26-портовый управляемый POEкоммутатор Optimus UMG1-26/24PM_v.1 Руководство пользователя

Содержание

Глава 1: Общая информация 6
1.1 Целевая аудитория 6
1.2 Обозначения, принятые в настоящем руководстве 6
Глава 2 Вводная информация о продукте 7
2.1 Вводная информация о продукте 7
2.2 Передняя панель 8
2.4 Список функций интерфейса 11
Глава 3: Управление коммутатором 15
3.1 Webавторизация 15
3.2 Состав веб-интерфейса 17
3.2.1 Системное сообщение 18
3.2.2 Статистика трафика (Trafficstatistics) 19
3.3 Сведения о журналах (Loginformation) 19
3.3.1 Список журналов (Loglist) 20
3.3.2 Logsave (Функция сохранения журнала) 22
Глава 4: Управление портом (Portmanagement) 23
4.1 Конфигурация порта (Portconfiguration) 23
4.2 Изоляция порта (Port isolation) 24
4.3 Зеркалирование портов (Portmirroring) 25
4.4 Ограничение скорости порта (Portspeedlimit) 26
4.5 Управление штормами (Stormcontrol) 27
4.6 Энергосбережение порта (Portenergysaving) 29
Глава 5 : Управление POE (POE management) 29
5.1 Управление портом POE (Port POE management) 29

5.2 Информация об устройстве (Deviceinformation) 30

5.3 Настройка графика источника питания (Timingsupplyconfiguration) 31
5.3.1 Конфигурация временного периода (Timeperiodconfiguration) 31
5.3.2 Настройка графика источника питания (Timingpowersupplyconfiguration) 33

5.4 Интеллектуальная конфигурация источника питания (Intelligentpowersupplyconfiguration) 33

Глава 6: Управление уровня 2 (Layer 2 Management) 34

6.1 Таблица MAC-адресов (MAC Address Table) 34
6.2.2 Конфигурация VLAN (VLANConfiguration) 39
6.2.3 Конфигурация voice VLAN (Voice VLAN Configuration) 42
Описание: 44
6.2.4 Конфигурация MAC VLAN (MAC VLAN Configuration) 44
6.2.5 Конфигурация IP VLAN (IP VLAN Configuration) 45

6.3 Агрегирование каналов (LinkAggregation) 46
6.3.1 Конфигурация статического агрегирования каналов (StaticLinkConfiguration) 47
6.3.2 Конфигурация динамического агрегирования (DynamicAggregationConfiguration) 48
6.3.3 Информация об агрегировании каналов (LinkAggregationInformation) 50

6.4 Конфигурация MSTP (MSTPconfiguration) 51
6.4.1 Глобальная конфигурация (GlobalConfiguration) 52
6.4.2 InstanceConfiguration 55
6.4.3 PortInstanceConfiguration 56
6.4.4 Конфигурация порта (PortConfig) 59

6.5 Защита от образования петель (Loopprotection) 60
6.5.1 Глобальная конфигурация (Globalconfiguration) 61
6.5.2 Конфигурация порта (PortConfiguration) 61

6.6 DHCP-snooping (Отслеживание DHCP-пакетов) 62
6.6.1 Глобальная конфигурация (Global Configuration) 64
6.6.2 Staticbinding 65

6.6.3 Управление портами (Port Management) 66

6.7 IGMP-snooping (Отслеживание IGMP-пакетов) 66
6.7.1 IGMP-snooping 68
6.7.2 IGMP-snoopingVLANconfiguration (Конфигурация VLAN с отслеживанием IGMP-пакетов) 69
6.7.3 Staticmulticast 70

6.8 Конфигурация 802.1x (802.1xconfiguration) 72
6.8.1 Конфигурация (Configuration) 77
6.8.2 Настройки сервера RADIUS (RADIUS server settings) 80
6.8.3 Аутентификация на основе порта (Port-basedauthentication) 82

Глава 7: Расширенные настройки (Advancedsettings) 83

7.1 КонфигурацияQOS (QOSconfiguration) 83
7.1.1 Глобальная конфигурация (Globalconfiguration) 88
7.1.2 Управление портом (PortConfig) 91

7.2 Конфигурация ACL (ACL Configuration) 92
7.2.1 Конфигурация MACACL (MACACLConfiguration) 93
7.2.2 Конфигурация IP ACL (IP ACL Configuration) 95
7.2.3 Конфигурация временного диапазона (TIMERANGEConfiguration) .. 97
7.2.4 Конфигурация ГруппыACL (ACL Group Configuration) 100

7.3 Конфигурация SNMP (SNMP Configuration) 101
7.3.1 Системная информация (Systeminformation) 104

7.4 Конфигурация RMON (RMONConfiguration) 105
7.4.1 Группа событий (EventGroup) 107
7.4.2 Группа статистики (StatisticalGroup) 108
7.4.3 Группа истории (HistoryGroup) 109
7.4.4 Группа аварийных сигналов (AlarmGroup) 109

7.5 Конфигурация LLDP (LLDPConfiguration) 111
8.5.1 Глобальная конфигурация (GlobalConfiguration) 115
8.5.2 Конфигурация порта (PortConfiguration) 116
7.5.3 Конфигурация порта (PortConfiguration) 117

7.6 Конфигурация NTP (NTPConfiguration) 117
7.6.1 Глобальная конфигурация NTP (NTP Global configuration) 117

7.6.2 Конфигурация сервера NTP (NTPserverconfiguration) 118
7.7 Защита от атак (Anti-attack) 118
Глава 8: Управление системой (SystemManagement)..... 119
8.1 Пользовательские настройки (UserSettings) 119
8.2 Настройки сети (Networksettings)..... 120
8.3 Конфигурация сервисов (Serviceconfiguration) 121
8.3.1 TELNET-сервис (TELNETservice) 122
8.3.2 SSH-сервис (SSHservice)..... 122
8.3.3 HTTP-сервис (HTTPservice)..... 123
8.4 Управление конфигурацией (Configurationmanagement) 126
8.5 Обновление прошивки (Firmwareupgrade) 126
8.6 Диагностический тест (Diagnostictest) 127
8.6.1 Пинг (Pingdetection)..... 127
8.6.2 Трассировка (Tracert detection)..... 128
8.6.3 Обнаружение сетевого кабеля (Networkcabledetection) 129
8.7 Перезагрузка системы (Restart the system)..... 131

Глава 1: Общая информация

Настоящее руководство предназначено для того, чтобы помочь вам правильно использовать коммутатор. Руководство включает описание рабочих характеристик коммутатора и подробное описание конфигурации. Пожалуйста, внимательно прочтите руководство перед началом использования устройства.

1.1 Целевая аудитория

Настоящее руководство предназначено для установщиков и системных администраторов, отвечающих за установку, настройку или обслуживание сети. Предполагается, что вы уже знакомы с протоколами управления, используемыми во всех сетях.

В настоящем руководстве также предполагается, что вы знакомы с терминологией, теоретическими принципами, практическими навыками и специальными знаниями о сетевых устройствах, протоколах и интерфейсах, связанных с сетью. Вы также должны иметь опыт работы с графическим пользовательским интерфейсом, интерфейсом командной строки, простым протоколом управления сетью и веб-браузером.

1.2 Обозначения, принятые в настоящем руководстве

В настоящем руководстве термины «коммутатор» и «этот продукт», упомянутые в статье, относятся к коммутатору управления сетью уровня 2, если не указано иное.

Текст, выделенный жирным шрифтом, обозначает название каждой функции коммутатора, например, страницу управления портами. Текст в «двойных кавычках», который появляется в тексте, обозначает существительное, которое появляется на странице конфигурации, например, «IP-адрес». В настоящем руководстве используются следующие специальные значки.

Значок	Обозначение
🕮Описание	Описание содержания операции,

	внесение необходимых дополнений и пояснений.
 Примечание	Напоминание о важном во время работы. Неправильная эксплуатация может привести к потере данных или повреждению оборудования.

Глава 2 Вводная информация о продукте

2.1 Вводная информация о продукте

Optimus UMG1-26/24PM_v.1 – 26-портовый управляемый PoE-коммутатор. Коммутатор оснащен 24 портами 10/100 Мбит/с с поддержкой PoE (технология передачи питания по сетевому кабелю вместе с данными), к каждому из которых можно подключать сетевые устройства (IP-камеры, IP-телефоны, беспроводные точки доступа).

24 порта соответствуют стандартам PoE IEEE802.3af/at. Каждый порт подает питание мощностью до 30Вт на сетевое оборудование при общем PoE-бюджете коммутатора 300 Вт. Это позволяет размещать оборудование в труднодоступных местах вне зависимости от расположения электрических розеток и минимизировать прокладку кабеля. Максимальная дальность подключения оборудования составляет 250 метров.

Предусмотрены 2 порта 10/100/1000 Мбит/с и 2 SFP 1000 Мбит/с порта для подключения коммутатора к локальной сети, сети интернет, видеорегистратору или другому коммутатору.

Поддерживает автоматическое определение MDI/MDIX на всех портах. Коммутатор распознает тип подключенного сетевого устройства и при

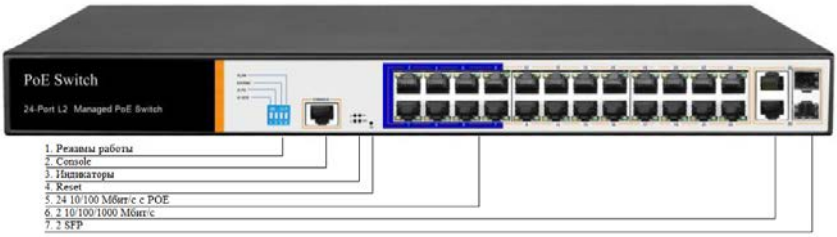
необходимости меняет контакты передачи данных, что позволяет использовать кабели, обжатые любым способом (кроссовые и прямые).

Имеет 4 режима работы AI Extend, AI VLAN, AI QOS, AI PoE.

Позволяет производить управление сетевыми протоколами через web-интерфейс и консоль.

2.2 Передняя панель

Включает индикаторы, порт RJ45, переключатели режимов, кнопку RST, порт SFP, порт консоли, как показано на рисунке ниже



Индикаторы

Индикаторы	Название	Цвет	Рабочий статус	Описание
POWER	Индикатор питания	Красный	Вкл.	Питание включено
			Выкл.	Нет питания от сети
POE	Индикатор питания POE	Желтый	Вкл.	Соответствующий порт RJ45 подключен к питаемому устройству и блок питания в норме

			Выкл.	Соответствующий порт RJ45 не подключен к питаемому устройству или источник питания неисправен
LINK/ACT	Индикатор соединения	Зеленый	Мигающий	Соединение установлено
			Выкл.	Соединение не установлено
SYS	Индикатор системы	Зеленый	Мигающий	Система работает нормально
			Выкл.	Система работает неправильно. Программное обеспечение повреждено

Переключатели режимов

Optimus UMG1-26/24PM_v.1 имеет 4 режима работы, которые могут выбираться переключателем на передней панели:

AI Extend
В данном режиме к PoE-портам (1-8) можно подключить устройства с PoE-питанием стандарта IEEE802.3af/at на расстояние до 250 метров. Скорость работы PoE-портов (1-8) составляет 10 Мбит/с. Порты 9-24 работают в стандартном режиме (расстояние до 100 метров, скорость до 100 Мбит/с).

AI VLAN
В данном режиме порты 1-24 изолированы друг от друга, коммутация осуществляется только с Uplink портами. Режим используется для того, чтобы исключить зависание системы в случае сетевого шторма, а также защищать подключенные устройства от сетевых атак.

AI PoE
В данном режиме коммутатор автоматически определяет рабочее состояние подключенного к нему устройства. В случае неисправности перезагружает его.

AI QOS
Для исключения задержек в видеопотоке, в режиме AI QOS приоритет в процессе передачи данных имеет видеопоток. Это даёт более стабильное и плавное изображение в случае сильной загруженности коммутатора.

- **Порт SFP**
  OptimusUMG1-26/24PM_v.1поддерживает 2 оптическихпортаGigabitSFP (SFP1, SFP2)

- **Кнопка RST**
  Когда коммутатор включен, нажмите кнопку для RSTдля перезапуска устройства.

- **Порт консоли**
  Порт консоли, используется для подключения к компьютеру или другому терминалу для управления или настройки коммутатора.

- **Задняя панель**
  Включает: разъем питания, клемму заземления

- **Разъем питания**
  Разъем питания100-240 В переменного тока 50/60 Гц для подключения кабеля питания в комплекте

- **Заземление**
  Пожалуйста, используйте заземляющий провод для предотвращения

электромагнитных наводок после удара молнии, чтобы продлить срок службы продукта.

2.4 Список функций интерфейса

1、Функции порта			
1.1	Управление портом (Port management)	Включить / отключить порт	
		Скорость (rate), дуплексный режим (duplex mode), настройки MTU (MTU settings)	
		Настройки управления потоком (Flowcontrolsettings)	
		Просмотр информации о порте (Portinformationview)	
1.2	Изоляция порта (Port isolation)	Поддержка одной группы изоляции (Singleisolationgroup)	Поддержка конфигурации глобальной изоляции портов (globalportisolation)
1.3	Зеркалирование портов (Port mirroring)	Поддержка зеркалирования	
1.4	Ограничение скорости порта (Portspeedlimit)	Поддержка настройки входящей и исходящей скорости	
1.5	Статистика трафика (Traffic statistics)	Поддержка статистики приема/отправки пакетов/ байтов	

1.6	Энергосбережение порта (Portenergysaving)	Поддержка технологии энергосбережения порта 802.3azEE	
2、Управление POE (POE management)			
2.1	Управление портом PoE (Port PoE management)	Включение/выключение источника питания POE (PoEpowersupply), настройка выходной мощности порта (portoutputpower)	
2.2	Информация об устройстве (Deviceinformation)	Просмотр температуры микросхемы POE (chiptemperature) и статуса выхода (outputstatus)	
2.3	Настройка источника питания (timingpowersupply)	Настройка режима электропитания, установка стратегии электропитания порта	
2.4	Конфигурация AI POE (AI POE configuration)	Установка общего питания, длительности нулевого расхода	
3、Функция уровня 2 (Layer 2 function)			
3.1	Таблица Mac-адресов (Mas Address table)	Поддержка добавления и удаления статических адресов, поддержка установки времени старения	
3.2	VLAN	Поддержка гибридного режима порта, режима транслирования	
		Поддержка режима обучения VLAN	
		Поддержка VoiceVLAN	
3.3	Агрегирование	Поддержка статического агрегирования	

	каналов (Link aggregation)	каналов	
		Поддержка динамического агрегирования LACP	
		Поддержка отображения на дисплее сведений об агрегировании каналов	
3.4	Управление штормом (Storm control)	Поддержка управления широковещательным штормом broadcast, multicastи unicast	
3.5	STP (spanning tree)	Поддержка 802.1d (STP)	Также поддерживает ERPS
		Поддержка 802.1w (RSTP)	
		Поддержка 802.1s (MSTP)	
3.6	DHCP-snooping	Поддержка статического связывания (staticbinding)	
		Поддержка конфигурации порта Untrust/IPSG	
3.7	IGMP-snooping (Отслеживание IGMP-пакетов)	Поддержка статического добавления, удаления	
		Поддержка динамическогоmulticastsnoopingv1/2/3	
4、Расширенные настройки (Advanced settings)			
4.1	QOS	На основании классификации 802.1p (COS)	

		На основании классификации DSCP	
		Поддержка стратегий планирования SP, WRR, DRR	
4.2	ACL	На основе MAC-адреса источника , MAC-адреса назначения, типа протокола), IP-адреса источника, IP-адреса назначения, номера порта	
		Поддержка управления временным диапазоном	
4.3	SNMP	Поддержка протокола управления сетью версии V1 / V2 / V3	
4.4	RMON	Поддерживает группы событий, группы статистики, группы истории и группы сигналов тревоги	
4.5	LLDP	Поддержка протокола обнаружения LLDP	
4.6	Защита от образования петель (Loopprotection)	Поддержка защиты образования петель в сети	
4.7	Конфигурация NTP (NTP configuration)	Поддержка выбора часового пояса, ручное добавление NTP-сервера	
4.8	Защита от атаки (Anti-attack)	Поддержка защиты от атак DDOS, ICMP	
5、Настройки системы (System settings)			
5.1	Настройки пользователя (User	Изменение пароля пользователя	

	settings)		
5.2	Настройки сети (Network settings)	Поддержка автоматического получения IP/статического IP	
5.3	Конфигурация сервиса (Service configuration)	Включение /выключение порта Telnet	
5.4	Настройка конфигурации (Configuration management)	сброс (reset)	
5.5	Обновление прошивки (Firmware upgrade)	Обновление до последней версии программного обеспечения	
5.6	Системный журнал (Log)	Логи пользователя, функционирование, статус, журнал событий	

Глава 3: Управление коммутатором

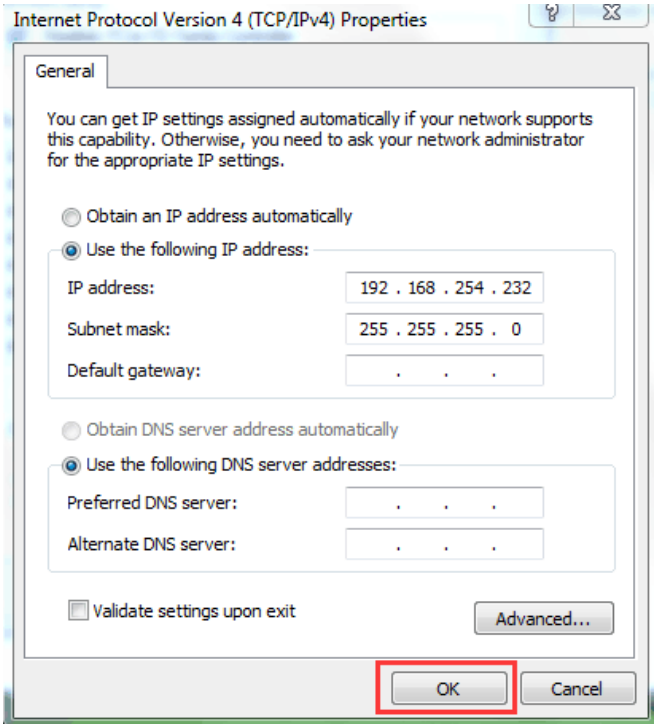
3.1 Webавторизация

Шаг 1

Подключите компьютер к любому порту RJ45 коммутатора с помощью сетевого кабеля.

Шаг 2

Вручную измените IP-адрес компьютера на 192.168.254.X (X - 2 ~ 254), маска подсети -255.255.255.0



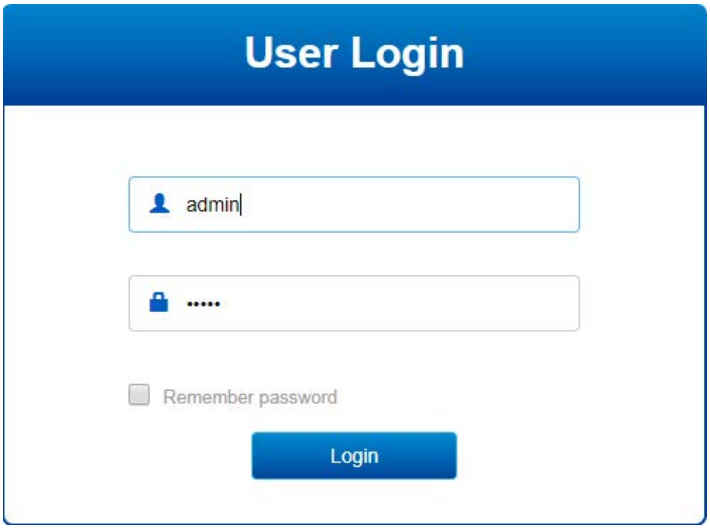
Шаг 3

Откройте браузер компьютера, введите 192.168.254.1 в адресной строке и

нажмите клавишу Enter.

Шаг 4

Введите имя пользователя и пароль по умолчанию «admin», а затем нажмите «Войти».

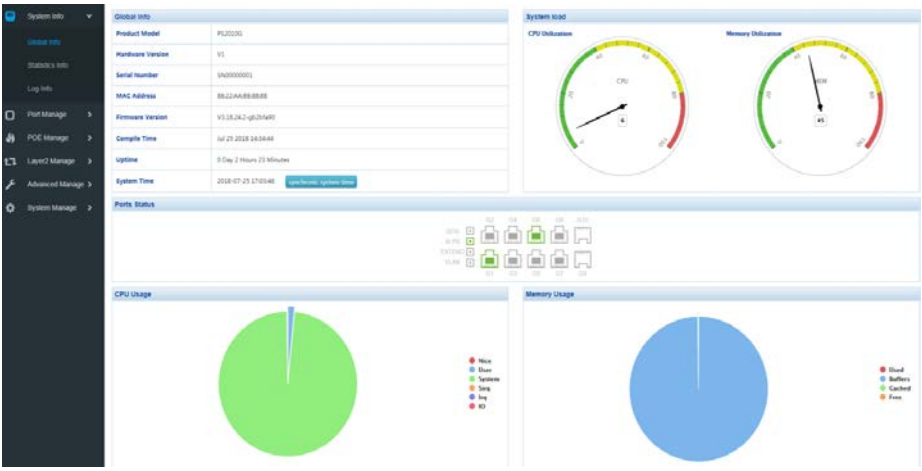


Шаг 5

Вы вошли в веб-интерфейс управления коммутатором и можете приступить к настройке коммутатора.

