Руководство по настройке
Конфигурация сетевого управления
Ethernet-коммутаторы агрегации
серия QSW-6910

Оглавление

1. НАСТРОЙКА SNMP

1.1. Обзор

Простой протокол управления сетью (SNMP) стал стандартом управления сетью RFC1157 в августе 1988 года. В настоящее время, поскольку многие поставщики поддерживают SNMP, SNMP фактически стал стандартом управления сетью и применим к среде, в которой взаимосвязаны системы различных поставщиков. Используя SNMP, сетевой администратор может реализовать основные функции, такие как запрос информации о сетевых узлах, конфигурация сети, обнаружение неисправностей, планирование пропускной способности, а также мониторинг и управление сетью.

Версии SNMP

В настоящее время поддерживаются следующие версии SNMP:

- SNMPv1: первая официальная версия SNMP, определенная в RFC1157.
- SNMPv2C: архитектура управления SNMPv2 на основе community, определенная в RFC1901.
- SNMPv3: SNMPv3 обеспечивает следующие функции безопасности путем идентификации и шифрования данных.

1. Обеспечение того, чтобы данные не были подделаны во время передачи.
2. Обеспечение передачи данных из легальных источников данных.
3. Шифрование пакетов и обеспечение конфиденциальности данных.

1.1.1. Протоколы и стандарты

- RFC 1157. Простой протокол управления сетью (SNMP).
- RFC 1901. Введение в SNMPv2 на основе сообщества.
- RFC 2578. Структура информации управления, версия 2 (SMIv2).
- RFC 2579. Текстовые соглашения для SMIv2.
- RFC 3411. Архитектура для описания инфраструктур управления Simple Network Management Protocol (SNMP).
- RFC 3412. Обработка и отправка сообщений для простого протокола управления сетью (SNMP).
- RFC 3413. Приложения простого протокола сетевого управления (SNMP).
- RFC 3414. Модель безопасности на основе пользователей (USM) для версии 3 простого протокола управления сетью (SNMPv3).
- RFC 3415. Модель управления доступом на основе View (VACM) для простого протокола управления сетью (SNMP).
- RFC 3416. Версия 2 протокольных операций для простого протокола управления сетью (SNMP).
- RFC 3417. Транспортные сопоставления для простого протокола управления сетью (SNMP).
- RFC 3418. База управляющей информации (MIB) для простого протокола управления сетью (SNMP).
- RFC 3419. Текстовые соглашения для транспортных адресов.

1.2. Приложения

Приложение	Описание
Управление сетевыми устройствами на основе SNMP	Сетевые устройства управляются и контролируются на основе SNMP

1.2.1. Управление сетевыми устройствами на основе SNMP

1.2.1.1. Сценарий

Возьмем в качестве примера следующий рисунок. Сетевое устройство A управляется и контролируется с помощью сетевого менеджера SNMP.

Рисунок 1-1.

A — это сетевое устройство, которым необходимо управлять.

ПК — это станция управления сетью.

1.2.1.2. Развертывание

Станция управления сетью подключается к управляемым сетевым устройствам. На станции управления сетью пользователи получают доступ к информационной базе управления (MIB) на сетевых устройствах через диспетчер сети SNMP и получают сообщения, активно отправляемые сетевыми устройствами, для управления и мониторинга сетевых устройств.

1.3. Функции

1.3.1. Базовые концепты

SNMP — это протокол прикладного уровня, работающий в режиме C/S. Он состоит из трех частей:

- SNMP-менеджер сети
- SNMP-агент
- MIB

Рисунок 1-2 показывает взаимосвязь между системой управления сетью (NMS) и агентом управления сетью.

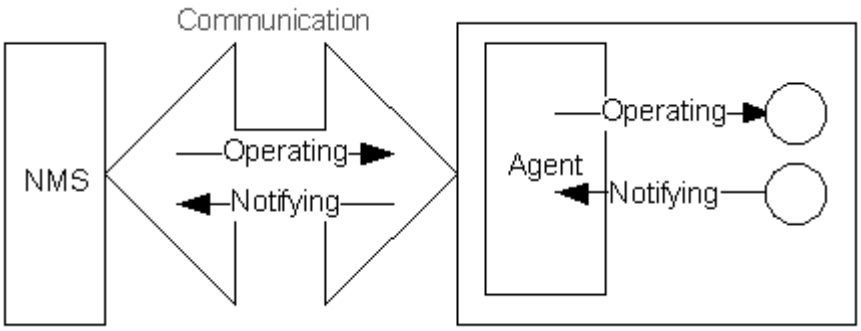


Рисунок 1-2.

SNMP-менеджер сети

Сетевой менеджер SNMP — это система, которая управляет и контролирует сеть на основе SNMP и также называется NMS.

SNMP-агент

Агент SNMP (далее — агент) — это программное обеспечение, работающее на управляемых устройствах. Он отвечает за получение, обработку и реагирование на пакеты мониторинга и управления от NMS. Агент также может активно отправлять сообщения в NMS.

MIB

MIB — это информационная база управления виртуальной сетью. Управляемые сетевые устройства содержат много информации. Чтобы однозначно идентифицировать конкретный блок управления среди пакетов SNMP, MIB использует древовидную иерархическую структуру. Узлы в дереве обозначают конкретные единицы управления. Строка цифр может использоваться для уникальной идентификации системы блока управления среди сетевых устройств. MIB представляет собой набор идентификаторов сетевых устройств.

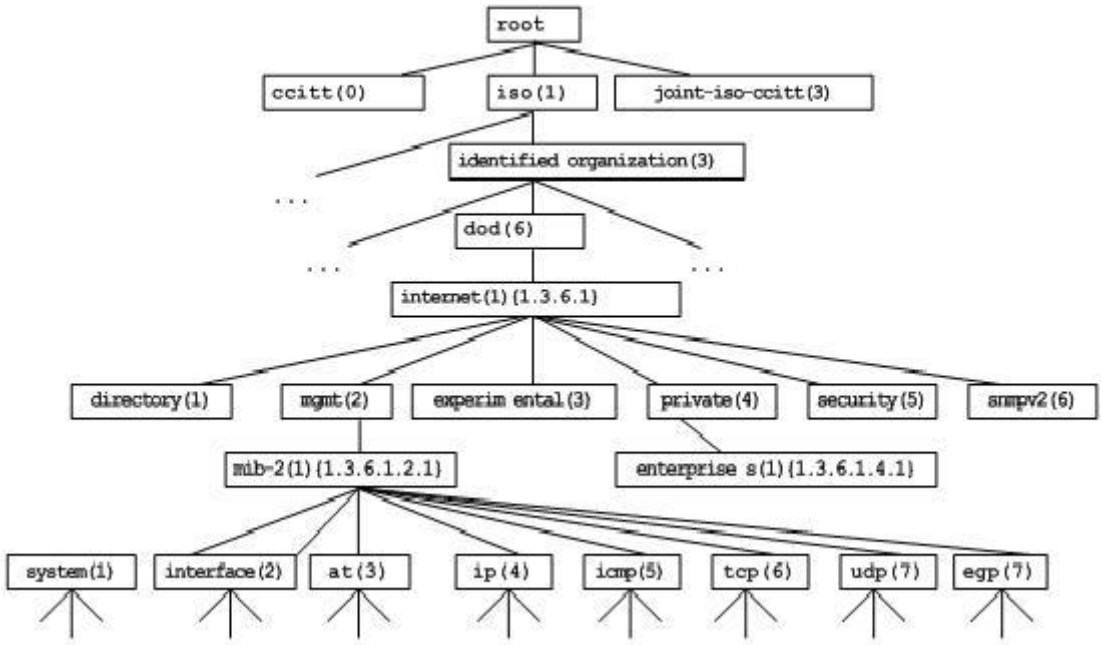


Рисунок 1-3. Древовидная иерархическая структура

1.3.2. Типы операций

Определено шесть типов операций для обмена информацией между NMS и агентом на основе SNMP:

- Get-request: NMS извлекает одно или несколько значений параметров из агента.
- Get-next-request: NMS извлекает значение параметра рядом с одним или несколькими параметрами от агента.
- Get-bulk: NMS извлекает пакет значений параметров из агента.
- Set-request: NMS устанавливает одно или несколько значений параметров агента.
- Get-response: агент возвращает одно или несколько значений параметров, которые представляют собой операции в ответ на три операции, выполненные агентом в NMS.
- Trap: агент активно отправляет сообщение, чтобы уведомить NMS о том, что происходит.

Первые четыре пакета отправляются NMS-агенту, а последние два пакета отправляются агентом NMS. (Примечание: SNMPv1 не поддерживает операцию Get-bulk.) Рисунок 1-4 описывает операции.

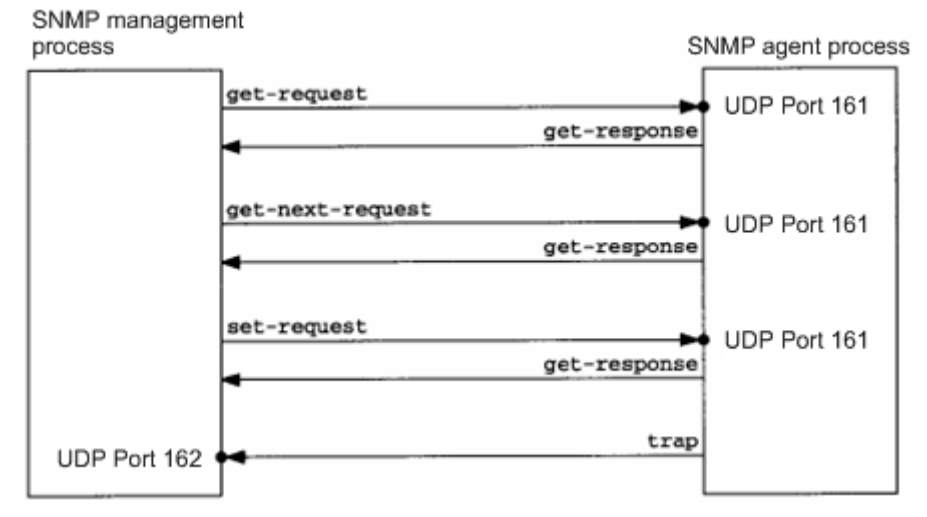


Рисунок 1-4. Типы пакетов SNMP

Три операции, выполняемые NMS на агенте, и операции ответа агента основаны на UDP-порте 161. Операция trap, выполняемая агентом, основана на UDP-порте 162.

1.3.3. Обзор

Особенность	Описание
Основные функции SNMP	Агент SNMP настраивается на сетевых устройствах для реализации основных функций, таких как запрос информации о сетевых узлах, конфигурация сети, обнаружение неисправностей и планирование емкости

Особенность	Описание
SNMPv1 и SNMPv2C	SNMPv1 и SNMPv2C используют архитектуру безопасности на основе community, включая имя аутентификации и разрешение на доступ
SNMPv3	SNMPv3 переопределяет архитектуру SNMP, а именно расширяет функции безопасности, включая модель безопасности на основе пользователей и модель управления доступом на основе View. Архитектура SNMPv3 уже включает все функции SNMPv1 и SNMPv2C

1.3.4. Основные функции SNMP

1.3.4.1. Принцип работы

Рабочий процесс

Взаимодействие по протоколу SNMP является ответным взаимодействием (об обмене пакетами см. Рисунок 1-4). NMS активно отправляет агенту запросы, включая Get-request, Get-next-request, Get-bulk и Set-request. Агент получает запросы, выполняет операции и возвращает Get-response. Иногда агент активно отправляет сообщение trap и сообщение Inform в NMS. NMS не нужно отвечать на сообщение trap, но необходимо вернуть агенту ответ Inform. В противном случае агент повторно отправляет сообщение Inform.

1.3.4.2. Связанная конфигурация

Экранирование или отключение агента SNMP

По умолчанию функция SNMP включена.

Команда **no snmp-server** используется для отключения агента SNMP.

Команда **no enable service snmp-agent** используется для прямого отключения всех служб SNMP.

Настройка основных параметров SNMP

По умолчанию информация о режиме контакта системы, расположении системы и сетевом элементе устройства (NE) пуста. Серийный номер по умолчанию — 60FF60, максимальная длина пакета по умолчанию — 1572 байта, а идентификатор порта UDP по умолчанию для службы SNMP — 161.

Команда **snmp-server contact** используется для настройки или удаления системного режима контакта.

Команда **snmp-server location** используется для настройки или удаления местоположения системы.

Команда **snmp-server chassis-id** используется для настройки серийного номера системы или восстановления значения по умолчанию.

Команда **snmp-server packetsize** используется для настройки максимальной длины пакета агента или восстановления значения по умолчанию.

Команда **snmp-server net-id** используется для настройки или удаления информации о сетевом элементе устройства.

Команда **snmp-server udp-port** используется для установки идентификатора UDP-порта службы SNMP или восстановления значения по умолчанию.

Настройка адреса узла SNMP

По умолчанию хост SNMP не настроен.

Команда **snmp-server host** используется для настройки адреса узла NMS, на который агент активно отправляет сообщения, или для удаления указанного адреса узла SNMP. В сообщениях, отправляемых на хост, могут быть привязаны версия SNMP, принимающий порт, имя аутентификации или пользователь. Эта команда используется с командой **snmp-server enable traps** для активной отправки сообщений trap в NMS.

Установка параметров сообщения trap

По умолчанию SNMP не разрешено активно отправлять trap-сообщение в NMS, функция отправки Link Trap-сообщения на интерфейсе включена, функция отправки trap-сообщения о перезагрузке системы отключена, а trap-сообщение не несет любое частное поле.

По умолчанию в качестве исходного адреса используется IP-адрес интерфейса, на который отправляются пакеты SNMP.

По умолчанию длина очереди сообщений trap составляет 10, а интервал отправки сообщения trap составляет 30 секунд.

Команда **snmp-server enable traps** используется для включения или отключения агента для активной отправки сообщения trap в NMS.

Команда **snmp trap link-status** используется для включения или отключения функции отправки сообщения Link Trap на интерфейсе.

Команда **snmp-server trap-source** используется для указания исходного адреса для отправки сообщений или для восстановления значения по умолчанию.

Команда **snmp-server queue-length** используется для установки длины очереди сообщений trap или для восстановления значения по умолчанию.

Команда **snmp-server trap-timeout** используется для установки интервала отправки trap-сообщения или для восстановления значения по умолчанию.

Команда **snmp-server trap-format private** используется для установки или отключения функции переноса приватных полей в trap-сообщении при его отправке.

Команда **snmp-server system-shutdown** используется для включения или отключения функции отправки сообщения trap перезагрузки системы.

1.3.5. SNMPv1 и SNMPv2C

SNMPv1 и SNMPv2C используют архитектуру безопасности на основе сообщества (community-based). Администратор, который может выполнять операции с MIB агента, ограничен путем определения адреса хоста и имени аутентификации (строка сообщества).

1.3.5.1. Принцип работы

SNMPv1 и SNMPv2 определяют, имеет ли администратор право использовать объекты MIB, используя имя аутентификации. Имя аутентификации NMS должно совпадать с именем аутентификации, определенным в устройствах.

SNMPv2C добавляет механизм операции Get-bulk и может возвращать более подробные типы сообщений об ошибке на управляющую рабочую станцию. Операция Get-bulk выполняется для получения всей информации из таблицы или получения большого количества данных за раз, чтобы уменьшить количество ответов на запросы. Расширенные возможности обработки ошибок SNMPv2C включают расширение кодов ошибок для различения типов ошибок. Однако в SNMPv1 для ошибок предоставляется только один код ошибки. Теперь ошибки можно различать по кодам ошибок. Поскольку в

сети могут существовать управляющие рабочие станции, поддерживающие SNMPv1 и SNMPv2C, агент SNMP должен иметь возможность идентифицировать пакеты SNMPv1 и SNMPv2C и возвращать пакеты соответствующих версий.

1.3.5.2. Безопасность

Одно имя аутентификации имеет следующие атрибуты:

- Только для чтения (Read-only): Предоставляет разрешение на чтение всех переменных MIB для авторизованных рабочих станций управления.
- Чтение-запись (Read-write): предоставление разрешения на чтение/запись всех переменных MIB для авторизованных рабочих станций управления.

1.3.5.3. Связанная конфигурация

Настройка имен аутентификации и прав доступа

Разрешение на доступ по умолчанию для всех имен проверки подлинности — только чтение.

Команда **snmp-server community** используется для настройки или удаления имени аутентификации и разрешения на доступ.

Эта команда является первой важной командой для включения функции агента SNMP. Он определяет атрибуты сообщества и область NMS, в которой разрешен доступ к MIB.

1.3.6. SNMPv3

SNMPv3 переопределяет архитектуру SNMP и включает функции SNMPv1 и SNMPv2 в систему SNMPv3.

1.3.6.1. Принцип работы

Агент NMS и SNMP являются объектами SNMP. В архитектуре SNMPv3 объекты SNMP состоят из механизма (engine) SNMP и приложений SNMP. Механизм SNMP используется для отправки и получения сообщений, идентификации и шифрования информации, а также для управления доступом к управляемым объектам. Приложения SNMP относятся к внутренним приложениям SNMP, которые работают с использованием служб, предоставляемых механизмом SNMP.

SNMPv3v определяет, имеет ли пользователь право использовать объекты MIB, используя модель безопасности на основе пользователей (USM). Уровень безопасности пользователя NMS должен быть таким же, как у пользователя SNMP, определенного в устройствах, чтобы управлять устройствами.

SNMPv3 требует, чтобы NMS получала идентификаторы механизма агента SNMP на устройствах, когда NMS управляет устройствами. SNMPv3 определяет механизмы обнаружения и создания отчетов. Когда NMS не знает идентификаторы механизма агента, NMS может сначала отправить сообщение об обнаружении агенту, и агент возвращает отчетное сообщение, содержащее идентификатор механизма. Позже операции управления между NMS и агентом должны иметь идентификатор механизма.

1.3.6.2. Безопасность

SNMPv3 определяет механизм безопасности данных на основе модели безопасности и уровня безопасности. В настоящее время модели безопасности включают: SNMPv1, SNMPv2C и SNMPv3. SNMPv3 включает SNMPv1 и SNMPv2C в модель безопасности.

Модели и уровни безопасности SNMPv1 и SNMPv2C

Модель безопасности	Уровень безопасности	Аутентификация	Шифрование	Описание
SNMPv1	noAuthNoPriv	Имя аутентификации	Нет	Достоверность данных подтверждается через аутентификационное имя
SNMPv2c	noAuthNoPriv	Имя аутентификации	Нет	Достоверность данных подтверждается через аутентификационное имя

Модель безопасности SNMPv3 и уровень безопасности

Модель безопасности	Уровень безопасности	Аутентификация	Шифрование	Описание
SNMPv3	noAuthNoPriv	Имя пользователя	Нет	Достоверность данных подтверждается через имя пользователя
SNMPv3	authNoPriv	MD5 или SHA	Нет	Предусмотрен механизм аутентификации данных на основе HMAC-MD5 или HMAC-SHA
SNMPv3	authPriv	MD5 или SHA	DES	Предоставляется механизм аутентификации данных на основе HMAC-MD5 или HMAC-SHA и механизм шифрования данных на основе CBC-DES

1.3.6.3. Идентификатор механизма

Идентификатор механизма используется для уникальной идентификации механизма SNMP. Поскольку каждый объект SNMP включает только один механизм SNMP, один модуль SNMP однозначно идентифицирует объект SNMP в домене управления. Следовательно, агент SNMPv3 как сущность должен иметь уникальный идентификатор механизма, то есть SnmpEngineID.

Идентификатор структура представляет собой восьмизначную строку (октет), состоящую из 5–32 байтов. RFC3411 определяет формат идентификатора механизма:

- Первые четыре байта указывают идентификатор частного предприятия (выделенный IANA) поставщика, который выражается в шестнадцатеричном формате.
- Пятый байт указывает оставшиеся байты:
- 0: зарезервировано.
- 1: последние четыре байта указывают адрес IPv4.

- 2: последние 16 байтов указывают адрес IPv6.
- 3: последние шесть байтов указывают MAC-адрес.
- 4: текст, состоящий из 27 байтов, определяется производителем.
- 5: шестнадцатеричное значение, состоящее из 27 байтов, которое определяется поставщиком.
- 6-127: зарезервировано.
- 128-255: форматы, указанные поставщиком.

1.3.6.4. Связанная конфигурация

Настройка MIB View и группы пользователей

По умолчанию настроено один MIB View, и доступны все объекты MIB.

По умолчанию группа пользователей не настроена.

Команда **snmp-server view** используется для настройки или удаления MIB View, а команда **snmp-server group** используется для настройки или удаления группы пользователей.

Можно настроить одну или несколько инструкций для указания разных имен сообществ, чтобы сетевые устройства могли управляться NMS с разными разрешениями.

Настройка пользователя SNMP

По умолчанию пользователь не настроен.

Команда **snmp-server user** используется для настройки или удаления пользователя.

NMS может связываться с агентом, используя только авторизованных пользователей.

Пользователь SNMPv3 может указать уровень безопасности (требуются ли аутентификация и шифрование), алгоритм аутентификации (MD5 или SHA), пароль аутентификации, пароль шифрования (в настоящее время доступен только DES) и пароль шифрования.

1.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций SNMP	(Обязательный) Используется для предоставления пользователям доступа к агенту через NMS	
	enable service snmp-agent	Включает функцию агента
	snmp-server community	Устанавливает имя аутентификации и разрешение на доступ
	snmp-server user	Настраивает пользователя SNMP
	snmp-server view	Настраивает SNMP View
Настройка основных функций SNMP	**snmp-server group**	Настраивает группу пользователей SNMP

Конфигурация	Описание и команда	
Настройка основных функций SNMP	**snmp-server authentication**	Настраивает функцию защиты и обнаружения атак SNMP
	snmp-server enable secret-dictionary-check	Настраивает проверку словаря паролей для сообществ и пользователей
Включение функции	(Опционально) Используется для того, чтобы агент мог активно отправлять сообщение trap в NMS	
	snmp-server host	Настраивает адрес хоста NMS
	snmp-server enable traps	Позволяет агенту активно отправлять trap-сообщения в NMS
	snmp trap link-status	Включает функцию отправки сообщения Link Trap на интерфейс
	snmp-server system-shutdown	Включает функцию отправки сообщения trap перезагрузки системы
	snmp-server trap-source	Указывает исходный адрес для отправки сообщения trap
	snmp-server trap-format private	Позволяет сообщению trap содержать закрытые поля при отправке сообщения
Экранирование функции агента	(Опционально) Используется для защиты функции агента, когда служба агента не требуется	
	no snmp-server	Закрывает функцию агента
Настройка параметров управления SNMP	(Опционально) Используется для установки или изменения параметров управления SNMP	
	snmp-server contact	Устанавливает режим контакта устройства
	snmp-server location	Устанавливает местоположение устройства

Конфигурация	Описание и команда	
Настройка параметров управления SNMP	**snmp-server chassis-id**	Устанавливает серийный номер устройства
	snmp-server net-id	Устанавливает информацию NE об устройстве
	snmp-server packetsize	Изменяет максимальную длину пакета
	snmp-server udp-port	Изменяет идентификатор порта UDP службы SNMP
	snmp-server queue-length	Изменяет длину очереди сообщений trap
	snmp-server trap-timeout	Изменяет интервал отправки trap-сообщения

1.4.1. Настройка основных функций SNMP

1.4.1.1. Эффект конфигурации

Разрешить пользователям доступ к агенту через NMS.

1.4.1.2. Примечания

По умолчанию на сетевых устройствах не задано имя аутентификации, и SNMPv1 или SNMPv2C нельзя использовать для доступа к MIB сетевых устройств. Когда задано имя аутентификации, если разрешение на доступ не указано, разрешение на доступ по умолчанию предоставляется только для чтения.

1.4.1.3. Шаги настройки

Настройка SNMP View

- Опционально
- SNMP View необходимо настроить при использовании модели управления доступом на основе View (VACM).

Настройка группы пользователей SNMP

- Опционально
- При использовании VACM необходимо настроить группу пользователей SNMP.

Настройка имени аутентификации и прав доступа

- Обязательный
- Имя аутентификации должно быть установлено на агенте, если SNMPv1 и SNMPv2C используются для управления сетевыми устройствами.

Настройка пользователя SNMP

- Обязательный

- Пользователь должен быть установлен, когда SNMPv3 используется для управления сетевыми устройствами.

Включение функции агента

- Опционально
- По умолчанию функция агента включена. Когда функцию агента необходимо снова включить после ее отключения, необходимо использовать эту команду.

1.4.1.4. Проверка

Запустите команду **show snmp**, чтобы проверить функцию SNMP на устройствах.

1.4.1.5. Связанные команды

Настройка SNMP View

Команда	**snmp-server view** *view-name oid-tree* **{ include | exclude }**
Описание параметров	*view-name*: имя View *oid-tree*: объекты MIB, связанные с View, которые отображаются в виде поддерева MIB. **include**: указывает, что поддерево объектов MIB включено во View. **exclude**: указывает, что поддерево объектов MIB не включено во View
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Укажите имя View и используйте его для управления на основе View

Настройка группы пользователей SNMP

Команда	**snmp-server group** *groupname* **{ v1 | v2c | v3 { auth | noauth | priv } } [read** *readview* **] [write** *writeview* **] [access { ipv6** *ipv6-aclname* **|** *aclnum* **|** *aclname* **}]**
Описание параметров	**v1| v2c |v3**: указывает версию SNMP. **auth**: сообщения, отправленные пользователями в группе, должны быть проверены, но конфиденциальность данных не требуется. Эта конфигурация действительна только для SNMPv3. **noauth**: сообщения, отправляемые пользователями в группе, не требуют проверки и конфиденциальности данных. Эта конфигурация действительна только для SNMPv3. **priv**: сообщения, отправляемые пользователями в группе, нуждаются в проверке и обязательной конфиденциальности передаваемых данных. Эта конфигурация действительна только для SNMPv3. *readview*: связывает одно View с read-only (только чтение). *writeview*: связывает одно View с read/write (чтения/записи). *aclnum*: ACL-номер. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB.

	aclname: имя ACL. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB. *ipv6-aclname*: имя ACL IPv6. Указанный ACL связывается и указывается диапазон IPv6-адресов NMS, с которых разрешен доступ к MIB
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Свяжите определенных пользователей с группой и свяжите группу с View. Пользователи в группе имеют одинаковые права доступа. Таким образом, вы можете определить, находятся ли управляемые объекты, связанные с операцией, в допустимом диапазоне View. Доступ возможен только к управляемым объектам в диапазоне View

Настройка имени аутентификации и прав доступа

Команда	**snmp-server community [** *0* **|** *7* **]** *string* **[view** *view-name* **] [[ro	rw] [host** *ipaddr* **]] [ipv6** *ipv6-aclname***] [** *aclnum* **|** *aclname* **]**
Описание параметров	*0*: указывает, что входная строка сообщества является строкой открытого текста. *7*: указывает, что входная строка сообщества является строкой зашифрованного текста. *string*: строка сообщества, эквивалентная паролю связи между NMS и агентом SNMP. *view-name*: указывает имя View для управления на основе View. **ro**: указывает, что NMS может только читать переменные MIB. **rw**: NMS может читать и записывать переменные MIB. *aclnum*: номер ACL. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB. *aclname*: имя ACL. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB. *ipv6-aclname*: имя ACL. Указанный ACL связывается и указывается диапазон IPv6-адресов NMS, с которых разрешен доступ к MIB
Описание параметров	*ipaddr*: связывает адреса NMS и указывает адреса NMS для доступа к MIB
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эта команда является первой важной командой для включения функции агента SNMP. Он определяет атрибуты сообщества и область NMS, в которой разрешен доступ к MIB. Чтобы отключить функцию агента SNMP, запустите команду **no snmp-server**

Настройка пользователя SNMP

Команда	**snmp-server user** *username groupname* **{ v1 | v2c | v3 [encrypted] [auth { md5 | sha }** *auth-password* **] [priv des56** *priv-password* **] } [access { ipv6** *ipv6-aclname* **|** *aclnum* **|** *aclname* **}]**
Описание параметров	*username*: имя пользователя. *groupname*: указывает имя группы для пользователя. **v1 | v2c | v3**: указывает версию SNMP. Только SNMPv3 поддерживает более поздние параметры безопасности. **encrypted**: указанный режим ввода пароля - ввод зашифрованного текста. В противном случае для ввода используется открытый текст. Если выбран ввод зашифрованного текста, введите ключ, состоящий из непрерывных шестнадцатеричных цифр. Ключ аутентификации протокола MD5 состоит из 16 байтов, а ключ протокола аутентификации SHA состоит из 20 байтов. Два символа обозначают один байт. Зашифрованные ключи действительны только для этого механизма. **auth**: указывает, используется ли аутентификация. **md5**: указывает протокол проверки подлинности MD5. **sha**: указывает протокол аутентификации SHA. *auth-password*: настраивает строку пароля (не более 32 символов), используемую протоколом аутентификации. Система преобразует пароли в соответствующие ключи аутентификации. **priv**: указывает, используется ли конфиденциальность. **des56:** указывает использование 56-битного протокола шифрования DES. *priv-password*: настраивает строку пароля (не более 32 символов), используемую для шифрования. Система преобразует пароль в соответствующий ключ шифрования. *aclnum*: номер ACL. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB. *aclname*: имя ACL. Указанный ACL связывается и указывается диапазон IPv4-адресов NMS, с которых разрешен доступ к MIB. *ipv6-aclname*: имя ACL IPv6. Указанный ACL связывается и указывается диапазон IPv6-адресов NMS, с которых разрешен доступ к MIB
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Настройте информацию о пользователе, чтобы NMS могла связываться с агентом, используя допустимого пользователя. Для пользователя SNMPv3 можно указать уровень безопасности, алгоритм аутентификации (MD5 или SHA), пароль аутентификации, алгоритм шифрования (в настоящее время доступен только DES) и пароль шифрования

Включение функции агента

Команда	**enable service snmp-agent**
Режим конфигурации	Привилегированный режим
Руководство по использованию	Эта команда используется для включения функции агента SNMP устройства

Отображение информации о состоянии SNMP

Команда	**show snmp [mib | user | view | group| host | process-mib-time]**
Описание параметров	**mib**: отображает информацию о SNMP MIB, поддерживаемом в системе. **user**: отображает информацию о пользователе SNMP. **view**: отображает информацию о SNMP View. **group**: отображает информацию о группе пользователей SNMP. **host**: отображает информацию о конфигурации пользователя. **process-mib-time**: отображает узел MIB с наибольшим временем обработки
Режим конфигурации	Привилегированный режим

Пример конфигурации Настройка SNMP v1/2c

Сценарий:

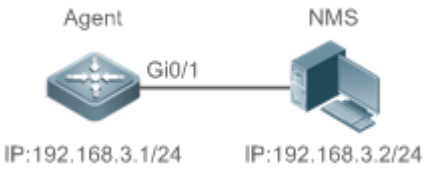


Рисунок 1-5.

	• NMS подключается к агенту через Ethernet. IP-адрес агента — 192.168.3.1/24, а IP-адрес NMS — 192.168.3.2/24. • NMS отслеживает и управляет агентом через SNMP v1 или SNMP v2c
	• Когда агент неисправен или возникает ошибка, агент может активно сообщать соответствующую информацию в NMS
Шаги настройки	• Настройте базовую информацию SNMP, включая версию и имя сообщества.

	• Разрешить NMS (192.168.3.2/24) отправлять Trap-сообщения. • Настройте IP-адрес агента и установите IP-адрес интерфейса Gi0/1 на 192.168.3.1/24
Агент	QTECH(config)#snmp-server community public rw QTECH(config)#snmp-server host 192.168.3.2 traps version 2c public QTECH(config)#snmp-server enable traps QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit
Проверка	• Запустите команду **show running-config**, чтобы отобразить информацию о конфигурации устройства. • Запустите команду **show snmp host**, чтобы отобразить информацию о хосте, настроенную пользователем
NMS	В NMS, использующей SNMP v1/v2c, настройте имя сообщества чтения/записи, время ожидания и время повтора. Вы можете использовать NMS для запроса и настройки устройства. **ПРИМЕЧАНИЕ:** конфигурации в NMS должны соответствовать конфигурациям на устройстве; в противном случае соответствующие операции не могут быть выполнены

Настройка SNMP v3 (View по умолчанию)

Сценарий:

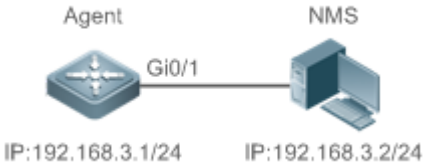


Рисунок 1-6.

	• NMS управляет сетевыми устройствами (агентами) на основе аутентификации пользователя и режима шифрования, например, NMS использует user1 в качестве имени пользователя, MD5 в качестве режима аутентификации, 123 в качестве пароля аутентификации, DES56 в качестве алгоритма шифрования и 321 в качестве пароль шифрования. • Вы можете получить доступ ко всем узлам MIB. («чтение по умолчанию, запись по умолчанию» ("read default write default") указывает, что доступ ко всем узлам MIB возможен. • Сетевые устройства могут активно отправлять сообщения аутентификации и шифрования в NMS

Шаги настройки	• Настройте группу MIB. Создайте группу «g1», выберите версию «v3», установите уровень безопасности на режим аутентификации и шифрования «priv», а также настройте разрешения на чтение и запись View «по умолчанию». «По умолчанию» указывает, что все узлы MIB могут быть доступны. • Настройте пользователя SNMP. Создайте пользователя с именем «user1» в группе «g1», выберите «v3» в качестве версии и установите режим аутентификации «md5», пароль аутентификации «123», режим шифрования «DES56» и пароль шифрования «321». • Настройте адрес узла SNMP. Установите адрес хоста на 192.168.3.2, выберите «3» в качестве версии, установите уровень безопасности на режим аутентификации и шифрования «priv» и свяжите имя пользователя «user1». Разрешите агенту активно отправлять сообщения trap в NMS. • Настройте IP-адрес агента. Установите адрес интерфейса Gi0/1 на 192.168.3.1/24
Агент	QTECH(config)#snmp-server group g1 v3 priv read default write default QTECH(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 QTECH(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 QTECH(config)#snmp-server enable traps QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit
Проверка	• Запустите команду **show running-config**, чтобы отобразить информацию о конфигурации устройства. • Запустите команду **show snmp user**, чтобы отобразить пользователя SNMP. • Запустите команду **show snmp view**, чтобы отобразить SNMP View. • Запустите команду **show snmp group**, чтобы отобразить группу SNMP. • Запустите команду **show snmp host**, чтобы отобразить информацию о хосте, настроенную пользователем. • Установите MIB-браузер
NMS	SNMP v3 использует механизмы безопасности аутентификации и шифрования. В NMS настройте имя пользователя и выберите уровень безопасности. В зависимости от выбранного уровня безопасности настройте режим аутентификации, пароль аутентификации, режим шифрования и пароль шифрования. Кроме того, настройте время ожидания и время повтора. Вы можете использовать NMS для запроса и настройки устройства. Подробнее о конфигурации см. Рисунок 1-7.

