16/24-портовый PoE-коммутатор

16/24-портовый PoE-коммутатор

Руководство по настройке через веб-интерфейс

Необходимо внимательно прочитать следующие предупреждения по технике безопасности и предостережения, прежде чем приступать к использованию устройства, чтобы избежать повреждений и потерь.

Внимание!

- Не помещайте устройство в места, подверженные воздействию копоти, пара или пыли, чтобы избежать возгорания или поражения электрическим током.
- Не устанавливайте устройство в местах, подверженных воздействию солнечных лучей или высокой температуры.
- Нагревание устройства может привести к пожару.
- Не подвергайте устройство воздействию влажной среды, чтобы не произошло возгорания.
- Для обеспечения безопасности при нагрузке или землетрясении устройство должно быть установлено на твердой плоской поверхности. Это необходимо, чтобы устройство не вышло из строя и не перевернулось.
- Не кладите устройство на ковер или одеяло.
- Не закрывайте вентиляционное отверстие устройства и не ограничивайте вентиляцию вокруг него. В противном случае устройство может нагреться и стать причиной пожара.
- Не кладите на устройство никаких предметов.
- Не разбирайте устройство без профессионального инструктажа.

Предупреждение.

- Соблюдайте правила эксплуатации аккумулятора, чтобы избежать пожара, взрыва и других рисков.
- Замените неработоспособный аккумулятор на аккумулятор того же типа.
- Не подключайтесь к электрическим сетям, отличным от указанных. Следуйте инструкциям, чтобы избежать возгорания или поражения электрическим током.

Важное объявление.

- Данное руководство предназначено только для справки.
- Все проектные решения и программы могут меняться без предварительного письменного оповещения.
- Всегда следуйте инструкциям, приведенным в руководстве. Компания-производитель не несет ответственности за отказы или сбои в работе устройства, наступившие в результате несанкционированных действий по модификации или ремонту системы.
- Другие торговые марки и зарегистрированные торговые марки, упоминаемые в данном документе, являются собственностью соответствующих владельцев.
- Если вы нашли неточность или противоречие, см. наши последние разъяснения.
- Для получения дополнительной информации приглашаем посетить наш веб-сайт.

Содержание

1 Общие сведения

1.1. Введение

Устройство предусматривает 16/24 порта PoE Ethernet 10/100 Мбит/с и 2 Combo uplink-порта 1000 Мбит/с, поддерживает сетевое управление 2-го уровня и управление PoE через веб-интерфейс, что помогает реализовать высокоскоростную передачу данных. Оно широко применяется для таких задач, как охранное видеонаблюдение, управление сетью и так далее.

1.2. Особенности устройства

- Предоставляет управление сетью на уровне 2 через веб-интерфейс.
- Поддерживает передачу данных на расстояние до 250 м.
- Поддерживает два Combo порта 1000 Мбит/с.
- Поддерживает 16/24 самонастраивающихся RJ45 порта 10/100 Мбит/с.
- Соответствует стандартам IEEE802.3, IEEE802.3u, IEEE802.3ab/z и IEEE802.3X.
- Поддерживает стандарт 802.1Q VLAN (порты Access/Trunk/Hybrid).
- Автоматическое внесение/удаление MAC-адресов, емкость таблицы маршрутизации — 4 тысячи MAC-адресов.
- IEEE802.3X полнодуплексное управление потоком и управление потоком методом обратного давления в полудуплексном режиме.
- Поддерживает подачу питания 100—240 В пост. тока.
- Соответствует стандартам IEEE802.3af и IEEE802.3at, порты 1 и 2 поддерживают Hi-PoE 60 Вт.
- Поддерживает управления энергопотреблением PoE.
- Поддерживает управление сетью SNMP V1/V2/V3.
- Поддерживает протокол закольцованной сети STP/RSTP.
- Поддерживает ручную агрегацию и статический LACP.
- Поддерживает зеркалирование «многие к одному».
- Поддерживает привязку MAC-адреса к порту.
- Отличная защита от короткого замыкания.
- Защита от молнии до уровня 4.

2 Конструкция устройства

2.1. Конструкция

2.1.1. Передняя панель

Рисунок 2-1
См. таблицу 2-1 для описания передней панели

№	Параметр	Примечание
1	Порт RJ45	Порт Ethernet, поддерживает 10/100 Мбит/с с автосогласованием
2	Combo порт	Порт Ethernet, поддерживает 10/100/1000 Мбит/с с автонастойкой, оптоволоконный порт поддерживает 1000 Мбит/с
3	Кнопка сброса	Нажмите и удерживайте кнопку, чтобы сбросить настройки устройства и восстановить конфигурацию по умолчанию.
4	Консольный последовательный порт	Отладочный порт устройства
5	Использование питания через PoE	Отображение текущего энергопотребления
6	Исходящая линия связи	Текущий статус линии порта и статус PoE.
7	Combo порт	Combo порт отображает link/act
8	Система	Статус системы. Когда устройство загружается, индикатор быстро мигает. Когда устройство работает правильно, индикатор мигает медленно.
9	Питание	Состояние питания устройства.

Таблица 2-1

2.1.2. Задняя панель

Рисунок 2-2

См. таблицу 2-2 для описания задней панели

№	Параметр	Примечание
1	Выключатель питания	Включение и выключение устройства управления
2	Входная мощность	Поддерживает переменный ток 100—240 В
3	Клемма заземления	Провод заземления

Таблица 2-2

3 Вход в систему управления коммутатором

3.1. Вход в систему управления коммутатором

Перед настройкой коммутатора необходимо сначала войти в систему. Затем пользователь сможет интуитивно управлять Ethernet-коммутатором серии PFS42 и поддерживать его через веб-интерфейс управления сетью.

Рисунок 3-1

Получить доступ к коммутатору можно через веб-браузер, убедившись, что ваш компьютер подключен к сети, где находится коммутатор. При первом использовании коммутатора необходимо задать пароль пользователю **admin** на веб-интерфейсе.

1 Измените IP-адрес и маску подсети сетевого адаптера вашего компьютера на 192.168.1.50 и 255.255.255.0 соответственно.

2 Откройте веб-браузер, введите 192.168.1.110 в адресной строке. Обратите внимание, что 192.168.1.110 является адресом управления по умолчанию для коммутатора.

3 После того как будет задан пароль для пользователя **admin**, в браузере отобразится интерфейс системы управления коммутатором.

3.2. Вводные положения о веб-интерфейсе

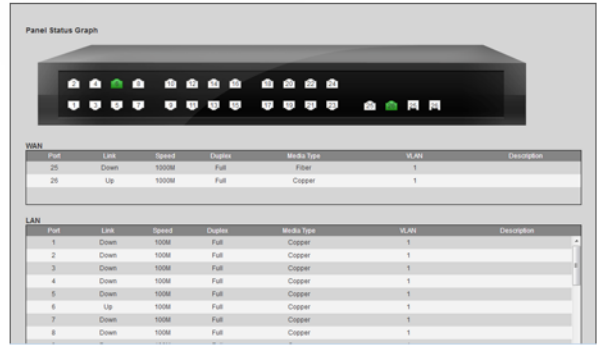
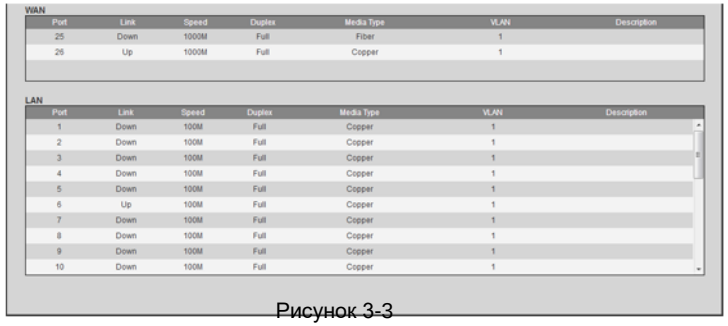


Рисунок 3-2

Как показано на рисунке 3-2, весь веб-интерфейс системы управления разделен на несколько частей, которые включают раздел, отображающий информацию об устройстве, панель навигации, раздел конфигурации и т. д.

3.2.1. Раздел информации о портах

На рисунке 3-3 показано, что экран с информацией о портах разделен на разделы, отображающие состояния портов WAN и состояние портов LAN. Показаны текущее состояние связи порта, скорость, дуплексный режим и т. д.



WAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
25	Down	1000M	Full	Fiber	1	
26	Up	1000M	Full	Copper	1	

LAN

Port	Link	Speed	Duplex	Media Type	VLAN	Description
1	Down	100M	Full	Copper	1	
2	Down	100M	Full	Copper	1	
3	Down	100M	Full	Copper	1	
4	Down	100M	Full	Copper	1	
5	Down	100M	Full	Copper	1	
6	Up	100M	Full	Copper	1	
7	Down	100M	Full	Copper	1	
8	Down	100M	Full	Copper	1	
9	Down	100M	Full	Copper	1	
10	Down	100M	Full	Copper	1	

Рисунок 3-3

3.2.2. Панель навигации

Панель навигации управляет теми параметрами, которые отображаются в разделе конфигурации. Содержимое панели навигации отображается в виде списка. Оно делится на несколько категорий. Если необходимо настроить какой-либо элемент, сначала щелкните название группы. В развернутом списке щелкните подпункт. Например, необходимо проверить поток текущего порта. Сначала нажмите Port Management («Управление портами»), а затем Port Statistics («Статистика портов»), см. рисунок 3-4 с более подробной информацией.

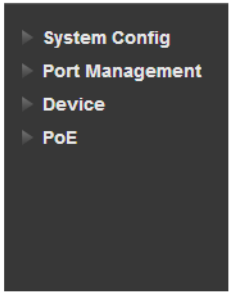


Рисунок 3-4

3.2.3. Раздел отображения конфигурации

В разделе конфигурации отобразится содержимое, которое выбрано на панели навигации. В нем можно включить и отключить функции, настроить и изменить параметры.
Четыре конфигурационных модуля будут рассмотрены в следующих четырех главах, а именно: конфигурация системы, управление портами, управление устройствами и PoE.

4 Конфигурация системы

4.1. Обзор конфигурации системы

Нажмите System Info («Информация о системе»), отобразится список, показанный на рисунке 4-1.

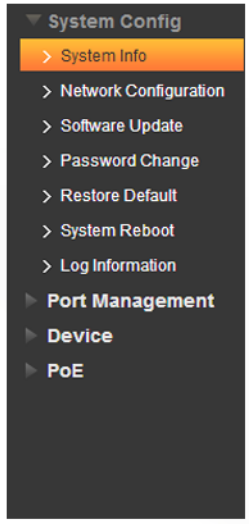


Рисунок 4-1

4.1. Информация о системе

На рисунке 4-2 показан интерфейс раздела информации о системе коммутатора, на котором можно посмотреть модель устройства, MAC-адрес, версию программного обеспечения и аптайм - время работы устройства в онлайн.

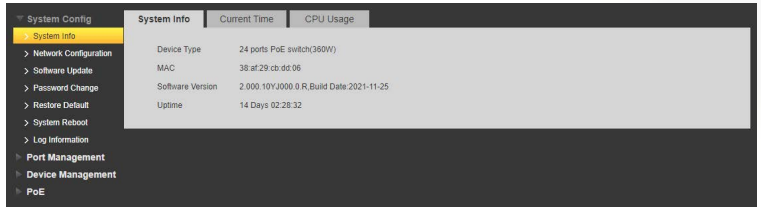


Рисунок 4-2

4.1.2. Текущее время

На рисунке 4-3 показан интерфейс настройки системного времени коммутатора, с помощью которого можно установить текущее время и часовой пояс устройства.

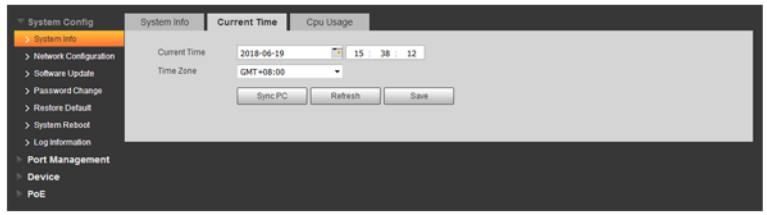


Рисунок 4-3

4.1.3. Загрузка ЦПУ

На рисунке 4-4 показан интерфейс раздела с параметрами ЦПУ коммутатора, в котором можно посмотреть загрузку ЦПУ во время работы устройства.

Рисунок 4-4

4.2. Настройка сети

Каждому хосту требуется IP-адрес для сетевого взаимодействия.

IP-адрес (Internet Protocol address) — это 32-разрядный адрес, используемый в Интернете. У этого адреса, назначаемого протоколом IP, единый формат: он обычно отображается в виде четырех десятичных чисел. IP-адрес — это логический адрес, который назначается для каждой сети и хоста в Интернете и используется для идентификации каждого хоста и реализации сетевого взаимодействия.

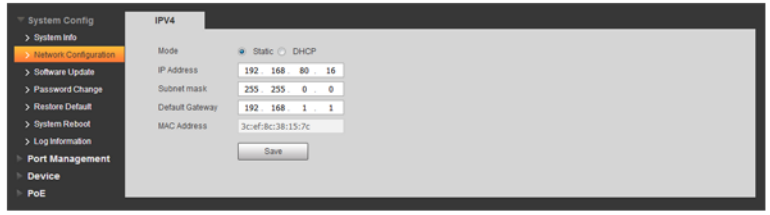


Рисунок 4-5

На рисунке 4-5 представлен интерфейс настройки IP-конфигурации, где можно проверить IP-адрес устройства, маску подсети, шлюз по умолчанию и MAC-адрес. IP-адрес по умолчанию — 192.168.1.110, он может быть изменен в этом разделе. См. таблицу 4-1 с информацией о конфигурации адреса.

Таблица 4-1

Параметр	Примечание
IP-адрес	IP-адрес для управления коммутатором, который можно изменять в разделе настройки IP-адреса коммутатора
Маска подсети	Адрес маски подсети коммутатора, конфигурацию которого можно изменить.
Шлюз по умолчанию:	Маршрут коммутатора по умолчанию
MAC-адрес	Физический адрес коммутатора, который не может быть изменен.

