или одному или нескольким нетегированным VLAN. VLAN по умолчанию этого порта может быть изменен. В практическом применении пользователь может выбрать режим VLAN порта в соответствии с конкретной ситуацией.

6.1.6 Ретрансляция VLAN

Если порт принадлежит двум или более тегированным VLAN, то этот порт также называется портом ретрансляции VLAN. Два коммутатора могут быть подключены к порту ретрансляции VLAN, чтобы два коммутатора можно было разделить на две или более общих VLAN. Ниже приведен пример ретрансляции VLAN, между двумя коммутаторами, подключенными к порту ретрансляции VLAN, порту ретрансляции VLAN 2 и VLAN 3, каждый коммутатор разделен на две VLAN, соответственно,

VLAN 2 и VLAN 3, каждая VLAN имеет пользователя. Таким образом, пользователь 1 может общаться с пользователем 3, а пользователь 2 может общаться с пользователем 4, а пользователь 1 и пользователь 3 не могут общаться с пользователем 2 и пользователем 4.



6.1.7 Перенаправление потока данных в VLAN

Когда коммутатор получает пакет с одного из портов, он пересылается в соответствии со следующими шагами:

- Определить VLAN, к которой принадлежит пакет.
- Определить, является ли пакет широковещательным пакетом данных, многоадресным пакетом или одноадресным пакетом.
- В соответствии с различными пакетами, чтобы определить выходной порт (может быть ноль, один или несколько выходных портов), если нет выходного порта, отбросить пакет
- Отправка из выходного порта.

1) Как определить VLAN пакета:

Если получена метка пакета данных и поле VID в метке не равно 0, то VLAN, к которой принадлежит пакет, является значением VID в метке.

Если полученный пакет не помечен или помечен, но значение VID в теге равно 0, то VLAN пакета принадлежит к VLAN по умолчанию порта.

2) Как определить тип пакетов:

Если MAC-адрес назначения полученного пакета FF:FF:FF:FF:FF:FF:FF:FF, пакет является широковещательным пакетом.

Если полученные пакеты не являются широковещательными пакетами и сороковые биты их MAC-адресов назначения равны 1, то эти пакеты являются многоадресными пакетами.

Если он не является ни широковещательным, ни многоадресным пакетом, то пакет является одноадресным пакетом.

3) Как определить выходной порт пакета:

Если входной пакет является широковещательным пакетом, все порты-участники VLAN, к которым принадлежит пакет, являются выходным портом пакета.

Если входной пакет данных представляет собой многоадресные пакеты данных, то в соответствии с назначением многоадресного MAC-адреса и VLAN для двухуровневой аппаратной многоадресной пересылки записей таблицы пересылки, если они найдены, это многоадресные записи в выходном порту и участник VLAN порта в общем порту (и операция) в качестве пакета выходного порта и если нет общего порта, пакет отбрасывается.

Если две аппаратные многоадресные рассылки перенаправляются многоадресными пакетами и в таблице нет записей, то в соответствии с двухуровневым многоадресным режимом пересылки, аппаратный пересылка на идет на выходной порт, а если многоадресный режим перенаправления не зарегистрирован, многоадресные пакеты используются в качестве радиообработки, все VLAN порта являются портами вывода пакетов, если режим переадресации не зарегистрирован, выходной порт отбрасывает пакеты данных.

Если входной пакет данных является одноадресным пакетом, в соответствии с VLAN найти два аппаратных назначения MAC-адрес и таблицы пересылки, если он находит совпадение, то выходной порт и участников VLAN порт в общий порт (и операции) для пакета данных выходной порт, если не общий порт, пакет отбрасывается. Если в двухуровневой таблице аппаратной переадресации не найдено соответствующих записей, пакет рассматривается как широковещательный пакет, и все порты VLAN относятся к выходному порту пакета.

4) Отправка пакетов данных:

Выходной порт решает отправить пакет со всех выходных портов:

Если выходной порт является нетегированным VLAN, соответствующем пакету данных, пакет не тегируется при отправке с выходного порта.
Если выходной порт является тегированным VLAN, соответствующем пакету данных, пакет тегируется при отправке из выходного порта, а значение VID в теге — это значение VLAN, к которому принадлежит пакет.

6.2 Конфигурация VLAN

В этом разделе содержится подробное введение в конфигурацию VLAN, включая следующие:

- Создание и удаление VLAN
- Настройка режима VLAN порта
- Конфигурация VLAN в режиме ACCESS
- Конфигурация VLAN в режиме TRUNK
- Конфигурация VLAN в гибридном режиме
- Просмотр сведений о VLAN

6.2.1 Создание и удаление VLAN

Перед созданием и удалением VLAN пользователям необходимо использовать команду базы данных VLAN в режиме глобального конфигурирования для перехода в режим конфигурации VLAN и создавать и удалять VLAN в этом режиме.
Система создает VLAN 1 по умолчанию, и VLAN 1 не может быть удален пользователем. Ниже приведены команды для создания и удаления VLAN.

Команда	Описание	Режим CLI
vlan <vlan-id>	Создать VLAN. Если VLAN уже существует, команда не будет обработана. Параметры варьируются от 2 до 4094.	Режим конфигурации VLAN
no vlan <vlan-id>	Удалить VLAN, если VLAN не существует, команда не будет обработана. Параметры варьируются от 2 до 4094.	Режим конфигурации VLAN

6.2.2 Настройка режима VLAN порта

Перед настройкой порта VLAN необходимо указать режим VLAN порта. По умолчанию режимом VLAN порта является режим ACCESS.

Команды настройки режимов VLAN порта в следующей таблице:

Команда	Описание	Режим CLI
switchport mode access	Настроить режим VLAN порта как ACCESS. После выполнения этой команды порт является нетегированным участником VLAN1, VLAN порта по умолчанию — 1.	Режим конфигурирования интерфейса
switchport mode trunk	Настроить режим VLAN порта как TRUNK. После выполнения этой команды порт является тегированным участником VLAN1, VLAN порта по умолчанию — 1.	Режим конфигурирования интерфейса
no switchport trunk	Отменить настройку порта VLAN в режиме TRUNK, порт вернется к режиму по умолчанию, то есть ACCESS.	Режим конфигурирования интерфейса
switchport mode hybrid	Настроить режим VLAN порта как HYBRID. После выполнения этой команды порт является нетегированным участником VLAN1, VLAN порта по умолчанию — 1.	Режим конфигурирования интерфейса
no switchport hybrid	Отменить настройку порта VLAN в режиме HYBRID, порт вернется к режиму по умолчанию, то есть ACCESS.	Режим конфигурирования интерфейса

6.2.3 Конфигурация VLAN в режиме ACCESS

Перед настройкой VLAN на порту, режим VLAN порта должен быть указан как ACCESS. В этом режиме VLAN порт по умолчанию имеет нетегированный VLAN1. Команды настроек VLAN в режиме ACCESS выглядят следующим образом:

Команды	Описание	Режим CLI
switchport access vlan <vlan-id>	Порт конфигурации является нетегированным участником указанной VLAN, а VLAN по умолчанию для порта — указанной VLAN. Диапазон параметров от 2 до 4094.	Режим конфигурирования интерфейса
no switchport access vlan	Конфигурация VLAN порта возвращается к конфигурации по умолчанию, то есть порт является нетегированным участником VLAN1, а VLAN порта по умолчанию — 1.	Режим конфигурирования интерфейса

6.2.4 Конфигурация VLAN в режиме TRUNK

Перед настройкой VLAN на порту, режим VLAN порта должен быть указан как TRUNK. В этом режиме VLAN порт по умолчанию имеет тегированный VLAN1. Команды настроек VLAN в режиме TRUNK выглядят следующим образом:

Команда	Описание	Режим CLI
switchport trunk allowed vlan all	Настроить порт тегированным участником всех VLAN. Для только созданных VLAN порт также является тегированным участником этих VLAN.	Режим конфигурирования интерфейса
switchport trunk allowed vlan none	За исключением VLAN1, порт больше не является участником всех других тегированных VLAN.	Режим конфигурирования интерфейса
switchport trunk allowed vlan add <vlan-list>	Настроить порт в качестве тегированного участника указанной одной или нескольких VLAN. Параметром <vlan-list> может быть VLAN, диапазон VLAN или множество VLAN. Например, параметры могут быть «1», «2-4» или «1,3,5».	Режим конфигурирования интерфейса
switchport trunk allowed vlan remove <vlan-list>	Очистить порт от указанной одной или нескольких VLAN. Порт больше не будет являться тегированным участником этих VLAN. Параметром <vlan-list> может быть VLAN, диапазон VLAN или множество VLAN. Например, параметры могут быть «1», «2-4» или «1,3,5».	Режим конфигурирования интерфейса

6.2.5 Конфигурация VLAN в гибридном режиме

Перед настройкой VLAN на порту, режим VLAN порта должен быть указан как HYBRID. В этом режиме VLAN порт по умолчанию имеет нетегированный VLAN1. Команда настройки VLAN в режиме HYBRID выглядит следующим образом:

Команда	Описание	Режим CLI
switchport hybrid vlan <vlan-id>	Настроить порт в качестве нетегированного участника указанной VLAN и VLAN по умолчанию для порта — указанный VLAN. Диапазон параметров от 2 до 4094.	Режим конфигурирования интерфейса
no switchport hybrid vlan	Очистить порт от значения VLAN по умолчанию, порт больше не является тегированным или нетегированным участником VLAN, а VLAN по умолчанию порта возвращается к 1.	Режим конфигурирования интерфейса
switchport hybrid allowed vlan all	Настроить порт в качестве тегированного участника(кроме VLAN1). Для вновь созданной VLAN порт также является тегированным участником этих VLAN.	Режим конфигурирования интерфейса
switchport hybrid allowed vlan none	За исключением VLAN1, порт больше не является участником всех других VLAN, помеченных или не помеченных тегами, и VLAN по умолчанию порта возвращается к 1.	Режим конфигурирования интерфейса
switchport hybrid allowed vlan add <vlan-list> egress-tagged enable	Настроить порт в качестве тегированного участника указанной одной или нескольких VLAN. Параметром <vlan-list> может быть VLAN, диапазон VLAN или множество VLAN. Например, параметры могут быть «1», «2-4» или «1,3,5».	Режим конфигурирования интерфейса

switchport hybrid allowed vlan add <vlan-list> egress-tagged disable	Настроить порт в качестве тегированного участника указанной одной или нескольких VLAN. Параметром <vlan-list> может быть VLAN, диапазон VLAN или множество VLAN. Например, параметры могут быть «1», «2-4» или «1,3,5».	Режим конфигурирования интерфейса
switchport hybrid allowed vlan remove <vlan-list>	Очистить порт от указанной одной или нескольких VLAN, порт более не является тегированным или нетегированным участником этих VLAN. Если VLAN порта по умолчанию принадлежит указанной VLAN, то VLAN по умолчанию возвращается в 1.	Режим конфигурирования интерфейса

6.2.6 Просмотр информации о VLAN

Команды для просмотра сведений о VLAN перечислены ниже:

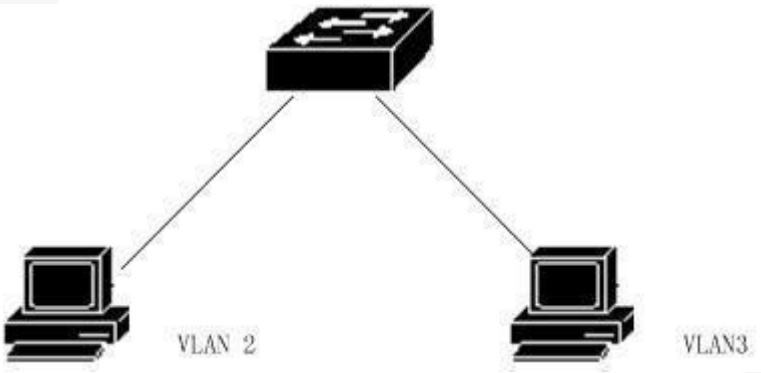
Команда	Описание	Режим CLI
show vlan [vlan-id]	Если параметры не введены, отображает всю информацию VLAN, если вы вводите параметры, отображает указанную информацию VLAN. Параметры варьируются от 1 до 4094.	Обычный режим, привилегированный режим
show interface switchport	Отображение информации, связанной с VLAN всех портов системы, таких как режим VLAN, VLAN по умолчанию и т.д.	Обычный режим, привилегированный режим
show running-config	Просматривая текущую конфигурацию системы, можно узнать конфигурацию VLAN.	Привилегированный режим

6.3 Пример конфигурации VLAN

6.3.1 VLAN на основе порта

1) Конфигурация

Есть два пользователя, 1 пользователь и 2 пользователя. Два пользователя должны находиться в разных VLAN из-за разных сетевых функций и сред. Пользователь 1 принадлежит к VLAN2, подключает порт коммутатора ge1/1, пользователь 2 принадлежит к VLAN3, подключает порт коммутатора ge1/2.



Конфигурация коммутатора выглядит следующим образом:
Создание VLAN

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
```

Назначение портов для VLAN

```
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan
```

2) **Устранение неполадок**

Если при конфигурации обнаруживается, что ПК с разными VLAN не могут общаться, это является нормальным явлением, потому что разные VLAN для связи, должны пройти маршрутизацию уровня 3. Если компьютеры в одной виртуальной локальной сети не могут взаимодействовать друг с другом, необходимо выполнить следующую проверку:

```
show vlan
```

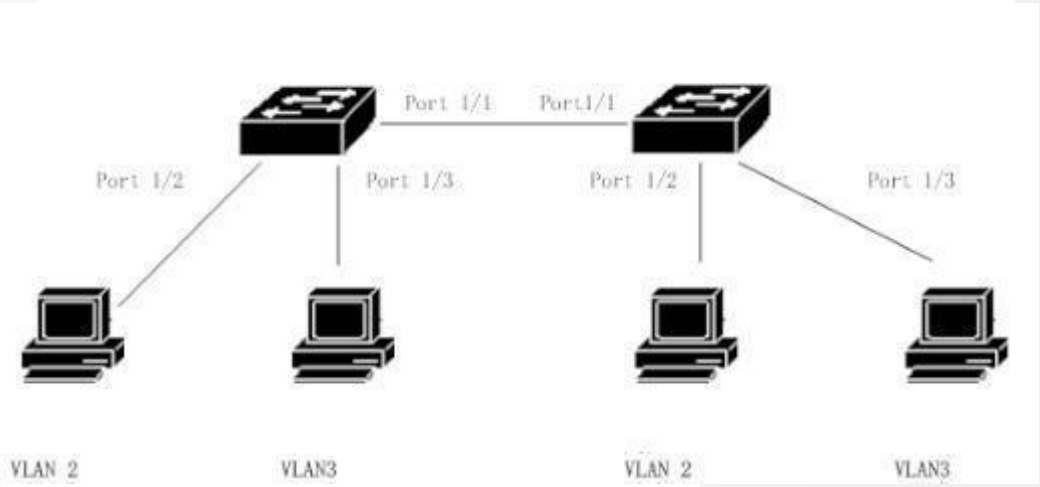
Просмотр всех портов-участников VLAN

```
show vlan <vlan-id>
```

Проверьте, находится ли порт, соединяющий определенный компьютер с ПК, в указанной VLAN

6.3.2 VLAN на базе 802.1Q

1) **Конфигурация**



Два коммутатора, подключенных к двум пользователям:

Пользователь	принадлежит к VLAN	Порт подключения	Собственный коммутатор	Каскадный порт
Пользователь 1	2	1/2	коммутатор 1	1/1
Пользователь 2	3	1/3	коммутатор 1	1/1
Пользователь 3	2	1/2	коммутатор 2	1/1
Пользователь 4	3	1/3	коммутатор 2	1/1

Вам нужно настроить на два коммутатора.
Конфигурация коммутатора 1:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3
```

Конфигурация коммутатора 2:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch#config t
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 2
Switch(config-ge1/1)#switchport trunk allowed vlan add 3
Switch(config)#interface ge1/2 Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 2
Switch(config-ge1/2)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 3
```

2) **Устранение неполадок**

Межкоммутаторная VLAN, в пределах одной VLAN ПК должен взаимодействовать, если нет. Смотрите ниже:

- Подключите порт ПК который принадлежит к соответствующему VLAN, и настройте режим ACCESS для добавления к VLAN.
- Каскадный порт 1/1 добавлен в каждую VLAN, а порт 1/1 находится в режиме TRUNK.

6.4 VLAN на основе MAC, IP-подсети, протокола

VLAN на основе MAC основывается на MAC-адресе источника текста для разделения. После получения нетегированного (или тег 0) сообщения от порта, VLAN сообщения определяется в соответствии с MAC-адресом источника сообщения, а затем сообщение автоматически делится на назначенную VLAN передачи;

VLAN на основе IP подсети делится в соответствии с IP-адресом и маской подсети источника газеты. После получения нетегированного сообщения от порта, VLAN сообщения определяется в соответствии с адресом источника сообщения, а затем сообщение автоматически делится на назначенную передачу VLAN. Эта функция в основном используется для отправки сообщений из назначенных сегментов сети или IP-адресов в указанных VLAN;

VLAN на основе протокола назначает различные VLAN ID сообщению в соответствии с типом протокола сообщения, полученного портом. Протоколы, которые могут быть использованы для разделения VLAN, это IP, IPV6, IPX и т.д.

Перед конфигурированием VLAN на основе MAC, IP подсети и протокола, сначала должна быть создана соответствующая VLAN.

Команда	Описание	Режим CLI
mac-vlan mac WORD vlan <1-4094>	Создание VLAN на основе MAC-адреса источника	Режим конфигурирования интерфейса
no mac-vlan mac WORD	Удаление VLAN на основе MAC-адреса источника	Режим конфигурирования интерфейса
no mac-vlan	Удалить все VLAN на основе MAC-адреса источника	Режим конфигурирования интерфейса
show mac-vlan	Отображает все VLAN на основе MAC-адреса источника	Привилегированный режим
ip-subnet-vlan ip A.B.C.D A.B.C.D vlan <1-4094>	Создание VLAN на основе IP-подсети источника	Режим конфигурирования интерфейса
no ip-subnet-vlan ip A.B.C.D A.B.C.D	Удаление VLAN на основе IP-подсети источника	Режим конфигурирования интерфейса
no ip-subnet-vlan	Удаление всех VLAN на основе IP-подсети источника	Режим конфигурирования интерфейса
show ip-subnet-vlan	Отображение всех VLAN на основе IP-подсети источника	Привилегированный режим
protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>) vlan <1-4094>	Создание VLAN на основе протокола	Режим конфигурирования интерфейса
no protocol-vlan ether-type (ip|ipv6|ipx|…|<0-65535>)	Удаление сети VLAN на основе протокола	Режим конфигурирования интерфейса
no protocol-vlan	Удалить все VLAN на основе протокола	Режим конфигурирования интерфейса

show protocol-vlan	Показать все VLAN на основе протокола	Привилегированный режим
show vlan-partition interface IFNAME	Интерфейс отображения позволяет использовать VLAN на основе MAC, IP-подсети, протокола	Привилегированный режим

6.5 Голосовая VLAN

Голосовая VLAN является специализированной VLAN для голосовых потоков данных пользователей. По разделению Голосовая VLAN и голосовой порт подключения устройства присоединиться к Голосовой VLAN, для голосовых данных конфигурации QoS (качество обслуживания) параметры, голосовые данные в приоритете, обеспечивает качество связи.

Устройство может определить, является ли поток данных потоком голосовых данных в соответствии с полем OUI MAC-адреса источника в пакете данных, поступающем в порт. Если MAC-адрес источника соответствует системным настройкам голосового устройства, OUI-адрес пакета считается потоком голосовых данных, делится на передачу Voice VLAN.

Пользователь может предварительно установить OUI-адрес или использовать OUI-адрес по умолчанию в качестве стандарта суждения, как показано ниже

Серийный номер	OUI адрес	Производитель
1	0001-e300-0000	телефон Siemens
2	0003-6b00-0000	телефон Cisco
3	0004-0d00-0000	телефон Avaya
4	00d0-1e00-0000	телефон Pingte
5	0060-b900-0000	телефон Philips/NEC
6	00e0-7500-0000	телефон Polycom
7	00e0-bb00-0000	телефон 3com

Вручную добавить IP порт доступа к Voice VLAN. Затем, путем определения MAC источника сообщения и сопоставления OUI адреса, после успешного сопоставления, система будет отправлять приоритет в правила ACL и конфигурационные сообщения.

Режим безопасности и общий режим голосовой VLAN, безопасный режим: В голосовой VLAN разрешено передавать только совпадающие по OUI языковые потоки, а несовпадающие по OUI потоки данных не разрешено передавать в голосовой VLAN; Нормальный режим: Все потоки данных могут передаваться в голосовой VLAN.

Перед настройкой Voice VLAN необходимо сначала создать соответствующую VLAN.

Команда	Описание	Режим CLI
voice-vlan security (enable|disable)	Включить режим безопасности голосовой VLAN	Режим глобального конфигурирования
voice-vlan oui WORD mask WORD	Настройка пользовательского OUI	Режим глобального конфигурирования
voice-vlan oui WORD mask WORD description WORD	Настройка OUI и имени пользователя	Режим глобального конфигурирования
no voice-vlan oui WORD mask WORD	Удаление конфигурации OUI пользователя через адрес и маску OUI	Режим глобального конфигурирования
no voice-vlan oui description WORD	Удаление конфигурации OUI пользователя по имени	Режим глобального конфигурирования
no voice-vlan oui	Удаление всех пользовательских конфигураций OUI	Режим глобального конфигурирования
no voice-vlan default-oui WORD mask WORD	Удаление стандартной конфигурации OUI через адрес и маску OUI	Режим глобального конфигурирования
no voice-vlan default-oui description WORD	Удаление конфигурации OUI по имени	Режим глобального конфигурирования
no voice-vlan default-oui	Удаление всех конфигураций OUI по умолчанию	Режим глобального конфигурирования
voice-vlan default-oui resume	Восстановление всех стандартных конфигураций OUI	Режим глобального конфигурирования
show voice-vlan oui	Отображение всех конфигураций пользовательского интерфейса и пользовательских конфигураций по умолчанию	Режим глобального конфигурирования
voice vlan <1-4094> (enable|disable)	Интерфейс включения голосовой VLAN	Режим глобального конфигурирования
voice vlan qos map-queue <0-7> remark-dscp <0-63>	Приоритет QoS конфигурации интерфейса, очередь по умолчанию 6, DSCP 46	Режим глобального конфигурирования
no voice vlan qos	Восстановление конфигурации приоритета QoS интерфейса по умолчанию	Режим глобального конфигурирования
no voice vlan	Удалить конфигурацию интерфейса Голосовой VLAN	Привилегированный режим
show voice-vlan state	Отображение всех интерфейсов, настроенных с помощью голосовой VLAN	Режим конфигурирования интерфейса

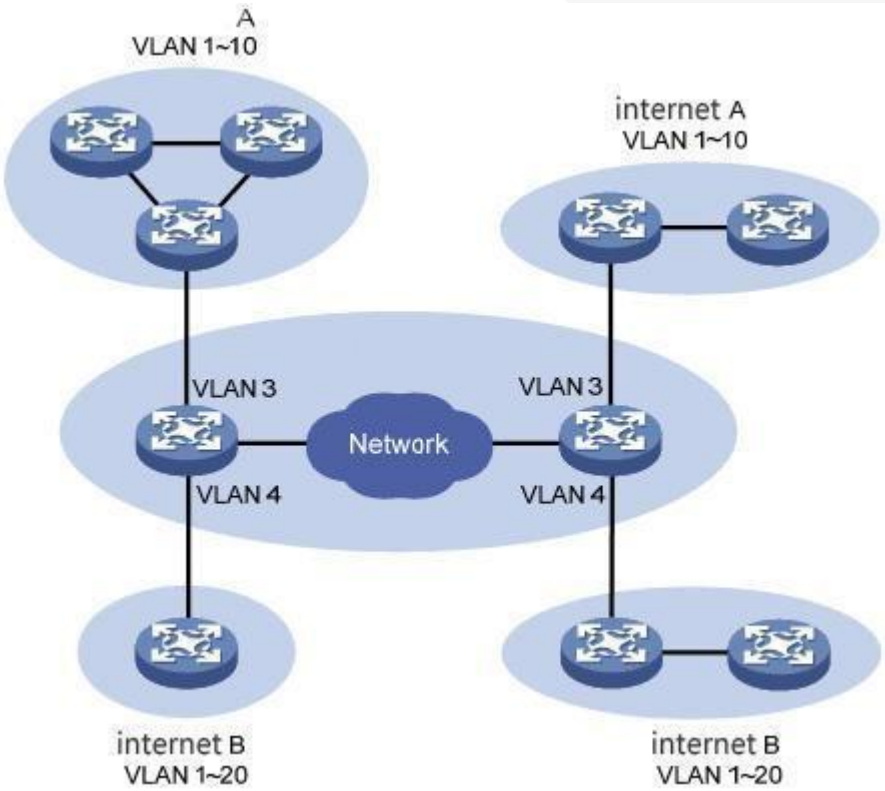
6.6 Сопоставление VLAN

Функция сопоставления VLAN (т.е. VLAN Mapping) может изменять тег VLAN с сообщением, обеспечивая следующую связь сопоставления: Сопоставление VLAN 1:1: сообщение, несущее тег VLAN в идентификаторе VLAN, изменяется на другой идентификатор VLAN.
Перед настройкой сопоставления VLAN необходимо сначала создать соответствующую VLAN.

Команда	Описание	Режим CLI
vlan-mapping vlan <1-4094> map-vlan <1-4094>	Отношение сопоставления VLAN для настройки портов	Режим конфигурирования интерфейса
no vlan-mapping vlan <1-4094>	Сопоставление VLAN для удаления портов	Режим конфигурирования интерфейса
no vlan-mapping	Все сопоставления VLAN для удаления портов	Режим конфигурирования интерфейса
show vlan-mapping	Отображение сопоставления VLAN всех конфигураций	Привилегированный режим

6.7 QinQ

Характеристики порта QinQ обеспечиваются простой и гибкой двухуровневой технологией VPN, через оператор сети пограничного устройства для пользователей в частной сети пакетов уровня инкапсуляции VLAN Tag магистральной сети, сообщения, которые несут двухслойные VLAN Tag traversal (public). В общедоступной сети только по внешнему VLAN Tag оборудование для передачи сообщения, а сообщение из исходной таблицы MAC-адресов для изучения внешнего тега, где таблица MAC-адресов VLAN и частная сеть VLAN Tag пользователей в процессе передачи будут находиться в составе передаваемых пакетов данных. Функция QinQ позволяет оператору использовать VLAN для обслуживания сети пользователей с несколькими VLAN. Как показано ниже, пользовательская сеть A частная сеть VLAN - это VLAN 1 ~ 10, пользовательская сеть B частная сеть VLAN - VLAN 1 ~ 20. A, выделенная оператором для пользовательской сети VLAN, является VLAN 3, а выделенная для пользовательской сети B, — VLAN 4. Пользователь сети A с пакетами VLAN Tag в сети операторов, сообщение будет находиться вне пакета на уровне VLAN ID 3 VLAN Tag; Пользователь B сети с пакетами VLAN Tag в сетевых операторах, сообщение будет находиться вне пакета на уровне VLAN ID 4 VLAN Tag. Таким образом, пакеты различных пользовательских сетей полностью отделены друг от друга при передаче в общедоступную сеть. Даже если диапазон VLAN из двух пользовательских сетей перекрывается, нет путаницы в передаче в общедоступную сеть.



Функции QinQ позволяют сети предоставлять максимум 4094 * 4094 VLAN и соответствовать требованиям VLAN в городской сети, это в основном решает следующие проблемы:

(1) Уменьшить растущую нехватку ресурсов VLAN общедоступной сети.

(2) Пользователи могут установить свой собственный идентификатор VLAN частной сети и это не приведет к конфликту с идентификатором VLAN публичной сети.

(3) Предоставление относительно простого двухуровневого VPN-решения для небольших городских сетей или корпоративных сетей.

QinQ можно разделить на два типа: базовый QinQ и гибкий QinQ.

(1) Базовый QinQ: базовый QinQ реализован в режиме порта. После открытия основной функции QinQ порта, когда порт получает сообщение, устройство отправит сообщение по умолчанию VLAN - VLAN Tag для этого сообщения. Если полученное сообщение уже является VLAN Tag, оно становится сообщением двойного тега; Если полученное сообщение не является VLAN Tag, оно становится сообщением с тегом VLAN по умолчанию для порта.

(2) Гибкий QinQ: является более гибкой реализацией QinQ, которая основана на комбинации порта и VLAN. В дополнение ко всем основным функциям QinQ, сообщение, полученное одним и тем же портом, также может выполнять различные действия в соответствии с другой VLAN, чтобы добавить разные внешние теги VLAN для пакетов с разным идентификатором VLAN внутреннего уровня.

Команда	Описание	Режим CLI
qinq tpid WORD	Настройте значение TPID, содержащееся в теге VLAN порта, по умолчанию 0x8100	Режим конфигурирования интерфейса
no qinq tpid	TPID порта восстановления по умолчанию	Режим конфигурирования интерфейса
qinq uplink	Настраиваемый порт является портом исходящей линии связи	Режим конфигурирования интерфейса
no qinq uplink	Конфигурация исходящей линии связи для отмены настройки портов	Режим конфигурирования интерфейса
qinq customer	Настраиваемый порт является клиентским портом	Режим конфигурирования интерфейса
no qinq customer	Конфигурация клиента для отмены настройки портов	Режим конфигурирования интерфейса
qinq outer-vid <1-4094> inner-vid VLAN_ID	Преобразование VLAN для настройки интерфейсов	Режим конфигурирования интерфейса
no qinq inner-vid VLAN_ID	Преобразование VLAN для удаления интерфейсов	Режим конфигурирования интерфейса
no qinq outer-vid <1-4094>	Преобразование VLAN для удаления интерфейсов	Режим конфигурирования интерфейса
show qinq	Отображение всех настроенных условий QinQ	Привилегированный режим

Седьмая глава

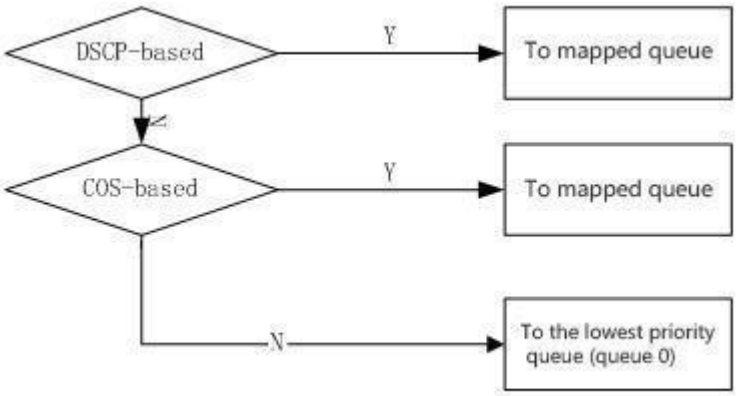
Конфигурация QoS

В этой главе описывается QoS и его конфигурация, включая следующее:

- Введение в QoS
- Конфигурация QoS
- Пример базовой настройки QoS
- Пример конфигурации политик QoS

7.1 Введение в QoS

Используя функцию QoS коммутатора, вы можете задать важность потока данных, пересылаемых коммутатором, приоритетной обработкой, сделать использование полосы пропускания вашей сети более разумным, производительность сети станет предсказуемой.
В пакете определяется его очередность в соответствии с информацией о приоритете пакета.
Коммутатор реализует QoS на основе COS (802.1p), QoS на основе DSCP (DiffServ) и QoS на основе MAC. QoS на основе DSCP можно настроить на физическом порту; физический порт по умолчанию запускает QoS на основе COS.
Ниже приведен процесс пересылки пакетов с поддержкой QoS:



Коммутаторы поддерживают 0~7 восьми приоритетных очередей, очередь 7 имеет наивысший приоритет, а очередь 0 имеет самый низкий приоритет. Существует три метода планирования очереди с приоритетом: SP, WRR, WFQ. SP - это планирование со строгим приоритетом, приоритетная очередь всегда пересылает пакеты данных очереди 7, пока не будет завершена пересылка очереди 7, после начнется пересылка очереди 6, пересылка очереди 6 должна быть завершена прежде чем начнется пересылка пакетов очереди 5. WRR - опрос с взвешенным приоритетом на коммутаторе, при пересылке пакетов, в соответствии с распределением прав очереди с высоким приоритетом на очередь с низким приоритетом, пересылка первым пакета данных с высоким приоритетом в нужное время, пакеты с низким приоритетом пересылаются в

конец очереди. Из высокоприоритетного класса пакеты выдвигаются вперед. Алгоритмы планирования очередей WFQ и WRR аналогичны, в алгоритме взвешивания поддерживается подсчет байтов и вес, а также поддержка пакетов SP, которые могут заменять друг друга. Разница заключается в следующем: WRR поддерживает максимальную задержку, может гарантировать максимальную задержку конфигурационного сообщения в очереди от входа в очередь до максимального времени выхода из очереди, не превышающего установленного; WFQ поддерживает гарантированную пропускную способность, минимальная пропускная способность очереди может гарантировать перегрузку трафика порта, если она доступна.

Чтобы упростить настройку, мы вводим концепцию QosProfile. QosProfile — это атрибут отношения сопоставления, настроенный с 802.1p и приоритетными очередями, который не может быть настроен пользователем. Их отношения отображения следующие:

QosProfile	802.1p(CoS)	Очередь с приоритетом
Qp0	0	0
Qp1	1	1
Qp2	2	2
Qp3	3	3
Qp4	4	4
Qp5	5	5
Qp6	6	6
Qp7	7	7

7.1.1 QoS на основе COS

Порт включен по умолчанию в режиме QoS на основе COS. Возможность обмена получает значение приоритета VLAN TAG в пакете, входящем в порт, и определяет выходную очередь пакета в соответствии с отношением отображения между значением COS, настроенным пользователем, и очередью. Если пакет данных не является VLAN TAG или VLAN TAG VID равен 0, то коммутатор в соответствии с пользовательской конфигурацией порта и порта VID приоритета по умолчанию заполняет пакет данных, а затем в соответствии с выходной очередью пакета определяет приоритет по умолчанию.

7.1.2 QoS на основе DSCP

Если на порту включен DSCP на основе QoS, то обмен возможностью получения пакетов IP-данных в порт по значениям DSCP в выходной очереди и принятие решения по пакету в соответствии с отношением отображения между значением DSCP и пользовательской конфигурацией очереди.

Тип cos-dscp является расширением на основе типа cos типа DSCP, который по сути является типом DSCP или типом cos. Если используется тип cos-dscp, система IP-сообщений будет автоматически соответствовать приоритету DSCP, а система не IP-сообщений будет основываться на приоритете cos.

В соответствии с типом приоритета (dscp/cos) осуществляется соответствующее планирование.

7.1.3 QOS на основе политики

Политика QoS включает классы и действия политики. Класс используется для идентификации потока, и пользователь может определить серию правил по команде для классификации пакета; действие политики используется для определения действия QoS для сообщения правила согласования. Если порт включен стратегии на основе QoS, коммутатор будет вводить порт классификации пакетов, чтобы удовлетворить требования классификации пакетов данных, коммутатор будет обрабатывать пакет в соответствии со стратегией действий обработки данных порта, пакет не соответствующий требованиям классификации пакетов не обрабатывается.

7.2 Конфигурация QoS

7.2.1 Конфигурация по умолчанию для QoS

Элемент конфигурации	Значение	Можно ли настроить
Номер очереди	8	нет
Диспетчерский режим	WRR	да
Включить ли планирование SP	disable	да
Включить ли планирование WFQ	disable	да
Вес очереди	qp0[1],qp1[2],qp2[4],qp3[8],qp4[16] qp5[32],qp6[64],qp7[127]	да
Отображение отношений между COS и qosprofile	COS0[qp0] COS1[qp1] COS2[qp2] COS3[qp3] COS4[qp4] COS5[qp5] COS6[qp6] COS7[qp7]	нет
Сопоставление отношений между DSCP и qosprofile	DSCP0~DSCP7[qp0] DSCP8~DSCP15[qp1] DSCP16~DSCP23[qp2] DSCP24~DSCP31[qp3] DSCP32~DSCP39qp4] DSCP40~DSCP47[qp5] DSCP48~DSCP55[qp6] DSCP56~DSCP64[qp7]	да
Атрибуты Qosprofile	qp0 cos[0] 0 qp1 cos[1] 1 qp2 cos[2] 2 qp3 cos[3] 3 qp5 cos[4] 4 qp5 cos[5] 5 qp6 cos[6] 6 qp7 cos[7] 7	нет
Включает ли интерфейс DSos на основе DSCP.	disable	нет
Включает ли интерфейс QOS на основе COS.	enable	нет
Приоритет пользователя интерфейса (значение COS)	0	да

7.2.2 Режим планирования конфигурации

Планирование коммутаторов по умолчанию — WRR. Конфигурацию SP и WFQ можно настроить с помощью команды.

Команда	Описание	Режим CLI
qos sched { sp | wrr | wfq}	Настройка планирования QoS	Режим конфигурирования интерфейса

7.2.3 Настройка веса очереди

Команда	Описание	Режим CLI
qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight <1-127>	Настройте вес каждой приоритетной очереди	Режим конфигурирования интерфейса
no qos qosprofile (qp0| qp1| qp2| qp3| qp4| qp5| qp6| qp7) weight	Вес очереди восстановления настроен как конфигурация по умолчанию	Режим конфигурирования интерфейса

Вес очереди — это количество пакетов, пересылаемых приоритетной очередью при опросе и пересылке. Поэтому при настройке веса очереди следует учитывать, что вес очереди с низким приоритетом не превышает вес очереди с высоким приоритетом.

7.2.4 Настройка сопоставления отношений между DSCP и QosProfile.

Команда	Описание	Режим CLI
qos dsc-map-qp <0-63> qosprofile {qp0|qp1|qp2|qp3|qp4|qp5|qp6|qp7 }	Сопоставление отношений между DSCP и qosprofile.	Режим глобального конфигурирования
no qos dscp-map-qp <0-63>	Восстановление сопоставления между DSCP и qosprofile, является конфигурацией по умолчанию.	Режим глобального конфигурирования

7.2.5 Настройка QoS порта

Этапы настройки политики QoS: определение класса, определение действия политики, стратегия применения.

Определите класс и определите набор правил классификации потока:

В общей сложности приоритет 802.1p, DSCP, ACL три правила классификации потока:

- Класс может использовать только набор правил классификации потока.
- Группа правил классификации потока может использоваться несколькими классами.
- Конфигурация по умолчанию не соответствует ни одному правилу.

Команда	Описание	Режим CLI
qos class <1-256> name WORD	Наименование указанного класса	Режим глобального конфигурирования
qos class <1-256> match cos <0-7> (<0-7>…)	Определите соответствующее правило приоритета 802.1p, которое может настроить 8 правил одновременно.	Режим глобального конфигурирования
qos class <1-256> match dscp <0-63> (<0-63>…)	Определение соответствующих правил DSCP позволяет настроить 8 правил одновременно.	Режим глобального конфигурирования
qos class <1-256> match acl <1-99>|<100-199>…	Определите соответствующие правила ACL, одновременно можно настроить только 1 группу правил.	Режим глобального конфигурирования
no qos class <1-256>	Восстановить конфигурацию по умолчанию	Режим глобального конфигурирования
show qos class (<1-256>|)	Отображает информацию о настроенных классах	Привилегированный режим

Определите стратегию и определите набор действий QoS для соответствующих правил:

Существует шесть видов действий QoS, таких как сопоставление очереди вывода сообщений, перемаркировка DSCP, подсчет, копирование в ЦП, зеркалирование, ограничение скорости, при которых копирование в ЦП и зеркалирование не может быть настроено одновременно. Политика может подключаться несколько классов, и класс может быть связан несколькими политиками. Группа действий QoS может использоваться, когда политика связана с классом. В конфигурации по умолчанию политика не подключается ни к какому классу и не использует никаких действий QoS.

Команда	Описание	Режим CLI
qos policy <1-256> name WORD	Наименование указанной политики	Режим глобального конфигурирования
qos policy <1-256> class <1-256> remark dscp <0-63>	Сопоставление правил классификации, маркировка значения DSCP сообщения	Режим глобального конфигурирования
no qos policy <1-256> class <1-256> remark	Действие по удалению нового маркирующего сообщения	Режим глобального конфигурирования
qos policy <1-256> class <1-256> meter <1-1000000> <1-65535>	Соответствующие правила классификации ограничивают пропускную способность и пакетный трафик пакетов.	Режим глобального конфигурирования
no qos policy <1-256> class <1-256> meter	Удаление ограниченной полосы пропускания сообщений и пакетного трафика	Режим глобального конфигурирования
qos policy <1-256> class <1-256> statistic-packets	Сопоставьте правила классификации и подсчитайте количество сообщений	Режим глобального конфигурирования
no qos policy <1-256> class <1-256> statistic-packets	Действие по удалению количества статистических сообщений	Режим глобального конфигурирования
qos policy <1-256> class <1-256> mirror-to cpu	Сопоставление правил классификации, зеркалирование сообщений на ЦП	Режим глобального конфигурирования
qos policy <1-256> class <1-256> mirror-to monitor-interface	Соответствие правилам классификации, зеркалирование сообщений на зеркальный порт (эффективна конфигурация зеркального порта)	Режим глобального конфигурирования
no qos policy <1-256> class <1-256> mirror	Удалить действие зеркалирования сообщений	Режим глобального конфигурирования
no qos policy <1-256> (class <1-256>|)	Стратегия удаляет соответствующие соответствующие правила и действия	Режим глобального конфигурирования
qos policy <1-256> class <1-256> map-queue <0-7>	Сопоставьте правила классификации и назначьте сообщения соответствующей очереди вывода	Режим глобального конфигурирования
no qos policy <1-256> class <1-256> map-queue	Сопоставьте правила классификации и назначьте сообщения в очередь вывода по умолчанию 0	Режим глобального конфигурирования
clear interface IFNAME qos policy statistic-packets	Очистить статистическую информацию политики QoS интерфейса	Режим глобального конфигурирования
show qos policy (<1-256>|)	Показать информацию о настроенных политиках	Привилегированный режим
show qos	Отображение информации о настроенном QoS	Привилегированный режим

Применить политику и применить соответствующую стратегию к интерфейсу;
Интерфейс имеет только одну политику, и только одна политика может использоваться несколькими интерфейсами.

Порт может быть включен только для выбора и включения QoS. Функция QoS может быть настроена только на физическом порту и не может быть настроена в группе TRUNK или трехуровневом интерфейсе.

Команда	Описание	Режим CLI
qos {dscp-based| cos-based| dscp qos-based| apply-policy <1-256>}	Включите функцию QoS порта	Режим конфигурирования интерфейса
no qos	Восстановить порт по умолчанию	Режим конфигурирования интерфейса
show qos	Отображение информации о конфигурации для всех QoS	Привилегированный режим
show qos interface IFNAME	Конфигурация интерфейса отображения информации QoS	Привилегированный режим
show qos interface	Отображение информации QoS для всех конфигураций интерфейса	Привилегированный режим

7.2.6 Настройка приоритета пользователя порта (значение COS)

Команда	Описание	Режим CLI
qos user-priority <0-7>	Настройка приоритета пользователя (значение COS) порта	Режим конфигурирования интерфейса
no qos user-priority	Приоритет пользователя (значение COS) порта восстановления, является конфигурацией по умолчанию	Режим конфигурирования интерфейса

7.3 Пример базовой конфигурации QoS

Настройка приоритета пользователя ge1/3 (значение COS) равна 3, а функция QoS на основе COS по умолчанию загружается:

```
Switch#configure terminal
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos user-priority 3
Switch#(config-ge1/3)#end
```

Настройте интерфейс ge1/3 для запуска функции QoS на основе DSCP и сопоставьте значение DSCP 3 с приоритетной очередью 2:

```
Switch#configure terminal
Switch#(config)#qos dscp-map-qp 3 qosprofile qp2
Switch#(config)#interface ge1/3
Switch#(config-ge1/3)#qos dscp-based
Switch#(config-ge1/3)#end
```

7.4 Пример конфигурации политики QoS

Настройте ACL для захвата потоков данных источника MAC1, MAC2, MAC3 соответственно (правила ACL могут быть изменены в соответствии с требованиями, но это лишь несколько примеров):

```
access-list 700 permit host 0000.0000.1111 vid any ip any any
access-list 701 permit host 0000.0000.2222 vid any ip any any
access-list 702 permit host 0000.0000.3333 vid any ip any any
```

Настройте класс QOS для соответствия потокам данных исходного MAC1, MAC2 и MAC3 соответственно (вы можете изменить правило сопоставления cos или DSCP в соответствии с требованием, что является простым примером):

```
qos class 10 match acl 700
qos class 11 match acl 701
qos class 12 match acl 702
```

Настройте политику QOS, чтобы отметить приоритет 802.1p для потоков данных MAC1, MAC2 и MAC3 соответственно (вы можете изменить политики в соответствии с требованиями, но вот лишь несколько примеров):

```
qos policy 10 class 10 remark cos 7
qos policy 10 class 11 remark cos 5
qos policy 10 class 12 remark cos 3
```

Отправить политику QOS на интерфейс порта ge1/23:

```
qos apply-policy 10
```

Проверка информации о конфигурации, анализ результатов тестирования в порту G1/24:

```
Switch#show qos interface ge1/23
```

Восьмая глава

Конфигурация MSTP

В этой главе описывается MSTP и его конфигурация, включая следующее:

- Введение в MSTP
- Конфигурация MSTP
- Пример настройки MSTP

8.1 Введение в MSTP

Коммутатор поддерживает стандартный протокол STP IEEE802.1d, IEEE802.1w, IEEE802.1s.

8.1.1 Описание MSTP

MSTP использует RSTP для быстрой конвергенции, так что несколько VLAN могут быть объединены в экземпляр связующего дерева, и каждый экземпляр имеет топологию связующего дерева, независимую от других экземпляров. Эта архитектура предоставляет несколько путей пересылки для потоков данных, может балансировать нагрузку и уменьшать количество экземпляров связующего дерева, необходимых для поддержки большого количества VLAN.

8.1.2 Множественные домены связующего дерева

Для экземпляров, участвующих в вычислениях множественного связующего дерева (MST), одна и та же информация о конфигурации MST должна быть настроена согласованным образом. Набор подключенных коммутаторов, имеющих одинаковую конфигурацию MST, образует домен MST.

Конфигурация MST определяет домен, к которому принадлежит каждый коммутатор. Конфигурация включает имя домена, номер ревизии и сопоставление экземпляров MST и назначений VLAN; эта информация создает уникальную абстракцию (Digest) в конфигурации MST. Резюме в одном домене одинаковы, и они должны быть одинаковыми. Вы можете просмотреть информацию с помощью команды show spanning-tree MST config.

Один домен может иметь один или несколько участников с одинаковой конфигурацией MST; каждый участник должен иметь возможность обрабатывать RSTP BPDU. На количество доменов MST в сети ограничений нет, но каждый домен поддерживает не более 16 экземпляров. Одновременно можно назначить только одну VLAN одному экземпляру spanning tree.

8.1.3 IST, CIST и CST

Внутреннее связующее дерево (IST), связующее дерево, работающее в домене MST.

В каждом домене MST, MSTP поддерживает несколько экземпляров создания. Экземпляр 0 является специальным экземпляром домена под названием IST. Все остальные экземпляры MST имеют номера от 1 до 15.

Этот IST является просто экземпляром spanning tree для приема и отправки BPDU; вся остальная информация об экземпляре spanning tree сжимается в MSTI BPDU. Поскольку MSTI BPDU несет всю информацию об экземпляре, он должен обрабатываться коммутатором, который поддерживает несколько экземпляров связующего дерева, что означает упрощение количества BPDU. Все экземпляры MST в одном домене используют один и тот же таймер протокола, но каждый

экземпляр MST имеет свои собственные параметры топологии, такие как ID корневого коммутатора, стоимость корневого пути и т.д. По умолчанию все VLAN назначаются на IST.
Общее и внутреннее связующее дерево (CIST) - это совокупность всех связующих деревьев в каждом домене MST, а общее связующее дерево, соединяющее домен MST и единое связующее дерево (IST). Дерево разветвления, вычисленное в домене, выглядит как поддерево CST, которое содержит все домены коммутаторов. CIST формируется по результатам вычисления дерева разветвления между коммутаторами, которые поддерживают протоколы 802.1W и 802.1D. CIST в домене MST такой же, как и в домене CST.
Общее охватывающее дерево (CST), охватывающее охватывающее дерево между доменами MST.

8.1.4 Операции внутри домена

IST соединяет все коммутаторы MSTP в домене. Когда IST сходится, корень IST становится ведущим IST, что является минимальным идентификатором моста в домене и накладными расходами пути коммутатора до корня CST. Если в сети есть только один домен, мастер IST также является корнем CST.
Если корень CST находится вне пределов домена, в качестве ведущего IST выбирается коммутатор MSTP на границе домена (boundary).
Когда коммутатор MSTP инициализируется, он посылает BPDU себе в качестве корня CST и ведущего IST, а стоимость пути к корню CST и ведущему IST устанавливается равной 0. Коммутаторы также инициализируют все экземпляры MST и требуют, чтобы они были их корнями. Если коммутатор получает корневую информацию MST, чем текущий приоритет хранения информации порта (низкий ID моста, низкая стоимость и так далее, он отказывается от пути), то он становится ведущим по требованиям IST.
При инициализации домен может иметь много поддоменов, каждый из которых имеет свой собственный главный IST. Когда коммутатор получает более предпочтительную информацию IST, он покидает свой старый поддомен и добавляет в новый поддомен, который может содержать реальный главного IST. Поэтому все поддомены заключают контракты, за исключением реального главного поддомена IST.
Для правильной работы все коммутаторы в домене MST должны распознавать один и тот же главного IST. Таким образом, коммутаторы в любых двух доменах синхронизируют роли портов одного из своих экземпляров MST, только если они сходятся к общему главному IST.

8.1.5 Междоменная работа

При наличии в сети нескольких доменов или ранних коммутаторов 802.1D MSTP устанавливает и обслуживает CST, который содержит все домены MST в сети и все ранние STP-коммутаторы. Экземпляры MST присоединяются к IST в границах домена (границах), чтобы стать CST.
IST соединяет все коммутаторы в домене MSTP и выглядит как поддерево CST (окруженное всеми доменами коммутатора), а корень поддерева становится хозяином IST. Домен MST выглядит как виртуальный коммутатор, прилегающий к коммутатору STP и домену MST.
Только экземпляры CST отправляют и получают BPDU, а экземпляры MST увеличивают информацию о связующем дереве до BPDU для взаимодействия с соседними коммутаторами и вычисления последней топологии связующего дерева. Из-за этого параметры связующего дерева, участвующие в передаче BPDU (такие как время приветствия, время пересылки, максимальный возраст и максимальный прыжок), настраиваются только в экземплярах CST, но не во всех экземплярах MST. Параметры, используемые в топологии связующего дерева (например, приоритет

коммутатора, стоимость порта VLAN, приоритет VLAN порта), могут быть настроены в экземплярах CST и MST.
Коммутаторы MSTP используют связь между коммутаторами версии 3 RSTP BPDU или 802.1D BPDU и 802.1D. Коммутаторы MSTP взаимодействуют с помощью коммутаторов MSTP BPDU и MSTP.

8.1.6 Количество переходов

Экземпляры IST и MST не используют сведения о возрасте сообщения и максимальном возрасте в BPDU, которые настраивают топологию связующего дерева. Вместо этого используйте путь к корню и потратьте эквивалент механизма подсчета переходов IP TTL.
Можно настроить максимальное количество переходов для этого домена и применить его к этому домену.
IST и все экземпляры MST. Количество вычислений прыжков совпадает с результатом возраста сообщения (определяется после начала перенастройки). Корневой коммутатор экземпляра всегда отправляет BPDU (или-M-запись) со стоимостью 0 и количеством прыжков в качестве максимального. Когда коммутатор получает BPDU, он уменьшает оставшиеся прыжки и распространяет оставшиеся прыжки в BPDU, который он генерирует. Когда число достигает 0, коммутатор отбрасывает BPDU и возраст информации для этого порта.
В домене информация о возрасте сообщения и максимальном возрасте в разделе RSTP BPDU является согласованной, и одно и то же значение распространяется на указанный порт домена (границы).

8.1.7 Пограничный порт

Граница — это домен связующего дерева, который соединяет регион MST с одним RSTP, или доменом связующего дерева только 801.1D, или другим регионом MST. Пограничный порт также подключен к локальной сети, и назначенным коммутатором для этой локальной сети является либо один коммутатор связующего дерева, либо коммутатор с другой конфигурацией региона MST.
В пограничных портах роли порта MST не важны, и их состояния вынуждены быть такими же, как состояние порта IST (при перенаправлении IST портом, MST порт на границе так же перенаправляет). Порт IST на границе может играть любую роль, кроме порта резервного копирования.
В общем пограничном соединении MST-порт ожидает истечения времени прямой задержки в блокирующем состоянии, прежде чем он будет преобразован в состояние обучения. Порт MST ожидает истечения еще одного времени прямой задержки, прежде чем он будет преобразован в переадресацию.

Если пограничный порт является соединением точка-точка и является корневым портом IST, порт IST преобразуется в состояние переадресации, а порт MST преобразуется в состояние переадресации.
Если пограничный порт преобразуется в состояние пересылки в экземпляре, он перенаправляется во всех экземплярах и инициируется изменение топологии. Если пограничный порт с корнем IST или указанной ролью порта получает уведомление об изменении топологии, коммутатор MSTP инициирует изменение топологии активного порта экземпляра IST и всех экземпляров MST.

8.1.8 Совместимость MSTP 802.1d и STP

Коммутатор, работающий под управлением MSTP, поддерживает встроенный механизм миграции протокола, который позволяет ему координировать свои действия с 802.1D. Если коммутатор получает BPDU с конфигурацией 802.1D от порта, он отправляет BPDU 802.1D на этот порт. Когда пограничный порт домена получает 802.1D BPDU или другой MSTP BPDU или RSTP BPDU, коммутатор MSTP может быть обнаружить. Однако, если коммутатор больше не получает 802.1D BPDU, он не будет автоматически возвращаться в режим MSTP, поскольку он не может определить, была ли обменная другая сторона удалена из соединения, если другой коммутатор не является назначенным коммутатором. Аналогичным образом, когда коммутатор, подключенный к этому коммутатору, был добавлен в этот домен, коммутатор может продолжать назначать порту роль пограничного порта. Миграционная обработка протокола перезапуска (обязательное и соседское согласование коммутатора).

Если все коммутаторы на другой стороне являются коммутаторами RSTP, они могут обрабатывать MSTP BPDU и RSTP BPDU. Поэтому коммутатор MSTP отправляется на пограничный порт или для отправки конфигурации версии 0 и TCN BPDU или версии 3 MSTP BPDU. Пограничный порт, который подключается к локальной сети. Его назначенный коммутатор является либо отдельным коммутатором дерева, либо коммутатором с различными конфигурациями MST.

8.1.9 Роль порта

Быстрый алгоритм конвергенции для MSTP с использованием RSTP. В этом документе кратко описывается роль порта MSTP и быстрая конвергенция в сочетании с RSTP.

RSTP обеспечивает быструю конвергенцию указанных ролей портов и топологий действий принятия решений. RSTP, основанный на IEEE802.1D STP, выбирает высокоприоритетные коммутаторы в качестве корневых коммутаторов. Когда RSTP указывает роль для порта:

Корневой порт - При пересылке пакетов на корневой коммутатор коммутатор обеспечивает оптимальную стоимость пути.

Назначенный порт - Подключение указанного коммутатора. При пересылке пакетов из локальной сети на корневой коммутатор имеют самый короткий путь. Указывает, что порт, через который коммутатор подключается к локальной сети, называется указанным портом.

Альтернативный порт — обеспечивает путь замены корневого коммутатора текущего корневого рог.

Порт резервного копирования — резервное копирование пути, который воспроизводит указанный порт на листе связующего дерева. Порт резервного копирования существует только в том случае, если два порта соединены вместе в контуре точка-точка или когда коммутатор имеет два или более подключений к общему сегменту локальной сети.

Отключить порт — в операции связующего дерева роль порта отсутствует.

Главный порт — на кратчайшем пути корня домена или общего корня это порт, соединяющий домен с общим корнем.

Корневой порт или указанная роль порта включена в активную топологию. Роль заменяющего порта или порта резервного копирования не включена в активную топологию.

В стабильной топологии и фиксированной роли порта всей сети, RSTP гарантирует, что каждый корневой порт и назначенный порт немедленно перешли в состояние переадресации, когда все заменяющие порты и резервные порты всегда находятся в состоянии отбрасывания. Управление портовым государством экспедированием и обработкой обучения.

Быстрая конвергенция

RSTP обеспечивает быстрое восстановление в следующих случаях: отказ коммутатора, отказ порта или неисправность ЛВС. Это обеспечивает быстрое восстановление для граничащих портов, новых корневых портов и соединений точка-точка:

Пограничные порты - Если вы настроите порт, как пограничный порт, он немедленно переводится в состояние пересылки. Вы можете открыть его как пограничный порт, только если этот порт подключен к одному терминалу или для определения устройства, которому не нужно вычислять spanning tree.

Корневые порты - Если RSTP выбирает новый корневой порт. Он блокирует старый корневой порт и немедленно переводит новый корневой порт в состояние пересылки.

Соединения "точка-точка" - Если вы соединяете порт с другими портами через соединение "точка-точка" и локальный порт с назначенным портом и другими портами, он проходит через предложение-согласие, согласование, рукопожатие, быструю миграцию для определения быстрой конвергенции без петлевой топологии (loop-free).

Изменения топологии

В этом разделе описаны различия между RSTP и 802.1D в работе с топологическими изменениями в spanning-tree.

Обнаружение - Любой переход между состоянием блокировки и 802.1D в качестве состояния пересылки вызовет изменение топологии, только для того, чтобы мигрировать из состояния блокировки в состояние пересылки в RSTP (изменение топологии состояния только для увеличения связности рассматриваемого изменения топологии). Изменение состояния на одном краю порта (краевой порт) не приводит к изменению топологии. Когда коммутатор RSTP исследует модификацию топологии, он рассылает ее для изучения информации на все не граничные порты (nonedge ports), в дополнение к портам приема информации TC.

Уведомление - В отличие от 802.1D, использующего TCN BPDU, RSTP его не использует. Однако, для обеспечения 802.1D и совместимости, RSTP коммутатор и TCP BPDU обработка.

Подтверждение — когда коммутатор RSTP получает сообщение TCN от коммутатора 802.1D на указанном порту, он отвечает BPDU 802.1D и устанавливает бит флага TCA. Однако, если таймер TC-while (такой же, как и таймер изменения топологии 802.1D) активен, он подключается к коммутатору 802.1D на корневом порту и получает конфигурацию BPDU с TCA, TC-while timer restart (reset). Это поведение требуется только для поддержки коммутатора 802.1D. RSTP BPDU никогда не имеет бита флага TCA.

Распространение - Когда коммутатор RSTP получает сообщение TC от другого коммутатора через указанный порт или корневой порт, оно распространяется на все не граничащие порты, назначенные порты и корневые порты (кроме принимающего порта). Все эти порты запускают таймер TC-while и передают полученную информацию.

Миграция протокола - Для обеспечения обратной совместимости коммутаторов 802.1D, RSTP выборочно отправляет 802.1D конфигурационный BPDU и TCN BPDU на каждый порт. Когда один инициализирован и запускается таймер migrate-delay (указанное минимальное значение отправляется во время RSTP BPDU), отправляется RSTP BPDU. Когда этот таймер активен, коммутатор обрабатывает все BPDU, полученные от порта, и игнорирует тип протокола.

После остановки таймера задержки миграции порта, если коммутатор получает 802.1D BPDU, он предполагает, что подключен к 802.1D коммутатору и начинает использовать протокол 802.1D BPDU. Однако, если RSTP коммутатор использует 802.1D BPDU на порту, после получения таймера, принимается RSTP BPDU, который перезапускает таймер и начинает использовать RSTP BPDU.

8.1.10 Краткое введение в связующее дерево 802.1D

Протокол связующего дерева основан на следующих пунктах:

1) Существует уникальный групповой адрес (01-80-C2-00-00-00), который идентифицирует все коммутаторы в конкретной локальной сети. Эта группа адресов может быть идентифицирована всеми коммутаторами;
2) Каждый коммутатор имеет уникальный идентификатор (Brideg Identifier);
3) Порт каждого коммутатора имеет уникальный идентификатор порта (Port Identifier). Управление конфигурацией связующего дерева также требует: для настройки каждого коммутатора относительный приоритет; каждый порт каждого коммутатора имеет относительный приоритет каждого порта; может выбирать координирование пути.

Коммутатор с наивысшим приоритетом называется корневым (root) коммутатором. Каждый порт коммутатора имеет значение корневого пути, а значение корневого пути представляет собой сумму значения каждого сегмента коммутатора до корневого коммутатора. Минимальное значение корневого пути в коммутаторе называется корневым портом, и если имеется несколько портов с одинаковым значением корневого пути, корневым портом является порт с наивысшим приоритетом.

В каждой локальной сети есть коммутатор, называемый назначенным коммутатором, который принадлежит коммутатору с наименьшим значением в корневом пути локальной сети. Порт, соединяющий локальную сеть с указанным коммутатором, является назначенным портом локальной сети (назначенный порт). Если к этой локальной сети подключено более двух портов указанного коммутатора, в качестве указанного порта выбирается порт с наивысшим приоритетом.

Существенные факторы, определяющие формирование остовного дерева:

1) Решения корневого коммутатора
   a. Сначала все коммутаторы считают себя корневым коммутатором;
   b. Коммутатор отправляет конфигурационный BPDU в широковещательную рассылку подключенной локальной сети, чей root_id совпадает с bridge_id;
   c. Когда коммутатор получает другой BPDU конфигурации коммутатора, если обнаруживается, что полученное значение поля root_id в конфигурационном BPDU больше чем значение в параметре root_id коммутатора, кадр отбрасывается или root_id обновляется, коммутатор получает root параметры пути, такие как значение root_path_cost, коммутатор продолжит широковещательную передачу с новым значением конфигурации BPDU.

2) Решение корневого порта

Минимальное значение корневого пути в коммутаторе называется корневым портом.

Если несколько портов имеют одинаковое минимальное значение корневого пути, порт с наивысшим приоритетом является корневым портом. Если два или более порта имеют одинаковое минимальное значение корневого пути и наивысший приоритет, порт с наименьшим номером порта является корневым портом по умолчанию.

3) Коммутатор назначенный для локальной сети
   a. Поначалу все коммутаторы считают себя назначенными коммутаторами ЛВС.
   b. Когда коммутатор получает BPDU, отправленный другими коммутаторами в той же локальной сети (той же) с более низким корневым путем, коммутатор больше не утверждает, что он является назначенным коммутатором. Если в локальной сети имеется два или более коммутаторов с одинаковым значением корневого пути, в качестве назначенных коммутаторов выбираются коммутаторы с наивысшим приоритетом.

c. Если вы указываете коммутатор и в это же время выбран другой коммутатор в локальной сети, отправляете в указанную конфигурацию коммутатора BPDU, указанный коммутатор отправит ответ конфигурации BPDU, чтобы повторно определить назначенный коммутатор.

4) Определение указанного порта

Указанный порт в указанном коммутаторе LAN подключен к порту LAN. Если указанный коммутатор имеет два или более портов, подключенных к локальной сети, то указанным портом является порт с наименьшим идентификатором порта.

Помимо корневого порта и указанного порта, блокируются и другие порты. Таким образом, топология spanning tree определяется после принятия решения о корневом коммутаторе, назначенном коммутаторе и назначенном порте каждой локальной сети.

8.2 Конфигурация MSTP

8.2.1 Конфигурация по умолчанию

Параметр команды	Значение по умолчанию
spanning-tree mst enable(Запуск MSTP)	Закрыто
Spanning-tree mst priority(CIST приоритет коммутатора)	32768
spanning-tree mst hello-time(CIST время приветствия коммутатора)	2
spanning-tree mst forward-time(CIST время пересылки коммутатора)	15
spanning-tree mst max-age(CIST максимальный возраст коммутатора)	20
spanning-tree mst max-hops(CIST максимальное количество прыжков коммутатора)	20
instance 1 priority(Приоритет экземпляра)	32768
spanning-tree mst instance 1 priority(Приоритет экземпляра порта)	128
spanning-tree mst instance 1 path-cost(Путь-значение экземпляра порта)	20000000
spanning-tree mst priority(приоритет порта CIST)	128
spanning-tree mst path-cost(порт CIST путь-значение)	20000000

8.2.2 Общая конфигурация

Запуск MSTP

При запуске системы конфигурация MSTP по умолчанию закрыта.

Процесс настройки для запуска MSTP:

Switch#configure terminal
Switch(config)#spanning-tree mst enable
The command to close MSTP is:
Switch#configure terminal
Switch(config)#no spanning-tree mst

Конфигурация максимального возраста

Настройка максимального возраста — это настройка всех экземпляров. Максимальный возраст — это количество секунд, в течение которых коммутатор ожидает информацию о конфигурации связующего дерева, прежде чем инициировать реконфигурацию.

Конфигурация по умолчанию составляет 20 секунд, а диапазон конфигурации составляет от 6 до 40 секунд.

Процесс настройки:

Switch#configure terminal
Switch(config)#spanning-tree mst max-age <seconds>

Конфигурация максимального количества прыжков

Максимальное количество прыжков — это количество прыжков, указанное до того, как BPDU будет отброшен в домене.
Значение по умолчанию — 20, диапазон конфигурации — от 1 до 40.
Процесс настройки:

Switch#configure terminal
Switch(config)#spanning-tree mst max-hops <hop-count>

Конфигурация времени пересылки

Настройка времени пересылки предназначена для всех экземпляров.
Время пересылки — это количество секунд, в течение которых порты ожидают от отказа до обучения и от обучения до пересылки.
Конфигурация по умолчанию составляет 15 секунд, а диапазон конфигурации составляет от 4 до 30 секунд. В соответствии с временем пересылки протокола номера поколения должны выполняться следующие условия:

2*(время пересылки – 1) >= максимальный возраст.

Процесс настройки:

Switch#configure terminal
Switch(config)#spanning-tree mst forward-time <seconds>

Настройка времени приветствия

Настройка времени приветствия — это настройка всех экземпляров. Время приветствия — это интервал времени, в течение которого корневые коммутаторы создают информацию о конфигурации.
Время настройки по умолчанию составляет 2 секунды, а диапазон настройки составляет от 1 до 10 секунд. В соответствии с протоколом приветствия по номеру поколения должны выполняться следующие условия:

2*(время приветствия + 1) =< максимальный возраст.

Процесс настройки:

Switch#configure terminal
Switch(config)# spanning-tree mst hello-time <seconds>

Настройка приоритета моста CIST (приоритет)

Конфигурация по умолчанию 32768, диапазон конфигурации <0-61440>; значение приоритета CIST кратно 4096.
Процесс настройки:

Switch#configure terminal

Switch(config)#spanning-tree mst priority <priority>

Конфигурация совместимости сетевого коммутатора с CISCO использует протокол MSTP на основе 802.1s, длина каждого сообщения MSTI составляет 16 байт;
BPDU коммутатора CISCO, длина каждого сообщения MSTI составляет 26 байт. Для взаимодействия с коммутатором CISCO коммутаторы, настраиваемые сеть, должны запустить коммутатор, совместимый с CISCO.
В случае начальной конфигурации, совместимой с CISCO, при оценке того, является ли домен одним и тем же, рассматривается один и тот же домен, если имя домена и номер версии совпадают.
Система по умолчанию не запускает эту функцию.

Открытый и совместимый с CISCO:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability enable

Совместимость с CISCO:

Switch#configure terminal

Switch(config)#spanning-tree mst cisco-interoperability disable

Сброс задачи проверки протокола
Для совместимости с протоколом 802.1D STP система может автоматически определять протокол другой запущенной системы. Определите протокол для работающего порта в соответствии с протоколом, используемым другой стороной.
В некоторых случаях требуются протоколы сброса. Например, система согласовала порт для работы протокола STP, а через некоторое время на другой стороне устройства, работающего по протоколу STP, появился хост. Когда нужно настроить порт на быстрый порт, но на порту работает протокол STP, и задача согласования протокола остановлена; тогда необходимо сбросить задачу согласования протокола и позволить ему повторно согласовать протокол с хостом.
Сброс задачи разведки протокола всего устройства:

Switch#clear spanning-tree detected protocols

Задача разведки протокола - сброс порта:

Switch#clear spanning-tree detected protocols interface <if-name>

8.2.3 Конфигурация домена

При использовании двух или более устройств в одном домене, они должны иметь одинаковые сопоставления экземпляров VLAN, одинаковый номер модифицированной версии и одинаковое имя домена. Один домен имеет один или несколько участников с одинаковой конфигурацией MST, и каждый участник может работать с возможностью RSTP BPDUS. Нет ограничений на количество участников в сети, но каждый домен может поддерживать до 16 экземпляров.

Конфигурация экземпляра, в которой представлена только конфигурация имени домена и конфигурация номера версии ревизии.
Настройка доменных имен:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#region <region-name>

Номер ревизии конфигурации:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration Switch(config-mst)# revision <revision-num>

8.2.4 Конфигурация экземпляра

Система поддерживает 16 экземпляров, а диапазон идентификационного номера экземпляра составляет 0-15. VLAN может быть назначена только одному экземпляру spanning tree одновременно.
По умолчанию существует только один экземпляр 0, и все сети VLAN принадлежат этому экземпляру.
Процесс конфигурирования экземпляра:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> vlan <vlan-id>

Настройка приоритета моста MSTI (приоритет)

Конфигурация по умолчанию 32768, диапазон конфигурации <0-61440>; значение приоритета MSTI кратно 4096.
Процесс конфигурирования:

Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance <instance-id> priority <priority>

8.2.5 Конфигурация порта

Сведения о конфигурации порта, связанные с MSTP, описаны ниже. Здесь отдельно представлен только простой раздел конфигурации, port fast и root guard.
Процесс настройки порта для присоединения к экземпляру:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id>

Настройка приоритета порта CIST (приоритет)

Конфигурация по умолчанию — 128, диапазон конфигурации — <0-240>, а значение приоритета порта CIST кратно 16.
Процесс настройки:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst priority <priority>

Настройка приоритета порта MSTI (приоритет)

Конфигурация по умолчанию — 128, диапазон конфигурации — <0-240>, а значение приоритета порта MSTI кратно 16.
Процесс настройки:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> priority <priority>

Настройка значения пути порта CIST (path-cost)

Конфигурация по умолчанию — 20000000, а диапазон конфигурации — 1-200000000. Ниже приведена таблица сопоставления изменений пропускной способности и пути.

Пропускная способность (бит/с)	Значение пути
100,000(100K)	200000000
1,000,000(1M)	20000000
10,000,000(10M)	2000000
100,000,000(100M)	200000
1,000,000,000(1G)	20000
10,000,000,000(10G)	2000
100,000,000,000(100G)	200
1,000,000,000,000(1T)	20
>1000000000000	2

Процесс настройки:

Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst path <path-cost>

Настройка стоимости пути порта MSTI (path-cost)
Конфигурация по умолчанию - 20000000, а диапазон конфигурации - 1-200000000.

Пропускная способность и путь и вышеуказанная таблица затрат.
Процесс конфигурирования:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst instance <instance-id> path-cost <path-cost>
```

Настройка номера версии пакета протокола отправки

Конфигурация по умолчанию отправляет пакет протокола MSTP с диапазоном конфигурации 0-3 и отношениями отображения 0-stp, 2-rstp, 3-mstp.
Процесс конфигурирования:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)# spanning-tree mst force-version <version-id>
```

Настройка типа соединения

Если происходит подключение к другому порту в режиме точка-точка, и порт необходимо сделать локальным портом (назначенный порт, RSTP предложение-согласие через назначенный порт)произойдет согласование быстрой миграции своих подключенных портов стать корневым портом для определения петли свободной топологии.

Вот краткое введение в процесс согласования предложения-соглашения.
Когда коммутатор получает сообщение о предложении на одном из своих портов и порт выбран в качестве нового корневого порта, RSTP заставляет все остальные порты синхронизировать информацию о новом корневом порту.
Если все остальные порты синхронизированы с лучшей (превосходной) корневой информацией, полученной от корневого порта, коммутаторы синхронизируются.

Когда RSTP заставляет его синхронизировать новую корневую информацию, если указанный порт находится в состоянии пересылки и не настроен в качестве пограничного порта, он переходит в состояние блокировки. Как правило, когда RSTP заставляет порт синхронизировать новое корневое сообщение, а порт не удовлетворяет вышеуказанным условиям, состояние порта устанавливается на блокировку.
Когда все порты синхронизированы, коммутатор отправляет сообщение о согласии на соответствующий порт корневого порта. Когда коммутатор подключен к соединению точка-точка в их портовой роли соглашения, RSTP немедленно передает состояние порта на переадресацию.
При общем соединении порт 802.1D вычисляется для определения состояния порта.
Тип подключения порта по умолчанию — соединение точка-точка.

Тип подключения порта конфигурации — соединение точка-точка:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst link-type point-to-point
```

Тип подключения порта конфигурации — общее подключение:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config-ge1/2)#spanning-tree mst link-type shared
```

8.2.6 Конфигурация, связанная с PORTFAST

1) **Быстрый порт**

Быстрый порт немедленно переводит порт доступа или магистральный порт из состояния блокировки в состояние пересылки, минуя состояния прослушивания и обучения. Вы можете подключиться к отдельной рабочей станции и серверу с помощью Быстрого порта, что позволяет этим устройствам подключаться к сети немедленно, не дожидаясь сходимости связующего дерева.
Настройка быстрого порта:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast
```

2) **Фильтрация BPDU**

Фильтрация BPDU может быть открыта глобально на основе коммутаторов или на основе каждого порта, но их характеристики различаются.
На глобальном уровне вы можете использовать команду spanning-tree MST portfast bpdu-filter, чтобы запустить функцию фильтрации BPDU на порту в состоянии portfast bpdu-filter по умолчанию.
На уровне порта вы можете открыть фильтр BPDU на любом порту с включенным портом MST связующего дерева и быстрым фильтром bpdu.
Эта функция предотвращает получение или отправку BPDU на портах Быстрого порта.

Настройка фильтрации BPDU

В режиме глобального конфигурирования:

```
Switch#configure terminal
Switch(config)# spanning-tree mst portfast bpdu-filter
```

В режиме конфигурирования интерфейса:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast bpdu-filter enable
```

3) **Защита BPDU**

Функции защиты BPDU можно открыть глобально или для каждого порта, но их характеристики различаются.
На глобальном уровне вы можете использовать spanning-tree MST portfast bpdu-guard, чтобы открыть функцию защиты BPDU на порту в состоянии по умолчанию portfast bpdu-guard.
На уровне порта вы можете открыть защиту BPDU на любом порту.
Когда порт, настроенный с помощью BPDU, получает BPDU, связующее дерево отключает порт. В эффективной конфигурации порт с включенным портом Fast не получает BPDU. BPDU работающий на порту с поддержкой Port Fast для представления недопустимой конфигурации переходит в состояние отключения из-за ошибки, например, подключения к неавторизованному устройству.

Error-disabled будет, когда порт запуска BPDU получает BPDU, если в системе настроен механизм отключения при ошибках. Он запускает таймер отключения при ошибках. Error-disable перезапускает порт по истечении тайм-аута конфигурации системы.

В режиме глобального конфигурирования:

```
Switch#configure terminal
Switch(config)# spanning-tree mst portfast bpdu-guard
```

В режиме конфигурирования интерфейса:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst portfast bpdu-guard enable
```

Конфигурация отключения при ошибках, запуск механизма отключения при ошибках:

```
Switch#configure terminal
Switch(config)#spanning-tree mst errdisable-timeout enable
```

Настройка тайм-аута для отключения при ошибках

```
Switch#configure terminal
Switch(config)#spanning-tree mst errdisable-timeout interval <seconds>
```

8.2.7 Конфигурация Root Guard

Двухуровневая сеть SP может содержать множество коммутаторов, не связанных друг с другом. В такой топологии связующее дерево может переконфигурировать и выбрать клиентский коммутатор в качестве корневого коммутатора. Этого можно избежать, настроив root guard в коммутаторе SP на порт коммутатора в клиентской сети. Если вычисление связующего дерева приводит к тому, что порт в клиентской сети выбирается в качестве корневого порта, корневая защита настроит порт в несовместимом с корнем (заблокированном) состоянии, чтобы предотвратить превращение клиентского коммутатора в корневой коммутатор или в корневой путь. Если коммутатор за пределами сети SP становится корневым коммутатором, порт блокируется (несовместимый с корнем STAT), и связующее дерево выбирает новый корневой коммутатор. Коммутатор клиента не становится корневым коммутатором и пути к корню нет.

Если коммутатор работает в режиме MST, обязательным портом root Guard становится указанный порт, если это граничный порт, поскольку корневая защита находится в заблокированном состоянии в экземпляре IST, этот порт заблокирован во всех экземплярах MST. Граничный порт — это порт, подключенный к локальной сети, который указывает, что коммутатор является либо коммутатором 802.1D, либо коммутатором, настроенным в разных доменах MST.

Когда порт открыт, Root Guard применяется ко всем VLAN, которым принадлежит этот порт.

VLAN можно объединить и сопоставить с экземпляром MST.

Процесс настройки:

```
Switch#configure terminal
Switch(config)#interface <if-name>
Switch(config)#spanning-tree mst guard root
```

8.3 Пример конфигурации MSTP

(1) Конфигурация

Три коммутатора соединены в круг, и протокол связующего дерева каждого коммутатора необходим, чтобы избежать образования петли. Выполните настройку каждого коммутатора отдельно.

Конфигурация коммутатора 1:

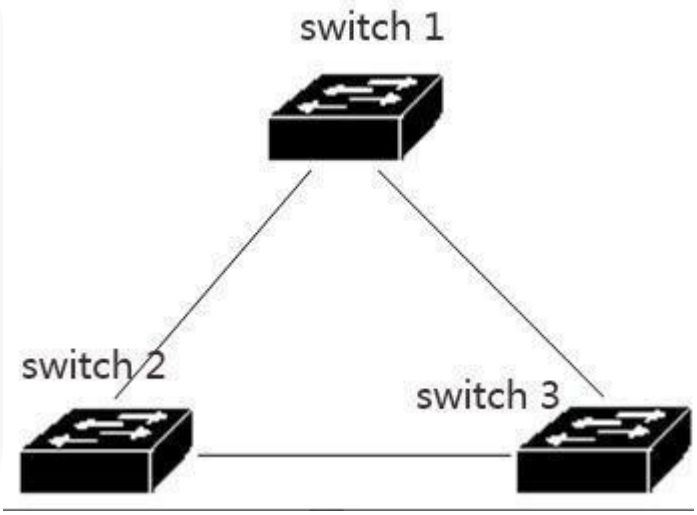
```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```

Конфигурация коммутатора 2:

```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```

Конфигурация коммутатора 3:

```
Switch>en
Switch#configure terminal
Switch(config)#spanning mst enable
```



(2) Поиск и устранение неисправностей:

Посмотреть, какой коммутатор выбран в качестве корневого моста:

Show spanning-tree MST выполняется, и значение CIST Root наблюдается как наименьший из трех MAC-адресов в обмене, то есть корневой результат правильный.

```
Switch#show spanning-tree mst
```

Просмотр состояния портов коммутаторов в связующем дереве:

Выполните инструкцию show spanning-tree MST interface ge1/1 и наблюдайте за значением состояния PORT ge1/1 в экземпляре 0.

```
Switch#show spanning-tree mst interface ge1/1
```

Девятая глава

Конфигурация EAPS

В этой главе описывается EAPS и его конфигурация, включая следующее:

- Краткое введение EAPS
- Основные понятия EAPS
- Введение протокола EAPS
- Конфигурация EAPS
- Ограничительные условия
- Краткое введение в команду EAPS
- Пример конфигурации с одним контуром
- Пример конфигурации переадресации данных по перекрестному кольцу

9.1 Краткое введение EAPS

EAPS - это аббревиатура Ethernet Automatic Protecting Switching. EAPS использует стандартные технологии Ethernet и VLAN для обеспечения топологии петли и механизма восстановления петли. Когда в контуре возникает ошибка, EAPS может восстановить передачу данных в течение секунды. Работа EAPS не ограничена количеством узлов, а время восстановления цикла не ограничено количеством узлов. EAPS не зависит от других устройств, то есть кольца EAPS могут иметь устройства, не поддерживающие протокол EAPS.

9.2 Основные понятия EAPS

Вот некоторые из основных концепций, используемых в EAPS:

1. Домен EAPS, в сети домен EAPS работает в одном цикле. Это ряд узловых устройств, состоящих из одного контура, а домен EAPS содержит один главный узел и один или несколько транзитных узлов.
2. Главный узел, коммутатор EAPS или узловое устройство EAPS имеют домен EAPS только с одним главным узлом.
3. Транзитный узел, коммутатор, на котором работает EAPS, или узловое устройство EAPS в домене EAPS, другие узлы, кроме главного узла.
4. Первичный порт, порт для подключения узловых устройств EAPS в домене EAPS. Узловое устройство имеет только один основной порт, подключенный к этому циклу в домене EAPS.
5. Вторичный порт, порт для подключения узловых устройств EAPS в домене EAPS. Узловое устройство имеет только один вторичный порт, подключенный к этому циклу в домене EAPS.
6. Управление VLAN, управление VLAN, ответственный за передачу пакетов протокола домена EAPS в VLAN, домен EAPS имеет только одну VLAN управления.
7. Защищенная VLAN, защищенная VLAN, передача VLAN бизнес-данных в домене EAPS, домен EAPS должен иметь защищенную VLAN или более одной защищенной VLAN.

9.3 Введение в протокол EAPS

Домен EAPS работает на кольце EAPS. Домен EAPS содержит главный узел с одним или несколькими транзитными узлами EAPS; каждый узел содержит один и тот же Control VLAN и несколько Protected VLAN; каждый узел EAPS содержит первичный порт и вторичный порт в домене EAPS, два порта

принадлежат этому кольцу Control VLAN и Protected VLAN. Благодаря соединениям Первичного и Вторичного портов каждого узлового устройства EAPS все узлы в домене EAPS составляют кольцо EAPS.

При нормальных обстоятельствах, когда домен EAPS и вторичный порт все первичные порты соединяются, вторичный порт главного узла (блокировка состояния порта вторичного порта блокируется), отмена бизнес-данных EAPS в домене. При сбое домена EAPS Вторичный порт главного узла немедленно открывается (состояние Вторичного порта — Пересылка), что позволяет ему пересылать бизнес-данные и возобновлять обычную пересылку служебных данных.

Транзитный узел не имеет никакого значения для обработки Первичного и Вторичного портов.

Две проверки неисправности и восстановление контура EAPS описаны ниже:

9.3.1 Аварийный сигнал об отсутствии связи

Когда транзитный узел обнаруживает, что его основной порт или порт вторичного порта отображается как LINK DOWN, он немедленно отправит пакет протокола LINK-DOWN на главный узел через другой порт LINK UP из Control VLAN.

Когда главный узел получает этот пакет протокола LINK-DOWN:

Master Node Complete Не удалось немедленно войти в состояние, открыть вторичный порт (переадресация состояния вторичного порта), обновить две или три собственные переадресации, отправить уведомление в домен EAPS RING-DOWN-FLUSH-FDB, другой транзит для обновления свою таблицу пересылки, повторно изучая двух- или трехуровневую пересылку.

Когда мастер-узел обнаруживает, что локальный первичный порт находится в состоянии LINK DOWN, его действие такое же, как и у пакета протокола LINK-DOWN.

Когда вторичный порт главного узла обнаружил, что локальный LINK DOWN, Master Node Complete Failed немедленно по состоянию, чтобы войти в состояние, обновить две или три собственные переадресации, отправив пакеты RING-DOWN-FLUSH-FDB, домен EAPS уведомляет другой транзит к обновить свою таблицу переадресации, повторно изучив двух- или трехуровневую пересылку.

9.3.2 Проверка контура

Главный узел периодически отправляет пакеты протокола HEALTH с основного порта. Если петля завершена, главный узел может получить пакет протокола HEALTH на свой собственный вторичный порт, когда главный узел перезапустит свой таймер периода сбоев, а состояние главного узла будет завершено.

Если сбой не получен до истечения срока действия их пакетов HEALTH, главный узел оставит состояние Complete в состоянии Failed Port (переадресация состояния вторичного открытого вторичного порта), обновит две или три собственные переадресации, отправит RING-DOWN-FLUSH - FDB. Домен EAPS уведомляет другой транзит, чтобы он обновил свою таблицу переадресации, чтобы изучить двух- или трехуровневую пересылку.

9.3.3 Восстановление кольца

Мастер-узел отправляет пакеты HEALTH со своего основного порта, независимо от того, завершилось ли кольцо, не удалось или нет. Когда главный узел находится в состоянии Failed, как только пакет протокола HEALTH получен от его вторичного порта, петля вернется в состояние Complete. Затем мастер-узел установит состояние вторичного порта в состояние блокировки, обновит две или три собственные переадресации и отправит пакет RING-UP-FLUSH-FDB, уведомит другое оборудование об обновлении двух или трех собственных переадресаций, чтобы изучить двух- или трехуровневую переадресацию.

В узле транзитного порта от LINK DOWN до LINK UP и Master Node обнаруживается, что вторичный порт главного узла все еще может находиться в состоянии переадресации во время восстановления цикла, и в этом случае будет создано временное кольцо. Поэтому в транзитном порту в узле находится LINK UP, другой порт LINK DOWN стал LINK UP, транзитным узлом для входа в «Переадресацию» (PRE-FORWARDING), в этом состоянии за портом LINK UP будет находиться в состоянии Pre-forwarding, не передавать бизнес-данные, прерывать возможный цикл данных. Дождитесь восстановления главного узла и отправки RING-UP-FLUSH-FDB, транзитный узел получил пакет после перехода состояния узла в состояние LINK-UP, состояние предварительной пересылки порта установлено в состояние пересылки, восстановите нормальную передачу бизнес-данных.
Если транзитный узел не получает пакет протокола RING-UP-FLUSH-FDB, он будет установлен в состояние пересылки портом состояния предварительной пересылки после удвоения времени сбоя.

9.3.4 Экстремальная совместимость с EAPS

Продукт компании Extreme первым поддерживает производителей EAPS, серия устройств с поддержкой протокола EAPS должна соответствовать стандарту RFC3619; и протокол EAPS и RFC3619 Extreme протокол аппаратного обеспечения определение имеют некоторые различия. Протокол EAPS, поддерживаемый устройством сети, может быть полностью совместим с устройством Extreme, а совместимый коммутатор открыт по умолчанию.

9.3.5 Мульти EAPS домен

Устройства серии могут поддерживать несколько доменов EAPS, который поддерживает 16.

9.4 Конфигурация EAPS

Базовая конфигурация протокола EAPS включает в себя следующие основные элементы: Управление VLAN, режим узла, основной порт, вторичный порт, защищенная VLAN, время приветствия и время сбоя. Время приветствия и время сбоя имеют конфигурацию по умолчанию, время приветствия - 1 секунду, время сбоя - 3 секунды.

9.5 Ограничительные условия

1. Первичный порт должен принадлежать VLAN управления доменом EAPS и всем участникам Protected VLAN TRUNK.
2. Протокол EAPS не может работать одновременно с протоколом MSTP. Протокол EAPS не может быть запущен, если MSTP запущен или настроен экземпляр MSTP.
3. VLAN запускает протокол VLLP и не может быть настроена как VLAN Control VLAN или Protected EAPS.
4. EAPS VLAN Control может содержать только первичный порт и вторичный порт и может быть только в режиме TRUNK VLAN.
5. Если VLAN настроен в качестве домена управления VLAN EAPS, и этот домен был запущен, то VLAN нельзя удалить, а ее элементы порта нельзя изменить или удалить. Control VLAN не может настроить трехуровневый интерфейс.
6. В Protected VLAN первичный и вторичный порты могут быть только в режимах TRUNK. Другие порты-участники не ограничены.
7. Порт можно настроить только как основной порт домена EAPS или как дополнительный порт.
8. Одна и та же VLAN может принадлежать только VLAN управления доменом EAPS или Protected VLAN.
9. Управляющая VLAN всех узлов в домене EAPS должна быть одинаковой.

9.6 Краткое введение в команду EAPS

Чтобы создать домен EAPS, прежде всего, убедитесь, что конфигурация VLAN и порта соответствует вышеуказанным условиям.
Конфигурация EAPS имеет определенные требования к порядку, сначала создать домен EAPS, перед запуском домена EAPS, в соответствии с требованиями предыдущей конфигурации других параметров; в противном случае запуск не удастся. Если вы хотите изменить время приветствия на значение текущего времени сбоя, вы должны сначала изменить время сбоя на большее число; в противном случае он не будет успешно настроен. Другие последовательности конфигурации не требуют специальных требований.
Control-vlan, mode, primary-port, secondary-port не могут быть изменены при запуске Домена EAPS; защищенные vlan, отказоустойчивость, hello-time и экстремальная совместимость могут быть изменены.
Основной и вторичный порты поддерживают порты LACP (то есть группы TRUNK).

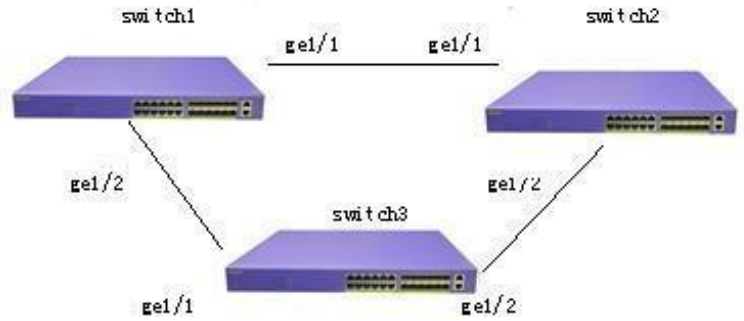
9.6.1 Команды настройки EAPS

Команда	Описание	Режим CLI
eaps create <ring-id>	Создание домена EAPS	Режим глобального конфигурирования
eaps control-vlan <ring-id> <vlan-id>	Настройка виртуальной локальной сети управления доменом EAPS.	Режим глобального конфигурирования
eaps protected-vlan <ring-id> <vlan-id>	Добавить защищенную виртуальную локальную сеть для домена EAPS.	Режим глобального конфигурирования
eaps mode <ring-id> <master|transit>	Настроить режим узла запуска домена EAPS.	Режим глобального конфигурирования
eaps primary-port <ring-id> <ifname>	Настроить основной порт домена EAPS.	Режим глобального конфигурирования
eaps secondary-port <ring-id> <ifname>	Настроить дополнительный порт домена EAPS.	Режим глобального конфигурирования
eaps data-span <ring-id>	Настроить пересылки ринговых данных EAPS	Режим глобального конфигурирования
eaps fail-time <ring-id> <secs>	Настроить время ожидания таймера периода сбоя домена EAPS. Значение по умолчанию 3 секунды. Единицы измерения — секунды.	Режим глобального конфигурирования
eaps hello-time <ring-id> <secs>	Настройка домена EAPS для отправки пакетов HEALTH через регулярные промежутки времени. Значение по умолчанию — 1 секунда. Единицы измерения — это секунды. Таймер-	Режим глобального конфигурирования

	приветствия должен быть меньше времени отказа.	
eaps extreme-interoperability <ring-id> <enable|disable>	Совместимость запуска или выключения с Extreme, по умолчанию - совместимость запуска.	Режим глобального конфигурирования
eaps enable <ring-id>	Запуск домена EAPS	Режим глобального конфигурирования
eaps disable <ring-id>	Закрыть домен EAPS	Режим глобального конфигурирования
show eaps	Информация о домене EAPS отображается в системе отображения	Обычный режим / Привилегированный режим
Show eaps <ring-id>	Отображает подробную информацию о домене EAPSDomain	Обычный режим / Привилегированный режим

9.7 Пример конфигурации с одним контуром

Есть три комплекта оборудования Коммутатор 1, Коммутатор 2, Коммутатор 3, через EAPS протокол VLAN 1 защита при пересылке трафика не образует петлю, при этом гарантируя, что Коммутатор 1, Коммутатор 2 имеют резервный канал через Коммутатор 3. В соответствии с вышеуказанными требованиями, вы можете настроить Коммутатор 1 в режим ведущего устройства; настройте коммутаторы Коммутатор 2 и Коммутатор 3 на транзитный режим. Добавьте сеть VLAN VLAN 2 для управления пакетами протокола.



Конфигурация коммутатора 1:

Коммутатор 1 настроен как ведущий EAPS Domain ring 1, управляющая VLAN - VLAN 2, защищенная VLAN - VLAN 1, основной порт - ge1/1, вторичный порт - ge1/2, другие конфигурации используют значения по умолчанию.

```
Switch#configure terminal

#Добавление VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
```

#Настроить ge1/1 как агрегированный участник VLAN 1 и VLAN 2.

```
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2
```

#Настроить ge1/2 как агрегированный участник VLAN 1 и VLAN 2.

```
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2
Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
```

```
VLAN  Name       State    Member ports ([u]-Untagged, [t]-Tagged)
----  --------   -------- ------------------------------------------------
1     vlan1      active   [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4
                          [u]ge1/5
                          [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                          [u]ge1/10
                          [u]ge1/11 [u]ge1/12
2     vlan2      active   [t]ge1/1 [t]ge1/2
```

```
Switch#configure terminal
#Создание доменного кольца EAPS 1
Switch(config)#eaps create 1
#Настройка VLAN 2 в управляющую VLAN
Switch(config)#eaps control-vlan 1 2
#Настройка VLAN 1 в качестве защищенной VLAN
Switch(config)#eaps protected-vlan 1 1
#Настроить коммутатор 1 в качестве главного узла
Switch(config)#eaps mode 1 master
#Настроить ge1/1 как основной порт
Switch(config)#eaps primary-port 1 ge1/1
#Настроить ge1/2 как вторичный порт
Switch(config)#eaps secondary-port 1 ge1/2
#Запуск доменного кольца EAPS 1
Switch(config)#eaps enable 1
```

Конфигурация коммутатора 2:

Коммутатор 2 настроен как транзит доменного кольца 1 EAPS, VLAN управления — VLAN 2, защищенная VLAN — VLAN 1, первичный порт — ge1/1, вторичный порт — ge1/2, в других конфигурациях используются значения по умолчанию.

```
Switch#configure terminal
#Добавить VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
#Настроить ge1/1 в качестве агрегированного участника VLAN 1 и VLAN 2.
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2
#Настроить ge1/2,  в качестве агрегированного участника VLAN 1 и VLAN 2.
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2
Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
```

```
VLAN       Name       State     Member ports ([u]-Untagged, [t]-Tagged)
----  --------  ---------  ------------------------------------------------
  1             vlan1      active  [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4 [u]ge1/5
                                   [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9 [u]ge1/10
  2             vlan2      active  [t]ge1/1 [t]ge1/2
```

```
Switch#configure terminal
#Создание доменного кольца EAPS 1
Switch(config)#eaps create 1
#Настроить VLAN 2 как VLAN управления
Switch(config)#eaps control-vlan 1 2
#Настройка VLAN 1 как защищенной VLAN
Switch(config)#eaps protected-vlan 1 1
#Настроить коммутатор 2 в качестве транзитного узла
Switch(config)#eaps mode 1 transit
#Настройте ge1/1 как основной порт
Switch(config)#eaps primary-port 1 ge1/1
#Настроить ge1/2 на вторичный порт
Switch(config)#eaps secondary-port 1 ge1/2
#Запуск доменного кольца EAPS 1
Switch(config)#eaps enable 1
```

Конфигурация коммутатора 3:

Коммутатор 3 настроен как транзитное кольцо 1 домена EAPS, VLAN управления — VLAN 2, защищенная VLAN — VLAN 1, первичный порт — ge1/1, вторичный порт — ge1/2, в других конфигурациях используются значения по умолчанию.

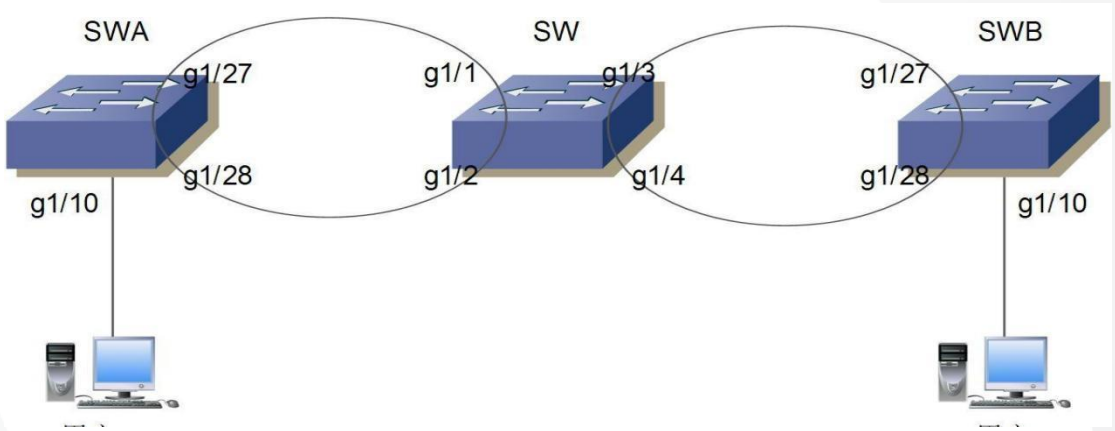
```
Switch#configure terminal

#Добавить VLAN 2
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit

#Настроить ge1/1 в качестве агрегированного участника VLAN 1 и VLAN 2.
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode trunk
Switch(config-ge1/1)#switchport trunk allowed vlan add 1,2

#Настроить ge1/2, в качестве агрегированного участника VLAN 1 и VLAN 2.
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#switchport mode trunk
Switch(config-ge1/2)#switchport trunk allowed vlan add 1,2
Switch(config-ge1/2)#exit
Switch(config)#exit
Switch#show vlan
```

```
VLAN  Name       State    Member ports ([u]-Untagged, [t]-Tagged)
----  --------   -------- ------------------------------------------------
1     vlan1      active   [t]ge1/1 [t]ge1/2 [u]ge1/3 [u]ge1/4
                          [u]ge1/5
                          [u]ge1/6 [u]ge1/7 [u]ge1/8 [u]ge1/9
                          [u]ge1/10
                          [u]ge1/11 [u]ge1/12
2     vlan2      active   [t]ge1/1 [t]ge1/2
```

```
Switch#configure terminal
#Создание доменного кольца EAPS 1
Switch(config)#eaps create 1
#Настроить VLAN 2 как VLAN управления
Switch(config)#eaps control-vlan 1
#Настройка VLAN 1 как защищенной VLAN
Switch(config)#eaps protected-vlan 1 1
#Настроить коммутатор 3 в качестве транзитного узла
Switch(config)#eaps mode 1 transit
#Настроить ge1/1 на основной порт
Switch(config)#eaps primary-port 1 ge1/1
#Настроить ge1/2 на вторичный порт
Switch(config)#eaps secondary-port 1 ge1/2
#Запуск доменного кольца EAPS 1
Switch(config)#eaps enable 1
```

9.8 Пример конфигурации пересылки данных через кольцо

Есть три устройства SWA, SW, SWB через кольцо протокола EAPS для обеспечения взаимодействия vlan1 vlan2. Топология следующая:



Контур 1 SWA контролирует vlan111, защищает vlan1, 2, настроен следующим образом:

```
vlan database
vlan 2 vlan 111
interface ge1/10
access vlan 2
interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 111
eaps create 1 eaps mode 1
```

Transit eaps primary-port 1 ge1/27 eaps secondary-port 1 ge1/28 eaps control-vlan 1 111 eaps protected-vlan 1 1 eaps protected-vlan 1 2 eaps enable 1

SW loop 1 и стыковка SWA, управление vlan111, защита vlan1, 2. Ring 2 и стыковка SWB, управление vlan222, защита vlan3333 (виртуальная VLAN, а интерфейс нужно добавить). Если вы хотите достичь кольцевой переадресации передачи данных по кольцу 1 и кольцу 2, вам необходимо настроить диапазон данных команды EAP. Конфигурация выглядит следующим образом:

```
vlan database
vlan 2 vlan 111
vlan 222 vlan 3333
interface ge1/1
switchport mode trunk
switchport trunk allowed vlan add 2
```

switchport trunk allowed vlan add 111
interface ge1/2
switchport mode trunk
switchport trunk allowed vlan add 2 trunk allowed vlan add 111
interface ge1/3
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333

###Добавить виртуальную VLAN 3333
interface ge1/4
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
switchport trunk allowed vlan add 3333

###Добавить виртуальную VLAN 3333
eaps create 1
eaps mode 1 Master
eaps primary-port 1 ge1/1
eaps secondary-port 1 ge1/2
eaps control-vlan 1 111
eaps protected-vlan 1 1
eaps protected-vlan 1 2
eaps data-span 1
eaps enable 1
eaps create 2
eaps mode 2 Transit
eaps primary-port 2 ge1/3
eaps secondary-port 2 ge1/4
eaps control-vlan 2 222
eaps protected-vlan 2 3333

###Здесь показана настройка виртуальной защиты VLAN
eaps data-span 2 eaps enable 2

SWB кольцо 2 и SW кольцо 2 встык, управление vlan222, защита vlan1, 2. Конфигурация следующая:
vlan database
vlan 2 vlan 222
interface ge1/10
access vlan 2
interface ge1/27
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222

interface ge1/28
switchport mode trunk
switchport trunk allowed vlan add 2
switchport trunk allowed vlan add 222
eaps create 2
eaps mode 2

Master eaps primary-port 2 ge1/27 eaps secondary-port 2 ge1/28 eaps control-vlan 2 222 eaps protected-vlan 2 1 eaps protected-vlan 2 2 eaps enable 2

После того, как эта конфигурация завершена, пользователь 1 и пользователь 2 взаимодействуют, данные vlan1 также совместимы. Режим узла Eaps можно изменить в соответствии с требованиями.

Десятая глава

Конфигурация ERPS

10.1 Обзор ERPS

ERPS (Ethernet Ring Protection Switching) — это протокол защиты кольцевой сети, разработанный ITU, также известный как G.8032. Это протокол канального уровня, специально используемый в кольцевой сети Ethernet. Это может предотвратить широковещательный шторм, вызванный петлей данных, когда петля Ethernet обнаружена, может быстро восстановить связь между узлами в кольце Ethernet при отключении канала. Протокол ERPS обеспечивает быстрый механизм защиты кольца Ethernet, который может быстро восстанавливать сетевую передачу при сбое кольцевой сети, тем самым обеспечивая высокую доступность и высокую надежность коммутатора в условиях кольцевой топологии сети.

10.2 Внедрение в технологию ERPS

10.2.1 Кольцо ERPS

Кольца ERPS основаны на минимизации колец, каждое кольцо должно быть наименьшим кольцом, разделенным на основное кольцо и вспомогательное кольцо: основное кольцо представляет собой замкнутое кольцо; кольцо является незамкнутым кольцом или замкнутым кольцом; и все они должны быть настроены командой.

Каждое кольцо ERPS (будь то основное кольцо или другое кольцо) имеет пять состояний:

(1) Состояние простоя: кольцо каждого физического канала в состоянии ожидания;
(2) Состояние защиты: состояние одной или нескольких физических каналов сети с разомкнутым контуром;
(3) Ручной режим коммутатора: изменение состояния кольца;
(4) Состояние принудительного режима коммутатора: состояние принудительного изменения кольца;
(5) Состояние ожидания: промежуточное состояние ожидания.

10.2.2 Узел ERPS

Двухуровневое коммутационное устройство, соединяющее кольцо ERPS, называется узлом. У каждого узла не может быть более двух портов для присоединения к одному и тому же кольцу ERPS, один порт является портом RPL, а другой — портом общего кольца.

Для общей ситуации роли узлов делятся на два типа следующим образом:

(1) Узел пересечения: в пересечении цикла ERPS узлы принадлежат нескольким кольцам, называемым узлом пересечения;
(2) Узлы без пересечения: пересечение кольца ERPS, узел принадлежит только кольцу ERPS и называется узлом без пересечения.

В протоколе ERPS существует три типа режимов узлов:

(1) Узлы-владельцы RPL: кольцо ERPS является только узлом-владельцем RPL, определяемым конфигурацией пользователя, для предотвращения зацикливания в кольце ERPS путем блокировки порта RPL, когда узел-владелец RPL получает сообщение об ошибке, что другой узел или отказ канала на кольце ERPS автоматически откроет порт RPL, порт, принимающий восстановление и отправляющий трафик, чтобы поток не был прерван;

(2) Соседний узел RPL: узел напрямую подключен к порту RPL узла-владельца RPL, при нормальных обстоятельствах порт RPL узла-владельца RPL и порт RPL соседнего узла RPL будут заблокированы, чтобы предотвратить возникновение петли. При сбое кольца ERPS порт RPL узла-владельца RPL и порт RPL соседнего узла RPL будут освобождены;

(3) Обычный кольцевой узел в кольце ERPS, узлы, за исключением узлов-владельцев RPL и соседних узлов RPL, являются обычным кольцевым узлом, порт RPL и порт обычного обычного кольцевого кольцевого узла. для мониторинга их прямого протокола ERPS, а также для изменения состояния канала связи, своевременно уведомляющего другие узлы;

10.2.3 Связь и канал

(1) RPL (Ring Protection Link): каждое кольцо ERPS имеет только один RPL, то есть RPL-порт узла-владельца RPL находится на связи. Когда кольцо Ethernet находится в состоянии ожидания, канал RPL находится в состоянии блокировки и не пересылает пакет данных, чтобы избежать образования петли;

(2) Подпетлевая связь: в перекрестном кольце, принадлежащем подкольцу, звено за петлей управления;

(3) Виртуальный канал RAPS (Ring Auto Protection Switch): в кольце пересечения узлы пересечения используются для передачи сообщения кольцевого протокола, но путь, не принадлежащий подкольцу, называется виртуальным каналом кольца RAPS.