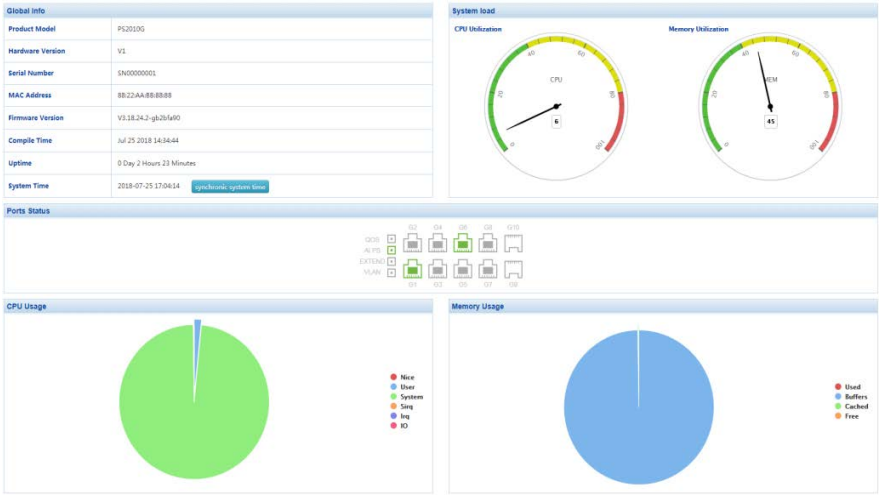
3.2 Состав веб-интерфейса

Начало работы в рабочем интерфейсе показано ниже.



3.2.1 Системное сообщение

На экране будут отображаться сведения о версиях программного обеспечения, оборудования, MAC-адресе, времени загрузки, системном времени, загрузке системы, состоянии порта, использовании ЦП и памяти.



📖Описание :

➢ При наведении указателя мыши на порт отображается номер порта, тип, скорость и информация о состоянии этого порта.

➢ Переключите режимы «AIQos», «AIPoe», «AIExtend» и «AIVLAN» напанеликоммутатора, изначокрежимов на интерфейсе станетзеленым.

3.2.2 Статистика трафика (Trafficstatistics)

Интерфейс статистики трафика отображает подробную информацию о пакетах, отправленных и полученных каждым портом, включая статистику количества отправленных и полученных пакетов, типа и длины фрейма передачи.

3.3 Сведения о журналах (Loginformation)

Система журналов, предоставляемая коммутатором, может записывать, классифицировать и управлять всей системной информацией, а также предоставляет сетевым администраторам мощную поддержку для мониторинга работы устройства и диагностики неисправностей. Системный журнал этого коммутатора разделен на восемь уровней.

Название уровня	Уровень	Описание
Emergencies (Чрезвычайные ситуации)	0	Система недоступна
Alerts (Оповещения)	1	Информация, которая требует немедленной реакции

Critical (Критическое)	2	Серьезная информация
Errors (Ошибки)	3	Сообщение об ошибке
Warnings (Предупреждения)	4	Предупреждающее сообщение
Notifications (Уведомления)	5	Обычная, но важная информация
Informational (Информация)	6	Уведомление с информацией, которую необходимо записать
Debugging (Отладка)	7	Информация, генерируемая в процессе отладки

Эта функция включает два списка страниц функций: список журналов (loglist) и экспорт журналов (logexport).

3.3.1 Список журналов (Loglist)

Системные журналы можно сохранять в двух разных местах: в буферах журналов (logbuffers) и в файлах журналов (logfiles). Информация из буфера журнала будет потеряна в случае перезапуска коммутатора. Информация в файле журнала в случае перезапуска сохранится. В списке журналов отображается информация системного журнала из файла журнала.

time	level	type	module	param	log
1970-01-01 08:17	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:17	5	Link	mono	G2	Interface[G2] state change to down.
1970-01-01 08:01	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:01	5	Enable	poe	G2	Interface[G2] poe power enable state change.
1970-01-01 08:01	5	Status	poe	G2	Interface[G2] poe power good state change.
1970-01-01 08:01	5	Connect	poe	G2	Interface[G2] poe disconnect.
1970-01-01 08:01	5	Enable	poe	G2	Interface[G2] poe power enable state change.
1970-01-01 08:01	5	Status	poe	G2	Interface[G2] poe power good state change.
1970-01-01 08:01	5	Link	mono	G2	Interface[G2] state change to down.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.
1970-01-01 08:00	5	Link	mono	G6	Interface[G6] state change to up.
1970-01-01 08:00	5	Link	mono	G2	Interface[G2] state change to up.

Описание:

Список системного журнала

Serial number (Серийный номер) : Отображает серийный номер записи журнала

Time (Время) : Отображает время создания записи журнала. Системный журнал может получить время локальной синхронизации после выполнения операции системного времени на странице системной информации.

Modulename (Название модуля) : Отображается функциональный модуль записи журнала, и из раскрывающегося списка можно выбрать информацию по определенному модулю.

Severitylevel (Уровень критичности) : Отображает уровень критичности записи журнала. Выберите уровень из раскрывающегося списка, чтобы посмотреть запись журнала, уровень которой меньше или равен необходимому значению.

Log Отображение содержимого записи журнала

information

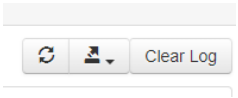
(Информация

Примечание: всего насчитывается восемь уровней критичности, от 0 до 7. Чем меньше значение, тем выше критичность. На данной странице отображается информация, записанная в буфере журнала (logbuffer). Максимальное количество отображаемых записей - 512.

3.3.2 Logsave (Функция сохранения журнала)

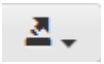
Благодаря функции экспорта журнала информацию из журнала, сохраненную в коммутаторе, можно экспортировать в виде файла для диагностики устройства и статистического анализа. В случаях сбоя системы вследствие серьезной ошибки вы можете экспортировать информацию из журнала после перезапуска и получить важные сведения о данной ошибке, это поможет провести диагностику устройства.

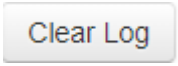
Войдите на страницу: System settings >> Log information >> Log export



Описание:

 Обновите страницу

 Нажмите эту кнопку, чтобы экспортировать информацию в файл журнала



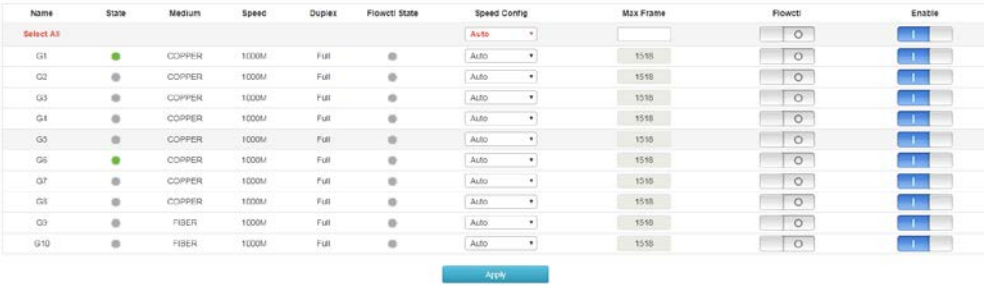
Очистите журнал

Глава 4: Управление портом (Portmanagement)

4.1 Конфигурация порта (Portconfiguration)

В разделе управления портами вы можете установить режим порта, скорость и другие параметры.

Нажмите на Portmanagement>>Portconfiguration на панели навигации, чтобы войти в интерфейс управления портами, как показано ниже:



Функции:

- **Состояние (State)**

СерыйПорт не подключен

ОранжевыйСкорость работы порта 100 Мбит/с

ЗеленыйСкорость работы порта 1000 Мбит/с

- **Скорость (Speed)**

Отображение скорости подключения текущего порта

- **Дуплексная передача (Duplex)**

Отображает рабочий режим текущего порта; half -полудуплекс, full- дуплекс.

- **Конфигурация скорости (Speed configuration)**

1） Вы можете установить скорость сразу для всех портов или отдельно для одного порта. Глобальная конфигурация: прямо в раскрывающемся списке на странице с красным шрифтом выберите скорость, которую вы хотите

установить. Затем нажмите «Применить настройки этой страницы» (Applythispagesettings).

2) Настройка одного порта: в функции «Rateconfiguration» соответствующего порта выберите скорость, которую вы хотите установить. Затем нажмите «Применить настройки этой страницы» (Applythispagesettings).

- **Максимальныйразмер фрейма**

Вы можете установить размер фрейма сразу для всех портов или для одного порта отдельно.

1) Глобальная конфигурация: введите соответствующийразмер фрейма в общий столбец, затем нажмите клавишу Enter, а затем нажмите Apply для завершения настройки.

1） Настройка одного порта: в разделе Maximumframe соответствующего порта введите размер фрейма, которую вы хотите установить, а затем нажмите Apply.

- **Управление потоками (Flow control)**

По умолчанию эта функция отключена. Рекомендуется не включать эту функцию, когда ваша сеть сильно загружена.

- **Включено (Enabled)**

Включите/выключите соответствующий порт.

4.2 Изоляция порта (Port isolation)

Изоляция порта позволяет указать порт пересылки для любого физического порта коммутатора. После установки функции изоляции порта каждый физический порт может пересылать данные только на свой собственный порт пересылки.

Нажмите на Portmanagement>>Portisolation на панели навигации, чтобы войти в интерфейс изоляции порта, как показано ниже:

Функции:

- **Выбрать все (Select all)**

Изоляция всех портов: после выбора нажмите Apply. Все порты изолированы и не могут обмениваться данными между собой.

- **Изоляция порта (Port isolation)**

Вкл/Выкл: Включение/выключение функции изоляции порта.

4.3 Зеркалирование портов (Portmirroring)

Зеркалирование портов позволяетпакеты указанного порта коммутатора копировать в порт назначения, который называется портом зеркалирования.

Нажмите на Portmanagement>>Portmirroring на панели навигации, чтобы войти в интерфейс зеркалирования портов, как показано на следующей схеме:

Функции:

- **Целевой порт зеркалирования (Mirrortargetport)**

Выберите порт, с которого нужно получить реплицированные данные.

- **Управление портом (Port management)**

Notmirroring： Не копировать данные на целевой порт зеркалирования.

Rxmirror： Копировать только входящих данных в порт зеркалирования.

Txmirror： Копирование только исходящих данных в порт зеркалирования.

Bothmirror： Копирование всех данных в целевой порт

➢ **Направление зеркалирования (Mirror direction)**

Установите параметры зеркалирования для одного порта

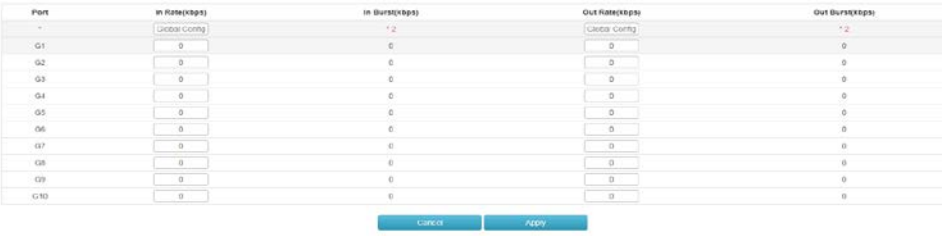
📖 Описание:

- Параметры в Portmanagement можно настроить для всех портов.

4.4 Ограничение скорости порта (Portspeedlimit)

Ограничение скорости порта предназначено для ограничения входящей и исходящей пропускной способности порта путем установки скорости порта.

Нажмите на Portmanagement>>Portlimit на панели навигации, чтобы войти в интерфейс ограничения скорости порта, как показано на рисунке ниже:



Функции:

➢ **Входящая скорость (Ingress Rate)**

Настройте скорость, с которой порт получает данные. Разрешенное максимальное значение -- 100 000 кбит/с

- **Исходящая скорость (Egress Rate)**

Настройте скорость, с которой порт отправляет данные, разрешенное максимальное значение -- 100 000 кбит/с.

Примечание: функции подавления шторма и ограничений скорости входящего потока нельзя использовать одновременно. Если включена функция подавления шторма, включение ограничения скорости входящего потока отключит ее.

4.5 Управление штормами (Stormcontrol)

Broadcast штормы означают быстрое увеличение количества широковещательных фреймов в сети, что серьезно ухудшает производительность сети. Критерием broadcast шторма является непрерывное принятие портом большого количества broadcast фреймов за короткое время. Функция StormControl предотвращает возникновение broadcast штормов, неизвестных multicast рассылок и unicast пакетов следующим образом. Данное устройство поддерживает функцию управления штормом для трех типов пакетов с ограничением пропускной способности**.**

В течение интервала обнаружения (detectioninterval) устройство отслеживает среднюю скорость полученных трех типов пакетов и сравнивает ее с максимальным порогом (maximumthreshold). Если скорость передачи пакетов превышает максимальный порог, активируется функция управления штормом — установленные действия по управлению штормом.

Если устройство отправляет broadcast, multicast или неизвестный unicast пакет на интерфейс Ethernet уровня 2, устройство перейдет в тот же VLAN

(виртуальную локальную сеть), если устройство не может указать исходящий интерфейс пакета на основе MAC-адреса пакета. Другие интерфейсы Ethernet уровня 2 пересылают эти пакеты, что может вызвать broadcast штормы и снизить производительность устройства. Функция подавления шторма может использоваться для управления трафиком этих трех типов пакетов для предотвращения broadcast штормов.

Нажмите на Portmanagement>>Stormcontrol на панели навигации, чтобы войти в интерфейс управления штормом, как показано ниже:

Функции:

Broadcast

Введите максимальную скорость приема broadcast пакета, пакет с превышением будет отклонен. Диапазон составляет 0–1000000, где «0» означает отсутствие ограничений.

Multicast

Введите максимальную скорость приема multicast пакета, пакет с превышением будет отклонен. Диапазон составляет 0–1000000, где «0» означает отсутствие ограничений.

Unicast

Введите максимальную скорость приема unicast пакета, и пакет, превышающий часть трафика, будет отклонен. Диапазон составляет 0–1000000, а «0» означает отсутствие ограничений.

Глобальная конфигурация

Установите максимальную скорость приема для всех портов. После заполнения параметров нажмите Apply для успешной настройки.

Примечание. Если для порта включен лимит входящей полосы пропускания, то включение подавления broadcast шторма отключит его.

4.6 Энергосбережение порта (Portenergysaving)

Когда эта функция включена, коммутатор автоматически отключает некоторые свободные каналы, эффективно снижая энергопотребление и экономя электроэнергию.

Нажмите на Portmanagement>>Portenergysaving на панели навигации, чтобы войти в интерфейс энергосбережения порта, как показано ниже:

Функции:

- **Выбрать все (Selectall)**Включите функцию EEE (сохранение порта) для всех портов.
- **EEE**Включите функцию EEE (сохранение порта, portsaving) для одного порта.

Глава 5 : Управление POE (POE management)

5.1 Управление портом POE (Port POE management)

С помощью этой функции вы можете установить максимальную мощность каждого порта POE и включить/выключить функцию POE определенного порта. Кроме того, здесь отображается текущий статус каждого порта POE,

включая статус соединения (linkstate), статус питания (powersupplestate), напряжение (voltage), ток (current) и мощность в реальном времени (power).

Нажмите на POEManagement>>PortPOEmanagement на панели навигации, чтобы войти в интерфейс энергосбережения порта, как показано ниже:

Функции:

- **Максимальная мощность (Maximum power)**

Установите максимальную мощность для каждого порта POE.

- **Вкл/выкл**

Включение/отключение функции POE порта

Примечание: Сумма мощностей всех портов POE, которые вы настроите, не должна превышать максимальную общую мощность питания (maximumtotalpowersupply).

5.2 Информация об устройстве (Deviceinformation)

В этом интерфейсе вы сможете просмотреть текущую общую мощность порта POE, а также основную информацию о каждой микросхеме POE, включая температуру, напряжение и мощность.

Нажмите на POEmanagement>>Devicepowersupply на панели навигации, чтобы войти в интерфейс энергосбережения порта, как показано ниже:

Максимальная общая мощность питания (Maximumtotalpowersupply)

Установите общую мощность порта PoE коммутатора.

📖Описание:

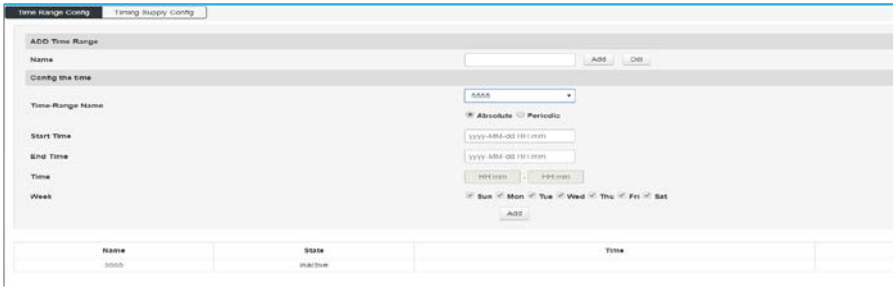
Этот интерфейс отображает только информацию о POE. Если температура выделена красным цветом, это означает, что температура микросхемы POE коммутатора слишком высокая.

5.3 Настройка графика источника питания (Timingsupplyconfiguration)

Эта функция позволяет установить время подачи питания на порт POE в соответствии с вашими потребностями, можно установить абсолютное время (год-месяц-день-час-минута-секунда) и время цикла (неделя-час-минута-секунда). После установки времени необходимо сопоставить его с фиксированным портом, в противном случае график не будет работать.

5.3.1 Конфигурация временного периода (Timeperiodconfiguration)

Нажмите на POEManagement>>Timingsupplyconfiguration>>Timerangeconfiguration, чтобы войти в интерфейс настройки времени, как показано ниже:



Функции:

- **Добавление временного интервала (AddTimeRange)**

Имя (Name) Задайте имя временного интервала. Оно может состоять из цифр, букв. Нажмите Add. Введите нужное имя, чтобы удалить добавленное имя, нажмите Del.

- **Время настройки (Configuration time)**

Имя временного интервала (Time-rangeName) Выберите имя, которое было установлено в раскрывающемся списке.

Время начала (StartTime)

Установите время начала интервала. Перед настройкой необходимо выбрать «абсолютное время».

Время окончания (EndTime) Установка времени окончания интервала.

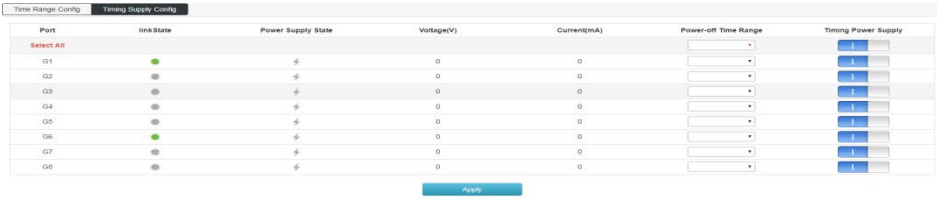
Время (Time) Установка интервала цикла. Перед настройкой необходимо выбрать время цикла.

Неделя (Week) Выберите определенное количество дней в цикле.

Примечание: перед установкой временного интервала POE, необходимо синхронизировать системное время коммутатора с местным временем.

5.3.2 Настройка графика источника питания (Timingpowersupplyconfiguration)

Нажмите на POEmanagement>>TimingSupplyConfiguration>>TimingSupplyConfigurationна панели навигации, чтобы войти в интерфейс настройки времени, как показано ниже:



Функции:

- **Период выключения (Power off time range)**

Нажмите на раскрывающийся список, чтобы выбрать интервал, установленный в «Настройке временного интервала». После успешного применения настроек здесь будет показано, что в течение установленного интервала порт POE не подает питание на устройство. Чтобы применить это ко всем портам, нажмите «Выбрать все» (Selectall).

- **Активация функции графика питания (Timingpowersupply)**

Вы можете включить/выключить эту функцию. Функция графика питания активируется после включения коммутатора.

5.4 Интеллектуальная конфигурация источника питания (Intelligentpowersupplyconfiguration)

Эта интеллектуальная функция определяет состояние порта POE и выполняет соответствующие операции с помощью программного обеспечения. 1) Если

через порт POE в течение длительного времени нет передачи данных, питание POE будет автоматически прервано, затем питание будет автоматически восстановлено через 10 секунд. 2) Обнаружена полная загруженность коммутатора POE. Когда общая мощность всех портов POE коммутатора превышает мощность, установленную в «максимальной общей мощности питания», питание порта POE прерывается по очереди до тех пор, пока общая мощность не снизится до установленного значения.

Функции:

Функция интеллектуальной подачи питания (Intelligentpowersupply)

Включение/выключение с помощью кнопки «AIPower» на передней панели коммутатора.

Длительность нулевого расхода (Zeroflowduration)

Установите время (в секундах) для периода отсутствия трафика на порту POE. В случае успешной настройки программное обеспечение сможет обнаружить, что порт POE не передает данные в течение установленного времени, затем подача питания POE прерывается и возобновляется через 10 секунд.

Глава 6: Управление уровня 2 (Layer 2 Management)

6.1 Таблица MAC-адресов (MAC Address Table)

Основная функция коммутатора Ethernet— пересылка пакета на канальном

уровне, то есть вывод пакета на соответствующий порт в соответствии с MAC-адресом назначения пакета. Таблица адресов содержит адресную информацию для пересылки пакетов между портами. Это основа для реализации в коммутаторе быстрой пересылки пакетов. Записи в адресной таблице можно обновлять и поддерживать с помощью автоматического обучения и ручной привязки. Большинство записей в таблице адресов создаются и поддерживаются с помощью функции автоматического обучения. Для некоторых относительно фиксированных соединений ручная привязка адреса может повысить эффективность коммутатора. Функция фильтрации MAC-адресов позволяет коммутатору фильтровать фреймы данных, которые не предполагается пересылать, тем самым повышается безопасность сети.

Нажмите на Layer 2 Management>>MACAddressTable и войдите в интерфейс таблицы MAC-адресов, как показано ниже:

Функции:

>Добавление (Add)

В открывшемся диалоговом окне заполните поля «MAC-адрес» (MACAddress), «VLAN», «Порт» (Port) и нажмите «Добавить» (Add) для завершения статической привязки адреса.

>Удаление (Delete)
Сначала выберите в адресной таблице элемент, который необходимо удалить, а затем нажмите «Удалить» (Delete), чтобы завершить удаление.

>Оставшееся время аренды (Lease time remaining)

Введите здесь время старения адреса, нажмите «Настройки» (Settings), и время старения будет успешно установлено. Время старения устанавливается только для динамических адресов. На статически добавленные адреса время старения не влияет.