	ПРИМЕЧАНИЕ: конфигурации в NMS должны соответствовать конфигурациям на устройстве; в противном случае соответствующие операции не могут быть выполнены

Настройка конфигурации SNMPv3 (указанный вид)

Сценарий:

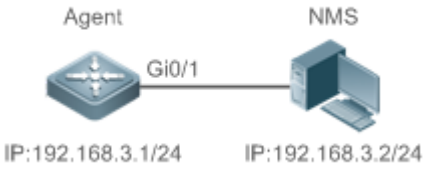
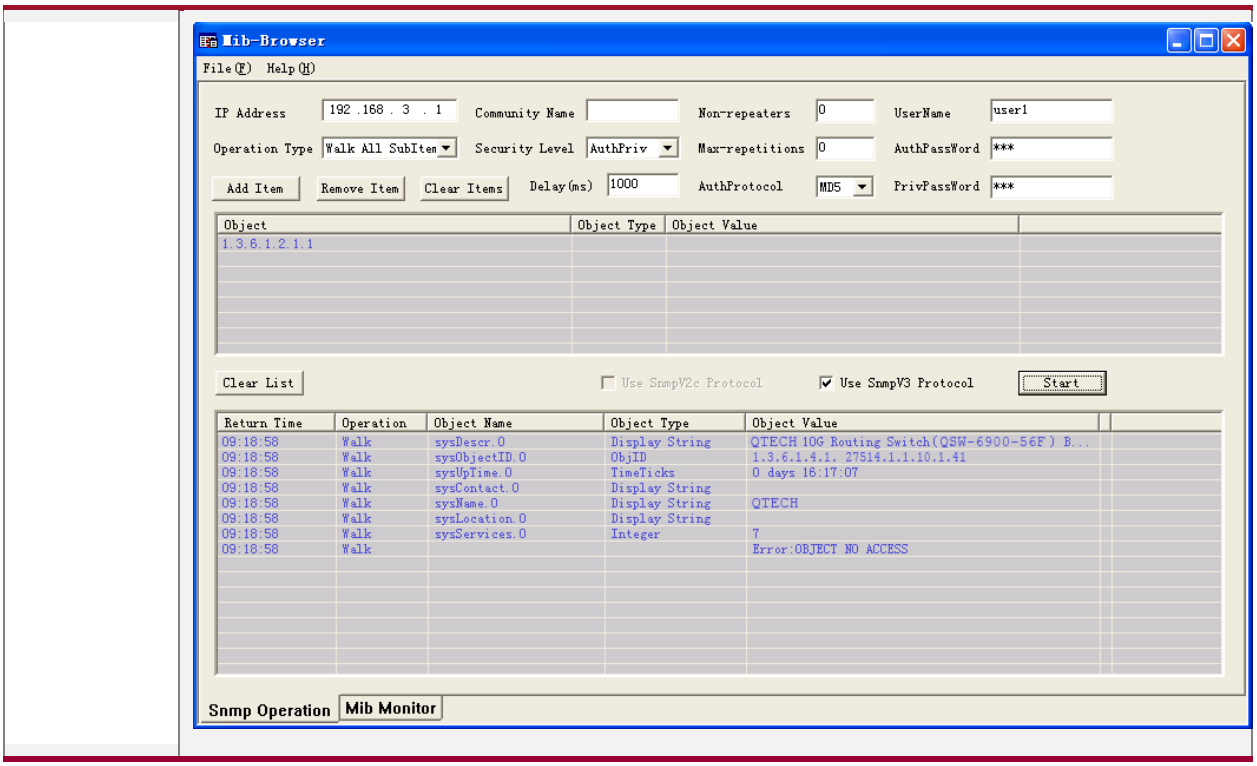


Рисунок 1-7.

	• NMS управляет сетевыми устройствами (агентами) на основе аутентификации пользователя и режима шифрования, например, NMS использует user1 в качестве имени пользователя, MD5 в качестве режима аутентификации, 123 в качестве пароля аутентификации, DES56 в качестве алгоритма шифрования и 321 в качестве пароль шифрования. • Сетевые устройства могут управлять разрешениями пользователей на доступ к объектам MIB. Например, пользователь с именем user1 может читать объекты MIB в системном узле (1.3.6.1.2.1.1) и может записывать объекты MIB только в узле SysContact (1.3.6.1.2.1.1.4.0). • Сетевые устройства могут активно отправлять сообщения аутентификации и шифрования в NMS
Шаги настройки	• Настройте MIB View и группу MIB. Создайте MIB View «view1», которое включает связанный объект MIB (1.3.6.1.2.1.1); затем создайте MIB View «view2», которое включает связанный объект MIB (1.3.6.1.2.1.1.4.0). Создайте группу «g1», выберите версию «v3», установите уровень безопасности на режим аутентификации и шифрования «priv» и настройте разрешения на чтение View «view1» и запись View «view2». • Настройте пользователя SNMP. Создайте пользователя с именем «user1» в группе «g1», выберите «v3» в качестве версии и установите режим аутентификации «md5», пароль аутентификации «123», режим шифрования «DES56» и пароль шифрования «321». • Настройте адрес узла SNMP. Установите адрес хоста на 192.168.3.2, выберите «3» в качестве версии, установите уровень безопасности на режим аутентификации и шифрования «priv» и свяжите имя пользователя «user1». Разрешите агенту активно отправлять сообщение trap в NMS. • Установите IP-адрес агента. Установите адрес интерфейса Gi0/1 на 192.168.3.1/24

Агент	QTECH(config)#snmp-server view view1 1.3.6.1.2.1.1 include QTECH(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include QTECH(config)#snmp-server group g1 v3 priv read view1 write view2 QTECH(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321 QTECH(config)#snmp-server host 192.168.3.2 traps version 3 priv user1 QTECH(config)#snmp-server enable traps QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit
Проверка	1. Запустите команду **show running-config**, чтобы отобразить информацию о конфигурации устройства. 2. Запустите команду **show snmp user**, чтобы отобразить пользователя SNMP. 3. Запустите команду **show snmp view**, чтобы отобразить SNMP View. 4. Запустите команду **show snmp group**, чтобы отобразить группу SNMP. 5. Запустите команду **show snmp host**, чтобы отобразить информацию о хосте, настроенную пользователем. 6. Установите MIB-браузер
Агент	QTECH# show running-config ! interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 ! snmp-server view view1 1.3.6.1.2.1.1 include snmp-server view view2 1.3.6.1.2.1.1.4.0 include snmp-server user user1 g1 v3 encrypted auth md5 7EBD6A1287D3548E4E52CF8349CBC93D priv des56 D5CEC4884360373ABBF30AB170E42D03 snmp-server group g1 v3 priv read view1 write view2 snmp-server host 192.168.3.2 traps version 3 priv user1 snmp-server enable traps
	QTECH# show snmp user User name: user1 Engine ID: 800013110300d0f8221120 storage-type: permanent active

	Security level: auth priv Auth protocol: MD5 Priv protocol: DES Group-name: g1
	QTECH#show snmp view view1(include) 1.3.6.1.2.1.1 view2(include) 1.3.6.1.2.1.1.4.0 default(include) 1.3.6.1
	QTECH# show snmp group groupname: g1 securityModel: v3 securityLevel:authPriv readview: view1 writeview: view2 notifyview:
	QTECH#show snmp host Notification host: 192.168.3.2 udp-port: 162 type: trap user: user1 security model: v3 authPriv
	Установите MIB-браузер, введите IP-адрес **192.168.3.1** в **IP Address** и **user1** в поле **UserName**, выберите **AuthPriv** для **Security Level**, введите **123** в **AuthPassWord**, выберите **MD5** для **AuthProtocol** и введите **321** в **PrivPassWord**. Нажмите «**Add Item**» и выберите единицу управления, для которой необходимо запросить MIB, например, «**System**» на следующем рисунке. Нажмите **Start**. MIB запрашивается для сетевых устройств. В нижней панели на следующем рисунке показаны результаты запроса.



1.4.2. Включение функции Trap

1.4.2.1. Эффект конфигурации

Разрешите агенту активно отправлять сообщение trap в NMS.

1.4.2.2. Шаги настройки

Настройка адреса узла SNMP

- Опционально
- Настройте адрес хоста NMS, когда от агента требуется активная отправка сообщений.

Включение агента для активной отправки сообщения trap в NMS

- Опционально
- Настройте этот элемент на агенте, когда от агента требуется активная отправка сообщения trap в NMS.

Включение функции отправки сообщения Link Trap на интерфейсе

- Опционально
- Настройте этот элемент в агенте, когда сообщение link trap необходимо отправить на интерфейс.

Включение функции отправки сообщения trap о перезагрузке системы

- Опционально
- Настройте этот элемент на агенте, когда от системы RGOS требуется отправить сообщение trap в NMS, чтобы уведомить о перезагрузке системы перед перезагрузкой или перезагрузкой устройства.

Указание исходного адреса для отправки сообщения trap

- Опционально

- Настройте этот элемент на агенте, если необходимо постоянно использовать локальный IP-адрес в качестве исходного адреса SNMP для облегчения управления.

Включение сообщения trap для переноса личных полей при отправке сообщения

- Опционально
- Настройте этот элемент в агенте, если в сообщении trap необходимо передавать приватные поля.

1.4.2.3. Проверка

Запустите команду **show snmp**, чтобы отобразить статус SNMP.

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

1.4.2.4. Связанные команды

Настройка адреса хоста NMS

Команда	**snmp-server host [oob] {** *host-addr* **| ipv6** *ipv6-addr* **| domain** *domain-name* **} [vrf** *vrfname* **] [traps | inrorms] [version { 1 | 2c | 3 { auth | noauth | priv }]** *community string* **[udp-port** *port-num* **] [** *notification-type* **]**
Описание параметров	**oob**: настраивает внеполосную связь (OOB) для сервера предупреждений (то есть информация отправляется на сервер предупреждений через интерфейс MGMT). *host-addr*: адрес хоста SNMP. *ipv6-addr*: (IPv6) адрес хоста SNMP. *domain-name*: доменное имя хоста SNMP. *vrfname*: настраивает имя таблицы переадресации VRF
Описание параметров	**traps | inrorms**: настраивает хост для отправки сообщения trap или информационного сообщения. **version**: версия SNMP, которая может быть установлена на V1, V2C или V3. **auth | noauth | priv**: устанавливает уровень безопасности для пользователей V3. *community string*: строка сообщества или имя пользователя (V3). *port-num*: настраивает идентификатор порта узла SNMP. *notification-type*: тип сообщений trap, которые активно отправляются, например, snmp. Если тип trap не указан, отправляются все сообщения trap
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Эта команда используется с командой **snmp-server enable traps** для активной отправки сообщений trap в NMS. Вы можете настроить различные хосты SNMP для получения сообщений trap. Хост может поддерживать различные trap, порты и таблицы переадресации VRF. Если настроен один и тот же хост (порт и конфигурация VRF одинаковы), последняя конфигурация объединяется с предыдущими конфигурациями, то есть для отправки разных trap-сообщений на один и тот же хост каждый раз настраивается один тип trap-сообщений. Эти конфигурации, наконец, объединены. В этой команде параметр **via** может быть указан только тогда, когда включен параметр **oob**. Кроме того, нельзя использовать параметр **vrf**

Включение агента для активной отправки сообщения trap в NMS

Команда	**snmp-server enable traps** [*notification-type*]
Описание параметров	*notification-type*: включает trap-уведомления для соответствующих событий, включая следующие типы: snmp: включает trap-уведомление для событий SNMP. bgp: включает trap-уведомление для событий BGP. bridge: включает trap-уведомление для событий моста. isis: включает trap-уведомление для событий ISIS. mac-notification: включает trap-уведомление для событий MAC. ospf: включает trap-уведомление для событий OSPF. urpf: включает trap-уведомления для событий URPF. vrrp: включает trap-уведомление для событий VRRP. web-auth: включает trap-уведомление для событий веб-аутентификации
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эта команда должна использоваться с командой **snmp-server host**, чтобы сообщения trap можно было активно отправлять

Включение функции отправки сообщения Link Trap на интерфейсе

Команда	**snmp trap link-status**
Режим конфигурации	Режим конфигурации интерфейса

Руководство по использованию	Для интерфейсов (интерфейс Ethernet, интерфейс AP и интерфейс SVI), когда эта функция включена, SNMP отправляет сообщение Link Trap, если статус соединения на интерфейсах изменяется. В противном случае SNMP не отправляет сообщение

Включение функции отправки сообщения trap о перезагрузке системы

Команда	**snmp-server system-shutdown**
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Когда функция уведомления при перезагрузке системы SNMP включена, в NMS отправляется сообщение trap, чтобы уведомить о перезагрузке системы перед перезагрузкой или перезагрузкой устройства

Указание исходного адреса для отправки сообщения trap

Команда	**snmp-server trap-source** *interface*
Описание параметров	*interface*: используется в качестве интерфейса для исходного адреса SNMP
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	По умолчанию в качестве исходного адреса используется IP-адрес интерфейса, на который отправляются пакеты SNMP. Для облегчения управления и идентификации эту команду можно запустить, чтобы постоянно использовать один локальный IP-адрес в качестве исходного адреса SNMP

Включение сообщения trap для переноса приватных полей при отправке сообщения

Команда	**snmp-server trap-format private**
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Эта команда может использоваться, чтобы позволить сообщению trap содержать приватные поля при отправке сообщения. В настоящее время поддерживаемые приватные поля включают время генерации предупреждения. Конкретные типы данных и диапазоны данных полей см. в QTECH-TRAP-FORMAT-MIB.mib

1.4.2.5. Пример конфигурации

Включение функции Trap

Сценарий:

Рисунок 1-8.

	NMS управляет сетевыми устройствами (агентами) на основе режима аутентификации сообщества, и сетевые устройства могут активно отправлять сообщения в NMS
Шаги настройки	1. Выполните настройку, чтобы агент мог активно отправлять сообщения в NMS. Установите адрес узла SNMP на 192.168.3.2, формат сообщения на Version2c и имя аутентификации на user1. Включите агент для активной отправки сообщений trap. 2. Установите IP-адрес агента. Установите адрес интерфейса Gi0/1 на 192.168.3.1/24
Агент	QTECH(config)#snmp-server host 192.168.3.2 traps version 2c user1 QTECH(config)#snmp-server enable traps QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit
Проверка	• Запустите команду **show running-config**, чтобы отобразить информацию о конфигурации устройства. • Запустите команду **show snmp**, чтобы отобразить статус SNMP
Агент	QTECH# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location Moscow snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact QTECH.com

	snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	QTECH#show snmp Chassis: 1234567890 0 SNMP packets input 0 Bad SNMP version errors 0 Unknown community name 0 Illegal operation for community name supplied 0 Encoding errors 0 Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0 Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1472) 0 No such name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs SNMP global trap: enabled SNMP logging: disabled SNMP agent: enabled

1.4.3. Экранирование функции агента

1.4.3.1. Эффект конфигурации

Защитите функцию агента, когда служба агента не требуется.

1.4.3.2. Примечания

- Запустите команду **no snmp-server**, чтобы скрыть функцию агента SNMP, когда служба агента не требуется.
- В отличие от команды экранирования, после запуска команды **no enable service snmp-agent** все службы SNMP напрямую отключаются (то есть функция агента SNMP отключается, пакет не принимается, а ответный пакет или пакет trap не отправляются), но информация о конфигурации агента не экранируется.

1.4.3.3. Шаги настройки

Экранирование функции агента SNMP для устройства

- Опционально
- Используйте эту конфигурацию, чтобы скрыть конфигурацию всех служб агента SNMP.

Отключение функции агента SNMP для устройства

- Опционально
- Чтобы напрямую отключить все службы, используйте эту конфигурацию.

1.4.3.4. Проверка

Запустите команду **show services**, чтобы проверить, включены ли службы SNMP.

Запустите команду **show snmp**, чтобы отобразить статус SNMP.

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

1.4.3.5. Связанные команды

Экранирование функции агента SNMP для устройства

Команда	**no snmp-server**
Режим команд	Режим глобальной конфигурации
Руководство по использованию	По умолчанию функция агента SNMP отключена. Когда параметры агента SNMP (например, адрес узла NMS, имя аутентификации и разрешение на доступ) установлены, служба агента SNMP включается автоматически. Команда **enable service snmp-agent** также должна быть запущена одновременно, чтобы служба агента SNMP могла работать. Если служба агента SNMP отключена или не запущена команда **enable service snmp-agent**, служба агента SNMP не действует. Запустите команду **no snmp-server**, чтобы отключить службы агента SNMP всех версий, поддерживаемых устройством. После выполнения этой команды все конфигурации службы агента SNMP экранируются (то есть после выполнения команды **show running-config** конфигурация не отображается. Конфигурации восстанавливаются после повторного включения службы агента SNMP). После выполнения команды **enable service snmp-agent** конфигурации агента SNMP не экранируются

Отключение функции агента SNMP для устройства

Команда	**no enable service snmp-agent**
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Эту команду можно использовать для отключения службу SNMP, но она не будет экранировать параметры агента SNMP

1.4.3.6. Пример конфигурации

Включение службы SNMP

Сценарий:

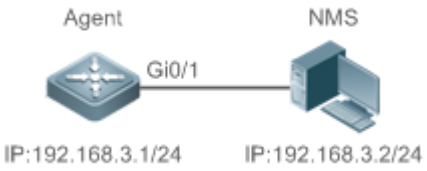


Рисунок 1-9.

	После включения службы SNMP и настройки сервера агента SNMP NMS может получить доступ к устройствам на основе SNMP
Шаги настройки	1. Включите службу SNMP. 2. Задайте параметры для сервера агента SNMP, чтобы служба SNMP вступила в силу
Агент	QTECH(config)#enable service snmp-agent
Проверка	Запустите команду **show services**, чтобы проверить, включена ли служба SNMP
Агент	QTECH#show service web-server : disabled web-server(https): disabled snmp-agent : enabled ssh-server : disabled telnet-server : enabled

1.4.4. Настройка параметров управления SNMP

1.4.4.1. Эффект конфигурации

Задайте основные параметры агента SNMP, включая режим контакта с устройством, местоположение устройства, серийный номер и параметры для отправки trap-сообщения. Получив доступ к параметрам, NMS может получить контактное лицо устройства и физическое местоположение устройства.

1.4.4.2. Шаги настройки

Установка режима системного контакта

- Опционально
- Когда контактный режим системы необходимо изменить, настройте этот элемент на агенте.

Настройка местоположения системы

- Опционально
- Если необходимо изменить расположение системы, настройте этот элемент на агенте.

Установка серийного номера системы

- Опционально
- Если необходимо изменить серийный номер системы, настройте этот элемент на агенте.

Установка информации NE об устройстве

- Опционально
- Если необходимо изменить код NE, настройте этот элемент на агенте.

Настройка максимальной длины пакета агента SNMP

- Опционально
- Если необходимо изменить максимальную длину пакета агента SNMP, настройте этот элемент на агенте.

Настройка идентификатора порта UDP службы SNMP

- Опционально
- Если необходимо изменить идентификатор порта UDP службы SNMP, настройте этот элемент на агенте.

Настройка длины очереди сообщений trap

- Опционально
- Если необходимо настроить размер очереди сообщений для управления скоростью отправки сообщений, настройте этот элемент на агенте.

Настройка интервала отправки сообщения trap

- Опционально
- Если необходимо изменить интервал отправки trap-сообщения, настройте этот пункт в агенте.

Настройка управления потоком SNMP

- Опционально
- Если большое количество пакетов запросов SNMP приводит к высокой загрузке ЦП для задач SNMP, настройте управление потоком SNMP, чтобы ограничить количество пакетов запросов, обрабатываемых в секунду в каждой задаче SNMP, чтобы контролировать использование ЦП для задач SNMP.

1.4.4.3. Проверка

Запустите команду **show snmp**, чтобы отобразить статус SNMP.

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

1.4.4.4. Связанные команды

Установка режима системного контакта

Команда	**snmp-server contact** *text*
Описание параметров	*text*: строка, описывающая режим контакта системы
Режим команд	Режим глобальной конфигурации

Настройка местоположения системы

Команда	**snmp-server location** *text*
Описание параметров	*text*: строка, описывающая системную информацию
Режим конфигурации	Режим глобальной конфигурации

Установка серийного номера системы

Команда	**snmp-server chassis-id** *text*
Описание параметров	*text*: текст серийного номера системы, который может состоять из цифр или символов
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Как правило, серийный номер устройства используется в качестве серийного номера SNMP для облегчения идентификации устройства

Установка информации NE об устройстве

Команда	**snmp-server net-id** *text*
Описание параметров	*text*: текст, который используется для установки кода NE устройства. Текст представляет собой строку, содержащую от 1 до 255 символов с учетом регистра и может включать пробелы
Режим конфигурации	Глобальный режим
Руководство по использованию	Установите код NE устройства

Настройка максимальной длины пакета агента SNMP

Команда	**snmp-server packetsize** *byte-count*
Описание параметров	*byte-count*: размер пакета от 484 байт до 17 876 байт
Режим конфигурации	Глобальный режим

Настройка идентификатора порта UDP службы SNMP

Команда	**snmp-server udp-port** *port-num*
Описание параметров	*port-num*: указывает идентификатор порта UDP службы SNMP, то есть идентификатор порта протокола, который получает пакеты SNMP
Режим конфигурации	Глобальный режим
Руководство по использованию	Укажите идентификатор порта протокола для приема пакетов SNMP

Настройка длины очереди сообщений trap

Команда	**snmp-server queue-length** *length*
Описание параметров	*length*: длина очереди в диапазоне от 1 до 1000
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Отрегулируйте размер очереди сообщений, чтобы контролировать скорость отправки сообщений

Настройка интервала отправки сообщения trap

Команда	**snmp-server trap-timeout** *seconds*
Описание параметров	*seconds*: интервал (единица измерения: секунда). Диапазон значений от 1 до 1000
Режим конфигурации	Режим глобальной конфигурации
Руководство по использованию	Настройте интервал отправки сообщения, чтобы контролировать скорость отправки сообщения

Настройка управления потоком SNMP

Команда	**snmp-server flow-control pps** [*count*]
Описание параметров	*count*: количество пакетов запросов SNMP, обрабатываемых в секунду. Диапазон значений составляет от 50 до 65 535
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Если большое количество пакетов запросов SNMP приводит к высокой загрузке ЦП для задач SNMP, настройте управление потоком SNMP, чтобы ограничить количество пакетов запросов, обрабатываемых в секунду в каждой задаче SNMP, чтобы контролировать использование ЦП для задач SNMP

1.4.4.5. Пример конфигурации

Настройка параметров управления SNMP

Сценарий:

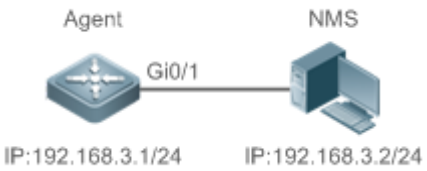


Рисунок 1-10.

	NMS управляет сетевыми устройствами (агентами) на основе режима аутентификации сообщества и может получать базовую системную информацию об устройствах, например, режим контакта с системой, местоположение и серийный номер
Шаги настройки	1. Задайте параметры агента SNMP. Установите местоположение системы, режим контакта и серийный номер. 2. Установите IP-адрес агента. Установите адрес интерфейса Gi0/1 на 192.168.3.1/24
Агент	QTECH(config)#snmp-server location Moscow QTECH(config)#snmp-server contact QTECH.ru QTECH(config)#snmp-server chassis-id 1234567890 QTECH(config)#interface gigabitEthernet 0/1 QTECH(config-if-gigabitEthernet 0/1)#ip address 192.168.3.1 255.255.255.0 QTECH(config-if-gigabitEthernet 0/1)#exit

Проверка	Проверьте информацию о конфигурации устройства. Проверьте SNMP View и информацию о группе
Агент	QTECH# show running-config ip access-list standard a1 10 permit host 192.168.3.2 interface gigabitEthernet 0/1 no ip proxy-arp ip address 192.168.3.1 255.255.255.0 snmp-server view v1 1.3.6.1.2.1.1 include snmp-server location Moscow snmp-server host 192.168.3.2 traps version 2c user1 snmp-server enable traps snmp-server contact QTECH.ru snmp-server community user1 view v1 rw a1 snmp-server chassis-id 1234567890
	QTECH#show snmp view v1(include) 1.3.6.1.2.1.1 default(include) 1.3.6.1 QTECH#show snmp group groupname: user1 securityModel: v1 securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview: groupname: user1 securityModel: v2c securityLevel:noAuthNoPriv readview: v1 writeview: v1 notifyview:

1.5. Мониторинг

1.5.1. Отображение

Описание	Команда
Отображает статус SNMP	**show snmp [mib | user | view | group| host]**

2. НАСТРОЙКА RMON

2.1. Обзор

Удаленный мониторинг сети (RMON) направлен на решение проблем управления локальными сетями (LAN) и удаленными сайтами с использованием одной центральной точки. В RMON данные мониторинга сети состоят из группы статистики и индикаторов производительности, которые можно использовать для мониторинга использования сети, чтобы облегчить планирование сети, оптимизацию производительности и диагностику сетевых ошибок.

RMON в основном используется управляющим устройством для удаленного мониторинга и управления управляемыми устройствами.

Протоколы и стандарты

STD 0059/RFC 2819: информационная база управления удаленным сетевым мониторингом.

RFC4502: информационная база управления удаленным мониторингом сети, версия 2.

RFC 3919: идентификаторы протокола удаленного мониторинга сети (RMON) для IPv6 и многопротокольной коммутации по меткам (MPLS).

RFC 3737: руководство IANA для модулей MIB реестра удаленного мониторинга (RMON).

RFC 3434: расширения MIB удаленного мониторинга для сигналов предупреждения большой емкости.

RFC 3395: справочные расширения идентификатора протокола MIB удаленного мониторинга сети.

RFC 3287: расширения MIB удаленного мониторинга для дифференцированных служб.

RFC 3273: информационная база управления удаленным мониторингом сети для сетей с высокой пропускной способностью.

RFC 2896: макросы идентификатора протокола MIB удаленного мониторинга сети.

RFC 2895: справочник по идентификатору протокола MIB удаленного мониторинга сети.

2.2. Приложения

Приложение	Описание
Сбор статистики по информации контролируемого интерфейса	Применяет четыре функции RMON к интерфейсу для мониторинга сетевой связи интерфейса

2.2.1. Сбор статистики по информации контролируемого интерфейса

2.2.1.1. Сценарий

Функция статистики RMON Ethernet используется для мониторинга накопленной информации об интерфейсе, функция статистики истории используется для контроля количества пакетов интерфейса в каждом интервале мониторинга, а функция сигнализации используется для немедленного получения исключений счетчика пакетов интерфейса. На следующем рисунке показана топология сети.

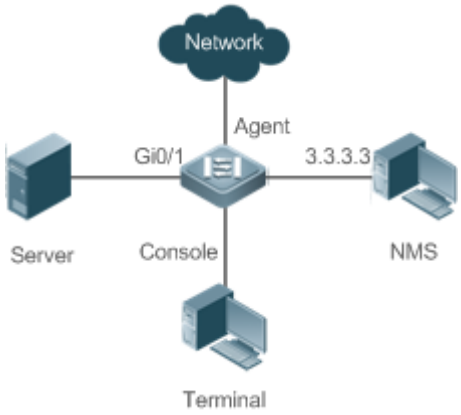


Рисунок 2-1.

2.2.1.2. Развертывание

Интерфейс отслеживается, чтобы накапливать статистику по количеству пакетов интерфейса и собирать статистику по количеству пакетов и использованию пропускной способности интерфейса в течение интервала мониторинга. Если на интерфейсе происходит исключение количества пакетов, в систему управления сетью (NMS) передается сигнал предупреждения. Ключевые моменты конфигурации следующие:

- Настройте функцию статистики RMON Ethernet на интерфейсе.
- Настройте функцию статистики истории RMON на интерфейсе.
- Настройте таблицу сигналов предупреждения RMON и определите действия по обработке событий RMON в режиме конфигурации. Контролируемые объекты сигналов предупреждений представляют собой значения идентификатора объекта (OID) определенных полей в статистической таблице RMON Ethernet, сконфигурированной для интерфейса.

2.3. Функции

2.3.1. Базовые концепты

RMON определяет несколько групп RMON. Продукты QTECH поддерживают группу статистики, группу истории, группу тревог и группу событий, которые описываются следующим образом:

Группа статистики

Группа статистики используется для мониторинга и сбора статистики по информации о трафике интерфейса Ethernet, которая накапливается с момента создания записи до текущего времени. Статистические элементы включают отброшенные пакеты данных, широковещательные пакеты данных, ошибки проверки циклического резервирования (CRC), большие и малые блоки и аварии. Статистические результаты сохраняются в статистической таблице Ethernet.

Группа истории

Группа истории используется для периодического сбора информации о сетевом трафике. Он записывает накопленные значения информации о сетевом трафике и использовании пропускной способности в течение каждого интервала и сохраняет их в таблице управления историей. Включает в себя две небольшие группы:

- Группа HistoryControl используется для установки интервала выборки, источника данных выборки и другой управляющей информации.

- Группа EthernetHistory предоставляет администраторам данные истории, включая статистику трафика сетевого сегмента, пакетов ошибок, широковещательных пакетов, использования и количества аварий.

Группа сигналов тревоги

Группа сигналов предупреждений используется для наблюдения за указанным объектом базы управляющей информации (MIB). Когда значение объекта MIB превышает заданный верхний предел или ниже заданного нижнего предела, срабатывает сигнал тревоги, который обрабатывается как событие.

Группа событий

Группа событий используется для определения режима обработки событий. Когда контролируемый объект MIB соответствует условиям тревоги, запускается событие. Событие может быть обработано в любом из следующих режимов:

- none: никаких действий не предпринимается.
- log: информация, относящаяся к событию, записывается в таблицу записей журнала, чтобы администраторы могли просматривать ее в любое время.
- snmp-trap: сообщение trap передается в NMS, чтобы уведомить NMS о возникновении события.
- log-and-trap: информация, относящаяся к событию, записывается в таблицу записей журнала, и в NMS передается сообщение trap.

2.3.1.1. Принцип работы

RMON поддерживает несколько мониторов и два метода сбора данных. Способ 1. Для сбора данных используется специальный зонд RMON, и NMS может напрямую получать всю информацию о MIB RMON из зонда RMON. Способ 2: агенты RMON встроены в сетевые устройства, чтобы устройства имели функцию проверки RMON. NMS использует основные команды простого протокола управления сетью (SNMP) для обмена данными с агентами RMON и сбора информации об управлении сетью. Этот метод, однако, ограничен ресурсами устройства, и собирается информация только о четырех группах, а не обо всех данных RMON MIB.

На следующем рисунке показан пример связи между агентами NMS и RMON. NMS через агентов RMON, работающих на устройствах, может получать информацию об общем трафике, статистике ошибок и статистике производительности сегмента сети, где находится интерфейс управляемого сетевого устройства, тем самым реализуя удаленное управление сетевыми устройствами.

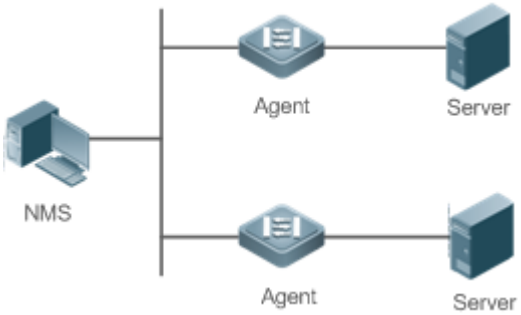


Рисунок 2-2.

2.3.1.2. Обзор

Особенность	Описание
RMON Статистика Ethernet	Собирает накопительно статистику по количеству пакетов, количеству байтов и другим данным отслеживаемого интерфейса Ethernet
Статистика истории RMON	Записывает количество пакетов, байтов и других данных, переданных интерфейсом Ethernet в течение настроенного интервала, и вычисляет использование полосы пропускания в течение этого интервала
Сигнал предупреждения RMON	Выборка значений контролируемых переменных через определенные промежутки времени. Таблица сигналов предупреждений используется в сочетании с таблицей событий. При достижении верхнего или нижнего предела соответствующая таблица событий инициируется для выполнения обработки событий или обработка не выполняется

2.3.2. RMON Статистика Ethernet

2.3.2.1. Принцип работы

Функция статистики RMON Ethernet накопительно собирает статистику по информации о сетевом трафике интерфейса Ethernet с момента создания записи до текущего времени.

2.3.2.2. Связанная конфигурация

Настройка статистических записей RMON

- Функция статистики RMON Ethernet по умолчанию отключена.
- Запустите команду **rmon collection stats**, чтобы создать записи статистики Ethernet на указанном интерфейсе Ethernet.
- После успешного создания статистических записей на указанном интерфейсе группа статистики собирает статистику по информации о трафике текущего интерфейса. Статистические элементы представляют собой переменные, определенные в статистической таблице RMON Ethernet, а записанная информация представляет собой накопленные значения переменных с момента создания статистической таблицы RMON до текущего времени.

2.3.3. Статистика истории RMON

2.3.3.1. Принцип работы

Функция статистики истории RMON записывает накопленную статистику по информации о трафике интерфейса Ethernet в течение каждого интервала.

2.3.3.2. Связанная конфигурация

Настройка контрольных записей истории RMON

- Функция статистики истории RMON отключена по умолчанию.

- Запустите команду **rmon collection history**, чтобы создать контрольные записи истории на интерфейсе Ethernet.
- Группа истории RMON собирает статистику по переменным, определенным в таблице истории RMON, и записывает накопленные значения переменных в течение каждого интервала.

2.3.4. Сигнал предупреждения RMON

2.3.4.1. Принцип работы

Функция сигнализации RMON периодически отслеживает изменения значений переменных сигнализации. Если значение переменной предупреждения достигает заданного верхнего порога или нижнего порога, запускается соответствующее событие для обработки, например, передается сообщение trap или создается одна запись в таблице журнала. Если нижнее пороговое значение или верхнее пороговое значение достигается несколько раз подряд, запускается только одно соответствующее событие, а другое событие запускается до тех пор, пока не будет достигнуто обратное пороговое значение.

2.3.4.2. Связанная конфигурация

Настройка таблицы событий

- Функция группы событий RMON отключена по умолчанию.
- Запустите команду **rmon event**, чтобы настроить таблицу событий.

Настройка записей предупреждений

- Функция группы сигналов предупреждений RMON отключена по умолчанию.
- Запустите команду **rmon event**, чтобы настроить таблицу событий, и запустите команду **rmon alarm**, чтобы настроить таблицу сигналов предупреждений RMON.
- Функция предупреждений RMON реализуется таблицей предупреждений и таблицей событий вместе. Если сообщение trap должно быть передано на управляющее устройство в случае события предупреждений, сначала необходимо правильно настроить агент SNMP. Для настройки агента SNMP см. Настройка SNMP.
- Если сконфигурированный объект сигнала предупреждений является узлом поля в группе статистики RMON или группе истории, функция статистики RMON Ethernet или функция статистики истории RMON должна быть настроена в первую очередь на контролируемом интерфейсе Ethernet.

2.4. Конфигурация

Конфигурация	Описание и команда	
Настройка статистики RMON Ethernet	(Обязательный) Используется для накопительного сбора статистики по информации о трафике интерфейса Ethernet	
	rmon collection stats	Настраивает статистические записи Ethernet

Конфигурация	Описание и команда	
Настройка статистики истории RMON	(Обязательный) Используется для периодического сбора статистических данных о трафике интерфейса Ethernet и использовании пропускной способности в течение интервала	
	rmon collection history	Настраивает контрольные записи истории
Настройка сигнала предупреждения RMON	(Обязательный) Используется для контроля того, находятся ли изменения данных переменной в допустимом диапазоне	
	rmon event	Настраивает записи событий
	rmon alarm	Настраивает записи предуреждений

2.4.1. Настройка статистики RMON Ethernet

2.4.1.1. Эффект конфигурации

Получите накопленную статистику по информации о трафике контролируемого интерфейса Ethernet с момента создания записи до текущего времени.

2.4.1.2. Примечания

Эта функция не может быть настроена в режиме пакетной настройки интерфейса.

2.4.1.3. Шаги настройки

Настройка статистических записей RMON

- Обязательный.
- Если для определенного интерфейса требуется статистика и мониторинг, для этого интерфейса необходимо настроить записи статистики Ethernet.

2.4.1.4. Проверка

Запустите команду **show rmon stats**, чтобы отобразить статистику Ethernet.