10.2.4 ERPS VLAN

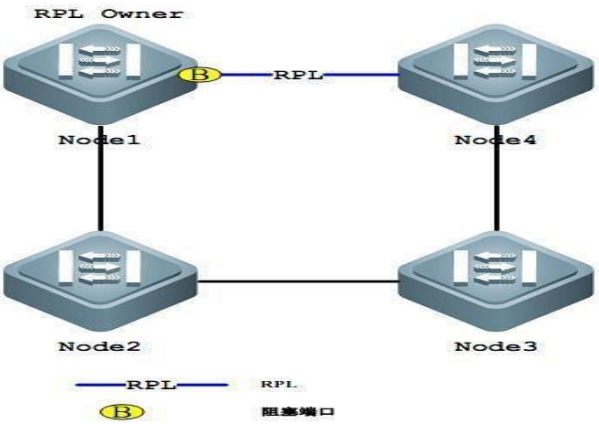
Существует два типа VLAN:

(1) RAPS VLAN в ERPS, которые используются для передачи пакетов протокола ERPS, порты, которые обращаются к кольцу ERPS на устройстве, принадлежат к RAPS VLAN и только порты, обращающиеся к кольцу ERP, могут присоединиться к VLAN. RAPS VLAN разных колец должен быть разным. Интерфейс RAPS VLAN не позволяет настраивать IP-адрес;

(2) VLAN данных: относительно RAPS VLAN, VLAN данных используется для передачи пакетов данных, VLAN данных может включать в себя кольцевой порт ERP, также может включать не-ERP-кольцевой порт.

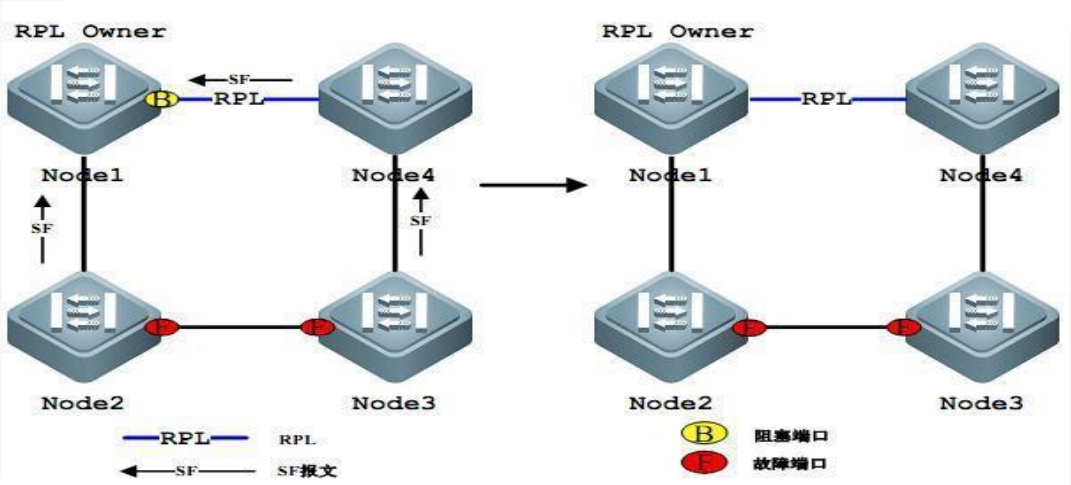
10.3 Принцип работы ERPS

10.3.1 Нормальное состояние



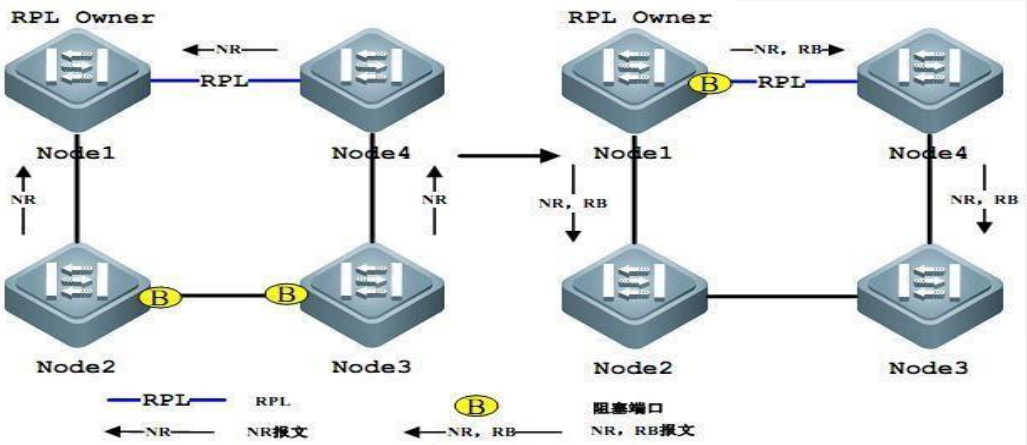
(1) Все узлы соединены в кольцо физической топологией;
(2) Протоколы защиты циклов гарантируют, что циклы не будут заблокированы блокировкой канала RPL. Как показано на рисунке выше, связь между Node1 и Node4 является связью RPL;
(3) Обнаружение неисправностей выполняется для каждого звена между соседними узлами.

10.3.2 Сбои связи



(1) Узлы, приводящие к неисправности и перегрузке канала связи, и использование сообщения RAPS (SF) для других узлов сообщают о неисправности на кольце, как показано выше, предполагая, что Node2, Node3 между Node2 и Node3 сбой связи, ожидая таймера удержания после тайм-аута, он заблокирует сбой связи, соответственно, кольцевые сетевые узлы отправили сообщение RAPS (SF);
(2) Триггер сообщения RAPS (SF) RPL имеет узел для открытия порта RPL. Сообщение RAPS (SF) также запускает все узлы для обновления соответствующих записей таблицы MAC, а затем узлы переходят в состояние защиты.

10.3.3 Восстановление связи



(1) Когда неисправность возобновляется, соседние узлы неисправности продолжают блокировать и отправлять сообщения RAPS (NR), указывающие на отсутствие локальной неисправности;

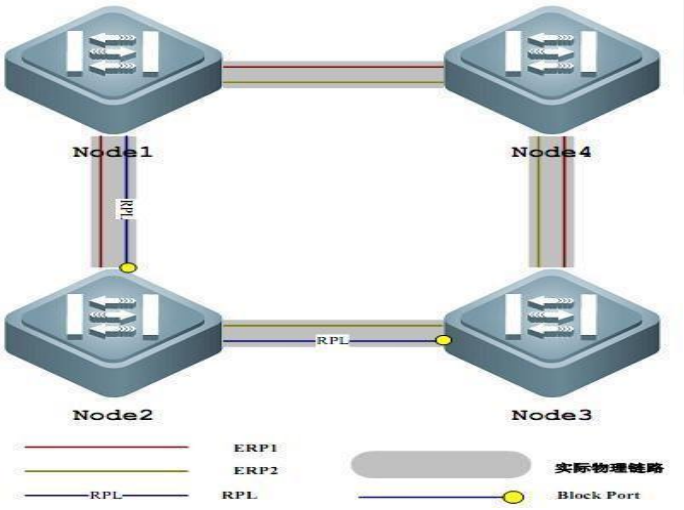
(2) После истечения срока действия таймера защиты узел владельца RPL запускает таймер WTR после получения первого сообщения RAPS (NR);

(3) Когда таймер WTR заканчивается, узел владелец RPL блокирует RPL и отправляет сообщения RAPS (NR, RB);

(4) Когда другие узлы получают это сообщение, они обновляют соответствующие записи таблицы MAC, и узел, отправляющий сообщение RAPS (NR) периодически прекращает отправку сообщений и открывает ранее заблокированные порты. Кольцевая сеть вернулась в исходное нормальное состояние.

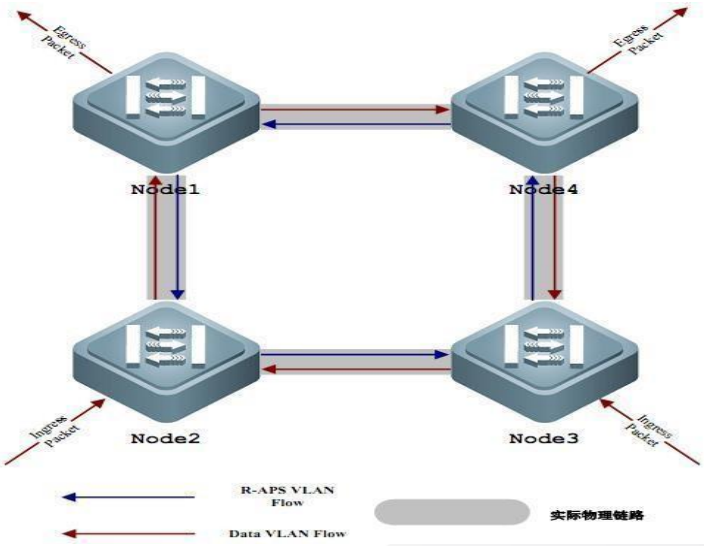
10.4 Технические характеристики ERPS

10.4.1 Балансировка нагрузки ERPS



Через Интернет в одной и той же конфигурации физического кольца несколько экземпляров кольца ERPS, кольца ERPS VLAN отправляют разный (называемый защитой VLAN) трафик, реализация топологического трафика данных с разными VLAN в кольцевой сети отличается, так что для достижения цели распределения нагрузки. Как показано на рисунке выше, физическая кольцевая сеть соответствует двум экземплярам двух колец ERPS, и два кольца ERPS по-разному защищают VLAN, Node2 является узлом владельца RPL ERP1, а Node3 является узлом владельца ERP2 RPL. При настройке различные VLAN могут использоваться для блокировки различных каналов, чтобы реализовать разделение нагрузки одного цикла.

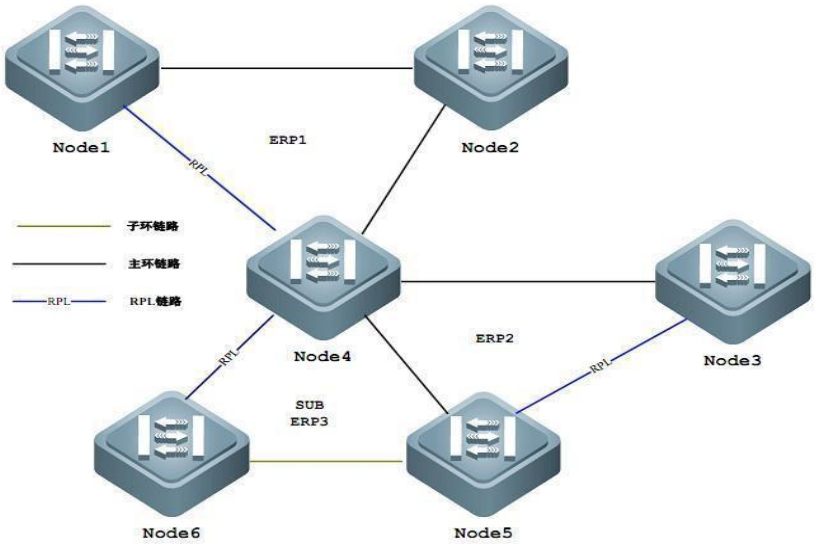
10.4.2 Хорошая безопасность



В VLAN существует два типа ERPS, один из которых - RAPS VLAN, а другой - VLAN данных. RAPS VLAN используется только для передачи пакетов протокола ERPS; ERPS также имеет дело только с

пакетами протоколов из RAPS VLAN, не обрабатывает никаких пакетов атак по протоколу из VLAN данных и повышает безопасность ERPS.

10.4.3 Поддерживается пересечение нескольких контуров



Как показано на рисунке выше, ERPS поддерживает добавление нескольких колец в одном узле (Node4) в качестве касательной или пересечения, что значительно повышает гибкость сети.

10.5 Команды протокола ERPS

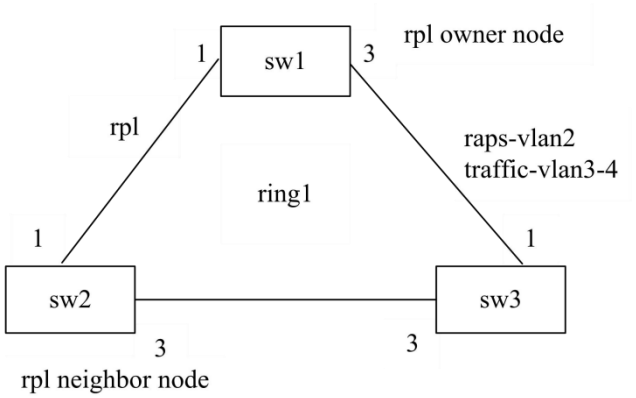
Команда	Описание	Режим CLI
erps <1-8>	Создание экземпляра ERPS	Режим глобального конфигурирования
no erps <1-8>	Удаление экземпляра ERPS	Режим глобального конфигурирования
node-role (interconnection | none-interconnection)	Роль узла конфигурации в цикле ERPS, узла межсоединения или узла без межсоединения	Режим ERPS
ring <1-32>	Создание кольца ERPS	Режим ERPS
no ring <1-32>	Удаление кольца ERPS	Режим ERPS
ring <1-32> ring-mode (major-ring | sub-ring)	Настройка шаблона кольца ERPS, основного кольца или дочернего кольца	Режим ERPS
ring <1-32> node-mode (rpl-owner-node | rpl-neighbor-node | ring-node)	Настройка шаблона кольцевого узла ERPS, узла владельца RPL, соседнего узла RPL или общего кольцевого узла	Режим ERPS
ring <1-32> raps-vlan <2-4094>	Настройка VLAN кольцевого протокола ERPS	Режим ERPS
no ring <1-32> raps-vlan	Удаление VLAN кольцевого протокола ERPS	Режим ERPS
ring <1-32> traffic-vlan <1-4094>	Настройка VLAN кольцевых данных ERPS	Режим ERPS
no ring <1-32> traffic-vlan <1-4094>	Удаление VLAN кольцевых данных ERPS	Режим ERPS

ring <1-32> (rpl-port|rl-port) IFNAME	Настройка кольцевого порта ERPS, порта RPL или общего кольцевого порта	Режим ERPS
no ring <1-32> (rpl-port|rl-port)	Удаление кольцевого порта ERPS	Режим ERPS
ring <1-32> revertive-behaviour (revertive|non-revertive)	Настройка циклов ERPS для восстановления поведения может быть восстанавливаемой или невосстанавливаемой	Режим ERPS
ring <1-32> hold-off-time <0-10000>	Настройка времени задержки кольца ERPS	Режим ERPS
no ring <1-32> hold-off-time	Установить время задержки кольца ERPS по умолчанию	Режим ERPS
ring <1-32> guard-time <10-2000>	Настройка времени кольцевой защиты ERPS	Режим ERPS
no ring <1-32> guard-time	Восстановить время по умолчанию кольцевой защиты ERPS	Режим ERPS
ring <1-32> wtr-time <1-12>	Настройка времени WTR кольца ERPS	Режим ERPS
no ring <1-32> wtr-time	Восстановить время WTR кольца ERPS по умолчанию	Режим ERPS
ring <1-32> wtb-time <1-10>	Настройка времени WTB кольца ERPS	Режим ERPS
no ring <1-32> wtb-time	Восстановить время WTB кольца ERPS по умолчанию	Режим ERPS
ring <1-32> raps-send-time <1-10>	Настройка времени доставки пакетов кольцевого протокола ERPS	Режим ERPS
no ring <1-32> raps-send-time	Восстановить время отправки сообщения кольцевого протокола ERPS по умолчанию	Режим ERPS
ring <1-32> (enable|disable)	Включить или выключить кольцо ERPS	Режим ERPS
ring <1-32> forced-switch IFNAME	Принудительное переключение кольцевого порта ERPS	Режим ERPS
ring <1-32> clear forced-switch	Принудительная передача чистого кольца ERPS	Режим ERPS
ring <1-32> manual-switch IFNAME	Вручную переключите кольцевой порт ERPS	Режим ERPS
ring <1-32> clear manual-switch	Ручное переключение на очистку кольца ERPS	Режим ERPS
ring <1-32> clear recovery	Ручное восстановление невосстанавливаемого поведения цикла ERPS или ручное восстановление до истечения срока действия WTR/WTB	Режим ERPS
show erps	Отображение всех экземпляров ERPS и циклов на устройстве	Привилегированный режим
show erps <1-8>	Отображение одного экземпляра ERPS устройства и сведений о цикле	Привилегированный режим

10.6 Типичное использование ERPS

10.6.1 Пример одиночного кольца

На следующей диаграмме узлы SW1, SW2 и SW3 составляют одно кольцо ERP ring1, 1, 3 портов каждого узла в качестве кольцевого порта ERPs, протокол VLAN — это данные 2, 3, 4 VLAN, узел SW1 является узлом-владельцем RPL, Узел SW2 к узлу RPL соседа, SW1 и SW2 между ссылкой RPL link



Настройка SW1:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и VLAN данных

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройка режима VLAN кольцевого порта в качестве агрегированного, добавление к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройка экземпляра ERP 1, одиночное кольцо ERP 1

```
Switch(config-erps-1)#ring 1
Switch(config)#erps 1
Switch(config-erps-1)#ring ring-mode major-ring node-mode rpl-owner-node raps-vlan 2 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка sw2:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и VLAN данных

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройка режима VLAN кольцевого порта в качестве агрегированного, добавление к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настроить экземпляр ERP 1, одиночное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring node-mode rpl-neighbor-node raps-vlan 2 traffic-vlan 3 traffic-vlan 4 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка SW3:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

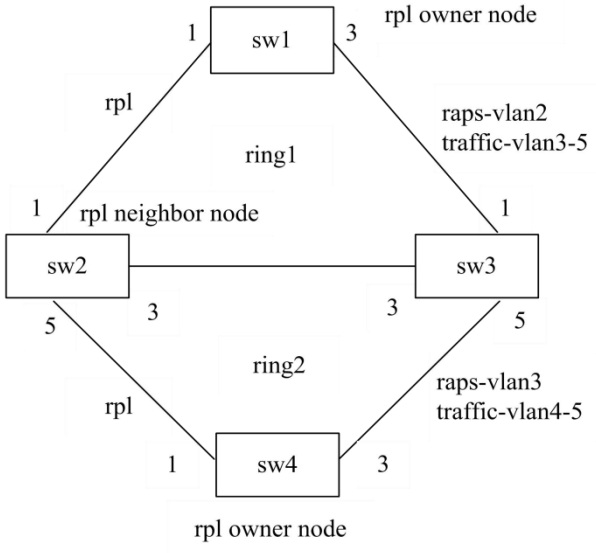
```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настроить экземпляр ERP 1, одиночное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring traffic-vlan 3 traffic-vlan 4 rpl-port xe1/1 rl-port xe1/3 enable
Switch(config-erps-1)#exit
```

10.6.2 Пример с несколькими кольцами

На следующей диаграмме узлы SW1, SW2 и SW3 составляют основное кольцо ERP ring1, SW1,
Узлы SW2 и SW3 1, 3 порт в качестве основного кольца порт Ring1, основное кольцо протокола Ring1 VLAN 2, 3, 4, VLAN 5, SW1 ring1 RPL узел владельца основного кольца, узел SW2 основной цикл Ring1 RPL соседнего узла, канал SW1 между SW2 и кольцевым каналом RPL на основе кольца1.
Узлы SW2, SW3 и SW4 составляют кольцо ERPs RING2, узлы SW2, SW3 и узлы SW4 5 порт 1, порт 3 в качестве подкольца порт RING2, протокол RING2 VLAN 3, данные 4 VLAN, 5,
Владелец SW4 RING2 RPL является узлом подкольца, связь SW2 между SW4 и подкольцом RING2 RPL.



Настройка SW1:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настроить экземпляр ERP 1, основное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка SW2:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
```

Настроить режим VLAN кольцевого порта в качестве агрегированного, добавить к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
```

```
Switch(config-xe1/5)#exit
```

Настроить экземпляр ERP 1, основное кольцо ERP 1, вспомогательное кольцо 2.

```
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

Настройка SW3:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-5
Switch(config-vlan)#exit
```

Настроить режим VLAN кольцевого порта в качестве агрегированного, добавить к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
Switch(config)# interface xe1/5
Switch(config-xe1/5)# switchport mode trunk
Switch(config-xe1/5)# switchport trunk allowed vlan add 3
Switch(config-xe1/5)# switchport trunk allowed vlan add 4
Switch(config-xe1/5)# switchport trunk allowed vlan add 5
Switch(config-xe1/5)# switchport trunk allowed vlan remove 1
Switch(config-xe1/5)#exit
```

Настройте экземпляр ERP 1, основное кольцо ERP 1, вспомогательное кольцо 2.

```
Switch(config)#erps 1
Switch(config-erps-1)# node-role interconnection
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 traffic-vlan 5
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode ring-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/5
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

Настройка SW4:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 3-5
Switch(config-vlan)#exit
```

Настройка режима VLAN кольцевого порта в качестве агрегированного, добавление к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

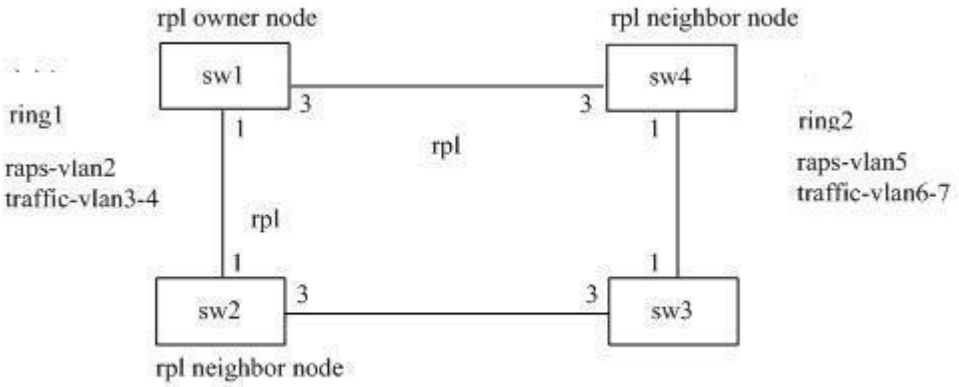
Настройка экземпляра ERP 1, подкольца ERP 2

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 2
Switch(config-erps-1)# ring 2 ring-mode sub-ring
Switch(config-erps-1)# ring 2 node-mode rpl-owner-node
Switch(config-erps-1)# ring 2 raps-vlan 3
Switch(config-erps-1)# ring 2 traffic-vlan 4
Switch(config-erps-1)# ring 2 traffic-vlan 5
Switch(config-erps-1)# ring 2 rpl-port xe1/1
Switch(config-erps-1)# ring 2 rl-port xe1/3
Switch(config-erps-1)# ring 2 enable
Switch(config-erps-1)#exit
```

10.6.3 Пример балансировки нагрузки с несколькими экземплярами

На следующей диаграмме узлы SW1, SW2, SW3 и SW4 составляют экземпляр ERP. 1 одноконтурный порт Ring1, 1, 3 каждого узла в качестве кольцевого порта ERP. Узел-владелец RPL, узел SW2 является соседним узлом RPL, каналом и SW1 SW2 для канала RPL.

Узлы SW1, SW2, SW3 и SW4 составляют экземпляр ERP 2 одноконтурных порта RING2, 1, 3 каждого узла в качестве кольцевого порта ERP, протокол VLAN — это данные VLAN 5, 6, 7, узел SW1 является узлом-владельцем RPL, Узел SW4 является соседним узлом RPL, канал между SW4 и SW1 для канала RPL.



Экземпляр конфигурации 1:

Настройка SW1:

Switch>enable
Switch#configure terminal

Создание протокола ERP и данных VLAN

Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit

Настройка режима VLAN кольцевого порта в качестве агрегированного, добавление к протоколу ERP и VLAN данных

Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit

Настройте экземпляр ERP 1, одиночное кольцо ERP 1

Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-owner-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3

```
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка SW2:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 1, одиночное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode rpl-neighbor-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка SW3:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 1, одиночное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Настройка SW4:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 2-4
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 2
Switch(config-xe1/1)# switchport trunk allowed vlan add 3
Switch(config-xe1/1)# switchport trunk allowed vlan add 4
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 2
Switch(config-xe1/3)# switchport trunk allowed vlan add 3
Switch(config-xe1/3)# switchport trunk allowed vlan add 4
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 1, одиночное кольцо ERP 1

```
Switch(config)#erps 1
Switch(config-erps-1)#ring 1
Switch(config-erps-1)# ring 1 ring-mode major-ring
Switch(config-erps-1)# ring 1 node-mode ring-node
Switch(config-erps-1)# ring 1 raps-vlan 2
Switch(config-erps-1)# ring 1 traffic-vlan 3
Switch(config-erps-1)# ring 1 traffic-vlan 4
Switch(config-erps-1)# ring 1 rpl-port xe1/1
Switch(config-erps-1)# ring 1 rl-port xe1/3
Switch(config-erps-1)# ring 1 enable
Switch(config-erps-1)#exit
```

Экземпляр конфигурации 2:

Настройка SW1:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
```

```
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 2, одиночное кольцо ERP 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-owner-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/3
Switch(config-erps-2)# ring 2 rl-port xe1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Настройка SW2:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
```

```
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 2, одиночное кольцо ERP 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/1
Switch(config-erps-2)# ring 2 rl-port xe1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Настройка SW3:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5
Switch(config-xe1/1)# switchport trunk allowed vlan add 6
Switch(config-xe1/1)# switchport trunk allowed vlan add 7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5
Switch(config-xe1/3)# switchport trunk allowed vlan add 6
Switch(config-xe1/3)# switchport trunk allowed vlan add 7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 2, одиночное кольцо ERP 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode ring-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
```

```
Switch(config-erps-2)# ring 2 rpl-port xe1/1
Switch(config-erps-2)# ring 2 rl-port xe1/3
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Настройка SW4:

```
Switch>enable
Switch#configure terminal
```

Создание протокола ERP и данных VLAN

```
Switch(config)#vlan database
Switch(config-vlan)#vlan 5-7
Switch(config-vlan)#exit
```

Настройте режим VLAN кольцевого порта в качестве агрегированного, добавьте к протоколу ERP и VLAN данных

```
Switch(config)# interface xe1/1
Switch(config-xe1/1)# switchport mode trunk
Switch(config-xe1/1)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/1)# switchport trunk allowed vlan remove 1
Switch(config-xe1/1)#exit
Switch(config)# interface xe1/3
Switch(config-xe1/3)# switchport mode trunk
Switch(config-xe1/3)# switchport trunk allowed vlan add 5-7
Switch(config-xe1/3)# switchport trunk allowed vlan remove 1
Switch(config-xe1/3)#exit
```

Настройте экземпляр ERP 2, одиночное кольцо ERP 2

```
Switch(config)#erps 2
Switch(config-erps-2)#ring 2
Switch(config-erps-2)# ring 2 ring-mode major-ring
Switch(config-erps-2)# ring 2 node-mode rpl-neighbor-node
Switch(config-erps-2)# ring 2 raps-vlan 5
Switch(config-erps-2)# ring 2 traffic-vlan 6
Switch(config-erps-2)# ring 2 traffic-vlan 7
Switch(config-erps-2)# ring 2 rpl-port xe1/3
Switch(config-erps-2)# ring 2 rl-port xe1/1
Switch(config-erps-2)# ring 2 enable
Switch(config-erps-2)#exit
```

Одиннадцатая глава
Конфигурация AAA

В этой главе описывается, как настроить коммутаторы 802.1x и RADIUS, чтобы предотвратить доступ к сети неавторизованных пользователей. Для использования клиента 802.1x и HyperBoss см. соответствующие руководства по эксплуатации. Основное содержание этой главы состоит в следующем:

- Введение в 802.1x
- Введение в RADIUS
- Настройка 802.1x
- Настройка RADIUS

AAA - это аббревиатура аутентификации, авторизации и аккаунтинга (Authorization, and, Accounting). Он обеспечивает согласованную структуру для настройки проверки подлинности, авторизации и биллинга для этих трех функций безопасности. Конфигурация AAA фактически является управлением сетевой безопасностью, где сетевая безопасность в основном относится к контролю доступа. Какие пользователи могут получить доступ к сети?
К каким сервисам пользователи могут получить доступ?
Как учитывать пользователей, использующих сетевые ресурсы?

Аутентификация (Authentication): проверьте, может ли пользователь получить доступ.
Авторизация (Authorization): какими сервисами могут пользоваться авторизованные пользователи?.
Аккаунтинг (Accounting): учет использования пользователем сетевых ресурсов.
Сетевая компания запустила набор AAA-решений, имеет клиент продукт 802.1x, множество поддерживающих аутентификацию коммутаторов и аутентификацию биллинговой системы HyperBoss. Клиент 802.1x установлен на ПК, к которому пользователи имеют доступ в Интернет. Когда пользователю требуется доступ к сети, он должен использовать клиент 802.1x для проверки подлинности. Только пользователь, прошедший проверку подлинности, может использовать сеть.
Это биржа аутентификации, которая получает запрос аутентификации клиента, передает имя пользователя и пароль в систему аутентификации и биллинга HyperBoss, а сам коммутатор не выполняет фактическую работу аутентификации. HyperBoss получает запрос на аутентификацию, отправленный коммутатором, и выполняет фактическую аутентификацию, а также выполняет обработку биллинга для успешного пользователя аутентификации.
Протокол 802.1x используется между клиентом 802.1x и коммутатором для связи, а протокол RADIUS используется между коммутатором и HyperBoss.

11.1 Введение в 802.1x

Протокол 802.1x основан на порту протокола управления доступом и аутентификации, порт здесь относится к логическому порту, хотя может быть физическим портом, MAC-адресом или идентификатором Vlan, реализация сетевого коммутатора основана на MAC-адресе и порт на основе протокола 802.1x.
802.1x является двухуровневым протоколом, коммутатор с проверкой подлинности и компьютер пользователя должны находиться в одной подсети, и пакет протокола не может пересекать сегмент

сети. Проверка подлинности 802.1x использует модель клиентского сервера и должна иметь сервер для проверки подлинности всех пользователей.

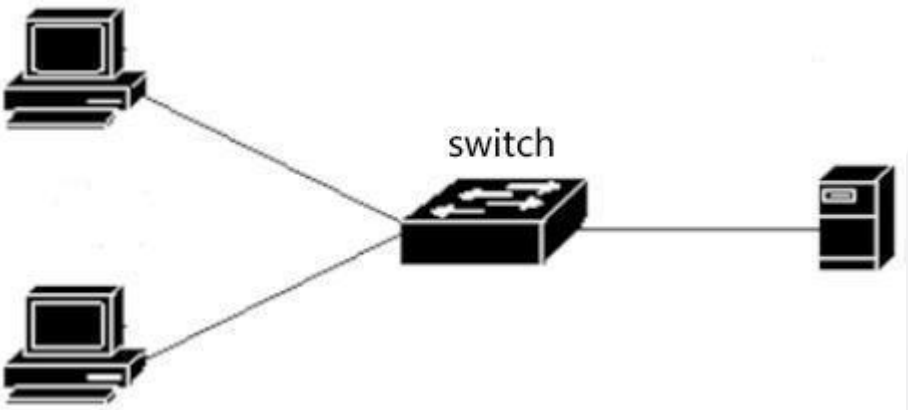
В режиме MAC пользователь через аутентификацию до, только поток аутентификации может проходить через порт коммутатора, после успешной проверки подлинности данные могут проходить через порт коммутатора, что означает, что пользователи должны получить доступ к сети после принятия сертификации. Режим порта: вы можете открыть функцию Guest Vlan, по умолчанию закрыта. Отключите гостевую Vlan и MAC-данные по одному и тому же шаблону, но после аутентификации необходимо открыть порт для незарегистрированного MAC-адреса; Откройте гостевую VLAN, когда пользователь проходит проверку подлинности перед данными гостевой VLAN, аутентификация выполняется успешно, с помощью Auth Vlan, этот метод можно использовать для указания области аутентификации пользователя с ограниченным доступом - до или после проверки подлинности доступа к общедоступной сети.

Основное содержание этого раздела заключается в следующем:

- Состав устройства 802.1x
- Краткое введение в пакет протоколов
- Взаимодействие потока протоколов
- Состояние порта 802.1x

11.1.1 Состав устройств 802.1x

Устройство 802.1x состоит из трех частей: клиент (Supplicant System), система аутентификации (Authenticator System) и сервер аутентификации (Authentication Server System). Как показано на следующем рисунке.



802.1x

Относится к клиентским запросам доступа к сетевому оборудованию, общей пользовательской терминальной системе, например, пользователям ПК, пользовательская терминальная система должна установить клиентское программное обеспечение 802.1x, программная реализация протокола 802.1x в клиентской части. Клиент инициирует запрос на аутентификацию 802.1x и просит сервер аутентификации проверить его имя пользователя и пароль. Если аутентификация прошла успешно, пользователь может получить доступ к сети.

Системы аутентификации относятся к аутентифицированным устройствам, таким как коммутаторы. Система аутентификации пользователя по логическому порту (см. MAC-адрес) определяет состояние, может ли пользователь получить доступ к сети, если пользователь не является

логическим центром состояния порта, пользователь не может получить доступ к сети, если пользователь авторизован в состояние логического порта, пользователь может получить доступ к сети.

Система аутентификации — это ретранслятор между клиентом и сервером аутентификации. Система проверки подлинности запрашивает идентификационные данные пользователя и пересылает идентификационные данные пользователя на сервер аутентификации, а также пересылает результат проверки подлинности, отправленный сервером проверки подлинности клиенту. Серверная часть системы аутентификации для реализации протокола 802.1x в ближайших конечных пользователях, клиентская часть рядом с сервером аутентификации для реализации протокола RADIUS, система аутентификации клиента протокола RADIUS 802.1x клиент отправил информационный пакет EAP, отправленный на сервер аутентификации в RADIUS, и с сервера аутентификации на протокол RAIDUS в пакете информационного решения EAP и отправлен сервером 802.1x на клиент 802.1x.

Сервер аутентификации относится к устройству, которое фактически аутентифицирует пользователя. Сервер аутентификации идентификации для получения системы аутентификации пользователя и проверки успешности аутентификации, аутентификация сервера аутентификации система аутентификации позволяет пользователю получить доступ к сети, если аутентификация не удается, система аутентификации сервера аутентификации сообщает о сбое аутентификации пользователя, пользователь не может получить доступ к сети. Связь между сервером аутентификации и системой аутентификации через расширенный протокол RADIUS EAP. Сеть обеспечивает аутентификацию и биллинговую систему, аутентификацию HyperBoss и биллинг для пользователей.

11.1.2 Краткое введение в пакет протоколов

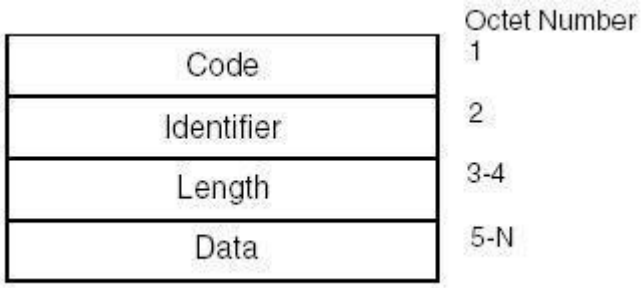
Передача данных аутентификации по протоколу 802.1x в сетевом потоке представляет собой формат кадра EAPOL (EAP Over LAN), вся идентификационная информация пользователя (включая имя пользователя и пароль) инкапсулирована в EAP (Extensible Authentication Protocol), EAP инкапсулирована в кадры EAPOL.

Имя пользователя существует в виде открытого текста в EAP, а пароль существует в виде шифрования MD5 в EAP.

Формат кадра EAPOL выглядит следующим образом. ТИП PAE Ethernet — это номер типа протокола Ethernet EAPOL, значение которого равно 0x888E. Версия протокола – это номер версии EAPOL, который равен 1. Тип пакета относится к типу кадра EAPOL. Длина тела пакета — длина содержимого кадра EAPOL. Тело пакета относится к содержимому фрейма EAPOL.

	Octet Number
PAE Ethernet Type	1-2
Protocol Version	3
Packet Type	4
Packet Body Length	5-6
Packet Body	7-N

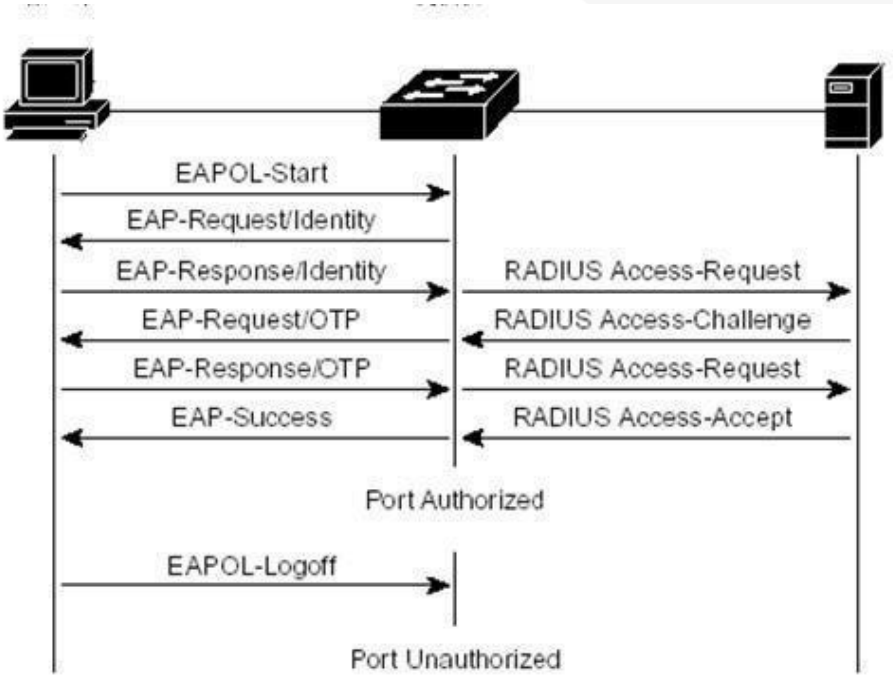
Коммутаторы формата кадров EAPOL используют три кадра протокола EAPOL соответственно:
Значение EAPOL-Start:Packet Type равно 1, инициируется фрейм аутентификации, а когда пользователю требуется аутентификация, кадр сначала запускается, а клиент отправляется коммутатору.
Значение параметра EAPOL-Logoff:Тип пакета равно 2. Кадр запроса закрывается, и фрейм уведомляется, когда пользователю не нужно использовать сеть.
Значение параметра EAP-Packet:Packet Type равно 0, а информационный фрейм аутентификации используется для передачи сведений об аутентификации.
Формат пакета EAP выглядит следующим образом. Код относится к типу пакета EAP, включая запрос, ответ, успех и сбой. Идентификатор относится к идентификаторам, которые используются для сопоставления ответа и запроса. Длина относится к длине пакета EAP, включая Baotou. Данные относятся к данным пакета EAP.
Пакет EAP состоит из следующих четырех типов:
Значение EAP-Request:Code равно 1, EAP запрашивает пакет и запрашивает имя пользователя и/или пароль от коммутатора к клиенту.
Значение EAP-Response:Code равно 2, пакет ответа EAP отправляется от клиента коммутатору, а имя пользователя и/или пароль отправляются коммутатору.
EAP-Success:Значение code равно 3, EAP успешно упакован, отправлен от коммутатора к клиенту, сообщил клиенту об успешной аутентификации пользователя.
Значение EAP-Failure:Code равно 4, пакет сбоя EAP отправляется от коммутатора клиенту, и клиенту сообщается, что проверка подлинности не удалась.



Формат пакета EAP

11.1.3 Взаимодействие потока протокола

Если коммутатор включает 802.1x и состояние порта — Auto, все пользователи доступа через порт должны пройти проверку подлинности для доступа к сети. Взаимодействие по протоколу, как показано ниже.



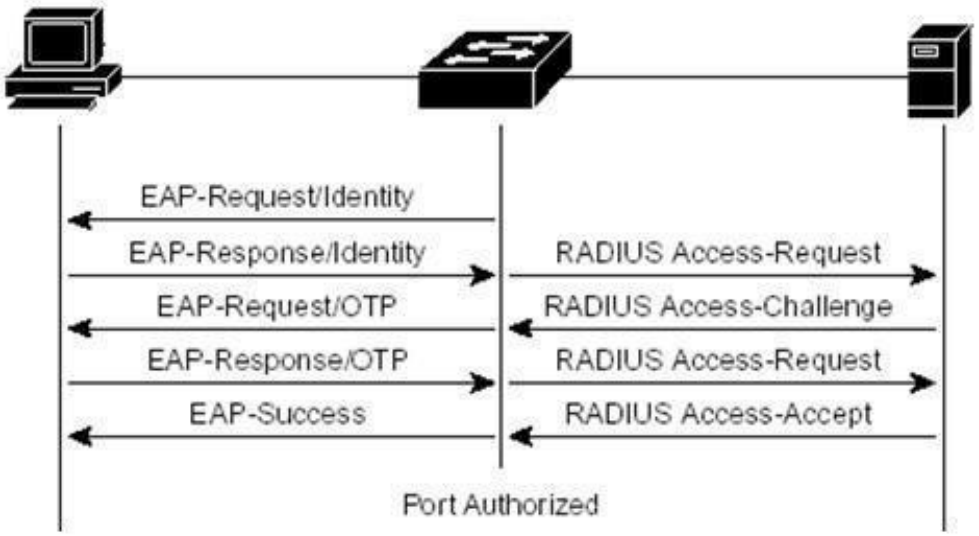
Взаимодействие по протоколу аутентификации, инициированное клиентом

Когда пользователям необходимо получить доступ к сети, клиент отправляет первый EAPOL-Start для обмена запросами, полученными после аутентификации запроса аутентификации, коммутатор отправляет имя пользователя запроса EAP-Request, клиент отправляет EAP-Response, переключает информацию EAP, извлеченную из пакета в пакете RADIUS, отправляется на сервер аутентификации, сервер аутентификации запрашивает пароль пользователя, переключиться на отправку EAP-запроса клиенту, запрос пользователя пароль клиента EAP-Response, эхо-коммутатор, информация EAP инкапсулируется в RADIUS аутентификации сервера для отправки пакетов, в соответствии с аутентификацией сервера аутентифицирует имя пользователя и пароль. Если проверка подлинности прошла успешно, сервер аутентификации уведомляет коммутатор, коммутатор отправляет клиенту EAP-Success, а логический порт пользователя находится в авторизованном состоянии. Когда клиент получает EAP-Success, проверка подлинности выполняется успешно, и пользователь может получить доступ к сети.

Когда пользователю больше не нужно пользоваться сетью, клиент отправляет коммутатору EAPOL-Logoff, а коммутатор переводит состояние логического порта пользователя в несанкционированное состояние, когда пользователь не может получить доступ к сети.

Чтобы проверить некорректного пользователя в автономном режиме, коммутатор предоставляет механизм повторной сертификации, временной интервал может быть установлен в повторной сертификации на коммутаторе, когда приходит время аутентификации, коммутатор инициирует повторную сертификацию, если аутентификация прошла успешно, пользователь может продолжать использовать сеть, если аутентификация не удалась, пользователь не сможет использовать сеть.

Взаимодействие по протоколу, показано ниже.



Взаимодействие по протоколу с проверкой подлинности

11.1.4 Состояние порта 802.1x

Состояние порта — это состояние физического порта коммутатора. В физическом порту коммутатора есть четыре состояния: состояние Н/Д, состояние авто, состояние, санкционированное силой, и состояние, не имеющее разрешения на применение силы. Если коммутатор не открывает 802.1x, все порты находятся в состоянии N/A. Когда порты коммутатора в состоянии Auto, принудительно авторизован или принудительно-несанкционирован, 802.1x должен быть включен.

Когда порт коммутатора находится в состоянии N/A, все пользователи под портом могут получить доступ к сети без аутентификации. Когда коммутатор получает пакет протокола 802.1x от порта, пакеты протоколов отбрасываются.

Когда порт коммутатора находится в состоянии принудительной авторизации, все пользователи на порту могут получить доступ к сети без проверки подлинности. Когда коммутатор получает пакет EAPOL-Start от порта, коммутатор отправляет пакет EAP-Success. Когда коммутатор получает другие пакеты протокола 802.1x от порта, пакеты протоколов отбрасываются.

Когда порт коммутатора находится в принудительно-несанкционированном состоянии, все пользователи порта не могут получить доступ к сети все время, и запрос аутентификации никогда не пройдет. Когда коммутатор получает пакет протокола 802.1x от порта, пакеты протоколов отбрасываются.

Когда порт коммутатора находится в состоянии Auto, следует различать режим проверки подлинности. Режим порта, если гостевой Vlan не настроен, порт пользователя должен иметь доступ к сети через сертификацию, закрывая порт не сертифицирован; Если конфигурация порта гостевой Vlan, пользователь может получить доступ к Auth Vlan через сертификацию, не сертифицированный может получить доступ к гостевой VLAN. Все пользователи порта должны пройти проверку подлинности для доступа к сети. Взаимодействие протокола 802.1x показано на схеме. Если пользователю требуется проверка подлинности, для порта обычно устанавливается состояние Auto. Когда порт коммутатора установлен в состояние Auto, и включена функция защиты от спуфинга ARP; функция анти-спуфинга ARP может управлять только IP-пакетом, MAC-источника и исходный IP-адрес согласуются с информацией, предоставленной пакетом данных аутентификации клиента, а IP-адрес отправителя пакета ARP и MAC соответствуют ip-адресу аутентификации отправителя, клиент

предоставляет информационные пакеты для этой переадресации порта, в противном случае он будет отброшен. Эта функция должна быть IP-адресом конфигурации клиента статической конфигурации, если она предназначена для получения IP-адреса через динамические условия протокола DHCP для достижения этой функции для включения протокола DHCP SNOOPING; Если вам нужна дополнительная информация, обратитесь к конфигурации привязки IP MAC.

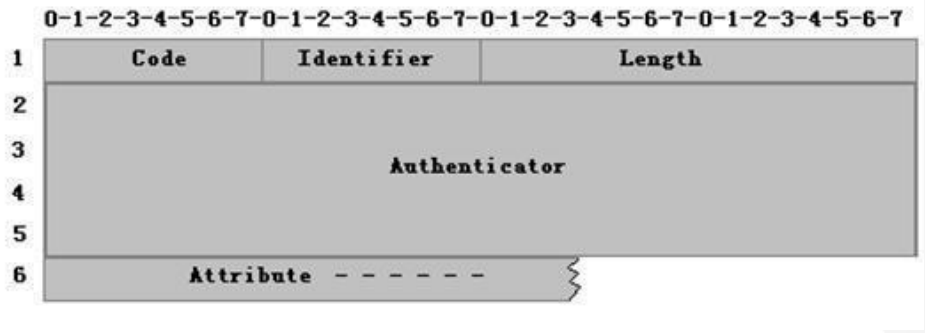
11.2 Введение в RADIUS

Когда пользователь проходит проверку подлинности, exchange и сервер проверки подлинности взаимодействуют с протоколом RADIUS, поддерживающим расширение EAP. Протокол RADIUS использует клиент-серверную модель, коммутаторы должны реализовывать RADIUS-клиент, а сервер аутентификации должен реализовывать RADIUS-сервер.
Для обеспечения безопасности взаимодействия между коммутатором и сервером аутентификации, а также для предотвращения несанкционированного взаимодействия между коммутаторами и серверами, необходима взаимная аутентификация между коммутатором и сервером аутентификации. Коммутатор и сервер аутентификации нуждаются в одном и том же ключе, когда коммутатор или сервер аутентификации отправляет пакеты протокола RADIUS, все пакеты в соответствии с ключом и используемым алгоритмом HMAC для генерации дайджеста сообщения, когда коммутатор и сервер аутентификации получают пакет протокола RADIUS, все пакеты протокола для проверки дайджеста сообщения с помощью ключа, если это проверено, то это допустимые RADIUS, в противном случае это недопустимые пакеты RADIUS, отбрасываемые.
Основное содержание этого раздела заключается в следующем:

- Краткое введение в пакет протоколов
- Взаимодействие потока протоколов
- Метод аутентификации пользователя

11.2.1 Краткое введение в пакет протоколов

RADIUS — это протокол, основанный на UDP, и RADIUS может инкапсулировать информацию о проверке подлинности и платежную информацию. Ранее порт проверки подлинности RADIUS был — 1645, текущий используемый порт — 1812, раннее порт биллинга RADIUS был — 1646, текущий используемый порт — 1813.
Поскольку RADIUS работает на UDP, RADIUS имеет механизм повторной передачи времени ожидания. При этом для повышения надежности связи между системой аутентификации и RADIUS-сервером приняты две схемы RADIUS-сервера, то есть принят резервный серверный механизм.
Формат сообщения RADIUS выглядит следующим образом. Код относится к типу сообщения протокола RADIUS. Идентификатор индекса для сопоставления запросов и ответов. Длина относится к длине всего сообщения (включая заголовок). Authenticator — это 16-байтовая строка, случайное число для пакета запроса и дайджест сообщения для пакета ответа, создаваемого MD5. Атрибут относится к атрибутам в пакете протокола RADIUS.

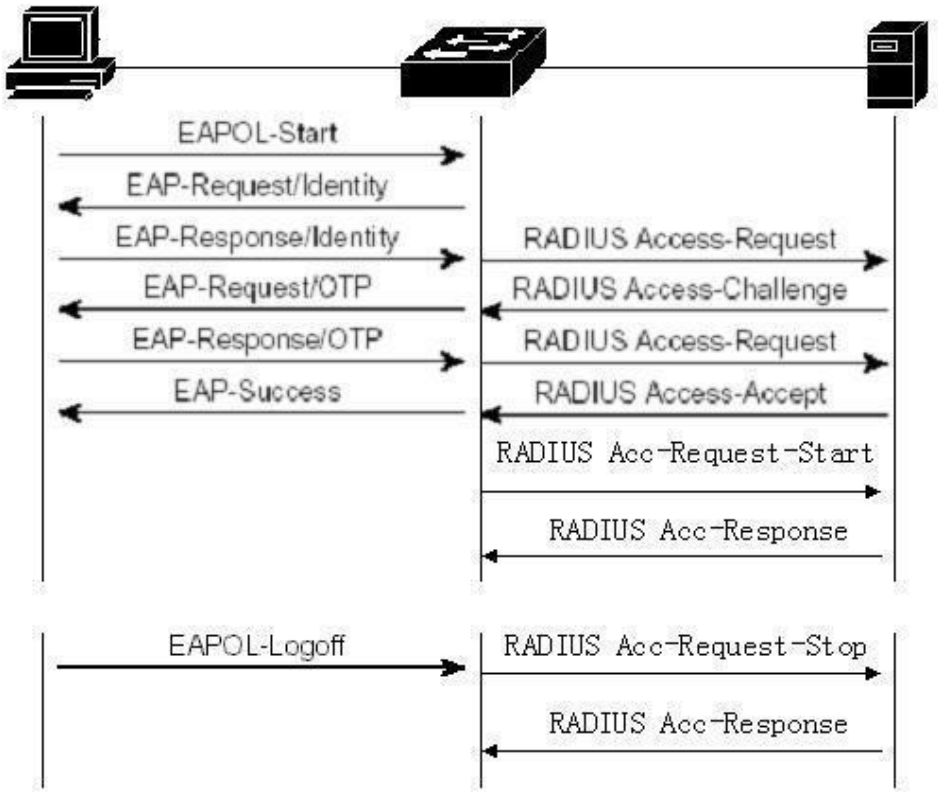


Формат сообщения RADIUS

Сеть использует следующие пакеты протоколов RADIUS:
Значение Access-Request:Code равно 1, пакет запроса проверки подлинности отправляется на сервер аутентификации из системы аутентификации, а имя пользователя и пароль инкапсулируются в пакете.
Значение Access-Accept:Code равно 2 от сервера аутентификации до пакета ответа системы аутентификации, что означает, что проверка подлинности пользователя выполнена успешно.
Значение Access-Reject:Code равно 3, пакет аутентификации отправляется в систему аутентификации с сервера аутентификации, что указывает на сбой аутентификации пользователя.
Значение Access-Challenge:Code равно 11 от сервера аутентификации до пакета ответа системы аутентификации, что указывает на то, что серверу аутентификации требуется дополнительная информация о пользователе, такая как пароли.
Значение Accounting-Request:Code равно 4, пакет запроса биллинга из системы аутентификации отправляется на сервер аутентификации, включая начальный биллинг и конечный пакет биллинга, а платежная информация инкапсулируется в пакете.
Значение Accounting-Response:Code равно 5 от сервера аутентификации до пакета ответа на билинг системы аутентификации, что указывает на то, что платежная информация была получена.

11.2.2 Взаимодействие потока протокола

Когда пользователь инициирует аутентификацию, система аутентификации и сервер аутентификации взаимодействуют друг с другом через протокол RADIUS. Система аутентификации не отправляет поток протокола пакета биллинга RADIUS, как показано на схеме ниже. Как правило, когда проверка подлинности пользователя выполнена успешно или пользователь находится в автономном режиме, системе проверки подлинности необходимо отправить пакет биллинга RADIUS на сервер проверки подлинности, а взаимодействие потока протокола показано на следующем рисунке.