Примечание

Не изменяйте маску подсети коммутатора случайным образом. Если она была изменена неправильно, могут возникнуть проблемы со входом в систему коммутатора.

4.2. DHCP

DHCP (Dynamic Host Configuration Protocol — протокол динамической настройки узла) используется для динамического распределения IP-адресов и других параметров конфигурации сети между сетевыми устройствами.

DHCP использует режим связи клиент-сервер. Клиент обращается к серверу, сервер возвращает ему IP-адрес и другие необходимые данные о конфигурации, которые выделены клиенту и предназначены для реализации динамической конфигурации IP-адреса и других параметров.

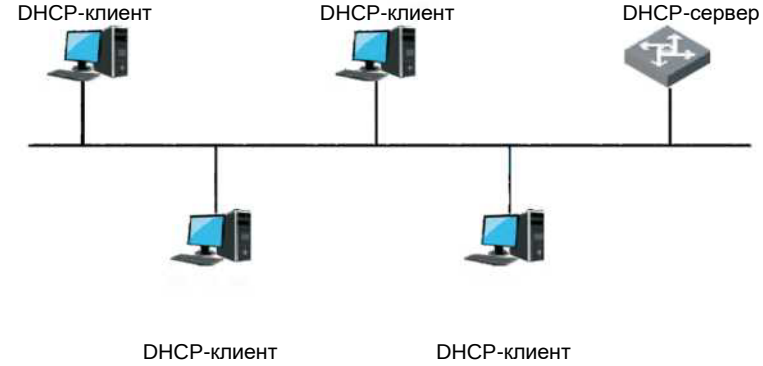


Рисунок 4-6

Пример конфигурации.

1 Сетевое требование

Необходимо настроить коммутатор как DHCP-клиент и автоматически получить IP-адрес для управления коммутатором.

2 Шаги настройки

а. Установите флажок DHCP, как показано на рисунке 4-7.

Рисунок 4-7

b. Нажмите Save («Сохранить»).

4.4. Обновление программного обеспечения

На снимке экрана ниже показан раздел обновления системных файлов коммутатора через Интернет.

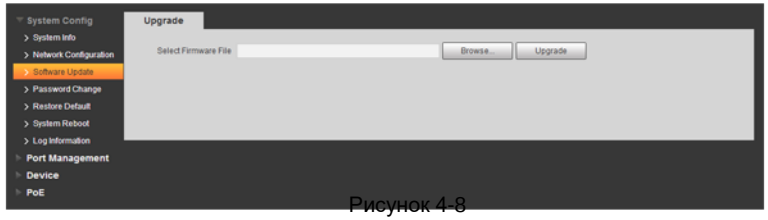


Рисунок 4-8

4.5. Изменение пароля

Пароль пользователя можно изменить в следующем разделе; имя пользователя - **admin**, его изменить нельзя; пароль, устанавливается при первом посещении веб-интерфейса коммутатора.

Рисунок 4-9

4.6. Восстановление настроек по умолчанию

Когда необходимо вернуть конфигурацию коммутатора к исходным значениям, воспользуйтесь функцией восстановления настроек
системы по умолчанию.
За исключением IP-адреса для управления устройством и пароля для входа, все остальные параметры будут восстановлены до
значений по умолчанию.

Рисунок 4-10

4.7. Перезагрузка системы

Перед перезагрузкой устройства необходимо сохранить сделанные настройки. В противном случае все они будут потеряны после перезагрузки. После перезагрузки устройства вам необходимо снова войти в веб-интерфейс.

Рисунок 4-11

4.8. Регистрируемая информация

На рисунке 4-12 показан интерфейс отображения системного журнала, где можно проверить информацию о системном журнале во время работы устройства, что упростит анализ проблем для обслуживающего персонала.

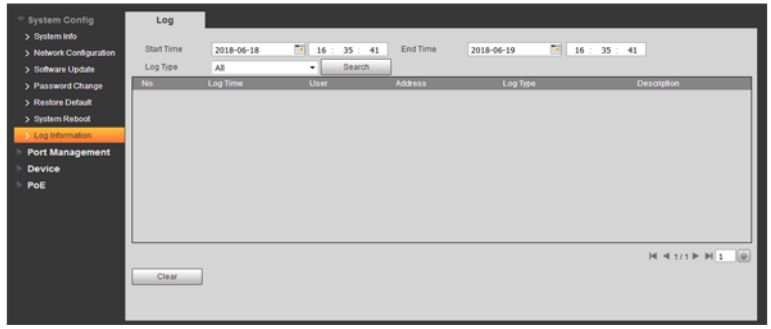


Рисунок 4-12

Пример конфигурации.

1 Настройте Start Time («Время начала») и End Time («Время окончания»), задав период для поиска.
2 Выберите тип события, например Error («Ошибка»), Warning («Предупреждение») или Info («Информация»).
3 Щелкните Search («Поиск») .

5 Управление портами

5.1. Конфигурация порта

Раздел конфигурации портов служит для настройки каждого базового параметра, который связан с портом коммутатора. Базовые параметры порта будут напрямую влиять на его работу. Необходимо произвести настройки в соответствии с практическими требованиями.

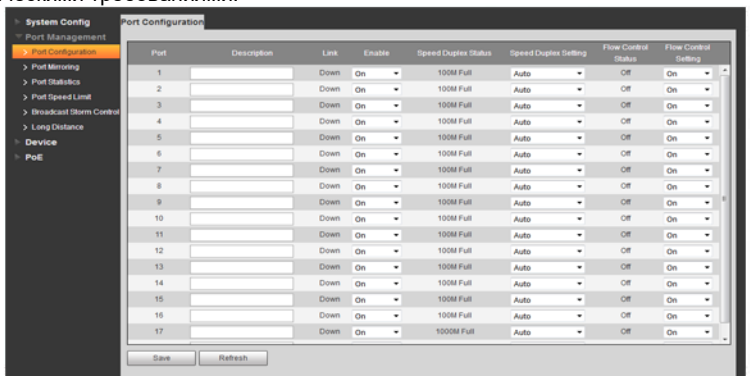


Рисунок 5-1

На рисунке 5-1 показан интерфейс раздела конфигурации портов коммутатора. Здесь можно посмотреть описание портов, состояние соединения, скорость в дуплексном режиме, состояние управления потоком каждого порта, можно добавить описание порта, настроить включение и выключение состояния, скорость, дуплексный режим и функцию управления потоком каждого порта.

- Порт: отображает номер порта коммутатора.
- Описание порта: здесь можно внести описание порта.
- Включить: здесь можно включить/выключить порт.

См. таблицу 5-1 для конфигурации состояния порта.

Состояние	Примечание
On («Вкл.»)	Статус соединения в настройках: включено.
Off («Выкл.»)	Статус соединения в настройках: отключено.

Таблица 5-1

• Соединение: отображает статус канала порта.

См. таблицу 5-2 для конфигурации состояния порта.

Состояние	Примечание
Up («Вверх»)	Означает, что соединение установлено.
Down («Вниз»)	Означает, что соединение не установлено.

Таблица 5-2

- Текущая скорость: отображает текущее состояние скорости порта. См. таблицу 5-3, в которой показана скорость порта в дуплексном режиме.

Порт	Текущая скорость	Скорость в дуплексном режиме
Порт Ethernet	Авто (по умолчанию)	Режим автосогласования
	10M FULL	10 Мбит/с, полный дуплекс
	10M HALF	10 Мбит/с, полудуплекс
	100M FULL	100 Мбит/с, полный дуплекс
	100M HALF	100 Мбит/с, полудуплекс
	1000M FULL	1000 Мбит/с, полный дуплекс
Порт оптоволокна	1000M-X	1000 Мбит/с, полный дуплекс

Таблица 5-3

- Конфигурация скорости: настройка скорости портов в дуплексном режиме.

Примечание

Будьте внимательны: если вы измените скорость порта в дуплексном режиме, это сразу же отразится на соединении.

См. таблицу 5-4 для конфигурации скорости порта в дуплексном режиме.

Порт	Текущая скорость	Скорость в дуплексном режиме
Порт Ethernet	Авто (по умолчанию)	Самонастройка скорости порта в дуплексном режиме
	10M FULL	Скорость порта в дуплексном режиме 10 Мбит/с с полным дуплексом
	10M HALF	Скорость порта в дуплексном режиме 10 Мбит/с с полудуплексом
	100M HALF	Скорость порта в дуплексном режиме 100 Мбит/с с полудуплексом
	100M FULL	Скорость порта в дуплексном режиме 100 Мбит/с с полным дуплексом
	1000M FULL	Скорость порта в дуплексном режиме 1000 Мбит/с с полным дуплексом
Порт оптоволокна	1000-X	Для порта оптоволоконного соединения устанавливается скорость 1000 Мбит/с в полнодуплексном режиме

Таблица 5-4

- Управление потоком: настройка функции управления потоком коммутатора (включена настройка по умолчанию).

В интерфейсе управления потоком портов **on** означает включение функции управления потоком порта, тогда кадры Pause можно будет отправлять или принимать в обычном режиме, **off** — отключение функции управления потоком порта.

Примечание

Для Ethernet-порта следует включить функцию управления потоком портов, чтобы синхронизировать скорость входящего и исходящего трафика и исключить потерю пакетов в результате разных скоростей.

5.2. Зеркалирование портов

Зеркалирование портов (так называемый мониторинг порта) — это процесс копирования пакета, проходящего через порт или несколько портов (исходный порт) на другой порт (порт назначения), соединенный с устройством мониторинга для анализа пакетов. Зеркалирование портов используется для мониторинга сети и устранения ее неисправностей. См. рисунок 5-2.

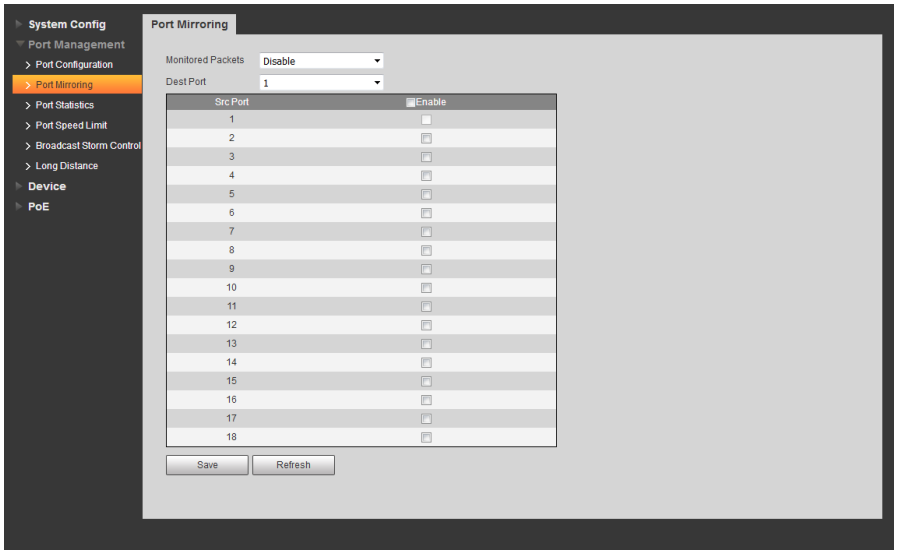


Рисунок 5-2

- Порт назначения: порт, осуществляющий мониторинг. Выберите только один элемент. Настройка по умолчанию: отключено.
- Исходный порт: проводится его мониторинг. Выберите один или несколько элементов.
- Включение зеркалирования: существует четыре режима: отключено, только Tx, только Rx, включено.

См. таблицу 5-5 для настройки зеркалирования портов.

Наименование	Примечание	
Пакеты для зеркалирования	Отключено (по умолчанию)	Функция мониторинга отключена
	Только Tx	Отслеживаются только исходящие пакеты
	Только Rx	Отслеживаются только входящие пакеты
	Включено	Мониторинг входящих/исходящих пакетов
Порт назначения	Порт, осуществляющий мониторинг. Выберите только один элемент. Настройка по умолчанию: отключено.	
Исходный порт	проводится его мониторинг. Выберите один или несколько элементов.	

Таблица 5-5

Пример конфигурации.

1 Сетевое подключение.
Включить функцию зеркалирования портов, чтобы порт 1 мог осуществлять мониторинг пакетов порта 2 и 3.

2 Настройки
(1) Включите функцию зеркалирования портов и выберите потоки данных для мониторинга.
(2) Выберите исходный порт.
(3) Выберите порт назначения. Вид раздела показан на рисунке 5-3.

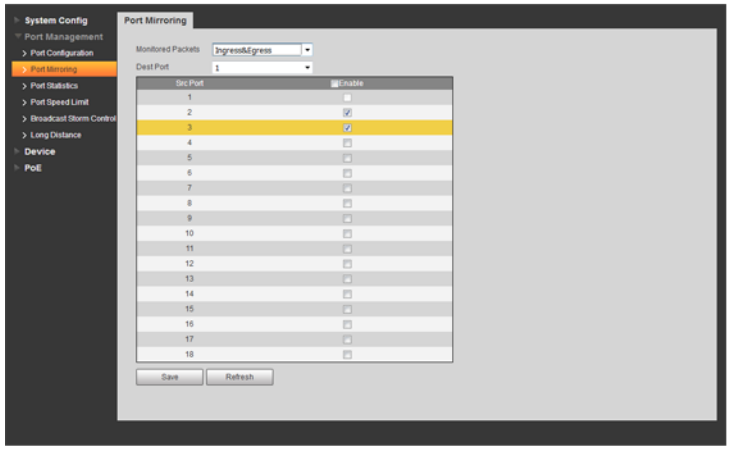


Рисунок 5-3

5.3. Статистика портов

Рисунок 5-4 — интерфейс статистики портов коммутатора. Здесь отображается количество входящих/исходящих пакетов для каждого порта, статистика конфликтов, количество потерянных пакетов, пакеты с ошибками CRC (циклический избыточный код) и т. д. Производительность порта низкая, если количество пакетов с ошибками слишком велико; проверьте подключение кабеля к порту или проверьте исправность соответствующего противоположного порта.