2.4.2. Связанные команды

Настройка статистических записей RMON

Команда	**rmon collection stats** *index* [**owner** *ownername*]
Описание параметров	*index*: указывает порядковый номер статистической записи со значением в диапазоне от 1 до 65 535. **owner** *ownername*: указывает создателя записи, т. е. имя владельца, которое представляет собой строку из 1–63 символов с учетом регистра

Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Значения параметров статистического ввода не могут быть изменены

2.4.2.1. Пример конфигурации

Настройка статистики RMON Ethernet

Сценарий:

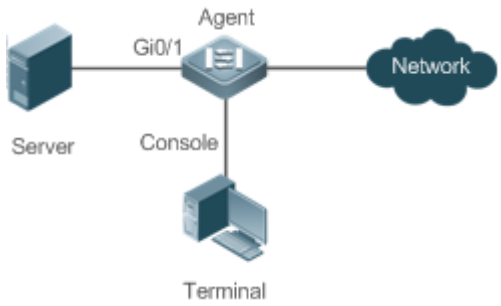


Рисунок 2-3.

	Как показано на предыдущем рисунке, агент RMON подключен к серверу, и NMS требует, чтобы группа статистики RMON выполняла статистику производительности по полученным пакетам интерфейса Gi0/1. Администраторы могут просматривать статистику в любое время, чтобы понимать данные о полученных пакетах интерфейса и своевременно принимать меры для обработки сетевых исключений
Шаги настройки	Настройте экземпляр статистической таблицы на интерфейсе GigabitEthernet 0/1 для сбора статистики по трафику этого интерфейса
Агент	QTECH# configure terminal QTECH (config)# interface gigabitEthernet 0/1 QTECH (config-if-GigabitEthernet 0/1)# rmon collection stats 1 owner admin
Проверка	Запустите команду **show rmon stats**, чтобы отобразить статистику Ethernet
Агент	QTECH# show rmon stats ether statistic table: index = 1 interface = GigabitEthernet 0/1 owner = admin status = 1 dropEvents = 0 octets = 25696

	pkts = 293 broadcastPkts = 3 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 packets64Octets = 3815 packets65To127Octets = 1695 packets128To255Octets = 365 packets256To511Octets = 2542 packets512To1023Octets = 152 packets1024To1518Octets = 685

2.4.2.2. Распространенные ошибки

Записи статистической таблицы реконфигурируются или изменяются сконфигурированные записи статистической таблицы.

2.4.3. Настройка статистики истории RMON

2.4.3.1. Эффект конфигурации

Получите накопленную статистику по трафику отслеживаемого интерфейса Ethernet и использованию полосы пропускания в каждом интервале.

2.4.3.2. Примечания

Эта функция не может быть настроена в режиме пакетной настройки интерфейса.

2.4.3.3. Шаги настройки

- Обязательный.
- Если необходимо собрать сетевую статистику на указанном интерфейсе, на этом интерфейсе должны быть настроены контрольные записи истории RMON.

2.4.3.4. Проверка

Запустите команду **show rmon history**, чтобы отобразить статистику группы истории.

2.4.3.5. Связанные команды

Настройка контрольных записей истории RMON

Команда	**rmon collection history** *index* **[owner** *ownername***] [buckets** *bucket-number***] [interval** *seconds***]**
Описание параметров	*index*: указывает порядковый номер статистической записи истории со значением в диапазоне от 1 до 65 535. **owner** *ownername*: указывает создателя записи, т. е. имя владельца, которое представляет собой строку из 1–63 символов с учетом регистра. **buckets** *bucket-number*: устанавливает емкость таблицы истории, в которой существует статистическая запись истории, то есть устанавливает максимальное количество записей (*bucket-number*), которое может быть размещено в таблице истории. Значение *bucket-number* находится в диапазоне от 1 до 65 535, а значение по умолчанию — 10. **interval** *seconds*: устанавливает статистический интервал в секундах. Диапазон значений составляет от 1 секунды до 3600 секунд, а значение по умолчанию — 1800 секунд
Режим команд	Режим конфигурации интерфейса
Руководство по использованию	Значения параметров записи статистики истории не могут быть изменены

2.4.3.6. Пример конфигурации

Настройка статистики истории RMON

Сценарий:

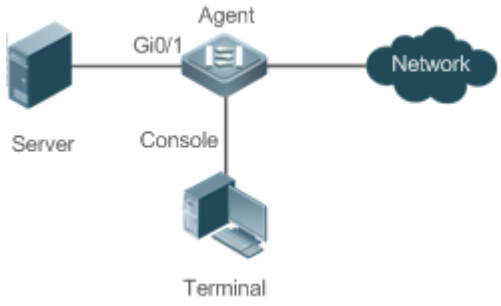


Рисунок 2-4.

	Как показано на предыдущем рисунке, агент RMON подключен к серверу, и NMS необходимо собирать статистику по полученным пакетам интерфейса Gi0/1 через группу истории RMON с интервалом в 60 секунд, чтобы контролировать сеть и понимать аварийные данные

Шаги настройки	Настройте таблицу управления историей на интерфейсе GigabitEthernet 0/1, чтобы периодически собирать статистику по трафику этого интерфейса
Агент	QTECH# configure terminal QTECH(config)# interface gigabitEthernet 0/1 QTECH(config-if-GigabitEthernet 0/1)# rmon collection history 1 buckets 5 interval 300 owner admin
Проверка	Запустите команду **show rmon history**, чтобы отобразить статистику группы истории
Агент	QTECH# show rmon history rmon history control table: index = 1 interface = GigabitEthernet 0/1 bucketsRequested = 5 bucketsGranted = 5 interval = 60 owner = admin stats = 1 rmon history table: index = 1 sampleIndex = 786 intervalStart = 6d:18h:37m:38s dropEvents = 0 octets = 2040 pkts = 13 broadcastPkts = 0 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0

```
index = 1
sampleIndex = 787
intervalStart = 6d:18h:38m:38s
dropEvents = 0
octets = 1791
pkts = 16
broadcastPkts = 1
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 788
intervalStart = 6d:18h:39m:38s
dropEvents = 0
octets = 432
pkts = 6
broadcastPkts = 0
multiPkts = 0
crcAlignErrors = 0
underSizePkts = 0
overSizePkts = 0
fragments = 0
jabbers = 0
collisions = 0
utilization = 0

index = 1
sampleIndex = 789
intervalStart = 6d:18h:40m:38s
dropEvents = 0
```

	octets = 432 pkts = 6 broadcastPkts = 0 multiPkts = 0 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0 index = 1 sampleIndex = 790 intervalStart = 6d:18h:41m:38s dropEvents = 0 octets = 86734 pkts = 934 broadcastPkts = 32 multiPkts = 23 crcAlignErrors = 0 underSizePkts = 0 overSizePkts = 0 fragments = 0 jabbers = 0 collisions = 0 utilization = 0

2.4.3.7. Распространенные ошибки

Записи таблицы управления историей настраиваются повторно или изменяются настроенные записи таблицы управления историей.

2.4.4. Настройка сигнала предупреждения RMON

2.4.4.1. Эффект конфигурации

Периодически проверяйте, находятся ли изменения значений переменных сигнализации в пределах указанного допустимого диапазона.

2.4.4.2. Примечания

Если сообщение trap должно быть передано на управляющее устройство при срабатывании события предупреждения, агент SNMP должен быть правильно настроен. Для настройки агента SNMP см. Настройка SNMP.

Если сигнальная переменная является переменной MIB, определенной в группе статистики RMON или группе истории, функция статистики RMON Ethernet или функция статистики истории RMON должна быть настроена на контролируемом интерфейсе Ethernet. В противном случае таблица сигналов предупреждения не будет создана.

2.4.4.3. Шаги настройки

Настройка записей событий

- Обязательный.
- Завершите настройку в режиме глобальной конфигурации.

Настройка записей предупреждений

- Обязательный.
- Завершите настройку в режиме глобальной конфигурации.

2.4.4.4. Проверка

- Запустите команду **show rmon event**, чтобы отобразить таблицу событий.
- Запустите команду **show rmon alarm**, чтобы отобразить таблицу сигналов предупреждений.

2.4.4.5. Связанные команды

Настройка таблицы событий

Команда	**rmon event** *number* [**log**] [**trap** *community*] [**description** *description-string*] [**owner** *ownername*]
Описание параметров	*number*: указывает порядковый номер таблицы событий со значением в диапазоне от 1 до 65 535. **log**: указывает на событие журнала. Система регистрирует инициированное событие. **trap** *community*: обозначает сообщение trap. Когда событие инициируется, система передает сообщение trap с именем сообщества *community*. **description** *description-string*: задает информацию описания события, то есть строку описания. Значение представляет собой строку от 1 до 127 символов. **owner** *ownername*: указывает создателя записи, т. е. имя владельца, которое представляет собой строку из 1–63 символов с учетом регистра
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Можно изменить значения сконфигурированных параметров записи события, включая тип события, имя группы trap, описание события и создателя события

Настройка группы сигналов предупреждений RMON

Команда	**rmon alarm** *number variable interval* **{absolute | delta} rising-threshold** *value* **[***event number***] falling-threshold** *value* **[***event-number***] [owner** *ownername***]**
Описание параметров	*number*: указывает порядковый номер записи сигнала предупреждения со значением в диапазоне от 1 до 65 535. *variable*: указывает переменную сигнала предупреждения, которая представляет собой строку из 1–255 символов и представлена в формате с точками с использованием OID узла (формат: entry.integer.instance (запись.целое число.экземпляр); пример: 1.3.6.1.2.1.2.1.10.1). *interval*: указывает интервал выборки в секундах и значение в диапазоне от 1 до 2 147 483 647. **absolute**: указывает, что тип выборки — выборка абсолютного значения, то есть значения переменных извлекаются напрямую, когда время выборки истекло. **delta**: указывает, что тип выборки — выборка изменяющегося значения, т. е. изменения значений переменных в пределах интервала выборки извлекаются по истечении времени выборки. **rising-threshold**: устанавливает верхний предел количества выборки (значение) со значением в диапазоне от −2 147 483 648 до +2 147 483 647. *event number*: указывает, что событие с номером события *event number* запускается при достижении верхнего или нижнего предела. **falling-threshold**: устанавливает нижний предел количества выборки (значение) со значением в диапазоне от −2 147 483 648 до +2 147 483 647. **owner** *ownername*: указывает создателя записи, т. е. имя владельца, которое представляет собой строку из 1–63 символов с учетом регистра
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Значения сконфигурированных параметров записи предупреждений могут быть изменены, включая переменные предупреждений, тип выборки, создатель записи, интервал выборки, верхний/нижний предел количества выборки и соответствующие триггерные события

2.4.4.6. Пример конфигурации

Настройка сигнала предупреждения RMON

Сценарий:

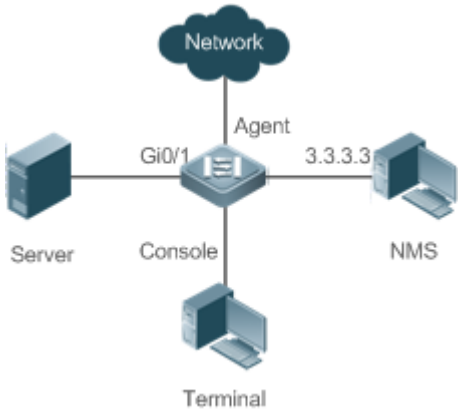


Рисунок 2-5.

	Предположим, что SNMPv1 работает в NMS, имя сообщества, используемое для доступа к настройкам, является общедоступным, с атрибутом read-write, а IP-адрес, используемый NMS для получения сообщений trap, — 3.3.3.3. Предположим, что значение OID пакетов неизвестного протокола, полученных контролируемым интерфейсом GigabitEthernet0/1, равно 1.3.6.1.2.1.2.2.1.15.3, режим выборки — относительная выборка, а интервал выборки — 60 секунд. Когда относительное значение выборки больше 100 или меньше 10, события 1 и 2 запускаются соответственно. В событии 1 передается сообщение trap, и событие регистрируется. В событии 2 событие только регистрируется. Настройка агента RMON завершена на терминале. Агент RMON подключен к NMS и подключен к серверу через интерфейс GI0/1. Агент RMON должен контролировать количество пакетов неизвестного протокола, полученных интерфейсом GI0/1. Интервал выборки составляет 60 секунд. Когда абсолютное значение выборки меньше 10, событие только регистрируется. Когда абсолютное значение выборки превышает 100, событие регистрируется, и в NMS передается сообщение trap
Шаги настройки	• Настройте адрес хоста для получения сообщений trap. • Настройте группу событий для обработки триггера предупреждений. • Настройте функцию предупреждений
Агент	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# snmp-server community public rw QTECH(config)# snmp-server host 3.3.3.3 trap public QTECH(config)# rmon event 1 description rising-threshold-event log trap public owner admin

	QTECH(config)# rmon event 2 description falling-threshold-event log owner admin QTECH(config)# rmon alarm 1 1.3.6.1.2.1.2.2.1.15.3 60 delta rising-threshold 100 1 falling-threshold 10 2 owner admin
Проверка	• Запустите команду **show rmon event**, чтобы отобразить таблицу событий. • Запустите команду **show rmon alarm**, чтобы отобразить таблицу сигналов предупреждений
Агент	QTECH# show rmon event rmon event table: index = 1 description = rising-threshold-event type = 4 community = public lastTimeSent = 0d:0h:0m:0s owner = admin status = 1 index = 2 description = falling-threshold-event type = 2 community = lastTimeSent = 6d:19h:21m:48s owner = admin status = 1 rmon log table: eventIndex = 2 index = 1 logTime = 6d:19h:21m:48s logDescription = falling-threshold-event QTECH# show rmon alarm rmon alarm table: index: 1, interval: 60, oid = 1.3.6.1.2.1.2.2.1.15.3

	sampleType: 2, alarmValue: 0, startupAlarm: 3, risingThreshold: 100, fallingThreshold: 10, risingEventIndex: 1, fallingEventIndex: 2, owner: admin, stauts: 1

2.4.4.7. Распространенные ошибки

- Введенный OID отслеживаемого объекта неверен, переменная, соответствующая OID, не существует, или тип не является целым числом или целым числом без знака.
- Верхний порог меньше или равен нижнему порогу.

2.5. Мониторинг

2.5.1. Отображение

Описание	Команда
Отображает всю информацию о конфигурации RMON	**show rmon**
Отображает статистическую таблицу Ethernet	**show rmon stats**
Отображает таблицу управления историей	**show rmon history**
Отображает таблицу сигналов предупреждений	**show rmon alarm**
Отображает таблицу событий	**show rmon event**

3. НАСТРОЙКА NTP

3.1. Обзор

Протокол сетевого времени (NTP) — это протокол уровня приложений, который позволяет сетевым устройствам синхронизировать время. NTP позволяет сетевым устройствам синхронизировать время со своими серверами или источниками часов и обеспечивает высокоточную коррекцию времени (разница со стандартным временем составляет менее одной миллисекунды в локальной сети и менее нескольких десятков миллисекунд в глобальной сети). Кроме того, NTP может предотвращать атаки с помощью зашифрованного подтверждения.

В настоящее время устройства QTECH можно использовать как в качестве NTP-клиентов, так и в качестве NTP-серверов. Другими словами, устройство QTECH может синхронизировать время с сервером времени и использоваться в качестве сервера времени для обеспечения синхронизации времени для других устройств. Когда устройство QTECH используется в качестве сервера, оно поддерживает только режим одноадресного сервера.

Протоколы и стандарты

RFC 1305: протокол сетевого времени (версия 3).

3.2. Приложения

Приложение	Описание
Синхронизация времени на основе внешнего эталонного источника	В качестве клиента используется устройство, синхронизирующее время с внешним источником часов. После успешной синхронизации он используется в качестве сервера для обеспечения синхронизации времени для других устройств
Синхронизация времени на основе локального источника эталонных часов	Устройство использует локальные часы в качестве надежного источника эталонных часов NTP, а также используется в качестве сервера для обеспечения синхронизации времени для других устройств

3.2.1. Синхронизация времени на основе внешнего эталонного источника часов

3.2.1.1. Сценарий

Как показано на Рисунке 3-1

- DEVICE-A используется в качестве надежного эталонного источника часов для обеспечения синхронизации времени для внешних устройств.
- DEVICE-B указывает DEVICE-A в качестве NTP-сервера и синхронизирует время с DEVICE-A.
- После успешной синхронизации DEVICE-B обеспечивает синхронизацию времени для DEVICE-C.

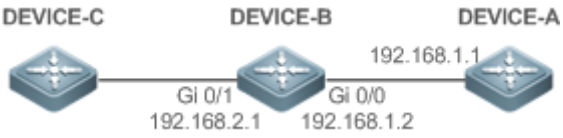


Рисунок 3-1.

3.2.1.2. Развертывание

Настройте DEVICE-B на режим внешнего эталонного источника часов NTP.

3.2.2. Синхронизация времени на основе локального источника эталонных часов

3.2.2.1. Сценарий

Как показано на Рисунке 3-2, DEVICE-B использует локальные часы в качестве источника опорных часов NTP и обеспечивает синхронизацию времени для DEVICE-C.

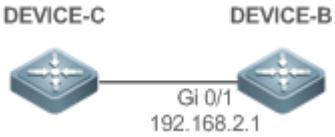


Рисунок 3-2.

3.2.2.2. Развертывание

Настройте DEVICE-B на режим локальных эталонных часов NTP.

3.3. Функции

3.3.1. Базовые концепты

NTP-пакет

Как определено в RFC1305, NTP использует пакеты протокола пользовательских датаграмм (UDP) для передачи, а используемый идентификатор порта UDP — 123.

На Рисунке 3-3 показан формат пакета синхронизации времени NTP.

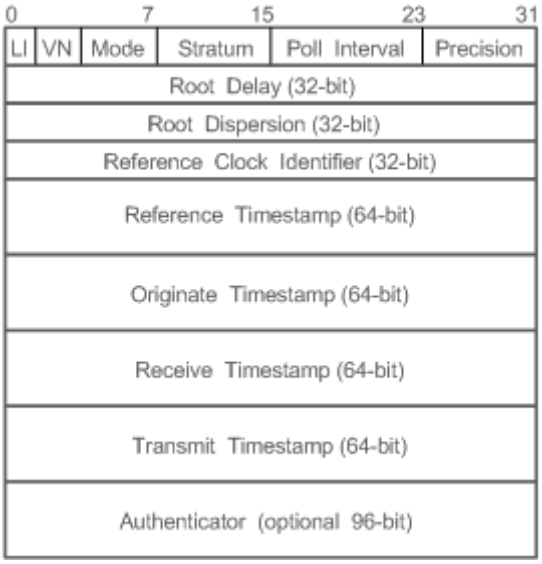


Рисунок 3-3. Формат пакета синхронизации времени NTP

- Индикатор секунды координации (LI): указывает 2-битный индикатор дополнительной секунды.

ПРИМЕЧАНИЕ: 00: указывает на отсутствие предупреждающей информации; 01: указывает, что в предыдущей минуте 61 секунда; 10: указывает, что в предыдущей минуте 59 секунд; 11: указывает, что часы не синхронизированы.

- Номер версии (VN): указывает 3-битный номер версии NTP. Текущий номер версии — 3.
- Режим (Mode): указывает на 3-битный рабочий режим NTP.

ПРИМЕЧАНИЕ: 0: указывает на отсутствие определения; 1: указывает на симметричную активность; 2: указывает на симметричный пассив; 3: указывает на клиента; 4: указывает на сервер; 5: указывает на широковещание; 6: указывает управляющую информацию; 7: зарезервировано.

- Stratum: указывает 8-битный слой (Stratum) локальных часов. 0: указывает на отсутствие определения; 1: указывает master-источник эталонных часов; другие значения: указывают slave-источники эталонных часов.
- Poll Interval (Интервал опроса): указывает интервал опроса (в секундах), который представляет собой 8-битное целое число.
- Precision (Точность): указывает точность времени (в секундах) местных часов, которая представляет собой 8-битное целое число.
- Root Delay (Корневая задержка): указывает время прохождения туда и обратно до master-источника эталонных часов, которое представляет собой 32-разрядное целое число.
- Root Dispersion (Корневая дисперсия): указывает самую большую разницу от master-эталонного источника тактового сигнала, который представляет собой 32-разрядное целое число.
- Reference Clock Identifier (Идентификатор эталонных часов): указывает 32-битный идентификатор источника эталонных часов.
- Reference Timestamp (Эталонная временная метка): указывает 64-битную временную метку, а именно время, которое было установлено или исправлено в последний раз.
- Originate Timestamp (Исходная временная метка): указывает 64-битную метку времени, а именно местное время, когда от клиента уходит запрос на синхронизацию времени.
- Receive Timestamp (Отметка времени получения): указывает 64-битную отметку времени, а именно местное время, когда пакет запроса синхронизации времени поступает на сервер.
- Transmit Timestamp (Отметка времени передачи): указывает 64-битную отметку времени, а именно местное время, когда ответный пакет синхронизации времени отправляется с сервера.
- Authenticator (Опционально): указывает информацию для аутентификации.

NTP-сервер

Устройство использует локальные часы в качестве источника эталонных часов для обеспечения синхронизации времени для других устройств в сети.

NTP-клиент

Устройство используется как NTP-клиент, синхронизирующий время с NTP-сервером в сети.

Stratum (Слой)

В NTP «stratum» используется для описания переходов от устройства к авторитетным (достоверным) часам. Сервер NTP, stratum которого равен 1, имеет непосредственно подключенные атомные часы или часы с радиоуправлением; сервер NTP, stratum которого равен 2, получает время от сервера, stratum которого равен 1; сервер NTP, stratum которого равен 3, получает время от сервера, stratum которого равен 2; и так далее. Следовательно, источники часов с более низким stratum имеют более высокую точность часов.

Аппаратные часы

Аппаратные часы работают на частоте кварцевого резонатора устройства и питаются от батареи устройства. После выключения устройства аппаратные часы продолжают работать. После запуска устройства оно получает информацию о времени от аппаратных часов в виде программного времени устройства.

3.3.2. Обзор

Особенность	Описание
Синхронизация времени NTP	Сетевые устройства синхронизируют время со своими серверами или надежными источниками часов для реализации высокоточной коррекции времени
Аутентификация Security NTP	Аутентификация с шифрованием пакетов NTP используется для предотвращения помех синхронизации времени на устройстве от ненадежных источников часов
NTP-контроль доступа	Список контроля доступа (ACL) используется для фильтрации источников полученных пакетов NTP

3.3.3. Синхронизация времени NTP

3.3.3.1. Принцип работы

Синхронизация времени NTP реализована путем взаимодействия пакетов NTP между клиентом и сервером:

- Клиент отправляет пакет синхронизации времени на все серверы каждые 64 секунды. После получения пакетов ответов от серверов клиент фильтрует и выбирает пакеты ответов со всех серверов и синхронизирует время с оптимальным сервером.
- После получения пакета запроса на синхронизацию времени сервер использует локальные часы в качестве эталонного источника и заполняет информацией о локальном времени ответный пакет, который должен быть отправлен клиенту, в соответствии с требованиями протокола.

На Рисунке 3-4 показан формат пакета синхронизации времени NTP.

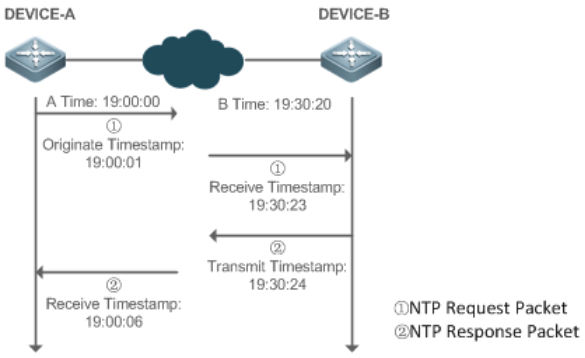


Рисунок 3-4. Принцип работы NTP

DEVICE-B (сокращенно B) используется в качестве источника эталонных часов NTP, DEVICE-A (сокращенно A) используется в качестве клиента NTP, который синхронизирует время с DEVICE-B. В момент времени местные часы A показывают 19:00:00, а местные часы B — 19:30:20.

1. A отправляет пакет запроса NTP. Местное время (T0), когда пакет отправляется из A, составляет 19:00:00 и заполняется в Originate Timestamp.
2. После 2-секундной сетевой задержки местное время (T1), когда B получает пакет запроса, составляет 19:30:23 и заполняется в Receive Timestamp.
3. B обрабатывает запрос NTP и через секунду отправляет ответный пакет NTP. Местное время (T2), когда ответный пакет уходит из B, составляет 19:30:24 и заполняется в Transmit Timestamp.
4. После 2-секундной сетевой задержки A получает ответный пакет. Местное время (T3), когда ответный пакет прибывает в A, составляет 19:00:06.

Конкретные расчеты для синхронизации времени следующие:

- A получает разницу во времени в 30 минут и 20 секунд между B и A, используя формулу ((T1-T0)+(T2-T3))/2.
- A получает четырехсекундную задержку пакета туда и обратно между A и B, используя формулу (T3-T0)-(T2-T1).

3.3.3.2. Режим работы NTP

- Режим внешней синхронизации часов

В этом режиме устройство используется и как сервер, и как клиент. При получении запросов на синхронизацию времени от других клиентов устройство должно сначала синхронизировать время с указанным сервером и обеспечить синхронизацию времени для клиентов после успешной синхронизации.

- Режим отсчета локальных часов

В этом режиме устройство использует локальные часы по умолчанию в качестве надежного источника часов и обеспечивает синхронизацию времени непосредственно для других клиентов.

3.3.3.3. Связанная конфигурация

Настройка NTP-сервера

- Функция NTP по умолчанию отключена.
- Запустите команду **ntp server**, чтобы указать NTP-сервер (внешний источник эталонных часов), который может включить NTP.

- После настройки устройство работает в режиме внешнего эталона часов.

Синхронизация в реальном времени

По умолчанию устройство выполняет синхронизацию времени каждые 64 секунды.

Обновление аппаратных часов

- По умолчанию устройство не обновляет синхронизированное время до аппаратных часов.
- Запустите команду **ntp update-calendar**, чтобы устройство автоматически обновляло аппаратные часы каждый раз после успешной синхронизации времени.

Настройка основных часов NTP

- По умолчанию устройство работает в режиме внешних эталонных часов.
- Запустите команду **ntp master**, чтобы настроить устройство на режим локальных эталонных часов.

3.3.4. Аутентификация Security NTP

Чтобы предотвратить злонамеренное повреждение сервера NTP, NTP использует механизм аутентификации, чтобы проверить, действительно ли информация о синхронизации времени поступает с объявленного сервера, и проверить путь возврата информации, чтобы обеспечить механизм защиты от помех.

3.3.4.1. Принцип работы

Клиент NTP и сервер NTP настроены с одним и тем же ключом. При отправке пакетов запроса и ответа устройство вычисляет хеш-значения пакетов с помощью алгоритма MD5 на основе указанного ключа и содержимого пакета NTP и заполняет хэш-значения в информации аутентификации пакета. Принимающее устройство проверяет, отправлены ли пакеты доверенным устройством или изменены на основе информации аутентификации.

3.3.4.2. Связанная конфигурация

Настройка механизма глобальной аутентификации Security для NTP

- По умолчанию механизм проверки подлинности Security NTP не включен.
- Запустите команду **ntp authentication**, чтобы включить механизм аутентификации Security NTP.

Настройка глобального ключа аутентификации для NTP

- По умолчанию глобальный ключ аутентификации не настроен.
- Запустите команду **ntp authentication-key**, чтобы включить глобальный ключ аутентификации NTP.

Настройка идентификатора глобально доверенного ключа для NTP

- По умолчанию глобально доверенный ключ не настроен.
- Запустите команду **ntp trust-key**, чтобы настроить устройство в качестве эталонного источника часов, чтобы предоставить доверенный ключ для внешней синхронизации времени.

Настройка идентификатора доверенного ключа для внешнего источника эталонных часов

Запустите команду **ntp server**, чтобы указать внешний эталонный источник, а также доверенный ключ этого источника синхронизации.

3.3.5. NTP-контроль доступа

3.3.5.1. Принцип работы

Обеспечьте минимальную меру безопасности, используя ACL.

3.3.5.2. Связанная конфигурация

Настройка прав управления доступом для служб NTP

- По умолчанию права управления доступом для NTP отсутствуют.
- Запустите команду **ntp access-group**, чтобы настроить права доступа для NTP.

3.4. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций NTP	(Обязательно) Используется для включения NTP. После включения NTP устройство работает в режиме внешних эталонных часов	
	ntp server	Настраивает NTP-сервер
	ntp update-calendar	Автоматически обновляет аппаратные часы
	(Опционально) Используется для настройки устройства на режим локальных часов	
	ntp master	Настраивает master-часы NTP
	(Опционально) Используется для отключения NTP	
	no ntp	Отключает все функции NTP и очищает все конфигурации NTP
	ntp disable	Отключает получение пакетов NTP с указанного интерфейса
	ntp service disable	Отключает службу синхронизации времени NTP
Настройка аутентификации безопасности NTP	(Опционально) Используется для предотвращения помех синхронизации времени на устройстве от ненадежных источников тактового сигнала	
	ntp authenticate	Включает механизм аутентификации security

Конфигурация	Описание и команда	
Настройка аутентификации безопасности NTP	**ntp authentication-key**	Настраивает глобальный ключ аутентификации
	ntp trusted-key	Настраивает доверенный ключ для синхронизации времени
	ntp server	Настраивает доверенный ключ для внешнего эталонного источника синхронизации
Настройка контроля доступа NTP	(Опционально) Используется для фильтрации источников полученных NTP-пакетов	
	ntp access-group	Настраивает права управления доступом для NTP

3.4.1. Настройка основных функций NTP

3.4.1.1. Эффект конфигурации

Режим внешней опорной частоты

- Используйте устройство в качестве клиента для синхронизации времени от внешнего эталонного источника часов с локальными часами.
- После успешной синхронизации времени используйте устройство в качестве сервера синхронизации времени, чтобы обеспечить синхронизацию времени.

Режим отсчета локальных часов

Используйте локальные часы устройства в качестве источника эталонных часов NTP для обеспечения синхронизации времени.

3.4.1.2. Примечания

- В режиме клиент/сервер устройство можно использовать в качестве сервера синхронизации времени для обеспечения синхронизации времени только после успешной синхронизации времени с надежным внешним источником часов.
- После настройки режима локальных эталонных часов система не будет синхронизировать время с источником часов с более высоким stratum.
- Настройка локальных часов в качестве master-часов (особенно при указании нижнего stratum) может перезаписать действующий источник часов. Если эта команда используется для нескольких устройств в сети, разница в часах между устройствами может привести к нестабильной синхронизации времени в сети.
- Прежде чем локальные часы будут настроены в качестве master-часов, если система никогда не синхронизирует время с внешним источником часов, вам может потребоваться вручную откалибровать системные часы, чтобы убедиться в отсутствии чрезмерной разницы. Дополнительные сведения о ручной калибровке системных часов см. в разделе конфигурации системного времени в руководстве System Configuration.

3.4.1.3. Шаги настройки

Настройка NTP-сервера

- (Обязательно) Должен быть указан хотя бы один внешний источник эталонных часов (можно настроить не более 20 различных внешних источников эталонных часов).
- Если необходимо настроить ключ NTP, вы должны настроить аутентификацию security NTP перед настройкой сервера NTP.

Автоматическое обновление аппаратных часов

- Опционально.
- По умолчанию система обновляет только системные часы, но не аппаратные часы после успешной синхронизации времени.
- После настройки этой команды система автоматически обновляет аппаратные часы после успешной синхронизации времени.

Настройка master-часов NTP

Чтобы переключить устройство в режим локальных эталонных часов, выполните эту команду.

Отключение NTP

- Чтобы отключить NTP и очистить настройки NTP, выполните команду **no ntp**.
- По умолчанию все интерфейсы могут получать пакеты NTP после включения NTP. Чтобы отключить NTP для указанного интерфейса, выполните команду **ntp disable**.

Отключение службы синхронизации времени NTP

NTP работает в режиме клиент/сервер. После того, как устройство NTP синхронизирует время с внешним надежным источником часов, оно служит сервером времени для предоставления службы синхронизации времени. Если устройство просто нужно обслуживать в качестве клиента NTP, настройте команду **ntp service disable**, чтобы отключить службу синхронизации времени NTP.

3.4.1.4. Проверка

- Запустите команду **show ntp status**, чтобы отобразить конфигурацию NTP.
- Запустите команду **show clock**, чтобы проверить, завершена ли синхронизация времени.

3.4.1.5. Связанные команды

Настройка NTP-сервера

Команда	**ntp server[oob | vrf** *vrf-name*]{ *ip-addr* | *domain* | **ip** *domain* | **ipv6** *domain*}[**version** *version*] [**source** *if-name*] [**key** *keyid*][**prefer**] [**via** *mgmt-name*]
Описание параметров	**oob**: указывает, привязан ли источник эталонных часов к интерфейсу MGMT. *vrf-name*: указывает имя VRF, привязанного к эталонному источнику часов. *ip-addr*: указывает адрес IPv4/IPv6 источника эталонных часов

Описание параметров	*domain*: указывает доменное имя IPv4/IPv6 источника эталонных часов. *version*: указывает номер версии NTP в диапазоне от 1 до 3. *if-name*: указывает тип интерфейса, включая AggregatePort, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template и VLAN. *keyid*: указывает ключ, используемый для связи с источником эталонных часов, в диапазоне от 1 до 4 294 967 295. **prefer**: указывает, имеет ли источник эталонных часов высокий приоритет. *mgmt-name*: задает исходящий интерфейс управления для пакетов в режиме oob
Режим команд	Режим глобальной конфигурации
Руководство по использованию	По умолчанию сервер NTP не настроен. Клиентская система QTECH поддерживает взаимодействие до 20 NTP-серверов. Вы можете настроить ключ проверки подлинности для каждого сервера (после настройки глобальной проверки подлинности и соответствующего ключа), чтобы инициировать зашифрованную связь с серверами. **ПРИМЕЧАНИЕ:** если необходимо настроить ключ аутентификации, вы должны настроить аутентификацию NTP security перед настройкой NTP-сервера. Версия NTP по умолчанию для связи с сервером — NTP версии 3. Кроме того, вы можете настроить исходный интерфейс для передачи NTP-пакетов и указать, что NTP-пакеты от соответствующего сервера могут быть получены только на передающем интерфейсе

Обновление аппаратных часов

Команда	**ntp update-calendar**
Режим команд	Режим глобальной конфигурации

Настройка локального источника эталонных часов

Команда	**ntp master**[*stratum*]
Описание параметров	*stratum*: указывает stratum локальных часов в диапазоне от 1 до 15. Значение по умолчанию — 8
Режим команд	Режим глобальной конфигурации

Отключение NTP

Команда	**no ntp**
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эту команду можно использовать для быстрого отключения всех функций NTP и очистки всех конфигураций NTP

Отключение приема пакетов NTP на интерфейсе

Команда	**ntp disable**
Режим команд	Режим конфигурации интерфейса

Отключение службы синхронизации времени, предоставляемой NTP

Команда	**ntp service disable**
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Эта команда отключает службу синхронизации времени NTP. После настройки этой команды внешние устройства не могут синхронизировать время с устройства NTP (эта команда поддерживается только в некоторых версиях)

3.4.1.6. Пример конфигурации

Режим внешних эталонных часов NTP

Сценарий:

Рисунок 3-5.

	DEVICE-B настроен на режим внешней опорной частоты NTP. DEVICE-A используется в качестве источника эталонных часов для DEVICE-B. DEVICE-C синхронизирует время с DEVICE-B
Шаги настройки	DEVICE-A настраивает локальные часы в качестве источника эталонных часов NTP. DEVICE-B настраивает DEVICE-A в качестве источника эталонных часов. DEVICE-C настраивает DEVICE-B в качестве источника эталонных часов

DEVICE-A	A#configure terminal A(config)# ntp master A(config)#exit
DEVICE-B	B#configure terminal B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Проверка	Запустите команду **show ntp status** на DEVICE-B, чтобы отобразить конфигурацию NTP. DEVICE-B отправляет пакет синхронизации времени на 192.168.1.1, чтобы синхронизировать время с DEVICE-A. После успешной синхронизации времени с DEVICE-A DEVICE-B может ответить на запрос синхронизации времени от DEVICE-C. Запустите команду **show clock** на DEVICE-B и DEVICE-C, чтобы проверить, успешно ли выполнена синхронизация времени

Локальный режим эталонных часов NTP

Сценарий:

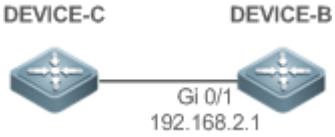


Рисунок 3-6.