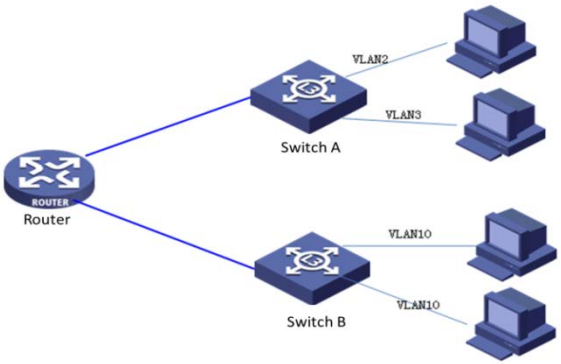
⚠Внимание: Если порт адреса указан некорректно, или порт (устройство) был изменен вручную во время использования, введенный статический адрес может быть сброшен, иначе пересылка данных коммутатором не будет корректной. После установки статического адреса, если сетевое устройство с данным адресом соединено с другим портом коммутатора, коммутатор не сможет динамически распознать его. Таким образом вы должны удостовериться, что введенные значения в таблице статических адресов действительны. Любой адрес, добавленный в таблицу статических адресов, не может быть в то же самое время добавлен в таблицу отфильтрованных адресов, а также он не может быть динамически привязан портом.

📖Описание:

Если время старения слишком велико, коммутатор сохранит слишком много устаревших адресных записей в адресной таблице, что приведет к исчерпанию ее ресурсов. В результате коммутатор не сможет обновлять таблицу адресов в соответствии с изменениями в сети. Если время старения слишком мало, таблица адресов будет обновляться слишком быстро. Адрес назначения для большого количества полученных пакетов не сможет быть найден в таблице адресов, поэтому коммутатор сможет транслировать эти пакеты только на все порты, что снижает общую производительность устройства. Рекомендуется использовать значение по умолчанию.

6.2 Настройка VLAN (VLANConfiguration)

Ethernet— это технология передачи данных по сети, основанная на совместно используемой среде связи CSMA/CDCSMA (CarrierSenseMultipleAccess/CollisionDetection). При наличии большого количества хостов могут возникнуть коллизии. Несмотря на то, что соединение LAN через коммутатор может решить серьезную проблему коллизии, оно не может изолировать broadcast сообщение. Для таких случаев предназначена технология VLAN (VirtualLocalAreaNetwork), которая делит локальную сеть на несколько логических локальных сетей —VLAN. Каждый VLAN— это широковещательный домен. Связь между хостами в VLAN такая же, как и в LAN. Сети VLAN не могут напрямую связываться друг с другом. Таким образом, broadcast пакеты ограничиваются одним VLAN, как показано ниже.



По сравнению с традиционным Ethernet, VLAN имеет следующие преимущества:

>Управление областью broadcast домена: broadcast пакеты в локальной сети ограничиваются одним VLAN, что позволяет экономить полосу пропускания и

улучшать возможности обработки сети.

>Повышенная безопасность LAN: поскольку пакеты изолированы на уровне канала передачи данных broadcast доменом, разделенным на VLAN, узлы в каждом VLAN не могут связываться напрямую, и пакеты должны отправляться через устройства сетевого уровня, такие как маршрутизаторы или коммутаторы уровня 3. Выполняется трехуровневая пересылка.

>Упрощенное управление сетью. Хосты одной виртуальной рабочей группы не ограничены определенной физической областью, что упрощает управление сетью и облегчает создание рабочих групп людьми в разных регионах.

Данный коммутатор поддерживает сети VLAN 802.1Q, VLAN на основе MAC-адресов и VLAN на основе портов. В конфигурации по умолчанию VLAN находится в режиме 802.1QVLAN.

VLAN с использованием портов основаны на том принципе, что VLAN назначаются на основе номера интерфейса коммутирующего устройства. Сетевой администратор настраивает разные PVID для каждого интерфейса коммутатора, то есть VLAN, к которой интерфейс принадлежит по умолчанию. Когда фрейм данных поступает в интерфейс коммутатора, если тег VLAN отсутствует и PVID настроен, фрейм данных будет помечен с помощью PVID интерфейса. Если во входящем фрейме уже есть тег VLAN, коммутатор не будет добавлять тег VLAN, даже если интерфейс был настроен с PVID.

6.2.1 Конфигурация VLAN (VLANConfiguration)

Нажмите на Layer 2 Management>>VLANConfiguration>>VLANState, чтобы войти в интерфейс состояния VLAN, как показано ниже:

Функции:

Обучение VLAN: у каждого VLAN есть своя таблица сопоставления Mac-> портов, поэтому один и тот же MAC-адрес может отображаться в нескольких таблицах сопоставления (возможно, эти записи хранятся вместе, но логически кажется, что это точки для множества разных записей, то есть режим обучения состоит в изучении всей таблицы MAC-адресов, используя MAC-адрес плюс номер VID в качестве индекса (необходимо иметь тот же MAC-адрес и тот же VID, чтобы быть одной и той же записью). Таким образом, при одинаковых MAC-адресах номера VID могут отличаться. Это также означает, что изученный MAC-адрес в каждом VLAN принадлежит VLAN и не будет использоваться совместно с другими VLAN.

6.2.2 Конфигурация VLAN (VLANConfiguration)

На этой странице можно настроить сети VLAN и настроить режим VLAN для каждого порта.

Нажмите на Layer 2 Management>>VLANConfiguration>>VLANConfiguration на панели навигации, чтобы войти в интерфейс конфигурации VLAN, как показано ниже:

Функции:

Режим VLAN (VLANmode):

A. ACCESS: Порт, принадлежащий одному VLAN и передающий нетегированный трафик. Когда ACCESS порт добавляется к другому VLAN, исходный VLAN автоматически закрывается.

B. TRUNK: Порт может пропускать несколько VLAN, а также может принимать и отправлять пакеты из нескольких VLAN. В сети VLAN часто подключены к разным коммутаторам. Передает тегированный трафик. При пересылке данных VLAN по умолчанию информация о VLAN удаляется. При пересылке оставшихся данных VLAN, исходная информация VLAN сохраняется.

C.Hybrid:Порт может пропускать несколько VLAN. Он может принимать и отправлять пакеты из нескольких VLAN. Его можно использовать для подключения между сетевыми устройствами и подключения к пользовательским устройствам. Передача трафика настраивается в зависимости от фактических условий устройства, подключенного к порту.

PVID :

PVID (PortVLANID) — это VID порта по умолчанию. Если пакет, полученный портом, не содержит тега VLAN, коммутатор вставляет тег VLAN на основе значения PVID принимающего порта и пересылает пакет.

При разделении VLAN на LAN, PVID является важным параметром каждого порта, указывающим тот VLAN, к которой порт принадлежит по умолчанию. Он применяется в двух случаях:

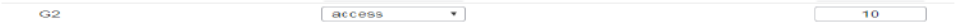
A. Когда порт получает нетегированный пакет, он вставляет тег VLAN для пакета на основе PVID.

B. PVID указывает широковещательный домен порта по умолчанию. Когда порт получает пакет UL или широковещательный пакет, коммутатор передает пакет данных в VLAN порта по умолчанию.

Тип порта	Обработка получения сообщения		Обработка при отправке сообщения
	UNTAH	TAG	
ACCESS	Получает пакет и добавляет к нему тег VLAN по умолчанию, то есть PVID входного порта.	Когда VID = PVID порта, сообщение получено. Когда VID ≠ PVID порта, пакет отбрасывается.	После удаления тега сообщение отправляется.
Trunk		Получает пакет, когда VID принадлежит идентификатору VLAN, который порт может передавать.	Когда данные порта по умолчанию VLAN пересылаются, пакет отправляется после отправки тега, а затем отправляется остальная часть исходного тега.
Hybrid		Пакеты отбрасываются, если VID не принадлежит идентификатору VLAN, разрешенному портом.	Когда правило выхода настроено как TAG, исходный тег отправляется для отправки пакета. Если правило выхода настроено как UNTAG, пакет отправляется после отправки тега.

Пример настройки

Добавьте порт G2 к VLAN 10 и проведите настройку следующим образом.



Добавьте порты G2-G6 в VLAN10, просто измените PVID на 10 после соответствующего порта.

Добавьте порт G9 в несколько VLAN

📖Описание:

При настройке порта для принадлежности к нескольким VLAN сначала измените режим на режим Trunk или Hybrid, а затем настройте информацию тега VLAN. Вам нужно обратить внимание на конфигурацию информации тега. Пробел указывает на прерывистый VLAN. Специальный символ координат "" — на последовательный VLAN.

VLANuntag— 1-5, что означает, что поддерживаются все VLAN от VLAN 1 до VLAN 5.

6.2.3 Конфигурация voice VLAN (Voice VLAN Configuration)

VoiceVLAN— это VLAN, который делится на потоки голосовых данных для пользователей. Создав voiceVLAN и добавив порт, подключенный к голосовому устройству, вы можете разрешить передачу голосовых данных в voiceVLAN. Это облегчает настройку QoS (качества обслуживания) и улучшает передачу голоса. Приоритет передачи трафика обеспечивает качество звонка.

Нажмите на Layer 2 Management>>VLANConfiguration>>VoiceVLANConfiguration, чтобы войти в интерфейс voiceVLAN, как показано на рисунке ниже:

Функции:

> Включить voiceVLAN

Включение/отключение функции voiceVLAN.

>VLANID

Значение идентификатора VLANID находится в диапазоне от 1 до 4094. Например: 1-3, 5, 7, 9. По умолчанию используется VLAN 1. Другие сети VLAN должны существовать и добавляются к порту, который необходимо связать в режиме без тегов.

>COS

Введите значение COSvoiceVLAN в диапазоне от 0 до 7. После установки значения COS вам необходимо установить отображение очереди COS в QOS. Для обеспечения приоритета голоса.

>dscp

Заполните отображение очереди dscp очереди voiceVLAN в диапазоне от 0 до 63. После установки значения dscp вам необходимо установить отображение очереди dscp в QOS. Для обеспечения приоритета голоса.

>MAC

Введите адрес указанного IP-телефона или голосового клиента. Например: 0812-f231-05e1.

>MAC-маска

Заполните маску, например: ffff-ff00-0000.

Описание:
>VLAN 1 не может быть указан в качестве voiceVLAN. Для управления рекомендуется назначить разные VLAN для голосовых и сервисов и сервисов данных.
>Для обеспечения нормального использования разных функций назначьте разные VLANID для voiceVLAN и интерфейса по умолчанию.
>В то же время только VLAN интерфейса может быть настроен как voiceVLAN.
>VLANmapping, VLANstacking и политики передачи трафика не разрешены в интерфейсе, подключенном к voiceVLAN.
>Невозможно установить VLANIDна 0 на IP-телефоне.

6.2.4 Конфигурация MAC VLAN (MAC VLAN Configuration)

MAC-VLAN— это еще один метод разделения VLAN. Сеть VLAN делится в соответствии с MAC-адресом каждого хоста. То есть MAC-адрес каждого хоста разделен по VLAN. Если получен нетегированный (без тега VLAN) фрейм, идентификатор VLAN добавляется в соответствии с таблицей.

> Преимущество: при изменении физического местоположения конечного пользователя нет необходимости перенастраивать VLAN. После привязки устройство, соответствующее MAC-адресу, может переключать порты, пока оно подключено к порту-участнику соответствующей VLAN, без изменения конфигурации участника VLAN. Это позволяет повысить безопасность для конечных пользователей и улучшить гибкость доступа.

> Недостатки: применимо только в сценариях, где сетевая карта не часто заменяется и сетевая среда относительно проста. Все участники сети должны быть определены заранее.

Нажмите на Layer 2 Management>>VLANConfiguration>>MACVLANConfiguration на панели навигации, чтобы войти в интерфейс MACVLAN, как показано ниже:

Функции:

>VLANID

Введите VLANID в диапазоне от 1 до 4094. Например: 5,7,9. VLAN 1 используется по умолчанию и не может быть переустановлен. Другие сети VLAN должны существовать и добавляются к порту, который необходимо связать в режиме без тегов.

>MAC

Введите MAC-адрес клиента. Завершите и нажмите кнопку «Добавить» (Add) для успешной настройки.

6.2.5 Конфигурация IP VLAN (IP VLAN Configuration)

VLAN, основанная на протоколе IP, назначает пакеты различным VLANID в зависимости от IP-адреса, на который эти пакеты принимаются. Преимущество состоит в том, что VLAN делится на основе IP, а тип услуги, предоставляемой в сети, привязан к VLAN, что удобно для управления и обслуживания.

Недостатком является то, что вам необходимо изначально настроить mapping таблицу всех IP-протоколов и VLANID в сети. Необходимо проанализировать формат адреса различных IP-протоколов и выполнить соответствующие преобразования, что потребляет больше ресурсов коммутатора и имеет недостаточно высокую скорость.

Нажмите на Layer 2 Management>>VLANConfiguration>>IPVLANConfiguration, чтобы войти в интерфейс IPVLAN, как показано ниже:

Функции:

>VLANID

Введите добавляемый VLANID в диапазоне от 1 до 4094. Например: 5,7,9. VLAN 1 используется по умолчанию и не может быть переустановлен. Другие сети VLAN должны существовать и добавляются к порту, который необходимо связать в режиме без тегов.

>IP

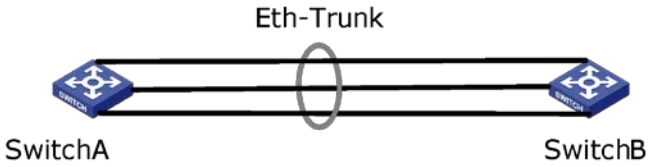
Введите IP-адрес клиента. Нажмите «Добавить» (Add) для успешной установки.

6.3 Агрегирование каналов (LinkAggregation)

Физический порт объединен в логический порт для реализации балансировки нагрузки входящего/исходящего трафика на каждом порте-участнике. Коммутатор определяет порт, с которого отправляется пакет, на основе политики балансировки нагрузки порта, настроенной пользователем. Переключитесь на одноранговый узел. Вы можете разделить трафик между портами-участниками в группе агрегации, чтобы увеличить пропускную способность. В то же время каждый порт-участник одной и той же группы агрегации динамически выполняет резервное копирование друг друга, что повышает надежность соединения.

Порты-участники одной группы агрегации должны иметь одинаковую конфигурацию. Эти конфигурации включают STP, QoS, VLAN, атрибуты порта и изучение MAC-адресов.

Как показано на следующем рисунке, SwitchA (коммутатор A) и SwitchB (коммутатор B) подключены через три физических канала Ethernet. Три канала объединяются вместе, образуя логическое соединение Eth-Trunk. Пропускная способность этого логического канала равна исходным трем портам Ethernet. Сумма пропускной способности физического канала сети, таким образом достигается цель увеличения пропускной способности канала.



6.3.1 Конфигурация статического агрегирования каналов (StaticLinkConfiguration)

На данной странице вы можете вручную настроить группу агрегации. Статус LACP настроенного вручную порта агрегации отключен.

Нажмите на Layer 2 Management>>LinkAggregation>>StaticAggregationConfig, войдите в интерфейс настройки статического агрегирования, как показано ниже:

Функции:

Создать (Establish). Нажмите «Создать» (Establish) и нажмите на появившееся всплывающее диалоговое окно, чтобы ввести идентификатор группы агрегации, нажмите «Establish», как показано ниже:

> Удалить (Delete)

Выберите группу агрегации, которую вы хотите удалить, в списке агрегации и нажмите «Удалить» (Delete).

> Режим балансировки нагрузки (Loadbalancingmode):

SrcMac: выполняет распределение нагрузки на основе MAC-адреса источника.

DstMac: выполняет распределение нагрузки на основе MAC-адреса назначения.

Src&DstMac: выполняет распределение нагрузки на основе исключающего ИЛИ исходного MAC-адреса и MAC-адреса назначения.

SrcIP: балансировка нагрузки на основе IP-адреса источника.

DstIP: выполняет распределение нагрузки на основе IP-адреса назначения.

Src&DstMac: выполняет распределение нагрузки на основе исключающего ИЛИ исходного IP-адреса и целевого IP-адреса.

По умолчанию используется разделение нагрузки на основе XOR исходного MAC-адреса и MAC-адреса назначения.

6.3.2 Конфигурация динамического агрегирования (DynamicAggregationConfiguration)

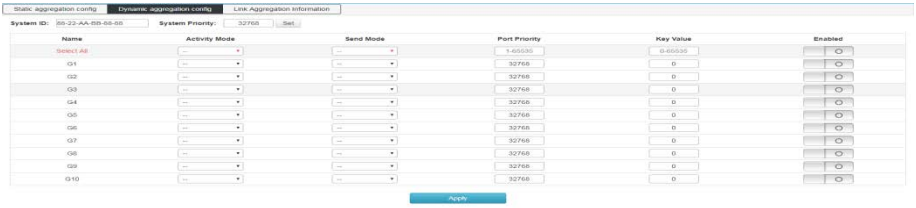
Протокол управления агрегацией каналов (LACP), основанный на стандарте IEEE 802.3ad, представляет собой протокол для реализации динамической

агрегации и деагрегации каналов. Протокол LACP обменивается информацией с одноранговым узлом через LACPDU.

ПослевключенияпротоколаLACPнапорту,портобъявляетпартнерусвойсистемныйприоритет, системныйMAC-адрес, приоритетпорта, номерпортаирабочийключ, отправляяLACPDU. После получения информации одноранговый узел сравнивает информацию с сохраненной другими портами, чтобы выбрать порт, который можно агрегировать. Таким образом, обе стороны могут договориться присоединиться к порту или выйти из него.

Динамическое агрегирование LACP— это агрегирование, которое автоматически создается или удаляется системой. Добавление и удаление портов в группе динамической агрегации автоматически выполняется протоколом. Только порты с одинаковой скоростью и duplex атрибутами, подключенные к одному устройству и с одинаковой базовой конфигурацией, могут быть агрегированы динамически.

Нажмите на Layer 2 Management>>LinkAggregation>>DynamicAggregationConfig, войдите в интерфейс настройки динамического агрегирования, как показано ниже:



Функции:

- **Системный приоритет (Systempriority)**

Приоритет устройства определяется вместе с MAC-адресом системы. Устройство с наивысшим приоритетом будет доминировать при агрегировании и деагрегации. По умолчанию 32768.

➢ **Активный режим. Пассивный режим и активный режим (Activemode, passivemode)**

Активный режим (Activemode): порт автоматически периодически отправляет пакеты протокола LACP.

Пассивный режим (Passivemode): порт не отправляет автоматически пакеты протокола LACP; он отвечает только на пакеты протокола LACP, отправленные от одноранговой устройства.

➢ Режим отправки (Sendmode). Вы можете выбрать медленный, быстрый или режим без отправки.

➢ **Приоритет порта (Portpriority)**

Определяется приоритет порта, который становится участником агрегации. Определяется приоритет порта в группе агрегации. Предпочтительны порты с небольшими значениями приоритета портов. Если приоритеты портов одинаковые, будет учитываться номер порта. По умолчанию 32768.

➢ **Значение ключа (keyvalue)**

Задайте значение ключа порта. В соответствующей группе агрегации вам нужно установить такое же значение ключа.

➢ **Переключатель**

Включение / отключение LACP (динамическое агрегирование). По умолчанию выключено.

6.3.3 Информация об агрегировании каналов (LinkAggregationInformation)

На этой странице отображается подробная информация об агрегировании каналов, включая количество портов (numberofports), приоритет (priority), режим балансировки нагрузки (loadbalancingmode) и значения ключа (keyvalues) в статической и динамической агрегации.

Нажмите на Layer 2 Management>>LinkAggregation>>LinkAggregationInformation, чтобы войти в интерфейс информации об агрегировании каналов, как показано ниже:

Функции:

Группа агрегации (Aggregationgroup): отображает название группы агрегации.

Режим (Mode): отображает режим агрегирования (динамический или статический) текущей группы агрегирования.

Количество портов (Numberofports): отображает количество агрегированных на данный момент портов.

Список портов (Portlist): отображает номер порта, который был агрегирован.

Балансировка нагрузки (Loadbalancing): отображает текущий режим балансировки нагрузки.

6.4 Конфигурация MSTP (MSTPconfiguration)

SpanningTreeProtocol (STP) — это протокол, установленный в соответствии со стандартом IEEE 802.1D для устранения физических петель на уровне канала передачи данных в локальной сети. Устройство, использующее протокол, обнаруживает петли в сети, взаимодействуя друг с другом, и выборочно блокирует определенные порты. Наконец, петлевая сетевая структура обрезается до свободной от петель древовидной сетевой структуры для предотвращения кольцевания пакетов. Сеть продолжает разрастаться и бесконечно зацикливаться, избегая проблемы снижения возможностей обработки устройства из-за повторного приема одного и того же пакета.

Как и многие процессы разработки протоколов, протокол STP постоянно обновляется по мере развития сети, от начального STP, определенного в IEEE

802.1D, до протокола RSTP, определенного в IEEE 802.1W. Затем к последнему протоколу MSTP, определенному в IEEE 802.1S. MSTP совместим с RSTP и STP, а RSTP совместим с STP. Сравнение трех протоколов показано в таблице.

Протокол	Функция	Применение
STP	Формирует дерево без петель, которое устраняет broadcast штормы и обеспечивает резервный канал. Скорость конвергенции ниже.	Нет необходимости проводить различие между пользовательским или служебным трафиком
RSTP	Формирует дерево без петель, которое устраняет broadcast штормы и обеспечивает резервный канал. Быстрая конвергенция	
MSTP	Формирует дерево без петель, которое устраняет broadcast штормы и обеспечивает резервный канал. Скорость конвергенции высокая.Реализуется балансировка нагрузки между VLAN. Трафик разныхVLAN пересылается по разным путям.	Необходимо различать пользовательский или служебный трафик и реализовывать распределение нагрузки. Различные сети VLAN пересылают трафик через разные связующие деревья, и каждое не зависит друг от друга.

6.4.1 Глобальная конфигурация (GlobalConfiguration)

В некоторых конкретных сетевых средах вам необходимо настроить параметры STP некоторых устройств для достижения наилучших результатов.

Нажмите на Layer 2 Management>>MSTPConfiguration>>GlobalConfiguration на панели навигации, чтобы войти в интерфейс глобальной конфигурации, как показано ниже.

Функции:

Нажмите на Включить ST (EnableSpanning-tree), чтобы включить/выключить ST.