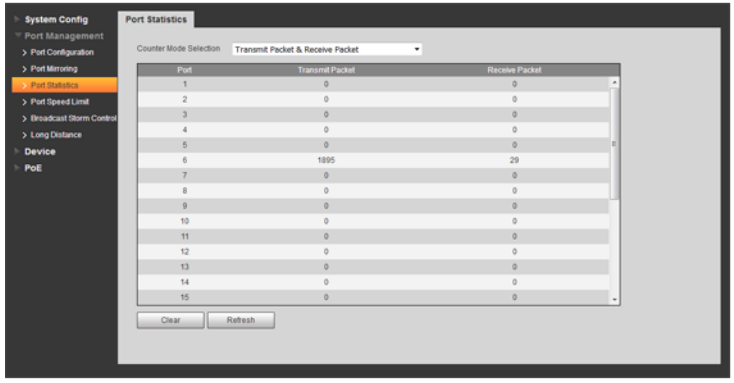


Рисунок 5-4

5.4. Ограничение скорости порта

Здесь устанавливаются параметры ограничения скорости порта, ограничивается пропускная способность для входящих/исходящих пакетов данных. См. рисунок 5-5.

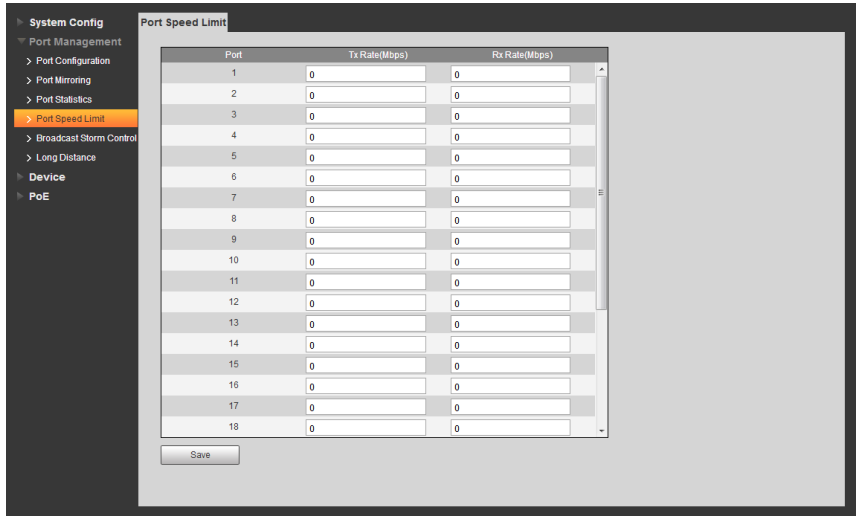


Рисунок 5-5

См. рисунок 5-5, чтобы определить политику ограничения скорости для каждого порта. См. таблицу 5-6 с параметрами ограничения скорости порта.

Наименование	Примечание
Порт	Отображается список портов.
Скорость Tx	Служит для установки скорости исходящего трафика для порта. Диапазон значений от 0 до 63 Мбит/с. Настройка по умолчанию 0, ограничение скорости отсутствует.
Скорость Rx	Служит для установки скорости входящего трафика для порта. Диапазон значений от 0 до 63 Мбит/с. Настройка по умолчанию — 0, ограничение скорости отсутствует.

Таблица 5-6

Пример конфигурации.

1 Сетевое соединение

Установите ограничение скорости портов 1 и 2. Скорость каждого порта меньше 50 Мбит/с.

2 Настройки

(1) Установите Tx/Rx скорость порта. См. рисунок 5-6.

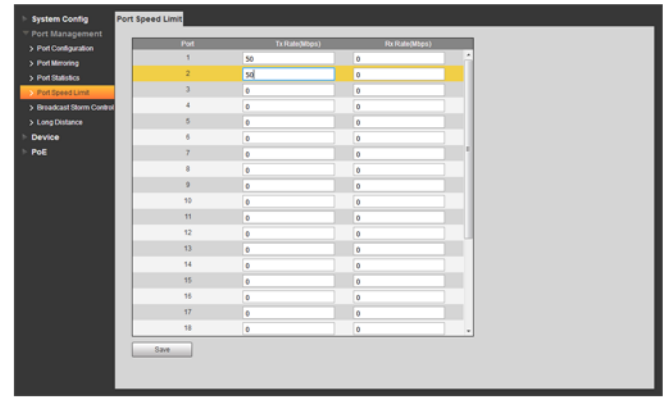


Рисунок 5-6

(2) Нажмите кнопку Save («Сохранить»).

5.5. Контроль широковещательных штормов

Широковещательный шторм — это такое явление, при котором широковещательные кадры повторно пересылаются по сети, нарушая ее работу. Это значительно снижает производительность сети. Контроль над штормом поможет ограничить прием широковещательных кадров портом и прекратить их обработку, как только поток превысит указанный порог.

Эта функция снижает риск широковещательного шторма и гарантирует правильную работу сети. См. рисунок 5-7.

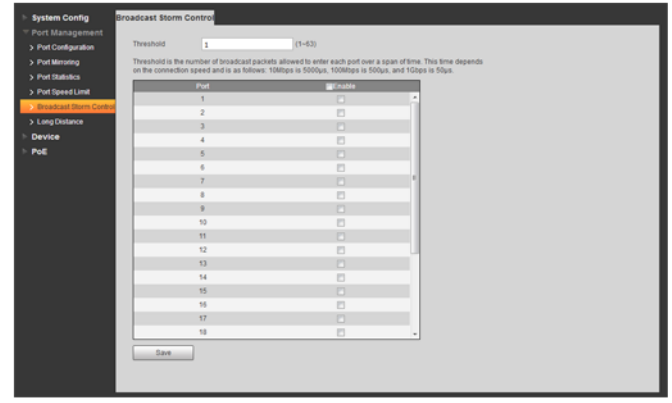


Рисунок 5-7

См. таблицу 5-7 с параметрами управления трансляцией.

Наименование	Примечание
Пороговое значение	Лимит широковещательных пакетов для одного порта в течение указанного периода.
Порт	Имя порта.

Таблица 5-7

Пример конфигурации.

1 Сетевое соединение
Установите функцию контроля широковещательных штормов для всех портов на случай сбоя порта, если устройство не сможет правильно передать данные из-за большого числа широковещательных пакетов.

2 Настройки
(1) Установите пороговое значение. Это количество широковещательных пакетов для одного порта.
(2) Выберите порт для настройки.

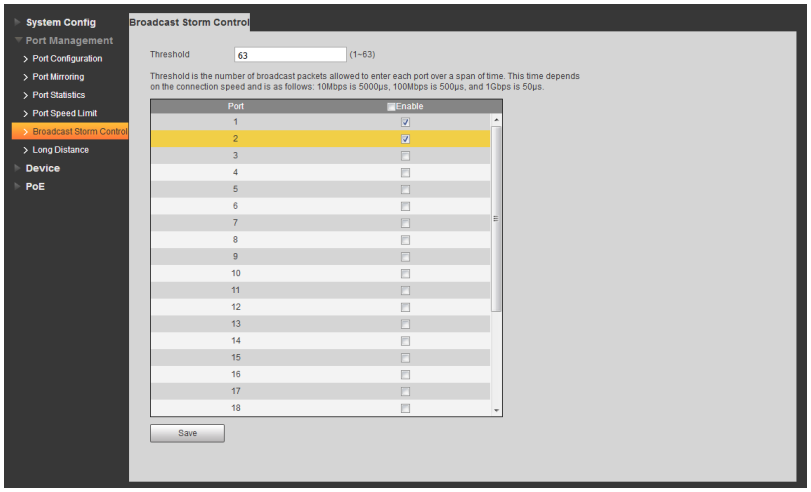


Рисунок 5-8

(2) Нажмите кнопку Save («Сохранить»).

5.6. Передача на большие расстояния

В этом разделе настраивается режим передачи данных на большие расстояния. Для стандартного режима Ethernet можно установить скорость передачи 10 Мбит/с на 250 м вместо 100 Мбит/с на 100 метров. См. рисунок 5-9.

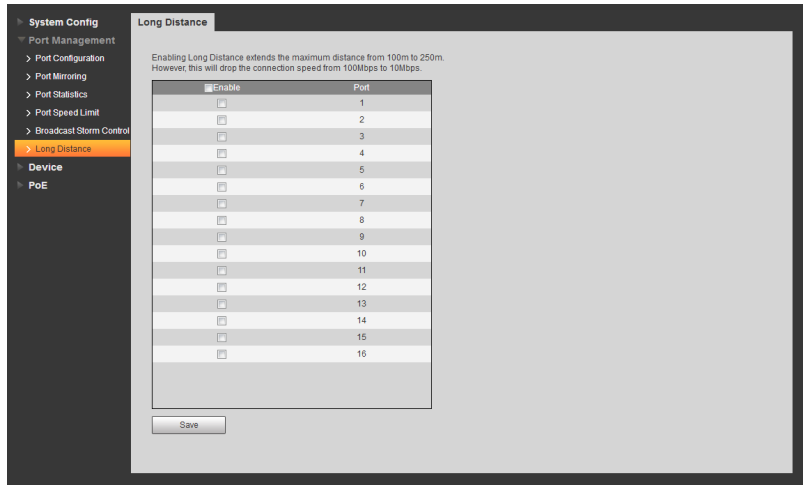


Рисунок 5-9

Пример конфигурации.

1 Сетевое соединение
Установите для всех портов функцию передачи на большие расстояния, чтобы поддерживалась качественная передача данных на 250 метров.

2 Настройки
(1) Установите флажок рядом с портом, чтобы включить функцию передачи на большие расстояния.
(2) Нажмите кнопку Save («Сохранить»). См. рисунок 5-10.

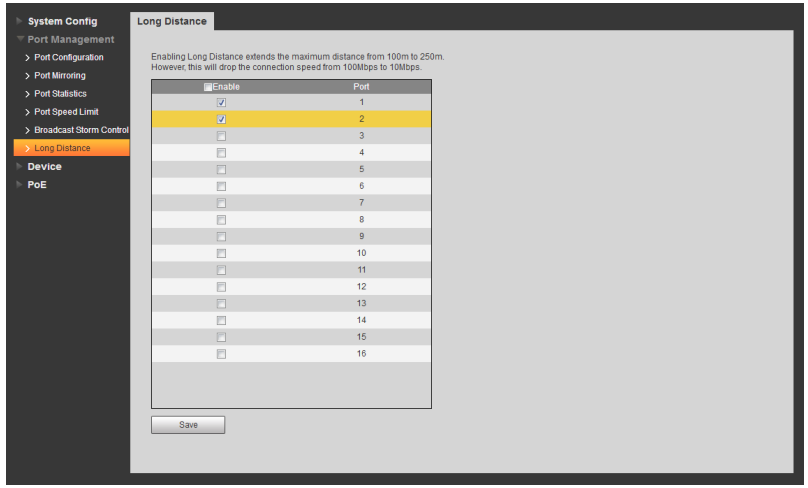


Рисунок 5-10

6 Управление устройствами

6.1. Кольцевая топология сети

6.1.1. Определение STP

Основная идея протокола STP очень проста. Известно, что в последовательно развивающейся сети с топологией дерева закольцовывания не происходит, если эта сеть растет подобно деревьям в природе. Таким образом, определяются корневой мост, корневой порт, назначенный порт, стоимость пути и другие понятия протокола STP, который служит для отсечения избыточного цикла посредством структурирования дерева, а также может реализовать резервное копирование соединений и оптимизацию пути. Алгоритм структурирования дерева называется алгоритмом связующего дерева (Spanning Tree).
Пакет протокола, принятый STP, — BPDU (Bridge Protocol Data Unit — фрейм протокола управления сетевыми мостами), который также называется конфигурационной информацией. BPDU содержит достаточную информацию, чтобы обеспечить процесс расчета по алгоритму связующего дерева. STP может подтвердить топологическую структуру сети посредством передачи устройствам BPDU.
Формат BPDU и описание поля реализуют функции связующего дерева, осуществляют обмен информацией посредством передачи пакета BPDU коммутаторам. Все коммутаторы, поддерживающие протокол STP, получат и обработают пакет. Пакет несет всю необходимую информацию, которая может использоваться для расчета алгоритма связующего дерева. Формат кадра BPDU и описание поля стандартного связующего дерева показаны на рисунке 6-1.

2	1	1	1	8	4
Идентификатор протокола	Версия	Сообщение Тип	Флаг	Идентификатор корня	Стоимость корневого пути
Идентификатор моста	Идентификатор порта	Возраст Сообщения	Максимальный возраст	Время приветствия	Вперед Задержка
8	2	2	2	2	2

Рисунок 6-1

- Идентификатор протокола: идентификация протокола.
- Версия: версия протокола
- Тип сообщения: тип BPDU.
- Флаг: флаговый бит.
- ИДЕНТИФИКАТОР КОРНЯ: ID корневого моста, который состоит из 2-байтовой записи приоритета и 6-байтового MAC-адреса.
- Стоимость корневого пути: стоимость корневого пути.
- Bridge ID: это идентификатор моста, который отправляет BPDU, состоящие из 2-байтового приоритета и 6-байтового MAC-адреса.
- ID порта: идентифицирует порт, который отправляет BPDU.
- Время жизни сообщения: время жизни сообщения BPDU.
- Максимальное время жизни: время жизни текущего сообщения BPDU, которое является максимальным сроком сохранения BPDU для порта.

- Время приветствия: цикл периода корневого моста, отправляющего BPDU.
- Задержка смены состояний: продолжительность отслеживания и исследования статуса перед отправкой пакета данных после изменения топологии.