	DEVICE-B настраивает локальные часы в качестве источника эталонных часов NTP. DEVICE-C синхронизирует время с DEVICE-B
Шаги настройки	DEVICE-B настраивает локальные часы в качестве источника эталонных часов NTP. DEVICE-C настраивает DEVICE-B в качестве источника эталонных часов
DEVICE-B	B#configure terminal B(config)# ntp master B(config)# exit

DEVICE-C	C#configure terminal C(config)# ntp server 192.168.2.1 C(config)# exit
Проверка	Запустите команду **show clock** на DEVICE-C, чтобы проверить, успешно ли выполнена синхронизация времени

3.4.2. Настройка аутентификации безопасности NTP

3.4.2.1. Эффект конфигурации

Синхронизация времени из надежного источника эталонных часов

Используйте устройство в качестве клиента для синхронизации времени только из доверенного внешнего эталонного источника часов с локальными часами.

Обеспечение синхронизации времени для доверенного устройства

Используйте локальные часы устройства в качестве источника эталонных часов NTP, чтобы обеспечить синхронизацию времени только для доверенного устройства.

3.4.2.2. Примечания

Ключи аутентификации клиента и сервера должны быть одинаковыми.

3.4.2.3. Шаги настройки

Настройка механизма глобальной Security аутентификации для NTP

- Обязательный.
- По умолчанию устройство отключает механизм Security аутентификации.

Настройка глобального ключа аутентификации для NTP

- Обязательный.
- По умолчанию для устройства не настроен ключ аутентификации.

Настройка глобально доверенного ключа для NTP

- Опционально.
- Чтобы обеспечить синхронизацию времени для доверенного устройства, необходимо указать доверенный ключ проверки подлинности с помощью идентификатора ключа.
- Можно настроить только один доверенный ключ. Указанный ключ аутентификации должен соответствовать ключу доверенного устройства.

Настройка идентификатора ключа аутентификации для внешнего источника эталонных часов

- Опционально.
- Чтобы синхронизировать время с доверенным источником эталонных часов, необходимо указать доверенный ключ проверки подлинности с помощью идентификатора ключа.
- Каждый доверенный источник эталонных часов сопоставляется с ключом аутентификации. Ключи аутентификации должны быть согласованы с ключами доверенных источников эталонных часов.

3.4.2.4. Проверка

- Запустите команду **show run**, чтобы проверить конфигурацию NTP.
- Запустите команду **show clock**, чтобы проверить, синхронизируется ли время только с доверенным устройством.

3.4.2.5. Связанные команды

Включение механизма аутентификации Security

Команда	**ntp authenticate**
Режим команд	Режим глобальной конфигурации
Руководство по использованию	По умолчанию клиент не использует механизм проверки подлинности глобальной Security. Если механизм аутентификации Security не используется, связь не будет зашифрована. Глобального индикатора Security недостаточно, чтобы предположить, что связь между клиентом и сервером реализована в зашифрованном виде. Другие глобальные ключи и ключ шифрования для сервера также должны быть настроены для инициирования зашифрованной связи между клиентом и сервером

Настройка ключа глобальной аутентификации

Команда	**ntp authentication-key** *key-id* **md5** *key-string* **[***enc-type***]**
Описание параметров	*key-id*: указывает идентификатор глобального ключа аутентификации в диапазоне от 1 до 4 294 967 295. *key-string*: указывает строку ключа. *enc-type*: (Опционально) указывает, зашифрован ли введенный ключ. 0 указывает на отсутствие шифрования, а 7 указывает на простое шифрование. Настройкой по умолчанию является отсутствие шифрования
Режим команд	Режим глобальной конфигурации

Настройка доверенного ключа для NTP

Команда	**ntp trusted-key** *key-id*
Описание параметров	*key-id*: указывает идентификатор доверенного ключа в диапазоне от 1 до 4 294 967 295
Режим команд	Режим глобальной конфигурации

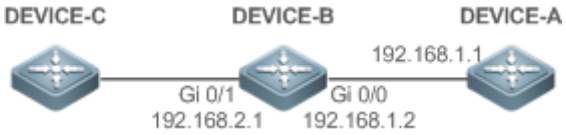
Настройка доверенного ключа для внешнего источника эталонных часов

См. раздел «Связанные команды».

3.4.2.6. Пример конфигурации

Аутентификация Security

Сценарий:



	• DEVICE-B настроен на работу в режиме клиент/сервер NTP и предоставляет службы NTP, требующие проверки подлинности Security для DEVICE-C. Ключ аутентификации — «abcd». • DEVICE-A используется в качестве источника эталонных часов для DEVICE-B. • DEVICE-C синхронизирует время с DEVICE-B
Шаги настройки	• DEVICE-B настраивает DEVICE-A в качестве источника эталонных часов. • DEVICE-C настраивает DEVICE-B в качестве источника эталонных часов
DEVICE-B	B#configure terminal B(config)# ntp authentication-key 1 md5 abcd B(config)# ntp trusted-key 1 B(config)# ntp server 192.168.1.1 B(config)# exit
DEVICE-C	C#configure terminal C(config)# ntp authentication-key 1 md5 abcd C(config)# ntp server 192.168.2.1 key 1 C(config)# exit
Проверка	• DEVICE-B отправляет пакет синхронизации времени, содержащий информацию об аутентификации, на адрес 192.168.1.1, чтобы синхронизировать время с DEVICE-A. • Запустите команду **show clock** на DEVICE-B, чтобы проверить, успешно ли выполнена синхронизация времени

3.4.3. Настройка контроля доступа NTP

3.4.3.1. Эффект конфигурации

Контроль доступа к службам NTP обеспечивает минимальную меру безопасности (security). Более безопасным методом является использование механизма аутентификации NTP.

3.4.3.2. Примечания

- В настоящее время система не поддерживает контрольный запрос (используется для управления NTP-серверами с помощью устройств управления сетью, таких как установка индикатора секунды координации или мониторинг его рабочего состояния). Хотя сопоставление правил реализовано в предыдущей последовательности, никакие запросы, связанные с управляющими запросами, не поддерживаются.
- Если правило управления доступом не настроено, все виды доступа разрешены. Если настроено какое-либо правило управления доступом, могут быть реализованы только доступы, разрешенные этим правилом.

3.4.3.3. Связанная конфигурация

Настройка прав доступа для NTP

- Опционально.
- Запустите команду **ntp access-group**, чтобы настроить права управления доступом и соответствующий ACL для NTP.

3.4.3.4. Проверка

Запустите команду **show run**, чтобы проверить конфигурацию NTP.

3.4.3.5. Связанные команды

Настройка прав управления доступом для служб NTP

Команда	**ntp access-group { peer | serve |serve-only | query-only }***access-list-number* **|** *access-list-name*
Описание параметров	**peer**: позволяет запрашивать время и управлять запросом для локальных служб NTP, а также позволяет локальному устройству синхронизировать время с удаленной системой (полные права доступа). **serve**: разрешает запрос времени и контрольный запрос для локальных служб NTP, но не позволяет локальному устройству синхронизировать время с удаленной системой. **serve-only**: разрешает только запрос времени для локальных служб NTP. **query-only**: разрешает только контрольный запрос для локальных служб NTP. *access-list-number*: указывает номер IP ACL в диапазоне от 1 до 99 и от 1300 до 1999. Подробнее о том, как создать IP ACL, см. в разделе ACL&QoS Configuration/Настройка ACL. *access-list-name*: указывает имя IP ACL. Подробнее о том, как создать IP ACL, см. в разделе ACL&QoS Configuration/Настройка ACL
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Настройте права управления доступом NTP. Когда поступает запрос на доступ, служба NTP сопоставляет правила в последовательности от минимального ограничения доступа до максимального ограничения доступа и использует первое совпадающее правило. Соответствующая последовательность может быть peer, serve, serve-only, and query-only (peer, обслуживающий, только для обслуживания и только для запросов)

3.4.3.6. Пример конфигурации

Настройка прав управления доступом NTP

Шаги настройки	Разрешить только устройству с IP-адресом 192.168.1.1 отправлять запрос синхронизации времени на локальное устройство
	QTECH(config)# access-list 1 permit 192.168.1.1 QTECH(config)# ntp access-group serve-only

3.5. Мониторинг

3.5.1. Отображение

Описание	Команда
show ntp status	Отображает текущую информацию NTP

3.5.2. Отладка

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

Описание	Команда
debug ntp	Включает отладку
no debug ntp	Отключает отладку

4. НАСТРОЙКА SNTP

4.1. Обзор

Простой протокол сетевого времени (SNTP) — это упрощенная версия протокола сетевого времени (NTP), который используется для синхронизации часов компьютеров в Интернете. SNTP применяется в сценариях, где нет необходимости использовать все функции NTP.

NTP использует сложный алгоритм и предъявляет более высокие требования к системе, тогда как SNTP использует более простой алгоритм и обеспечивает более высокую производительность. Как правило, точность SNTP может достигать 1 секунды, что соответствует основным требованиям большинства сценариев. Поскольку пакеты SNTP аналогичны пакетам NTP, клиент SNTP, реализованный на устройстве, полностью совместим с сервером NTP.

Протоколы и стандарты

RFC 2030: простой протокол сетевого времени (SNTP) версии 4 для IPv4, IPv6 и OSI.

4.2. Приложения

Приложение	Описание
Синхронизация времени с сервером NTP	Устройство используется как клиент для синхронизации времени с сервером NTP

4.2.1. Синхронизация времени с сервером NTP

4.2.1.1. Сценарий

Как показано на Рисунке 4-1, DEVICE-B использует локальные часы в качестве источника эталонных часов NTP и обеспечивает синхронизацию времени для DEVICE-C.

DEVICE-C используется как клиент SNTP для синхронизации времени с DEVICE-B.

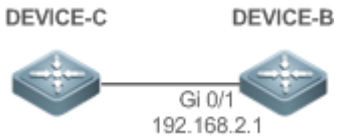


Рисунок 4-1.

4.2.1.2. Развертывание

- Укажите DEVICE-B в качестве сервера SNTP для DEVICE-C.
- Включите SNTP для DEVICE-C.

4.3. Функции

4.3.1. Базовые концепты

SNTP-пакет

SNTPV4 разработан на основе NTP и призван упростить функции NTP. Это не изменяет спецификации NTP и исходную реализацию NTP. Формат сообщения SNTPV4 такой же,

как у NTP, определенный в RFC1305, только некоторые поля данных инициализируются в предустановленные значения.

Как определено в RFC1305, SNTP использует для передачи пакеты протокола пользовательских датаграмм (UDP), а идентификатор используемого порта UDP — 123.

Рисунок 4-2 показывает формат пакета синхронизации времени SNTP.

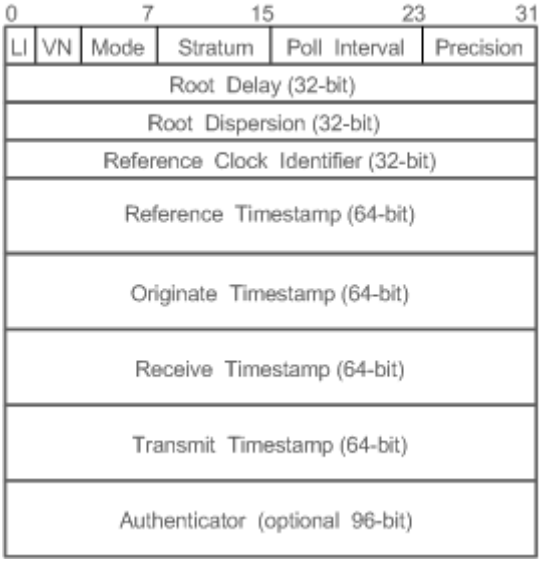


Рисунок 4-2. Формат пакета синхронизации времени SNTP

- Индикатор секунды координации (LI): указывает 2-битный индикатор дополнительной секунды.

ПРИМЕЧАНИЕ: 00: указывает на отсутствие предупреждающей информации; 01: указывает, что в предыдущей минуте 61 секунда; 10: указывает, что в предыдущей минуте 59 секунд; 11: указывает, что часы не синхронизированы.

- Номер версии (VN): указывает 3-битный номер версии NTP/SNTP. Текущий номер версии — 3.
- Режим (Mode): указывает 3-битный рабочий режим SNTP/NTP.

ПРИМЕЧАНИЕ: 0: указывает на отсутствие определения; 1: указывает на симметричную активность; 2: указывает на симметричный пассив; 3: указывает на клиента; 4: указывает на сервер; 5: указывает на широковещание; 6: указывает управляющую информацию; 7: зарезервировано.

- Stratum: указывает 8-битный Stratum (слой) локальных часов. 0: указывает на отсутствие определения; 1: указывает master-источник эталонных часов; другие значения: указывают slave-источники эталонных часов.
- Poll Interval (Интервал опроса): указывает интервал опроса (в секундах), который представляет собой 8-битное целое число.
- Precision (Точность): указывает точность времени (в секундах) местных часов, которая представляет собой 8-битное целое число.
- Root Delay (Корневая задержка): указывает время прохождения туда и обратно до источника эталонных часов, которое представляет собой 32-разрядное целое число.
- Root Dispersion (Корневая дисперсия): указывает самую большую разницу от master-источника эталонных часов, который представляет собой 32-разрядное целое число.

- Reference Clock Identifier (Идентификатор эталонных часов): указывает 32-битный идентификатор источника эталонных часов.
- Reference Timestamp (Эталонная временная метка): указывает 64-битную временную метку, а именно время, которое было установлено или исправлено в последний раз.
- Originate Timestamp (Исходная временная метка): указывает 64-битную метку времени, а именно местное время, когда от клиента уходит запрос на синхронизацию времени.
- Receive Timestamp (Отметка времени получения): указывает 64-битную отметку времени, а именно местное время, когда пакет запроса синхронизации времени поступает на сервер.
- Transmit Timestamp (Отметка времени передачи): указывает 64-битную отметку времени, а именно местное время, когда ответный пакет синхронизации времени отправляется с сервера.
- Authenticator (Опционально): указывает информацию для аутентификации.

4.3.2. Обзор

Особенность	Описание
Синхронизация времени SNTP	Синхронизирует время с сервера SNTP/NTP на локальное устройство

4.3.3. Синхронизация времени SNTP

4.3.3.1. Принцип работы

Синхронизация времени SNTP реализуется путем взаимодействия пакетов SNTP/NTP между клиентом и сервером. Клиент отправляет пакет синхронизации времени на сервер через определенные промежутки времени (по умолчанию полчаса). После получения ответного пакета от сервера клиент синхронизирует время.

Рисунок 4-3 показывает формат пакета синхронизации времени SNTP.

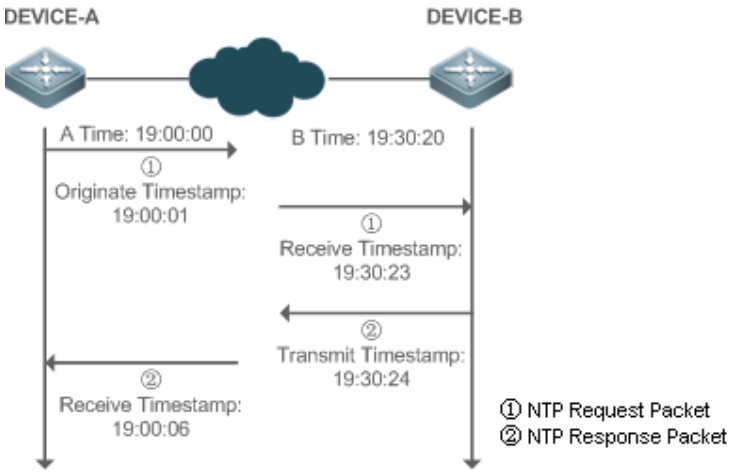


Рисунок 4-3. Принцип работы SNTP

DEVICE-B (сокращенно B) используется в качестве источника эталонных часов NTP, DEVICE-A (сокращенно A) используется в качестве клиента SNTP, который

синхронизирует время с DEVICE-B. В момент времени местные часы A показывают 19:00:00, а местные часы B — 19:30:20.

1. A отправляет пакет запроса SNTP/NTP. Местное время (T0), когда пакет отправляется из A, составляет 19:00:00 и заполняется в Originate Timestamp.
2. После 2-секундной сетевой задержки местное время (T1), когда B получает пакет запроса, составляет 19:30:23 и заполняется в Receive Timestamp.
3. B обрабатывает запрос NTP и через секунду отправляет ответный пакет NTP. Местное время (T2), когда ответный пакет уходит из B, составляет 19:30:24 и заполняется в Transmit Timestamp.
4. После 2-секундной сетевой задержки A получает ответный пакет. Местное время (T3), когда ответный пакет прибывает в A, составляет 19:00:06.

Конкретные расчеты для синхронизации времени следующие:

- A получает разницу во времени в 30 минут и 20 секунд между B и A, используя формулу ((T1-T0)+(T2-T3))/2.
- A получает четырехсекундную задержку пакета туда и обратно между A и B, используя формулу (T3-T0)-(T2-T1).

4.3.3.2. Связанная конфигурация

Включение SNTP

- SNTP по умолчанию отключен.
- Запустите команду **sntp enable**, чтобы включить SNTP.

Настройка SNTP-сервера

- По умолчанию сервер SNTP не настроен.
- Запустите команду **sntp server**, чтобы указать сервер SNTP.

Настройка интервала синхронизации времени SNTP

- По умолчанию интервал синхронизации времени SNTP составляет 1800 секунд.
- Запустите команду **sntp interval**, чтобы указать интервал синхронизации времени.

4.4. Конфигурация

Конфигурация	Описание и команда	
Настройка SNTP	(Обязательно) Используется для включения SNTP	
	sntp enable	Включает SNTP
	sntp server	Настраивает IP-адрес сервера SNTP
	(Опционально) Используется для настройки интервала синхронизации времени SNTP	
	sntp interval	Настраивает интервал синхронизации времени SNTP

4.4.1. Настройка SNTP

4.4.1.1. Эффект конфигурации

Клиент SNTP обращается к серверу NTP через фиксированные промежутки времени, чтобы регулярно корректировать часы.

4.4.1.2. Примечания

Все время, полученное через связь SNTP, является средним временем по Гринвичу (GMT). Чтобы получить точное местное время, вам необходимо установить местный часовой пояс для согласования с GMT.

4.4.1.3. Шаги настройки

Включение SNTP

(Обязательно) SNTP по умолчанию отключен.

Настройка IP-адреса SNTP-сервера

(Обязательно) По умолчанию сервер SNTP/NTP не настроен.

Настройка интервала синхронизации времени SNTP

- Опционально.
- По умолчанию устройство синхронизирует время каждые полчаса.

Проверка

Запустите команду **show sntp**, чтобы отобразить параметры, связанные с SNTP.

4.4.1.4. Связанные команды

Включение SNTP

Команда	**sntp enable**
Режим команд	Режим глобальной конфигурации
Руководство по использованию	SNTP по умолчанию отключен. Запустите команду глобальной конфигурации **no sntp enable**, чтобы отключить SNTP

Настройка IP-адреса сервера SNTP/NTP

Команда	**sntp server** [**oob**] *ip-address* [**via** *mgmt-name*]
Описание параметров	*ip-address*: указывает IP-адрес сервера NTP/SNTP. По умолчанию сервер NTP/SNTP не настроен. **oob**: указывает, что сервер NTP/SNTP поддерживает внешний интерфейс управления (интерфейс mgmt). *mgmt-name*: задает исходящий интерфейс управления для пакетов в режиме oob
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Поскольку SNTP полностью совместим с NTP, сервер можно настроить как общедоступный сервер NTP в Интернете. Поскольку пакеты SNTP аналогичны пакетам NTP, клиент SNTP полностью совместим с сервером NTP. В Интернете существует множество NTP-серверов. Вы можете выбрать NTP-сервер с более короткой задержкой в качестве SNTP-сервера на вашем устройстве

Настройка интервала синхронизации времени SNTP

Команда	**sntp interval** *seconds*
Описание параметров	*second*: указывает интервал синхронизации времени в диапазоне от 60 до 65 535 секунд. Значение по умолчанию — 1800 секунд
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Запустите эту команду, чтобы установить интервал для клиента SNTP для синхронизации времени с сервером NTP/SNTP. **ПРИМЕЧАНИЕ:** настроенный здесь интервал вступает в силу не сразу. Чтобы он вступил в силу немедленно, запустите команду **sntp enable**

4.4.1.5. Пример конфигурации

Синхронизация времени SNTP

Сценарий:

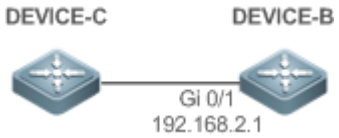


Рисунок 4-4.

	DEVICE-B указывает на сервер NTP в Интернете. DEVICE-C синхронизирует время с DEVICE-B
Шаги настройки	Включите SNTP для DEVICE-C и настройте DEVICE-B как NTP-сервер
DEVICE-C	C#configure terminal C(config)# sntp server 192.168.2.1 C(config)# sntp enable C(config)# exit

Проверка	• Запустите команду **show clock** на DEVICE-C, чтобы проверить, успешно ли выполнена синхронизация времени. • Запустите команду **show sntp** на DEVICE-C, чтобы отобразить статус SNTP и проверить, успешно ли настроен сервер

4.5. Мониторинг

4.5.1. Отображение

Описание	Команда
show sntp	Отображает параметры, связанные с SNTP

4.5.2. Отладка

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

Описание	Команда
debug sntp	Включает отладку

5. НАСТРОЙКА SPAN-RSPAN

5.1. Обзор

Анализатор коммутируемых портов (SPAN) предназначен для копирования пакетов указанного порта на другой порт коммутатора, который подключен к устройству мониторинга сети, чтобы обеспечить мониторинг сети и устранение неполадок.

Все входящие и исходящие пакеты исходного порта можно отслеживать через SPAN. Например, как показано на следующем рисунке, все пакеты на порту 5 сопоставляются с портом 10, а анализатор сети, подключенный к порту 10, получает все пакеты, проходящие через порт 5.

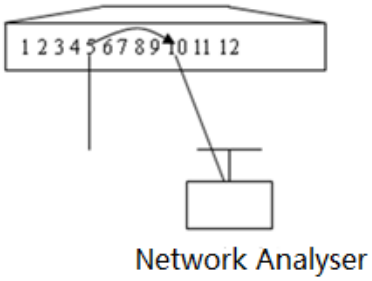


Рисунок 5-1. Экземпляр конфигурации SPAN

Функция SPAN в основном применяется в сценариях мониторинга сети и устранения неполадок, чтобы отслеживать информацию о сети и устранять сбои в сети.

Удаленный SPAN (RSPAN), расширение SPAN, позволяет удаленно контролировать несколько устройств. Каждый сеанс RSPAN устанавливается в указанной удаленной VLAN. RSPAN преодолевает ограничение, согласно которому mirrored-порт и mirroring-порт должны находиться на одном и том же устройстве, и позволяет mirrored-порту находиться на расстоянии нескольких сетевых устройств от mirroring-порта. Пользователи могут наблюдать за пакетами данных удаленного mirrored-порта с помощью анализатора в центральной серверной.

Сценарии применения RSPAN аналогичны сценариям SPAN. RSPAN позволяет пользователям проводить мониторинг данных в режиме реального времени, не находясь в серверной, что обеспечивает большое удобство для пользователей.

VLAN SPAN (VSPAN) рассматривает потоки данных некоторых VLAN как источники данных и зеркалирует их на порт назначения. Конфигурация аналогична конфигурации SPAN на основе портов. VSPAN имеет следующие особенности:

- VLAN, не являющаяся удаленной VLAN, может быть указана в качестве источника данных VSPAN.
- Некоторые VLAN, которые не являются удаленными VLAN, могут быть указаны в качестве источников данных VSPAN.
- Когда VLAN настроена как источник данных, пакеты могут отражаться только в направлении Rx.

5.2. Приложения

Приложение	Описание
SPAN на основе потока	Потоки данных с определенными характеристиками необходимо отслеживать, например, необходимо отслеживать потоки данных, использующие указанную политику списка управления доступом (ACL)
One-to-Many RSPAN	Несколько пользователей должны отслеживать данные одного и того же порта
Основные приложения RSPAN	Пакеты на исходном устройстве зеркалирования необходимо зеркалировать на целевое устройство для мониторинга

5.2.1. SPAN на основе потока

5.2.1.1. Сценарий

Как показано на следующем рисунке, сетевой анализатор можно настроить так, чтобы он мог отслеживать все потоки данных, пересылаемые коммутатором A на коммутатор B, и определенные потоки данных коммутатора B (например, потоки данных с PC1 и PC2).

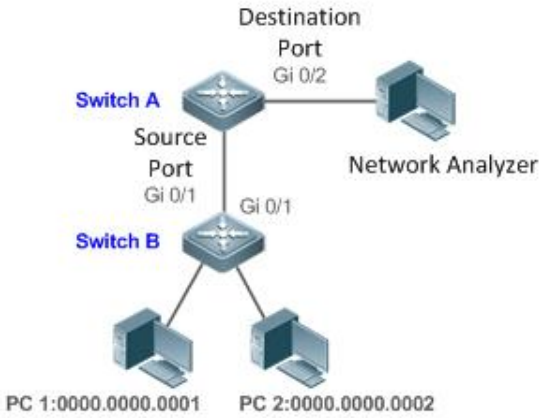


Рисунок 5-2. Топология простого приложения SPAN

0000.0000.0001 — это MAC-адрес PC1.

0000.0000.0002 — это MAC-адрес PC2.

5.2.1.2. Развертывание

- На предыдущем рисунке настройте функцию SPAN на коммутаторе A, подключенном к сетевому анализатору, установите порт Gi 0/1, подключенный к коммутатору B, в качестве исходного порта SPAN и установите порт Gi 0/2, который напрямую подключен к сетевому анализатору, в качестве порт назначения SPAN.

- Настройте SPAN на основе потоков (разрешены только потоки данных PC1 и PC2) для исходного порта Gi 0/1 SPAN.

5.2.2. One-to-Many RSPAN

5.2.2.1. Сценарий

Как показано на следующем рисунке, One-to-Many RSPAN может быть реализован на одном устройстве, то есть и ПК 1, и ПК 2 можно настроить для мониторинга передаваемого и принимаемого трафика порта, подключенного к серверу. Пользователи могут выполнить соответствующую настройку (например, удаленную VLAN и Loopback MAC-порта) для мониторинга потоков данных, проходящих через порт Gi 4/1 на ПК 1 и ПК 2, тем самым контролируя потоки данных сервера.

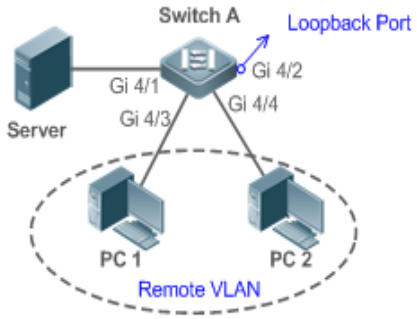


Рисунок 5-3. Топология приложений One-to-Many RSPAN

5.2.2.2. Развертывание

- Создайте удаленную VLAN на коммутаторе A.
- Настройте коммутатор A в качестве исходного устройства RSPAN и настройте порт Gi 4/1, который напрямую подключен к серверу, в качестве исходного порта RSPAN. Выберите порт, который находится в состоянии Down, в данном примере Gi 4/2, в качестве выходного порта RSPAN, добавьте этот порт в удаленную VLAN и настройте Loopback MAC (запустите команду **mac-loopback** в режиме настройки интерфейса).
- Добавьте порты, напрямую подключенные к ПК 1 и ПК 2, в удаленную сеть VLAN.

5.2.3. Основные приложения RSPAN

5.2.3.1. Сценарий

Как показано на следующем рисунке, функция RSPAN позволяет сетевому анализатору контролировать STA, подключенную к коммутатору исходного устройства A, от коммутатора устройства назначения C до коммутатора промежуточного устройства B. Обычно устройства могут обмениваться данными друг с другом.

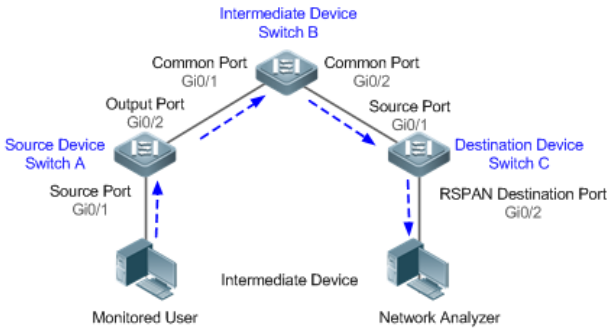


Рисунок 5-4. Базовая топология приложений RSPAN

5.2.3.2. Развертывание

- Настройте удаленную VLAN на коммутаторе A, коммутаторе B и коммутаторе C.
- На коммутаторе A настройте порт Gi 0/1, напрямую подключенный к STA, в качестве исходного порта, настройте порт Gi 0/2, подключенный к коммутатору B, в качестве выходного порта и настройте функцию переключения для выходного порта.
- На коммутаторе B настройте порт Gi 0/1, подключенный к коммутатору A, и порт Gi 0/2, подключенный к коммутатору C, как общие порты.
- На коммутаторе C настройте порт Gi0/1, подключенный к коммутатору B, в качестве общего исходного порта, настройте порт Gi0/2, подключенный к сетевому анализатору, в качестве порта назначения RSPAN и настройте функцию переключения для порта назначения RSPAN.

5.3. Функции

5.3.1. Базовые концепты

Сеанс SPAN

Сеанс SPAN — это потоки данных между исходным портом SPAN и портом назначения, которые можно использовать для мониторинга пакетов одного или нескольких портов на входе, выходе или в обоих направлениях. Коммутируемые порты, маршрутизируемые порты и агрегированные порты (AP) могут быть настроены как исходные порты или порты назначения для сеансов SPAN. После добавления портов коммутатора в сеанс SPAN нормальная работа коммутатора не изменяется.

Пользователи могут настроить сеанс SPAN на отключенном порту, но сеанс SPAN неактивен. Сеанс SPAN находится в активном состоянии только после включения порта, на котором настроен сеанс SPAN. Кроме того, сеанс SPAN не вступает в силу после включения коммутатора. Он активен только после того, как порт назначения находится в рабочем состоянии. Пользователи могут запустить команду **show monitor** [**session** *session-num*] для отображения рабочего состояния сеанса SPAN.

Потоки данных SPAN

Сеанс SPAN охватывает потоки данных в трех направлениях:

- Входные потоки данных: все пакеты, полученные исходным портом, копируются в порт назначения. Пользователи могут отслеживать входящие пакеты одного или нескольких исходных портов в сеансе SPAN. Некоторые входные пакеты исходного порта могут быть отброшены по некоторым причинам (например, в

целях безопасности порта). Это не влияет на функцию SPAN, и такие пакеты по-прежнему зеркалируются на порт назначения.

- Выходные потоки данных: все пакеты, переданные исходным портом, копируются в порт назначения. Пользователи могут отслеживать выходные пакеты одного или нескольких исходных портов в сеансе SPAN. Пакеты, передаваемые с других портов на порт-источник, по некоторым причинам могут быть отброшены, и такие пакеты не будут переданы на порт-получатель. Формат выходных пакетов исходного порта может быть изменен по некоторым причинам. Например, после маршрутизации у пакетов, передаваемых из исходного порта, изменяются MAC-адреса источника, MAC-адреса получателя, идентификаторы VLAN и TTL, а также их форматы после копирования в порт назначения.
- Двунаправленные потоки данных. Двунаправленные потоки данных включают потоки входных данных и потоки выходных данных. В сеансе SPAN пользователи могут отслеживать потоки данных одного или нескольких исходных портов во входном и выходном направлениях.

Исходный порт

Исходный порт называется контролируемым портом. В сеансе SPAN потоки данных исходного порта отслеживаются для сетевого анализа и устранения неполадок. В одном сеансе SPAN пользователи могут отслеживать входные, выходные и двунаправленные потоки данных, а количество исходных портов не ограничено.

Исходный порт имеет следующие особенности:

- Исходный порт может быть коммутируемым портом, маршрутизируемым портом или агрегируемым портом.
- Исходный порт не может одновременно использоваться в качестве порта назначения.
- Исходный порт и порт назначения могут принадлежать одной и той же VLAN или разным VLAN.

Порт назначения

Сеанс SPAN имеет один порт назначения (называемый портом мониторинга) для приема пакетов, скопированных с исходного порта.

Порт назначения имеет следующие характеристики:

- Порт назначения может быть коммутируемым портом, маршрутизируемым портом или агрегируемым портом.
- Порт назначения не может одновременно использоваться в качестве исходного порта.

5.3.2. Обзор

Особенность	Описание
SPAN	Настраивает зеркалирование портов на одном устройстве
RSPAN	Настраивает зеркалирование портов на разных устройствах

5.3.3. SPAN

SPAN используется для мониторинга потоков данных на коммутаторах. Он копирует кадры с одного порта на другой порт коммутатора, подключенный к сетевому анализатору или анализатору RMON, чтобы проанализировать связь порта.

5.3.3.1. Принцип работы

Когда порт передает или получает пакеты, SPAN после проверки того, что порт настроен как исходный порт SPAN, копирует пакеты, переданные и полученные портом, в порт назначения.

- Настройка исходного порта SPAN

Пользователям необходимо указать идентификатор сеанса SPAN и идентификатор исходного порта, чтобы настроить исходный порт SPAN, а также установить опциональный элемент направления SPAN, чтобы определить направление потоков данных SPAN, или указать политику ACL для зеркалирования определенных потоков данных.

- Настройка порта назначения SPAN

Пользователям необходимо указать идентификатор сеанса SPAN и идентификатор порта назначения, чтобы настроить порт назначения SPAN, а также установить опциональный элемент функции переключения, чтобы определить, следует ли включать функцию переключения и функцию удаления тегов на порте назначения SPAN.

5.3.3.2. Связанная конфигурация

Функция SPAN отключена по умолчанию. Он включается только после создания сеанса и настройки исходного и целевого портов SPAN. Сеанс SPAN может быть создан, когда настроен исходный порт SPAN или порт назначения.

Настройка исходного порта SPAN

Сеанс SPAN по умолчанию не имеет исходного порта SPAN. Пользователи могут запустить следующую команду для настройки исходного порта SPAN:

monitor session *session-num* **source interface** *interface-id* **[both | rx | tx] [acl** *name* **]**

В предыдущей команде:

session-num: указывает идентификатор сеанса SPAN. Количество поддерживаемых сеансов SPAN зависит от продукта.

interface-id: указывает исходный порт SPAN, который необходимо настроить.

rx: указывает, что после настройки **rx** отслеживаются только пакеты, полученные исходным портом.

tx: указывает, что после настройки **tx** отслеживаются только пакеты, передаваемые исходным портом.

both: указывает, что пакеты, переданные и полученные исходным портом, копируются в порт назначения для мониторинга после того, как **both** настроен, то есть **both** включает **rx** и **tx**. Если ни один из параметров **rx**, **tx** или **both** не выбраны, **both** включен по умолчанию.

acl: определяет политику ACL. После настройки этого параметра пакеты, разрешенные политикой ACL на исходном порту, отслеживаются. Эта функция отключена по умолчанию.

Настройка порта назначения SPAN

Сеанс SPAN по умолчанию не имеет порта назначения SPAN. Пользователи могут запустить следующую команду для настройки порта назначения SPAN:

monitor session *session-num* **destination interface** *interface-id* [**switch**]

В предыдущей команде:

switch: указывает, что порт назначения SPAN получает только пакеты, зеркалированные от исходного порта SPAN, и отбрасывает другие пакеты, если эта опция отключена, и получает как пакеты, зеркалированные от исходного порта SPAN, так и пакеты от неисходных портов, если эта опция включена, то есть связь между этим портом назначения и другими устройствами не затрагивается.