- **Режим (Mode)** :Выберите STP, RSTP, MSTP
- **Максимальный возраст (Maxage):** указывает максимальное время жизни сообщения. Это значение составляет от 6 до 40 секунд. По умолчанию 20 секунд.

Hellotime: указывает период, в течение которого было отправлено сообщение. Мост через определенные промежутки времени посылает сообщение о работоспособности окружающим мостам.

Сообщение. Для подтверждения того, что ссылка неисправна, этот интервал равняется периоду Hello.

Задержка передачи (Forwarddelay): указывает задержку перехода состояния порта. Это значение составляет от 4 до 30 секунд. Значение по умолчанию -- 15 секунд.

Максимальное количество хопов (MaxHops): выбирается максимальное количество хопов. Это значение находится в диапазоне от 1 до 20, а по умолчанию — 20. Большое количество хопов используется для ограничения

сетевого размера связующего дерева в области MST. Начиная с корневого моста связующего дерева в области MST, количество хопов уменьшается на единицу, когда информация о конфигурации в домене пересылается в каждый коммутатор. Коммутатор отбрасывает хопы конфигурации со счетчиком хопов 0. Участвует в вычислении связующего дерева, который ограничивает размер домена MST.

Изменение (Revision): Уровень изменений MSTP. Уровень изменений MSTP используется для определения назначения с именем домена и таблицей сопоставления VLAN.

Регион MST, к которому принадлежит коммутационное устройство.

- **Имя:** доменное имя MST. Значение по умолчанию -- это MAC-адрес главной платы управления коммутатора.

После завершения настройки нажмите «Apply».

Примечание:

- Длина задержки передачи устройства связана с размером STP. Если задержка передачи слишком мала, может возникнуть временная петля. Если задержка передачи слишком велика, сеть может не возобновить подключение в течение длительного времени. Рекомендуется значение по умолчанию.
- Если время устаревания слишком мало, коммутатор будет часто вычислять связующее дерево, и перегрузка сети может быть ошибочно принята за неисправность канала. Если время устаревания слишком велико, коммутатор не сможет вовремя обнаружить неисправность канала и не сможет вовремя пересчитать связующее дерево. Уменьшите адаптивную способность сети. Рекомендуется значение по умолчанию.
- Если лимит трафика слишком велик, количество пакетов MSTP, отправляемых в течение каждого времени контакта, будет слишком большим, что потребляет слишком много сетевых ресурсов. Рекомендуется значение по умолчанию.

6.4.2 InstanceConfiguration

Коммутационная сеть делится на несколько доменов с помощью MSTP, и в каждом домене формируется несколько связующих деревьев, и они не зависят друг от друга. Каждое связующее дерево называется экземпляром MSTI, а каждый домен называется областью MST.

Описание:

Экземпляр — это совокупность нескольких VLAN. Объединяя несколько виртуальных локальных сетей в один экземпляр, вы можете сэкономить на коммуникационных накладных расходах и использовании ресурсов. Вычисление топологии каждого экземпляра MSTP не зависит друг от друга, и нагрузка на этих экземплярах может быть сбалансирована. Несколько виртуальных локальных сетей с одинаковой топологией могут быть сопоставлены с экземпляром (mapping). Состояние пересылки этих VLAN на порт зависит от состояния порта в соответствующем экземпляре MSTP.

Проще говоря, это mapping одного или нескольких VLAN на указанный экземпляр MST. Одновременно одному экземпляру связующего дерева можно назначить один или несколько VLAN.

Нажмите на Layer 2 Management>>MSTPConfiguration>>Instanceconfiguration на панели навигации, чтобы войти в интерфейс настройки экземпляра, как показано ниже:

Функции:

1. MSTIID: выберите любой номер экземпляра в пределах 1–63.

2. Приоритет (Priority): установите приоритет указанного экземпляра, который должен быть кратным 4096. Его диапазон от 0 до 65535, значение по умолчанию -- 32768.

3. VlanMapped: входит в VLAN для mapping. VLANmapping может изменять передаваемые пакеты

Тег VLAN. Есть четыре вида отношений mapping:

1) VLANmapping 1: 1: Тег VLAN, передаваемый в пакете из определенной VLAN, заменяется новым тегом VLAN.

2) VLANmappingN: 1: Разные теги VLAN, передаваемые в пакетах из двух или более VLAN, заменяются одним и тем же тегом VLAN.

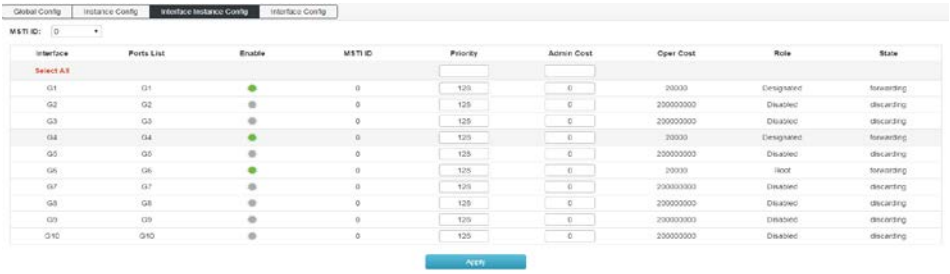
3) VLANmapping 1: 2: К пакету, несущему тег VLAN, применяется тег внешнего VLAN, чтобы пакет содержал два тега VLAN.

4) VLANmapping 2: 2: Внутренний и внешний теги VLAN пакетов, содержащих два тега VLAN, заменяются новыми тегами VLAN.

6.4.3 PortInstanceConfiguration

Пример, показывающий, как настроить порт коммутатора:

Нажмите на Layer 2 Management>>MSTPConfiguration>>PortInstanceConfiguration на панели навигации, чтобы войти в интерфейс конфигурации экземпляра порта, как показано ниже:



Функции:

1 **MSTID:** выберите настроенный экземпляр в конфигурации экземпляра (InstanceConfiguration) из раскрывающегося меню.

2 **Приоритет (Priority):** выберите приоритет порта. Меньшее значение указывает на более высокий приоритет.

Приоритет интерфейса может повлиять на роль интерфейса в указанном MSTI. Вы можете настроить разные приоритеты для одного и того же интерфейса на разных MSTI, чтобы разрешить пересылку трафика из разных VLAN по разным физическим каналам. Когда приоритет интерфейса изменяется, MSTP пересчитывает роль интерфейса и выполняет изменение состояний.

3 **Стоимость пути (AdminCost):** справочное значение, используемое для выбора пути и расчета стоимости пути. Также определите, будет ли порт выбран в качестве корневого.

Меньшее значение указывает на более высокий приоритет (0 означает отсутствие настройки).

4 **Роль (Role):** отображает роль, которую порт играет в связующем дереве.

1) Отключить (Disable): порт, физическое соединение которого прервано.

2) Назначенный (Designated): порт, отвечающий за пересылку данных в нисходящие сегменты сети или устройства.

3) Корневой (Root): порт с наименьшей стоимостью пути к корневому мосту, отвечающий за пересылку данных на корневой мост.

4) Альтернативный (Alternate): резервный порт корневого порта и главного порта.

5) Главный порт (Masterport): подключите несколько доменов связующего дерева к общему корню, расположенному на кратчайшем пути от всего домена к общему корню.

6) Backup (порт резервного копирования): указывает порт резервного копирования.

Статус (Status): отображает текущий рабочий статус порта.

1) отбрасывание (discarding): порт с отключенным физическим соединением.

2) пересылка (forwarding): принимает и пересылает данные, принимает и отправляет пакеты протокола и выполняет изучение адресов.

3) Блокировка (blocking): не получает и не пересылает данные, но не отправляет пакеты протокола. Изучение адресов не производится.

4) обучение (learning): не получает и не пересылает данные, принимает и отправляет сообщения протокола и изучает адреса.

Описание: Для отражения накладных расходов STP широкополосного канала со скоростью ниже 1 Гбит/с используется стандартное обновленное определение стоимости IEEE 802.1D (см. таблицу ниже):

пропускная способность	стоимость STP
4 Мбит/с	250
10 Мбит/с	100
16 Мбит/с	62
45 Мбит/с	39
100 Мбит/с	19
155 Мбит/с	14
622 Мбит/с	6

1 Гбит/с	4
10 Гбит/с	2

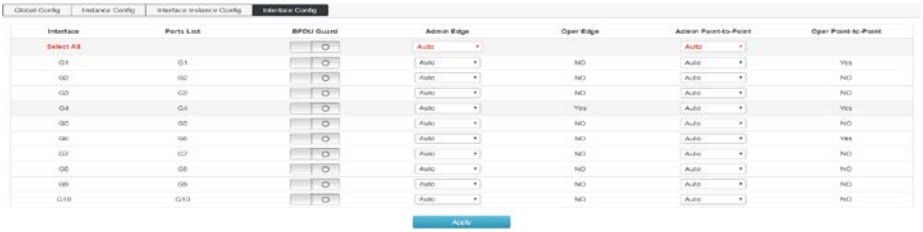
Примечание:

Установите порт, напрямую подключенный к терминалу, как граничный (edgeport) и включите защиту BPDU. Таким образом, порт может быть быстро переведен в состояние пересылки, а сеть может быть защищена.

6.4.4 Конфигурация порта (PortConfig)

В отдельных сетевых средах для достижения наилучших результатов необходимо провести настройку параметров STP некоторых интерфейсов коммутирующих устройств.

Нажмите на Layer 2 Management>>MSTPConfiguration>>Instanceconfiguration на панели навигации, чтобы войти в интерфейс управления портами, как показано ниже.



Функции:

1 BPDU Guard (BPDU Guard). Выберите, следует ли включать защиту BPDU. Есть два случая: открытие и не открытие. По умолчанию стоит не открытие.

Когда на устройстве включена функция защиты BPDU, если интерфейс получает BPDU, устройство отключает эти интерфейсы и уведомляет NMS.

Закрытый интерфейс может быть восстановлен только администратором сети вручную.

2 Граничный порт (Edgeport) должен быть подключен непосредственно к пользовательскому терминалу, а не к другому коммутатору или сегменту сети. Граничный порт может служить быстрым переходом в состояние пересылки, поскольку на граничном порту изменения топологии сети не создают петель. Если вы устанавливаете порт как граничный, протокол STP позволяет ему быстро переходить в состояние пересылки. Рекомендуется управлять портами Ethernet, напрямую подключенными к пользовательскому терминалу, в качестве граничных портов, чтобы они могли быстро перейти в состояние пересылки.

3 Point-to-Point выбирает Force_True, Force_False и Auto.

Auto: указывает, установлен ли порт в состояние по умолчанию автоматического определения того, подключен ли он к двухточечному каналу.

Force-true: указывает, что конкретный порт подключен к двухточечному каналу.

Force-false: указывает, что конкретный порт не подключен к двухточечному каналу.

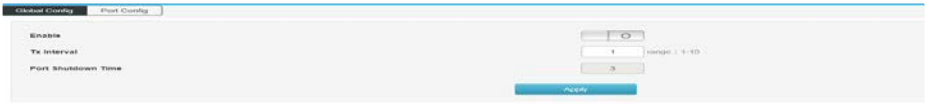
6.5 Защита от образования петель (Loopprotection)

Когда топология сети стабильна, коммутатор продолжает получать пакеты BPDU, отправленные вышестоящим коммутатором, чтобы поддерживать состояние каждого порта локального устройства. Однако, когда канал неисправен или однонаправленный канал неисправен, нисходящий коммутатор не может получать BPDU. Связующее дерево пересчитывается, и роль порта повторно выбирается. Заблокированный порт переводится в состояние пересылки. В середине создается петля. Функция защиты от петель предотвращает их возникновение. Если порт, для которого включена защита от петель, не получает BPDU от вышестоящего коммутатора и вызывает пересчет STP, он будет установлен в состояние блокировки независимо от роли порта.

6.5.1 Глобальная конфигурация (Globalconfiguration)

На этой странице вы можете установить глобальную информацию о защите от петель.

Как зайти на страницу: Advanced settings >> Loop Protection >> Global Configuration



Описание:

Включить (Enable)защиту от петель

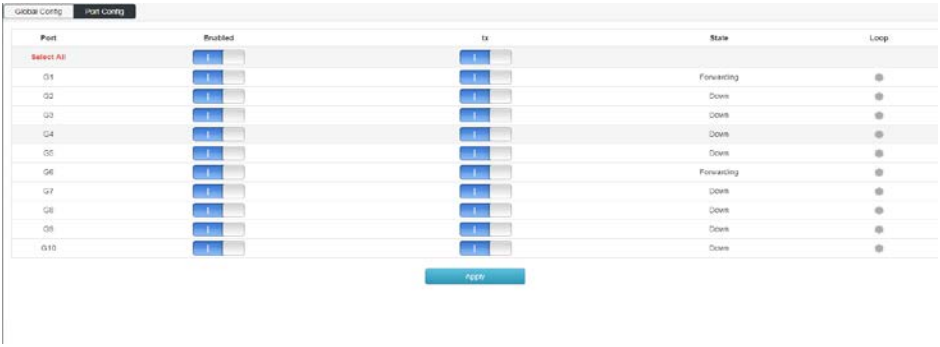
Период передачи сообщения (Txinterval). Время цикла отправки пакета обнаружения защиты от петель. По умолчанию - 1 секунда.

Время закрытия порта (PortShutdownTime): Время от обнаружения петли до блокировки одного из портов составляет 3 с.

6.5.2 Конфигурация порта (PortConfiguration)

На этой странице вы можете настроить информацию о порте защиты от петель.

Как зайти на страницу : Advanced Settings >> Loop Protection >> Port Configuration



Описание :

Порт (Port): Все физические порты устройства
Вкл./Выкл. (On/Off): Включение функции защиты от петель.
Tx: Укажите, будет ли порт активно отправлять пакеты обнаружения петель.
Статус (State): Статус текущего порта. Есть три состояния: отключено (Down), пересылка (Forwarding) и блокировка (Blocking).
Не работает (Down): Порт не подключен.
Пересылка (Forwarding): Порт пересылает все пакеты в обычном режиме.
Блокировка (Blocking): Порт находится в заблокированном состоянии. Порт не может пересылать данные, пока он не будет восстановлен в состоянии пересылки.

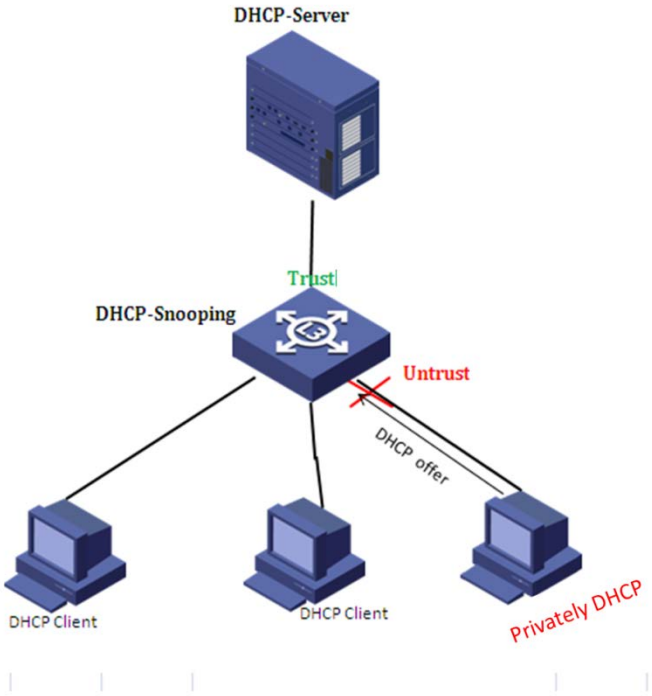
Примечание: данную функцию следует предварительно включить в меню глобальной конфигурации, чтобы она активировалась в конфигурации порта.

6.6 DHCP-snooping (Отслеживание DHCP-пакетов)

Из соображений безопасности сетевому администратору может потребоваться зафиксировать IP-адрес, используемый пользователем для доступа в Интернет, и подтвердить соответствие между IP-адресом, полученным пользователем от DHCP-сервера, и MAC-адресом хоста пользователя.

Коммутатор может записывать информацию об IP-адресе пользователя с помощью функции безопасности DHCP-relay, работающего на сетевом уровне. Коммутатор может прослушивать сообщения DHCP и записывать информацию об IP-адресе пользователя с помощью функции DHCP-snooping, выполняемой на уровне канала данных. Кроме того, если в сети есть настроенный в частном порядке DHCP-сервер, пользователь может получить неправильный IP-адрес. Чтобы пользователи могли получать IP-адреса через легитимный DHCP-сервер, механизм безопасности DHCPSnooping позволяет назначать портам надежные и ненадежные порты.

Надежный порт — это порт, который прямо или косвенно подключен к надежному DHCP-серверу. Надежный порт пересылает полученные пакеты DHCP, гарантируя, что клиент DHCP получит правильный IP-адрес. Ненадежный порт — это порт, который не подключен к надежному DHCP-серверу. Сообщения DHCP-ACK и DHCP-OFFER, полученные от ненадежного порта в ответ на DHCP-сервер, отбрасываются, предотвращая получение DHCP-клиентом неправильного IP-адреса.



6.6.1 Глобальная конфигурация (Global Configuration)

Нажмите на Layer 2 Management >> DHCP-snooping >> Global Configuration на панели навигации, чтобы войти в интерфейс глобальной конфигурации, как показано ниже:

Функции:

- Включить/выключить DHCP-snooping

6.6.2 Staticbinding

В сети DHCP пользователи, которые являются статически полученными IP-адресами (пользователи, не использующие DHCP), могут подвергаться множественным атакам, таким как подмена DHCP-серверов и создание ложных сообщений DHCP-запроса. Это создаст определенные риски безопасности для нормального использования сети надежными пользователями DHCP.

Чтобы предотвратить атаки пользователей, не использующих DHCP, вы можете разрешить устройству создавать записи статических MAC-адресов на основе таблицы привязки DHCP-snooping. После создания записи привязки DHCP-snooping устройство автоматически создает записи статического MAC-адреса пользователя и отключает интерфейс для изучения динамических записей MAC. В настоящее время через интерфейс могут пройти только пакеты, MAC-адрес источника которых совпадает со статическим MAC-адресом. В противном случае пакет будет отброшен. Следовательно, для пользователя интерфейса, не использующего DHCP, только администратор может вручную настроить запись статического MAC-адреса пользователя для передачи пакета. В противном случае пакет будет отброшен.

Нажмите на Layer 2 Management>>DHCP-snooping>>Staticbinding на панели навигации, чтобы войти в интерфейс функции, как показано ниже:

Функции:

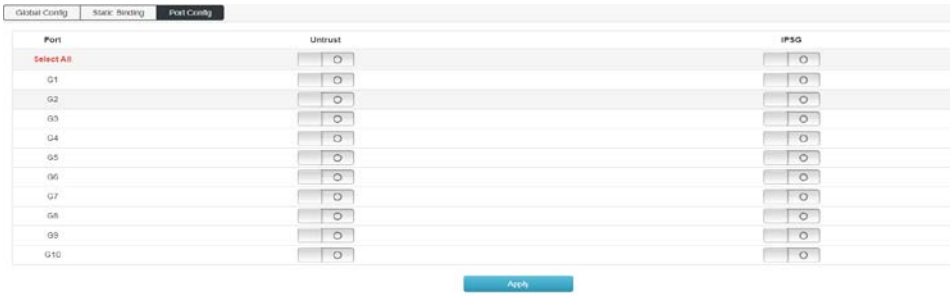
- **MAC**Введите MAC-адрес привязанного пользователя.
- **IP-адрес (IPaddress)** Статический IP-адрес пользователя.

➢ **Порт (Port)** Отображает порт коммутатора.

Нажмите «Добавить» (Add), чтобы завершить настройку, как показано ниже:

6.6.3 Управление портами (Port Management)

Нажмитена Layer 2 Management>>DHCP-snooping>>PortManagement напанелинавигации, чтобывойтивинтерфейсфункции, какпоказанониже:



Функции:

➢ Не доверять ненадежному порту, открывать как ненадежный порт, закрывать как надежный порт.

➢ Проверка исходного адреса IPSGIP, пересылка только легитимных хостов для отправки IP-пакетов. Необходимо включить функцию Staticbinding (Статическая привязка) запись в нем будет активирована.

6.7 IGMP-snooping (Отслеживание IGMP-пакетов)

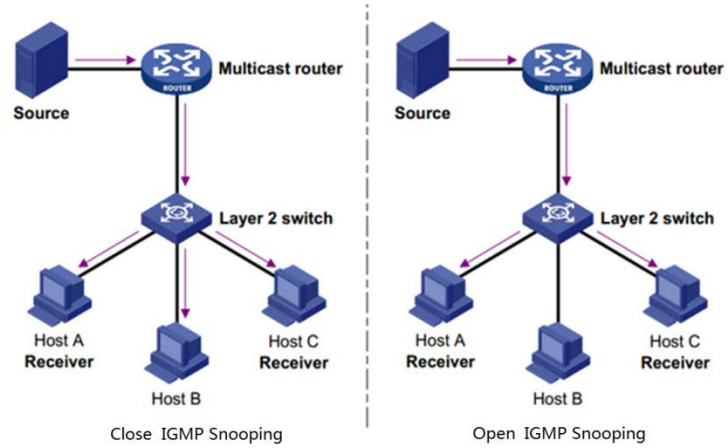
IGMP-snooping (отслеживание протокола управления группами в Интернете) — это механизм ограничения multicast рассылки, который работает на устройствах уровня 2 для управления группами multicast рассылки.

Устройство уровня 2, на котором запущено IGMP-snooping, анализирует полученные сообщения IGMP и устанавливает отношение mapping между портом и MAC-адресом multicast рассылки и пересылает данные multicast рассылки в соответствии с этим отношением.