6.2. Основные понятия STP

Идентификатор моста: комплексное числовое значение приоритета моста и его MAC-адрес, а приоритет моста — это параметр, который можно установить. Чем ниже значение идентификатора моста, тем выше приоритет моста, что увеличивает вероятность того, что он станет корневым мостом.
Корневой мост: коммутатор с минимальным идентификатором моста. Выберите лучший коммутатор в контуре и установите его как корневой мост, который будет обеспечивать производительность и надежность сети.
Назначенный мост: в каждом сегменте сети мост с наименьшей стоимостью пути к корневому мосту будет являться назначенным мостом, через который пакет данных будет перенаправляться в сегмент сети. Когда все коммутаторы имеют одинаковую стоимость корневого пути, коммутатор с самым низким идентификатором моста будет выбран как назначенный мост.
Стоимость корневого пути: общая сумма всех затрат на пути между двумя сетевыми мостами.
Стоимость корневого пути корневого моста равна нулю.
Приоритет моста: параметр, который может быть задан пользователями, диапазон численных значений от 0 до 61 440. Чем меньше значение, тем выше приоритет. Чем выше приоритет моста, тем больше вероятность, что он станет корневым мостом.
Корневой порт: ближайший порт к корневому мосту на некорневом мостовом коммутаторе, отвечающий за связь с корневым мостом, стоимость пути от этого порта до корневого моста является самой низкой. Порт с наивысшим приоритетом станет корневым портом, в случае если несколько портов имеют одну стоимость пути до корневого моста.
Назначенный порт: порт на назначенном мосту, который передает данные коммутатору.
Приоритет порта: диапазон от 0 до 240 с шагом 16. Чем ниже число, тем выше приоритет, и такой порт скорее станет корневым.
Стоимость пути: Протокол STP используется для выбора ссылочного значения соединения. Протокол STP может привести сеть к древовидной структуре без петель путем вычисления стоимости пути и блокировки избыточных соединений.
Сетевая схема базовой концепции связующего дерева показана на рисунке 6-2.
Коммутатор A
B и C последовательно подключаются, коммутатор A выбирается как корневой мост после вычисления STP, соединение между портом 2 и портом 6 блокируется.
Мост: Коммутатор A является корневым мостом всей сети; Коммутатор B является назначенным мостом Коммутатора C.
Порт: порт 3 и порт 5 являются корневыми портами Коммутатора B и Коммутатора C соответственно; порт 1 и порт 4 — назначенные порты Коммутатора A и Коммутатора B соответственно; порт 6 является заблокированным портом Коммутатора C.

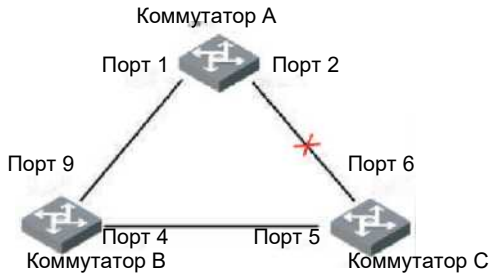


Рисунок 6-2

Таймер STP

Время приветствия

Составляет от 1 до 10 секунд. Это интервал, в течение которого корневой мост отправляет пакет данных BPDU всем коммутаторам, чтобы проверить наличие неисправностей в обнаружении каналов коммутаторов.

Максимальное время жизни

Составляет от 6 до 40 секунд. Коммутатор отправит пакет данных BPDU всем коммутаторам и снова рассчитает алгоритм связующего дерева, если будет превышено время устаревания и пакет данных BPDU, отправленный корневым мостом, не будет получен.

Задержка смены состояний:

Составляет от 4 до 30 секунд. Это время перехода порта коммутатора в состояние прослушивания.
Из-за сбоя в сети алгоритмы связующего дерева пересчитываются, а в структуре связующего дерева происходят соответсвующие изменения. Новое сообщение пересчитанной конфигурации не может быть распространено по всей сети немедленно, так как мгновенное изменение статуса порта может привести к закольцовыванию. Поэтому протокол связующего дерева использует механизм перехода состояния. Перед пересылкой данных произойдут две задержки передачи: для нового корневого порта и для назначенного порта. Задержка гарантирует, что новое сообщение конфигурации будет распространено по всей сети.

Примечание:

Если топологическое состояние стабильно, то только корневой порт и назначенный порт реализуют передачу данных, другие порты находятся в состоянии блокировки, они получают только пакет BPDU, но не пересылают данные.

6.1.3. Настройки STP для моста

Интерфейс конфигурации моста STP показан на рисунке 6-3.

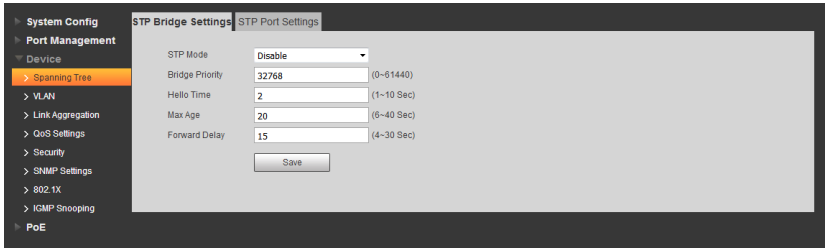


Рисунок 6-3

- Режим STP: включает или отключает функцию кольцевой топологии сети.
- Приоритет моста: установите приоритет моста в диапазоне от 0 до 61440.
- Время приветствия: установите период отправки BPDU для корневого моста в диапазоне от 1 до 10 секунд.
- Максимальное время жизни: установите время жизни текущего BPDU в диапазоне от 6 до 40 секунд.
- Задержка смены состояний: после установки топологических изменений мост находится в режиме наблюдения и изучения, продолжительность периода составляет от 4 до 30 секунд.

6.1.4. Настройки STP для порта

Интерфейс конфигурации порта STP показан на рисунке 6-4.

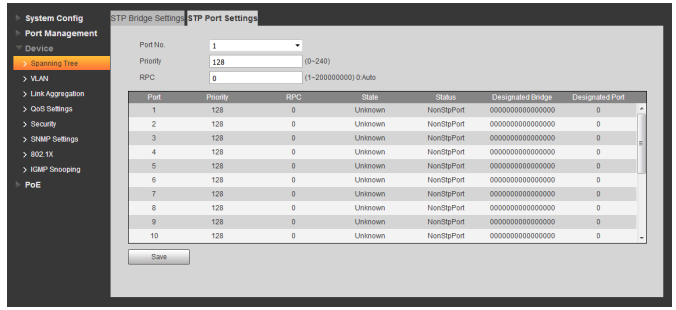


Рисунок 6-4

- № порта: выберите порт, который вы хотите настроить.
- Приоритет: настройте приоритет порта в диапазоне от 0 до 240, это должно быть целое число кратное 16.
- RPC: настройте стоимость пути от текущего порта до корневого моста в диапазоне от 1 до 200 000 000. Чтобы установить стоимость пути по умолчанию, введите значение 0.

6.2. Настройки VLAN

6.2.1. Определение VLAN

Это логическая функция, которая позволяет разделить одну локальную сеть на несколько виртуальных. Каждая подсеть имеет собственную зону вещания, так называемую виртуальную локальную сеть (VLAN). VLAN логически разделена на организационном, а не на физическом уровне, создавая изолированную область вещания VLAN.

6.2.2. Функции VLAN

1 Повышает производительность сети. Широковещательные пакеты находятся в VLAN, они могут эффективно управлять широковещательным штормом, снизить пропускную способность сети и повысить возможности процессов в ней.
2 Повышает безопасность сети. Устройства в разных VLAN не могут обращаться друг к другу, а узлы в разных VLAN не могут взаимодействовать друг с другом. Им нужен маршрутизатор или трехуровневый коммутатор для пересылки кадров.
3 Упрощает управление сетью. Хост в той же виртуальной рабочей группе не ограничен одной физической областью; это упрощает управление сетью и создание рабочих групп пользователей в разных областях.

6.2.3. 802.1Q VLAN

Кадры коммутатора могут быть с тегами или без них. См. следующий рисунок, показывающий позицию тега.

Рисунок 6-5

У Ethernet-кадров обычно отсутствуют теги. Сетевой адаптер обычного ПК может распознать кадр и затем обмениваться данными.

Для кадров с тегами добавляется 4-битная информация VLAN после MAC-адреса источника и адреса назначения. На приведенном выше рисунке это голубой прямоугольник с заголовком тега VLAN. Как правило, сетевой адаптер обычного ПК не может распознать этот вид кадра. Коммутатор должен использовать тег VLAN для различения разных VLAN, чтобы они не могли обмениваться данными друг с другом. Иногда возникает необходимость обмена данными между различными VLAN. Для этого существуют разные типы портов, позволяющие VLAN связываться друг с другом.

Существует три типа портов:

- Порт доступа, который относится к одной VLAN. Обычно он подключается к порту компьютера.
- Магистральный порт позволяет нескольким VLAN обмениваться кадрами между собой. Обычно используется для соединения коммутаторов.
- Гибридный тип может пропускать трафик нескольких VLAN и получать или отправлять кадры из нескольких VLAN, используется для подключения коммутаторов и ПК пользователей.

Для обработки данных между гибридным и магистральным портами нет различий. Единственная разница — когда они отправляют данные: гибридный порт может отправлять кадр из нескольких VLAN и без тега, в то время как магистральный порт может отправлять без тега только кадр VLAN по умолчанию.

В таблице 6-1 показаны типы соединения и методы обработки кадров для VLAN по умолчанию.

Тип порта	Для кадров без тега	Для кадров с тегом	Для отправки кадров
Доступ	Получает кадр и добавляет тег для VLAN по умолчанию.	Если идентификатор VLAN совпадает с идентификатором VLAN по умолчанию, получает текущий кадр. Если идентификатор VLAN отличается от идентификатора VLAN по умолчанию, кадр отбрасывается.	Удаляет тег и отправляет кадр.
Магистральный Гибридный	Добавляет идентификатор VLAN по умолчанию, если этот идентификатор включен в список разрешенных, то получает кадр и добавляет тег VLAN по умолчанию. Добавляет идентификатор VLAN по умолчанию, если этот идентификатор находится в списке блокировки, то отбрасывает кадр.	Если идентификатор VLAN находится в списке разрешенных, то получает кадр. Если идентификатор VLAN находится в списке блокировки, то отбрасывает кадр.	Если идентификатор VLAN совпадает с идентификатором VLAN по умолчанию, и он находится в списке разрешенных, то удаляет тег и отправьте кадр. Если идентификатор VLAN включен
			в список разрешенных, то отправляет кадр. Используйте параметр port hybrid untagged/ tagged vlan («vlan гибридного порта с тегами/без тегов») для настройки отправки с тегом или без него.

Таблица 6-1

Пример конфигурации.

1 Сетевое соединение

ПК 1 и IP-камера 2 относятся к одному отделу, ПК 2 и IP-камера 1 относятся к другому отделу. Связь внутри отдела установлена, но связь между отделами не реализована.

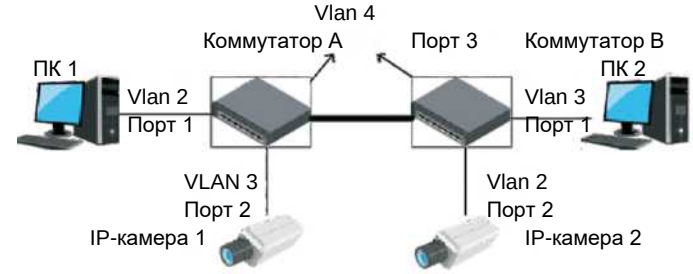


Рисунок 6-6

2. Аппаратное подключение

(1) ПК 1 подключается к порту 1 коммутатора A и относится к vlan 2, IP-камера 1 подключается к порту 2 коммутатора A и относится к vlan 3.

(2) ПК 2 подключается к порту 1 коммутатора B и относится к vlan 3, IP-камера 2 подключается к порту 2 коммутатора B и относится к vlan 2.

(3) Порт 3 коммутатора A подключается к порту 3 коммутатора B и относится к vlan 4.

3 Настройки

коммутатор A: порт 1 относится к vlan 2, он настроен как порт доступа, порт 2 относится к vlan 3, он настроен как порт доступа, порт 3 настроен как магистральный порт и относится к vlan 4, и он позволяет пропускать трафик vlan 2, 3 и 4.

Коммутатор B: порт 1 относится к vlan 2, он настроен как порт доступа, порт 2 относится к vlan 3, он настроен как порт доступа, порт 3 настроен как магистральный и относится к vlan 4, и он позволяет пропускать трафик vlan 2, 3 и 4.

См. рисунок 6-7.

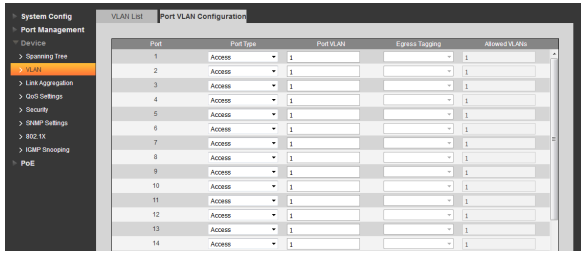


Рисунок 6-7

6.3. Агрегирование каналов

Агрегирование каналов состоит в том, чтобы объединить несколько физических портов коммутатора в один логический. Несколько каналов, принадлежащих к одной и той же группе агрегации, можно рассматривать как логический канал с большей пропускной способностью.

Агрегирование каналов позволит обрабатывать поток сразу нескольким портам-членам группы агрегации, что увеличивает пропускную способность. Между тем, взаимное динамическое резервное копирование может быть реализовано между каждым портом-членом в той же группе агрегации, что улучшает надежность соединения.

Необходимы определенные настройки портов-членов, принадлежащих к одной и той же группе агрегации. Эти настройки включают в себя STP, QoS, VLAN, свойства порта, исследование MAC-адресов, зеркалирование, 802,1x фильтрацию MAC-адресов и т. д.

Примечание:

Не рекомендуется настраивать отдельные порты и применять расширенные функции для портов, которые используются для агрегирования каналов.

Существует два типа агрегирования каналов — статическая агрегация и LACP. Как правило, противоположные конечные устройства агрегирования коммутационных каналов — это коммутационные и сетевые карты.

6.1.3. Режим статического агрегирования

Режим статического агрегирования позволяет вручную добавлять несколько членов в группу агрегации, все порты находятся в состоянии пересылки и совместно используют перегруженный поток. Необходимо создать группу агрегации и добавить порты-члены через ручную настройку без участия LACP (Link Aggregation Control Protocol — протокола агрегирования каналов).

- **Режим балансировки нагрузки**

Существует три типа алгоритма балансировки нагрузки для порта, который показан в следующей таблице.