Аутентифицировать пользователя, переключить пакет в сообщении Access-Request, отправленном на сервер аутентификации имени пользователя, сервер в ответ на запрос Access-Challenge пользователя и пароль, на коммутаторе запроса клиента и пароль пользователя, пароль к клиенту в упаковке EAP, коммутатор попадает в этот EAP, инкапсулированный в Access-Request к серверу аутентификации аутентифицирует сервер аутентификации пользователя, если проверка подлинности прошла успешно, эхо Access-Accept к коммутатору, коммутатор сообщит об успешной проверке подлинности клиента, и отправляет сервер аутентификации с уведомлением Accounting-Request для начала биллинга, замыкания сервера аутентификации Accounting-Response.

Когда пользователь не хочет пользоваться Интернетом, уведомляет абонентскую линию, переключает Accounting-Request уведомляет сервер аутентификации об окончании биллинга, платежная информация инкапсулируется в этот пакет, сервер аутентификации отправляет Accounting-Response.

11.2.3 Методы аутентификации пользователя

Существует три метода проверки подлинности пользователей для RADIUS:

- PAP (Password Authentication Protocol). Пользователь передает имя пользователя и свой пароль коммутатору в виде открытого текста. Коммутатор передает имя пользователя и пароль серверу RADIUS через пакет протокола RADIUS, а RADIUS-сервер ищет базу данных. Если есть одно и то же имя пользователя и пароль, это указывает на то, что проверка подлинности пройдена, в противном случае это указывает на то, что проверка подлинности не прошла.

- CHAP (Challenge Handshake Authentication Protocol). Когда пользователь запрашивает доступ к Интернету, коммутатор генерирует пользователю 16-байтовый случайный код. Пользователь шифрует случайный код, пароль и другие домены для генерации ответа, передавая имя пользователя и ответ коммутатору. Коммутатор передает имя пользователя, ответ и исходный 16-байтовый случайный код на сервер RADIUS. Согласно имени пользователя RADIU в базе данных поиска на стороне коммутатора, конечные пользователи используют один и тот же пароль шифрования, затем шифруется на основе случайного кода до 16 байт, и результаты сравниваются, если они совпали то проверка проходит, если не совпали, то проверка не удалась.

- EAP (Extensible Authentication Protocol). При таком методе верификации коммутатор на самом деле не участвует в верификации, а играет только роль пересылки между пользователем и RADIUS-сервером. Когда пользователь запрашивает доступ, exchange запрашивает имя пользователя, имя пользователя и перенаправляется на сервер RADIUS, сервер RADIUS генерирует 16-байтовый случайный код для пользователя и сохраняет случайный код, пользователь генерирует случайный код, пароль шифрования ответа и другой домен, имя пользователя и ответ на переключение, пересылку на сервер RADIUS. По имени пользователя RADIU в базе данных поиска на стороне коммутатора конечные пользователи используют один и тот же пароль шифрования, а затем шифруются по случайному коду, хранящемуся в 16 байтах, если результаты сравнения ответов показали совпадение то проверка удалась, если совпадения отсутствуют, то проверка не удалась.

Решение для аутентификации и биллинга сети использует метод EAP аутентификации пользователя.

11.3 Настройка 802.1x

В этом разделе приводится подробное описание конфигурации 802.1x, включая следующие:

- Конфигурация 802.1x по умолчанию
- Запуск и отключение 802.1x
- Настройка состояния порта 802.1x
- Настройка аутентификации порта 802.1x
- Настройка гостевой VLAN порта 802.1x
- Механизм повторной проверки подлинности конфигурации
- Максимальное количество узлов доступа к портам конфигурации
- Настройка интервального времени и времени повторной отправки
- Конфигурация порта в роли транспортного порта
- Настройка номера версии клиента 802.1x
- Настройка проверки номера версии клиента
- Метод проверки подлинности конфигурации
- Настройка необходимости проверки пакета синхронизации клиента
- Отображение информации 802.1x

11.3.1 Конфигурация 802.1x по умолчанию

Параметры конфигурации 802.1x по умолчанию выглядят следующим образом:

- 802.1x отключен
- Состояние всех портов — N/A
- Механизм аутентификации отключен, а интервал проверки подлинности составляет 3600 секунд
- Максимальное количество узлов доступа для всех портов составляет 100
- Интервал ожидания повторной передачи EAP-запроса составляет 30 секунд
- Время ожидания ретрансляции EAP-Request составляет 3 раза
- При ошибка аутентификации пользователь ожидает в течение 60 секунд
- Интервал тайм-аута сервера составляет 10 секунд

Коммутатор предоставляет команду в режиме глобальной конфигурации для возврата всей конфигурации обратно в состояние по умолчанию. Команда следующие:

Switch(config)#dot1x default

11.3.2 Запуск и закрытие 802.1x

Первым шагом в настройке 802.1x является запуск 802.1x. в режиме глобальной конфигурации введите следующую команду, чтобы запустить 802.1x:

Switch(config)#dot1x

Когда 802.1x отключается, все порты возвращаются в состояние N/A. В режиме глобальной конфигурации введите следующую команду, чтобы закрыть 802.1x:

Switch(config)#no dot1x

11.3.3 Настройка состояния порта 802.1x

Необходимо запустить 802.1x перед настройкой состояния порта 802.1x. Если необходимо чтобы все пользователи порта проходили проверку подлинности для доступа к сети, порт должен быть установлен в состояние Auto.

Следующая команда устанавливает порт ge1/1 в состояние Auto в режиме конфигурации интерфейса и включает функцию спуфинга анти ARP:

Switch(config-ge1/1)dot1x control auto

Если настройка анти-ARP спуфинга не удалась, это может быть вызвано следующими причинами:

1. Исчерпание ресурсов системы CFP.
2. Текущий интерфейс настраивается с помощью функции фильтра ACL.
3. Текущий интерфейс включает функцию DHCP SNOOPING.
4. Настраиваемый интерфейс представляет собой трехслойный интерфейс или магистральный интерфейс.

Следующая команда устанавливает порт ge1/1 в состояние Force-authorized в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x control force-authorized

Следующая команда устанавливает порт ge1/1 в состояние Force-unauthorized в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x control force-unauthorized

Следующая команда задает состояние порта ge1/1 в состояние N/A в режиме конфигурации интерфейса:

Switch(config-ge1/1)no dot1x control

Примечание: если на порту привязан MAC-адрес, то порт не может быть установлен в состояние Auto, Force-authorized или Force-unauthorized.

11.3.4 Настройка аутентификации порта 802.1x

Перед настройкой метода проверки подлинности порта 802.1x необходимо запустить 802.1x. Если порт подключен только к пользователю, которому требуется проверка подлинности, порт открывается путем проверки подлинности, и порт должен быть установлен в portbase. Если аутентификация основана на MAC-адресе, она будет установлена на macbase. Состояние по умолчанию — macbase.

Следующая команда устанавливает port ge1/1 в состояние portbase в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x method portbase

Следующая команда устанавливает состояние порта ge1/1 в состояние macbase в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x method macbase

11.3.5 Настройка гостевой VLAN порта 802.1x

Перед настройкой гостевой VLAN порта 802.1x необходимо запустить 802.1x и настроить порты для состояния auto и состояния portbase. Доступ к гостевой VLAN можно получить до аутентификации пользователя под нужным портом. После проверки подлинности можно получить доступ к VLAN конфигурации, а затем порт будет настроен на гостевую VLAN.

Следует отметить, что гостевая VLAN поддерживает только режим access и не поддерживает trunk. После настройки порта с гостевой VLAN его режим не может быть изменен, а гостевая VLAN не может быть настроена на режим отсутствия доступа. При настройке гостевой VLAN необходимо убедиться, что виртуальная локальная сеть создана.

Следующая команда устанавливает для гостевой VLAN порта значение 2 в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x guest-vlan 2

11.3.6 Механизм повторной аутентификации конфигурации

Чтобы клиент не знал о коммутаторе и сервере аутентификации, коммутатор предоставляет механизм повторной проверки подлинности, который инициирует проверку подлинности один раз каждый второй интервал времени.

Следующая команда запускает механизм повторной проверки подлинности в режиме глобального конфигурирования:

Switch(config)#dot1x re-authenticate

Следующая команда закрывает механизм проверки подлинности в режиме глобального конфигурирования:

Switch(config)#no dot1x re-authenticate

Следующая команда задает временной интервал для повторной проверки подлинности режиме глобального конфигурирования:

Switch(config)#dot1x timeout re-authperiod <interval>

Примечание: интервал между повторной аутентификацией не должен быть слишком коротким, иначе пропускная способность сети и потребление ресурсов ЦП коммутатором будут слишком большими.

11.3.7 Максимальное количество узлов доступа к портам конфигурации

Каждый порт коммутатора может управлять максимальным количеством узлов доступа. Эта функция может ограничить незаконный доступ пользователей к сети с помощью нескольких хостов. Максимальное количество портов доступа к хосту по умолчанию составляет 100. Если для максимального числа портов узла доступа установлено значение 0, то порт отклоняет доступ любого пользователя.

Следующая команда задает максимальное количество узлов доступа к порту ge1/1 в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x support-host <number>

11.3.8 Настройка интервального времени и времени повторной отправки

Стандартный протокол 802.1x и конечное устройство протокола некоторый интервал времени и количество повторных передач, коммутаторы, использующие стандартный временной интервал и количество повторных передач, предполагают, что пользователи при их использовании не изменяют временной интервал и количество повторных передач.

Tx-period говорит об интервальном времени повторения протокола EAP-Request коммутатора; max-req указывает количество ретрансляционных коммутаторов EAP-Request; quiet-period представляет собой временной интервал сбоя аутентификации пользователя в ожидании повторной сертификации; сервер-тайм-аут означает переключение на сервер аутентификации RADIUS пакетов интервал времени ретрансляции; supp-timeout указанный временной интервал переключения пакетов на клиентский запрос на повторную передачу EAP.

Следующая команда настраивает интервал и время повторной передачи в режиме глобального конфигурирования:

Switch(config)#dot1x timeout tx-period <interval>
Switch(config)#dot1x max-req <number>
Switch(config)#dot1x timeout quiet-period <interval>
Switch(config)#dot1x timeout server-timeout <interval>
Switch(config)#dot1x timeout supp-timeout <interval>

11.3.9 Конфигурация порта в роли транспортного порта

Если на коммутаторе не открыта проверка подлинности 802.1x и другие коммутаторы подсети открывают сертификацию 802.1x, можно настроить клиент подключения коммутатора и порт коммутатора проверки подлинности для передачи портов пересылки пакетов проверки подлинности eapol между клиентом и проверки подлинности коммутаторов 802.1x. Чтобы реализовать аутентификацию 802.1x других коммутаторов на клиенте.

Следующая команда устанавливает порт ge1/1 в качестве транспортного порта в режиме конфигурации интерфейса:

Switch(config-ge1/1)dot1x transmit-port

Следующая команда устанавливает порт ge1/1 в качестве не транспортного порта в режиме конфигурации интерфейса:

Switch(config-ge1/1)no dot1x transmit-port

11.3.10 Настройка номера версии клиента 802.1x

Настройка номера версии клиента 802.1x, и только клиент, версия которого не меньше номера версии конфигурации, может пройти проверку подлинности, в противном случае проверка подлинности не будет пройдена. Номер версии клиента коммутатора по умолчанию — 2.

Следующая команда настраивает номер версии клиента в режиме глобальной конфигурации:

Switch(config)# dot1x client-version <string>

11.3.11 Настройка проверки номера версии клиента

Настройте проверку номера версии клиента 802.1x. Если проверка настроена, коммутатор сначала проверяет номер версии клиента при проверке подлинности. По умолчанию проверка включена.

Следующая команда настраивает включение проверки номера версии клиента в режиме глобального конфигурирования:

Switch(config)# dot1x check-version open

11.3.12 Метод проверки подлинности конфигурации

Метод аутентификации конфигурации переключается на пакет 802.1x, клиент инициирует метод аутентификации, который делится на универсальную аутентификацию и расширенную аутентификацию, на коммутаторе можно настроить, какой путь аутентификации будет первый. Если инициированный клиентом метод проверки подлинности не соответствует методу проверки подлинности конфигурации коммутатора, клиент инициирует проверку подлинности после очередного сбоя проверки подлинности.

Следующая команда настраивает метод проверки подлинности коммутатора в режиме глобального конфигурирования для расширения режима проверки подлинности:

Switch(config)# dot1x extended

11.3.13 Настройка необходимости проверки пакета синхронизации клиента

Устанавливает на коммутаторе время проверки, успешна ли конфигурация пакета клиента при аутентификации, позволяет изменить возможность опроса клиента регулярно отправлять пакеты 802.1x, но не все клиенты будут регулярно отправлять пакеты 802.1x на сертификацию, эта конфигурация работает через командный коммутатор синхронизации проверки пакетов клиента.

Следующая команда в режиме глобального конфигурирования настраивает, на коммутаторе нужна ли проверка пакета синхронизации клиента:

Switch(config)# dot1x check-client

11.3.14 Отображение информации 802.1x

Следующие команды в обычном режиме / привилегированном режиме отображают информацию 802.1x, отображает информацию о конфигурации 802.1x для всех, включая информацию о конфигурации для всех портов; при выполнении команды show dot1x interface, отображает всю информацию о порте доступа пользователя:

Switch#show dot1x

Switch#show dot1x interface

11.4 Конфигурация RADIUS

В этом разделе приводится подробное описание конфигурации RADIUS, включая следующие:

- Конфигурация RADIUS по умолчанию
- Настройка IP-адреса сервера аутентификации
- Настройка общих ключей
- Запуск и закрытие биллинга
- Настройка портов RADIUS и информации об атрибутах
- Настройка функции роуминга RADIUS
- Отображение информации о RADIUS

11.4.1 Конфигурация RADIUS по умолчанию

Параметр конфигурации RADIUS по умолчанию выглядит следующим образом:

- Для основного сервера аутентификации и резервного сервера аутентификации нет IP-адреса, то есть IP-адрес 0.0.0.0.
- Отсутствует общий ключ конфигурации, то есть строка общего ключа пуста.
- Биллинг инициируется по умолчанию.
- UDP-порт аутентификации RADIUS — 1812, UDP-порт для биллинга — 1813.
- Значение атрибута RADIUS NASPort равно 0xc353, значение NASPortType — 0x0f, а значение NASPortServer — 0x02.

11.4.2 Настройка IP-адреса сервера аутентификации

Для связи между коммутатором и сервером аутентификации необходимо настроить IP-адрес сервера аутентификации на коммутаторе RADIUS . В практических приложениях вы можете использовать сервер аутентификации, вы также можете использовать два сервера аутентификации, один в качестве основного сервера аутентификации, один в качестве резервного сервера аутентификации. Если коммутатор настроен с двумя IP-адресами сервера аутентификации, когда коммутатор и главный сервер аутентификации прерывают связь, вы можете переключиться на резервный сервер аутентификации.

Следующая команда настраивает IP-адрес главного сервера проверки подлинности в режиме глобального конфигурирования:

Switch(config)#radius-server host <ip-address>

Следующая команда настраивает IP-адрес резервного сервера проверки подлинности в режиме глобального конфигурирования:

Switch(config)#radius-server option-host <ip-address>

11.4.3 Настройка общих ключей

Взаимная проверка подлинности необходима между коммутатором и сервером аутентификации, и один и тот же общий ключ необходим на коммутаторе и сервере аутентификации. Обратите внимание, что общий ключ на коммутаторе должен совпадать с сервером аутентификации.

Следующая команда настраивает общий ключ коммутатора в режиме глобального конфигурирования:

Switch(config)#radius-server key <string>

11.4.4 Запуск и закрытие биллинга

Когда коммутатор закрывает биллинг, коммутатор не отправит пакет RADIUS на сервер аутентификации, если проверка подлинности прошла успешно или пользователь находится в автономном режиме. В общем случае, биллинг открыт в практических приложениях.

Следующая команда инициирует биллинг в режиме глобальной конфигурации:

Switch(config)#radius-server accounting

Следующая команда закрывает биллинг в режиме глобальной конфигурации:

Switch(config)#no radius-server accounting

11.4.5 Настройка портов RADIUS и информации об атрибутах

Пользователям не рекомендуется изменять конфигурацию порта RADIUS и информации об атрибутах.

Следующая команда изменяет UDP-порт аутентификации RADIUS в режиме глобальной конфигурации:

Switch(config)#radius-server udp-port <port-number>

Следующие команды изменяют информацию атрибута RADIUS в режиме глобальной конфигурации:

Switch(config)#radius-server attribute nas-portnum <number>
Switch(config)#radius-server attribute nas-porttype <number>
Switch(config)#radius-server attribute service-type <number>

11.4.6 Настройка функции RADIUS-роуминга

При привязке MAC, IP или VLAN к клиенту, когда клиент перемещается в другое место, привязанный клиент не может выполнить аутентификацию 802.1x из-за изменения MAC-адреса, IP-адреса или VLAN. Откройте функцию роуминга RADIUS, будет игнорировать MAC клиента, IP или VLAN привязки, с тем чтобы продолжать достигать 802.1x аутентификации.

Следующая команда настраивает функцию роуминга RADIUS в режиме глобальной конфигурации:

Switch(config)#radius-server roam

Следующая команда закрывает функцию роуминга RADIUS в режиме глобальной конфигурации:

Switch(config)#no radius-server roam

11.4.7 Отображение информации RADIUS

Следующая команда отображает информацию о конфигурации RADIUS в нормальном режиме / привилегированном режиме : .

Switch#show radius-server

11.5 Пример конфигурации

Откройте протокол 802.1x, настройте порт ge1/1 в состояние Auto, настройте основной сервер аутентификации 198.168.80.111, настройте общий секретный ключ коммутатора ABCDEF.

```
Switch#
Switch# dot1x
Switch#config t
Switch(config)#radius-server host 198.168.80.111
Switch(config)#radius-server key abcdef
Switch(config)# interface ge1/1
Switch(config-ge1/1)# dot1x control auto
```

Двенадцатая глава

Конфигурация GMRP

Основное содержание этой главы следующее:

- Введение в GMRP
- Конфигурация GMRP
- Примеры типичных конфигураций GMRP

12.1 Введение в GMRP

В настоящее время GMRP (GARP Multicast Registration Protocol) - это протокол многоадресной регистрации на основе GARP, который используется для поддержания информации о многоадресной регистрации в коммутаторе. Все поддерживающие GMRP коммутаторы могут получать информацию о многоадресной регистрации от других коммутаторов и динамически обновлять локальную информацию о многоадресной регистрации, а также распространять локальную информацию о многоадресной регистрации на другие коммутаторы. Этот механизм обмена информацией обеспечивает согласованность многоадресной информации, поддерживаемой всеми устройствами с поддержкой GMRP в одной коммутационной сети.

Когда узел хочет присоединиться к многоадресной группе, он отправляет сообщение GMRP для присоединения. Коммутатор получит порт добавления сообщения GMRP в многоадресную группу и будет транслировать GMRP в сообщение в VLAN, где находится принимающий порт. Источник многоадресной рассылки в VLAN может знать о существовании участников многоадресной рассылки. Когда источник многоадресной рассылки отправляет многоадресные пакеты в многоадресную группу, коммутатор пересылает многоадресные пакеты только на порты, являющиеся участниками многоадресной группы, тем самым реализуя двухуровневую многоадресную рассылку в VLAN.

12.2 Конфигурация GMRP

Основная конфигурация GMRP включает:

- Открытие настроек GMRP
- Просмотр информации GMRP
- В задачах конфигурации, вы должны сначала открыть глобальный GMRP, чтобы открыть порт GMRP.

12.2.1 Открыть настройки GMRP

Команда	Описание	Режим настройки
set gmrp enable | disable	Включить/выключить глобальную VLAN GMRP	Режим глобального конфигурирования
set gmrp enable vlan <vlan-id>	Включение глобально специфической VLAN GMRP	Режим глобального конфигурирования
set gmrp registration{fixed | forbidden | normal} <if-name>	Настройка режима многоадресной регистрации интерфейса	Режим глобального конфигурирования
set gmrp timer {join | leave | nleaveall} <time-value>	Сроки настройки различных таймеров	Режим глобального конфигурирования

set port gmrp enable <if-name>	Включить функцию GMRP порта	Режим глобального конфигурирования
set port gmrp disable <if-name>	Включить функцию GMRP на порту	Режим глобального конфигурирования

12.2.2 Просмотр информации GMRP

После завершения вышеуказанной конфигурации, выполнение команды show в любом представлении может отобразить работу GMRP после конфигурации, и проверить эффект конфигурации путем проверки отображаемой информации.

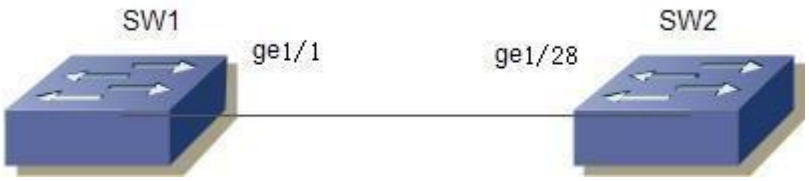
Команда	Описание	Режим настройки
show gmrp configuration	Просмотр информации о конфигурации GMRP	Привилегированный режим
show gmrp machine	Просмотр информации о устройстве состояния GMRP	Привилегированный режим
show gmrp statistics vlanid	Просмотр статистики GMRP для конкретного vlan id	Привилегированный режим
show gmrp timer <ifname>	Просмотр сведений о таймере для определенных портов	Привилегированный режим

12.3 Примеры типичных конфигураций GMRP

1. Требования к сети

Для того чтобы реализовать динамическую регистрацию и обновление многоадресной информации между коммутаторами, необходимо запустить GMRP на коммутаторе.

2. Схема сети



GMRP example network diagram

3. Этапы настройки

Настройка SW1

Запуск глобального GMRP

Switch(config)# set gmrp enable

Начальный порт GMRP на гигабитном порте Ethernet ge1/1

Switch(config)# set port gmrp enable ge1/1

Switch(config)#

Настройка SW2

Запуск глобального GMRP

Switch(config)# set gmrp enable

Пусковой порт GMRP на гигабитном порте Ethernet ge1/28

Switch(config)# set port gmrp enable ge1/28

Switch(config)#

Тринадцатые главы

Конфигурация SNOOPING

В столичной вычислительной сети /Internet использование одноадресной рассылки отправляет один и тот же пакет в сеть у многих, но не у всех получателей, из-за необходимости копировать каждый пакет в принимающую конечную точку, с увеличением числа приемников, количество пакетов потребует линейного увеличения, что заставляет хост, обмениваться общей нагрузкой на маршрутизирующее оборудование и увеличивать пропускную способность сети, это сильно влияет на эффективность. С ростом спроса на многоточечные видеоконференции, видео по запросу и приложения групповой связи, многоадресная рассылка стала самым популярным способом общения с целью улучшения использования ресурсов.
Коммутатор реализует функцию IGMP SNOOPING для службы многоадресных приложений. IGMP SNOOPING отслеживает пакеты IGMP в сети для реализации динамического обучения IP-многоадресных MAC-адресов.
В этой главе описывается концепция и конфигурация IGMP SNOOPING, включая следующее содержание:

- Введение в IGMP SNOOPING
- Конфигурация IGMP SNOOPING
- Пример конфигурации IGMP SNOOPING

13.1 Введение в IGMP SNOOPING

Традиционная сеть в подсети многоадресных пакетов, как широковещательная обработка, поэтому легко делает сетевой трафик, вызывая перегрузку сети. Когда коммутатор реализован на IGMP SNOOPING, IGMP SNOOPING может узнать IP динамический многоадресный MAC-адрес, чтобы поддерживать список выходных портов IP многоадресного MAC-адреса, многоадресный поток данных только на выходной порт для отправки, это может уменьшить нагрузку сетевого трафика.
Основное содержание этого раздела заключается в следующем:

- Обработка IGMP SNOOPING
- Динамическая многоадресная рассылка второго уровня
- Присоединение к группе
- Выход из группы

13.1.1 Обработка IGMP SNOOPING

IGMP SNOOPING - это сетевой протокол второго уровня пакетов протокола IGMP через мониторинг коммутатора, в соответствии с принимающим портом эти пакеты протоколов IGMP, идентификатор VLAN и адрес многоадресной рассылки для поддержки группы многоадресной рассылки, а затем пересылаются эти протоколы IGMP. Для приема потоков многоадресных данных можно добавлять только порты многоадресной рассылки; таким образом, снижается сетевой трафик и сохраняется пропускная способность сети. Многоадресная группа включает адрес группы многоадресной рассылки, порт участника, идентификатор VLAN, время жизни. Формирование многоадресной группы IGMP SNOOPING является процессом обучения. Когда один порт коммутатора получает пакет

IGMP REPORT, IGMP SNOOPING создает новую группу многоадресной рассылки, а порт, принимающий пакет IGMP REPORT, добавляется в группу многоадресной рассылки. Если пакет IGMP QUERY принимается коммутатором, если многоадресная группа уже существует в коммутаторе, то порт, получивший запрос IGMP, добавляется в группу многоадресной рассылки, в противном случае он будет пересылать только пакет IGMP QUERY. Leave SNOOPING также поддерживает механизм IGMP IGMP V2 IGMP SNOOPING; если конфигурация fast-leave ENABLE в IGMP V2, полученный пакет leave при его получении порта может немедленно покинуть многоадресную группу; Если конфигурация fast-leave оставила время ожидания (fast-leave-timeout), то группа многоадресной рассылки, ожидающая этого времени, истекает после выхода из группы многоадресной рассылки.
Существует два механизма обновления для IGMP SNOOPING. Одним из них является механизм отпуска, описанный выше. В большинстве случаев IGMP SNOOPING удаляет просроченные многоадресные группы по возрасту. Когда группа многоадресной рассылки присоединяется к IGMP SNOOPING, записывается добавленное время. Если группа многоадресной рассылки имеет более одного настроенного времени возраста в коммутаторе, возможность обмена удаляет группу многоадресной рассылки.

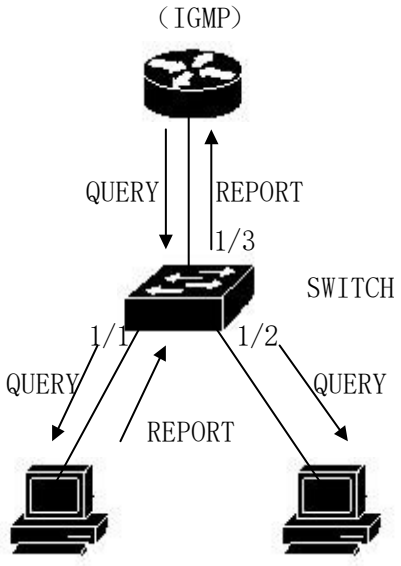
Когда порт принимает Leave пакетов, этот порт будет немедленно удален из многоадресной группы, к которой он принадлежит, такая ситуация может повлиять на непрерывность сетевого потока данных; Поскольку этот порт сетевого оборудования может быть подключен к функции HUB или без функции IGMP SNOOPING, оборудование, подключенное для приема многоадресных данных, под многими из текущего оборудования. Устройство отправляет Leave, что может повлиять на другие устройства и не может принимать потоки данных многоадресной рассылки. Механизм Fast-leave-timeout может предотвратить возникновение этой ситуации, благодаря конфигурации Fast-leave-timeout левого времени ожидания, пакеты портового выхода, полученные после ожидания Fast-leave-timeout длительное время, а затем удаленные из многоадресной группы, к которой он принадлежит, чтобы гарантировать непрерывность сетевого многоадресного потока.

13.1.2 Динамическая многоадресная рассылка второго уровня

Записи MAC-адресов многоадресной рассылки в двухуровневой аппаратной таблице многоадресной рассылки могут быть динамически изучены IGMP SNOOPING. MAC-адрес IP-мультикаста динамически узнается через IGMP SNOOPING.
При выключении IGMP SNOOPING, два слоя аппаратной многоадресной пересылки таблицы в незарегистрированном режиме пересылки, многоадресной MAC-адрес не может быть динамически изучен, что два слоя аппаратной многоадресной пересылки таблицы без записей, два слоя многоадресной поток данных, как все широковещательной обработки.
В целях эффективного контроля многоадресной сети трафика, коммутатор может открыть IGMP SNOOPING, два слоя аппаратных многоадресной пересылки таблицы в режиме регистрации пересылки, коммутатор может узнать многоадресной MAC-адрес через сеть мониторинга по протоколу IGMP, и два слоя аппаратных многоадресной пересылки записей в таблице, два слоя многоадресной, чтобы иметь возможность потока вперед.

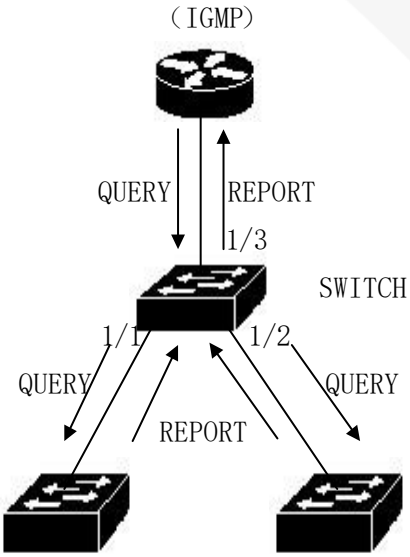
13.1.3 Присоединение к группе

Когда хост хочет присоединиться к многоадресной группе, он отправляет пакет IGMP REPORT, в котором указывается многоадресная группа, к которой он хочет присоединиться. Когда коммутатор получает пакет IGMP QUERY, пересылка пакетов будет переключена на ту же VLAN, что и все остальные порты, когда пакет IGMP QUERY будет переключен на VLAN.
Пакет IGMP QUERY принимается портом для присоединения к многоадресной группе после того, как хост возвращает пакет IGMP REPORT. Когда принимается пакет IGMP REPORT, создается двухуровневая многоадресная запись, а порт пакета IGMP QUERY и порт пакета IGMP REPORT добавляются к двухуровневому многоадресному элементу, чтобы стать его выходным портом.



Если все устройства на рисунке находятся в подсети, предположим, что VLAN подсети равна 2. Маршрутизатор работает по протоколу IGMPv2 и регулярно отправляет пакеты IGMP QUERY. Хост 1 хочет присоединиться к группе многоадресной рассылки 224.1.1.1. После получения пакета IGMP QUERY с порта 1/3 коммутатор запишет порт и перенаправит пакет на порты 1/1 и 1/2. Узел 1 отправляет пакет IGMP REPORT после получения пакета IGMP QUERY, а узел 2 не отправляет пакеты IGMP REPORT, поскольку не хочет присоединяться к группе многоадресной рассылки. После получения пакета IGMP REPORT с порта 1/1 коммутатор пересылает пакет с порта запроса 1/3 и создает элемент многоадресной рассылки второго уровня (при условии, что элемент не существует). Запись многоадресной рассылки второго уровня включает следующие элементы:

Адрес многоадресной рассылки второго уровня	VLAN ID	Список выходных портов
01:00:5e:01:01:01	2	1/1, 1/3



Как показано на рисунке 1, узел 1 добавил группу многоадресной рассылки 224.1.1.1, и теперь хост 2 хочет присоединиться к группе многоадресной рассылки 224.1.1.1. Когда хост 2 получил пакет IGMP QUERY после отправки обратно пакетного коммутатора IGMP REPORT, полученный с порта 1/2, поместит пакет из переадресованного порта запроса 1/3 и сделает порт 1/2 добавленным к двухуровневой многоадресной записи, запись в двухуровневую многоадресную рассылку:

Адрес многоадресной рассылки второго уровня	VLAN ID	Список выходных портов
01:00:5e:01:01:01	2	1/1, 1/2, 1/3

13.1.4 Выход из группы

Чтобы иметь возможность формировать стабильную многоадресную среду, устройства IGMP (например, маршрутизаторы) отправляют пакет IGMP QUERY на все хосты через регулярные промежутки времени. Узел, присоединившийся к группе многоадресной рассылки или желающий присоединиться к группе многоадресной рассылки, возвращает отчет IGMP после получения запроса IGMP.

Если хост хочет покинуть группу многоадресной рассылки, есть два способа: активный выход и пассивный выход. Активное выход- это то, что хост отправляет пакет IGMP LEAVE маршрутизатору, а пассивный выход - это когда хост получает запрос IGMP, отправленный маршрутизатором, и не отправляет обратно отчет IGMP.

Когда хост покидает группу многоадресной рассылки, есть два способа отключить многоадресную рассылку второго уровня на коммутаторе: оставить вне времени и получить пакет IGMP LEAVE. При переключении в течение определенного времени с одного порта на прием IGMP REPORT группы многоадресной рассылки, порт должен быть удален из соответствующей многоадресной записи второго уровня, если многоадресные записи без порта, удалите многоадресные записи второго уровня.

Если коммутатор fast-leave настроен как ENABLE, если порт получает пакет IGMP LEAVE многоадресной группы, очистите порт от соответствующей многоадресной записи многоадресной рассылки второго уровня, если у многоадресной рассылки нет порта записи, удалите записи многоадресной рассылки второго уровня.

Быстрый отпуск, как правило, используется одним хостом в порту в данных обстоятельствах; Если порт находится под несколькими узлами, можно настроить время ожидания быстрого ожидания времени ожидания, чтобы обеспечить непрерывность и надежность потока многоадресной рассылки.

13.2 Конфигурация IGMP SNOOPING

13.2.1 Конфигурация IGMP SNOOPING по умолчанию

- IGMP SNOOPING по умолчанию закрыт, а двухуровневая аппаратная таблица многоадресной пересылки находится в режиме незарегистрированной пересылки.
- Fast-leave по умолчанию закрыт.
- Fast-leave-timeout time составляет 300 секунд.
- Возраст порта REPORT группы многоадресной рассылки по умолчанию равен 400 секундам.
- Возраст порта QUERY группы многоадресной рассылки по умолчанию равен 300 секундам.

13.2.2 Открытие и закрытие IGMP SNOOPING

Открыть протокол IGMP SNOOPING можно глобально, также можно открыть часть VLAN; для открытия или закрытия VLAN IGMP SNOOPING используется только глобальное открытие IGMP SNOOPING.

Открыть глобальный IGMP SNOOPING

```
Switch#configure terminal
Switch(config)#ip igmp snooping
```

Открытие VLAN IGMP SNOOPING

```
Switch#configure terminal
Switch(config)#ip igmp snooping vlan <vlan-id>
```

Закрыть глобальный IGMP SNOOPING

```
Switch#configure terminal
Switch(config)#no ip igmp snooping
```

Закрытие VLAN IGMP SNOOPING

```
Switch#configure terminal
Switch(config)#no ip igmp snooping vlan <vlan-id>
```

13.2.3 Время жизни конфигурации

Настройка времени жизни групп многоадресной рассылки

```
Switch#configure terminal
Switch(config)#ip igmp snooping group-membership-timeout <interval> vlan <vlan-id>
```

Единицей измерения интервала являются миллисекунды.

Время существования групп запросов конфигурации

```
Switch#configure terminal
Switch(config)#ip igmp snooping query-membership-timeout <interval> vlan <vlan-id>
```

Единицей измерения интервала являются миллисекунды.

13.2.4 Конфигурация fast-leave

Быстрый выход из VLAN

```
Switch#configure terminal
```

Switch(config)#ip igmp snooping fast-leave vlan <vlan-id>

Закрыть быстрый отпуск

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave vlan <vlan-id>

Настройка времени ожидания fast-leave

Switch#configure terminal

Switch(config)# ip igmp snooping fast-leave-timeout <interval> vlan <vlan-id>

Время ожидания быстрого выхода из системы восстановления по умолчанию

Switch#configure terminal

Switch(config)#no ip igmp snooping fast-leave-timeout vlan <vlan-id>

13.2.5 Конфигурация MROUTER

Настройка статического порта запроса

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ip igmp snooping mrouter vlan [vlan-id]

13.2.6 Отображение информации

Отображение информации о конфигурации IGMP SNOOPING

Switch#show ip igmp snooping

Отображает сведения о конфигурации для VLAN

Switch#show ip igmp snooping vlan <vlan-id>

Отображение информации о старении многоадресной группы REPORT

Switch#show ip igmp snooping age-table group-membership

Отображение информации о старении QUERY

Switch#show ip igmp snooping age-table query-membership

Отображение информации о пересылке группы многоадресной рассылки

Switch#show ip igmp snooping forwarding-table

Отображение информации MROUTER

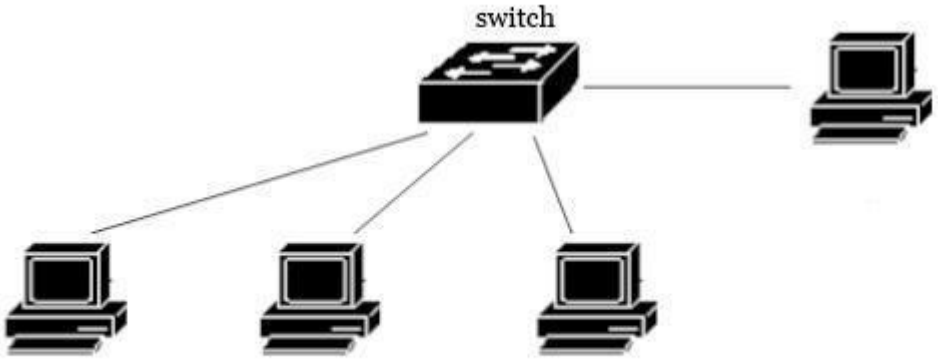
Switch#show ip igmp snooping mrouter

Настройка системы отображения, включая конфигурацию IGMP SNOOPING

Switch#show running-config

13.3 Пример конфигурации IGMP SNOOPING

Функция IGMP SNOOPING включена на коммутаторе. Пользователь 1, пользователь 2 и пользователь 3 могут быть добавлены в определенную группу многоадресной рассылки.




```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config)#ip igmp snooping
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ip igmp snooping group-membership-timeout 60000 vlan 200
```

Четырнадцатая глава

Конфигурация MVR

Основное содержание этой главы заключается в следующем:

- Профиль MVR
- Конфигурация MVR
- Пример конфигурации MVR

14.1 Профиль MVR

Многоадресная регистрация VLAN (MVR) применяется к многоадресным потоковым приложениям в сетях поставщиков услуг, таких как vod. MVR позволяет пользователям подписываться или отменять потоки многоадресной рассылки в рамках многоадресной VLAN, позволяя многоадресной VLAN совместно использовать потоки данных с другими VLAN. MVR имеет две цели: (1) благодаря простой настройке он может эффективно и безопасно передавать потоки многоадресной рассылки между VLAN; (2) поддержка групп многоадресной рассылки, динамически присоединяющихся и покидающих их;

MVR похож на отслеживание IGMP в том, что две функции могут быть запущены одновременно, MVR обрабатывает только присоединение и выход настроенных групп многоадресной рассылки, а другие группы присоединяются и уходят с помощью управления отслеживанием IGMP. Разница между ними заключается в том, что потоки многоадресной рассылки в отслеживании IGMP могут быть перенаправлены только в пределах одной VLAN, в то время как потоки многоадресной рассылки MVR могут быть перенаправлены в разные VLAN.

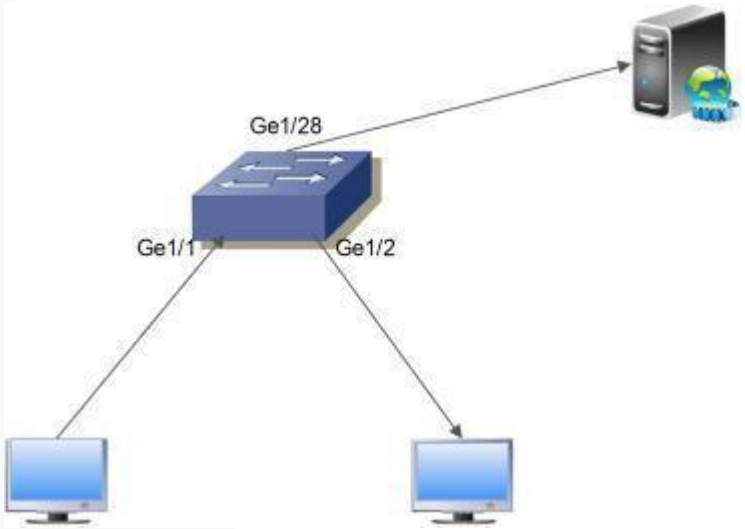
14.2 Конфигурация MVR

Команда	Описание	Режим CLI
mvr (enable|disable)	Запуск глобального MVR	Режим глобального конфигурирования
no mvr	Очистка всех конфигураций MVR	Режим глобального конфигурирования
mvr group A.B.C.D	Настройка IP-адреса многоадресной рассылки	Режим глобального конфигурирования
no mvr group A.B.C.D	Удаление IP-адреса многоадресной рассылки	Режим глобального конфигурирования
mvr group A.B.C.D <1-256>	Настройка IP-адреса многоадресной рассылки и непрерывный адрес группы MVR	Режим глобального конфигурирования
mvr vlan <1-4094>	Указывает VLAN для получения многоадресных данных	Режим глобального конфигурирования
no mvr vlan	Восстановление VLAN 1 по умолчанию для получения многоадресных данных	Режим глобального конфигурирования

mvr-interface (enable|disable)	Загрузочный интерфейс MVR	Режим конфигурирования интерфейса
show mvr	Отображение информации о конфигурации MVR	Привилегированный режим

14.3 Пример конфигурации MVR

Топология сети, как показано ниже, пользователь 1 и пользователь 2 принадлежат vlan10 vlan20 соответственно, пользователь 1 и пользователь 2 видят одну и ту же программу, программный диапазон 225.1.1.1 ~ 225.1.1.64, MVR VLAN составляет 100:



Настройка VLAN, запуск глобального отслеживания IGMP, настройка MVR VLAN, диапазон групп программ MVR, глобальное включение MVR:

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)# mvr enable
Switch(config)#mvr vlan 100
Switch(config)#mvr group 225.1.1.1 64
Switch#
```

Настройте пользовательский порт коммутатора Ge1/1 Ge1/2 и восходящего канала Ge1/28:

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode hybrid
Switch(config-ge1/1)#switchport hybrid allowed vlan add 10 egress-tagged disable
Switch(config-ge1/1)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/1)#mvr enable Switch(config-ge1/1)#
Switch#configure terminal
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode hybrid
Switch(config-ge1/2)#switchport hybrid allowed vlan add 20 egress-tagged disable
Switch(config-ge1/2)#switchport hybrid allowed vlan add 100 egress-tagged disable
Switch(config-ge1/2)#mvr enable Switch(config-ge1/2)#
Switch#configure terminal
```

```
Switch(config)#interface ge1/28
Switch(config-ge1/28)#switchport mode trunk
Switch(config-ge1/28)#switchport trunk allowed vlan add 100
Switch(config-ge1/28)#
```

Пятнадцатая глава

Конфигурация DHCP SNOOPING

В сетевой среде динамического доступа узел получает IP-адрес и параметр сети через DHCP-сервер. DHCP SNOOPING - это своего рода протокол перехвата для ARP-атаки. Прослушивая сообщение DHCP, динамически привязывается DHCP-сервер к IP-адресу клиента и MAC-адресу клиента, чтобы отфильтровать сообщение ARP-атаки на коммутаторе.

Коммутатор поддерживает функцию DHCP SNOOPING, может эффективно защищать ARP-атаку. DHCP SNOOPING прослушивает сообщение DHCP в сети и связывает информацию о порте ARP.

Можно настроить четыре соединения с физическими портами DHCP-сервера, в некоторой степени, чтобы предотвратить помехи неизвестных сетей сервера.

При перезапуске выключенного питания таблица привязки будет потеряна и нуждается в повторном изучении; коммутатор обеспечивает функцию загрузки и загрузки таблиц привязки, а таблица привязки может храниться на TFTP-сервере.

В этой главе описывается концепция и конфигурация DHCP SNOOPING, включая следующее содержание:

- Вступление в DHCP SNOOPING
- Конфигурация DHCP SNOOPING
- Пример конфигурации DHCP SNOOPING
- Ошибки в конфигурации DHCP SNOOPING

15.1 Введение в DHCP SNOOPING

Из-за простого механизма доверия протокол ARP вызвал лазейку в сетевой безопасности. Когда сообщение ARP-атаки, несущее ложное сообщение MAC, поступает на хост, оно переопределяет локальную таблицу кэша ARP напрямую без ограничений, что приводит к нормальному потоку данных для злоумышленника. Таким образом, ARP-привязка портов может быть реализована на сетевом коммутаторе второго уровня, что может эффективно фильтровать пакеты ARP-атак и делать пакеты атаки недоступными для доступа к хосту атаки. Если сеть не предусмотрена в DHCP-сервере, распределение IP-адресов приведет к путанице, протокол DHCP SNOOPING предоставляет физический порт привязки к канальному серверу, физический порт не может быть не указан DHCP-сервером, пересылаемым DHCP-пакеты, может уменьшить возможность доступа неизвестного сервер в сеть.

Основное содержание этого раздела заключается в следующем:

- Обработка DHCP SNOOPING
- Таблица привязки DHCP SNOOPING
- Указание физического порта связанного сервера DHCP SNOOPING
- Загрузка и скачивание списка привязок DHCP SNOOPING

15.1.1 Обработка DHCP SNOOPING

Протокол DHCP SNOOPING слушает только сообщения DHCPrequest, DHCPack, DHCPrelease трех типов, не принимает другие типы пакетов DHCP и связывает отношения отображения между IP и MAC в соответствии с этими сообщениями.

Глобальный DHCP SNOOPING на коммутаторе отвечает за открытие коммутатора для приема пакетов DHCP, т.е. UDP портов 67 и 68 IP пакетов.

15.1.2 Таблица привязки DHCP SNOOPING

Записи таблицы привязки DHCP SNOOPING индексируются по MAC-адресу, включая тип элемента, IP-адрес, MAC-адрес, информацию об интерфейсе, таймер задержки, таймер аренды. Тип REQ и ACK в двух, тип записи REQ указывает, что сообщение DHCPrequest получено, DHCPack еще не получил сообщение, затем таймер задержки запуска, интервал времени по умолчанию составляет 10 секунд, 10 секунд, если он не получает сообщение DHCPack, записи таблицы привязки типа REQ удаляются; Запись типа ACK указывает, что сообщение DHCPack получено и записано, что IP-серверу назначен IP-адрес, затем запускается таймер аренды, интервал времени включается в сообщение DHCPack DHCP-сервер предоставляет значение договора аренды, таймер перезапускается, срок аренды истекает, записи таблицы привязки удаляются. Информация об интерфейсе записывает интерфейс, в котором находится клиент, то есть интерфейс между IP-адресом и привязкой MAC-адреса.

При получении сообщения DHCPrequest создаются записи таблицы привязки, тип записей — REQ, IP-адрес, MAC-адрес, информация об интерфейсе и 10-секундный таймер задержки.

При получении сообщения DHCPrequest записи таблицы привязки типа REQ уже существуют, записи обновляются, а таймеры задержки перезапускаются.

При получении сообщения DHCPrequest запись таблицы привязки типа ACK уже существует, после чего записывается информация об интерфейсе.

При получении сообщения DHCPack, если есть запись таблицы привязки типа REQ, записывается IP-адрес, выделенный сервером в сообщении DHCPack, таймер задержки закрывается и запускается таймер аренды.

При получении сообщения DHCPack запись таблицы привязки типа REQ отсутствует, после чего сообщение отбрасывается.

При получении пакетов DHCPack записи таблицы привязки типа ACK уже существуют. Если интерфейс изменился, записи таблицы привязки исходного интерфейса удаляются, а записи обновляются.

Если интерфейс не изменяется, IP-адрес, назначенный сервером, изменяется, удаляя записи таблицы привязки исходного интерфейса и обновляя записи.

Если интерфейс не меняется, IP-адрес не меняется, что указывает на то, что процесс продления, перезапуск таймера аренды может быть.

По истечении времени ожидания записи таблицы привязки типа REQ удаляются.

При истечении времени ожидания таймера аренды записи таблицы привязки типа ACK удаляются.

15.1.3 Указание физического порта связанного сервера DHCP SNOOPING

DHCP SNOOPING указывает физический порт связанного сервера, и сообщение DHCP может быть получено только на указанный порт. Если в сети несколько DHCP-серверов, предложение, предоставляемое сервером с неуказанного порта, будет отфильтровано, и IP-адрес не сможет быть назначен клиенту. Назначенные порты способствуют унифицированному распределению IP-адресов в сети, во избежание неизвестного пула адресов серверов не входящих в IP-планирование, некоторые клиенты не смогут нормально подключаться к сети. В некоторой степени это снижает вероятность аномалий сетевой связи, вызванных несанкционированным доступом к серверу.

15.1.4 Загрузка и скачивание списка привязок DHCP SNOOPING

DHCP SNOOPING записывает связь привязки между IP и MAC, отслеживая сообщение DHCP, и поддерживает его таблицу привязки. Когда коммутатор выключен, происходит перезапуск или неисправность, таблица привязки будет потеряна при неожиданном отключении питания, и коммутатору необходимо изучить записи таблицы привязки после перезапуска. В топологии сети трудно определить прерывание сетевого подключения и перезапустить процесс обнаружения DHCP, если хост не подключен напрямую, и коммутатору будет трудно повторно изучить информацию о привязке. По этой причине таблица привязки сохраняется на TFTP-сервере, а таблица привязки загружается после перезапуска коммутатора, что может устранить временный пробел в памяти при перезапуске коммутатора.Коммутатор обеспечивает функцию загрузки и скачивания таблицы привязки, администратор может вручную загружать или скачивать таблицы привязки, может автоматически загружать команды конфигурации, загружать таблицу привязки; команда таблицы привязки в процессе запуска с TFTP-сервера для загрузки резервного файла и таблицы привязки имеет таблицу привязки в модуль протокола DHCP SNOOPING автоматически может перезапустить загрузку.

15.2 Конфигурация DHCP SNOOPING

15.2.1 Конфигурация по умолчанию DHCP SNOOPING

По умолчанию DHCP SNOOPING закрыт.

Привязка таблицы DHCP SNOOPING типа REQ задержка записи таймер по умолчанию составляет 10 секунд.

15.2.2 Глобальное открытие и закрытие DHCP SNOOPING

Когда DHCP SNOOPING открыт глобально, DHCP SNOOPING интерфейса может быть включен или выключен, а DHCP SNOOPING всех интерфейсов должен быть отключен, прежде чем глобальный DHCP SNOOPING сможет быть отключен.

Открытие глобального отслеживания DHCP

```
Switch#configure terminal
Switch(config)#ip dhcp snooping [IF_LIST]
```

Параметр представляет собой список физических портов связанного DHCP-сервера, который необходимо привязать. Всего можно указать четыре порта, а список портов разделен на "", "ge1/1", "ge1/25", "ge1/26"

Закрытие глобального отслеживания DHCP

```
Switch#configure terminal
Switch(config)#no ip dhcp snooping
```

15.2.3 Открытие и закрытие интерфейса DHCP SNOOPING

Открытие интерфейса для DHCP SNOOPING

Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping

Отслеживание DHCP, закрывающего интерфейс

Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#no dhcp snooping

15.2.4 Загрузка и скачивание список привязок DHCP SNOOPING

Загрузка таблицы привязки DHCP SNOOPING на TFTP-сервер

Switch#configure terminal
Switch(config)#dhcp snooping upload A.B.C.D FILE_NAME

Параметры: IP-адрес TFTP-сервера A.B.C.D; имя файла таблицы привязки, который сохраняется на TFTP-сервере по FILE_NAME.

Загрузите таблицу привязки DHCP SNOOPING с TFTP-сервера

Switch#configure terminal
Switch(config)#dhcp snooping download A.B.C.D FILE_NAME

Настройка загрузки таблицы привязки DHCP SNOOPING на сервер TFTP по таймеру

Switch#configure terminal
Switch(config)#dhcp snooping auto-upload A.B.C.D FILE_NAME interval

Параметры: интервал время интервала загрузки, в диапазоне от 1 минуты до одного дня.

Регулярная отмена конфигурации таблицы привязки DHCP SNOOPING на TFTP-сервере

Switch#configure terminal
Switch(config)#no dhcp snooping auto-upload

Автоматическая загрузка таблицы привязки DHCP SNOOPING с сервера TFTP при перезагрузке конфигурации

Switch#configure terminal
Switch(config)#dhcp snooping reset-download A.B.C.D FILE_NAME

Автоматически настройте конфигурацию таблицы привязки DHCP SNOOPING от TFTP-сервер при отмене перезапуска

Switch#configure terminal
Switch(config)#no dhcp snooping reset-download

15.2.5 Отображение информации

Отображение информации о конфигурации DHCP SNOOPING

Switch#show dhcp snooping

Отображение информации таблицы привязки DHCP SNOOPING Switch#show dhcp snooping binding-table

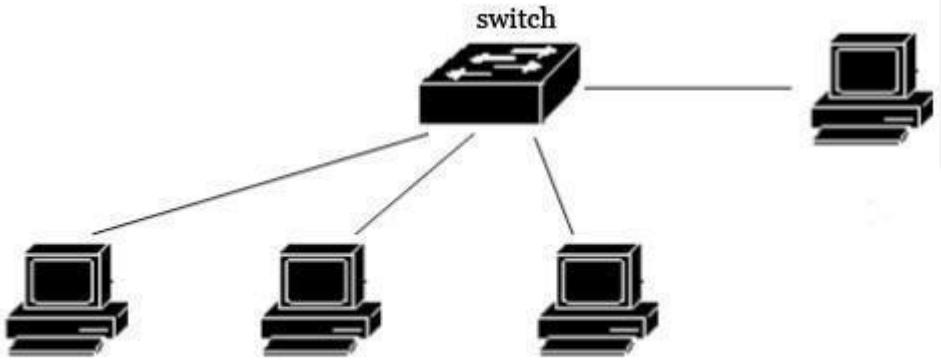
В настоящее время система отображения настроена, включая конфигурацию DHCP SNOOPING.