Когда порт назначения SPAN настроен, соответствующая функция отключена по умолчанию, если коммутатор не настроен.

Настройка SPAN на основе потока

Эта функция отключена по умолчанию. Пользователи могут выполнить команду **monitor session** *session-num* **source interface** *interface-id* **rxacl** *acl-name* для настройки SPAN на основе потока.

Обратите внимание на следующие моменты при использовании SPAN:

ПРИМЕЧАНИЯ:

- Порт назначения SPAN используется для расчета протокола связующего дерева (STP).
- SPAN недоступен, если исходный порт или порт назначения отключены.
- Если VLAN (или список VLAN) используется в качестве источника SPAN, убедитесь, что порт назначения имеет достаточную пропускную способность для получения зеркалированных данных VLAN (или списка VLAN).
- Не все продукты поддерживают все параметры предыдущих команд из-за различий между продуктами.

5.3.4. RSPAN

RSPAN может контролировать несколько устройств. Каждый сеанс RSPAN устанавливается в указанной удаленной VLAN. RSPAN преодолевает ограничение, согласно которому mirrored-порт и mirroring-порт должны находиться на одном и том же устройстве, и позволяет mirrored-порту находиться на расстоянии нескольких сетевых устройств от mirroring-порта.

5.3.4.1. Принцип работы

Удаленная VLAN создается для исходного устройства, промежуточного устройства и целевого устройства, все порты, участвующие в сеансе RSPAN, должны быть добавлены в удаленную VLAN. Mirrored-пакеты широковещательно передаются в удаленной VLAN таким образом, что они передаются из исходного порта исходного коммутатора в порт назначения целевого коммутатора.

- Настройка удаленной VLAN

Пакеты из исходного порта RSPAN широковещательно передаются в удаленную VLAN, чтобы быть скопированными с локального коммутатора на удаленный коммутатор. Порт источника RSPAN, порт вывода, reflection-порт отражения, порты прозрачной передачи промежуточного устройства (порт ввода пакетов и порт вывода промежуточного устройства), порт назначения и порт ввода порта назначения должны быть добавлены в удаленную VLAN. Функция RSPAN требует настройки VLAN как удаленной VLAN в режиме VLAN.

- Настройка сеанса RSPAN

Конфигурация порта источника и порта назначения RSPAN аналогична настройке порта источника и порта назначения SPAN, но идентификатор mirroring-сеанса, указанный во время настройки, должен быть идентификатором сеанса RSPAN.

- Настройка исходного порта RSPAN

Конфигурация исходного порта RSPAN такая же, как у исходного порта SPAN, но указанный идентификатор mirroring-сеанса должен быть идентификатором сеанса RSPAN.

- Настройка выходного порта RSPAN

Выходной порт расположен на исходном устройстве и должен быть добавлен в удаленную сеть VLAN. Mirrored-пакеты исходного порта транслируются в эту удаленную VLAN. Исходное устройство передает пакеты промежуточному коммутатору или коммутатору назначения через выходной порт.

- Настройка порта назначения RSPAN

При настройке порта назначения RSPAN необходимо указать идентификатор сеанса RSPAN, удаленную VLAN и имя порта, чтобы пакеты из исходного порта копировались в порт назначения через удаленную VLAN.

- Настройка RSPAN на основе потока

RSPAN является расширением SPAN и также поддерживает зеркалирование на основе потоков. Конфигурация такая же, как у потокового SPAN. RSPAN на основе потока не влияет на нормальную связь.

Пользователи могут настроить ACL в направлении ввода исходного порта на исходном устройстве RSPAN. Поддерживаются стандартные ACL, расширенные ACL, MAC ACL и определяемые пользователем ACL.

Пользователи могут настроить ACL порта в направлении ввода исходного порта на исходном устройстве RSPAN и настроить ACL порта в направлении вывода порта назначения на целевом устройстве RSPAN. Пользователи также могут настроить ACL для исходящего направления удаленной VLAN на исходном коммутаторе RSPAN и настроить ACL для входного направления удаленной VLAN на целевом коммутаторе RSPAN.

- Настройка RSPAN One-to-Many

Если потоки данных одного исходного порта необходимо зеркалировать на несколько портов назначения, пользователи могут настроить сеанс RSPAN, настроить исходный порт сеанса RSPAN как исходный mirroring-порт One-to-Many и выбрать другой порт Ethernet в качестве порта пересылки. (выходной порт на устройстве-источнике). Кроме того, функция обратной связи MAC должна быть настроена на порте пересылки RSPAN в режиме конфигурации интерфейса, ожидаемый выходной порт RSPAN и порт пересылки RSPAN должны быть добавлены в удаленную VLAN. Затем mirrored-пакеты зацикливаются (looped back) на порте пересылки RSPAN, а затем широковещательно передаются в удаленную VLAN, тем самым реализуя RSPAN One-to-Many.

5.3.4.2. Связанная конфигурация

Функция RSPAN отключена по умолчанию. Он включается только после создания сеанса RSPAN и настройки удаленной VLAN, исходного порта RSPAN и порта назначения RSPAN.

Настройка удаленной VLAN

По умолчанию для RSPAN не указана удаленная VLAN. Пользователи могут запустить команду **remote-span** в режиме VLAN, чтобы настроить VLAN как удаленную VLAN. Одна удаленная VLAN соответствует одному сеансу RSPAN.

Настройка исходного устройства RSPAN

Эта функция отключена по умолчанию. Пользователи могут запустить команду **monitor session** *session-num* **remote-source** в режиме глобальной конфигурации, чтобы настроить устройство в качестве удаленного исходного устройства указанного сеанса RSPAN.

Настройка целевого устройства RSPAN

Эта функция отключена по умолчанию. Пользователи могут запустить команду **monitor session** *session-num* **remote-destination** в режиме глобальной конфигурации, чтобы настроить устройство в качестве удаленного целевого устройства указанного сеанса RSPAN.

Настройка исходного порта RSPAN

Исходный порт сеанса RSPAN настраивается на исходном устройстве. Конфигурация такая же, как у исходного порта SPAN, но необходимо указать идентификатор сеанса RSPAN. Эта функция отключена по умолчанию.

Настройка выходного порта на исходном устройстве RSPAN

Эта функция отключена по умолчанию. Пользователи могут запустить команду **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* [**switch**] в режиме глобальной конфигурации, чтобы настроить выходной порт на исходном устройстве RSPAN. Если опция **switch** сконфигурирована, выходной порт может участвовать в обычной коммутации пакетов данных. По умолчанию он не настроен. Выходной порт должен быть добавлен в удаленную VLAN.

Настройка целевого порта на целевом устройстве RSPAN

Эта функция отключена по умолчанию. Пользователи могут запустить команду **monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface-name* [**switch**] в режиме глобальной конфигурации, чтобы настроить порт назначения на целевом устройстве RSPAN. Если опция **switch** настроена, порт назначения может участвовать в обычной коммутации пакетов данных. По умолчанию он не настроен. Порт назначения должен быть добавлен в удаленную сеть VLAN.

При использовании RSPAN обратите внимание на следующие моменты:

ПРИМЕЧАНИЯ:

- Удаленная VLAN должна быть настроена на каждом устройстве, их идентификаторы VLAN должны быть согласованы, и все порты, участвующие в сеансе, должны быть добавлены в VLAN.
- Не рекомендуется добавлять общие порты в удаленную VLAN.
- Не настраивайте порт, подключенный к промежуточному коммутатору или коммутатору назначения, в качестве исходного порта RSPAN. В противном случае трафик в сети может оказаться в хаосе.

5.4. Конфигурация

Конфигурация	Описание и команда	
Настройка базовых функций SPAN	(Обязательно) Используется для создания SPAN	
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Настраивает исходный порт SPAN

Конфигурация	Описание и команда	
Настройка базовых функций SPAN	**monitor session** *session-num* **destination interface** *interface-id*[**switch**]	Настраивает порт назначения SPAN
	monitor session *session-num* **source interface** *interface-id* **rxacl** *acl-name*	Настраивает SPAN на основе потока
	monitor session *session-num* **source vlan** *vlan-id* [**rx**]	Указывает VLAN в качестве источника данных SPAN
	monitor session *session-num* **source filter vlan** *vlan-id-list*	Указывает некоторые сети VLAN в качестве источников данных для SPAN
Настройка основных функций RSPAN	(Обязательно) Используется для создания RSPAN	
	monitor session *session-num* **remote-source**	Настраивает идентификатор сеанса RSPAN и указывает исходное устройство
	monitor session *session-num* **remote-destination**	Настраивает идентификатор сеанса RSPAN и указывает целевое устройство
	remote-span	Настраивает удаленную VLAN
	monitor session *session-num* **source interface** *interface-id* [**both | rx | tx**]	Настраивает исходный порт RSPAN
	monitor session *session-num* **destination remote vlan** *remote-vlan-id* **interface** *interface-id* [**switch**]	Настраивает выходной порт на исходном устройстве RSPAN или порт назначения на целевом устройстве RSPAN

5.4.1. Настройка базовых функций SPAN

5.4.1.1. Эффект конфигурации

- Настройте порты источника и назначения для сеанса SPAN.
- Настройте порт назначения для отслеживания любых пакетов, переданных и полученных исходным портом.

5.4.1.2. Примечания

Если функция коммутатора отключена на порте назначения SPAN, порт назначения получает только mirrored-пакеты и отбрасывает другие пакеты, проходящие через порт. После включения функции коммутатора порт назначения может принимать не mirrored-пакеты.

5.4.1.3. Шаги настройки

Настройка сеанса SPAN

- Режим глобальной конфигурации. Обязательный.
- Вы можете настроить сеанс SPAN при настройке исходного порта SPAN или порта назначения, или при настройке указанной VLAN или некоторых VLAN в качестве источника данных или источников данных SPAN.

Настройка исходного порта SPAN

- Режим глобальной конфигурации. Обязательный.
- Вы можете выбрать направление SPAN при настройке исходного порта SPAN. Оба направления настроены по умолчанию, то есть отслеживаются как передаваемые, так и принимаемые пакеты.

Настройка порта назначения SPAN

- Режим глобальной конфигурации. Обязательный.
- Сеанс SPAN активен, только если настроен исходный порт SPAN (или в качестве источника данных SPAN указана VLAN) и настроен порт назначения SPAN.

5.4.1.4. Проверка

Запустите команду **show monitor** или команду **show running**, чтобы проверить конфигурацию SPAN. В качестве альтернативы проведите анализ захвата пакетов на порту назначения SPAN и проверьте, действует ли функция SPAN в соответствии с захваченными пакетами.

5.4.1.5. Связанные команды

Настройка исходного порта SPAN

Команда	**monitor session** *session-num* **source interface** *interface-id* [**both** | **rx** |**tx**]
Описание параметров	*session-num*: указывает идентификатор сеанса SPAN. *interface-id*: указывает идентификатор интерфейса. **both**: указывает, что пакеты во входящем и исходящем направлениях отслеживаются. Это значение по умолчанию. **rx**: указывает, что пакеты во входящем направлении отслеживаются. **tx**: указывает, что пакеты в направлении вывода отслеживаются
Режим команд	Режим глобальной конфигурации

Настройка порта назначения SPAN

Команда	**monitor session** *session-num* **destination interface** *interface-id***[switch]**
Описание параметров	*session-num*: указывает идентификатор сеанса SPAN. *interface-id*: указывает идентификатор интерфейса. **switch**: указывает, что функция переключения включена на порте назначения SPAN. По умолчанию он отключен
Режим команд	Режим глобальной конфигурации

Настройка SPAN на основе потока

Команда	**monitor session** *session-num* **source interface** *interface-id* **rx acl** *acl-name*
Описание параметров	*session-num*: указывает идентификатор сеанса SPAN. *interface-id*: указывает идентификатор интерфейса. *acl-name*: указывает имя ACL
Режим команд	Режим глобальной конфигурации

Указание VLAN в качестве источника данных SPAN

Команда	**monitor session** *session-num* **source vlan** *vlan-id* **[rx]**
Описание параметров	*session-num*: указывает идентификатор сеанса SPAN. *vlan-id*: указывает указанный идентификатор VLAN. **rx**: указывает, что пакеты во входящем направлении отслеживаются
Режим команд	Режим глобальной конфигурации

Указание некоторых VLAN в качестве источников данных SPAN

Команда	**monitor session** *session-num* **source filter vlan** *vlan-id-list*
Описание параметров	*session-num*: указывает идентификатор сеанса SPAN. *vlan-id-list*: указывает некоторые указанные идентификаторы VLAN
Режим команд	Режим глобальной конфигурации

5.4.1.6. Пример конфигурации

Ниже в качестве примера используется SPAN

Сценарий:

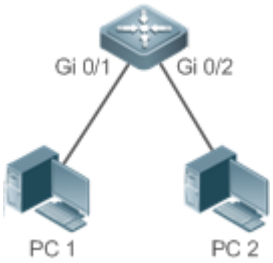


Рисунок 5-5.

Шаги настройки	• Как показано на Рисунке 5-5, добавьте порты Gi 0/1 и Gi 0/2 устройства A в сеть VLAN 1. • Создайте SVI 1 и установите адрес SVI 1 на 10.10.10.10/24. • Установите IP-адреса ПК 1 и ПК 2 на 10.10.10.1/24 и 10.10.10.2/24 соответственно. • Настройте SPAN для устройства A и настройте порты Gi 0/1 и Gi 0/2 в качестве исходного порта и порта назначения SPAN соответственно
A	QTECH# configure QTECH(config)# vlan 1 QTECH(config-vlan)# exit QTECH(config)# interface vlan 1 QTECH(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0 QTECH(config-if-VLAN 1)# exit QTECH(config)# monitor session 1 source interface gigabitEthernet 0/1 QTECH(config)# monitor session 1 destination interface gigabitEthernet 0/2
Проверка	Запустите команду **show monitor**, чтобы проверить, правильно ли настроен SPAN. После успешной настройки ПК 1 отправляет пакеты проверки связи на SVI 1, а ПК 2 осуществляет мониторинг с помощью инструмента захвата пакетов
A	QTECH# show monitor sess-num: 1 span-type: LOCAL_SPAN src-intf: GigabitEthernet 0/1 frame-type Both dest-intf: GigabitEthernet 0/2

5.4.1.7. Распространенные ошибки

- Идентификатор сеанса, указанный при настройке исходного порта SPAN, не соответствует идентификатору, указанному при настройке порта назначения SPAN.
- Потеря пакетов может произойти, если пакеты порта с большой пропускной способностью зеркалируются на порт с малой пропускной способностью.

5.4.2. Настройка основных функций RSPAN

5.4.2.1. Эффект конфигурации

- Настройте исходный порт и порт назначения на исходном устройстве сеанса RSPAN и настройте порт назначения на целевом устройстве.
- Настройте порт назначения на целевом устройстве RSPAN для отслеживания любых пакетов, которые передаются или принимаются исходным портом.

5.4.2.2. Примечания

- Если функция коммутатора отключена на порте назначения RSPAN, порт назначения получает только mirrored-пакеты и отбрасывает другие пакеты, проходящие через порт. После включения функции коммутатора порт назначения может принимать не mirrored-пакеты.
- Все порты, задействованные в RSPAN, должны быть добавлены в удаленную VLAN.
- Удаленная VLAN должна быть создана на промежуточном устройстве, и к удаленной VLAN должны быть добавлены прозрачные порты передачи.

5.4.2.3. Шаги настройки

Настройка сеанса RSPAN

- Режим глобальной конфигурации. Обязательный.
- Один и тот же идентификатор сеанса необходимо настроить на исходном устройстве RSPAN и целевом устройстве RSPAN.

Настройка исходного устройства RSPAN

- Режим глобальной конфигурации. Обязательный.
- Используется для указания устройства, которое будет контролироваться RSPAN.

Настройка целевого устройства RSPAN

- Режим глобальной конфигурации. Обязательный.
- Используется для указания целевого устройства для вывода пакетов RSPAN.

Настройка исходного порта RSPAN

- Режим глобальной конфигурации. Обязательный.
- Завершите настройку на исходном устройстве RSPAN. После настройки мониторинг RSPAN может проводиться для пакетов исходного порта RSPAN. Вы можете указать RSPAN для мониторинга пакетов удаленной VLAN во входном направлении, исходящем направлении или в обоих направлениях исходного порта RSPAN.

Настройка выходного порта RSPAN

- Режим глобальной конфигурации. Обязательный.

- Завершите настройку на исходном устройстве RSPAN. После настройки mirrored-пакеты, полученные портами, добавленными в удаленную VLAN, могут быть переданы на целевое устройство RSPAN через выходной порт.

Настройка порта назначения RSPAN

- Режим глобальной конфигурации. Обязательный.
- Завершите настройку целевого устройства RSPAN. После настройки целевое устройство RSPAN пересылает зеркальные пакеты, полученные портами, добавленными в удаленную VLAN, на устройство мониторинга через порт назначения.

5.4.2.4. Проверка

- Запустите команду **show monitor** или команду **show running**, чтобы проверить, успешно ли настроен RSPAN на каждом устройстве, или выполните захват пакетов на целевом mirroring-порту на целевом устройстве RSPAN, чтобы проверить, являются ли пакеты, зеркалированные с исходного порта исходного устройства RSPAN, захваченными.

5.4.2.5. Связанные команды

Настройка исходного устройства RSPAN

Команда	**monitor session** *session-num* **remote-source**
Описание параметров	*session-num*: указывает идентификатор сеанса RSPAN
Режим команд	Режим глобальной конфигурации

Настройка целевого устройства RSPAN

Команда	**monitor session** *session-num* **remote-destination**
Описание параметров	*session-num*: указывает идентификатор сеанса RSPAN
Режим команд	Режим глобальной конфигурации

Настройка удаленной VLAN

Команда	**remote-span**
Режим команд	Режим VLAN

Настройка исходного порта RSPAN

Команда	**monitor session** *session-num* **source interface** *interface-id* **[both | rx | tx][acl** *acl-name***]**
Описание параметров	*session-num*: указывает идентификатор сеанса RSPAN. *interface-id*: указывает идентификатор интерфейса. **both**: указывает, что пакеты во входящем и исходящем направлениях отслеживаются. Это значение по умолчанию. **rx**: указывает, что пакеты во входящем направлении отслеживаются. **tx**: указывает, что пакеты в направлении вывода отслеживаются. *acl-name*: указывает имя ACL
Режим команд	Режим глобальной конфигурации
Руководство по использованию	Конфигурация такая же, как у исходного порта SPAN, но необходимо указать идентификатор сеанса RSPAN

Настройка выходного порта на исходном устройстве RSPAN

Команда	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface id* **[switch]**
Описание параметров	*session-num*: указывает идентификатор сеанса RSPAN. *remote-vlan*: указывает на удаленную сеть VLAN. *interface id*: указывает идентификатор интерфейса. **switch**: указывает, участвует ли порт в коммутации пакетов
Режим команд	Режим глобальной конфигурации

Настройка целевого порта на целевом устройстве RSPAN

Команда	**monitor session** *session-num* **destination remote vlan** *remote-vlan* **interface** *interface id* **[switch]**
Описание параметров	*session-num*: указывает идентификатор сеанса RSPAN. *remote-vlan*: указывает на удаленную сеть VLAN. *interface id*: указывает идентификатор интерфейса. **switch**: указывает, участвует ли порт в коммутации пакетов
Режим команд	Режим глобальной конфигурации

5.4.2.6. Пример конфигурации

Настройка One-to-Many RSPAN

Сценарий:

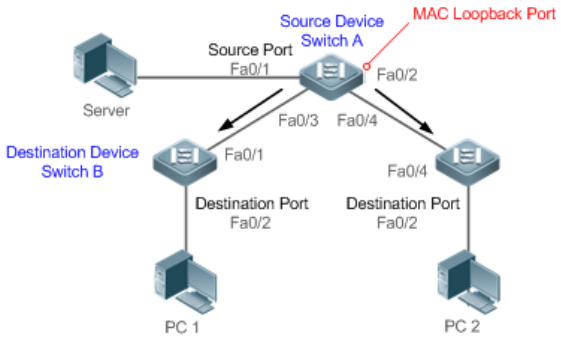


Рисунок 5-6.

Шаги настройки	• Как показано на предыдущем рисунке, настройте удаленную VLAN на коммутаторе A, коммутаторе B и коммутаторе C. • Настройте исходный порт, выходной порт и порт loopback на коммутаторе A. • Настройте порт назначения на коммутаторе B и коммутаторе C
A	QTECH# configure QTECH(config)# vlan 7 QTECH(config-vlan)# remote-span QTECH(config-vlan)# exit QTECH(config)# monitor session 1 remote-source QTECH(config)# monitor session 1 source interface fa 0/1 both QTECH(config)# monitor session 1 destination remote vlan 7 interface fa 0/2 switch QTECH(config)# interface fa0/2 QTECH(config-if)# mac-loopback QTECH(config-if)# switchport access vlan 7 QTECH(config-if)# exit QTECH(config)# interface range fa0/3-4 QTECH(config-if-range)# switchport mode trunck
B, C	QTECH(config)# vlan 7 QTECH(config-vlan)# remote-span QTECH(config-vlan)# exit

	QTECH(config)# monitor session 1 remote-destination QTECH(config)# monitor session 1 destination remote vlan 7 interface fa 0/2 QTECH(config)# interface fa0/1 QTECH(config-if)#switchport mode trunck
Проверка	Запустите команду **show monitor** или команду **show running** на коммутаторе A, коммутаторе B и коммутаторе C, чтобы проверить, успешно ли настроен RSPAN
A	QTECH# show monitor sess-num: 1 span-type: SOURCE_SPAN src-intf: FastEthernet 0/1 frame-type Both dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on
B	QTECH# show monitor sess-num: 1 span-type: DEST_SPAN dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on
C	QTECH# show monitor sess-num: 1 span-type: DEST_SPAN dest-intf: FastEthernet 0/2 Remote vlan 7 mtp_switch on

5.4.2.7. Распространенные ошибки

- Удаленная VLAN должна быть настроена на исходном устройстве, промежуточном устройстве и целевом устройстве, а их идентификаторы VLAN должны быть согласованы.

- Потеря пакетов может произойти, если пакеты порта с большой пропускной способностью зеркалируются на порт с малой пропускной способностью.
- Для реализации RSPAN One-to-Many необходимо настроить несколько выходных портов.

5.5. Мониторинг

5.5.1. Отображение

Описание	Команда
Отображает все mirroring-сеансы, существующие в системе	**show monitor**
Отображает указанный mirroring-сеанс	**show monitor session** *session-id*

5.5.2. Отладка

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

Описание	Команда
Диапазон отладки	**debug span**

6. НАСТРОЙКА ERSPAN

6.1. Обзор

Инкапсулированный анализатор удаленных коммутируемых портов (ERSPAN) является расширением анализатора удаленных коммутируемых портов (RSPAN). Пакеты данных SPAN обычных RSPAN могут передаваться только в пределах уровня 2 и не могут проходить через сети маршрутизации. Однако ERSPAN может передавать пакеты SPAN между сетями маршрутизации.

ERSPAN инкапсулирует все пакеты SPAN в пакеты IP через общий туннель инкапсуляции маршрутизации (GRE) и направляет их на порт назначения устройства RSPAN. На следующем рисунке показана топология типичного приложения:

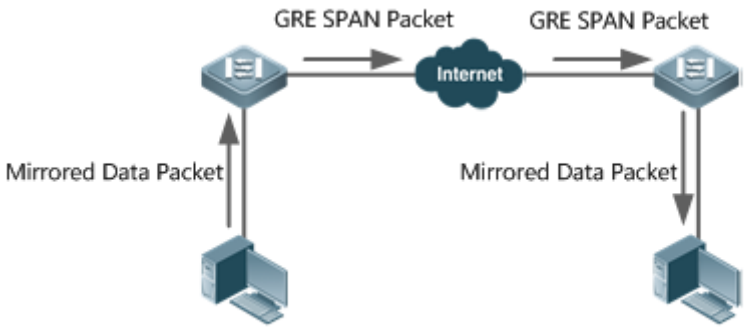


Рисунок 6-1. Топология типичного приложения туннеля ERSPAN GRE

Устройства на рисунке играют две роли:

- Коммутатор-источник. Коммутатор-источник относится к коммутатору, в котором находится исходный порт ERSPAN. Он копирует пакеты в исходный порт, выводит копии из выходного порта, инкапсулирует их в IP-пакеты и перенаправляет IP-пакеты на коммутатор назначения.
- Коммутатор назначения: Коммутатор назначения относится к коммутатору, в котором находится порт назначения ERSPAN. Он помещает полученные пакеты SPAN через порт назначения SPAN, декапсулирует их в пакеты GRE, а затем пересылает пакеты GRE на устройство мониторинга.

Для реализации ERSPAN IP-пакеты с GRE-инкапсуляцией должны иметь возможность нормально маршрутизироваться к целевому устройству SPAN.

6.2. Приложения

Приложение	Описание
Основные приложения ERSPAN	Пакеты на устройстве-источнике SPAN необходимо зеркалировать на целевом устройстве для мониторинга

6.3. Основные приложения ERSPAN

6.3.1. Сценарий

Как показано на следующем рисунке, ERSPAN позволяет сетевому анализатору отслеживать пользователей, подключенных к коммутатору A исходного устройства. Обычно устройства могут обмениваться данными друг с другом.

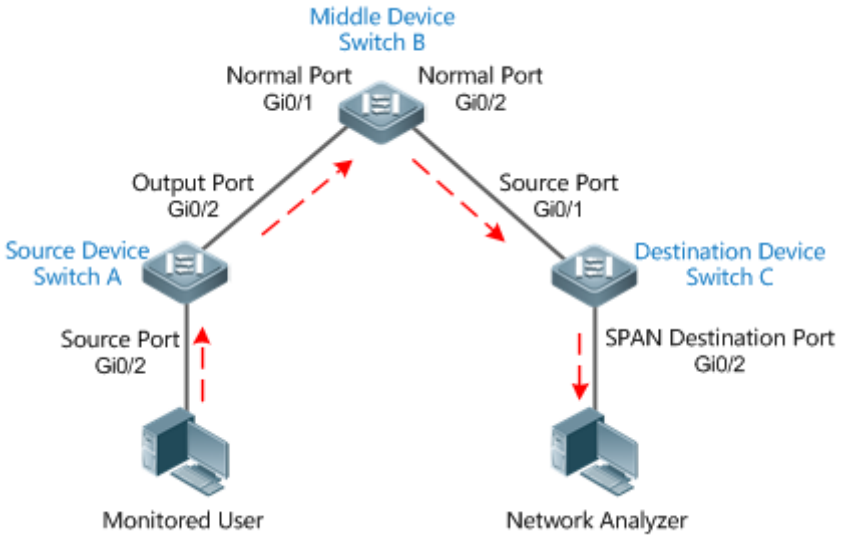


Рисунок 6-2. Топология основных приложений ERSPAN

6.3.2. Развертывание

- На коммутаторе A настройте порт, напрямую подключенный к пользователям (Gi 0/1), как исходный порт, а порт, подключенный к коммутатору B (Gi 0/2), настройте как выходной порт.
- На коммутаторе B порты, подключенные к коммутатору A и коммутатору C (Gi 0/1 и Gi 0/2), являются, соответственно, интерфейсами-участниками SVI-интерфейсов (виртуального интерфейса коммутатора) двух сегментов сети, обеспечивая взаимодействие между двумя сегментами IP-сети.

6.4. Функции

6.4.1. Базовые концепты

Сессия ERSPAN

Пакеты данных SPAN общих RSPAN могут передаваться только в пределах уровня 2 и не могут проходить через сети маршрутизации. Однако зеркалирование ERSPAN позволяет передавать пакеты SPAN между сетями маршрутизации. ERSPAN инкапсулирует все пакеты SPAN в пакеты IP через туннель GRE и направляет их на порт назначения устройства RSPAN. ERSPAN может отслеживать входящие, исходящие и двунаправленные пакеты одного или нескольких портов. Такие порты, как коммутируемый порт, маршрутизируемый порт и агрегируемый порт (AP), можно настроить в качестве исходного порта для сеанса ERSPAN. Коммутатор не затрагивается после добавления порта в сеанс ERSPAN.

Исходный порт

Исходный порт также называется контролируемым портом. В сеансе ERSPAN потоки данных исходного порта отслеживаются для сетевого анализа и устранения неполадок. В рамках одного сеанса ERSPAN пользователи могут отслеживать входные, выходные и двунаправленные потоки данных, а количество исходных портов не ограничено. Исходный порт имеет следующие особенности:

- Исходный порт может быть коммутируемым портом, маршрутизируемым портом или агрегируемым портом.
- Он поддерживает зеркалирование нескольких исходных портов на исходном устройстве на назначенные выходные порты.
- Исходный порт и выходной порт не могут быть на одном и том же порту; когда исходный порт SPAN является интерфейсом уровня 3, отслеживаются пакеты уровня 2 и уровня 3.
- Когда несколько портов отслеживаются в двух направлениях, пакет вводится с одного порта и выводится с другого. Такой мониторинг считается корректным, если контролируется только один пакет.
- Когда статус включенного STP-порта находится в состоянии блокировки, входящие и исходящие пакеты на порту можно отслеживать.
- Исходный порт и порт назначения могут принадлежать одной и той же VLAN или разным VLAN.

6.4.2. Обзор

Особенность	Описание
ERSPAN	Настраивает SPAN на разные интернет-порты

6.4.3. ERSPAN

Инкапсулированный ERSPAN является расширением RSPAN. Пакеты данных SPAN общих RSPAN могут передаваться только в пределах уровня 2 и не могут проходить через сети маршрутизации. Однако ERSPAN может передавать пакеты SPAN между сетями маршрутизации.

6.4.3.1. Принцип работы

Все mirrored-пакеты инкапсулируются в IP-пакеты через туннель GRE и направляются на порт назначения устройства RSPAN.

Настройка сеанса ERSPAN

Настройте ERSPAN коммутатора и различайте атрибуты коммутатора ERSPAN устройства. Вам необходимо назначить идентификатор сеанса ERSPAN и войти в режим конфигурации ERSPAN после успешной настройки.

Настройка исходного порта

После входа в режим конфигурации ERSPAN вам необходимо указать исходный порт, чтобы настроить исходный порт SPAN, и определить направление потоков данных SPAN в соответствии с дополнительными конфигурациями направления SPAN.

Включение сеанса ERSAN

По умолчанию включение сеанса ERSPAN означает включение зеркалирования ERSPAN. Вступают в силу только включенные сеансы ERSPAN.

Инкапсуляция исходного IP-адреса

Инкапсуляция исходного IP-адреса предназначена для настройки исходного IP-адреса инкапсулированного пакета GRE.

Инкапсуляция IP-адреса назначения

Инкапсуляция IP-адреса назначения предназначена для настройки IP-адреса назначения инкапсулированного пакета GRE и обеспечения нормальной маршрутизации пакетов SPAN в сети.

Инкапсуляция IP TTL/DSCP

Инкапсулируйте значения времени жизни (TTL) и точки кода дифференцированных услуг (DSCP) IP-пакетов.

Настройка режима захвата

Настройте режим захвата (зеркалировать ли весь пакет или байты заголовка исходного пакета).

Настройка частоты выборки

Настройте частоту выборки (количество пакетов для одной операции mirroring) для зеркалирования на исходном порту.

vrf vrf-name

Указывает имя виртуальной маршрутизации. Различные значения виртуальной маршрутизации могут иметь разные исходы для одного и того же IP-адреса назначения.

6.4.3.2. Связанная конфигурация

По умолчанию SPAN отключен. Он включается только после создания сеанса и настройки порта SPAN источника, исходного IP-адреса и IP-адреса назначения.

Настройка сеанса ERSPAN

QTECH(config)# **monitor session** *session_num* **erspan-source**

session_num: указывает, что количество сеансов SPAN, поддерживаемых идентификаторами сеансов SPAN, зависит от продукта.

Настройка исходного порта

QTECH(config-mon-erspan-src)# **source interface** {*single- interface* | **all** } { [**rx** | **tx** | **both**] }

single_interface: указывает исходный порт SPAN, который необходимо настроить.

all: указывает, что исходный порт SPAN, подлежащий настройке, является глобальным интерфейсом, поддерживающим зеркалирование.

rx: указывает, что после настройки **rx** отслеживаются только пакеты, полученные исходным портом.

tx: указывает, что после настройки **tx** отслеживаются только пакеты, отправленные с исходного порта.

both: указывает, что после того, как **both** настроен, пакеты, отправленные и полученные исходным портом, передаются на порт назначения для отслеживания; то есть **both** включают **rx** и **tx**. Если ни **rx**, ни **tx**, ни **both** не настроены, **both** включены по умолчанию.

Настройка SPAN на основе потока

По умолчанию функция отключена. Запустите команду QTECH(config-mon-erspan-src)# **source interface** *interface-id* **rx acl** *acl-name* {**sample**}, чтобы настроить SPAN на основе потоков и частоты выборки (Опционально).

Включение сеанса ERSAN

QTECH (config-mon-erspan-src)# **shutdown**

Эта команда используется для отключения зеркалирования ERSPAN. (По умолчанию) Запустите команду **no shutdown**, чтобы включить зеркалирование ERSPAN.

Инкапсуляция IP-адреса назначения

QTECH(config-mon-erspan-src)# **destination ip address** *ip-address*

ip-address: инкапсулирует IP-адрес назначения.

Инкапсуляция исходного IP-адреса

QTECH(config-mon-erspan-src)# **origin ip address** *ip-address*

ip-address: инкапсулирует исходный IP-адрес.

Инкапсуляция IP TTL

QTECH(config-mon-erspan-src)# **ip ttl** *ttl_value*

ttl_value: настраивает значение TTL инкапсулированного IP-адреса. Значение TTL находится в диапазоне от 0 до 255, а значение по умолчанию — 64.

Инкапсуляция IP DSCP

QTECH(config-mon-erspan-src)# **ip dscp** *dscp_value*

dscp_value: настраивает значение DSCP для инкапсулированного IP-адреса. Значение DSCP находится в диапазоне от 0 до 63, а значение по умолчанию равно 0. Функция вступает в силу только после настройки доверия DSCP на исходном порту SPAN.

Настройка режима захвата

QTECH(config-mon-erspan-src)# **capture-mode** [**all | truncate**]

all: значение по умолчанию, указывающее, что зеркалируется весь исходный пакет.

truncate: указывает, что байт заголовка исходного пакета зеркально отражен. Конкретное количество байтов заголовка, подлежащих зеркалированию, определяется чипом продукта.

Настройка частоты выборки

QTECH(config-mon-erspan-src)# **sampling-rate** *rate*

rate: Указывает значение частоты выборки в диапазоне от 1 до 1 000 000. Например, если частота выборки равна 100, один пакет выбирается из 100 пакетов, то есть коэффициент выборки составляет 100:1. Частота выборки по умолчанию составляет 1:1, то есть выборка осуществляется из каждого пакета.

Эта функция действительна только тогда, когда частота выборки настроена на исходном порту SPAN.

Инкапсуляция vrf vrf-name

QTECH(config-mon-erspan-src)# **vrf** *vrf-name*

vrf-name: указывает имя VRF (экземпляра маршрутизации и пересылки VPN).

ПРИМЕЧАНИЕ: во время использования обратите внимание на следующие проблемы:

- Подтвердите подключение маршрутизации уровня 3 от коммутатора-источника к коммутатору-адресату.
- ERSPAN недоступен, если исходный порт отключен.
- Если исходный порт или порт назначения добавляются к AP, исходный порт или порт назначения выходит из сеанса ERSPAN.

- Из-за различий продуктов не все продукты поддерживают все параметры вышеупомянутых команд.