Режим балансировки нагрузки	Примечание
MAC-адрес источника	Расчет балансировки нагрузки на основе MAC-адреса источника пакета
MAC-адрес назначения	Расчет балансировки нагрузки на основе MAC-адреса назначения пакета.
MAC источника и назначения	Расчет балансировки нагрузки на основе MAC-адресов источника и назначения пакета

Таблица 6-2

- **Группа агрегирования**

Это сборная группа портов Ethernet. Поддерживаемое количество групп агрегации по умолчанию равно трем, изменить это число нельзя. Статус по умолчанию для всех групп агрегации — отключено, по умолчанию порты в группах отсутствуют.

- **Порт-член группы**

По умолчанию коммутатор создал все доступные группы агрегации, но не добавил в них ни одного порта. Если вы хотите настроить порты-члены группы агрегации, то вначале включите группу агрегации. Для этого щелкните группу агрегации, в которой будет находиться порт, и включите функцию агрегации.

См. рисунок 6-8, на котором представлен интерфейс конфигурации статической агрегации, включающий режим балансировки нагрузки, группу агрегации и участвующие порты.

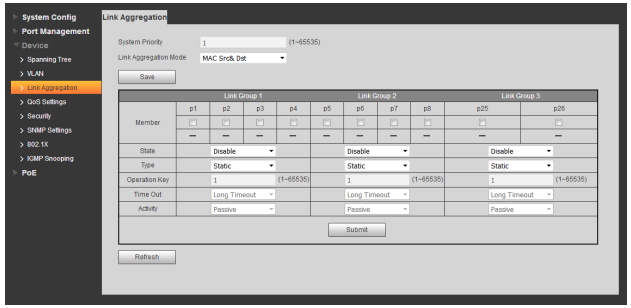


Рисунок 6-8

6.3.2. Режим LACP

LACP (Link Aggregation Control Protocol — протокол агрегирования каналов) используется для реализации динамической конвергенции и разделения конвергенции каналов на основе стандарта IEEE 802.3ad. Обе стороны устройств конвергенции конвергируют подходящие каналы и принимают и отправляют данные с помощью пакетов LACPDU, обмениваясь информацией о конвергенции. Протокол может автоматически добавлять и удалять порты в группе конвергенции, он обладает высокой гибкостью и обеспечивает возможность балансировки нагрузки.

После включения функции LACP порта порт будет информировать противоположную сторону о системном приоритете, системном MAC-адресе, номере порта, приоритете порта и операционном ключе (определяется физическими свойствами, информацией протокола верхнего уровня и управляющим ключом порта).

Сторона с высоким приоритетом устройства будет доминировать в конвергенции и разделении конвергенции. Приоритет устройства определяется системным приоритетом и системным MAC-адресом. Устройство с меньшим значением системного приоритета имеет более высокий приоритет. Если значение системного приоритета устройств одинаковое, более высокий приоритет имеет устройство с меньшим MAC-адресом системы. Сторона с более высоким приоритетом устройства выбирает порт конвергенции в соответствии с приоритетом порта, номером порта и операционным ключом. Порты с одинаковым операционным ключом будут выбраны в одну группу конвергенции. В группу конвергенции выбираются порты с меньшим значением приоритета; если приоритеты портов будут одинаковы, то будут выбраны порты с меньшими номерами. Выбранные порты будут вместе конвергировать входящий и исходящий трафик, после того как обе стороны обменяются информацией о конвергенции.

Параметры конфигурации протокола LACP в основном включают в себя возможность включения функции LACP порта, значение ключа, активность (активный/пассивный режим) и конфигурацию тайм-аута.
Порты, которые разрешают только протокол LACP, реализуют согласование LACP, а затем формируется канал конвергенции. Секретный ключ является основой для согласования, порты с одним и тем же секретным ключом ведут согласование для формирования канала конвергенции. Существует два режима согласования — активный и пассивный. Устройство будет активно запускать конвергенцию каналов при выборе active («активный»), устройство будет пассивно принимать согласования конвергенции, запущенные другими устройствами, когда выбрано passive («пассивный»).
Необходимо, чтобы по меньшей мере одна или две стороны находились в активном режиме, чтобы реализовать успешное согласование при взаимосвязи двух устройств.
Значение ключа: членам одной и той же группы конвергенции должен быть настроен один и тот же ключ операции в диапазоне от 1 до 65 535.
Активность: по умолчанию следует выбрать активный и пассивный режимы: одна сторона, которая участвует в динамической конвергенции, должна быть настроена в активном режиме, а другая сторона должна быть настроена с пассивном режиме.

Время ожидания: по умолчанию установлено значение Long Timeout («Длительное время ожидания»). Можно установить Long Timeout и Short Timeout («Короткое время ожидания»).**Пример конфигурации:**

1 Требование к сети.
Необходимо реализовать резервирование каналов и двухканальную связь по каналу GB через функцию агрегирование каналов, потому что есть скрытая проблема со связью только через канал GN.
2 Шаги настройки
(1) Выберите группу агрегации 3, щелкните по портам 25 и 26.
(2) Выберите режим агрегирования каналов LACP, настройте активность как Activity («Активный»).
(3) Нажмите Submit («Подтвердить»), чтобы применить конфигурацию.
(4) Выберите режим агрегирования каналов MAC Src&Dst («MAC источника и назначения»), результат конфигурации показан на рисунке 6-10. Для соответствующих успешно агрегированных портов будет отображаться V.

Таблица 6-9

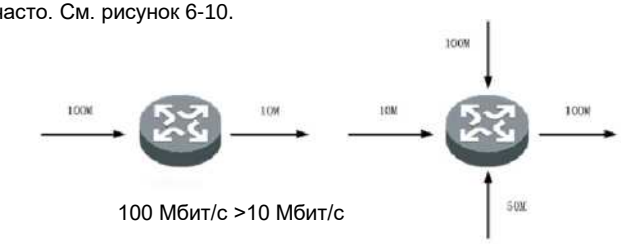
6.4. Настройки QoS

Качество обслуживания (QoS) отражает способность сети удовлетворять потребности клиентов. В Интернете QoS служит для оценки способности сети пересылать пакеты разных служб. Оценка основывается на разных критериях, поскольку сеть может предоставлять различные услуги. Как правило, эффективность QoS определяется пропускной способностью, задержкой, джиттером и потерей пакетов во время процесса пересылки.

В традиционной IP-сети без QoS устройство рассматривает все пакеты одинаково, на основе последовательной очереди (FIFO). Устройство выделяет необходимые ресурсы в зависимости от времени прибытия пакета. Все пакеты совместно используют ресурсы сети и устройства по мере поступления пакетов. Такой вид услуг называется негарантированной доставкой (Best-Effort). Он задействует максимальные усилия для отправки пакета в пункт назначения, но нет гарантии или уверенности в отношении задержки, джиттера и коэффициента потери пакетов во время процесса пересылки пакетов.
Традиционная политика негарантированной доставкой предназначена для WWW, службы электронной почты, которая нечувствительна к пропускной способности или задержке. Но сейчас новый развивающийся бизнес требует от IP-сети высокого уровня обслуживания. Пользователь не просто хочет отправить пакет в пункт назначения, он также хочет получить более качественный сервис во время процесса пересылки: особую пропускную способность сети, уменьшение потери пакетов, управление сетевыми перегрузками или их устранение, корректировку сетевых потоков. Все это требует от сети больших возможностей обслуживания.

6.4.1. Перегрузка сети

В сложной интернет-среде и меняющемся окружении перегрузки происходят очень часто. См. рисунок 6-10.



100 Мбит/с >10 Мбит/с

(100 Мбит/с + 10 Мбит/с + 50 Мбит/с) > 100 Мбит/с
Рисунок 6-10

1) На рисунке показаны групповые потоки от высокоскоростного соединения к устройству и далее через низкоскоростное соединение.
2) Групповые потоки подключаются к сетевому устройству через несколько портов, а затем передаются через один порт (скорости нескольких входных портов больше, чем скорость выходного порта).

Если скорость потока слишком велика, он может столкнуться с недостатком ресурсов, что приведет к перегрузке потока. Причиной перегрузки может быть не только низкая пропускная способность канала связи, но и любой недостаток ресурсов в месте назначения (например, доступное процессорное время, буфер, ресурсы памяти) могут привести к перегрузке. Кроме того, если управление потоком в какой-то момент выходит за пределы диапазона и нет достаточных сетевых ресурсов, это может вызвать перегрузку сети.
Перегрузка имеет ряд негативных последствий:

- Перегрузка увеличивает задержку передачи пакетов и джиттер, высокая латентность может привести к отправке пакета снова.
- Перегрузка замедляет входящие и исходящие потоки сети и снижает уровень использования сетевых ресурсов.

- Перегрузка потребляет огромное количество сетевых ресурсов (особенно ресурсов хранения), неправильное распределение ресурсов может привести к сбою системы.

Таким образом, перегрузка препятствует своевременному получению ресурсов потоками и является источником снижения производительности сети. В сложных условиях, когда происходит групповой обмен и многопользовательская работа, перегрузка неизбежна. Таким образом, должен быть найден надлежащий способ справиться с перегрузкой.

6.4.2. Урегулирование перегрузок

Прямым методом решения проблемы нехватки ресурсов является увеличение пропускной способности сети. Но пропускная способность имеет свой предел, она не может устранить все проблемы, возникающие в результате перегрузки сети. Более эффективным способом решения проблемы перегрузки сети является добавление функции управления потоком и распределения ресурсов сети. Это позволит предоставлять различные услуги в соответствии с различными бизнес-требованиями, а также распределять и использовать ресурсы более разумно. Во время процесса выделения ресурсов и управления потоком попытайтесь контролировать направление или косвенные факторы, которые могут вызвать перегрузку сети, чтобы уменьшить частоту возникновения перегрузки. Когда происходит перегрузка сети, можно выделять ресурсы в соответствии с типом бизнеса и требованиями, чтобы до минимума сократить влияние перегрузки на работу компании.

6.4.3. Планирование очереди

Обычно планирование очередей используется, чтобы отрегулировать управление перегрузками. Линейный алгоритм применяется для классификации потоков, а алгоритм приоритета — для отправки определенных типов потоков в первую очередь. Каждый алгоритм очереди предназначен для устранения проблем, связанных с ожиданием сетевого потока; он имеет большое влияние на распределение ресурсов полосы пропускания, задержку, джиттер и т. д.

Настоящая серия коммутаторов поддерживает две очереди приоритетов: очередь с высоким приоритетом и очередь с низким приоритетом. Приоритет каждого пакета устанавливается в соответствии со следующими четырьмя факторами.

1 Физический порт.
2 Тег 802.1Q VLAN.
3 Строка TOS/DS IP-пакета.
4 Порт TCP/UDP.

Когда есть несколько настроек QoS, один из приоритетных элементов настройки становится высокоприоритетным, затем элемент будет помещен в строку с высоким приоритетом, после чего отправлен. Когда есть несколько высоких приоритетов, для того же уровня, они обрабатываются на основе последовательной очереди (FIFO).

6.4.4. Режим приоритета

Каждый полученный пакет размечается как имеющий либо высокий, либо низкий приоритет. Установка приоритета пакета имеет три режима. См. рисунок 6-11.

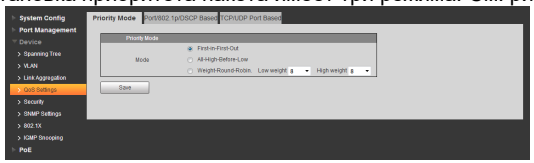


Рисунок 6-11

См. таблицу 6-3 с информацией о режиме приоритета.

Наименование	Примечание
First In First Out (FIFO)	Первый полученный пакет будет перенаправлен первым. При отключении функции QoS устройство использует режим FIFO для обработки пакетов.
Вначале высокий приоритет	Устройство пересылает пакеты в соответствии с указанным уровнем приоритета.
Взвешенный циклический алгоритм	Установите уровень веса, чтобы изменить процент пересылки пакетов с высоким приоритетом и низким приоритетом.

Таблица 6-3

6.4.5. QoS на основе порта/802.1 p/DSCP

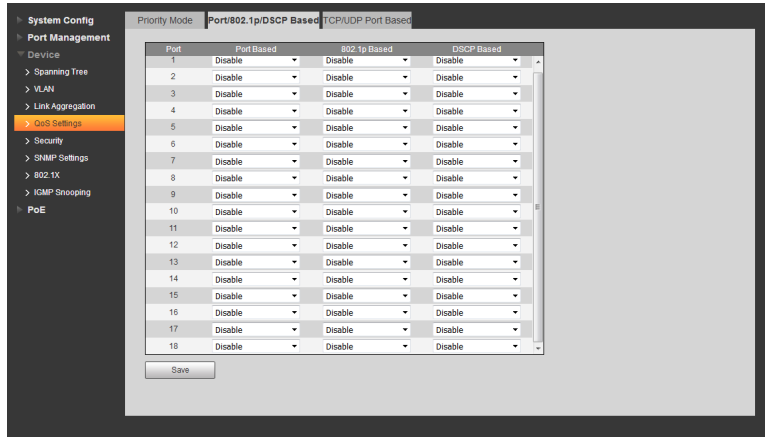


Рисунок 6-12

На основе порта

Когда для порта задан высокий приоритет, принятые пакеты помещаются в очередь с высоким приоритетом. Каждому порту может быть установлен высокий приоритет.

На основе 802.1 p

Приоритет 802.1 p находится на втором уровне заголовка пакета. Используется в среде, где нет необходимости анализировать заголовок третьего уровня и гарантирует соблюдение QoS на втором уровне.

Назначение Адрес	Источник Адрес	Заголовок 802. 1Q		Длина /тип	Данные	FCS (CRC-32)
		TPID	TCI			
6 байтов	6 байтов	4 байта	2 байта		46–1500 байтов	4 байта

Рисунок 6-13

На рисунке 6-8 четырехбайтовый тег заголовка 802.1Q включает 2-байтовый идентификатор протокола TPID (тег идентификатора протокола) и 2-байтовый TCI (тег управления информацией). Значение TPID равно 0x8100. На рисунке 6-14 отображается подробное содержимое заголовка тега 802.1Q, строка Priority — приоритет 802.1p. Приоритет называется 802.1 p, поскольку приоритет определен в спецификациях 802.1p.