- Процесс прослушивания фрейма IGMP

Коммутатор прослушивает сообщения IGMP, которыми обмениваются хост и маршрутизатор, чтобы отслеживать информацию multicast рассылки и порты, к которым она применяется. Когда коммутатор обнаруживает, что хост отправляет отчет IGMP на маршрутизатор, коммутатор добавляет порт в таблицу multicast адресов. Когда коммутатор обнаруживает сообщение IGMPLeave, отправленное хостом, маршрутизатор отправляет пакет. В случае определенного сообщения группового запроса (Group-SpecificQuery) порта, если есть другие хосты, которым нужна multicast рассылка, он ответит на сообщение отчета. Если маршрутизатор не получает ответа от хоста, коммутатор возьмет порт из multicast рассылки и удалит его в адресной таблице. Маршрутизатор периодически отправляет сообщение IGMPQuery. После получения сообщения Query коммутатор удаляет порт из таблицы multicast рассылки, если не получает сообщение отчета от хоста в течение определенного периода времени.

Как показано на рисунке ниже, когда устройства уровня 2 не используют IGMP-snooping, multicast данные передаются на уровне 2; когда устройства уровня 2 используют IGMP-snooping, multicast данные известных групп multicast рассылки не находятся на уровне 2. Они транслируются и передаются назначенному получателю на уровне 2, но неизвестные данные multicast рассылки все равно будут транслироваться на уровне 2.



6.7.1 IGMP-snooping

НажмитенаMulticast Manage— IGMP-snooping — IGMP-snoopingнапанелинавигации, чтобывойтивинтерфейсфункции, какпоказанониже:

Функции:

- **Включение (Enable)** Включает/выключает IGMP-snooping
- **Время старения хоста (Hostagingtime)** Когда порт-участник присоединяется к группе multicast рассылки, коммутатор выделяет время для порта в настройках.

Если коммутатор не получает пакет отчета, отправленный входящим портом, порт-участник считается недействительным.

6.7.2 IGMP-snoopingVLANconfiguration (Конфигурация VLAN с отслеживанием IGMP-пакетов)

Группа multicast рассылки, созданная с помощью IGMP-snooping, основана на broadcast домене VLAN. Различные сети VLAN могут быть настроены с разными параметрами IGMP. Эта страница используется для настройки параметров прослушивания фрейма IGMP для каждого VLAN.

Нажмите наMulticastManage>>IGMP-snooping>>IGMP-snoopingVLANconfiguration на панели навигации, чтобы войти в интерфейс функций, как показано ниже:

Функции:

- **Vlanid**введите VLANID, который позволяет прослушивать фреймы IGMP.
- **FastLeave.** Когда порт начинает быстро выходить из multicast, коммутатор напрямую получает сообщение IGMPLeave.

Удалить из группы multicast.

- **Адрес источника сообщения запроса(Querymessagesourceaddress)** Введите IP-адрес источника сообщения запроса.
- **Интервал сообщения запроса (Querymessageinterval)** Введите время интервала запроса, и генератор запросов будет отправлять общие сообщения запроса в соответствии с интервалом.

➢ **Максимальное время отклика (Maximumresponsetime)** Введите значение максимального времени ответа в поле сообщения запроса.

➢ **Интервал запроса последнего участника (Lastmemberqueryinterval)** Введите интервал для запроса участников multicast.

Routeagingtime -При маршрутизации multicast группы устройство выделяет время для маршрута

Когда порт маршрутизатора получает пакет запроса, он считает, что порт маршрутизации недействителен.

Примечание:

➢ Функция быстрого выхода может работать только в том случае, если хост поддерживает IGMPv2 или v3.

6.7.3 Staticmulticast

Static Multicast – отслеживание и добавление статических многоадресных MAC-адресов вручную для фильтрации многоадресного трафика. Некоторые устройства не поддерживают динамическую регистрацию в multicast-группе, но в то же время способны получать многоадресный трафик. Чтобы это было возможно, такие устройства нужно зарегистрировать вручную: создать запись с групповым адресом и номерами портов в таблице многоадресной рассылки маршрутизатора.

Нажмите на Layer 2 Management>>IGMP-snooping>>Staticmulticast на панели навигации, чтобы войти в интерфейс функции, как показано ниже:

Функции:

- **Vlan id**Введите VLAN ID для multicast VLAN.
- **Источник multicast (Multicast Source)** Введите IP-адрес исходного сервера multicast.
- **Адрес multicast (Multicast Address)** Введите IP-адрес multicast сервера, который должен быть адресом multicast.
- **Список портов (Portlist)** Выберите порт для добавления в группу multicast.

Примечание:

После установки статического multicast все сообщения IGMP обрабатываются только в статических multicast группах.

Описание:

- Адрес multicast (Multicast Address)

Согласно IANA (Internet Assigned Numbers Authority), IP-адрес multicast пакета использует IP-адрес класса D, а multicast IP-адрес находится в диапазоне от 224.0.0.0 до 239.255.255.255. Диапазон и описание нескольких специальных сегментов multicastIP-адреса следующие:

Диапазон адресов multicast	Отметка
224.0.0.0~224.0.0.255	Зарезервированный адрес протоколов маршрутизации и других протоколов обнаружения и обслуживания базовой топологии
224.0.1.0~224.0.1.255	Конференц-связь и видеоконференцсвязь. То есть публичный multicast адрес, который

	можно использовать в Интернете.
239.0.0.0~239.255.255.255	Адрес внутри LAN используется, и вы не можете использовать Интернет.

MulticastMAC-адрес

IANA предусматривает, что старшие 24 бита MAC-адреса multicast начинаются с 01-00-5E, а нижние 23 бита являются младшими 23 битами IP-адреса multicast.

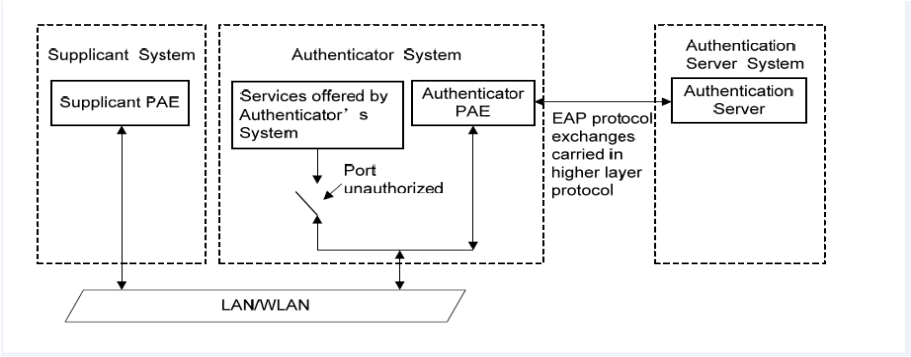
Большинство multicast адресов начинаются с 01-80-C2 и 01-00-5E, поскольку протоколы, которые используют эти multicast адреса, находятся под именем IEEE и IANA, их OUI— 00-80-C2 и 00- 00-5E, многоадресные адреса — 01-80-C2 и 01-00-5E. Конечно, помимо этих multicast адресов, занятых старшим братом, есть 01-00-0C- адрес, такой как CC-CC-CC, этот адрес занят Cisco, OUICisco— 00-00-0C.

6.8 Конфигурация 802.1x (802.1xconfiguration)

Протокол 802.1X был предложен комитетом IEEE 802 LAN/WAN для решения проблем безопасности сети WLAN. Протокол применяется к Ethernet как общий механизм управления доступом для порта LAN. В основном он используется для решения проблем аутентификации и безопасности в Ethernet. Устройство доступа реализовано на уровне порта сертификации и управления устройством доступа к локальной сети.
Коммутатор можно использовать в качестве системы аутентификации для компьютеров в сети. Если оборудование пользователя, подключенное к порту, может пройти аутентификацию коммутатора, оно получает доступ к ресурсам в локальной сети. Если коммутатор не может пройти аутентификацию коммутатора, ресурсы в локальной сети для него недоступны.

Архитектура 802.1X (802.1Xarchitecture)

Система 802.1X использует типичную архитектуру клиент/сервер и состоит из трех объектов, как показано на следующем рисунке.



1) Клиент (Client): объект в локальной сети, часто обычный компьютер. Пользователь инициирует аутентификацию 802.1X через клиентское программное обеспечение и аутентифицируется устройством. Клиентское программное обеспечение должно быть терминалом пользователя, поддерживающим аутентификацию 802.1X.
2) Устройство (Device): обычно сетевое устройство, поддерживающее протокол 802.1X, например коммутатор, предоставляет клиенту физический/логический порт для доступа к локальной сети и аутентифицирует клиента.
3) Сервер аутентификации (Authenticationserver): объект, который предоставляет услуги аутентификации для устройства. Например, сервер RADIUS может использоваться для реализации функций аутентификации и авторизации сервера аутентификации. Сервер может хранить информацию о клиенте, а также аутентифицировать и авторизовать клиента. Чтобы обеспечить стабильность системы аутентификации, вы можете настроить резервный сервер аутентификации для сети. Когда основной сервер аутентификации выходит из строя, резервный сервер может взять на себя его работу, чтобы обеспечить стабильность системы.

- **Механизм аутентификации 802.1X (802.1X Authentication Mechanism)**

Система аутентификации IEEE 802.1X использует EAP (ExtensibleAuthenticationProtocol) для обмена информацией аутентификации

между клиентом, устройством и сервером аутентификации.

1) Пакеты протокола EAP передаются напрямую в среде LAN с использованием формата инкапсуляции EAPOL между клиентом и устройством.

2) Есть два способа обмена информацией между устройством и RADIUS-сервером. Пакет протокола EAP переносится в формате инкапсуляции EAP (EAP через RADIUS) в протоколе RADIUS. Другой способ — устройство, которое завершает пакет протокола EAP и использует PAPили CHAP. Протокол аутентификации с помощью квитирования, сообщение протокола аутентификации с подтверждением связи, аутентифицируется на сервере RADIUS.

3) После того, как пользователь пройдет аутентификацию, сервер передаст соответствующую информацию о пользователе устройству. Устройство определяет авторизованный/неавторизованный статус контролируемого порта в соответствии с индикацией RADIUS-сервера (Accept или Reject).

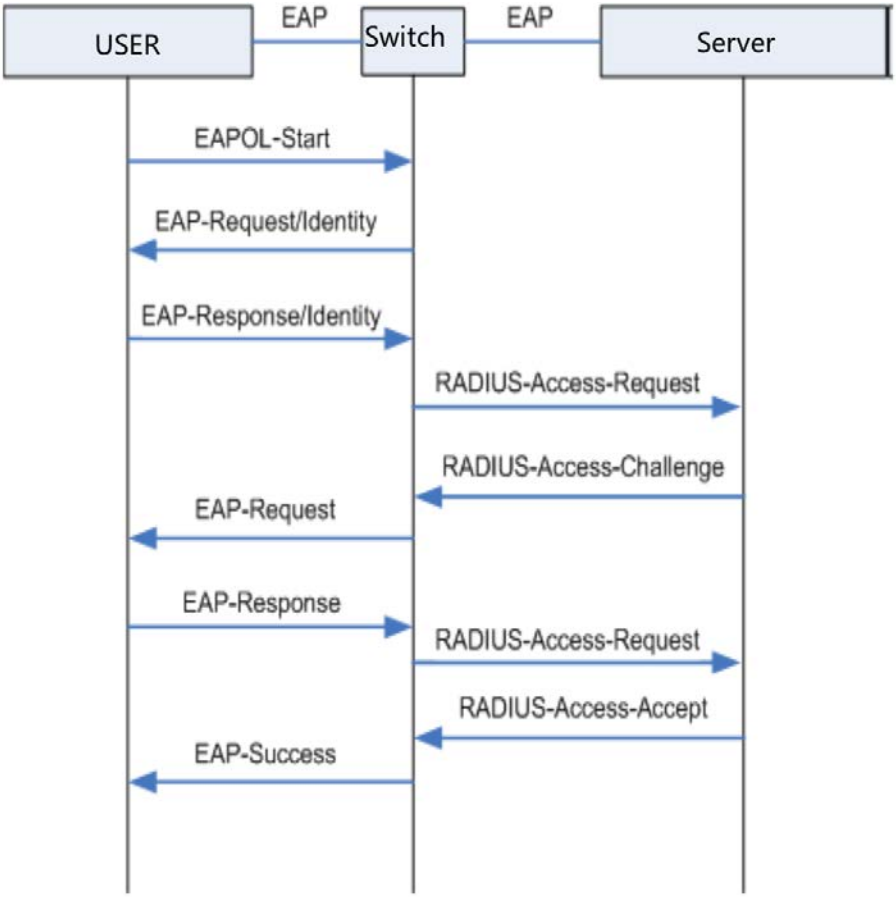
- Процесс аутентификации 802.1X (802.1X Authentication process)

Процесс аутентификации может быть инициирован клиентом или устройством. Когда устройство обнаруживает, что сеть использует неаутентифицированный пользователь, оно отправляет клиенту пакет EAP-Request/Identity для инициации аутентификации. С другой стороны, клиент может отправить EAPOL на устройство через клиентское программное обеспечение, чтобы инициировать аутентификацию.

Система 802.1X поддерживает режим ретрансляции EAP и режим завершения EAP для взаимодействия с удаленным сервером RADIUS. Далее следует описание процесса двух методов аутентификации по инициативе клиента в качестве примера.

Режим ретрансляции EAP (EAP relay mode)

Режим ретрансляции EAP определяется стандартом IEEE 802.1X. EAP (протокол расширенной аутентификации) передается в других протоколах высокого уровня, таких как EAP через RADIUS, так что пакеты протокола расширенной аутентификации проходят на сервер аутентификации через сложную сеть. Обычно для режима ретрансляции EAP требуется, чтобы сервер RADIUS поддерживал атрибут EAP: EAP-сообщение и аутентификатор сообщения. Коммутатор поддерживает режим ретрансляции EAP—EAP-MD5. Далее изображен процесс аутентификации EAP-MD5.



1) Когда у пользователя есть доступ к сети, откройте клиентскую программу 802.1X, введите имя пользователя и пароль, на которые были поданы заявки и которые были зарегистрированы, и инициируйте запрос на соединение (сообщение EAPOL-Start). На этом этапе клиентская программа отправляет на устройство сообщение с запросом аутентификации, чтобы начать процесс аутентификации.

2) После получения фрейма данных, запрашивающего аутентификацию, устройство отправляет фрейм (EAP-Request / Identitymessage), чтобы запросить клиентскую программу пользователя на отправку введенного имени

пользователя.

3) Клиентская программа отправляет информацию об имени пользователя на устройство через фрейм данных (EAP-Response / Identitypacket) в ответ на запрос от устройства. Устройство отправляет фрейм данных, отправленный клиентом, на сервер аутентификации для обработки после обработки пакета (пакет запроса доступа RADIUS).

4) После получения информации об имени пользователя, пересылаемой устройством, сервер RADIUS сравнивает информацию с таблицей имен пользователей в базе данных, находит информацию о пароле, соответствующую имени пользователя, и шифрует ее с помощью случайно сгенерированного слова шифрования. Зашифрованное слово отправляется на устройство через пакет RADIUSAccess-Challenge и пересылается устройством клиентской программе.

5) После получения от устройства зашифрованного слова (сообщения EAP-Request / MD5 Challenge) клиентская программа шифрует часть пароля с помощью зашифрованного слова. (Этот алгоритм шифрования обычно необратим и генерирует EAP-Response. Пакет MD5 Challenge передается на сервер аутентификации через устройство.)

6) Сервер RADIUS сравнивает полученную информацию о зашифрованном пароле (пакет запроса доступа RADIUS) с зашифрованной информацией о пароле. Если информация совпадает, пользователь считается действующим пользователем. Сообщение принимается успешно (EAP-Successmessage).

7) После получения сообщения о прохождении аутентификации устройство переводит порт в авторизованное состояние, позволяя пользователю получить доступ к сети через порт. В течение этого периода устройство отслеживает онлайн-статус пользователя, периодически отправляя клиенту пакеты подтверждения (handshakepackets). По умолчанию устройство не получает ответа от клиента. Устройство позволит пользователю перейти в автономный режим. Это предотвращает отключение устройства из-за ненормальных условий.

8) Клиент также может отправить на устройство пакет EAPOL-Logoff для активного запроса в автономном режиме. Устройство меняет статус порта с авторизованного на неавторизованный.

Таймер 802.1X (802.1Xtimer)

Во время процесса аутентификации 802.1X для управления взаимодействием между пользователями доступа, устройствами и серверами RADIUS запускается несколько таймеров. В данном коммутаторе имеется три основных типа таймеров 802.1X:

1) **Таймер тайм-аута повторной аутентификации (Re-authenticationtimeouttimer):**при установке этого таймера коммутатор периодически инициирует повторную аутентификацию 802.1X.

2) **Таймер тайм-аута сервера аутентификации (Authenticationservertimeouttimer):**этот таймер запускается после того, как коммутатор отправляет пакет на сервер аутентификации. Если коммутатор не получает ответ от сервера аутентификации в течение срока, установленного таймером, то он повторно отправляет пакет запроса аутентификации.

3) **Таймер молчания (Quiettimer):** После того, как пользователю не удается пройти аутентификацию, коммутатор должен некоторое время молчать (это время определяется таймером молчания). В период молчания коммутатор не обрабатывает запрос аутентификации пользователя.

6.8.1 Конфигурация (Configuration)

На странице глобальной конфигурации вы можете включить глобальную аутентификацию 802.1X, выбрать метод аутентификации, предоставляемый коммутатором, установить адрес и номер порта клиента RADIUS, а также настроить различные таймеры для управления аутентификацией 802.1X для всей системы.

Нажмите на Layer 2 Management >> 802.1X >> Global configuration на панели навигации. Интерфейс показан ниже.

Инструкция :

- **Глобальная конфигурация**

Функциональный коммутатор 802.1 (802.1 functional switch) : Выберите, следует ли включать аутентификацию 802.1X.

Метод верификации (verification method) : Выберите метод аутентификации 802.1X.

- Аутентификация на основе портов (port-basedauthentication): система аутентифицирует доступ пользователей (accessusers) на основе портов. То есть, пока первый пользователь под физическим портом успешно аутентифицирован, другие пользователи могут использовать сетевые ресурсы без аутентификации. После того, как пользователи перейдут в автономный режим, другим пользователям также будет отказано в доступе к сети.

  Аутентификация на основе MAC (MAC-basedauthentication): система аутентифицирует пользователей на основе MAC-адреса. То есть все пользователи доступа к физическому порту должны пройти аутентификацию индивидуально. Если пользователь переходит в автономный режим, он не

	может использовать аутентификацию. При этом сеть не меняет использование сетевых ресурсов другими пользователями.
Адрес клиента RADIUS (RADIUS client address) :	Установите IP-адрес клиента Radius
Номер порта клиента RADIUS (RADIUS Client port number) :	Установите номер порта клиента Radius
Общий пароль сервера RADIUS (RADIUS server share password) :	Установите общий ключ пакета сервера Radius
Ретрансмиссии сервера RADIUS (RADIUS server retransmissions) :	Установите количество повторных передач пакетов сервера Radius. Если совокупное количество передач превышает максимальное количество передач, а сервер Radius по-прежнему не отвечает, коммутатор принимает это за сбой аутентификации. По умолчанию максимальное количество повторных передач пакетов запроса Radius равно 5 раз.
Тайм-аут сервера RADIUS (RADIUS server timeout) :	Установите время ожидания ответа сервера Radius. Если коммутатор не получает ответ от сервера Radius после того, как пакет запроса Radius (запрос аутентификации/авторизации или запрос учета) передан в течение определенного периода времени, необходимо повторно запросить пакет запроса Radius, чтобы гарантировать безопасность пользователя. Сервис Radius на самом деле доступен. Это время называется таймаутом ответа сервера Radius; по умолчанию время ожидания ответа

Radius-сервера составляет 5 секунд.

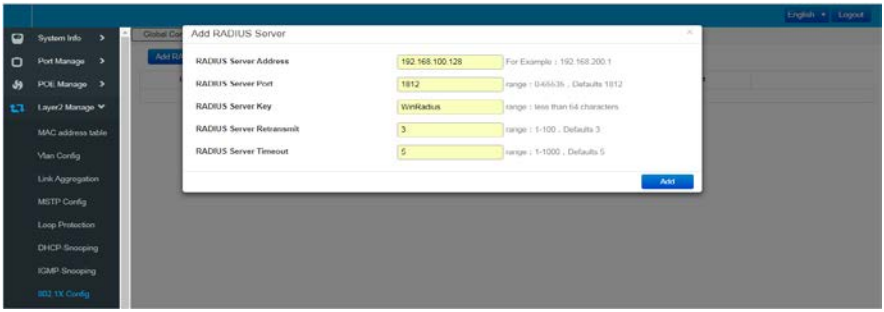
Потеря времени сервера RADIUS (RADIUS Server death time) :	Установите потерю времени сообщения сервераRadius.

6.8.2 Настройки сервера RADIUS (RADIUS server settings)

RADIUS (Служба удаленной аутентификации пользователя с телефонным подключением). Сервер аутентификации предоставляет для коммутатора услугу аутентификации, которая хранит информацию о пользователе, включая имя, пароль и другие параметры, для реализации аутентификации, авторизации и учета для пользователя. Страница конфигурации RADIUS используется для установки параметров сервера аутентификации в сети, чтобы гарантировать плавность и упорядоченность процесса аутентификации.

1. Нажмите на Layer 2 Configuration>> 802.1XConfiguration>>RADIUSserversettings, чтобы войти в интерфейс настроек сервера RADIUS, как показано на рисунке ниже:

2. Нажмите на “Добавить сервер RADIUS” (AddRADIUSServer), чтобы войти в интерфейс добавления сервера RADIUS и добавить информацию о конфигурации сервера RADIUS, как показано на рисунке ниже:



Описание:

- Конфигурация сервера (Serverconfiguration)

Адрес сервера (Server address)	Введите IP-адрес сервера.
Общий ключ (Shared key):	Введите ключ шифрования, общий для коммутатора и сервера.
Порт аутентификации (Authentication port):	Номер порта аутентификации, используемый сервером.。
Количество ретрансмиссий (Number of retransmissions):	Максимальное количество повторных передач после тайм-аута

Время ожидания (Overtime time) | Максимум времени ожидания

6.8.3 Аутентификация на основе порта (Port-basedauthentication)

На странице функции конфигурации порта вы можете установить функцию 802.1X порта в соответствии с фактическими условиями сети.

Нажмите на Layer 2 Configuration>> 802.1XConfiguration>>Port-basedauthentication, войдите в интерфейс «Аутентификация на основе портов», как показано ниже.