6.5. Конфигурация

Конфигурация	Описание и команда	
Настройка основных функций ERSPAN	(Обязательный) Используется для создания зеркалирования ERSPAN	
	monitor session *erspan_source_session_number* **erspan-source**	Настраивает идентификатор сеанса ERSPAN и входит в режим конфигурации исходного устройства ERSPAN
	source interface {*single-interface* | **all** } {[**rx** | **tx** | **both**]}	Связывает исходный порт ERSPAN и выбирает направление SPAN
	source interface { *single-interface* | **all** } **rx acl** *acl-name* [**sample**]	Настраивает источник SPAN на основе потока для ERSPAN и включает выборку
	shutdown	Отключает зеркалирование ERSPAN
	destination ip address *ip_address*	Настраивает IP-адрес назначения для потока ERSPAN. Адрес должен быть адресом интерфейса целевого устройства
	original ip address *ip_address*	Настраивает инкапсулированный исходный IP-адрес для ERSPAN
	ip ttl *ttl_value*	(Опционально) Настраивает значение TTL инкапсулированного IP-адреса для ERSPAN
Настройка основных функций ERSPAN	**ip dscp** *dscp_value*	(Опционально) Настраивает значение поля DSCP инкапсулированного IP-адреса для ERSPAN
	capture-mode [**all** | **truncate**]	(Опционально) Настраивает режим захвата для зеркалирования исходного пакета
	sampling-rate *rate*	(Опционально) Настраивает частоту выборки для зеркалирования

Конфигурация	Описание и команда	
Настройка основных функций ERSPAN	**vrf** *vrf_name*	(Опционально) Настраивает имя VRF

6.5.1. Настройка основных функций ERSPAN

6.5.1.1. Эффект конфигурации

- RSPAN позволяет сетевому анализатору отслеживать пользователей.
- Устройства могут нормально обмениваться данными друг с другом.

6.5.1.2. Примечания

- Если исходный порт добавляется к AP, исходный порт выходит из сеанса ERSPAN.
- Должна быть обеспечена маршрутизация уровня 3 от коммутатора-источника к коммутатору-адресату.

6.5.1.3. Шаги настройки

- Сессия ERSPAN.
- Режим глобальной конфигурации. Обязательный.
- Идентификатор сеанса, настроенный с локальным SPAN или RSPAN, не может использоваться для сеанса ERSPAN. Войдите в режим ERSPAN после настройки.

Исходный порт

- Режим конфигурации ERSPAN. Обязательный.
- Направление SPAN можно выбрать во время настройки исходного порта SPAN. Направление **both** по умолчанию; то есть отслеживаются как прием, так и передача пакетов.

Включение сеанса ERSPAN

- Режим конфигурации ERSPAN. Обязательный.
- По умолчанию включение сеанса ERSPAN означает включение зеркалирования ERSPAN. Вступают в силу только включенные сеансы ERSPAN.

Инкапсуляция исходного IP-адреса

- Режим конфигурации ERSPAN.Обязательный.
- Используется для инкапсуляции исходных IP-адресов пакетов SPAN.

Инкапсуляция IP-адреса назначения

- Режим конфигурации ERSPAN. Обязательный.
- Используется для инкапсуляции IP-адресов назначения пакетов SPAN.

Инкапсуляция IP TTL/DSCP

- Режим конфигурации ERSPAN. Опциональный.
- Используется для инкапсуляции значений DSCP IP-пакетов SPAN.

Настройка режима захвата

- Режим конфигурации ERSPAN. Опциональный.

- Используется для настройки режима захвата для зеркалирования исходного пакета.

Настройка частоты выборки

- Режим конфигурации ERSPAN. Опциональный.
- Используется для настройки частоты выборки для зеркалирования.

vrf vrf-name

- Режим глобальной конфигурации. Опциональный.
- Он указывает имя VRF. VRF должен существовать.

6.5.1.4. Проверка

Запустите команду **show monitor** или команду **show running**, чтобы проверить конфигурацию SPAN. Вы также можете провести анализ захвата пакетов на целевом порту SPAN и проверить, действует ли SPAN в соответствии с захваченными пакетами.

6.5.1.5. Связанные команды

Настройка сеанса ERSPAN

Команда	**monitor session** *session_number* **erspan-source**
Описание параметров	*session_number*: указывает идентификатор сеанса SPAN
Режим команд	Режим глобальной конфигурации

Настройка исходного порта

Команда	**source interface {** *single-interface* **| all } {[rx | tx | both]}**
Описание параметров	*single-interface*: указывает идентификатор сеанса SPAN. **all**: указывает глобальные интерфейсы, поддерживающие зеркалирование. **both**: по умолчанию отслеживает как входящие, так и исходящие пакеты
Описание параметров	**rx**: отслеживает только входящие пакеты. **tx**: отслеживает только исходящие пакеты
Режим команд	Режим сеанса ERSPAN

Настройка SPAN на основе потока

Команда	**source interface {** *single-interface* **| all } rx acl** *acl-name* **sample**
Описание параметров	*single-interface*: указывает имя интерфейса. **all**: указывает глобальные интерфейсы, которые поддерживают зеркалирование.

	acl-name: указывает имя ACL. **sample**: указывает, включена ли выборка
Режим команд	Режим сеанса ERSPAN

Включение сеанса ERSAN

Команда	**shutdown**
Режим команд	Режим сеанса ERSPAN

Инкапсуляция исходного IP-адреса

Команда	**original ip address** *ip_address*
Описание параметров	*ip_address*: указывает исходный IP-адрес, который необходимо инкапсулировать
Режим команд	Режим сеанса ERSPAN

Инкапсулирует IP-адрес назначения

Команда	**destination ip address** *ip_address*
Описание параметров	*ip_address*: указывает IP-адрес назначения для инкапсуляции
Режим команд	Режим сеанса ERSPAN

Настройка режима захвата

Команда	**capture-mode [all | truncate]**
Описание параметров	**all**: указывает, что весь исходный пакет зеркалирован. **truncate**: указывает, что байт заголовка исходного пакета зеркалирован. Конкретное количество байтов заголовка, подлежащих зеркалированию, определяется чипом продукта
Режим команд	Режим сеанса ERSPAN

Настройка частоты выборки

Команда	**sampling-rate** *rate*
Описание параметров	*rate*: указывает требуемую частоту выборки

Режим команд	Режим сеанса ERSPAN

Инкапсуляция IP TTL

Команда	**ip ttl** *ttl_value*
Описание параметров	*ttl_value*: настраивает значение TTL инкапсулированного IP-адреса для ERSPAN. Диапазон значений от 1 до 255
Режим команд	Режим сеанса ERSPAN

Инкапсуляция DSCP

Команда	**ip dscp** *dscp_value*
Описание параметров	*dscp_value*: настраивает значение поля DSCP инкапсулированного IP-адреса для ERSPAN. Диапазон значений от 0 до 64
Режим команд	Режим сеанса ERSPAN

Настройка VRF *vrf-name*

Команда	**vrf** *vrf-name*
Описание параметров	*vrf-name*: указывает имя VRF
Режим команд	Режим сеанса ERSPAN

6.5.1.6. Пример конфигурации

Ниже в качестве примера используется SPAN.

Сценарий:

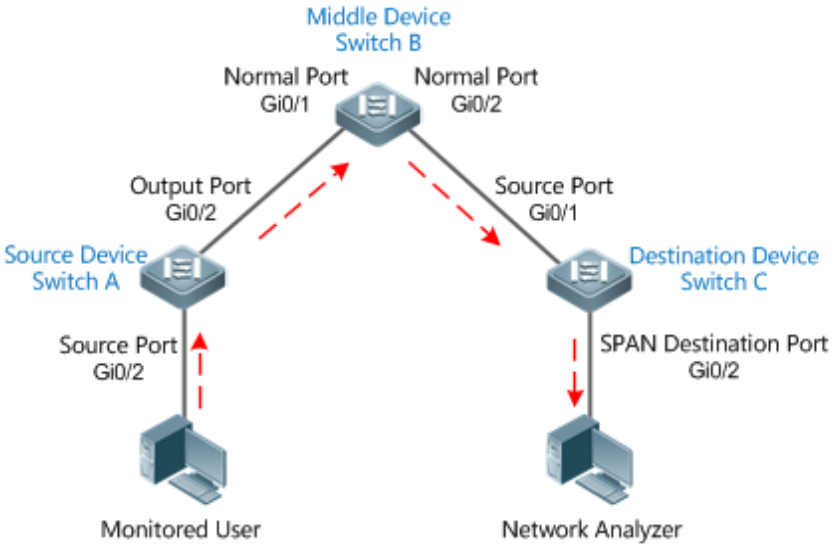


Рисунок 6-3.

Шаги настройки	Как показано на Рисунке 6-3, на коммутаторе A создайте сеанс ERSPAN 1 и настройте его как исходное устройство, а Gi 0/1 настройте как исходный порт
	SwitchA(config)#monitor session 1 erspan-source SwtichA(config-mon-erspan-src)#source interface gigabitEthernet 0/1 both SwtichA(config-mon-erspan-src)#origin ip address 10.1.1.2 SwtichA(config-mon-erspan-src)#destination ip address 12.1.1.2 SwtichA(config-mon-erspan-src)#vrf vrf-name
Проверка	Шаг 1. Проверьте конфигурацию устройства
	SwitchA#show running-config ! monitor session 1 erspan-src source interface GigabitEthernet 0/1 both origin ip address 10.1.1.2 destination ip address 12.1.1.2 vrf vrf-name
	Шаг 2. Проверьте информацию ERSPAN устройства. SwitchA#show monitor

	sess-num: 1 //ERSPAN Session span-type: ERSPAN_SOURCE //ERSPAN source device src-intf: //ERSPAN source port information GigabitEthernet 0/1 frame-type Both TX status: Inactive RX status: Inactive dest-intf: //ERPSAN output port information GigabitEthernet 0/2 orgin ip address 10.1.1.2 destination ip address 12.1.1.2 destination capture mode all SwitchA#show monitor sess-num: 1 span-type: ERSPAN_SOURCE src-intf: GigabitEthernet 0/1 frame-type Both TX status: Inactive RX status: Inactive dest-intf: GigabitEthernet 0/2 orgin ip address 10.1.1.2 destination ip address 12.1.1.2 destination capture mode all ip ttl 64 ip dscp 0 sample rate 0 vrf vrf-name

6.5.1.7. Распространенные ошибки

- Идентификатор сеанса, используемый для настройки зеркалирования ERSPAN, настраивается с помощью RSPAN или LOCAL SPAN.
- Сбой взаимодействия маршрутизации уровня 3 между коммутатором-источником и коммутатором-получателем.

6.6. Мониторинг

6.6.1. Отображение

Описание	Команда
Отображает все сеансы SPAN в системе	**show monitor**

Описание	Команда
Отображает определенные сеансы SPAN	**show monitor session** *session-id*

6.6.2. Отладка

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

Описание	Команда
Диапазон отладки	**debug span**

7. НАСТРОЙКА SFLOW

7.1. Обзор

sFlow — это технология мониторинга сети, совместно разработанная InMon, HP и FoundryNetworks в 2001 году. Эта технология была стандартизирована. Она может обеспечить полные потоки трафика от уровня 2 до уровня 4 и применим для анализа трафика в очень большой сети. Эта технология помогает пользователям детально анализировать производительность, тенденции и наличие потоков сетевого трафика в режиме реального времени.

sFlow имеет следующие преимущества:

- Accurate: sFlow поддерживает точный мониторинг трафика в гигабитной сети или сети с более высокой пропускной способностью.
- Scalable: один коллектор sFlow может контролировать тысячи агентов sFlow и обладает высокой масштабируемостью.
- Low cost: агент sFlow встроен в сетевое устройство, и его стоимость невелика.

Спецификация протокола

- sFlow версии 5
- RFC 1014

7.2. Приложения

Типичное применение	Сценарий
Мониторинг трафика локальной сети	Рассматривайте устройство как агента sFlow, выполняйте выборку трафика интерфейса в локальной сети и отправляйте датаграммы sFlow коллектору sFlow для анализа трафика, тем самым достигая цели мониторинга сети

7.2.1. Мониторинг трафика локальной сети

7.2.1.1. Сценарий приложения

Как показано на Рисунке 7-1, запустите коммутатор A, который служит агентом sFlow, включите выборку потока и выборку счетчика на порту Te 0/1, отслеживайте трафик в сегменте сети 192.168.1.0, инкапсулируйте данные выборки в датаграммы sFlow через регулярные промежутки времени или при заполнении буфера и отправляет данные sFlow в коллектор sFlow для анализа трафика.

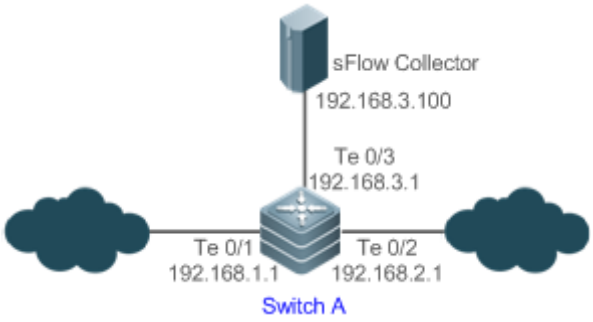


Рисунок 7-1.

7.2.1.2. Развертывание функций

- Настройте адреса агента sFlow и коллектора sFlow на коммутаторе A.
- Включите выборку потока и выборку счетчика на порте Te 0/1 коммутатора A.

Многие серверные программы поддерживают sFlow. Вы можете получить программное обеспечение, поддерживающее sFlow, по адресу http://www.sflow.org/products/collectors.php. Программное обеспечение sflowtrend является бесплатным.

7.3. Функции

7.3.1. Базовые концепты

Агент sFlow

Агент sFlow встроен в сетевое устройство. Как правило, одно сетевое устройство может служить агентом sFlow. Агент sFlow может выполнять выборку потока и выборку счетчика, инкапсулировать выборочные данные в датаграммы sFlow и отправлять датаграммы sFlow коллектору sFlow.

Датаграммы sFlow инкапсулируются в UDP. На Рисунке 7-2 показан формат датаграммы sFlow.

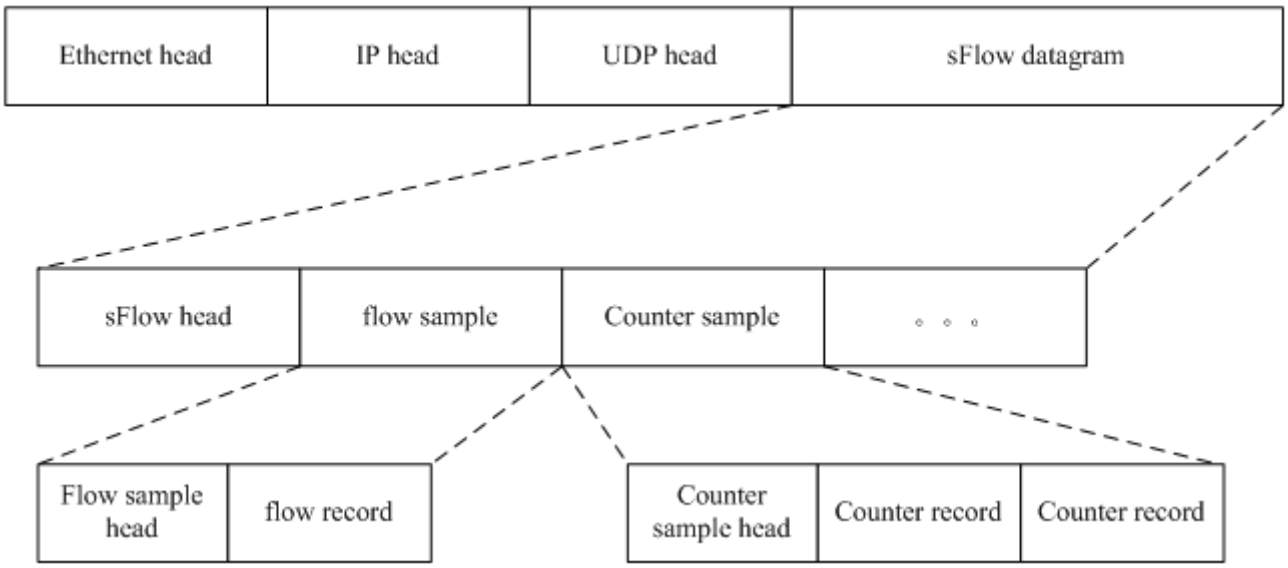


Рисунок 7-2. Формат датаграммы sFlow

Одна датаграмма sFlow может содержать одну или несколько выборок потока и выборок счетчика.

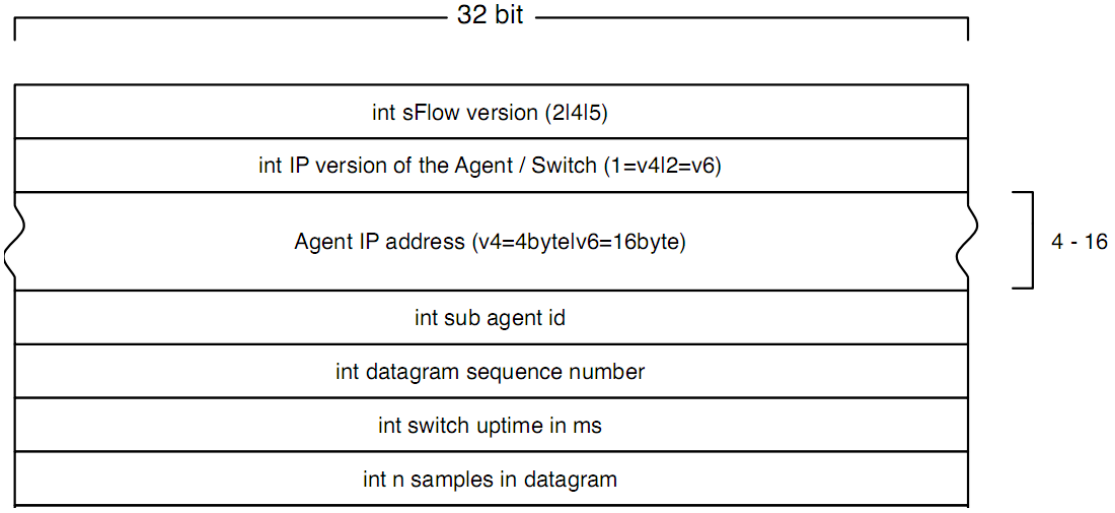


Рисунок 7-3. Заголовок sFlow

Описание заголовка: sFlow:

Поле	Описание
Версия sFlow	sFlow-версия. Доступны версии V2, V4 и V5. В настоящее время QTECH поддерживает только V5
IP-версия агента/коммутатора	Версия IP-адреса агента sFlow
IP-адрес агента	IP-адрес агента sFlow
Идентификатор субагента	Идентификатор субагента
Порядковый номер датаграммы	Серийный номер датаграммы sFlow
Время безотказной работы переключателя	Продолжительность от момента запуска коммутатора до текущего времени
n выборок в датаграмме	Количество выборок в датаграмме sFlow. Одна датаграмма sFlow может содержать одну или несколько выборок потока и выборок счетчика

Коллектор sFlow

Коллектор sFlow получает и анализирует датаграмму sFlow, отправленную агентом sFlow. Коллектор sFlow может быть ПК или сервером. ПК или сервер, на котором установлено прикладное программное обеспечение для анализа датаграмм sFlow, можно рассматривать как коллектор sFlow.

Выборка потока

На основе указанной частоты выборки устройство агента sFlow выполняет выборку потока трафика, проходящего через интерфейс, включая копирование заголовка пакета, извлечение заголовка Ethernet и IP-заголовка пакета и получение информации о маршруте пакета.

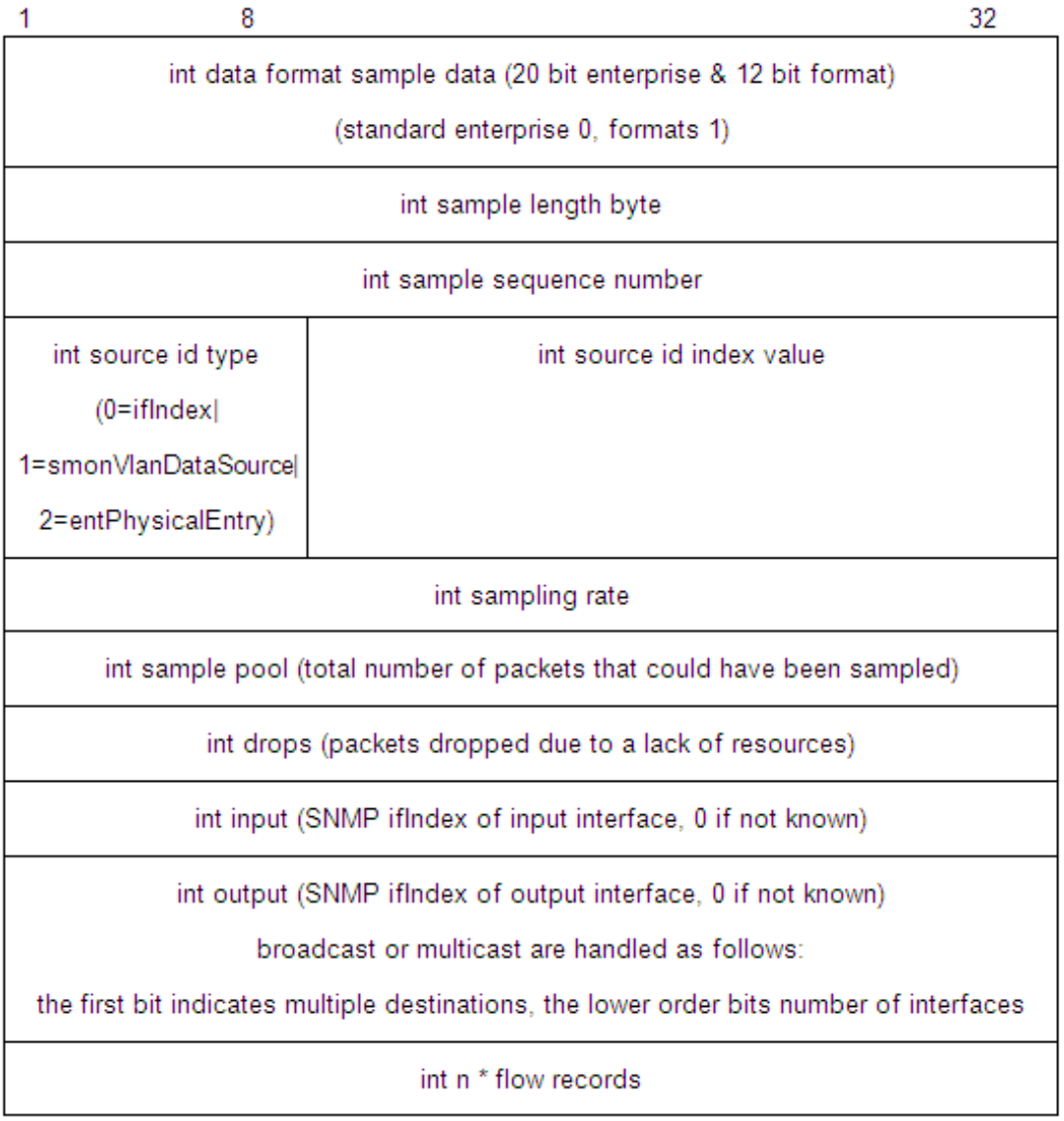


Рисунок 7-4. Заголовок выборки потока

Счетчик выборки

При выборке счетчика агент sFlow периодически получает статистику и данные об использовании ЦП на указанном интерфейсе. Статистика по интерфейсу включает количество пакетов, входящих через интерфейс, и количество пакетов, выводимых через интерфейс.

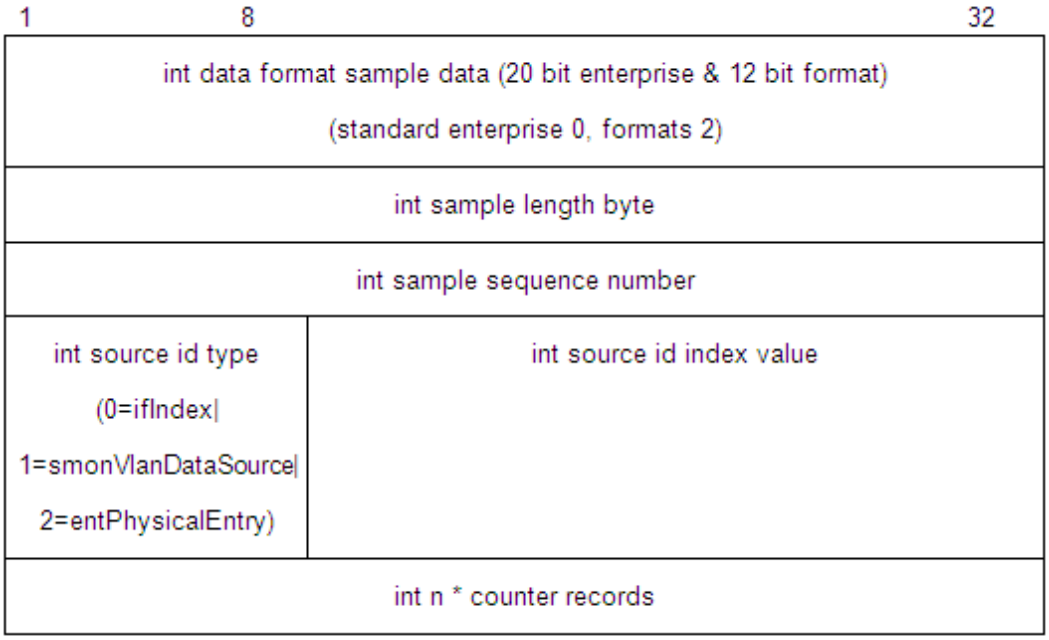


Рисунок 7-5. Заголовок выборки счетчика

7.3.2. Функции и особенности

Особенность	Описание
Выборка потока	Отбирает трафик, проходящий через интерфейс, и отправляет инкапсулированную датаграмму sFlow коллектору sFlow для анализа
Счетчик Выборки	Периодически отправлять статистику по интерфейсу в коллектор sFlow для анализа

7.3.3. Выборка потока

Отбирает трафик, проходящий через интерфейс, и отправляет инкапсулированную датаграмму sFlow коллектору sFlow для анализа.

7.3.3.1. Принцип работы

На основе указанной частоты выборки устройство агента sFlow выполняет выборку потока трафика, проходящего через интерфейс, включая копирование заголовка пакета, извлечение заголовка Ethernet и IP-заголовка пакета и получение информации о маршруте пакета. Затем агент sFlow инкапсулирует данные выборки потока в датаграмму sFlow и отправляет датаграмму коллектору sFlow для анализа.

7.3.4. Счетчик Выборки

Периодически отправляет статистику по интерфейсу в коллектор sFlow для анализа.

7.3.4.1. Принцип работы

Агент sFlow регулярно выполняет опрос интерфейса. Для интерфейса, интервал выборки счетчика которого истек, агент sFlow получает статистику по этому интерфейсу,

инкапсулирует статистику в датаграмму sFlow и отправляет датаграмму коллектору sFlow для анализа.

7.4. Конфигурация

Элемент конфигурации	Предложение и соответствующая команда	
Настройка основных функций sFlow	Обязательная конфигурация. Установите коммуникационные соединения между агентом sFlow и коллектором sFlow	
	sflow agent {address | interface}	Настраивает адрес агента sFlow
	sflow collector *collector-id* **destination**	Настраивает адрес коллектора sFlow
	Обязательная конфигурация. Включите выборку потока и выборку счетчика	
	sflow counter collector	Позволяет агенту sFlow отправлять счетчики выборок в коллектор sFlow
	sflow flow collector	Позволяет агенту sFlow отправлять выборки потока в коллектор sFlow
	sflow enable	Включает выборку sFlow для интерфейса конфигурации, то есть включает выборку счетчика и выборку потока
Настройка дополнительных параметров sFlow	Дополнительная конфигурация. Задает опциональные атрибуты параметров sFlow	
	sflow collector *collector-id* **max datagram-size**	Настраивает максимальную длину датаграммы sFlow
	sflow counter interval	Настраивает интервал выборки счетчика
	sflow flow max-header	Настраивает максимальную длину заголовка пакета, копируемого во время выборки потока
	sflow sampling-rate	Настраивает частоту выборки потока

Элемент конфигурации	Предложение и соответствующая команда	
Настройка дополнительных параметров sFlow	**sflow source {address | interface}**	Настраивает исходный адрес sFlow

7.4.1. Настройка основных функций sFlow

7.4.1.1. Эффект конфигурации

- Агент sFlow и коллектор sFlow могут взаимодействовать друг с другом.
- Трафик, проходящий через интерфейс, отбирается на основе частоты выборки по умолчанию и отправляется в коллектор sFlow для анализа.
- Статистика интерфейса периодически отправляется в коллектор sFlow на основе интервала выборки по умолчанию для анализа.

7.4.1.2. Примечания

- Выборка потока может быть настроена только на физических интерфейсах.
- Чтобы коллектор sFlow мог анализировать результаты выборки потока, требуется IP-адрес коллектора sFlow на устройстве агента sFlow.

7.4.1.3. Метод конфигурации

Настройка адреса агента sFlow

- Обязательная конфигурация.
- Используйте команду **sflow agent address** для настройки адреса агента sFlow.
- Адрес агента sFlow должен быть допустимым адресом. То есть адрес агента sFlow не должен быть многоадресным или широковещательным. Рекомендуется использовать IP-адрес устройства sFlow Agent.

Синтаксис команды	**sflow agent { address {***ip-address* **| ipv6** *ipv6-address* **}} | { interface {** *interface-name* **| ipv6** *interface-name* **}}**
Описание параметров	**address**: настраивает IP-адрес агента sFlow. *ip-address*: IPv4-адрес агента sFlow **ipv6** *ipv6-address*: IPv6-адрес агента sFlow. **interface**: настраивает интерфейс агента sFlow. *interface-name*: интерфейс IPv4-адреса. **ipv6** *interface-name*: интерфейс адреса IPv6
По умолчанию	По умолчанию адрес агента sFlow не настроен
Режим команд	Режим глобальной конфигурации

Использование конфигурации	Эта команда используется для настройки поля **agent ip address** в выходной датаграмме sFlow. Датаграмма, не сконфигурированная с этим полем, не может быть выведена. Адрес агента sFlow должен быть адресом хоста. Когда адрес, не являющийся хостом (например, многоадресный или широковещательный адрес), настроен в качестве адреса агента sFlow, отображается сообщение о сбое конфигурации. В качестве адреса агента sFlow рекомендуется настроить IP-адрес устройства sFlow Agent

Настройка адреса коллектора sFlow

- Обязательная конфигурация.
- Используйте команду **sflow collector** для настройки адреса коллектора sFlow.
- Адрес коллектора sFlow должен быть действительным адресом. То есть адрес коллектора sFlow не должен быть многоадресным или широковещательным. Коллектор sFlow должен существовать, и маршрут к нему должен быть доступен.

Синтаксис команды	**sflow collector** *collector-id* **destination {** *ip-address* **| ipv6** *ipv6_address* **}** *udp-port* **[[vrf** *vrf-name* **] | [oob] [via mgmt** *mgmt-name* **]]]] | [description** *collector-name* **]**
Описание параметров	*collector-id*: идентификатор коллектора sFlow. Диапазон от 1 до 2. *ip-address*: IPv4-адрес агента sFlow. По умолчанию он не настроен. **ipv6** *ipv6_address*: IPv6-адрес агента sFlow. По умолчанию он не настроен. *udp-port*: номер listening-портf коллектора sFlow. **vrf** *vrf-name*: имя экземпляра VRF. По умолчанию он не настроен. **oob**: отобранные данные о трафике выводятся через интерфейс управления. По умолчанию этот параметр не настроен. **via mgmt** *mgmt-name*: порт управления. По умолчанию он не настроен. **description** *collector-name*: описание коннектора sFlow. По умолчанию он не настроен
Режим команд	Режим глобальной конфигурации
Использование конфигурации	Эта команда используется для настройки адреса коллектора sFlow. Адрес коллектора sFlow должен быть адресом хоста. Когда адрес, не являющийся хостом (например, многоадресный или широковещательный адрес), настроен в качестве адреса коллектора sFlow, отображается сообщение о сбое конфигурации. Сборщик sFlow отслеживает датаграмму sFlow на указанном порту. При настройке параметра **vrf** должен существовать соответствующий экземпляр VRF. При удалении экземпляра VRF адрес коллектора sFlow будет удален, если этот экземпляр VRF также настроен для адреса коллектора sFlow. Когда параметр **oob** настроен, датаграмма отправляется коллектору sFlow через интерфейс управления

Включение вывода выборок sFlow в коллектор sFlow

- Обязательная конфигурация.
- Вы можете использовать команду **sflow flow collector**, чтобы позволить агенту sFlow отправлять выборки потока в коллектор sFlow.
- Эта функция должна быть включена в интерфейсе для отправки выборок потока в коллектор sFlow. Кроме того, должен существовать коллектор sFlow, маршрут к нему должен быть доступен, а IP-адрес соответствующего коллектора sFlow был настроен на устройстве агента sFlow.

Синтаксис команды	**sflow flow collector** *collector-id*
Описание параметров	*collector-id*: идентификатор коллектора sFlow. Диапазон от 1 до 2
По умолчанию	Отправка выборок потока в коллектор sFlow отключена по умолчанию
Режим команд	Режим конфигурации интерфейса
Использование конфигурации	Эту команду можно использовать для физических портов, портов SVI и портов с дополнительной маршрутизацией. Датаграммы sFlow могут выводиться только в том случае, если для соответствующего коллектора sFlow настроен IP-адрес

Включение вывода выборок счетчика в коллектор sFlow

- Обязательная конфигурация.
- Вы можете использовать команду **sflow counter collector**, чтобы позволить агенту sFlow отправлять выборки счетчиков коллектору sFlow.
- Это должно быть включено в интерфейсе, чтобы отправлять выборки счетчиков в коллектор sFlow. Кроме того, должен существовать коллектор sFlow, маршрут к нему должен быть доступен, а IP-адрес соответствующего коллектора sFlow был настроен на устройстве агента sFlow.

Синтаксис команды	**sflow counter collector** *collector-id*
Описание параметров	*collector-id*: идентификатор коллектора sFlow. Диапазон от 1 до 2
По умолчанию	Отправка счетчика выборок в коллектор sFlow отключена по умолчанию
Режим команд	Режим конфигурации интерфейса

Использование конфигурации	Эту команду можно использовать для физических портов, портов SVI и портов с дополнительной маршрутизацией. Датаграммы sFlow могут выводиться только в том случае, если для соответствующего коллектора sFlow настроен IP-адрес

Включение счетчика выборки и выборки потока

- Обязательная конфигурация.
- Вы можете использовать команду **sflow enable**, чтобы включить выборку потока и выборку счетчика на интерфейсе.
- На производительность пересылки интерфейса может повлиять включение выборки потока.

Синтаксис команды	**sflow enable [ingress | egress]**
Описание параметров	**ingress**: включает выборку sFlow в направлении входа. **egress**: включает выборку sFlow в направлении выхода
По умолчанию	Функция выборки sFlow на интерфейсе по умолчанию отключена
Режим команд	Режим конфигурации интерфейса
Использование конфигурации	Эту команду можно использовать для включения выборки счетчика и выборки потока для физических портов, портов SVI и портов с подмаршрутизацией. Если параметр направления не указан, включается выборка в обоих направлениях. Порты SVI и порты с подмаршрутизацией поддерживают только входной параметр

7.4.1.4. Метод проверки

Используйте команду **show sflow** для отображения конфигурации sFlow и проверьте, согласуется ли отображаемая информация с конфигурацией.

7.4.1.5. Примеры конфигурации

Настройка выборки потока и выборки счетчика для агента sFlow

Сетевое окружение:

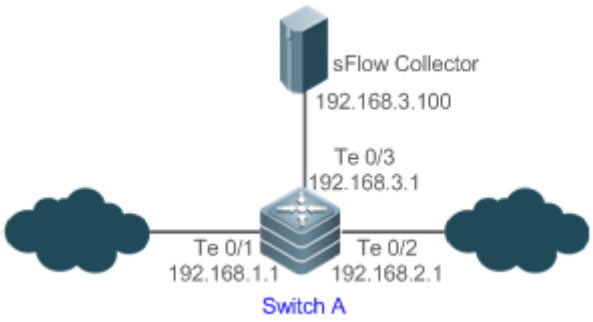


Рисунок 7-6.