Байт 1	Байт 2	Байт 3	Байт 4
TPID (Тег идентификатора протокола)		TCI (тег управления управления информацией)	
1 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0		Приоритет	CFI VLAN ID

сунок 6-14

См. таблицу 6-4 с информацией о приоритете 802.1р.

Таблица 6-4

Очередь приоритетов	Приоритет 802.1 р (десятичная система)	Приоритет 802.1 р (двоичная система)	Ключевые слова
Низкоприоритетная очередь	0	000	best-effort
	1	001	background
	2	010	spare
	3	011	excellent-effort
Высокоприоритетная очередь	4	100	controlled-load
	5	101	video
	6	110	voice
	7	111	network-management

На основе строки TOS/DS IP-пакета

Назначение Адрес*	Адрес источника*	802.1 в заголовках	Длина /тип	VER=0100.- IPV4-1	Заголовки Размер*	TOS*	--
6 байтов.	6 байтов.	4 байта	2 байта	4 бита	4 бита	6 битов	2 бита

Рисунок 6-15

На рисунке 6-10 строка ToS заголовка IP-пакета имеет 8 бит, RFC2474 переопределяет домен ToS заголовков IP-пакета, который называется дифференцированными службами. DSCP приоритет использует первые 6 битов (0–5). Значение находится в диапазоне от 0 до 63, а последние 2 бита (6,7) — зарезервированные. Информацию о приоритете IP см. в таблице 6-5.

Очередь приоритетов	IP-приоритет (десятичная система)	IP-приоритет (двоичная система)	Ключевые слова
Очередь с высоким приоритетом 1	46	101110	ef
	10	001010	af11
	18	010010	af21
	26	011010	af31
	34	100010	af41
	48	110000	cs6
	56	111000	cs7
Низкоприоритетная очередь	Прочие	XXXXXX	

Таблица 6-5

6.4.6. Порт TCP / UDP

TCP и UDP используют 16-битный порт для распознавания приложений. Обычно сервер использует порт для распознавания. Например, TCP-порт FTP-сервера — это 21-й порт, TCP-порт сервера Telnet — 23-й, UDP-порт TFTP-сервера — 69-й. Все службы TCP/IP используют общеизвестные порты с 1 по 1023.

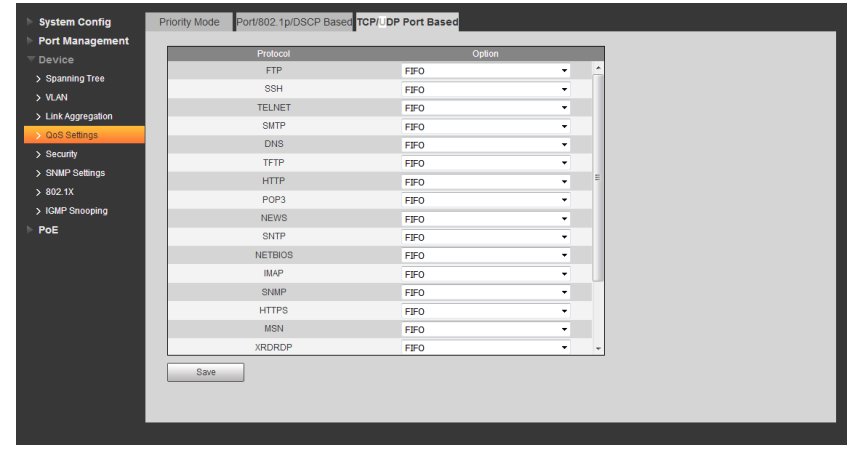


Рисунок 6-16

На рисунке 6-16 показано, что коммутатор этой серии может обрабатывать принятые пакеты на основе TCP/UDP-порта, такого как FTP, SSH, TELNET, SMTP и DNS. Здесь можно установить высокий, низкий приоритет пакета или сбросить его. Настройка по умолчанию — FIFO.

Пример конфигурации.

1. Подключение к сети

- На рисунке 6-17 показано подключение устройства к FTP-серверу и использование порта 1 и порта 2 для подключения устройства.
- Правильно настройте функцию QoS, порт 2 имеет более высокий приоритет, чем порт 1, и заблокирован для доступа к FTP-серверу.

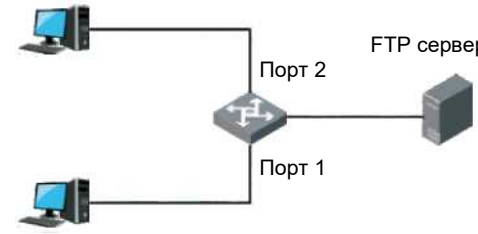


Рисунок 6-17

2. Настройки

(1) Установите режим устройства в режим all high before low («вначале высокий приоритет»)

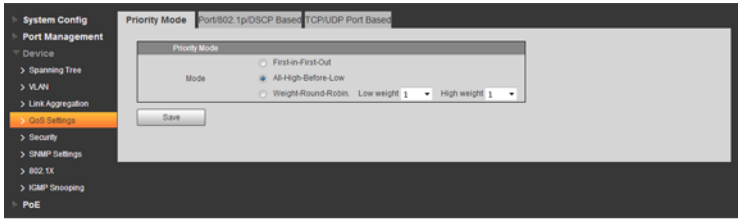


Рисунок 6-18

(2) Установите порту 2 высокий приоритет.

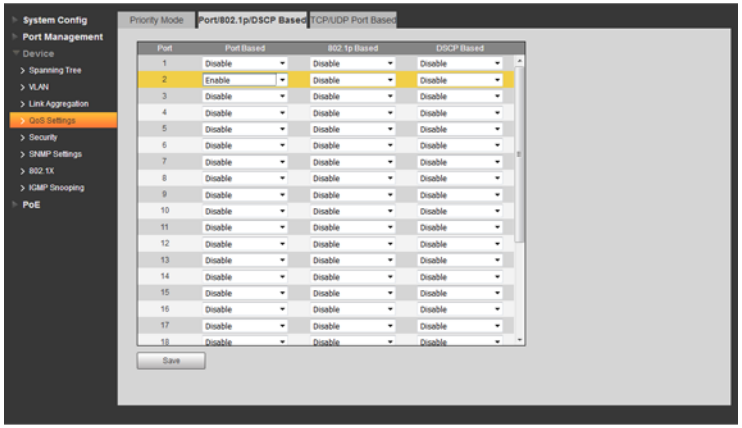


Рисунок 6-19

(3) Установите отказ от FTP-пакетов данных, заблокируйте доступ к FTP-серверу.

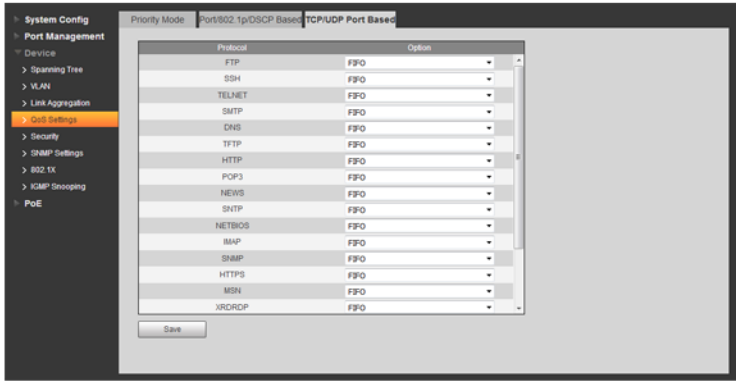


Рисунок 6-20

6.5. Безопасность

MAC (Media Access Control) регистрирует взаимосвязь между MAC-адресом и портом, а также порт, относящийся к VLAN, и т. д.

6.5.1. Список MAC-адресов

Когда устройство пересылает пакет, оно производит поиск MAC-адреса назначения пакета по списку MAC-адресов. Если в списке MAC-адресов имеется элемент, соответствующий MAC-адресу назначения пакета, устройство использует выходной порт для пересылки пакета. Если в списке нет элемента, соответствующего MAC-адресу назначения пакета, устройство переходит в широковещательный режим для пересылки пакета через соответствующую VLAN (за исключением входного порта). Более подробная информация о MAC-адресе приведена на следующем рисунке.

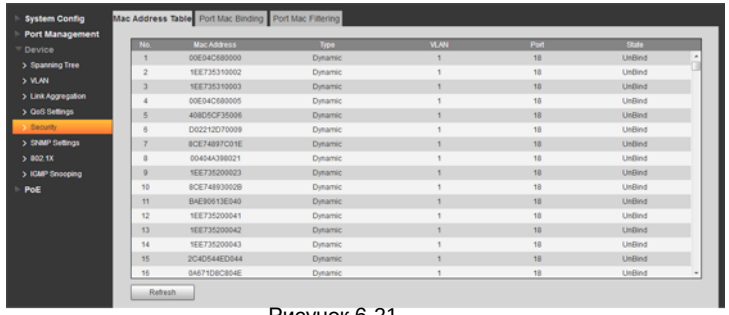


Рисунок 6-21

6.5.2. Привязка MAC-адресов к порту

На экране, показанном на рисунке 6-22, щелкните текущий подключенный порт, установите функцию привязки MAC-адреса, чтобы только текущий порт перенаправлял пакеты к привязанному MAC-адресу.

Рисунок 6-22

Пример конфигурации.

1 Сетевое подключение

Пользователь открыл веб-интерфейс для привязки MAC-адреса к порту, чтобы порт мог использоваться только текущим устройством.

2 Настройки

(1) Из раздела **Device Management > Security** («Управление устройствами > Безопасность»), перейдите в интерфейс **MAC Address Table** («Таблица MAC-адресов»).

(2) Выберите интерфейс **Port MAC Binding** («Привязка MAC-адресов к порту»).

(3) Выберите порт, состояние соединения которого помечено зеленым, а затем нажмите Bind («Привязать»). См. рисунок 6-23.

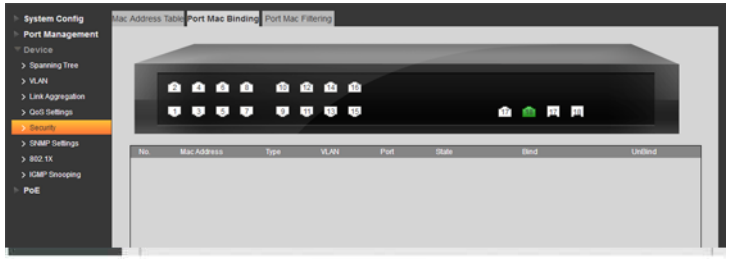


Рисунок 6-23

6.5.3. Фильтрация MAC-адресов для порта

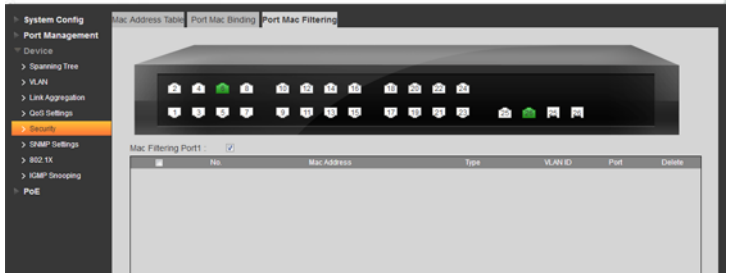


Рисунок 6-24

Как показано на рисунке 6-24, функция используется для ограничения разрешенных MAC-адресов пакетов для порта, чтобы предотвратить возможную атаку. После того как порт был настроен с помощью этой функции, при приеме пакета будет происходить проверка, совпадает ли MAC-адрес источника пакета с разрешенным MAC-адресом:

- Если адрес совпадает, пакет считается одобренным и его обработка продолжится.
- Если он отличается, то пакет считается неодобренным, и он будет отброшен.

6.6. Настройки SNMP

Сеть SNMP включает в себя два элемента: NMS и агент.

- NMS (Network Management System — система управления сетью) — это сетевой администратор SNMP. Он обеспечивает удобный интерактивный интерфейс. Подходит для выполнения большинства задач сетевого администратора по управлению.
- Агент является объектом управления в сети SNMP. Он получает и обрабатывает запросы NMS. В некоторых случаях, когда статус порта изменился, агент может автоматически отправлять сигнал оповещения в NMS.

При управлении устройством с помощью NMS уделяется значительное внимание некоторым параметрам, таким как статус порта, скорость ЦП и т. д. Все эти параметры вместе называются Management Information Base (MIB — база управляющей информации). Каждый из параметров называется узлом MIB. MIB определяет слои узлов и свойства управляемых объектов, например имя, права доступа, тип данных и т. д. У каждого Агента есть свой MIB. Совокупность управляемых устройств имеет собственный MIB-файл, и компиляция этих MIB-файлов в NMS может генерировать MIB каждого устройства. NMS считывает и записывает узлы MIB в соответствии с настройками прав доступа, чтобы управлять Агентом. См. следующий рисунок, иллюстрирующий отношения между NMS, Агентом и MIB.

Рисунок 6-19

MIB принимает древовидную организацию, состоящую из множества узлов. Каждый узел представляет собой один управляемый объект. Управляемый объект может использовать уникальный номер, представляющий собой путь, начинающийся с корневого каталога. Этот номер называется Object Identifier (OID — идентификатор объекта). Подробную информацию см. на следующем рисунке. Управляемый объект B может использовать последовательный номер {1.2.1.1} для идентификации. Это OID управляемого объекта.

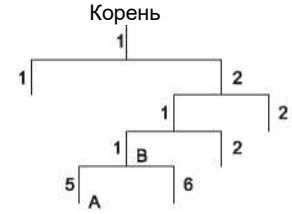


Рисунок 6-20

SNMP предоставляет три основные операции для реализации взаимодействия между NMS и агентом:

- Get: NMS использует ее для поиска значения одного или нескольких узлов MIB агента.
- Set: NMS использует ее для установки значения одного или нескольких узлов MIB агента.
- Trap: NMS использует ее для отправки trap-сообщений в NMS. Агент не требует от NMS отправить ответное сообщение, а NMS не отвечает на trap-сообщения.

SNMPv1, SNMPv2 и SNMPv3 поддерживают операции с ловушками (trap).