Описание

Описание

Конфигурация портов (PortConfiguration)

Включение аутентификации (Authentication enable) : Включите порт и настройте статус аутентификации 802.1X порта.

Порт (Port) : Отображение номера порта коммутатора

Режим контроля (Control mode) : Выберите режим управления для этого порта。
Автоматический: порт должен быть аутентифицирован。Принудительная сертификация: порт может получить доступ к сети без аутентификации。
Принудительно несертифицированный: порт никогда не пройдет аутентификацию。

Статус сертификации (Certification status) : Показать статус авторизации этого порта。
Введите время молчания. После сбоя

Время молчания (Silent time) :	аутентификации пользователя запрос аутентификации 802.1X того же пользователя больше не обрабатывается в режиме молчания.
Времяповторнойаутентификации (Reauthenticationtimes) :	Введите максимальное количество повторных передач для аутентификации
Цикл передачи EAP (EAP transmission Cycle):	Введите время передачи EAP
Цикл повторной аутентификации (Re-authentication cycle) :	Введите время цикла повторной аутентификации
Переключатель повторной аутентификации (Re-authenticationswitch) :	Включение или отключение повторной аутентификации

Глава 7: Расширенные настройки (Advancedsettings)

7.1 КонфигурацияQOS (QOSconfiguration)

Функция QoS (качество обслуживания) используется для повышения надежности сетевой передачи и предоставления высококачественных сетевых услуг. В традиционной IP-сети все пакеты обрабатываются одинаково без различия. Сеть отправляет пакеты с максимальным усилием, но не гарантирует никакой производительности, такой как задержка и надежность.

Наряду с быстрым развитием сетевых технологий и мультимедийных технологий IP-сети все чаще предоставляют услуги интерактивной мультимедийной связи, такие как видеоконференцсвязь, дистанционное обучение и видео по запросу, основанные на существующих услугах, таких как www, FTP и электронная почта, видеофоны и т. д. И для каждой такой услуги требуются разные задержки передачи, переменные

задержки, пропускная способность и скорость потери пакетов. Следовательно, обеспечение разного качества обслуживания (QoS) для разных услуг пользователей стало важной задачей для развития Интернета.

Так называемое QoS предназначено для различных нужд сетевых приложений и обеспечивает разное качество обслуживания, такое как предоставление выделенной полосы пропускания, снижение скорости потери пакетов и уменьшение задержки передачи пакетов и джиттера задержки. То есть в случае, если пропускной способности недостаточно, противоречия в полосе пропускания, занимаемой различными потоками услуг, уравновешиваются.

Принцип работы QoS

Коммутатор классифицирует потоки данных на этапе входа, а затем сопоставляет различные типы потоков данных с очередями с разными приоритетами на этапе экспорта и, наконец, определяет способ пересылки пакетов очередей с различным приоритетом в соответствии с режимом планирования, тем самым реализуя функцию QoS.

8-1 принцип работы

Классификация сообщений: объекты идентифицируются в соответствии с определенными правилами сопоставления.

Mapping: Пользователи могут отображать пакеты, поступающие на коммутатор, в очереди с разными приоритетами в соответствии с режимом приоритета. Коммутатор поддерживает три режима приоритета: приоритет на основе порта, приоритет 802.1P / COS и приоритет DSCP.

Планирование очереди (Queuescheduling): Когда сеть перегружена,

планирование очереди должно решить проблему одновременной конкуренции нескольких потоков данных за ресурсы.

Коммутатор обеспечивает четыре режима планирования: режим со строгим приоритетом (SP), режим циклического перебора с взвешиванием (WRR), режим циклического перебора (RR) и режим взвешенной справедливой очереди (WFQ).

Режим планирования (Schedulingmode)

Когда сеть перегружена, для решения проблемы одновременной конкуренции нескольких потоков данных за ресурсы обычно используется планирование очередей. Коммутатор реализует в общей сложности восемь очередей планирования — от TC0 до TC7. TC0 соответствует очереди с самым низким приоритетом, а TC7 соответствует очереди с самым высоким приоритетом. В то же время коммутатор обеспечивает четыре режима планирования, а именно режим строгого приоритета (SP), взвешенный циклический алгоритм (RoundRobin, WRR), режим RR и взвешенную справедливую очередь (WeightedFairQueue, WFQ).

1.SP-Mode: режим строгого приоритета. Режим SP заключается в том, что коммутатор предпочтительно пересылает фрейм данных с наивысшим приоритетом на данный момент. После пересылки всех фреймов данных с наивысшим приоритетом пересылаются фреймы данных со следующим наивысшим приоритетом. Коммутатор имеет восемь выходных очередей —TC0-TC7. В режиме очереди SP их приоритеты по очереди увеличиваются, и TC7 имеет наивысший приоритет. Недостаток очереди SP состоит в том, что если пакет находится в очереди с более высоким приоритетом в течение длительного времени при возникновении перегрузки, пакет в очереди с низким приоритетом будет «голодать» из-за отсутствия обслуживания.

2. WRR-Mode: режим приоритета WRR (WRR priority mode). Алгоритм планирования режима WRR выполняет циклическое планирование между очередями в соответствии с взвешенным соотношением, чтобы гарантировать, что каждая очередь получит определенное время обслуживания. Взвешенное значение указывает долю приобретенного ресурса. Очередь WRR позволяет избежать того недостатка, что пакеты с низким приоритетом могут не обслуживаться в течение длительного времени при использовании планирования SP, и хотя планирование нескольких очередей выполняется циклически, это не фиксированное время обслуживания, распределенное для каждой очереди. Если очередь пуста, следующее расписание очереди будет немедленно заменено, чтобы ресурсы полосы пропускания были полностью использованы. Взвешенное соотношение TC0-TC7 по умолчанию составляет 1: 2: 4: 8: 16: 32: 64: 127.

3.RR-Mode: Round-Robinmode, стратегия планирования каналов при обмене данными, которая позволяет пользователям по очереди использовать совместно используемые ресурсы без учета мгновенных состояний канала. С точки зрения того, что одинаковое количество радиоресурсов (один и тот же период времени планирования) выделяется каждому каналу связи, циклический перебор можно рассматривать как справедливое планирование. Однако циклический перебор несправедлив с точки зрения обеспечения одинакового качества обслуживания для всех каналов связи, и в этом случае для каналов связи с плохими условиями канала (больше времени) необходимо выделить больше ресурсов. Кроме того, поскольку циклический перебор не учитывает мгновенные состояния канала во время процесса планирования, это приведет к снижению общей производительности системы, но более сбалансированному качеству обслуживания между различными линиями

связи, чем максимальное планирование отношения мощности несущей к помехе.

4. WFQ-Mode: режим взвешенной справедливой очереди. WFQ— это сложный процесс организации очереди, который гарантирует справедливость между одинаковым приоритетом и весами между разными приоритетами. Количество очередей можно предварительно настроить, и диапазон составляет (16-4096).

WFQ воплощают вес на основе гарантии равноправия (полоса пропускания, задержка), значение веса зависит от приоритета IP, передаваемого в заголовке пакета JP.WFQ классифицирует пакеты по потоку (тот же исходный IP-адрес, целевой IP-адрес, номер исходного порта, номер порта назначения, номер протокола, сообщения приоритета принадлежат одному потоку). Каждый поток назначается в очередь. Этот процесс называется хешированием. Процесс регистрации WFQ автоматически завершается с использованием алгоритма HASH, и разные потоки максимально разделяются на разные очереди. Во время удаления из очереди WFQ распределяет полосу пропускания каждого потока для выхода в соответствии с приоритетом потока. Чем меньше значение приоритета, тем меньше пропускная способность. Чем больше значение приоритета, тем больше пропускная способность. Это обеспечивает справедливость между одинаковыми приоритетными услугами и отражает вес между разными приоритетными услугами. Например, в настоящее время в интерфейсе 8 потоков с приоритетами О, 2, 2, 3, 4, 5, 6 и 7. Общая квота на полосу пропускания будет: сумма всех (приоритет поток + 1). А именно: 1 + 3 + 3 + 4 + 5 + 6 + 7 + 8 = 37.

Соотношение пропускной способности, занимаемой каждым потоком, составляет: (его собственный номер приоритета + 1), (сумма всех (приоритет потока +1)). То есть доступная пропускная способность для каждого потока: 1/37, 3/37, 3/37, 4/37, 5/37, 5/37, 6/37, 7/37, 8/37.

Можно видеть, что WFQ отражает вес различных приоритетных услуг на основе обеспечения справедливости, а вес зависит от приоритета IP, передаваемого в заголовке IP-пакета.

7.1.1 Глобальная конфигурация (Globalconfiguration)

Когда сеть перегружена, должна быть решена проблема одновременной конкуренции нескольких пакетов за ресурсы. Обычно в этом случае используется планирование очереди. В управлении перегрузкой обычно используются методы планирования очередей, чтобы избежать периодической перегрузки в сети. Применяются следующие методы планирования очередей: SP (Strict-Priority, Строгий приоритет, очередь со строгим приоритетом)、WFQ（WeightedFairQueue,Взвешенная справедливая очередь）и WRR（WeightedRoundRobin, Взвешенный циклический алгоритм, Взвешенная очередь опроса、RR（RoundRobin, Циклическое планирование）。

Настроить этапы работы с типом планирования интерфейса

1. Нажмите на Advanced settings >> QOS configuration >> Global configuration, войдите в интерфейс Scheduling Policy, как показано ниже.

Описание:

Конфигурация режима планирования (Schedulingmodeconfiguration)

SP-Mode : Режим строгого приоритета. В этом режиме очередь с высоким приоритетом занимает всю полосу пропускания. Только после того, как высокоприоритетная очередь пуста,

низкоприоритетная очередь может пересылать свои данные.

WRR-Mode : Режим приоритета взвешенного опроса. Алгоритм планирования очереди WRR выполняет циклическое планирование между очередями, чтобы гарантировать, что каждая очередь получит определенное время обслуживания. Например, в примере с портом с 8 очередями вывода, WRR может настроить значение веса для каждой очереди.

(Весовые значения, соответствующие queue7 ~ queue0: w7, w6, w5, w4, w3, w2, w1, w0)

RR-Mode : Политика планирования позволяет пользователям использовать общие ресурсы по очереди, независимо от текущих условий канала. Поскольку при планировании опроса не учитываются мгновенные состояния канала во время процесса планирования, это приведет к снижению общей производительности системы.

Однако, по сравнению с планированием максимального отношения несущей к помехе, получается более сбалансированное качествообслуживания между линиями связи.

WFQ-Mode : Режим взвешенной справедливой очереди. Пользователи могут использовать алгоритм планирования очереди WFQ, чтобы указать

	полосу пропускания для каждой очереди от 0 до 7. Затем, в соответствии со значением CoS каждого потока и отношением отображения очереди, определяется, какой поток входит в какую очередь и какая полоса пропускания делится.
Значение веса очереди (Queueweightvalue) :	Введите значение веса для 8 очередей. Когда выбраны режимы RR и SP, настройка значения веса не допускается.

mapping COS

(Нажмите на Advanced Manage>> QOS Configuration >> Global configuration, войдите в интерфейс COS Queue Mapping, как показано ниже.

Значение интерфейса следующее:

Предмет настройки	Инструкции
Cos	Диапазон 0-7
Очередь (Queue)	Диапазон 0-7

mapping DSCP

(Нажмите на Advanced Manage >> QOS Configuration >> Global Configuration, войдите в интерфейс COS Queue Mapping, как показано ниже.

Описание：

- **Приоритет (Priority)**

DSCP： Приоритет DSCP пакета с уровнем приоритета от 0 до 63.

NEW DSCP: НОВЫЙ приоритет пакета DSCP с уровнем приоритета от 0 до 63.

COS： Соответствует разным уровням очередей приоритета. Выражается как COS0, COS1 ... COS7.

7.1.2 Управление портом (PortConfig)

Шаги по управлению портом

1. Нажмите на AdvancedManage>>QOSConfiguration>>PortConfig, войдите в интерфейс PortConfig, нажмите Apply, чтобы завершить настройку, как показано ниже.

Описание:

Настройка приоритета порта (Portprioritыconfiguration)

Порт (Port)： Физический порт коммутатора。

Приоритет (Priority) :	Настройте уровень приоритета порта.

7.2 Конфигурация ACL (ACL Configuration)

С расширением масштаба сети и увеличением трафика контроль безопасности сети и распределение полосы пропускания становятся важной частью управления сетью. Фильтруя пакеты, вы можете эффективно предотвратить доступ к сети неавторизованных пользователей. Вы также можете контролировать трафик и экономить сетевые ресурсы. ACL (список управления доступом) используется для реализации фильтрации пакетов путем настройки правил сопоставления и операций обработки пакетов.

После получения пакета порт коммутатора анализирует поле пакета в соответствии с правилом ACL, примененным к текущему порту. После идентификации конкретного пакета соответствующий пакет разрешается или запрещается в соответствии с предварительно установленной политикой.

На правило сопоставления пакетов, определенное списком ACL, также могут ссылаться другие функции, которым необходимо различать трафик, например определение правила классификации трафика в QoS.

Путем установки правил сопоставления и обработки операций список управления доступом (ACL) может реализовать фильтрацию пакетов. Список управления доступом (accesscontrollist) — это набор условий лицензирования и отклонения, которые применяются к пакету. При получении пакета на интерфейсе коммутатор определяет, что пакету разрешено пересылать, на основе критериев, указанных в списке доступа, по сравнению с используемым ACL. ACL классифицирует пакеты по ряду

совпадающих условий, таких как адрес источника, адрес назначения и номер порта пакета. ACL можно разделить на следующие категории в зависимости от цели приложения:

Базовый IPACL (BasicIPACL): правила формулируются на основе только исходного IP-адреса пакета. Диапазон идентификатора ACL: 100 ~ 999.

Расширенный IPACL (AdvancedIPACL): правила основаны на информации уровня 3 и уровня 4, такой как исходный IP-адрес, IP-адрес назначения, тип протокола IP-канала-носителя и характеристики протокола. Диапазон идентификатора ACL: 100 ~ 999.

MACACL : Правила формулируются на основе информации уровня 2, такой как MAC-адрес источника, MAC-адрес назначения, приоритет VLAN и тип протокола уровня 2 пакета данных. Диапазон идентификаторов ACL: 1 ~ 32.

7.2.1 Конфигурация MACACL (MACACLConfiguration)

MACACL: Правила формулируются на основе информации уровня 2, такой как MAC-адрес источника, MAC-адрес назначения, приоритет VLAN и тип протокола уровня 2.

Шаги:

1. Нажмите на AdvancedManage>>ACLConfiguration>>MACALCConfiguration и вы перейдете в интерфейс настройки MACALC, как показано ниже.

Описание:

MAC ACL

Список контроля доступа ID (Access control list ID):	Выберите ACLID, который нужно настроить.
ID правила (Rule ID) :	Введите ID правила。
Операция безопасности (SecurityOperation) :	Выберите, как коммутатор обрабатывает пакеты, соответствующие правилам сопоставления. По умолчанию “разрешить”. • Allow : Пересылает пакеты. • Discard : Отбрасывает пакеты.
Исходный MAC (Source MAC) :	Введите информацию об исходном MAC-адресе, содержащуюся в правиле.
Маска исходного MAC (Source MAC mask) :	Введите маску исходного MAC-адреса.
MAC-адрес назначения	Введите информацию о MAC-адресе назначения, содержащуюся в правиле.

(Destination
MAC) :

Маска MAC-адреса назначения (DestinationMACMask) : Введите маску MAC-адреса назначения.

Название временного диапазона (Time-rangename) : Выберите название периода времени правила. Значение не ограничено по умолчанию.

2.Заполните соответствующие элементы конфигурации.

3.Нажмите «Добавить» (Add), чтобы завершить настройку, как показано.

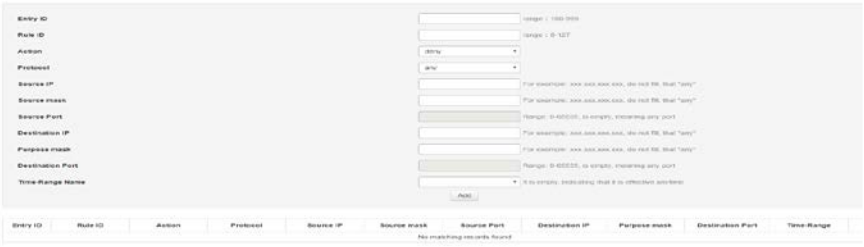
7.2.2 Конфигурация IP ACL (IP ACL Configuration)

Базовый IPACL (BasicIPACL) : Правила формулируются на основе только IP-адреса источника пакета. Диапазон ACLID: 100 ~ 999.

Расширенный IPACL (AdvancedIPACL) : Правила основаны на информации Уровня 3 и Уровня 4, такой как IP-адрес источника, IP-адрес назначения, тип протокола IP-канала-носителя и характеристики протокола. Диапазон ACLID: 100 ~ 999

Шаги:

1. Нажмите на AdvancedManage>>ACLConfiguration>>IPALCConfiguration и вы перейдете в интерфейс конфигурации IPALC, как показано ниже.



Описание:

Расширение IPACL (ExpansionIPACL)

Список контроля доступа **ID (Access control list ID)** :	ВыберитеACLID, который вы хотите настроить.
ID правила (Rule ID) :	Введите ID правила.
Безопасное функционирование(Safe Operation) :	Выберите, как коммутатор обрабатывает пакеты, соответствующие правилам сопоставления. По умолчанию “разрешено”. • Allow：Пересылает пакет. •Discard：Отбрасывает пакет.
Исходный IP (Source IP) :	Введите информацию об исходном IP-адресе, содержащуюся в правиле.
Исходная маска (Sourcemask) :	Введите маску IP-адреса источника。
IP-адрес назначения (DestinationIP):	Введите информацию об IP-адресе назначения, содержащуюся в правиле.

Маска назначения (Destination mask):	Введите маску IP-адреса назначения.
Протокол (Protocol):	Выберите информацию IP-протокола, содержащуюся в правиле.
Номер исходного порта (Source port number) :	Когда протокол IP выбирает TCP / UDP, здесь настраивается номер порта источника TCP / UDP, включенный в правило.
Номер порта назначения (Destination port number):	Когда протокол IP выбирает TCP / UDP, здесь настраивается номер порта назначения TCP / UDP, включенный в правило.
Временной период (Time period):	Выберите название периода времени, когда правило вступит в силу

2.Заполните соответствующий элемент конфигурации

3.Нажмите «Добавить» (Add) и вы завершите настройку, как показано на рисунке.

7.2.3 Конфигурация временного диапазона (TIMERANGEConfiguration)

Конфигурация эффективного временного диапазона позволяет пользователю контролировать ACL пакеты в зависимости от временного диапазона.

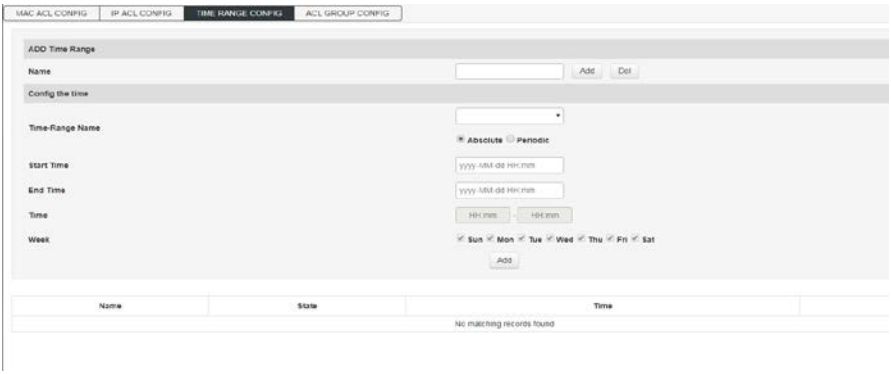
Период времени (Timeperiod) используется для описания определенного диапазона времени. У пользователей могут быть такие требования:

некоторые правила ACL должны быть действительными в течение одного или определенного времени, в то время как они не используются для фильтрации пакетов в другие периоды времени, что обычно называется фильтрацией по периоду времени. В это время пользователь может сначала настроить один или несколько периодов времени, а затем ссылаться на период времени при настройке правила ACL, тем самым реализуя фильтрацию ACL на основе времени.

Конфигурация периода времени содержит следующее: период времени конфигурации (configurationperiodtimeperiod) и период абсолютного времени (absolutetimeperiod). Период времени конфигурации имеет форму дня недели; период абсолютного времени конфигурации принимает форму от времени начала до времени окончания.

Шаги

Нажмите на Advanced Manage>> ACL Configuration >> TIME RANGE Configuration и войдите в интерфейс TIME RANGE Configuration, как показано ниже.



Описание:

Добавить временной диапазон (AddTimeRange)

Название временного диапазона (TimePeriodName):	Введите название диапазона времени, чтобы было легче различать информацию о каждом периоде времени.
Абсолютное время (Absolute time):	Настройте режим абсолютного времени для временного диапазона. Правило ACL на основе периода времени может вступить в силу только в том случае, если системная дата указана в абсолютном времени.
Цикл (Cycle) :	Настройте периодический режим временного диапазона. Только когда системная дата находится в пределах времени цикла, правило ACL, основанное на временном диапазоне, может вступить в силу.
Время начала (Starttime) :	Настройте время начала временного сегмента во временном диапазоне。
Время окончания (Endtime) :	Настройте время окончания временного сегмента во временном диапазоне。

Список временного диапазона (TimeRangeList)

Название (Name) :	Отображает название временного диапазона.
Статус (Status) :	Отображает статус временного периода.

Время (Time) : Отображает настроенный временной период.