Switch#show running-config

15.3 Пример конфигурации DHCP SNOOPING

15.3.1 Конфигурация

Функция DHCP SNOOPING включена на коммутаторе уровня 2. И пользователь 1, пользователь 2 и пользователь 3 получают IP-адрес и сетевые параметры динамически через DHCP-сервер. Пользователь 1, пользователь 2, пользователь 3 интерфейс запускают функцию DHCP SNOOPING, динамически связывая информацию ARP в интерфейсе.




```
Switch#configure terminal
Switch(config)#ip dhcp snooping ge1/9
Switch(config)#interface ge1/1
Switch(config-ge1/1)#dhcp snooping
Switch(config-ge1/1)#interface ge1/2
Switch(config-ge1/2)#dhcp snooping
Switch(config-ge1/2)#interface ge1/3
Switch(config-ge1/3)#dhcp snooping
Switch(config-ge1/3)#end
Switch#show dhcp snooping
Отслеживание DHCP включено глобально
Интерфейс DHCP-сервера:ge1/9
Включить интерфейс: ge1/1 ge1/2 ge1/3
Switch#show dhcp snooping binding-table
```

IP	MAC	FLAG	PORT	LEASE
192.168.1.100	00:11:5b:34:42:ad	ACK	ge1/1	23:59:58
192.168.1.101	00:11:64:52:13:5d	ACK	ge1/2	23:50:01
192.168.1.102	00:11:80:4d:a2:46	ACK	ge1/3	20:34:45

```
Switch#show running-config
!
ip dhcp snooping ge1/9
!
spanning-tree mst configuration
```

```
!
interface vlan1 Ip address 192.168.0.1/24
!
interface ge1/1 dhcp snooping
!
interface 1/2 dhcp snooping
!
interface 1/3 dhcp snooping
!
line vty
!
End
```

15.4 Ошибки в конфигурации DHCP SNOOPING

Если конфигурация отслеживания DHCP завершается сбоем, это может быть вызвано следующими причинами:

1. Исчерпание ресурсов системы CFP.
2. Если интерфейс настроен, функция фильтрации ACL не может глобально открыть DHCP SNOOPING.
3. Если интерфейс настроен с привязкой IP к MAC, глобальный открытый DHCP SNOOPING завершается ошибкой.
4. Текущий интерфейс настроен с функцией фильтра ACL.
5. Текущий интерфейс позволяет 802.1x анти-ARP спуфинг.
6. Сконфигурированный интерфейс представляет собой трехслойный интерфейс или магистральный интерфейс.

Шестнадцатая глава

Конфигурация MLD SNOOPING

В столичной вычислительной сети /Internet использование одноадресной рассылки отправляет один и тот же пакет в сеть у многих, но не у всех получателей, из-за необходимости копировать каждый пакет в принимающую конечную точку, с увеличением числа приемников, количество пакетов потребует линейного увеличения, что заставляет хост, обмениваться общей нагрузкой на маршрутизирующее оборудование и увеличивать пропускную способность сети, это сильно влияет на эффективность. С ростом спроса на многоточечные видеоконференции, видео по запросу и приложения групповой связи, многоадресная рассылка стала самым популярным способом общения с целью улучшения использования ресурсов.
Коммутатор реализует функцию MLD SNOOPING для службы многоадресных приложений. MLD SNOOPING отслеживает пакеты MLD в сети для реализации динамического обучения многоадресных MAC-адресов IPV6.
В этой главе описывается концепция и конфигурация MLD SNOOPING, включая следующее содержание:

- Введение в MLD SNOOPING
- Конфигурация MLD SNOOPING
- Пример конфигурации MLD SNOOPING

16.1 Введение в MLD SNOOPING

Традиционная сеть из подсети многоадресных пакетов, как широковещательная обработка, легко генерирует сетевой трафик, вызывая перегрузку сети. Когда коммутатор реализован на MLD SNOOPING, MLD SNOOPING может узнать динамический многоадресный MAC-адрес IPV6, чтобы поддерживать список выходных портов IPV6 многоадресный MAC-адрес, может передавать многоадресный поток данных только на выходной порт, это уменьшает сетевой трафик.
Основное содержание этого раздела заключается в следующем:

- Обработка MLD SNOOPING
- Динамическая многоадресная рассылка второго уровня
- Присоединение к группе
- Выход из группы

16.1.1 Обработка MLD SNOOPING

MLD SNOOPING - это сетевой протокол второго уровня, пакет протокола MLD через мониторинг коммутатора, в соответствии с принимающим портом эти пакеты протоколов MLD, идентификатор VLAN и адрес многоадресной рассылки для поддержки группы многоадресной рассылки, а затем пересылается эти протоколы MLD. Для приема потоков многоадресных данных можно добавлять только порты многоадресной рассылки; таким образом, снижается сетевой трафик и сохраняется пропускная способность сети.
Группа многоадресной рассылки включает адрес группы многоадресной рассылки, порт участника, идентификатор VLAN, возрастное время.

Формирование многоадресной группы MLD SNOOPING является обучаемым процессом. Когда один порт коммутатора получает пакет MLD REPORT, MLD SNOOPING создает новую многоадресную группу, а порт, принимающий пакет MLD REPORT, добавляется в группу многоадресной рассылки. Когда пакет MLD QUERY принимается коммутатором, если группа многоадресной рассылки уже существует в коммутаторе, то порт, получивший ЗАПРОС MLD, добавляется в группу многоадресной рассылки, в противном случае он будет пересылать только пакет MLD QUERY.

Done SNOOPING также поддерживает механизм MLD V2 MLD SNOOPING; если при конфигурации fast-leave ENABLE в MLD V2, полученный done пакет при его получении порта может покинуть многоадресную группу немедленно; Если конфигурация fast-leave оставила время ожидания (fast-leave-timeout), то время многоадресной рассылки, которую ожидает этого группа , истекает после выхода из группы многоадресной рассылки.

Существует два механизма обновления для MLD SNOOPING. Одним из них является механизм Done, описанный выше. В большинстве случаев MLD SNOOPING удаляет просроченные многоадресные группы по возрасту. Когда группа многоадресной рассылки присоединяется к MLD SNOOPING, записывается добавленное время. Если группа многоадресной рассылки имеет более одного настроенного времени возраста в коммутаторе, возможность обмена удаляет группу многоадресной рассылки.

Когда порт принимает пакеты Done, этот порт будет немедленно удален из многоадресной группы, к которой он принадлежит, такая ситуация может повлиять на непрерывность сетевого потока данных; поскольку этот порт сетевого оборудования ниже может быть подключен к функции HUB или без функции SNOOPING MLD, оборудование подключено для приема многоадресных данных под многим текущим оборудованием. Устройство отправляет Done, что может повлиять на другие устройства и оно не может принимать потоки многоадресных данных. Механизм Fast-leave-timeout может предотвратить возникновение этой ситуации, благодаря конфигурации Fast-leave-timeout левого времени ожидания, пакеты портового выхода, полученные после ожидания Fast-leave-timeout длительное время, а затем удаленные из многоадресной группы, к которой он принадлежит, чтобы гарантировать непрерывность сетевого многоадресного потока.

16.1.2 Динамическая многоадресная рассылка второго уровня

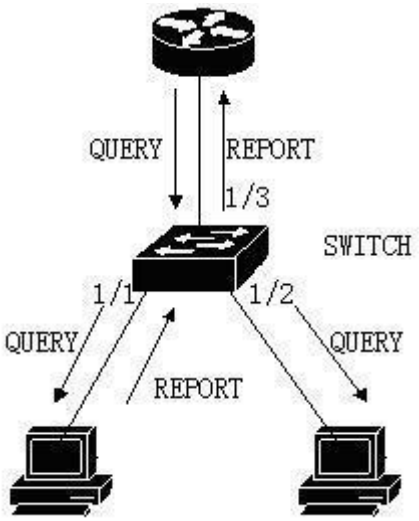
Записи многоадресных MAC-адресов второго уровня аппаратной таблице пересылки многоадресной рассылки могут динамически изучаться MLD SNOOPING. MAC-адрес многоадресной рассылки IPV6 динамически изучается с помощью MLD SNOOPING.

При отключении MLD SNOOPING, двухуровневой аппаратной таблицы многоадресной пересылки в режиме незарегистрированной пересылки, многоадресный MAC-адрес не может быть динамически изучен, что двухуровневая аппаратная таблица пересылки без записей, многоадресный поток данных второго уровня как вся широковещательная обработка.

Когда сетевая многоадресная среда, чтобы эффективно управлять сетью многоадресного трафика, коммутатор может открыть MLD SNOOPING, двухуровневую аппаратную таблицу многоадресной пересылки в режиме переадресации регистров, коммутатор может научиться многоадресному MAC-адресу через сеть мониторинга по протоколу MLD, а двухуровневую аппаратную многоадресную пересылку записей в таблице, многоадресная рассылка второго уровня, чтобы иметь возможность двигаться вперед.

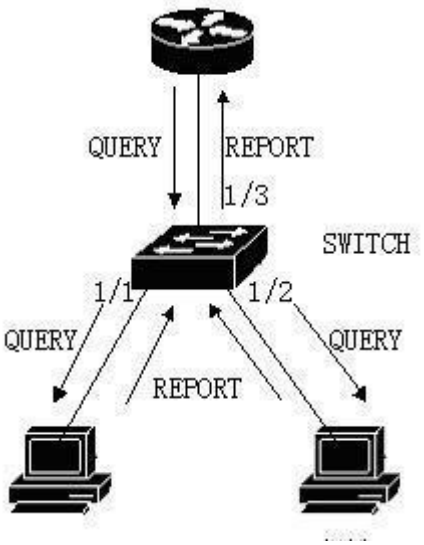
16.1.3 Присоединение к группе

Когда узел хочет присоединиться к группе многоадресной рассылки, он отправляет пакет MLD REPORT, в котором указывается группа многоадресной рассылки, к которой должен присоединиться узел. Когда коммутатор получает пакет MLD QUERY, пересылка пакетов переключается на ту же VLAN все остальные порты, когда пакет MLD QUERY принимается через порт для присоединения к группе многоадресной рассылки после того, как узел вернет пакет MLD REPORT. При получении пакета MLD REPORT устанавливается двухуровневая многоадресная запись, а порт пакета MLD QUERY и порт пакета MLD REPORT добавляются к двухуровневому элементу многоадресной рассылки, чтобы стать его выходным портом.



Если все устройства на рисунке находятся в подсети, предположим, что VLAN подсети равна 2. Маршрутизатор работает по протоколу MLDv2 и регулярно отправляет пакеты MLD QUERY. Узел 1 хочет присоединиться к группе многоадресной рассылки ff15:: 1. После получения пакета MLD QUERY с порта 1/3 коммутатор запишет порт и перенаправит пакет на порты 1/1 и 1/2. Узел 1 отправляет пакет MLD REPORT после получения пакета MLD QUERY, а узел 2 не отправляет пакеты MLD REPORT, поскольку не хочет присоединяться к группе многоадресной рассылки. После получения пакета MLD REPORT с порта 1/1 коммутатор пересылает пакет с порта запроса 1/3 и создает элемент второго уровня многоадресной рассылки (при условии, что элемент не существует). Запись многоадресной рассылки второго уровня включает следующие элементы:

Адрес многоадресной рассылки второго уровня	VLAN ID	Список выходных портов
33:33:00:00:00:01	2	1/1, 1/3



Как показано на рисунке 1, хост 1 добавил многоадресную группу ff15:: 1, и теперь хост 2 хочет присоединиться к многоадресной группе ff15:: 1. Когда хост 2 получил пакет MLD QUERY после отправки обратно пакета MLD REPORT, коммутатор MLD REPORT, полученный от порта 1/2, помещает пакет от порта 1/3 и пересылает пакет запроса порту 1/2 был добавлен в двухуровневую многоадресную запись, запись в двухуровневую многоадресную рассылку:

Адрес многоадресной рассылки второго уровня	VLAN ID	Список выходных портов
33:33:5e:00:00:01	2	1/1, 1/2, 1/3

16.1.4 Выход из группы

Чтобы иметь возможность сформировать стабильную многоадресную среду, устройства MLD (такие как маршрутизаторы) отправляют пакет MLD QUERY на все хосты через регулярные промежутки времени. Узел, присоединившийся к группе многоадресной рассылки или желающий присоединиться к группе многоадресной рассылки, возвращает MLD REPORT после получения запроса MLD.

Если хост хочет покинуть группу многоадресной рассылки, есть два способа: активный выход и пассивный выход. Активное выход - это когда хост отправляет пакет MLD LEAVE маршрутизатору, а пассивный выход - это когда хост получает запрос MLD, отправленный маршрутизатором, и не отправляет обратно MLD REPORT.

Когда хост покидает группу многоадресной рассылки, есть два способа отключить многоадресную рассылку второго уровня на коммутаторе: оставить вне времени и получить пакет MLD DONE.

При переключении в течение определенного времени с одного порта на прием многоадресной группы MLD REPORT пакета, порт следует удалить из соответствующей многоадресной записи второго уровня, если многоадресные записи без порта, удалите многоадресную запись.

Если коммутатор fast-leave настроен как ENABLE, если порт получает пакет MLD LEAVE группы многоадресной рассылки, очистите порт от соответствующей многоадресной записи второго уровня, если у многоадресной рассылки нет порта записи удалите записи многоадресной рассылки второго уровня.

Fast-leave , как правило, используется одним хостом в порту в данных обстоятельствах; Если порт находится под несколькими узлами, можно настроить fast-leave-timeout, чтобы обеспечить непрерывность и надежность потока многоадресной рассылки.

16.2 Конфигурация MLD SNOOPING

16.2.1 Конфигурация MLD SNOOPING по умолчанию

- По умолчанию MLD SNOOPING закрыт, а аппаратная таблица многоадресной пересылки второго уровня находится в режиме незарегистрированной пересылки.
- Fast-leave по умолчанию закрыт.
- Время Fast-leave-timeout составляет 300 секунд.
- Возраст порта REPORT группы многоадресной рассылки по умолчанию равен 400 секундам.
- Время жизни порта QUERY группы многоадресной рассылки по умолчанию равен 300 секундам.

16.2.2 Открытие и закрытие MLD SNOOPING

Открыть протокол MLD SNOOPING может быть глобально открытым, также можно открыть часть VLAN; только глобальное открытие MLD SNOOPING может использоваться для открытия или закрытия VLAN MLD SNOOPING.

Открытие глобального MLD SNOOPING

Switch#configure terminal
Switch(config)#ipv6 mld snooping

Открытие VLAN MLD SNOOPING

Switch#configure terminal
Switch(config)#ipv6 mld snooping vlan <vlan-id>

Закрыть глобальный MLD SNOOPING

Switch#configure terminal
Switch(config)#no ipv6 mld snooping

Закрытие VLAN MLD SNOOPING

Switch#configure terminal
Switch(config)#no ipv6 mld snooping vlan <vlan-id>

16.2.3 Время существования конфигурации

Настройка времени жизни групп многоадресной рассылки

Switch#configure terminal
Switch(config)#ipv6 mld snooping group-membership-timeout <interval> vlan <vlan-id> The unit of Interval is milliseconds.

Время существования групп запросов конфигурации

Switch#configure terminal
Switch(config)#ipv6 mld snooping query-membership-timeout <interval> vlan <vlan-id>

Единицей измерения интервала являются миллисекунды.

16.2.4 Конфигурация fast-leave

Быстрый уход из VLAN

Switch#configure terminal

Switch(config)#ipv6 mld snooping fast-leave vlan <vlan-id>

Закрытие fast-leave

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave vlan <vlan-id>

Конфигурация время ожидания fast-leave

Switch#configure terminal

Switch(config)# ipv6 mld snooping fast-leave-timeout <interval> vlan <vlan-id>

Время ожидания восстановления fast-leave по умолчанию

Switch#configure terminal

Switch(config)#no ipv6 mld snooping fast-leave-timeout vlan <vlan-id>

16.2.5 Конфигурация MROUTER

Настройка статического порта запроса

Switch#configure terminal

Switch#interface ge1/6

Switch(config-ge1/6)#ipv6 mld snooping mrouter vlan [vlan-id]

16.2.6 Отображение информации

Отображение информации о конфигурации MLD SNOOPING

Switch#show ipv6 mld snooping

Отображает сведения о конфигурации для VLAN

Switch#show ipv6 mld snooping vlan <vlan-id>

Отображение информации о старении многоадресной группы REPORT

Switch#show ipv6 mld snooping age-table group-membership

Отображение информации о старении QUERY

Switch#show ipv6 mld snooping age-table query-membership

Отображение информации о пересылке группы многоадресной рассылки

Switch#show ipv6 mld snooping forwarding-table

Отображение информации MROUTER

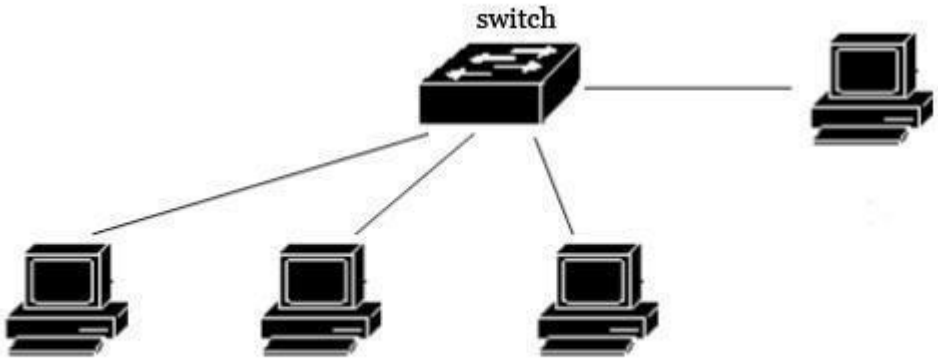
Switch#show ipv6 mld snooping mrouter

В настоящее время настроена система отображения, включая конфигурацию MLD SNOOPING

Switch#show running-config

16.3 Пример конфигурации MLD SNOOPING

Функция MLD SNOOPING включена на коммутаторе. Пользователь 1, пользователь 2 и пользователь 3 могут быть добавлены в определенную группу многоадресной рассылки.




```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 200
Switch(config)#ipv6 mld snooping
Switch(config)#interface ge1/1
Switch(config-ge1/1)#switchport mode access
Switch(config-ge1/1)#switchport access vlan 200
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 200
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport mode access
Switch(config-ge1/3)#switchport access vlan 200
Switch(config)#ipv6 mld snooping group-membership-timeout 60000 vlan 200
```

Семнадцатая глава

Конфигурация ACL

В реальной сети безопасность доступа к сети является заботой администратора. Коммутаторы поддерживают фильтрацию ACL для обеспечения безопасности доступа к сети. Настраивая правила ACL, коммутаторы фильтруют входной поток данных в соответствии с этими правилами для обеспечения безопасности доступа к сети.

В этой главе описывается, как настроить ACL, включая следующие:

- Введение в библиотеки ресурсов ACL
- Введение в фильтрацию ACL
- Конфигурация репозитория ACL
- ACL на основе временного интервала
- Конфигурация фильтрации ACL
- Пример конфигурации ACL
- Отладка конфигурации ACL

17.1 Введение библиотеки ресурсов ACL

Библиотека ресурсов ACL (Access Control List) представляет собой набор правил доступа для нескольких групп. Библиотека ресурсов ACL не управляет функцией пересылки данных, а только набором правил, отсортированных по конфликтам. При ссылке на библиотеку ресурсов ACL эти приложения контролируют пересылку данных в соответствии с правилами, предоставляемыми ресурсами ACL. ACL может применяться к фильтрации доступа к портам, фильтрации доступа к службам и QoS и т. д.

Группа ресурсов ACL (стандартные правила группы No 1 IP ~ 991300 ~ 1999), группа IP (группа No 100 правила расширения ~ 1992000 ~ 2699), IP-группа MAC группы ARP (700 ~ 799> <, группа 1100 ~ 1199); Каждая группа правил автоматически расставляет приоритеты по конфликтующим правилам. Когда пользователь настраивает правило ACL, система вставляет правило в соответствующее расположение в соответствии с параметрами сортировки.

В приложении, когда пакет данных проходит через порт, коммутатор будет сравнивать все поля, соответствующие каждому правилу в поле и в пакете данных; при полном соответствии правил, первое правило полностью действующее; с помощью этого правила сопоставления для определения данных пакет пересылается или отбрасывается. Так называемое идеальное соответствие заключается в том, что значение поля в правиле в точности равно значению соответствующего поля в пакете. Только если правило полностью соответствует списку управления доступом, оно может выполнять соответствующие операции запрета или разрешения.

В коммутаторах правила в пределах одной группы сортируются автоматически. Автоматическая сортировка правил относительно сложна. В процессе сортировки большой диапазон правил отстает, а небольшой диапазон впереди. Сфера применения правила определяется ограничивающим условием правила; чем меньше условие ограничения правила, тем больше диапазон соответствия правила; чем больше ограничений правила, тем меньше диапазон соответствия правил.

Правила ограничения в основном воплощены в количестве подстановочных адресов и некоторых неадресных полей. Подстановочный знак — это битовая строка. IP-адрес — четыре байта, а MAC-

адрес — шесть байт. Биты ' 1 'означает отсутствие соответствия, а биты ' 0' означает соответствие. Неадресные поля относятся к типам протоколов, типам ip-протоколов, портам протоколов, и эти поля также скрывают подстановочный знак. Их длина — это длина байта соответствующего поля, поэтому одна и та же длина поля равномерна, просто считая количество полей. Чем больше бит wildcard ' 0 ', тем больше ограничений.

На примере фильтрации доступа к портам проиллюстрирована необходимость ранжирования по правилам и преимущества автоматической сортировки. Если пользователю необходимо отклонить исходный адрес для пересылки адресов сегмента 192.168.0.0/16, разрешив исходный адрес для пересылки сетевых адресов 192.168.1.0/24, вы можете настроить следующие два правила: список доступа 1 разрешение 192.168.1.0 0 0.0.255 - Правило 1 список доступа 1 запретить 192.168.0.0 0 0.0.255.255 - Правило 2 Правило 1 и правило 2 далее именуются правилом 2.

Эти два правила противоречат друг другу; адрес правила 1 содержится в адресе правила 2, и один из них является отказным, а другой - разрешительным; согласно принципу фильтрации ACL, разные порядки имеют разные результаты. Если вы хотите выполнить вышеуказанные требования, порядок двух вышеуказанных правил должен быть следующим: правило 1 впереди, правило 2 позади. Коммутатор автоматически реализует вышеуказанную функцию сортировки, независимо от порядка, в котором пользователь настраивает вышеуказанные правила, а окончательным порядком является правило 1, которое находится перед правилом 2. Когда исходным адресом является адрес 192.168.1.1 пересылки пакета, сначала сравните первое правило, затем сравните второе правило, два правила совпадают, перед силой (вперед); если исходный адрес 192.168.0.1, только первое совпадение, то отбрасывается (не пересылка).

Если сортировка не выполняется, пользователь может сначала настроить правило 2, а затем настроить правило 1, правило 1 сзади, правило 2 впереди.

список доступа 1 отклонить 192.168.0.0 0.0.255.255 - Правило 2 Список доступа 1 Разрешение 192.168.1.0 0.0.0.255-Правило 1

Поскольку правило 2 содержит следующее правило 1, что может привести к тому, что пакеты, соответствующие правилу 1, полностью соответствуют правилу 2, правило 2 будет действовать каждый раз и не может соответствовать требованиям приложения.

В переключателе '0.0.255.255' - это биты с подстановочными знаками, биты ' 1' означает отсутствие соответствия, биты ' 0' означает соответствие. Видно подстановочные биты правила 2 для '0.0.255.255', должны соответствовать двум байтам (16 бит); биты подстановочных знаков в правиле 1 как '0 0.0.255', должны совпадать с тремя байтами (24 битами); поэтому правило 2 правил «больше, так после ряда в лицо». В расширенном IP-адресе при сортировке необходимо учитывать больше полей правил, таких как тип протокола IP, порт связи и т. д. Их правила упорядочения одинаковы, то есть чем больше предел конфигурации, тем меньше область действия правила и тем больше область. Упорядочивание правил реализовано в фоновом режиме, а команды пользователя могут отображаться только в порядке настройки пользователя.

Поля фильтра, поддерживаемые ACL, включают IP-адрес источника, IP-адрес назначения, тип протокола IP (например, TCP, UDP, OSPF), исходный порт (например, 161), порт назначения. Пользователи могут настраивать различные правила для управления доступом в соответствии с различными потребностями.

В коммутаторе набор правил может использоваться несколькими приложениями; например, набор правил фильтруется по доступу к портам и фильтрации доступа к службам, а также ссылается на порты двух портов или доступ к ним.

17.2 Введение в фильтрацию ACL

Фильтрация ACL осуществляется на входном порту коммутатора, а порт фильтруется по правилу соответствия потока данных, входящего в порт. Фильтр ACL обрабатывается скоростью линии коммутатора и не влияет на эффективность пересылки потока данных.

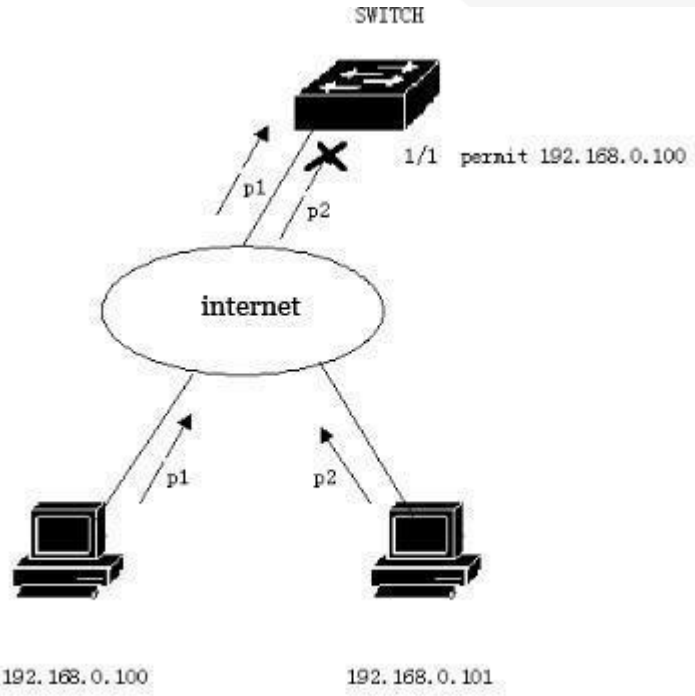
Если порт коммутатора не настраивает фильтрацию ACL, весь поток данных через порт не будет соответствовать правилам и может быть перенаправлен через порт. При настройке порта коммутатора фильтра ACL, всех входных данных через правило потока портов совпадают, совпадающие правила действия, если это разрешено, поток данных разрешает пересылку, если она запрещена, потоку данных не разрешается отбрасывать пересылку.

В порте конфигурации фильтра ACL порт может выбрать несколько правил ACL CFP группы, групповые правила в выборе порта, если не запретить или разрешить весь IP-протокол. К правилам свода правил в письменной форме, CFP добавит отказ от всех правил соглашения об ИС. При изменении правил репозитория ACL автоматически изменяются правила, записанные в CFP.

Например, в наборе правил есть только одно правило: access-list 1 permit 192.168.1.0 0.0.0.255, которое по умолчанию использует правило, которое отклоняет все пакеты протокола IP, и фактически есть два правила, импортированные в CFP порта. Когда данные проходят через фильтры, только потоки данных из 192.168.1.0 в 192.168.1.255 могут быть перенаправлены через этот порт, а все остальные потоки данных отфильтровываются.

Например, в наборе правил есть два правила: список доступа 1, запрет 192.168.1.0 0.0.0.255 и список доступа 1 разрешает любой. На этом этапе есть правило, которое разрешает все пакеты IP-протоколов, и нет никаких скрытых правил, и на самом деле есть два правила, импортированные в CFP порта. При прохождении данных через фильтры отфильтровываются только потоки данных с адресами источников от 192.168.1.0 до 192.168.1.255, а все остальные потоки данных могут быть перенаправлены.

Как показано ниже, приведен пример фильтрации ACL. Порт 1/1 коммутатора выбирает группу правил ACL 1. В этом наборе правил существует только одно правило access-list 1 разрешение 192.168.0.100. В порту коммутатора 1/1 есть два пользователя, которые хотят получить доступ к сети с этого порта, 1 IP-адрес пользователя — 192.168.0.100, 2 IP-адреса пользователя — 192.168.0.101. Только пользователь 1 может получить доступ к сети через порт 1/1 коммутатора, а пользователь 2 не может получить доступ к сети через порт 1/1 коммутатора. Поток данных P1, отправленный пользователем, может быть перенаправлен через порт 1/1 коммутатора, в то время как поток данных P2, отправленный пользователем 1, отбрасывается на порт 1/1 коммутатора 2.



Если для фильтрации ACL используется несколько портов, можно использовать одну и ту же группу правил ACL и одни и те же правила фильтрации.
Независимо от того, ссылается ли порт на набор правил или правила нескольких групп, они автоматически сортируются, даже если порядок между двумя наборами правил пересекается.
Когда пользователь ссылается на набор правил, если правила изменяются, то порты, которые ссылаются на этот набор правил, будут автоматически реагировать на конфигурацию пользователя; нет необходимости перенастраивать ссылку на этот порт.

17.3 Конфигурация репозитория ACL

Коммутатор используется по умолчанию без каких-либо правил.
Библиотека ресурсов коммутатора поддерживает четыре типа правил ACL: стандартные ip-правила, расширенные IP-правила, группы IP-MAC и группы ARP. Вот четыре правила для введения конфигурации ACL.
Стандартное IP-правило: стандартное IP-правило заключается в управлении пересылкой пакетов данных через исходный IP-адрес.
Форма команды:

access-list <groupId> {deny | permit} <source>

Описание параметра:

- groupId:Номер списка управления доступом, стандартная поддержка IP ACL от 1 до 99 или от 1300 до 1999.
- deny/permit: Если совпадение завершено, пакет отклоняется или разрешается пересылать.
- source:Source IP имеет три режима ввода:
    1) A.B.C.D подстановочный знак Вы можете управлять IP-адресом из сегмента сети;
    2) Любая сумма к A.B.C.D 255.255.255.255
    3) хост A.B.C.D Сумма к A.B.C.D 0.0.0 подстановочный знак:Определите, какие биты должны совпадать, '0' указывает на необходимость сопоставления, а '1' указывает на отсутствие необходимости сопоставления.

Расширенное правило IP: расширение IP-правила является расширением стандартного IP-правила. Пересылка пакетов может управляться IP-адресом источника, IP-адресом назначения, типом протокола IP и портом обслуживания.

Форма команды:

access-list <groupId> {deny | permit} <protocol> <source> [eq <srcPort>] <destination> [destPort] <tcp-flag>

Описание параметра:

- groupId: номер списка управления доступом, расширенный IP-ACL с поддержкой от 100 до 199 или от 2000 до 2699.
- deny/permit: Если совпадение завершено, пакет отклоняется или разрешается пересылать.
- protocol: типы протоколов на уровне IP, такие как TCP, UDP и т. д., также могут вводить соответствующий номер 6 (TCP). Если вам не нужно управлять этими протоколами, вы можете ввести IP или 0.
- source: Source IP имеет три режима ввода:
  1) A.B.C.D подстановочный знак вы можете управлять IP-адресом из сегмента сети;
  2) любая Сумма до A.B.C.D 255.255.255.255
  3) хост A.B.C.D Сумма до A.B.C.D 0.0.0 srcPort: В случае протокола TCP или UDP вы можете управлять исходным портом пакета, режим ввода может быть каким-то знакомым именем службы портов, например: www также может быть цифровым, например, 80.
- destination: Объектив IP имеет три режима ввода:
  1) Подстановочный знак A.B.C.D Вы можете управлять IP-адресом из сегмента сети;
  2) любая Сумма для A.B.C.D 255.255.255.255 3) host A.B.C.D Сумма для A.B.C.D 0.0.0.0 destPort: В случае, если используется протокол TCP или UDP, можно контролировать порт назначения пакета, а режим ввода такой же, как и у srcPort. .
- tcp-flag: для случая, когда используется протокол tcp. Сопоставлением полей TCP пакетов данных можно управлять, а необязательными параметрами являются ACK, fin, PSH, RST, syn, urg.

Правило IP MAC: группа IP MAC может управлять MAC-адресом источника и получателя IP-адреса IP-пакета.

Форма команды:

access-list <groupid> {deny | permit} <src-mac> vid <vlan-id|any> ip <src-ip> <dst-ip>

Описание параметра:

- groupId: номер списка управления доступом, расширенная группа поддержки IP ACL от 700 до 799. src-mac: исходный MAC-адрес.

MAC-адрес имеет три режима ввода:

1) Подстановочный знак HHHH.HHHH.HHHH Вы можете управлять MAC-адресом из сегмента;
2) любая Сумма до HHHH.HHHH.HHHH FFFF.FFFF.FFFF.
3) host A.B.C.D Сумма до HHHH.HHHH.HHHH 0000.0000.0000 Vid: внешний vid может быть либо vlan-id, либо любым vlan-id src-ip: исходный IP-адрес. dst-ip: IP-адрес назначения.

IP-адрес имеет три режима ввода:

1) Подстановочный знак A.B.C.D Вы можете управлять IP-адресом из сегмента сети;
2) любое Сумма для A.B.C.D 255.255.255.255 3) host A.B.C.D Сумма для A.B.C.D 0.0.0.0 Правило ARP: Группа ARP может управлять типом операции пакета ARP, MAC-адресом отправителя и IP-адресом отправителя.

Форма команды:

access-list <groupid> {deny | permit} arp <sender-mac> <sender-ip>

Описание параметра:

- groupId: номер списка управления доступом, расширенная группа поддержки IP ACL от 1100 до 1199.
- sender-mac: MAC-адрес отправителя пакета ARP.

MAC-адрес имеет три режима ввода:

1) Подстановочный знак HHHH.HHHH.HHHH Вы можете управлять MAC-адресом из сегмента;
2) любая Сумма до HHHH.HHHH.HHHH FFFF.FFFF.FFFF
3) принимающая сторона A.B.C.D Сумма до HHHH.HHHH.HHHH 0000.0000.0000 sender-ip: IP-адрес отправителя пакета ARP.

IP-адрес имеет три режима ввода:

1) A.B.C.D подстановочный знак Вы можете управлять IP-адресом из сегмента сети;
2) любая сумма к A.B.C.D 255.255.255.255
3) хост A.B.C.D Сумма к A.B.C.D 0.0.0

Список других команд:

- show access-list [groupId] - Отображает список правил, настроенных в текущем списке управления доступом. Если введен groupId, отображается список правил для текущей группы; в противном случае отображается весь список правил.
- no access-list <groupId> - Удаляет указанный список правил. Все правила группы groupId.

17.4 ACL на основе временного интервала

Раздел времени используется для описания определенного временного диапазона. У пользователей могут быть потребности: некоторые правила ACL должны действовать в течение определенного периода времени, и они не используют фильтрацию пакетов в другие периоды времени, что обычно называют фильтрацией в течение периода времени. В это время пользователь может сначала настроить одно или несколько времен, затем имя времени относится к периоду времени в соответствующем правиле, это правило действует только в указанном периоде времени, чтобы реализовать фильтр ACL на основе времени.

Если ссылки на правило времени не настроены, система выдает сообщение и позволяет таким правилам создавать успешные, но правило не вступит в силу до тех пор, пока не вступит в силу конфигурация пользователя ссылки на время и системное время в указанный период времени в пределах действия правил ACL.

Существует две ситуации для настройки раздела времени:

(1) Настройте относительный временной раздел: используйте один день за раз до определенной точки в виде точки;
(2) Конфигурация абсолютного времени: использование года, месяца, дня, части года, месяца, дня, части формы.

Настройка ACL на основе периода времени:

Команда	Описание	Режим CLI
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59>	Назначение относительного сегмента времени, содержащего время, только разделу времени	Режим глобального конфигурирования
time-range WORD cycle-time days from <0-6> to <0-6>	Настройка относительного периода времени только для недель	Режим глобального конфигурирования
time-range WORD cycle-time from <0-23> <0-59> to <0-23> <0-59> days from <0-6> to <0-6>	Настройка временного интервала между временем и неделей	Режим глобального конфигурирования
time-range WORD utter-time from <2000-2100> <1-12> <1-31> <0-23> <0-59> to <2000-2100> <1-12> <1-31> <0-23> <0-59>	Назначение абсолютного периода времени разделу даты	Режим глобального конфигурирования
no time-range WORD cycle-time	Удалить все относительные периоды времени	Режим глобального конфигурирования
no time-range WORD utter-time	Исключить все абсолютные периоды времени определенного периода времени	Режим глобального конфигурирования
no time-range WORD	Удаление периода времени (включая удаление всех относительных и абсолютных периодов времени)	Режим глобального конфигурирования
no time-range	Удаление всех периодов времени	Режим глобального конфигурирования
show time-range WORD cycle-time	Отображает все относительные периоды времени заданного периода времени	Привилегированный режим
show time-range WORD utter-time	Отображает все абсолютные периоды времени определенного периода времени	Привилегированный режим
show time-range WORD	Отображение определенного периода времени (включая все абсолютные и абсолютные периоды времени)	Привилегированный режим
show time-range	Показать все периоды времени	Привилегированный режим
acl (<1-99>|<100-199>|<1300-1 999>|<2000-2699>|<700-79 9>|<1100-1199>) time-range WORD	Такое-то правило ACL применяет определенный период времени и играет роль, когда ACL применяется к интерфейсу	Режим глобального конфигурирования

no acl (<1-99>|<100-199>|<1300-1 999>|<2000-2699>|<700-79 9>|<1100-1199>) time-range (WORD|)	Отмена определенного правила ACL и применение определенного периода времени или всех периодов времени	Режим глобального конфигурирования
show acl (<1-99>|<100-199>|<1300-1 999>|<2000-2699>|<700-79 9>|<1100-1199>) time-range	Отображает все периоды времени применения определенного правила ACL	Привилегированный режим
show all acl time-range	Отображает периоды времени для всех применяемых правил ACL	Привилегированный режим

Важно отметить, что:

(1) Временной интервал настраивается с рядом относительных периодов времени, соотношение между относительным временным интервалом, системным временем в любом относительном периоде времени, период времени активируется;

(2) Существует несколько абсолютных периодов времени для определенного периода времени, и абсолютный период времени является отношением. Системное время находится в любом абсолютном временном отрезке, а период времени находится в активном состоянии;

(3) Если к определенному времени при условии конфигурации относительного времени и абсолютного времени, относительного времени и абсолютного времени и системной временной зависимости, то при этом только в относительном времени и абсолютном времени, то период времени является активным;

(4) Определите до 256 временных периодов; максимальный период времени может быть сконфигурирован 256 относительного времени и абсолютного времени; правило ACL может использоваться до 256 периодов времени; в период действия ассоциативных правил ACL, применяемых к интерфейсу, когда наступает время.

17.5 Конфигурация фильтра ACL

По умолчанию все порты не выполняют фильтрацию ACL.

Список команд:

access-group <groupId>

Режим: параметр режима конфигурации интерфейса второго уровня:

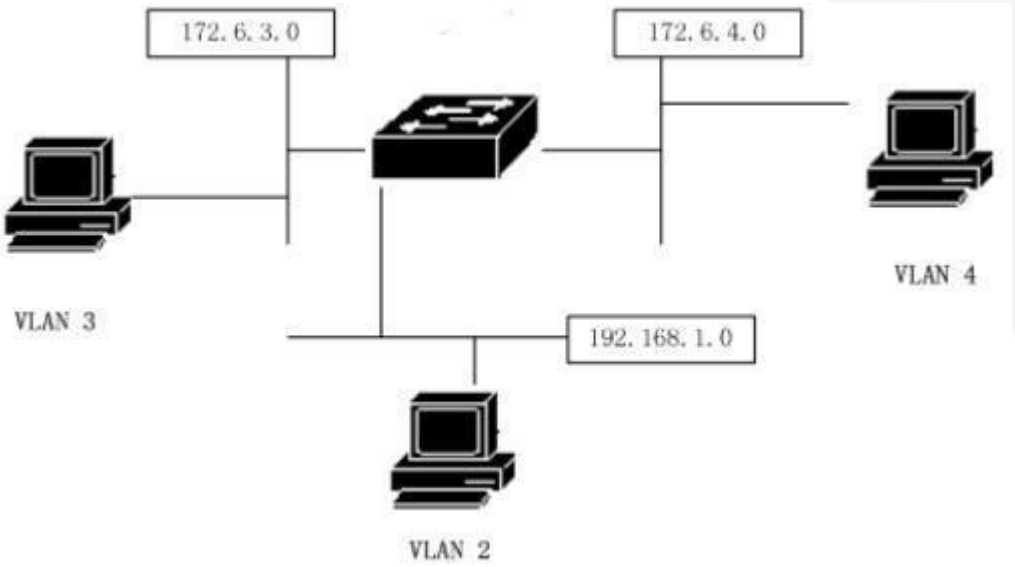
groupId: привязка ACL и номера порта Функция: настройка фильтра портов ACL.

Примечание: если приведенная выше конфигурация команды завершается сбоем или сбоем, может быть следующая причина:

1) Слишком много правил в группе ACL или аппаратные ресурсы исчерпаны или заняты другими приложениями.
2) Отображение конфигурации фильтра портов ACL show acccess-group
3) Удален текущий порт и конфигурация фильтра портов ACL без группы <groupId>ACL

17.6 Пример конфигурации ACL

Коммутатор соединяет три подсети, проектируя ACL, блокируя исходный адрес как сетевой адрес 192.168.1.0. Поток связи, пропускающий другие сетевые адреса. Сегмент 192.168.1.0 подключается к порту коммутатора 1/1.



Коммутаторы настроены следующим образом:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config)#interface ge1/1
Switch(config-ge1/1)# switchport mode access
Switch(config-ge1/1)#switchport access vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switchport mode access
Switch(config-ge1/2)#switchport access vlan 3
Switch(config)#interface vlan3
Switch(config-vlan2)#ip add 172.16.3.1/24
Switch(config)#access-list 10 deny 192.168.1.0 0.0.0.255
Switch(config)#access-list 10 permit any
Switch(config)#interface ge1/1
Switch(config-ge1/1)#access-group 10
Switch(config)#interface ge1/2
Switch(config-ge1/2)#access-group 10
```

Примечание: в соответствии с конкретными потребностями конфигурации периода времени, раздел времени, связанный с правилами ACL, относится к конфигурации следующим образом:

```
Switch(config)#time-range test cycle-time from 8 30 to 17 30 days from 1 to 5
Switch(config)#acl 1 time-range test
```

```
Switch(config)#interface ge1/20
Switch(config-ge1/2)#access-group 1
```

17.7 Отладка конфигурации ACL

Сбои конфигурации ACL могут возникнуть по следующим причинам:

1. Перед настройкой списка управления доступом убедитесь, что подключены все IP-адреса, а затем добавьте списки управления доступом. Этот список управления доступом блокирует через коммутатор поток IP-данных, исходный адрес которого — сегмент 192.168.1.0. Обратите внимание на метод дополнения подсети. Используйте команду show access-list, чтобы вывести список элементов управления доступом для просмотра, и обязательно обратите внимание на адрес источника и адрес назначения. Не пишите в ответ. Затем просмотрите список управления доступом. А в списке управления доступом по умолчанию наконец-то есть неявный deny any statement, если вы хотите пропустить другой, вам нужно добавить allow any statement, иначе он не может пройти.
2. Система настроена со статической привязкой IP MAC.
3. Текущий интерфейс включает протокол DHCP SNOOPING.
4. Исчерпание ресурсов системы CFP.

Восемнадцатая глава

Базовая конфигурация TCP/IP

Для коммутатора второго уровня с функцией управления сетью необходимо обеспечить базовую конфигурацию сети по протоколу TCP/IP и реализовать функцию связи с другими устройствами.
Основное содержание этой главы заключается в следующем:

- Настройка интерфейса VLAN
- Настройка ARP
- Настройка статической маршрутизации
- Пример базовой конфигурации TCP/IP

18.1 Настройка интерфейса VLAN

В коммутаторе каждый интерфейс третьего уровня подключен к определенной VLAN, поэтому интерфейс третьего уровня также называется интерфейсом VLAN. Создание и удаление интерфейса VLAN выполняется вручную. Коммутаторы могут быть разделены максимум на 4094 VLAN, но не более 32 подсетей могут быть построены. Создание интерфейса подсети может быть создано в соответствии с потребностями пользователей; Интерфейс подсети может быть удален пользователями вручную и может быть удален с удалением VLAN, в которой находится подсеть.
Каждый интерфейс VLAN имеет имя. Имя интерфейса VLAN — строка «VLAN», за которой следует идентификационный номер VLAN, например, имя интерфейса третьего уровня VLAN 1 — «vlan1», а имя интерфейса третьего уровня VLAN 4094 — «vlan4094».
Как и порты, интерфейс VLAN также имеет состояние управления и состояние связи. В настоящее время коммутатор не обеспечивает настройку состояния управления интерфейсом VLAN. Пока установлен интерфейс VLAN, состояние управления интерфейсом VLAN всегда up. Интерфейс VLAN состояния канала соответствует интерфейсу VLAN, содержащемуся в порту, до тех пор, пока состояние канала порта в VLAN выполняется, то состояние канала интерфейса VLAN выполняется, если VLAN во всех портах не запущена, то состояние канала интерфейса VLAN не работает.
На интерфейсе VLAN можно настроить IP-адрес и указать сетевой префикс сегмента сети, подключенного к интерфейсу (преобразованного в маску сети). В настоящее время коммутаторы поддерживают только один IP-адрес на одном интерфейсе VLAN. Перед настройкой IP-адреса пользователям необходимо сначала создать VLAN и добавить связанные порты в VLAN. По умолчанию коммутатор имеет интерфейс VLAN1, и на этом интерфейсе установить IP-адрес 192.168.0.1/24, пользователь также может изменить IP-адрес интерфейса VLAN1. Интерфейс VLAN, отличный от VLAN1, по умолчанию не устанавливает IP-адрес.

Ниже приведены команды для настройки IP-адреса интерфейса VLAN.

Команда	Описание	Режим CLI
Ip interface vlan <2-4094>	Создание интерфейса VLAN	Режим глобального конфигурирования
No Ip interface vlan <2-4094>	Удаление интерфейса VLAN	Режим глобального конфигурирования
ip address <ip-prefix>	Задайте IP-адрес на интерфейсе VLAN. Параметры включают IP-адрес интерфейса и сетевой префикс подключенного сегмента. Если в интерфейсе VLAN изначально существует IP-адрес, сначала удалите исходный IP-адрес, а затем задайте указанный IP-адрес. Формат параметра — A.B.C.D/M.	Режим конфигурирования интерфейса
no ip address [ip-prefix]	Удаление IP-адреса интерфейса VLAN. Если параметр указан, параметр должен совпадать с параметром, заданным во время настройки, в противном случае команда недопустима. Формат параметра — A.B.C.D/M.	Режим конфигурирования интерфейса

Команды интерфейса VLAN выглядят следующим образом:

Команда	Описание	Режим CLI
show interface [if-name]	Просмотр информации об интерфейсе VLAN, включая IP-адрес, MAC-адрес, состояние управления, состояние связи интерфейса и т. д.. Параметр представляет собой имя интерфейса VLAN. Если параметры не указаны, проверяются все порты и интерфейсы VLAN.	Нормальный режим, привилегированный режим
show running-config	Просматривая текущую конфигурацию системы, можно увидеть конфигурацию интерфейса VLAN.	Привилегированный режим

Пример:
Подсеть 193.1.1.0 настраивается на интерфейсе VLAN3, префикс подсети — 24 (то есть маска 255.255.255.0), IP-адрес интерфейса — 193.1.1.1, а информация о интерфейсе VLAN3 просматривается. Следующие команды:

```
switch(config)#interface vlan3
switch(config-vlan3)#ip address 193.1.1.1/24
switch(config-vlan3)#end switch#show interface vlan3
```

18.2 Настройка ARP

Протокол ARP (Address Resolution Protocol) — это протокол сопоставления IP-адреса с соответствующим MAC-адресом. Когда исходный конец кадра данных Ethernet отправляется в ту же VLAN в конце, это определение назначения в соответствии с 48-битным MAC-адресом Ethernet, пакет назначения в соответствии с MAC-адресом назначения, чтобы определить, следует ли получать пакет.

Предположим, что два смежных сегмента хоста A и B взаимодействуют через коммутатор, хост A к хосту B перед отправкой данных первому и хост A, непосредственно подключенный к интерфейсу коммутатора для отправки сообщения запроса ARP, получают ответ ARP для отправки пакетов данных на интерфейс. После получения пакета данных коммутатор сначала широковещает сообщение запроса ARP хосту B, затем получает ответное сообщение ARP от узла B, а затем отправляет пакет данных хосту B.

На коммутаторе есть кэш ARP, называемый таблицей ARP, в котором хранятся записи сопоставления IP-адреса с MAC-адресом в напрямую подключенной сети. Каждый элемент в таблице ARP имеет время жизни. Значение по умолчанию — 20 минут. Если коммутатор не получает ARP-запрос или ответное сообщение IP-адреса в течение жизни, таблица ARP, соответствующая IP-адресу, будет удалена.

Этот раздел содержит следующее содержание:

- Настройка статического ARP
- Настройка привязок ARP
- Настройка времени устаревания ARP
- Просмотр информации об ARP

18.2.1 Настройка статического ARP

В таблице ARP есть две разные записи таблицы ARP, одна из которых является статической ARP, а другая - динамической ARP. Статический ARP - это элемент таблицы ARP, настроенный пользователем, система не будет автоматически обновляться и удаляться, потребуется пользователю вручную завершить. Динамический ARP - это система автоматического обучения ARP в соответствии с полученным ARP-запросом или пакетом ответа. Система автоматически создает и удаляет, обновляет и поддерживает в режиме реального времени, без вмешательства пользователя, но пользователь может вручную удалить динамические элементы ARP.

По умолчанию коммутатор не настраивает статический элемент таблицы ARP. Важно отметить, что при удалении интерфейса VLAN или изменении IP-адреса сегмента подсети интерфейса удаляются статические и динамические записи таблицы ARP в исходном сегменте подсети.

Настройте статическую команду ARP следующим образом:

Команда	Описание	Режим CLI
arp <ip-address> <mac-address> [if-name]	Настройка статических записей таблицы ARP. Первым параметром является IP-адрес, IP-адрес должен находиться в сегменте подсети. Второй параметр — это MAC-адрес, MAC-адрес должен быть одноадресным MAC-адресом, а формат MAC-адреса — HHHH. HHHH. HHHH, например 0010.5cb1.7825. Третьим параметром является имя интерфейса второго уровня, необязательно, которое указывает, что статическая запись таблицы ARP связана с определенным двухслойным интерфейсом.	Режим глобального конфигурирования
no arp {<ip-address> | <ip-prefix> | all | dynamic | static }	Удаление записи таблицы ARP. Включает в себя удаление элемента таблицы ARP IP, удаление элемента таблицы ARP сегмента сети, удаление всех элементов таблицы ARP, удаление всех динамических элементов таблицы ARP, удаление всех статических элементов ARP.	Режим глобального конфигурирования
arp static {<ip-prefix> | all}	Изменить все элементы или все динамические элементы ARP в сегменте сети на статический таблицы ARP.	Режим глобального конфигурирования
arp aging <time>	Настройка времени устаревания ARP влияет только на динамическое обучение ARP	Режим глобального конфигурирования

18.2.2 Просмотр информации ARP

Команды для просмотра информации ARP перечислены ниже:

Команда	Описание	Режим CLI
show arp [<ip-prefix> | dynamic | static]	Просмотр информации об элементе таблицы ARP в таблице ARP, включая все записи таблицы ARP, записи таблицы ARP сегмента, динамические записи таблицы ARP и статические записи таблицы ARP.	Нормальный режим, привилегированный режим
show running-config	Просматривая текущую конфигурацию системы, можно увидеть конфигурацию ARP.	Привилегированный режим

18.3 Настройка статической маршрутизации

Статический маршрут определяется пользователем, а маршрутизация может отправлять пакеты с исходного адреса на адрес назначения по указанному пути. При настройке статического маршрута в качестве маршрута по умолчанию пакеты, которые не могут быть маршрутизированы, отправляются на шлюз по умолчанию.

Статическая маршрутизация настраивается администраторами вручную. Подходит для сети с более простой структурой сети. Администратор может настроить статический маршрут, чтобы коммутатор работал нормально. Статическая маршрутизация не использует преимущества пропускной способности сети, поскольку она не имеет обновлений маршрутизации.

Маршрутизация по умолчанию также является статическим маршрутом. Маршрут по умолчанию — это маршрут, который используется только тогда, когда соответствующий элемент маршрутизации не найден. То есть маршрут по умолчанию используется только тогда, когда нет правильной маршрутизации. В таблице маршрутизации маршрут по умолчанию отображается в виде сети 0.0.0.0/0 (маска 0.0.0.0). Если пункт назначения сообщения отсутствует в таблице маршрутизации и в таблице маршрутизации нет маршрута по умолчанию, сообщение будет отброшено, а от источника будет возвращено ICMP-сообщение с указанием адреса назначения или информации о недоступности сети. Маршрутизация по умолчанию очень полезна в сети. В типичной сети, состоящей из сотен коммутаторов, работающие протоколы динамической маршрутизации могут потреблять больше ресурсов пропускной способности, использование маршрутизации по умолчанию может сэкономить время и пакеты, занятые пересылкой ресурсов пропускной способности, поэтому вы можете удовлетворить большое количество пользователей в определенной степени и коммуникационные потребности.

Коммутатор может настроить несколько статических маршрутов к одному и тому же пункту назначения, но только один из маршрутов активируется для фактической пересылки данных. По умолчанию коммутатор не настраивает статическую маршрутизацию.

Настройка команд статической маршрутизации:

Команда	Описание	Режим CLI
ip route <ip-prefix> <nexthop-address>	Установить статическую маршрутизацию. Первый параметр задает длину IP-адреса сегмента сети и сетевого префикса, а второй - IP-адрес следующего прыжка.	Режим глобального конфигурирования
ip route <ip-address> <mask-address> <nexthop-address>	Функция такая же, как и у предыдущей команды. Первый параметр указывает IP-адрес сегмента сети, второй параметр - маску сегмента сети, а третий параметр - IP-адрес следующего прыжка.	Режим глобального конфигурирования
no ip route <ip-prefix> [nexthop-address]	Удалить статическую маршрутизацию. Первый параметр длина IP-адреса сегмента сети и префикс сети, а второй параметр IP-адрес следующего прыжка. Если нет вторых параметров, удалит все маршруты, соответствующие указанному сегменту. Если указаны вторые параметры, удалит маршрутизацию, которая соответствует указанному сегменту и следующему прыжку.	Режим глобального конфигурирования
no ip route <ip-address> <mask-address> [nexthop-address]	Функция такая же, как и предыдущая команда. Первый параметр IP-адрес сегмента сети, второй параметр маска сегмента сети, а третий параметр IP-адрес следующего прыжка. Если третий параметр отсутствуют, удалит все маршруты, соответствующие указанному сегменту. Если указан третий параметр, удалит маршрутизацию, которая соответствует указанному сегменту и следующему прыжку.	Режим глобального конфигурирования

Команды маршрутизации:

Команда	Описание	Режим CLI
show ip route [<ip-address> | <ip-prefix>	Просмотреть активную информацию о маршрутизации, вы можете выбрать для просмотра всю маршрутизацию, маршрут, сегмент сети маршрутизации, статическую маршрутизацию.	Нормальный режим, привилегированный режим
show ip route database	Просмотр всей информации о маршрутизации (включая активные и неактивные маршруты), при этом можно выбрать просмотр всех маршрутов.	Нормальный режим, привилегированный режим
show running-config	Просмотреть текущую конфигурацию системы, вы можете увидеть конфигурацию статического маршрута.	Привилегированный режим

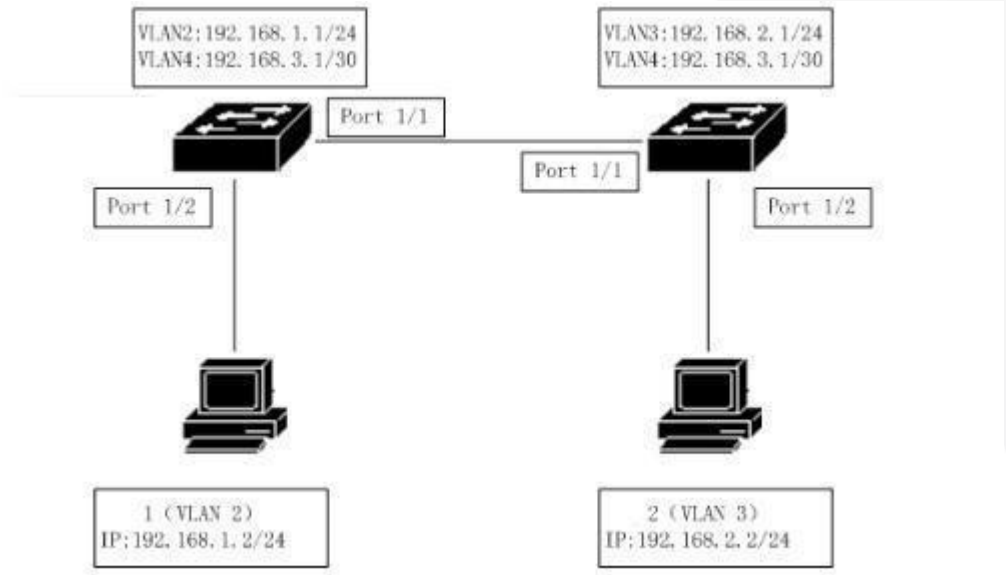
Пример:
Сеть назначения - 200.1.1.0, маска подсети - 255.255.255.0, следующий переход - 10.1.1.2.
Настройте команду как:

Switch(config)#ip route 200.1.1.0 255.255.255.0 10.1.1.2
или
Switch(config)#ip route 200.1.1.0/24 10.1.1.2

Удалите IP-адрес назначения 200.1.1.0, маску подсети 255.255.255.0, следующий прыжок 10.1.1.2 статической маршрутизации.
Настройте команду как:

Switch(config)#no ip route 200.1.1.0/24
или
Switch(config)#no ip route 2001.1.0/24 10.1.1.2
или
Switch(config)#no ip route 200.1.1.0 255.255.255.0
или
Switch(config)#no ip route 200.1.1.0 255.255.255.0 10.1.1.2

18.4 Пример базовой конфигурации TCP/IP



На схеме коммутатор 1 - это коммутатор второго уровня, а коммутатор 2 - это коммутатор третьего уровня.

18.4.1 Интерфейс третьего уровня

На коммутаторе 1 настройте соответствующий трехуровневый интерфейс VLAN2 и назначьте ему IP-адрес 192.168.1.1/24.

Конфигурация следующая:

```
Switch#config t
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#exit
Switch(config)#interface ge1/2
Switch(config-ge1/2)#switch access vlan 2
Switch(config)#ip interface vlan 2
Switch(config)#interface vlan2
Switch(config-vlan2)#ip add 192.168.1.1/24
```

Верификация: пользователь 1 может получить доступ к IP-адресу интерфейса третьего уровня VLAN2, соответствующего Ping коммутатора 1.

18.4.2 Статическая маршрутизация

Пользователь 2 должен получить доступ к коммутатору 1 и должен получить доступ к коммутатору 1 через функцию маршрутизации коммутатора 2.

Коммутатор 1 настроен следующим образом:

```
Switch#config t
Switch(config)#ip route 192.168.2.0 255.255.255.0 192.168.3.2
Switch 2 is configured as follows:
Switch#config t
```

Switch(config)#ip route 192.168.1.0/24 192.168.3.1

Верификация: Пользователь 2 может пинговать общий коммутатор 1.

18.4.3 ARP

Настройте 1 статический ARP пользователя, позволяя только 1 из пользователей получить доступ из VLAN2.

Предположим, что MAC-адрес пользователя 1 00:00:00:00:00:00:01.

Коммутатор 1 настроен следующим образом:

Switch#config t

Switch(config)#arp 192.168.1.2 0000.0000.0001

Верификация: пользователь 1 может получить доступ к IP-адресу интерфейса третьего уровня VLAN2, соответствующего Ping коммутатора 1.

Девятнадцатая глава

Конфигурация SNMP

Коммутаторы обеспечивают удаленное управление коммутаторами по протоколу SNMP. В этой главе описано, как настроить SNMP, включая следующее:
Основное содержание этой главы следующее:

- Введение в SNMP
- Конфигурация SNMP
- Пример конфигурации SNMP

19.1 Введение в SNMP

SNMP - это простой протокол управления сетью, является наиболее широко используемым протоколом управления сетью, он имеет пять основных функций: управление сбоями, управление биллингом, управление конфигурацией, управление производительностью, управление безопасностью. Он обеспечивает информационный формат для связи между прикладным программным обеспечением управления сетью и агентом управления сетью (агентом).
Протокол сетевого управления SNMP состоит из четырех основных элементов: рабочая станция управления, агент управления, база управленческой информации, протокол управления сетью. Агент управления - это сервер рабочей станции управления, имеющей доступ к коммутатору. Информация рабочей станции управления, обращающейся к агенту сетевого управления, организуется в виде MIB, и формируется база управленческой информации.
SNMP имеет три большие операции: Операция GET, операция SET, операция TRAP. Операция GET позволяет рабочей станции управления получить значение объекта в прокси. Операция SET позволяет рабочей станции управления установить значение объекта в прокси-сервере. Операция TRAP позволяет агенту уведомить о событии рабочую станцию управления.
Сообщение TRAP отправляется на рабочую станцию управления автоматически при возникновении события. Эти сообщения включают холодный запуск, горячий запуск, соединение порта вверх, соединение вниз, сбой аутентификации общего имени, переключение состояния STP и т. д.
В настоящее время SNMP имеет три версии: SNMPV1, SNMPV2, SNMPV3, причем последняя версия является обновленной версией в предыдущей, функция была улучшена, а безопасность была улучшена. Коммутатор поддерживает все три версии SNMP и может анализировать три версии пакета протокола SNMP. При отправке сообщений TRAP можно использовать любую версию SNMPV1, SNMPV2 и SNMPV3.
Коммутаторы поддерживают RFC, BRIDGE и частные объекты MIB и могут полностью управлять коммутаторами через SNMP. Некоторые MIB:RFC 1213, RFC 1493, RFC 1724, RFC 1850, RFC 1907, RFC 2233, RFC 2571, RFC 2572, RFC 2575, RFC 2573, RFC 2574 перечислены ниже, RFC 2674 и другие распространенные MIB.
На рисунке приведен пример взаимодействия протокола SNMP между рабочей станцией управления и агентом управления. Рабочая станция управления может получить доступ к SNMP-сообщению агента управления коммутатором, отправленному Get Request, GetNext Request, GetBulk Request и Set Request, получает или задает обменное значение объекта MIB, Get Response коммутатора агентство управления отправляет snMP-сообщение на станцию управления. При

возникновении каких-либо событий на коммутаторе агент управления коммутатора отправляет сообщение SNMP TRAP на рабочую станцию управления.
Взаимодействие по протоколу SNMP между рабочей станцией управления и агентом управления

19.2 Конфигурация SNMP

Конфигурация SNMP включает в себя конфигурацию коммутатора, конфигурацию рабочей станции TRAP, информацию о системе SNMP и конфигурацию группового ядра, идентификатора, пользователя и snmpV3. Коммутатор имеет общий доступ только для чтения по умолчанию, а имя общего ресурса является общедоступным. Коммутатор может настроить до 8 общих ресурсов. Коммутатор не настраивает рабочие станции TRAP по умолчанию. Коммутатор имеет идентификатор локального ядра по умолчанию, и коммутатор может изменять локальный идентификатор ядра. Коммутатор имеет значение по умолчанию userame:initialnone, которое принадлежит не идентифицированному незашифрованному имени пользователя. Коммутатор может настраивать несколько различных уровней имен пользователей. Коммутатор имеет имя группы по умолчанию:initial, и коммутаторы могут настраивать разные имена групп в соответствии с разными именами пользователей.
Команды SNMP следующие:

Команда	Описание	Режим CLI
snmp community <community-name> {ro | rw}	Настройка имени общего объекта, который обращается к сетевому управлению, является интерактивной командой. При настройке пользователь может ввести созданное имя общего тела и разрешение на чтение/запись в соответствии с запросом.	Режим глобального конфигурирования
no snmp community <community-name>	Удаляет указанное имя общего ресурса SNMP.	Режим глобального конфигурирования
snmp trap <notify-name> host <ipaddress> version {1 | 2c | 3}	Добавить или изменить целевой объект отправки ловушки SNMP. Это интерактивная команда. Имя уведомления уникально, и при изменении существующего имени можно изменить треппинг для отправки целевого элемента. Host — это адрес назначения для отправки ловушки; версия отправляется в режиме snmpV1, snmpV2c или snmpV3. По умолчанию для этой команды используется целевой порт 162.	Режим глобального конфигурирования
no snmp trap <notify-name>	Удалить указанную ловушку SNMP.	Режим глобального конфигурирования
snmp system information <contact | location | name> <information-string>	Настроить системную информацию, настраиваемую системную информацию, включающую: контакт, местоположение и имя.	Режим глобального конфигурирования
no snmp system information <contact | location | name >	Удаление сведений о конфигурации системы.	Режим глобального конфигурирования

snmp engine-id local <engine-id-octet-string>	Настройка идентификатора ядра для версии 3 SNMP. Идентификатор представляет собой 24-битное шестнадцатилетнее десятичное число; когда вход меньше 24 бит, он автоматически заполняется 0.	Режим глобального конфигурирования
snmp user <user-name> <group-name> v3 [auth {md5 | sha} <auth-key>]	Команда пользователя SNMP заключается в том, чтобы задать имя пользователя, соответствующее идентификатору локального ядра snmpv3. И имя группы, соответствующее имени пользователя. Если имя пользователя поддерживает проверку подлинности, необходимо установить протокол проверки подлинности (MD5 или Sha) и соответствующий идентификационный пароль.	Режим глобального конфигурирования
no snmp user <user-name> <group-name> v3	Удалить имя пользователя, соответствующее идентификатору локального ядра SNMPv3.	Режим глобального конфигурирования
snmp group <group-name> v3 {auth | noauth} [notify <notify view name> | write <write view name> | read <read view name>]	Команда SNMP группы представляет собой набор имен групп, уровень безопасности которых (auth или noauth), а также представление уведомлений, доступное для записи или чтения, заданное моделью безопасности (V3).	Режим глобального конфигурирования
no snmp group <group-name> v3 {auth | noauth}	Удалить имя группы, уровень безопасности (auth или noauth), указанное представление модели безопасности (V3).	Режим глобального конфигурирования
show snmp community	Отображение всех текущих общедоступных имен и соответствующих сведений о разрешениях на чтение и запись.	Нормальный режим, привилегированный режим
show snmp trap	Отображение всех имен ловушек и соответствующей IP-адреса и версии отправленного контейнера.	Нормальный режим, привилегированный режим
show snmp system information	Отображение информации о системе, заданной SNMP	Нормальный режим, привилегированный режим
show snmp engine-id	Отображение локального идентификатора ядра SNMPV3.	Нормальный режим, привилегированный режим
show snmp user [specify name of user]	Отображает сведения об имени пользователя, соответствующие идентификатору локального ядра snmpv3. Включите имя группы, соответствующее имени пользователя, а также сведения о проверке подлинности и шифровании, поддерживаемые именем пользователя.	Нормальный режим, привилегированный режим
show snmp group	Отображает все имена групп, уровни безопасности (auth или noauth), уведомления, заданные моделью безопасности (V3), записываемую или читаемую информацию о представлении.	Нормальный режим, привилегированный режим

19.3 Пример конфигурации SNMP

Настройка общего имени с именем private. Разрешения доступны на чтение и запись.

Настройте SNMP - ловушку, называемую test, и отправьте IP-адрес назначения на 192.168.0.10; используйте SNMP версии 1.

Конкретным содержимым системы конфигурации является контакты:

E-mail: networks@lenovo.com.

Конкретным содержанием системы конфигурации является местоположение: Шэньнань Роуд, Шэньчжэнь, Китай.

Задайте имя пользователя initialmd5, поддерживающее проверку подлинности MD5.

Имя группы — initia.

А пароль проверки подлинности — 047b473f93211a17813ce5fff290066b.

Задайте начальное имя группы, уровень безопасности (auth), уведомление, указанное моделью безопасности (V3), записываемые или читаемые имена представлений: Internet, Internet, Internet.

Конфигурация коммутатора выглядит следующим образом:

```
Switch#config t
Switch(config)#snmp community private rw
Switch(config)#snmp system information contact E-mail:networks@lenovo.com
Switch(config)#snmp system information location ShennanRoad,Shenzhen,China
Switch(config)# snmp user initialmd5 initial v3 auth md5 17813ce5fff290066b
Switch(config)# snmp group initial v3 auth read internet write internet notify internet
```

Двадцатая глава

Конфигурация RMON

Основное содержание этой главы заключается в следующем:

- Введение в RMON
- Конфигурация RMON
- Пример конфигурации RMON

20.1 Введение в RMON

RMON (Remote Monitoring) является стандартной спецификацией мониторинга. Он в основном используется для мониторинга потока данных в сегменте сети и даже во всей сети. Это один из широко используемых стандартов управления сетью. Спецификация RMON расширена SNMP MIB, поэтому она также является MIB, что является наиболее важным улучшением стандарта MIB II. RMON делает SNMP более эффективным и проактивным в мониторинге удаленных устройств.
Система мониторинга RMON состоит из двух частей: детектора (прокси или монитора) и станции управления. Агенты RMON хранят сетевую информацию в RMON MIB, которая непосредственно импортируется в сетевые устройства (такие как маршрутизаторы, коммутаторы и т. Д.). Станция управления использует SNMP для получения информации о данных RMON.

Это устройство поддерживает 4 наиболее часто используемые группы в RMON:

(1) Статистическая группа (Statistics): предоставление статистических данных для каждого интерфейса, где большинство объектов являются счетчиками, записывающими информацию, собранную монитором из интерфейса.
(2) Историческая группа (History): данные, хранящиеся с фиксированным интервалом времени в указанном интерфейсе.
(3) Группа тревоги (alarm): выборка заданных данных всех интерфейсов через фиксированный интервал времени, сравнение с заданным порогом и запуском соответствующего события при выполнении условия.
(4) Группа событий (event): устанавливая события, вы можете выбрать журнал записей или отправить Trap.

20.2 Конфигурация RMON

Команда RMON состоит из 4 групп конфигураций для просмотра конфигурации и просмотра данных:

Команда	Описание	Режим CLI
rmon statistics <1-100> (owner WORD|)	Конфигурация группы, задающая указанное количество портов для этого порта. Это интерактивная команда. Конфигурация заключается в том, что пользователь может ввести номер и владельца в соответствии с запросом, а владелец является необязательным. Серийный номер — это номер конфигурации статистической группы, а значение находится в диапазоне от 1 до 100.	Режим конфигурирования интерфейса
no rmon statistics <1-100>	Настройка статистической группы для отмены указанного номера.	Режим конфигурирования интерфейса
rmon history <1-100> buckets <1-100> interval <1-3600> (owner WORD|)	Параметр исторической группы, указывающий порядковый номер для этого порта, который является интерактивной командой. Пользователь конфигурации может ввести серийный номер, количество запрашивающих корзин, временной интервал и владельца в соответствии с запросом. Серийный номер — номер исторической конфигурации группы, диапазон значений — от 1 до 100; количество запросов корзины — максимальное количество сохраненных данных, диапазон значений — от 1 до 100; интервал выборки указан в секундах, а диапазон значений — от 1 до 3600.	Режим конфигурирования интерфейса
no rmon history <1-100>	Конфигурация группы журнала для отмены указанного номера.	Режим конфигурирования интерфейса
rmon alarm <1-60> WORD <1-3600> (absolute|delta) rising-threshold <1-2147483647> <1-60> falling-threshold <1-2147483647> <1-60> (owner WORD|)	Настройка параметра группы аварийных сигналов с заданным порядковым номером, который является интерактивной командой. Пользователь конфигурации может ввести серийный номер, объект монитора, интервал времени, режим контрастности, верхнее предельное значение события, верхний предел последовательности событий, нижнее предельное значение, нижний предел временного порядкового номера и владельца. Серийный номер - номер конфигурации сигнализации, диапазон от 1 до 60; объект мониторинга представляет собой OID узла MIB, интервал времени выборки в секундах, диапазон контрастности от 1 до 3600; можно выбрать абсолютное или дельта, указанное абсолютное значение (значение каждой выборки соответственно) и относительное значение (приращение относительно последней выборки выборки); предельное пороговое значение диапазона составляет от 1 до 2147483647; событие	Режим глобального конфигурирования

	должно опережать конфигурацию, от 1 до 60 — диапазон чисел.	
no rmon alarm <1-60>	Настройка группы аварийных сигналов для отмены указанного номера.	Режим глобального конфигурирования
rmon event <1-60> (log|log-trap WORD|none|trap WORD) (description WORD|) (owner WORD|)	Настройка параметра группы событий указанного порядкового номера, который является интерактивной командой. Пользователь конфигурации может ввести серийный номер, тип события, общее имя, описание и владельца в соответствии с запросом. Серийный номер — номер конфигурации группы событий, диапазон от 1 до 60; Типы событий могут выбирать log (log), log-trap (log и a Trap) и none (без действия) и trap (trap), при выборе log-trap или trap необходимо также указать имя оборудования (в общем теле конфигурация имени тела игнорируется).	Режим глобального конфигурирования
no rmon event <1-60>	Конфигурация группы для отмены событий указанного номера.	Режим глобального конфигурирования
show rmon (statistics|history-control|alarm|event) config	Просмотрите информацию о конфигурации RMON, которая является интерактивной командой. Пользователи конфигурации могут вводить и просматривать объекты в соответствии с подсказками.	Режим глобального конфигурирования
show rmon statistics-data interface IFNAME|	Просмотрите данные группы статистики RMON, настройте пользователя для ввода имя интерфейса.	Режим глобального конфигурирования
show rmon history-data interface IFNAME|	Просмотрите данные группы истории RMON, настройте пользователя для ввода имени интерфейса.	Режим глобального конфигурирования

20.3 Пример конфигурации RMON

Включите настройку группы портов для ge1/1, порядковый номер 10, владелец — tereco.

Включите сбор данных группы истории порта ge1/8, серийный номер 2, максимальное сохранение 80 данных, интервал выборки 1 минута, без владельца.

Настройте события с серийным номером 1, журнал журнала, без владельца.

Настройте событие с номером 3, отправьте ловушку, поделитесь именем публики, без владельца.

Группа сигналов тревоги с порядковым номером 5 используется для контроля количества байтов, полученных на порт. Аварийный сигнал Trap выдается, когда количество байтов на половину больше 1000, а журнал меньше 10. Нет владельца.

Коммутатор настроен следующим образом:

```
Switch#configure terminal
Switch(config)#interface ge1/1
Switch(config-ge1/1)#rmon statistics 10 owner tereco
Switch(config-ge1/1)#exit
Switch(config)#interface ge1/8
Switch(config-ge1/8)#rmon history 2 buckets 80 interval 60
Switch(config-ge1/8)#exit
Switch(config)#rmon event 1 log
Switch(config)#rmon event 3 trap public
```

Switch(config)#rmon alarm 5 1.3.6.1.2.1.2.2.1.10 30 delta rising-threshold 1000 3 falling-threshold 10 1

Двадцать первая глава

Конфигурация кластера

Коммутатор обеспечивает функцию управления кластером, которая позволяет одному устройству управлять набором сетевых устройств. В этой главе описывается, как настроить управление кластером, включая следующее:

- Введение в управления кластером
- Краткое введение в конфигурацию кластера
- Оборудование для управления конфигурацией
- Устройство участника конфигурации
- Настройка участников доступа кластера
- Отображение и обслуживание управления кластером
- Пример типовой конфигурации управления кластером

21.1 Введение управления кластером

21.1.1 Определение кластера

Кластер — это набор сетевых устройств, которыми можно управлять как одним устройством.

Цель управления кластером: решить централизованное управление большим количеством разрозненных сетевых устройств.

Преимущества кластера: сохранение IP-адреса общедоступной сети; упростить задачу управления конфигурацией. Сетевым администраторам нужно только настроить IP-адрес общедоступной сети на коммутаторе в кластере, чтобы можно было осуществлять управление и обслуживание других коммутаторов в кластере.

Коммутаторы, которые настраивают IP-адреса общедоступной сети и выполняют функции управления, являются командными коммутаторами, а другие управляемые коммутаторы являются коммутаторами-участниками, командными коммутаторами и коммутаторами-участниками, которые образуют кластер».

Кластер настраивает коммутаторы внутри кластера и управляет ими с помощью следующих трех протоколов.

- NDP (протокол обнаружения соседей)
- NTDP (протокол обнаружения соседней топологии)
- Cluster (протокол управления кластером)

Рабочий процесс кластера и сбора топологии кластера, включая создание и обслуживание, а также обслуживание процесса сбора топологии кластера, является относительно независимым, процесс сбора топологии начинает запускаться в кластере до установления принципа работы:

- Все устройства получают информацию о соседних устройствах через NDP, включая версию программного обеспечения, имя хоста, MAC-адрес и имя порта соседних устройств.
- Устройство управления собирает информацию об устройстве и информацию о подключении каждого устройства через NTDP и определяет устройства-кандидаты в кластер из собранной информации о топологии.

- Устройство управления завершает операцию добавления устройств-кандидатов в кластер и устройств-участников, покидающих кластер, в соответствии с информацией об устройстве-кандидате, собранной NTDP.

Сообщение кластера представляет собой сообщение Ethernet второго уровня, конкретный формат и интерактивный процесс относятся к национальному стандарту «Технические требования к управлению кластером коммутатора Ethernet YDT 1692-2007».

21.1.2 Роль кластера

В зависимости от положения и функций устройств в кластере формируются разные роли.

Пользователь может указать роли по конфигурации, и все роли следующие:

1) Командные коммутаторы:

- В кластере единственным коммутатором, который может настраивать весь кластер и управлять им, также является единственный коммутатор в кластере с IP-адресом общедоступной сети.
- Командные коммутаторы создают кластеры;
- Командные коммутаторы обнаруживают и определяют коммутаторы-кандидаты путем сбора информации из NDP (Протокол обнаружения соседей) и NTDP (Протокол обнаружения соседних топологий);
- Командные коммутаторы управляют обслуживанием кластера путем добавления потенциальных коммутаторов в кластеры или удаления коммутаторов-участников из кластеров;
- После создания кластера командный коммутатор предоставляет канал управления кластером.

2) Коммутатор участник

Управляемые коммутаторы в кластере.

Коммутатор-участник — это коммутатор-кандидат перед присоединением к кластеру.

Коммутатор-участник не имеет IP-адреса сети общего пользования;

Управление коммутатором-участником осуществляется агентом обмена командами.

3) Коммутатор-кандидат

Коммутатор, который имеет возможность присоединять кластеры, но еще не присоединился ни к одному кластеру.

Коммутатор должен сначала быть коммутатором-кандидатом, а затем он может стать коммутатором-участником.

4) Независимая биржа

Коммутатор без кластерной функции.

Различные роли могут быть преобразованы в соответствии с определенными правилами:

- Когда пользователь создает кластер на устройстве-кандидате, текущее устройство-кандидат назначается устройством управления кластером. В каждом кластере должно быть указано одно (и только одно) устройство управления. После назначения устройства управления устройство управления обнаруживает и идентифицирует устройства-кандидаты, собирая соответствующие сведения. Пользователь может присоединить устройство-кандидат к кластеру с помощью соответствующей конфигурации.
- Когда устройство-кандидат присоединяется к кластеру, оно становится участником.
- Когда устройство-участник в кластере удаляется, оно возвращается к устройству-кандидату.

- Устройства управления могут быть восстановлены на устройствах-кандидатах только после удаления кластера.

21.1.3 Профиль NDP

NDP используется для получения информации о непосредственно подключенном соседнем оборудовании, включая порт подключения, имя устройства, версию программного обеспечения и другую информацию. Принцип работы заключается в следующем:

- Запущенное устройство NDP периодически передает сообщение NDP соседям, включая информацию в сообщении (название оборудования, включая текущую версию программного обеспечения, порт оборудования и другую информацию) и информацию NDP о времени устаревания принимающего устройства. Он также получает и не пересылает сообщение NDP, отправленное соседними устройствами.
- Работающее устройство NDP хранит и поддерживает информационную таблицу соседей NDP и создает элемент таблицы для каждого соседнего устройства в информационной таблице NDP. Если найден новый сосед, который впервые отправляет полученное сообщение, NDP будет находиться в информационной таблице соседей, чтобы добавить таблицу; если полученная NDP информация и старая информация отличается от соседей, обновите таблицу NDP в соответствующем элементе данных, если она такая же, обновляется только в том случае, если вышло время устаревания. С течением времени устаревания не получено соседями, отправка NDP информации автоматически удалит соответствующую запись таблицы соседей.

21.1.4 Профиль NTDP

NTDP используется для сбора информации о каждом устройстве и информации о соединении между устройствами в определенном сетевом диапазоне. NTDP предоставляет сведения об устройствах управления для устройств управления, которые могут присоединиться к кластеру, и собирает топологическую информацию об устройствах в пределах указанного количества прыжков.

NDP предоставляет информацию о смежном списке для NTDP, NTDP отправляет и пересылает запрос на сбор топологии NTDP в соответствии с информацией о смежности, собирает информацию NDP каждого устройства в определенном диапазоне сети и информацию о его соединении со всеми соседями. После сбора информации управляющее оборудование или управление сетью может использовать информацию в соответствии с необходимостью выполнения требуемых функций. Когда обнаружение соседей NDP устройства-участника изменилось, сообщение о рукопожатии уведомит об изменении оборудования управления соседями, управление оборудованием может запустить NTDP для указанной коллекции топологий, чтобы NTDP мог отражать изменение топологии сети.

Устройство управления может периодически собирать топологии в сети, а пользователь может инициировать коллекцию топологий, вручную настраивая команды. Управляющее оборудование собирает топологическую информацию процессом следующим образом:

- Устройство управления отправляет топологию NTDP для сбора пакетов запросов с портов, которые включают функцию NTDP.
- Получив сообщение запроса, немедленно отправляется ответное сообщение в топологию оборудования управления, а также имеет функцию NTDP на порту копии сообщения запроса и отправляет его на соседнее оборудование; ответное сообщение содержит основную информацию о топологическом оборудовании и всю смежную информацию об оборудовании NDP.

- Соседнее устройство получает сообщение запроса и выполняет ту же операцию до тех пор, пока топология не соберет пакеты запросов на все устройства в указанном диапазоне прыжков.

Когда сбор топологий запрашивает распространение сообщений внутри сети, большое количество сетевого оборудования также получает запрос и отправляет ответное сообщение коллекции топологий топологии, во избежание перегрузки сети и загруженности устройства управления задачами можно принять следующие меры для управления скоростью распространения сообщений о сборе топологий:

- После получения запроса на сбор топологии устройство не сразу пересылает пакет запроса на сбор топологии, а откладывает ожидание в течение определенного времени, а затем начинает пересылать пакет запроса на сбор топологии на порт, включающий функцию NTDP.
- На том же устройстве, за исключением первого порта, каждый порт включил функцию NTDP для отправки сообщения запроса на сбор топологии на предыдущий порт, а затем он задержит определенный период времени перед пересылкой пакета запроса на сбор топологии.

21.1.5 Обслуживание управления кластерами

1) Устройства-кандидаты присоединяются к кластерам

Пользователь должен сначала указать режим управления оборудованием при создании кластера, управление оборудованием через протокол NDP и NTDP для обнаружения и идентификации оборудования-кандидата, оборудование-кандидат автоматически присоединяется к кластеру, а также может вручную настроить устройство-кандидат для присоединения к кластеру.

После успешного добавления устройства-кандидата в кластер порядковый номер участника кластера и управление кластером выделенного ему устройства управления получают используемые частные IP-адреса и т. д.

2) Магистральная связь

В кластере управляющее устройство и устройство-участник обмениваются данными друг с другом посредством сообщения handshake для поддержания состояния соединения между ними, а также управляют состоянием соединения оборудования и оборудования-участника, как показано на следующем рисунке.

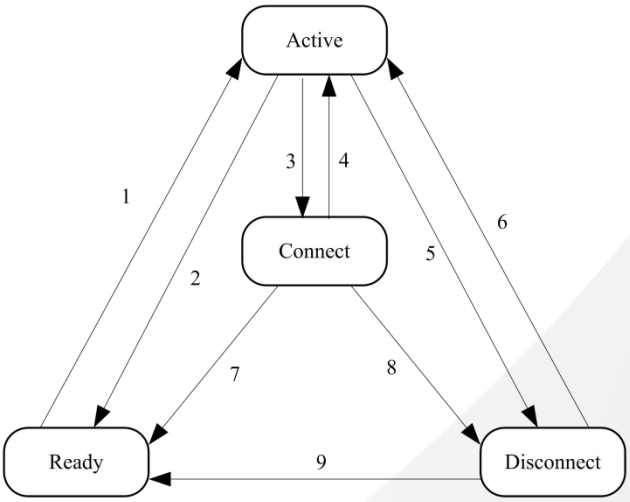
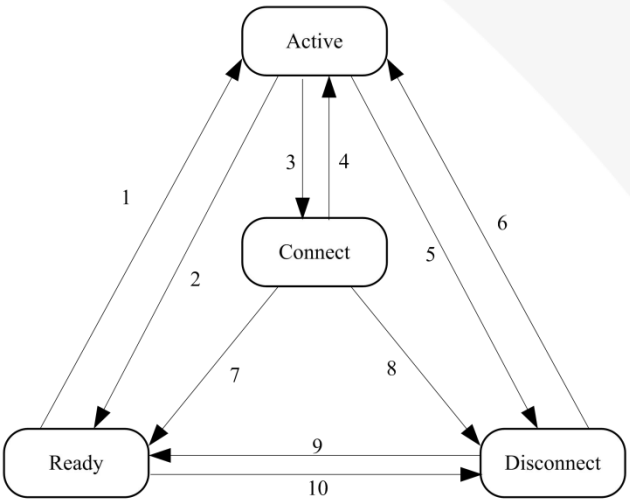


Диаграмма перехода состояний командного коммутатора



Граф переходов состояния коммутатора участника

Командный коммутатор собирает основную информацию об устройстве, идентифицирует устройство как коммутатор-кандидат и начинается с состояния Ready.

Удаление операций-участников в любом состоянии переносит состояние коммутатора элемента обратно в состояние Ready и идентифицирует его как коммутатор-кандидат.

- Кластер успешно создан, кандидат на членство оборудования в кластере, управление информацией о состоянии оборудования сохраняется для местных участников оборудования, а статус-участника идентифицируется как Активное, участник оборудования также будет сохранен в самой местной государственной информации, и его статус идентифицируется как Активный.
- Устройство управления и устройство-участник регулярно отправляют сообщения рукопожатия. После получения сообщения о рукопожатии оборудования-участника управляющее оборудование не отвечает, сохраняет оборудование участника в активном состоянии, а оборудование-участник не отвечает и сохраняет свое состояние как активное.
- Если управление оборудованием при отправке сообщения рукопожатия устройству-участнику в течении трех раз не получает ответное рукопожатие, устройство будет сохранено в состоянии локальных устройствах-участниках путем активной миграции в Connect; аналогичным образом, если участник оборудования для управления не получил сообщение рукопожатия, отправленное на оборудование управления в течении трех раз, передав сообщение рукопожатия, его статус переместится из «Active» в «Connect».
- Если управление оборудованием, полученным в состоянии Connect устройства, для отправки сообщения подтверждения времени эффективного резервирования или сообщения управления, состояние устройства-участника переводится обратно в Active, в противном случае выполняется миграция Disconnect, в котором оборудование управления, участник которого отключен; в состоянии подключения оборудования-участника, если время хранения получило сообщение подтверждения отправки или управления сообщением об управлении оборудованием, его состояние перейдет в активное, в противном случае оно перейдет в отключение.
- Когда восстановление коммуникационного оборудования и управление элементами оборудования прервано, когда устройство находится в состоянии «Отключено», участники присоединятся к объединению кластера после успешного управления элементами оборудования, и локальное состояние вернется в «Активно».

Если обнаружены изменения топологии, устройства-участники также передают информацию об изменениях на управляющее устройство посредством сообщений квитирования.

21.1.6 Управление VLAN

Управление VLAN ограничивает возможности управления кластером. Настроив VLAN, можно реализовать следующие функции:

- Сообщение управления кластером (включая сообщение NDP, NTDP и сообщение рукопожатия) будет ограничено в управлении VLAN, изолированно от других сообщений, что повышает безопасность.
- Управление устройствами и устройствами-участниками для реализации внутренних коммуникаций путем управления VLAN.

Требования к управлению кластером Оборудование для управления и элементы/порт устройства-кандидата, включая каскадный порт (когда устройство-кандидат подключен к другому оборудованию-кандидату и управление оборудованием, оборудование, подключенное к каждому кандидату между портами, называется каскадным портом) позволяет управлять через VLAN, поэтому:

- Если порт не пропускает VLAN, устройство, подключенное к порту, не может присоединиться к кластеру, поэтому кластер должен быть подключен к управляющему устройству до кластера, включая каскадный порт, что позволит передать управление VLAN.
- Только когда управление оборудованием и оборудование, подключенным к порту-участнику/кандидату и каскаду идентификаторов VLAN по умолчанию порта, является управлением VLAN, сообщение позволит управлять конфигурацией VLAN без сквозной метки, в противном случае управление сообщением должно быть помечено VLAN.

Информацию о VLAN см. в шестой главе «Настройка VLAN».

21.2 Краткое введение в конфигурацию кластера

Прежде чем пользователь настроит кластер, необходимо определить роли и функции каждого устройства в кластере и настроить соответствующие функции для выполнения работы по планированию связи с внутренним оборудованием кластера.

Задача конфигурации		Подробная конфигурация
Оборудование для управления конфигурацией	Функция NDP для включения системы и порта	15.3.1
	Настройка параметров НДП	15.3.2
	Функция NTDP для включения системы и порта	15.3.3
	Настройка параметров NTDP	15.3.4
	Настройка ручного сбора информации NTDP	15.3.5
	Включить функцию кластера	15.3.6
	Создание кластеров	15.3.7
	Настройка внутренних взаимодействий участников в кластерах	15.3.8
	Настройка управления участниками кластера	15.3.9
Configuration member device	Функция NDP для включения системы и порта	15.4.1
	Функция NTDP для включения системы и порта	15.4.2
	Настройка ручного сбора информации NTDP	15.4.3
	Включить функцию кластера	15.4.4
Настройка участников кластера для доступа друг к другу		15.5

примечание:

После того, как кластер установлен, кластер не аннулируется при закрытии функции NDP или NTDP на устройстве управления и устройстве-участнике, но это повлияет на нормальную работу установленного кластера.

21.3 Оборудование для управления конфигурацией

21.3.1 Включение возможностей системы и порта NDP

Команда	Описание	Режим CLI
ndp global enable	Включение глобальной функциональности NDP. Глобальное отключение по умолчанию.	Режим глобального конфигурирования
ndp enable	Функция NDP для включения портов. Все порты закрыты по умолчанию NDP	Режим конфигурирования интерфейса

примечание:

- Функция NDP как глобального порта, так и порта должна быть включена, и NDP может работать нормально.
- Функция NDP не поддерживает агрегированные порты.
- Чтобы избежать информации о топологии устройств, которым не требуется присоединяться к кластеру во время сбора топологии и добавления ее в кластер, рекомендуется закрыть функцию NDP на портах, которым не нужно присоединяться к кластерному устройству.

21.3.2 Настройка параметров NDP

Команда	Описание	Режим CLI
ndp aging-timer <aging-time>	Настройте время устаревания сообщения NDP, отправляемого устройством на принимающем устройстве. По умолчанию 180 секунд.	Режим глобального конфигурирования
ndp hello-timer <hello-time>	Настройка временного интервала для отправки пакетов NDP. По умолчанию 60 секунд.	Режим глобального конфигурирования

примечание:

Время устаревания сообщения NDP на принимающем устройстве не может быть меньше временного интервала передачи NDP, в противном случае это приведет к нестабильности таблицы информации соседнего порта NDP.

21.3.3 Включить возможности системы и интерфейса NTDP

Команда	Описание	Режим CLI
ntdp global enable	Включение глобальной функциональности NTDP. Глобальное отключено по умолчанию.	Режим глобального конфигурирования
ntdp enable	Функция NTDP для включения портов. Все порты закрыты по умолчанию NDP	Режим конфигурирования интерфейса

Примечание:

- Функция NTDP как глобального порта, так и порта должна быть включена, и NTDP сможет работать нормально.
- Функция NTDP не поддерживает агрегированные порты.
- Чтобы избежать передачи информации о топологии на устройства, которым не требуется присоединяться к кластеру во время сбора топологии и добавления ее в кластер, рекомендуется закрыть функцию NTDP на портах, которым не нужно присоединяться к кластерному устройству.

21.3.4 Настройка параметров NTDP

Команда	Описание	Режим CLI
ntdp hop <hop-value>	Диапазон сбора топологии конфигурации. По умолчанию максимальное количество переходов от устройства сбора топологии составляет 3 в собираемой топологии.	Режим глобального конфигурирования
ntdp timer <interval-time>	Интервал времени для настройки коллекции топологии синхронизации. По умолчанию 1 минута.	Режим глобального конфигурирования
ntdp timer hop-delay <time>	Настройка собранного устройства до того, как первый порт перенаправит топологию для сбора времени ожидания перед сообщением запроса. По умолчанию 200 миллисекунд.	Режим глобального конфигурирования
ntdp timer port-delay <time>	Настройте время задержки порта для текущей топологии переадресации устройств для сбора запросов. По умолчанию 20 миллисекунд.	Режим глобального конфигурирования

21.3.5 Настройка ручного сбора информации NTDP

После создания кластера управляющее оборудование периодически собирает информацию о топологии. Кроме того, пользователи могут вручную собирать информацию NTDP (независимо от того, установлен ли кластер) и инициировать процесс сбора информации NTDP, чтобы более эффективно управлять и контролировать оборудование.

Команда	Описание	Режим CLI
ntdp explore	Информация о топологии собирается вручную.	Обычный режим, привилегированный режим

21.3.6 Включение функции кластера

Команда	Описание	Режим CLI
cluster enable	Включить функцию кластера. Кластерная функция по умолчанию закрыта.	Режим глобального конфигурирования

21.3.7 Создание кластеров

Управление VLAN ограничивает возможности управления кластером. Настроив VLAN, можно реализовать следующие функции:

- Сообщение управления кластером (включая сообщение NDP, NTDP и сообщение рукопожатия) будет ограничено в управлении VLAN, изолированно от других сообщений, что повышает безопасность.
- Управление устройствами и устройствами-участниками для реализации внутренних коммуникаций путем управления VLAN.

Команда	Описание	Режим CLI
cluster management-vlan <vlan-id>	Назначенная управляющая VLAN. VLAN управления по умолчанию — VLAN1.	Режим глобального конфигурирования

примечание:

Если текущее устройство находится в кластере, ему не разрешено изменять управляющую VLAN.

Ситуация не в кластере:

1) Проверьте, существует ли VLAN, нет ли прямых сбоев, и перейдите к следующему шагу.
2) Повторно проверьте все интерфейсы, если интерфейс, в котором VLAN и VLAN управления, не является одной и той же VLAN, откройте глобальный NDP и ntdp, и выполните соответствующую закрытую пустую операцию, а затем снова откройте.
3) Найдите трехуровневый интерфейс, для которого вы хотите настроить VLAN. Если вы его не найдете, создайте новый трехуровневый интерфейс к VLAN. Если новая сборка не удалась, вы можете успешно управлять конфигурацией VLAN, вы можете NDP и ntdp, но вы не можете присоединиться к кластеру.
4) MAC-адрес интерфейса третьего уровня установлен на dev_id. Если VLAN настроена успешно, а новый интерфейс третьего уровня дает сбой, тогда vlan1 MAC используется как dev_id. установите на vlan1, NDP, ntdp и глобальный коммутатор будут открыты, а кластеры закрыты и соответствующая пустая закрытая операция.

При создании кластера пользователь должен сначала установить элементы оборудования, используемого в диапазоне частных IP-адресов кластера, когда добавлено устройство-кандидат, распределение частного IP-адреса может использоваться в кластере в рамках динамического управление оборудованием, и предоставляется кандидату на коммуникационное оборудование в пределах кластера, с тем чтобы добиться управления участниками управления оборудованием оборудования и технического обслуживания. примечание:

Команда	Описание	Режим CLI
cluster ip-pool <IP/MASK>	Настройка диапазона частных IP-адресов, используемых устройствами-участниками в кластере, на устройстве, которое вы хотите настроить для управления устройством.	Режим глобального конфигурирования

- IP-адрес и пул адресов кластера интерфейса VLAN для управления устройствами и устройствами-участниками не могут быть настроены в одном и том же сегменте сети, иначе кластер не будет работать должным образом.
- Только когда устройство не находится в кластере, его можно настроить.
- Используйте управляющую VLAN, чтобы определить, есть ли соответствующий трехуровневый порт. Если трехуровневого нет, то произойдет сбой прямого возврата. (это устройство не может быть кластерным командным обменом). Если есть три уровня интерфейса, базовый адрес пула IP-адресов настраивается на три порта, а если конфигурация дает сбой, пул IP-адресов настраивается на сбой.

По умолчанию устройство не управляется устройством, а кластер установлен:

Команда	Описание	Режим CLI
cluster build <name>	Создайте кластеры вручную, настройте текущее устройство для управления устройством и назначьте имя кластера.	Режим глобального конфигурирования
cluster auto-build <name>	Кластер автоматической сборки. Функция автоматического кластера автоматически добавляет все устройства-кандидаты, найденные в пределах указанного числа переходов, в созданный кластер.	Режим глобального конфигурирования
cluster delete <name>	Удалить кластер.	Режим глобального конфигурирования
cluster stop auto-add member	Автоматически настройте конфигурацию кластера, остановите автоматическое добавление коммутаторов-участников. Эта операция может только остановить добавление новых устройств, а устройства, которые были добавлены в кластер, останутся в кластере.	Режим глобального конфигурирования

примечание:

- Пользователь может указать управляющую VLAN только до создания кластера. После того, как устройство присоединилось к кластеру, пользователь не может изменить управляющую VLAN. Если вам нужно изменить VLAN управления после создания кластера, вам необходимо удалить кластер на устройстве управления, переназначить VLAN управления и, наконец, перестроить кластер.
- Из соображений безопасности рекомендуется не настраивать VLAN управления для управления портами подключения между устройствами и устройствами-участниками, а также идентификатором VLAN по умолчанию для каскадных портов.
- Только при подключении к оборудованию и управлению оборудованием и всеми участниками порта каскадный порт по умолчанию VLAN ID является управлением VLAN, сообщение не может разрешить управление через тег VLAN, в противном случае необходимо подключиться к

оборудованию управления конфигурацией, оборудованию и все участники каскада портов разрешили сообщение управления VLAN с меткой через, см. «Особая конфигурация VLAN».

- Конфигурация диапазона частных IP-адресов устройств-участников в кластере может быть настроена только тогда, когда кластер не установлен, и может быть настроена только на устройстве управления. Если кластер был создан, система не позволяет изменять диапазон IP-адресов.

21.3.8 Настройка внутренних участников кластера для взаимодействия

В кластере, управляющем оборудовании и оборудовании для связи в реальном времени между участниками, чтобы поддерживать сообщение рукопожатия, состояние соединения между ними, мы можем эффективно сохранять сообщение рукопожатия распределения времени, отправленное в управлении оборудованием по временному интервалу и оборудованию, конфигурации также повлияет на участников кластера всего оборудования.

Команда	Описание	Режим CLI
cluster timer <interval-time>	Настройка временного интервала для отправки пакетов рукопожатия. По умолчанию 10 секунд.	Режим глобального конфигурирования
cluster holdtime <hold-time>	Эффективное время хранения конфигурационного устройства. По умолчанию 60 секунд	Режим глобального конфигурирования

21.3.9 Настройка управления элементами кластера

Пользователь может вручную указать устройства-кандидаты для присоединения к кластеру или вручную удалить указанные устройства-участники в кластере. Операции присоединения/удаления участников кластера должны выполняться на управляющем устройстве, иначе будет возвращено сообщение об ошибке.

Команда	Описание	Режим CLI
cluster addmember mac-address <mac-address>	Добавление устройств-кандидатов в кластеры.	Режим глобального конфигурирования
cluster delete member mac-address <mac-address>	Удаление устройств-участников из кластера.	Режим глобального конфигурирования

21.4 Устройство-участника конфигурации

21.4.1 Включить возможности системы и порта NDP

См. систему с поддержкой 18.3.1 и функцию NDP порта.

21.4.2 Включить возможности системы и порта NTDP

См. включенную систему 18.3.3 и функцию NTDP порта.

21.4.3 Настройка ручного сбора информации NTDP

См. 18.3.5 конфигурация для ручного сбора информации NTDP.

21.4.4 Включение функции кластера

См. 18.3.6 включение функций кластера.

21.5 Настройка участника кластера доступа

После правильной настройки функций NDP, NTDP и кластера элементы кластера могут быть настроены, управляться и отслеживаться устройством управления. Вы можете настроить конфигурацию устройства-участника на устройстве управления для переключения на указанный операционный интерфейс устройства-участника.

Команда	Описание	Режим CLI
cluster switch-to member <member-number>	Переключиться с рабочего интерфейса устройства управления на рабочий интерфейс устройства-участника.	Обычный режим, привилегированный режим

примечание:

Соединение между оборудованием управления кластером и оборудованием-участником осуществляется через Telnet, поэтому необходимо обратить внимание на коммутатор:

- Перед переключением конечное устройство должно выполнить команду «telnet server enable», чтобы включить функцию telnet, иначе это приведет к сбою передачи обслуживания.
- От устройства управления к устройству-участнику, если номер участника n не существует, будет отображаться сообщение об ошибке. Если устройство, на котором зарегистрирован пользователь Telnet, заполнено, произойдет сбой передачи обслуживания.

21.6 Отображение и обслуживание управления кластером

Команда	Описание	Режим CLI
show ndp[interface <ifname>]	Отображение информации о конфигурации NDP	Обычный режим, привилегированный режим
reset ndp statistics [interface <ifname>]	Очистить статистику NDP	Режим глобального конфигурирования
show ntdp	Отображение системной информации NTDP	Обычный режим, привилегированный режим
show ntdp device-list	Отображение информации об устройстве, собранной NTDP	Обычный режим, привилегированный режим
show ntdp single-device mac-address <mac-address>	Отображает сведения о NTDP указанного устройства.	Обычный режим, привилегированный режим
show cluster	Статус и статистическая информация кластера, к которому принадлежит устройство	Обычный режим, привилегированный режим

show cluster topology	Показать информацию о топологии кластера	Обычный режим, привилегированный режим
show cluster candidates [mac-address <mac-address>]	Показать информацию об устройстве-кандидате	Обычный режим, привилегированный режим
show cluster members [<member-number>]	Отображение информации об элементе кластера.	Обычный режим, привилегированный режим

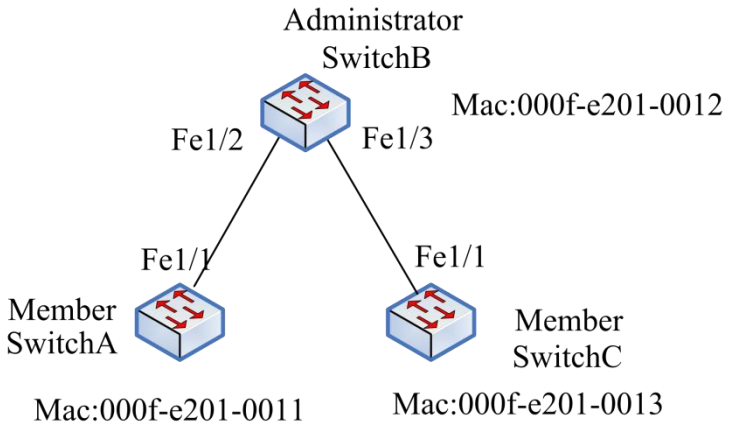
21.7 Пример типовой конфигурации управления кластером

1. Требования к сети:

ABC состоит из трех коммутаторов, а VLAN управления — это VLAN 10. Среди них коммутатор B — это оборудование управления (администратор); Коммутатор A и коммутатор C являются устройствами-участниками (Member).

Базовый IP-адрес пула адресов кластера — 10.0.0.1, поддерживающий 8 устройств.

2. Диаграмма сети:



3. Шаги настройки:

Настройка членского устройства SwitchA

Управление конфигурацией VLAN.

[SwitchA] cluster management-vlan 10
[SwitchA] interface ge1/1
[SwitchA-ge1/1] switch trunk vlan 10

Включение глобальной функциональности NDP и функциональности NDP на порту ge1/1.

[SwitchA] ndp enable
[SwitchA] interface ge1/1
[SwitchA-ge1/1] ndp enable

Включение глобальной функциональности NTDP и функциональности NTDP на порту Ethernet1/0/1.

[SwitchA] ntdp enable
[SwitchA] interface ge1/1
[SwitchA-ge1/1] ntdp enable # Enable cluster function.
[SwitchA] cluster enable

Настройка устройства-участника SwitchC

Поскольку конфигурация устройств-участников одинакова, конфигурация коммутатора C аналогична конфигурации коммутатора A, а процесс настройки немного лучше.
Устройство управления конфигурацией SwitchB
VLAN управления конфигурацией.

```
[SwitchB] cluster management-vlan 10
[SwitchB] interface ge1/2
[SwitchB-ge1/2] switch trunk vlan 10
[SwitchB] interface ge1/3
[SwitchB-ge1/3] switch trunk vlan 10
```

Включение глобальных функций NDP и NTDP и включение портов ge1/2 и ge1/3 в функциях NDP, NTDP.