Версия протокола SNMP

На текущий момент агент поддерживает SNMPv1, SNMPv2 и SNMPv3.

SNMPv1 принимает имя сообщества для сертификации. Имя сообщества подобно паролю и служит для ограничения связи между NMS и Агентом. Если имя сообщества NMS и имя сообщества управляемых устройств не совпадают, NMS и агент не смогут установить SNMP-соединение, что означает, что NMS не сможет получить доступ к Агенту и не примет предупреждение от Агента.

- SNMPv2 принимает имя сообщества для сертификации. SNMPv2c расширил функции SNMPvl, поддерживает больше типов операций и больше типов данных, предоставляет многочисленные коды ошибок и может точно различать ошибки.
- SNMFV3 применяет модель безопасности на основе имени пользователя User-Based Security Model (USM) для сертификации. Сетевой администратор может установить функцию аутентификации и шифрования. Проверка подлинности заключается в проверке действительности отправителя сообщения, чтобы избежать незаконного доступа. Шифрование заключается в шифровании сообщений связи между NMS и Агентом в случае подслушивания. Функция аутентификации и шифрования может повысить уровень безопасности между NMS и Агентом.

Примечание:

Убедитесь, что NMS и Агент используют одну и ту же версию SNMP, иначе соединение NMS и Агента может завершиться неудачей.

6.6.1. SNMP

Этот интерфейс предназначен для настройки SNMP. V1 и V2 включают следующие настройки.
Подробную информацию см. в таблице 6-6.

Рисунок 6-27

На рисунке 6-27 интерфейс настройки SNMP V1 и V2 включает порт SNMP, версию, сообщества с правами чтения, записи, адрес ловушки и ее порт.
На рисунке 6-28 показан интерфейс настройки SNMP V3.

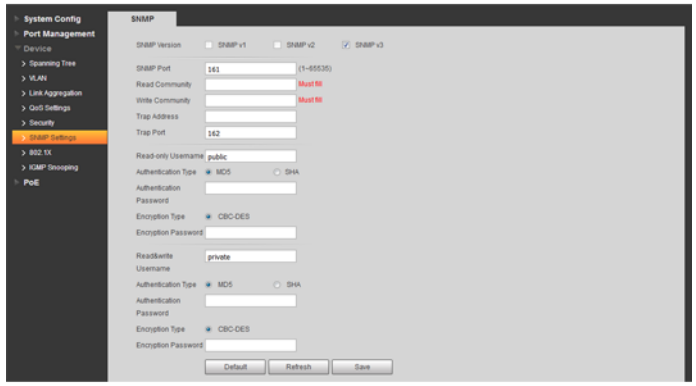


Рисунок 6-28

Подробную информацию см. в таблице 6-6.

Наименование	Примечание
Чтение общей строки	Имя сообщества, которое сетевой администратор использует для доступа. Право чтения. Настройка по умолчанию — общего пользования.
Запись общей строки	Имя сообщества, которое сетевой администратор использует для доступа. Право записи. Настройка по умолчанию — частный доступ.
Адрес ловушки	Указывает IP-адрес сервера.
Порт ловушки	Необходим для установки порта назначения ловушки.
Имя пользователя только для чтения	Задайте имя пользователя только для чтения. Только для V3.
Режим аутентификации	Устанавливает режим аутентификации при выборе уровня безопасности «Аутентификация без шифрования» или «Аутентификация и шифрование». Режим аутентификации включает MDS и SHA.
Пароль аутентификации	Устанавливает пароль аутентификации.
Режим шифрования	Когда режим аутентификации — «Аутентификация и шифрование», здесь устанавливается режим шифрования. Эта серия коммутаторов поддерживает только 3DES.
Пароль шифрования	Когда режим аутентификации «Аутентификация и шифрование», здесь устанавливается пароль шифрования.
Пароль чтения/записи	Он предназначен для установки прав пользователя на чтение/запись.

Таблица 6-6

Пример конфигурации.

SNMPv1/v2

1. Подключение к сети

   См. рисунок 6-29, NMS подключается к коммутатору и должен отвечать следующим требованиям.

   NMS контролирует и управляет коммутатором через SNMPv1 и SNMPv2.

   Коммутатор может автоматически отправлять сообщение Trap на NMS, когда есть неисправность.

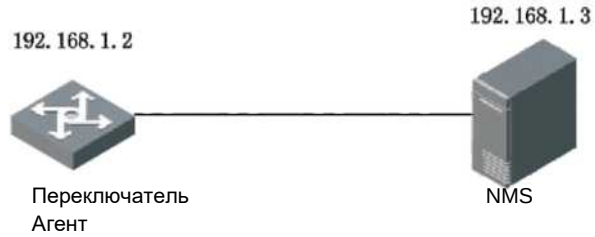


Рисунок 6-29

2. Настройки
   1) На панели навигации Device > SNMP Settings, («Устройство > Настройки SNMP») система переходит в интерфейс SNMPv1 по умолчанию.
   2) Выберите версию SNMP v1 или v2.
   3) Номер порта SNMP — 161, установите «Сообщество с правом чтения», «Сообщество с правом записи», «Адрес ловушки» и «Порт ловушки». См. рисунок 6-30.

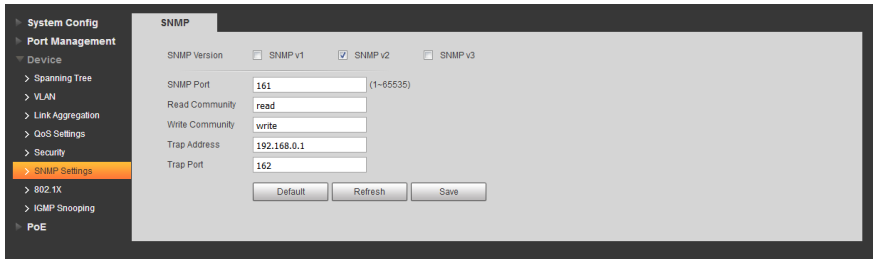
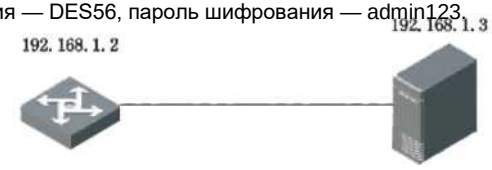


Рисунок 6-30

SNMPv3

1. Подключение к сети

- В соответствии с рисунком 6-31, NMS подключается к коммутатору, и реализует следующие требования.
- NMS контролирует и управляет коммутатором через SNMPv3.
- Коммутатор может автоматически отправлять сообщение Trap на NMS, когда есть неисправность.
- Когда NMS подключает Агента через SNMP, требуется аутентификация. Режим аутентификации MD5, пароль аутентификации — admin123.
- Сообщение SNMP между NMS и Агентом должно быть зашифровано, режим шифрования — DES56, пароль шифрования — admin123.



Переключатель Агент MS

Рисунок 6-31

2. Настройки

(1) На панели навигации Device > SNMP Settings («Устройство > Настройки SNMP») система по умолчанию переходит на интерфейс SNMPv1.
(2) Выберите версию SNMP как v3.
(3) Номер порта SNMP — 161, установите «Сообщество с правами на чтение», «Сообщество с правами на запись», «Адрес ловушки» и «Порт ловушки». Порт ловушки — 162.
(4) Введите имя пользователя только для чтения в поле «user»
(5) Режим аутентификации — Md5.
(6) Пароль аутентификации — «admin123».
(7) Режим шифрования — «CBC-DES»
(8) Пароль шифрования и пароль подтверждения — «admin123».
(9) Введите имя пользователя для чтения/записи «user1».
(10) Режим аутентификации — «Md5».
(11) Пароль шифрования — «admin123»
(12) Режим шифрования — «CBC-DES»
(13) Пароль шифрования — «admin123»
(14) Нажмите кнопку Save («Сохранить»). См. рисунок 6-32.

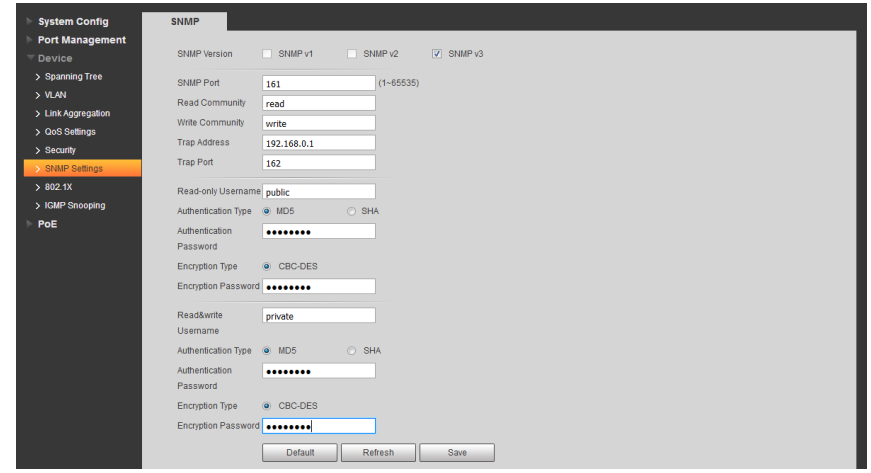


Рисунок 6-32

6.7. 802.1x

IEEE 802.1x — это стандарт аутентификации пользователя для доступа в сеть, который разработан IEEE. Это тип протокола управления доступом к сети на основе порта, поэтому на порте устройства должна быть настроена точная функция проверки подлинности 802.1 x. Что касается пользовательского устройства, к которому обращается порт, то необходимо контролировать доступ к источнику сети через аутентификацию.

6.7.1. Сетевая структура 802.1x

Система 802.1x включает в себя три части: это клиент, устройство и сервер аутентификации, которые показаны на рисунке 6-33.

Агент Сервер аутентификации

Заказчик

Рисунок 6-33

- Клиент — это пользовательское терминальное устройство, которое требует доступа к локальной сети и проходит аутентификацию сетевым конечным устройством в ней. На клиенте должно быть установлено клиентское программное обеспечение, поддерживающее аутентификацию 802.1x.
- Сетевое конечное устройство — это устройство, которое контролирует клиентский доступ в локальной сети. Оно расположено между клиентом и сервером аутентификации, который предоставляет порт доступа к локальной сети для клиентов (физический порт или логический порт) и реализует аутентификацию подключенного клиента посредством взаимодействия с сервером.
- Сервер аутентификации используется для реализации аутентификации, авторизации и биллинга, как правило, это сервер RADIUS (сервер удаленной аутентификации пользователя). Сервер проверки подлинности может проверить правомерность доступа клиента в соответствии с информацией аутентификации клиента, отправленной с сетевого конечного устройства, и по завершении сообщить устройству о результатах проверки. Сетевое конечное устройство определяет, разрешать ли клиентский доступ или нет. Роль сервера аутентификации может быть заменена устройством в малой сетевой среде, то есть устройство будет осуществлять локальную аутентификацию, авторизацию и биллинг клиента.

6.7.2. Контролируемый/неконтролируемый порт аутентификации 802.1x

Порты доступа к локальной сети, предоставляемые устройством для клиентов, можно разделить на две группы логических портов — контролируемые и неконтролируемые. Любой кадр, который прибыл в порт, может отображаться как на контролируемом порте, так и на неконтролируемом порте.

- Неконтролируемый порт всегда находится в состоянии двунаправленного соединения, которое в основном используется для передачи пакета аутентификации и гарантирует, что клиент всегда может отправить или получить пакет аутентификации.
- Контролируемый порт всегда находится в состоянии двунаправленного соединения в статусе авторизации, который используется для передачи пакета; запрещается получать какой-либо пакет от клиента, когда он находится в состоянии несанкционированного доступа.

6.7.3. Режим триггера аутентификации 802.1x

Процесс аутентификации 802.1x активно запускается клиентом, его также можно запустить с помощью устройства.

Режим активного триггера клиента

- Многоадресный триггер: клиент активно отправляет пакет запроса аутентификации на устройство для запуска аутентификации, адрес назначения пакета — это MAC-адрес многоадресной рассылки 01-80-C2-00-00-03.
- Широковещательный триггер: клиент активно отправляет пакет запроса аутентификации на устройство, чтобы инициировать аутентификацию, адресом назначения пакета является широковещательный MAC-адрес. Режим способен решить проблему, из-за которой устройство не может получить запрос аутентификации от клиента, потому что некоторые устройства не поддерживают многоадресный пакет, указанный выше, в сети.

Режим активного триггера устройства

Режим активного триггера устройства используется для поддержки клиента, который не может активно отправлять пакет запроса проверки подлинности; есть два типа активной триггерной аутентификации устройства:

- Многоадресный триггер: устройство активно отправляет пакет запроса типа идентификации для запуска аутентификации клиенту с регулярными интервалами (по умолчанию это 30 секунд).
- Одноадресный триггер: когда устройство получает неизвестный пакет MAC-адреса источника, оно будет активно отправлять пакет запроса с идентификатором на один MAC-адрес, чтобы инициировать аутентификацию. Оно снова отправит пакет, если устройство не получит ответ клиента во время настройки.

6.7.4. Статус авторизации порта

Можно настроить статус авторизации порта так, чтобы контролировать, должен ли пользователь, подключенный через порт,
проходить аутентификацию перед посещением сетевого источника. Порт поддерживает три следующих состояния авторизации:

- Форсированная авторизация: означает, что порт всегда находится в состоянии разрешенного доступа, что позволяет пользователям посещать сетевой источник без аутентификации.
- Форсированный неавторизованный доступ: означает, что порт всегда находится в состоянии неавторизованного доступа, не позволяя выполнять аутентификацию пользователей. Устройство не будет осуществлять аутентификацию клиента, который обращается к порту.
- Порт на основе 802.1x: означает, что изначально порт находится в статусе неавторизованного доступа, не позволяя пользователям посещать сетевой источник. Порт будет переключен на авторизованный статус, если пользователи пройдут аутентификацию, и тогда они смогут посещать сетевой источник.

Пример конфигурации.

1. Сетевые требования
IP-адрес клиента — 192.168.1.1 /24 сегмент, IP-адрес сервера аутентификации — 192.168.1.100, и это требуется для аутентификации сервером аутентификации, когда доступны все порты устройства.
2. Шаги конфигурации
(1) Включить функцию аутентификации, все порты включены на основе аутентификации 802.1x, как показано на рисунке 6-34.