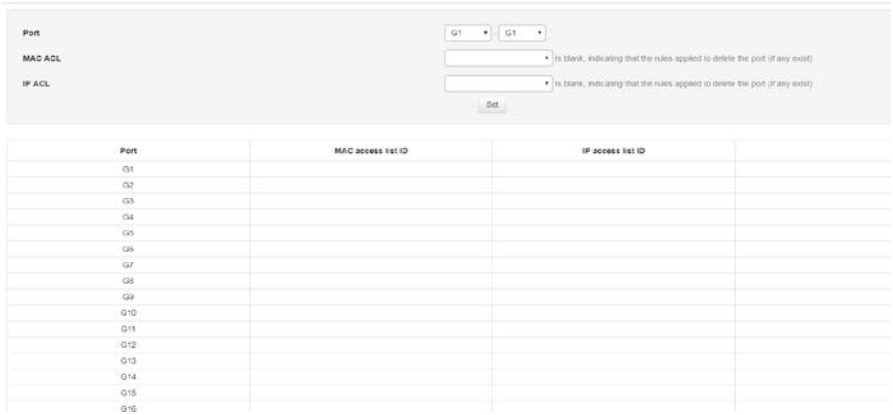
Удалить (Delete) : Удалить временной диапазон.

7.2.4 Конфигурация ГруппыACL (ACL Group Configuration)

После того, как вы создали список, вам нужно будет применить его ко всем интерфейсам, которые вы хотите использовать.

Шаги:

1.Нажмите на AdvancedManage>>ACLConfiguration>>ACLGROUPConfiguration, затем перейдите в интерфейс конфигурации группы ACL, как показано ниже.



Описание:

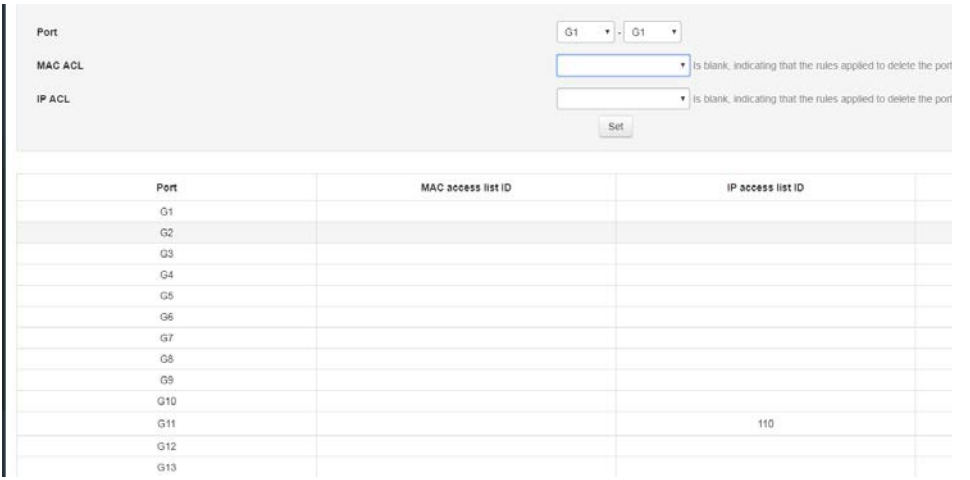
➢ **Конфигурация группы ACL (ACL GROUP Configuration)**

ID списка доступа MAC (MAC access list ID) Выберите ID созданного списка MAC-адресов и примените его к порту.

ID списка доступа IP (IP access list ID):	Выберите ID созданного списка доступа IP и примените его к порту.

2.Заполните соответствующий элемент конфигурации. Используйте acl 1 и acl 100 в качестве примеров, примените к G1-G2 и G3-G4 соответственно.

3. Нажмите Settings, чтобы завершить настройку, как показано на рисунке.



7.3 Конфигурация SNMP (SNMP Configuration)

➢ Обзор SNMP (SNMP Overview)

SNMP (простой протокол управления сетью) является наиболее распространенным протоколом управления сетью в сетях UDP / IP, он обеспечивает структуру управления для мониторинга и обслуживания интернет-устройств. Структура SNMP проста и удобна в использовании, он может скрыть физические различия между различными устройствами для достижения автоматического управления разными устройствами. Большинство систем и платформ управления сетью основаны на SNMP.

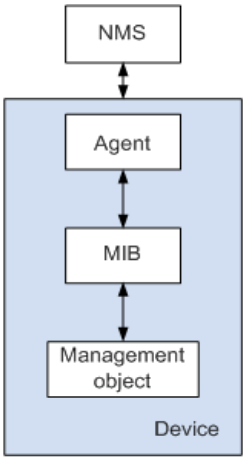
Самым большим преимуществом SNMP является его простой дизайн. Он не требует сложного процесса внедрения, а также не требует слишком много сетевых ресурсов, прост в использовании. Основные функции SNMP включают мониторинг производительности сети, обнаружение и анализ сетевых ошибок, а также настройку сетевых устройств. Когда сеть работает корректно, SNMP может предоставить статистику, функции конфигурации и тестирования. Когда сеть выходит из строя, SNMP может реализовать разнообразное обнаружение ошибок и восстановление.

- **Структура управления SNMP (SNMP Management framework)**

Система SNMP включает в себя NMS（систему управления сетью）、агент, объект управления и MIB（базу управляющей информации), NMS как центр сетевого управления всей сетью для управления устройствами.

Каждое управляемое устройство содержит процесс агента, MIB и несколько управляемых объектов на устройстве. NMS взаимодействует с агентом, работающим на управляемом устройстве, затем агент выполняет команду NMS, управляя MIB устройства.

Модель управления SNMP



- NMS играет роль управления в сети, используя SNMP— это протокол для систем управления/мониторинга сетевого оборудования, работающий на сервере NMS. NMS может отправить агенту на устройстве запрос на запрос или изменение одного или нескольких конкретных параметров. NMS может получать информацию о прерываниях (trapinformation), отправленную агентом на устройстве, чтобы узнать текущий статус управляемого устройства.
- Агент (Agent) — это агентский процесс в управляемом устройстве для поддержания информационных данных управляемого устройства и передачи данных управления в NMS, которая отправила запрос в ответ на запрос от NMS. После получения информации о запросе от NMS агент выполняет соответствующую инструкцию через таблицу MIB и отправляет результат операции в NMS. Если происходит сбой оборудования или другое событие, устройство автоматически отправляет информацию агенту NMS, чтобы изменить текущее состояние отчетного устройства NMS.
- Managementobject означает “управляемый объект”. Каждое устройство может содержать несколько управляемых объектов. Управляемым

объектом может быть какое-то оборудование в устройстве (например, интерфейсная плата), или это может быть набор оборудования, программного обеспечения (например, протокол маршрутизации) и его параметры конфигурации.

- MIB— это база данных, которая указывает, что переменные поддерживаются управляемыми устройствами (т. е. могут быть запросом агента и заданной информацией). MIB определяет набор атрибутов управляемого устройства в базе данных: имя объекта, его состояние, права доступа и тип данных. С помощью MIB могут быть выполнены следующие функции: Агент может получить информацию о текущем состоянии устройства, запросив MIB.

  Агент может установить параметры состояния устройства, изменив MIB.

Версия протокола SNMP

Данный коммутатор обеспечивает функции управления SNMPv3 и совместим с SNMPv1 и SNMPv2c. Версия управления SNMP и версия агента SNMP должны быть согласованы. Они могут общаться друг с другом. Вы можете выбрать различные режимы управления уровнем безопасности в соответствии с требованиями вашего приложения.

7.3.1 Системная информация (Systeminformation)

1. Нажмите на AdvancedManage>SNMPConfiguration, чтобы войти в интерфейс информации о системе, как показано ниже.

Описание:

Конфигурация системы SNMP (SNMP Configuration system)

Версия (Versions) :	Выбор невозможен, устройство SNMP по умолчанию поддерживает SNMPv2c и SNMPv3.
Имя (System Name)	Введите имя системы
Местоположение (Location)	Введите информацию о местоположении
Контакт (Contact) :	Введите контактную информацию

- **Конфигурация прерывания (Trap configuration)**

ɔ выбору (selectable), включить (enable) или отключить (disable), Trapнеобходим д

важных событиях (например, перезапуск управляемого устройства и т. д.).

7.4 Конфигурация RMON (RMONConfiguration)

RMON (RemoteMonitoring, RemoteNetworkMonitoring) основаннаархитектуреSNMPипредставляетсобойстандартнуюспецификацию мониторинга, предложеннуюИнженерной группой Интернета (IETF). Это позволяет SNMP более эффективно и проактивно контролировать удаленные устройства. С помощью функции RMONNMS может быстро отслеживать сбои в сети, сегменте сети или устройстве и принимать превентивные меры для предотвращения сбоя сетевых ресурсов. В то же время RMONMIB может также записывать данные о производительности сети и неисправностях, а также может в любое время получить доступ к

архивным данным для эффективной диагностики неисправностей. RMON сокращает коммуникационный трафик между менеджерами и агентами SNMP, позволяя сетевым администраторам просто и эффективно управлять большими сетями.

Принцип работы RMON (RMON working principle)

Агент RMON хранит сетевую информацию в RMONMIB. После того, как коммутатор помещается в агент RMON, он получает функцию обнаружения RMON. Администратор использует основные команды SNMP для обмена информацией данных с агентом RMON для сбора информации управления сетью. Однако из-за ограничения ресурсов устройства администратор не может получить все данные RMONMIB. Как правило, можно собрать только четыре группы информации: группа истории (historygroup), группа событий (eventgroup), группа статистики (statisticsgroup) и группа аварийных сигналов (alarmgroup).

Группы RMON
Данный коммутатор поддерживает группы истории (historygroup), событий (eventgroup), статистики (statisticsgroup) и группы аварийных сигналов (alarmgroup), как определено в спецификации RMON (RFC1757).

Группа RMON	Функция	Элемент
группы истории (history group)	Сетевая статистика периодически собирается и сохраняется для последующего извлечения для эффективного мониторинга сети.	Порт выборки, интервал, создатель
группы событий (event group)	Определяет номер события и способ его обработки. Определенные события в основном используются для событий, генерируемых триггером предупреждения в	Описание события, тип события, создатель, имя пользователя

	группе предупреждений.	
группы статистики (statistics group)	Отслеживает статистическое значение переменной аварийного сигнала на указанном порту.	Отбрасывание пакетов данных, отбрасывание байтов, передача пакетов данных, широковещательные пакеты данных, многоадресные пакеты данных, кадры ошибок CRC, слишком маленькие (или слишком большие) пакеты данных, фреймы коллизий и пакеты следующей длины: 64, 65 ~ 127, 128 ~ 255, 256 ~ 511, 512 ~ 1023 и 1024 ~ 10240 байт.
группы аварийных сигналов (alarmgroup)	Указанные аварийные переменные периодически контролируются, и аварийный сигнал запускается, когда счетчик превышает пороговое значение.	Переменная аварийного сигнала, тип выборки, временной интервал, верхний порог, нижний порог, триггер тревоги.

7.4.1 Группа событий (EventGroup)

Эта страница используется для настройки группы событий для RMON.

Как зайти на страницу: Advanced Manage>> RMON >> Event Group

Последовательный номер (Index) Отображает порядковый номер записи события.

Описание (Description) : Заполните описание события。

Тип (Type): Выберите тип события

none：нет необходимости.

log： Событие записывается в коммутаторе и считывается программным обеспечением управления SNMP.

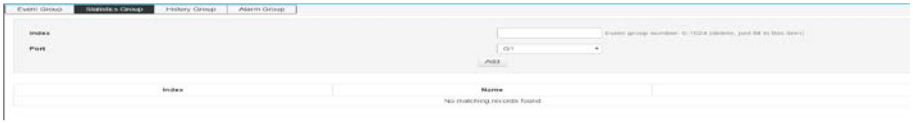
trap： Отправить аварийный сигнал на хост управления.

log&trap： Событие регистрируется в коммутаторе, и на управляющий хост отправляется аварийный сигнал.

7.4.2 Группа статистики (StatisticalGroup)

Эта страница используется для настройки группы статистики для RMON.

Как зайти на страницу: Advanced Settings >> RMON >> Statistics Group



Описание：

Настройка группы статистики

Последовательный номер Введите идентификационный номер статистической записи в диапазоне 1-

(Index) :	65535
Порт (Port) :	Введите или выберите порт Ethernet для подсчета.

7.4.3 Группа истории (HistoryGroup)

Эта страница используется для настройки группы статистики RMON.

Как зайти на страницу: Advanced Manage>> RMON >> History Group

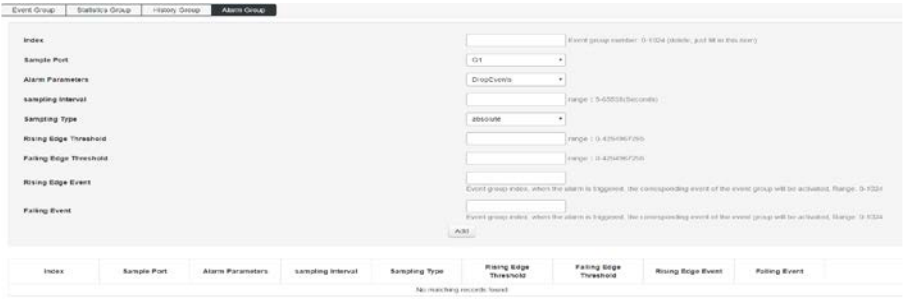
Описание :

Последовательный номер (Index) :	Отображает порядковый номер записи образца.
Порт выборки (Sampling port) :	Выберите порт для выборки.
Интервал выборки (Sampling interval) :	Введите интервал выборки порта. По умолчанию 1800 секунд.
Максимальное количество интервалов выборки (MaxSampleNumber) :	Отображает максимальное количество записей данных выборки, которые могут быть сохранены текущей записью управления историей. Диапазон составляет 1–100, по умолчанию — 50.

7.4.4 Группа аварийных сигналов (AlarmGroup)

Эта страница используется для настройки группы статистики RMON.

Как зайти на страницу: Advanced Manage>> RMON >> Alarm Group



номер (Index)	Отображает порядковый номер записи об аварийном сигнале.
порт выборки (sampling port)	Выбрать порт аварийных сигналов
параметрыаварийногосигнала (alarmparameters)	Выбрать переменную аварийного сигнала
интервал выборки (sampling interval)	Интервал, при котором заполняется поле аварийного сигнала. По умолчанию 1800 секунд.
Тип выборки (sample type)	Выберите метод выборки переменной аварийного сигнала и сравните полученное значение с пороговым значением. Абсолютный (absolute): Сравнивает результаты выборки непосредственно с порогом в конце периода выборки. Дельта (delta) : Прибавление после вычитания текущего значения сравнивается с порогом.
Порог роста (rising threshold)	Введите возрастающий порог, при котором сработал аварийный сигнал.

	По умолчанию 100
Событие превышения порога (risingevent)	Выберите порядковый номер события, которое вызвало аварийный сигнал о повышении порога.
Порог падения (fall threshold)	Введите порог падения, при котором сработал аварийный сигнал. По умолчанию 100.
Событие понижения (falling event)	Выберите порядковый номер события, вызвавшего аварийный сигнал о понижении порога.

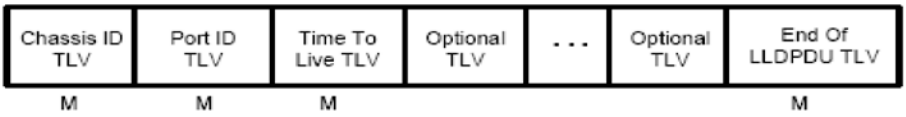
7.5 Конфигурация LLDP (LLDPConfiguration)

LLDP (LinkLayerDiscoveryProtocol) — это протокол уровня 2, который позволяет сетевым устройствам периодически объявлять информацию о своем собственном устройстве соседним устройствам в локальной сети, соответствующей стандарту IEEE 802. LLDP упорядочивает информацию об идентификации, производительности и конфигурации устройства в различные TLV в соответствии со стандартом IEEE802.1AB и инкапсулируется в блок данных протокола обнаружения канального уровня (LLDPDU). Блок данных протокола обнаружения объявляется соседнему устройству. После получения информации соседнее устройство сохраняет ее в виде стандартной MIB (ManagementInformationBase). Система управления сетью может получить эту информацию через протокол управления SNMP (простой протокол управления сетью), чтобы запросить и оценить состояние связи по каналу.Для описания физической топологии сети и связанных систем в топологии Инженерная группа Интернета (IETF) предложила стандартныйMIB, а некоторые компании предложили частные MIB. Однако сайты LANIEEE 802 не имеют единого стандарта для передачи информации MIB. LLDP решает эту проблему. Протокол LLDP позволяет сетевым устройствам разных производителей работать вместе. Устройства, на которых работает LLDP, могут автоматически обнаруживать и получать информацию о соседних устройствах. LLDP также позволяет системам, использующим разные протоколы сетевого уровня, узнавать информацию об устройствах друг друга. Приложения

SNMP могут использовать информацию, полученную LLDP, для устранения неполадок в сети, чтобы повысить стабильность сети и поддерживать правильную топологию сети.

LLDPDU

Каждый PDULLD несет четыре обязательных TLV и один или несколько дополнительных TLV. Как показано на рисунке ниже, ChassisTLVID, PortTLVID, TLVTTL и EndTLV— это четыре TLV, которые должны передаваться в каждом LLDPDU. Дополнительные TLV определяются системой управления сетью и предоставляют подробную информацию о локальных LLDP устройствах LLDP.



Максимальная длина LLDPDU определяется конкретной скоростью передачи и максимальной длиной сообщения, разрешенной протоколом. Что касается протокола MACIEEE 802.3, максимальная длина PDULLD— это максимальная длина базового фрейма MAC без тега, то есть 1500 байтов.

Рабочий механизм LLDP

1) Режим работы LLDP (LLDPOperatingmode)

Каждый порт может быть настроен с функциями приема и отправки LLDPDU, таким образом порт может быть настроен с четырьмя рабочими режимами:

- Sendandreceive: и отправка, и получение LLDPDU.
- Receiveonly: обрабатываются только полученные LLDPDU, LLDPDU не отправляются.
- Sendonly: только отправляет LLDPDU, но не обрабатывает полученные LLDPDU.
- Disabled: LLDPDU не отправляется или полученный LLDPDU не обрабатывается.

2) Механизм передачи LLDPDU

➢ Когда порт работает в режиме приема-передачи (transmit-receivemode) или в режиме только передачи (transmit-onlymode), устройство

периодически отправляет LLDPDU соседнему устройству для объявления своей собственной информации.

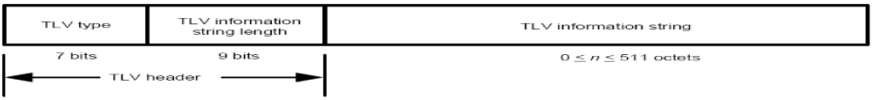
- Когда локальное устройство меняется, оно отправляет уведомление об изменении. Когда локальное устройство часто меняется в течение короткого периода времени, NMS (система управления сетью) устанавливает задержку передачи пакета, чтобы гарантировать отправку LLDPDU с фиксированной минимальной разницей во времени.
- Когда рабочий режим порта отключен или только режим приема переключается на режим отправки или получения или только в режим отправки, активируется механизм быстрого запуска устройства. Интервал отправки пакетов становится 1 с. После быстрой отправки нескольких LLDPDU устройство восстанавливает обычный цикл отправки.

3) Механизм получения LLDPDU

Когда порт работает в режиме передачи-приема или в режиме только приема, устройство проверяет достоверность полученных пакетов LLDP и передаваемых ими TLV. После проверки информация о соседях сохраняется локально и основана на TTL (TimeToLive). Значение TTL в TLV используется для установки времени устаревания информации о соседях на локальном устройстве. Если значение равно нулю, информация о соседях устарела.

TLV

TLV является основной единицей LLDPDU и является сокращением от Type/Length/Value, то есть типа/длины/значения. Формат базового TLVпоказан ниже:



Тип каждого TLV отличается. По типу TLV можно судить о типе информации в TLV.

В следующей таблице приведено подробное описание различных TLV, определенных в настоящее время.

Тип TLV	Название TLV	Описание	Обязательное поле
0	End LLDPDU	Определяет окончание LLDPDU. Любая информация после TLVEndOfLLDPDU будет отброшена.	Да
1	Chassis ID	Определяет идентификатор	Да

		шасси подключенного устройства	
2	Port ID	Определяет идентификационную информацию порта отправки	Да
3	Time To Live	Время устаревания информации о локальном устройстве на соседних устройствах	Да
4	Port description	Описание порта, указанное рабочей станцией IEEE 802 LAN, используемое для передачи этого порта соседу.	Нет
5	system name	Имя системы, используемое для публикации локального устройства для соседа.	Нет
6	system specification	Описание системной информации, используемой для публикации локального устройства для соседа, включая версию аппаратного и программного обеспечения системы.	Нет
7	system capability	Используется для публикации среди соседей функций, поддерживаемых локальным устройством, и того, разрешены ли они	Нет
8	management address	Используется для объявления соседу адреса управления локальным устройством. Протокол сетевого управления может управлять локальным устройством через адрес.	Нет
127	organizational definition	Позволяет различным организациям, производителям программного обеспечения и устройств определять TLV, которые отправляют информацию на соседние	Нет

		устройства.	

TLV обычно включают две категории: базовые TLV (basicTLVs) и организационно определенные TLV (organizationallydefinedTLVs).

1) Базовые TLV

Базовые TLV необходимы для реализации протокола LLDP, и они содержат основную информацию об управлении сетью.

2) Организационно определенные TLV

Различные организации определяют множество разных TLV.

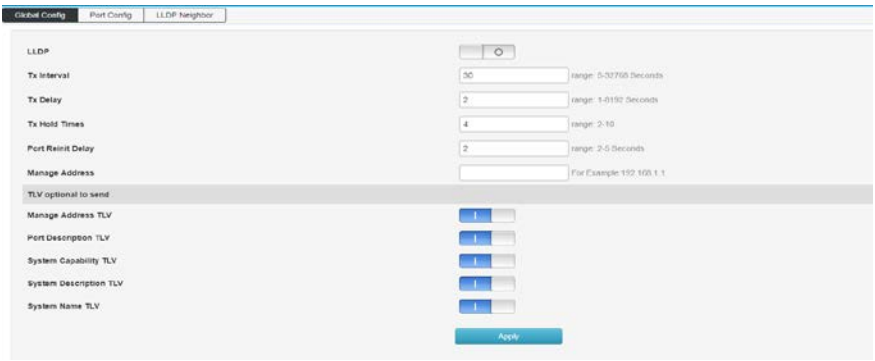
Идентификатор VLAN порта, идентификатор VLAN протокола, имя VLAN и идентификатор протокола TLV определяются IEEE 802.1.