	Как показано на Рисунке 7-6, запустите коммутатор A, который служит агентом sFlow, включите выборку потока и выборку счетчика на порту Te 0/1, отслеживайте трафик в сегменте сети 192.168.1.0, инкапсулируйте трафик выборки в датаграммы sFlow на через регулярные промежутки времени или при заполнении буфера и отправлять датаграммы sFlow коллектору sFlow для анализа трафика
Метод конфигурации	• Настройте 192.168.1.1 в качестве адреса агента sFlow. • Настройте 192.168.3.100 в качестве адреса коллектора sFlow 1 и 6343 в качестве номера порта. • Настройте интерфейс TenGigabitEthernet 0/1 для вывода выборок потока и выборок счетчика на коллектор sFlow 1 и включите функцию выборки sFlow на этом интерфейсе
Переключатель A	QTECH# configure terminal QTECH(config)# sflow agent address 192.168.1.1 QTECH(config)# sflow collector 1 destination 192.168.3.100 6343 QTECH(config)# interface TenGigabitEthernet 0/1 QTECH(config-if-TenGigabitEthernet 0/1)# sflow flow collector 1 QTECH(config-if-TenGigabitEthernet 0/1)# sflow counter collector 1 QTECH(config-if-TenGigabitEthernet 0/1)# sflow enable QTECH(config-if-TenGigabitEthernet 0/1)# end
Метод проверки	Используйте команду **show sflow**, чтобы проверить, согласуются ли выходные данные команды с конфигурацией
	QTECH# show sflow sFlow datagram version 5 Global information:

	Agent IP: 192.168.1.1 sflow counter interval:30 sflow flow max-header:64 sflow sampling-rate:8192 Collector information: ID IP Port Size VPN 1 192.168.3.100 6343 1400 2 NULL 0 1400 Port information Interface CID FID Enable TenGigabitEthernet 0/1 1 1 Y

7.4.2. Настройка дополнительных параметров sFlow

7.4.2.1. Эффект конфигурации

Вы можете настроить точность выборки данных, изменив соответствующие атрибуты параметров sFlow.

7.4.2.2. Примечания

На производительность пересылки может повлиять слишком низкая частота выборки.

7.4.2.3. Метод конфигурации

Настройка максимальной длины выходной датаграммы sFlow

- Дополнительная конфигурация.
- Вы можете использовать команду **sflow collector** для настройки длины датаграммы sFlow, исключая заголовок Ethernet, заголовок IP и заголовок UDP. Датаграмма sFlow может содержать одну или несколько выборок потока и выборок счетчика. Настройка максимальной длины выходной датаграммы sFlow может привести к тому, что количество датаграмм sFlow, выводимых при обработке определенного количества выборок потока, будет отличаться от количества датаграмм sFlow, выводимых при обработке того же количества пакетов счетчика. Если максимальная длина превышает MTU, выходные датаграммы sFlow будут сегментированы.

Синтаксис команды	**sflow collector** *collector-id* **max-datagram-size** *datagram-size*
Описание параметров	*collector-id*: идентификатор коллектора sFlow. Диапазон от 1 до 2 **max-datagram-size** *datagram-size*: максимальная длина выходной датаграммы sFlow. Диапазон от 200 до 9000
По умолчанию	Значение по умолчанию — 1400

Режим команд	Режим глобальной конфигурации

Настройка частоты выборки потока

- Дополнительная конфигурация.
- Вы можете использовать команду **sflow sample-rate** для настройки глобальной частоты выборки потока.
- Конфигурация частоты выборки потока может повлиять на точность выборки sFlow. Более низкая частота выборки означает более высокую точность и большее потребление ЦП. Таким образом, производительность пересылки интерфейса может быть снижена при низкой частоте выборки.

Синтаксис команды	**sflow sampling-rate** *rate*
Описание параметров	*rate*: частота выборки sFlow. Один пакет выбирается из каждых n пакетов (n равно значению скорости). Диапазон от 4096 до 65 535
По умолчанию	Частота выборки глобального потока по умолчанию составляет 8192
Режим команд	Режим глобальной конфигурации
Использование конфигурации	Эта команда используется для настройки глобальной частоты выборки потока sFlow, и выборка потока sFlow для всех интерфейсов использует эту частоту выборки

Настройка максимальной длины заголовка пакета, копируемого во время выборки потока

- Дополнительная конфигурация.
- Вы можете использовать команду **sflow flow max-header** для глобальной настройки длины заголовка пакета, копируемого во время выборки потока.
- Пользователи могут использовать эту команду для изменения информации о датаграмме, отправляемой коллектору sFlow. Например, если пользователя беспокоит заголовок IP, этот пользователь может задать длину 56 байт. Во время инкапсуляции образцов потока первые 56 байтов пакета образцов копируются в датаграмму sFlow.

Синтаксис команды	**sflow flow max-header** *length*
Описание параметров	*length*: максимальная длина копируемого заголовка пакета. Диапазон от 18 до 256
По умолчанию	По умолчанию длина заголовка пакета, копируемого во время выборки глобального потока, составляет 64 байта
Режим команд	Режим глобальной конфигурации

Использование конфигурации	Настройте максимальное количество байтов содержимого пакета, скопированного из заголовка исходного пакета. Скопированное содержимое записывается в сгенерированную выборку

Настройка интервала выборки

- Дополнительная конфигурация.
- Вы можете использовать команду **sflow counter interval** для настройки интервала выборки глобального счетчика.
- Включите интерфейс выборки счетчика, чтобы отправлять статистику по нему в коллектор sFlow с интервалом выборки.

Синтаксис команды	**sflow counter interval** *seconds*
Описание параметров	*seconds*: временной интервал. Диапазон составляет от 3 до 2 147 483 647. Измеряется в секундах
По умолчанию	Интервал выборки глобального счетчика по умолчанию составляет 30 секунд
Режим команд	Режим глобальной конфигурации
Использование конфигурации	Эта команда используется для настройки глобального интервала выборки счетчика sFlow, и выборка счетчика sFlow всех интерфейсов использует этот интервал выборки

Настройка исходного адреса sFlow

- Дополнительная конфигурация.
- Вы можете использовать источник sflow **{ address | interface }** для настройки исходного адреса sFlow исходящих пакетов.

Команда	**sflow source { address {***ip-address* **| ipv6** *ipv6-address* **}} | { interface {** *interface name* **| ipv6** *interface-name* **}}**
Описание параметров	**address**: настраивает исходный IP-адрес выходных пакетов sFlow. *ip-address*: IPv4-адрес источника sFlow. *ipv6-address*: IPv6-адрес источника sFlow. **interface**: настраивает исходный интерфейс выходных пакетов sFlow. *interface name*: исходный интерфейс sFlow (настроенный с IPv4-адресом). **ipv6** *interface-name*: исходный интерфейс sFlow (настроенный с адресом IPv6)
По умолчанию	По умолчанию адрес источника sFlow (sFlow Source) — это IP-адрес локального устройства, который используется для проверки связи с IP-адресом назначения

Режим команд	Режим глобальной конфигурации
Использование конфигурации	Эта команда используется для настройки исходного IP-адреса выходных пакетов. Если исходный интерфейс указан, первичный адрес интерфейса будет исходным IP-адресом выходных пакетов. Если исходный интерфейс не указан или IP-адрес исходного интерфейса недоступен, например, интерфейс отключен, будет использоваться исходный адрес по умолчанию

7.4.2.4. Метод проверки

- Проверьте, получена ли датаграмма sFlow с образцами потока на коллекторе sFlow.
- Используйте команду **show sflow** для отображения конфигурации sFlow и проверьте, согласуется ли отображаемая информация с конфигурацией.

7.4.2.5. Примеры конфигурации

Настройка дополнительных параметров sFlow

Сетевое окружение	• Установите частоту выборки потока на 4096 в режиме глобальной конфигурации. • Настройте длину заголовка пакета, копируемого во время выборки потока, на 128 байтов в режиме глобальной конфигурации. • Установите интервал выборки равным 10 в режиме глобальной конфигурации
Метод конфигурации	QTECH# configure terminal QTECH(config)# sflow sampling-rate 4096 QTECH(config)# sflow flow max-header 128 QTECH(config)# sflow counter interval 10
Сетевое окружение	• Сделать так, чтобы трафик проходил через интерфейс TenGigabitEthernet 0/1. • Проверьте, есть ли трафик на интерфейсе TenGigabitEthernet 0/1 на sFlow Collector 1. • Используйте команду **show sflow**, чтобы проверить, согласуются ли выходные данные команды с конфигурацией
Метод проверки	QTECH# show sflow sFlow datagram version 5 Global information: Agent IP: 10.10.10.10 sflow counter interval:10 sflow flow max-header:128

	sflow sampling-rate:4096 Collector information: ID IP Port Size VPN 1 192.168.2.100 6343 1400 2 NULL 0 1400 Port information Interface CID FID Enable TenGigabitEthernet 0/1 0 1 Y

7.5. Мониторинг

7.5.1. Отображение

Функция	Команда
Отображает конфигурацию sFlow	**show sflow**

8. НАСТРОЙКА NETCONF

8.1. Обзор

Протокол конфигурации сети (NETCONF) — это совершенно новый протокол на основе Extensible Markup Language (XML), предложенный рабочей группой NETCONF Целевой группы по разработке Интернета (IETF) в 2003 году. Его можно использовать для настройки устройств, извлечения параметров, мониторинг и управление. Этот протокол принимает режим связи клиент/сервер, в котором программа сервера протокола работает на устройстве, а программа клиента протокола работает на клиентах. Формат XML используется в пакетах этого протокола, включая все данные конфигурации и сообщения протокола. Протокол NETCONF состоит из четырех уровней: уровня содержимого, уровня операций, уровня удаленного вызова процедур (RPC) и транспортного уровня. Уровень контента представляет собой набор объектов управляемых данных, и на этом уровне хранятся данные конфигурации устройств. Уровень операций — это базовый примитивный набор операций, применяемый к RPC, например, <get>, <get-config>, <edit-config> и <delete-config>. Уровень RPC предоставляет простой механизм, не связанный с транспортными протоколами, и этот механизм определяет элементы некоторых сообщений обратной связи об ошибках. Транспортный уровень обеспечивает безопасный транспортный канал. Протокол NETCONF поддерживает Secure Shell (SSH) (обязательно), Simple Object Access Protocol (SOAP) и Block Extensible Exchange Protocol (BEEP).

Протоколы и стандарты

- RFC4741: протокол конфигурации NETCONF.
- RFC4742: использование протокола конфигурации NETCONF через Secure Shell (SSH).
- RFC4743: использование NETCONF по протоколу простого доступа к объектам (SOAP).
- RFC4744: использование протокола NETCONF по протоколу расширенного обмена блоками (BEEP).
- RFC5277: уведомления о событиях NETCONF.
- RFC5381: опыт реализации NETCONF через SOAP.
- RFC5539: NETCONF через безопасность транспортного уровня (TLS).
- RFC5717: RPC с частичной блокировкой для NETCONF.
- RFC6022: схема мониторинга NETCONF.
- RFC6241: протокол конфигурации сети.
- RFC6242: использование протокола конфигурации сети через Secure Shell.
- RFC6243: возможность использования значений по умолчанию для NETCONF.
- RFC6470: события уведомлений NETCONF.
- RFC6536: модель управления доступом NETCONF (NACM).
- RFC4741 и RFC4742 заменены на RFC6241 и RFC6242 соответственно.

8.2. Приложения

Приложение	Описание
Управление сетевыми устройствами NETCONF	Пользователи отправляют пакеты конфигурации NETCONF в формате XML на устройства с помощью программного обеспечения для управления сетью, установленного на Клиент NETCONF для настройки устройств и управления ими

8.2.1. Управление сетевыми устройствами NETCONF

8.2.1.1. Сценарий

Как показано на рисунке ниже, пользователи могут использовать программное обеспечение для управления сетью NETCONF для управления сетевыми устройствами и их мониторинга.

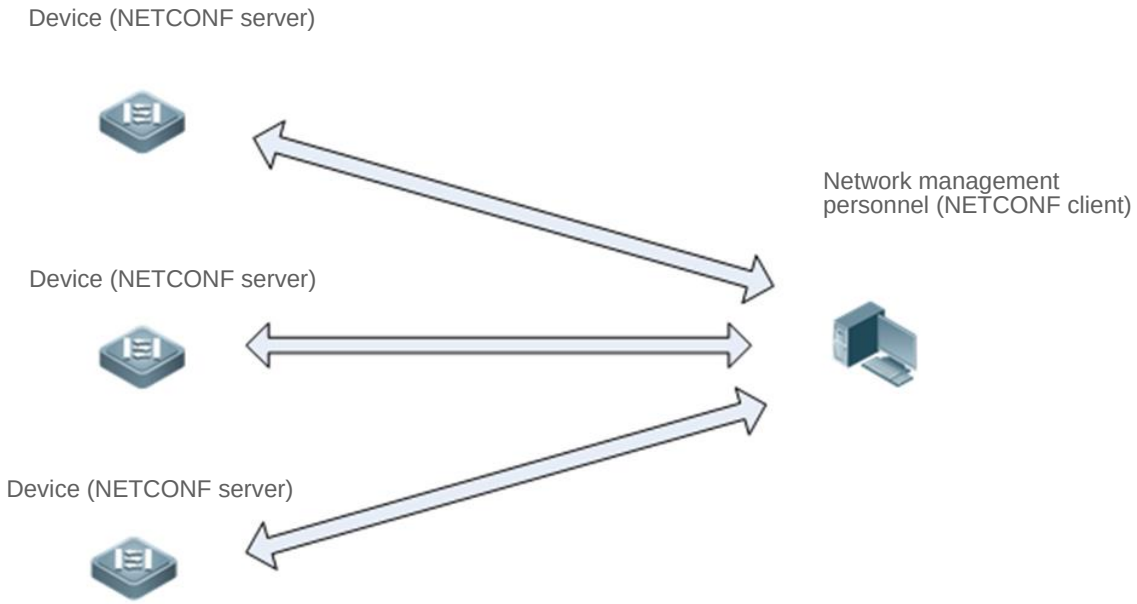


Рисунок 8-1.

8.2.1.2. Развертывание

Станция управления сетью и управляемые сетевые устройства связаны через сети. Протокол SSH должен работать как на программном обеспечении для управления сетью, так и на устройствах. На станции управления сетью с помощью программного обеспечения управления сетью NETCONF пользователи могут получить доступ к базам данных конфигурации и базам данных состояния на сетевых устройствах, получать уведомления о событиях, отправленные с сетевых устройств, а также управлять и контролировать сетевые устройства.

8.3. Функции

8.3.1. Базовые концепты

8.3.1.1. Общие условия

- RFC: удаленный вызов процедур.
- DM: модель данных.

8.3.1.2. Структура протокола

На рисунке ниже показана структура протокола NETCONF.

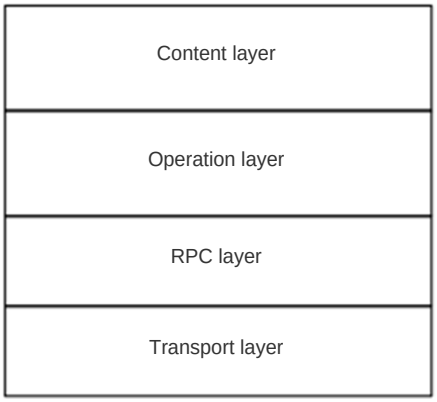


Рисунок 8-2. Структура протокола NETCONF

8.3.1.3. Сессионное соединение

- NETCONF через SSH

Сервер отслеживает порт 830. Перед использованием протокола NETCONF необходимо установить канал SSH. Установка канала SSH (подсистема SSH, называемая netconf) требует аутентификации пользователя и согласования ряда алгоритмов передачи (включая согласование ключей, алгоритм сжатия, алгоритм хеширования, алгоритм шифрования и алгоритм подписи).

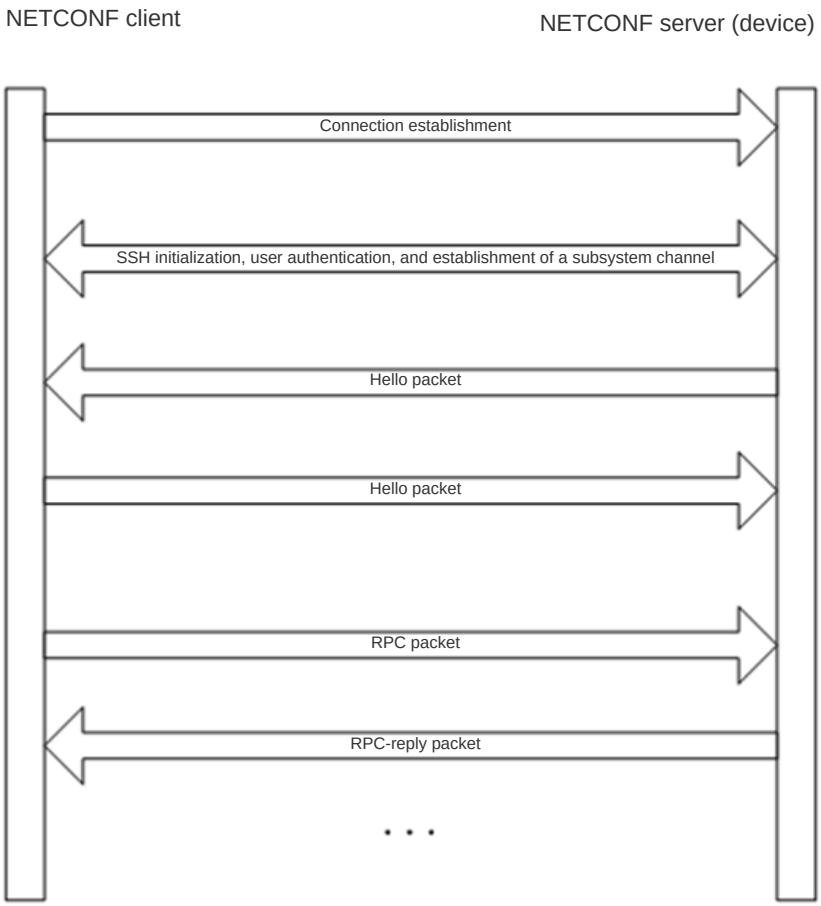


Рисунок 8-3. Пакеты, которыми обмениваются в сеансе NETCONF

8.3.1.4. Обмен наборами возможностей

Наборы возможностей должны быть обменены после того, как канал установлен. И сервер, и клиент предоставляют свои реализованные наборы возможностей и игнорируют возможности, которые не поняты или не реализованы. Каждый peer должен поддерживать как минимум базовые возможности протокола (urn:ietf:params:netconf:base:1.1). Если NETCONF-протокол совместим с более ранней версией протокола, peer должен поддерживать базовую возможность (urn:ietf:params:netconf:base:1.0) этой ранней версии.

Протокольные операции

Для операционного уровня NETCONF определены девять основных методов работы, а методы операций следующие: <get> и <get-config> — операции получения значения, <edit-config>, <copy-config> и <delete-config>. config> — операции настройки, <lock> и <unlock> — операции защиты от блокировки, предоставляемые в случае параллельных операций над критическими ресурсами устройства (файлами конфигурации), а <close-session> и <kill-session> — операции завершения сеанса.

- <get>: получает данные о состоянии и конфигурации устройства.
- <get-config>: получает данные конфигурации на основе узла фильтрации в запросе RPC.
- <edit-config>: настраивает устройство на основе предоставленного определения модели данных и атрибутов операции. Один важный атрибут **operation** можно настроить на **merge, replace, create, delete** или **remove**, а значение по умолчанию — **merge**.

- <copy-config>: скопирует конфигурационный файл, например, сорда аконфигурация-кандидат ваконфигурационный файл, копда аконфигурация запуска в текущую конфигурацию и напишитес аработающую конфигурацию в стартовую конфигурацию. Эти операции копирования требуютцелевые файлы для поддержкивозможность записи.
- <copy-config>: копирует файл конфигурации, например, копирует конфигурацию-кандидат в файл конфигурации, копирует конфигурацию запуска в текущую конфигурацию и записывает текущую конфигурацию в конфигурацию запуска. Для этих операций копирования необходимы целевые файлы, поддерживающие возможность записи.
- <delete-config>: удаляет файл конфигурации устройства. Запущенный файл конфигурации устройства не может быть удален.
- <lock>: обеспечивает защиту от блокировки файлов конфигурационных данных. Когда клиент получает доступ (или изменение) файла данных конфигурации устройства, другие клиенты или клиенты, не относящиеся к NETCONF (такие как SNMP или CLI-клиенты), не могут получить доступ (или изменить) файл данных конфигурации.
- <unlock>: разблокирует файл данных конфигурации.
- <close-session>: закрывает текущий сеанс, включая освобождение ресурсов, снятие блокировки и отключение. Когда выполняется эта операция, необходимо убедиться, что обработка текущей службы завершена и новый запрос не обрабатывается.
- <kill-session>: принудительно завершает сеанс (текущий сеанс не может быть завершен), включая освобождение ресурсов, снятие блокировки и разъединение. При выполнении этой операции текущая служба должна быть прекращена, а незавершенные службы должны быть возвращены в состояние, предшествующее обработке службы.

8.3.2. Обзор

Особенность	Описание
Обмен наборами возможностей	Сервер NETCONF и клиент взаимно отправляют наборы возможностей друг другу. Сервер (устройство) поддерживает NETCONF 1.0 и NETCONF 1.1
<get>	Клиент получает данные о конфигурации или состоянии устройства
<get-config>	Клиент получает данные конфигурации устройства
<edit-config>	Клиент изменяет данные конфигурации устройства
<copy-config>	Клиент копирует файл конфигурации на устройстве в другой файл конфигурации
<delete-config>	Клиент удаляет конфигурационный файл на устройстве
<close-session>	Клиент активно закрывает текущий сеанс NETCONF с устройством

Особенность	Описание
<lock>	Клиент блокирует файл конфигурации с устройства
<unlock>	Клиент разблокирует файл конфигурации с устройства

8.3.3. Обмен наборами возможностей

Клиент NETCONF и сервер NETCONF обмениваются своими наборами возможностей сразу после установления соединения. Они могут выполнять последующие операции с данными, только если они поддерживают ту же версию протокола NETCONF. Формат отправляемых пакетов следующий:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <capabilities>
         <capability>
               urn:ietf:params:netconf:base:1.1
         </capability>
         <capability>
               Capability set 1
         </capability>
         <capability>
               Capability set 2
         </capability>
   </capabilities>
   <session-id>Session ID</session-id>
</hello>
```

ПРИМЕЧАНИЕ: пакет обмена возможностями, отправленный от клиента к серверу, не может содержать идентификатор сеанса (<session-id>).

Пример обмена наборами возможностей на сервере:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <capabilities>
         <capability>urn:ietf:params:netconf:base:1.0</capability>
         <capability>urn:ietf:params:netconf:base:1.1</capability>
         <capability>urn:ietf:params:netconf:capability:writable-
running:1.0</capability>
         <capability>urn:ietf:params:xml:ns:yang:ietf-yang-types?module=ietf-
yangtypes&amp;revision=2013-07-15</capability>
         <capability>urn:rg:params:xml:ns:yang:rg-tacacs?module=rg-
tacacs&amp;revision=2016-10-25</capability>
         <capability>urn:rg:params:xml:ns:yang:rg-interfaces?module=rg-
interfaces&amp;revision=2016-10-25</capability>
```

<capability>urn:ietf:params:xml:ns:yang:ietf-inet-types?module=ietf-inettypes&revision=2010-09-24</capability>

<capability>urn:rg:params:xml:ns:yang:rg-openflow?module=rg-openflow&revision=2016-09-26</capability>

</capabilities>

<session-id>28</session-id>

</hello>

Пример обмена наборами возможностей на клиенте:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
  <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

8.3.4. <get>

Эта операция используется для получения данных конфигурации или состояния устройства.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
  <filter type="subtree">
        Configuration data (or state data) filtering rule
  </filter>
  </get-config>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
            Acquired configuration data (or state data)
  </data>
</rpc-reply>
```

Если ни одно из подмножеств данных состояния на устройстве не соответствует правилу фильтрации, устройство возвращает пустой узел данных, показанный ниже:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="message ID "
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
```

```
</rpc-reply>
```

8.3.5. <get-config>

Эта операция используется для получения данных конфигурации устройства. Он получает подмножества данных конфигурации на основе различных ответвлений правил фильтрации, но не может получить данные о состоянии устройства.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
  <rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <get-config>
          <source>
              <running/>
          </source>
          <filter type="subtree">
          Protocol filtering rules
              </filter>
      </get-config>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
  <rpc-reply message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
          Acquired configuration data
      </data>
</rpc-reply>
```

Если ни одно из подмножеств данных конфигурации на устройстве не соответствует правилам фильтрации, устройство возвращает пустой узел данных, показанный ниже:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc-reply>
```

8.3.6. <edit-config>

Эта операция используется для редактирования конфигурации на основе предоставленного определения модели данных и атрибутов операции. Пакеты edit-config содержат пять атрибутов операции, которые указаны в описании атрибута операции узла конфигурации в доставленных XML-пакетах. Пять атрибутов следующие:

merge: объединяет данные конфигурации в пакетах edit-config, которые содержат этот атрибут, в указанный файл конфигурации устройства (или базу данных). Если данные конфигурации не существуют, они создаются на основе доставленного контента.

replace: использует данные конфигурации в пакетах edit-config, которые содержат этот атрибут, для замены связанного узла данных конфигурации в указанном файле конфигурации устройства (или базе данных). Если данные конфигурации не существуют, они создаются на основе доставленного контента. Устройства QTECH временно не поддерживают эту операцию. Если такой атрибут доставлен, он рассматривается как атрибут слияния.

create: создает в указанном файле данных конфигурации (или базе данных) данные конфигурации в пакетах edit-config, которые содержат этот атрибут. Если данные конфигурации не существуют, они создаются на основе доставленного контента. Если данные конфигурации уже существуют, возвращается пакет rpc-error, а тег ошибки указывает, что данные уже существуют.

delete: удаляет данные конфигурации в пакетах edit-config, которые содержат этот атрибут, из указанного файла данных конфигурации (или базы данных). Если данные конфигурации уже существуют, они удаляются напрямую. Если данные конфигурации не существуют, возвращается пакет rpc-error, а тег ошибки указывает, что данные отсутствуют.

remove: удаляет данные конфигурации в пакетах edit-config, которые содержат этот атрибут, из указанного файла данных конфигурации (или базы данных). Если данные конфигурации уже существуют, они удаляются напрямую. Если данные конфигурации не существуют, эта операция игнорируется и возвращается ответ OK.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
      <target> <running/> </target>
          <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      Configuration data
          </config>
  </edit-config>
</rpc>
```

Если пакет не содержит узел error-option, значение этого узла по умолчанию равно **stop-on-error**, указывая на то, что, как только конфигурация узла в пакете неверна, последующая конфигурация в том же пакете останавливается и rpc-error возвращается. Если в пакете нет узла test-option, значением этого узла по умолчанию **является test-then-set**. Если пакет не содержит узел операции по умолчанию, значением этого узла по умолчанию является **merge**.

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="message ID "
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

Если пакет содержит узел error-option, формат обычно следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
```

```
<edit-config>
   <target> <running/> </target>
   <error-option>behavior option in the case of a configuration error</error-option>
   <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
         Configuration data
   </config>
</edit-config>
</rpc>
```

Узел error-option является узлом типа перечисления. Он может быть установлен в одно из следующих значений:

stop-on-error: немедленно останавливает текущую операцию редактирования конфигурации при возникновении первой ошибки. Это значение по умолчанию для error-option. Данные конфигурации перед ошибкой в текущем пакете конфигурации уже вступают в силу.

continue-on-error: продолжает обработку данных конфигурации, даже если возникает ошибка. Ошибки записываются, и после завершения всей обработки возвращается сообщение об ошибке (то есть для всех ошибок конфигурации возвращается rpc-error).

8.3.7. <copy-config>

Эта операция используется для синхронизации начальной конфигурации с текущей конфигурацией.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <copy-config>
         <target>
               <startup/>
         </target>
         <source>
               <running/>
         </source>
   </copy-config>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <ok/>
</rpc-reply>
```

8.3.8. <delete-config>

Эта операция используется для удаления начальной конфигурации устройства. Текущая конфигурация не может быть удалена.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <delete-config>
    <target>
      <startup/>
    </target>
  </delete-config>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

8.3.9. <close-session>

Эта операция используется для закрытия текущего сеанса, освобождения ресурсов и блокировок, и разрыва соединения.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <close-session/>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

8.3.10. <lock>

Согласно RFC6241, эта операция используется для блокировки базы данных конфигурации (файлов конфигурации) и предотвращения одновременного изменения файлов конфигурации устройства несколькими источниками (такими как CLI, SNMP и несколько одновременных сеансов NETCONF), чтобы избежать ненужных изменений конфигурации. Устройство упрощает эту операцию и может только предотвращать одновременные модификации (выполнение конфигурации) из нескольких сеансов NETCONF и обеспечивает безопасность модификации данных конфигурации.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <lock>
      <target>
          <running/>
      </target>
  </lock>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

8.3.11. <unlock>

Эта операция используется для разблокировки базы данных конфигурации (файлы конфигурации; здесь выполняется конфигурация на устройстве). <lock> и <unlock> являются парными операциями.

Формат пакетов, отправляемых клиентом, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <unlock>
      <target>
          <running/>
      </target>
  </unlock>
</rpc>
```

Формат пакетов, возвращаемых сервером, следующий:

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

8.4. Конфигурация

Настройте параметры, связанные с аутентификацией канала SSH, перед использованием NETCONF. Для настройки SSH см. Security Configuration/Настройка SSH.

Конфигурация	Описание и команда	
Настройка Candidate Capability NETCONF	(Опционально) Используется для настройки сервера NETCONF, чтобы он возвращал клиенту candidate capability при обмене возможностями с клиентом	
	netconf capability candidate	Включает candidate capability и подтвержденные возможности NETCONF
Настройка rollback capability NETCONF	(Опционально) Используется для настройки сервера NETCONF для обратной связи с клиентом о rollback-on-error capability при обмене возможностями с клиентом	
	netconf capability rollback	Включает rollback-on-error capability NETCONF
Настройка validate capability NETCONF	(Опционально) Используется для настройки сервера NETCONF для обратной связи с validate capability клиенту при обмене capability с клиентом	
	netconf capability validate	Включает validate capability NETCONF
Настройка функционала модуля YANG	(Опционально) Используется для настройки сервера NETCONF на то, чтобы он не передавал обратно атрибут функции клиенту при обмене capability с клиентом	
	netconf feature-disable	Отключает функционал NETCONF
Настройка уведомления многих версий (Multi-version) модуля YANG	(Опционально) Используется для настройки сервера для объявления всех версий всех поддерживаемых модулей YANG клиенту при обмене возможностями с клиентом	
	netconf yang multi-revision	Настраивает функции уведомления о многих версиях модуля YANG NETCONF

8.4.1. Настройка Candidate Capability NETCONF

8.4.1.1. Эффект конфигурации

Сервер NETCONF возвращает candidate capability и confirmed-commit capability при обмене capability с клиентом NETCONF (через пакеты Hello и пакеты capability).

8.4.1.2. Шаги настройки

Включение candidate capability и confirmed-commit capability NETCONF

Команда	**netconf capability candidate**
По умолчанию	Candidate capability и confirmed-commit capability NETCONF включены по умолчанию
Режим команд	Режим глобальной конфигурации

8.4.1.3. Пример конфигурации

Включение candidate capability и confirmed-commit capability NETCONF

Сценарий:

Рисунок 8-4.

Шаги настройки	Включите candidate capability и confirmed-commit capability NETCONF
NETCONF	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# netconf capability candidate QTECH(config)#

8.4.2. Настройка rollback capability NETCONF

8.4.2.1. Эффект конфигурации

Сервер NETCONF возвращает rollback capability при обмене capability с клиентом NETCONF (через пакеты Hello и пакеты capability).

8.4.2.2. Шаги настройки

Включение rollback capability NETCONF

Команда	**netconf capability rollback**
По умолчанию	Rollback capability NETCONF включена по умолчанию
Режим команд	Режим глобальной конфигурации

8.4.2.3. Пример конфигурации

Включение rollback capability NETCONF

Сценарий:

Рисунок 8-5.

Шаги настройки	Включите rollback capability NETCONF
NETCONF	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# netconf capability rollback QTECH(config)#

8.4.3. Настройка validate capability NETCONF

8.4.3.1. Эффект конфигурации

Сервер NETCONF возвращает validate capability при обмене capability с клиентом NETCONF (через пакеты Hello и пакеты capability).

8.4.3.2. Шаги настройки

Включение validate capability NETCONF

Команда	**netconf capability validate**
По умолчанию	Validate capability NETCONF включена по умолчанию
Режим команд	Режим глобальной конфигурации

8.4.3.3. Пример конфигурации

Включение validate capability NETCONF

Сценарий:

Рисунок 8-6.

Шаги настройки	Включите validate capability NETCONF
NETCONF	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# netconf capability validate QTECH(config)#

8.4.4. Настройка функционала модуля YANG

8.4.4.1. Эффект конфигурации

Сервер NETCONF не возвращает атрибут функции модуля YANG при обмене capability с клиентом NETCONF (через пакеты Hello и пакеты capability).

8.4.4.2. Шаги настройки

Отключение атрибута функции NETCONF

Команда	**netconf feature-disable**
По умолчанию	Атрибут функции NETCONF по умолчанию отключен
Режим команд	Режим глобальной конфигурации

8.4.5. Пример конфигурации

Отключение атрибута функции NETCONF

Сценарий:

Рисунок 8-7.

Шаги настройки	Отключите атрибут функции модуля YANG
NETCONF	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# netconf feature-disable QTECH(config)#

8.4.6. Настройка уведомления многих версий (Multi-version) модуля YANG

8.4.6.1. Эффект конфигурации

Сервер NETCONF объявляет все версии всех поддерживаемых модулей YANG на устройстве при обмене capability с клиентом NETCONF (через пакеты Hello).

8.4.6.2. Примечания

- Команда **netconf yang multi-revision** должна быть настроена до объявления пакета capability (пакета Hello) сервера NETCONF.
- Команда **no netconf yang multi-revision** должна быть настроена до объявления пакета capability (пакета Hello) сервера NETCONF, и один модуль YANG может объявить только свою текущую последнюю версию в пакете уведомления о capability.

8.4.6.3. Шаги настройки

Настройка уведомления многих версий модуля YANG

- Опционально.
- Эта конфигурация должна быть завершена до того, как сервер NETCONF объявит пакет capability (пакет Hello).

Команда	**netconf yang multi-revision**
По умолчанию	Уведомление ногих версий модуля YANG включено по умолчанию
Режим команд	Режим глобальной конфигурации

8.4.6.4. Пример конфигурации

Настройка уведомления многих версий модуля YANG

Сценарий:

Рисунок 8-8.

Шаги настройки	Настройте уведомление многих версий модуля YANG
NETCONF	QTECH# configure terminal Enter configuration commands, one per line. End with CNTL/Z. QTECH(config)# netconf yang multi-revision QTECH(config)#

9. НАСТРОЙКА GRPC

9.1. Обзор

Удаленный вызов процедур Google (gRPC) — это протокол удаленного вызова процедур, разработанный Google для разработки серверных программ. При вызове локальной процедуры сегмент кода выполняется на локальном устройстве для выполнения операции. Для RPC пользователь службы и поставщик могут находиться на разных компьютерах, и клиенту нужно только уведомить сервер о выполняемой операции. Этот запрос на операцию отправляется на сервер по сети, и сервер возвращает результат выполнения клиенту.

gRPC использует буферы протокола для реализации сериализации и десериализации данных и использует протокол передачи гипертекста версии 2 (HTTP/2) в качестве протокола передачи данных для повышения производительности.