```
[SwitchB] ndp enable
[SwitchB] ntdp enable
[SwitchB] interface ge1/1
[SwitchB-ge1/2] ndp enable
[SwitchB-ge1/2] ntdp enable
[SwitchB] interface ge1/3
[SwitchB-ge1/3] ndp enable
[SwitchB-ge1/3] ntdp enable
```

Время устаревания сообщения NDP, отправленного устройством, составляет 200 секунд на принимающем устройстве.

```
[SwitchB] ndp timer aging 200
```

Временной интервал для настройки сообщения NDP составляет 70 секунд.

```
[SwitchB] ndp timer hello 70
```

Максимальное количество прыжков, собранных топологией конфигурации, равно 2 прыжкам.

```
[SwitchB] ntdp hop 2
```

Настройка первого порта собираемого устройства на пересылку топологии, время задержки сбора пакетов запросов 150мс.

```
[SwitchB] ntdp timer hop-delay 150
```

Время задержки сбора пакетов запросов топологии переадресации других портов составляет 15 мс.

```
[SwitchB] ntdp timer port-delay 15
```

Топология конфигурации собирает данные с интервалом в 3 минуты.

```
[SwitchB] ntdp timer 3
```

Включить функцию кластера.

```
[SwitchB] cluster enable
```

Частный IP-адрес настроенного устройства-участника находится в диапазоне от 10.0.0.1 до 10.0.0.9.

```
[SwitchB] cluster ip-pool 10.0.0.1 8
```

Настройте текущее устройство для управления устройством и создайте кластер с именем ABC, участники автоматически присоединятся к кластеру.

```
[SwitchB] cluster autobuild abc
```

Когда вы добавите все коммутаторы, которые хотите добавить, вы можете отключить и автоматически присоединиться к функции кластера

```
[SwitchB]cluster stop auto-add member
```

Двадцать вторая глава

Конфигурация системного журнала

Основное содержание этой главы состоит в следующем:

- Введение в системный журнал
- Конфигурация системного журнала
- Системный журнал конфигурации

22.1 Введение в системный журнал

Модуль системного журнала является важной частью коммутатора, он используется для записи работы всей системы, рабочего поведения и недопустимого поведения пользователей, чтобы помочь администраторам понять и контролировать работу системы. Система управления модулями системного журнала исходит из информации журнала запущенных модулей, собирает, сортирует, сохраняет и отображает вывод информации журнала.

В системе журналов также есть важная функция отладки. Системный журнал с отладкой может помочь администраторам или другому техническому персоналу контролировать работу сети, отлаживать и диагностировать неисправности в сети. Администраторы могут легко выбрать контент, требующий отладки, и, просматривая информацию журнала выходных данных отладки, найти и устранить неисправность оборудования или сети.

Основное содержание этого раздела следующее:

- Формат информации журнала
- Хранение журналов
- Отображение журнала
- Инструменты отладки

22.1.1 Формат информации журнала

Формат информации журнала следующий:

Приоритет метки времени: имя модуля: содержимое журнала

Между отметкой времени и приоритетом есть пробел. Между приоритетом и именем модуля есть двоеточие и пробел. Между именем модуля и содержимым журнала есть двоеточие и пробел.

Пример формата информации журнала выглядит следующим образом:

2006/05/20 13:56:34 Warning: MSTP: Port up notification received for port ge1/2

В этом сообщении журнала отметка времени: 20.05.2006 13:56:34; приоритет — Предупреждение; имя модуля — MSTP; содержимое журнала: Уведомление об открытии порта, полученное для порта ge1/2.

1) отметка времени

Формат отметки времени: год/месяц/день часы: минуты: секунды.

Часы 24 часа, от 0 до 23.

Отметка времени записывает время создания информации журнала и использования системного времени коммутатора. Системное время было настроено на заводе коммутаторов, администраторы также могут изменять систему после сбоя питания, система по-прежнему будет работать.

2) приоритет

Приоритет записывает важность информации журнала. В соответствии с важностью, информация журнала разделена на четыре уровня. Порядок приоритета от высокого к низкому: критический, предупредительный, информационный и отладочный. Описание приоритета выглядит следующим образом:

Приоритет	Описание
Critical	Серьезная ошибка
Warning	Распространенные ошибки, предупреждения, очень важные советы
Information	Важные советы, общие советы, диагностическая информация
Debugging	отладочная информация

3) Имя модуля

Имя модуля записывает модуль, сгенерированный сообщением журнала, а в следующей таблице перечислены некоторые из основных модулей, генерирующих информацию журнала:

Имя модуля	Описание
CLI	Модуль интерфейса командной строки (Command line interface module)
MSTP	Модуль протокола связующего дерева с несколькими экземплярами (Multi instance spanning tree protocol module)
VLAN	Функциональный модуль VLAN
ARP	Модуль протокола ARP
IP	Модуль протокола IP
ICMP	Модуль протокола ICMP
UDP	Модуль протокола UDP
TCP	Модуль протокола TCP

4) Содержимое журнала

Содержимое журнала — это фраза или предложение, представляющее содержимое сообщения журнала. Администратор может узнать, что произошло в системе, прочитав содержимое журнала.

22.1.2 Хранение журнала

Существует три способа хранения журналов:

- Журнал хранится в памяти.
- Хранение журнала в NVM.
- Хранение журнала на сервере.

Существует четыре приоритета в соответствии с таблицей журнала в памяти, в каждой таблице журнала хранится информация о приоритете, который основан на приоритете журнала, разделенного на четыре категории, для каждого журнала существует отдельная таблица журнала. Каждая таблица журнала имеет 1 КБ записей, которые могут хранить 1 КБ информации журнала. Когда таблица журнала заполнена, информация журнала с наибольшим охватом находится позади журнала. У этого метода хранения есть проблема: когда система перезагружается, информация журнала исчезает, администратор не может видеть информацию журнала при сбое системы, не может найти проблему.

Важная информация журнала, такая как информация журнала с приоритетом Критический и Предупреждение, может храниться в энергонезависимой памяти системы. Таким образом, информация журнала в NVM может быть сохранена после перезапуска системы, чтобы администратор мог обнаружить проблему при сбое системы. Но есть проблема с этим методом хранения из-за ограниченной емкости NVM, а записи информации журнала, хранящиеся в NVM, очень ограничены.

Существует лучший способ - хранить сообщения журнала на сервере, используя протокол SYSLOG, который может работать в режиме реального времени, информация журнала может быть отправлена на сервер, сервер сохраняет информацию журнала и отображается на интерфейсе. Этот режим хранения не только удобен пользователям для просмотра информации журнала, но и имеет огромную емкость. Он может хранить большой объем информации журнала на сервере.

В настоящее время система поддерживает только хранение информации журнала в памяти и не поддерживает хранение информации журнала в энергонезависимой памяти или на сервере.

22.1.3 Отображение журнала

Существует два способа отображения журналов: отображение вручную и отображение в реальном времени. Ручное отображение заключается в том, что пользователь отображает информацию журнала, вводя команду, а отображение в реальном времени - это когда информация журнала генерируется, информация журнала напрямую выводится на терминал, и пользователь может видеть ее вовремя.

Для ручного отображения пользователь может просмотреть всю информацию журнала или просмотреть информацию журнала приоритета. Информация журнала отображается в порядке последней информации журнала, чтобы пользователь мог сначала увидеть последнее рабочее состояние коммутатора.

Для отображения в реальном времени пользователь должен открыть отображение в реальном времени на терминале. Если переключатель разомкнут, информация журнала не только записывается в таблицу журнала, но также информация журнала экспортируется на терминал. Если переключатель замкнут, информация журнала не будет отображаться на терминале в режиме реального времени. Система может только выводить информацию журнала в режиме реального времени на консольный терминал, не поддерживает вывод информации журнала на терминал Telnet.

22.1.4 Инструменты отладки

Отладка является полезным диагностическим инструментом для сетевого устройства, системы и модуля приемопередатчика пакетов данных, процесс отслеживания изменений конечного автомата позволяет администраторам понимать и контролировать системы и модули, или если сетевое оборудование оказалось в ненормальной ситуации, с помощью инструмента отслеживания отладки. Инструменты отладки предоставляют дорогие версии коммутаторов и контролируя эти коммутаторы, администраторы могут отслеживать то, что их интересует. Когда устройство или сеть вышли из строя, администратор может открыть режим отладки коммутатора, связанный с этим исключением, и найти проблему, отслеживая исполнение системы и модуля.

Когда режим отладки включен, система генерирует информацию журнала, которая будет записываться в соответствующую таблицу журнала. Как правило, приоритет сведений журнала, созданных при отладке, — информационный. Когда на коммутаторе дисплей терминала в режиме реального времени разомкнут, информация журнала будет выводиться на терминал в режиме реального времени. Когда режим отладки выключен, система не создает информацию журнала.

22.2 Конфигурация системного журнала

Конфигурация системного журнала включает в себя следующее:

- Настройка отображения терминала в реальном времени на коммутаторе
- Просмотр информации журнала
- Настроить отладки на коммутаторе
- Просмотр отладочной информации

22.2.1 Настройка отображения терминала в реальном времени на коммутаторе

По умолчанию отображения в реальном времени на терминале закрыт в коммутаторе, и информация журнала, создаваемая системой, записывается в таблицу журнала, но она не будет отображаться на терминале в реальном времени. В системе также есть некоторые журнальные данные, которые не ограничиваются этим коммутатором. Эти сообщения журнала всегда выводятся на терминал в режиме реального времени.

Отображение терминала коммутатора соответствует приоритету и системного журнала, если приоритет отображения терминала коммутатора в реальном времени включен, информация журнала приоритета будет отображаться на терминале в режиме реального времени, если отображение терминала коммутатора не включен приоритет, приоритет информации журнала не отображается в режиме реального времени на терминале.

Коммутатор может отображать информацию журнала только на терминале Console в реальном времени, и не может отображать информацию журнала на терминале Telnet в реальном времени.

Когда пользователь использует команду записи в конфигурацию системы, сохраненную в файле конфигурации, конфигурация терминального коммутатора реального времени будет сохранена в системных файлах, при перезагрузке системы конфигурация будет потеряна, необходимо повторное конфигурирование.

Команды настройки переключения отображения терминала в реальном времени выглядят следующим образом:

Команда	Описание	Режим CLI
log display [critical | warning | informational | debugging]	Открытая клемма отображение реального времени коммутатора. Если вы не вводите параметры, откроются все приоритетные терминалы, если вы введете один из параметров, откроется указанный приоритетный терминал.	Привилегированный режим
no log display [critical | warning | informational | debugging]	Замкните отображение в реальном времени терминала. Если вы не вводите параметры, выключите все переключатели отображения реального времени приоритетного терминала, если вы вводите один из параметров, замкните указанный переключатель отображения реального времени приоритетного терминала.	Привилегированный режим

22.2.2 Просмотр информации журнала

Команды для просмотра информации журнала перечислены ниже:

Команда	Описание	Режим CLI
show log display	Конфигурация переключателя дисплея реального времени для отображения всех приоритетных терминалов.	Обычный режим, привилегированный режим
show log [critical | warning | informational | debugging]	Отображение информации о журнале в таблице журналов. Если вы не вводите параметры, отображается вся информация журнала таблицы журналов, если вы вводите один из параметров, отображается информация журнала указанной приоритетной таблицы журналов.	Обычный режим, привилегированный режим

22.2.3 Настройка переключателя отладки

Система предоставляет богатый отладочный режим, включающий несколько модулей, в котором перечислены только команды каждого модуля. Полный формат команд. См. руководство по работе с командой.

Когда пользователь использует команду записи в конфигурацию системы, хранящуюся в конфигурационном файле, конфигурация отладочного коммутатора будет сохранена в системных файлах, при перезагрузке системы конфигурация будет потеряна, потребуется повторная настройка.

Схематично команда для настройки переключателя отладки выглядит следующим образом:

Команда	Описание	Режим CLI
debug ip …	Открытая система для отправки и получения IP-пакетов, связанных с отладкой переключателя.	Привилегированный режим
no debug ip …	Закройте отладочные переключатели для отправки и получения IP-пакетов.	Привилегированный режим
debug ip icmp …	Открытая система для отправки и получения пакетов ICMP, связанных с отладочным коммутатором.	Привилегированный режим
no debug ip icmp …	Закройте отладочный режим для отправки и получения пакетов ICMP.	Привилегированный режим
debug ip arp …	Открытая система для отправки и получения ARP-пакетов, связанных с отладочным коммутатором.	Привилегированный режим

no debug ip arp …	Закройте отладочный режим для отправки и получения ARP-пакетов.	Привилегированный режим
debug ip udp …	Открытая система для отправки и получения пакетов UDP, связанных с отладочным режимом коммутатора.	Привилегированный режим
no debug ip udp …	Закройте отладочные режим для отправки и получения пакетов UDP.	Привилегированный режим
debug ip tcp …	Открытая система для отправки и получения пакетов TCP, связанных с отладочным режмом.	Привилегированный режим
no debug ip tcp …	Закройте отладочные режимы для отправки и получения TCP-пакетов.	Привилегированный режим
debug mstp …	Откройте отладки, связанный с диагностикой протокола MSTP.	Привилегированный режим
no debug mstp …	Закрыть отладочные режимы, связанные с диагностикой протокола MSTP.	Привилегированный режим
debug igmp snooping …	Открыть режим отладки функции IGMP SNOOPING, связанной с диагностикой.	Привилегированный режим
no debug igmp snooping …	Закрыть режимы отладки, связанные с диагностикой функции IGMP SNOOPING.	Привилегированный режим
debug dhcp snooping …	Открытый протокол DHCP SNOOPIN для диагностики соответствующих отладочных режимов	Привилегированный режим
no debug dhcp snooping …	Закройте режим отладки диагностики протокола DHCP SNOOPIN	Привилегированный режим
no debug all	Выключите все переключатели отладки в системе.	Привилегированный режим

22.3.1 Ввод SYSLOG

SYSLOG - это стандартный протокол для управления журнальной информацией оборудования, который получил широкое применение благодаря простоте конструкции. В системе SYSLOG он разделен на три части. Один из них заключается в определении каждого подмодуля для разграничения журнальной информации, создаваемой различными модулями; определять различные уровни журнальной информации для наблюдения за состоянием работы устройства. Сбор всех видов журнальной информации оборудования осуществляется в соответствии с настоящим соглашением. Второй - это файл конфигурации, как работать с собранной пользовательской информацией журнала, которая может храниться локально, может быть отправлена на указанный сетевой сервер, может быть отправлена указанному пользователю для входа в журнал и так далее; конфигурационным файлом, чтобы решить, как сохранить оборудование. В-третьих, отправка сообщения по протоколу SYSLOG в соответствии с форматом сообщения, определенным RFC. Как вы можете видеть, в нашей системе коммутаторов вся рабочая конвенция SYSLOG является модулем системного журнала. Первая часть протокола SYSLOG завершается каждым функциональным подмодулем коммутатора и отправляет лог-информацию каждого уровня в модуль системного журнала. Поддержка четырех уровней таблиц журналов в модуле системного журнала. Вторая часть протокола SYSLOG с помощью модуля системного журнала для равномерного распределения логовой информации, одна через коммутатор отображения терминала или отображение в реальном времени в терминале последовательного порта два сохраняется вручную; таблица четырех уровней в памяти; в-третьих, сохранение информации журнала высокого уровня в записях журнала NVM во избежание потери важного сбоя питания; четыре — журнал отправляется в удаленное хранилище сервера, собирая и сортируя

сообщение SYSLOG. Подмодуль SYSLOG в модуле системного журнала реализует только третьи части и передает системный журнал на сервер.

22.3.2 Конфигурация SYSLOG

Команды настройки SYSLOG содержит:

- Открытый протокол системного журнала
- Закрытие протокола системного журнала
- Установка уровня отправки системного журнала
- Восстановление уровня отправки системного журнала до значения по умолчанию

Команда	Описание	Режим CLI
syslog open <server-ip> [udp-port]	Откройте протокол syslog; требуется параметры server-ip для IP-адреса сервера; параметры udp-порта для номера порта назначения, сообщение протокола необязательно, если не установлено значение по умолчанию 514; если конфигурация сервера настроена на согласованность.	Режим глобального конфигурирования
syslog close	Закрытие протокола системного журнала	Режим глобального конфигурирования
syslog level <critical | warning | informational | debugging>	Установите уровень отправки журнала, например установите уровень отладки, все журналы будут отправлены на сервер.	Режим глобального конфигурирования
no syslog level	Восстановление уровня отправки до значения по умолчанию при отладке	Режим глобального конфигурирования

22.3.3 Пример конфигурации SYSLOG

(1) Настройка

Настройка IP-адреса сервера системного журнала для программного обеспечения конфигурации сервера 192.168.2.201 получает сообщение syslog UDP на порт 200; порт ge1/3 подключен к серверу; Сервер сохраняет не более двух уровней ведения журнала.

Коммутатор настраивается следующим образом:

```
Switch#configure terminal
Switch(config)#vlan database
Switch(config-vlan)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#exit
Switch(config)#interface ge1/3
Switch(config-ge1/3)#switchport access vlan 2
Switch(config-ge1/3)#interface ge1/4
Switch(config-ge1/4)#switchport access vlan 2
Switch(config-ge1/4)#interface ge1/5
Switch(config-ge1/5)#switchport access vlan 3
Switch(config-ge1/5)#interface ge1/6
Switch(config-ge1/6)#switchport access vlan 3
```

```
Switch(config-ge1/6)#interface vlan2
Switch(config-vlan2)#ip address 192.168.2.1/24
Switch(config-vlan2)#exit
Switch(config)#syslog open 192.168.2.201 200
Switch(config)#syslog level warning
```

(2) Верификация

```
Switch#show running-config
!
syslog open 192.168.2.201 200 syslog level warning
!
……
!
line vty
!
end
Switch#show syslog Syslog is opened!
server ip address: 192.168.2.201 udp destination port: 200 severity level: warning
```

Двадцать третья

Петля порта

Основное содержание этой главы заключается в следующем:

- Профиль
- Принцип протокола
- Введение в конфигурацию

23.1 Профиль

Когда петля появляется на порту коммутатора она вызовет широковещательный шторм пакетов данных источника MAC-адреса петли переадресации порта приведет к выходу из строя оборудования.

23.2 Принцип протокола

Протокол Ethernet Loop Detection (Ethernet Loopback Detection, далее ELD) обнаруживает петли по взаимодействию пакетов и блокирует порт, на котором происходит петля ELD - это протокол, основанный на вычислении порта и может обнаруживать петли только на этом порту.

23.2.1 Процесс обнаружения

Когда на порту включен протокол ELD, можно включить регулярный таймер, посылая пакеты обнаружения петли, если в период таймера порт получил пакеты обнаружения петли, предполагается, что существующий порт будет выполнять цикл операций блокировки, и пустой этот порт FDB.

Если порт является участником нескольких VLAN, то этот порт автоматически отправляет пакеты обнаружения петли во все VLAN. То есть, этот порт автоматически определяет принадлежность всех петель VLAN к нему.

23.2.2 Режим восстановления

В нем говорится, что при появлении петли порт будет заблокирован. Протокол ELD имеет два типа шаблонов восстановления, которые пользователи могут настроить: автоматическое восстановление и ручное восстановление.

Автоматическое восстановление - это когда порт блокируется после замыкания, протокол ELD включает таймер восстановления, по истечении таймера выполняется обратная операция блокировки петли, и в порту таймер обнаружения петли снова включается.

Ручное восстановление - порт заблокирован, протокол больше не включен таймер для восстановления порта, пользователь должен ввести свои собственные команды для выполнения обратной операции блокировки петли.

23.2.3 Безопасность протокола

Протокол ELD в сети легко атакуется, что означает, что пользователь может в соответствии с форматом пакета протокола ELD на порт протокола ELD отправить пакет, чтобы включить протокол ELD, порт не может в цикле блокируется из-за неправильного решения.

Протокол ELD использует две стратегии для предотвращения подобных атак и минимизации ошибок.

Во-первых, протокол ELD - это протокол без взаимодействия, то есть он не зависит от других устройств, тогда сам пакет может быть просто зашифрован. Наша операция здесь заключается в отправке пакета протокола ELD с ключом, и пользователь не может замаскировать пакет протокола без ключа.

Решение два, в основном для предотвращения атак злоумышленника через захват пакетов, может получить выделение определенного периода формата пакета коммутатора для предотвращения атаки, пользователь должен это настроить.

23.3 Введение в конфигурацию

Протокол ELD реализован на основе портов, и единой команды включения не существует.

23.3.1 Глобальная конфигурация

Команда	Описание	Режим CLI
loop-detection detection-time <1-65535>	Настройте время обнаружения петли, это время должно быть в 2 раза меньше чем время восстановления, по умолчанию 5 секунд.	Режим глобального конфигурирования
loop-detection resume-time <10-65535>	Время автоматического восстановления должно быть в 2 раза больше, чем время проверки цикла. Если автоматическое восстановление включено, эта конфигурация вступит в силу. Время восстановления по умолчанию составляет 600 секунд.	Режим глобального конфигурирования
loop-detection protocol-safety	Включить проверку безопасности протокола, по умолчанию закрыто.	Режим глобального конфигурирования
loop-detection respond-packets	Настройте количество пакетов, которые должны быть получены в течение определенного периода времени. Если проверка безопасности протокола включена, эта конфигурация вступит в силу, а значение по умолчанию составит 10	Режим глобального конфигурирования

Глобальная конфигурация - это единый атрибут протокола конфигурации.

23.3.2 Конфигурация интерфейса

Конфигурация интерфейса настраивается для каждого порта.

Команда	Описание	Режим CLI
Loop-detection enable	Включить протокол ELD на порту.	Режим конфигурирования интерфейса
Loop-detection resume	Ручное восстановление, проверка цикла перезапуска.	Режим конфигурирования интерфейса

loop-detection resume-mode {automation | manual}	Настройте режим восстановления, выберите ручное восстановление или автоматическое восстановление, по умолчанию установлено автоматическое восстановление.	Режим конфигурирования интерфейса
loopback-detection shutdown-mode {no-shutdown | shutdown}	Команда настраивает, будет ли порт отключен при наличии петли.	Режим конфигурирования интерфейса

23.3.3 Отображение конфигурации

Show loop-detection [ifname]

Отображение всей конфигурации протокола и конфигурации интерфейса.

Двадцать четвертая глава

Конфигурация SNTP

Основное содержание этой главы заключается в следующем:

- Введение в SNTP
- Конфигурация SNTP
- Отображение информации SNTP

24.1 Внедрение SNTP

В настоящее время Интернет широко используется в протоколе связи для реализации синхронизации сетевого времени, а именно NTP (Network Time Protocol), протокол является упрощенной версией протокола NTP, а именно SNTP (Simple Network Time Protocol).

Протокол NTP может охватывать различные платформы и операционные системы, с очень сложным алгоритмом, поэтому эффект задержки и джиттера почти не зависит от сети, может обеспечить точность 1-50 мс при обеспечении. Механизм аутентификации NTP, уровень безопасности очень высок. Но алгоритм NTP сложный, система требует больше мощности.

SNTP (Simple Network Time Protocol) представляет собой упрощенную версию NTP, при реализации вычисления времени с использованием простого алгоритма производительность высока, а точность обычно может достигать около 1 секунды, но также в основном удовлетворяет потребности большинства случаев.

Поскольку сообщение SNTP и сообщение NTP полностью идентичны, клиент SNTP, реализованный этим коммутатором, может быть полностью совместим с NTP-сервером.

24.2 Конфигурация SNTP

Поект	Значение по умолчанию
Состояние SNTP	Отключение закрывает службы SNTP
NTP сервер	Существует три значения по умолчанию для NTP-сервера 211.115.194.21 203.109.252.5 192.43.244.18
Временной интервал синхронизации SNTP	1800 second
Местный часовой пояс	+8, East eight district

24.2.1 Настройки SNTP по умолчанию

Открытие и закрытие SNTP

Конфигурация следующая:

Switch# configure terminal

Войдите в режим глобальной конфигурации

Открыть SNTP

Switch(config)# sntp enable

Закрыть SNTP

Switch(config)# sntp disable

24.2.2 Configuring SNTP Server address

Поскольку пакеты SNTP и NTP абсолютно одинаковы, SNTP Client может быть полностью совместим с NTP Server. В сети имеется несколько серверов NTP, вы можете выбрать меньшую задержку сети в качестве переключателя на сервере NTP.

Конкретный адрес NTP-сервера можно зарегистрировать на сайте http://www.ntp.org/, чтобы получить Например, 192.43.244.18 (time.nist.gov).

Этот коммутатор имеет три адреса сервера по умолчанию, 211.115.194.21, 203.109.252.5 и 192.43.244.18 соответственно, первым коммутатор использует первый адрес сервера для синхронизации времени, если синхронизации нет, использует второй адрес сервера, и так далее. Как правило, пользователям не нужно настраивать адрес сервера, и они используют адрес сервера по умолчанию напрямую. Если вам нужно настроить адрес сервера в особом случае, вам нужно сначала удалить адрес сервера по умолчанию, а затем добавить новый адрес сервера.

Добавьте конфигурацию адреса сервера следующим образом:

Переход в режим глобальной конфигурации

Switch# configure terminal

Добавьте SNTP сервер IP, если на коммутаторе уже существует три адреса сервера, это увеличит сбой, нужно удалить адрес и затем добавить

Switch(config)# sntp server 210.72.145.44

Конфигурация удаления адреса Сервера выглядит следующим образом:

Удалить все адреса сервера

Switch(config)# no sntp server

Удаление одного из адресов сервера

Switch(config)# no sntp server 210.72.145.44

Конфигурация возврата адреса сервера к адресу по умолчанию выглядит следующим образом:

Адрес Сервера сбрасывается до адреса по умолчанию, то есть адреса 211.115.194.21, 203.109.252.5 and 192.43.244.18

Switch(config)# sntp server default

24.2.3 Настройка тактового интервала синхронизации SNTP

Клиент SNTP требует синхронизации и синхронных тактовых сигналов NTP-сервера, чтобы синхронизация часов была положительной.
Конфигурация выглядит следующим образом:

Switch# configure terminal

Установите интервал синхронизации синхронизации, единица измерения равна секундам, диапазон составляет 60 секунд - 65535 секунд. Значение по умолчанию — 1800 секунд, здесь установлено значение 60 секунд

Switch(config)# sntp interval 60

Интервал синхронизации синхронизации восстанавливается до значения по умолчанию 1800 секунд

Switch(config)# no sntp interval

24.2.4 Настройка местного часового пояса

После связи по протоколу SNTP время — среднее время по Гринвичу (GMT), чтобы протокол работал по местному времени, нужно установить регион для корректировки стандартного времени. Коммутатор по умолчанию использует местный часовой пояс в Восточном восьмом поясе и часовой пояс, в котором находится Китай.
Конфигурация выглядит следующим образом:

Switch# configure terminal

Установите местный часовой пояс на западную восьмую область

Switch(config)# sntp time-zone -8

Местный часовой пояс восстановлен на востоке восемь районов

Switch(config)# no sntp time-zone

24.3 Отображение информации SNTP

Конфигурация выглядит следующим образом:

Switch# show sntp

Switch# show running-config

Двадцать пятая глава

Конфигурация OAM

Основное содержание этой главы заключается в следующем:

- Введение в OAM
- Конфигурация OAM
- Типичные примеры конфигурации OAM

25.1 Внедрение в OAM

Ethernet OAM (Operations, Administration and Maintenance) - это инструмент для мониторинга сетевых проблем. Он работает на канальном уровне и использует блоки данных протокола OAM (OAMPDU) для отчетности о состоянии сети, чтобы сетевой администратор мог более эффективно управлять сетью.

В настоящее время Ethernet OAM в основном решает общую проблему связи «последней мили» в доступе Ethernet. Включив функцию Ethernet OAM на двух устройствах типа «точка-точка», можно контролировать состояние связи между двумя устройствами.

В этом разделе в основном представлены основные функции Ethernet OAM, в том числе основные функции Ethernet:

- Мониторинг производительности канала: может обнаруживать сбои канала
- Обнаружение и предупреждение неисправностей: своевременно уведомляет администратора сети о выходе из строя соединения;
- Тест петли: обнаружение сбоев канала путем возврата петли, отличных от OAMPDU.

25.1.1 Мониторинг производительности канала

Мониторинг каналов используется для обнаружения сбоев канального уровня в различных средах. Ethernet OAM использует взаимодействие OAMPDU уведомления о событиях для мониторинга связи. При возникновении сбоя связи после того, как локальная связь отслеживает неисправность, OAMPDU с уведомлением о событии отправляется сущности Ethernet OAM для уведомления об общем событии связи. Администраторы могут динамически наблюдать за информацией журнала, чтобы понять состояние сети.

Тип события	Значение	Описание
Errored Symbol Event	Событие сигнала об ошибке	В единицу времени количество ложных сигналов превышает пороговое значение
Errored Frame Event	Событие кадра ошибки	В единицу времени количество кадров погрешности превышает пороговое значение

Errored Frame Period Event	Периодические события неправильного кадра	Количество кадров ошибки превышает пороговое значение при получении указанного количества кадров
Errored Frame Seconds Summary Event	Итоговое событие «Неправильный кадр секунд»	В течение указанного времени количество кадров в секунду превышает пороговое значение

25.1.2 Удаленное обнаружение неисправностей

Обнаружить неисправность Ethernet очень сложно, особенно когда физическая связь сети не прерывается, а производительность сети медленно падает.

OAMPDU определяет флаг (флаг домена), который позволяет сущностям OAM Ethernet передавать информацию о неисправности на противоположный конец. Флаг может представлять следующие чрезвычайные события связи:

Таблица 5 События аварийной связи

Тип события	Значение	Описание	Частота отправки OAMPDU
Link Fault	Неисправность соединения	Потеря сигнала сквозного канала связи	Отправлять раз в секунду
Dying Gasp	Фатальная неисправность	Неожиданные локальные сбои, например, отключение электроэнергии	Бесперебойная передача
Critical Event	Чрезвычайная ситуация	Неясные чрезвычайные события, такие как однократный проход звена	Бесперебойная передача

Процесс Ethernet OAM соединения постоянно отправляет Information OAMPDU, конец OAM субъекта может быть концом информации о событии аварийной связи через Information OAMPDU, чтобы сообщить удаленному OAM субъекту. Таким образом, администратор может динамически понимать состояние канала связи и своевременно устранять соответствующие ошибки.

25.1.3 Обратная петля находящаяся на расстоянии

Функция замыкания Yuan Duan относится к активному режиму сущности OAM, чтобы конец (Yuan Duan) отправлял все остальные сообщения, кроме OAMPDU, полученное сообщение напрямую возвращается в конец. Его можно использовать для обнаружения сбоев связи и определения качества канала: сетевые администраторы могут судить о производительности канала (включая скорость потери пакетов, задержку, джиттер и т. Д.), Наблюдая за возвратом пакетов, отличных от OAMPDU.

25.2 Конфигурация OAM

Команда	Описание	Режим CLI
oam errored-frame period <1-60>	Настройка портов Ethernet для периодических значений обнаружения событий кадра ошибок. Период события кадра по умолчанию равен 1с.	Привилегированный режим

Команда	Описание	Режим CLI
no oam errored-frame period	Сброс портов Ethernet для периодических значений обнаружения событий кадра ошибок. Период события кадра по умолчанию равен 1с.	Привилегированный режим
oam errored-frame threshold <0-4294967295>	Настройка пороговых значений для обнаружения событий кадра ошибки. Пороговое значение события кадра ошибки по умолчанию равно 1.	Привилегированный режим
no oam errored-frame threshold	Сброс порога для обнаружения события кадра ошибки. Пороговое значение события кадра ошибки по умолчанию равно 1.	Привилегированный режим
oam errored-frame-period period <100-6000>	Настройка портов Ethernet для обнаружения периодических значений периодического обнаружения ложных кадров. Период события цикла кадра по умолчанию составляет 1000 миллисекунд.	Привилегированный режим
no oam errored-frame-period period	Сбросьте порты Ethernet для периодического определения значений периодических событий ложных кадров. Период события цикла кадра по умолчанию составляет 1000 миллисекунд.	Привилегированный режим
oam errored-frame-period threshold <0-4294967295>	Настройка пороговых значений для периодического обнаружения событий в кадрах ошибок. Пороговое значение события кадра ошибки по умолчанию равно 1.	Привилегированный режим
no oam errored-frame-period threshold	Сбросьте пороговое значение периодического обнаружения событий для кадров ошибок. Пороговое значение события кадра ошибки по умолчанию равно 1.	Привилегированный режим
oam errored-frame-seconds period <10-90>	Настройка портов Ethernet для периодических значений обнаружения событий секунд погрешности кадра. Период события кадра по умолчанию равен 60-м годам.	Привилегированный режим
no oam errored-frame-seconds period	Сбросьте порт Ethernet для периодических значений обнаружения событий секунд погрешности кадра. Период события кадра по умолчанию равен 60-м годам.	Привилегированный режим
oam errored-frame-seconds threshold <0-900>	Настройка пороговых значений для обнаружения событий в секундах кадра ошибки. Пороговое значение события секунд кадра ошибки по умолчанию равно 1.	Привилегированный режим
no oam errored-frame-seconds threshold	Сброс порогового значения секунды кадра ошибки для обнаружения событий. Пороговое значение события секунд кадра ошибки по умолчанию равно 1.	Привилегированный режим
oam mode (active| passive)	Настройте режим Ethernet OAM, режим связи Ethernet OAM по умолчанию как активный режим.	Режим конфигурирования интерфейса
oam enable	Откройте функцию Ethernet OAM, функция Ethernet OAM по умолчанию закрыта.	Режим конфигурирования интерфейса

Команда	Описание	Режим CLI
oam loopback	Включите функцию замыкания Ethernet OAM. Завершение работы функции замыкания OAM по умолчанию.	Режим конфигурирования интерфейса
no oam loopback	Отключите функцию замыкания Ethernet OAM. Завершение работы функции замыкания OAM по умолчанию.	Режим конфигурирования интерфейса
show oam configuration	Отображает окно и пороговое значение общих событий связи.	Привилегированный режим
show oam local-state (IFNAME|)	Просмотр локальной информации OAM	Привилегированный режим
show oam remote-state (IFNAME|)	Просмотр одноранговых сведений OAM	Привилегированный режим
show oam link-event (IFNAME|)	Просмотр сведений о событии связи OAM	Привилегированный режим
show oam-loopback IFNAME	Отображение информации о замыкании порта.	Привилегированный режим

25.3 Типовые примеры конфигурации OAM

1 Требования к сети

При настройке протокола Ethernet OAM на устройстве A и устройстве B осуществляется управление канальным уровнем данных; (Порт устройства A: fe1/1, порт устройства B: fe1/1)

(1) Конфигурация устройства A:

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

На порту Ethernet1/0/1 настройте режим подключения Ethernet OAM как пассивный режим и включите функцию Ethernet OAM.

```
Switch(config-fe1/1)#oam mode passive
Switch(config-fe1/1)#oam enable
```

(2) Конфигурация устройства B:

```
Switch>enable
Switch#configure terminal
Switch(config)# interface fe1/1
```

Рабочий режим Ethernet OAM для настройки порта Ethernet1/0/1 является активным режимом по умолчанию и может выполнять функцию Ethernet OAM.

```
Switch(config-fe1/1)#oam enable
```

(3) Проверка влияния конфигурации на (устройство A):