Примечание:

Более подробная информация о TLV изложена в стандарте IEEE 802.1AB.

8.5.1 Глобальная конфигурация (GlobalConfiguration)

Чтобы настроить LLDP на коммутаторе, вам необходимо настроить глобальную функцию LLDP и соответствующие параметры на странице. Какзайтинастраницу: AdvancedManage>>LLDP>>GlobalConfiguration



Описание

Функция LLDP: Выберите, включить ли LLDP。

Период отправки пакета (Packetsendingperiod): настройте интервал времени, через который локальное устройство отправляет LLDPDU соседним устройствам.

Задержка (Delay):

Настройте задержку отправки локальным устройством LLDPDU соседям. Когда локальная конфигурация изменяется, LLDPDU отправляются на соседнее устройство в течение определенного времени, чтобы предотвратить непрерывную передачу LLDPDU при частых изменениях локальной конфигурации.

Множество сохранений информации об устройстве (Deviceinformationsavemultiple):

Множество сохранений информации об устройстве используется для управления значением поля TTL в LLDPDU, отправляемом локальным устройством. TTL— это время жизни локальной информации на соседнем устройстве. TTL = множитель TTL * интервал передачи.

Задержка инициализации (Initializationdelay):

При изменении рабочего режима LLDP порта, будет срабатывать задержка, а затем инициализация, чтобы предотвратить постоянную инициализацию порта при частых изменениях рабочего режима LLDP.

Адрес управления (Managementaddress):

Адрес управления устройством: по умолчанию 192.168.254.1

8.5.2 Конфигурация порта (PortConfiguration)

На этой странице вы можете настроить получение и отправку для всех портов.

Войдите на страницу: Advanced Manage>> LLDP Configuration >> Port Configuration.

7.5.3 Конфигурация порта (PortConfiguration)

На этой странице вы можете просмотреть информацию об устройстве LLDP рядом с вашим устройством.

Войдите на страницу: Advanced Manage>> LLDP Configuration>> LLDP Neighbours.

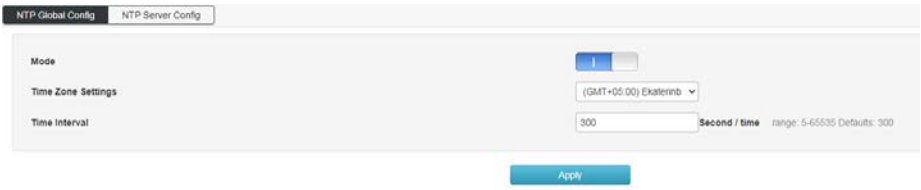
7.6 Конфигурация NTP (NTPConfiguration)

Эта страница используется для настройки системного времени коммутатора. Системное время — это время, в течение которого коммутатор работает. Информация о времени в других функциях (таких как контроль доступа) зависит от этого. Вы также можете выбрать синхронизацию с местным временем (SynchronizeLocalTime) в глобальной конфигурации, чтобы установить текущее время ПК управления в качестве системного времени коммутатора.

7.6.1 Глобальная конфигурация NTP (NTP Global configuration)

На этой странице вы можете установить глобальную информацию NTP.

Войдите на страницу: Advanced Manage>> NTP Configuration >> Global Configuration



Описание:

Режим (Mode) : Установите включение и выключение службы NTP.

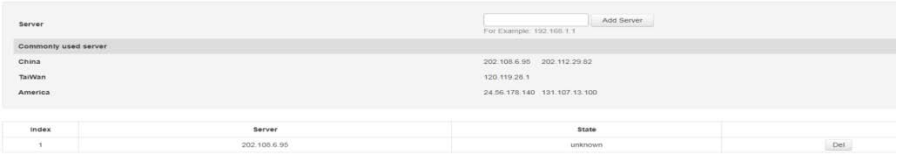
Настройка часового пояса (TimeZoneSettings): Выберите часовой пояс, в котором находится место синхронизации времени коммутатора.

Интервал времени (TimeInterval) : Период калибровки времени, по умолчанию 300 с.

7.6.2 Конфигурация сервера NTP (NTPserverconfiguration)

Вы можете вручную настроить адрес NTP-сервера на этой странице.

Как зайти на страницу: Advanced Settings >> NTP Configuration >> NTP server configuration



Описание

Сервер (server) Адрес сервера

Общий сервер (Commonserver) Рекомендуемый адрес общего сервера NTP

7.7 Защита от атак (Anti-attack)

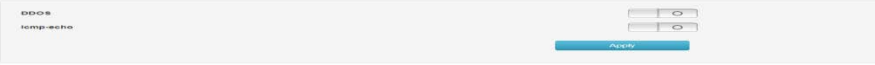
Модуль защиты от атак обеспечивает несколько мер безопасности для защиты безопасности локальной сети, включая модуль DDOS и модуль Icmp-echo.

DDoS

Предотвращает DDoS атаки.

ICMP

ICMP—InternetControlMessageProtocol.Это протокол набора протоколов TCP/IP для передачи управляющих сообщений между IP-узлами и маршрутизаторами. Управляющее сообщение относится к самой сети, например, сеть недоступна, хост доступен и маршрут доступен. Протокол ICMP чрезвычайно важен для сетевой безопасности. Характеристики самого протокола ICMP позволяют очень легко использовать его для атак на маршрутизаторы и хосты в сети. Он может использовать операционную систему, чтобы указать максимальный размер пакетов ICMP, не превышающий 64 КБ, и запустить «PingofDeath» для хоста, пинг-атаку. Принцип атаки «PingofDeath» заключается в следующем: если размер пакета ICMP превышает предел в 64 КБ, на хосте будет ошибка выделения памяти, что приведет к сбою стека TCP/IP, что приведет к сбою хоста. Кроме того, непрерывная отправка пакетов ICMP в больших количествах на целевой хост в течение длительного времени в конечном итоге приведет к параличу системы. Большое количество пакетов ICMP образует «шторм ICMP», который заставляет целевой хост потреблять много ресурсов ЦП, и он истощается.



Глава 8: Управление системой (SystemManagement)

8.1 Пользовательские настройки (UserSettings)

Эта страница используется для настройки идентификации пользователя, который входит на веб-страницу коммутатора. Если иное не указано в данной спецификации, веб-страницы «Администратор» имеют приоритет для входа в систему.

Как зайти на страницу: System Manage>> User Management

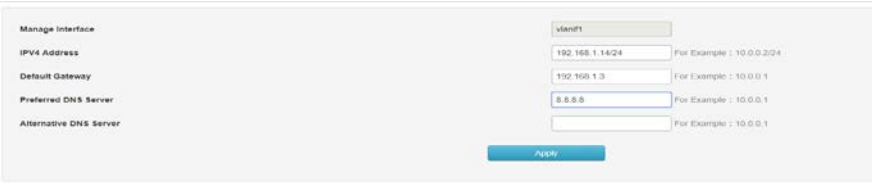
Учетная запись администратора (Administratoraccount):	Вы можете редактировать, изменять и просматривать конфигурацию каждой функции коммутатора.
Пароль (Password) :	Введите пароль для входа для этого имени пользователя.
Подтвердите пароль (Confirmpassword :	Введите пароль для входа в систему еще раз. Введенные пароли должны быть одинаковыми.

8.2 Настройки сети (Networksettings)

Эта страница используется для настройки IP-адреса управления коммутатором входа. Коммутатор уровня 2 также может быть настроен с использованием IP-адреса VLAN в качестве адреса управления.

Устройства в разных VLAN могут входить в коммутатор через IP-адрес VLAN для управления.

Как зайти на страницу: System Settings >> Network Settings



IP адрес (IP address)	Установите IP-адрес коммутатора. По

	умолчанию 192.168.254.1. Вы можете изменить это значение в соответствии с реальной сетью. Изменение адреса может быть передано внутри LAN. Маска подсети: установите маску подсети коммутатора. Значение по умолчанию — 24, которое можно изменить в соответствии с фактическими условиями сети.
Шлюз по умолчанию (Defaultgateway)	Когда вам нужно подключить коммутатор к Интернету, вам необходимо установить шлюз коммутатора по умолчанию. Вы можете указать текущий сетевой шлюз по умолчанию в соответствии с фактическими сетевыми условиями.

Предпочтительный DNS-сервер (PreferredDNS-server)Когда коммутатору необходимо получить доступ к доменному имени или связаться с адресом доменного имени, вам необходимо настроить сервер службы DNS коммутатора. Вы можете указать текущий адрес сетевого DNS-сервера в соответствии с текущими условиями сети.

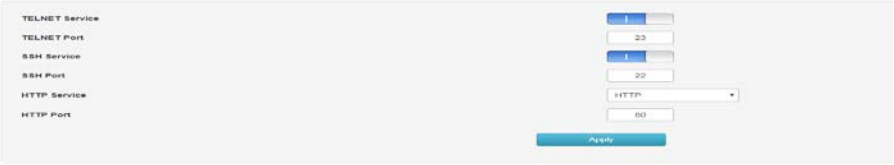
Альтернативный DNS-сервер (AlternativeDNS-server)Альтернативный DNS-сервер, текущая сеть может быть заполнена в соответствии с фактической сетью альтернативного DNS-сервера.

8.3 Конфигурация сервисов (Serviceconfiguration)

Функция конфигурации сервисов заключается в настройке соответствующего порта для различных режимов удаленного входа в систему для повышения безопасности коммутатора управления пользователями.

Эта функция включает конфигурацию TELNET, конфигурацию SSH, конфигурацию HTTP

Как зайти на страницу: System Settings >> Service Configuration

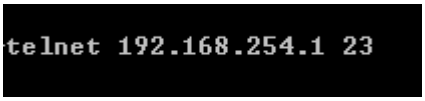


8.3.1 TELNET-сервис (TELNETservice)

Эта страница используется для включения или отключения Telnet на коммутаторе.

Порт TELNET (TELNETPort) После 23 изменений по умолчанию, необходимо увеличить номер порта при использовании команды Telnet

Формат (Format): Telnet 192.168.254.1 xx (где xx это порт)



8.3.2 SSH-сервис (SSHservice)

SSH (SecureShell) — это протокол безопасности, разработанный инженерной группой Интернета (IETF) на основе прикладного и транспортного уровня. Зашифрованное соединение SSH обеспечивает функциональность, аналогичную telnet-соединению, но традиционное удаленное управление telnet, по сути, небезопасно, поскольку оно находится в сети с использованием текстовых паролей и передачи данных, люди со скрытыми мотивами могут легко перехватить эти пароли и данные. При удаленном входе в устройство через сетевую среду, которая не может гарантировать безопасность, функция SSH может

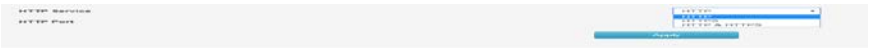
обеспечить надежное шифрование и безопасность аутентификации. Он может шифровать все передаваемые данные и эффективно предотвращать утечку информации во время удаленного управления. SSH состоит из сервера и клиента, и есть две несовместимые версии V1 и V2. Во время процесса связи сервер SSH и клиент автоматически согласовывают номер версии SSH и алгоритм шифрования. После достижения соглашения клиент инициирует запрос аутентификации для входа на сервер. После прохождения аутентификации две стороны могут обмениваться информацией. Коммутатор поддерживает функцию сервера SSH. Вы можете использовать клиентское программное обеспечение SSH для входа в коммутатор через SSH. Импорт ключа SSH предназначен для импорта файла открытого ключа SSH в коммутатор. Если ключ успешно импортирован, коммутатор будет использовать метод аутентификации ключа, чтобы принять вход по SSH.

Опция обслуживания SSH может выбрать, следует ли включать функцию SSH. Версия протокола по умолчанию —SSHv2.

Порт SSH (SSHport) Настройте порт входа по SSH. По умолчанию — 22. Этот элемент не рекомендуется.

8.3.3 HTTP-сервис (HTTPservice)

Сервис предоставляет три варианта протокола: HTTP, HTTPS, HTTP и HTTPS. По умолчанию —http. Вы можете вручную выбрать HTTPS и HTTP и HTTPS. Если используется протокол HTTPS, формат WEB-интерфейса будет https://192.168.254.1. Когда выбран протокол HTTP и HTTPS, пользователь может выбрать любой режим входа!



Описание:

Протокол HTTP (HTTPProtocol) :

HTTP (HyperTextTransferProtocol) позволяет пользователям управлять коммутаторами в браузере. Стандарт HTTP является результатом совместного исследования InternetEngineeringTaskForce и WorldWideWebConsortium. Этот элемент можно настроить для включения и отключения функции HTTP.

Порт HTTP (HTTPport) Порт по умолчанию — 80, его можно изменить в зависимости от реальной ситуации. После внесения изменений вам нужно снова добавить номер порта. Формат: 192.168.254.1:xx (xx - это измененный номер порта)

Протокол HTTPS (HTTPSProtocol)

SSL (SecureSocketsLayer) — это безопасный протокол, который обеспечивает безопасные соединения для протоколов уровня приложений на основе TCP, например, обеспечивает более безопасное соединение HTTPS для обычных соединений HTTP. Протокол SSL широко используется для аутентификации личности и передачи зашифрованных данных между веб-браузерами и серверами. Он используется в электронной коммерции, онлайн-банкинге и других областях для обеспечения безопасности передачи данных в сети.

Услуги, предоставляемые протоколом SSL, в основном включают:

1. Выполнение аутентификации на основе сертификатов для пользователей и серверов, чтобы гарантировать, что данные отправляются правильным пользователям и серверам;
2. Шифрование передаваемых данных, чтобы предотвратить кражу данных в середине;
3. Поддержка целостности данных и обеспечение отсутствия изменений во время передачи.

SSL использует технологию асимметричного шифрования для шифрования/дешифрования данных с использованием «пары ключей» (keypair), состоящей из открытого ключа (publickey, содержится в сертификате) и закрытого ключа (privatekey). Изначально коммутатор уже имеет сертификат по умолчанию (самоподписанный) и соответствующий закрытый ключ. Пара ключей по умолчанию также может быть заменена функцией импорта сертификата/ключа, но сертификат/ключ SSL должны быть объединены в пару и импортированы, иначе HTTPS не может быть подключен нормально.

После включения функции вы можете авторизоваться на веб-странице коммутатора через https://192.168.254.1. Когда вы входите в коммутатор через HTTPS в первый раз для использования сертификата коммутатора по умолчанию, браузер может выдать сообщение «Сертификат самоподписан, но не является надежным» (Thecertificateisself-signedwithoutbeingtrusted) или «Ошибка сертификата» (Certificateerror). В этом случае добавьте этот сертификат в качестве надежного сертификата или продолжайте просматривать веб-сайт без каких-либо изменений, оба варианта допустимы.

Порт HTTP (HTTPPort)Порт по умолчанию —443, его можно изменить в зависимости от реальной ситуации. После модификации вам нужно снова добавить номер порта. Формат 192.168.254.1: xx (xx -- это измененный номер порта)

8.4 Управление конфигурацией (Configurationmanagement)

С помощью программного сброса можно восстановить заводские настройки коммутатора, и все данные конфигурации будут удалены.

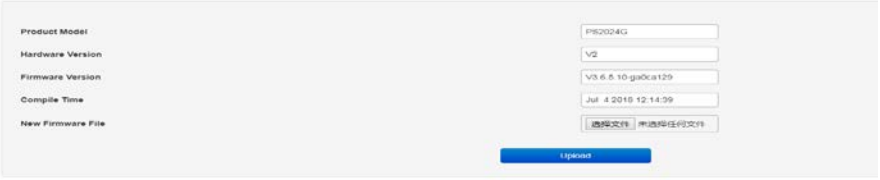
Как зайти на страницу: System Settings >> Configuration management

Примечание: После перезагрузки ПО настройки коммутатора вернутся к заводским и данные будут потеряны.

8.5 Обновление прошивки (Firmwareupgrade)

Коммутатор может обновлять системные файлы через Интернет. После обновления система увеличивает набор функций.

Как зайти на страницу: System Settings>> Firmware upgrade



Примечание:

Обновление прошивки может осуществляться только при помощи программного обеспечения соответствующей модели. Рекомендуется делать резервную копию настроек перед обновлением.

➢ При обновлении выберите программное обеспечение, совместимое с текущей версией оборудования.

Процесс обновления займет некоторое время, в течение которого устройство нельзя выключить, иначе устройство будет повреждено и его нельзя будет использовать.

8.6 Диагностический тест (Diagnostictest)

Коммутатор поддерживает три метода диагностики: пинг (pingdetection), трассировка (Tracertdetection) и обнаружение сетевого кабеля (networkcabledetection).

8.6.1 Пинг (Pingdetection)

Функция обнаружения пинга может определить, есть ли соединение с коммутатором и сетевым устройством, и удобно ли сетевому администратору проверять возможность подключения к сети и определять местонахождение неисправности сети.

Процесс обнаружения пинга выглядит следующим образом:

1) Коммутатор отправляет сообщение с запросом ICMP на целевое устройство.

2) Если сеть работает нормально, целевое устройство возвращает коммутатору пакет ответа ICMP после получения пакета, отображая соответствующую статистику.

3) Если сеть работает ненормально, исходное устройство будет отображать сообщение, например, о недоступности адреса назначения или тайм-ауте.

Как перейти на эту страницу: **System Settings >> Diagnostic Test >> Ping detection**

Описание :

Пинг (pingdetection)

IP Введите IP-адрес целевого узла, который вы хотите протестировать. Поддержка адресов IPv4 / IPv6。

8.6.2 Трассировка (Tracert detection)

Обнаружение Tracert может видеть маршрутизатор, через который коммутатор проходит к целевому узлу. Используйте эту команду для анализа неисправного сетевого узла, когда сеть выходит из строя.

Поле TTL включено в заголовок IP-пакета. Когда пакет пересылается в сети, значение каждого поля TTL маршрута уменьшается на единицу. Когда поле TTL полученного IP-пакета равно 0 или 1, маршрутизатор отбрасывает пакет и отвечает на сообщение тайм-аута ICMP источнику. Это эффективно предотвращает образование бесконечного потока пакетов в сети в случае сбоя сети.

Процесс обнаружения Tracert выглядит следующим образом:

1) Коммутатор отправляет пакет с TTL 1 на устройство назначения.

2) Первый переход (то есть первый маршрутизатор, на который приходит пакет) отвечает пакетом ICMP тайм-аута TTL (пакет содержит IP-адрес первого перехода), так что коммутатор получает адрес первого маршрутизатора.

3) Коммутатор повторно отправляет пакет с TTL 2 на устройство назначения.

4) Второй переход отвечает сообщением ICMP о тайм-ауте TTL, так что коммутатор получает адрес второго маршрутизатора;

5) Повторяйте описанный выше процесс до тех пор, пока целевое устройство не будет наконец достигнуто, и коммутатор не получит адреса всех маршрутизаторов, через которые он проходит к целевому устройству.。

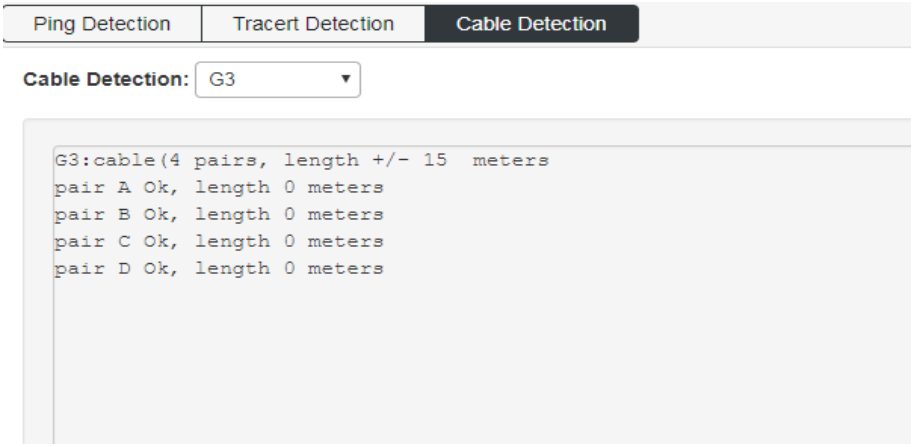
Как перейти на эту страницу: **System Manage>> Diagnostic test >>Tracert test**

8.6.3 Обнаружение сетевого кабеля (Networkcabledetection)

Функция обнаружения кабеля может определить, исправен ли кабель, подключенный к коммутатору, и поможет обнаружить место неисправности. Эта функция может использоваться для ежедневной диагностики инженерных систем.

Какперейтинаэтустраницу:

SystemManage>>Systemdiagnostics>>Cabledetection



Описание

Обнаружение сетевого кабеля (Networkcabledetection)

Порт (PortDetection) :	Выберите порт для тестирования кабеля.
Пара (Pair):	Показывает номер пары.
Статус линии (Line status) :	Проверьте состояние кабеля, подключенного к порту. Возможные состояния: нормальное, открытое. Кроме того, возможны ситуации, когда не поддерживается обнаружение или возникает сбой обнаружения. Обрыв цепи: обрыв в линии. Причины такой ситуации - плохой контакт кабеля. Также для определения места повреждения можно использовать оборудование для тестирования кабеля.
Длина линии (Line length) :	Если линия находится в нормальном состоянии, отображается диапазон длины кабеля.

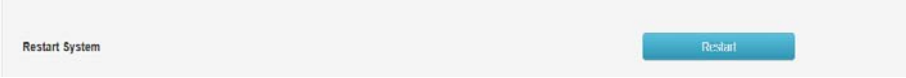
Примечание:

- До или после диагностики одного порта следует подождать в течение более трех секунд.
- Чем длиннее кабель, тем результат диагностики будет точнее.
- Тест дает приблизительное значение, возможна погрешность в 5-10 м, в отдельных случаях тест может не сработать.

8.7 Перезагрузка системы (Restart the system)

Здесь вы можете перезагрузить коммутатор и автоматически вернуться на страницу входа после перезапуска коммутатора. Перед перезапуском сохраните текущую конфигурацию. В противном случае несохраненная информация о конфигурации будет потеряна.

Как перейти на эту страницу: **System management >> Restart system**



Примечание: Во избежание повреждений не выключайте питание устройства во время его перезагрузки.