Протоколы и стандарты

https://github.com/grpc/grpc

9.2. Приложения

Приложение	Описание
Топология One-to-one	Позволяет одному устройству передавать информацию gRPC на один сервер
Топология One-to-many	Позволяет одному устройству передавать информацию gRPC на несколько серверов

9.2.1. Топология One-to-one

9.2.1.1. Сценарий

Одно протестированное устройство подключено только к одному серверу и передает данные gRPC на сервер, как показано на Рисунке 9-1.

Рисунок 9-1. Топология One-to-one

S: проверенное устройство для сборагинформация RPC.

ПК: gRPC-сервер для приемагинформация RPC.

9.2.1.2. Развертывание

- Убедитесь, что PC1 доступен для S.
- Включите функцию gRPC на S.
- На S настройте события, которые будут передаваться на сервер.

9.2.2. Топология One-to-many

9.2.2.1. Сценарий

Одно протестированное устройство подключено к нескольким серверам и одновременно передает данные gRPC на серверы, как показано на Рисунке 9-2.

Рисунок 9-2. Топология One-to-many

S: проверенное устройство для сборагинформация RPC.

ПК: gRPCсервер для приемагинформация RPC.

9.2.2.2. Развертывание

- Убедитесь, что PC1 и PC2 доступны для S.
- Убедитесь, что IP-адреса PC1 и PC2 различаются.
- Включите функцию gRPC на S.
- На S настройте события, которые будут передаваться на сервер.

9.3. Функции

9.3.1. Базовые концепты

gRPC

gRPC — это высокопроизводительная межъязыковая среда RPC с открытым исходным кодом, разработанная Google. Он соответствует протоколам HTTP/2 и protobuf3.x.

Канал

Канал устанавливается между устройством и сервером.

Заглушка

Заглушка — это объект, созданный во время мультиплексирования канала.

ПРИМЕЧАНИЕ: Дополнительные сведения об условиях gRPC см. https://github.com/grpc/grpc.

9.3.2. Обзор

Особенность	Описание
Включение функции gRPC	Включает службу gRPC на устройстве. Устройство может служить gRPC-сервером для получения сообщений о событиях аутентификации и сбора данных или служить gRPC-клиентом для передачи gRPC-данных

Особенность	Описание
Поддержка функции входа и выхода gRPC	Поддерживает операции входа и выхода, инициированные сервером
Типы событий, поддерживаемые gRPC	Поддерживает события в реальном времени, периодические события и события сбора данных
Привязка указанного интерфейса для отправки пакетов gRPC	Привязывает указанный интерфейс для отправки пакетов
Предварительная настройка серверов и событий, на которые нужно подписаться	Предварительно настраивает серверы и события, на которые необходимо подписаться
Предварительная настройка информации о пользователях для входа на серверы gRPC	Предварительно настраивает информацию о пользователях, входящих в систему на серверах

9.3.3. Включение функции gRPC

Настройте gRPC, запустите службы клиента gRPC и сервера gRPC, настройте события для подписки для устройства и получите событие подписки, отправленное диспетчером NETCONF, чтобы завершить процесс создания отчетов о данных gRPC.

9.3.3.1. Принцип работы

Связь gRPC соответствует протоколу HTTP/2. Клиент инициирует запрос, и сервер отвечает на этот запрос, чтобы завершить один обмен данными. Запрос данных может быть инициирован только клиентом, и один обмен данными должен заканчиваться ответом сервера. См. рисунок ниже.

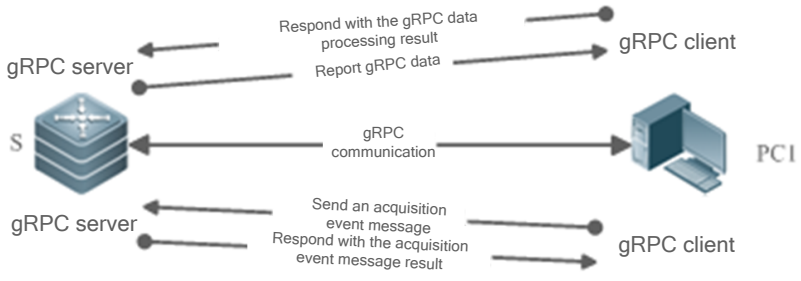


Рисунок 9-3. Связь gRPC

- Настройте функцию gRPC на устройстве S и запустите службы клиента gRPC и сервера gRPC.
- Устройство S получает сообщение о событии захвата от сервера и отвечает серверу результатом сообщения о событии захвата.

- Служба сервера gRPC, настроенная на устройстве S, ожидает подписанного события, отправленного диспетчером NETCONF.
- Служба клиента gRPC, настроенная на устройстве S, передает данные gRPC на сервер gRPC на основе подписанного события и ожидает ответа.

9.3.4. Поддержка функции входа и выхода gRPC

gRPC поддерживает операции входа и выхода, инициированные сервером.

9.3.4.1. Принцип работы

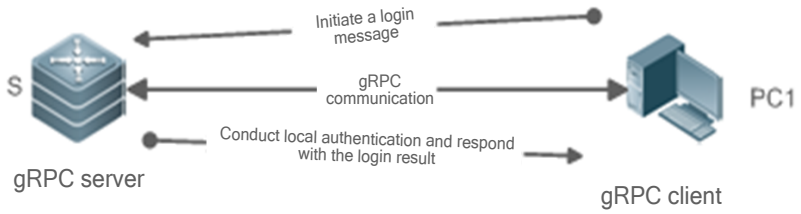


Рисунок 9-4. Вход в gRPC

- Настройте функцию gRPC на устройстве S и запустите службу сервера gRPC.
- Устройство S получает сообщение о входе в систему, инициированное сервером, проводит локальную аутентификацию и отвечает серверу с результатом входа в систему.
- Служба сервера gRPC, настроенная на устройстве S, получает только события получения, инициированные аутентифицированными серверами входа.

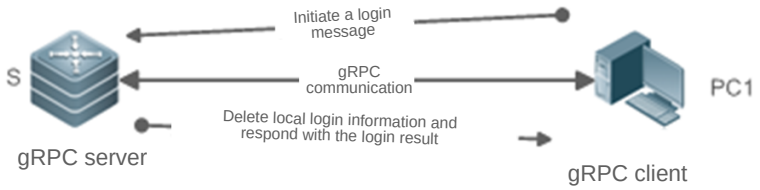


Рисунок 9-5. Выход из gRPC

- Настройте функцию gRPC на устройстве S и запустите службу сервера gRPC.
- Устройство S получает сообщение о выходе из системы, инициированное сервером, удаляет локальную совпадающую информацию для входа в систему и отвечает серверу с результатом выхода из системы.
- Служба сервера gRPC, настроенная на устройстве S, больше не получает события получения, инициированные отключенными серверами.

9.3.5. Типы событий, поддерживаемые gRPC

gRPC поддерживает три типа событий: события в реальном времени, периодические события и события сбора данных.

9.3.5.1. Принцип работы

События в реальном времени: События реального времени используют порог срабатывания события в качестве условия для сбора информации. Когда достигается порог срабатывания события, устройство собирает информацию и передает собранную информацию на сервер.

Периодические события. Информация об устройстве собирается на основе временного интервала. Когда наступает интервал, устройство собирает информацию и передает собранную информацию на сервер.

События сбора данных: событие сбора данных инициируется сервером для запроса данных за раз. После получения сообщения устройство собирает информацию и передает собранную информацию на сервер.

9.3.6. Привязка указанного интерфейса для отправки пакетов gRPC

9.3.6.1. Принцип работы

После того как диспетчер NETCONF отправляет на устройство команду gRPC для создания канала, устройство создает сокет перед отправкой пакетов на сервер, чтобы выполнить операцию проверки связи для проверки доступности пути. Устройство отправляет пакеты данных gRPC на сервер только при наличии пути. По умолчанию созданный сокет случайным образом привязывает исходный адрес порта устройства для отправки ping-пакетов. Когда сервер получает только пакеты с указанного исходного адреса, путь не может стать доступным после выполнения действия gRPC по умолчанию, и пакеты данных gRPC не могут быть загружены.

Поэтому привязывайте указанный исходный адрес при создании сокета, чтобы проверить доступность пути. Таким образом, пакеты данных gRPC могут быть загружены правильно.

9.3.7. Предварительная настройка серверов и событий, на которые нужно подписаться

9.3.7.1. Принцип работы

Устройство может заранее создавать серверы и события, на которые нужно подписаться, с помощью команд, или можно смоделировать контроллер для уведомления устройства о серверах и событиях, на которые нужно подписаться, через NETCONF.

Устройство может удалять серверы и события, на которые подписаны, с помощью команд, или можно смоделировать контроллер для уведомления устройства о серверах и событиях, на которые не подписаны, через NETCONF.

9.3.8. Предварительная настройка информации о пользователях для входа на серверы gRPC

9.3.8.1. Принцип работы

Устройство может заранее создавать пользователей для входа на аутентифицированные серверы с помощью команд, или сервер можно имитировать, чтобы инициировать запрос на вход, пройти аутентификацию и сохранить информацию о пользователях, вошедших в систему.

Устройство может удалять пользователей, вошедших в систему, на аутентифицированных серверах с помощью команд, или можно имитировать сервер, чтобы инициировать запрос на выход из системы и удалить информацию о пользователях, вошедших в систему.

9.4. Конфигурация

Конфигурация	Описание и команда	
Включение функции gRPC	(Обязательно) Используется для включения функции gRPC. Подписка и предоставление отчетов о данных поддерживаются только после включения функции gRPC	
	grpc	Создает режим gRPC и включает функцию gRPC
Настройка режима аутентификации и атрибутов аутентификации сервера AAA для функции входа и выхода gRPC	(Опционально) Используется для настройки режима аутентификации и атрибутов аутентификации сервера AAA для функции gRPC входа и выхода, когда требуется аутентификация при входе на сервер	
	authen login {**local** | **authentication** *mlist*}	Настраивает режим аутентификации для входа на сервер
	authen aaa-config {**retry** *times* | **timeout** *second*}	Настраивает количество повторных попыток входа и время ожидания для аутентификации сервера AAA
Настройка типов событий, поддерживаемых gRPC	(Обязательный) Используется для настройки указанных подписанных событий	
	subscr realtime enable	Включает все подписанные события gRPC в реальном времени
	subscr sample enable	Включает все подписанные периодические события gRPC
	subscr-sample-interval *interval*	Устанавливает интервал таймера для периодических событий
	subscr-realtime-interval {all *interval* **| realtime** *json-event interval***}**	Устанавливает время подавления для событий реального времени
Привязка указанного интерфейса для отправки пакетов gRPC	**subscr-source-interface** *interface type interface-number*	Привязывает указанный интерфейс для отправки пакетов gRPC

Конфигурация	Описание и команда	
Предварительная настройка серверов и событий, на которые нужно подписаться	**user-server** *ip-address port-id*	Предварительно настраивает серверы, которые могут подписываться на события
	type *json-event* **value** *value*	Предварительно настраивает события для подписки указанного сервера
Предварительная настройка информации о пользователях для входа на серверы gRPCc	**user-client** *id user-name ip-address*	Предварительно настраивает информацию о пользователях, вошедших в систему серверов gRPC

9.4.1. Включение функции gRPC

9.4.1.1. Эффект конфигурации

Включите службы клиента gRPC и сервера gRPC.

9.4.1.2. Примечания

- Обеспечьте сетевое подключение между устройством и сервером.
- Идентификатор порта локального сервера gRPC — 50 051.

9.4.1.3. Шаги настройки

Включение функции gRPC

- Обязательный.
- Включите функцию gRPC на каждом устройстве в режиме глобальной конфигурации, если не указано иное.

Команда	**grpc**
По умолчанию	Функция gRPC отключена по умолчанию
Режим команд	Режим глобальной конфигурации

Руководство по использованию	Используйте эту команду для создания экземпляра gRPC, включения функции gRPC и перехода в режим настройки процесса gRPC. Службы gRPC-клиента и gRPC-сервера создаются одновременно, когда включена функция gRPC. Клиентская служба gRPC загружает данные на сервер, в то время как серверная служба gRPC анализирует сообщения аутентификации и сообщения сбора данных, отправленные с сервера

9.4.1.4. Проверка

Запустите команду **show grpc status**, чтобы отобразить время работы после включения функции gRPC.

9.4.1.5. Пример конфигурации

ПРИМЕЧАНИЕ: описана только конфигурация, связанная с gRPC.

Включение функции gRPC

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

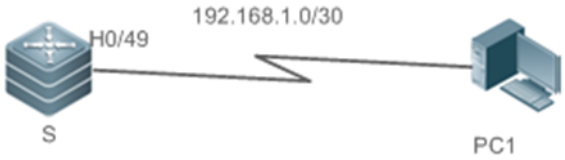


Рисунок 9-6. Топология One-to-one

Шаги настройки	Включите функцию gRPC. Настройте WAN-порт
S	S(config)# grpc S(config-grpc)# exit S(config)# interface HundredGigabitEthernet 0/49 S(config-if-HundredGigabitEthernet 0/49)# ip address 192.168.1.1 255.255.255.252
Проверка	Пропингуйте адрес сервера и проверьте, можно ли успешно пропинговать адрес. Проверьте, включена ли функция gRPC
S	S# show grpc status

9.4.2. Настройка режима аутентификации и атрибутов аутентификации сервера AAA для функции входа и выхода gRPC

9.4.2.1. Эффект конфигурации

Установите режим аутентификации функции входа и выхода gRPC в режим без аутентификации, локальную аутентификацию AAA или аутентификацию сервера AAA (время ожидания и количество повторных попыток можно настроить).

9.4.2.2. Примечания

- Для аутентификации сервера AAA необходимо включить режим новой модели.
- Режим без аутентификации не рекомендуется.
- Не рекомендуется изменять время ожидания и количество повторных попыток.

9.4.2.3. Шаги настройки

Настройка режима аутентификации функции входа и выхода gRPC

- Опциональный.
- Выполните эту настройку по мере необходимости.
- Запустите команду **authen login** на требуемом устройстве в режиме конфигурации процесса gRPC, если не указано иное.

Команда	**authen login {local | authentication** *mlist***}**
Описание параметров	**local**: использует локальную библиотеку имен пользователей для аутентификации. Это режим аутентификации по умолчанию. **authentication**: использует указанный список серверов AAA для аутентификации. *mlist*: указывает имя списка AAA
Режим команд по умолчанию	Локальный вход настроен по умолчанию, то есть настроена команда **authen login local**. Режим конфигурации процесса gRPC
Руководство по использованию	После получения запроса на вход с сервера устройство выбирает локальную аутентификацию AAA, аутентификацию сервера AAA или режим без аутентификации по мере необходимости. Когда аутентификация проходит успешно, устройство записывает информацию о пользователе для входа в систему, а именно IP-адрес и имя пользователя сервера. Устройство отвечает только на запросы событий получения, инициированные аутентифицированными серверами

Настройка атрибутов аутентификации сервера AAA для функции входа и выхода gRPC

- Опционально.
- Выполните эту настройку по мере необходимости.
- Не рекомендуется изменять эту конфигурацию на устройстве, если не указано иное.

Команда	**authen aaa-config {retry** *times* **| timeout** *second***}**
Описание параметров	**retry**: задает количество повторных попыток аутентификации сервера AAA. *times*: указывает количество повторных попыток. Значение колеблется от **1** до **100**
Описание параметров	**timeout**: устанавливает время ожидания для аутентификации сервера AAA. *second*: указывает время ожидания в секундах. Значение находится в диапазоне от 0 до 300, а значение 0 указывает, что аутентификация считается неудачной после получения сообщения об истечении времени ожидания сервера AAA
По умолчанию Режим команд	Количество повторных попыток по умолчанию равно 1, а время ожидания по умолчанию равно 4 секундам. Режим конфигурации процесса gRPC
Руководство по использованию	Используйте эту команду для настройки количества повторных попыток аутентификации и времени ожидания для режима аутентификации сервера AAA в случае входа на сервер. Не рекомендуется изменять количество повторных попыток по умолчанию и время ожидания. Большое количество повторных попыток или неправильное время ожидания может привести к блокировке AAA на 15 минут (вы можете запустить команду **clear aaa local user lockout all**, чтобы снять блокировку AAA)

9.4.2.4. Проверка

Запустите команду **show running**, чтобы проверить правильность конфигурации.

9.4.2.5. Пример конфигурации

ПРИМЕЧАНИЕ: описывается только конфигурация, связанная с gRPC.

Настройка режима аутентификации функции входа и выхода gRPC

Сценарий: Сетевая связь между устройством S и PC1 осуществляется в обычном режиме.

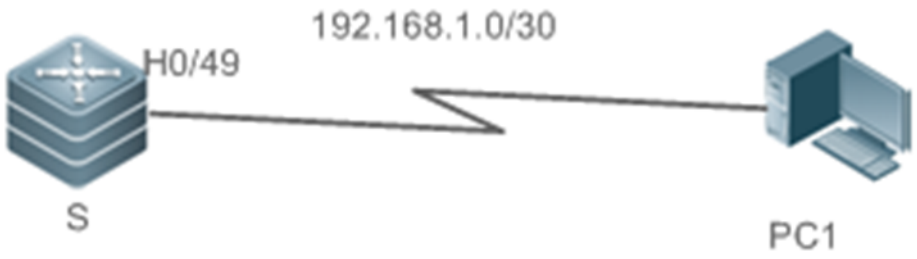


Рисунок 9-7. Топология One-to-one

Шаги настройки	Включите функцию gRPC. Настройте режим новой модели аутентификации AAA и списка mlist с именем test
S	S(config)# grpc S(config-grpc)# authen login authentication test
Проверка	Проверьте, правильно ли сохранена конфигурация. Проверьте, можно ли успешно пропинговать устройство с ПК-клиента. Проверьте, может ли ПК-клиент проводить аутентификацию и делать записи
S	S# show running S# show grpc client

9.4.3. Настройка типов событий, поддерживаемых gRPC

9.4.3.1. Эффект конфигурации

- Включить все подписанные события реального времени устройства.
- Включить все подписанные периодические события устройства.
- Измените время таймера для периодических событий.

9.4.4. Примечания

События, на которые подписан сервер, вступают в силу только после того, как указанные события с подпиской настроены на устройстве.

9.4.4.1. Шаги настройки

Включение подписки на события устройства

- Обязательный.
- Запустите команду **subscr realtime enable**, чтобы включить все подписанные события реального времени устройства.
- Запустите команду **subscr sample enable**, чтобы включить все подписанные периодические события устройства.
- Запустите команду **show grpc channel [counter]** для отображения событий реального времени/периодических событий, подписанных сервером, или для отображения статистики.

Команда	**subscr [realtime | sample] enable**
Описание параметров	**realtime**: указывает подписанные события в реальном времени. **sample**: указывает на подписанные периодические события
По умолчанию	Подписка на события в реальном времени/периодические события отключена по умолчанию

Режим команд	Режим конфигурации процесса gRPC
Руководство по использованию	После настройки событий, на которые нужно подписаться, процесс gRPC ожидает, пока диспетчер NETCONF отправит подписки на событие. Когда полученное сообщение о подписке совпадает с локальным событием, требующим подписки, процесс gRPC включает функцию отправки данных gRPC о событии на сервер. После того, как диспетчер NETCONF отправляет отказ от подписки на событие, если полученное сообщение об отказе от подписки совпадает с локальным событием, требующим подписки, процесс gRPC отключает функцию отправки данных gRPC о событии на сервер. Если процесс gRPC не настраивает подписки на событие, процесс gRPC не выполняет никакой обработки при получении подписки на события или отказа от подписки от диспетчера NETCONF

Настройка интервала таймера для периодических событий

- Опционально.
- Выполните эту настройку по мере необходимости.
- Запустите команду **subscr-sample-interval** на требуемом устройстве в режиме конфигурации процесса gRPC, чтобы изменить интервал таймера для периодических событий, если не указано иное.

Команда	**subscr-sample-interval** *interval*
Описание параметров	*interval*: указывает локально настроенный интервал для отчетов о периодических событиях в секундах. Значение варьируется от 1 до 65 535, а значение по умолчанию равно 10
По умолчанию	Интервал таймера по умолчанию для периодических событий используется по умолчанию
Режим конфигурации	Режим конфигурации процесса gRPC
Руководство по использованию	После того, как подписанное периодическое событие устройства включено и NETCONF manager отправляет подписанное периодическое событие, процесс gRPC запускает таймер периодического события и отправляет данные gRPC на сервер, который подписывается на событие. Когда периодическое событие, отправляемое NETCONF manager, не содержит временного интервала, интервал таймера определяется командой **subscr-sample-interval**. Если периодическое событие, отправляемое NETCONF manager, содержит интервал таймера, этот интервал таймера имеет преимущественную силу

Настройка времени подавления для событий реального времени

- Опционально.
- Выполните эту настройку по мере необходимости.

- Запустите команду **subscr-realtime-interval** на требуемом устройстве в режиме конфигурации процесса gRPC, чтобы изменить время подавления событий в реальном времени, если не указано иное.

Команда	**subscr-realtime-interval {all** *interval* **| realtime** *json-event interval***}**
Описание параметров	**all**: указывает, что конфигурация влияет на все события в реальном времени. **realtime**: указывает, что конфигурация вступает в силу при определенном событии реального времени. *json-event*: указывает тип настроенного события в реальном времени. *interval*: задает интервал подавления для предоставления данных о событиях реального времени в миллисекундах. Значение варьируется от 1 до 1 000 000, и события реального времени по умолчанию не подавляются
По умолчанию Режим конфигурации	События в реальном времени не подавляются по умолчанию. Режим конфигурации процесса gRPC
Руководство по использованию	После того, как устройство активирует подписанное событие реального времени, если срабатывает пороговое значение события, генерируются пакеты реального времени и отправляются на сервер, который подписывается на событие. Когда пороговое значение срабатывает часто, за короткий промежуток времени генерируется и отправляется на сервер большое количество пакетов. Данные в этих пакетах могут быть одинаковыми, но обработка этих пакетов значительно увеличивает нагрузку на устройство и сервер. Чтобы предотвратить этот случай, запустите команду **subscr-real time-interval** для подавления генерации новых пакетов для событий реального времени в течение определенного периода времени

9.4.4.2. Проверка

- Запустите команду **show grpc subscr realtime**, чтобы отобразить подписанные события в реальном времени.
- Запустите команду **show grpc subscr sample**, чтобы отобразить подписанные периодические события.
- Запустите команду **show grpc channel [counter]**, чтобы отобразить IP-адрес, идентификатор порта и подписанные события сервера или отобразить различную статистику.

9.4.4.3. Пример конфигурации

Включение подписки на события в реальном времени устройства

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

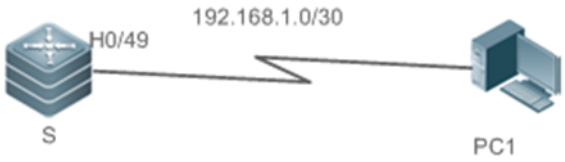


Рисунок 9-8. Топология One-to-one

Шаги настройки	• Включите функцию gRPC (опущено). • Установите событие реального времени изменения конфигурации CLI, на которые нужно подписаться. • Менеджер NETCONF подписывается на событие изменения конфигурации CLI в реальном времени
S	S(config)# grpc S(config-grpc)# subscr realtime enable
Проверка	Запустите команду **show grpc subscr realtime**, чтобы отобразить количество серверов, которые подписались на событие в реальном времени изменения конфигурации CLI. Запустите команду **show grpc channel [counter]**, чтобы отобразить IP-адреса, идентификаторы портов и подписанные события серверов или различную статистику
S	S# show grpc subscr realtime S# show grpc channel counter

Включение подписки на периодические события устройства

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

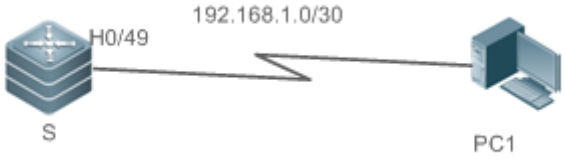


Рисунок 9-9. Топология One-to-one

Шаги настройки	• Включите функцию gRPC (опущено). • Настройте периодическое событие DCB PFC для подписки. • Менеджер NETCONF подписывается на периодическое событие DCB PFC

S	S(config)# grpc S(config-grpc)# subscr sample enable
Проверка	Запустите команду **show grpc subscr sample**, чтобы отобразить количество серверов, которые подписаны на периодическое событие DCB PFC. Запустите команду **show grpc channel [counter]**, чтобы отобразить IP-адреса, идентификаторы портов и подписанные события серверов или различную статистику
S	S# show grpc subscr sample S# show grpc channel counter

Настройка интервала таймера для периодических событий

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

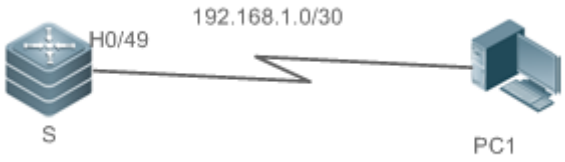


Рисунок 9-10. Топология One-to-one

Шаги настройки	• Включите функцию gRPC (опущено). • Установите интервал для периодического получения подписанного периодического события на 10 секунд
S	S(config)# grpc S(config-grpc)# subscr-sample-interval 10
Проверка	Запустите примерную команду show grpc subscr, чтобы отобразить интервал таймера всех подписанных периодических событий
S	S# show grpc subscr sample

Настройка времени подавления для событий реального времени

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

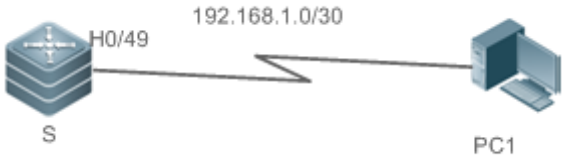


Рисунок 9-11. Топология One-to-one

Шаги настройки	• Включите функцию gRPC (опущено). • Установите время подавления на 500 мс для всех подписанных событий в реальном времени
S	S(config)# grpc S(config-grpc)# subscr-realtime-interval all 500
Проверка	Запустите команду **show grpc subscr realtime**, чтобы отобразить время подавления всех подписанных событий в реальном времени
S	S# show grpc subscr realtime

9.4.5. Привязка указанного интерфейса для отправки пакетов gRPC

9.4.5.1. Эффект конфигурации

gRPC использует IP-адрес указанного интерфейса для отправки пакетов.

9.4.5.2. Примечания

- Связанный интерфейс должен быть включен.
- Для связанного интерфейса необходимо настроить IP-адрес.

9.4.5.3. Шаги настройки

Привязка указанного интерфейса для отправки пакетов gRPC

- Опционально.
- Выполните эту настройку по мере необходимости.
- Запустите команду **subscr-source-interface** на требуемом устройстве в режиме настройки процесса gRPC, если не указано иное.

9.4.5.4. Проверка

Запустите команду **show running**, чтобы проверить правильность конфигурации.

9.4.5.5. Связанные команды

Привязка указанного интерфейса для отправки пакетов gRPC

Команда	**subscr-source-interface** *interface-type interface-number*
Описание параметров	*interface-type interface-number*: указывает имя интерфейса
По умолчанию Режим команд	gRPC случайным образом привязывает исходный адрес для отправки пакетов по умолчанию. Режим конфигурации процесса gRPC
Руководство по использованию	Действие gRPC по созданию канала по умолчанию заключается в случайной привязке адреса источника для отправки пакетов. Когда сервер получает пакеты только с указанного адреса источника, действие gRPC по умолчанию не может соответствовать требованиям приложения. В этом случае запустите команду **subscr source-interface**, чтобы указать адрес источника для отправки пакетов

9.4.5.6. Пример конфигурации

ПРИМЕЧАНИЕ: описывается только конфигурация, связанная с gRPC.

Привязка указанного интерфейса для отправки пакетов gRPC

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

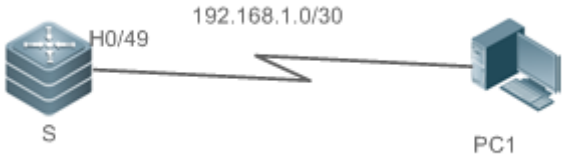


Рисунок 9-12. Топология One-to-one

Шаги настройки	Включите функцию gRPC. Настройте WAN-порт
S	S(config)# interface HundredGigabitEthernet 0/49 S(config-if-HundredGigabitEthernet 0/49)# ip address 192.168.1.1 255.255.255.252 S(config-if-HundredGigabitEthernet 0/49)# exit S(config)# grpc S(config-grpc)# subscr-source-interface HundredGigabitEthernet 0/49

Проверка	Проверьте, правильно ли сохранена конфигурация. Пропингуйте адрес сервера и проверьте, можно ли успешно пропинговать адрес. Проверьте, могут ли устройство и сервер правильно взаимодействовать друг с другом
S	S# show running S# show grpc channel

9.4.6. Предварительная настройка серверов и событий, на которые нужно подписаться

9.4.6.1. Эффект конфигурации

После предварительной настройки серверов и событий, подлежащих подписке, на серверы можно отправлять отчеты о связанных событиях gRPC.

9.4.6.2. Примечания

- Адрес и идентификатор порта сервера должны быть действительными.
- События и параметры для подписки должны быть правильными и действующими.

9.4.6.3. Шаги настройки

Предварительная настройка сервера, который может подписываться на события

- Обязательный.

Команда	**user-server** *ip-address port-id*
Описание параметров	*ip-address*: указывает IPv4-адрес сервера. *port-id*: указывает идентификатор порта сервера
Режим команд	Режим конфигурации процесса gRPC
Руководство по использованию	Используйте эту команду для предварительного создания указанного канала сервера и переключения на Режим подписки сервера gRPC. В этом режиме можно настроить события канала, на которые нужно подписаться. Устройство может заранее создавать серверы и события, на которые нужно подписаться, с помощью команд, или можно смоделировать контроллер для уведомления устройства о серверах и событиях, на которые нужно подписаться, через NETCONF. Устройство может удалять серверы и события, на которые подписаны, с помощью команд, или можно смоделировать контроллер для уведомления устройства о серверах и событиях, на которые не подписаны, через NETCONF

Предварительная настройка событий, на которые нужно подписаться

- Обязательный.

Команда	**type** *json-event* **value** *value*
Описание параметров	*json-event*: указывает тип события. Подробнее см. в выводе команды **show grpc subscr | include json**
Описание параметров	*value*: настраивает значение параметра, т. е. пороговое значение для событий в реальном времени и временной интервал для периодических событий
Режим команд	Режим подписки сервера gRPC
Руководство по использованию	Настройте события и параметры для подписки на канал, которые должны соответствовать конфигурации в NETCONF

9.4.6.4. Проверка

- Запустите команду **show running**, чтобы проверить правильность конфигурации.
- Запустите команду **show grpc channel**, чтобы проверить правильность серверов и событий, подлежащих подписке.

9.4.6.5. Пример конфигурации

ПРИМЕЧАНИЕ: описывается только конфигурация, связанная с gRPC.

Предварительная настройка серверов и событий, на которые нужно подписаться

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

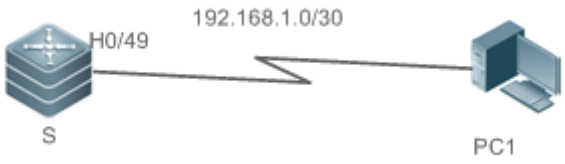


Рисунок 9-13. Топология One-to-one

Шаги настройки	Включите функцию gRPC. Настройте канал. Настройте тип подписки
S	S(config)# grpc S(config-grpc)# user-server 192.168.0.1 12345 S(config-grpc-us)# type 0x10000000 value 10

Проверка	Проверьте, правильно ли сохранена конфигурация. Пропингуйте адрес сервера и проверьте, можно ли успешно пропинговать адрес. Проверьте, могут ли устройство и сервер правильно взаимодействовать друг с другом
S	S# show running S# show grpc channel

9.4.6.6. Распространенные ошибки

Пороговое значение для событий в реальном времени находится в диапазоне от –1 до 100, временной интервал для периодических событий находится в диапазоне от –1 до 65 535, и необходимо использовать существующий тип. В противном случае конфигурация не вступает в силу и не сохраняется.

9.4.7. Предварительная настройка информации о пользователях для входа на серверы gRPC

9.4.7.1. Эффект конфигурации

После того, как информация о пользователе для входа на сервер gRPC предварительно настроена, информация может быть правильно получена для запросов событий сбора анных, инициированных указанным сервером gRPC.

9.4.7.2. Примечания

- Адрес сервера должен быть действительным.
- Идентификатор пользователя, вошедшего в систему, должен быть уникальным.

9.4.7.3. Связанные команды

Предварительная настройка информации о пользователях входа на сервер gRPC

- Обязательный.

Команда	**user-client** *id user-name ip-address*
Описание параметров	*id*: указывает идентификатор логина пользователя. *user-name*: указывает имя пользователя (не связанное с библиотекой AAA; может быть не зарегистрированным пользователем). *ip-address*: указывает разрешенный адрес
Режим команд	Режим конфигурации процесса gRPC
Руководство по использованию	Устройство может предварительно создавать пользователей для входа на аутентифицированные серверы с помощью команд, или сервер может быть смоделирован для инициирования запроса на вход,

	прохождения аутентификации и сохранения информации о пользователях, вошедших в систему. Устройство может удалять пользователей, вошедших в систему с аутентифицированных серверов, с помощью команд, или сервер может быть смоделирован для инициирования запроса на выход из системы и удаления информации о пользователях, вошедших в систему

9.4.7.4. Проверка

- Запустите команду **show running**, чтобы проверить правильность конфигурации.
- Запустите команду **show grpc client**, чтобы отобразить информацию о пользователях, вошедших в систему.

9.4.7.5. Пример конфигурации

ПРИМЕЧАНИЕ: описывается только конфигурация, связанная с gRPC.

Предварительная настройка информации о пользователях входа на сервер gRPC

Сценарий: сетевая связь между устройством S и PC1 работает нормально.

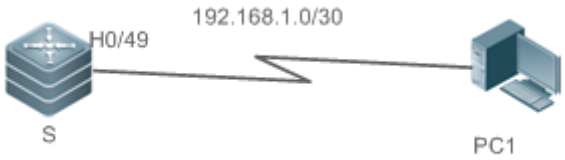


Рисунок 9-14. Топология One-to-one

Шаги настройки	Включите функцию gRPC. Настройте информацию о пользователе для входа на указанный сервер
S	S(config)# grpc S(config-grpc)# user-client 12345 test-user 192.168.0.1
Проверка	Проверьте, правильно ли сохранена конфигурация. Пропингуйте адрес сервера и проверьте, можно ли успешно пропинговать адрес. Проверьте, можно ли получить информацию для запроса события сбора данных, инициированного сервером
S	S# show running S# show grpc client

9.5. Мониторинг

9.5.1. Очистка

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

Описание	Команда
Очищает статистику сервера, который может подписываться на события gRPC	**clear grpc channel** [*ip-address port-id*] [**counter**]
Очищает данные о периодических событиях gRPC и событиях реального времени	**clear grpc subscr** [**sample**] [**counter**]

9.5.2. Отображение

Описание	Команда
Отображает IP-адрес, идентификатор порта и подписанные события сервера или различные статистические данные	**show grpc channel** [**counter**]
Отображает информацию о пользователях, вошедших в систему на серверах gRPC	**show grpc client**
Отображает текущее состояние gRPC	**show grpc status**
Отображает статусы и статистику подписанных событий на устройстве	**show grpc subscr** [**realtime | sample**]

9.5.3. Отладка

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

Описание	Команда
Отладка функции gRPC	**debug grpc { all | event }**

10. ОБЩАЯ ИНФОРМАЦИЯ

10.1. Гарантия и сервис

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

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

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

10.2. Техническая поддержка

Если вам необходимо содействие в вопросах, касающихся нашего оборудования, то можете воспользоваться нашей автоматизированной системой запросов технического сервис-центра helpdesk.qtech.ru.

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

Центральный офис +7 (495) 477-81-18

10.3. Электронная версия документа

Дата публикации 26.12.2024

https://files.qtech.ru/upload/switchers/QSW-6910/QSW-6910_network_manage_config_guide.pdf