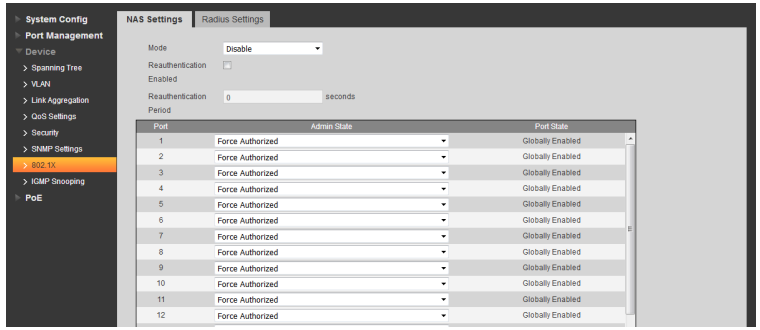


Рисунок 6-34

(2) Настройте адрес сервера аутентификации, как показано на рисунке 6-35.

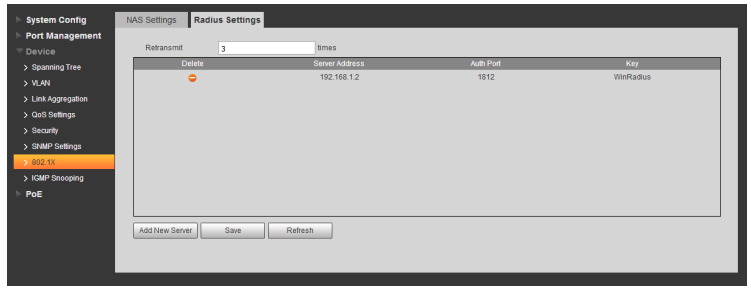


Рисунок 6-35

6.8. Отслеживание трафика, передающегося по протоколу управления сетью Интернет

IGMP snooping (процесс отслеживания трафика, передающегося по протоколу управления сетью Интернет) управляется устройством второго уровня, которое генерирует таблицу перенаправления многоадресной передачи второго уровня посредством отслеживания пакета IGMP между устройством третьего уровня и хостом. Процесс предназначен для управления пересылкой пакетов многоадресной передачи и реализации второго уровня управления, необходимого для распространения этих пакетов.

6.8.1. Теория IGMP snooping

Устройство второго уровня IGMP snooping может установить сопоставление для адреса порта и MAC-адреса через анализ по принятому пакету IGMP и осуществлять многоадресную передачу в соответствии с отношениями сопоставления.

Данные многоадресной передачи будут транслироваться в сети второго уровня, если устройство второго уровня не использует IGMP snooping; после того, как устройство второго уровня будет использовать IGMP snooping, известные многоадресные данные группы многоадресной рассылки не будут транслироваться в сети второго уровня, но будут переданы многоадресной рассылкой назначенным получателям.

IGMP snooping может перенаправлять информацию только необходимым получателям, используя многоадресную рассылку второго уровня, что дает следующие преимущества:

- Уменьшается широковещательная рассылка пакетов в сети второго уровня, сохраняя пропускную способность сети;
- Повышается безопасность многоадресного рассылки информации;
- Становится удобной реализация индивидуального биллинга для каждого хоста.

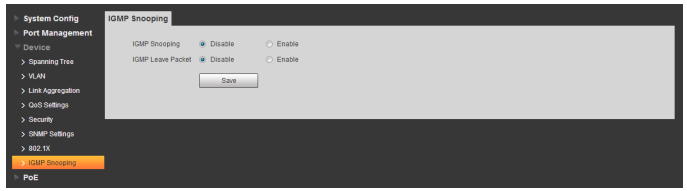


Рисунок 6-36

Интерфейс конфигурации IGMP snooping показан на рисунке 6-36.

- IGMP snooping: включение или отключение функции IGMP snooping.
- IGMP Leave Packet: включить или отключить функцию быстрого исключения.

7 PoE

7.1. Настройки PoE

Power over Ethernet (PoE) означает, что устройство использует порт Ethernet для передачи электропитания устройству через кабель витой пары. Функция PoE реализует централизованное энергоснабжение и простое аварийное дублирование. Сетевой терминал использует один простой сетевой кабель без внешнего источника питания. Он соответствует стандартам IEEE 802.3af и IEEE 802.3at и использует универсальный общепризнанный порт питания. Он используется для IP-камер, IP-телефонов, точек беспроводного доступа, переносных зарядных устройств, POS, сбора данных и т. д.

См. рисунок 7-1 с системой PoE. На нем изображено питание PoE, оборудование снабжение электропитанием (PSE), интерфейс питания (PI) и питание устройства (PD).

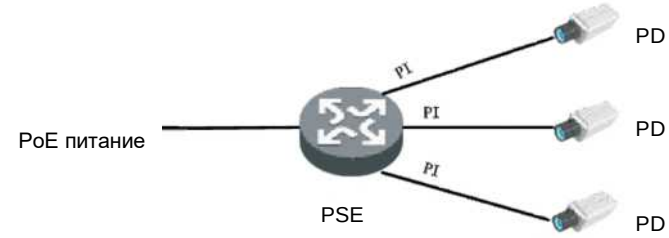


Рисунок 7-1

1 PoE питание
PoE обеспечивает питание всей системы.

2 PSE
PSE должен напрямую обеспечивать питание PD. PSE поддерживает такие функции, как поиск, обнаружение PD, классификация PD и обеспечение его питанием, управление потреблением энергии, проверка соединения PD и т. д.

3 PI
PI относится к интерфейсу Ethernet, который имеет функцию PoE. Он называется портом PoE. Он включает FE и GE.
Пульт дистанционного управления PoE имеет два режима:
- Сигнальные провода — PSE использует пары (1, 2, 3, 6) для передачи данных в кабеле витой пары категории 3/5 для питания постоянным током при передаче данных в PD.
- В качестве запасных проводов PSE использует пары (4, 5, 7, 8), непередающие данные в кабеле витой пары категории 3/5, для питания постоянным током PD.

Примечание:

Режим питания зависит от технических характеристик PD. Выбранный режим должен поддерживать PSE и PD одновременно. Если PSE и режим питания PD не совпадают (например, PSE не поддерживает резервное питание от электросети, или PD поддерживает только резервное питание), используйте преобразователь, чтобы обеспечить питание PD.

4 PD

PD означает устройство, принимающему энергию от PSE. Это может быть IP-телефоном, беспроводной точкой доступа, портативным зарядником, POS, сетевой камерой и т. д.

Когда PD питается от устройства PoE, он может подключаться к другому устройству для резервного питания. См. таблицу 7-1 с подробной информацией о настройке порта.

Наименование	Примечание
Порт	На рисунке панели выберите порт PoE. Выбранный порт будет отображаться в списке «Выбранные порты» в нижней части интерфейса. Примечание Порт 1 и 2 поддерживают Hi-PoE.
Состояние питания	Включить или отключить PoE на выбранных портах. Система не подает или резервирует питание для PD, подключенного к порту PoE, если порт PoE не включен с помощью функции PoE. Разрешается включить PoE для порта, если это не приведет к перегрузке питания PoE; в противном случае вам включать PoE не разрешено. По умолчанию, PoE отключен на порту PoE. Примечание Перегрузка мощности PSE. Когда общая потребляемая мощность всех портов превышает максимальную мощность PSE, система считает, что PSE перегружен.
Итоговое значение резервируемого энерго-потребления	Оно необходимо для установки зарезервированное значение общего потребления энергии порта PoE. Общее значение потребляемой мощности PoE относится к общему потреблению энергии для PD со всего порта PoE. Когда потребляемая мощность подключенного PD выше, чем общая потребляемая мощность PoE, она перестает обеспечивать питание PD.

Таблица 7-1

См. рисунок 7-2 с интерфейсом настройки.

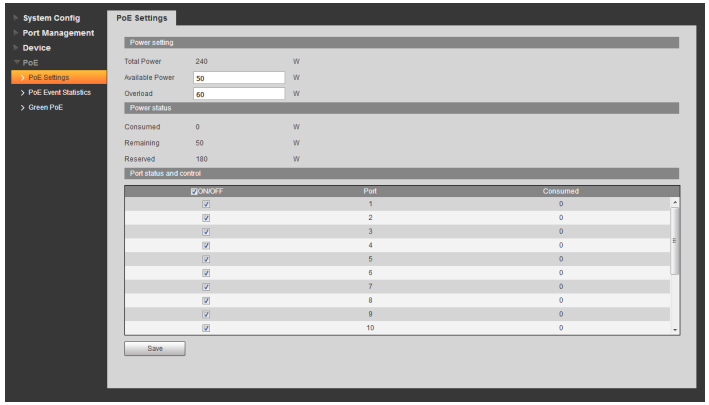


Рисунок 7-2

7.2. Статистика событий PoE

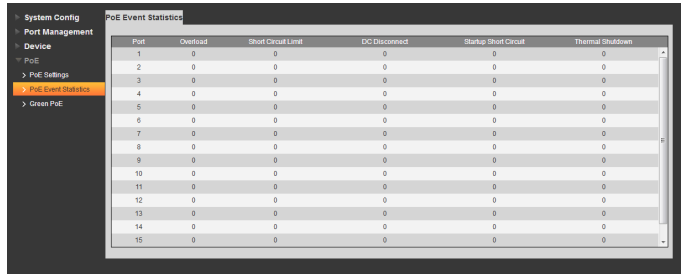


Рисунок 7-3

На рисунке 7-3 отображается статистика событий PoE для каждого порта. Он включает в себя перегрузку, лимит короткого замыкания, отключение постоянного тока. короткого замыкания сервера и термического отключения.

См. таблицу 7-2 с параметрами событий PoE.

Наименование	Примечание
Перегрузка	Ток рабочей мощности одного порта превысил текущий порог.
Ограничение короткого замыкания	Короткое замыкание при включении питания начинает посылать питание на порт.
Отключение питания	Питание одного порта выключено.
Короткое замыкание сервера	Короткое замыкание, когда питающая микросхема посылает питание.
Тепловое отключение	Температура питающей микросхемы слишком высока в результате короткого замыкания или по другой причине.

Таблица 7-2

7.3. Энергосберегающий PoE

На рисунке 7-4 показаны энергосберегающие параметры PoE. Функция PoE отключена в указанный период для экономии энергии. Когда период закончится, порт автоматически возобновляет подачу питания.

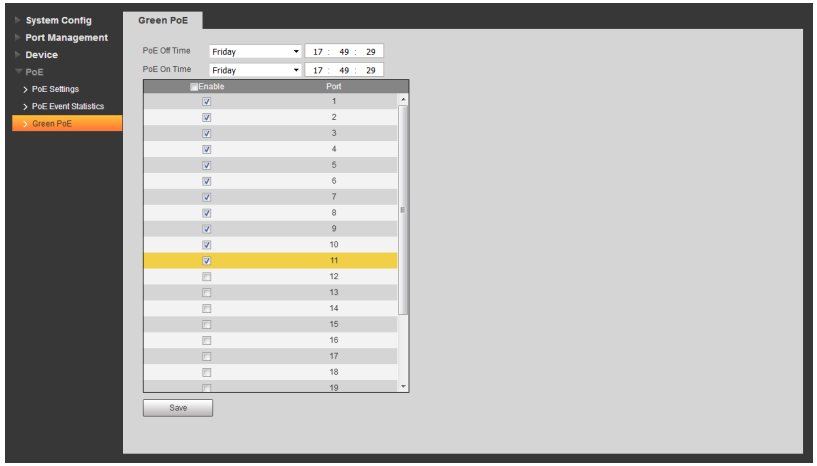


Рисунок 7-4

Информацию о настройке Green PoE см. в таблице 7-3.

Наименование	Примечание
Время отключения PoE	Входной ток одного порта превысил порог тока выходного порта.
PoE по времени	Передающий порт замыкается накоротко, когда чип подтверждает питание порта.
Порт	Выбираемые порты.

Таблица 7-3

Пример конфигурации.

1 Сетевое соединение
Порты 1–10 должны отключаться каждую субботу и каждое воскресенье и автоматически включаться каждый понедельник.

2 Настройки
(1) Установите период отключения порта с субботы по воскресенье и автоматическое возобновление питания в понедельник.
(2) Установите порты.
(3) Нажмите Save («Сохранить»). Подробную информацию см. на рисунке 7-5.

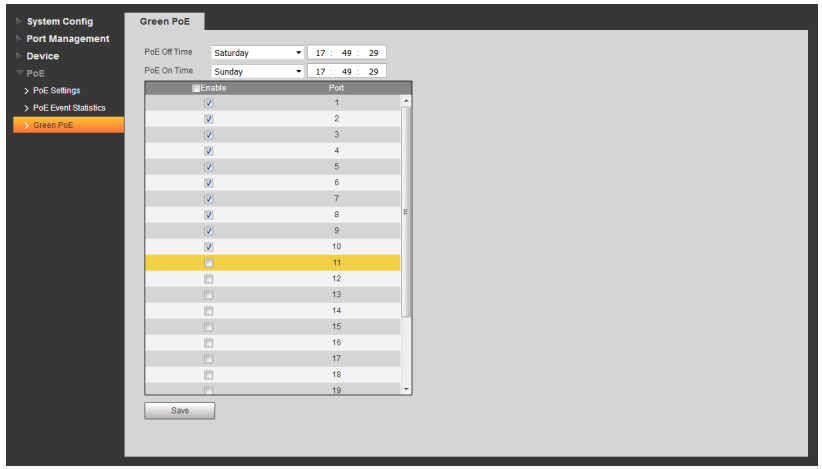


Рисунок 7-5

- Данное руководство пользователя предназначено только для справки.
- В интерфейсе пользователя могут быть небольшие отличия.
- Все проектные решения и программы могут меняться без предварительного письменного оповещения.
- Все товарные знаки и зарегистрированные товарные знаки являются собственностью соответствующих владельцев.
- Если вы нашли неточность или противоречие, см. наши последние разъяснения.
- Для получения дополнительной информации приглашаем посетить наш веб-сайт.