```
Switch>enable
Switch#show oam fe1/1
```

Двадцать шестая глава

Конфигурация CFM

Коммутатор обеспечивает функцию CFM, которая в основном используется для обнаружения канала связи в двухуровневой сети, подтверждения неисправности и определения местоположения неисправности, в основном включая следующее содержимое:

- Профиль CFM
- Краткое введение в задачу настройки CFM
- Базовая конфигурация CFM
- Настройка различных функций CFM
- Отображение и обслуживание CFM
- Типичные примеры конфигурации

26.1 Профиль CFM

CFM — это аббревиатура от Connectivity Fault Management (connected error management). CFM коммутатора в основном относится к обнаружению подключенных ошибок, которое следует протоколу CFM, определенному IEEE 802.1ag. Это двухуровневый канальный механизм, основанный на сквозном механизме OAM VLAN (Operations Administration, and Maintenance) в основном используемый на двух уровнях подключения канала обнаружения сети, подтверждения неисправности и определения позиции неисправности.

26.1.1 Основные понятия CFM

1 Обслуживающий домен

Домен обслуживания (MD) указывает на сеть, на которую распространяется обнаружение ошибок подключения, границы которой определяются серией конечных точек обслуживания, настроенных на порту. Обслуживающий домен помечен как "обслуживание доменного имени".

Чтобы точно определить точку неисправности, в область обслуживания вводится понятие уровня (иерархии). Область обслуживания разделена на восемь уровней, представленных целым числом от 0 до 7, чем больше число, чем выше уровень, тем больше область действия домена обслуживания. Различные домены обслуживания могут быть смежными или вложенными, но не могут пересекаться, а вложенные могут быть внедрены только высокоуровневым доменом обслуживания в домен низкоуровневого обслуживания, то есть домен низкого уровня обслуживания должен быть включен в домен высокого уровня обслуживания. Блок распределения питания CFM низкоуровневого домена обслуживания будет отброшен после входа в домен обслуживания высокого уровня; CFM PDU высокоуровневого домена обслуживания может пересекать домен обслуживания низкого уровня; БЛОК распределения распределения питания CFM одного уровня домена обслуживания не может пересекаться друг с другом.

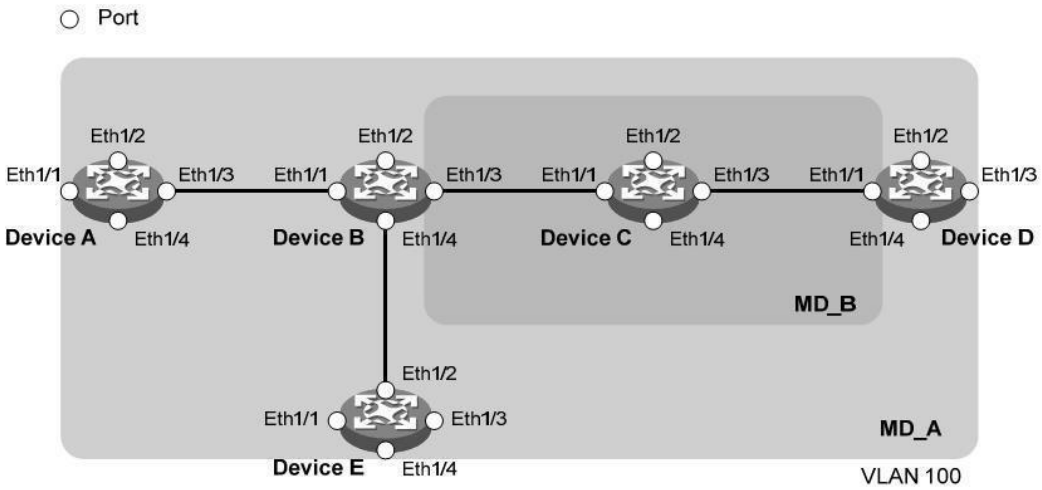


Рисунок 1-1

В практическом применении для рационального планирования домена обслуживания: как показано на рисунке 1-1, MD_B вложен в домен обслуживания MD_A, для обнаружения подключения в MD_A, MD_A CFM PDU требуется для пересечения MD_B, его необходимо MD_A лучше, чем MD_B высокоуровневой конфигурации. Таким образом, MD_A CFM PDU может проходить через MD_B, чтобы достичь всей MD_A управления сбоями подключения, и MD_B CFM PDU не будет распространяться на MD_A.

Классификация домена обслуживания делает местоположение неисправности более удобным и точным, как показано на рисунке 1-1, MD_B встроены в домен обслуживания домена обслуживания MD_A, если будет установлено, что ссылка находится на границе MD_A указывает на то, что в домене неисправности оборудования может произойти сбой в устройстве A ~ Устройстве E пять устройств. В это время, если не обнаружено в MD_B звено на границе диапазона неисправностей сводится к устройству B и устройству D трех комплектов оборудования; с другой стороны, если MD_B оборудование работает должным образом, оно может, по крайней мере, определить, что устройство C не неисправно.»

2 Комплект технического обслуживания

В домене обслуживания ассоциация обслуживания (MA) может быть настроена в соответствии с требованиями. Каждый набор обслуживания представляет собой набор точек обслуживания в домене. Набор обслуживания помечен "имя домена обслуживания + имя набора обслуживания".

Набор обслуживания обслуживает VLAN, а сообщение, отправленное точкой обслуживания обслуживания, имеет тег VLAN. Между тем, централизованная точка обслуживания может получать сообщение, отправленное другими точками обслуживания в наборе технического обслуживания.

3 Точка технического обслуживания

Точка обслуживания (Maintenance Point, MP) в конфигурации порта, относится к набору обслуживания, обслуживание можно разделить на конечную точку (Maintenance Association End Point, MEP) и обслуживание средней точки (Maintenance Association Intermediate Point, MIP) на две.

1) Конечная точка обслуживания

Конечная точка обслуживания идентифицируется целым числом, называемым MEP ID, которое определяет область и границу домена обслуживания. Набор обслуживания и домен обслуживания,

принадлежащие конечной точке обслуживания, определяют атрибут VLAN и уровень сообщения, отправляемого конечной точкой обслуживания.

Уровень конечной точки определяет уровень сообщения, которое она может обрабатывать, а уровень сообщения, поддерживающего конечную точку, является уровнем конечной точки обслуживания. Когда конечная точка обслуживания получает сообщение выше своего уровня, не обработанное, а в соответствии с его первоначальным путем пересылки; и если полученное сообщение меньше или равно уровню обслуживания, конечная точка больше не будет поддерживать конечную точку пересылки для соответствующей обработки, чтобы гарантировать, что низкоуровневое сообщение домена обслуживания не будет распространяться в домен высокого уровня обслуживания.

Конечные точки обслуживания имеют направленность, которую можно разделить на два типа: экстравертный MEP и внутренний MEP. Направление обслуживания конечной точки указывает расположение домена обслуживания относительно порта.

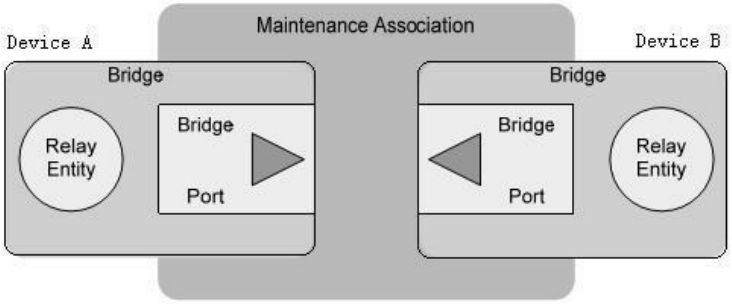


Рис.1-2 Принципиальная схема исходящего MEP

Как показано на рисунке 1-2, исходящая конечная точка обслуживания отправляет сообщение наружу через свой порт,

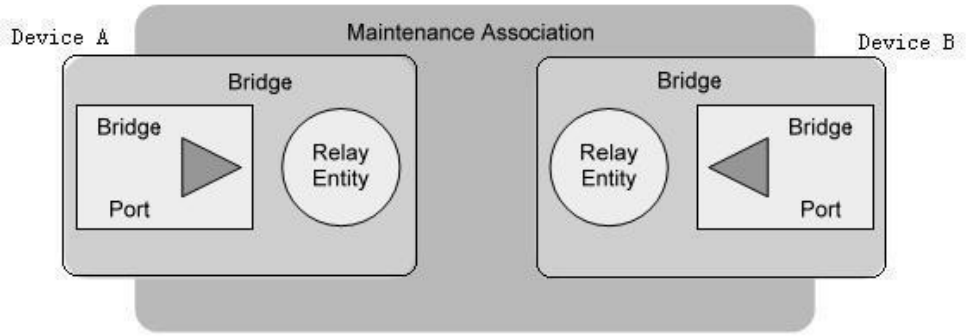


Рис. 1-3

1-3, конечная точка внутреннего обслуживания не отправляет сообщения наружу через свои порты, а отправляет сообщения наружу с других портов устройства.

2) Промежуточная точка технического обслуживания

Промежуточная точка обслуживания расположена в домене обслуживания и не может активно отправлять сообщения протокола CFM, но может обрабатывать сообщения протокола CFM и реагировать на них. Ведение набора обслуживания и домена обслуживания промежуточной точки определяет атрибут VLAN и уровень полученного сообщения промежуточной точки обслуживания. Обслуживание промежуточной точки может использоваться с конечной точкой обслуживания для выполнения функций, аналогичных Ping и tracert. Аналогичное обслуживание конечных точек, при сохранении средней точки полученного сообщения выше их уровня, обрабатывается не в

соответствии с его исходным путем вперед; и когда полученное сообщение меньше или равно их собственному промежуточному уровню обслуживания баллов, будет обработано.

Как показано на рисунке 1-4, это иерархическая конфигурация CFM, предполагающая, что все шесть устройств являются только двумя портами, а распределение конечных точек обслуживания и промежуточных точек обслуживания в некоторых портах, таких как точки обслуживания конфигурации порта B 1, выглядят следующим образом: Уровень 5, уровень обслуживания промежуточной точки 3 в конечной точке обслуживания, уровень 2 - уровень 0 конечных точек обслуживания и исходящей конечной точки обслуживания. На графике есть четыре уровня областей обслуживания. Область обслуживания идентификационного номера выше, а диапазон регулирования широк; Зона обслуживания идентификационного номера меньше, а диапазон управления мал.

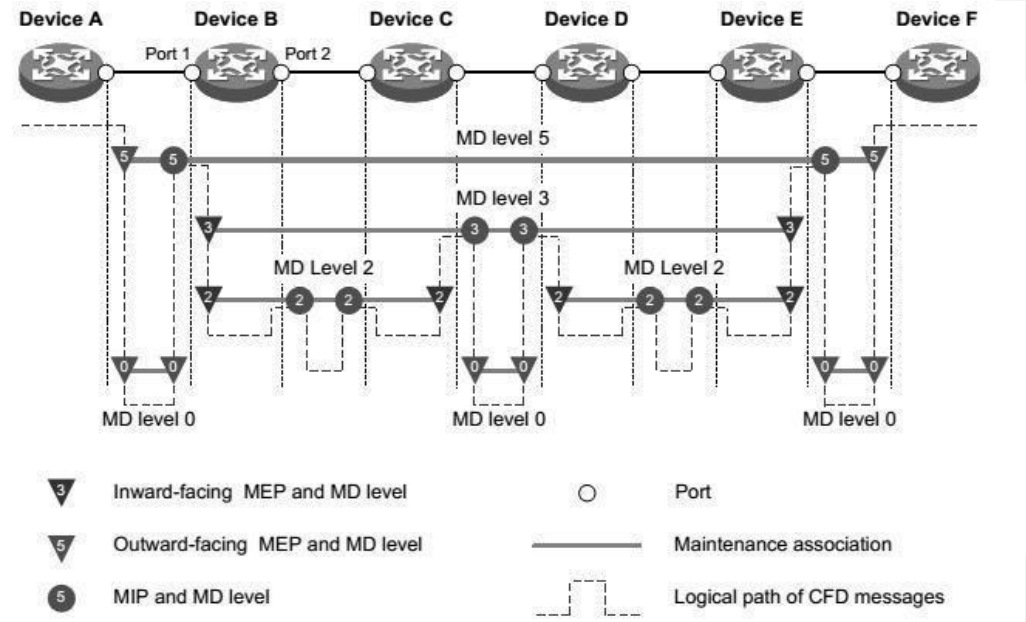


Рисунок 1-4 Иерархическая конфигурация точек обслуживания

4 Ведение списка конечных точек

В списке находится одна и та же конечная точка обслуживания, позволяющая настраиваться в пределах набора локальных конечных точек обслуживания и необходимость мониторинга набора конечных точек удаленного обслуживания, который определяет диапазон набора конечных точек обслуживания обслуживания: разные устройства на одном и том же обслуживании в пределах набора всех конечных точек обслуживания должны быть включены в этот список, MEP и ID не повторяются. Если конечная точка обслуживания получает сообщение CCM (Continuity Check Message, Continuity Check Message) от удаленного устройства, а конечная точка обслуживания отсутствует в списке конечных точек обслуживания того же набора обслуживания, то сообщение отбрасывается.

5 Экземпляр службы

Экземпляр службы представлен целым числом, представляющим набор обслуживания в домене обслуживания. Домен обслуживания и набор обслуживания определяют атрибут level и атрибут VLAN сообщения, обрабатываемого точкой обслуживания в экземпляре службы.

26.1.2 Различные функции CFM

Эффективное применение обнаружения ошибок подключения основано на разумном развертывании и настройке сети. Его функция реализована между настроенными точками обслуживания, в том числе:

- Функция непрерывного тестирования (Continuity Check，CC)
- Функция замыкания (Loopback，LB）
- Функция отслеживания ссылок（Linktrace，LT）

1. Функция непрерывного тестирования

Функция обнаружения непрерывности используется для обнаружения связи между конечными точками обслуживания. Сбои подключения могут быть вызваны сбоями устройств или ошибками конфигурации. Реализация этой функции заключается в том, что сообщение CCM периодически отправляется из конечной точки обслуживания, которая является многоадресным сообщением, и другие конечные точки обслуживания того же набора обслуживания получают сообщение, и получается удаленное состояние. Если конечная точка обслуживания не получает сообщение CCM от удаленной конечной точки обслуживания в течение 3,5 циклов передачи пакетов CCM, соединение будет проблематичным, и будет выведен отчет журнала. При обслуживании нескольких конечных точек обслуживания в домене для отправки пакетов CCM реализовано обнаружение связи между многоточечной и многоточечной точками.

2. Функция замыкания

Функция замыкания, аналогичная функции ping IP-уровня, используется для проверки состояния соединения между локальным устройством и удаленным устройством. Функция реализации заключается в следующем: обслуживание конечной точки (Loopback Message, LBM отправляет сообщение в удаленный цикл обслуживания), и в соответствии с концом может получить обратную связь LBR (Loopback Reply, loopback reply message) для проверки состояния связи. И LBM, и LBR являются одноадресными сообщениями.

3. Функция отслеживания ссылок

Функция отслеживания ссылок используется для определения источника к целевому пути обслуживания конечной точки, это отправляется источником: LTM (Linktrace Message) обслуживание на целевую конечную точку, обслуживание после того, как конечная точка LTM промежуточной точки получила сообщение, отправит LTR (Linktrace Reply, link tracking response message) на сторону источника, источник основан на полученном LTR для определения пути к обслуживанию целевой конечной точки. LTM — это многоадресное сообщение, а LTR — одноадресное сообщение.

26.2 Краткое введение в задачу настройки CFM

Перед настройкой функции CFM спланируйте сеть следующим образом:

- Домен обслуживания всей сети оценивается для определения границы домена обслуживания каждого уровня.
- Определите имя каждого домена обслуживания, и один и тот же домен обслуживания будет иметь одно и то же имя на разных устройствах.
- В соответствии с VLAN, которую необходимо отслеживать, определяется набор обслуживания в каждом домене обслуживания.

- Определите имя каждого набора обслуживания, и один и тот же набор обслуживания в одном домене будет иметь одинаковое имя на разных устройствах.
- Конечная точка обслуживания должна планироваться на пограничном порту домена обслуживания и набора обслуживания, а промежуточная точка обслуживания может быть запланирована на неграничном оборудовании или порту.
- Список конечных точек удаленного обслуживания для определения конечных точек обслуживания. После завершения планирования сети настройте следующее.

Задача настройки		Подробная конфигурация
CFM базовая конфигурация	Включить функцию CFM	1.3.1
	Экземпляр службы конфигурации	1.3.2
	Конечная точка обслуживания конфигурации	1.3.3
	Промежуточная точка обслуживания конфигурации	1.3.4
Настройка различных функций CFM	Функция определения непрерывности конфигурации	1.4.1
	Функция замыкания конфигурации	1.4.2
	Настройка функции отслеживания ссылок	1.4.3

Примечание:

- Порт, заблокированный протоколом STP, не может принимать, отправлять и отвечать на пакет протокола CFM; но если порт настроен на исходящий MEP, то даже если порт был заблокирован протоколом STP, он все равно будет получать и отправлять сообщение CCM.
- Только Ethernet порты поддерживают настройку функций CFM.

26.3 Базовая конфигурация CFM

26.3.1 Включение функции CFM

Команда	Описание	Режим CLI
cfm enable	Включите функцию CFM. Завершение работы по умолчанию.	Режим глобального конфигурирования

26.3.2 Экземпляр службы конфигурации

Перед настройкой конечной точки обслуживания и промежуточной точки необходимо сначала настроить экземпляр службы. Экземпляр службы представлен целым числом, представляющим набор обслуживания в домене обслуживания. Домен обслуживания и набор обслуживания определяют атрибут level и атрибут VLAN сообщения, обрабатываемого точкой обслуживания в экземпляре службы.

Создание доменов обслуживания, наборов обслуживания и экземпляров обслуживания в строгом соответствии со следующим порядком.

Команда	Описание	Режим CLI
cfm md <md-name> level <level-value>	Создайте обслуживающий домен. По умолчанию обслуживающего домена нет.	Режим глобального конфигурирования
cfm ma <ma-name> md <md-name> vlan <vlan-id>	Создайте набор обслуживания. Набор обслуживания не создан по умолчанию	Режим глобального конфигурирования
cfm service-instance <instance-id> md <md-name> ma <ma-name>	Создание экземпляров службы. Экземпляр службы по умолчанию не создан	Режим глобального конфигурирования

26.3.3 Конечная точка обслуживания конфигурации

Конечная точка обслуживания является функциональной сущностью в экземпляре службы, а функция CFM в основном реализуется в работе конечной точки обслуживания. Он реализует функции CC, LB и LT, а также предупреждает ложное сообщение CCM и перекрестное соединение. Поскольку конечная точка обслуживания настраивается на экземпляре службы, уровень домена обслуживания и атрибут VLAN, представленный экземпляром службы, естественным образом становятся атрибутами обслуживания конечной точки. После создания конечной точки обслуживания необходимо настроить список конечных точек удаленного обслуживания указанной конечной точки обслуживания, а список конечных точек удаленного обслуживания представляет собой коллекцию конечных точек удаленного обслуживания, которые необходимо отслеживать в одном наборе обслуживания.

Команда	Описание	Режим CLI
cfm mep <mep-id> service-instance <instance-id> {inbound | outbound}	Создание конечных точек обслуживания. На порту по умолчанию нет конечной точки обслуживания.	Режим конфигурирования интерфейса
cfm remote-meplist <mep-list> service-instance <instance-id> mep <mep-id>	Список конечных точек удаленного обслуживания, настроенных с указанными конечными точками обслуживания. По умолчанию отсутствует список конечных точек обслуживания для порта.	Режим конфигурирования интерфейса
cfm mep service-instance <instance-id> mep <mep-id> enable	Включите обслуживание конечных точек. Конечная точка обслуживания по умолчанию закрыта.	Режим конфигурирования интерфейса

Примечание:

● После включения конечной точки конечная точка обслуживания обрабатывает полученные пакеты CCM.

26.3.4 Промежуточная точка обслуживания конфигурации

Промежуточная точка обслуживания — это функциональная сущность в экземпляре службы, которая отвечает на сообщения LBM и LTM.

Обслуживание средней точки представляет собой систему в соответствии с правилами, в каждом порту создаваемые автоматически, правила создания следующие: если в средней точке нет обслуживания порта, то в соответствии с уровнем от низкого до высокого порядка проверяет каждое обслуживание заданного домена, как показано на рисунке 1-5 и в соответствии с процессом принятия решения о создании обслуживания (промежуточная точка в той же VLAN).

Рисунок 1-5, поддерживающий процесс создания промежуточной точки

Пожалуйста, настройте и поддерживайте правила создания промежуточных точек в соответствии с планированием сети.

Команда	Описание	Режим CLI
cfm mip-rule {explicit | default} service-instance <instance-id>	Создание правил для промежуточных точек обслуживания конфигурации. По умолчанию отсутствуют правила обслуживания для создания промежуточных точек и промежуточная точка обслуживания создания.	Режим глобального конфигурирования

Примечание:

После настройки правил создания для обслуживания промежуточных точек любое из следующих условий может вызвать создание или удаление промежуточной точки обслуживания:

- Включить функцию CFM.
- Создание или удаление конечных точек обслуживания на порту.
- Изменяется свойство VLAN порта.
- Изменяются правила создания для поддержания промежуточных точек.

26.4 Настройка различных функций CFM

Перед настройкой различных функций CFM необходимо завершить базовую конфигурацию CFM.

26.4.1 Функция определения непрерывности конфигурации

Настроив функцию обнаружения непрерывности, сообщения CCM могут отправляться между конечными точками обслуживания для определения состояния подключения между конечными точками обслуживания, чтобы реализовать управление подключением канала.

Команды	Описание	Режим CLI
cfm cc interval <interval-value> service-instance <instance-id>	Значение интервала времени в сообщении CCM, отправляемом конечной точкой обслуживания конфигурации. По умолчанию значение временного домена в сообщении CCM, отправленном конечной точкой обслуживания, равно 4.	Режим глобального конфигурирования
cfm cc service-instance <instance-id> mep <mep-id> enable	Функция отправки сообщений CCM, которая может поддерживать конечную точку. По умолчанию функция отправки сообщений CCM для обслуживания конечных точек закрыта.	Режим конфигурирования интерфейса

Связь между значением временного домена (интервального домена) в сообщении CCM, отправленном обслуживанием конечной точки, и интервалом времени отправки CCM и временем удаленного тайм-аута MEP показана в таблице 1-1.

Таблица 1-1 соотношение между значением временного интервала и временным интервалом отправки CCM и примечанием о времени ожидания MEP:

- Конечная точка сообщения CCM должна быть одинаковой в конечной точке обслуживания одного и того же домена обслуживания и набора обслуживания на разных устройствах.
- Если значение временного домена отправки сообщения CCM в конечную точку обслуживания равно 3, рекомендуется не настраивать больше конечных точек обслуживания в одном домене и наборе обслуживания, в противном случае это повлияет на производительность всего устройства.

26.4.2 Функция замыкания конфигурации

Настроив функцию замыкания, можно проверить состояние связи, чтобы проверить подключение канала.

Команда	Описание	Режим CLI
cfm loopback service-instance <instance-id> mep <mep-id> { target-mep <target-mep-id> | target-mac <mac-address>} [number <number>]	Включите функцию замыкания для проверки состояния ссылки.	Привилегированный режим

26.4.3 Настройка функции отслеживания ссылок

Настроив функцию отслеживания ссылок, можно найти путь между указанной точкой обслуживания и конечной точкой обслуживания назначения, таким образом, можно реализовать местоположение сбоя связи.

Он включает в себя следующие две функции:

- Найдите путь от указанной конечной точки обслуживания к конечной точке обслуживания назначения: отправив сообщение LTM из назначенной конечной точки обслуживания в конечную точку обслуживания назначения и обнаружив сообщение LTR ответа, чтобы определить путь между устройствами.
- Автоматическое сообщение отслеживания канала передачи: включите эту функцию, сохраняя в конце 3.5 CCM период отправки пакетов не полученное сообщение, отправленное на удаленное обслуживание конечной точки CCM, которые определяют ту же ошибку удаленного обслуживания подключения терминалов, будут отправлять сообщение LTM сообщение LTM message (цель для конечных точек удаленного обслуживания, поле TTL сообщения LTM максимум 255), через ответ на сообщение LTR, чтобы найти обнаружение неисправностей.

Команда	Описание	Режим CLI
cfm linktrace service-instance <instance-id> mep <mep-id> {target-mep <target-mep-id> | target-mac <mac-address> } [ttl<ttl-value>] [hw-only]	Найдите путь от указанной конечной точки обслуживания к конечной точке обслуживания назначения.	Привилегированный режим
cfm linktrace auto-detection [size <size-value>]	Включите функцию автоматической отправки сообщений отслеживания ссылок. По умолчанию функция автоматического отслеживания ссылок на отправку закрыта.	Режим глобального конфигурирования

26.5 CFM дисплей и обслуживание

После завершения приведенной выше конфигурации, выполнив команду show в любом представлении, можно отобразить работу CFM после настройки, а также проверить эффект конфигурации, проверив отображаемую информацию.

Команда	Описание	Режим CLI
show cfm status	Отображает состояние CFM.	Привилегированный режим
show cfm md	Отображение сведений о конфигурации обслуживаемого домена.	Привилегированный режим
show cfm ma [[<ma-name>] md <md-name>]	Отображение информации о конфигурации комплекта технического обслуживания.	Привилегированный режим
show cfm service-instance [<instance-id>]	Отображение сведений о конфигурации для экземпляров служб.	Привилегированный режим
show cfm mp [interface <interface-name>]	Отображение информации о точке обслуживания.	Привилегированный режим
show cfm mep <mep-id> service-instance <instance-id>	Отображает атрибуты и сведения о выполнении конечной точки обслуживания.	Привилегированный режим
show cfm linktrace-reply [service-instance <instance-id> [mep <mep-id>]]	Сведения о сообщениях LTR, полученные из конечной точки обслуживания дисплея.	Привилегированный режим
show cfm remote-mep service-instance <instance-id> mep <mep-id>	Отображение сведений о конечных точках удаленного обслуживания	Привилегированный режим
show cfm linktrace-reply auto-detection [size <size-value>]	Отображение содержимого сообщения LTR, полученного автоматически путем отправки сообщения LTM	Привилегированный режим

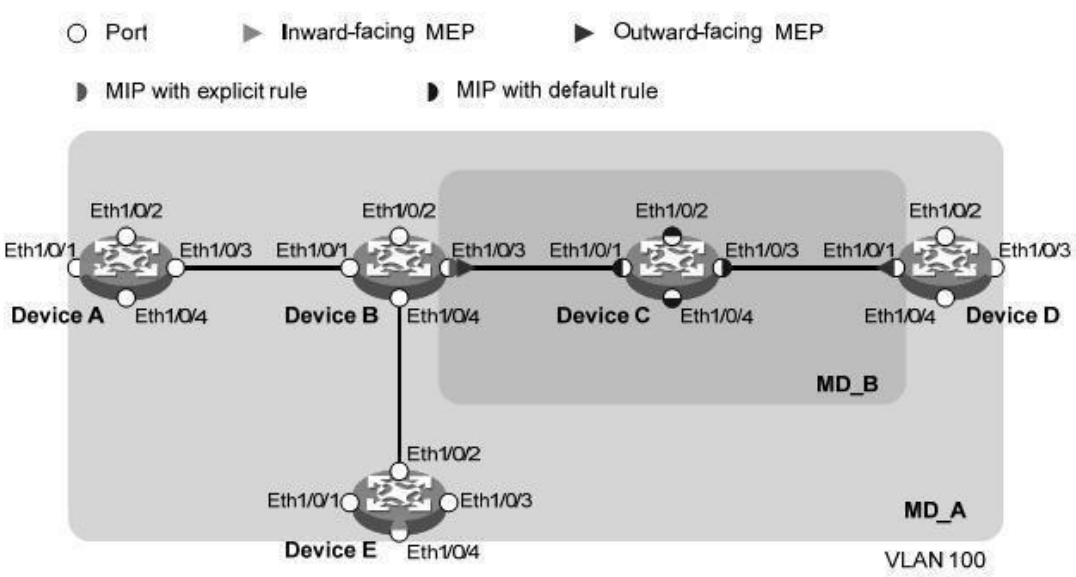
26.6 Типовые примеры конфигурации

Требования к сети:
Состоящая из пяти комплектов оборудования сеть разделена на MD_A и MD_B два обслуживающих домена, его уровни были 5 и 3, порт Ethernet1/0/1 к каждому устройству Ethernet1/0/4 относятся к VLAN 100, а обслуживание домена обслуживает VLAN.

Ethernet1/0/4 Устройство A Устройство Ethernet1/0/1, D Ethernet1/0/3 и Устройство E MD_A пограничных портов, и в этих портах они сконфигурированы для обслуживания конечной точки; граница порта MD_B для устройства B Ethernet1/0/3 и устройства D Ethernet1/0/1, а также в конфигурации порта исходящей конечной точки.
Необходимо спланировать промежуточную точку обслуживания MD_A на устройстве B и настроить ее только на порту с низкоуровневыми конечными точками обслуживания. Согласно этому плану, точка обслуживания MD_A настраивается на устройстве B из-за конфигурации конечной точки обслуживания MD_B на устройстве B Ethernet1/0/3, и правило создается как явное правило.

Необходимо спланировать промежуточную точку обслуживания MD_B на устройстве C и настроить ее на всех портах. Согласно этому плану, промежуточная точка обслуживания MD_B настраивается на устройстве C, а правилом ее создания является правило Default.

Использование функции обнаружения непрерывности для обнаружения всех MD_A и MD_B в поддержании связи между конечными точками, для связывания при обнаружении сбоев, использование функции замыкания для определения местоположения неисправности; или ко всему состоянию сети после получения, используя функцию поиска пути ссылки или отслеживания местоположения неисправности.
Схема сети:



Этапы настройки:

1) Настройка VLAN и портов

VLAN 100 создается на каждом устройстве и настроенные порты Ethernet1/0/1 ~ Ethernet1/0/4 принадлежат VLAN 100.

2) Включить функцию CFM

Включить функцию CFM на устройстве A. устройство A> config t

[DeviceA] cfm enable

Устройство B~Device Конфигурация аналогична конфигурации устройства A, и процесс настройки немного лучше.

3) Экземпляр службы конфигурации

Создание MD_A обслуживающего домена с уровнем 5 на устройстве A, создание MA_A набора обслуживания для VLAN 100 в MD_A и создание экземпляра службы для MD_A и MA_A 1

[DeviceA] cfm md MD_A level 5
[DeviceA] cfm ma MA_A md MD_A vlan 100
[DeviceA] cfm service-instance 1 md MD_A ma MA_A

Конфигурация устройства E аналогична конфигурации устройства A, и процесс настройки немного лучше.

В устройстве B для создания MD_A домена обслуживания уровня 5, созданного в MD_A службы обслуживания VLAN 100 для установки MA_A, а для MD_A и MA_A для создания экземпляра службы 1; , чтобы создать MD_B домена обслуживания уровня 3, созданную в службе обслуживания VLAN 100 MD_B для установки MA_B, а также для MD_B и MA_B создать экземпляр службы 2.

[DeviceB] cfm md MD_A level 5
[DeviceB] cfm ma MA_A md MD_A vlan 100
[DeviceB] cfm service-instance 1 md MD_A ma MA_A
[DeviceB] cfm md MD_B level 3
[DeviceB] cfm ma MA_B md MD_B vlan 100
[DeviceB] cfm service-instance 2 md MD_B ma MA_B

Конфигурация устройства D аналогична конфигурации устройства B, а процесс настройки немного лучше.

Создание домена обслуживания MD_B с уровнем 3 на устройстве C, создание набора обслуживания MA_B для VLAN 100 в MD_B и создайте экземпляр службы для MD_B и MA_B 2

[DeviceC] cfm md MD_B level 3
[DeviceC] cfm ma MA_B md MD_B vlan 100
[DeviceC] cfm service-instance 2 md MD_B ma MA_B

4) Конечная точка обслуживания конфигурации

Создайте внутреннюю конечную точку обслуживания 1001 в экземпляре службы 1 на порту устройства A Ethernet1/0/1, настройте список конечных точек удаленного обслуживания, соответствующий конечной точке обслуживания 1001, а затем включите обслуживание конечной точки 1001.

[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm mep 1001 service-instance 1 inbound
[DeviceA-Ethernet1/0/1] cfm remote-meplist 4002 5001 service-instance 1 mep 1001
[DeviceA-Ethernet1/0/1] cfm mep service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit

На порту устройство B Ethernet1/0/3 создайте исходящую конечную точку обслуживания 2 в экземпляре службы 2001, настройте список конечных точек удаленного обслуживания,

соответствующий конечной точке обслуживания 2001, а затем включите конечную точку обслуживания 2001.

[DeviceB] interface ethernet 1/0/3
[DeviceB-Ethernet1/0/3] cfm mep 2001 service-instance 2 outbound
[DeviceB-Ethernet1/0/3] cfm remote-meplist 2001 4001 service-instance 2 mep 2001
[DeviceB-Ethernet1/0/3] cfm mep service-instance 2 mep 2001 enable
[DeviceB-Ethernet1/0/3] quit

#On порт Ethernet1/0/1 устройства D, создайте исходящую конечную точку обслуживания 2 в экземпляре службы 4001, настройте список конечных точек удаленного обслуживания, соответствующий конечной точке обслуживания 4001, а затем включите конечную точку обслуживания 4001. Создайте внутреннюю конечную точку обслуживания 4002 в экземпляре службы 1 на порту Ethernet1/0/3 и одновременно создайте список конечных точек удаленного обслуживания 4002.

[DeviceD] interface ethernet 1/0/1
[DeviceD-Ethernet1/0/1] cfm mep 4001 service-instance 2 outbound
[DeviceD-Ethernet1/0/1] cfm remote-meplist 2001 service-instance 2 mep 4001
[DeviceD-Ethernet1/0/1] cfm mep service-instance 2 mep 4001 enable
[DeviceD-Ethernet1/0/1] quit
[DeviceD] interface ethernet 1/0/3
[DeviceD-Ethernet1/0/3] cfm mep 4002 service-instance 1 inbound
[DeviceD-Ethernet1/0/3] cfm remote-meplist 1001 5001 service-instance 1 mep 4002
[DeviceD-Ethernet1/0/3] cfm mep service-instance 1 mep 4002 enable
[DeviceD-Ethernet1/0/3] quit

#On порт Ethernet1/0/4 устройства E, создайте и включите внутреннюю конечную точку обслуживания 1 в экземпляре службы 5001 и настройте список конечных точек удаленного обслуживания в экземпляре службы 1.

[DeviceE] interface ethernet 1/0/4
[DeviceE-Ethernet1/0/4] cfm mep 5001 service-instance 1 inbound
[DeviceE-Ethernet1/0/4] cfm remote-meplist 1001 service-instance 1 mep 5001
[DeviceE-Ethernet1/0/4] cfm mep service-instance 1 mep 5001 enable [DeviceE-Ethernet1/0/4] quit

5) Промежуточная точка обслуживания конфигурации

Правила конфигурации для обслуживания промежуточных точек настроены как явные правила в экземпляре службы 1 устройства B.

[DeviceB] cfm mip-rule explicit service-instance 1

Правила конфигурации для обслуживания промежуточных точек настроены как правила по умолчанию в экземпляре службы 2 устройства C.

[DeviceC] cfm mip-rule default service-instance 2

6) Функция определения непрерывности конфигурации

На порту Ethernet1/0/1 устройства A функция отправки сообщений CCM конечной точки 1001 поддерживается в экземпляре службы включения 1.

[DeviceA] interface ethernet 1/0/1
[DeviceA-Ethernet1/0/1] cfm cc service-instance 1 mep 1001 enable
[DeviceA-Ethernet1/0/1] quit

На порту Ethernet1/0/3 устройства B функция отправки сообщений CCM конечной точки 2001 поддерживается в экземпляре службы включения 2.

[DeviceB] interface ethernet 1/0/3

[DeviceB-Ethernet1/0/3] cfm cc service-instance 2 mep 2001 enable
[DeviceB-Ethernet1/0/3] quit

На порту Ethernet1/0/1 устройства D функция отправки сообщений CCM конечной точки 4001 поддерживается в экземпляре 2 службы включения, а функция отправки сообщений CCM конечной точки обслуживания 4002 в экземпляре 1 службы включения включена на порту Ethernet1/0/3.

[DeviceD] interface ethernet 1/0/1
[DeviceD-Ethernet1/0/1] cfm cc service-instance 2 mep 4001 enable
[DeviceD-Ethernet1/0/1] quit
[DeviceD] interface ethernet 1/0/3
[DeviceD-Ethernet1/0/3] cfm cc service-instance 1 mep 4002 enable
[DeviceD-Ethernet1/0/3] quit

На порту Ethernet1/0/4 устройства E функция отправки сообщений CCM конечной точки 5001 поддерживается в экземпляре службы включения 1.

[DeviceE] interface ethernet 1/0/4
[DeviceE-Ethernet1/0/4] cfm cc service-instance 1 mep 5001 enable
[DeviceE-Ethernet1/0/4] quit

7) Проверка эффекта конфигурации

Когда неисправность соединения обнаруживается функцией обнаружения непрерывности, функция замыкания может использоваться для обнаружения неисправности. Например:

Функция зацикливания включена на устройстве A для проверки состояния связи конечных точек с 1001 по 5001, поддерживаемых в экземпляре службы 1.

[DeviceA] cfm loopback service-instance 1 mep 1001 target-mep 5001
Loopback to 0010-FC00-6512 with the sequence number start from 43404:
Reply from 0010-FC00-6512: sequence number = 43404
Reply from 0010-FC00-6512: sequence number=43405
Reply from 0010-FC00-6512: sequence number=43406
Reply from 0010-FC00-6512: sequence number=43407
Reply from 0010-FC00-6512: sequence number=43408
Send:5 Received:5 Lost:0

После получения всего состояния сети с помощью функции обнаружения непрерывности функция отслеживания канала может быть использована для поиска пути или обнаружения неисправности. Например:

Найдите путь для обслуживания конечных точек с 1001 по 5001 в экземпляре службы 1 устройства A.

[DeviceA] cfm linktrace service-instance 1 mep 1001 target-mep 5001
Linktrace to MEP 5001 with the sequence number 1001-43462

MAC Address	TTL	Last MAC	Relay Action
0010-FC00-6512	63	0010-FC00-6511	Hit
0010-FC00-6511	62	0010-FC00-6510	FDB

Двадцать седьмая глава

Базовая конфигурация IPv6

Коммутаторы поддерживают основные функции IPv6, включая двухуровневую пересылку IPv6, функцию IPv6 ND. В этой главе описывается, как настроить IPv6, включая следующие:

- Профиль IPv6
- Профиль задачи базовой конфигурации IPv6
- Настройка базовой функциональности IPv6
- Настройка протокола обнаружения соседей IPv6
- Конфигурация статической маршрутизации IPv6
- Отображение и обслуживание IPv6

27.1 Профиль IPv6

IPv6 (Internet Protocol Version 6, Internet Protocol version 6) — стандартный протокол второго поколения протокола сетевого уровня, также известный как IPng (IP Next Generation, следующее поколение Интернета), это IETF (Internet Engineering Task Force, Internet engineering task force) набор стандартизированного проектирования, является модернизированной версией IPv4. Наиболее существенное различие между IPv6 и IPv4 заключается в том, что длина IP-адреса увеличивается с 32 бит до 128 бит.

27.1.1 Характеристики протокола IPv6

1 Упрощенный формат заголовка сообщения

Уменьшая или перемещая некоторые поля в заголовке IPv4 в расширенный заголовок, длина заголовка основного сообщения IPv6 уменьшается. IPv6 использует фиксированную длину заголовка базового пакета, что упрощает переадресующее оборудование для обработки пакетов IPv6 и повышает эффективность пересылки. Хотя длина IPv6-адреса в четыре раза превышает длину IPv4-адреса, длина основного заголовка сообщения IPv6 составляет всего 40 байт, что в два раза превышает длину заголовка IPv4 (за исключением поля параметра).

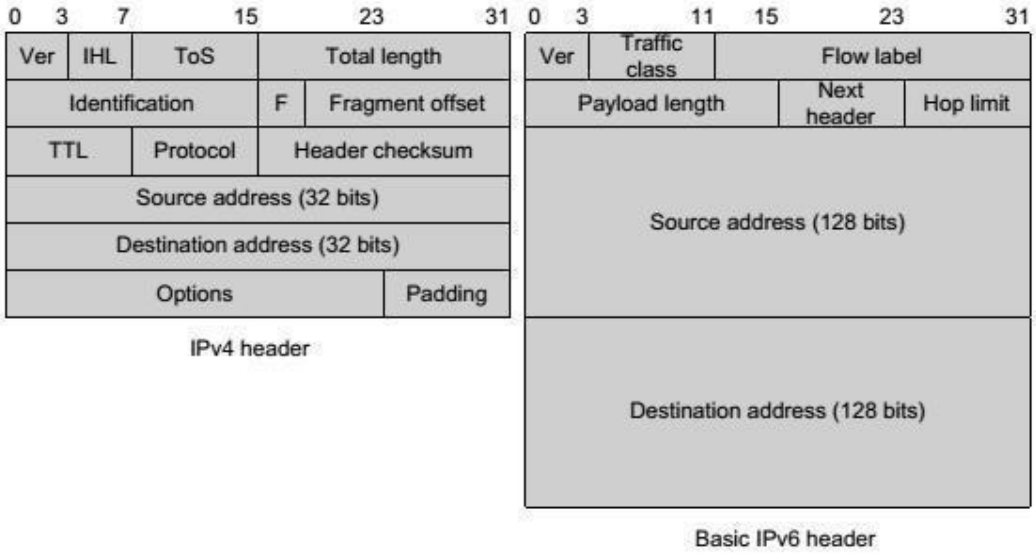


Рисунок 1-1 Сравнение заголовка IPv4 и базового формата заголовка сообщения IPv6

2 Много адресного пространства

Длина адреса источника и назначения IPv6 составляет 128 бит (16 байт). Он может обеспечить более 3,4 * 1038 возможных адресных пространств, полностью удовлетворить потребности многоуровневого адресного деления и адресного распределения частных сетей в рамках публичных сетей и организаций.

3 Иерархическая структура адресов

Адресное пространство IPv6 принимает иерархическую структуру адресов, что выгодно для быстрого поиска маршрутизации и может эффективно уменьшить системный ресурс, занимаемый таблицей маршрутизации IPv6, с помощью агрегации маршрутов.

4 Автоматическая настройка адресов

Чтобы упростить настройку хоста, IPv6 поддерживает конфигурацию адресов с отслеживанием состояния и конфигурацию адресов без отслеживания состояния:

1) Конфигурация адреса с отслеживанием состояния относится к получению IPv6-адресов и связанных с ними сведений с сервера (например, DHCP-сервера);
2) Конфигурация адреса без сохранения состояния означает, что хост автоматически настраивает IPv6-адрес и связанную с ним информацию в соответствии с его адресом канального уровня и префиксной информацией, выданной маршрутизатором.

В то же время хост также может сформировать локальный адрес ссылки в соответствии со своим собственным адресом канального уровня и префиксом по умолчанию (FE80:: /10), чтобы реализовать связь с другими хостами в цепочке.

5 Встроенная безопасность

IPv6 использует IPSec в качестве стандартной главы расширения, обеспечивая сквозные функции безопасности. Эта функция также обеспечивает стандарт для решения проблем сетевой безопасности и улучшает взаимодействие между различными приложениями IPv6.

6 Поддержка QoS

Поле метки потока (Flow Label) заголовка IPv6 реализует идентификацию трафика и позволяет устройству идентифицировать пакеты в трафике и обеспечивать специальную обработку.

7 Улучшенный механизм обнаружения соседей

Протокол обнаружения соседей IPv6 группой сообщений ICMPv6 (Internet Control Message Protocol for IPv6, протокол управляющих сообщений Интернета) управляет информационным взаимодействием соседних узлов (т.е. узлов на одном канале). Он заменяет ARP (протокол разрешения адресов), обнаружение маршрутизатора ICMPv4 и сообщение перенаправления ICMPv4 и предоставляет ряд других функций.

8 Гибкие расширенные заголовки

IPv6 отменяет поле параметра в заголовке IPv4 и вводит множество расширенных заголовков, что повышает эффективность обработки и значительно повышает гибкость IPv6, а также обеспечивает хорошую масштабируемость протокола IP. Поле параметра в заголовке IPv4 составляет не более 40 байт, в то время как размер заголовка расширения IPv6 ограничен размером сообщения IPv6.

27.1.2 Введение в IPv6-адреса

1. Представление IPv6-адреса

IPv6-адрес представлен в виде серии из 16-битных шестнадцати двоичных чисел, разделенных двоеточиями (:). Каждый IPv6-адрес разделен на 8 групп, каждая из которых представлена 16 битами в 4 шестнадцати десятичных числах, а группы и группы разделены двоеточиями, такими как 2001:0000:130F:0000:0000:09C0:876A:130B.

Чтобы упростить представление IPv6-адреса, «0» в IPv6-адресе может быть обработан следующим образом:

1) Преамбула «0» в каждой группе может быть опущена, то есть приведенный выше адрес может быть записан как 2001:0:130F:0:0:9C0:876A:130B.
2) Если адрес содержит группу из двух или более последовательных 0, его можно заменить двойным двоеточием ":: "то есть указанный выше адрес может быть записан как 2001:0:130F:: 9C0:876A:130B.

заметка:

Только одно двойное двоеточие может быть использовано в IPv6-адресе"::" , в противном случае, когда устройство преобразует ":" в "0" для восстановления 128-битного адреса, невозможно определить число "0", представленное "::".

IPv6-адрес состоит из двух частей: префикса адреса и идентификатора интерфейса. Префикс адреса эквивалентен части поля номера сети в IPv4-адресе, а идентификатор интерфейса соответствует части номера хоста в IPv4-адресе.

Префикс адреса представлен как: IPv6 адрес / длина префикса. Среди них IPv6-адрес — это любая форма, указанная ранее, а длина префикса — десятичное число, которое представляет собой самое левое число IPv6-адреса — префикс адреса.

2. Классификация адресов IPv6

В IPv6 существует три типа адресов: адрес одноадресной рассылки, адрес многоадресной рассылки и адрес любой рассылки.

1) Адрес одноадресной рассылки (unicast): используется для уникальной идентификации интерфейса, аналогичного адресу одноадресной рассылки IPv4. Сообщение данных, отправленное на одноадресный адрес, будет передано на интерфейс, идентифицированный этим адресом.

2) Адрес многоадресной рассылки (multicast): используется для идентификации набора интерфейсов (обычно это группа интерфейсов, принадлежащих разным узлам), аналогично адресу многоадресной рассылки IPv4. Пакеты данных, отправленные на адрес многоадресной рассылки, передаются на все интерфейсы, идентифицированные этим адресом.
3) Любой адрес (anycast): используется для идентификации набора интерфейсов (обычно эта группа интерфейсов относится к разным узлам). Отправка любого сообщения адрес многоадресной передачи данных передается набором интерфейсов на адрес, указанный на расстоянии от исходного узла (недавно измеренный в соответствии с протоколом маршрутизации с помощью интерфейса).

В IPv6 нет широковещательного адреса, а функция широковещательного адреса реализуется многоадресным адресом.

Тип адреса IPv6 задается несколькими предыдущими адресами (называемыми префиксом формата), а соответствующая связь между основным типом адреса и префиксом формата показана в таблице 1-1.

В таблице 1-1 Соответствующая взаимосвязь между типом адреса и префиксом формата

3. Типы адресов одноадресной рассылки

Существует множество типов одноадресных адресов IPv6, включая глобальные адреса одноадресной рассылки, локальные адреса ссылок и локальные адреса сайтов.

1) Глобальный одноадресный адрес эквивалентен общедоступному адресу IPv4, который предоставляется поставщику сетевых услуг. Этот тип адреса позволяет агрегировать префиксы маршрутизации, тем самым ограничивая количество глобальных таблиц маршрутизации.
2) Локальный адрес связи используется для протокола обнаружения соседей и связи между локальными верхними узлами в автоматической настройке без сохранения состояния. Пакеты данных, использующие локальный адрес ссылки в качестве адреса источника или назначения, не пересылаются другим ссылкам.
3) Локальный адрес сайта аналогичен частному адресу в IPv4. Пакеты данных, использующие локальный адрес сайта в качестве адреса источника или назначения, не перенаправляются на другие сайты за пределами сайта (эквивалент частной сети).
4) Адрес замыкания на себя: адрес одноадресной рассылки 0:0:0:0:0:0:0:1 (упрощенный как:: 1) называется адресом замыкания на себя и не может быть назначен какому-либо физическому интерфейсу. Его функция такая же, как и адрес замыкания на себя в IPv4, то есть узлы отправляют себе сообщения IPv6
5) Неизвестный адрес: Адрес::: называется неопределенным адресом и не может быть назначен какому-либо узлу. Прежде чем узел получит действительный IPv6-адрес, он может заполнить адрес в поле исходного адреса передаваемого сообщения IPv6, но его нельзя использовать в качестве адреса назначения в сообщении IPv6.

4. Многоадресная рассылка

Адрес многоадресной рассылки, указанный в таблице 1-2, зарезервирован для адреса многоадресной рассылки специального назначения.

В таблице 1-2 Список зарезервированных адресов многоадресной рассылки IPv6

Кроме того, существует класс адреса многоадресной рассылки: адрес запрошенного узла (Solicited-Node). Этот адрес в основном используется для получения адреса канального уровня соседних узлов

в одной цепочке и реализации обнаружения дубликатов адресов. Каждый одноадресный или любой IPv6-адрес имеет соответствующий адрес запрошенного узла. Его формат:
FF02:0:0:0:0:1:FFXX:XXXX
Среди них FF02:0:0:0:0:1:FF является 104-битным фиксированным форматом; XX:XXXX - это 24-битный одноадресный или любой другой IPv6-адрес.

5. Идентификатор интерфейса формата IEEE EUI-64
Идентификатор интерфейса в адресе одноадресной рассылки IPv6 используется для идентификации уникального интерфейса по ссылке. В настоящее время одноадресный адрес IPv6 в основном требует, чтобы идентификатор интерфейса был 64-битным. Идентификатор интерфейса формата IEEE EUI-64 изменяется от адреса канального уровня (MAC-адреса) интерфейса. Идентификатор интерфейса в IPv6-адресе — 64 бита, а MAC-адрес — 48 бит. Поэтому необходимо вставить шестнадцать десятичных чисел FFFE (1111111111111110) в среднюю позицию MAC-адреса (начиная с двадцать четвертого бита после высокой позиции). Чтобы убедиться, что идентификатор интерфейса, полученный с MAC-адреса, является уникальным, бит Universal/Local (U/L) (начиная с высокого бита) устанавливается равным 1 седьмому". Наконец, количество групп используется в качестве идентификатора интерфейса формата EUI-64.

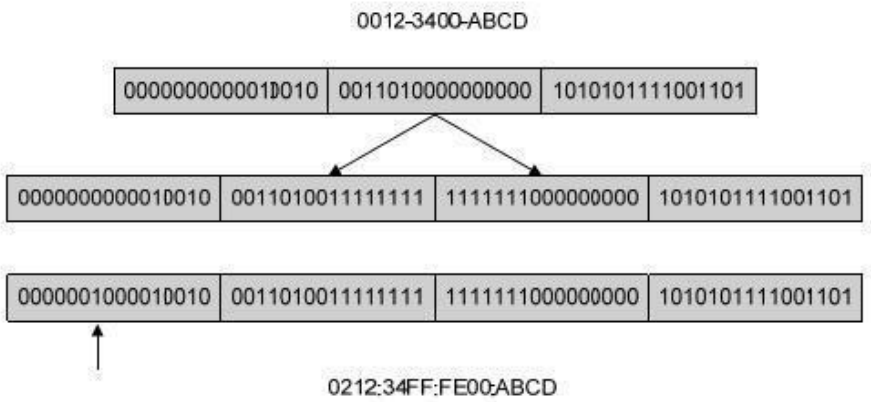


Рисунок 1-2 Процесс преобразования из MAC-адреса в идентификатор интерфейса формата EUI-64

27.1.3 Протокол обнаружения соседей IPv6

Протокол обнаружения соседей IPv6 с использованием сообщений ICMPv6 пяти типов, некоторые функции для достижения следующего: разрешение адресов, проверка доступности соседей, обнаружение дубликатов адресов, обнаружение маршрутизатора / обнаружение префиксов, автоматическая настройка и перенаправление адресов.

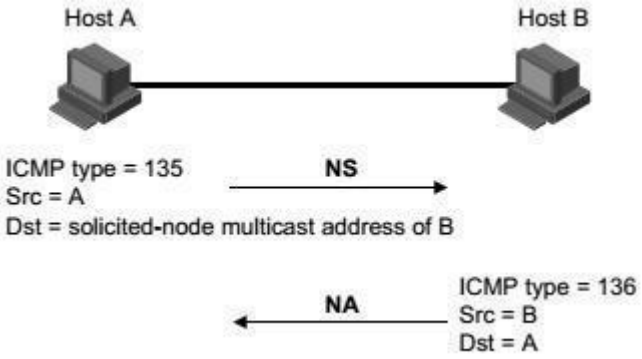
Тип и роль сообщений ICMPv6, используемых протоколами обнаружения соседей, показаны в таблице 1-3.

В таблице 1-3 Тип и роль сообщений ICMPv6, используемых в протоколах обнаружения соседей

Основные функции протокола обнаружения соседей заключаются в следующем:

1 Разрешение адресов

Получается адрес канального уровня соседнего узла той же цепочки (такой же, как и функция ARP IPv4), который реализуется сообщением запроса соседа NS и сообщением уведомления о соседе NA. Как показано на рисунке 1-3, узел A необходим для получения адреса канального уровня узла B.



Принципиальная схема разрешения адресов на рисунке 1-3

(1) Узел A отправляет сообщения NS в режиме многоадресной рассылки. Исходным адресом сообщения NS является IPv6-адрес интерфейса узла A, а адресом назначения — адрес многоадресной рассылки запрошенного узла узла B. Содержимое сообщения содержит адрес канального уровня узла A.

(2) После того как узел B получает сообщение NS, он определяет, является ли адрес назначения сообщения многоадресным адресом запрошенного узла, соответствующим его собственному IPv6-адресу. Если это так, то узел B может узнать адрес канального слоя узла A и вернуть сообщение NA в режиме одноадресной рассылки, которое содержит собственный адрес канального слоя.

(3) Узел A получает адрес канального уровня узла B из полученного сообщения NA.

2 Проверка доступности соседей

После получения адреса канального уровня соседнего узла, сообщение запроса соседа NS и сообщение уведомления о соседе NA могут проверить, доступен ли соседний узел или нет.

(1) Узел отправляет сообщение NS, где адрес назначения — это IPv6-адрес соседнего узла.

(2) Если получено сообщение о подтверждении соседнего узла, сосед доступен; в противном случае сосед недоступен.

3 Обнаружение дубликатов адресов

Когда узел получает IPv6-адрес, необходимо использовать функцию обнаружения повторяющихся адресов, чтобы определить, использовался ли адрес другими узлами (аналогично бесплатной

функции ARP IPv4). Обнаружение дубликатов адресов может быть реализовано ns и NA, как показано на рисунке 1-4.

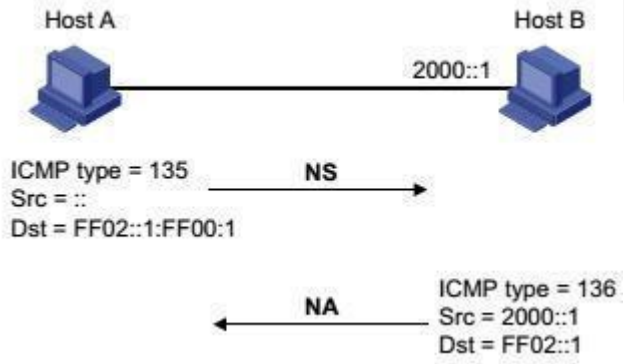


Рис.1-4 Принципиальная схема обнаружения дубликатов адресов

(1) Узел A отправляет сообщение NS, а исходный адрес сообщения NS является неопределенным адресом: адрес назначения — это адрес многоадресной рассылки запрошенного узла, соответствующий IPv6-адресу, который необходимо обнаружить, а содержимое сообщения содержит IPv6-адрес, который необходимо обнаружить.

(2) Если узел B уже использовал этот IPv6-адрес, будет возвращено сообщение NA. Он содержит свой собственный IPv6-адрес.

(3) Узел A получает сообщение NA от узла B и знает, что IPv6-адрес уже используется. В противном случае адрес не используется, и узел A может использовать IPv6-адрес.

4 Обнаружение маршрутизатора / обнаружение префиксов и автоматическая настройка адресов

Обнаружение маршрутизатора / обнаружение префикса заключается в том, что узел получает префикс соседнего маршрутизатора и его сети из полученного сообщения RA и других параметров конфигурации.

Автоматическая настройка адреса без сохранения состояния относится к узлу для обнаружения полученной информации в соответствии с обнаружением / префиксом маршрутизатора и автоматической настройкой IPv6-адреса. Обнаружение маршрутизатора / обнаружение префикса реализуется через сообщение запроса маршрутизатора RS и уведомление маршрутизатора RA, и конкретный процесс выглядит следующим образом:

(1) Когда узел запускается, он отправляет запрос маршрутизатору через сообщение RS, запрашивая префикс и другую информацию о конфигурации узла.

(2) Маршрутизатор возвращает сообщение RA, включая параметры префиксной информации (маршрутизатор также периодически выпускает сообщения RA).

(3) Узел автоматически настраивает IPv6-адрес и другую информацию интерфейса, используя префикс адреса и другие параметры конфигурации в сообщении RA, возвращаемом маршрутизатором.

- Параметры префиксной информации включают в себя не только информацию о префиксе адреса, но и префикс префикса lifetime (предпочтительное время жизни) и действительный (жизненный цикл). Когда узел получает периодически передаваемое сообщение RA, предпочтительное время жизни префикса и действительное время жизни обновляются в соответствии с сообщением.
- В течение срока действия автоматически сгенерированный адрес может использоваться в обычном режиме; по истечении действительного срока службы автоматически сгенерированный адрес будет удален.

5 Перенаправление

При запуске узла в таблице маршрутизации может быть только один маршрут по умолчанию к шлюзу по умолчанию. Когда определенное условие выполнено, шлюз по умолчанию отправит сообщение перенаправления на исходный узел ICMPv6, уведомит хост выбрать отправку последующего сообщения на следующий прыжок (сообщения перенаправления IPv4 и ICMP одна и та же функция).

- Сообщение о перенаправлении ICMPv6 отправляется на узел при выполнении следующих условий:
- Интерфейс приема и пересылки пакетов данных является одним и тем же интерфейсом;
- Сам выбранный маршрут не был создан или изменен сообщением перенаправления ICMPv6;
- Выбранный маршрут не является маршрутом по умолчанию;
- Пересылаемый пакет данных IPv6 не содержит заголовка расширения маршрута.

27.1.4 Обнаружение PMTU IPv6

Ссылки, передаваемые от источника к месту назначения, могут иметь разные ссылки MTU. В IPv6, когда длина сообщения больше MTU канала, фрагмент сообщения будет осуществляться на исходном конце, тем самым уменьшая давление обработки промежуточного устройства пересылки и рационально используя сетевые ресурсы.

Цель механизма обнаружения PMTU (Path MTU) состоит в том, чтобы найти наименьший MTU на пути от исходного конца до места назначения. Рабочий процесс ПМТУ показан на рисунке 1-5.

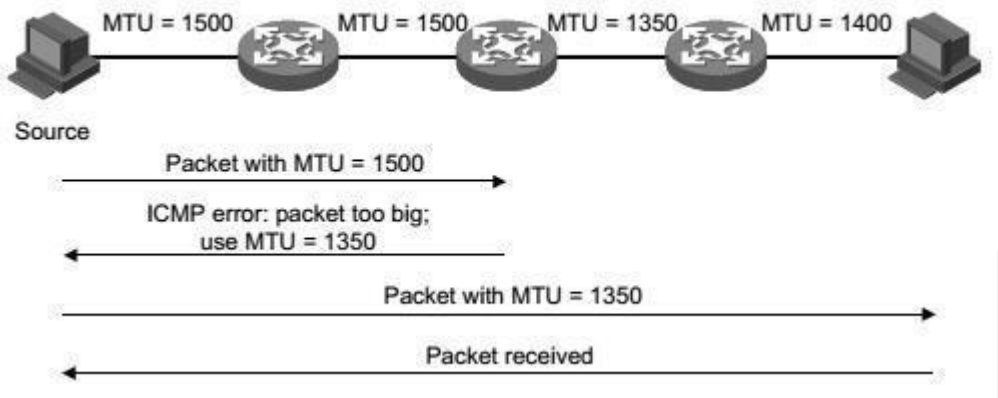


Рисунок 1-5 Рабочий процесс обнаружения PMTU

(1) Исходный узел использует свой собственный MTU для сегментации сообщения, а затем отправляет сообщение на узел назначения.

(2) Промежуточное устройство пересылки получает пересылку сообщений, если интерфейс пересылки пакетов поддерживает значение MTU меньше длины пакетов сообщений, отбрасываемых, а источник для возврата сообщения об ошибке ICMPv6, включая пересылку, не работает интерфейс MTU.

(3) Когда исходный узел получает сообщение об ошибке, он фрагментирует и отправляет сообщение с помощью MTU, переносимого сообщением.

(4) Это повторяется до тех пор, пока узел назначения не получит это сообщение, тем самым определяя минимальный MTU сообщения от исходного конца до пути назначения.

27.1.5 Спецификация протокола

Спецификация протокола, относящаяся к основам IPv6, доступна:

- RFC 1881: Управление распределением адресов IPv6
- RFC 1887: Архитектура для распределения одноадресных адресов IPv6
- RFC 1981: Обнаружение MTU пути для IP версии 6
- RFC 2375: Назначения адресов многоадресной рассылки IPv6
- RFC 2460: Спецификация протокола Интернета, версия 6 (IPv6).
- RFC 2461: Обнаружение соседей для IP версии 6 (IPv6)
- RFC 2462: Автоматическая настройка адресов IPv6 без сохранения состояния
- RFC 2463: Протокол ICMPv6 для спецификации протокола IPv6
- RFC 2464: Передача пакетов IPv6 по сетям Ethernet
- RFC 2526: Зарезервированные адреса любой подсети IPv6
- RFC 3307: Рекомендации по распределению для многоадресных адресов IPv6
- RFC 3513: Архитектура адресации протокола Интернета версии 6 (IPv6)
- RFC 3596: Расширения DNS для поддержки IP версии 6

27.2 Профиль задачи базовой конфигурации IPv6

- Настройка основных функций IPv6
- Настройка протокола обнаружения соседей IPv6
- Настройка обнаружения PMTU
- Настройка отправки сообщений ICMPv6

27.3 Настройка базовой функциональности IPv6

27.3.1 Настройка одноадресного адреса IPv6

Глобальные одноадресные адреса IPv6 назначаются вручную.

Локальный адрес канала IPv6 получается двумя способами:

- Автоматическая генерация: при использовании порта VLAN UP устройство автоматически генерирует локальный адрес канала для интерфейса в соответствии с префиксом локального адреса канала (FE80:: /10) и адресом канального уровня интерфейса;
- Назначается вручную: настроенный вручную пользователем локальный адрес IPv6-ссылки.

Команда	Описание	Режим CLI
ipv6 address <ipv6-address>/<prefix-length>	Вручную укажите IPv6-адрес. По умолчанию локальный адрес канала автоматически генерируется в соответствии с MAC-адресом интерфейса VLAN под трехуровневым интерфейсом.	Режим глобального конфигурирования

27.4 Настройка протокола обнаружения соседей IPv6

27.4.1 Настройка параметров сообщения RA

Пользователь может настроить интерфейс для отправки сообщений RA и сообщений RA в соответствии с фактической ситуацией, а также настроить соответствующие параметры в сообщении RA для уведомления хоста. Когда хост получает сообщение RA, мы можем использовать эти параметры для выполнения соответствующей операции. Параметры и значения настраиваемых сообщений PA приведены в таблице 1-4.

Таблица 1-4 Параметры и описания в сообщении PA

Параметр	Описание
Ограничение по прыжкам	Когда узел отправляет сообщение IPv6, он заполняет поле Hop Limit в заголовке IPv6 значением параметра. В то же время значение параметра также используется в качестве значения поля Hop Limit в ответном сообщении устройства.
Информация о префиксе	Когда хост по той же ссылке получает префиксную информацию устройства, он может выполнять автоматическую настройку без сохранения состояния и другие операции.
M флаг	Чтобы определить, использует ли узел автоматическую настройку с отслеживанием состояния для получения адреса IPv6. Если для этого флага установлено значение 1, хост будет иметь состояние посредством автоматической настройки (например, DHCP-сервера) для получения адреса IPv6; в противном случае автоматическая конфигурация без сохранения состояния для получения адреса IPv6, адрес IPv6 генерируется в соответствии с их адресом канального уровня и выпуском информации о префиксе маршрутизатора.
O flag	Чтобы определить, использует ли узел автоматическую настройку с отслеживанием состояния для получения дополнительной информации, кроме IPv6-адреса. Если вы установите другой флаг конфигурации равным 1, хост будет иметь состояние через автоматическую настройку (например, DHCP-сервер) для получения информации в дополнение к другому IPv6-адресу; в противном случае автоконфигурация без сохранения состояния для получения дополнительной информации.
Router Lifetime	Время, используемое для установки маршрутизатора, который выпускает сообщение RA, в качестве маршрутизатора по умолчанию для хоста. В соответствии со значением параметра времени существования маршрутизатора в полученном сообщении RA хост может определить, будет ли маршрутизатор, который публикует сообщение RA, маршрутизатором по умолчанию.
Retrans Timer	Когда устройство отправляет сообщения NS, сообщение NS отправляется повторно, если ответ не получен в течение заданного интервала времени.
Reachable Time	При обнаружении недоступности соседа, чтобы убедиться, что сосед, вовремя установив, оборудование до этого соседа; превышает установленное время, если вам нужно отправить сообщения соседям, соседи повторно подтвердят, могут ли они связаться.
Link MTU	Параметр MTU используется в сообщении RA, чтобы гарантировать, что все узлы в цепочке используют одно и то же значение MTU, что используется в основном в случае, если узлы могут не знать MTU канала. Другие сообщения Neighbor Discovery должны быть тихими и игнорировать эту опцию.

Настроить лимит прыжков
Команда: ipv6 nd cur-hop-limit value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию количество переходов, выдаваемых маршрутизатором, ограничено 64 переходами.

Устранение запрета на публикацию сообщений RA
Команда: ipv6 и send-ra
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: подавляет публикацию сообщений RA при публикации по умолчанию.

Команда: ipv6 nd max-ra-interval value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию максимальный интервал времени для выпуска сообщения RA составляет 600 секунд.

Команда: ipv6 nd min-ra-interval value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию минимальный временной интервал для выдачи сообщений RA составляет 198 секунд.
Примечание:

- Когда сообщение RA периодически публикуется, интервал между двумя смежными моментами времени выбирается случайным образом между максимальным интервалом времени и минимальным интервалом времени в качестве интервала времени для периодической выдачи сообщений RA.
- Минимальный временной интервал должен быть не более чем в 0,75 раза максимального временного интервала.

Настройка информации префикса в сообщениях RA
Команда: ipv6 nd prefix X:X::X:X/M (valid-lifetime preferred-lifetime (off-link | no-autoconfig))
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию префиксная информация в сообщении RA не настроена.
Адрес IPv6 сообщения RA будет использоваться в качестве информации о префиксе в сообщении RA.

Установка бита флага конфигурации управляемого адреса
Команда: ipv6 nd managed-config-flag
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию флаг управляемого адреса автоматически получает адрес IPv6 в конфигурации без сохранения состояния.

Установка других битов флага конфигурации
Команда: ipv6 nd other-config-flag
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию другие флаги конфигурации автоматически получают другую информацию с помощью конфигурации без сохранения состояния.

Настройка времени жизни маршрутизатора в сообщениях RA
Команда: ipv6 nd ra-lifetime value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию время жизни маршрутизатора в сообщении RA составляет 1800 секунд.

Настройка интервала повторной передачи сообщения запроса соседа
Команда: ipv6 nd base retrans-timer value
Режим просмотра: режим конфигурации
Конфигурация по умолчанию: по умолчанию временной интервал для отправки NS-сообщений интерфейсом составляет 1000 миллисекунд.

Настройка интервала повторной передачи маршрутизаторов в сообщениях RA
Команда: ipv6 nd retrans-timer value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию значение поля Retrans Timer в сообщении RA, выдаваемом интерфейсом, равно 0.

Настройка времени доступности соседей
Команда: ipv6 nd base reachable-time value
Режим просмотра: режим конфигурации
Конфигурация по умолчанию: по умолчанию интерфейс поддерживает состояние доступности соседей в течение 30000 миллисекунд.

Настройка времени, чтобы соседи оставались доступными
Команда: ipv6 nd reachable-time value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию значение поля Reachable Timer в сообщении RA, выдаваемом интерфейсом, равно 0.

Настройка размера MTU каналам
Команда: ipv6 nd link-mtu value
Режим просмотра: режим интерфейса VLAN
Конфигурация по умолчанию: по умолчанию значение поля MTU канала в сообщении RA, выдаваемом интерфейсом, равно 0.

Когда хост-источник отправляет сообщение с интерфейса, он сравнивает MTU и MTU канала интерфейса. Если длина сообщения больше двух, для сегментации сообщения используется минимальное значение.

27.4.2 Количество отправляемых сообщений запроса соседей при настройке дублирования

обнаружение адреса

IPv6-адрес интерфейса после отправки сообщения соседу запросить обнаружение дубликатов адресов, если в течение заданного промежутка времени (командой конфигурации IPv6 nd retrans-timer) не получен ответ, то продолжит отправку информации запроса, при отправке номер достигнут, номер установлен, ответа пока не получил, адрес свободен.

Команда	Описание	Режим CLI
ipv6 nd dad attempts <value>	По умолчанию количество запросов к соседям, отправляемых повторным обнаружением адреса, равно 1, а когда значение равно 0, это указывает на запрещенное обнаружение повторяющихся адресов.	Режим глобального конфигурирования

27.5 Конфигурация статической маршрутизации IPv6

Команда	Описание	Режим CLI
ipv6 route <X:X::X:X/M> (<X:X::X:X> | <ifName>) <distance>	Настройка статической маршрутизации IPv6.	Режим глобального конфигурирования

27.6 Отображение и обслуживание IPv6

После завершения приведенной выше настройки выполнение команды show в привилегированном представлении может отобразить работу IPv6 после настройки и проверить эффект конфигурации, проверив отображаемую информацию.

Команда	Описание	Режим CLI
show ipv6 ndp nc	Отображение информации о соседях.	Привилегированный режим
show ipv6 interface (<ifName>) brief	Отображение информации IPv6, которая может настроить интерфейс адреса IPv6.	Привилегированный режим
show ipv6 route (database)	Показать маршрутизацию IPv6	Привилегированный режим